paloalto TECHDOCS

PAN-OS® 管理員指南

Version 11.0

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2022-2023 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

March 28, 2023

Table of Contents

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

開始使用

以下主題提供可幫助您部署 Palo Alto Networks 新一代防火牆的詳細步驟。其提供了如何將新防火牆整合至網路以及如何設定基本安全性原則的詳細資訊。有關如何繼續部署安全性平台功能以滿足您的網路安全性需求，請參閱完成防火牆部署的最佳做法。

- 將防火牆整合至管理網路
- 管理防火牆資源
- 使用介面與區域來分割網路
- 設定基本安全性原則
- 存取網路流量
- 啟用免費 WildFire 轉送
- 完成防火牆部署的最佳做法

將防火牆整合至管理網路

所有 Palo Alto Networks 防火牆都提供頻外管理連接埠 (MGT)，可用來執行防火牆的管理功能。在使用 MGT 連接埠後，您即可由資料處理功能中區隔防火牆的管理功能、保護防火牆存取和強化效能。在使用 Web 介面時，即使已計劃使用頻內資料連接埠來管理防火牆，您仍必須執行所有由 MGT 連接埠的初始組態工作。

某些管理工作 (例如，擷取授權和更新防火牆威脅及應用程式特徵碼) 需要存取網際網路。如果您不想啟用外部存取 MGT 連接埠，則需要設定頻內資料連接埠來提供存取必要外部服務（使用服務路由）或計劃定時手動上傳更新。

請勿透過網際網路或企業安全性界限內的其他不信任區域啟用管理介面的存取權。無論您是使用專用管理連接埠 *(MGT)*，還是將資料連接埠設定為管理介面，這一點均適用。將防火牆整合至管理網路時，請遵照管理存取權的最佳做法，來確保您可以保障防火牆以及其他安全性裝置的管理存取權，以防攻擊成功。

下列主題說明如何執行將新防火牆整合至管理網路並部署在基本安全性組態中的必要初始組態步驟。

- 確定業務連續性的存取策略
- 決定管理策略
- 執行初始組態
- 設定外部服務的網路存取權

下列主題說明如何將單一 *Palo Alto Networks* 新一代防火牆整合至網路。然而對於備援，需考慮在高可用性組態中部署一對防火牆。

確定業務連續性的存取策略

業務連續性計劃應包括在以下期間如何連接關鍵裝置（包括防火牆和 Panorama）的規定：在停電期間以及在發生無法透過正常通訊通道連接到這些裝置的其他事件期間。連接到頻外 (OOB) 網路上裝置並予以管理的功能，可讓您在主要網路中斷和電源斷電時繼續執行業務。業務連續性應該是網路架構的核心考量。

OOB 網路是遠端存取和管理裝置的安全方法，並且不使用主要通訊通道。相反地，*OOB* 網路會使用單獨的通訊通道，如果主要通道發生故障且使用與主要網路不同的電源，則這些通訊通道始終可用。根據網路架構，您可以同時使用主要網路和 *OOB* 網路來存取和管理日常操作中的裝置。

OOB 網路絕不應該依賴可能會與主要存取網路同時發生故障的電源或網路。如何設計對裝置的 OOB 存取權取決於您的網路架構和業務考量，因此沒有「一體通用」的方法來確保連線。但是，有一些指導方針可以協助您瞭解如何實現 OOB 存取網路的目標：

©2024 Palo Alto Networks, Inc.

- 電源考量：OOB 網路使用與一般存取網路不同的電源（單獨的電路、受保護的電源或電池供電的電源）。如果一般網路斷電，則 OOB 網路將不會斷電。

  使用配電裝置 (PDU) 控件遠端開關裝置電源。

- 安全連線方法—有許多方法可用於安全地連接到 OOB 網路，例如終端機伺服器裝置、數據機或序列主控台伺服器。您可以用於 OOB 存取的安全網路範例包括 LTE、撥號和寬頻（一般寬頻網路完全分離）網路。您使用的連線方法取決於您的業務需求和網路架構。

  無論您選取哪種方法，連線都必須安全，並具有強大的加密和驗證功能。請參閱管理存取權的最佳做法，以取得如何保護與防火牆和 Panorama 之管理連線的建議。

  您可以透過乙太網路 LAN 使用採用增強式驗證的 SSH 遠端連接到 OOB 網路，也可以透過序列連線撥入。輸出連線將是序列連線。

決定管理策略

Palo Alto Networks 防火牆可在本機設定及管理，或者可集中使用 Panorama 進行管理，即 Palo Alto Networks 中央安全管理系統。如果您在網路中部署六個以上的防火牆，請使用 Panorama 實現下列優勢：

- 減少管理設定、原則、軟體及動態內容更新的複雜度與管理負荷。您可以使用 Panorama 上的裝置群組及範本在本機防火牆上有效管理防火牆特定組態，並強制所有防火牆或裝置群組共享原則。
- 彙總所有管理防火牆的資料及取得網路所有流量的可見度。Panorama 上的應用程式控管中心 (ACC) 提供單一透明窗格的所有防火牆統一報告，可讓您集中分析、調查和報告網路流量、安全性事件與管理修改。

接下來的程序說明如何使用本機網頁介面來管理防火牆。如果您想要使用 Panorama 進行中央管理，請先執行初始組態，並確定防火牆能夠與 Panorama 建立連線。之後您便能使用 Panorama 集中設定防火牆。

執行初始組態

依預設，PA 系列防火牆的 IP 位址為 192.168.1.1，且使用者名稱/密碼為 admin/admin。基於安全因素，您必須在繼續設定其他的防火牆設定前變更這些設定。即使未計劃使用此介面進行防火牆管理，您必須由 MGT 介面中執行這些設定工作，或者使用防火牆上的直接序列連線至主機連接埠。

STEP 1 | 安裝防火牆並接通電源。

如果防火牆型號具有雙電源，請連接第二個電源以實現備援。如需詳細資料，請參閱型號的硬體參考指南。

©2024 Palo Alto Networks, Inc.

STEP 2 | 從網路管理員收集必要資訊。

- MGT 連接埠的 IP 位址
- 網路遮罩
- 預設閘道
- DNS 伺服器位址

STEP 3 | 將電腦連接至防火牆。

您可使用下列其中一個方法連接至防火牆：

- 從電腦中將序列纜線連接至主控台連接埠，然後使用終端模擬軟體連接至防火牆 (9600-8-N-1)。等候幾分鐘待開機序列完成；防火牆準備就緒後，會出現變更防火牆名稱的提示，例如 `PA-220 login`。
- 從電腦將 RJ-45 乙太網路 纜線連接至防火牆上的 MGT 連接埠。在瀏覽器中移至 **`https://192.168.1.1`**。

> 您可能需要將電腦上的 *IP* 位址變更為 *192.168.1.0/24* 網路中的位址（例如 *192.168.1.2*）才可存取此 *URL*。

STEP 4 | 出現提示時，登入防火牆。

您必須使用預設使用者名稱與密碼 (admin/admin) 登入。防火牆將開始初始化。

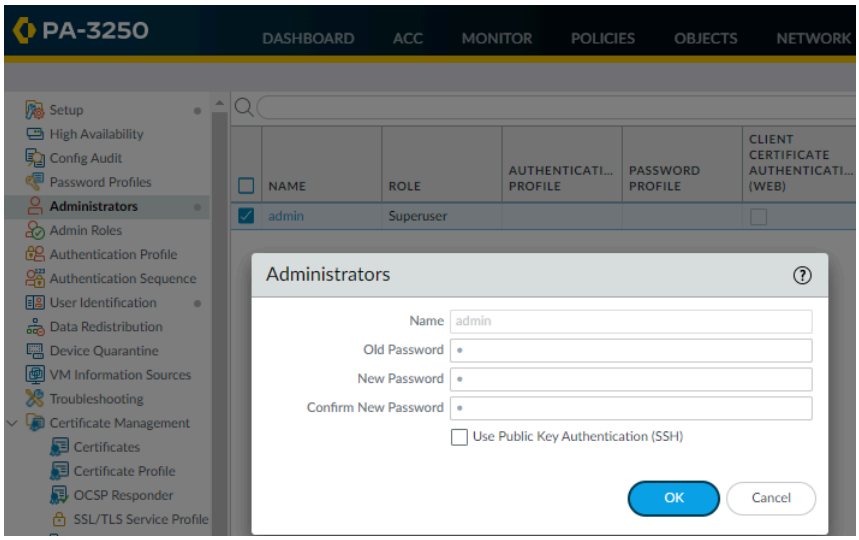
©2024 Palo Alto Networks, Inc.

STEP 5 | 為管理員帳戶設定安全的使用者名稱和密碼。

從 *PAN-OS 9.0.4* 開始，第一次登入裝置時必須變更預定義的預設密碼 *(admin)*。新密碼至少必須包含八個字元，並且包含至少一個小寫字母與一個大寫字母，以及一個數字與特殊字元。雖然您不是一定要設定新的使用者名稱，但最佳做法是這樣做，並為每個管理員使用唯一的使用者名稱和密碼。從 *PAN-OS 10.2* 開始，登入必須包含至少一個字母字元或符號（底線、句點或連字號，但連字號不能是使用者名稱中的第一個字元），並且不能僅為數字。

務必採用密碼強度最佳做法 以確保嚴格的密碼，並檢閱密碼複雜性設定。

1. 選取 **Device**（裝置） > **Administrators**（管理員）。
2. 選取 **admin**（管理員）角色。
3. 輸入目前的預設密碼及新密碼。



4. 按一下 **OK**（確定）來儲存設定。

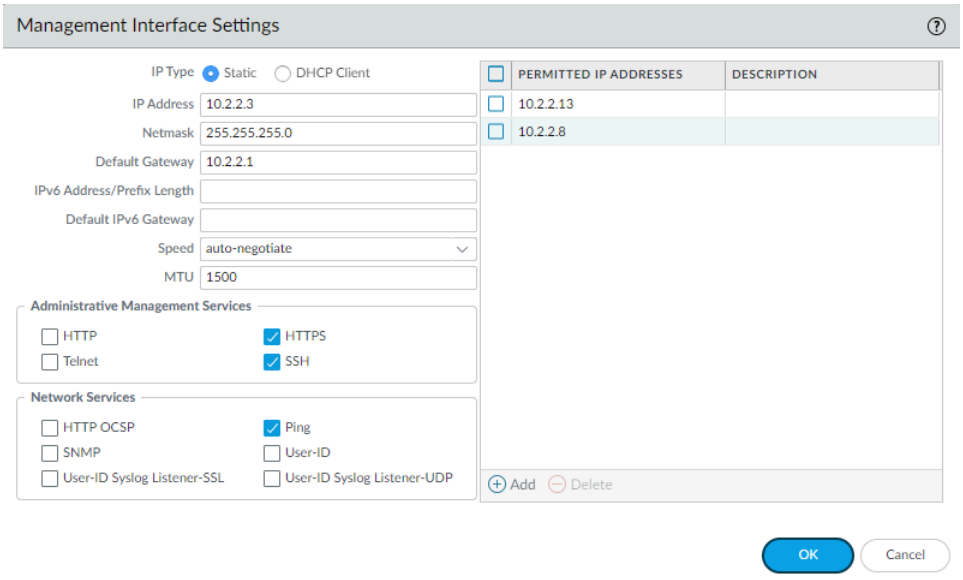
©2024 Palo Alto Networks, Inc.

STEP 6 | 設定 MGT 介面。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Interfaces**（介面），然後編輯 **Management**（管理） 介面。
2. 使用下列其中一種方法設定 MGT 介面的位址設定：
   - 若要對 MGT 介面進行靜態 IP 位址設定，請將 **IP Type**（**IP** 類型）設定為 **Static**（靜態）並輸入 **IP Address**（**IP** 位址）、**Netmask**（網路遮罩）及 **Default Gateway**（預設閘道）。
   - 若要以動態方式設定 MGT 介面位址設定，請將 **IP Type**（**IP** 類型）設定為 **DHCP Client**（**DHCP** 用戶端）。若要使用此方法，您必須將管理介面設定為 DHCP 用戶端。

   若要避免管理介面的未經授權存取，管理最佳做法為 ***Add***（新增）管理員可從中存取 *MGT* 介面的 ***Permitted IP Addresses***（允許的 ***IP*** 位址）。
3. 將 **Speed**（速度）設定為 **auto-negotiate**。
4. 選取介面上允許的管理服務。

   確定未選取 ***Telnet*** 及 ***HTTP***，因為相較於其他服務，這些服務會使用較不安全的明文並影響管理員認證。



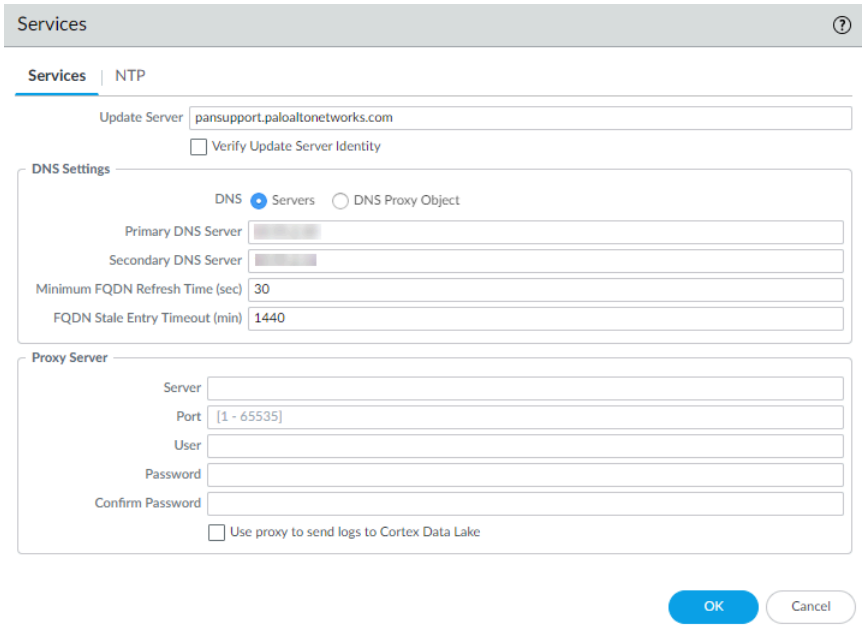
5. 按一下 **OK**（確定）。

©2024 Palo Alto Networks, Inc.

STEP 7 | 設定 DNS、更新伺服器以及 Proxy 伺服器設定。

您必須在防火牆上手動設定至少一個 *DNS* 伺服器，否則將無法解析主機名稱；其不會使用其他來源的 *DNS* 伺服器設定，例如 *ISP*。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Services**（服務）。
   - 針對多個虛擬系統平台，選取 **Global**（全域）並編輯服務區段。
   - 針對單一虛擬系統平台，編輯服務區段。
2. 在 **Services**（服務）頁籤上，為 **DNS** 選取下列選項之一：
   - 伺服器—輸入 **Primary DNS Server**（主要 **DNS** 伺服器） 位址與 **Secondary DNS Server**（次要 **DNS** 伺服器）位址。
   - **DNS Proxy** 物件—從下拉式清單中，選取您想要用來設定全域 DNS 服務的 **DNS Proxy**，或是按一下 **DNS Proxy** 以設定新的 DNS Proxy 物件。

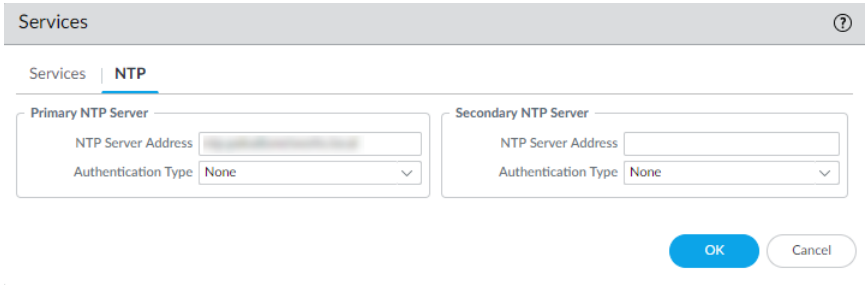


3. 按一下 **OK**（確定）。

©2024 Palo Alto Networks, Inc.

STEP 8 | 設定日期與時間 (NTP) 設定。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Services**（服務）。
   - 針對多個虛擬系統平台，選取 **Global**（全域）並編輯服務區段。
   - 針對單一虛擬系統平台，編輯服務區段。
2. 在 **NTP** 頁籤上，若要在網際網路上使用時間伺服器的虛擬叢集，請輸入主機名稱 `pool.ntp.org` 作為 **Primary NTP Server**（主要 **NTP** 伺服器）或輸入您主要 NTP 伺服器的 IP 位址。



3. （選用）輸入 **Secondary NTP Server**（次要 **NTP** 伺服器）位址。
4. （選用）若要驗證 NTP 伺服器的時間更新，為每個伺服器選取下列的 **Authentication Type**（驗證類型）：
   - 無—（預設）停用 NTP 驗證。
   - 對稱金鑰—防火牆使用對稱金鑰交換 (共用密碼）來驗證時間更新。
     - 金鑰 **ID**—輸入金鑰 ID (1-65534)。
     - 演算法—選取在 NTP 驗證中要使用的演算法（**MD5** 或 **SHA1**）。
   - **Autokey**—防火牆使用 Autokey (公開金鑰密碼編譯) 來驗證時間更新。
5. 按一下 **OK**（確定）。

STEP 9 | （選用）根據需要設定一般防火牆設定。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理），然後編輯 General Settings（一般設定）。
2. 輸入防火牆的 **Hostname**（主機名稱），然後輸入網路的 **Domain**（網域）名稱。網域名稱只是一種標籤；不會用於加入網域。
3. 輸入 **Login Banner**（登入橫幅）文字，告知即將登入的使用者，他們需要獲得授權才可存取防火牆管理功能。

   最佳做法是，避免使用歡迎措辭。此外，您應當請法務部門檢閱橫幅訊息，確保該訊息顯示禁止未經授權存取的適當警告。
4. 輸入 **Latitude**（緯度）和 **Longitude**（經度）以在世界地圖上啟用精確的防火牆位置。
5. 按一下 **OK**（確定）。

©2024 Palo Alto Networks, Inc.

STEP 10 | Commit（提交）您的變更。

儲存組態變更後，會與 *Web* 介面中斷連線，因為 *IP* 位址已變更。

按一下 Web 介面右上方的 **Commit**（提交）。防火牆會花費最多 90 秒的時間來儲存變更。

STEP 11 | 將防火牆連線至網路。

1. 中斷防火牆與電腦的連線。
2. （除 PA-5450 以外的所有防火牆）使用 RJ-45 乙太網路纜線將 MGT 連接埠連線至管理網路上的交換機連接埠。確定您以纜線連接至防火牆的交換器連接埠設定為自動交涉。
3. （僅適用於 PA-5450）使用 Palo Alto Networks 認證的 SFP/SFP+ 收發機和纜線將 MGT 連接埠連線至管理網路上的交換機連接埠。

STEP 12 | 開啟防火牆的 SSH 管理工作階段。

使用終端模擬軟體 (例如 PuTTY) 時，請使用您為其指定的新 IP 位址來啟動防火牆的 SSH 工作階段。

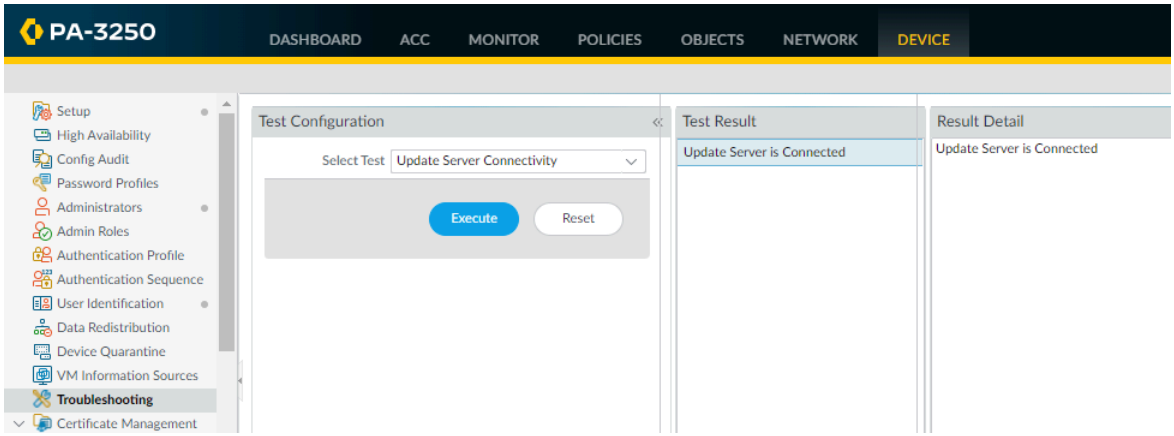
©2024 Palo Alto Networks, Inc.

STEP 13 | 驗證執行防火牆管理所需要的外部服務之網路存取權，例如 Palo Alto Networks 更新伺服器。

您可使用下列其中一種方法執行此操作：

- 如果您不想要允許外部網路存取 MGT 介面，則需要設定資料連接埠擷取必要的服務更新。繼續設定外部服務的網路存取權。
- 如果您計劃允許外部網路存取 MGT 介面，請確認您具有連線，然後繼續註冊防火牆並啟動訂閱授權。

1. 使用更新伺服器連線測試來確認與 Palo Alto Networks 更新伺服器的網路連線，如下列範例所示：
   1. 選取 **Device**（裝置） > **Troubleshooting**（疑難排解），然後從選取測試下拉式清單中選取 **Update Server Connectivity**（更新伺服器連線）。
   2. **Execute**（執行）更新伺服器連線測試。



2. 使用以下 CLI 命令，從 Palo Alto Networks 更新伺服器擷取 防火牆支援權利的相關資訊：

```
request support check
```

如果您可以連線，則更新伺服器將回應防火牆的支援狀態。如果防火牆尚未註冊，更新伺服器將傳回以下訊息：

```
聯絡我們 https://www.paloaltonetworks.com/company/contact-
us.html Support Home https://www.paloaltonetworks.com/support/
tabs/overview.html 在此更新伺服器上找不到裝置
```

設定外部服務的網路存取權

依預設，防火牆會使用 MGT 介面來存取遠端服務，例如 DNS 伺服器、內容更新及授權擷取。如果您不想讓外部網路存取您的管理網路，必須設定頻內資料連接埠，以存取所需的外部服務，並設定服務路由，通知防火牆使用哪個連接埠來存取外部服務。

請勿透過網際網路或企業安全性界限內的其他不信任區域啟用管理存取。請遵照管理存取權的最佳做法，以確保您正確保護防火牆。

©2024 Palo Alto Networks, Inc.

此工作需要熟悉防火牆介面、區域及原則。關於這些主題的詳細資訊，請參閱設定介面和區域以及設定基本安全性原則。

STEP 1 | 決定要用於存取外部服務的介面，並將其連線至交換器或路由器連接埠。

您使用的介面必須有靜態 IP 位址。

STEP 2 | 登入網頁介面。

在網頁瀏覽器中使用安全連線 (HTTPS)，使用您在初始設定期間指派的新 IP 位址及密碼登入 (https://<IP address>)。您將看見憑證警告；此為正常現象。繼續開啟網頁。

STEP 3 | （選用）防火牆會以連接埠 Ethernet 1/1 和 Ethernet 1/2（及對應的預設安全性原則與區域）之間的預設虛擬連接介面預先設定。如果您不打算使用此虛擬介接設定，則必須手動刪除此設定，以防止干擾您定義的其他介面設定。

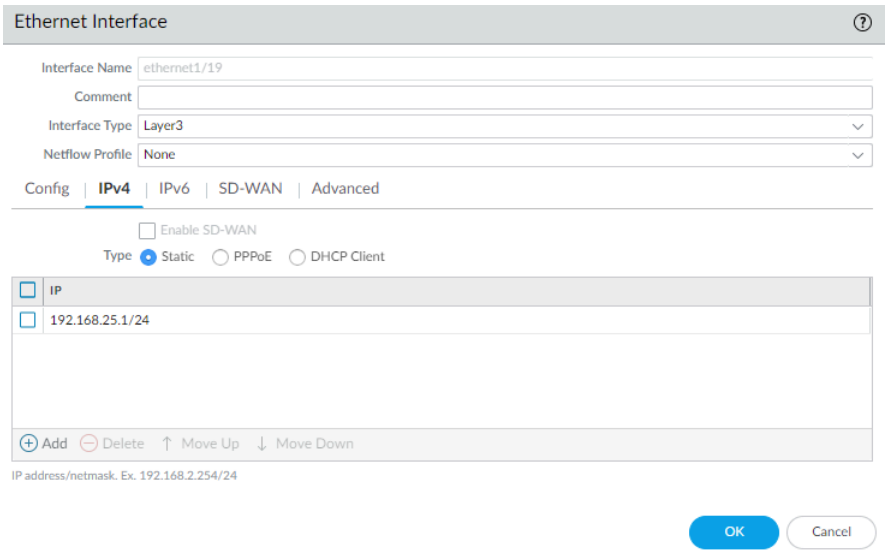
您必須依下列順序刪除組態：

1. 若要刪除預設安全性原則，則選取 **Policies**（原則） > **Security**（安全性），選取規則，然後按一下 **Delete**（刪除）。
2. 若要刪除預設 Virtual Wire，則選取 **Network**（網路） > **Virtual Wires**，然後選取 Virtual Wire 並按一下 **Delete**（刪除）。
3. 若要刪除預設信任及不信任區域，則選取 **Network** > **Zones**，然後選取每個區域並按一下 **Delete**（刪除）。
4. 若要刪除介面組態，選取 **Network**（網路） > **Interfaces**（介面），然後選取每個介面（ethernet1/1 和 ethernet1/2）並按一下 **Delete**（刪除）。
5. **Commit**（提交）變更。

©2024 Palo Alto Networks, Inc.

STEP 4 | 設定您計劃用於從外部存取管理服務的介面。

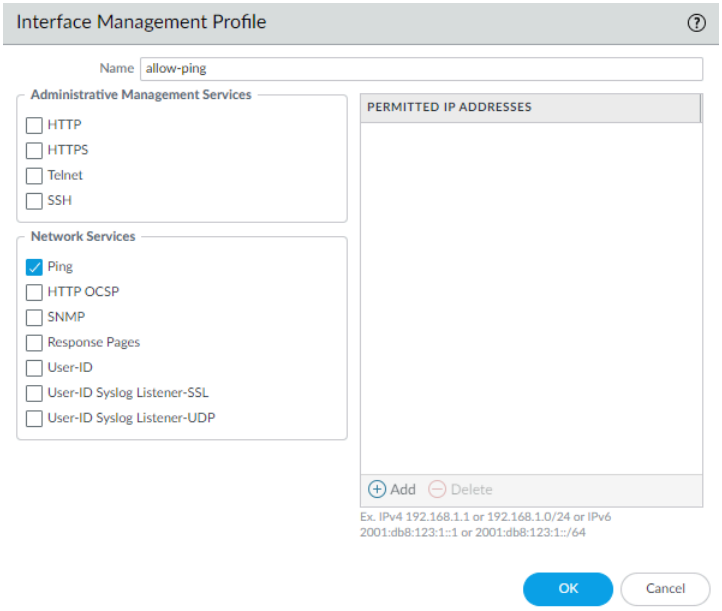
1. 選取 **Network**（網路） > **Interfaces**（介面），然後選取對應步驟 1 中所連線之介面的介面。
2. 選取 **Interface Type**（介面類型）。雖然您在此的選擇需視網路拓撲而定，但此範例說明 **Layer3** 的步驟。
3. 在 **Config**（設定）頁籤上，展開 **Security Zone**（安全性區域）下拉式清單並選取 **New Zone**（新增區域）。
4. 在 Zone（區域）對話方塊中，輸入新區域的 **Name**（名稱），例如管理，然後按一下 **OK**（確定）。
5. 選取 **IPv4** (IPv4) 頁籤，選取 **Static**（靜態）選項按鈕，在 IP 區段中按一下 **Add**（新增），然後輸入 IP 位址及網路遮罩以指定至介面，例如 192.168.1.254/24。您必須使用此介面上的靜態 IP 位址。



6. 選取 **Advanced**（進階） > **Other Info**（其他資訊），展開 **Management Profile**（管理設定檔）下拉式清單，然後選取 **New Management Profile**（新增管理設定檔）。
7. 輸入設定檔的 **Name**（名稱），例如 allow_ping，然後選取要在介面上允許的服務。若要允許存取外部服務，您可能只需要啟用 **Ping** (偵測)，然後按一下 **OK**（確定）。

©2024 Palo Alto Networks, Inc.

這些服務可提供防火牆的管理存取權，因此只能選取對應要在介面上允許的管理活動服務。例如，不要啟用 *HTTP* 或 *Telnet*，因為這些通訊協定以明文傳輸，因此不安全。或者，如果您打算透過 *Web* 介面或 *CLI* 將 *MGT* 介面用於防火牆組態工作，則不應啟用 *HTTP*、*HTTPS*、*SSH* 或 *Telnet*，以防止透過此介面未經授權的存取 (若在此情況下，您必須允許 *HTTPS* 或 *SSH*，則應限制 ***Permitted IP Addresses***（許可的 ***IP*** 位址）特定組合的存取)。如需詳細資訊，請參閱U使用介面管理設定檔限制存取。



8. 若要儲存介面設定，請按一下 **OK**（確定）。

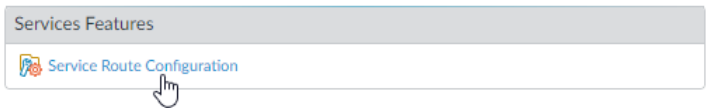
©2024 Palo Alto Networks, Inc.

STEP 5 | 設定服務路由。

依預設，防火牆在其需要時使用 MGT 介面來存取外部服務。若要變更防火牆用於傳送請求至外部服務的介面，您必須編輯服務路由。

此範例顯示設定全域服務路由的方式。如需在虛擬系統而非全域上設定外部服務的網路存取，請參閱自訂虛擬系統服務的服務路由。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Services**（服務） > **Global**（全域），然後按一下 **Service Route Configuration**（服務路由組態）。



若要啟動授權及取得最新內容和軟體更新，您必須變更 ***DNS***、***Palo Alto Networks Services***（***Palo Alto Networks*** 服務）、***URL Updates***（***URL*** 更新）及 ***WildFire*** 的服務路由。

2. 按一下 **Customize**（自訂）選項按鈕並選取下列一個選項：

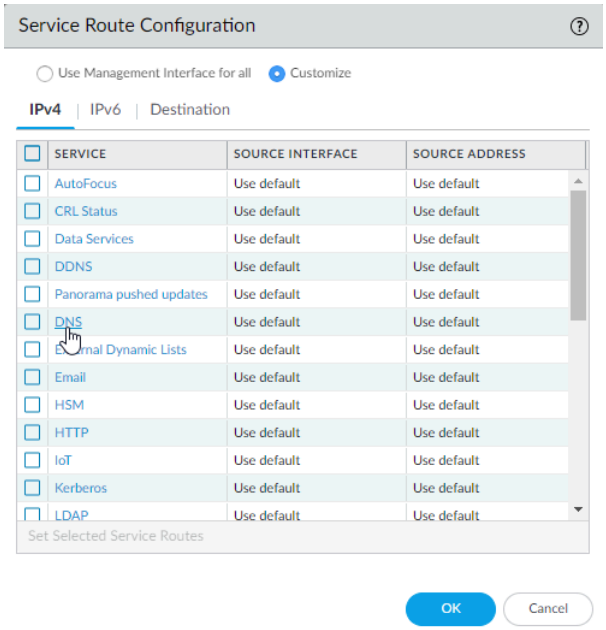
   - 對於預先定義的服務，選取 **IPv4** 或 **IPv6**，並按一下服務的連結。若要限制來源位址的下拉式清單，可選取 **Source Interface**（來源介面），然後選取您剛剛設定的介面。然後（從該介面）選取 Source Address（來源位址），作為服務路由。

     若為選取的介面設定多個 IP 位址，**Source Address**（來源位址）下拉式清單可讓您選取某個 IP 位址。

   - 若要建立自訂目的地的服務路由，請選取 **Destination**（目的地），再按一下 **Add**（新增）。請輸入 **Destination**（目的地）IP 位址。帶有目的地位址的傳入封包若符合此位址，則將作為您為此服務路由所指定的來源位址來源。若要限制來源位址下拉式清

©2024 Palo Alto Networks, Inc.

單，請選取 **Source Interface**（來源介面）。若為選取的介面設定多個 IP 位址，**Source Address**（來源位址）下拉式清單可讓您選取某個 IP 位址。



3. 按一下 **OK**（確定）以儲存設定。
4. 針對每個要修改的服務路由重複以上的步驟 5.2-5.3。
5. **Commit**（提交）您的變更。

STEP 6 | 設定對外介面及關聯區域，然後建立安全性原則規則，以允許防火牆從內部區域將服務要求傳送至外部區域。

1. 選取 **Network**（網路）> **Interfaces**（介面），然後選取對外介面。選取 **Layer3** 作為 **Interface Type**（介面類型）、**Add**（新增）**IP** 位址（位於 **IPv4** 或 **IPv6** 頁籤），並建立關聯的 **Security Zone**（安全性地區）（位於 **Config**（組態）頁籤），例如網際網路。此介面必須具有靜態 IP 位址；您不需要在此介面上設定管理服務。
2. 若要設定允許內部網路至 Palo Alto Networks 更新伺服器流量的安全性規則，可選取 **Policies**（原則）> **Security**（安全性），然後按一下 **Add**（新增）。

最佳做法是，建立安全性規則時，使用基於應用程式的規則而非基於連接埠的規則，無論使用中的連接埠、通訊協定、規避策略會加密技術如何，都能確保準確識別基礎應用程式。務必將 ***Service***（服務）設定為 ***application-default***（應用程式預設值）。在此情況下，建立允許存取更新伺服器（及其他 *Palo Alto Networks* 服務）的安全性原則規則。

	NAME	Source ZONE	Destination ZONE	APPLICATION	SERVICE	ACTION
1	Palo Alto Networks Services	Management	Internet	paloalto-dns-security paloalto-logging-service paloalto-updates paloalto-wildfire-cloud	application-...	Allow

©2024 Palo Alto Networks, Inc.

STEP 7 | 建立 NAT 原則規則。

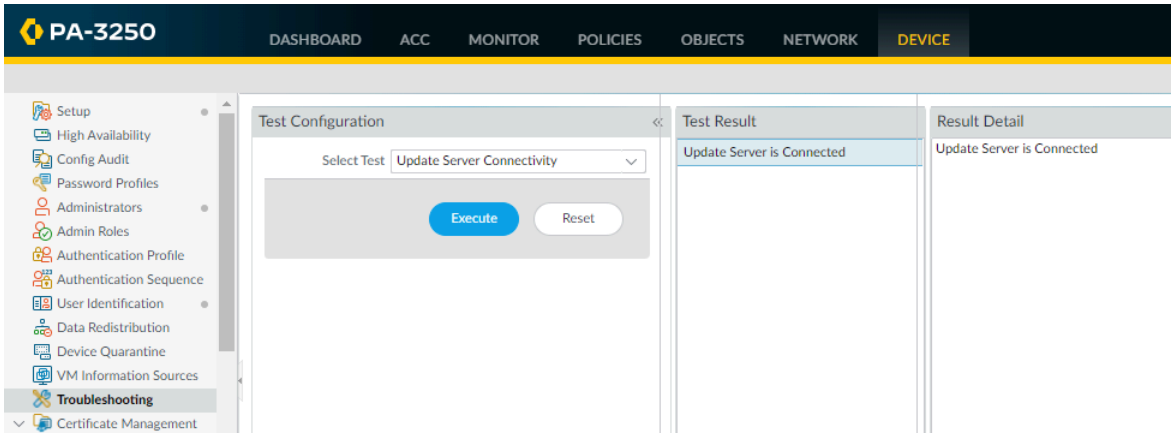
1. 如果您在對內介面上使用私人 IP 位址，則您需要建立來源 NAT 規則以將位址轉譯為可公開路由的位址。選取 **Policies**（原則）> **NAT**，然後按一下 **Add**（新增）。您至少必須定義規則的名稱（**General**（一般）頁籤），指定來源及目的地區域（在此情況下為管理至網際網路）（**Original Packet**（原始封包）頁籤），並定義來源位址轉譯設定（**Translated Packet**（轉譯的封包）頁籤），然後按一下 **OK**（確定）。
2. **Commit**（提交）您的變更。

		Original Packet			Translated Packet	
	NAME	SOURCE ZONE	DESTINATION ZONE	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
1	Source NAT	Management	Internet	any	dynamic-ip-and-port	none

STEP 8 | 選取 **Device**（裝置）> **Troubleshooting**（疑難排解），並使用 **Ping** 連線測試，驗證資料連接埠與外部服務的連線，包括預設閘道，並使用 **Update Server Connectivity**（更新伺服器連線）測試來驗證 Palo Alto Networks 更新伺服器的網路連線。在此範例中，測試了防火牆與 Palo Alto Networks 更新伺服器的連線。

確認您已建立所需的網路連線後，繼續註冊防火牆並啟動訂閱授權。

1. 從選取測試下拉式清單中選取 **Update Server**（更新伺服器）。
2. **Execute**（執行）Palo Alto Networks 更新伺服器連線測試。



3. 存取防火牆 CLI，並使用以下命令，從 Palo Alto Networks 更新伺服器擷取防火牆支援權利的相關資訊：

```
request support check
```

如果您可以連線，則更新伺服器將回應防火牆的支援狀態。由於防火牆未註冊，更新伺服器將傳回以下訊息：

```
聯絡我們 https://www.paloaltonetworks.com/company/contact-us.html Support Home https://www.paloaltonetworks.com/support/tabs/overview.html 在此更新伺服器上找不到裝置
```


©2024 Palo Alto Networks, Inc.

管理防火牆資源

- 註冊防火牆
- 管理硬體耗用
- 解除委任防火牆

註冊防火牆

在您啟動支援及其他授權與訂閱之前，您首先必須註冊防火牆。但是，在註冊防火牆之前，必須先擁有一個使用中的支援帳戶。根據您是否擁有使用中的支援帳戶，執行以下其中一項工作：

- 若沒有作用中的支援帳戶，則建立新的支援帳戶並註冊防火牆。
- 若已擁有作用中的支援帳戶，則將備妥註冊防火牆。
- 註冊防火牆上的 （選用）執行第 1 天組態。
- 如果您的防火牆使用 NPC（網路處理卡）之類的線路卡，則 註冊防火牆線路卡。

如果您正在註冊 VM 系列防火牆，請參閱 《VM 系列部署指南》 獲取相關說明。

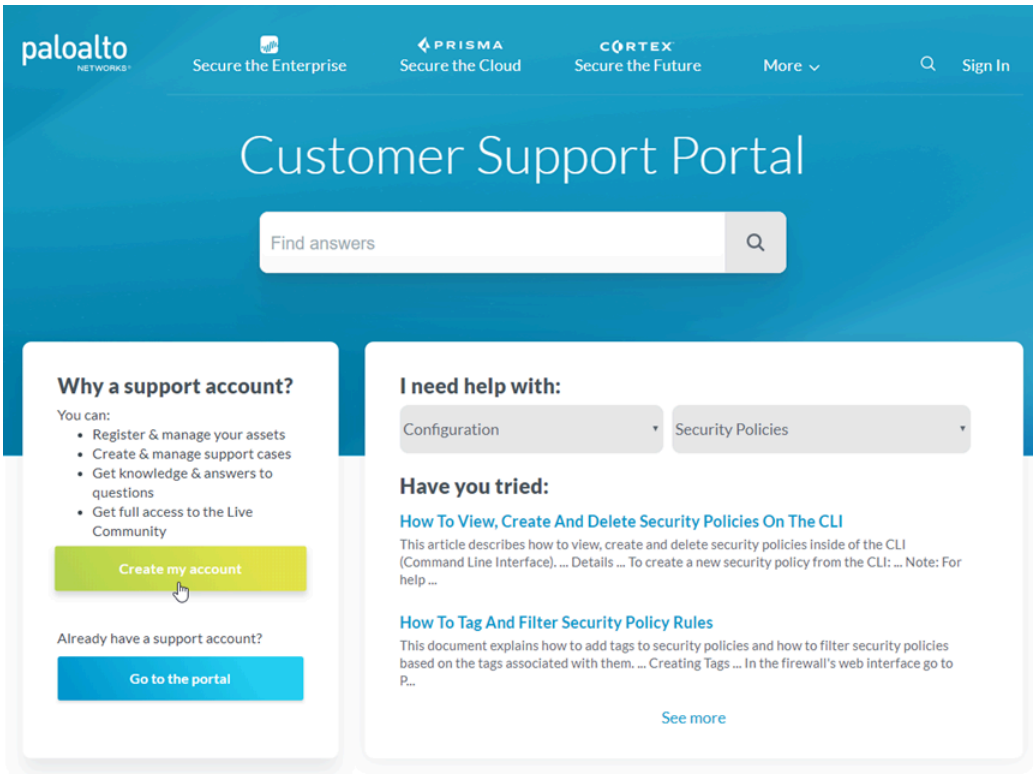
建立新的支援帳戶並註冊防火牆

若還沒有使用中的 Palo Alto Networks 支援帳戶，則需要在建立新支援帳戶時註冊防火牆。

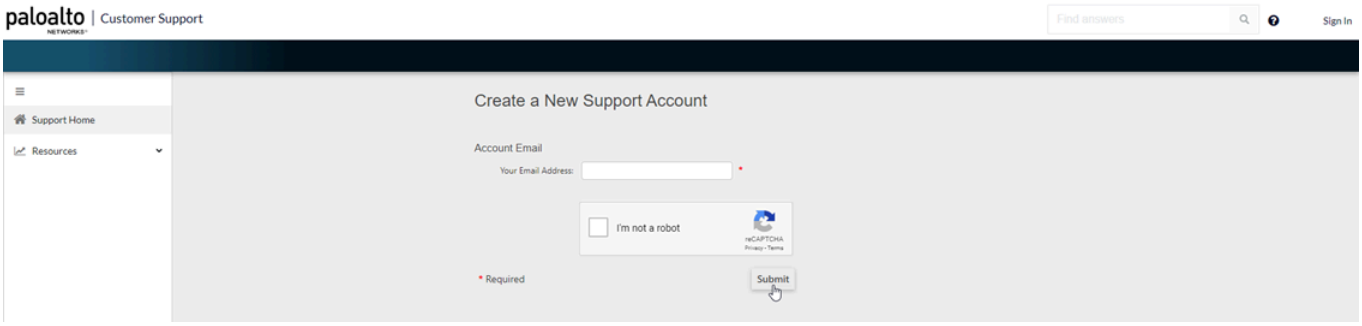
STEP 1 | 移至 Palo Alto Networks 客戶支援入口網站。

©2024 Palo Alto Networks, Inc.

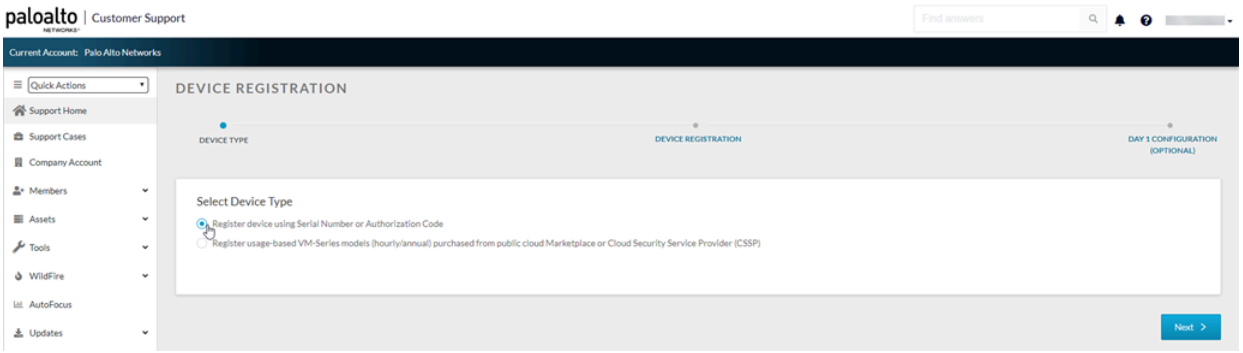
STEP 2 | 按一下 **Create My Account**（建立我的帳戶）。



STEP 3 | 輸入 **Your Email Address**（您的電子郵件地址），選中 **I'm not a robot**（我不是機器人），然後按一下 **Submit**（提交）。



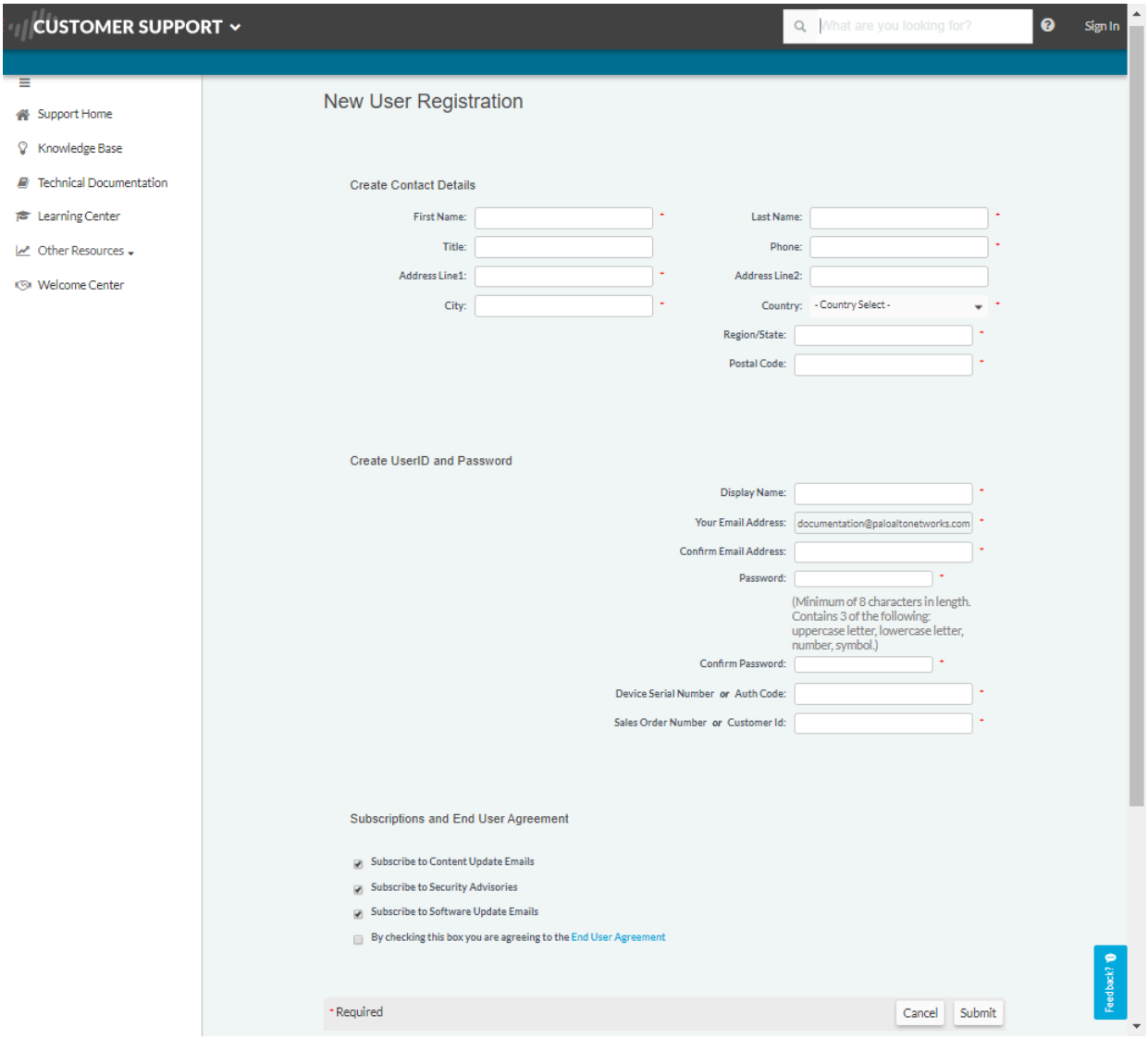
STEP 4 | 選取 **Register device using Serial Number or Authorization Code**（使用序號或驗證碼註冊裝置），然後按一下 **Next**（下一步）。



 ©2024 Palo Alto Networks, Inc.

STEP 5 | 填寫註冊表。

1. 輸入您的聯絡詳細資訊。必填欄位用紅色星號表示。
2. 建立該帳戶的使用者 ID 和密碼。必填欄位用紅色星號表示。
3. 輸入 **Device Serial Number**（裝置序號）或 **Auth Code**（驗證碼）。
4. 輸入 **Sales Order Number**（銷售訂單號碼）或 **Customer ID**（客戶 **ID**）。
5. 若要確保一律向您發出最新更新與安全性公告的警示，請 **Subscribe to Content Update Emails**（訂閱內容更新電子郵件）、**Subscribe to Security Advisories**（訂閱安全性公告），以及 **Subscribe to Software Update Emails**（訂閱軟體更新電子郵件）。
6. 選取核取方塊，同意一般使用者合約並 **Submit**（提交）。



註冊防火牆

若已擁有使用中的 Palo Alto Networks 客戶支援帳戶，請執行下列工作以註冊防火牆。

©2024 Palo Alto Networks, Inc.

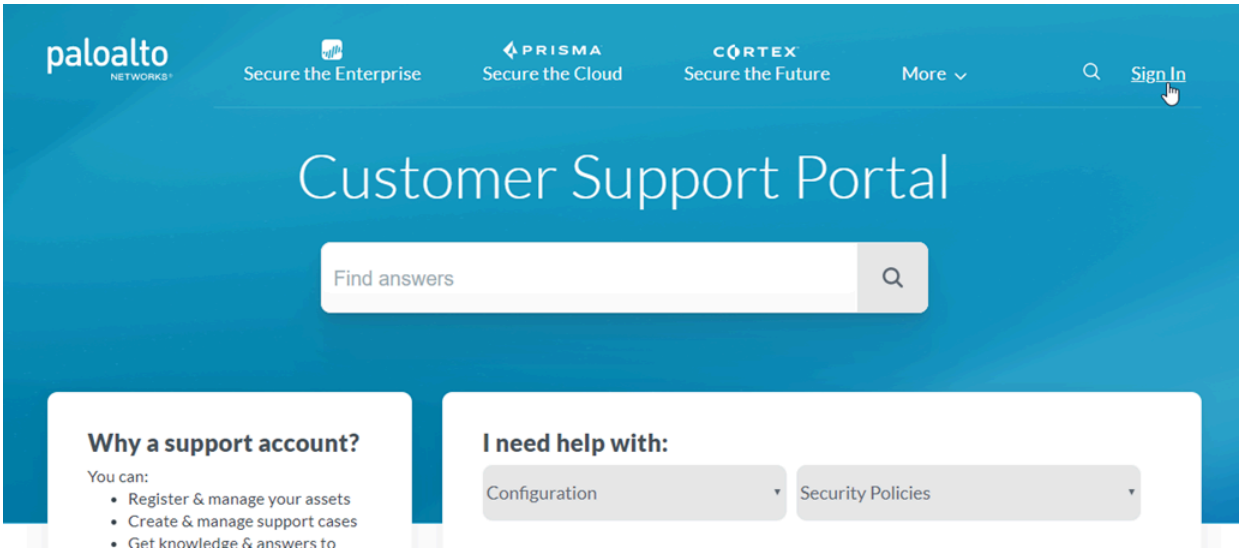
STEP 1 | 登入防火牆 Web 介面。

在網頁瀏覽器中使用安全連線 (HTTPS)，使用您在初始設定期間指派的新 IP 位址及密碼登入 (https://<IP address>)。

STEP 2 | 找到您的序號，並將其複製到剪貼簿。

在 **Dashboard**（儀表板）上，在畫面的 General Information（一般資訊）部分中找到 **Serial Number**（序號）。

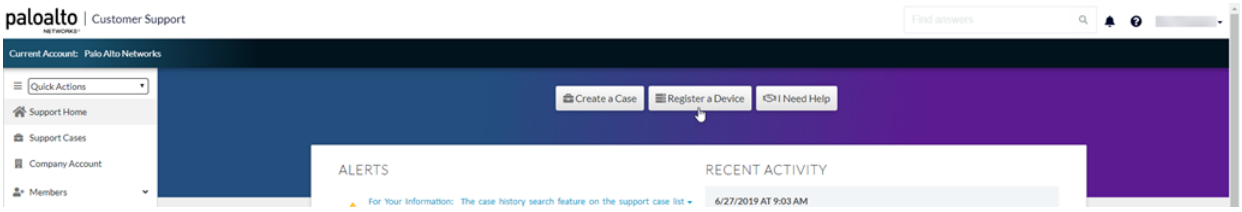
STEP 3 | 移至 Palo Alto Networks Customer Support Portal（Palo Alto Networks 客戶支援入口網站），若尚未登入，請立即 **Sign In**（登入）。



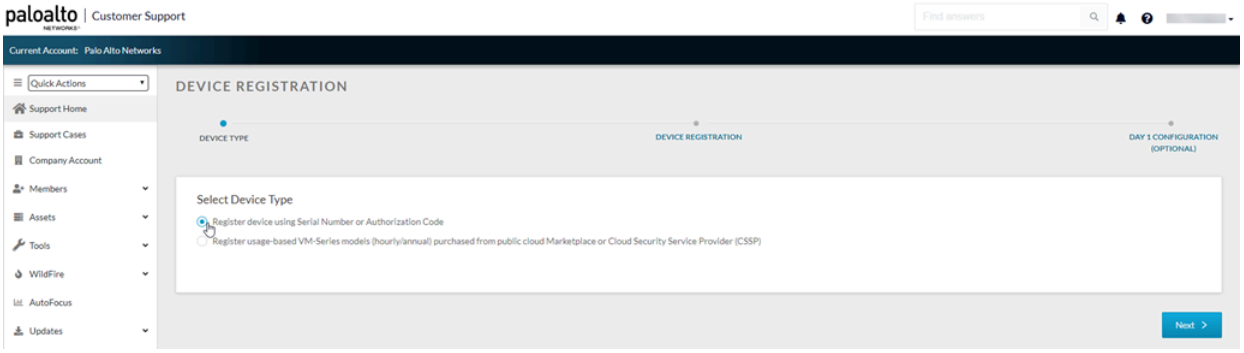
©2024 Palo Alto Networks, Inc.

STEP 4 | 註冊防火牆。

1. 在支援首頁，按一下 **Register a Device**（註冊裝置）。

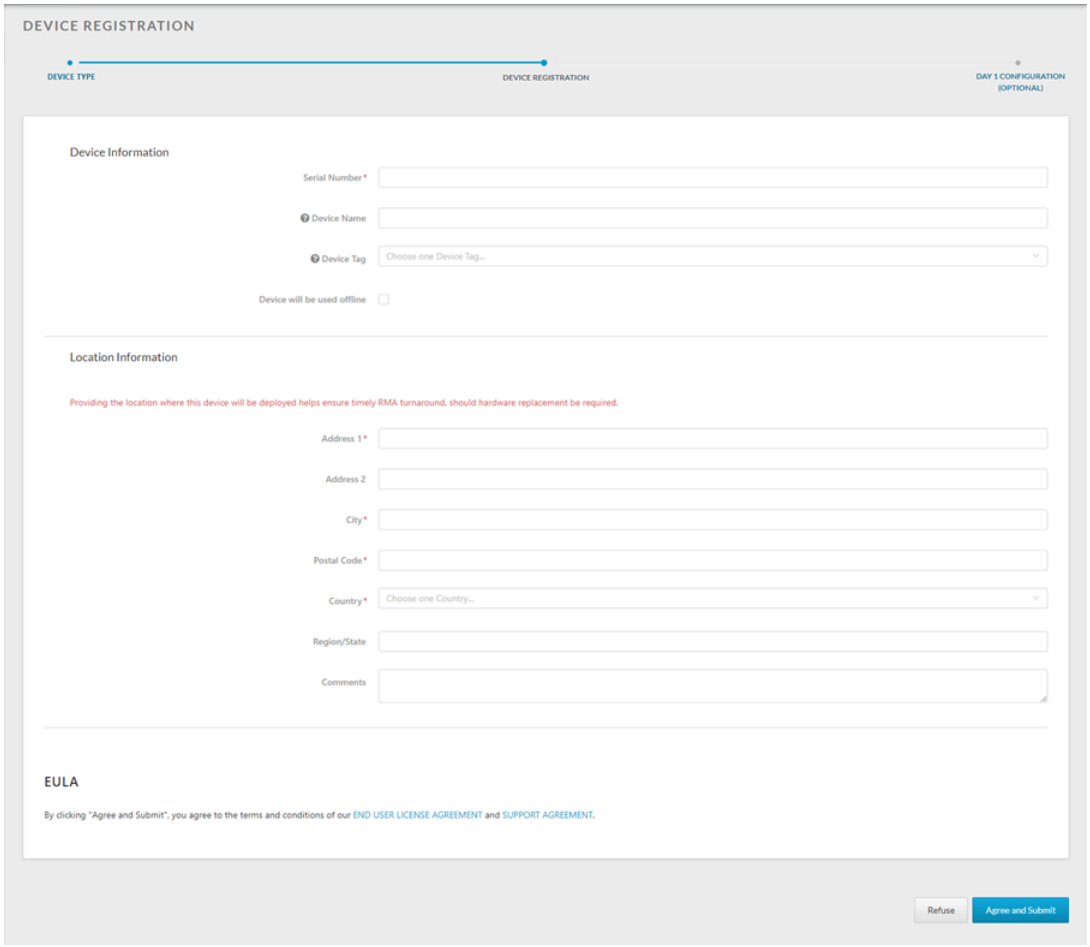


2. 選取 **Register device using Serial Number or Authorization Code**（使用序號或授權碼註冊裝置），然後按一下 **Next**（下一步）。



3. 輸入防火牆 **Serial Number**（序號）（您可以從防火牆儀表盤複製並貼上）。
4. （選用）輸入 **Device Name**（裝置名稱）和 **Device Tag**（裝置標籤）。
5. （選用）若裝置尚未連線至網際網路，請選取 **Device will be used Offline**（裝置將離線使用）核取方塊，然後從下拉式清單中，選取計劃使用的 **OS Release**（作業系統版本）。
6. 提供您計劃部署防火牆的位置資訊，包括 **Address**（地址）、**City**（城市）、**Postal Code**（郵遞區號）和 **Country**（國家）。
7. 閱讀一般使用者授權合約 (EULA) 以及支援合約，然後按一下 **Agree and Submit**（同意並提交）。

©2024 Palo Alto Networks, Inc.



您可以從 **Network Security**（網路安全性）頁面搜尋和管理剛剛註冊的防火牆。

STEP 5 | （具有線路卡的防火牆）若要確保您獲得防火牆線路卡的支援，請務必 註冊防火牆線路卡。

（選用）執行第 1 天組態

註冊防火牆後，您可選擇執行 Day 1 Configuration（第 1 天組態）。Day 1 Configuration（第 1 天組態）工具提供了 Palo Alto Networks 通知的設定範本的最佳做法，您可將其用作建立其他組態的起點。

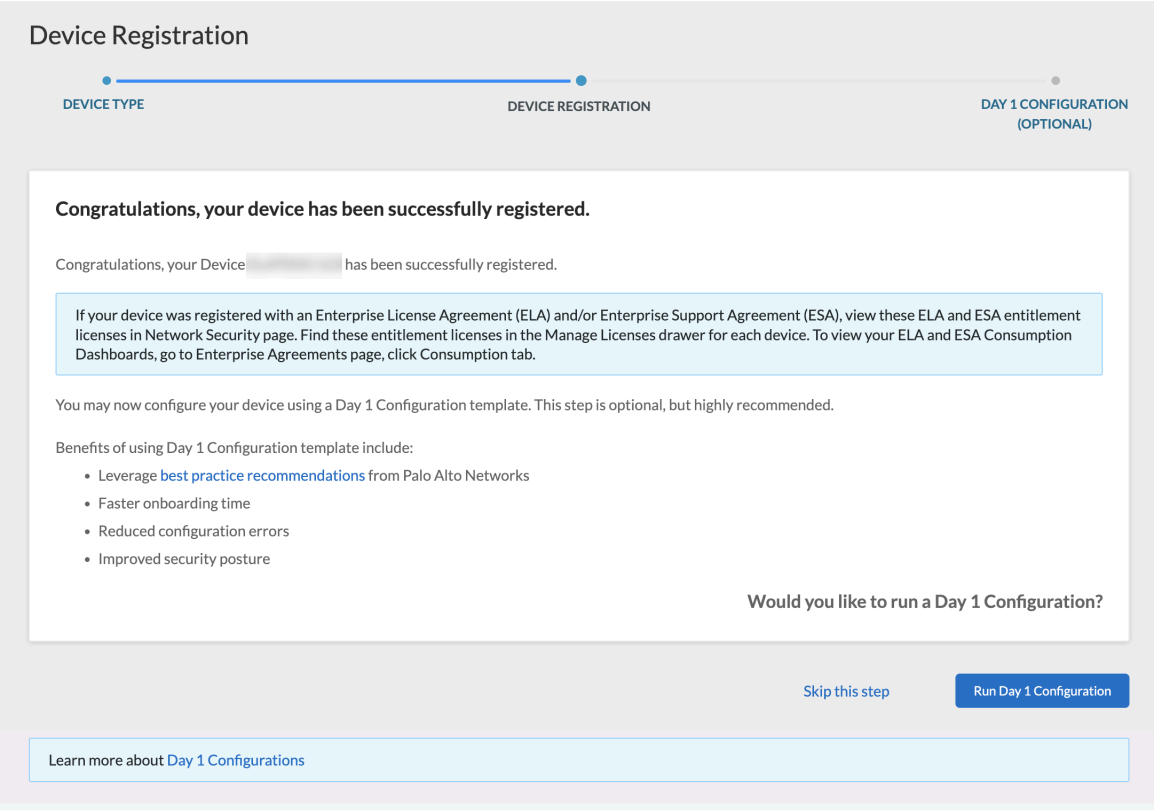
Day 1 Configuration（第 1 天組態）範本的優勢包括：

- 更快速的實作速度
- 更少的組態錯誤
- 更高的安全性

按照以下步驟執行 Day 1 Configuration（第 1 天組態）：

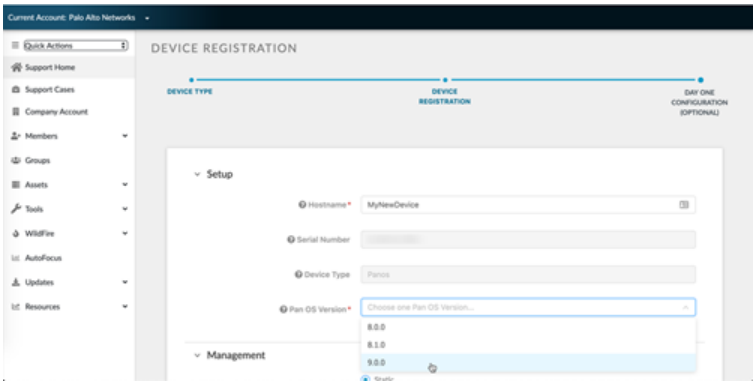
©2024 Palo Alto Networks, Inc.

STEP 1 | 在註冊防火牆後顯示的頁面上，選取 **Run Day 1 Configuration**（執行第 **1** 天組態）。



如果您已經註冊了防火牆但沒有執行 *Day 1 Configuration*（第 *1* 天組態），則還可以透過選取 ***Tools***（工具） > ***Day 1 Configuration***（第 ***1*** 天組態），從客戶支援入口網站執行。

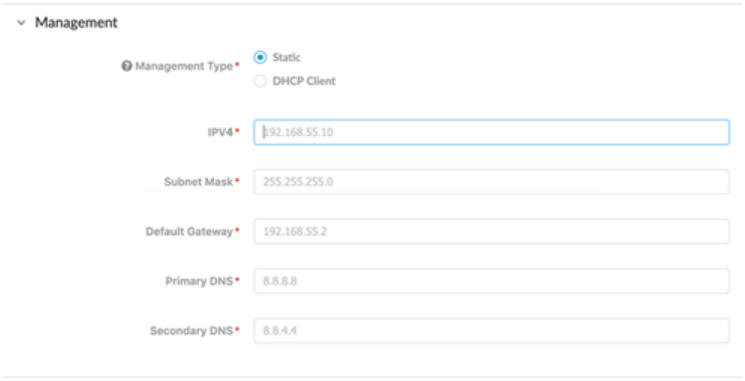
STEP 2 | 輸入新裝置的 **Hostname**（主機名稱）和 **Pan OS Version**（**Pan** 作業系統版本），並輸入 **Serial Number**（序號）和 **Device Type**（裝置類型）（選用）。



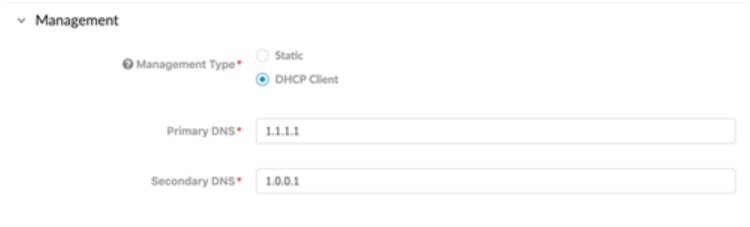
 ©2024 Palo Alto Networks, Inc.

STEP 3 | 在 **Management**（管理）下，選取 **Static**（靜態）或 **DHCP Client**（**DHCP** 用戶端）作為 **Management Type**（管理類型）。

選取 **Static**（靜態）將需要填寫 **IPV4**、**Subnet Mask**（子網路遮罩）及 **Default Gateway**（預設閘道）欄位。

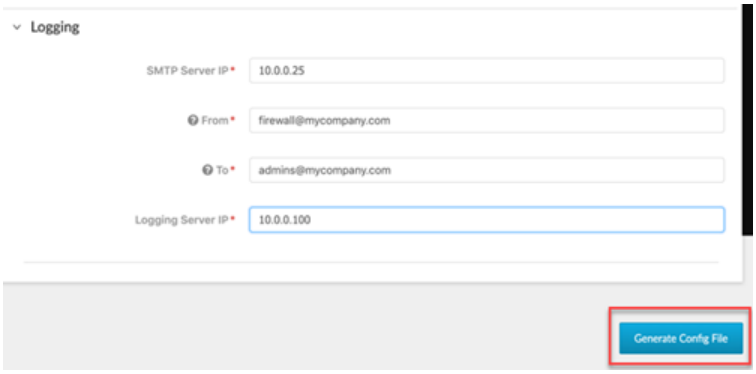


選取 **DHCP Client**（**DHCP** 用戶端）則只需輸入 **Primary DNS**（主要 **DNS**）和 **Secondary DNS**（次要 **DNS**）。在 DHCP 用戶端模式下設定的裝置可確保管理介面從本機 DHCP 伺服器接收 IP 位址，或在參數已知的情況下填寫所有參數。



STEP 4 | 填寫 **Logging**（日誌記錄）下的所有欄位。

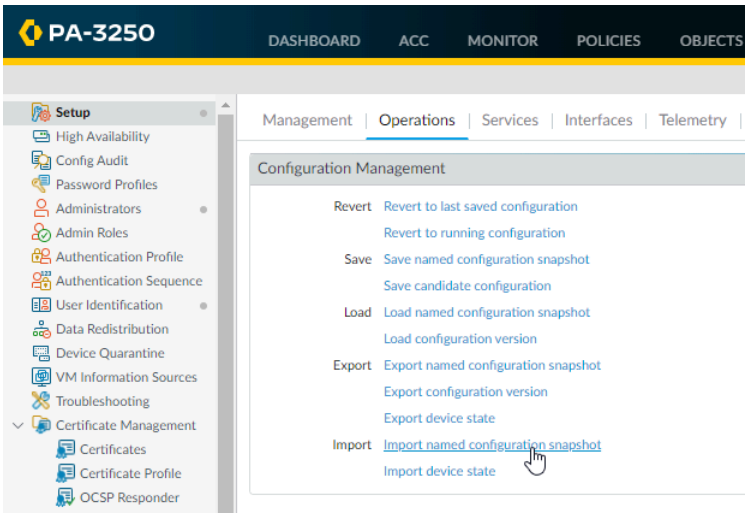
STEP 5 | 按一下 **Generate Config File**（產生組態檔案）。



©2024 Palo Alto Networks, Inc.

STEP 6 | 若要匯入並載入您剛剛下載到防火牆的 Day 1 Configuration（第 1 天組態）檔案：

1. 登入防火牆 Web 介面。
2. 選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作）。
3. 按一下 **Import named configuration snapshot**（匯入具名組態快照）。
4. 選取檔案。



註冊防火牆線路卡

下列防火牆使用線路卡，必須註冊才能獲得疑難排解和退貨方面的支援：

- PA-7000 系列防火牆
- PA-5450 防火牆

如果您沒有 Palo Alto Networks 客戶支援帳戶，請依照 建立新的支援帳戶並註冊防火牆 中的步驟建立一個帳戶。建立客戶支援帳戶並註冊防火牆後，再返回遵循這些指示。

STEP 1 | 移至 Palo Alto Networks Customer Support Portal（Palo Alto Networks 客戶支援入口網站），若尚未登入，請立即 **Sign In**（登入）。

STEP 2 | 選取 **Assets**（資產） > **Line Cards/Optics/FRUs**（線路卡/光纖/**FRU**）。

STEP 3 | **Register Components**（註冊元件）。

STEP 4 | 將線路卡的 Palo Alto Networks 銷售訂單號碼輸入 **Sales Order Number**（銷售訂單號碼）欄位，以顯示有資格註冊的線路卡。

STEP 5 | 在 **Serial Number**（序號）欄位中輸入其底座序號，將線路卡註冊到防火牆。下方的 **Location Information**（位置資訊）會依據防火牆的註冊資訊自動填入。

STEP 6 | 按一下 **Agree and Submit**（同意並提交）以接受法律條款。系統會更新以在 **Assets**（資產） > **Line Cards/Optics/FRUs**（線路卡/光纖/**FRU**）下顯示已註冊的線路卡。

©2024 Palo Alto Networks, Inc.

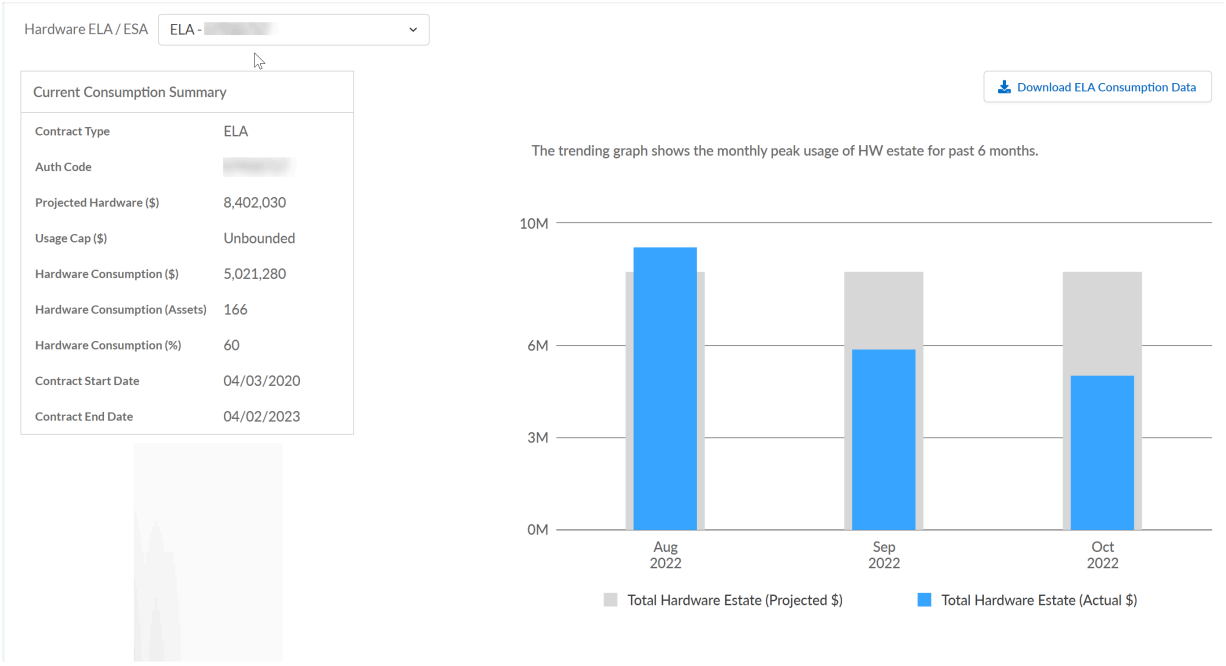
管理硬體耗用

如果您有企業協議，則可以在客戶支援入口網站上管理 PA 系列硬體耗用。

STEP 1 | 登入客戶支援入口網站。

STEP 2 | 若要檢視耗用資料，請選擇 **Assets**（資產） > **Enterprise Agreements**（企業協議） > **Consumption**（耗用）。

根據 ELA/ESA，檢視耗用摘要和關聯的 CSP 帳戶。過去六個月中啟用和解除委任的資產變更會反映在摘要和相關使用情況圖表中。您還可以下載包含帳戶耗用資料的 CSV 檔案。



©2024 Palo Alto Networks, Inc.

STEP 3 | 要管理資產，選擇 **Assets**（資產） > **Network Security**（網路安全性），然後篩選以檢視 **NGFW**。

STEP 4 | 透過 **Account Actions**（帳戶動作）管理資產。

您可以採取下列動作：

- 啟用資產 — 註冊新防火牆。
- 停用授權 — 停用硬體功能授權或 VM 功能授權和支援權利。
- 解除委任資產 — 檢視您已根據企業協議解除委任的資產清單。
- 裝置標籤 — 新增新裝置標籤或搜尋現有裝置標籤。
- 下載 **CSV** — 下載與帳號關聯的所有資產的 CSV 檔案。
- 傳入轉移 — 接受或拒絕資產轉移到帳戶。

解除委任防火牆

如果您有企業協議，則可以在客戶支援入口網站上解除委任 PA 系列硬體。

您可以解除委任不屬於 *ELA* 的硬體。

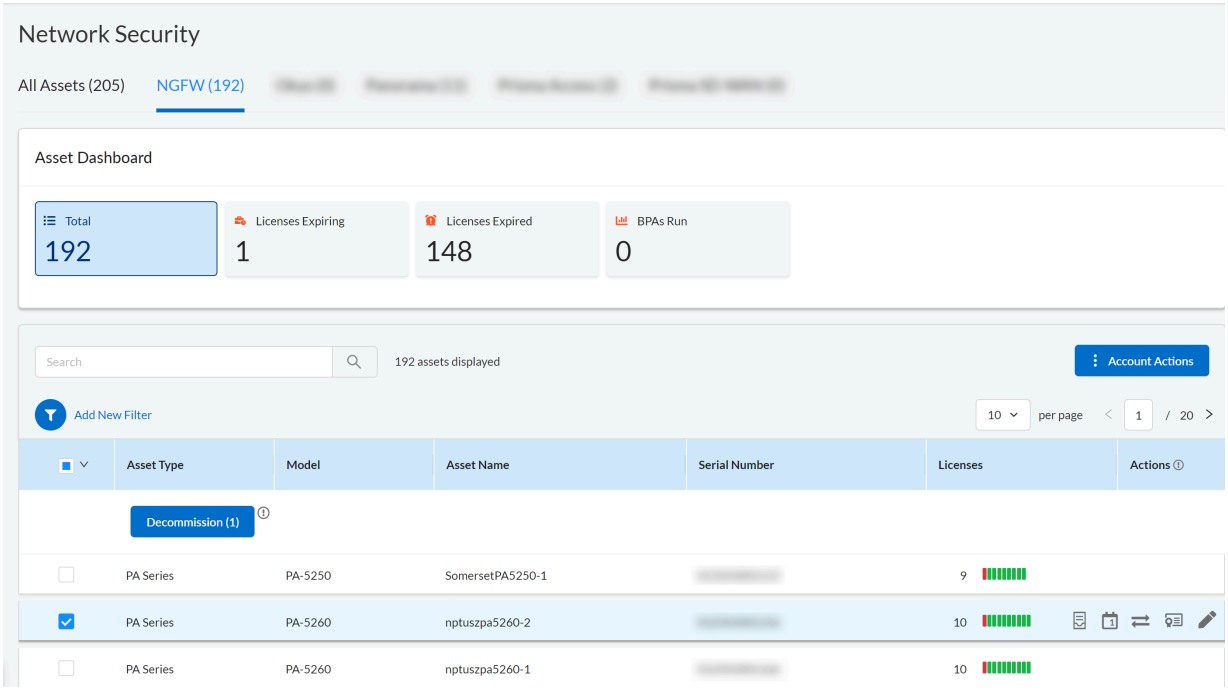
- 大量解除委任資產
- 解除委任單一資產

大量解除委任資產

STEP 1 | 登入客戶支援入口網站。

©2024 Palo Alto Networks, Inc.

STEP 2 | 選擇 **Assets**（資產） > **Network Security**（網路安全性），然後篩選以檢視 **NGFW**。



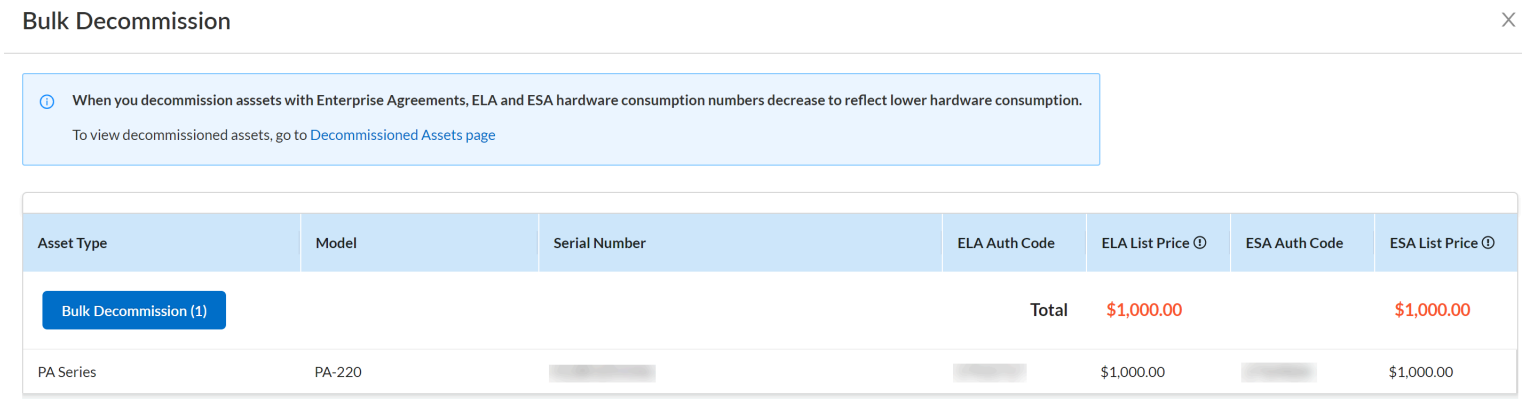
STEP 3 | 選擇要解除委任的資產。

STEP 4 | **Decommission**（解除委任）所選資產。

檢閱「大量解除委任」清單中的資產。

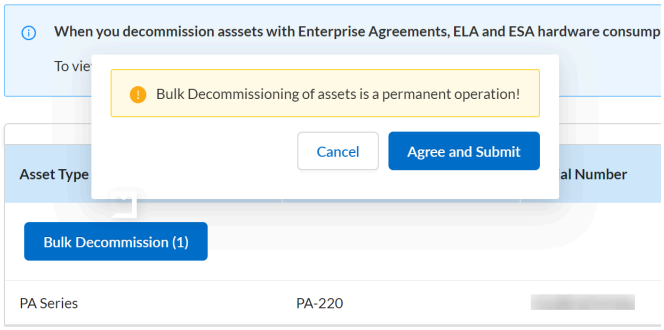
©2024 Palo Alto Networks, Inc.

STEP 5 | **Bulk Decommission**（大量解除委任）資產。

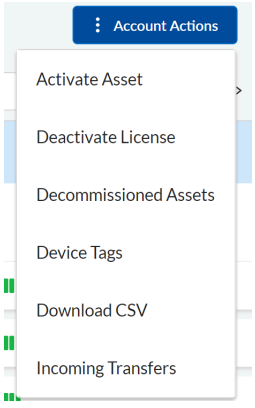


STEP 6 | **Agree and Submit**（同意並提交）以解除委任列出的資產。

解除委任資產是一項永久性操作。



STEP 7 | 透過 **Account Actions**（帳戶動作）> **Decommissioned Assets**（已解除委任資產）檢視已解除委任的資產。



解除委任單一資產

使用資產動作解除委任單個資產。

©2024 Palo Alto Networks, Inc.

STEP 1 | 登入客戶支援入口網站。

STEP 2 | 選擇 **Assets**（資產）> **Network Security**（網路安全性），然後篩選以檢視 **NGFW**。

STEP 3 | 在 **Actions**（動作）中為要解除委任的資產選擇 **Licenses/Subscriptions**（授權/訂閱）。

檢閱 **Licenses & Subscriptions**（授權和訂閱）面板中的資產詳細資訊。

STEP 4 | **Decommission Asset**（解除委任資產）。

STEP 5 | 選擇解除委任資產的原因。

- 丟失或被盜
- 客戶要求

STEP 6 | **Decommission**（解除委任）資產。

STEP 7 | **Agree and Submit**（同意並提交）以解除委任列出的資產。

解除委任資產是一項永久性操作。

STEP 8 | 透過 **Account Actions**（帳戶動作）> **Decommissioned Assets**（已解除委任資產）檢視已解除委任的資產。

©2024 Palo Alto Networks, Inc.

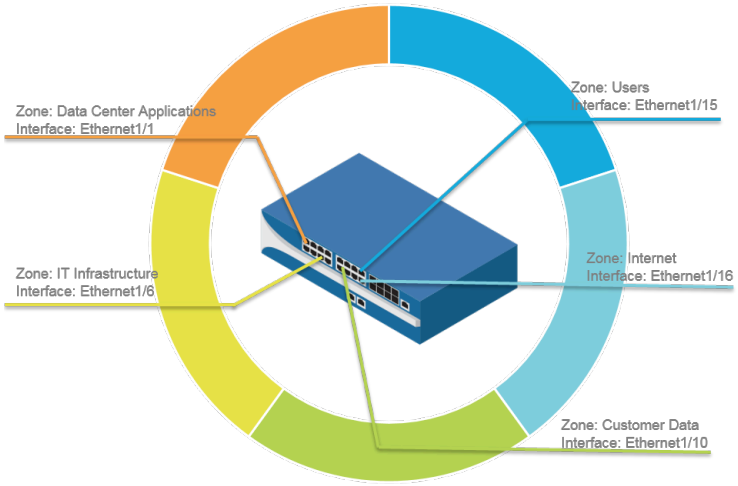
使用介面與區域來分割網路

流量必須通過防火牆，讓防火牆管理及控制。在實體上，流量會透過介面進入及離開防火牆。防火牆將根據封包是否符合安全性原則規則來決定封包的動作方式。就最基本的功能而言，每個安全性原則規則必須識別流量的來源及目的地。在 Palo Alto Networks 新世代防火牆上，安全性原則規則皆可套用在這些區域之間。區域是一組介面（物理或虛擬），表示連線至防火牆且受防火牆控制的網路區段。由於存在安全性原則原則允許流量只能在區域間流動，因此這是您的第一道防線。您建立的區域越精確，對機敏資訊與資料的存取控制就越強，也越能有效防範惡意軟體在整個網路蔓延。例如，您可能需要將資料庫伺服器分割一塊稱為「客戶資料」的區域，用於儲存客戶資料。然後您可以定義安全性原則，只允許某些使用者或使用者群組存取「客戶資料」區域，從而防止未經授權的內部存取或外部存取儲存在該區段的資料。

- 用於減少攻擊面的網路區段
- 設定介面及區域

用於減少攻擊面的網路區段

下列圖表顯示了使用區域分割網路的非常基本的範例。您建立的區域（以及允許區域間流量的相應安全性原則）越精確，就越能夠有效減少網路上的攻擊面。這是因為流量可在區域內自由流動（區域內流量），但流量無法在區域間流動（區域間流量），直至您定義允許其流動的安全性原則規則。此外，您將介面指派給區域之前，該介面不能處理流量。因此，將網路分割成精確的區域，您能夠更有效地控制機敏應用程式或資料的存取權，並且您可以防範惡意流量在網路中建立通訊通道，從而減少成功攻擊網路的可能性。



設定介面及區域

確定您想要分割網路的方式，以及您需要建立的區域以設定區段（以及鏡像至各區域的介面）之後，您可以開始設定介面及防火牆上的區域。在防火牆上設定介面，以支援您所連線的網路的每一部分拓撲。下列工作流程顯示如何設定 Layer 3 並將其指派給區域。關於使用不同類型的介面部

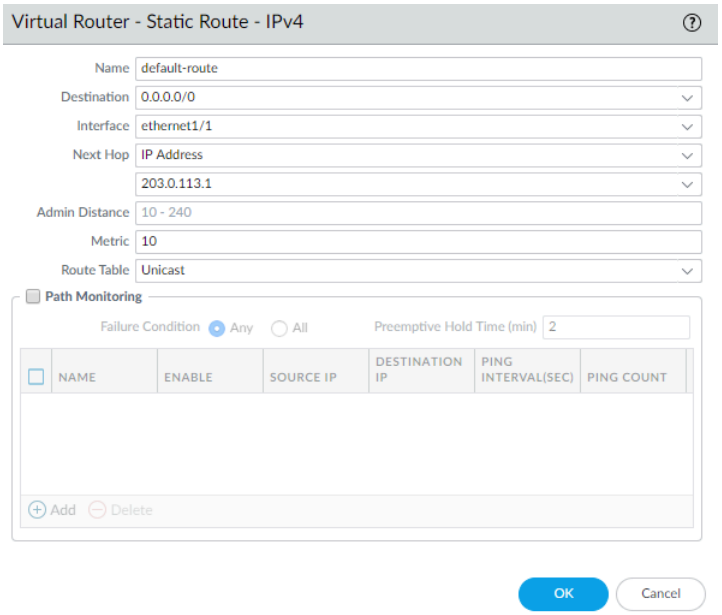
©2024 Palo Alto Networks, Inc.

署整合防火牆的詳細資訊（例如，虛擬介接介面或第二層介面），請參閱 PAN-OS 網路管理員指南。

防火牆會以連接埠乙太網路 *1/1* 和乙太網路 *1/2* (及對應的預設安全性原則與虛擬路由器) 之間的預設虛擬介接介面預先設定。如果您不打算使用此預設虛擬介接，您必須手動刪除組態並事先認可變更以防止干擾您定義的其他介面設定。如需刪除預設虛擬介接方式及其關聯安全性原則和區域的指示，請參閱設定外部服務的網路存取權中的步驟 *3*。

STEP 1 | 設定網際網路路由器的預設路由。

1. 選取 **Network**（網路）> **Virtual Router**（虛擬路由器），然後選取 **default**（預設）連結以開啟 Virtual Router（虛擬路由器）對話方塊。
2. 選取 **Static Routes**（靜態路由）頁籤，然後按一下 **Add**（新增）。輸入路由器的 **Name**（名稱)，然後在 **Destination**（目的地）欄位中輸入路由（例如 0.0.0.0/0）。
3. 在 **Next Hop**（下一個躍點）欄位中選取 **IP Address**（**IP** 位址）選項按鈕，然後輸入網際網路閘道的 IP 位址及網路遮罩（例如 203.0.113.1）。

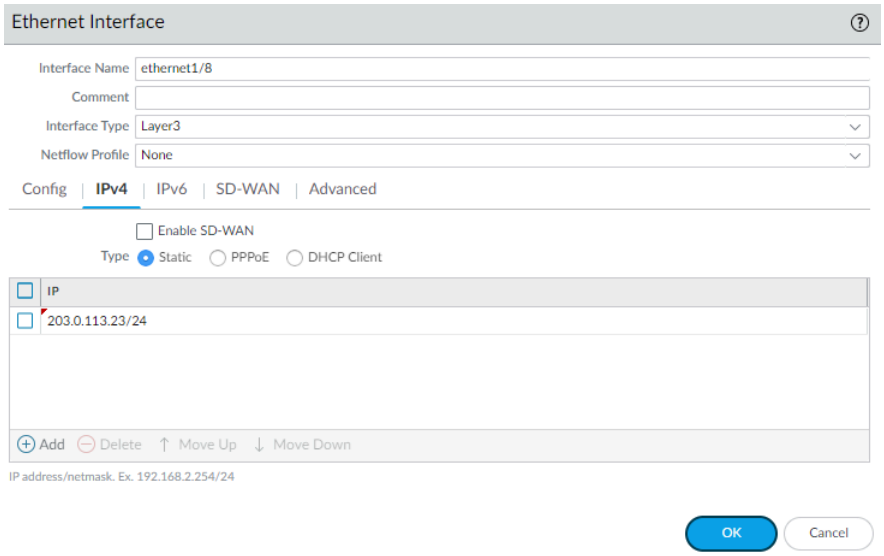


4. 按兩下 **OK**（確定）以儲存虛擬路由器組態。

©2024 Palo Alto Networks, Inc.

STEP 2 | 設定外部介面（連接網際網路的介面）。

1. 選取 **Network**（網路）> **Interfaces**（介面），然後選取要設定的介面。在此範例中，我們將 Ethernet1/8 設定為外部介面。
2. 選取 **Interface Type**（介面類型）。雖然您在此的選擇需視介面拓撲而定，但此範例說明 **Layer3** 的步驟。
3. 在 **Config**（介面類型）頁籤上，從 **Security Zone**（安全性區域）下拉式清單中選取 **New Zone**（新區域）。在 Zone（區域）對話方塊中，定義新區域的 **Name**（名稱），例如網際網路，然後按一下 **OK**（確定）。
4. 在 **Virtual Router**（虛擬路由器）下拉式清單中，選取 **default**（預設值）。
5. 若要將 IP 位址指定至介面，請選取 **IPv4** 頁籤，在 [IP] 區段中按一下 **Add**（新增），然後輸入 IP 位址及網路遮罩以指定至介面，例如 203.0.113.23/24。



6. 若要偵測介面，可選取 **Advanced**（進階）> **Other Info**（其他資訊），展開 **Management Profile**（管理設定檔）下拉式清單，然後選取 **New Management Profile**（新增管理設定檔）。輸入設定檔的 **Name**（名稱），選取 **Ping**，然後按一下 **OK**（確定）。
7. 若要儲存介面設定，請按一下 **OK**（確定）。

©2024 Palo Alto Networks, Inc.

STEP 3 | 設定連接內部網路的介面。

在此範例中，介面會連接至使用私人 *IP* 位址的網路區段。由於私人 *IP* 位址無法在外部進行路由，因此您必須設定 NAT。

1. 選取 **Network**（網路）> **Interfaces**（介面），然後選取要設定的介面。在此範例中，我們將 Ethernet1/15 設定為使用者連線的內部介面。
2. 選取 **Layer3** 作為 **Interface Type**（介面類型）。
3. 在 **Config**（設定）頁籤上，展開 **Security Zone**（安全性區域）下拉式清單並選取 **New Zone**（新增區域）。在 Zone（區域）對話方塊中，定義新區域的 **Name**（名稱），例如使用者，然後按一下 **OK**（確定）。
4. 選取之前使用的同一個虛擬路由器，在此範例中為預設值。
5. 若要將 IP 位址指定至介面，請選取 **IPv4** 頁籤，在 [IP] 區段中按一下 **Add**（新增），然後輸入 IP 位址及網路遮罩以指定至介面，例如 192.168.1.4/24。
6. 若要讓您可偵測介面，請選取您剛才建立的管理設定檔。
7. 若要儲存介面設定，請按一下 **OK**（確定）。

STEP 4 | 設定連線資料中心應用程式的介面。

確保定義精確區域，以防止未經授權存取敏感應用程式或資料，消除惡意軟體在您的資料中心內橫向移動的可能性。

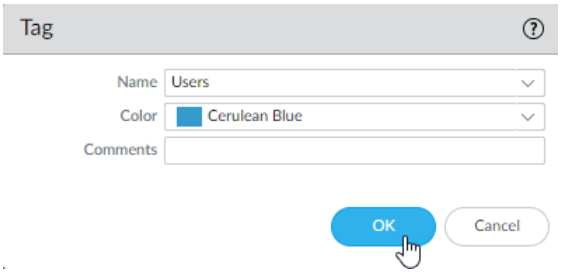
1. 選取您要設定的介面。
2. 從 **Interface Type**（介面類型）下拉式清單中選取 **Layer3**。在此範例中，我們設定 Ethernet1/1 作為用於存取資料中心應用程式的介面。
3. 在 **Config**（設定）頁籤上，展開 **Security Zone**（安全性區域）下拉式清單並選取 **New Zone**（新增區域）。在 Zone（區域）對話方塊中，定義新區域的 **Name**（名稱），例如資料中心應用程式，然後按一下 **OK**（確定）。
4. 選取之前使用的同一個虛擬路由器，在此範例中為預設值。
5. 若要將 IP 位址指定至介面，請選取 **IPv4** 頁籤，在 [IP] 區段中按一下 **Add**（新增），然後輸入 IP 位址及網路遮罩以指定至介面，例如 10.1.1.1/24。
6. 若要讓您可偵測介面，請選取您所建立的管理設定檔。
7. 若要儲存介面設定，請按一下 **OK**（確定）。

©2024 Palo Alto Networks, Inc.

STEP 5 | （選用）建立各區域的標籤。

標籤允許您以可視方式掃描原則規則。

1. 選取 **Objects**（物件） > **Tags**（標籤），然後選取 **Add**（新增）。
2. 選取區域 **Name**（名稱）。
3. 選取標籤 **Color**（顏色），然後按一下 **OK**（確定）。



STEP 6 | 儲存介面組態。

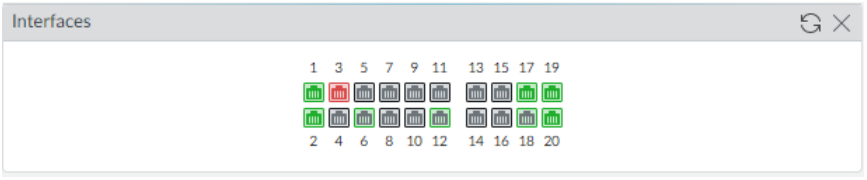
按一下 **Commit**（交付）。

STEP 7 | 使用纜線連接防火牆。

將直通式纜線從設定的介面中連接至各網路區段上對應的交換器或路由器。

STEP 8 | 確認介面正在使用中。

選取 **Dashboard**（儀表盤）並確認您設定的介面在 Interface（介面）widget 中顯示為綠色。



©2024 Palo Alto Networks, Inc.

設定基本安全性原則

既然您已定義某些區域並將其附加至介面，可隨時開始建立您的安全性原則。防火牆將不允許任何流量從一個區域流向另一個區域，除非設定一項安全性原則規則允許其流動。當封包進入防火牆介面時，防火牆按照安全性原則規則比對封包屬性，以根據屬性來決定是否封鎖或允許工作階段，例如來源及目的地安全性區域、來源與目的地 IP 位址、應用程式、使用者及服務。防火牆按照安全性原則規則庫評估各個方向傳入的流量，然後採取相符的第一項安全性規則中所指定的動作（例如，是否允許、拒絕或丟棄封包）。這意味著您必須對安全性原則規則庫中的規則排序，因此，規則庫頂部的規則更具體，底部的規則則更一般，以確保防火牆按照預期強制執行原則。

即使安全性原則規則允許封包，也不意味著該流量沒有威脅。若要讓防火牆掃描根據安全性政策規則允許的流量，您還必須附加安全性設定檔到每個規則，包括 URL 篩選、防毒、反間諜軟體、檔案封鎖以及 WildFire 分析（您可以使用的設定檔取決於您已購買的訂閱）。在建立基本安全性原則時，使用預先定義的安全性設定檔來確保對您允許進入網路的流量進行威脅檢查。您日後可以按環境的需要自訂這些設定檔。

使用下列工作流程設定非常基礎的安全性原則，該原則可設定網路基礎結構、資料應用程式及網際網路的存取權。這可使防火牆啟動並執行，以便您確認已成功設定防火牆。但是，此初始原則並非足夠全面保護您的網路。您確認已成功設定防火牆並將其整合至網路後，繼續建立一個最佳做法網際網路閘道安全性原則，以確保在保護網路免受攻擊的同時，安全地啟用應用程式存取權。

STEP 1 | （選用）刪除預設安全性原則規則。

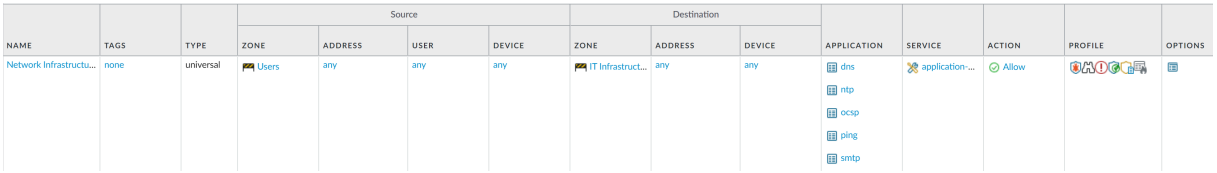
依預設，本防火牆包括名為 *rule1* 的安全性原則規則，並允許信任區域到不信任區域的所有流量。您可刪除或修改規則，以反映您的區域命名慣例。

©2024 Palo Alto Networks, Inc.

STEP 2 | 允許存取您的網路基礎結構資源。

1. 選取 **Policies**（原則）> **Security**（安全性），然後按一下 **Add**（新增）。
2. 在 **General**（一般）頁籤中，輸入規則的描述性 **Name**（名稱）。
3. 在 **Source**（來源）頁籤中，將 **Source Zone**（來源區域）設定為 **Users**（使用者）。
4. 在 **Destination**（目的地）頁籤中，將 **Destination Zone**（目的地區域）設定為 **IT Infrastructure**（**IT** 基礎結構）。

   作為最佳做法，使用 ***Destination Address***（目的地位址）欄位中的位址物件，來啟用僅對特定伺服器或伺服器群組的存取權限，特別是針對容易被入侵的 *DNS* 和 *SMTP* 等服務。憑藉限制使用者僅使用特定的目的地伺服器位址，可以防止資料外洩以及命令與控制流量透過 *DNS* 通道等技術來建立通訊。
5. 在 **Applications**（應用程式）頁籤，**Add**（新增）您希望安全啟用來回應網路服務的應用程式。例如，選取 **dns**、**ntp**、**ocsp**、**ping** 和 **smtp**。
6. 在 **Service/URL Category**（服務/**URL** 類別）頁籤，確保將 **Service**（服務）設定為 **application-default**（應用程式預設值）。
7. 在 **Actions**（動作）頁籤中，設定 **Action Setting**（動作設定）為 **Allow**（允許）。
8. 將 **Profile Type**（設定檔類型）設定為 **Profiles**（設定檔），然後選取下列安全性設定檔以附加至原則規則：
   - 對於 **Antivirus**（防毒），選取 **default**（預設）
   - 對於 **Vulnerability Protection**（漏洞保護），選取 **strict**（嚴格）
   - 對於 **Anti-Spyware**（反間諜軟體），選取 **strict**（嚴格）
   - 對於 **URL Filtering**（**URL** 篩選），選取 **default**（預設）
   - 對於 **File Blocking**（檔案封鎖），選取 **basic file blocking**（基本檔案封鎖）
   - 對於 **WildFire Analysis**（**WildFire** 分析），選取 **default**（預設）
9. 確認已啟用 **Log at Session End**（工作階段結束時記錄）。只有符合安全性原則規則的流量才會被記錄。
10. 按一下 **OK**（確定）。

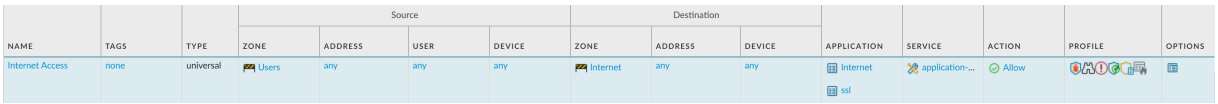


 ©2024 Palo Alto Networks, Inc.

STEP 3 | 啟用存取一般網際網路應用程式。

這是允許您收集網路流量相關資訊的暫時性規則。在您更深入洞悉您的使用者需要存取哪些應用程式之後，您就能在允許哪些應用程式方面做出明智決策，以及為各使用者群組建立更精確的基於應用程式的規則。

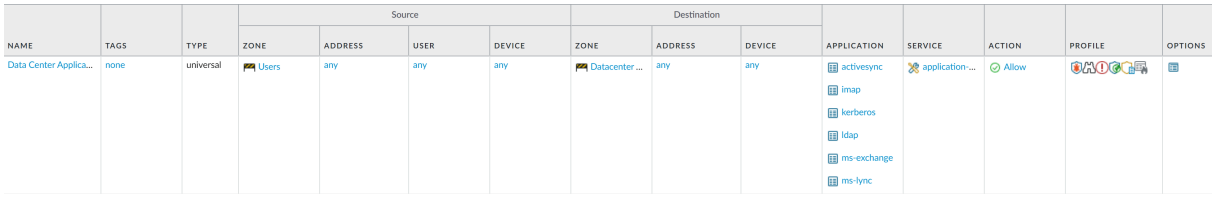
1. 選取 **Policies**（原則）> **Security**（安全性），並 **Add**（新增）規則。
2. 在 **General**（一般）頁籤中，輸入規則的描述性 **Name**（名稱）。
3. 在 **Source**（來源）頁籤中，將 **Source Zone**（來源區域）設定為 **Users**（使用者）。
4. 在 **Destination**（目的地）頁籤中，設定 **Destination Zone**（目的地區域）為 **Internet**（網際網路）。
5. 在 **Applications**（應用程式）頁籤中，**Add**（新增）**Application Filter**（應用程式篩選器）並輸入 **Name**（名稱）。若要安全啟用存取基於 Web 的合法應用程式，將應用程式篩選器中的 **Category**（類別）設定為 **general-internet**（一般網際網路），然後按一下 **OK**（確定）。若要啟用存取加密網站，請 **Add**（新增）**ssl** 應用程式。
6. 在 **Service/URL Category**（服務/**URL** 類別）頁籤，確保將 **Service**（服務）設定為 **application-default**（應用程式預設值）。
7. 在 **Actions**（動作）頁籤中，設定 **Action Setting**（動作設定）為 **Allow**（允許）。
8. 將 **Profile Type**（設定檔類型）設定為 **Profiles**（設定檔），然後選取下列安全性設定檔以附加至原則規則：
   - 對於 **Antivirus**（防毒），選取 **default**（預設）
   - 對於 **Vulnerability Protection**（漏洞保護），選取 **strict**（嚴格）
   - 對於 **Anti-Spyware**（反間諜軟體），選取 **strict**（嚴格）
   - 對於 **URL Filtering**（**URL** 篩選），選取 **default**（預設）
   - 對於 **File Blocking**（檔案封鎖），選取 **strict file blocking**（嚴格檔案封鎖）
   - 對於 **WildFire Analysis**（**WildFire** 分析），選取 **default**（預設）
9. 確認已啟用 **Log at Session End**（工作階段結束時記錄）。只有符合安全性規則的流量才會被記錄。
10. 按一下 **OK**（確定）。



 ©2024 Palo Alto Networks, Inc.

STEP 4 | 啟用存取資料中心應用程式。

1. 選取 **Policies**（原則） > **Security**（安全性），並 **Add**（新增）規則。
2. 在 **General**（一般）頁籤中，輸入規則的描述性 **Name**（名稱）。
3. 在 **Source**（來源）頁籤中，將 **Source Zone**（來源區域）設定為 **Users**（使用者）。
4. 在 **Destination**（目的地）頁籤中，將 **Destination Zone**（目的地區域）設定為 **Data Center Applications**（資料中心應用程式）。
5. 在 **Applications**（應用程式）頁籤，**Add**（新增）您希望安全啟用來回應網路服務的應用程式。例如，選取 **activesync**、**imap**、**kerberos**、**ldap**、**ms-exchange** 及 **ms-lync**。
6. 在 **Service/URL Category**（服務/URL 類別）頁籤，確保將 **Service**（服務）設定為 **application-default**（應用程式預設值）。
7. 在 **Actions**（動作）頁籤中，設定 **Action Setting**（動作設定）為 **Allow**（允許）。
8. 將 **Profile Type**（設定檔類型）設定為 **Profiles**（設定檔），然後選取下列安全性設定檔以附加至原則規則：
   - 對於 **Antivirus**（防毒），選取 **default**（預設）
   - 對於 **Vulnerability Protection**（漏洞保護），選取 **strict**（嚴格）
   - 對於 **Anti-Spyware**（反間諜軟體），選取 **strict**（嚴格）
   - 對於 **URL Filtering**（**URL** 篩選），選取 **default**（預設）
   - 對於 **File Blocking**（檔案封鎖），選取 **basic file blocking**（基本檔案封鎖）
   - 對於 **WildFire Analysis**（**WildFire** 分析），選取 **default**（預設）
9. 確認已啟用 **Log at Session End**（工作階段結束時記錄）。只有符合安全性規則的流量才會被記錄。
10. 按一下 **OK**（確定）。



STEP 5 | 將原則規則儲存到防火牆上的執行中組態。

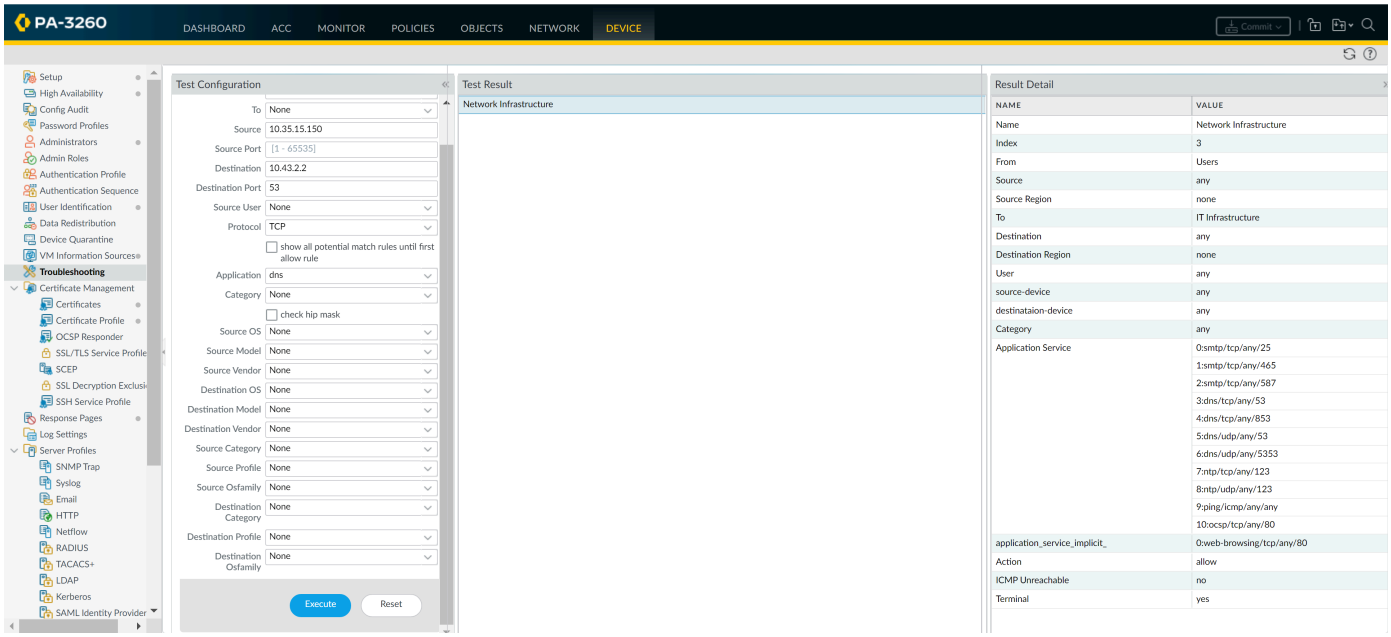
按一下 **Commit**（交付）。

©2024 Palo Alto Networks, Inc.

STEP 6 | 若要確認已有效設定基本的原則，請測試安全性原則規則是否經過評估，再決定要套用流量的安全性原則規則。

例如，若要確認原則規則將在 IP 位址 10.35.14.150 的使用者區域中的用戶端傳送 DNS 查詢至資料中心的 DNS 伺服器時套用：

1. 選取 **Device**（裝置） > **Troubleshooting**（疑難排解），然後選取 **Security Policy Match**（安全性原則比對）（**Select Test**（選取測試））。
2. 輸入 **Source**（來源）與 **Destination**（目的地）IP 位址。
3. 輸入 **Protocol**（通訊協定）。
4. 選取 **dns**（**Application**（應用程式））
5. **Execute**（執行）安全性原則比對測試。



 ©2024 Palo Alto Networks, Inc.

存取網路流量

既然您已有基本的安全性原則，即可檢閱 Application Command Center (應用程式控管中心，ACC)、流量日誌及威脅日誌中的統計資料，藉此觀察您網路的趨勢。使用此資訊來識別需建立更精確安全性原則規則的部分。

使用應用程式監測中心和使用自動關聯引擎。

在 ACC 中，檢閱您網路上最常使用的應用程式及高風險的應用程式。ACC 會以圖形方式彙總日誌資訊以凸顯在網路上周遊的應用程式、使用者（啟用 User-ID）及內容的潛在安全影響，協助您即時識別網路上發生的事件。之後您即可使用此資訊建立適當的安全性原則規則封鎖不需要的應用程式，同時採用安全的方式來允許及啟用應用程式。

ACC > **Threat Activity**（威脅活動）中的受危害的主機 Widget 會顯示您網路及日誌上可能受危害的主機，並比對證實事件的證據。

決定網路安全性原則規則與執行變更所需的更新/修改。

例如：

- 評估是否允許 Web 內容要以排程、使用者或群組為主。
- 允許或控制特定應用程式或應用程式中的功能。
- 解密並檢查內容。
- 允許但掃描是否有威脅及入侵。

關於調整安全性原則以及附加自訂安全性設定檔的資訊，請參閱建立安全性原則規則和安全性設定檔。

檢視日誌。

尤其是檢視流量及威脅日誌（**Monitor**（監控） > **Logs**（日誌））。

流量日誌視您安全性原則定義和記錄流量設定的方式而定。但是不論原則設定為何，***ACC*** 中的受危害的主機 *Widget* 都會記錄應用程式與統計資料；以及顯示您網路上允許通過的所有流量，因此包含原則允許的內部區域流量及允許隱含的相同區域流量。

©2024 Palo Alto Networks, Inc.

組態日誌儲存配額和到期期間。

檢閱 AutoFocus 日誌構件情報摘要。構件是指與防火牆記錄事件相關聯的項目、屬性、活動或行為。情報摘要顯示工作階段編號以及 WildFire 偵測到構件的範例。使用 WildFire 裁定資訊（良性、灰色、惡意）和 AutoFocus 相符標籤來尋找網路中的潛在風險。

Unit 42 建立的 *AutoFocus* 標籤、*Palo Alto Networks* 威脅情報團隊、進階提醒、針對性活動以及網路中的威脅。

從 AutoFocus 情報摘要中，您可以開始 AutoFocus 構件搜尋，並評估其在全域、行業及網路內容中的廣泛性。

監控網路使用者的 Web 活動。

檢閱 URL 篩選日誌以掃描警示、拒絕的類別/URL。當流量符合某項安全性規則，此規則具備附有警示、繼續、取代或封鎖等動作的 URL 篩選設定檔時，便會產生 URL 日誌。

©2024 Palo Alto Networks, Inc.

啟用免費 WildFire 轉送

WildFire 是一個雲端虛擬環境，可分析並執行未知範例（檔案和電子郵件連結），並確定範例是否為惡意、網路釣魚、灰色或良性。啟用 WildFire 後，Palo Alto Networks 防火牆可將未知範例轉送至 WildFire 進行分析。對於新發現的惡意軟體，WildFire 會產生一個特徵碼來偵測惡意軟體，且對於作用中 WildFire 訂閱的所有防火牆，該特征碼可即時用於擷取。這可讓全球的所有 Palo Alto 新一代防火牆偵測並防禦單一防火牆發現的惡意軟體。惡意軟體特徵碼通常與多個相同惡意軟體系列的變體相符，因此要封鎖防火牆之前從未遇到過的新惡意軟體變體。Palo Alto Networks 威脅研究團隊使用從惡意軟體變體收集的威脅情報來分所惡意 IP 位址、網域及 URL。

基本 WildFire 服務是 Palo Alto Networks 下一代防火牆的一部分，並且不需要 WildFire 訂閱。憑藉基本 WildFire 服務，您可讓防火牆轉送可攜式可執行檔 (PE) 檔案。此外，如果您沒有進行 WildFire 訂閱，但有威脅防範使用授權，可以接收 WildFire 每 24-48 小時內識別的惡意軟體特徵碼（作為防毒軟體更新的一部分）。

除 WildFire 服務之外，防火牆需要 WildFire 訂閱執行下列動作：

- 即時獲取最新 WildFire 特徵碼。
- 使用 WildFire 內嵌 ML，即時防止惡意的可攜式執行檔 (PE)、ELF、MS Office 檔案、PowerShell 及 shell 指令碼進入您的網路。
- 轉送進階檔案類型及電子郵件連結進行分析。
- 使用 WildFire API。
- 使用 WildFire 裝置來裝載 WildFire 私人雲端或 WildFire 混合雲端。

如果您有 WildFire 使用授權，可繼續並開始使用 WildFire，以最大限度利用您的使用授權。否則，採用下列步驟來啟用基本 WildFire 轉送：

STEP 1 | 確認是否已註冊防火牆，而且您擁有有效的支援帳戶以及需要的任何使用授權。

1. 登入 Palo Alto Networks 客戶支援入口網站 (CSP)，並於左側的導覽窗格中，選取 **Assets**（資產） > **Devices**（裝置）。
2. 驗證防火牆已列入。若未列出，請選取 **Register New Device**（註冊新裝置），然後繼續註冊防火牆。
3. （選用）如果您有威脅防護訂閱，請務必啟動訂閱授權。

©2024 Palo Alto Networks, Inc.

STEP 2 | 登入防火牆，並對 WildFire 轉送進行設定。

1. 選取 **Device**（裝置） > **Setup**（設定） > **WildFire**，然後編輯 General Settings（一般設定）。
2. 設定 **WildFire Public Cloud**（**WildFire** 公用雲端）欄位，以將檔案轉送至 WildFire 全域雲端（美國）：**`wildfire.paloaltonetworks.com`**。

   您還可以根據您的位置和組織要求，將檔案轉送至 *WildFire* 地區雲端或私人雲端。
3. 檢閱防火牆轉送進行 WildFire 分析的 PE **File Size Limits**（檔案大小限制）。將防火牆可轉送的 PE **Size Limit**（大小限制）設定為最大可選值 10 MB。

   作為 WildFire 最佳做法，將 *PE* 的***Size Limit***（大小限制）設定為最大可選值 *10 MB*。
4. 按一下 **OK**（確定）儲存您的變更。

STEP 3 | 啟用防火牆以轉送 PE 進行分析。

1. 選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **WildFire Analysis**（**WildFire** 分析），然後 **Add**（新增） 新的設定檔規則。
2. 設定新設定檔規則的 **Name**（名稱）。
3. **Add**（新增）轉送規則，然後輸入其 **Name**（名稱）。
4. 在 **File Types**（檔案類型）欄中，新增 **PE** 檔案到轉送規則。
5. 在 **Analysis**（分析）欄中，選取 **public-cloud**（公共雲端）以轉送 PE 至 WildFire 公共雲端。
6. 按一下 **OK**（確定）。

STEP 4 | 將新的 WildFire 分析設定檔套用至防火牆允許的流量。

1. 選取 **Policies**（原則） > **Security**（安全性），再選取現有的原則或建立新原則，如 設定基本安全性原則 中所述。
2. 選取 **Actions**（動作）並在 Profile Settings（設定檔組態）區段，將 **Profile Type**（設定檔類型）設定為 **Profiles**（設定檔）。
3. 選取您剛剛建立的 **WildFire Analysis**（**WildFire** 分析）設定檔，以將該設定檔規則套用至此原則規則允許的所有流量。
4. 按一下 **OK**（確定）。

STEP 5 | 啟用防火牆以轉送解密 SSL 流量進行 WildFire 分析。

STEP 6 | 檢閱並實作 WildFire 最佳做法，確保充分利用 WildFire 的偵測和防禦功能。

STEP 7 | **Commit**（提交）組態更新。

©2024 Palo Alto Networks, Inc.

STEP 8 | 確認防火牆正在將檔案轉送 PE 檔案至 WildFire 公共雲端。

選取 **Monitor**（監控） > **Logs**（日誌） > **WildFire Submissions**（**WildFire** 提交），以檢視防火牆成功提交進行 WildFire 分析的 PE 日誌項目。Verdict（裁定）欄顯示 WildFire 發現 PE 為惡意、灰色或良性。（WildFire 僅會為電子郵件連結指派網路釣魚裁定）。動作列表示防火牆允許還是封鎖樣本。嚴重性欄指示使用以下值的範例對組織的威脅程度：重要、高、中、低、資訊。

STEP 9 | （僅限威脅防範使用授權）如果您有威脅防範使用授權，但沒有 WildFire 使用授權，仍然可以每 24-48 小時接收一次 WildFire 特徵碼更新。

1. 請選取 **Device**（裝置） > **Dynamic Updates**（動態更新）。（裝置 > 動態更新）.
2. 檢查防火牆是否排程下並安裝防毒軟體更新。

©2024 Palo Alto Networks, Inc.

完成防火牆部署的最佳做法

現在您已將防火牆整合至網路並啟用基本安全性功能，因此可以開始設定更進階的功能。以下是需要考慮的部分事項：

- 請遵循管理存取權的最佳做法，確保恰當保護管理介面。
- 設定安全性原則規則庫最佳做法，以啟用應用程式來保護您的網路免受攻擊。移至最佳做法頁面，為您的防火牆部署選取安全性原則最佳做法。
- 設定高可用性—高可用性 (HA) 是一種單一群組中配置兩個防火牆的組態，且這兩個防火牆的組態及工作階段表會同步處理，防止單點在網路上失效。兩個防火牆對等間的活動訊號連線可確保當其中一個對等損壞時能夠無縫容錯移轉。在兩個防火牆叢集中設定可提供備援能力，並能讓您確保業務連續性。
- 啟用使用者識別 (User-ID)—User-ID 是 Palo Alto Networks 新一代的防火牆功能，可讓您根據使用者及群組來建立原則和執行報告，而非個別 IP 位址。
- 啟用解密—Palo Alto Networks 防火牆能夠將流量解密並檢查，藉此獲得可見度、控制力與精確安全性。在防火牆上使用解密功能可防止惡意內容進入您的網路，或防止機敏內容隱藏為加密或通道流量而離開您的網路。
- 請遵循保護網路發生 Layer 4 與 Layer 7 規避攻擊的最佳做法。
- 與 Palo Alto Networks 分享威脅情報 — 允許防火牆定期收集並向 Palo Alto Networks 傳送與應用程式、威脅和裝置健康狀況相關的資訊。遙測包括以下選項：啟用被動 DNS 監控；允許實驗性質的測試特徵碼在背景中執行，以免影響安全性原則規則、防火牆日誌或防火牆效能。所有 Palo Alto Networks 客戶均將從透過遙測收集的情報中獲益，而 Palo Alto Networks 利用遙測來提升防火牆的威脅防禦能力。

©2024 Palo Alto Networks, Inc.

訂閱

瞭解所有與防火牆相容的訂閱與服務，並透過啟動訂閱授權開始使用：

- 您可透過防火牆使用的訂閱
- 啟動訂閱授權
- 當授權到期時會怎麼樣？
- Palo Alto Networks 雲端服務的增強型應用程式日誌

某些雲端服務（如 *Cortex XDR*™）不會直接與防火牆整合，而是依賴 *Cortex* 資料湖中儲存的資料來詳細瞭解網路活動。增強型應用程式日誌記錄是 *Cortex* 資料湖訂閱隨附的功能—其允許防火牆收集專門供 *Cortex XDR* 使用的資料，以偵測異常的網路活動。開啟增強型應用程式日誌記錄是 Cortex XDR 的最佳做法。

您可透過防火牆使用的訂閱

下列 Palo Alto Networks 訂閱可解鎖某些防火牆功能或讓防火牆能夠利用 Palo Alto Networks 雲端傳遞服務（或兩者）。在這裡，您可以詳細瞭解需要訂閱才能在防火牆中使用的所有服務或功能。若要啟用訂閱，您必須首先啟動訂閱授權；一旦啟動，大部分訂閱服務均可使用動態內容更新，為防火牆提供全新及更新的功能。

您可透過防火牆使用的訂閱	
IoT Security	IoT Security 解決方案與新世代防火牆配合工作，可以動態探索和維護網路上 IoT 裝置的即時詳細目錄。透過 AI 和機器學習演算法，IoT Security 解決方案實現了高層次的準確性，甚至可將首次遇到的 IoT 裝置類型進行分類。而且因為它是動態的，您的 IoT 裝置詳細目錄將始終為最新。IoT Security 還可自動產生用於控制 IoT 裝置流量的原則建議，以及自動建立 IoT 裝置屬性以在防火牆原則中使用。 • 開始使用 IoT Security。
PAN-OS SD-WAN	在 PAN-OS 軟體提供的業界領先的安全性上提供智慧型動態路徑選擇。由 Panorama 管理的 PAN-OS SD-WAN 實作包括： • 集中設定管理 • 自動建立 VPN 拓撲 • 流量散佈 • 監控和疑難排解 • 開始使用 PAN-OS SD-WAN
威脅防禦	威脅防禦提供： • 防毒、反間諜軟體（命令和控制）及漏洞防護。 • 內建外部動態清單，您可用於保護網路免遭惡意主機攻擊。 • 能夠識別受感染的主機，這些主機會嘗試連線至惡意網域。 • 開始使用威脅防禦
進階 **Threat Prevention**	除了 Threat Prevention 包含的所有功能外，進階 Threat Prevention 訂閱還提供基於雲端的內嵌威脅偵測和預防引擎，利用基於 Palo Alto Networks 收集的高保真威脅情報訓練的深度學習模型，透過檢查所有網路流量來保護您的網路，避免受到規避性和未知的命令與控制 (C2) 威脅。 • 開始使用 Threat Prevention

©2024 Palo Alto Networks, Inc.

您可透過防火牆使用的訂閱	
DNS 安全性	透過查詢 DNS 安全性提供增強的 DNS Sinkholing 功能。DNS 安全性是一項可延伸的雲端服務，能夠使用進階預測分析和機器學習來產生 DNS 特徵碼。此服務可以全面存取 Palo Alto Networks 產生的不斷擴大的 DNS 威脅情報。 若要設定 DNS 安全性，您必須先購買和安裝威脅防禦授權。 • 開始使用 DNS 安全性
URL 篩選	不僅可以控制網路存取，還能根據動態 URL 類別控制使用者與線上內容的互動方式。您還能透過控制使用者可提交公司認證的網站，來防止認證被竊取。 若要設定 URL 篩選，您必須購買並安裝受支援的 URL 篩選資料庫 PAN-DB 的訂閱。有了 PAN-DB，您便可以設定對 PAN-DB 公共雲端或 PAN-DB 私人雲端的存取。 *URL* 篩選已不再作為獨立訂閱提供。所有 *URL* 篩選功能都包含在進階 *URL* 篩選訂閱中。 • 開始使用 URL 篩選
進階 **URL Filtering**	進階 URL 篩選使用基於雲端且由 ML 提供支援的 Web 安全引擎，即時對 Web 流量執行基於 ML 的檢查。這可減少對 URL 資料庫和頻外 Web 編目的依賴，來偵測並防止進階、無檔案的 Web 式攻擊，包括針對性網路釣魚、Web 傳遞的惡意軟體和入侵、命令與控制、社交工程以及其他類型的 Web 攻擊。 • 開始使用進階 URL 篩選
WildFire	雖然威脅防護授權包括基本 WildFire® 支援，但 WildFire 訂閱服務可為需要立即接受威脅保護、經常 WildFire 特徵碼更新、進階檔案類型轉送 (APK、PDF、Microsoft Office 和 Java Applet)，以及具備使用 WildFire API 上傳檔案之能力的組織提供增強型服務。如果防火牆會將檔案轉送至內部 WF-500 裝置，則另外需要 WildFire 使用授權。 • 開始使用 WildFire
進階 **WildFire**	進階 WildFire 是一款訂閱產品，可提供對智慧型執行階段記憶體分析的存取權：後者是一款基於雲端的進階分析引擎，可補充靜態和動態分析，以偵測並阻止規避式惡意軟體威脅。智慧型執行階段記憶體分析偵測引擎利用基於雲端的偵測基礎結構，運作各式各樣的偵測機制，以這些高度規避式惡意軟體為目標。

©2024 Palo Alto Networks, Inc.

您可透過防火牆使用的訂閱	
	• 開始使用進階 WildFire
AutoFocus	提供防火牆流量日誌的圖形分析，並使用來自 AutoFocus 入口網站的威脅情報，識別您的網路的潛在風險。如啟用授權，您還可以根據防火牆上記錄的日誌進行 AutoFocus 搜尋。 • 開始使用 AutoFocus
Cortex Data Lake Cortex 資料湖	提供雲端式集中日誌儲存與彙總。必須使用或強烈建議使用 Cortex 資料湖，以支援其他幾種雲端傳遞服務，包括 Cortex XDR、IoT Security、Prisma Access 和 Traps 管理服務。 • 開始使用 Cortex 資料湖
GlobalProtect 閘道	提供行動解決方案及/或大規模 VPN 功能。依預設，您可在沒有授權的情況下部署 GlobalProtect 入口網站與閘道 (不含 HIP 檢查)。如果要使用進階 GlobalProtect 功能（HIP 檢查和相關內容更新、GlobalProtect 行動應用程式、IPv6 連線或 GlobalProtect 無用戶端 VPN），每個閘道都需要一個 GlobalProtect 閘道授權。 • 開始使用 GlobalProtect
虛擬系統	這是一個永久性授權，在 PA-3200 系列防火牆上啟用多個虛擬系統支援需要此授權。此外，若要增加虛擬系統的數量並超過 PA-400 系列、PA-3400 系列、PA-5200 系列、PA-5400 系列及 PA-7000 系列防火牆（基本數量因平台而有所不同）預設的基本數量，您必須購買虛擬系統授權。PA-220、PA-800 系列與 VM-Series 防火牆不支援虛擬系統。 • 開始使用虛擬系統
企業資料遺失防護 **(DLP)**	提供基於雲端的保護，以防止未經授權的存取、誤用、擷取和共用敏感資訊。企業 DLP 使用基於機器學習的資料分類、幾百個使用規則運算式或關鍵字的資料模式以及使用布林邏輯掃描集體類型資料的資料設定檔，提供單個引擎對靜態和動態敏感資料進行準確的偵測和一致的原則實施。 • 開始使用企業 DLP
SaaS 安全性內嵌	SaaS 安全性解決方案可與 Cortex Data Lake 搭配使用，以探索您網路上使用的所有 SaaS 應用程式。SaaS 安全性內嵌可以探索數以千計的影子 IT 應用程式及其使用者和使用詳細資料。SaaS 安全性內嵌還會在您現有的 Palo Alto Networks 防火

©2024 Palo Alto Networks, Inc.

您可透過防火牆使用的訂閱	
	牆上順暢地執行 SaaS 原則規則建議。App-ID 雲端引擎 (ACE) 也需要 SaaS 安全性內嵌。 • 開始使用 SaaS 安全性內嵌

©2024 Palo Alto Networks, Inc.

啟動訂閱授權

按照下列步驟在防火牆上啟動新授權。

解密鏡像功能要求您啟動免費授權以解鎖功能。對於這些功能，您應該按照以下步驟啟動解密功能的免費授權。

STEP 1 | 找到購買的授權啟動碼。

購買使用授權後，您就會收到列出與每個使用授權相關聯的啟動碼的 Palo Alto Networks 客戶服務電子郵件。如果您找不到此封電子郵件，繼續執行前，請聯絡客戶支援以取得啟動碼。

STEP 2 | 啟動支援授權。

如果沒有有效的支援授權，您將無法更新 PAN-OS 軟體。

1. 登入 Web 介面，然後選取 **Device**（裝置） > **Support**（支援）。
2. 按一下 **Activate support using authorization code**（使用授權碼啟動支援）。
3. 輸入 **Authorization Code**（授權碼），然後按一下 **OK**（確定）。

STEP 3 | 啟動購買的每個授權。

選取 **Device**（裝置） > **Licenses**（授權），然後採用下列其中一種方式啟動授權與訂閱：

- **Retrieve license keys from license server**（從授權伺服器擷取授權金鑰）—如果您已在客戶支援入口網站上啟動您的授權，請使用此選項。
- 使用授權碼啟動功能 — 使用此選項可讓購買的使用授權使用先前未在支援入口網站上啟動的授權碼。出現提示時，請輸入 **Authorization Code**（授權碼），然後按一下 **OK**（確定）。
- 手動上傳授權金鑰 — 如果您的防火牆未連線至 Palo Alto Networks 客戶支援入口網站，請使用此選項。在此情況下，您必須使用連接網際網路的電腦從支援網站下載授權金鑰檔案，然後上傳至防火牆。

若要使用客戶支援入口網站 *API* 自動啟動，請參閱啟用授權的程序。此程序適用於硬體和 *VM-Series* 防火牆。

STEP 4 | 確認授權已成功啟動

在 **Device**（裝置） > **Licenses**（授權）頁面上，確認已成功啟動授權。例如，在啟動 WildFire 授權後，您必須查看該授權是否有效：

 ©2024 Palo Alto Networks, Inc.

STEP 5 | （僅限 WildFire、進階 URL 篩選和 DNS 安全性訂閱）**Commit**（提交）設定變更以完成訂閱啟用。

在啟用 WildFire、進階 URL 篩選或 DNS 安全性訂閱授權後，防火牆需要提交才能根據安全性設定檔組態設定開始處理其相應的流量和資料類型。您應該：

- 提交任何擱置中的變更。如果您沒有擱置中的變更，這會阻止您提交任何設定更新，您可以：透過 CLI 發出 commit force 命令，或進行寫入候選設定的更新，從而啟用提交選項。

  使用以下 CLI 設定模式命令發起 commit force：

  ```
  username@hostname> configure Entering configuration mode [edit]
   username@hostname# commit force
  ```

  commit force 會繞過一些在正常提交操作中通常會發生的驗證檢查。在發出 *commit force* 更新之前，請確保您的設定有效並且在語義和語法上都是正確的。

- 僅限 WildFire檢查 WildFire 分析設定檔規則是否包含 WildFire 訂閱現在支援的進階檔案類型。如果不需要變更任何規則，則對規則說明進行微幅編輯並執行認可。

©2024 Palo Alto Networks, Inc.

當授權到期時會怎麼樣？

Palo Alto Networks 訂閱 為防火牆提供新增功能和/或存取 Palo Alto Networks 雲端提供的服務。如果授權在 30 天內到期，系統日誌中會每天顯示一條警告訊息，直到訂閱更新或到期為止。授權到期後，某些訂閱將繼續以有限的容量運行，而另一些訂閱將完全停止運行。您可在此處瞭解每個訂閱到期後會怎麼樣。

授權到期的確切時間是到期日第二天凌晨 *12:00* 點 *(GMT)*。例如，如果您的授權排程於 *1* 月 *20* 日結束服務，則您在當天剩餘時間內可以使用功能。在新的一天起始之際，即 *1* 月 *21* 日凌晨 *12:00* 點 *(GMT)*，授權將到期。無論防火牆上設定的時區為何，所有授權相關功能都按照格林威治標準時間 *(GMT)* 運作。

（*Panorama* 授權）如果支援授權到期，則 *Panorama* 仍然可以管理防火牆以及收集日誌，但軟體和內容更新將無法使用。*Panorama* 上的軟體和內容更新版本必須與受管理的防火牆版本一致或更新，否則將發生錯誤。請參閱 Panorama、日誌收集器、防火牆和 WildFire 版本相容性。

訂閱	到期行為
進階威脅防禦/威脅防禦	系統日誌中顯示警示，表明授權已過期。 您仍可以： • 使用授權到期時安裝的特徵碼，除非您使用手動方式或作為自動排程的一部分安裝新的僅針對應用程式的內容更新。如果是後者，此更新將刪除您現有的威脅特徵碼，且您將不再獲得針對它們的保護。 • 使用和修改自訂 App-ID™ 和威脅威脅。 您不可再： • 安裝新的特徵碼。 • 將特徵碼降至以前的版本。 • 使用進階威脅防禦提供的基於 ML 的即時偵測引擎偵測和預防未知威脅。
DNS 安全性	您仍可以： • 如果您具有有效的威脅防護授權，請使用本機的 DNS 特徵碼。 您不可再： • 取得新的 DNS 特徵碼。
進階 URL 篩選/URL 篩選	您仍可以：

©2024 Palo Alto Networks, Inc.

訂閱	到期行為
	• 使用自訂 URL 類別強制執行原則。 您不可再： • 獲取有關快取的 PAN-DB 類別的更新。 • 連線至 PAN-DB URL 篩選資料庫。 • 取得 PAN-DB URL 類別。 • 使用進階 URL 篩選即時分析 URL 要求。
WildFire	您仍可以： • 轉送 PE 進行分析。 • 如果您具有有效的威脅防護訂閱，則每 24-48 小時獲取一次特徵碼更新。 您不可再： • 透過 WildFire 公開和私人雲端獲取五分鐘更新。 • 轉送高級檔案類別，如 APK、Flash 檔案、PDF、Microsoft Office 檔案、Java Applet、Java 檔案（.jar 和 .class），以及 SMTP 和 POP3 電子郵件訊息中包含的 HTTP/HTTPS 電子郵件連結。 • 使用 WildFire API。 • 使用 WildFire 裝置來裝載 WildFire 私人雲端或 WildFire 混合雲端。
AutoFocus	您仍可以： • 將外部動態清單與 AutoFocus 資料一起使用，寬限期為三個月。 您不可再： • 存取 AutoFocus 入口網站。 • 檢視 AutoFocus 情報摘要以獲取監控日誌或 ACC 構件。
Cortex Data Lake Cortex 資料湖	您仍可以： • 存儲日誌資料，寬限期為 30 天，之後將其刪除。 • 將日誌轉送到 Cortex 資料湖，直到 30 天寬限期結束。
GlobalProtect	您仍可以： • 將應用程式用於執行 Windows 和 macOS 的端點。 • 設定一個或多個內部/外部閘道。

©2024 Palo Alto Networks, Inc.

訂閱	到期行為
	您不可再： • 存取 Linux OS 應用程式和 iOS、Android、Chrome OS 及 Windows 10 UWP 的行動應用程式。 • 使用外部閘道 IPv6。 • 執行 HIP 檢查。 • 使用無用戶端 VPN。 • 根據目的地網域、用戶端處理序和視訊串流應用程式強制執行分割通道。
VM-Series	請參閱 VM-Series 部署指南。
支援	您不可再： • 接收軟體更新。 • 下載 VM 映像。 • 受益於技術支援。

©2024 Palo Alto Networks, Inc.

Palo Alto Networks 雲端服務的增強型應用程式日誌

防火牆可收集資料，來深入瞭解 Palo Alto Networks 應用程式的網路活動及服務，如 Cortex XDR 和 IoT Security。這些增強型應用程式日誌採用嚴格設計，供 Palo Alto Networks 應用程式和服務使用和處理；您無法在防火牆或 Panorama 上檢視增強型應用程式日誌。只有防火牆將日誌傳送到記錄服務，才能產生增強型應用程式日誌。

請按照以下步驟為 Cortex XDR 和 IoT Security 的增強型應用程式日誌啟用日誌轉送：

- Cortex XDR
- IoT Security

Cortex XDR

增強型應用程式日誌所收集的資料類型範例包括：DNS 查詢記錄、指定存取 URL 所使用 Web 瀏覽器或工具的 HTTP 標頭「使用者代理程式」欄位，以及有關 DHCP 自動 IP 位址指派的資訊。憑藉 DHCP 資訊，（打個比方）Cortex XDR™ 可依據主機名稱而非 IP 位址對異常活動發出警示。透過這一點，安全性分析員可使用 Cortex XDR 以有意義的方式評估使用者的活動是否在其角色範圍內，若超出角色範圍，能夠更快速地採取措施來阻止活動。

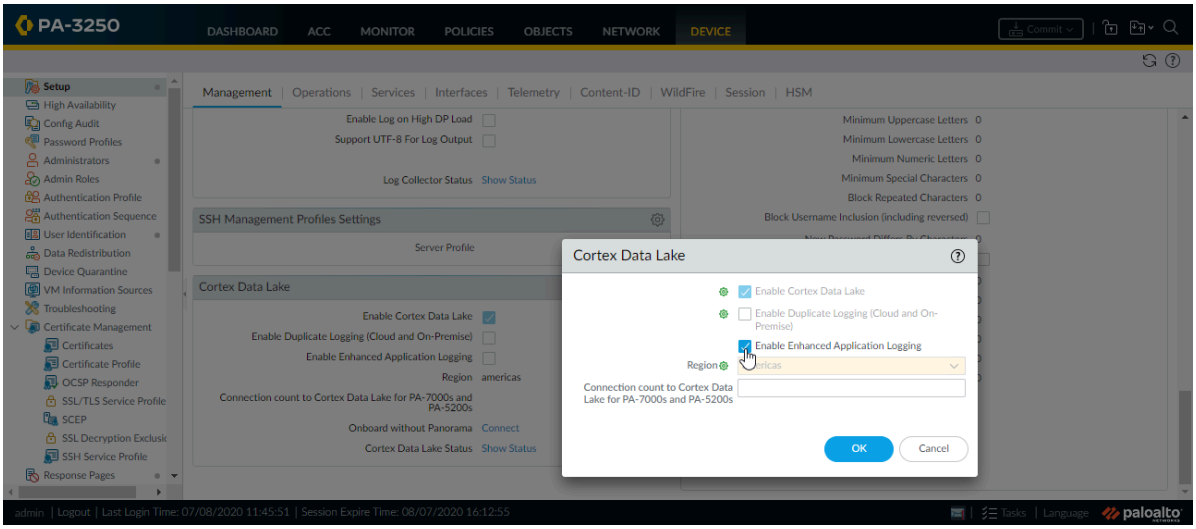
為受益於最全面的增強型應用程式日誌集，應啟用 User-ID；部署基於Windows的 User-ID 代理程式和 PAN-OS 整合式 User-ID 代理程式，均會收集一些防火牆 User-ID 日誌中不會加以反映但有助於關聯網路活動與特定使用者的資料。

若要開始將增強型應用程式日誌轉送至 Cortex 資料湖，請以全域方式開啟增強型應用程式日誌記錄，然後依據安全性規則進行啟用（使用日誌轉送設定檔）。需採用全域設定，它會擷取不基於工作階段的流量的資料（例如 ARP 請求）。強烈建議依據安全性原則規則進行設定；大部分增強型應用程式日誌從安全性原則規則所執行的基於工作階段的流量中進行收集。

STEP 1 | 增強型應用程式日誌要求訂閱 Cortex 資料湖，同時推薦 User-ID。以下步驟說明了如何開始使用 Cortex 資料湖以及啟用 User-ID。

©2024 Palo Alto Networks, Inc.

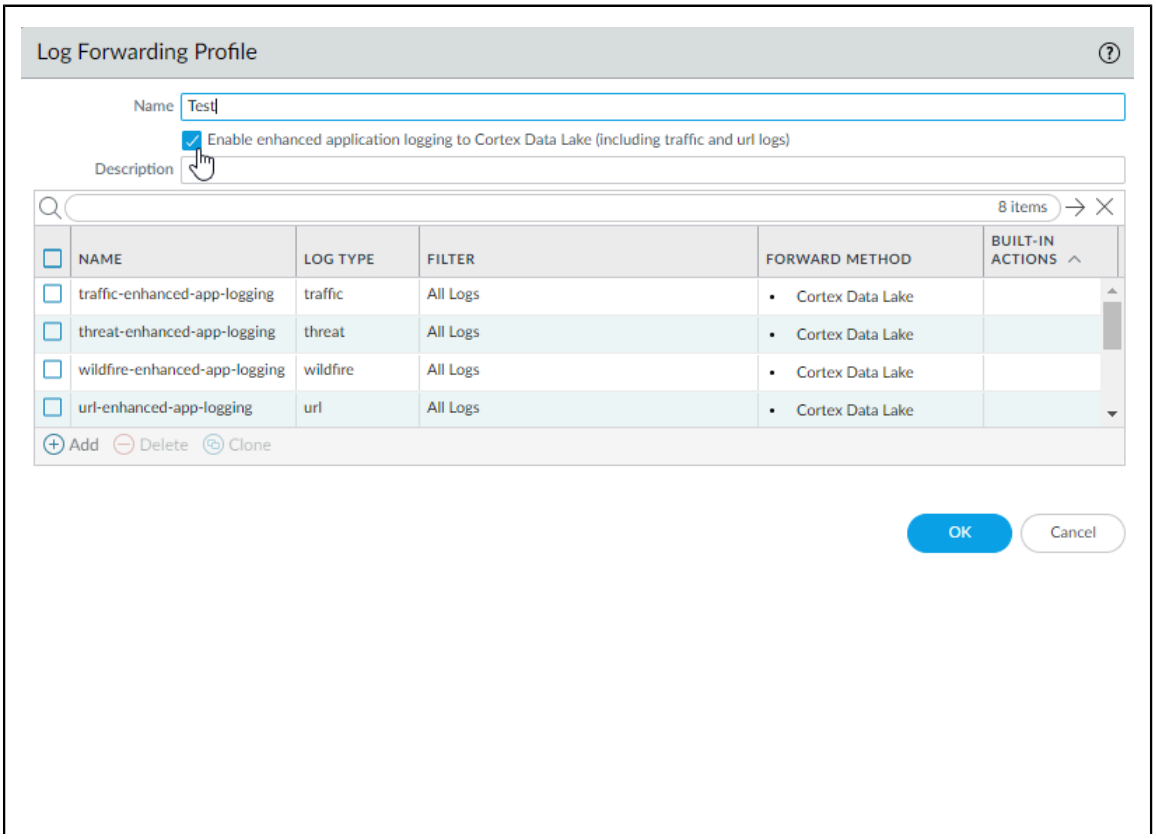
STEP 2 | 若要在防火牆上 **Enable Enhanced Application Logging**（啟用增強型應用程式日誌記錄），請選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理） > **Cortex Data Lake**（**Cortex** 資料湖），並編輯 Cortex 資料湖設定。



©2024 Palo Alto Networks, Inc.

STEP 3 | 針對控制流量的安全性原則規則繼續啟用增強型應用程式日誌記錄，提高對流量的可見度。

1. 選取 **Objects**（物件） > **Log Forwarding**（日誌轉送），並 **Add**（新增） 或修改日誌轉送設定檔。
2. 更新設定檔以啟用 **Cortex** 資料湖的增強型應用程式日誌記錄（包含流量以及 **url** 日誌）。



注意在日誌轉送設定檔中啟用增強型應用程式日誌記錄時，指定增強型應用程式日誌記錄所需日誌類型的比對清單會自動新增至設定檔。

3. 按一下 **OK**（確定）以儲存設定檔，並繼續按需更新儘可能多的設定檔。
4. 確保您已更新的日誌轉送設定檔附加至安全性原則規則，以為與規則相符的流量觸發日誌產生與轉送。
   1. 選取 **Policies**（原則） > **Security**（安全性） 以檢視附加至各安全性原則規則的設定檔。
   2. 若要更新附加至規則的日誌轉送設定檔，**Add**（新增） 或編輯規則並選取 **Policies**（原則） > **Security**（安全性） > **Actions**（動作） > **Log Forwarding**（日誌轉送），選取已啟用增強型應用程式日誌記錄的日誌轉送設定檔。

IoT Security

IoT Security 防火牆設定的一部分涉及建立日誌轉送設定檔並將其套用於安全性政策規則。雖然您可以將設定檔分別套用於每個規則，但更簡單的方法是選取預定義的日誌轉送設定檔，並將其批量

 ©2024 Palo Alto Networks, Inc.

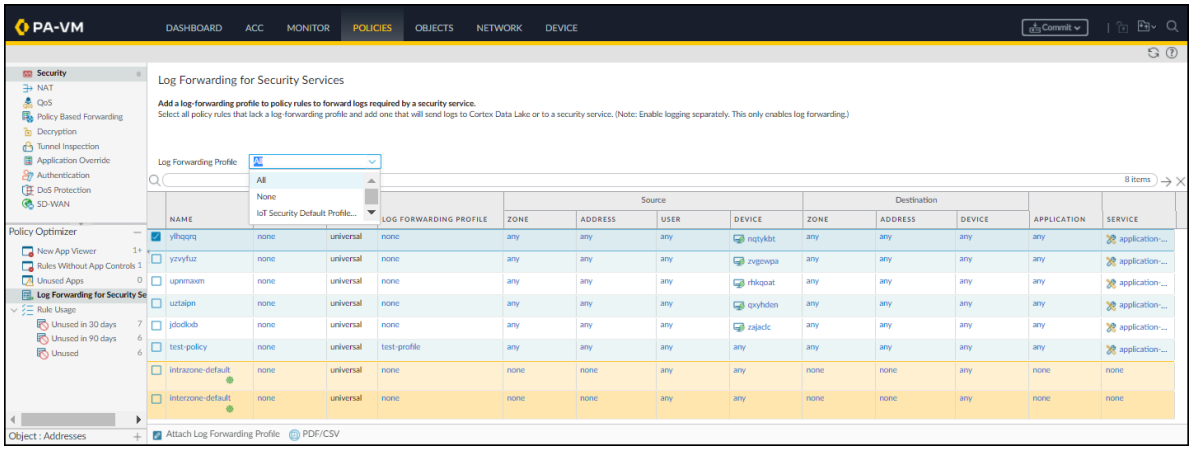
套用於任意數量的規則。以下步驟介紹了將預定義的日誌轉送設定檔批量新增到安全性政策規則的方法。

若要使用此工作流程，您必須已設定安全性政策規則、已針對規則啟用記錄並且已啟用具有增強型應用程式記錄的記錄服務。

©2024 Palo Alto Networks, Inc.

STEP 1 | 將 IoT Security 的日誌轉送設定檔套用於安全性政策規則。

1. 登入新世代防火牆并在 Policy Optimizer（政策最佳化工具）區段中選取 **Policies**（政策） > **Log Forwarding for Security Services**（安全服務的日誌轉送）。
2. 若要檢視所有安全性政策規則（包括含有和沒有日誌轉送設定檔的規則），請為日誌轉送設定檔選擇 **All**（全部）。

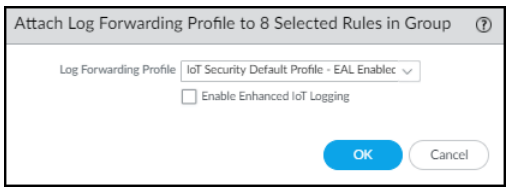


3. 選取要為其將日誌轉送到記錄服務的規則。
4. 在頁面底部 **Attach Log Forwarding Profile**（附加日誌轉送設定檔）。
5. 若要將預設日誌轉送設定檔套用於您的規則，請選擇 **IoT Security Default Profile - EAL Enabled**（**IoT Security** 預設設定檔 **- EAL** 已啟用）和 **OK**（確定）。

   預設設定檔已預先設定，以便為 IoT Security 提供所需的所有日誌類型，包括增強型應用程式日誌 (EAL)。

   您不必 ***Enable Enhanced IoT Logging***（啟用增強型 ***IoT*** 記錄），因為已在 *IoT Security* 預設設定檔上啟用增強型應用程式日誌 *(EAL)*。

©2024 Palo Alto Networks, Inc.



或

若要將 EAR 的轉送新增到尚無 EAL 的現有日誌轉送設定檔，請從日誌轉送設定檔清單中進行選擇，選取 **Enable Enhanced IoT Logging**（啟用增強型 **IoT** 記錄），然後選取 **OK**（確定）。

當您 ***Enable Enhanced IoT Logging***（啟用增強型 ***IoT*** 記錄）時，*PAN-OS* 會更新所選的日誌轉送設定檔本身，從而在使用相同日誌轉送設定檔的所有規則上啟用增強型日誌轉送。

PAN-OS 將所選的日誌轉送設定檔新增到那些尚無日誌轉送設定檔的規則中，並將以前指派的設定檔替換為此設定檔。

STEP 2 | **Commit**（提交）您的變更。

©2024 Palo Alto Networks, Inc.

防火牆管理

管理員可以使用網頁介面、CLI 及 API 管理介面來設定、管理與監控 Palo Alto Networks 防火牆。您可以自訂存取管理介面且基於角色的管理存取權，以對某些管理員委派特定工作或權限。

如需如何保護管理網路、防火牆和 Panorama 管理介面的資訊，請參閱管理存取權的最佳做法。

- 管理介面
- 使用 Web 介面
- 管理組態備份
- 管理防火牆管理員
- 參考：網頁介面管理員存取
- 參考：連接埠號使用
- 將防火牆重設為原廠預設設定
- 啟動程序防火牆

管理介面

您可以使用下列使用者介面來管理 Palo Alto Networks 防火牆：

請勿透過網際網路或企業安全性界限內的其他不信任區域啟用管理存取。請遵照管理存取權的最佳做法，以確保您正確保護防火牆。

- 使用 Web 介面執行設定和監控工作會相對簡單一些。此圖形式介面可讓您使用 HTTPS（推薦）或 HTTP 存取防火牆，而且是執行管理工作的最佳方法。
- 透過快速連續地輸入對 SSH（推薦）、Telnet 或主控台的命令，使用命令列介面 (CLI) 執行一系列工作。CLI 是一種簡潔的介面，支援兩種命令模式（操作和設定），且每個模式均有獨特的命令和陳述式階層。當您熟悉命令的巢狀結構和語法時，CLI 即可加快回應時間並進行有效率的管理。
- 使用 XML API 可讓您順暢地操作，並整合內部開發的現有應用程式和儲存庫。XML API 是一種使用 HTTP/HTTPS 要求和回應所實作的 Web 服務。
- 使用 Panorama 對多個防火牆執行基於 Web 的管理、報告和日誌收集。Panorama Web 介面類似於防火牆 Web 介面，但還具有集中管理功能。

©2024 Palo Alto Networks, Inc.

使用 Web 介面

下列主題說明如何使用防火牆 Web 介面。如需 Web 介面中特定頁籤與欄位的詳細資訊，請參閱《Web 介面參考指南》。

- 啟動 Web 介面
- 設定橫幅、當日訊息與標誌
- 使用管理員登入活動指標來偵測帳戶誤用情況
- 管理並監控管理工作
- 提交、驗證及預覽防火牆組態變更
- 提交選擇性設定變更
- 匯出組態表格資料
- 使用全域搜尋來搜尋防火牆或 Panorama 管理伺服器
- 管理限制組態變更的鎖定

啟動 Web 介面

下列是支援的網路瀏覽器，可以用於存取的 Web 介面：

- Google Chrome 104+
- Microsoft Edge 104+
- Mozilla Firefox 103+
- Safari 15+

執行下列工作以啟動 Web 介面。

STEP 1 | 啟動網際網路瀏覽器並在 URL 欄位中輸入防火牆的 IP 位址 (https://<IP address>)。

依預設，管理 *(MGT)* 介面僅允許透過 *HTTPS* 存取 *Web* 介面。若要啟用其他通訊協定，可選取 ***Device***（裝置） > ***Setup***（設定） > ***Interfaces***（介面），然後編輯 ***Management***（管理） 介面。

STEP 2 | 根據帳戶所用的驗證類型，登入防火牆。如果是首次登入防火牆，則使用預設值 **admin** 作為使用者名稱和密碼。

- **SAML**—按一下 **Use Single Sign-On**（使用單一登入）(SSO)。如果防火牆執行管理員驗證（角色指派），則輸入 **Username**（使用者名稱），然後 **Continue**（繼續）。如果由 SAML 身分提供者 (IdP) 執行授權，則 **Continue**（繼續）而不輸入 **Username**（使用者名稱）。在這兩種情況下，防火牆會將您重新導向之 IdP，提示您輸入使用者名稱和密碼。通過 IdP 的驗證後，將顯示防火牆 Web 介面。

©2024 Palo Alto Networks, Inc.

- 任何其他驗證類型—輸入使用者 **Name**（名稱）和 **Password**（密碼）。如果登入頁面上有橫幅和核取方塊，則閱讀登入橫幅並選取 **I Accept and Acknowledge the Statement Below**（我接受並確認下方陳述）。然後按一下 **Login**（登入）。

STEP 3 | 閱讀並 **Close**（關閉）當日訊息。

設定橫幅、當日訊息與標誌

登入橫幅 是您可以新增至登入頁面的可選文字，可讓管理員看到其在登入之前必須知道的資訊。例如，您可以新增訊息來告知使用者對未經授權使用者防火牆的限制。

您可以在 Web 介面的頂部（標頭橫幅）和底部（頁尾橫幅）新增反白顯示疊加文字的彩色帶，確保管理員看到關鍵資訊，例如防火牆管理的分類級別。

當日訊息 對話方塊在您登入後會自動顯示。對話方塊顯示 Palo Alto Networks 內嵌的訊息，反白顯示與軟體或內容版本相關的重要資訊。您還可以新增一則自訂訊息，以確保管理員看到可能影像其工作的資訊，例如系統即將重新啟動。

您可以使用您組織的標誌取代出現在登入頁面及 Web 介面標頭上的預設標誌。

STEP 1 | 設定登入橫幅。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理），然後編輯 General Settings（一般設定）。
2. 輸入 **Login Banner**（登入橫幅）（最多 3,200 個字元）。
3. （選用）選取 **Force Admins to Acknowledge Login Banner**（強制管理員確認登入橫幅）以強制管理員選取橫幅文字上方的 **I Accept and Acknowledge the Statement Below**（我接受並確認下方陳述）核取方塊來啟動 **Login**（登入）按鈕。
4. 按一下 **OK**（確定）。

STEP 2 | 設定當日訊息。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理），然後編輯 Banners and Messages（橫幅及訊息）設定。
2. 啟用 **Message of the Day**（當日訊息）。
3. 輸入 **Message of the Day**（當日訊息）（最多 3,200 個字元）。

   在您輸入訊息之後，按一下 ***OK***（確定），後續登入的管理員及重新整理其瀏覽器的作用中管理員會立即看到新訊息或更新訊息；不必再提交。這可讓您對即將執行且可能會影響組態變更之提交通知其他管理員。根據指定的訊息提交時間，管理員隨後可決定是否完成、儲存或還原變更。
4. （選用）選取 **Allow Do Not Display Again**（允許「不要再顯示」）（預設會停用）可讓管理員在其首次執行登入工作階段之後隱藏當日訊息。每個管理員僅可隱藏其自己的登入工作階段訊息。在「當日訊息」對話方塊中，每則訊息將擁有其自身的隱藏選項。
5. （選用）輸入當日訊息對話方塊標頭文字的 **Title**（標題）（預設為 `Messageof the Day`。

©2024 Palo Alto Networks, Inc.

STEP 3 | 設定標頭與頁尾橫幅。

明亮的背景顏色和對比鮮明的文字顏色可增加管理員注意並閱讀橫幅的可能性。您還可以使用對應您組織的分類級別來使用顏色。

1. 輸入 **Header Banner**（標頭橫幅）（最多 3,200 個字元）。
2. （選用）清除 **Same Banner Header and Footer**（標頭與頁尾的橫幅相同）（預設會啟用）以使用不同的標頭及頁尾橫幅。
3. 如果標頭與頁尾橫幅不同，輸入 **Footer Banner**（頁尾橫幅）（最多 3,200 個字元）。
4. 按一下 **OK**（確定）。

STEP 4 | 取代登入頁面及標頭中的標誌。

任何標誌影像的最大大小是 *128KB*。支援 *png* 和 *jpg* 格式的檔案類型。防火牆不支援交錯式映像檔案、包含 *Alpha* 色頻的映像以及 *gif* 檔案類型，因為此類檔案會干擾 *PDF* 的產生。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作），再按一下 Miscellaneous（雜項）區段中的 **Custom Logos**（自訂標誌）。
2. 對 **Login Screen**（登入螢幕）標誌和 **Main UI**（主 **UI**）（標頭）標誌執行下列步驟：
   1. 按一下上載 。
   2. 選取標誌影像並按一下 **Open**（開啟）。

      您可以按一下放大鏡圖示預覽影像，查看 *PAN-OS* 如何裁剪才合適。

   3. 按一下 **Close**（關閉）。
3. **Commit**（提交）您的變更。

STEP 5 | 驗證橫幅、當日訊息以及預期顯示的標誌。

1. 登出以返回登入頁面，將會顯示您選取的新標誌。
2. 輸入您的登入憑證，檢閱橫幅，選取 **I Accept and Acknowledge the Statement Below**（我接受並確認下方陳述）以啟用 **Login**（登入）按鈕，然後 **Login**（登入）。

   對話方塊即會顯示當日訊息。Palo Alto Networks 內嵌的訊息將顯示在相同對話方塊中的單獨頁面。若要導覽頁面，按一下對話方塊旁邊的右箭頭和左 箭頭，或者按一下對話方塊底部的頁面選取器 。
3. （選用）您可以對您設定的訊息及任何 Palo Alto Networks 內嵌的訊息選取 **Do not show again**（不再顯示）。
4. **Close**（關閉）當日訊息對話方塊，以存取 Web 介面。

   標頭及頁尾橫幅採用您設定的文字與顏色，顯示在每一個 Web 介面頁面中。您為 Web 介面選取的新標誌顯示在標頭橫幅下方。

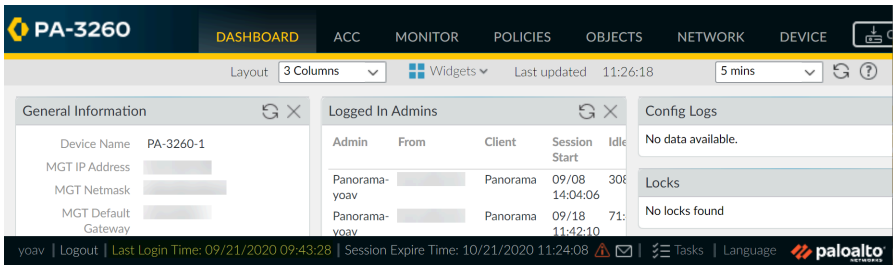
©2024 Palo Alto Networks, Inc.

使用管理員登入活動指標來偵測帳戶誤用情況

上次登入時間及失敗登入嘗試指標以可視方式偵測 Palo Alto Networks 防火牆或 Panorama 管理伺服器上對管理員帳戶的誤用情況。使用上次登入資訊來確定是否有其他人使用您的憑證登入，以及使用失敗登入嘗試指標來確定帳戶是否為強力攻擊的目標。

STEP 1 | 檢視登入活動指標來監控帳戶最近的活動。

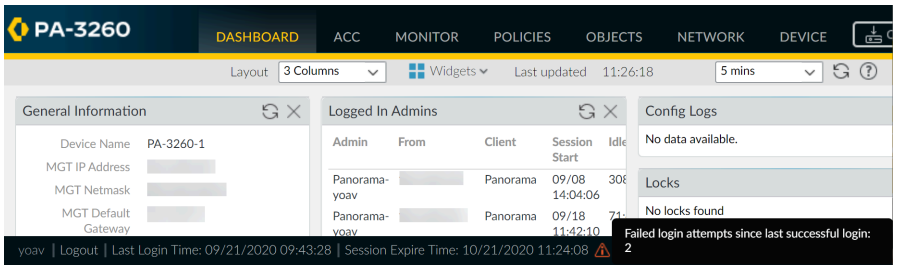
1. 登入防火牆或 Panorama 管理伺服器上的 Web 介面。
2. 檢視位於視窗左下方的上次登入詳細資訊，並確認對應於上次登入的時間戳記。



3. 針對失敗的登入嘗試，找到上次登入時間資訊右側的注意符號。

   如果自上次成功登入後，您的帳戶出現一次或多次失敗的登入嘗試，則會顯示失敗的登入指標。

   1. 如果您看到注意符號，將游標停留在其上方，顯示失敗的登入嘗試次數。



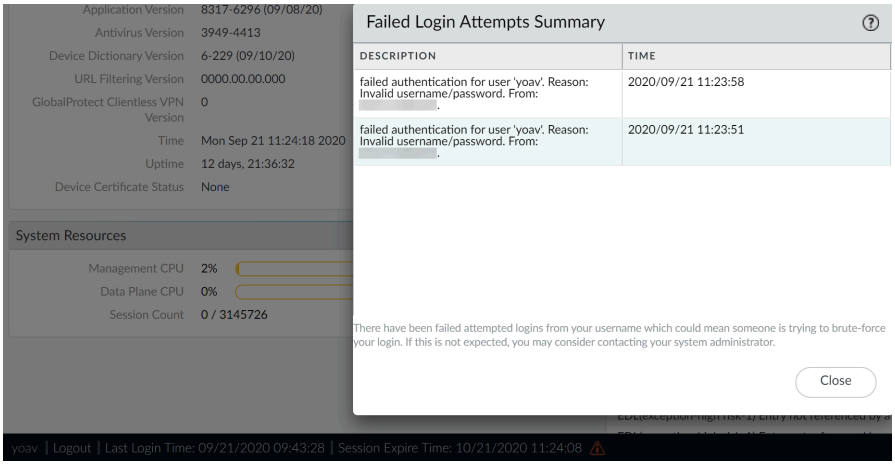
   2. 按一下注意符號可檢視失敗的登入嘗試摘要。詳細資訊包括管理員帳戶名稱、登入失敗的原因、來源 IP 位址以及日期與時間。

      成功登入然後登出之後，失敗的登入計數器將重設為零，以便您下次登入時看到新的失敗登入詳細資訊（如有）。

©2024 Palo Alto Networks, Inc.

STEP 2 | 尋找繼續嘗試登入您的防火牆或 Panorama 管理伺服器的主機。

1. 按一下失敗登入注意符號可檢視失敗的登入嘗試摘要。
2. 尋找並記錄嘗試登入主機的來源 IP 位址。例如，下圖顯示多次失敗登入嘗試。



3. 與網路管理員一起尋找使用已識別 IP 位址的使用者和主機。

   如果無法找到執行強力攻擊的系統，考慮路由該帳戶以防止今後繼續受到攻擊。

STEP 3 | 如果偵測到帳戶受到影響，請採取下列動作。

1. 選取 **Monitor**（監控） > **Logs**（日誌） > **Configuration**（組態），檢視組態變更及提交歷程記錄，以確定您的帳戶是否在您不知情的情況下用於做出變更。
2. 選取 **Device**（裝置） > **Config Audit**（組態稽核），以在您懷疑憑證被用於變更組態之前，對目前組態與正在執行的組態作比較。您還可以使用 Panorama 來執行。

   如果管理員帳戶被用於建立新帳戶，執行組態稽核也有助於您偵測與任何未經授權的帳戶相關的變更。
3. 如果您發現日誌被刪除或難以確定使用您的帳戶做出的變更是否得當，則將組態還原至已知的適當組態。

   在提交之前的組態前，進行檢閱以確保其包含正確的設定。例如，您還原的組態可能不包含最近變更，因此在您提交備份組態後應用這些變更。

   使用下列最佳做法，防止對權限帳戶進行強力攻擊。

   - 在驗證設定檔或驗證設定中設定失敗嘗試的次數及鎖定時間（分），限制允許的嘗試次數（***Device***（裝置） > ***Setup***（設定） > ***Management***（管理） > ***Authentication Settings***（驗證設定））。
   - 使用介面管理設定檔限制存取。
   - 對權限帳戶強制執行複雜密碼。

©2024 Palo Alto Networks, Inc.

管理並監控管理工作

工作管理員顯示關於您與其他管理員啟動的（例如手動提交）或自上次防火牆重新啟動後啟動的（例如排程的報告產生）所有操作的詳細資訊。您可以使用工作管理員來排解失敗操作，調查與完成的提交相關的警告，檢視關於排入佇列的提交項的詳細資訊，或取消擱置提交。

您還可以檢視系統日誌以監控防火牆上的系統事件，或檢視組態日誌以監控防火牆組態變更。

STEP 1 | 按一下 Web 介面下方的 **Tasks**（工作）。

STEP 2 | 僅 **Show**（顯示）**Running**（執行中）工作（正在進行中）或 **All**（全部）工作（預設）。選擇性地按下列類型篩選工作：

- 工作—管理員啟動的提交、防火牆啟動的提交、軟體或內容下載及安裝。
- 報告—排程的報告。
- **Log Requests**（日誌請求）—透過存取 **Dashboard**（儀錶板）或 **Monitor**（監控）頁面觸發的日誌查詢。

STEP 3 | 執行下列任何動作：

- 顯示或隱藏工作詳細資訊—依預設，工作管理員顯示類型、狀態、開始時間及每項工作的訊息。若要查看工作的結束時間及工作 ID，您必須手動設定顯示，以顯示這些欄。若要顯示或隱藏欄，在任何欄標頭中開啟下拉式清單，選取 **Columns**（欄），然後視需選取或取消選取欄名稱。
- 調查警告或失敗—閱讀 Messages（訊息）欄中的項目，瞭解工作詳細資訊。如果欄顯示 `Too many messages`（太多訊息），則按一下 Type（類型）欄中的相應項目，以檢視更多資訊。
- 顯示提交說明—如果管理員在設定提交時輸入了說明，您可以在 Messages（訊息）欄按一下 **Commit Description**（提交說明）以顯示說明。
- 在佇列中檢查提交的位置—Messages（訊息）欄表示正在進行之提交的佇列位置。
- 取消擱置提交—按一下 **Clear Commit Queue**（清除提交佇列）以取消所有擱置提交（僅對預先定義的管理角色可用）。若要取消個別提交，在 Action（動作）欄按一下該提交的 **x**（提交保留在佇列中，直至防火牆將其移除佇列）。您無法取消正在進行的提交。

提交、驗證及預覽防火牆組態變更

提交是指對防火牆組態啟用擱置中變更的過程。您可以依據管理員或位置來篩選擱置中的變更，然後僅對這些變更進行預覽、驗證或提交。位置可以是特定的虛擬系統、共用的原則和物件，或共用的裝置和網路設定。

防火牆佇列將提交要求，以便您在之前的提交正在進行中時，啟動新的提交。防火牆會依其啟動順序執行認可，但優先處理防火牆所啟動的自動認可（例如 FQDN 重新整理）。不過，如果佇列

©2024 Palo Alto Networks, Inc.

中由管理員啟動的認可已達數目上限，則必須等候防火牆完成擱置中認可的處理，才能啟動新的認可。若要取消擱置提交或檢視關於任何狀態的提交詳細資訊，請參閱管理並監控管理工作。

啟動提交後，防火牆將會檢查變更的有效性後再啟動。驗證輸出顯示封鎖提交的條件（錯誤）或務必知曉的條件（警告）。例如，驗證可能會指示您需要修復無效路由目的地，才能提交成功。驗證程序可讓您在認可前找出錯誤並加以修正（此程序並不會變更執行中的組態）。如果您使用固定認可視窗，而想要確定認可將成功而不發生錯誤，驗證程序將有所幫助。

在 Panorama™ 管理伺服器啟用並管理後，受管理防火牆將本機測試本機提交的設定或從 Panorama 推送的設定，以確認新變更不會中斷 Panorama 與受管理防火牆之間的連線。如果提交的設定中斷了 Panorama 與受管理防火牆之間的連線，則防火牆將會自動使提交失敗，且設定將還原至之前執行的設定。此外，Panorama 管理伺服器管理的防火牆會每 60 分鐘測試一次與 Panorama 的連線，如果受管理防火牆偵測到其不能成功連線至 Panorama， 則會將其設定還原至之前執行的設定。

提交、驗證、預覽、儲存和還原操作僅適用于上次提交後所做的變更。若要將組態還原到上次提交之前的狀態，必須載入之前備份的組態。

若要防止多個管理員在並行工作階段中做出組態變更，請參閱管理限制組態變更的鎖定。

STEP 1 | 設定您要提交、驗證或預覽的組態變更範圍。

1. 按一下 Web 介面上方的 **Commit**（交付）。
2. 選取下列其中一個選項：
   - **Commit All Changes**（交付所有變更）（預設）—對您擁有管理員權限的所有變更套用提交。選取此選項後，您無法手動篩選提交範圍。而指派給您用於登入之帳戶的管理員角色將決定提交範圍。
   - **Commit Changes Made By**（交付以下所做的變更）—允許您按管理員或位置篩選提交範圍。指派給您用來登入之帳戶的管理員角色，將決定您可以篩選的變更。

     若要提交其他管理員的變更，您用于登入的帳戶必須被指派超級使用者角色或管理員角色設定檔（其中***Commit For Other Admins***（為其他管理員提交）權限已啟用）。
3. （選用）若要按管理員篩選提交範圍，則選取 **Commit Changes Made By**（提交以下所做的變更），按一下旁邊的連結，選取管理員，然後按一下 **OK**（確定）。
4. （選用）若要按位置篩選，**Commit Changes Made By**（提交以下所做的變更），清除任何您要從提交範圍中排除的變更。

   如果包含與排除的組態變更之間的相依性導致驗證錯誤，請對所有包含的變更執行提交。例如，在提交虛擬系統的變更時，必須包含對該虛擬機器中的相同規則庫新增、刪除或重新定位了規則的所有管理員所做的變更。

©2024 Palo Alto Networks, Inc.

STEP 2 | 預覽提交將啟用的變更。

例如，如果您不記得所有變更，以及不確定要啟動所有變更，則此選項十分有用。

防火牆將比較您在 Commit Scope（提交範圍）中選取的設定與執行中的組態。預覽視窗將並列顯示組態，並以不同的顏色指出哪些變更是新增（綠色）、修改（黃色）或刪除（紅色）。

Preview Changes（預覽變更）並選取 **Lines of Context**（內容行），這是比較設定檔案的行數，在各反白顯示的差異前後顯示。這些附加行可幫助您將預覽輸出關聯至 Web 介面中的設定。完成變更檢閱後，關閉預覽視窗。

預覽結果會顯示在新的瀏覽器視窗中，因此您的瀏覽器必須允許快顯視窗。如果預覽視窗未開啟，請參考瀏覽器文件，以取得允許快顯視窗的步驟。

STEP 3 | 預覽要提交變更的個別設定。

如果您想要知曉變更的詳細資訊，例如設定類型以及變更者，這將很有用。

1. 按一下 **Change Summary**（變更摘要）。
2. （選用）按欄名稱（例如設定 **Type**（類型））**Group By**（分組）。
3. 完成變更檢閱後，**Close**（關閉）Change Summary（變更摘要）對話方塊。

STEP 4 | 驗證變更後再提交以確保提交成功。

1. **Validate Changes**（驗證變更）。

   結果顯示實際提交將顯示的所有錯誤和警告。
2. 解析驗證結果識別的任何錯誤。

STEP 5 | 提交組態變更。

Commit（提交）變更，以進行驗證並啟用。

若要檢視擱置中（您仍可取消）、進行中、已完成或失敗的提交詳細資訊，請參閱管理並監控管理工作。

提交選擇性設定變更

設定變更經常發生，並且通常由多個管理員進行，他們不知道進行了哪些其他設定變更。能夠控制提交哪些設定物件並防止將不完整的設定提交到防火牆至關重要。您可以選取要提交的設定物件，而不是提交所有擱置中的設定變更。成功進行選擇性提交後，會產生系統日誌。

如果能夠選取要提交的特定物件，多個管理員就能有效地進行設定變更，而不會干擾其他管理員進行的尚未準備好提交的設定變更。利用選擇性提交設定變更的功能，您可以維護已定義的操作程序，同時仍能夠成功進行未在操作範圍內定義的獨立設定變更。

STEP 1 | 登入防火牆網頁介面。

STEP 2 | 在防火牆上執行設定變更並 **Commit**（提交）。

©2024 Palo Alto Networks, Inc.

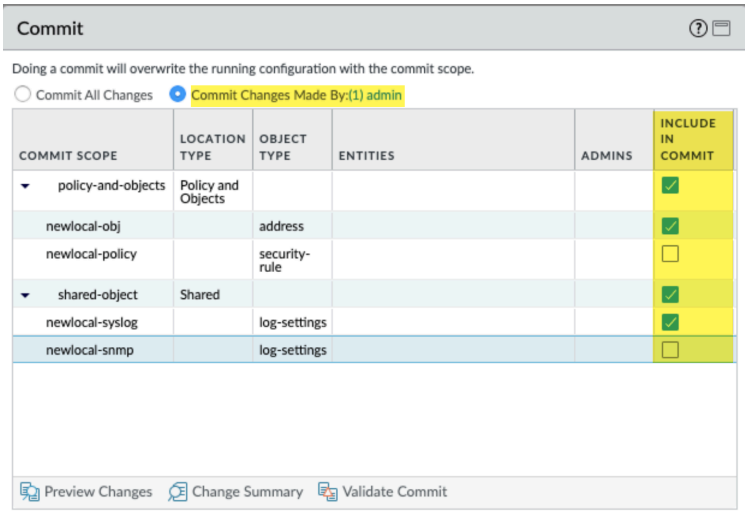
STEP 3 | 將提交範圍變更為 **Commit Changes Made By**（依做成者提交變更），以選取要提交的設定變更。

推送範圍顯示目前登入的管理員的名稱。按一下管理員名稱可檢視已進行設定變更但尚未提交的管理員清單。

STEP 4 | （選用）預覽並驗證擱置中的設定變更，以確保您希望提交選取的設定物件。

STEP 5 | **Commit**（認可）。

Commit Status（提交狀態）頁面顯示進行了已提交設定變更的管理員以及已提交設定變更的位置。



匯出組態表格資料

匯出 Panorama™ 以及防火牆的原則規則、組態物件以及 IPS 特徵碼，可向外部稽核員表明法規合規性，定期執行防火牆組態檢閱，以及產生有關防火牆原則的報告。透過此功能，無需允許稽核員直接存取您的防火牆與設備、擷取螢幕畫面或者存取 XML API 以產生組態報告。透過網頁介面，您能夠以 PDF 或 CSV 檔案的形式匯出原則、物件、網路、防火牆與 Panorama 組態的組態表格資料，以及防毒、反間諜軟體和漏洞保護安全性設定檔的特徵碼例外項。

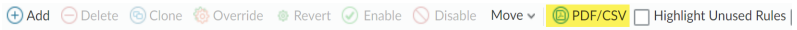
匯出為 *PDF* 檔案僅支援英文描述。

組態表格匯出的運作類似於列印功能—您無法將產生的檔案匯入回 Panorama 或防火牆。以 PDF 檔案匯出資料且表格資料超過 50,000 列時，資料會分割成多個 PDF 檔案（例如，<report-name>_part1.pdf 以及 <report-name>_part2.pdf）；以 CSV 檔案匯出資料時，資料以單個檔案的形式進行匯出。透過這些匯出格式，您可套用與報告準則相符的篩選器，並可在 PDF 報告中執行搜尋，以快速找到特定資料。此外，匯出組態表格資料時，會產生系統日誌以記錄事件。

STEP 1 | 啟動網頁介面並識別您需匯出的組態資料。

©2024 Palo Alto Networks, Inc.

STEP 2 | 按需套用篩選器以產生需匯出的組態資料，然後按一下 **PDF/CSV**。



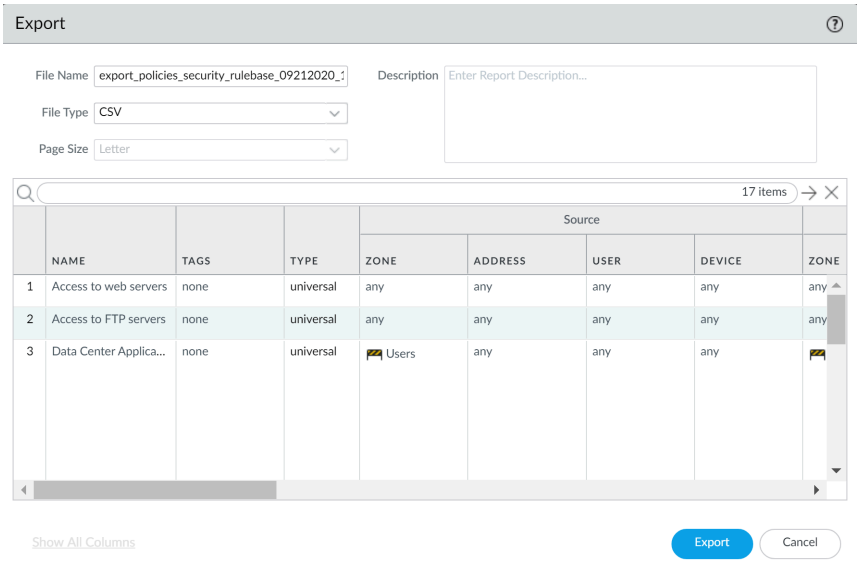
STEP 3 | 設定組態表格匯出報告：

1. 輸入 **File Name**（檔案名稱）。
2. 選取 **File Type**（檔案類型）。
3. （選用）輸入報告 Description（描述）。
4. 確認組態表格資料與套用的篩選器相符。

> 選取 ***Show All Columns***（顯示所有欄） 以顯示所有套用的篩選器。

STEP 4 | **Export**（匯出）組態表格資料。

組態表格匯出的運作類似於列印功能—您無法將產生的檔案匯入回 Panorama 或防火牆。



STEP 5 | 選取儲存匯出檔案的位置。

使用全域搜尋來搜尋防火牆或 Panorama 管理伺服器

全域尋找可搜尋防火牆或 Panorama 的候選組態中是否有特定的字串，例如 IP 位址、物件名稱、原則名稱、威脅 ID、UUID 或應用程名稱。除了搜尋組態物件和設定以外，您還可以按工作 ID 過工作類型，搜尋管理員執行的手動提交或防火牆或 Panorama 執行的自動提交。搜尋結果會依類別分組，並提供連結可連至網頁介面中的設定位置，讓您可以輕鬆找到所有參照字串的位置。搜尋結果也可協助您識別取決於或參考搜尋字詞或字串的其他物件。例如，當取代安全性設定檔時，請在全域尋找中輸入設定檔名稱，找到設定檔的所有實例，然後按一下每個實例，導覽至設定頁面，並進行必要變更。移除所有參考之後，便可以刪除設定檔。您可以針對具有依賴性的任何組態項目執行此操作。

©2024 Palo Alto Networks, Inc.

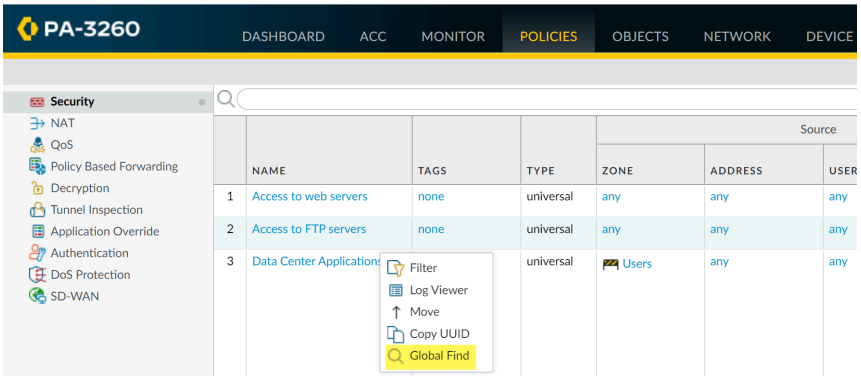
觀賞影片。

全域尋找不會搜尋動態內容（例如日誌、位址範圍，或配置的 *DHPC* 位址）。若為 *DHCP*，您可以搜尋 *DHCP* 伺服器屬性，例如 *DNS* 項目，但您無法搜尋配置給使用者的個別位址。全域尋找也無法搜尋 *User-ID* 所識別的個別使用者或群組名稱，除非在原則中定義使用者/群組。一般而言，您只能搜尋防火牆寫入組態的內容。

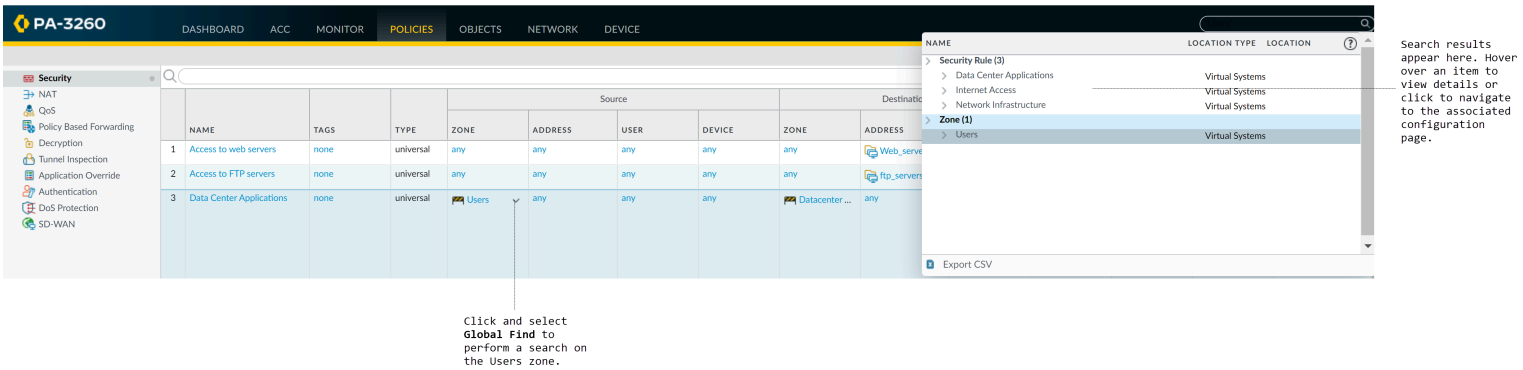
按一下網頁介面右上角的 **Search**（搜尋）圖示，啟動全域尋找。

©2024 Palo Alto Networks, Inc.

若要存取組態區域內的 Global Find（全域尋找）功能，請按一下項目旁的下拉式清單，然後按一下 **Global Find**（全域尋找）：



例如，在名為 **Users** 的區域上按一下 **Global Find**（全域尋找），可在候選組態中搜尋參考該區域的每個位置。下列螢幕擷取畫面顯示 Users 區域的結果：



搜尋技巧：

- 如果您在已啟用多個虛擬系統的防火牆上啟動搜尋，或如果已定義自訂管理角色類型，而「全域尋找」將只針對管理員具備其權限的防火牆區域傳回結果。這同樣也適用於 Panorama 設備群組。
- 搜尋字詞中的空格會以 AND 運算來處理。例如，如果您搜尋 **`corp policy`**，則搜尋結果會包含設定中存在 corp 與 policy 的實例。
- 若要尋找完全相同的字詞，請用引號括住字詞。
- 輸入不超過五個關鍵字或使用帶引號的精確字詞比對。
- 若要再次執行先前的搜尋，請按一下 Search（搜尋）（位於 Web 介面右上角）可查看最近 20 次搜尋的清單。按一下清單中的項目便可再次執行該搜尋。每個管理員帳戶都有獨一無二的搜尋歷程。
- 若要搜尋 UUID，您必須複製並貼上 UUID。

©2024 Palo Alto Networks, Inc.

管理限制組態變更的鎖定

您可以使用組態鎖定功能來防止其他管理員在您手動移除鎖定或防火牆自動移除鎖定（提交變更後）之前，變更候選組態或提交組態變更。鎖定可確保在並行登入工作階段期間，管理員不會對相同的設定或相互依存的設定做出產生衝突的變更。

防火牆佇列提交請求並執行請求，以便管理員啟動提交。如需詳細資訊，請參閱提交、驗證及預覽防火牆組態變更。若要檢視佇列中提交的狀態，請參閱管理與監控管理工作。

檢視目前鎖定的詳細資訊。

例如，您可以查看其他管理員是否設定鎖定，並閱讀其輸入的鎖定說明註解。

按一下 Web 介面上方的鎖。旁邊的數字指示目前的鎖定數。

鎖定組態。

1. 按一下 Web 介面上方的鎖。

   鎖定圖示會根據是否已設定現有鎖定而變化（已設定；未設定）。

2. **Take a Lock**（鎖定）並選取鎖 **Type**（類型）：
   - **Config**（組態）—封鎖其他管理員對候選組態進行變更。
   - 提交—阻止其他管理員提交對候選組態所進行的變更。
3. （僅限具有多個虛擬系統的防火牆）為特定虛擬系統選取鎖定組態的 **Location**（位置）或 **Shared**（共用）位置。
4. （選用）最佳做法是輸入 **Comment**（註解），以便其他管理員瞭解鎖定原因。
5. 按一下 **OK**（確定）與 **Close**（關閉）。

解鎖組態。

只有鎖定組態的超級使用者或管理員可手動解鎖組態。不過，防火牆可在完成提交操作後自動移除鎖定。

1. 按一下 Web 介面上方的鎖。
2. 選取清單中的鎖定項目。
3. 按一下 **Remove Lock**（移除鎖定）、**OK**（確定）與 **Close**（關閉）。

設定防火牆在您變更候選組態時自動套用提交鎖定。此設定適用於所有管理員。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理），然後編輯 General Settings（一般設定）。
2. 選取 **Automatically Acquire Commit Lock**（自動擷取提交鎖定）然後按一下 **OK**（確定）並 **Commit**（提交）。

©2024 Palo Alto Networks, Inc.

管理組態備份

防火牆上的執行中組態包含您提交從而啟用的所有設定，例如目前封鎖的原則規則，或在網路中允許各種類型的流量。候選組態是執行中組態的副本，以及上次提交後做出的任何未啟用變更。儲存執行中或候選組態的備份版本可讓您稍後還原這些版本。例如，如果提交驗證顯示目前的候選組態具有多個錯誤，使得您不想修復，您可以還原之前的候選組態。您也可以將還原至目前執行中的組態，而先不儲存備份。如果您需匯出組態的特定部分以進行內部檢閱或稽核，可匯出組態表格資料。

如需關於提交操作的詳細資訊，請參閱提交、驗證及預覽防火牆組態變更。

- 儲存及匯出防火牆組態
- 還原防火牆組態變更

儲存及匯出防火牆組態

儲存候選組態的備份以永久儲存在防火牆上，方便您以後還原至該備份（請參閱還原防火牆組態變更）。這對與保留當系統事件或管理員動作使防火牆重新啟動時可能會丟失的變更非常有用。重新啟動後，PAN-OS 會自動還原至目前版本的執行中組態，防火牆將該組態儲存在名稱為 running-config.xml 的檔案中。如果您要還原至比目前執行中組態更早的防火牆組態，儲存備份也非常有用。防火牆不會自動將候選組態儲存在永續性儲存空間中。您必須手動儲存候選組態為預設快照檔案 (.snapshot.xml) 或自訂名稱的快照檔案。防火牆會在本機儲存快照檔案，但您可以將其匯出至外部主機。

您不必儲存組態變更即可還原自上次提交或重新啟動以來所做的變更；只需選取 ***Config***（組態） > ***Revert Changes***（還原變更）即可（請參閱還原防火牆組態變更）。

編輯設定並按一下 ***OK***（確定）後，防火牆將更新候選組態，但不會儲存備份快照。

此外，儲存變更不會啟動它們。若要啟用變更，則執行提交（請參閱提交、驗證及預覽防火牆組態變更）。

Palo Alto Networks 建議您將任何重要的組態備份至防火牆外部主機。

STEP 1 | 若防火牆重新啟動時包含您想要保存的變更，則儲存候選組態的本機備份快照。

這些是您不準備提交的變更，例如，在目前登入階段中無法完成的變更。

若要覆寫儲存有所有管理員所做變更的預設快照檔案 (.snapshot.xml)，可執行下列任何步驟：

- 選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作），然後 **Save candidate configuration**（儲存候選組態）。

©2024 Palo Alto Networks, Inc.

- 使用指派了超級使用者角色的管理帳戶或啟用了 **Save For Other Admins**（為其他管理員儲存）權限的管理員角色設定檔登入防火牆。然後選取 Web 介面頂端的 t**Config**（組態） > **Save Changes**（儲存變更），再選取 **Save All Changes**（儲存所有變更） 和 **Save**（儲存）。

若要建立包含所有管理員所做變更的快照，但不覆寫預設快照檔案：

1. 選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作），然後 **Save named configuration snapshot**（儲存具名組態快照）。
2. 指定新組態檔案或現有組態檔案的 **Name**（名稱）。
3. 按一下 **OK**（確定）與 **Close**（關閉）。

若要僅儲存候選組態的特定變更，而不覆寫預設快照檔案的任何部分：

1. 使用具有儲存相應變更所需角色權限的管理帳戶登入防火牆。
2. 按一下 Web 介面頂端的 **Config**（組態） > **Save Changes**（儲存變更）。
3. 選取 **Save Changes Made By**（儲存下列管理員所做的變更）。
4. 若要按管理員篩選儲存範圍，按一下 **<administrator-name>**，選取管理員，然後按一下 **OK**（確定）。
5. 若要按位置篩選儲存範圍，可清除要排除的位置。位置可以是特定的虛擬系統、共用的原則和物件，或共用的裝置和網路設定。
6. 按一下 **Save**（儲存），指定新組態檔案或現有組態檔案的 **Name**（名稱），然後按一下 **OK**（確定）。

STEP 2 | 匯出候選組態、執行中組態或防火牆狀態資訊至防火牆外部主機。

選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作），然後按一下匯出選項：

- 匯出具名組態快照—匯出目前的執行中組態，即具名候選組態快照，或之前匯入的組態（候選後執行中）。防火牆將組態匯出為您指定 **Name**（名稱）的 XML 檔案。
- 匯出組態版本—選取執行中組態 **Version**（版本）以匯出 XML 檔案格式。每當您提交組態變更時，防火牆會建立一個版本。
- 匯出裝置狀態—匯出防火牆狀態資訊包。除了執行中設定，狀態資訊還包括從 Panorama 推送的裝置群組及範本設定。如果防火牆是 GlobalProtect 入口網站，資訊還將包含憑證資訊、衛星清單以及衛星驗證資訊。如果取代防火牆或入口網站，您可透過匯入狀態包來還原取代時匯出的資訊。

還原防火牆組態變更

還原操作將用其他組態中的設定取代目前候選組態中的設定。若您希望復原多項設定的變更，還原操作將非常有用，因為只需要執行一次操作，無需手動重新設定每項設定。

您可以還原自上次提交以來對防火牆組態所做的擱置中變更。防火牆將提供按管理員或位置篩選擱置中變更的選項。位置可以是特定的虛擬系統、共用的原則和物件，或共用的裝置和網路設定。如果您儲存了比目前執行中的組態更簡單的候選組態快照檔案（請參閱儲存及匯出防火牆組態），

 ©2024 Palo Alto Networks, Inc.

還可以還原至該快照。還原至快照可讓您還原上次提交之前就已存在的候選組態。每當您提交變更時，防火牆將自動儲存新版本的執行中組態，並且您可以還原任何這些版本。

還原至目前執行中的組態（檔案名稱為 running-config.xml）。

此操作將復原自上次提交以來對候選組態做出的變更。

若要還原所有管理員做出的變更，可執行下列任何步驟：

- 選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作），**Revert to running configuration**（還原至執行中的組態），然後按一下 **Yes**（是）以確認操作。
- 使用指派了超級使用者角色的管理帳戶或啟用了 **Commit For Other Admins**（提交其他管理員）權限的管理員角色設定檔登入防火牆。然後選取 Web 介面頂端的 **Config**（組態） > **Revert Changes**（還原變更），再選取 **Revert All Changes**（還原所有變更）和 **Revert**（還原）。

若要還原對候選組態做出的特定變更：

1. 使用具有還原相應變更所需角色權限的管理帳戶登入防火牆。

   控制提交操作的權限也用於控制還原操作。

2. 按一下 Web 介面頂端的 **Config**（組態） > **Revert Changes**（還原變更）。
3. 選取 **Revert Changes Made By**（還原下列管理員所做的變更）。
4. 若要按管理員篩選還原範圍，請按一下 **<administrator-name>**，選取管理員，然後按一下 **OK**（確定）。
5. 若要按位置篩選還原範圍，可清除要排除的位置。
6. **Revert**（還原）變更。

還原至候選組態的預設快照。

這是您在按一下 Web 介面頂端的 **Config**（組態） > **Save Changes**（儲存變更）時建立或覆寫的快照。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作），然後 **Revert to last saved configuration**（還原至上次儲存的組態）。
2. 按一下 **Yes**（是）以確認操作。
3. （選用）按一下 **Commit**（提交）可使用快照覆寫執行中組態。

還原至之前儲存於防火牆上的執行中組態版本。

每當您提交組態變更時，防火牆會建立一個版本。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作），然後 **Load configuration version**（載入組態版本）。
2. 選取組態 **Version**（版本），然後按一下 **OK**（確定）。
3. （選用）按一下 **Commit**（提交）可使用您剛才復原的版本覆寫執行中組態。

©2024 Palo Alto Networks, Inc.

還原至下列其中一項：

- 您之前匯入的自訂版本執行中組態
- 自訂具名候選組態快照（而非預設快照）

1. 選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作），然後按一下 **Load named configuration snapshot**（載入具名組態快照）。
2. 選取快照 **Name**（名稱），然後按一下 **OK**（確定）。
3. （選用）按一下 **Commit**（提交）可使用快照覆寫執行中組態。

還原至您之前匯出至外部主機的執行中組態或候選組態。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作），按一下 **Import named configuration snapshot**（匯入具名組態快照），**Browse**（瀏覽）至外部主機上的組態檔案，然後按一下 **OK**（確定）。
2. 按一下 **Load named configuration snapshot**（上載具名組態快照），選取您剛才匯入的組態 **Name**（名稱），然後按一下 **OK**（確定）。
3. （選用）按一下 **Commit**（提交）可使用您剛才匯入的快照覆寫執行中組態。

還原您從防火牆匯出的狀態資訊。

除了執行中設定，狀態資訊還包括從 Panorama 推送的裝置群組及範本設定。如果防火牆是 GlobalProtect 入口網站，資訊還將包含憑證資訊、衛星清單以及衛星驗證資訊。如果取代防火牆或入口網站，您可透過匯入狀態包來還原取代時的資訊。

匯入狀態資訊：

1. 選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作），按一下 **Import device state**（匯入裝置狀態），**Browse**（瀏覽）至狀態包，然後按一下 **OK**（確定）。
2. （選用）按一下 **Commit**（提交）將匯入的狀態資訊套用至執行中組態。

©2024 Palo Alto Networks, Inc.

管理防火牆管理員

管理帳戶為 Palo Alto Networks 防火牆的管理員指定角色與驗證方法。每個 Palo Alto Networks 防火牆都已預先定義預設管理帳戶（管理員），此帳戶擁有完整的防火牆讀寫存取權（也稱為超級使用者存取權）。

最佳做法是為每個需要存取防火牆的管理或報告功能的人員，建立單獨的管理帳戶。這可讓您更有效保護防火牆免於未經授權設定，並啟用個別管理員的動作日誌記錄。務必遵照管理存取權的最佳做法，來確保您可以保護防火牆以及其他安全性裝置的管理存取權，以防攻擊成功。

- 管理角色類型
- 設定管理員角色設定檔
- 管理驗證
- 設定管理帳戶和驗證
- 設定管理員活動的追蹤

管理角色類型

角色可定義管理員具有的防火牆存取權類型。管理員類型包括：

- 以角色為基礎的角色 — 為了能夠更精確地存取控制網頁介面、CLI 及 XML API 的功能區，您可以設定的自訂角色。例如，您可為操作人員建立管理員角色設定檔，提供網頁介面防火牆及網路設定區域的存取權，以及為安全性管理員建立單獨設定檔，提供安全性原則定義、日誌與報告的存取權。在具有多個虛擬系統的防火牆上，您可以選取角色是為所有虛擬系統定義存取權還是為特定虛擬系統定義存取權。新功能新增至產品後，您必須用相應的存取權限更新角色：防火牆不會自動新增新功能至自訂角色定義。如需可以為自訂管理員角色設定的權限詳細資料，請參閱 參考：Web 介面管理員存取權 。
- 動態角色 — 此內建角色可提供防火牆的存取權。當新增新功能時，防火牆會自動更新動態角色的定義，您永遠不用手動更新這些定義。下表列出與動態角色相關的存取權限。

動態角色	權限
超級使用者	擁有完整存取防火牆的權限，包括定義新管理員帳戶及虛擬系統。您必須擁有超級使用者權限，才可建立具有超級使用者權限的管理員使用者。
超級使用者（唯讀）	對防火牆的唯讀存取（以唯讀狀態啟用 XML API）。
裝置管理員	擁有完整存取所有防火牆設定的權限，定義新帳戶或虛擬系統除外。

©2024 Palo Alto Networks, Inc.

動態角色	權限
裝置管理員（唯讀）	擁有唯讀存取所有防火牆設定的權限，密碼設定檔（不可存取）及管理員帳戶（僅登入帳戶可見）除外。
虛擬系統管理員	存取防火牆上的選定虛擬系統以建立和管理虛擬系統的特定方面。虛擬系統管理員無法存取網路介面、VLAN、Virtual Wire、虛擬路由器、IPSec 通道、GRE 通道、DHCP、DNS Proxy、QoS、LLDP 或網路設定檔。
虛擬系統管理員（唯讀）	對防火牆上的選定虛擬系統和虛擬系統的特定方面具有唯讀存取權限 。具有唯讀存取權限的虛擬系統管理員無法存取網路介面、VLAN、Virtual Wire、虛擬路由器、IPSec 通道、GRE 通道、DHCP、DNS Proxy、QoS、LLDP 或網路設定檔。

設定管理員角色設定檔

管理員角色設定檔可讓您定義精確的管理存取權限，以確保對敏感公司資訊與一般使用者隱私權的保護。

遵照最低權限存取的原則，建立僅允許管理員存取執行其工作必須存取之管理介面區域的管理員角色設定檔，并遵照管理存取權的最佳做法。

STEP 1 | 選取 **Device**（裝置） > **Admin Roles**（管理員角色），然後按一下 **Add**（新增）。

STEP 2 | 輸入用來識別角色的 **Name**（名稱）。

STEP 3 | 針對 **Role**（角色）的範圍，選取 **Device**（裝置）或 **Virtual System**（虛擬系統）。

STEP 4 | 在 **Web UI**（**Web** 使用者介面）及 **REST API** 頁籤中，按一下每個功能區域的圖示，以將其切換為所需設定：啟用、唯讀或停用。對於 **XML API** 頁簽，選取「啟用」或「停用」。關於 **Web UI**（**Web** 使用者介面）選項的詳細資訊，請參閱 Web 介面存取權限。

©2024 Palo Alto Networks, Inc.

STEP 5 | 選取 **Command Line**（命令列）頁籤，然後選取 CLI 存取權選項。**Role**（角色）範圍控制可用選項：

- 裝置角色：
  - **None**（無）—不允許存取 CLI（預設值）。
  - **superuser**（超級使用者）—完整存取權。可以定義新的管理員帳戶和虛擬系統。只有超級使用者可以建立具有超級使用者權限的管理員使用者。
  - **superreader**（超級讀取者）—完整唯讀存取權。
  - **deviceadmin**（裝置管理員）—對所有設定的完整存取權，定義新帳戶或虛擬系統除外。
  - **devicereader**（裝置讀取者）—對所有設定的唯讀存取權，密碼設定檔（不可存取）及管理員帳戶（僅登入帳戶可見）除外。
- 虛擬系統角色：
  - **None**（無）—不允許存取（預設值）。
  - **vsysadmin**（虛擬系統管理員）—可存取特定虛擬系統以建立和管理虛擬系統的特定方面。不支援對防火牆層級或網路層級功能的存取，包括靜態和動態路由、介面 IP 位址、IPsec 通道、VLAN、虛擬介接、虛擬路由器、GRE 通道、DCHP、DNS Proxy、QoS、LLDP 或網路設定檔。
  - **vsysreader**（虛擬系統讀取者）—對特定虛擬系統或虛擬系統之特定層面的唯讀存取權。不支援對防火牆層級或網路層級功能的存取，包括靜態和動態路由、介面 IP 位址、IPsec 通道、VLAN、虛擬介接、虛擬路由器、GRE 通道、DCHP、DNS Proxy、QoS、LLDP 或網路設定檔。

STEP 6 | 按一下 **OK**（確定）來儲存設定檔。

STEP 7 | 為管理員指定角色。請參閱設定防火牆管理員帳戶。

管理員角色設定檔建構範例

此範例顯示需要存取權以調查潛在問題之安全性作業中心 (SOC) 管理員的管理員角色設定檔。SOC 管理員需要對防火牆內許多區域的讀取權限，但通常不需要寫入權限。此範例涵蓋了管理員角色設定檔的全部四個頁籤，每個步驟說明設定檔為 SOC 管理員啟用或停用對特定區域存取權限的原因。

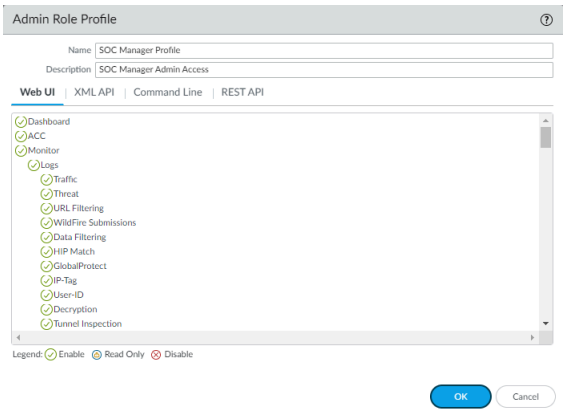
這是虛構 *SOC* 管理員的範例設定檔。根據管理員管理員管理的功能和完成工作所需的存取權限，為您的管理員設定管理員角色設定檔。不要啟用不必要的存取權限。為擁有相同職責的每個管理群組以及擁有獨特職責的管理員建立單獨的設定檔。每個管理員都應具有執行其職責所需的確切存取層級，而不能擁有除此之外的存取權限。

©2024 Palo Alto Networks, Inc.

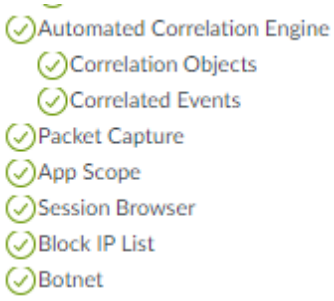
STEP 1 | 設定 Web UI 存取權限。Web UI 螢幕的每個剪取都會顯示不同的 Web UI 權限區域。權限會列在防火牆頁籤中，依您在 Web UI 中看到頁籤的順序列出，然後是其他動作的權限。

防火牆的 **Dashboard**（儀表板）、**ACC** 和 **Monitor**（監控）> **Logs**（日誌）區域不包含設定元素—所有物件都是資訊內容（您只能在啟用和停用之間進行切換，因為它們已經是唯讀）。由於 SOC 管理員需要調查潛在的問題，因此 SOC 管理員需要存取這些頁籤上的資訊。

設定檔名稱和描述可讓您輕鬆理解設定檔的目標。此剪取不會顯示所有的 **Logs**（日誌）權限，但所有這些權限都已對此設定檔啟用。



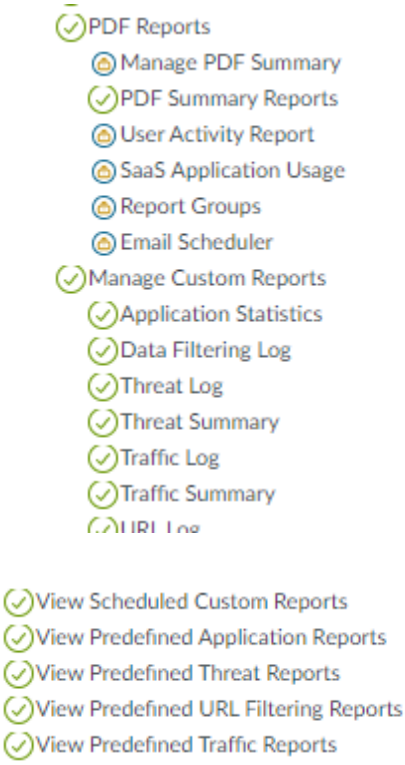
下一個剪取會顯示 **Monitor**（監控）頁籤上更多資訊性物件的權限。SOC 管理員使用這些工具來調查潛在的問題，因此需要存取權限。



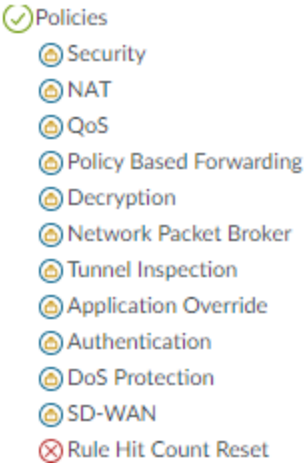
接下來的兩個剪取會顯示 **Monitor**（監控）頁籤上 PDF 報告、自訂報告和預先定義報告的權限。雖然 SOC 管理員需要存取 PDF 報告才能收集資訊，但在此範例中，SOC 管理員不需要設定報告，因此存取權限設定為唯讀（摘要報告無法設定）。不過，SOC 管理員需要管理自訂報

©2024 Palo Alto Networks, Inc.

告以調查具體潛在問題，因此會授予對所有自訂報告（包括剪取中未顯示的報告）的完整存取權限。最後，SOC 管理員需要存取預先定義的報告，以調查潛在問題。



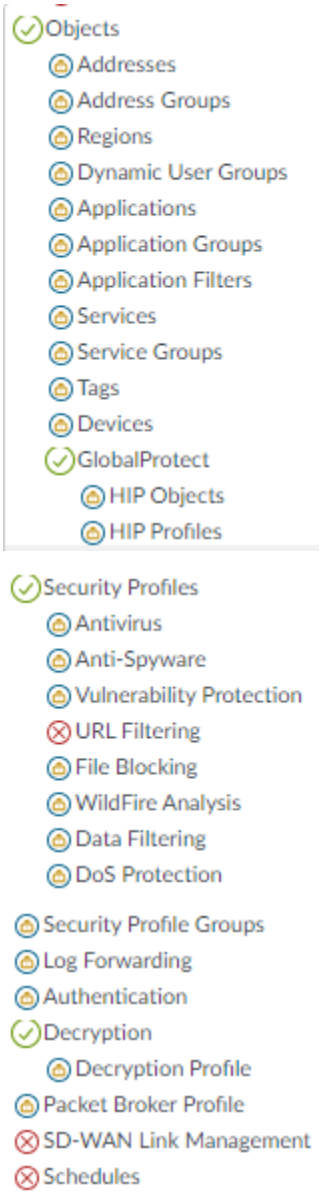
由於 SOC 管理員是調查員，而不是設定防火牆的管理員，所以 **Policies**（原則）頁籤的權限為唯讀，但重設規則命中計數除外。重設規則命中計數不是 SOC 管理員的職責之一（變更命中計數可能會對其他管理員造成不利影響或產生混淆），因此會停用存取權限。讀取權限可讓 SOC 管理員調查其懷疑可能造成問題的原則之建構。



Objects（物件）頁籤也出於相同原因而具有唯讀權限—SOC 管理員的工作不需要設定，因此不會指派任何設定權限。對於未包含在 SOC 管理員職責中的區域，會停用存取權限。在此範例中，SOC 管理員擁有唯讀權限，可調查所有物件的物件設定，但 **URL Filtering**（**URL** 篩

 ©2024 Palo Alto Networks, Inc.

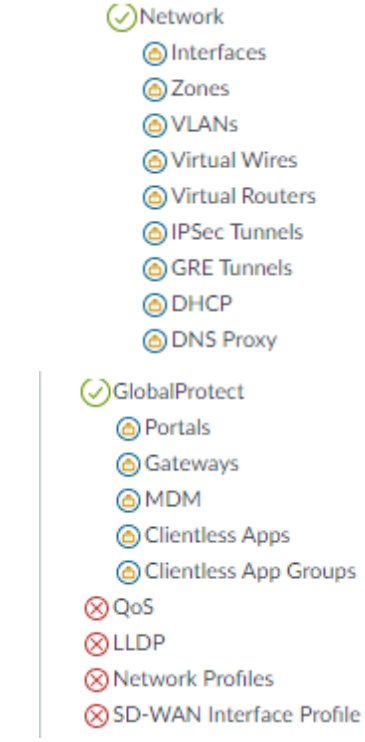
選）、**SD-WAN Link Management**（**SD-WAN** 連結管理）和 **Schedules**（排程）除外，這些設定在此範例中由其他管理員控制。



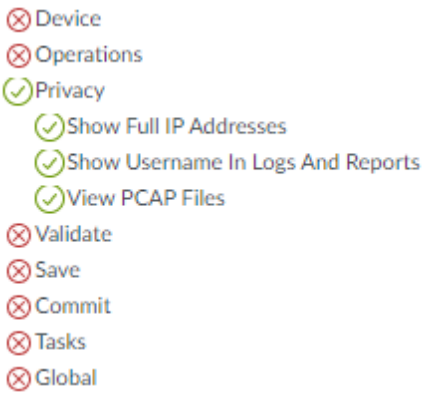
對於 **Network**（網路）頁籤權限，情況類似：SOC 管理員不需要設定任何物件，但可能需要資訊來調查問題，因此會向 SOC 管理員指派其可能需要調查之區域的唯讀權限。在此範例中，已

 ©2024 Palo Alto Networks, Inc.

停用對 QoS、LDP、網路設定檔或 SD-WAN 介面設定檔的存取權限，因為這些項目不屬於 SOC 管理員職責的一部分。



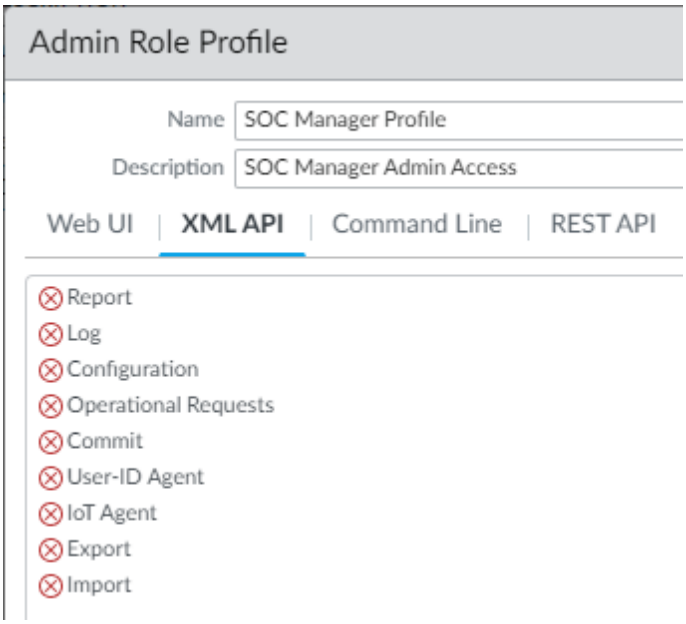
在此範例中，SOC 管理員不需要存取 **Device**（裝置）頁籤功能來進行調查，因此所有 **Device**（裝置）頁籤權限都會被封鎖。此外，調查不需要提交動作或存取任何其餘動作，因此這些權限也會被封鎖。



 ©2024 Palo Alto Networks, Inc.

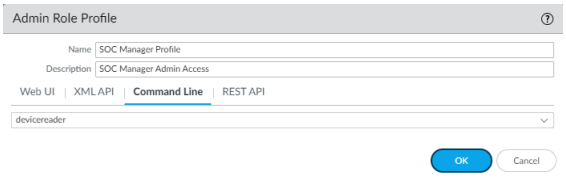
STEP 2 | 設定 XML API 存取權限。

下列剪取顯示已為 SOC 管理員停用所有 XML API 權限，因為 SOC 管理員不會使用 XML API 命令存取防火牆。



STEP 3 | 設定命令列 (CLI) 存取權限。

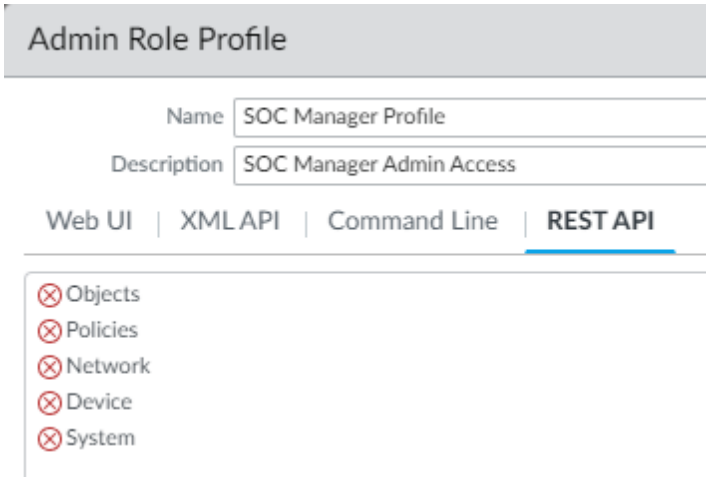
SOC 管理員擁有 CLI 唯讀存取權限，因為 SOC 管理員需要存取日誌和其他監控工具，而且還需要能夠查看特定設定，才能調查潛在問題。不過，SOC 管理員不會設定防火牆，因此不會指派任何設定權限。存取層級設定為 **devicereader**（裝置讀取者），而非 **superreader**（超級讀取者），因為 SOC 管理員不需要存取密碼設定檔或其他管理帳戶。



©2024 Palo Alto Networks, Inc.

STEP 4 | 設定 REST API 存取權限。

SOC 管理員不會使用 REST API 命令來存取防火牆，因此所有 REST API 存取權限都會停用。



管理驗證

您可以為防火牆管理員設定以下類型的驗證及授權（角色和存取網域指派）：

驗證方法	授權方法	說明
本地	本地	管理帳戶認證與驗證機制對於防火牆而言都屬於本機。您可以定義具有或不具有屬於防火牆本機之使用者資料庫的帳戶—關於使用本機資料庫的優點和缺點，請參閱本機驗證。您可以使用防火牆管理角色指派，但不支援存取網域。詳細資訊，請參閱為防火牆管理員設定本機或外部驗證。
SSH 金鑰	本地	管理帳戶屬於防火牆本機，但 CLI 的驗證基於 SSH 金鑰。您可以使用防火牆管理角色指派，但不支援存取網域。如需詳細資訊，請參閱設定 CLI 的 SSH 金鑰式管理員驗證。
憑證	本地	管理帳戶屬於防火牆本機，但 Web 介面的驗證基於用戶端憑證。您可以使用防火牆管理角色指派，但不支援存取網域。如需詳細資訊，請參閱設定 Web 介面的憑證式管理員驗證。
外部服務	本地	您在防火牆上本機定義的管理帳戶將用作在外多因素驗證、SAML、Kerberos、TACACS+、RADIUS 或 LDAP 伺服器上定義之帳戶的參考。外部伺服器將執行驗證。您可以使用防火牆管理角色指派，但不支援存取網域。詳細資訊，請參閱為防火牆管理員設定本機或外部驗證。
外部服務	外部服務	在外部 SAML、TACACS+ 或 RADIUS 伺服器上定義管理帳戶。伺服器將執行驗證和授權。對於授權，您需在 TACACS+ 或

©2024 Palo Alto Networks, Inc.

驗證方法	授權方法	說明
		RADIUS 伺服器上定義廠商特定屬性 (VSA)，或在 SAML 伺服器上定義 SAML 屬性。PAN-OS 會將這些屬性對應到您在防火牆上定義的管理員角色、存取網域、使用者群組以及虛擬系統。如需詳細資訊，請參閱： • 設定 SAML 驗證 • 設定 TACACS+ 驗證 • 設定 RADIUS 驗證

設定管理帳戶和驗證

如果您已設定驗證設定檔（請參閱設定驗證設定檔和順序）或者您不要求驗證管理員，則您隨時可以設定防火牆管理員帳戶。否則，執行下列其他程序之一，以為特定驗證類型設定管理帳戶。

- 設定防火牆管理員帳戶
- 為防火牆管理員設定本機或外部驗證
- 將憑證式管理員驗證設定為網頁介面
- 設定 CLI 的 SSH 金鑰式管理員驗證
- 設定 API 金鑰生命週期

設定防火牆管理員帳戶

管理帳戶指定了防火牆管理員的角色和驗證方法。您用於指派角色和執行驗證的服務將決定您是要在防火牆、外部伺服器還是二者上新增帳戶（請參閱管理驗證）。如果驗證方法依賴於本機防火牆資料庫或外部服務，您必須在新增管理帳戶之前，設定驗證設定檔（請參閱設定管理帳戶和驗證）。如果您已設定驗證設定檔或者您將使用沒有防火牆資料庫的本機驗證，則執行以下步驟，以在防火牆上新增管理帳戶。

為每個需要存取防火牆的管理或報告功能的人員建立單獨的管理帳戶。這可讓您更有效保護防火牆免於未經授權設定，並啟用個別管理員的動作記錄。

務必遵照管理存取權的最佳做法，來確保您可以保障防火牆以及其他安全性裝置的管理存取權，以防攻擊成功。

©2024 Palo Alto Networks, Inc.

STEP 1 | 修改支援的管理員帳戶數目。

在正常操作模式或 FIPS-CC 模式中，設定防火牆支援的並行管理帳戶工作階段總數。您可以允許最多四個並行管理帳戶工作階段，或將防火牆設定為支援無限數目的並行管理帳戶工作階段。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理），然後編輯 Authentication Settings（驗證設定）。
2. 編輯 **Max Session Count**（最大工作階段計數）以指定允許為所有管理員和使用者帳戶支援的並行工作階段數目（範圍為 **0** 至 **4**）。

   輸入 **0** 以設定防火牆支援無限數目的管理帳戶。
3. 為管理帳戶編輯 **Max Session Time**（最大工作階段時間）（分鐘）。預設值為 720 分鐘。
4. 按一下 **OK**（確定）。
5. **Commit**（認可）。

您也可以透過登入防火牆 CLI 來設定支援的並行工作階段總數。

```
admin> configure
```

```
admin# set deviceconfig setting management admin-session
 max-session-count <0-4>
```

```
admin# set deviceconfig setting management admin-session
 max-session-time <0, 60-1499>
```

```
admin# 提交
```

STEP 2 | 選取 **Device**（裝置） > **Administrators**（管理員），然後**Add**（新增）帳戶。

STEP 3 | 輸入使用者 **Name**（名稱）。

如果防火牆使用本機資料庫來驗證帳戶，則在資料庫中輸入您為帳戶指定的名稱（請參閱新增使用者群組到本機資料庫。）

STEP 4 | 如果您已為管理員設定任何一項，則選取 **Authentication Profile**（驗證設定檔）或順序。

如果防火牆為帳戶使用沒有本機使用者資料庫的本機驗證，則選取 **None**（無）（預設），然後輸入 **Password**（密碼）。

STEP 5 | 選取 **Administrator Type**（管理員類型）。

如果您為使用者設定自訂角色，請選取 **Role Based**（以角色為基礎），並選取管理員角色 **Profile**（設定檔）。否則，請選取**Dynamic**（動態）（預設值），並選取動態角色。如果動態

©2024 Palo Alto Networks, Inc.

角色為 **virtual system administrator**（虛擬系統管理員），新增一個或多個允許虛擬系統管理員管理的虛擬系統。

STEP 6 | （選用）為防火牆在沒有本機使用者資料庫的情況下本機驗證的管理員選取 **Password Profile**（密碼設定檔）。詳細資訊，請參閱定義密碼設定檔。

STEP 7 | 按一下 **OK**（確定）與 **Commit**（提交）。

為防火牆管理員設定本機或外部驗證

您可以使用本機驗證及外部驗證服務來驗證存取防火牆的管理員。這些驗證方法將提示管理員回應一個或多個驗證挑戰，例如輸入使用者名稱和密碼的登入頁面。

如果您使用外部服務來管理驗證和授權（角色和存取網域指派），請參閱：

- 設定 SAML 驗證
- 設定 TACACS+ 驗證
- 設定 RADIUS 驗證

若要在不使用挑戰回應機制的情況下驗證管理員，可以設定 Web 介面的憑證式管理員驗證及設定 CLI 的 SSH 金鑰式管理員驗證。

STEP 1 | （僅限外部驗證）啟用防火牆，以連線至用於驗證管理員的外部伺服器。

設定伺服器設定檔：

- 新增 RADIUS 伺服器設定檔。

  如果防火牆透過 RADIUS 整合 多因素驗證 (MFA) 服務，則必須新增 RADIUS 伺服器設定檔。在此情況下，MFA 服務將提供所有驗證因素（挑戰）。若防火牆透過廠商 API 整合 MFA 服務，您仍可使用 RADIUS 伺服器作為第一個因素，但其他因素需要使用 MFA 伺服器設定檔。
- 新增 MFA 伺服器設定檔。
- 新增 TACACS+ 伺服器設定檔。
- 新增 SAML IdP 伺服器設定檔。無法組合使用 Kerberos 單一登入 (SSO) 和 SAML SSO；您只能使用一種類型的 SSO 服務。
- 新增 Kerberos 伺服器設定檔。
- 新增 LDAP 伺服器設定檔。

STEP 2 | （僅限本機資料庫驗證）設定屬於伺服器本機的使用者資料庫。

1. 新增使用者帳戶到本機資料庫。
2. （選用）新增使用者帳戶到本機資料庫。

©2024 Palo Alto Networks, Inc.

STEP 3 | （僅限本機驗證）定義密碼複雜性和過期設定。

這些設定讓攻擊者難以猜測密碼，保護防火牆免受未經授權的存取。

1. 定義所有本機管理員的全域密碼複雜性及到期設定。這些設定並不會套用於您指定了密碼雜湊取代密碼的本機資料庫帳戶（請參閱本機驗證）。
   1. 選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理），然後編輯 Minimum Password Complexity（最小密碼複雜性）設定。
   2. 選取 **Enabled**（已啟用）。
   3. 定義密碼設定，然後按一下 **OK**（確定）。
2. 定義 Password Profile（密碼設定檔）。

   將設定檔指派給您要覆寫全域密碼過期設定的管理員帳戶。這些設定檔僅可供與本機設定檔無關聯的帳戶使用（請參閱本機驗證）。
   1. 選取 **Device**（裝置） > **Password Profiles**（密碼設定檔），然後 **Add**（新增） 設定檔。
   2. 輸入用來識別設定檔的 **Name**（名稱）。
   3. 定義密碼到期設定，然後按一下 **OK**（確定）。

STEP 4 | （僅限 Kerberos SSO）建立 Kerberos 金鑰標籤。

金鑰標籤是一個檔案，包含了防火牆的 Kerberos 帳戶資訊。您的網路必須有 Kerberos 基礎結構才能支援 Kerberos SSO。

STEP 5 | 設定驗證設定檔。

如果您的管理帳戶儲存在多種類型的伺服器上，則可以為每種類型建立一個驗證設定檔，並將所有設定檔新增至驗證順序。

設定驗證設定檔和順序。在驗證設定檔中，指定驗證服務的 **Type**（類型）和相關設定：

- 外部服務—選取外部服務的 **Type**（類型），然後選取您為其建立的 **Server Profile**（伺服器組態）。
- 本機資料庫驗證—將 **Type**（類型）設定為 **Local Database**（本機資料庫）。
- 不使用資料庫的本機驗證—將 **Type**（類型）設定為 **None**（無）。
- **Kerberos SSO**—指定 **Kerberos Realm**（**Kerberos** 領域），然後 **Import**（匯入）**Kerberos Keytab**（**Kerberos** 金鑰標籤）。

©2024 Palo Alto Networks, Inc.

STEP 6 | 將驗證設定檔或順序指定給管理員帳戶。

1. 設定防火牆管理員帳戶。
   - 指派您所設定的 **Authentication Profile**（驗證設定檔）或順序。
   - （僅限本機資料庫驗證）指定您新增至本機資料庫的使用者帳戶 **Name**（名稱）。
2. **Commit**（提交）您的變更。
3. （選用）測試驗證伺服器連線，以驗證防火牆是否能使用驗證設定檔驗證管理員。

將憑證式管理員驗證設定為網頁介面

作為對防火牆 Web 介面來說比密碼式驗證更安全的驗證方法，您可以設定憑證式管理員帳戶驗證，該驗證為防火牆本機驗證。憑證式驗證涉及交換及驗證數位特徵碼，而非密碼。

為任何管理員設定憑證式驗證會停用防火牆上所有管理員的使用者名稱/密碼登入；因此之後管理員需要憑證才能登入。

STEP 1 | 在防火牆上產生憑證授權單位 (CA) 憑證。

您將使用此 CA 憑證來簽署每個管理員的用戶端憑證。

建立自我簽署根 CA 憑證。

或者，從企業 *CA* 或協力廠商 *CA* 匯入憑證與私密金鑰。

STEP 2 | 設定憑證設定檔以安全存取網頁介面。

設定憑證設定檔。

- 將 **Username Field**（使用者名稱欄位）設定為 **Subject**（主旨）。
- 在 CA 憑證區段中，**Add**（新增）您剛建立或匯入的 **CA Certificate**（**CA** 憑證）。

STEP 3 | 將防火牆設定為使用憑證設定檔以驗證管理員。

1. 選取 **Device**（裝置）> **Setup**（設定）> **Management**（管理），然後編輯 Authentication Settings（驗證設定）。
2. 選取您建立用於驗證管理員的 **Certificate Profile**（憑證設定檔），然後按一下 **OK**（確定）。

STEP 4 | 將管理員帳戶設定為使用用戶端憑證驗證。

對於每位將存取防火牆 Web 介面的管理員，設定防火牆管理員帳戶，然後 **Use only client certificate authentication**（僅使用用戶端憑證驗證）。

如果您已部署企業 CA 產生的用戶端憑證，請跳至步驟 8。否則，進行步驟 5。

STEP 5 | 針對每個管理員產生用戶端憑證。

產生憑證。在 **Signed By**（簽署者）下拉式清單中，選取自我簽署的根 CA 憑證。

©2024 Palo Alto Networks, Inc.

STEP 6 | 匯出用戶端憑證。

1. 匯出憑證與私密金鑰。
2. **Commit**（提交）您的變更。防火牆會重新啟動並終止您的登入工作階段。之後管理員只能從擁有您產生之用戶端憑證的用戶端系統存取網頁介面。

STEP 7 | 將用戶端憑證匯入將存取網頁介面之每個管理員的用戶端系統。

請參閱您的網頁瀏覽器文件。

STEP 8 | 確認管理員可以存取 Web 介面。

1. 在擁有用戶端憑證之電腦上的瀏覽器中開啟防火牆 IP 位址。
2. 出現提示時，選取您匯入憑證，並按一下 **OK**（確定）。瀏覽器會顯示憑證警告。
3. 將憑證新增至瀏覽器例外狀況清單：
4. 按一下 **Login**（登入）。網頁介面會顯示出來，而不會提示您輸入使用者名稱或密碼。

設定 CLI 的 SSH 金鑰式管理員驗證

針對使用 Secure Shell（安全殼層，SSH）存取 Palo Alto Networks 防火牆之 CLI 的管理員，SSH 金鑰會提供比密碼更安全的驗證方法。SSH 金鑰幾乎可以消除暴力密碼破解攻擊的風險，提供雙因素驗證（金鑰與複雜密碼）的選項，且不會透過網路傳送密碼。SSH 金鑰也可以啟用自動指令碼來存取 CLI。

STEP 1 | 使用 SSH 金鑰產生工具，在管理員的用戶端系統上建立非對稱金鑰配對。

支援的金鑰格式是 IETF SECSH 與 Open SSH。支援的演算法是 DSA (1024 位元) 和 RSA (768 - 4,096 位元)。

如需產生金鑰配對的命令，請參閱您的 SSH 用戶端文件。

公開金鑰與私密金鑰是不同的檔案。將這兩個檔案儲存至防火牆可存取的位置。為了增加安全性，請輸入複雜密碼來加密私人金鑰。登入期間，防火牆會提示管理員輸入此複雜密碼。

STEP 2 | 將管理員帳戶設定為使用公開金鑰驗證。

1. 設定防火牆管理員帳戶。
   - 將驗證方法設定為 SSH 金鑰驗證失敗時作為遞補使用。如果您已為管理員設定 **Authentication Profile**（驗證設定檔），請在下拉式清單中選取它。如果您選取 **None**（無），則必須輸入 **Password**（密碼）與 **Confirm Password**（確認密碼）。
   - 選取 **Use Public Key Authentication (SSH)**（使用私人金鑰驗證 **(SSH)**），然後按一下 **Import Key**（使用私人金鑰驗證 **(SSH)**），**Browse**（瀏覽）至您剛產生的公開金鑰，再按一下 **OK**（確定）。
2. **Commit**（提交）您的變更。

STEP 3 | 設定 SSH 用戶端，使用私人金鑰向防火牆進行驗證。

對管理員的用戶端系統執行此工作。如需步驟相關資訊，請參閱您的 SSH 用戶端文件。

©2024 Palo Alto Networks, Inc.

STEP 4 | 確認管理員可以使用 SSH 金鑰驗證存取防火牆 CLI。

1. 使用管理員之用戶端系統上的瀏覽器，前往防火牆 IP 位址。
2. 以管理員身分登入防火牆 CLI。輸入使用者名稱之後，您將看到下列輸出 (金鑰值為範例)：

```
使用公開金鑰「dsa-key-20130415」驗證
```

3. 如果出現提示，請輸入您在建立金鑰時所定義的複雜密碼。

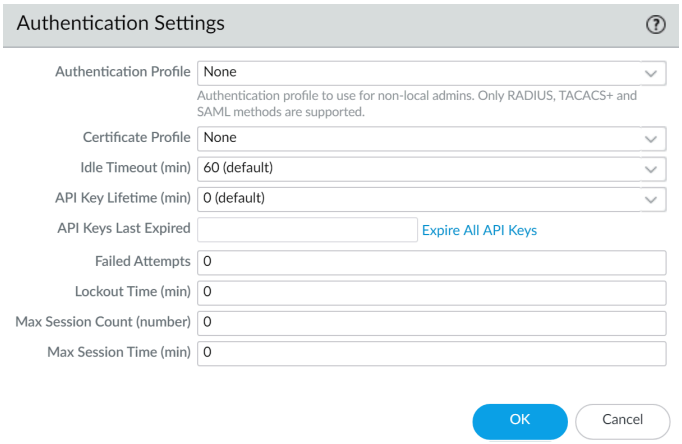
設定 API 金鑰生命週期

防火牆和 Panorama 上的 API 金鑰讓您可以驗證對 XML API 和 REST API 的 API 呼叫。由於這些金鑰能夠授予防火牆和 Panorama 的存取權限，而防火牆和 Panorama 是確保網路安全的重要因素，因此最佳做法是，指定 API 金鑰生命週期以定期執行金鑰輪換。指定金鑰生命週期後，在重新產生 API 金鑰時，所有金鑰都是唯一的。

除了設定金鑰生命週期以提示您定期重新產生新的金鑰外，您還可在一個或多個金鑰遭到洩漏時撤消目前有效的所有 API 金鑰。撤消金鑰會使目前有效的所有金鑰到期。

STEP 1 | 選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理）。

STEP 2 | 編輯驗證設定以指定 **API Key Lifetime (min)**（**API** 金鑰生命週期（分鐘））。



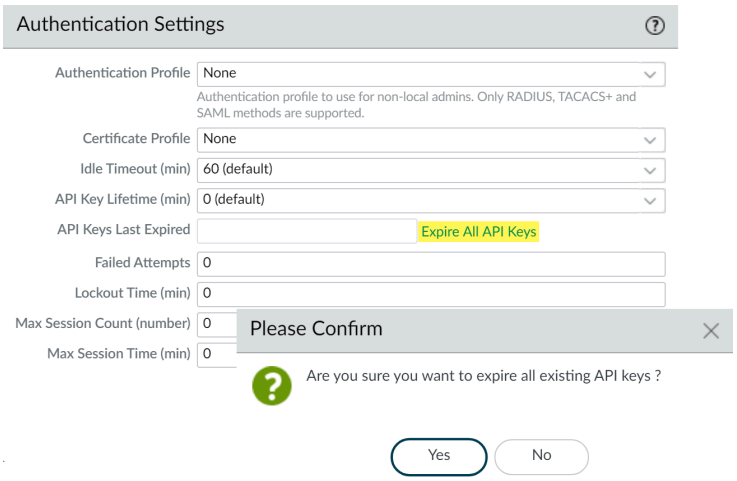
設定 API 金鑰生命週期以防止金鑰遭到洩漏並降低意外洩漏的影響。依預設，API 金鑰生命週期設為 0，這意味著金鑰永遠都不會到期。若要確保金鑰經常輪換且所有金鑰在重新產生時都是唯一的，您必須指定一個介於 1 和 525600 分鐘之間的有效期間。請參閱您企業的稽核與合規原則，以確定應如何指定 API 金鑰有效的生命週期。

STEP 3 | **Commit**（提交）變更。

©2024 Palo Alto Networks, Inc.

STEP 4 | （要撤消所有 API 金鑰）選取 **Expire all API Keys**（使所有 **API** 金鑰到期）以重設目前有效的 API 金鑰。

如果您剛剛設定了金鑰生命週期並希望重設所有 API 金鑰以符合新的期限，可以使所有現有金鑰到期。



確認後，金鑰將被撤消，且您可檢視 **API Keys Last Expired**（**API** 金鑰上次到期時間）的時間戳記。

設定管理員活動的追蹤

追蹤管理員在防火牆網頁介面和 CLI 上的活動，以即時報告防火牆內的活動。如果您有理由認定管理員帳戶遭到入侵，則可以瞭解此管理員帳戶在整個網頁介面中所瀏覽位置或者他們所執行操作命令的完整歷程記錄，以便您可以詳細分析並對遭入侵管理員採取的所有動作作出回應。

當發生事件時，每次管理員瀏覽網頁介面或在 CLI 中執行操作命令時，都會產生稽核日誌並轉送至指定的 syslog 伺服器。系統會為每次導覽或執行命令產生稽核日誌。例如，如果您想要建立新的位址物件。當您按下 **Objects**（物件）時會產生稽核日誌，然後當您按下 Addresses（位址）時會產生第二條稽核日誌。

稽核日誌只會顯示為轉送至 syslog 伺服器的 syslog，無法在防火牆網頁介面中檢視。稽核日誌只能轉送至 syslog 伺服器，無法轉送至 Cortex Data Lake (CDL)，且不會本機儲存在防火牆上。

STEP 1 | 設定 syslog 伺服器設定檔，以轉送防火牆上管理員活動的稽核日誌。

需要執行這一步驟才能成功儲存稽核日誌，以便追蹤防火牆上的管理員活動。

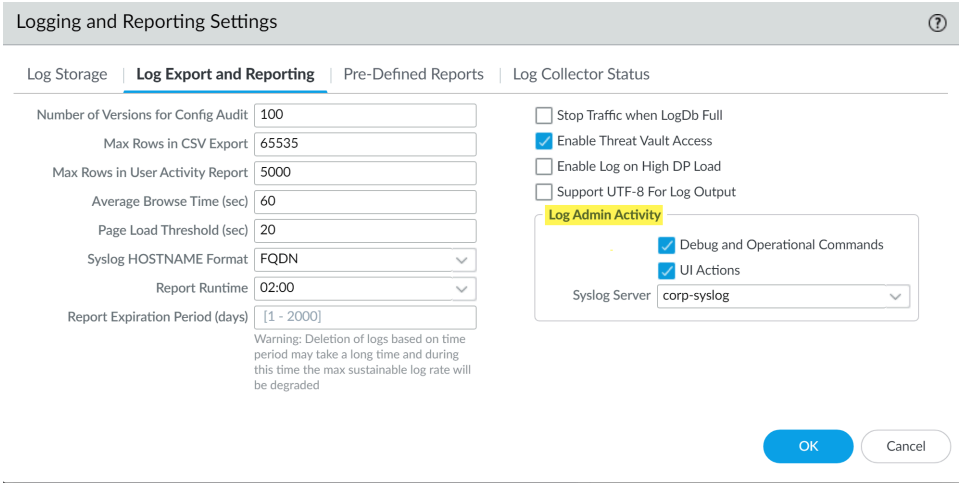
1. 登入防火牆網頁介面。
2. 設定 syslog 伺服器設定檔。

©2024 Palo Alto Networks, Inc.

STEP 2 | 設定管理員活動的追蹤。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理），然後編輯 Logging and Reporting Settings（日誌記錄與報告設定）。
2. 選取 **Log Export and Reporting**（日誌匯出與報告）。
3. 在「日誌管理員活動」區段中，設定要追蹤的管理員活動。
   - 操作命令—當管理員在 CLI 中執行操作或偵錯命令時，或者執行從網頁介面觸發的操作命令時，產生稽核日誌。如需 PAN-OS 操作和偵錯命令的完整清單，請參閱 CLI 操作命令階層。
   - **UI** 動作—當管理員瀏覽網頁介面時產生稽核日誌。這包括在設定頁籤之間進行導覽，以及在頁籤內的單個物件之間進行導覽。

     例如，當管理員從 **ACC** 導覽到 **Policies**（原則）頁籤時，會產生稽核日誌。此外，當管理員從**Objects**（物件） > **Addresses**（位址）導覽到**Objects**（物件） > **Tags**（標籤）時，會產生稽核日誌。
   - **Syslog** 伺服器—選取目標 syslog 伺服器設定檔以轉送稽核日誌。
4. 按一下 **OK**（確定）
5. 選取 **Commit**（提交）。



 ©2024 Palo Alto Networks, Inc.

參考：網頁介面管理員存取

您可以為整個防火牆或一或多個虛擬系統（在支援多個虛擬系統的平台上）設定權限。在指定 **Device**（裝置）或 **Virtual System**（虛擬系統）的情況下，您可以為自訂管理員角色設定權限，這些權限比與動態管理員角色相關聯的固定權限更精確。

設定精確層級的權限可確保較低層級的管理員無法存取某些資訊。您可以為防火牆管理員（請參閱設定防火牆管理員帳戶）、Panorama 管理員或裝置群組和範本管理員建立自訂角色（請參閱 Panorama 管理者指南）。您可以將管理員角色套用至基於角色的管理員帳戶，您可以在此指定一個或多個虛擬系統。下列主題說明您可以為自訂管理員角色設定的權限。

- 網頁介面存取權限
- Panorama Web 介面存取權限

網頁介面存取權限

如果您想要防止角色式管理員存取網頁介面上特定的標籤，您可以停用該標籤，如此當管理員使用相關聯的角色式管理帳戶登入時，甚至看不到該標籤。例如，您可為操作人員建立一個只能存取 **Device**（裝置）與 **Network**（網路）標籤的管理員角色設定檔，並為安全性管理員另外建立一個可存取 **Object**（物件）、**Policy**（原則）與**Monitor**（監控）頁簽的設定檔。

管理員角色可以在使用 **Device**（裝置）或 **Virtual System**（虛擬系統）選項按鈕定義的 **Device**（裝置）層級或 **Virtual System**（虛擬系統）層級套用。如果您選取 **Virtual System**（虛擬系統），指定此設定檔的管理員會受其獲指定的虛擬系統限制。此外，只有 **Device**（裝置） > **Setup**（設定） > **Services**（服務） > **Virtual Systems**（虛擬系統） 頁籤可供該管理員使用，而 **Global**（全域） 頁籤無法使用。

下列主題介紹了如何為 Web 介面的不同部分設定管理角色權限：

- 定義 Web 介面頁籤的存取權
- 提供監控標籤的精確存取權
- 提供原則標籤的細微存取權
- 提供物件標籤的精確存取權
- 提供網路標籤的精確存取權
- 提供裝置頁籤的精確存取權
- 定義管理員角色設定檔中的使用者隱私權設定
- 限制管理員存取提交和驗證功能
- 提供全域設定的精確存取權
- 提供 Panorama 頁籤的精確存取權
- 提供對操作設定的精確存取權

©2024 Palo Alto Networks, Inc.

定義 Web 介面頁籤的存取權

下表列出您可以指派給管理員角色設定檔的頂層存取權限（**Device**（裝置） > **Admin Roles**（管理員角色））。您可以為 Web 介面的頂層頁籤啟用、停用或定義唯讀存取權限。

存取層級	說明	啟用	唯讀	停用
儀錶盤	控制 **Dashboard**（儀表板）標籤的存取權。如果您停用此權限，管理員將看不到此標籤，也無法存取任何儀表板 Widget。	是	否。	是
ACC	控制存取應用程式監測中心 (ACC)。如果您停用此權限，**ACC** 標籤將不會顯示在 Web 介面中。請記住，如果您想要保護使用者的隱私權，但仍提供給使用者 ACC 的存取權，您可以停用 **Privacy**（隱私權） > **Show Full IP Addresses**（顯示完整 **IP** 位址）選項和/或 **Show User Names In Logs And Reports**（在日誌與報告中顯示使用者名稱） 選項。	是	否。	是
監控	控制 **Monitor**（監控）標籤的存取權。如果您停用此權限，管理員將看不到 **Monitor**（監控）標籤，且無法存取任何日誌、封包擷取、工作階段資訊、報告或 App Scope。若要更細微地控制管理員可看到的監控資訊，將 Monitor（監控）選項保持啟用，然後依照為監控頁籤提供細微存取權中所述啟用或停用頁籤上的特定節點。	是	否。	是
原則	控制**Policies**（原則）標籤的存取權。如果您停用此權限，管理員將看不到**Policies**（原則）標籤，也無法存取任何原則資訊。若要更細微地控制管理員可看到的原則資訊，例如允許存取特定類型的原則或允許唯讀存取原則資訊，將 **Policies**（原則）選項保持為啟用，然後依照為原則頁籤提供細微存取權中所述啟用或停用頁籤上的特定節點。	是	否。	是
物件	控制存取 **Objects**（物件）標籤。如果您停用此權限，管理員將看不到 **Objects**（物件）標籤，也無法存取任何物件、安全性	是	否。	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	啟用	唯讀	停用
	設定檔、日誌轉送設定檔、解密設定檔或排程。若要更細微地控制管理員可看到的物件，將 **Objects**（物件）選項保持啟用，然後按為物件頁籤提供細微存取權中所述啟用或停用頁籤上的特定節點。			
網路	控制存取 **Network**（網路）標籤。如果您停用此權限，管理員將看不到 **Network**（網路）標籤，也無法存取任何介面、區域、VLAN、虛擬連接、虛擬路由器、IPsec 通道、DHCP、DNS Proxy、GlobalProtect、QoS 組態資訊或網路設定檔。若要更細微地控制管理員可看到的物件，將 **Network**（網路）選項保持啟用，然後按為網路頁籤提供細微存取權中所述啟用或停用頁籤上的特定節點。	是	否。	是
裝置	控制 **Device**（裝置）標籤的存取權。如果您停用此權限，管理員將看不到 **Device**（裝置）頁籤，也無法存取任何裝置全域設定資訊，例如 User-ID、高可用性、伺服器設定檔或憑證組態資訊。若要更細微地控制管理員可看到的物件，將 **Objects**（物件）選項保持啟用，然後按為裝置頁籤提供細微存取權中所述啟用或停用頁籤上的特定節點。 即使您已啟用 ***Device***（裝置）頁籤的完整存取權，仍無法為角色式管理員啟用 ***Admin Roles***（管理員角色）或 ***Administrators***（管理員）節點的存取權。	是	否。	是

提供監控標籤的精確存取權

在某些狀況下，您可能需要允許管理員檢視 **Monitor**（監控）標籤的某些（但非全部）區域。例如，您可能想要限制操作管理員只能存取設定日誌與系統日誌，因為這些日誌不包含機密使用者資料。雖然管理員角色定義的這個區段可指定管理員能看到 **Monitor**（監控）頁籤的哪些區域，但您也可以將此區段中的權限與隱私權權限結合，例如停用能在日誌與報告看到使用者名稱的功能。但請記住，任何系統產生的報告仍將顯示使用者名稱與 IP 位址，即使您已停用角色的這個功能。基

©2024 Palo Alto Networks, Inc.

於此原因，如果您不想要管理員看到任何使用者的私人資訊，請停用特定報告的存取權，請見下表的詳細說明。

下表列出 **Monitor**（監控）頁籤存取層級，及這些層級可用的管理員角色。

設備群組與範本角色只能看到指定給這些角色之存取網域內設備群組的日誌資料。

存取層級	說明	管理員角色可用性	啟用	唯讀	停用
監控	啟用或停用 **Monitor**（監控）標籤的存取權。如果停用，管理員將看不到此標籤或任何相關聯的日誌或報告。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
日誌	啟用或停用所有日誌檔案的存取權。您也可以將此權限保持啟用，然後停用您不要管理員看到的特定日誌。請記住，如果您想要保護使用者的隱私權，但仍提供給使用者一或多個日誌的存取權，您可以停用 **Privacy**（隱私權） > **Show Full IP Addresses**（顯示完整 **IP** 位址）選項和/或 **Show User Names In Logs And Reports**（在日誌與報告中顯示使用者名稱）選項。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
流量	指定管理員是否能看到流量日誌。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
威脅	指定管理員是否能看到威脅日誌。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
URL 篩選	指定管理員是否能看到 URL 篩選日誌。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	管理員角色可用性	啟用	唯讀	停用
WildFire 提交	指定管理員是否能看到 WildFire 日誌。這些日誌只有您具備 WildFire 使用授權時才可供使用。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
資料篩選	指定管理員是否能看到資料篩選日誌。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
HIP 比對	指定管理員是否能看到 HIP 比對日誌。HIP 比對日誌只有在您具備 GlobalProtect 授權（訂閱）時才可供使用。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
GlobalProtect	指定管理員是否能看到 GlobalProtect 日誌。這些日誌只有在您具備 GlobalProtect 授權（訂閱）時才可供使用。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
使用者-ID	指定管理員是否能看到 User-ID 日誌。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
GTP	指定行動網路營運商是否可查看 GTP 日誌。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
通道檢查	指定管理員是否能看到通道檢查日誌。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
SCTP	指定行動網路營運商是否可查看串流控制傳輸通訊協定 (SCTP) 日誌。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	管理員角色可用性	啟用	唯讀	停用
	您必須先在 *Panorama* 上啟用 *SCTP*（***Device***（裝置）> ***Setup***（設定）> ***Management***（管理）），才能控制管理員存取 *Panorama* 與裝置群組/範本的 *SCTP* 日誌、自訂報告或預先定義報告。				
組態設定	指定管理員是否能看到組態日誌。	防火牆：是 Panorama:是 裝置群組/範本：否。	是	否。	是
系統	指定管理員是否能看到系統日誌。	防火牆：是 Panorama:是 裝置群組/範本：否。	是	否。	是
警示	指定管理員是否能看到系統產生的警報。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
驗證	指定管理員是否能看到驗證日誌。	防火牆：是 Panorama:是 裝置群組/範本：否。	是	否。	是
自動關聯引擎	啟用或停用防火牆上產生之關聯物件與關聯事件日誌的存取權。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
關聯物件	指定管理員是否能檢視及啟用/停用關聯物件。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	管理員角色可用性	啟用	唯讀	停用
關聯的事件	指定管理員是否能檢視及啟用/停用關聯事件。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
封包擷取	指定管理員是否能從 **Monitor**（監控）頁籤看到封包擷取 (pcaps)。請記住，封包擷取是原始流量資料，因此可能包含使用者 IP 位址。停用**Show Full IP Addresses**（顯示完整 **IP** 位址）權限並不會混淆 pcap 中的 IP 位址，因此如果您對於使用者隱私權有所疑慮，應停用封包擷取權限。	防火牆：是 Panorama:否 裝置群組/範本：否。	是	是	是
App Scope	指定管理員是否能看到 App Scope 可見度與分析工具。啟用 App Scope 便允許存取所有的 **App Scope** 圖表。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
工作階段瀏覽器	指定管理員是否能瀏覽及篩選防火牆上的目前執行中工作階段。請記住，工作階段瀏覽器會顯示原始流量資料，因此可能包含使用者 IP 位址。停用**Show Full IP Addresses**（顯示完整 **IP** 位址）權限並不會混淆工作階段瀏覽器中的 IP 位址，因此如果您對於使用者隱私權有所疑慮，應停用**Session Browser**（工作階段瀏覽器）權限。	防火牆：是 Panorama:否 裝置群組/範本：否。	是	否。	是
封鎖 IP 清單	指定管理員是否可檢視封鎖清單（「啟用」或「唯讀」）並從清單中刪除項目（「啟用」）。如果停用此設定，則管理員將無法檢視或刪除封鎖清單中的項目。	防火牆：是 Panorama：在 Context Switch UI（內容切換 UI）下：是 範本:是	是	是	是
殭屍網路	指定管理員是否能產生與檢視 Botnet 分析報告，或以唯讀模	防火牆：是	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	管理員角色可用性	啟用	唯讀	停用
	式檢視 Botnet 報告。停用 **Show Full IP Addresses**（顯示完整 **IP** 位址）權限並不會混淆已排程 Botnet 報告中的 IP 位址，因此如果您對於使用者隱私權有所疑慮，應停用 **Botnet** 權限。	Panorama:否 裝置群組/範本：否。			
PDF 報告	啟用或停用所有 PDF 報告的存取權。您也可以將此權限保持啟用，然後停用不要讓管理員看到的特定 PDF 報告。請記住，如果您想要保護使用者的隱私權，但仍提供給使用者一或多個報告的存取權，您可以停用 **Privacy**（隱私權）> **Show Full IP Addresses**（顯示完整 **IP** 位址）選項和/或 **Show User Names In Logs And Reports**（在日誌與報告中顯示使用者名稱）選項。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
管理 PDF 摘要	指定管理員是否能檢視、新增或刪除 PDF 摘要報告定義。管理員具備唯讀存取權時能夠檢視 PDF 摘要報告定義，但無法新增或刪除定義。如果您停用此選項，管理員將無法檢視或新增/刪除報告定義。	防火牆：是 Panorama:是 裝置群組/範本：是	是	是	是
PDF 摘要報告	指定管理員是否能在 **Monitor**（監控）> **Reports**（報告）中檢視產生的 PDF 摘要報告。如果您停用此選項，**PDF Summary Reports**（**PDF** 摘要報告）類別將不會在 **Reports**（報告）節點中顯示。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
使用者活動報告	指定管理員是否能檢視、新增或刪除使用者活動報告定義並下載報告。管理員具備唯讀存取權時能夠檢視使用者活動報告定義，但無法新增、刪除或下載定義。	防火牆：是 Panorama:是 裝置群組/範本：是	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	管理員角色可用性	啟用	唯讀	停用
	如果您停用此選項，管理員會看不到此類別的 PDF 報告。				
SaaS 應用程式使用情況報告	指定管理員是否能檢視、新增或刪除 SaaS 應用程式使用報告。管理員具備唯讀存取權時能夠設定 SaaS 應用程式使用報告定義，但無法新增或刪除定義。如果您停用此選項，管理員將無法檢視或新增或刪除報告定義。	防火牆：是 Panorama:是 裝置群組/範本：是	是	是	是
報告群組	指定管理員是否能檢視、新增或刪除報告群組定義。管理員具備唯讀存取權時能夠檢視報告群組定義，但無法新增或刪除定義。如果您停用此選項，管理員會看不到此類別的 PDF 報告。	防火牆：是 Panorama:是 裝置群組/範本：是	是	是	是
電子郵件排程器	指定管理員是否能排程要以電子郵件傳送的報告群組。由於所產生要以電子郵件傳送的報告可能包含機密的使用者資料，且該資料無法藉由停用 **Privacy**（隱私權） > **Show Full IP Addresses**（顯示完整 **IP** 位址）選項及/或 **Show User Names In Logs And Reports**（在日誌與報告中顯示使用者名稱）選項予以刪除，又因為這些報告也可能會顯示管理員無法存取的日誌資料，因此如果您有使用隱私權需求的話，應停用 **Email Scheduler**（電子郵件排程器）選項。	防火牆：是 Panorama:是 裝置群組/範本：是	是	是	是
管理自訂報告	啟用或停用所有自訂報告功能的存取權。您也可以將此權限保持啟用，然後停用您不要管理員能夠存取的特定自訂報告類別。請記住，如果您想要保護使用者的隱私權，但仍提供給使用者一或多個報告的存取權，您可以停用	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	管理員角色可用性	啟用	唯讀	停用
	Privacy（隱私權） > **Show Full IP Addresses**（顯示完整 **IP** 位址）選項和/或 **Show User Names In Logs And Reports**（在日誌與報告中顯示使用者名稱）選項。 依排程執行的報告（而非視需要執行的報告）將顯示 *IP* 位址與使用者資訊。在此狀況下，請確定限制存取對應的報告區域。此外，對於包含日誌資料的報告，且該日誌資料包含在自管理員角色中排除的日誌內，自訂報告功能並不會限制產生此類報告的功能。				
應用程式統計資料	指定管理員是否能夠建立自訂報告以包含應用程式統計資料資料庫中的資料。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
資料篩選記錄	指定管理員是否能夠建立自訂報告以包含資料篩選日誌中的資料。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
威脅日誌	指定管理員是否能夠建立自訂報告以包含威脅日誌中的資料。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
威脅摘要	指定管理員是否能夠建立自訂報告以包含威脅摘要資料庫中的資料。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
流量日誌	指定管理員是否能夠建立自訂報告以包含流量日誌中的資料。	防火牆：是 Panorama:是	是	否。	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	管理員角色可用性	啟用	唯讀	停用
		裝置群組/範本：是			
流量摘要	指定管理員是否能夠建立自訂報告以包含流量摘要資料庫中的資料。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
URL 日誌	指定管理員是否能夠建立自訂報告以包含 URL 篩選日誌中的資料。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
URL 摘要	指定管理員是否能夠建立自訂報告以包含 URL 摘要資料庫中的資料。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
HIP 比對	指定管理員是否能夠建立自訂報告以包含 HIP 比對日誌中的資料。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
GlobalProtect	指定管理員是否能夠建立自訂報告以包含 GlobalProtect 日誌中的資料。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
WildFire 日誌	指定管理員是否能夠建立自訂報告以包含 WildFire 日誌中的資料。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
GTP 日誌	指定行動網路營運商是否能夠建立自訂報告以包含 GTP 日誌中的資料。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
GTP 摘要	指定行動網路營運商是否能夠建立自訂報告以包含 GTP 日誌中的資料。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	管理員角色可用性	啟用	唯讀	停用
通道日誌	指定管理員是否能夠建立自訂報告以包含通道檢查日誌中的資料。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
通道摘要	指定管理員是否能夠建立自訂報告以包含通道摘要資料庫中的資料。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
SCTP 日誌	指定行動網路營運商是否能夠建立自訂報告以包含 SCTP 日誌中的資料。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
SCTP 摘要	指定行動網路營運商是否能夠建立自訂報告以包含 SCTP 摘要資料庫中的資料。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
使用者-ID	指定管理員是否能夠建立自訂報告以包含 User-ID 日誌中的資料。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
驗證	指定管理員是否能夠建立自訂報告以包含驗證日誌中的資料。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
檢視排程的自訂報告	指定管理員是否能檢視已排程產生的自訂報告。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
檢視預先定義的應用程式報告	指定管理員是否能檢視應用程式報告。隱私權權限不會影響 **Monitor**（監控） > **Reports**（報告）節點上提供的報告，因此如果您有使用者隱私權需求的話，應停用報告的存取權。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	管理員角色可用性	啟用	唯讀	停用
檢視預先定義的威脅報告	指定管理員是否能檢視威脅報告。隱私權權限不會影響 **Monitor**（監控）> **Reports**（報告）節點上提供的報告，因此如果您有使用者隱私權需求的話，應停用報告的存取權。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
檢視預先定義的 URL 篩選報告	指定管理員是否能檢視 URL 篩選報告。隱私權權限不會影響 **Monitor**（監控）> **Reports**（報告）節點上提供的報告，因此如果您有使用者隱私權需求的話，應停用報告的存取權。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
檢視預先定義的流量報告	指定管理員是否能檢視流量報告。隱私權權限不會影響 **Monitor**（監控）> **Reports**（報告）節點上提供的報告，因此如果您有使用者隱私權需求的話，應停用報告的存取權。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
檢視預先定義的 GTP 報告	指定行動網路營運商是否可檢視 GTP 報告。隱私權權限不會影響 **Monitor**（監控）> **Reports**（報告）節點上提供的報告，因此如果您有使用者隱私權需求的話，應停用報告的存取權。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是
檢視預先定義的 SCTP 報告	指定行動網路營運商是否可檢視 SCTP 報告。隱私權權限不會影響 **Monitor**（監控）> **Reports**（報告）節點上提供的報告，因此如果您有使用者隱私權需求的話，應停用報告的存取權。	防火牆：是 Panorama:是 裝置群組/範本：是	是	否。	是

提供原則標籤的細微存取權

如果您啟用 Admin Role（管理員角色）設定檔中的 Policy（原則）選項，則您可以視需要為您正在定義的角色啟用或停用特定節點的存取權，或提供唯讀存取權。您可以透過啟用特定原則類型的存取權，來啟用檢視、新增或刪除原則規則的功能。您也可以啟用特定原則的唯讀存取權，讓管理員

©2024 Palo Alto Networks, Inc.

能夠檢視對應的原則規則庫，但無法新增或刪除規則。停用特定類型原則的存取權，會讓管理員看不到原則規則庫。

因為以特定使用者（根據使用者名稱或 IP 位址）為基礎的原則必須明確定義，所以會停用查看完整 IP 位址或使用者名稱功能的隱私權設定不會套用到隱私權標籤上。因此，您應僅允許自使用者隱私權限制中排除的管理員能夠存取原則標籤。

存取層級	說明	啟用	唯讀	停用
security	若啟用此權限，管理員便能夠檢視、新增和/或刪除安全性規則。如果您想要管理員能夠檢視規則，但無法修改，請將此權限設成唯讀。若要讓管理員無法檢視安全性規則庫，請停用此權限。	是	是	是
NAT	若啟用此權限，管理員便能夠檢視、新增及/或刪除 NAT 規則。如果您想要管理員能夠檢視規則，但無法修改，請將此權限設成唯讀。若要讓管理員無法檢視 NAT 規則庫，請停用此權限。	是	是	是
QoS	若啟用此權限，管理員便能夠檢視、新增及/或刪除 QoS 規則。如果您想要管理員能夠檢視規則，但無法修改，請將此權限設成唯讀。若要讓管理員無法檢視 QoS 規則庫，請停用此權限。	是	是	是
基於原則的轉送	若啟用此權限，管理員便能夠檢視、新增及/或刪除建立基於原則的轉送 (PBF) 規則。如果您想要管理員能夠檢視規則，但無法修改，請將此權限設成唯讀。若要讓管理員無法檢視 PBF 規則庫，請停用此權限。	是	是	是
解密	若啟用此權限，管理員便能夠檢視、新增及/或刪除解密規則。如果您想要管理員能夠檢視規則，但無法修改，請將此權限設成唯讀。若要讓管理員無法檢視解密規則庫，請停用此權限。	是	是	是
網路封包代理程式	若啟用此權限，管理員便能夠檢視、新增及/或刪除網路封包代理程式原則規則。如果您想要管理員能夠檢視規則，但無法修改，請將此權限設成唯讀。若要阻止管	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	啟用	唯讀	停用
	理員在介面中看到網路封包代理程式規則庫，請停用此權限。			
通道檢查	若啟用此權限，管理員便能夠檢視、新增及/或刪除通道檢查規則。如果您想要管理員能夠檢視規則，但無法修改，請將此權限設成唯讀。若要讓管理員無法檢視通道檢查規則庫，則停用此權限。	是	是	是
應用程式覆寫	若啟用此權限，管理員便能夠檢視、新增及/或刪除應用程式覆寫原則規則。如果您想要管理員能夠檢視規則，但無法修改，請將此權限設成唯讀。若要讓管理員無法檢視應用程式取代規則庫，請停用此權限。	是	是	是
驗證	若啟用此權限，管理員便能夠檢視、新增及/或刪除驗證原則規則。如果您想要管理員能夠檢視規則，但無法修改，請將此權限設成唯讀。若要讓管理員無法檢視驗證規則庫，則停用此權限。	是	是	是
DoS 保護	若啟用此權限，管理員便能夠檢視、新增及/或刪除 DoS 保護規則。如果您想要管理員能夠檢視規則，但無法修改，請將此權限設成唯讀。若要讓管理員無法檢視 DoS 保護規則庫，請停用此權限。	是	是	是
SD-WAN	若啟用此權限，管理員便能夠檢視、新增和/或刪除 SD-WAN 原則規則。如果您想要管理員能夠檢視規則，但無法修改，請將此權限設成唯讀。若要讓管理員無法檢視 SD-WAN 原則規則庫，請停用此權限。	是	是	是

提供物件標籤的精確存取權

物件是一種容器，能夠將已簡化規則定義的特定原則篩選值—如 IP 位址、URL、應用程式或服務—分組在一起。例如，位址物件可包含您 DMZ 區域中 Web 與應用程式伺服器的特定 IP 位址定義。

©2024 Palo Alto Networks, Inc.

當決定是否允許整體存取物件標籤時，請判斷管理員是否將具備原則定義責任。如果不具備，則管理員或許不需要該標籤的存取權。但如果管理員需要建立原則，您可以啟用標籤的存取權，並提供節點層級的精確存取權限。

透過啟用特定節點的存取權，您便能授予管理員檢視、新增與刪除對應物件類型的權限。授予唯讀存取權可讓管理員檢視已定義的物件，但不能建立或刪除。停用節點可讓管理員在 Web 介面中看不到該節點。

存取層級	說明	啟用	唯讀	停用
位址	指定管理員是否能檢視、新增或刪除用於安全性原則中的位址物件。	是	是	是
位址群組	指定管理員是否能檢視、新增或刪除用於安全性原則中的位址群組物件。	是	是	是
地區	指定管理員是否能檢視、新增或刪除用於安全性、解密或 DoS 原則中的地區物件。	是	是	是
應用程式	指定管理員是否能檢視、新增或刪除用於原則中的應用程式物件。	是	是	是
應用程式群組	指定管理員是否能檢視、新增或刪除用於原則中的應用程式群組物件。	是	是	是
應用程式篩選器	指定管理員是否能檢視、新增或刪除應用程式篩選器以簡化重複搜尋。	是	是	是
服務	指定管理員是否能檢視、新增或刪除用於建立限制應用程式可使用連接埠號碼之原則規則的服務物件。	是	是	是
服務群組	指定管理員是否能檢視、新增或刪除用於安全性原則中的服務群組物件。	是	是	是
標籤	指定管理員是否能檢視、新增或刪除已定義在防火牆上的標籤。	是	是	是
GlobalProtect	指定管理員是否能檢視、新增或刪除 HIP 物件與設定檔。您可以同時限制存取 GlobalProtect 層級的這兩種類型物件，或啟用 GlobalProtect 權限並限制 HIP 物件或 HIP 設定檔的存取權，以提供更精確的控制。	是	否。	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	啟用	唯讀	停用
HIP 物件	指定管理員是否能檢視、新增或刪除用於定義 HIP 設定檔的 HIP 物件。HIP 物件也會產生 HIP 比對日誌。	是	是	是
無用戶端應用程式	指定管理員是否能檢視、新增、修改或刪除 GlobalProtect 無用戶端 VPN 應用程式。	是	是	是
無用戶端應用程式群組	指定管理員是否能檢視、新增、修改或刪除 GlobalProtect 無用戶端 VPN 應用程式群組。	是	是	是
HIP 設定檔	指定管理員是否能檢視、新增或刪除用於安全性原則中及/或用於產生 HIP 比對日誌的 HIP 設定檔。	是	是	是
外部動態清單	指定管理員是否能檢視、新增或刪除用於安全性原則中的外部動態清單。	是	是	是
自訂物件	指定管理員是否能看到自訂間諜軟體與漏洞簽章。您可以限制存取權以啟用或停用此層級所有自訂特徵碼的存取權，或啟用自訂物件權限並限制每種類型特徵碼的存取權，以提供更精確的控制。	是	否。	是
資料模式	指定管理員是否能檢視、新增或刪除用於建立自訂弱點保護設定檔的自訂資料模式特徵碼。	是	是	是
間諜軟體	指定管理員是否能檢視、新增或刪除用於建立自訂弱點保護設定檔的自訂間諜軟體特徵碼。	是	是	是
漏洞	指定管理員是否能檢視、新增或刪除用於建立自訂漏洞保護設定檔的自訂漏洞特徵碼。	是	是	是
URL 類別	指定管理員是否能檢視、新增或刪除用於原則中的自訂 URL 類別。	是	是	是
安全性設定檔	指定管理員是否能看到安全性設定檔。您可以限制存取權以啟用或停用此層級所有安全性設定檔的存取權，或啟用安全性	是	否。	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	啟用	唯讀	停用
	設定檔權限並限制每種類型設定檔的存取權，以提供更精確的控制。			
防毒軟體	指定管理員是否能檢視、新增或刪除防毒設定檔。	是	是	是
反間諜軟體	指定管理員是否能檢視、新增或刪除反間諜軟體設定檔。	是	是	是
漏洞保護	指定管理員是否能檢視、新增或刪除漏洞保護設定檔。	是	是	是
URL 篩選	指定管理員是否能檢視、新增或刪除 URL 篩選設定檔。	是	是	是
檔案封鎖	指定管理員是否能檢視、新增或刪除檔案封鎖設定檔。	是	是	是
WildFire 分析	指定管理員是否能檢視、新增或刪除 WildFire 分析設定檔。	是	是	是
資料篩選	指定管理員是否能檢視、新增或刪除資料篩選設定檔。	是	是	是
DoS 保護	指定管理員是否能檢視、新增或刪除 DoS 保護設定檔。	是	是	是
GTP 保護	指定行動網路營運商是否能檢視、新增或刪除 GTP 保護設定檔。	是	是	是
SCTP 保護	指定行動網路營運商是否能檢視、新增或刪除串流控制傳輸通訊協定 (SCTP) 保護設定檔。	是	是	是
安全性設定檔群組	指定管理員是否能檢視、新增或刪除安全性設定檔群組。	是	是	是
日誌轉送	指定管理員是否能檢視、新增或刪除日誌轉送設定檔。	是	是	是
驗證	指定管理員是否能檢視、新增或刪除驗證強制物件。	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	啟用	唯讀	停用
解密規則	指定管理員是否能檢視、新增或刪除解密設定檔。	是	是	是
SD-WAN 連結管理	指定管理員是否可以新增或刪除路徑品質、SaaS 品質、流量散佈和錯誤更正設定檔。	是	否。	是
Saas 品質設定檔	指定管理員是否可以檢視、新增或刪除 SD-WAN 路徑品質設定檔。	是	是	是
SaaS 品質設定檔	指定管理員是否可以檢視、新增或刪除 SD-WAN SaaS 品質設定檔。	是	是	是
流量散佈設定檔	指定管理員是否可以檢視、新增或刪除 SD-WAN 流量散佈設定檔。	是	是	是
錯誤更正設定檔	指定管理員是否可以檢視、新增或刪除 SD-WAN 錯誤更正設定檔。	是	是	是
封包代理程式設定檔	指定管理員是否可以檢視、新增或刪除封包代理程式設定檔。	是	是	是
排程	指定管理員是否能檢視、新增或刪除排程，藉以將安全性原則限制在特定日期及/或時間範圍。	是	是	是

提供網路標籤的精確存取權

當決定是否允許以整體方式存取 **Network**（網路）標籤時，請判斷管理員是否具備包括 GlobalProtect 管理在內的網路管理責任。如果不具備，則管理員或許不需要該標籤的存取權。

您也可以定義節點層級的 **Network**（網路）標籤存取權。透過啟用特定節點的存取權，您便授予管理員檢視、新增與刪除對應網路組態的權限。授予唯讀存取權可讓管理員檢視已定義的組態，但不能建立或刪除。停用節點可讓管理員在 Web 介面中看不到該節點。

只有在裝置啟用 **Advanced Routing**（進階路由）時（在此情況下，邏輯路由器會取代虛擬路由器），一些路由存取層級才會顯示出來並且可以套用。

存取層級	說明	啟用	唯讀	停用
介面	指定管理員是否能檢視、新增或刪除介面組態。	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	啟用	唯讀	停用
地區	指定管理員是否能檢視、新增或刪除區域。	是	是	是
VLAN	指定管理員是否能檢視、新增或刪除 VLAN。	是	是	是
Virtual Wire	指定管理員是否能檢視、新增或刪除 Virtual Wire。	是	是	是
虛擬路由器	指定管理員是否能檢視、新增、修改或刪除虛擬路由器。	是	是	是
路由	（進階路由引擎）指定管理員是否可以檢視、新增、修改或刪除「進階路由引擎」的任何路由欄位。	是	是	是
邏輯路由器	（進階路由引擎）指定管理員是否可以檢視、新增、修改或刪除邏輯路由器。	是	是	是
路由設定檔	（進階路由引擎）指定管理員是否可以檢視、新增、修改或刪除路由設定檔。	是	是	是
BGP	（進階路由引擎）指定管理員是否可以檢視、新增、修改或刪除 BGP 路由設定檔。	是	是	是
BFD	（進階路由引擎）指定管理員是否可以檢視、新增、修改或刪除 BFD 路由設定檔。	是 S	是	是
OSPF	（進階路由引擎）指定管理員是否可以檢視、新增、修改或刪除 OSPFv2 路由設定檔。	是	是	是
OSPFv3	（進階路由引擎）指定管理員是否可以檢視、新增、修改或刪除 OSPFv3 路由設定檔。	是	是	是
RIPv2	（進階路由引擎）指定管理員是否可以檢視、新增、修改或刪除 RIPv2 路由設定檔。	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	啟用	唯讀	停用
篩選器	（進階路由引擎）指定管理員是否可以檢視、新增、修改或刪除篩選器。	是	是	是
多點傳送	（進階路由引擎）指定管理員是否可以檢視、新增、修改或刪除 IPv4 多點傳送路由設定檔。	是	是	是
IPSec 通道	指定管理員是否能檢視、新增、修改或刪除 IPSec 通道組態。	是	是	是
GRE 通道	指定管理員是否能檢視、新增、修改或刪除 GRE 通道組態。	是	是	是
DHCP	指定管理員是否能檢視、新增、修改或刪除 DHCP 伺服器與 DHCP 轉送組態。	是	是	是
DNS Proxy	指定管理員是否能檢視、新增、修改或刪除 DNS Proxy 組態。	是	是	是
GlobalProtect	指定管理員是否能檢視、新增、修改 GlobalProtect 入口網站與閘道組態。您可以將 GlobalProtect 功能的存取權整個停用，或者啟用 GlobalProtect 權限並將角色限制在入口網站或閘道設定區域。	是	否。	是
入口網站	指定管理員是否能檢視、新增、修改或刪除 GlobalProtect 入口網站組態。	是	是	是
閘道	指定管理員是否能檢視、新增、修改或刪除 GlobalProtect 閘道組態。	是	是	是
MDM	指定管理員是否能檢視、新增、修改或刪除 GlobalProtect MDM 伺服器組態。	是	是	是
設備封鎖清單	指定管理員是否能檢視、新增、修改或刪除裝置封鎖清單。	是	是	是
無用戶端應用程式	指定管理員是否能檢視、新增、修改或刪除 GlobalProtect 無用戶端 VPN 應用程式。	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	啟用	唯讀	停用
無用戶端應用程式群組	指定管理員是否能檢視、新增、修改或刪除 GlobalProtect 無用戶端 VPN 應用程式群組。	是	是	是
QoS	指定管理員是否能檢視、新增、修改或刪除 QoS 組態。	是	是	是
LLDP	指定管理員是否能檢視、新增、修改或刪除 LLDP 組態。	是	是	是
網路設定檔	設定預設狀態以啟用或停用下述所有的網路設定。	是	否。	是
GlobalProtect IPSec 加密	控制 **Network Profiles**（網路設定檔）> **GlobalProtect IPSec Crypto**（**GlobalProtect IPSec** 加密）節點的存取權。 如果您停用此權限，管理員將看不到該節點，或無法設定演算法，以驗證與加密 GlobalProtect 閘道和用戶端之間的 VPN 通道。 如果您將權限設為唯讀，則管理員可檢視現有 GlobalProtect IPSec 密碼設定檔，但無法新增或編輯這些設定檔。	是	是	是
IKE 閘道	控制 **Network Profiles**（網路設定檔）> **IKE Gateways**（**IKE** 閘道）節點的存取權。如果您停用此權限，管理員將看不到 **IKE** 閘道節點，或無法定義閘道以包含執行 IKE 通訊協定與對等閘道間交涉所需的組態資訊。 如果權限狀態設為唯讀，則您可檢視目前設定的 IKE 閘道，但無法新增或編輯閘道。	是	是	是
IPSec 加密	控制 **Network Profiles**（網路設定檔）> **IPSec Crypto**（**IPSec** 加密）節點的存取權。如果您停用此權限，管理員將看不到 **Network Profiles**（網路設定檔）> **IPSec Crypto**（**IPSec** 加密） 節點，或無法根據	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	啟用	唯讀	停用
	IPSec SA 交涉指定用於在 VPN 通道中識別、驗證與加密的通訊協定與演算法。 如果權限狀態設為唯讀，則您可檢視目前設定的 IPSec 加密設定，但無法新增或編輯設定。			
IKE 加密	控制裝置交換資訊的方式以確保安全通訊。根據 IPSec SA 交涉 (IKEv1 階段-1) 在 VPN 通道中所指定，用於識別、驗證與加密的通訊協定與演算法。	是	是	是
監控	控制 **Network Profiles**（網路設定檔） > **Monitor**（監控）節點的存取權。如果停用此權限，管理員將看不到 **Network Profiles**（網路設定檔） > **Monitor**（監控） 節點，或無法建立或編輯監控設定檔以用於監控 IPSec 通道並監控基於原則的轉送 (PBF) 規則的下一個躍點裝置。 如果權限狀態設為唯讀，則您可檢視目前設定的監控設定檔設定，但無法新增或編輯設定。	是	是	是
介面管理	控制 **Network Profiles**（網路設定檔） > **Interface Mgmt**（介面管理）節點的存取權。如果停用此權限，管理員將看不到 **Network Profiles**（網路設定檔） > **Interface Mgmt**（介面管理）節點，或無法指定用於管理防火牆的通訊協定。 如果權限狀態設為唯讀，則您可檢視目前設定的介面管理設定檔設定，但無法新增或編輯設定。	是	是	是
地區保護	控制 **Network Profiles**（網路設定檔） > **Zone Protection**（區域保護）節點的存取權。如果停用此權限，管理員將看不到 **Network Profiles**（網路設定檔） > **Zone Protection**（區域保護）節點，或無法設定好設定檔以決定防火牆要如何回應來自指定安全性區域的攻擊。	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	啟用	唯讀	停用
	如果權限狀態設為唯讀，則您可檢視目前設定的地區保護設定檔設定，但無法新增或編輯設定。			
QoS 設定檔	控制 **Network Profiles**（網路設定檔）> **QoS** 節點的存取權。如果停用此權限，管理員將看不到 **Network Profiles**（網路設定檔）> **QoS** 節點，或無法設定 QoS 設定檔以決定要如何處理 QoS 流量類別。 如果權限狀態設為唯讀，則您可檢視目前設定的 QoS 設定檔設定，但無法新增或編輯設定。	是	是	是
LLDP 設定檔	控制 **Network Profiles**（網路設定檔）> **LLDP** 節點的存取權。如果停用此權限，管理員將看不到 **Network Profiles**（網路設定檔）> **LLDP** 節點，或無法設定 LLDP 設定檔以控制防火牆的介面是否可以參與連結層探索通訊協定。 如果權限狀態設為唯讀，則您可檢視目前設定的 LLDP 設定檔設定，但無法新增或編輯組態。	是	是	是
RFD 設定檔	控制 **Network Profiles**（網路設定檔）> **BFD Profile**（**BFD** 設定檔）節點的存取權。如果停用此權限，管理員將看不到 **Network Profiles**（網路設定檔）> **BFD Profile**（**BFD** 設定檔） 節點，或無法設定 BFD 設定檔。雙向轉送偵測 (BFD) 設定檔可讓您設定 BFD 設定，以套用至一個或更多靜態路由或路由通訊協定。因此，BFD 可偵測失敗連結或 BFD 對等，實現極快速容錯轉移。 如果權限狀態設為唯讀，則您可檢視目前設定的 BFD 設定檔，但無法新增或編輯 BFD 設定檔。	是	是	是
SD-WAN 介面設定檔	控制對 **SD-WAN Interface Profile**（**SD-WAN** 介面設定檔）節點的存取。如果停用此權限，管理員將看不到 **SD-WAN Interface Profile**（**SD-WAN** 介面設定	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	啟用	唯讀	停用
	檔）節點，也無法設定 SD-WAN 介面設定檔。SD-WAN 介面設定檔定義 ISP 連線的特性，並指定連結速度和防火牆監控連結的頻率。 如果權限狀態設為唯讀，則您可檢視目前設定的 SD-WAN 介面設定檔，但無法進行新增或編輯。			

提供裝置頁籤的精確存取權

若要為 **Device**（裝置）頁籤定義細微存取權限，在建立或編輯管理員角色設定檔時（**Device**（裝置）> **Admin Roles**（管理員角色）），在 **WebUI** 頁籤上向下捲動至 **Device**（裝置）節點。

存取層級	說明	啟用	唯讀	停用
設定	控制**Setup**（設定）節點的存取權。如果您停用此權限，管理員將看不到 **Setup**（設定）節點，或無法存取防火牆全域組態設定資訊，例如管理、操作、服務、Content-ID、WildFire 或工作階段設定資訊。 如果權限狀態設為唯讀，則您可檢視目前組態，但無法進行任何變更。	是	是	是
管理	控制 **Management**（管理）節點的存取權。如果您停用此權限，管理員將無法進行主機名稱、網域、時區、驗證、日誌記錄與報告、Panorama 連線、橫幅、訊息及密碼複雜性等設定。 如果權限狀態設為唯讀，則您可檢視目前組態，但無法進行任何變更。	是	是	是
操作人員	控制對 **Operations**（操作）和 **Telemetry and Threat Intelligence**（遙測和威脅情報）節點的存取。如果您停用此權限，則管理員將無法： • 載入防火牆組態。	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	啟用	唯讀	停用
	• 儲存或還原防火牆組態。 此權限僅適用於 ***Device***（裝置） > ***Operations***（操作） 選項。儲存並提交權限控制，無論管理員是可以透過 ***Config***（組態） > ***Save***（儲存） 和 ***Config***（組態） > ***Revert***（還原）選項儲存或還原組態。 • 建立自訂標誌。 • 設定防火牆設定的 SNMP 監控。 • 設定統計服務功能。 • 設定 **Telemetry and Threat Intelligence**（遙測和威脅情報） 設定。 只有具有預先定義超級使用者角色的管理員，才可匯出或匯入防火牆組態以及關閉防火牆。 只有具有預先定義超級使用者或裝置管理員角色的管理員，才可重新啟動防火牆或重新啟動資料平面。 若管理員具有僅允許存取特定虛擬系統的角色，則無法透過 **Device**（裝置） > **Operations**（操作） 選項載入、儲存或還原防火牆組態。			
服務	控制 **Services**（服務）節點的存取權。如果您停用此權限，管理員將無法設定 DNS 伺服器服務（更新伺服器、代理程式伺服器或 NTP 伺服器），或者設定服務路由等。 如果權限狀態設為唯讀，則您可檢視目前組態，但無法進行任何變更。	是	是	是
內容 ID	控制 **Content-ID**（內容 **ID**）節點的存取權。如果您停用此權限，管理員將無法設定 URL 篩選或內容 ID。	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	啟用	唯讀	停用
	如果權限狀態設為唯讀，則您可檢視目前組態，但無法進行任何變更。			
WildFire	控制 **WildFire** 節點的存取權。如果您停用此權限，管理員將無法進行 WildFire 設定。 如果權限狀態設為唯讀，則您可檢視目前組態，但無法進行任何變更。	是	是	是
工作階段	控制 **Session**（工作階段）節點的存取權。如果您停用此權限，管理員將無法對 TCP、UDP 或 ICMP 進行工作階段設定或逾時設定，或進行解密或 VPN 工作階段設定。 如果權限狀態設為唯讀，則您可檢視目前組態，但無法進行任何變更。	是	是	是
Hsm	控制 **HSM** 節點的存取權。如果您停用此權限，管理員將無法設定硬體安全性模組。 如果權限狀態設為唯讀，則您可檢視目前組態，但無法進行任何變更。	是	是	是
High availability（高可用性）	控制 **High Availability**（高可用性）節點的存取權。如果您停用此權限，管理員將看不到 **High Availability**（高可用性）節點，或無法存取防火牆全域高可用性組態資訊，例如一般設定資訊或連結與路徑監控。 如果您將此權限設為唯讀，則管理員可檢視防火牆的高可用性組態資訊，但無法執行任何設定程序。	是	是	是
設定稽核	控制組態檔稽核節點的存取權。如果您停用此權限，管理員將看不到 **Config Audit**（組態稽核）節點，或無法存取任何防火牆全域組態資訊。	是	否。	是
管理員	控制 **Administrators**（管理員）節點的存取權。只允許唯讀存取此功能。	否	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	啟用	唯讀	停用
	如果您停用此權限，管理員將看不到 **Administrators**（管理員）節點，或無法存取其管理員帳戶的相關資訊。 如果您將此權限設為唯讀，則管理員可檢視其管理員帳戶的組態資訊。管理員將看不到防火牆上所設定其他管理員帳戶的任何資訊。			
管理員角色	控制 **Admin Roles**（管理員角色）節點的存取權。只允許唯讀存取此功能。 如果您停用此權限，管理員將看不到 **Admin Roles**（管理員角色）節點，或無法存取任何與管理員角色設定檔組態相關的防火牆全域資訊。 如果您將此權限設為唯讀，則您可檢視防火牆上所設定所有管理員角色的組態資訊。	否	是	是
驗證設定檔	控制驗證設定檔節點的存取權。如果您停用此權限，管理員將看不到 **Authentication Profile**（驗證設定檔）節點，或無法建立或編輯驗證設定檔，以用於指定 RADIUS、TACACS+、LDAP、Kerberos、SAML、多因素驗證 (MFA) 或本機資料庫驗證設定。PAN-OS 使用驗證設定檔來驗證防火牆管理員以及驗證入口網站或 GlobalProtect 使用者。 如果您將此權限設為唯讀，則管理員可檢視 **Authentication Profile**（驗證設定檔）資訊，但無法建立或編輯驗證設定檔。	是	是	是
驗證順序	控制 **Authentication Sequence**（驗證順序）節點的存取權。如果您停用此權限，管理員將看不到驗證順序節點，或無法建立或編輯驗證順序。 如果您將此權限設為唯讀，則管理員可檢視 **Authentication Profile**（驗證設定檔）資訊，但無法建立或編輯驗證順序。	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	啟用	唯讀	停用
虛擬系統	控制**Virtual Systems**（虛擬系統）節點的存取權。如果您停用此權限，管理員將看不到或無法設定虛擬系統。 如果權限狀態設為唯讀，則您可檢視目前設定的虛擬系統，但無法新增或編輯設定。	是	是	是
共用閘道	控制 **Shared Gateways**（共用閘道）節點的存取權。共用閘道可讓虛擬系統共用通用介面進行外部通訊。 如果您停用此權限，管理員將看不到或無法設定共用閘道。 如果權限狀態設為唯讀，則您可檢視目前設定的共用閘道，但無法新增或編輯設定。	是	是	是
使用者識別機制	控制 **User Identification**（使用者識別）節點的存取權。如果您停用此權限，使用者將看不到 **User Identification**（使用者識別）節點，或無法存取防火牆全域使用者識別組態資訊，例如使用者識別、連線安全性、User-ID 代理程式、終端機伺服器代理程式、群組對應設定或驗證入口網站設定。 如果您將此權限設為唯讀，則管理員可檢視防火牆的組態資訊，但無法執行任何設定程序。	是	是	是
VM 資訊來源	控制 **VM Information Source**（**VM** 資訊來源）節點的存取權，讓您能夠設定防火牆/Windows User-ID 代理程式以自動收集 VM 詳細目錄。如果您停用此權限，管理員將看不到 **VM Information Source**（**VM** 資訊來源）節點。 如果您將此權限設為唯讀，則管理員可檢視設定的 VM 資訊來源，但無法新增、編輯或刪除任何來源。	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	啟用	唯讀	停用
	裝置群組和範本管理員不具此權限。			
憑證管理	設定預設狀態以啟用或停用下述所有的憑證設定。	是	否。	是
憑證	控制 **Certificates**（憑證）節點的存取權。如果您停用此權限，管理員將看不到 **Certificates**（憑證）節點，或無法設定或存取「裝置憑證」或「受信任的憑證授權單位」的相關資訊。 如果您將此權限設為唯讀，則管理員可檢視防火牆的憑證組態資訊，但無法執行任何設定程序。	是	是	是
憑證設定檔	控制 **Certificate Profile**（憑證設定檔）節點的存取權。如果您停用此權限，管理員將看不到 **Certificate Profile**（憑證設定檔）節點，或無法建立憑證設定檔。 如果您將此權限設為唯讀，則管理員可檢視目前為防火牆設定的憑證設定檔，但無法建立或編輯憑證設定檔。	是	是	是
OCSP 回應程式	控制 **OCSP Responder**（**OCSP** 回應程式）節點的存取權。如果您停用此權限，管理員將看不到 **OCSP Responder**（**OCSP** 回應程式）節點，或無法定義伺服器以用於驗證防火牆所發出憑證的撤銷狀態。 如果您將此權限設為唯讀，則管理員可檢視防火牆的 **OCSP Responder**（**OCSP** 回應程式）組態，但無法建立或編輯 OCSP 回應程式設定。	是	是	是
SSL/TLS 服務設定檔	控制 **SSL/TLS Service Profile**（**SSL/TLS** 服務設定檔）節點的存取權。 如果您停用此權限，管理員將看不到節點，或無法設定針對使用 SSL/TLS 的防火牆服務，指定憑證和通訊協定版本或通訊協定範圍的設定檔。	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	啟用	唯讀	停用
	如果您將此權限設為唯讀，則管理員可檢視現有 SSL/TLS 服務設定檔，但無法建立或編輯這些設定檔。			
SCEP	控制 **SCEP** 節點的存取權。如果您停用此權限，管理員將看不到節點，或無法定義指定簡易憑證註冊通訊協定 (SCEP) 設定的設定檔，以簽發唯一的裝置憑證。 如果您將此權限設為唯讀，則管理員可檢視現有 SCEP 設定檔，但無法建立或編輯這些設定檔。	是	是	是
SSL 解密排除	控制 **SSSL Decryption Exclusion**（**SSL** 解密排除）節點的存取權。如果停用此權限，管理員將看不到該節點，也無法新增自訂排除項。 如果您將此權限設為唯讀，則管理員可檢視現有 SSL 解密排除項，但無法建立或編輯這些排除項。	是	是	是
SSH 服務設定檔	控制對 **SSH Service Profile**（**SSH** 服務設定檔）節點的存取權。如果停用此權限，管理員將看不到該節點，也無法對設定檔進行設定來指定與 Palo Alto Networks 管理和高可用性 (HA) 設備進行 SSH 連線的參數。 如果您將此權限設定為唯讀，則管理員可檢視現有 SSH 服務設定檔，但無法編輯或建立這些設定檔。	是	是	是
回應頁面	控制 **Response Pages**（回應頁面）節點的存取權。如果您停用此權限，管理員將看不到 **Response Page**（回應頁面）節點，或無法定義自訂已下載與顯示的 HTML 訊息，但是可定義要求的網頁或檔案。 如果您將此權限設為唯讀，則管理員可檢視裝置的 **Response Page**（回應頁面）組態，但無法建立或編輯回應頁面設定。	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	啟用	唯讀	停用
日誌設定	設定預設狀態以啟用或停用下述所有的日誌設定。	是	否。	是
系統	控制 **Log Settings**（日誌設定）> **System**（系統）節點的存取權。如果停用此權限，管理員將看不到 **Log Settings**（日誌設定）> **System**（系統）節點，或無法指定防火牆將向 Panorama 或外部服務（例如 syslog 伺服器）轉送哪些系統日誌。 如果您將此權限設為唯讀，則管理員可檢視防火牆的 **Log Settings**（日誌設定）> **System**（系統）設定，但無法新增、編輯或刪除設定。	是	是	是
組態設定	控制 **Log Settings**（日誌設定）> **Configuration**（組態）節點的存取權。如果停用此權限，管理員將看不到 **Log Settings**（日誌設定）> **Configuration**（組態） 節點，或無法指定防火牆將向 Panorama 或外部服務（例如 syslog 伺服器）轉送哪些系統組態。 如果您將此權限設為唯讀，則管理員可檢視防火牆的 **Log Settings**（日誌設定）> **Configuration**（組態） 設定，但無法新增、編輯或刪除設定。	是	是	是
使用者-ID	控制 **Log Settings**（日誌設定）> **User-ID** 節點的存取權。如果停用此權限，管理員將看不到 **Log Settings**（日誌設定）> **User-ID** 節點，或無法指定防火牆將向 Panorama 或外部服務（例如 syslog 伺服器）轉送哪些 User-ID 日誌。 如果您將此權限設為唯讀，則管理員可檢視防火牆的 **Log Settings**（日誌設定）> **User-ID** 設定，但無法新增、編輯或刪除設定。	是	是	是
HIP 比對	控制 **Log Settings**（日誌設定）> **HIP Match**（**HIP** 比對）節點的存取權。如果停用此權限，管理員將看不到 **Log**	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	啟用	唯讀	停用
	Settings（日誌設定） > **HIP Match**（**HIP** 比對） 節點，或無法指定防火牆將向 Panorama 或外部服務（例如 syslog 伺服器）轉送哪些主機資訊設定檔 (HIP) 比對日誌。HIP 比對日誌提供了套用於 GlobalProtect 端點之安全性原則規則的資訊。 如果您將此權限設為唯讀，則管理員可檢視防火牆的 **Log Settings**（日誌設定） > **HIP** 設定，但無法新增、編輯或刪除設定。			
GlobalProtect	控制 **Log Settings**（日誌設定） > **GlobalProtect**節點的存取權。如果停用此權限，管理員將看不到**Log Settings**（日誌設定） > **GlobalProtect** 節點，或無法指定防火牆將向 Panorama 或外部服務（例如 syslog 伺服器）轉送哪些 GlobalProtect 日誌。 如果您將此權限設為唯讀，則管理員可檢視防火牆的 **Log Settings**（日誌設定） > **GlobalProtect**設定，但無法新增、編輯或刪除設定。	是	是	是
關聯	控制 **Log Settings**（日誌設定） > **Correlation**（關聯性）節點的存取權。如果停用此權限，管理員將看不到 **Log Settings**（日誌設定） > **Correlation**（關聯性） 節點，或無法新增、刪除或修改關聯性日誌轉送設定或標記來源或目的地 IP 位址。 如果您將此權限設為唯讀，則管理員可檢視防火牆的 **Log Settings**（日誌設定） > **Correlation**（關聯性）設定，但無法新增、編輯或刪除設定。	是	是	是
警報設定	控制 **Log Settings**（日誌設定） > **Alarm Settings**（警報設定）節點的存取權。如果停用此權限，管理員將看不到 **Log Settings**（日誌設定） > **Alarm**	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	啟用	唯讀	停用
	Settings（警報設定）節點，或無法設定在設定時段內重複與一項安全性原則規則（或一組規則）相符時，防火牆所產生的通知。 如果您將此權限設為唯讀，則管理員可檢視防火牆的 **Log Settings**（日誌設定）> **Alarm Settings**（警報設定），但無法編輯設定。			
管理日誌	控制 **Log Settings**（日誌設定）> **Manage Logs**（管理日誌）節點的存取權。如果停用此權限，管理員將看不到 **Log Settings**（日誌設定）> **Manage Logs**（管理日誌）節點，或無法清除指示的日誌。 如果您將此權限設為唯讀，則管理員可檢視 **Log Settings**（日誌設定）> **Manage Logs**（管理日誌）資訊，但無法清除任何日誌。	是	是	是
伺服器設定檔	設定預設狀態以啟用或停用下述所有的伺服器設定檔設定。	是	否。	是
SNMP 陷阱	控制 **Server Profiles**（伺服器設定檔）> **SNMP Trap**（**SNMP** 設陷）節點的存取權。如果停用此權限，管理員將看不到 **Server Profiles**（伺服器設定檔）> **SNMP Trap**（**SNMP** 設陷）節點，或無法指定一或多個用於系統日誌項目的 SNMP 設陷目的地。 如果您將此權限設為唯讀，則管理員可檢視 **Server Profiles**（伺服器設定檔）> **SNMP Trap**（**SNMP** 設陷）資訊，但無法指定 SNMP 設陷目的地。	是	是	是
Syslog	控制 **Server Profiles**（伺服器設定檔）> **Syslog** 節點的存取權。如果停用此權限，管理員將看不到 **Server Profiles**（伺服器設定檔）> **Syslog** 節點，或無法指定一或多個 syslog 伺服器。	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	啟用	唯讀	停用
	如果您將此權限設為唯讀，則管理員可檢視 **Server Profiles**（伺服器設定檔）> **Syslog** 資訊，但無法指定系統日誌伺服器。			
電郵	控制伺 **Server Profiles**（伺服器設定檔）> **Email**（電子郵件）節點的存取權。如果停用此權限，管理員將看不到 **Server Profiles**（伺服器設定檔）> **Email**（電子郵件）節點，或無法設定電子郵件設定以用於為系統與設定日誌項目啟用電子郵件通知。 如果您將此權限設為唯讀，則管理員可檢視 **Server Profiles**（伺服器設定檔）> **Email**（電子郵件）資訊，但無法設定電子郵件伺服器設定檔。	是	是	是
HTTP	控制 **Server Profiles**（伺服器設定檔）> **HTTP** 節點的存取權。如果停用此權限，管理員將看不到 **Server Profiles**（伺服器設定檔）> **HTTP** 節點，或無法設定 HTTP 設定檔以用於啟用日誌轉送，向 HTTP 目的地轉送任何日誌項目。 如果您將此權限設為唯讀，則管理員可檢視 **Server Profiles**（伺服器設定檔）> **HTTP** 資訊，但無法設定 HTTP 伺服器設定檔。	是	是	是
Netflow	控制 **Server Profiles**（伺服器設定檔）> **Netlow** 節點的存取權。如果停用此權限，管理員將看不到 **Server Profiles**（伺服器設定檔）> **Netflow** 節點，或無法定義 NetFlow 伺服器設定檔，以指定匯出頻率與接收匯出資料的 NetFlow 伺服器。 如果您將此權限設為唯讀，則管理員可檢視 **Server Profiles**（伺服器設定檔）> **Netlow** 資訊，但無法定義 Netflow 設定檔。	是	是	是
RADIUS	控制 **Server Profiles**（伺服器設定檔）> **RADIUS** 節點的存取權。如果停用此權	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	啟用	唯讀	停用
	限，管理員將看不到 **Server Profiles**（伺服器設定檔）> **RADIUS** 節點，或無法為驗證設定檔中所識別的 RADIUS 伺服器進行設定。 如果您將此權限設為唯讀，則管理員可檢視 **Server Profiles**（伺服器設定檔）> **RADIUS** 資訊，但無法設定 RADIUS 伺服器的設定。			
TACACS+	控制 **Server Profiles**（伺服器設定檔）> **TACACS+** 節點的存取權。 如果停用此權限，管理員將看不到節點，或無法針對驗證設定檔所參考的 TACACS + 伺服器進行設定。 如果您將此權限設為唯讀，則管理員可檢視現有 TACACS+ 伺服器設定檔，但無法新增或編輯這些設定檔。	是	是	是
LDAP	控制 **Server Profiles**（伺服器設定檔）> **LDAP** 節點的存取權。如果停用此權限，管理員將看不到 **Server Profiles**（伺服器設定檔）> **LDAP** 節點，或無法設定 LDAP 伺服器的設定，以用於使用驗證設定檔進行驗證。 如果您將此權限設為唯讀，則管理員可檢視 **Server Profiles**（伺服器設定檔）> **LDAP** 資訊，但無法設定 LDAP 伺服器的設定。	是	是	是
Kerberos	控制 **Server Profiles**（伺服器設定檔）> **Kerberos** 節點的存取權。如果停用此權限，管理員將看不到 **Server Profiles**（伺服器設定檔）> **Kerberos** 節點，或無法設定 Kerberos 伺服器以允許使用者用原生方式驗證網域控制站。 如果您將此權限設為唯讀，則管理員可檢視 **Server Profiles**（伺服器設定檔）> **Kerberos** 資訊，但無法設定 Kerberos 伺服器的設定。	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	啟用	唯讀	停用
SAML 識別提供者	控制 **Server Profiles**（伺服器設定檔）> **SAML Identity Provider**（**SAML** 識別提供者）節點的存取權。如果停用此權限，管理員將看不到該節點或無法設定 SAML 識別提供者 (IdP) 伺服器設定檔。 如果您將此權限設為唯讀，則管理員可檢視 **Server Profiles**（伺服器設定檔）> **SAML Identity Provider**（**SAML** 識別提供者）資訊，但無法設定 SAML IdP 伺服器設定檔。	是	是	是
多因素驗證	控制 **Server Profiles**（伺服器設定檔）> **Multi Factor Authentication**（多因素驗證）節點的存取權。如果停用此權限，管理員將看不到該節點或無法設定多因素驗證 (MFA) 伺服器設定檔。 如果您將此權限設為唯讀，則管理員可檢視 **Server Profiles**（伺服器設定檔）> **Multi Factor Authentication**（多因素驗證）資訊，但無法設定 MFA 伺服器設定檔。			
本地使用者資料庫	設定預設狀態以啟用或停用下述所有的本地使用者資料庫設定。	是	否。	是
使用者	控制 **Local User Database**（本機使用者資料庫）> **Users**（使用者）節點的存取權。如果停用此權限，管理員將看不到 **Local User Database**（本機使用者資料庫）> **Users**（使用者）節點，或無法在防火牆上設定本地資料庫，以儲存遠端存取使用者、防火牆管理員與驗證入口網站使用者的驗證資訊。 如果您將此權限設為唯讀，則管理員可檢視 **Local User Database**（本機使用者資料庫）> **Users**（使用者） 資訊，但無法在防火牆上設定本地資料庫以儲存驗證資訊。	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	啟用	唯讀	停用
使用者群組	控制 **Local User Database**（本機使用者資料庫） > **Users**（使用者）節點的存取權。如果停用此權限，管理員將看不到 **Local User Database**（本機使用者資料庫） > **Users**（使用者） 節點，或無法將使用者群組資訊新增至本地資料庫。 如果您將此權限設為唯讀，則管理員可檢視 **Local User Database**（本機使用者資料庫） > **Users**（使用者）資訊，但無法將使用者群組資訊新增至本地資料庫。	是	是	是
存取網域	控制 **Access Domain**（存取網域）節點的存取權。如果您停用此權限，管理員將看不到 **Access Domain**（存取網域）節點，或無法建立或編輯存取網域。 如果您將此權限設為唯讀，則管理員可檢視 **Access Domain**（存取網域）資訊，但無法建立或編輯存取網域。	是	是	是
已排程的日誌匯出	控制**Scheduled Log Export**（已排程的日誌匯出）節點的存取權。如果停用此權限，管理員將看不到 **Scheduled Log Export**（已排程的日誌匯出）節點，或無法排程日誌匯出並以 CSV 格式儲存至檔案傳輸通訊協定 (FTP) 伺服器，也無法使用 Secure Copy (SCP)（安全複製 (SCP)）安全地在防火牆與遠端主機之間傳輸資料。 如果您將此權限設為唯讀，則管理員可檢視 **Scheduled Log Export Profile**（已排程的日誌匯出設定檔）資訊，但無法排程日誌匯出。	是	否。	是
軟體	控制 **Software**（軟體）節點的存取權。如果您停用此權限，管理員將看不到 **Software**（軟體）節點，或無法檢視 Palo Alto Networks 提供的最新版 PAN-OS 軟體、讀取每個版本的版本資訊，及選取要下載與安裝的版本。	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	啟用	唯讀	停用
	如果您將此權限設為唯讀，則管理員可檢視 **Software**（軟體）資訊，但無法下載或安裝軟體。			
GlobalProtect 用戶端	控制 **GlobalProtect Client**（**GlobalProtect** 用戶端）節點的存取權。如果停用此權限，管理員將看不到 **GlobalProtect Client**（**GlobalProtect** 用戶端）節點，或無法檢視可用的 GlobalProtect 版本、下載指令碼或啟動 GlobalProtect 應用程式。 如果您將此權限設為唯讀，則管理員可檢視可用的 **GlobalProtect Client**（**GlobalProtect** 用戶端）版本，但無法下載或安裝應用程式軟體。	是	是	是
動態更新	控制 **Dynamic Updates**（動態更新）節點的存取權。如果您停用此權限，管理員將看不到 **Dynamic Updates**（動態更新）節點，或無法檢視最新的更新、讀取每個更新的版本資訊，或選取要上傳與安裝的更新。 如果您將此權限設為唯讀，則管理員可檢視可用的 **Dynamic Updates**（動態更新）版本及讀取版本資訊，但無法上傳或安裝軟體。	是	是	是
授權	控制 **Licenses**（授權）節點的存取權。如果停用此權限，管理員將看不到 **Licenses**（授權）節點，或無法檢視安裝的授權或啟動授權。 如果您將此權限設為唯讀，則管理員可檢視安裝的 **Licenses**（授權），但無法執行授權管理功能。	是	是	是
支援	控制 **Support**（支援）節點的存取權。如果停用此權限，管理員將看不到 **Support**（支援）節點，無法啟動支援或存取來自 Palo Alto Networks 的生產及安全性警示。	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	啟用	唯讀	停用
	如果您將此權限設為唯讀，則管理員可檢視 **Support**（支援）節點及存取生產及安全性警報，但無法啟動支援。			
主要金鑰與診斷	控制**Master Key and Diagnostics**（主要金鑰與診斷）節點的存取權。如果您停用此權限，管理員將看不到 **Master Key and Diagnostics**（主要金鑰與診斷）節點，或無法指定用於在防火牆加密私密金鑰的主要金鑰。 如果您將此權限設為唯讀，則管理員可檢視 **Master Key and Diagnostics**（主要金鑰與診斷）節點及已指定主要金鑰的相關資訊，但無法新增或編輯新的主要金鑰組態。	是	是	是
Policy Recommendation (原則建議)	控制對 **IoT** 和 **SaaS** 原則規則建議的存取。如果您停用這些權限，管理員將無法看到 **Policy Recommendation**（原則建議）> **IoT** 節點、**Policy Recommendation**（原則建議）> **SaaS** 節點或二者，具體視您停用的權限而定。 如果您將這些權限設定為唯讀，則管理員可以檢視節點，但無法匯入原則規則或編輯資訊。	是	是	是

定義管理員角色設定檔中的使用者隱私權設定

若要定義管理員可存取的使用者私人資料，在建立或編輯管理員角色設定檔時（**Device**（裝置）> **Admin Roles**（管理員角色）），在 **WebUI** 頁籤上向下捲動至 **Privacy**（隱私權）選項。

存取層級	說明	啟用	唯讀	停用
私人	設定預設狀態以啟用或停用下述所有的隱私權設定。	是	無	是
顯示完整 IP 位址	停用時，日誌或報告中不會顯示通過 Palo Alto Networks 防火牆的流量所取得的完整 IP 位址。在一般會顯示 IP 位址的位置處會顯示相關的子網路。	是	無	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	啟用	唯讀	停用
	透過 ***Monitor***（監控） > ***Reports***（報告）在介面中顯示的已排程報告，以及透過已排程電子郵件傳送的報告，仍會顯示完整的 *IP* 位址。因為有此例外狀況，所以我們建議將 ***Monitor***（監控）標籤中的下列設定設為停用：自訂報告、應用程式報告、威脅報告、*URL* 篩選報告、流量報告，以及電子郵件排程器。			
在日誌與報告中顯示使用者名稱	停用時，日誌或報告中不會顯示透過 Palo Alto Networks 防火牆的流量所取得的使用者名稱。一般會顯示使用者名稱的欄會是空白的。 透過 ***Monitor***（監控） > ***Reports***（報告）在介面中顯示的已排程報告，以及透過電子郵件排程器傳送的報告，仍會顯示使用者名稱。因為有此例外狀況，所以我們建議將 *Monitor*（監控）標籤中的下列設定設為停用：自訂報告、應用程式報告、威脅報告、*URL* 篩選報告、流量報告，以及電子郵件排程器。	是	無	是
檢視 PCAP 檔案	停用時，不會顯示流量、威脅與資料過濾等日誌中一般會有的封包擷取檔案。	是	無	是

限制管理員存取提交和驗證功能

若要在建立或編輯管理員角色設定檔（**Device**（裝置） > **Admin Roles**（管理員角色））時限制存取提交（和還原）、儲存和驗證功能，在 **WebUI** 頁籤上向下捲動至 **Commit**（提交）、**Save**（儲存）和 **Validate**（驗證）選項。

©2024 Palo Alto Networks, Inc.

存取層級	說明	啟用	唯讀	停用
提交	為下述所有提交和還原權限設定預設狀態（啟用或停用）。	是	無	是
裝置	停用時，管理員將無法提交或還原任何管理員對防火牆組態所做的變更，包括該管理員自己做的變更。	是	無	是
為其他管理員提交	停用時，管理員無法提交或還原其他管理員對防火牆組態所做的變更。	是	無	是
Save	為下述所有儲存操作權限設定預設狀態（啟用或停用）。	是	無	是
部分儲存	停用時，管理員將無法儲存任何管理員對防火牆組態所做的變更，包括該管理員自己做的變更。	是	無	是
為其他管理員儲存	停用時，管理員無法儲存其他管理員對防火牆組態所做的變更。	是	無	是
驗證	停用時，管理員無法驗證組態。	是	無	是

提供全域設定的精確存取權

若要定義管理員可存取的全域設定，在建立或編輯管理員角色設定檔時（**Device**（裝置） > **Admin Roles**（管理員角色）），在 **WebUI** 頁籤上向下捲動至 **Global**（全域）選項。

存取層級	說明	啟用	唯讀	停用
全域	設定預設狀態以啟用或停用下述所有的全域設定。事實上，此設定目前僅適用於系統警示。	是	無	是
系統警示	停用時，管理員無法檢視或認可產生的警報。	是	無	是

提供 **Panorama** 頁籤的精確存取權

下表列出 **Panorama** 頁籤存取層級，及這些層級可用的自訂 Panorama 管理員角色。防火牆管理員無法存取下述任何權限。

©2024 Palo Alto Networks, Inc.

存取層級	說明	管理員角色可用性	啟用	唯讀	停用
設定	指定管理員是否可以檢視或編輯 Panorama 設定資訊，包括 **Management**（管理）、**Operationsand Telemetry**（操作與遙測）、**Services**（服務）、Content-ID（內容 ID）、**WildFire**、Session（工作階段）或 **HSM**。 如果您將此權限設定為： • 唯讀，則管理員可看到資訊，但無法編輯。 • 停用此權限，則管理員無法看到或編輯資訊。	Panorama:是 裝置群組/範本：否。	是	是	是
High availability（高可用性）	指定管理員是否能夠檢視與管理 Panorama 管理伺服器的高可用性 (HA) 設定。 如果您將此權限設為唯讀，則管理員可檢視 Panorama 管理伺服器的 HA 組態資訊，但無法管理組態。 如果您停用此權限，則管理員無法看到或管理 Panorama 管理伺服器的 HA 組態設定。	Panorama:是 裝置群組/範本：否。	是	是	是
設定稽核	指定管理員是否能執行 Panorama 組態稽核。如果您停用此權限，則管理員無法執行 Panorama 組態稽核。	Panorama:是 裝置群組/範本：否。	是	否。	是
管理員	指定管理員是否能檢視 Panorama 管理員帳戶詳細資料。 您無法啟用此功能的完整存取權：只能啟用唯讀存取權。(只有具備動態角色的 Panorama 管理員能夠新增、編輯或刪除	Panorama:是 裝置群組/範本：否。	否。	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	管理員角色可用性	啟用	唯讀	停用
	Panorama 管理員。) 存取權為唯讀時，管理員可看到自己帳戶的相關資訊，但無法看到其他 Panorama 管理員帳戶的相關資訊。 如果您停用此權限，管理員無法看到任何 Panorama 管理員帳戶（包括自己）的相關資訊。				
管理員角色	指定管理員是否能夠檢視 Panorama 管理員角色。 您無法啟用此功能的完整存取權：只能啟用唯讀存取權。(只有具備動態角色的 Panorama 管理員能夠新增、編輯或刪除自訂 Panorama 角色。) 存取權為唯讀時，管理員可看到 Panorama 管理員角色組態，但無法管理組態。 如果您停用此權限，則管理員無法看到或管理 Panorama 管理員角色。	Panorama:是 裝置群組/範本：否。	否。	是	是
存取網域	指定管理員是否能檢視、新增、編輯、刪除或複製 Panorama 管理員的存取網域設定。（此權限僅控制存取網域設定的存取權，而非指定給存	Panorama:是 裝置群組/範本：否	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	管理員角色可用性	啟用	唯讀	停用
	取網域之設備群組、範本與防火牆內容的存取權。） 如果您將此權限設為唯讀，則管理員可檢視 Panorama 存取網域組態，但無法管理這些網域組態。 如果您停用此權限，則管理員無法看到或管理 Panorama 存取網域組態。	您可以將存取網域指定給裝置群組與範本管理員，使其可以存取指定給存取網域之裝置群組、範本與防火牆內容中的設定與監控資料。			
驗證設定檔	指定管理員是否能檢視、新增、編輯、刪除或複製 Panorama 管理員的驗證設定檔。 如果您將此權限設為唯讀，則管理員可檢視 Panorama 驗證設定檔，但無法管理這些設定檔。 如果您停用此權限，則管理員無法看到或管理 Panorama 驗證設定檔。	Panorama:是 裝置群組/範本：否。	是	是	是
驗證順序	指定管理員是否能檢視、新增、編輯、刪除或複製 Panorama 管理員的驗證順序。 如果您將此權限設為唯讀，則管理員可檢視 Panorama 驗證順序，但無法管理這些設定檔。 如果您停用此權限，則管理員無法看到或管理 Panorama 驗證順序。	Panorama:是 裝置群組/範本：否。	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	管理員角色可用性	啟用	唯讀	停用
使用者識別機制	指定管理員是否可以設定 User-ID 連線安全性，以及檢視、新增、編輯或刪除資料重新散佈點（例如 User-ID 代理程式）。 如果將此權限設為唯讀，則管理員可檢視 User-ID 連線安全性和重新散佈點設定，但無法管理這些設定。 如果停用此權限，管理員將無法看到或管理 User-ID 連線安全性或重新散佈點設定。	Panorama:是 裝置群組/範本：否。	是	是	是
受管理的裝置	指定管理員是否能夠檢視、新增、編輯或刪除用作受管理裝置的防火牆，並在這些防火牆上安裝軟體或內容更新。 如果您將此權限設為唯讀，則管理員可看到受管理的防火牆，但無法在防火牆上新增、刪除、加上標籤或安裝更新。 如果您停用此權限，則管理員無法在受管理的防火牆上檢視、新增、編輯、加上標籤、刪除或安裝更新。 具有裝置部署權限的管理員仍可選取 ***Panorama*** > ***Device Deployment***（裝置部署），以在受管理防火牆上安裝更新。	Panorama:是 裝置群組/範本：是	是 （若為裝置群組和範本角色則為 No（否））	是	是
範本	指定管理員是否能檢視、編輯、新增或刪除範本與範本堆疊。	Panorama:是 裝置群組/範本：是	是 （若為裝置群	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	管理員角色可用性	啟用	唯讀	停用
	如果您將權限設為唯讀，則管理員可看到範本與堆疊組態，但無法管理這些範本與堆疊組態。 如果您停用此權限，則管理員無法看到或管理範本與堆疊組態。	設備群組與範本管理員只能看到指定給這些管理員之存取網域內的範本與堆疊。	組和範本管理員則為 No（否））		
裝置群組	指定管理員是否能夠檢視、編輯、新增或刪除設備群組。 如果您將此權限設為唯讀，則管理員可看到裝置群組組態，但無法管理這些組態。 如果您停用此權限，則管理員無法看到或管理裝置群組組態。	Panorama:是 裝置群組/範本：是 設備群組與範本管理員只能存取指定給這些管理員之存取網域內的設備群組。	是	是	是
受管理的收集器	指定管理員是否能夠檢視、編輯、新增或刪除受管理的收集器。 如果您將此權限設為唯讀，則管理員可看到受管理的收集器設定，但無法管理這些組態。 如果您停用此權限，則管理員無法檢視、編輯、新增、或刪除受管理的收集器組態。 具有裝置部署權限的管理員仍可使用 ***Panorama > Device Deployment***（裝置部署）選項在受管理收集器上安裝更新。	Panorama:是 裝置群組/範本：否。	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	管理員角色可用性	啟用	唯讀	停用
收集器群組	指定管理員是否能夠檢視、編輯、新增或刪除收集器群組。 如果您將此權限設為唯讀，則管理員可看到收集器群組，但無法管理這些群組。 如果您停用此權限，則管理員無法看到或管理收集器群組。	Panorama:是 裝置群組/範本：否。	是	是	是
VMware 服務管理員	指定管理員是否能夠檢視與編輯 VMware Service Manager 設定。 如果您將此權限設為唯讀，則管理員可看到設定，但無法執行任何相關設定或操作程序。 如果您停用此權限，則管理員無法看到設定或執行任何相關的設定或操作程序。	Panorama:是 裝置群組/範本：否。	是	是	是
憑證管理	為所有 Panorama 憑證管理權限設定預設狀態為啟用或停用。	Panorama:是 裝置群組/範本：否。	是	否。	是
憑證	指定管理員是否能夠檢視、編輯、產生、刪除、撤銷、更新或匯出憑證。此權限也指定管理員是否能匯入或匯出 HA 金鑰。 如果您將此權限設為唯讀，則管理員可看到 Panorama 憑證，但無法管理憑證或 HA 金鑰。 如果您停用此權限，則管理員無法看到或管理 Panorama 憑證或 HA 金鑰。	Panorama:是 裝置群組/範本：否。	是	是	是
憑證設定檔	指定管理員是否能檢視、新增、編輯、刪除或複製 Panorama 憑證設定檔。	Panorama:是 裝置群組/範本：否。	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	管理員角色可用性	啟用	唯讀	停用
	如果您將此權限設為唯讀，則管理員可看到 Panorama 憑證設定檔，但無法管理這些設定檔。 如果您停用此權限，則管理員無法看到或管理 Panorama 憑證設定檔。				
SSL/TLS 服務設定檔	指定管理員是否能檢視、新增、編輯、刪除或複製 SSL/TLS 服務設定檔。 如果您將此權限設為唯讀，則管理員可看到 SSL/TLS 服務設定檔，但無法管理這些設定檔。 如果您停用此權限，則管理員無法看到或管理 SSL/TLS 服務設定檔。	Panorama:是 裝置群組/範本：否。	是	是	是
日誌設定	為所有日誌設定權限設定預設狀態為啟用或停用。	Panorama:是 裝置群組/範本：否。	是	否。	是
系統	指定管理員是否能夠看到與設定能控制將 Syslog 轉送至外部服務（syslog、電子郵件、SNMP 設陷或 HTTP 伺服器）的設定。 如果您將此權限設為唯讀，則管理員可看到系統日誌轉送設定，但無法管理這些設定。 如果您停用此權限，則管理員無法看到或管理設定。	Panorama:是 裝置群組/範本：否。	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	管理員角色可用性	啟用	唯讀	停用
	此權限僅與系統 *Panorama* 和日誌收集器產生的系統日誌相關。收集器群組權限（***Panorama*** > ***Collector Groups***（收集器群組））用於控制日誌收集器從防火牆接收之系統日誌的轉送。***Device***（裝置） > ***Log Settings***（日誌設定） > 系統權限用於控制從防火牆直接向外部服務（不在日誌收集器上彙總）轉送日誌。				
設定	指定管理員是否能夠看到與設定能控制將組態日誌轉送至外部服務（syslog、電子郵件、SNMP 設陷或 HTTP 伺服器）的設定。 如果您將此權限設為唯讀，則管理員可看到設定日誌轉送設定，但無法管理這些設定。 如果您停用此權限，則管理員無法看到或管理設定。	Panorama:是 裝置群組/範本：否。	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	管理員角色可用性	啟用	唯讀	停用
	此權限僅與系統 *Panorama* 和日誌收集器產生的組態日誌相關。收集器群組權限（***Panorama*** > ***Collector Groups***（收集器群組））用於控制日誌收集器從防火牆接收之組態日誌的轉送。***Device***（裝置） > ***Log Settings***（日誌設定） > Configuration（組態）權限用於控制從防火牆直接向外部服務（不在日誌收集器上彙總）轉送日誌。				
使用者-ID	指定管理員是否能夠看到與設定能控制將 User-ID 日誌轉送至外部服務（syslog、電子郵件、SNMP 設陷或 HTTP 伺服器）的設定。 如果您將此權限設為唯讀，則管理員可看到設定日誌轉送設定，但無法管理這些設定。 如果您停用此權限，則管理員無法看到或管理設定。	Panorama:是 裝置群組/範本：否。	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	管理員角色可用性	啟用	唯讀	停用
	此選項僅與 *Panorama* 產生的 *User-ID* 日誌相關。收集器群組權限（***Panorama*** > ***Collector Groups***（收集器群組））用於控制日誌收集器從防火牆接收之 *User-ID* 日誌的轉送。***Device***（裝置） > ***Log Settings***（日誌設定） > User-ID 權限用於控制從防火牆直接向外部服務（不在日誌收集器上彙總）轉送日誌。				
HIP 比對	指定管理員是否能夠看到與設定能控制將 HIP 比對日誌從傳統模式 Panorama 虛擬裝置轉送至外部服務（syslog、電子郵件、SNMP 設陷或 HTTP 伺服器）的設定。 如果您將此權限設為唯讀，則管理員可看到 HIP 比對日誌轉送設定，但無法管理這些設定。 如果您停用此權限，則管理員無法看到或管理設定。	Panorama:是 裝置群組/範本：否。	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	管理員角色可用性	啟用	唯讀	停用
	收集器群組權限（***Panorama*** > ***Collector Groups***（收集器群組））用於控制日誌收集器從防火牆接收之 *HIP* 比對日誌的轉送。***Device***（裝置） > ***Log Settings***（日誌設定） >HIP Match（HIP 比對） 權限用於控制從防火牆直接向外部服務（不在日誌收集器上彙總）轉送日誌。				
GlobalProtect	指定管理員是否能夠看到和設定能控制將 GlobalProtect 日誌從傳統模式 Panorama 虛擬裝置轉送至外部服務（syslog、電子郵件、SNMP 設陷或 HTTP 伺服器）的設定。 如果您將此權限設為唯讀，則管理員可看到 GlobalProtect 日誌轉送設定，但無法管理這些設定。 如果您停用此權限，則管理員無法看到或管理設定。	Panorama:是 裝置群組/範本：否。	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	管理員角色可用性	啟用	唯讀	停用
	收集器群組權限（***Panorama*** > ***Collector Groups***（收集器群組））用於控制日誌收集器從防火牆接收之 *GlobalProtect* 日誌的轉送。***Device***（裝置） > ***Log Settings***（日誌設定） > ***GlobalProtect***權限用於控制從防火牆直接向外部服務（不在日誌收集器上彙總）轉送日誌。				
關聯	指定管理員是否能夠看到與設定能控制將關聯性日誌從傳統模式 Panorama 虛擬裝置轉送至外部服務（syslog、電子郵件、SNMP 設陷或 HTTP 伺服器）的設定。 如果您將此權限設為唯讀，則管理員可看到關聯日誌轉送設定，但無法管理這些設定。 如果您停用此權限，則管理員無法看到或管理設定。	Panorama:是 裝置群組/範本：否。	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	管理員角色可用性	啟用	唯讀	停用
	收集器群組權限（***Panorama*** > ***Collector Groups***（收集器群組））用於控制從 *Panorama M* 系列裝置或處於 *Panorama* 模式之 *Panorama* 虛擬裝置轉送關聯性日誌。				
流量	指定管理員是否能夠看到與設定能控制將流量日誌從傳統模式 Panorama 虛擬裝置轉送至外部服務（syslog、電子郵件、SNMP 設陷或 HTTP 伺服器）的設定。 如果您將此權限設為唯讀，則管理員可看到流量日誌轉送設定，但無法管理這些設定。 如果您停用此權限，則管理員無法看到或管理設定。 收集器群組權限（***Panorama*** > ***Collector Groups***（收集器群組））用於控制日誌收集器從防火牆接收之流量日誌的轉送。日誌轉送權限（***Objects***（物件） > ***Log Forwarding***（日誌轉送））用於控制從防火牆直接向外部服務（不在日誌收集器上彙總）轉送日誌。	Panorama:是 裝置群組/範本：否。	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	管理員角色可用性	啟用	唯讀	停用
威脅	指定管理員是否能夠看到與設定能控制將威脅日誌從傳統模式 Panorama 虛擬裝置轉送至外部服務（syslog、電子郵件、SNMP 設陷或 HTTP 伺服器）的設定。 如果您將此權限設為唯讀，則管理員可看到威脅日誌轉送設定，但無法管理這些設定。 如果您停用此權限，則管理員無法看到或管理設定。 收集器群組權限（***Panorama*** > ***Collector Groups***（收集器群組））用於控制日誌收集器從防火牆接收之威脅日誌的轉送。日誌轉送權限（***Objects***（物件） > ***Log Forwarding***（日誌轉送））用於控制從防火牆直接向外部服務（不在日誌收集器上彙總）轉送日誌。	Panorama:是 裝置群組/範本：否。	是	是	是
WildFire	指定管理員是否能夠看到與設定能控制將 WildFire 日誌從傳統模式 Panorama 虛擬裝置轉送至外部服務（syslog、電子郵件、SNMP 設陷或 HTTP 伺服器）的設定。 如果您將此權限設為唯讀，則管理員可看到 WildFire 日誌	Panorama:是 裝置群組/範本：否。	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	管理員角色可用性	啟用	唯讀	停用
	轉送設定，但無法管理這些設定。 如果您停用此權限，則管理員無法看到或管理設定。 收集器群組權限（***Panorama*** > ***Collector Groups***（收集器群組））用於控制日誌收集器從防火牆接收之 *WildFire* 日誌的轉送。日誌轉送權限（***Objects***（物件） > ***Log Forwarding***（日誌轉送））用於控制從防火牆直接向外部服務（不在日誌收集器上彙總）轉送日誌。				
伺服器設定檔	為所有伺服器設定檔權限設定預設狀態為啟用或停用。	Panorama:是 裝置群組/範本：否。	是	否。	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	管理員角色可用性	啟用	唯讀	停用
	這些權限適用於伺服器設定檔，且僅限於用於轉送來自於 *Panorama* 或日誌收集器的日誌或用於驗證 *Panorama* 管理員的設定檔。***Device***（裝置）> 伺服器設定檔權限用於控制對伺服器設定檔的存取權，這些設定檔用於從防火牆直接向外部服務轉送日誌及驗證防火牆管理員。				
SNMP 陷阱	指定管理員是否能夠檢視與設定 SNMP 設陷伺服器設定檔。 如果您將此權限設為唯讀，則管理員可看到 SNMP 設陷伺服器設定檔，但無法管理這些設定檔。 如果您停用此權限，則管理員無法看到或管理 SNMP 設陷設定檔。	Panorama:是 裝置群組/範本：否。	是	是	是
Syslog	指定管理員是否能看到與設定 Syslog 伺服器設定檔。 如果您將此權限設為唯讀，則管理員可看到 Syslog 伺服器設定檔，但無法管理這些設定檔。 如果您停用此權限，則管理員無法看到或管理 Syslog 伺服器設定檔。	Panorama:是 裝置群組/範本：否。	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	管理員角色可用性	啟用	唯讀	停用
電郵	指定管理員是否能看到與設定電子郵件伺服器設定檔。 如果您將此權限設為唯讀，則管理員可看到電子郵件伺服器設定檔，但無法管理這些設定檔。 如果您停用此權限，則管理員無法看到或管理電子郵件伺服器設定檔。	Panorama:是 裝置群組/範本：否。	是	是	是
RADIUS	指定管理員是否能看到與設定用於驗證 Panorama 管理員的 RADIUS 伺服器設定檔。 如果您將此權限設為唯讀，則管理員可看到 RADIUS 伺服器設定檔，但無法管理這些設定檔。 如果您停用此權限，則管理員無法看到或管理 RADIUS 伺服器設定檔。	Panorama:是 裝置群組/範本：否。	是	是	是
TACACS+	指定管理員是否能看到與設定用於驗證 Panorama 管理員的 TACACS+ 伺服器設定檔。 如果您停用此權限，管理員將看不到節點，或無法針對驗證設定檔所參考的 TACACS+ 伺服器進行設定。 如果您將此權限設為唯讀，則管理員可檢視現有 TACACS+ 伺服器設定檔，但無法新增或編輯這些設定檔。	Panorama:是 裝置群組/範本：否。	是	是	是
LDAP	指定管理員是否能看到與設定用於驗證 Panorama 管理員的 LDAP 伺服器設定檔。	Panorama:是 裝置群組/範本：否。	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	管理員角色可用性	啟用	唯讀	停用
	如果您將此權限設為唯讀，則管理員可看到 LDAP 伺服器設定檔，但無法管理這些設定檔。 如果您停用此權限，則管理員無法看到或管理 LDAP 伺服器設定檔。				
Kerberos	指定管理員是否能看到與設定用於驗證 Panorama 管理員的 Kerberos 伺服器設定檔。 如果您將此權限設為唯讀，則管理員可看到 Kerberos 伺服器設定檔，但無法管理這些設定檔。 如果您停用此權限，則管理員無法看到或管理 Kerberos 伺服器設定檔。	Panorama:是 裝置群組/範本：否。	是	是	是
SAML 識別提供者	指定管理員是否能看到與設定用於驗證 Panorama 管理員的 SAML 識別提供者 (IdP) 伺服器設定檔。 如果您將此權限設為唯讀，則管理員可看到 SAML IdP 伺服器設定檔，但無法管理這些設定檔。 如果停用此權限，管理員將無法看到或管理 SAML IdP 伺服器設定檔。	Panorama:是 裝置群組/範本：否。	是	是	是
已排程的設定匯出	指定管理員是否能檢視、新增、編輯、刪除或複製排程的 Panorama 組態匯出項目。 如果您將此權限設為唯讀，則管理員可檢視已排程的匯出項目，但無法管理這些項目。	Panorama:是 裝置群組/範本：否。	是	否。	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	管理員角色可用性	啟用	唯讀	停用
	如果您停用此權限，則管理員無法看到或管理已排程的匯出項目。				
軟體	指定管理員是否可以：檢視 Panorama 管理伺服器上所安裝之軟體更新的相關資訊；下載、上傳或安裝更新；以及檢視相關的版本資訊。 如果您將此權限設為唯讀，則管理員可檢視 Panorama 軟體更新的相關資訊，並檢視相關的版本資訊，但無法執行任何相關的操作。 如果您停用此權限，則管理員無法看到 Panorama 軟體更新、檢視相關的版本資訊，或執行任何相關的操作。 **Panorama** > Device Deployment（裝置部署） > Software（軟體） 權限用於控制存取防火牆上部署的 *PAN-OS* 軟體及專用日誌收集器上部署的 *Panorama* 軟體。	Panorama:是 裝置群組/範本：否。	是	是	是
動態更新	指定管理員是否可以：檢視 Panorama 管理伺服器上所安裝之內容更新的相關資訊（例如，WildFire 更新）；下載、上傳、安裝或還原更新；檢視相關聯的版本資訊。 如果您將此權限設為唯讀，則管理員可檢視 Panorama 內容更新的相關資訊，並檢視相關的	Panorama:是 裝置群組/範本：否。	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	管理員角色可用性	啟用	唯讀	停用
	版本資訊，但無法執行任何相關的操作。 如果您停用此權限，則管理員無法看到 Panorama 內容更新、檢視相關的版本資訊，或執行任何相關的操作。 ***Panorama*** > Device Deployment（管理部署） > Dynamic Updates（動態更新）權限用於控制存取防火牆和專用日誌收集器上部署的內容更新。				
支援	指定管理員是否可：檢視 Panorama 支援授權資訊、產品警報與安全性警報；啟動支援授權，以及管理個案。僅超級使用者管理員可產生技術支援檔案。 如果您將此權限設為唯讀，則管理員可檢視 Panorama 支援資訊、產品警示與安全性警示，但無法啟動支援授權、產生技術支援檔案，或管理個案。 如果您停用此權限，則管理員無法：檢視 Panorama 支援資訊、產品警示與安全性警示；啟動支援授權、產生技術支援檔案，或管理個案。	Panorama:是 裝置群組/範本：否。	是	是	是
設備部署	為所有與部署授權及軟體或內容更新到防火牆及日誌收集器的權限設定預設狀態（啟用或停用）。	Panorama:是 裝置群組/範本：是	是	否。	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	管理員角色可用性	啟用	唯讀	停用
	Panorama > Software（軟體）和 ***Panorama*** > Dynamic Updates（動態更新）權限用於控制在 *Panorama* 管理伺服器上安裝的軟體與內容更新。				
軟體	指定管理員是否可以：檢視安裝在防火牆與日誌收集器上的軟體更新相關資訊；下載、上傳或安裝更新；以及檢視相關的版本資訊。 如果您將此權限設為唯讀，則管理員可檢視軟體更新相關資訊，並檢視相關的版本資訊，但無法將更新部署至防火牆或專用的日誌收集器。 如果您停用此權限，則管理員無法檢視軟體更新相關資訊、檢視相關的版本資訊，或將更新部署至防火牆或專用的日誌收集器。	Panorama:是 裝置群組/範本：是	是	是	是
GlobalProtect 用戶端	指定管理員是否可以：檢視防火牆上 GlobalProtect 應用程式軟體更新相關資訊；下載、上傳或啟動更新；檢視相關聯的版本資訊。 如果您將此權限設為唯讀，則管理員可檢視 GlobalProtect 應用程式軟體更新相關資訊，並檢視相關的版本資訊，但無法啟動防火牆上的更新。 如果您停用此權限，則管理員無法看到 GlobalProtect 應用程	Panorama:是 裝置群組/範本：是	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	管理員角色可用性	啟用	唯讀	停用
	式軟體更新相關資訊、檢視相關的版本資訊，或啟動防火牆上的更新。				
動態更新	指定管理員是否可以：檢視安裝在防火牆與專用日誌收集器上的內容更新（例如應用程式更新）相關資訊；下載、上傳或安裝更新；以及檢視相關的版本資訊。 如果您將此權限設為唯讀，則管理員可檢視內容更新相關資訊，並檢視相關的版本資訊，但無法將更新部署至防火牆或專用的日誌收集器。 如果您停用此權限，則管理員無法檢視內容更新相關資訊、檢視相關的版本資訊，或將更新部署至防火牆或專用的日誌收集器。	Panorama:是 裝置群組/範本：是	是	是	是
授權	指定管理員是否能檢視、重新整理及啟動防火牆授權。 如果您將此權限設為唯讀，則管理員可檢視防火牆授權，但無法重新整理或啟動這些授權。 如果您停用此權限，則管理員無法檢視、重新整理或啟動防火牆授權。	Panorama:是 裝置群組/範本：是	是	是	是
主要金鑰與診斷	指定管理員是否能檢視與設定用於在 Panorama 上加密私密金鑰的主要金鑰。 如果您將此權限設為唯讀，則管理員可檢視 Panorama 主要金鑰設定，但無法變更此設定。	Panorama:是 裝置群組/範本：否。	是	是	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	管理員角色可用性	啟用	唯讀	停用
	如果您停用此權限，則管理員無法看到或編輯 Panorama 主要金鑰組態。				

提供對操作設定的精確存取權

若要定義管理員可存取的操作設定，在建立或編輯防火牆的管理員角色設定檔（**Device**（裝置）> **Admin Roles**（管理員角色））時，請向下捲動至 **Web UI** 頁籤上的 **Operations**（操作）選項。

存取層級	說明	啟用	唯讀	停用
重新啟動	重新啟動防火牆。防火牆會登出所有使用者，重新載入 PAN-OS 軟體和作用中設定，關閉並記錄現有工作階段，以及建立一個系統日誌項目，顯示發起重新啟動的管理員名稱。此存取也會影響關機操作。	是	無	是
產生技術支援檔案	產生技術支援系統檔案，Palo Alto Networks 支援團隊可使用該檔案對您可能遇到的防火牆問題進行疑難排解。	是	無	是
產生統計資料傾印檔案	產生並下載一組 XML 報告，總結防火牆過去七天的網路流量。	是	無	是
下載核心檔案	如果防火牆遭遇系統程序失敗，會自動產生一個核心檔案，其中包含關於程序的詳細資料及失敗原因。您可以下載此核心檔案並上傳至您的 Palo Alto Networks 支援案例，以取得解決問題的進一步協助。	是	無	是
下載偵錯和管理 Pcap 檔案	如果防火牆遇到封包擷取失敗，則其會產生一個封包擷取 (pcap) 檔案，其中包含有關失敗原因的除錯和管理詳細資料。您可以下載這個 pcap 檔案並將其上傳到 Palo Alto Networks 支援案例，以取得解決問題的協助。	是	無	是

©2024 Palo Alto Networks, Inc.

Panorama Web 介面存取權限

自訂 Panorama 管理員角色可讓您定義 Panorama 上選項的存取權，並能夠只允許存取 Device Groups and Templates（裝置群組和範本）（**Policies**（原則）、**Objects**（物件）、**Network**（網路）、**Device**（裝置）頁籤）。

您可以建立的管理員角色有 **Panorama** 與 **Device Group and Template**（裝置群組與範本）。您無法將 CLI 存取權限指派給 **Device Group and Template**（裝置群組和範本）管理員角色設定檔。如果您將 CLI 超級使用者權限指派給 **Panorama** 管理員角色，則為該角色的管理員可存取所有的功能，無論您指派的網頁介面權限為何。

存取層級	說明	啟用	唯讀	停用
儀錶盤	控制 **Dashboard**（儀表板）標籤的存取權。如果您停用此權限，管理員將看不到此標籤，也無法存取任何儀表板 Widget。	是	否。	是
ACC	控制存取應用程式監測中心 (ACC)。如果您停用此權限，**ACC** 標籤將不會顯示在 Web 介面中。請記住，如果您想要保護使用者的隱私權，但仍提供給使用者 ACC 的存取權，您可以停用 **Privacy**（隱私權） > **Show Full IP Addresses**（顯示完整 **IP** 位址）選項和/或 **Show User Names In Logs And Reports**（在日誌與報告中顯示使用者名稱） 選項。	是	否。	是
監控	控制 **Monitor**（監控）標籤的存取權。如果您停用此權限，管理員將看不到 **Monitor**（監控）標籤，且無法存取任何日誌、封包擷取、工作階段資訊、報告或 App Scope。若要更細微地控制管理員可看到的監控資訊，將 Monitor（監控）選項保持啟用，然後依照為監控頁籤提供細微存取權中所述啟用或停用頁籤上的特定節點。	是	否。	是
原則	控制**Policies**（原則）標籤的存取權。如果您停用此權限，管理員將看不到**Policies**（原則）標籤，也無法存取任何原則資訊。若要更細微地控制管理員可看到的原則資訊，例如允許存取特定類型的原則或允許唯讀存取原則資訊，將 **Policies**（原則）選項保持為啟用，然後依	是	否。	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	啟用	唯讀	停用
	照為原則頁籤提供細微存取權中所述啟用或停用頁籤上的特定節點。			
物件	控制存取 **Objects**（物件）標籤。如果您停用此權限，管理員將看不到 **Objects**（物件）標籤，也無法存取任何物件、安全性設定檔、日誌轉送設定檔、解密設定檔或排程。若要更細微地控制管理員可看到的物件，將 **Objects**（物件）選項保持啟用，然後按為物件頁籤提供細微存取權中所述啟用或停用頁籤上的特定節點。	是	否。	是
網路	控制存取 **Network**（網路）標籤。如果您停用此權限，管理員將看不到 **Network**（網路）標籤，也無法存取任何介面、區域、VLAN、虛擬連接、虛擬路由器、IPsec 通道、DHCP、DNS Proxy、GlobalProtect、QoS 組態資訊或網路設定檔。若要更細微地控制管理員可看到的物件，將 **Network**（網路）選項保持啟用，然後按為網路頁籤提供細微存取權中所述啟用或停用頁籤上的特定節點。	是	否。	是
裝置	控制 **Device**（裝置）標籤的存取權。如果您停用此權限，管理員將看不到 **Device**（裝置）頁籤，也無法存取任何裝置全域設定資訊，例如 User-ID、高可用性、伺服器設定檔或憑證組態資訊。若要更細微地控制管理員可看到的物件，將 **Device**（裝置）選項保持啟用，然後按為裝置頁籤提供細微存取權中所述啟用或停用頁籤上的特定節點。 即使您已啟用 ***Device***（裝置）頁籤的完整存取權，仍無法為角色式管理員啟用 ***Admin Roles***（管理員角色）或 ***Administrators***（管理員）節點的存取權。	是	否。	是
Panorama	控制 **Panorama** 頁籤的存取權。如果您停用此權限，則管理員將看不到 **Panorama**	是	否。	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	啟用	唯讀	停用
	頁籤，且將無法存取任何涵蓋整個 Panorama 的組態資訊，例如受管理的裝置、受管理的收集器，或收集器群組。 若要更細微地控制管理員可看到的物件，將 **Panorama** 選項保持啟用，然後按為 Panorama 頁籤提供細微存取權中所述啟用或停用頁籤上的特定節點。			
私人	控制對定義管理員角色設定檔中的使用者隱私權設定中所述之隱私權設定的存取權。	是	否。	是
驗證	停用時，管理員無法驗證組態。	是	否。	是
Save	針對下述儲存權限（部分儲存或為其他管理員儲存），設定預設狀態（啟用或停用）。	是	否。	是
• 部分儲存	停用時，管理員無法儲存任何管理員對 Panorama 組態所做的變更。	是	否。	是
• 為其他管理員儲存	停用時，管理員無法儲存其他管理員對 Panorama 組態所做的變更。	是	否。	是
提交	針對下述所有提交、推送和還原權限（Panorama、裝置群組、範本、強制範本值、收集器群組、WildFire 裝置叢集），設定預設狀態（啟用或停用）。	是	否。	是
• Panorama	停用時，管理員將無法提交或還原任何管理員所做的組態變更，包括該管理員自己做的變更。	是	否。	是
• 為其他管理員提交	停用時，管理員將無法提交或還原其他管理員所做的組態變更。	是	否。	是
• 推送所有變更	停用后，管理員無法推送管理員所做的所有設定變更。	是	否。	是
• 為其他管理員推送	停用后，管理員無法選取和推送其他管理員所做的設定變更。	是	否。	是

©2024 Palo Alto Networks, Inc.

存取層級	說明	啟用	唯讀	停用
• 物件層級變更	停用后，管理員無法選取要推送的單個設定物件。	是	否。	是
裝置群組	停用時，管理員將無法推送變更到裝置群組。	是	否。	是
範本	停用時，管理員將無法推送變更到範本。	是	否。	是
強制範本值	此權限控制 Push Scope Selection（推送範圍選擇）對話方塊中的 **Force Template Values**（強制範本值）選項。 停用時，管理員無法用 Panorama 從範本推送的設定取代本機防火牆組態中的覆寫設定。 如果您在啟用 ***Force Template Values***（強制範本值）的情況下推送一個設定，則防火牆上所有的取代值都將替換為範本中的數值。在使用此選項之前，請檢查防火牆上的取代值，以確保您的提交不會導致任何意外的網路中斷或因為更換這些取代值導致的問題。	是	否。	是
收集器群組	停用時，管理員將無法推送變更到收集器群組。	是	否。	是
WildFire 裝置叢集	停用時，管理員將無法推送變更到 WildFire 裝置叢集。	是	否。	是
工作	停用時，管理員將無法存取工作管理員。	是	否。	是
全域	控制提供全域設定的細微存取權中所述全域設定（系統警報）的存取權。	是	否。	是

©2024 Palo Alto Networks, Inc.

參考：連接埠號使用

下表列出防火牆與 Panorama 用來互相通訊或與網路上其他服務通訊的連接埠。

- 用於管理功能的連接埠
- 用於 HA 的連接埠
- 用於 Panorama 的連接埠
- 用於 GlobalProtect 的連接埠
- 用於 User-ID 的連接埠
- 用於 IPsec 的連接埠
- 用於路由的連接埠
- 用於 DHCP 的連接埠
- 用於基礎結構的連接埠

用於管理功能的連接埠

防火牆和 Panorama 將下列連接埠用於管理功能。

目的地連接埠	通訊協定	說明
22	TCP	用於從用戶端系統對防火牆　CLI 介面的通訊。
80	TCP	防火牆作為 OCSP 回應程式時用來接聽線上憑證狀態通訊協定 (OCSP) 更新的連接埠。 如果在伺服器憑證中指定，連接埠 *80* 也用於 *OCSP* 驗證。
123	Udp	防火牆針對 NTP 更新所使用的連接埠。
443	TCP	用於從用戶端系統對防火牆網頁介面通訊。此外，防火牆以及 User-ID 代理程式也使用此連接埠來接聽更新（在您啟用 VM 監控以追蹤虛擬網路變更時）。 用於從防火牆到 Palo Alto Networks 更新伺服器的輸出通訊。 如需監控 AWS 環境，這是唯一使用的連接埠。 如需監控 VMware vCenter/ESXi 環境，則接聽的連接埠預設為 443，但這是可設定的。

©2024 Palo Alto Networks, Inc.

目的地連接埠	通訊協定	說明
4443	TCP	用作 HTTPS 的替代 SSL 連接埠。
162	Udp	防火牆、Panorama 或日誌收集器用來將設陷轉送至 SNMP 管理員的連接埠。 *Palo Alto Networks* 防火牆上不需要開啟此連接埠。您必須設定簡易網路管理通訊協定 *(SNMP)* 管理員才能接聽此連接埠。如需詳細資訊，請參閱您 *RADIUS* 管理軟體的文件。
161	Udp TCP	防火牆用來接聽來自 SNMP 管理員之輪詢要求（GET 訊息）的連接埠。
514 514 6514	TCP Udp SSL	如果您設定 Syslog 監控，防火牆、Panorama 或日誌收集器用來將日誌傳送至 Syslog 伺服器的連接埠，以及整合了 PAN-OS 的 User-ID 代理程式或基於 Windows 的 User-ID 代理程式的將用於接聽驗證 Syslog 訊息的連接埠。
2055	Udp	若您設定 NetFlow 匯出，防火牆用來將 NetFlow 記錄傳送至 NetFlow 收集器的預設連接埠，但這是可設定的。
5008	TCP	GlobalProtect Mobile Security Manager 用來接聽來自 GlobalProtect 閘道之 HIP 要求的連接埠。 如果您使用的是第三方 MDM 系統，則您可以設定閘道依照 MDM 廠商的需求使用不同的連接埠。
6080 6081 6082	TCP TLS 1.2 TCP	用於 User-ID™ 驗證入口網站的連接埠： • 6080 用於 NT LAN Manager (NTLM) 驗證 • 6081 用於驗證沒有 SSL/TLS 伺服器設定檔的入口網站 • 6082 用於驗證具有 SSL/TLS 伺服器設定檔的入口網站
10443	SSL	防火牆與 Panorama 使用此連接埠來提供有關威脅的內容資訊，並將威脅調查無縫地轉移到威脅保存庫和 AutoFocus。

用於 HA 的連接埠

設定為 高可用性 (HA) 對等體的防火牆必須能夠互相通訊，才能維護狀態資訊（HA1 控制連結）與同步資料（HA2 資料連結）。在主動/主動 HA 部署中，對等防火牆也必須將封包轉送到擁有工作階段的 HA 對等。HA3 連結是 Layer 2 (MAC 中 MAC) 連結，不支援 Layer 3 定址或加密。

©2024 Palo Alto Networks, Inc.

目的地連接埠	通訊協定	說明
28769 28260	TCP TCP	用於 HA1 控制連結，讓 HA 對等防火牆之間進行純文字通訊。HA1 連結為 Layer 3 連結，且需 IP 位址。
28	TCP	用於 HA1 控制連結，讓 HA 對等之間進行加密的通訊 (TCP 上的 SSH)。
28770	TCP	用於 HA1 備份連結的接聽連接埠。
28771	TCP	用於活動訊號備份的連接埠。如果您在 HA1 或 HA1 備份連結使用頻內連接埠，Palo Alto Networks 建議啟用 MGT 介面上的活動訊號備份。
99 29281	ip Udp	用於 HA2 連結，藉以在 HA 配對中的防火牆之間同步化工作階段、轉送表格、IPSec 安全性關聯和 ARP 表格。HA2 連結中的資料流永遠為單一方向性（HA2 保持運作除外）；其流向會從主動防火牆（主動/被動）或主動-主要（主動/主動），流往被動防火牆（主動/被動）或主動-次要（主動/主動）。HA2 連結為 Layer 2 連結，而預設為使用 ether 類型 0x7261。 HA 資料連結也可設定為使用 IP (通訊協定編號 99) 或 UDP (連接埠 29281) 作為傳輸用途，並允許 HA 資料連結跨越子網路。

用於 Panorama 的連接埠

Panorama 將使用下列連接埠。

目的地連接埠	通訊協定	說明
22	TCP	用於從用戶端系統對 Panorama CLI 介面通訊。
443	TCP	用於從用戶端系統對 Panorama Web 介面通訊。 用於從 Panorama 到 Palo Alto Networks 更新伺服器的輸出通訊。
444	TCP	用於 Panorama 和 Cortex 資料湖之間的通訊。
3978	TCP	用於 Panorama 與受管理防火牆或受管理收集器之間的通訊，以及收集器群組中受管理收集器之間的通訊：

©2024 Palo Alto Networks, Inc.

目的地連接埠	通訊協定	說明
		• 用於 Panorama 和防火牆之間的通訊。此連線從受管理防火牆發起，連線到 Panorama，並促進雙向資料交換，即防火牆將日誌轉送到 Panorama，Panorama 將設定變更推送至防火牆。會透過相同的連線傳送內容切換命令。 • 日誌收集器使用此目的地連接埠將日誌轉送至 Panorama。 • 適用於與在 Panorama 模式中 M 系列裝置上預設日誌收集器的通訊，及與專用的日誌收集器。
28443	TCP	用於受管理裝置（防火牆及日誌收集器）從 Panorama 擷取軟體和內容更新。 僅執行 *PAN-OS 8.x* 及更新版本的裝置才會透過此連接埠從 *Panorama* 擷取更新。對於執行之前版本的裝置，*Panorama* 將透過連接埠 *3978* 推送更新套件.
28769（5.1 與更新版本） 28260（5.0 與更新版本） 49160（5.0 與更舊版本）	TCP TCP TCP	用於使用純文字通訊進行 HA 連線及在 Panorama HA 對等之間同步化。通訊可由任何對等啟動。
28	TCP	用於使用加密通訊 (TCP 上的 SSH) 進行的 HA 連線及 Panorama HA 對等之的通訊。通訊可由任何對等啟動。 用於收集器群組中日誌收集器之間為了散佈日誌進行的通訊。
28270（6.0 與更新版本） 49190（5.1 與更舊版本）	TCP	用於收集器群組中日誌收集器之間為了散佈日誌進行的通訊。
2049	TCP	Panorama 虛擬裝置用來將日誌寫入 NFS 資料存放區。
10443	SSL	Panorama 使用此連接埠來提供有關威脅的內容資訊，並將威脅調查無縫地轉移到威脅保存庫和 AutoFocus。

©2024 Palo Alto Networks, Inc.

目的地連接埠	通訊協定	說明
23000 到 23999	TCP、UDP 或 SSL	用於 Panorama 與 Traps ESM 元件之間的 Syslog 通訊。

用於 GlobalProtect 的連接埠

GlobalProtect 將使用下列連接埠。

目的地連接埠	通訊協定	說明
443	TCP	用於 GlobalProtect 應用程式和入口網站之間的通訊，或 GlobalProtect 應用程式與閘道之間的通訊，以及 SSL 通道連線。 GlobalProtect 閘道也將使用此連接埠從 GlobalProtect 應用程式收集主機資訊，並執行主機資訊設定檔 (HIP) 檢查。
4501	Udp	用於 GlobalProtect 應用程式與閘道之間的 IPSec 通道連線。

如需使用回送介面來為不同連接埠與位址的 GlobalProtect 提供存取權的方法提示，請參閱是否可以將 GlobalProtect 入口網站頁面設定為可在任何連接埠存取？

用於 User-ID 的連接埠

User-ID 是讓使用者 IP 位址對應到使用者名稱與群組成員的功能，並為您網路上的使用者活動啟用以使用者或群組為基礎的原則與可見度（例如，能夠快速追蹤到可能是威脅受害者的使用者）。若要執行此對應，防火牆、User-ID 代理程式 (無論是安裝在 Windows 系統上，或是在防火牆上執行的 PAN-OS 整合代理程式上) 和/或終端機伺服器代理程式必須能夠連線至您網路上的目錄服務，才能執行群組對應與使用者對應。此外，如果代理程式是在防火牆外部的系統上執行，則代理程式必須能夠連線至防火牆，藉以向防火牆傳達 IP 位址對使用者名稱的對應。下表列出 User-ID 的通訊需求，以及建立連線所需的連接埠號碼。

目的地連接埠	通訊協定	說明
389	TCP	防火牆用來與 LDAP 伺服器（純文字或啟動傳輸層安全性啟動 TLS）連線以對應使用者到群組的連接埠。
3268	TCP	防火牆用來與 Active Directory Global Catalogue 伺服器（純文字或啟動 TLS）連線以對應使用者到群組的連接埠。

©2024 Palo Alto Networks, Inc.

目的地連接埠	通訊協定	說明
636	TCP	防火牆用來透過 SSL 連線將 LDAP 與 LDAP 伺服器連線以對應使用者到群組的連接埠。
3269	TCP	防火牆用於透過 SSL 連線將 LDAP 與 Active Directory Global Catalogue 伺服器連線以對應使用者到群組的連接埠。
514 6514	TCP Udp SSL	User-ID 代理程式將接聽驗證 syslog 訊息的連接埠（如果您設定 User-ID 以監控用於使用者對應的 Syslog 傳送程式）。連接埠視乎代理程式類型和通訊協定而定： • 整合了 PAN-OS 的 User-ID 代理程式—連接埠 6514 用於 SSL，連接埠 514 用於 UDP。 • 基於 Windows 的 User-ID 代理程式—連接埠 514 用於 TCP 和 UDP。
5007	TCP	防火牆接聽使用者對應資訊的連接埠。代理程式只要得知有全新或更新後的對應，就會傳送 IP 位址與使用者對應及時間戳記。此外，它還會重新整理已知對應。
5006	TCP	User-ID 代理程式用於接聽 XML API 要求的連接埠。此通訊的來源一般為執行會呼叫 API 之指令碼的系統。
88	UDP/TCP	User-ID 代理程式用來驗證 Kerberos 伺服器的連接埠。防火牆會先嘗試 UDP，然後再回復至 TCP。
1812	Udp	User-ID 代理程式用來驗證 RADIUS 伺服器的連接埠。
49	TCP	User-ID 代理程式用來驗證 TACACS+ 伺服器的連接埠。
135	TCP	User-ID 代理程式與 Microsoft 遠端程序呼叫 (RPC) 端點對應程式之間建立 TCP 式 WMI 連線時所使用的連接埠。接著端點對應程式會將隨機指派的連接埠 (範圍為 49152-65535) 指派給代理程式。代理程式會使用此連線進行 Exchange Server 或 AD 伺服器安全性日誌、工作階段表格的 RPC 查詢。這也是用於存取終端機伺服器的連接埠。 User-ID 代理程式也使用此連接埠來連線至用戶端系統，以執行 Windows Management Instrumentation (WMI) 探查。

©2024 Palo Alto Networks, Inc.

目的地連接埠	通訊協定	說明
139	TCP	User-ID 代理程式在與 AD 伺服器之間建立 TCP 式 NetBIOS 連線，使其能夠傳送安全性日誌與工作階段資訊的 RPC 查詢時，所使用的連接埠。
445	TCP	User-ID 代理程式使用與 Active Directory (AD) 伺服器間的 TCP 式 SMB 連線，連線至 AD 以存取使用者登入資訊 (列印多工緩衝處理器與 Net Logon) 時，所使用的連接埠。
5985	HTTP	User-ID 代理程式用於透過 WinRM over HTTP 通訊協定監控安全性日誌和工作階段資訊的連接埠。
5986	HTTPS	User-ID 代理程式用於透過 WinRM over HTTPS 通訊協定監控安全性日誌和工作階段資訊的連接埠。
5009	TCP	防火牆用於連線至終端機伺服器代理程式的連接埠。

用於 IPsec 的連接埠

防火牆和 Panorama 將下列連接埠用於 IPSec 功能。

目的地連接埠	通訊協定	說明
500	Udp	管理平面上的 IKE 用於與遠端 IKE 對等連線的連接埠。
4500	Udp	管理平面上的 IKE 用於與遠端 IKE 對等連線的連接埠。
4510	Udp	資料平面用於將要求傳送至 IKE 的連接埠。
4511	Udp	資料平面用於將要求傳送至 `keymgr` 的連接埠。

用於路由的連接埠

防火牆和 Panorama 將下列連接埠用於路由功能。

目的地連接埠	通訊協定	說明
179	TCP	BGP 用於連線到對等的連接埠。

©2024 Palo Alto Networks, Inc.

目的地連接埠	通訊協定	說明
3784 3785 4784	Udp	BGP 用於連線到對等的連接埠。
520	Udp	用於 RIPv2 的連接埠。
89	ip	用於 OSPF 和 OSPFv3 的連接埠。
103	ip	用於通訊協定獨立多點傳送 (PIM) 的連接埠。
639	TCP	用於 BGP 連線到對等的連接埠。

用於 DHCP 的連接埠

防火牆和 Panorama 將下列連接埠用於 DHCP 功能。

目的地連接埠	通訊協定	說明
67 68 546 547	Udp	用作 DHCP 伺服器接聽連接埠的連接埠。

用於基礎結構的連接埠

防火牆和 Panorama 將下列連接埠用於基礎結構功能。

目的地連接埠	通訊協定	說明
111	TCP/UDP	用作連接埠對應程式的連接埠。
23	TCP/UDP	用於 Telnet 應用程式通訊協定的連接埠。
69	TCP/UDP	用於 TFTP 的連接埠。

©2024 Palo Alto Networks, Inc.

目的地連接埠	通訊協定	說明
2049	TCP/UDP	用於網路檔案系統 (NFS) 的連接埠。
28260	TCP	內部 sysd IPC 通訊用於內部程序的連接埠。
28261	TCP	內部 md 應用程式用於管理內部程序的連接埠。
動態	TCP/UDP	NFS 操作使用的動態連接埠，用於連接管理平面中的主機資料平面檔案系統。

©2024 Palo Alto Networks, Inc.

將防火牆重設為原廠預設設定

將防火牆重設為原廠預設值，將會失去所有的組態設定與日誌。

STEP 1 | 設定防火牆的主控台連線。

1. 從電腦中將序列纜線連接至主控台連接埠，然後使用終端模擬軟體連接至防火牆 (9600-8-N-1)。

   如果您的電腦沒有 *9* 針腳的序列埠，請使用 *USB* 對序連接埠接頭。

2. 輸入您的登入認證。
3. 輸入下列 CLI 命令：

   `debug system maintenance-mode`

   防火牆將以維護模式重新開機。

STEP 2 | 將系統重設為原廠預設設定。

1. 防火牆重新開機時，請按下 **Enter** 繼續進行維護模式功能表。
2. c選取 **Factory Reset**，然後按下 **Enter**。
3. 選取 **Factory Reset**，然後再次按下 **Enter**。

   防火牆將會重新開機，但沒有任何組態設定。登入防火牆的預設使用者名稱與密碼是 admin/admin。

   若要在防火牆上執行初始設定及設定網路連線，請參閱將防火牆整合至管理網路。

©2024 Palo Alto Networks, Inc.

啟動程序防火牆

啟動程序可加速設定程序並授權防火牆，使其無需存取網際網路即可在網路上運作。啟動程序可讓您選擇是否使用基本組態檔案 (init-cfg.txt) 設定防火牆，以便連線至 Panorama 並取得完整的組態，或使用基本組態與可選 bootstrap.xml 檔案完全設定防火牆。

- USB 快閃磁碟機支援
- 範例 init-cfg.txt 檔案
- 準備 USB 快閃磁碟機以啟動防火牆
- 使用 USB 快閃磁碟機啟動防火牆

USB 快閃磁碟機支援

啟動基於硬體的 Palo Alto Networks 防火牆的 USB 快閃磁碟機必須支援下列其中一項：

- File Allocation Table 32 (FAT32)
- Third Extended File System (ext3)

防火牆可從下列快閃磁碟機（採用 USB2.0 或 USB3.0 連接）啟動的防火牆：

支援的 **USB** 快閃磁碟機
Kingston • Kingston SE9 8GB (2.0) • Kingston SE9 16GB (3.0) • Kingston SE9 32GB (3.0)
SanDisk • SanDisk Cruzer Fit CZ33 8GB (2.0) • SanDisk Cruzer Fit CZ33 16GB (2.0) • SanDisk Cruzer CZ36 16GB (2.0) • SanDisk Cruzer CZ36 32GB (2.0) • SanDisk Extreme CZ80 32GB (3.0)
Silicon Power • Silicon Power Jewel 32GB (3.0) • Silicon Power Blaze 16GB (3.0)
PNY

©2024 Palo Alto Networks, Inc.

支援的 **USB** 快閃磁碟機
• PNY Attache 16GB (2.0) • PNY Turbo 32GB (3.0)

範例 init-cfg.txt 檔案

啟動程序需要 init-cfg.txt 檔案；此檔案為您使用文字編輯器建立的基本組態檔案。若要建立此檔案，請參閱5。下列範例 init-cfg.txt 檔案顯示檔案中支援的參數；您必須提供的參數以粗體顯示。

範例 init-cfg.txt（靜態 IP 位址）

```
type=static ip-
address=10.5.107.19 default-
gateway=10.5.107.1 netmask=255.255.25
address=2001:400:f00::1/64 ipv6-
default-gateway=2001:400:f00::2
 hostname=Ca-FW-DC1 panorama-
server=10.5.107.20 panorama-
server-2=10.5.107.21
 tplname=FINANCE_TG4
 dgname=finance_dg dns-
primary=10.5.6.6 dns-
secondary=10.5.6.7 op-command-
modes=multi-vsys,jumbo-frame
 dhcp-send-hostname=no dhcp-send-
client-id=no dhcp-accept-server-
hostname=no dhcp-accept-server-
domain=no
```

範例 init-cfg.txt（DHCP 用戶端）

```
type=dhcp-client ip-address=
 default-gateway= netmask=
 ipv6-address= ipv6-default-
gateway= hostname=Ca-FW-DC1
 panorama-server=10.5.107.20
 panorama-server-2=10.5.107.21
 tplname=FINANCE_TG4
 dgname=finance_dg dns-
primary=10.5.6.6 dns-
secondary=10.5.6.7 op-command-
modes=multi-vsys,jumbo-frame
 dhcp-send-hostname=yes dhcp-
send-client-id=yes dhcp-
accept-server-hostname=yes
 dhcp-accept-server-
domain=yes
```

下表說明 init-cfg.txt 檔案中的欄位。類型為必填；如果類型為靜態，則 IP 位址、預設閘道及網路遮罩為必填，或者 IPv6 位址和 IPv6 預設閘道為必填。

欄位	說明
type	（必填）管理 IP 位址的類型：靜態或 DHCP 用戶端。
ip-address	（需要 IPv4 靜態管理位址）IPv4 位址。如果類型為 DHCP 用戶端，則防火牆會略過此欄位。
default-gateway	（需要 IPv4 靜態管理位址）管理介面的 IPv4 預設閘道。如果類型為 DHCP 用戶端，則防火牆會略過此欄位。

©2024 Palo Alto Networks, Inc.

欄位	說明
網路遮罩	（需要 IPv4 靜態管理位址）IPv4 網路遮罩。如果類型為 DHCP 用戶端，則防火牆會略過此欄位。
ipv6-address	（需要 IPv6 靜態管理位址）管理介面的 IPv6 位址及/首碼長度。如果類型為 DHCP 用戶端，則防火牆會略過此欄位。
ipv6-default-gateway	（需要 IPv6靜態管理位址）管理介面的 IPv6 預設閘道。如果類型為 DHCP 用戶端，則防火牆會略過此欄位。
主機名稱	（選用）防火牆的主機名稱。
panorama-server	（推薦）主要 Panorama 伺服器的 IPv4 或 IPv6 位址。
panorama-server-2	（選用）次要 Panorama 伺服器的 IPv4 或 IPv6 位址。
tplname	（建議）Panorama 範本名稱。
dgname	（建議）Panorama 裝置群組名稱。
dns-primary	（選用）主要 DNS 伺服器的 IPv4 或 IPv6 位址。
dns-secondary	（選用）次要 DNS 伺服器的 IPv4 或 IPv6 位址。
vm-auth-key	（僅限 VM 系列防火牆）虛擬電腦驗證金鑰。
op-command-modes	（選用）輸入多個虛擬系統、Jumbo Frame 或兩者（僅用逗號分隔）。啟動時，啟用多個虛擬系統及 Jumbo Frame。
dhcp-send-hostname	（僅限 DHCP 用戶端類型）DHCP 伺服器確定「是」或「否」值。如果為「是」，防火牆將傳送主機名稱至 DHCP 伺服器。
dhcp-send-client-id	（僅限 DHCP 用戶端類型）DHCP 伺服器確定「是」或「否」值。如果為「是」，防火牆將傳送用戶端 ID 至 DHCP 伺服器。
dhcp-accept-server-hostname	（僅限 DHCP 用戶端類型）DHCP 伺服器確定「是」或「否」值。如果為「是」，防火牆將從 DHCP 伺服器接受其主機名稱。
dhcp-accept-server-domain	（僅限 DHCP 用戶端類型）DHCP 伺服器確定「是」或「否」值。如果為「是」，防火牆將從 DHCP 伺服器接受其 DNS 伺服器。

©2024 Palo Alto Networks, Inc.

準備 USB 快閃磁碟機以啟動防火牆

您可以使用 USB 快閃磁碟機來啟動物理防火牆。但您為此必須執行 PAN-OS 7.1.0 或更新版本映像且防火牆重設為原廠預設設定。出於安全考慮，您可以僅在出於原廠預設狀態或刪除所有私密資料時啟動防火牆。

STEP 1 | 取得序號 (S/N) 及驗證碼，以從訂購完成電子郵件中支援訂閱。

STEP 2 | 在客戶支援入口網站上註冊新防火牆的 S/N。

1. 移至 support.paloaltonetworks.com，登入並選取 **Assets**（資產） > **Devices**（裝置） > **Register New Device**（註冊新裝置） > **Register device using Serial Number or Authorization Code**（使用序號或授權碼註冊裝置）。
2. 按照下列步驟註冊防火牆。
3. 按一下 **Submit**（提交）。

STEP 3 | 在客戶支援入口網站上啟動驗證碼，可建立授權金鑰。

1. 移至 support.paloaltonetworks.com 進行登入，並在左側導覽窗格上選取 **Assets**（資產） > **Devices**（裝置）。
2. 對於您剛才註冊的每個裝置 S/N，按一下 **Action**（動作）連結（鉛筆圖示）。
3. 在 Activate Licenses（啟動授權）下方，選取 **Activate Auth-Code**（啟動授權碼）。
4. 輸入 **Authorization code**（驗證碼），然後按一下 **Agree**（同意）並 **Submit**（提交）。

STEP 4 | 在 Panorama 中新增 S/N。

完成《Panorama 管理者指南》將防火牆新增為受管理裝置中的步驟 1。

STEP 5 | 建立 init-cfg.txt 檔案。

建立 init-cfg.txt 檔案（提供啟動參數的強制檔案）。init-cfg.txt 檔案範例中介紹了這些欄位。

如果缺少 *init-cfg.txt* 檔案，啟動程序將會失敗，且防火牆將在標準啟動序列中啟動預設組態。

各欄位金鑰與值之間沒有任何空格；請勿新增空格，因為這會導致管理員伺服器解析期間發生故障。

可能有多個 init-cfg.txt 檔案，用於不同的遠端站點，並在檔案名稱前加上 S/N。例如：

0008C200105-init-cfg.txt

0008C200107-init-cfg.txt

如果不顯示加上的檔案名稱，防火牆將使用 init-cfg.txt 檔案並繼續啟動程序。

©2024 Palo Alto Networks, Inc.

STEP 6 | （選用）建立 bootstrap.xml file。

選用 bootstrap.xml 檔案是一個完整的防火牆組態，您可以從現有生產防火牆匯出該組態。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作） > **Export named configuration snapshot**（匯出具名組態快照）。
2. 選取儲存或執行中組態的 **Name**（名稱）。
3. 按一下 **OK**（確定）。
4. 將檔案重新命名為 **`bootstrap.xml`**。

STEP 7 | 從客戶支援入口網站建立並下載啟動程序包。

對於物理防火牆，啟動程序包僅需要 /license 及 /config 目錄。

使用下列一種方法來建立並下載啟動程序包：

- 使用方法 **1** 建立遠端網站特定啟動程序包（僅有一個 init-cfg.txt 檔案）。
- 使用方法 **2** 為多個網站建立一個啟動程序包。

方法 **1**

1. 在本機系統上，移至 support.paloaltonetworks.com 並登入。
2. 選取 **Assets**（資產）。
3. 選取您要啟動的防火牆 S/N。
4. 選取 **Bootstrap Container**（啟動程序容器）。
5. 按一下 **Select**（選取）。
6. 上載並 **Open**（開啟）您建立的 init-cfg.txt 檔案。
7. （選用）選取您建立的 bootstrap.xml 檔案並 **Upload Files**（上傳檔案）。

   您必須從具有相同型號及 *PAN-OS* 版本的防火牆中使用 *bootstrap.xml* 檔案。

8. 選取 **Bootstrap Container Download**（啟動程序容器下載）以將名為 **`bootstrap_<S/N>_<date>.tar.gz`** 的 tar.gz 檔案下載到您的本機系統。此啟動程序容器包括與防火牆 S/N 相關的授權金鑰。

方法 **2**

使用頂級目錄在本機系統上建立 tar.gz 檔案： /license 及 /config。包括所有授權及加入檔案名稱的所有 init-cfg.txt 檔案（帶有序號）。

您從客戶支援入口網站下載的授權金鑰檔案的授權檔案名稱帶有 S/N。PAN-OS 根據防火牆的 S/N 檢查檔案 S/N，同時執行啟動程序。

©2024 Palo Alto Networks, Inc.

STEP 8 | 使用安全複製 (SCP) 或 TFTP 將您建立的 tar.gz 檔案匯入 PAN-OS 7.1.0 或更新版本的映像防火牆。

存取 CLI 並輸入下列其中一項命令：

- **tftp import bootstrap-bundle file <path and filename> from <host IP address>**

  例如：

  tftp import bootstrap-bundle file /home/userx/bootstrap/devices/pa5000.tar.gz from 10.1.2.3

- **scp import bootstrap-bundle from <<user>@<host>:<path to file>>**

  例如：

  scp import bootstrap-bundle from userx@10.1.2.3:/home/userx/bootstrap/devices/pa200_bootstrap_bundle.tar.gz

STEP 9 | 準備 USB 快閃磁碟機。

1. 將 USB 快閃磁碟機插入您在上一步中使用的防火牆。
2. 輸入下列 CLI 操作命令，使用 tar.gz 檔案名稱取代「**pa5000.tar.gz**」。此命令將格式化 USB 快閃磁碟機，解壓縮檔案，及驗證 USB 快閃磁碟機：

   request system bootstrap-usb prepare from pa5000.tar.gz
3. 請按下 **y** 以繼續。下列訊息顯示 USB 磁碟機何時就緒：

   ```
   USB prepare completed successfully.
   ```
4. 從防火牆移除 USB 快閃磁碟機。
5. 您可以視需準備盡可能多的 USB 快閃磁碟機。

STEP 10 | 將 USB 快閃磁碟機傳送至遠端網站。

如果您使用方法 2 來建立啟動程序包，您可以使用相同的 USB 快閃磁碟機內容在多個遠端網站上啟動防火牆。您可以將內容轉譯為多個 USB 快閃磁碟機或多次使用的單一 USB 快閃磁碟機。

使用 USB 快閃磁碟機啟動防火牆

在您收到新的 Palo Alto Networks 防火牆以及載入啟動檔案的 USB 快閃磁碟機後，您可以啟動防火牆。

Microsoft Windows 與 *Apple Mac* 作業系統無法讀取 *USB* 快閃磁碟機，因為該磁碟機使用 *ext4* 檔案系統進行格式化。您必須安裝第三方軟體或使用 *Linux* 系統來讀取 *USB* 磁碟機。

STEP 1 | 防火牆必須處於原廠預設狀態或必須刪除所有私密資料。

©2024 Palo Alto Networks, Inc.

STEP 2 | 若要確保與公司總部的連線，使用乙太網路纜線將管理介面 (MGT) 連接至下列其中一項來連線防火牆：

- 上游數據機
- 交換器或路由器的連接埠
- 牆上的乙太網路插孔

STEP 3 | 將 USB 快閃磁碟機插入防火牆上的 USB 連接埠或防火牆電源。原廠預設防火牆從 USB 快閃磁碟機自行啟動。

設定好防火牆後，防火牆狀態燈從黃色變為綠色；自動提交成功。

STEP 4 | 驗證啟動程序完成。您可以在啟動期間在主控台上查看基本狀態，並且可驗證程序是否完成。

1. 如果 init-cfg.txt 檔案中包含 Panorama 值（panorama-server、tplname 及 dgname），則檢查 Panorama 受管理裝置、裝置群組及範本名稱。
2. 存取 Web 介面並選取 **Dashboard**（儀錶板） > **Widgets** > **System**（系統）或使用 CLI 操作命令 **`show system info`** 及 **`show config running`**，可驗證一般系統設定及組態。
3. 選取 **Device**（裝置） > **Licenses**（授權）或使用 CLI 操作命令 **`request license info`** 可驗證授權安裝情況。
4. 如果設定了 Panorama，可從 Panorama 管理內容版本及軟體版本。如果未設定 Panorama，則使用 Web 介面來管理內容版本及軟體版本。

©2024 Palo Alto Networks, Inc.

STEP 5 | （僅適用於 Panorama 管理的防火牆）建立裝置註冊驗證金鑰並將其新增到防火牆。

這是成功將已啟動載入的防火牆新增到 Panorama 管理的必需步驟。裝置註冊驗證金鑰的生命週期有限，不支援在 init-cfg.txt 檔案中包含裝置註冊驗證金鑰。

1. 登入 Panorama 網頁介面。
2. 選取 **Panorama** > **Device Registration Auth Key**（裝置註冊驗證金鑰）並 **Add**（新增）新的驗證金鑰。
3. 設定驗證金鑰。
   - 名稱—為驗證金鑰新增一個描述性名稱。
   - 生命週期—指定金鑰存留期，以限制您可以使用驗證金鑰裝載新防火牆的時間長度。
   - 計數—指定您可以使用驗證金鑰裝載新防火牆的次數。
   - 裝置類型—指定此驗證金鑰僅用於驗證防火牆。

     您可以選取 ***Any***（任何）以使用裝置註冊驗證金鑰來裝載防火牆、日誌收集器和 *WildFire* 設備。
   - （選用）裝置—輸入一個或多個裝置序號，以指定驗證金鑰對其有效的防火牆。
4. 按一下 **OK**（確定）。

   出現提示時，**Copy Auth Key**（複製驗證金鑰）並 **Close**（關閉）。
5. 登入防火牆網頁介面。

   您還可以登入防火牆 CLI 以新增裝置註冊驗證金鑰。

   ```
   admin> request authkey set <auth key>
   ```
6. 選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理），再編輯 [Panorama 設定]。
7. 貼上您在上一個步驟中複製的裝置註冊驗證金鑰，然後按一下 **OK**（確定）。
8. **Commit**（認可）。
9. 登入 Panorama 網頁介面並選取 **Panorama** > **Managed Devices**（受管理的裝置） > **Summary**（摘要）以驗證防火牆已 `Connected`（連接）到 Panorama

©2024 Palo Alto Networks, Inc.

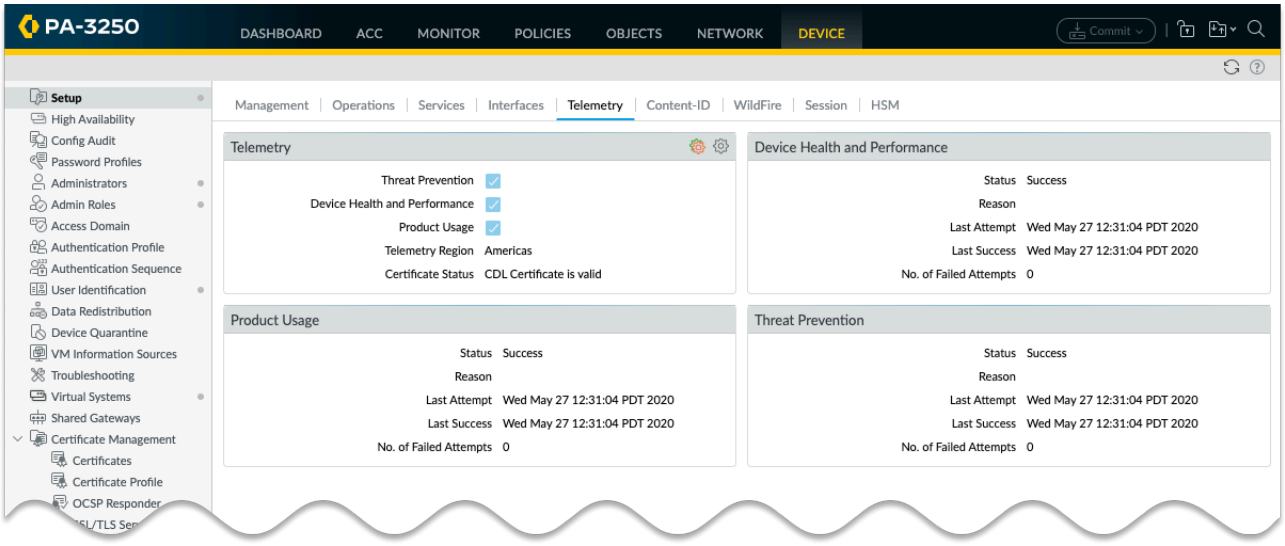
裝置遙測

裝置遙測收集有關新世代防火牆或 Panorama 的資料，並透過將資料上傳到 Cortex 資料湖與 Palo Alto Networks 共用。這些資料用於為遙測應用程式提供動力，以及共用威脅情報。

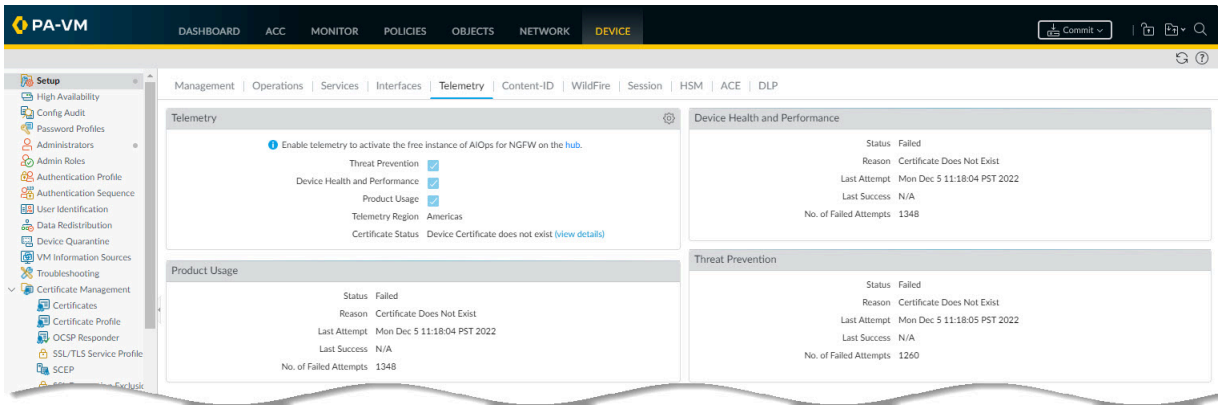
裝置遙測概要介紹

裝置遙測收集有關新世代防火牆或 Panorama 的資料，並透過將資料上傳到 Cortex 資料湖與 Palo Alto Networks 共用。此資料用於為遙測應用程式提供動力，遙測應用程式是基於雲端的應用程式，可輕鬆監控和管理新世代防火牆和 Panoramas。這些應用程式可讓您更好地瞭解裝置健康情況、效能、容量規劃和設定。透過這些應用程式，您可以從 Palo Alto Networks 提供的產品和服務中獲得最大的利益。

遙測資料還用於共用威脅情報、提供增強的入侵防禦、威脅特徵碼評估，以及改進 PAN-DB URL 篩選、基於 DNS 的命令和控制 (C2) 特徵碼、WildFire 中的惡意軟體偵測，並進一步改善 Palo Alto Networks 產品和服務。檢閱 PAN-OS 隱私權資訊資料表，瞭解有關 Palo Alto Networks 所收集資料的詳細資訊。



（PAN-OS v11.0.1 及更高的 11.0 版本）Palo Alto Networks 自動啟用裝置遙測收集。參閱 停用裝置遙測 以手動選擇退出裝置遙測收集。



遙測資料將收集在本機裝置上並儲存一段有限的時間。僅當您為資料設定目的地區域時，此資料才與 Palo Alto Networks 共用。如果您的組織擁有 Cortex 資料湖授權，那麼您只能將資料傳送到 Cortex 資料湖執行個體所在的區域。如果您的組織沒有 Cortex 資料湖授權，則您必須安裝一個裝

©2024 Palo Alto Networks, Inc.

置憑證以便共用此資料。在這種情況下，您可以選擇任何可用區域，但必須遵守所有關於隱私權和資料儲存的適用當地法律。

遙測資料將以預先定義的收集間隔進行收集並與 Palo Alto Networks 共用。您可以透過啟用/停用資料類別來控制是否收集和共用資料。您也可以監控資料收集和傳輸的當前狀態。

最後，您可以獲取防火牆出於遙測目的收集的即時資料範例。有關可與 Palo Alto Networks 共用的所有遙測指標的完整說明，包括每個指標在隱私權方面的含義，請參閱 PAN-OS 裝置遙測指標參考指南。

啟用遙測時，自動建立的使用者 ***_cliadmin*** 可能會出現在儀表板上的 ***Logged in Admins***（已登入管理員）下。建立此使用者只是為了用於遙測收集。

©2024 Palo Alto Networks, Inc.

裝置遙測收集和傳輸間隔

PAN-OS 按固定間隔收集和傳送遙測資料。收集以度量為基礎進行定義，可以是以下值之一：

- （預設）每 5 分鐘一次。
- 每小時。
- 每天。

遙測會收集到資料包。每個包是直到資料傳輸時為止收集的所有資料的彙總。這些資料包將儲存在裝置上，直到發生傳輸事件為止，傳輸事件每小時發生一次。將資料包成功傳送到 Palo Alto Networks 後，會在裝置中將其刪除。

如果將資料包傳送到 Palo Alto Networks 時發生錯誤，防火牆將等待 10 分鐘，然後重試。防火牆將繼續嘗試傳送資料包，直到傳送成功或需要儲存空間來收集新的遙測資料。

在每個常規的傳輸間隔，防火牆首先傳送為該事件排程的資料包。成功傳輸這些資料包之後，防火牆會傳送其可能從之前的傳輸事件中儲存的所有失敗資料包。

©2024 Palo Alto Networks, Inc.

管理裝置遙測

要管理裝置遙測，您可以：

- 啟用裝置遙測
- 停用裝置遙測
- 為遙測啟用服務路由
- 管理裝置遙測收集的資料
- 管理歷史裝置遙測

啟用裝置遙測

依預設，您的裝置不會與 Palo Alto Networks 共用資料。如果共用已啟用，您可以透過以下方式停止共用所有裝置遙測：**Device**（裝置） > **Setup**（設定） > **Telemetry**（遙測），取消選中 **Enable Telemetry**（啟用遙測）方塊，然後提交您的變更。

要啟用裝置遙測以便與 Palo Alto Networks 共用資料：

STEP 1 | 啟用 Cortex 資料湖。

1. 如果您的組織沒有 Cortex 資料湖授權，則安裝一個裝置憑證（如果您的裝置上尚未安裝憑證）。

   如果您的組織擁有 Cortex Data Lake 授權，確保其已啟用。
2. 確保您的網路已正確設定，以便防火牆可傳送資料至 Cortex 資料湖。

STEP 2 | 導覽至 **Device**（裝置） > **Setup**（設定） > **Telemetry**（遙測）

STEP 3 | 編輯 **Telemetry**（遙測）Widget。

STEP 4 | 在 **Telemetry Destination**（遙測目的地）中，選取您的地區。如果您的組織正在使用 Cortex 資料湖，您必須使用您的 Cortex 資料湖設定使用的地區。

STEP 5 | 按一下 **OK**（確定），然後提交您的變更。

每當防火牆將遙測檔案傳送到它的目的地時，`_cliuser` 就會顯示為已登入的管理員。

停用裝置遙測

如果您的新世代防火牆設定為與 Palo Alto Networks 共用資料，則可以透過以下方式停用此共用：

STEP 1 | 導覽至 **Device**（裝置） > **Setup**（設定） > **Telemetry**（遙測）

STEP 2 | 編輯 **Telemetry**（遙測）Widget。

STEP 3 | 取消選中 **Enable Telemetry**（啟用遙測）方塊。

©2024 Palo Alto Networks, Inc.

STEP 4 | 按一下 **OK**（確定），然後提交您的變更。

STEP 5 | 防火牆上傳資料一年後，當前儲存在 Cortex 資料湖中的所有遙測資料都會自動清除。（選用）如果您在停用遙測後不希望資料在這段時間內保留在 Cortex 資料湖中，則可以開啟支援票證並要求 Palo Alto Networks 清除您的遙測資料。

為遙測啟用服務路由

您可以為收集有關新世代防火牆或 Panorama 之資料的裝置遙測設定特定的組態設定要求。對於每個虛擬系統，您可以將服務路由設定為對輸出遙測資料使用特定介面，並透過上傳到 Cortex Data Lake 來分享資料。

STEP 1 | 選取 **Device**（裝置） > **Setup**（設定） > **Services**（服務）。

STEP 2 | 按一下 **Services Features**（服務功能）下的 **Service Route Configuration**（服務路由設定）連結。

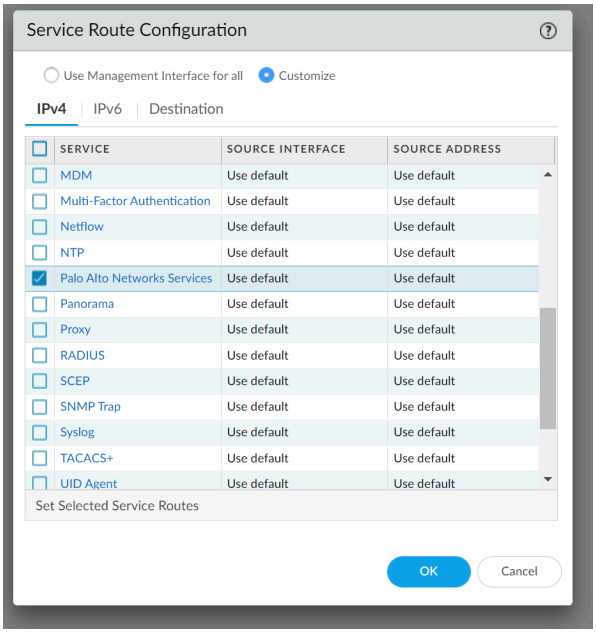
STEP 3 | 選擇 **Customize**（自訂）。

STEP 4 | 選取 **IPv4**。

STEP 5 | 選擇 **Palo Alto Networks Service**（**Palo Alto Networks** 服務）。

選擇要用作遙測介面的自訂 **Source Interface**（來源介面）。

選擇與介面關聯的自訂 **Source Address**（來源位址）。

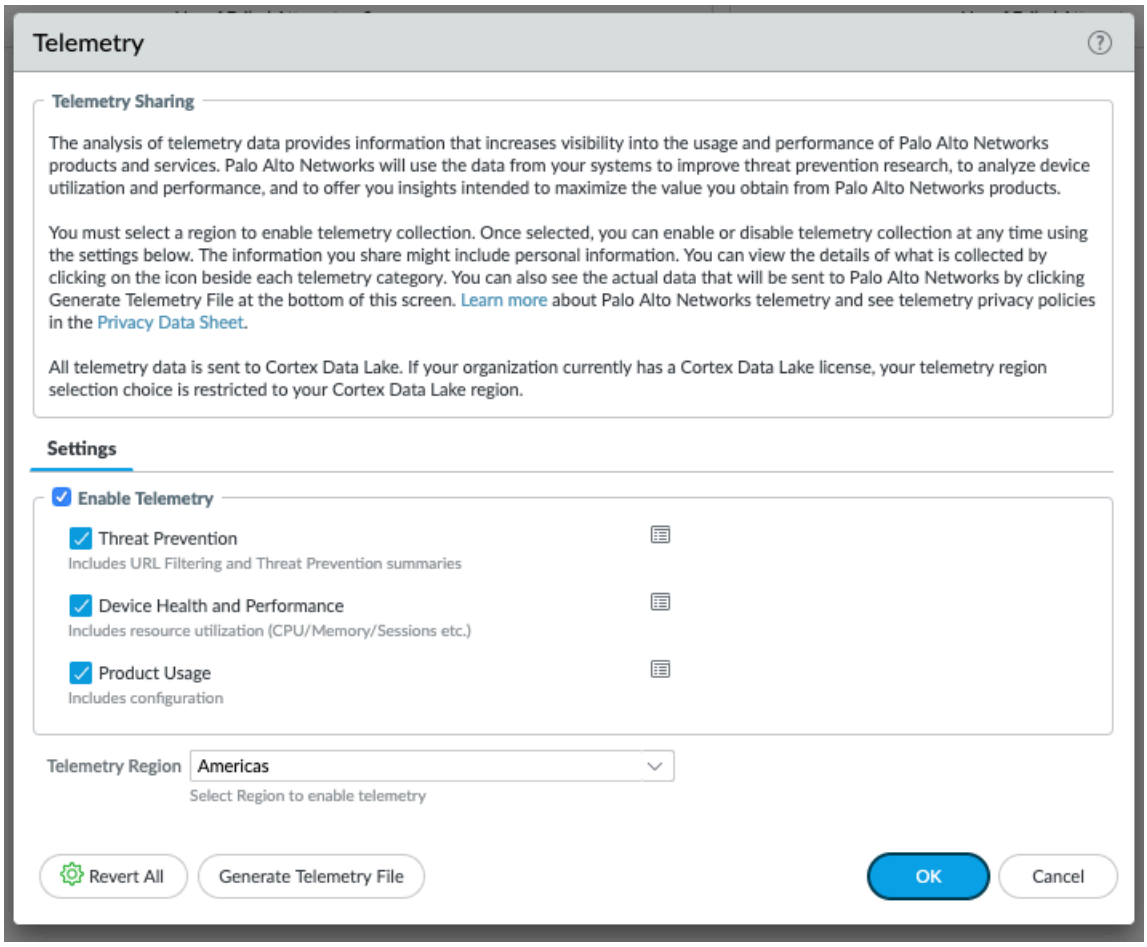


STEP 6 | **Commit**（提交）組態。

©2024 Palo Alto Networks, Inc.

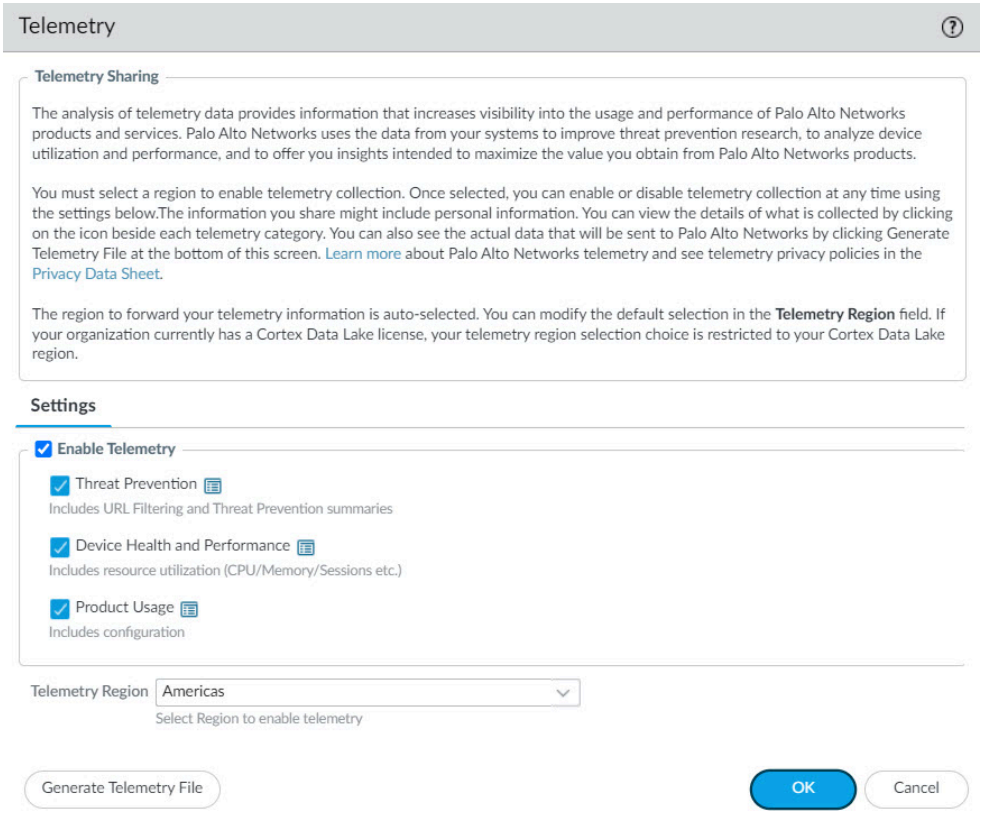
管理裝置遙測收集的資料

選取 **Device**（裝置） > **Setup**（設定） > **Telemetry**（遙測）以查看當前收集的遙測類別。要變更這些類別，請編輯遙測 Widget。取消選取您不希望防火牆收集的任何類別，按一下 **OK**（確定），然後提交變更。



（PAN-OS v11.0.1 及更高的 11.0 版本）遙測區域會自動選取。

©2024 Palo Alto Networks, Inc.



要停止共用所有裝置遙測，請取消選中 ***Enable Telemetry***（啟用遙測）方塊，然後提交您的變更。

管理歷史裝置遙測

對於 PAN-OS 11.0 版本，裝置遙測發生了重大變更。在 10.0 之前，遙測資料主要用於威脅情報目的。從 10.0 版開始，威脅情報指標在裝置收集的資料中仍然佔很大一部分，但同時還收集了涉及裝置健康情況、效能和設定的大量資料。

換句話說，PAN-OS 11.0 裝置遙測擴展了先前版本收集的資料。PAN-OS 11.0 還將遙測資料傳送到與先前版本不同的雲端位置。但是，對於執行 PAN-OS 10.0 的新世代防火牆，歷史遙測支援仍然存在。唯一的區別是 11.0 裝置遙測使用者介面無法管理此歷史資料收集。

如果您有現存的新世代防火牆，且已啟用任何歷史遙測資料類別，那麼當您升級到 PAN-OS 11.0 時，防火牆將繼續收集和共用此資訊。如果要關閉此遙測資料共用，請使用以下 CLI 命令：

```
set deviceconfig system update-schedule statistics-service
 application-reports no set deviceconfig system update-schedule
 statistics-service threat-prevention-reports no set deviceconfig
 system update-schedule statistics-service threat-prevention-
information no set deviceconfig system update-schedule statistics-
service threat-prevention-pcap no set deviceconfig system
 update-schedule statistics-service passive-dns-monitoring no set
 deviceconfig system update-schedule statistics-service url-reports
 no set deviceconfig system update-schedule statistics-service
```


©2024 Palo Alto Networks, Inc.

```
 health-performance-reports no set deviceconfig system update-
schedule statistics-service file-identification-reports no
```

如果您擁有 11.0 防火牆，且此遙測共用已關閉，但是您想與 Palo Alto Networks 共用此資料，則可以使用以下命令將其開啟：

```
set deviceconfig system update-schedule statistics-service
 application-reports yes set deviceconfig system update-schedule
 statistics-service threat-prevention-reports yes set deviceconfig
 system update-schedule statistics-service threat-prevention-
information yes set deviceconfig system update-schedule statistics-
service threat-prevention-pcap yes set deviceconfig system
 update-schedule statistics-service passive-dns-monitoring yes set
 deviceconfig system update-schedule statistics-service url-reports
 yes set deviceconfig system update-schedule statistics-service
 health-performance-reports yes set deviceconfig system update-
schedule statistics-service file-identification-reports yes
```

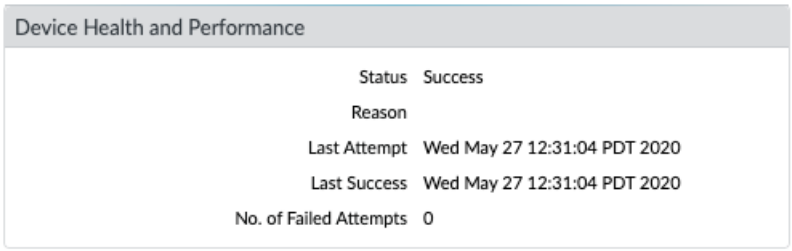
您可以使用以下 CLI 命令查看您的裝置是否正在收集和共用此歷史遙測資料：

```
show deviceconfig system update-schedule statistics-service
```


©2024 Palo Alto Networks, Inc.

監控裝置遙測

PAN-OS 顯示每個遙測類別的共用狀態。每個指標類別的 Widget 可在 **Device**（裝置） > **Setup**（設定） > **Telemetry**（遙測）中找到。



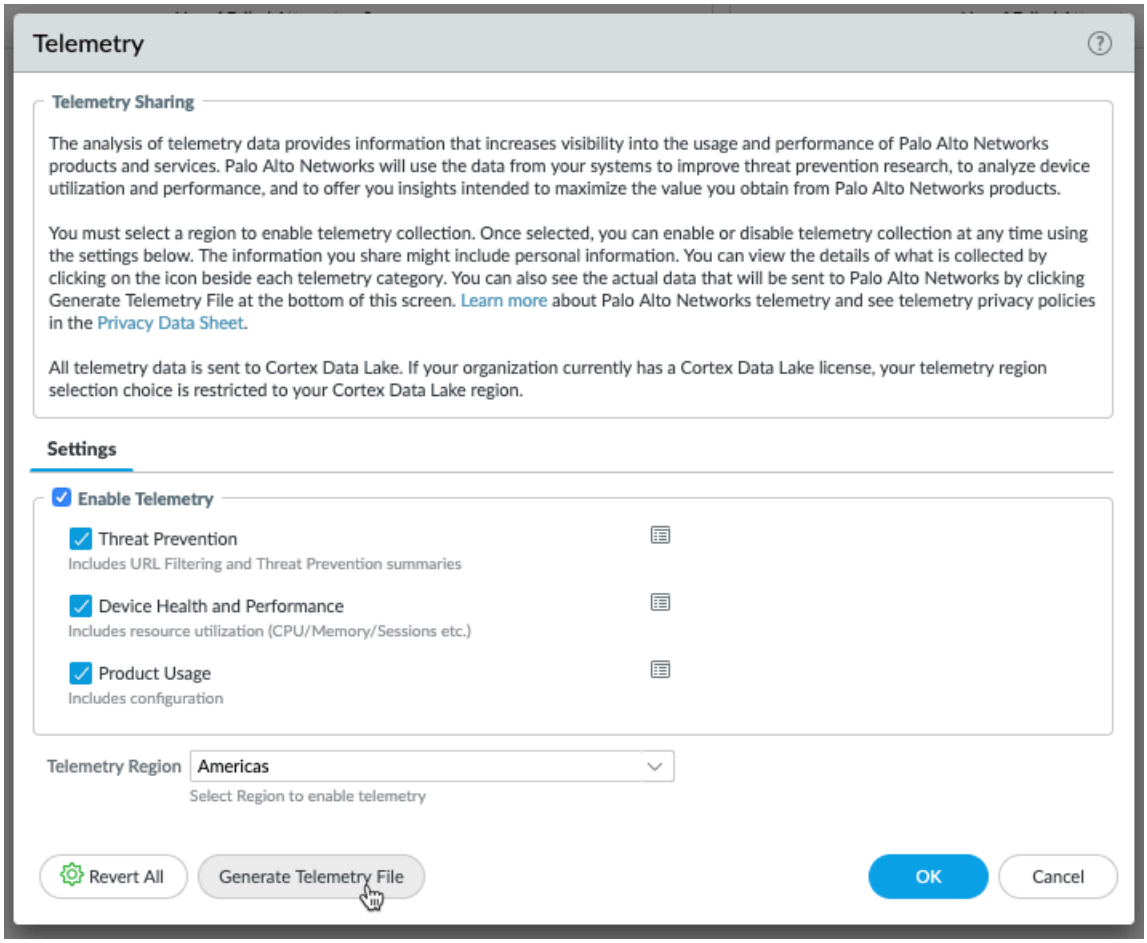
如果失敗，您的裝置將在下一個傳輸時間重新嘗試傳送。如果問題仍然存在，請檢查以確保您的裝置已正確設定為傳送資料到 Cortex 資料湖：

- 如果您的組織擁有 Cortex 資料湖授權，那麼請確保您的 Cortex 資料湖授權已啟動，且您的防火牆已設定為使用 Cortex 資料湖。
- 如果您的組織沒有 Cortex 資料湖授權，那麼請確保您已安裝裝置憑證，且您的網路已設定為允許流量進入 Cortex 資料湖。

©2024 Palo Alto Networks, Inc.

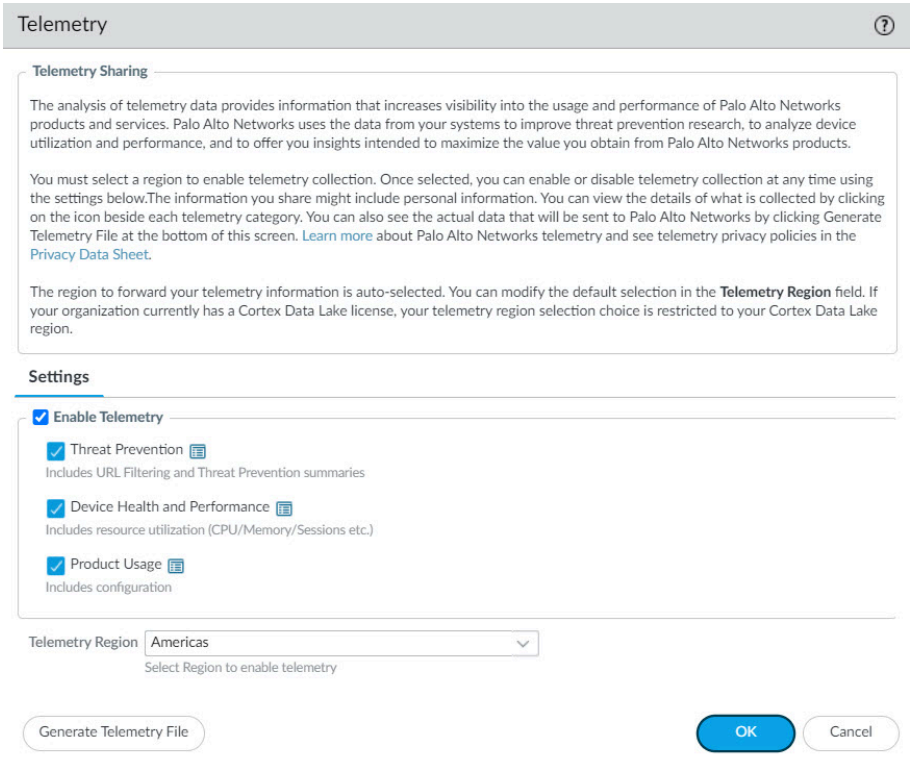
抽樣裝置遙測收集的資料

您可以下載裝置遙測收集並與 Palo Alto Networks 共用的資料的即時範例。要進行此操作，請轉至 **Device**（裝置） > **Setup**（設定） > **Telemetry**（遙測），然後編輯 **Telemetry**（遙測）Widget。然後按一下 **Generate Telemetry File**（產生遙測檔案）。



（PAN-OS v11.0.1 及更高的 11.0 版本）

©2024 Palo Alto Networks, Inc.



資料收集將需要幾分鐘，具體取決於防火牆的速度。此過程完成後，按一下 **Download Device Telemetry Data**（下載裝置遙測資料）。遙測包是壓縮的 tarball 檔案，位於您的預設瀏覽器下載目錄中。

有關裝置遙測收集並與 Palo Alto Networks 共用的每個指標的說明，請參閱 PAN-OS 裝置遙測指標參考指南。

©2024 Palo Alto Networks, Inc.

驗證

驗證是一種保護服務和應用程式的方式，透過驗證使用者身份，以確保僅有合法使用者擁有存取權。一些防火牆和 Panorama 功能需要驗證。管理員通過驗證才能存取防火牆和 Panorama 的 Web 介面、CLI 或 XML API。一般使用者透過驗證入口網站或 GlobalProtect 進行驗證，以存取各種服務和應用程式。您可以從多種嚴重服務中進行選擇，以保護您的網路並在確保流暢使用者體驗的同時，適應現有的安全性基礎結構。

如果有公開金鑰基礎結構，您可以部署憑證以啟用認證，無需使用者手動回應登入問題（請參閱憑證管理）。或者除了憑證，您還可以實作互動式驗證，要求使用者使用一種或多種方式進行驗證。以下主題介紹了如何實作、測試不同類型的交互式驗證以及進行疑難排解：

- 驗證類型
- 規劃驗證部署
- 設定多因素驗證
- 設定 SAML 驗證
- 設定 Kerberos 單一登入
- 設定 Kerberos 伺服器驗證
- 設定 TACACS+ 驗證
- 設定 RADIUS 驗證
- 設定 LDAP 驗證
- 驗證伺服器的連線逾時
- 設定本機資料庫驗證
- 設定驗證設定檔和順序
- 測試驗證伺服器連線
- 驗證原則
- 疑難排解驗證問題

驗證類型

- 外部驗證服務
- 多因素驗證
- SAML
- Kerberos
- TACACS+
- RADIUS
- LDAP
- 本機驗證

外部驗證服務

防火牆和 Panoram 可使用外部伺服器控制對 Web 介面的管理存取以及使用者通過驗證入口網站和 GlobalProtect 對服務或應用程式的存取。在這種情況下，任何不屬於防火牆或 Panorama 本機的驗證服務均被視為外部服務，無論該服務相對於網路是屬於內部（例如 Kerberos）還是外部（例如 SAML 識別提供者）。防火牆和 Panorama 可整合的伺服器類型包括多因素驗證 (MFA)、SAML、Kerberos、TACACS+、RADIUS 和 LDAP。雖然您也可以使用防火牆和 Panorama 支援的本機驗證服務，但一般優先選擇外部服務，因為它們提供：

- 在外部識別身分存放區內集中管理所有使用者帳戶的功能。所有受支援的外部服務均為使用者和管理員提供此選項。
- 帳戶授權（角色與存取網域指派）的集中管理功能。SAML、TACACS+ 和 RADIUS 支援管理員使用此選項。
- 單一登入 (SSO)，讓使用者均需驗證一次即可存取多個服務和應用程式。SAML 和 Kerberos 支援 SSO。
- 不同類型的多種驗證挑戰（因素），保護最敏感的服務和應用程式。MFA 服務支援此選項。

透過外部服務驗證需要設定伺服器設定檔，定義防火牆連線至服務的方式。您需將該伺服器設定檔指派給驗證設定檔（其中定義了為每個應用程序和使用者集合自訂的設定）。例如，您可以為存取 Web 介面的管理員設定一個驗證設定檔，為存取 GlobalProtect 入口網站的使用者設定另一個設定檔。詳細資訊，請參閱設定驗證設定檔和順序。

多因素驗證

您可以設定多因素驗證 (MFA) 來確保每個使用者在存取高度敏感服務和應用程式時，均使用多種方式（因素）進行驗證。例如，您可以強制要求使用者輸入登入密碼，再輸入手機上收到的驗證碼，然後訪客存取重要的財務文件。這種方法有助於防止攻擊者透過竊取密碼的方式存取網路中的服務和應用程式。當然，並不是每個服務和應用程式都需要同等程度的保護，對於使用者經常存取的不太敏感的服務和應用程式，則無需採用 MFA。為了適應各種安全性需求，您可以設定驗證

©2024 Palo Alto Networks, Inc.

原則規則，用於根據特定服務、應用程式和使用者觸發 MFA 或單一驗證因素（例如登入認證或憑證）。

在選擇要強制執行多少個以及哪些類型的驗證因素時，務必要瞭解原則評估會對使用者體驗造成什麼影響。在使用者要求服務或應用程式時，防火牆將首先評估驗證原則。如果使用者的要求符合啟用了 MFA 的安全性原則規則，則防火牆將顯示驗證入口網站 Web 表單，以便使用者驗證第一個因素。如果驗證成功，防火牆隨後將顯示每一個額外因素的 MFA 登入頁面。某些 MFA 服務將提示使用者從 2-4 個因素中選擇一個，當部分因素不可用時，這將很有用。如果所有因素均驗證成功，防火牆將為所請求的服務或應用程式評估安全性原則。

若要減小驗證挑戰中斷使用者工作流程的頻率，請設定第一個因素使用 Kerberos 或 SAML 單一登入 *(SSO)* 驗證。

若要為 *GlobalProtect* 實作 *MFA*，請參閱設定 GlobalProtect 以協作多因素驗證通知。

您不能在驗證順序中使用 *MFA* 驗證設定檔。

對於透過驗證原則執行的一般使用者驗證，防火牆直接與數個 MFA 平台整合（Duo v2、Okta Adaptive、PingID 以及 RSA SecurID），並透過 RADIUS 或 SAML 與所有其他 MFA 平台進行整合。對於 GlobalProtect 入口網站及閘道的遠端使用者驗證，以及 Panorama 及 PAN-OS 網頁介面的管理員驗證，防火牆僅使用 RADIUS 及 SAML 與 MFA 廠商整合。

防火牆支援下列 MFA 因素：

因素	說明
Push	端點裝置（如手機或平板電腦）將提示使用者允許或拒絕驗證。
簡訊服務 (SMS)	端點裝置上的 SMS 訊息將提示使用者允許或拒絕驗證。在某些情況下，端點裝置將提供使用者必須在 MFA 登入頁面中輸入的代碼。
語音	自動呼出的電話將提示使用者透過在手機上按鍵或在 MFA 登入頁面輸入代碼的方式進行驗證。
一次性密碼 (OTP)	端點裝置將提供自動產生的英數字元字串，使用者需在 MFA 登入頁面出入該字串，才能為單一交易或工作階段啟用驗證。

SAML

您可以使用安全性聲明標記語言 (SAML) 2.0 來驗證存取防火或 Panorama Web 介面的管理員以及存取組織內部或外部 Web 應用程式的使用者。若每個使用者要存取多個應用程式，而每一個都驗證會降低使用者的生產效率，則您可以設定 SAML 單一登入 (SSO) 來實現一次登入即可存取多個應用程式。同樣地，SAML 單一登出 (SLO) 將允許使用者登出一個工作階段即可結束多個應用程式的工作階段。SSO 適用於存取 Web 介面的管理員以及透過 GlobalProtect 或驗證入口網站存取應用程式的使用者。SLO 適用於管理員和 GlobalProtect 一般使用者，但不適用於驗證入口網

©2024 Palo Alto Networks, Inc.

站一般使用者。在防火牆上或在 Panorama 上設定 SAML 時，您可以為管理員授權指定 SAML 屬性。SAML 屬性可讓您透過目錄服務快速變更管理員的角色、存取網域以及使用者群組，這通常比在防火牆和 Panorama 上重新設定更加簡單。

管理員無法使用 *SAML* 驗證防火牆或 *Panorama* 上的 *CLI*。

您不能在驗證順序中使用 *SAML* 驗證設定檔。

SAML 驗證需要服務提供者（防火牆或 Panorama）以控制對應用應用程式的存取，還需要識別提供者 (IdP)，例如 PingFederate，以驗證使用者。當使用者要求服務或應用程式時，防火牆或 Panorama 將攔截要求，並將使用者重新導向至 IdP 進行驗證。IdP 隨後將驗證使用者，並傳回 *SAML* 聲明，指示驗證成功還是失敗。驗證入口網站一般使用者的 SAML 驗證介紹了對透過驗證入口網站存取應用程式的一般使用者的 SAML 驗證。

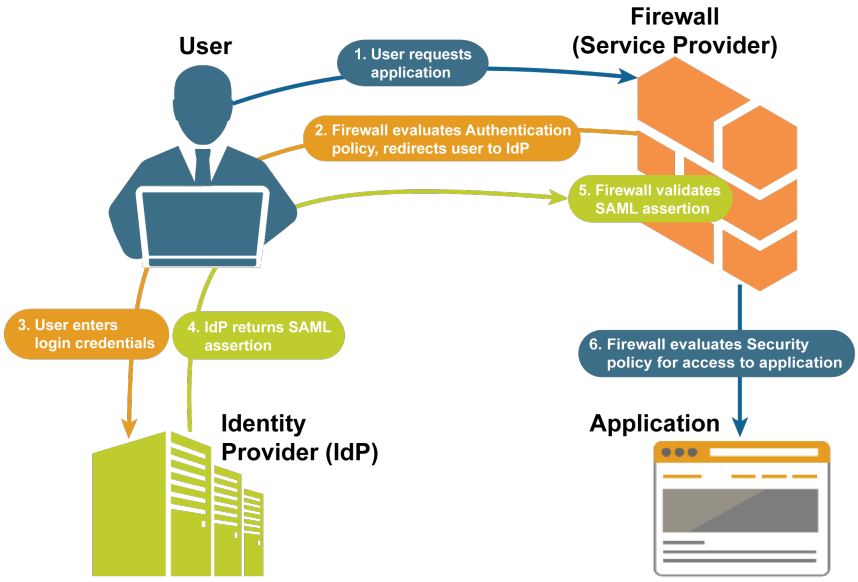


圖 **1:** 驗證入口網站一般使用者的 **SAML** 驗證

Kerberos

Kerberos 是一種驗證通訊協定，可允許在不安全網路上的各方之間使用唯一金鑰（稱為「票證」）安全地交換資訊，以識別各方。防火牆和 Panorama 支援兩種類型的 Kerberos 驗證（針對管理員和使用者）：

- **Kerberos** 伺服器驗證—Kerberos 伺服器設定檔可讓使用者原生驗證 Active Directory 網域控制站或 Kerberos V5 相容的驗證伺服器。這是一種互動式驗證方法，需要使用者輸入使用者名稱和密碼。組態設定步驟，請參閱設定 Kerberos 伺服器驗證。
- **Kerberos** 單一登入 **(SSO)**—支援 Kerberos V5 SSO 的網路會提示使用者僅針對網路的初始存取登入（例如，登入至 Microsoft Windows）。在首次登入之後，使用者便可存取網路中任何以瀏覽器為基礎的服務（例如防火牆網頁介面），而不必再次登入，直到 SSO 工作階段到期為止。（您的 Kerberos 管理員可設定 SSO 工作階段的期間。） 如果您同時啟用 Kerberos SSO 和其他

©2024 Palo Alto Networks, Inc.

外部驗證服務 (例如 TACACS+ 伺服器)，防火牆會先嘗試 SSO，且只有在其失敗時，才會回復至外部服務進行驗證。若要支援 Kerberos SSO，您的網路需要：

- Kerberos 基礎結構，包括具有 Authentication Server（驗證伺服器，AS）與 Ticket-Granting Service（票證授予服務，TGS）的 Key Distribution Center（金鑰散佈中心，KDC）。
- 將驗證使用者之防火牆或 Panorama 的 Kerberos 帳戶。必須有帳戶才能建立 Kerberos 金鑰標籤，即包含防火牆或 Panorama 主體名稱與雜湊密碼的檔案。SSO 程序需要金鑰標籤。

組態設定步驟，請參閱設定 Kerberos 單一登入。

Kerberos SSO 僅適用於 *Kerberos* 環境內部的服務和應用程式。若要為外部服務和應用程式啟用 *SSO*，需使用 SAML。

TACACS+

終端存取控制器存取控制系統 + (TACACS+) 是一個通訊協定家族，允許透過集中伺服器進行驗證和授權。TACACS+ 會加密使用者名稱和密碼，因此比 RADIUS 更安全，因為後者僅加密密碼。TACACS+ 更加可靠，因為它使用了 TCP，則 RADIUS 則使用 UDP。您可以為防火牆上的使用者或管理員以及 Panorama 上的管理員設定 TACACS+ 驗證。您也可以使用 TACACS+ 廠商特定屬性 (VSA) 來管理管理員授權。TACACS+ VSA 可讓您透過目錄服務快速變更管理員的角色、存取網域以及使用者群組，而不必在防火牆和 Panorama 上重新設定。

防火牆和 Panorama 支援下列 TACACS+ 屬性和 VSA。關於在 TACACS+ 伺服器上定義這些 VSA 的步驟，請參閱 TACACS+ 伺服器文件。

名稱	值
service	識別 Palo Alto Networks 之特定 VSA 需要此屬性。您必須將此值設定為 **`PaloAlto`**。
通訊協定	識別 Palo Alto Networks 裝置之特定 VSA 需要此屬性。您必須將此值設定為 **`firewall`**。
PaloAlto-Admin-Role	防火牆上的預設（動態）管理角色名稱或自訂管理角色名稱。
PaloAlto-Admin-Access-Domain	防火牆管理員之存取網域的名稱（在 **Device**（裝置）> **Access Domains**（存取網域）頁面中設定）。如果防火牆擁有多個虛擬系統，請定義此 VSA。
PaloAlto-Panorama-Admin-Role	Panorama 上的預設（動態）管理角色名稱或自訂管理角色名稱。

©2024 Palo Alto Networks, Inc.

名稱	值
PaloAlto-Panorama-Admin-Access-Domain	裝置群組與範本管理員之存取網域的名稱（在 **Panorama** > **Access Domains**（存取網域）頁面中設定）。
PaloAlto-User-Group	驗證設定檔允許清單中使用者群組的名稱。

RADIUS

遠端驗證撥號使用者服務 (RADIUS) 是一種受到普遍支援的網路通訊協定，提供集中驗證和授權。您可以為防火牆上的使用者或管理員以及 Panorama 上的管理員設定 RADIUS 驗證。您也可以使用 RADIUS 廠商特定屬性 (VSA) 來管理管理員授權。RADIUS VSA 可讓您透過目錄服務，快速變更管理員的角色、存取網域以及使用者群組，而不必在防火牆和 Panorama 上重新設定。您還可以設定防火牆使用 RADIUS 伺服器：

- 從 GlobalProtect 端點收集 VSA。
- 實作多因素驗證。

傳送驗證伺服器請求至 RADIUS 伺服器時，防火牆及 Panorama 將驗證設定檔名稱用作網路存取伺服器（NAS）識別碼，即使設定檔已指定給啟動驗證程序之服務（例如對 Web 介面的管理存取）的驗證順序。

防火牆和 Panorama 支援下列 RADIUS VSA。若要在 RADIUS 伺服器上定義 VSA，您必須指定廠商代碼（針對 Palo Alto Networks 防火牆或 Panorama，為 25461），以及 VSA 名稱與號碼。某些 VSA 也需要值。關於定義這些 VSA 的步驟，請參閱 RADIUS 伺服器文件。

或者，您也可以下載 Palo Alto Networks RADIUS 字典，它定義了 Palo Alto Networks 防火牆和 RADIUS 伺服器用於相互通訊的驗證屬性，並將其安裝在 RADIUS 伺服器上以將這些屬性對應到 RADIUS 二進位資料。

當您在伺服器上預先定義使用者的動態管理員角色時，使用小寫字母指定角色（例如，輸入 ***superuser***，而不是 ***SuperUser***）。

在 *Cisco Secure Access Control Server ACS (ACS)* 上設定進階廠商選項時，您必須將 ***Vendor Length Field Size***（廠商長度欄位大小）和 ***Vendor Type Field Size***（廠商類型欄位大小）設定為 ***1***。否則，驗證將失敗。

名稱	數量	值
適用於管理員帳戶管理與驗證的 VSA		
PaloAlto-Admin-Role	1	防火牆上的預設（動態）管理角色名稱或自訂管理角色名稱。

©2024 Palo Alto Networks, Inc.

名稱	數量	值
PaloAlto-Admin-Access-Domain	2	防火牆管理員之存取網域的名稱（在 **Device**（裝置）> **Access Domains**（存取網域）頁面中設定）。如果防火牆擁有多個虛擬系統，請定義此 VSA。
PaloAlto-Panorama-Admin-Role	3	Panorama 上的預設（動態）管理角色名稱或自訂管理角色名稱。
PaloAlto-Panorama-Admin-Access-Domain	4	裝置群組與範本管理員之存取網域的名稱（在 **Panorama** > **Access Domains**（存取網域）頁面中設定）。
PaloAlto-User-Group	5	驗證設定檔參考之使用者群組的名稱。
從 GlobalProtect 端點轉送至 RADIUS 伺服器的 VSA		
PaloAlto-User-Domain	6	當您定義這些 VSA 時，請勿指定值。
PaloAlto-Client-Source-IP	7	
PaloAlto-Client-OS	8	
PaloAlto-Client-Hostname	9	
PaloAlto-GlobalProtect-Client-Version	10	

LDAP

輕量型目錄存取通訊協定 (LDAP) 是用於存取資訊目錄的標準通訊協定。您可以為使用者以及防火牆和 Panorama 管理員設定 LDAP 驗證。

設定防火牆連線 LDAP 伺服器還能讓您根據使用者和使用者群組而非僅根據 IP 位址定義原則規則。相關步驟，請參閱對應使用者到群組和啟用基於使用者和基於群組的原則。

本機驗證

雖然防火牆和 Panorama 針對管理員和使用者提供了本機驗證，但是在大部分情況下都優先選擇外部驗證服務，因為後者提供了集中管理帳戶的功能。但是，您可能需要一些特殊的使用者帳戶，這些帳戶將不透過組織為普通帳戶保留的目錄伺服器管理。例如，您可以定義屬於防火牆本機的超級使用者帳戶，以便在目錄伺服器關閉時存取防火牆。在這種情況下，您可以使用本機驗證方法：

- （僅限防火牆）本機資料庫驗證—若要設定本機資料庫驗證，您需建立一個在防火牆上本機執行、包含使用者帳戶（使用者名稱和密碼或雜湊密碼）和使用者群組的資料庫。這種驗證方

©2024 Palo Alto Networks, Inc.

法適用於當您僅知道雜湊密碼而不知道純文字密碼時，重複使用現有 Unix 帳戶憑證建立使用者帳戶。由於本機資料庫驗證與驗證設定檔關聯，因此您可以採用不同使用者集合需要不同驗證設定的部署，例如 Kerberos 單一登入 (SSO) 或多因素驗證 (MFA)。（如需詳細資訊，請參閱設定驗證設定檔和順序）。對於使用驗證設定檔的管理員帳戶，不套用密碼複雜性和過期設定。這種驗證方法適用於存取防火牆（而非 Panorama）的管理員以及透過驗證入口網站或 GlobalProtect 存取服務和應用程式的使用者。

- 不使用資料庫的本機驗證—您可以設定防火牆管理帳戶或 Panorama 管理帳戶，而不建立在防火牆或 Panorama 上本機執行的使用者和使用者群組資料庫。因為這種方法不會與驗證設定檔關聯，您不能將其與 Kerberos SSO 或 MFA 結合使用。但是，這是唯一一種允許使用密碼設定檔的驗證方法，您可以將各帳戶與不同於全域設定的密碼過期設定關聯。（如需詳細資訊，請參閱定義密碼複雜性和過期設定）

©2024 Palo Alto Networks, Inc.

規劃驗證部署

在您對存取防火牆的管理員，以及透過驗證入口網站存取服務和應用程式的使用者實作驗證解決方案之前，須考量下列關鍵問題。

對於使用者和管理員，需考量：

- 如何利用現有的安全性基礎結構？通常，整合防火牆與現有基礎結構比僅為防火牆服務建立單獨的新解決方案要更快、更實惠。防火牆可整合多因素驗證、SAML、Kerberos、TACACS+、RADIUS 和 LDAP 伺服器。如果使用者存取網路外部服務和應用程式，則可使用 SAML 為防火牆整合識別提供者 (IdP)，以控制對外部和內部服務和應用程式的存取。
- 如何最佳化使用者體驗？如果您不希望使用者手動驗證並且您有公用金鑰基礎結構，則可以實作憑證驗證。另一個選項是實作 Kerberos 或 SAML 單一登入 (SSO)，以便使用者能夠在登入一個服務和應用程式後存取多個服務和應用程式。如果網路需要額外的安全性，可以將憑證驗證與互動式（挑戰-回應）驗證結合起來。
- 您是否需要一些特殊的使用者帳戶（這些帳戶將不透過組織為普通帳戶保留的目錄伺服器管理）？例如，您可以定義屬於防火牆本機的超級使用者帳戶，以便在目錄伺服器關閉時存取防火牆。您可以為這些特殊用途帳戶設定本機驗證。

  外部驗證服務一般是本機驗證的首選，因為它們提供了集中式帳戶管理功能、可靠的驗證服務，通常還提供日誌記錄和疑難排解功能。
- 使用者帳戶的使用者名稱格式是否正確？使用 SAML、Kerberos、TACACS+、RADIUS 和 LDAP 驗證要求所有使用者名稱遵循規則運算式 Linux 登入名稱規則。使用者名稱的格式必須為 **`[a-zA-Z0-9_.][a-zA-Z0-9_.-]{0,30}[a-zA-Z0-9_.$-]`**。

  這意味著：

  - 使用者名稱的第一個字元必須是大寫或小寫字母、數字 (0-9) 或者 **_**（底線）或 **.**（句點）。
  - 除了第一個和最後一個字元外，使用者名稱可以包含大寫或小寫字母字元、數字 (0-9) 和 **_**（底線）、**.**（句點）或 **-**（破折號）。除開第一個字元和最後一個字元外，最大長度為 30 個字元。
  - 使用者名稱的最後一個字元可以是大寫或小寫字母、數字 (0-9) 或者 **_**（底線）、**.**（句點）、**$** 或 **-**（破折號）。

  只有 PAN-OS 管理員才需要遵守規則運算式 Linux 登入名稱規則。GlobalProtect 和網頁驗證入口使用者不需要遵守。

對於使用者，需考量：

- 哪些服務和應用程式更為敏感？例如，您可能希望對重要財務文件實作比搜尋引擎更強的驗證措施。為保最敏感的服務和應用程式，您可以設定多因素驗證 (MFA) 來確保每個使用者在存取這些敏感服務和應用程式時，均使用多種方式（因素）進行驗證。為了適應各種安全性需求，可以設定驗證原則規則，用於根據特定服務、應用程式和使用者觸發 MFA 或單一因素驗證（例如登入認證或憑證）。其他減少攻擊面的方法包括網路分割和允許應用程式的使用者群組。

©2024 Palo Alto Networks, Inc.

對於管理員，考量：

- 是否使用外部服務集中管理所有管理帳戶的授權？透過對外部伺服器定義廠商特定屬性 (VSA)，您可以利用目錄服務快速變更管理角色指派，而不用在防火牆上重新設定。VSA 還讓您能夠對多虛擬系統防火牆的管理員指定存取網域。SAML、TACACS+ 和 RADIUS 支援外部授權。

©2024 Palo Alto Networks, Inc.

設定多因素驗證

若要使用多因素驗證 (MFA) 來保護敏感服務及應用程式，您必須設定驗證入口網站來顯示第一個驗證因素的 Web 表單並記錄驗證時間戳記。防火牆將使用這些時間戳記來評估驗證原則規則的逾時。若要啟用其他嚴重因素，可以透過 RADIUS 或廠商 API 將防火牆與 MFA 廠商整合。評估驗證原則後，防火牆將評估安全性原則，因此您必須為兩種原則類型設定規則。

Palo Alto Networks 會透過應用程式內容更新來為 MFA 廠商提供支援。這意味著如果您使用 *Panorama* 推送裝置群組組態到防火牆，則必須在防火牆上安裝相同的應用程式更新（與 *Panorama* 上的相同），以免廠商支援不相符。

僅透過驗證原則為一般使用者驗證支援 *MFA* 廠商 *API* 整合。對於 *GlobalProtect* 入口網站或閘道的遠端使用者驗證，或者 *PAN-OS* 或 *Panorama* 網頁介面的管理員驗證，僅可使用透過 *RADIUS* 或 *SAML* 支援的 *MFA* 廠商；在這些使用案例中，不支援透過廠商 *API* 提供的 *MFA* 服務。

STEP 1 | 在重新導向模式下設定驗證入口網站，以針對第一個驗證因素顯示 Web 表單、記錄驗證時間戳記以及更新使用者對應。

STEP 2 | 設定以下任何伺服器設定檔，以定義防火牆透過何種方式連線之針對第一個驗證因素驗證使用者的服務。

- 新增 RADIUS 伺服器設定檔。如果防火牆透過 RADIUS 與 MFA 廠商整合，必須執行此操作。在這種情況下，MFA 廠商將提供第一個和所有其他驗證因素，因此您可以跳過下一步（設定 MFA 伺服器設定檔）。若防火牆透過 API 整合 MFA 廠商，您仍可使用 RADIUS 伺服器作為第一個因素，但其他因素需要使用 MFA 伺服器設定檔。
- 新增 SAML IdP 伺服器設定檔。
- 新增 Kerberos 伺服器設定檔。
- 新增 TACACS+ 伺服器設定檔。
- 新增 LDAP 伺服器設定檔。

在大部分情況下，建議將外部服務作為第一個驗證因素。但是，您可以設定本機資料庫驗證，作為替代方案。

©2024 Palo Alto Networks, Inc.

STEP 3 | 新增 MFA 伺服器設定檔。

設定檔定義了防火牆將採用何種方式連線 MFA 伺服器。為第一個因素之後的每個驗證因素新增單獨的設定檔。防火牆可透過廠商 API 與這些 MFA 伺服器整合。您最多可指定三個其他因素每個 MFA 廠商會提供一個因素，但部分廠商允許使用者從多個因素中選擇一個。

1. 選取 **Device**（裝置） > **Server Profiles**（伺服器設定檔） > **Multi Factor Authentication**（多因素驗證），然後 **Add**（新增） 設定檔。
2. 輸入用來識別 MFA 伺服器的 **Name**（名稱）。
3. 選取 **Certificate Profile**（憑證設定檔），在建立與 MFA 伺服器的安全連線時，防火牆將用其驗證 MFA 伺服器憑證。
4. 選取所部署的 **MFA Vendor**（**MFA** 廠商）。
5. 設定每個廠商熟悉的 **Value**（值）。

   屬性定義了防火牆將採用何種方式連線 MFA 伺服器。每個廠商 **Type**（類型）都需要不同的屬性和值；詳細資訊，請參閱廠商文件。
6. 按一下 **OK**（確定）來儲存設定檔。

STEP 4 | 設定驗證設定檔。

此設定檔定義了使用者必須回應的驗證因素的順序。

1. 選取 **Device**（裝置） > **Authentication Profile**（驗證設定檔），然後 **Add**（新增） 設定檔。
2. 輸入用來識別驗證設定檔的 **Name**（名稱）。
3. 選取第一個驗證因素的 **Type**（類型），然後選取相應的 **Server Profile**（伺服器設定檔）。
4. 選取 **Factors**（因素）、**Enable Additional Authentication Factors**（啟用其他驗證因素），然後 **Add**（新增）您說設定的 MFA 伺服器設定檔。

   防火牆將按照所列順序，從上到下地叫用每個 MFA 服務。
5. 按一下 **OK**（確定）來儲存驗證設定檔。

STEP 5 | 設定驗證強制物件。

該物件會將每個驗證設定檔與一種驗證入口網站方法關聯。該方法決定了第一個驗證挑戰（因素）是透明還是需要使用者回應。

選取您所設定的 **Authentication Profile**（驗證設定檔），然後輸入 **Message**（訊息），提示使用者如何驗證第一個因素。此訊息顯示在驗證入口網站 Web 表單中。

如果將 ***Authentication Method***（驗證方法）設定為***browser-challenge***（瀏覽器挑戰），驗證入口網站 *Web* 表單將僅在 *Kerberos SSO* 驗證失敗時顯示。否則，將自動驗證第一個因素；使用者將不會看到 *Web* 表單。

©2024 Palo Alto Networks, Inc.

STEP 6 | 設定驗證原則規則。

該規則必須與您要保護和服務及應用程式以及必須要驗證的使用者相符。

1. 選取 **Policies**（原則） > **Authentication**（驗證），然後 **Add**（新增） 規則。
2. 輸入用來識別規則的 **Name**（名稱）。
3. 選取 **Source**（來源），**Add**（新增）特定的區域和 IP 位址，或選取 **Any**（任何）區域或 IP 位址。

   該規則將僅套用於來自於特定 IP 位址或來自於特定區域中介面的流量。
4. 選取 **User**（使用者），然後選取或 **Add**（新增）將套用該規則的來源使用者和使用者群組（預設值為 **any**（任何））。
5. 選取 **Destination**（目的地），**Add**（新增）特定的區域和 IP 位址，或選取 **Any**（任何）區域或 IP 位址。

   這些 IP 位址可以是您要控制存取的資源（例如伺服器）。
6. 選取 **Service/URL Category**（服務/**URL** 類別），然後選取或 **Add**（新增）規則將控制存取的 services and service groups（服務和服務群組）（預設值為 **service-http**）。
7. 選取或 **Add**（新增）規則將控制存取的 URL 類別（預設值為 **any**（任何））。例如，您可以建立自訂 URL 類別，指定最敏感的內部網站。
8. 選取 **Actions**（動作），然後選取您所建立的 **Authentication Enforcement**（驗證強制）物件。
9. 指定 **Timeout**（逾時）期間（以分鐘為單位，預設值為 60），在此期間內防火牆僅提示使用者驗證一次，以便於重複存取服務和應用程式。

   Timeout（逾時）是更嚴格的安全性（兩次出現驗證提示的間隔時間較短）與使用者體驗（兩次出現驗證提示的間隔時間較長）之間的權衡。存取重要系統以及敏感區域（如資料中心）時，通常需要進行更為頻繁的驗證。對於網路周邊以及那些使用者體驗對其至關重要的企業而言，進行驗證的頻率通常較低。
10. 按一下 **OK**（確定）來儲存規則。

STEP 7 | 自訂 MFA 登入頁面。

防火牆將顯示此頁面來提示使用者如何驗證 MFA 因素並指示驗證狀態（進度以及結果是成功還是失敗）。

1. 選取 **Device**（裝置） > **Response Pages**（回應頁面），然後選取 **MFA Login Page**（**MFA** 登入頁面）。
2. 選取 **Predefined**（預定義）回應頁面，然後將該頁面 **Export**（匯出）至用戶端系統。
3. 在用戶端系統上，使用 HTML 編輯器來自訂下載的回應頁面，並使用唯一檔案名稱儲存該頁面。
4. 返回防火牆上的 MFA Login Page（MFA 登入頁面）對話方塊，**Import**（匯入）自訂頁面，**Browse**（瀏覽）並選取 **Import File**（匯入檔案），選取 **Destination**（目的地）（虛擬系統或 **shared**（共用）位置），按一下 **Ok**（確定），然後按一下 **Close**（關閉）。

 ©2024 Palo Alto Networks, Inc.

STEP 8 | 設定安全性原則規則，允許使用者存取需要驗證的服務及應用程式。

1. 建立安全性原則規則。
2. **Commit**（提交）您的變更。

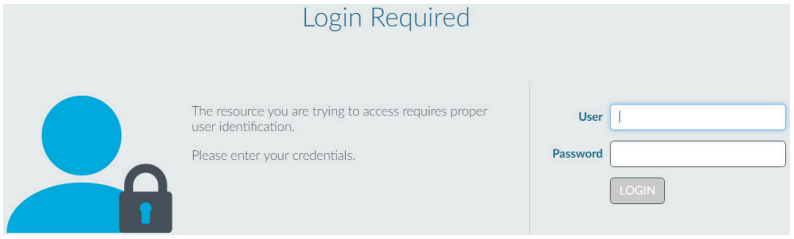
防火牆上的自動關聯引擎將使用多個關聯物件偵測網路上可能指示與 *MFA* 相關之認證濫用的事件。若要檢視這些惡事件，可選取 ***Monitor***（監控） > ***Automated Correlation Engine***（自動關聯引擎） > ***Correlated Events***（關聯事件）。

©2024 Palo Alto Networks, Inc.

STEP 9 | 確認防火牆是否已執行 MFA。

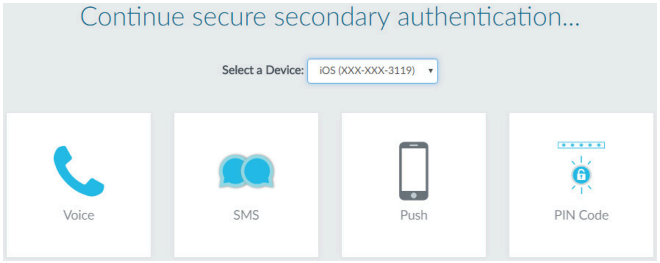
1. 以您在驗證規則中指定的一個來源使用者的身分登入網路。
2. 要求與規則中指定的一個服務或應用程式相符的服務或應用程式。

   防火牆將顯示第一個驗證因素的驗證入口網站 Web 表單。頁面中包含了您在驗證強制物件中輸入的訊息。例如：



3. 輸入第一個驗證挑戰的使用者認證。

   防火牆隨後將顯示下一個驗證因素的 MFA 登入頁面。例如，MFA 服務可能會提示您選取語音、簡訊、推送或 PIN 碼 (OTP) 驗證方法。如果您選擇推送，手機上會提示您認可驗證。



4. 驗證下一個因素。

   防火牆將顯示提示驗證成功或失敗的訊息。如果驗證成功，防火牆隨後將顯示下一個驗證因素的 MFA 登入頁面（若有）。

   為每個 MFA 因素重複此步驟。驗證所有因素後，防火牆將評估安全性原則，以確定是否允許存取服務或應用程式。
5. 結束您所存取之服務或應用程式的工作階段。
6. 對相同的服務或應用程式啟動新工作階段。務必在您於驗證規則中設定的 **Timeout**（逾時）期間內執行此步驟。

   防火牆將允許存取，無需重新驗證。
7. 等待 **Timeout**（逾時）期間過期，然後要求相同的服務或引用程式。

   防火牆將提示您重新驗證。

在 RSA SecurID 與防火牆之間設定 MFA

憑藉多因素驗證，您可透過使用多個因素驗證使用者的識別資訊，再允許其存取網路資源，來保護公司資產。若要在防火牆與 RSA SecurID Access 雲端驗證服務之間啟用多因素驗證 (MFA)，必須

©2024 Palo Alto Networks, Inc.

先設定 RSA SecurID 服務，從而能夠獲取所需詳細資訊，來設定防火牆使用多個因素驗證使用者。在 RSA SecurID Access 主控台上執行所需設定後，可將防火牆設定為整合 RSA SecurID。

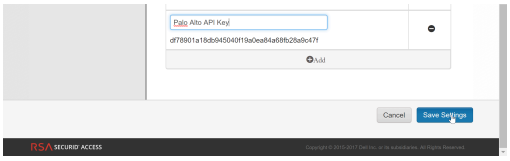
Palo Alto Networks 新一代防火牆可與 *RSA SecurID Access* 雲端驗證服務整合。*MFA API* 與 *RSA SecurID* 的整合僅受雲端型服務支援，並在第二個因素使用廠商特定 *API* 時，不支援對內部部署的驗證管理程式進行雙因素驗證。此整合所需的最低內容版本為 *752* 與 *PAN-OS 8.0.2*。

- 獲取 RSA SecurID Access 雲端驗證服務詳細資訊
- 設定防火牆與 RSA SecurID 執行 MFA

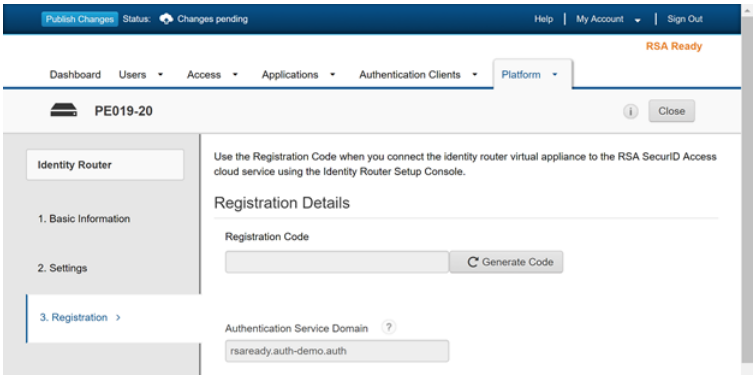
獲取 RSA SecurID Access 雲端驗證服務詳細資訊

為安全傳送進出防火牆與 RSA SecurID Access 雲端驗證服務的使用者驗證請求，必須先移至 RSA SecurID Access 主控台並設定 RSA 存取 ID、驗證服務 URL 以及用戶端 API 金鑰，防火牆需獲取此類資訊來驗證服務並與服務互動。此外，防火牆還需獲取存取原則 ID，原則使用「RSA 核准」或「RSA 權杖代碼」驗證方法來驗證識別來源。

產生 **RSA SecurID API** 金鑰—登入 RSA SecurID Access 主控台，並選取 **My Account**（我的帳戶）> **Company Settings**（公司設定）> **Authentication API Keys**（驗證 **API** 金鑰）。**Add**（新增）新金鑰，然後 **Save Settings**（儲存設定）並 **Publish Changes**（發佈變更）。

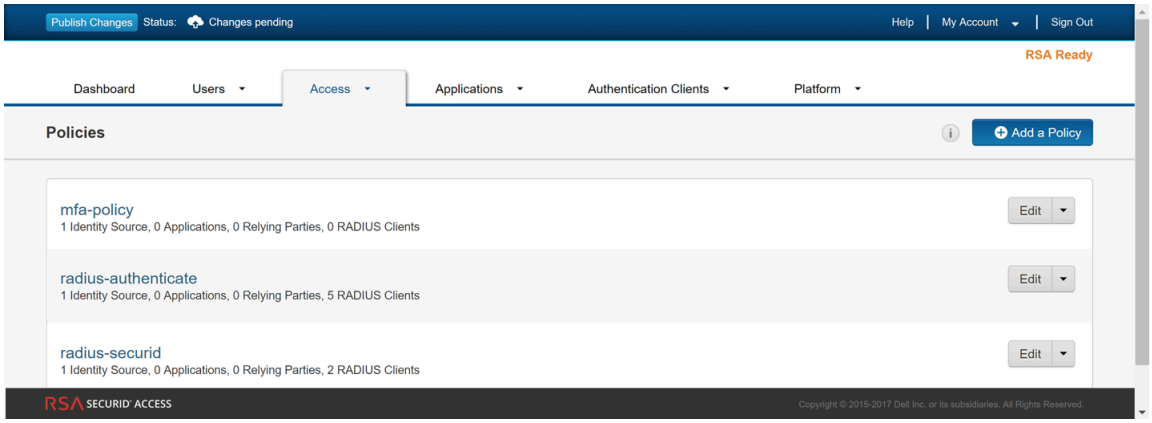


獲取防火牆必須連線的 **RSA SecurID Access** 端點 **API**（驗證服務網域）—選取 **Platform**（平台）> **Identity Routers**（識別路由器），選取要 **Edit**（編輯）的 Identity Router（識別路由器），並記下 **Authentication Service Domain**（驗證服務網域）。在此範例中，它為 https://rsaready.auth-demo.auth。



©2024 Palo Alto Networks, Inc.

獲取存取原則 **ID**—選取 **Access**（存取） > **Policies**（原則），並記下存取原則的名稱，該原則允許防火牆充當 RSA SecurID 服務的驗證用戶端。原則必須設定為僅使用「RSA 核准」或「RSA 權杖代碼」驗證方法。



設定防火牆與 RSA SecurID 執行 MFA

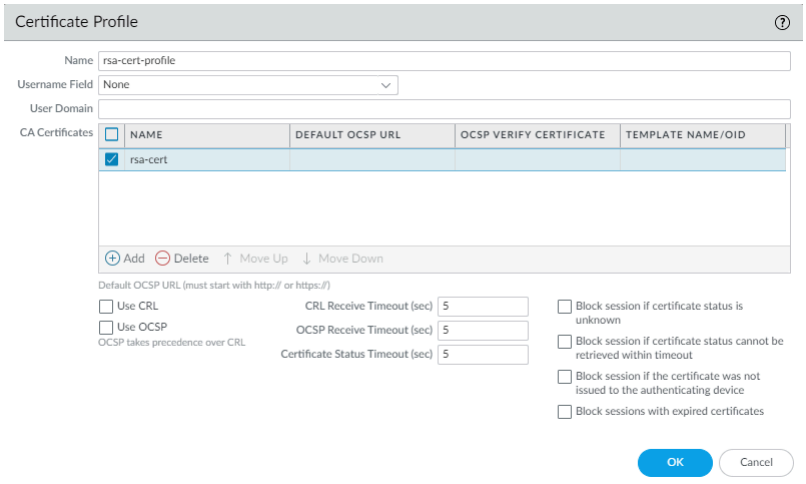
在您獲取 RSA SecurID Access 雲端驗證服務詳細資訊後，可將防火牆設定為提示使用者提供 RSA SecurID 權杖（若已叫用 MFA）。

STEP 1 | 將防火牆設定為信任 RSA SecurID Access 端點 API 提供的 SSL 憑證。

1. 匯出 RSA SecurID Access 端點提供的 SSL 憑證並將其匯入防火牆。

   若要在防火牆與 RSA SecurID Access 端點 API 之間啟用信任，必須匯入自我簽署的憑證或者用於簽署憑證的 CA 憑證。

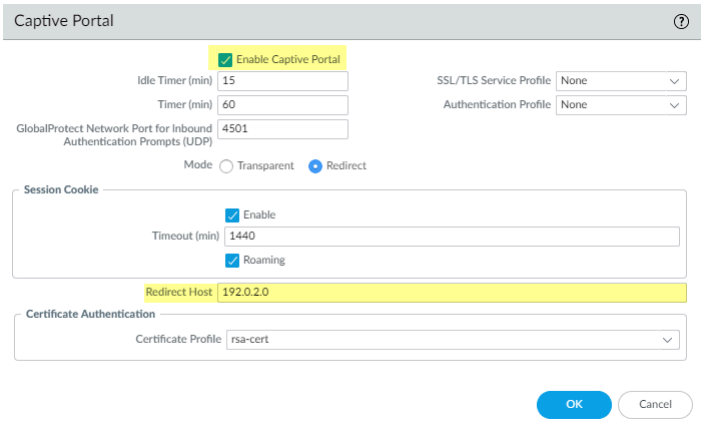
2. 設定憑證設定檔（**Device**（裝置） > **Certificate Management**（憑證管理） > **Certificate Profile**（憑證設定檔），並按一下 **Add**（新增））。



STEP 2 | 在 Redirect（重新導向）模式中設定驗證入口網站（**Device**（裝置） > **User Identification**（使用者識別） > **Authentication Portal Settings**（驗證入口網站設定）），以顯示驗證 RSA SecureID 的 Web 表單。確保將 Redirect Host（重新導向主機）指定為 IP 位址或主機名稱（在

©2024 Palo Alto Networks, Inc.

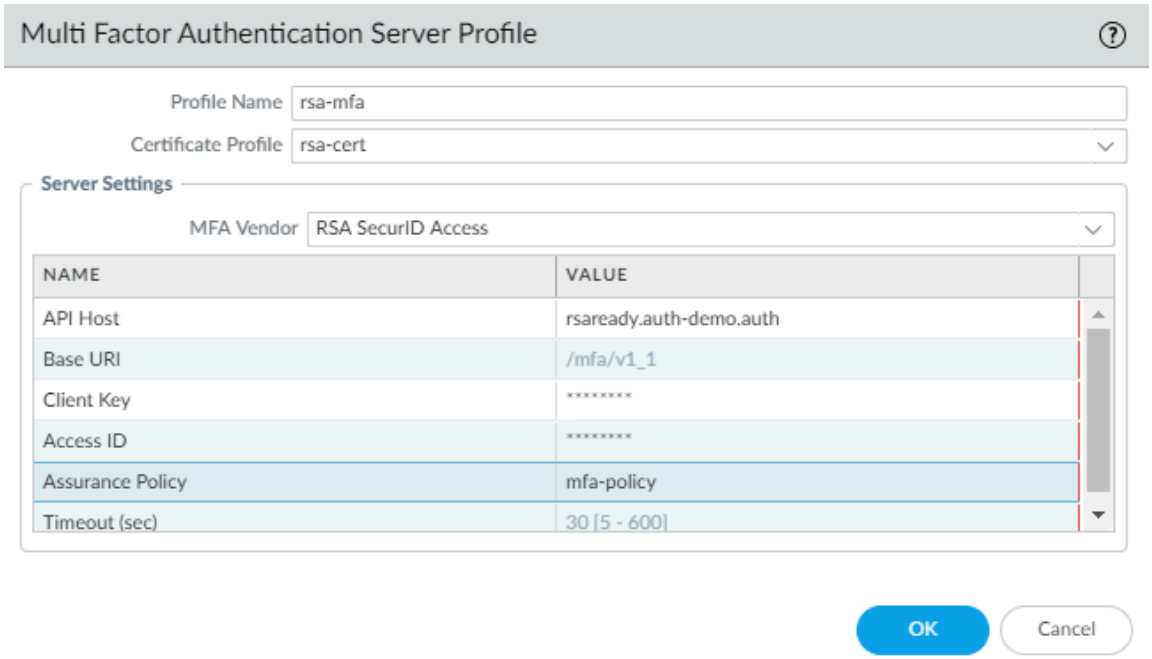
其名稱中沒有句點），它會在防火牆上解析為 Web 要求將被重新導向到的 Layer 3 介面的 IP 位址。



©2024 Palo Alto Networks, Inc.

STEP 3 | 設定多因素驗證伺服器設定檔，以指定防火牆必須以何種方式連線 RSA SecurID 雲端服務（**Device**（裝置） > **Server Profiles**（伺服器設定檔） > **Multi Factor Authentication**（多因素驗證），並按一下 **Add**（新增））。

1. 輸入用來識別 MFA 伺服器設定檔的 **Name**（名稱）。
2. 選取您之前建立的 **Certificate Profile**（憑證設定檔），在此範例中為 rsa-cert-profile。與 RSA SecurID 雲端服務建立安全連線後，防火牆將使用此憑證。
3. 在 **MFA Vendor**（**MFA** 廠商）下拉式清單中，選取 **RSA SecurID Access**。
4. 為在獲取 RSA SecurID Access 雲端驗證服務詳細資訊中所看到的每個屬性設定 **Value**（值）：
   - **API Host**（**API** 主機）—輸入防火牆必須連線的 RSA SecurID Access API 端點的主機名稱或 IP 位址，在此範例中為 rsaready.auth-demo.auth。
   - **Base URI**（基底 **URI**） —請勿修改預設值 (/mfa/v1_1)
   - **Client Key**（用戶端金鑰）—輸入 RSA SecurID 用戶端金鑰。
   - **Access ID**（存取 **ID**）—輸入 RSA SecurID 存取 ID。
   - **Assurance Policy**（保證原則）—輸入 RSA SecurID Access 原則名稱，在此範例中為 mfa-policy。
   - **Timeout**（逾時）—預設值是 30 秒。



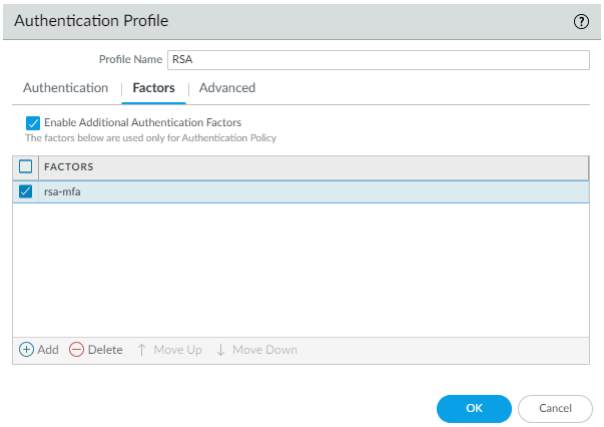
5. 儲存設定檔。

©2024 Palo Alto Networks, Inc.

STEP 4 | 設定驗證設定檔（**Device**（裝置） > **Authentication Profile**（驗證設定檔） 並按一下 **Add**（新增））。

此設定檔定義了使用者必須回應的驗證因素的順序。

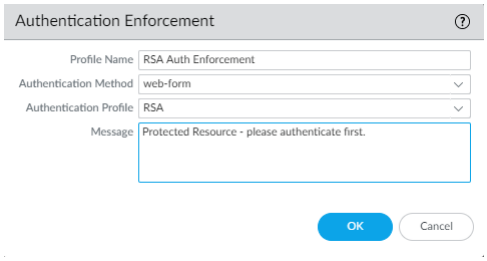
1. 選取第一個驗證因素的 **Type**（類型），然後選取相應的 **Server Profile**（伺服器設定檔）。
2. 選取 **Factors**（因素）、**Enable Additional Authentication Factors**（啟用其他驗證因素），然後 **Add**（新增）您先前在此範例中建立的 rsa-mfa 伺服器設定檔。



3. 按一下 **OK**（確定）來儲存驗證設定檔。

STEP 5 | 設定驗證強制物件。(**Objects**（物件） > **Authentication**（驗證） 並按一下 **Add**（新增））。

確保選取您剛剛在此範例中定義的稱為 RSA 的驗證設定檔。

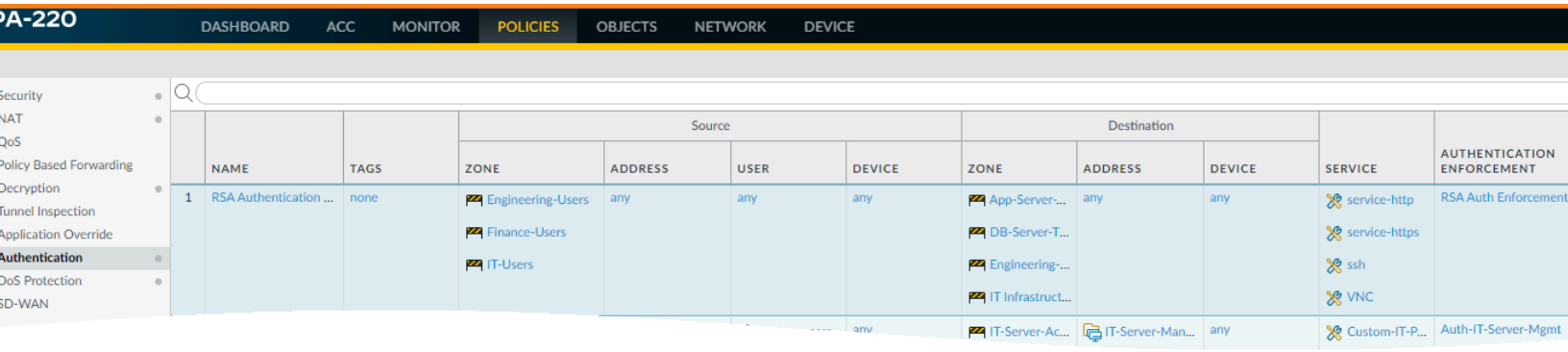


STEP 6 | 設定驗證原則規則。（**Policies**（原則） > **Authentication**（驗證），並按一下 **Add**（新增））

您的驗證原則規則必須與要保護的服務與應用程式相符，指定必須驗證的使用者，並包含會觸發驗證設定檔的驗證強制物件。在此範例中，RSA SecurID Access 使用稱作 RSA Auth Enforcement（RSA 驗證強制）的驗證強制物件，來驗證所有存取 HTTP、HTTPS、SSH 以及

©2024 Palo Alto Networks, Inc.

VNC 流量的使用者（在 **Actions**（動作）中，選取 **Authentication Enforcement**（驗證強制）物件）。



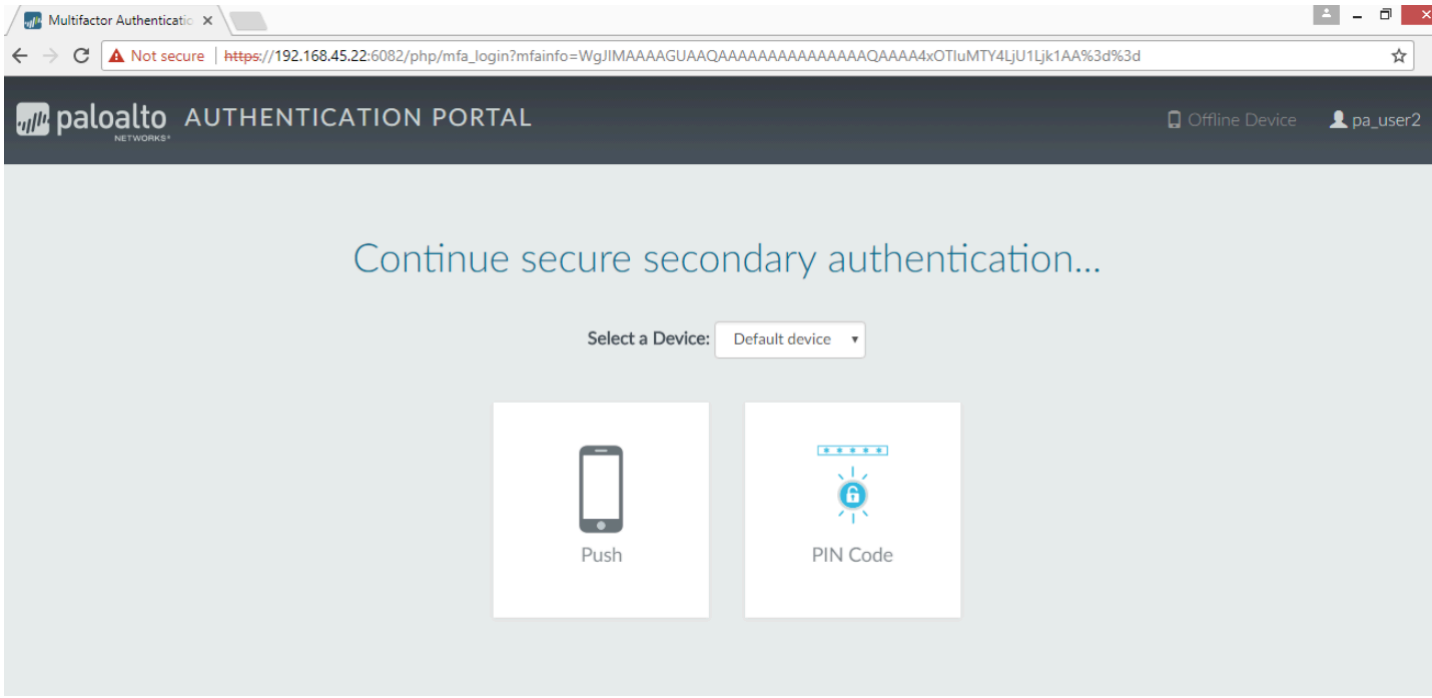
STEP 7 | 在防火牆中 **Commit**（提交）您的變更。

 ©2024 Palo Alto Networks, Inc.

STEP 8 | 確認透過 RSA SecurID 使用您已啟用的「推送」或「PIN 碼」驗證方法保護您網路中的使用者。

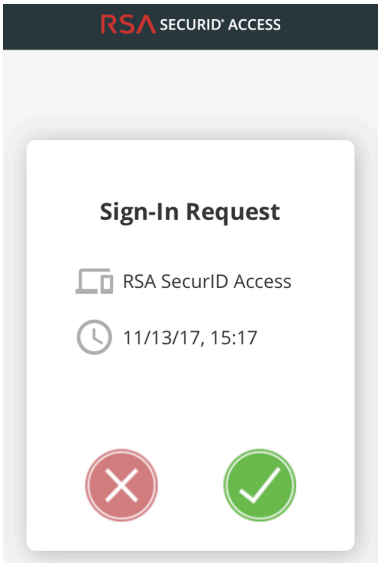
1. 推送驗證

   1. 要求網路中的使用者啟動網頁瀏覽器並存取網站。應該會顯示包含您先前定義的「重新導向主機」IP 位址或主機名稱的驗證入口網站頁面。
   2. 確認使用者輸入首個驗證因素的認證，然後繼續移至第二個驗證因素，並選取 **Push**（推送）。



   3. 查看使用者行動裝置上的 RSA SecurID Access 應用程式是否出現 **Sign-In request**（登入請求）。
   4. 要求使用者 **Accept**（接受）行動裝置上的 Sign-In Request（登入請求），並等待數秒，等待防火牆接收成功驗證的通知。使用者應該能夠存取所要求的網站。

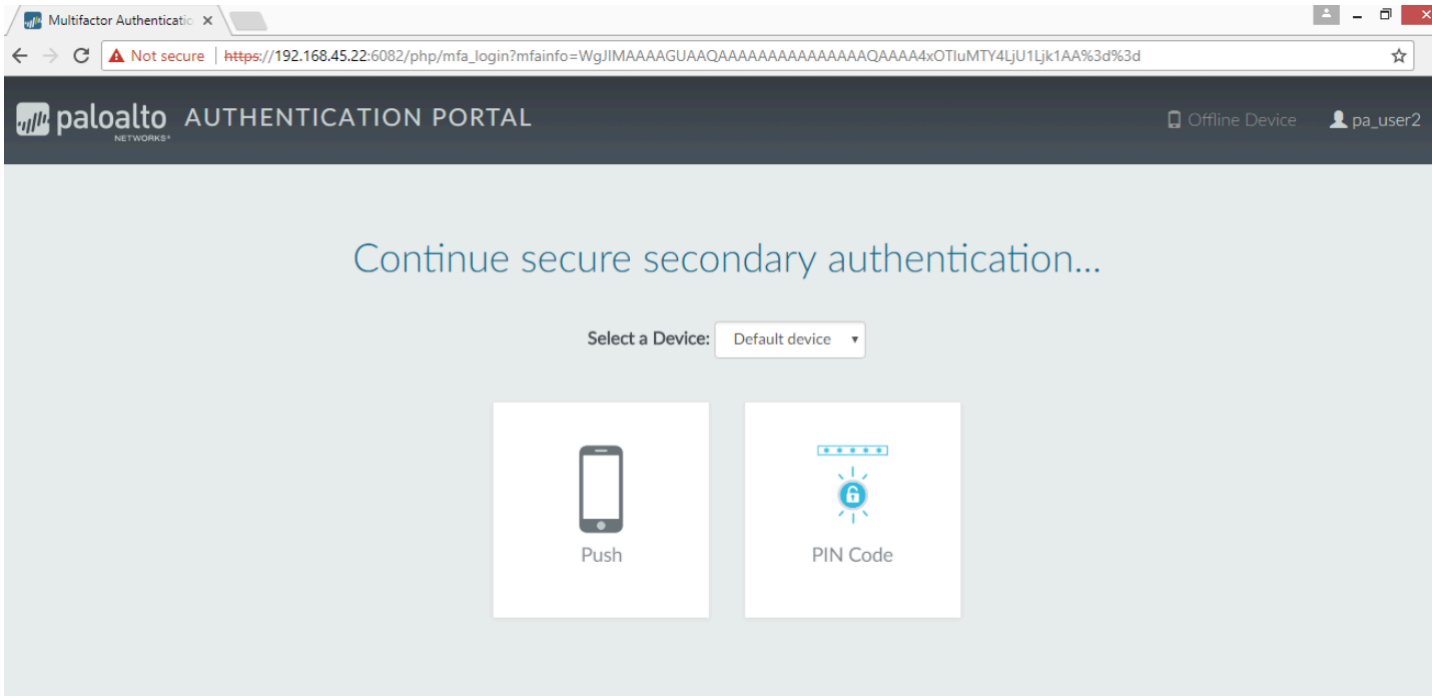
©2024 Palo Alto Networks, Inc.



若要測試驗證故障，在行動裝置上 ***Decline***（拒絕）登入請求。

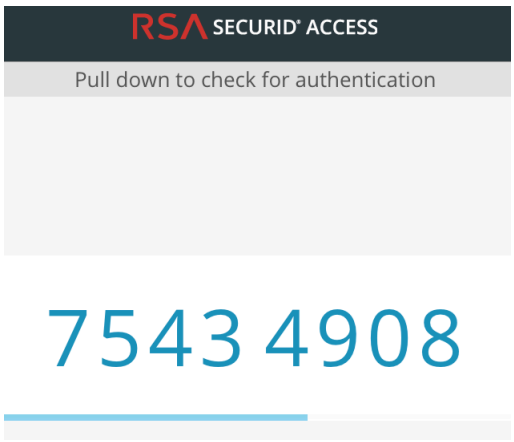
2. **PIN** 碼驗證

   1. 要求網路中的使用者啟動網頁瀏覽器並存取網站。應該會顯示包含您先前定義的「重新導向主機」IP 位址或主機名稱的驗證入口網站頁面。
   2. 確認使用者輸入首個驗證因素的認證，然後繼續移至第二個驗證因素，並選取 **PIN Code**（**PIN** 碼）。



   3. 查看使用者行動裝置上的 RSA SecurID Access 應用程式中是否顯示 **PIN Code**（**PIN** 碼）。

©2024 Palo Alto Networks, Inc.



4. 要求使用者將該 PIN 碼複製到網頁瀏覽器的 **Enter the PIN...**（輸入 **PIN...**）提示中，並按一下 **Submit**（提交）。等待數秒，等待防火牆接收成功驗證的通知。使用者此時應該能夠存取所請求的網站。

在 Okta 與防火牆之間設定 MFA

憑藉多因素驗證，您可使用多個因素先確認使用者的身分，再允許其存取網路資源，從而保護公司資產。

若要在防火牆與 Okta 身分管理服務之間啟用多因素驗證 (MFA)：

- 設定 Okta
- 設定防火牆與 Okta 進行整合
- 透過 Okta 驗證 MFA

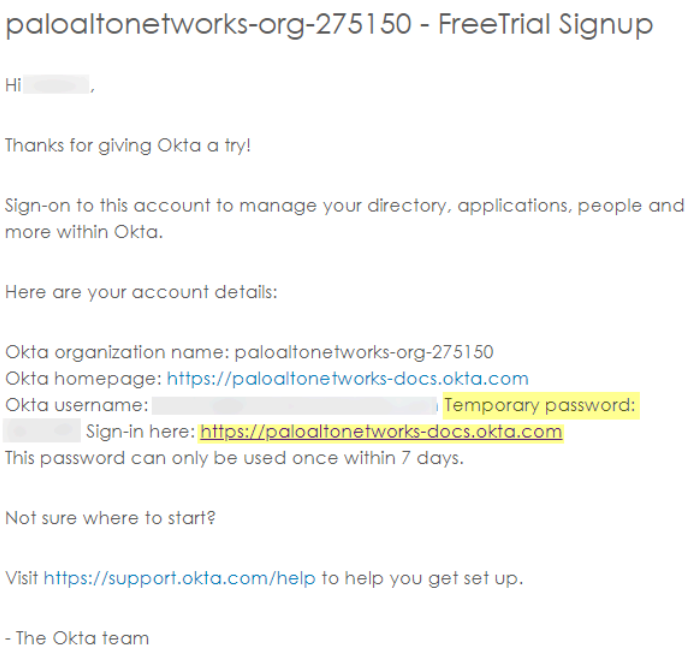
設定 **Okta**

登入 Okta Admin Portal（Okta 管理員入口網站）以建立使用者帳戶，定義 Okta MFA 原則，並獲取透過防火牆上的 Okta 設定 MFA 所需的權杖資訊。

©2024 Palo Alto Networks, Inc.

STEP 1 | 建立 Okta 管理員使用者帳戶。

1. 提交您的電子郵件地址與名稱，然後按一下 **Get Started**（開始使用）。
2. 按一下確認電子郵件中的連結，然後使用隨附的臨時密碼登入 Okta Admin Portal（Okta 管理員入口網站）。



paloaltonetworks-org-275150 - FreeTrial Signup

Hi [redacted],

Thanks for giving Okta a try!

Sign-on to this account to manage your directory, applications, people and more within Okta.

Here are your account details:

Okta organization name: paloaltonetworks-org-275150
Okta homepage: https://paloaltonetworks-docs.okta.com
Okta username: [redacted] Temporary password: [redacted]
Sign-in here: https://paloaltonetworks-docs.okta.com
This password can only be used once within 7 days.

Not sure where to start?

Visit https://support.okta.com/help to help you get set up.

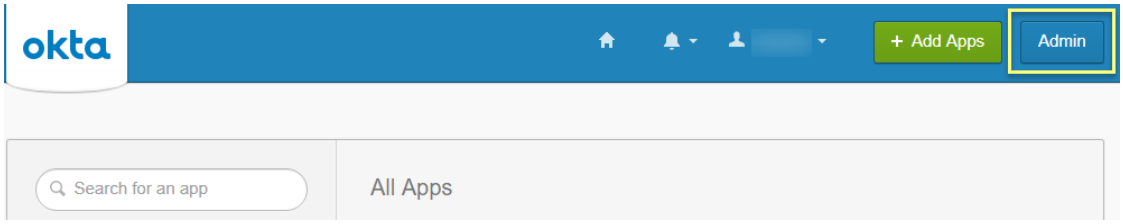
- The Okta team

3. 建立一個新密碼，其中至少包含 8 個字元，一個小寫字母，一個大寫字母，一個數字，並且不包含使用者名稱的任何部分。
4. 選取密碼提醒問題並輸入答案。
5. 選取安全性影像，然後 **Create My Account**（建立我的帳戶）。

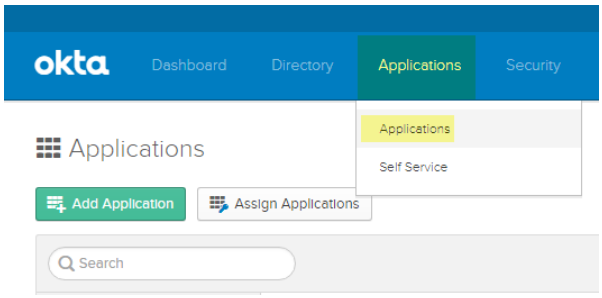
©2024 Palo Alto Networks, Inc.

STEP 2 | 設定 Okta 服務。

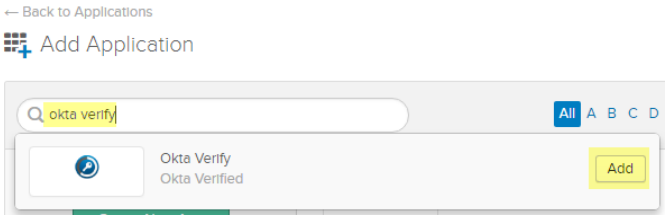
如果您已登入並且未重新導向至 *Okta Admin Portal*（*Okta* 管理員入口網站），請選取右上角 ***Admin***（管理員）。



1. 在 Okta 儀表板中，使用 Okta 管理員認證登入，然後選取 **Applications**（應用程式） > **Applications**（應用程式）。



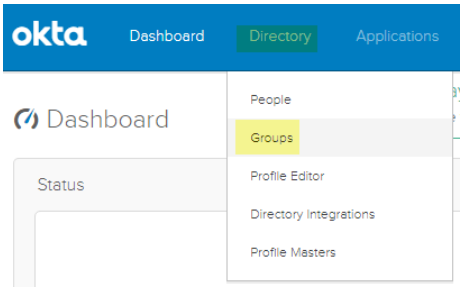
2. 選取 **Add Application**（新增應用程式）。
3. 搜尋 **`Okta Verify`**。
4. 選取 **Add**（新增），然後 **Done**（完成）。



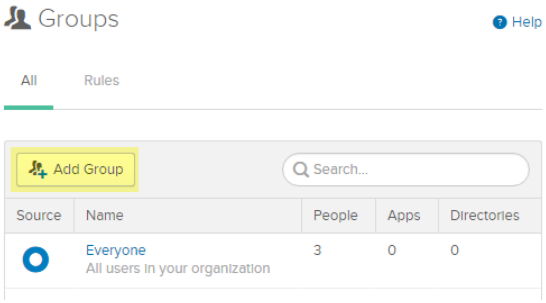
 ©2024 Palo Alto Networks, Inc.

STEP 3 | 建立一個或多個使用者群組以對使用者進行分類（例如，按裝置、按原則或按部門分類）並指派 Okta Verify 應用程式。

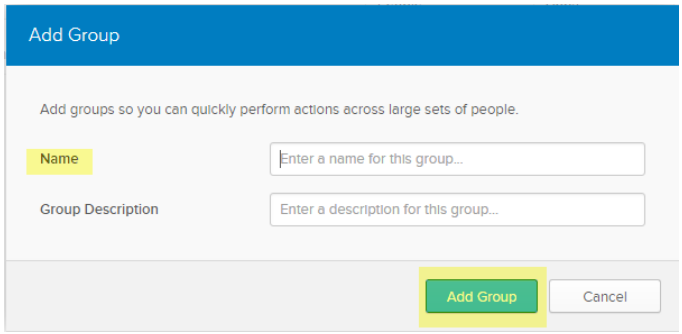
1. 選取 **Directory**（目錄） > **Groups**（群組) 。



2. 按一下 **Add Group**（新增群組）。



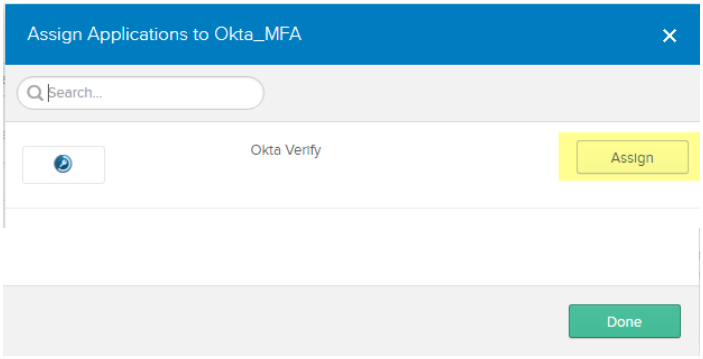
3. 輸入群組 **Name**（名稱），選擇性輸入 **Group Description**（群組說明），然後 **Add Group**（新增群組）。



預設群組每人包含在設定 Okta 的第一步中為貴組織設定的所有使用者。

4. 選取您建立的群組，然後選取 **Manage Apps**（管理應用程式）。
5. **Assign**（指派）您在步驟 2 中新增的 Okta Verify 應用程式。

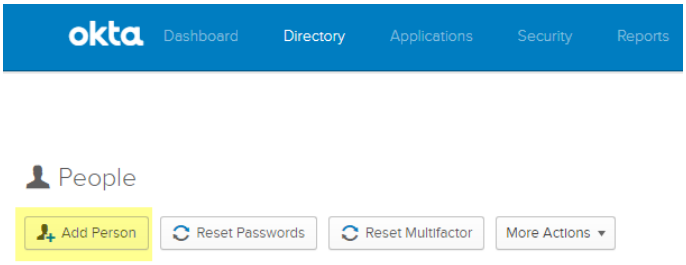
©2024 Palo Alto Networks, Inc.



6. **Assigned**（指派）應用程式之後，按一下 **Done**（完成）。
7. 對將使用 Okta Verify 應用程式進行 MFA 的所有群組重複此過程。

STEP 4 | 新增使用者並將其指派至群組。

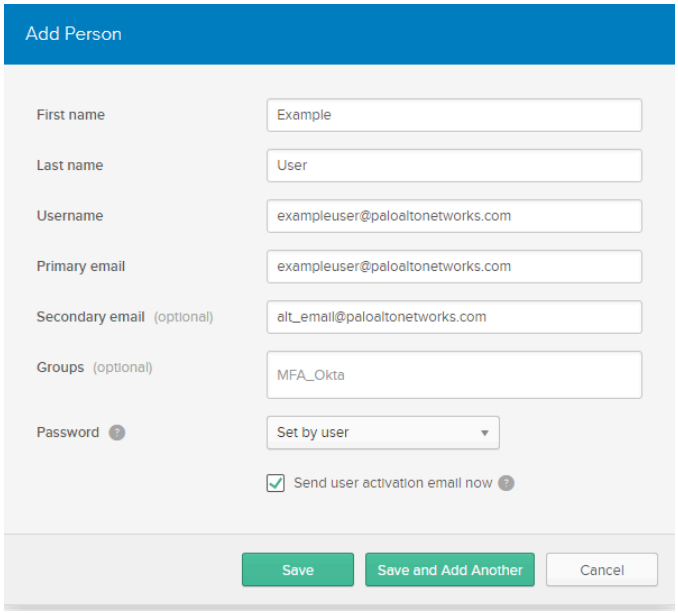
1. 在 Okta 儀表板中，選取 **Directory**（目錄） > **People**（人員） > **Add Person**（新增人員）。



2. 輸入使用者的 **First Name**（名字）、**Last Name**（姓氏）以及 **Username**（使用者名稱）。使用者名稱必須與自動填入的 **Primary email**（主要電子郵件）及防火牆上輸入的

 ©2024 Palo Alto Networks, Inc.

使用者名稱相符。您也可選擇為使用者輸入替代電子郵件地址作為 **Secondary Email**（次要電子郵件）。



3. 輸入要與此使用者關聯之一個或多個 **Groups**（群組）的名稱。開始鍵入時，群組名稱會自動填入。
4. 核取 **Send user activation email now**（立即傳送使用者啟用電子郵件），然後 **Save**（儲存）以新增單一使用者 或 **Save and Add Another**（儲存並新增另一使用者）以繼續新增使用者。

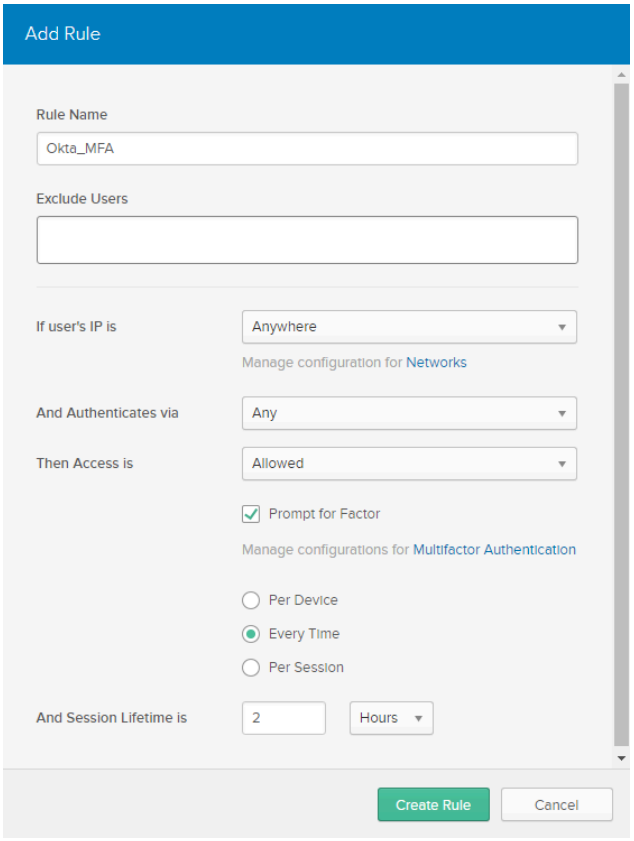
©2024 Palo Alto Networks, Inc.

STEP 5 | 為使用者指派測試原則。

1. 選取 **Security**（安全性） > **Authentication**（驗證） > **Sign On**（登入）。

   具有 **Default Rule**（預設規則）的 **Default Policy**（預設原則）不會提示使用者使用 MFA 登入。

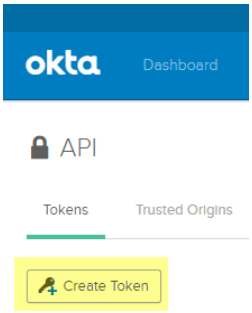
2. 輸入 **Rule Name**（規則名稱）並核取 **Prompt for Factor**（因素提示）以強制執行 MFA 提示，然後選取提示類型（**Per Device**（每個裝置）、**Every Time**（每次）或 **Per Session**（每個工作階段）），然後 **Create Rule**（建立規則）。



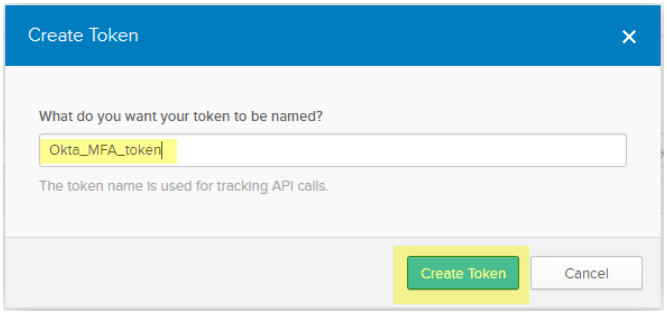
 ©2024 Palo Alto Networks, Inc.

STEP 6 | 由於 Okta 驗證權杖資訊只顯示一次，務必將其安全記錄。

1. 選取 **Security**（安全） > **API** > **Tokens**（權杖）。
2. 選取 **Create Token**（建立權杖）。

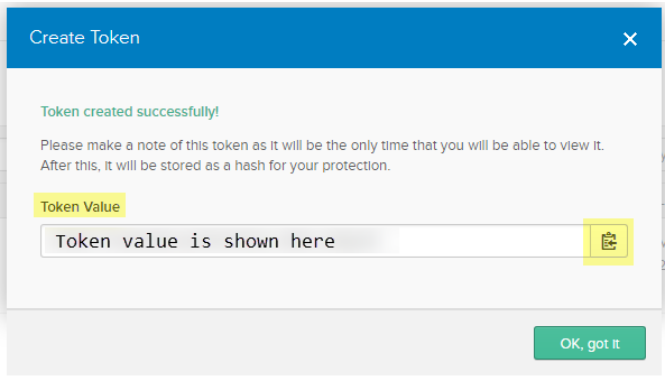


3. 輸入權杖的名稱，然後 **Create Token**（建立權杖）。

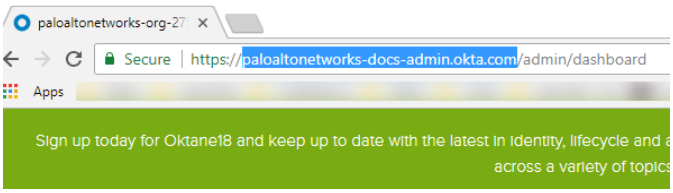


4. 複製 **Token Value**（權杖值）。

   您可以按一下 **Copy to clipboard**（複製到剪貼簿）按鈕，以將 Token Value（權杖值）複製到剪貼簿。

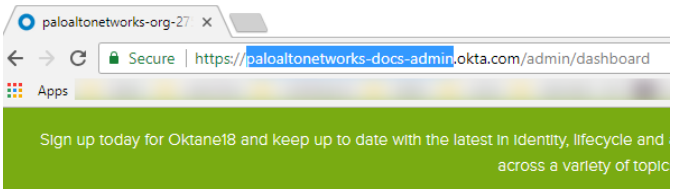


5. 在 Okta 管理員儀表板 URL 中，複製 URL 中 **`https://`** 之後 **`/admin`** 之前的部分以用作 **API host**（**API** 主機）。



6. 省略此 URL 中的網域 **`okta.com`** 以用作 **Organization**（組織）。

©2024 Palo Alto Networks, Inc.



例如，在上述 Okta 管理員儀表板 URL **`https://paloaltonetworks-doc-admin.okta.com/admin/dashboard`** 示例中：

- API 主機名稱為 **`paloaltonetworks-doc-admin.okta.com`**。
- 組織為 **`paloaltonetworks-doc-admin`**。

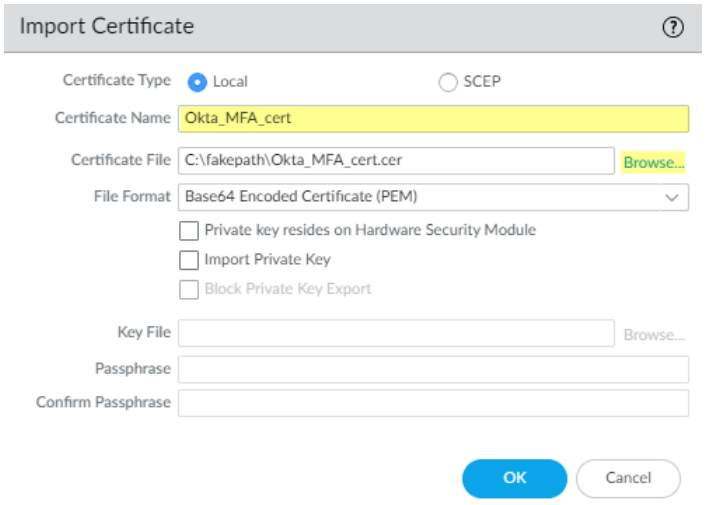
STEP 7 | 使用 Base-64 encoding 匯出憑證鏈中的全部憑證：

1. 視乎您的瀏覽器而定，使用以下一種方法匯出憑證鏈中的全部憑證。
   - **Chrome**—按下 **F12**，然後選取 **Security**（安全性） > **View Certificate**（檢視憑證） > **Details**（詳細資料） > **Copy to File**（複製到檔案）。
   - **Firefox**—選取 **Options**（選項） > **Privacy & Security**（隱私權與安全性） > **View Certificates**（檢視憑證） > **Export**（匯出）。
   - **Internet Explorer**—選取 **Settings**（設定） > **Internet Options**（網際網路選項） > **Content**（內容） > **Certificates**（憑證） > **Export**（匯出）。
2. 使用憑證匯出精靈匯出鏈中的全部憑證，然後選取 **Base-64 encoded X.509**（**Base-64** 編碼 **X.509**） 作為格式。

設定防火牆與 Okta 進行整合

作為先決條件，請確認您對應了要使用 Okta 進行驗證的所有使用者。

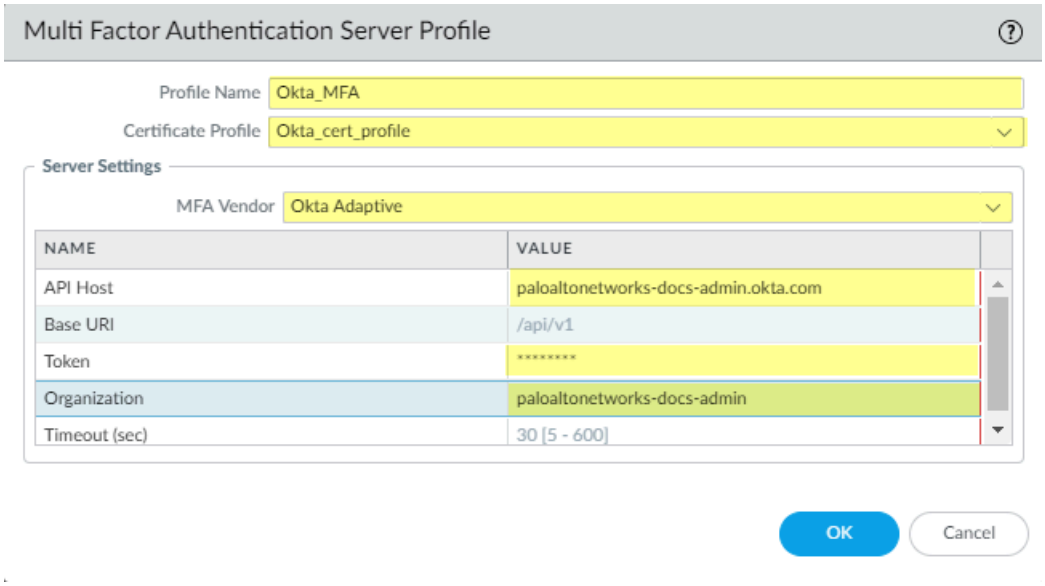
STEP 1 | 匯入防火牆上憑證鏈中的全部憑證，並將匯入的 CA 憑證（根憑證和中間憑證）新增至憑證設定檔。



 ©2024 Palo Alto Networks, Inc.

STEP 2 | 為 Okta 新增 **Multi Factor Authentication Server Profile**（多因素驗證伺服器設定檔）。

1. 選取 **Device**（裝置） > **Server Profiles**（伺服器設定檔） > **Multi Factor Authentication**（多因素驗證）。
2. **Add**（新增）MFA 伺服器設定檔。

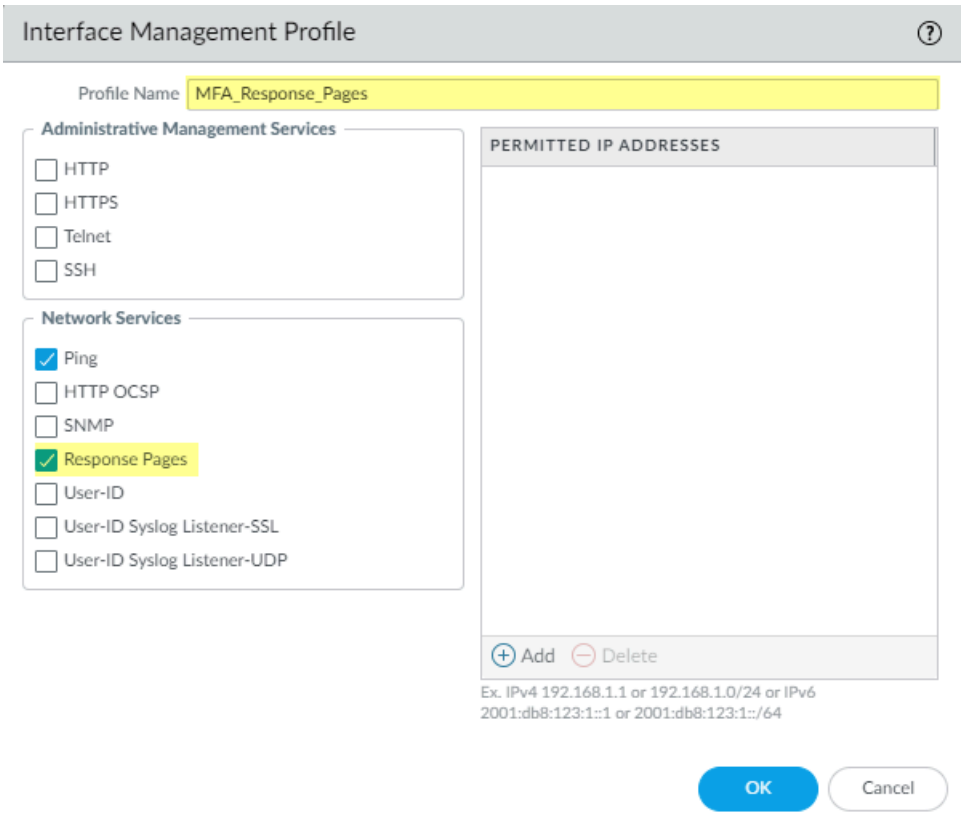


3. 輸入 **Profile Name**（設定檔名稱）。
4. 選取在設定防火牆與 Okta 進行整合步驟 1 中建立的 **Certificate Profile**（憑證設定檔）。
5. 選取 **Okta Adaptive** 作為 **MFA Vendor**（**MFA** 廠商）。
6. 輸入設定防火牆與 Okta 進行整合步驟 4 中的 **API Host**（**API** 主機）、**Token**（權杖）以及 **Organization**（組織）。

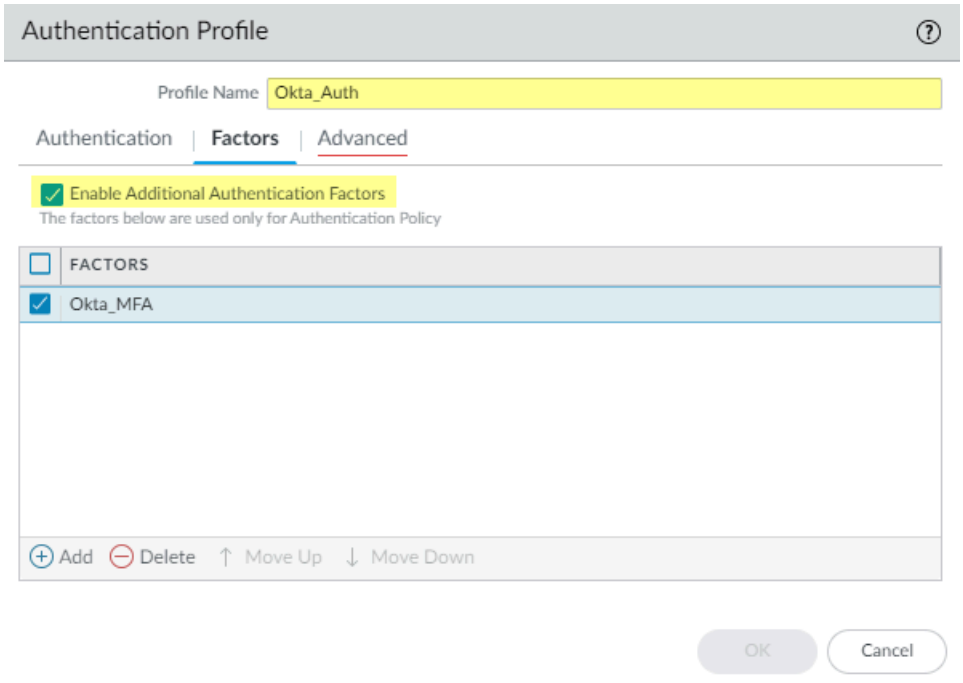
STEP 3 | 使用 **Redirect Mode**（重新導向模式）設定驗證入口網站即可將使用者重新導向至 MFA 廠商的質詢。

©2024 Palo Alto Networks, Inc.

STEP 4 | 啟用介面管理設定檔上的回應頁面即可將使用者重新導向至回應頁面質詢。



STEP 5 | 建立驗證設定檔，然後新增 MFA 廠商作為 **Factor**（因素）（參見設定多因素驗證步驟 3）。



STEP 6 | 在來源區域上啟用 User-ID，要求已識別的使用者使用您的 MFA 廠商回應質詢。

©2024 Palo Alto Networks, Inc.

STEP 7 | 建立驗證強制物件以使用 MFA 廠商，然後建立驗證原則規則（參見設定驗證原則步驟 4 與 5）。

STEP 8 | **Commit**（提交）您的變更。

透過 Okta 驗證 MFA

STEP 1 | 驗證您的使用者是否已收到其註冊電子郵件、已啟用其帳戶，以及是否已在其裝置上下載了 Okta Verify 應用程式。

STEP 2 | 移至提示回應頁面質詢的網站。

如果您使用的是自簽憑證而不是來自組織的 *PKI* 指派憑證，則會顯示一條安全性警告，指出使用者必須按一下才能存取該質詢。

STEP 3 | 使用 Okta 認證登入回應頁面。

STEP 4 | 確認裝置是否收到質詢推送通知。

STEP 5 | 在使用者接受其裝置上的推送通知以對質詢進行驗證之後，確認使用者是否可以順利存取該頁面。

在 Duo 與防火牆之間設定 MFA

憑藉多因素驗證 (MFA)，您可使用多個因素先確認使用者的身分，再允許其存取網路資源，從而保護公司資產。使用 Duo 身分管理服務對防火牆進行驗證的方法有多種：

- 使用 GlobalProtect 閘道與 RADIUS 伺服器設定檔進行 VPN 登入的雙因素驗證（在 PAN-OS 7.0 及更高版本上受支援）。
- 使用驗證入口網站與 MFA 伺服器設定檔的 API 型整合（不需要 Duo 驗證 Proxy 或 SAML IdP - 在 PAN-OS 8.0 及更高版本上受支援）。
- 內部部署伺服器的 SAML 整合（在 PAN-OS 8.0 及更高版本上受支援）。

要在防火牆和 Duo 之間啟用 SAML MFA，以確保對防火牆的管理存取權：

- 使用 Duo Access Gateway 為 SAML MFA 設定 Duo
- 設定防火牆與 Duo 進行整合
- 透過 Duo 驗證 MFA

使用 Duo Access Gateway 為 SAML MFA 設定 Duo

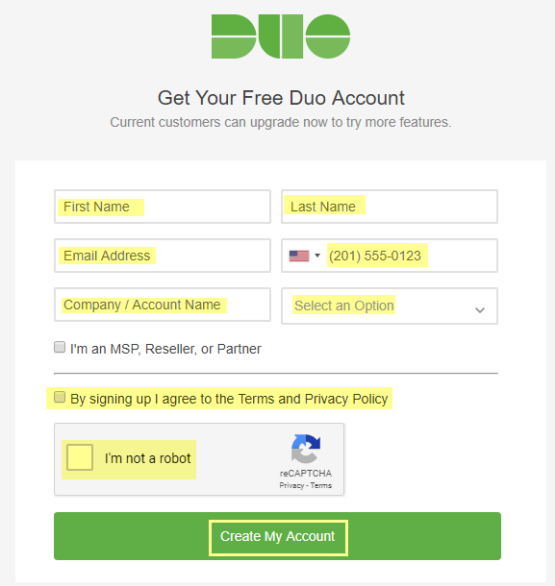
在開始之前，請確認您已在 DMZ 區域中的內部部署伺服器上部署了 DuoAccessGateway (DAG)。

建立 Duo 管理員帳戶並設定 Duo Access Gateway 以在使用者可以存取資源之前對其進行驗證。

©2024 Palo Alto Networks, Inc.

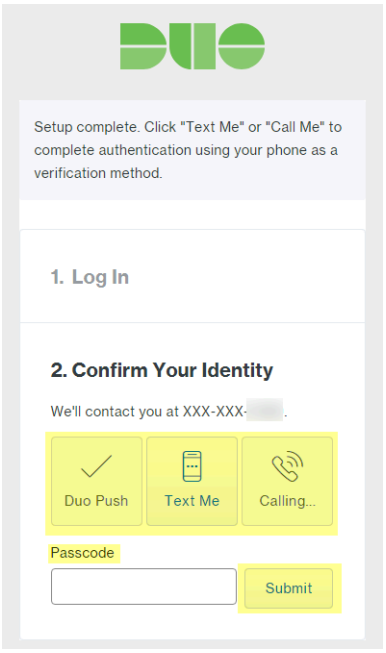
STEP 1 | 建立 Duo 管理員帳戶。

1. 在建立 Duo 帳戶頁面上，輸入您的 **First Name**（名字）、**Last Name**（姓氏）、**Email Address**（電子郵件地址）、**Cell Phone Number**（電話號碼）、**Company / Account Name**（公司#帳戶名稱），然後選取組織中的員工人數。
2. 同意「條款和隱私權原則」，並回應 reCAPTCHA 質詢來 **Create My Account**（建立我的帳戶）。



STEP 2 | 確認 Duo 管理員帳戶。

1. 選取驗證確認方法（**Duo Push**（**Duo** 推送）、**Text Me**（傳送簡訊）或 **Calling...**（呼叫中**...**））。
2. 輸入您收到的 **Passcode**（密碼），然後將其 **Submit**（提交）以確認您的帳戶。

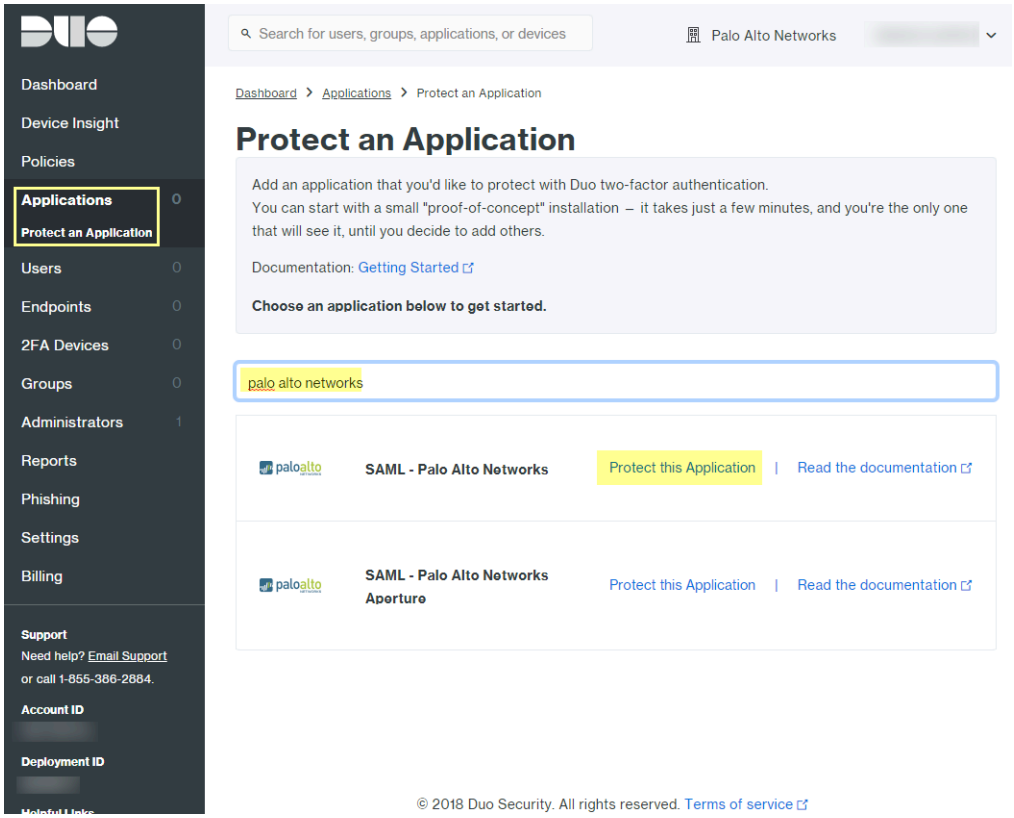


 ©2024 Palo Alto Networks, Inc.

STEP 3 | 為 SAML 設定 Duo 服務。

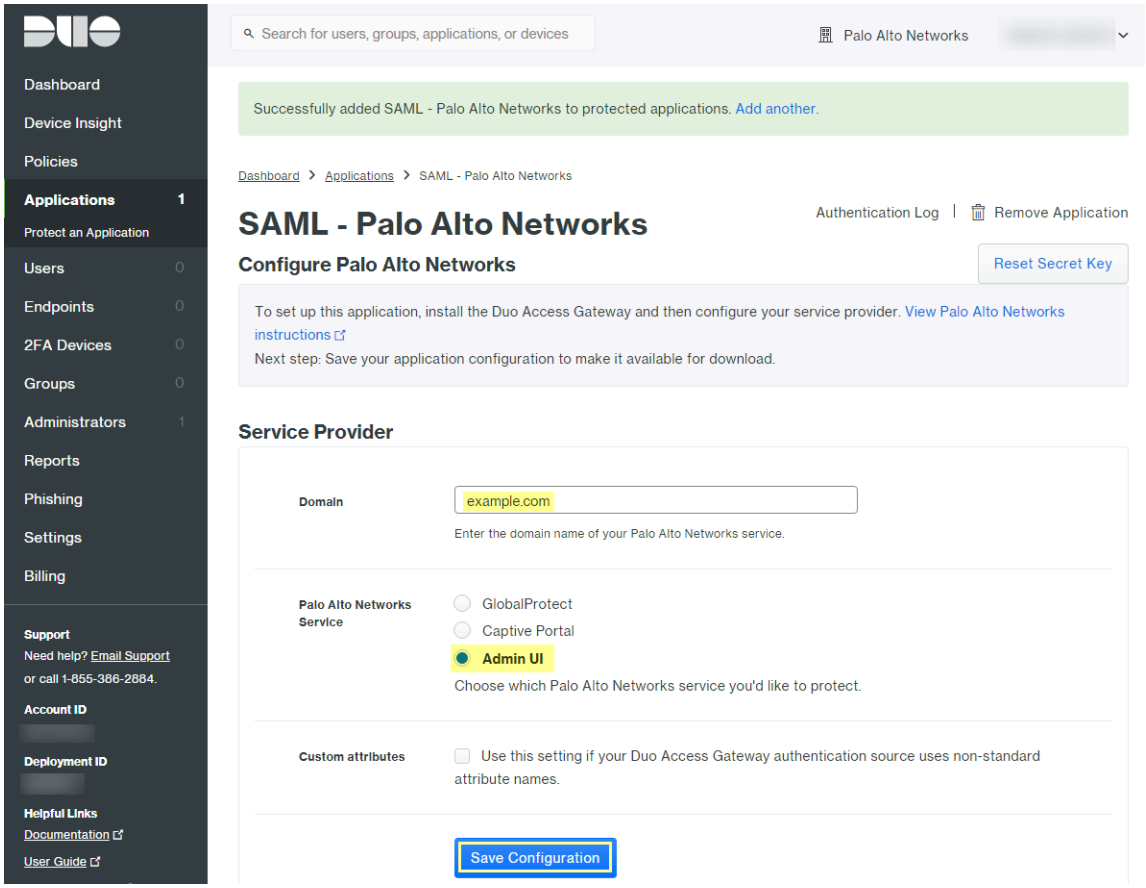
建立組態後，於頁面頂端下載組態檔案。

1. 在 Duo Admin Panel（Duo 管理員畫面）中，選取 **Applications**（應用程式） > **Protect an Application**（保護應用程式）。
2. 輸入 **`Palo Alto Networks`** 即可搜尋應用程式。
3. 在結果清單中找到 **SAML - Palo Alto Networks**，然後 **Protect this Application**（保護此應用程式）。



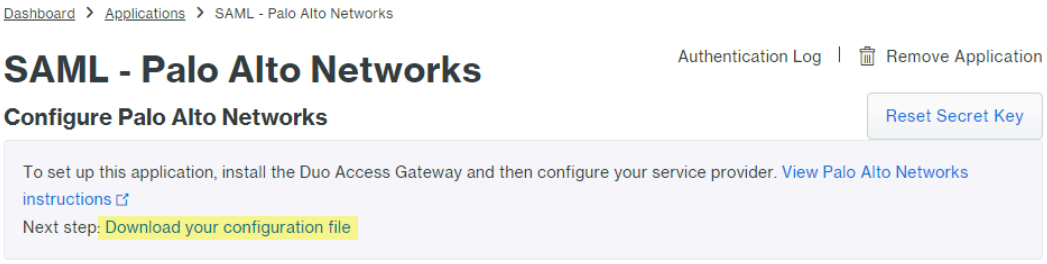
4. 輸入 **Domain**（網域）。
5. 選取 **Admin UI**（管理員使用者介面）作為 **Palo Alto Networks Service**（**Palo Alto Networks** 服務）。
6. 設定 **Policy**（原則）以及其他 **Settings**（設定），然後 **Save Configuration**（儲存組態）。

©2024 Palo Alto Networks, Inc.



7. **Download your configuration file**（下載組態檔案）。

   用於下載檔案的連結位於頁面頂端。



STEP 4 | 將組態檔案上傳到 Duo Access Gateway (DAG)。

1. 在 DAG Admin Console（DAG 管理員主控台）中，選取 **Applications**（應用程式）。
2. 按一下 **Choose File**（選擇檔案），選取已下載的組態檔案，然後將其 **Upload**（上傳）。
3. 在 **Settings**（設定） > **Session Management**（工作階段管理）中，停用 **User agent binding**（使用者代理程式連結），然後 **Save Settings**（儲存設定）。

©2024 Palo Alto Networks, Inc.

STEP 5 | 在 DAG Admin Console（DAG 管理員主控台）中，將 Active Directory 或 OpenLDAP 伺服器設定為驗證來源並下載中繼資料檔案。

1. 登入 DAG Admin Console（DAG 管理員主控台）。
2. 在 **Authentication Source**（驗證來源） > **Set Active Source**（設定使用中來源）中，選取 **Source type**（來源類型）（Active Directory 或 OpenLDAP）與 **Set Active Source**（設定使用中來源）。
3. 在 **Configure Sources**（設定來源）中，輸入 **Attributes**（屬性）。
   - 若為 Active Directory，請輸入 **`mail,sAMAccountName,userPrincipalName,objectGUID`**。
   - 若為 OpenLDAP，請輸入 **`mail,uid`**。
   - 對於任何自訂屬性，將其附加到清單末尾，並用逗點隔開每個屬性。切勿刪除任何現有屬性。
4. **Save Settings**（儲存設定）即可儲存組態。
5. 選取 **Applications**（應用程式） > **Metadata**（中繼資料），然後按一下 **Download XML metadata**（下載 **XML** 中繼資料）來下載需要匯入防火牆的 XML 中繼資料。

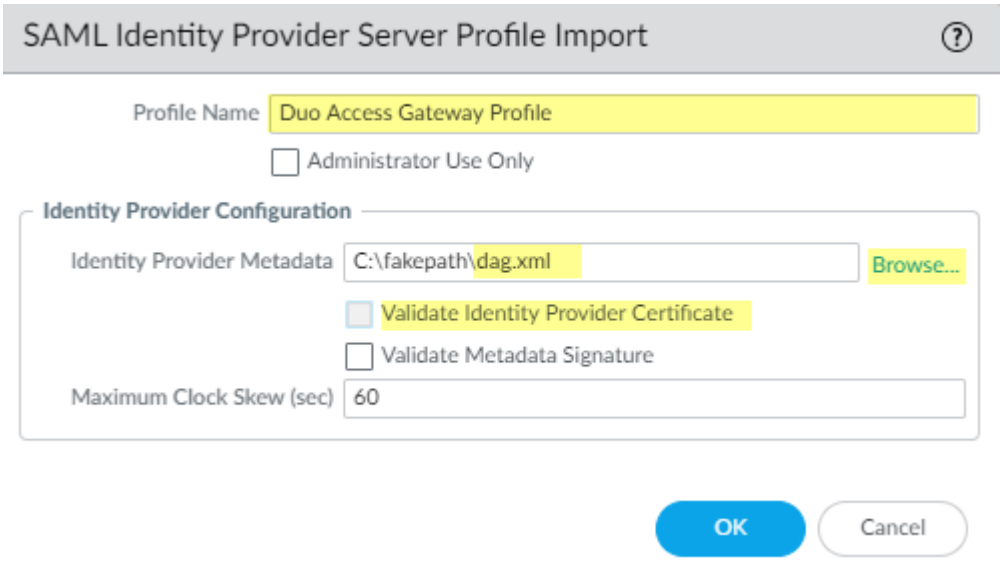
   檔案將被命名為 dag.xml。由於此檔案包含了用於透過防火牆驗證 Duo 帳戶的敏感資訊，請務必將檔案保存在安全位置，以避免此資訊洩漏。

設定防火牆與 **Duo** 進行整合

©2024 Palo Alto Networks, Inc.

STEP 1 | 匯入 Duo 中繼資料。

1. 登入防火牆 Web 介面。
2. 在防火牆上，選取 **Device**（裝置） > **Server Profiles**（伺服器設定檔） > **SAML Identity Provider**（**SAML** 身分提供者） > **Import**（匯入）。
3. 輸入 **Profile Name**（設定檔名稱）。
4. **Browse**（瀏覽）至**Identity Provider Metadata**（身分提供者中繼資料）檔案 **(dag.xml)**。
5. 如果 Duo Access Gateway 提供自我簽署憑證作為 IdP 的簽署憑證，則您無法 **Validate Identity Provider Certificate**（驗證識別提供者憑證）。在這種情況下，請確保您使用的是 PAN-OS 11.0，以減少對 CVE-2020-2021 的接觸。

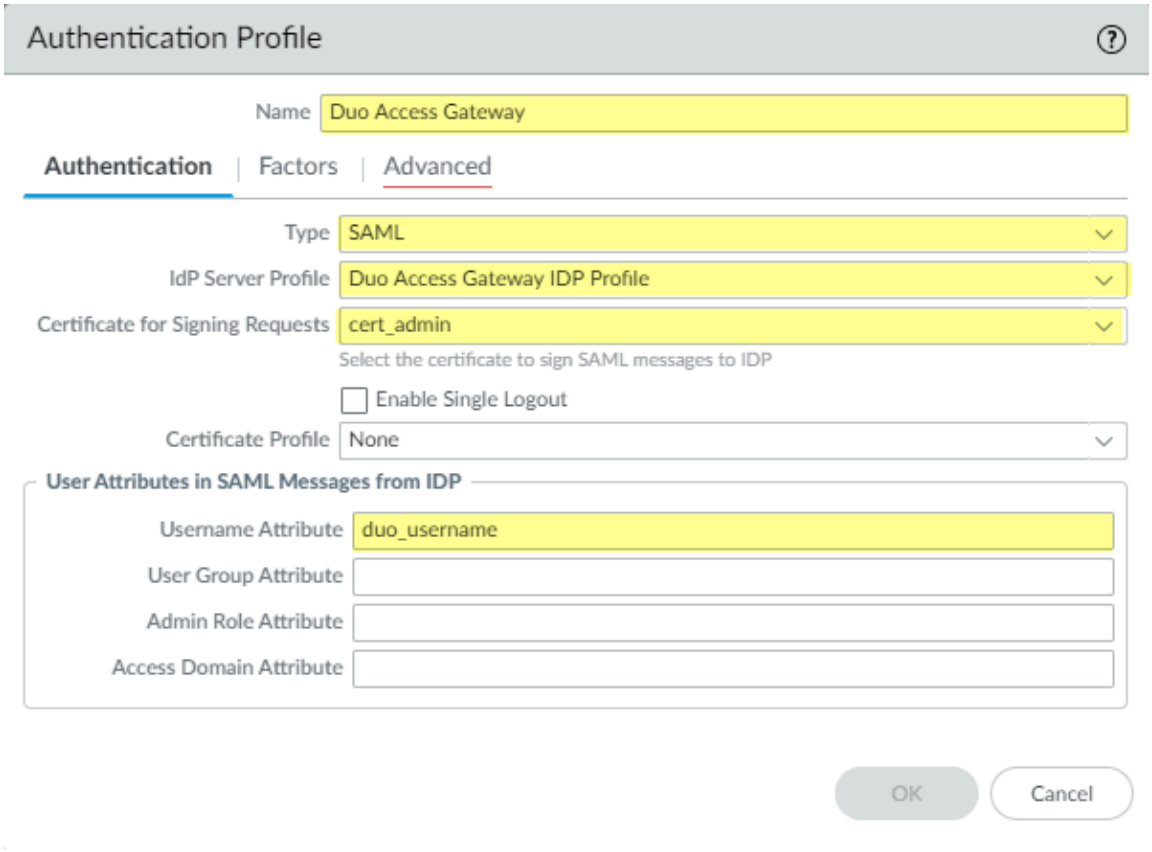


©2024 Palo Alto Networks, Inc.

STEP 2 | 新增驗證設定檔。

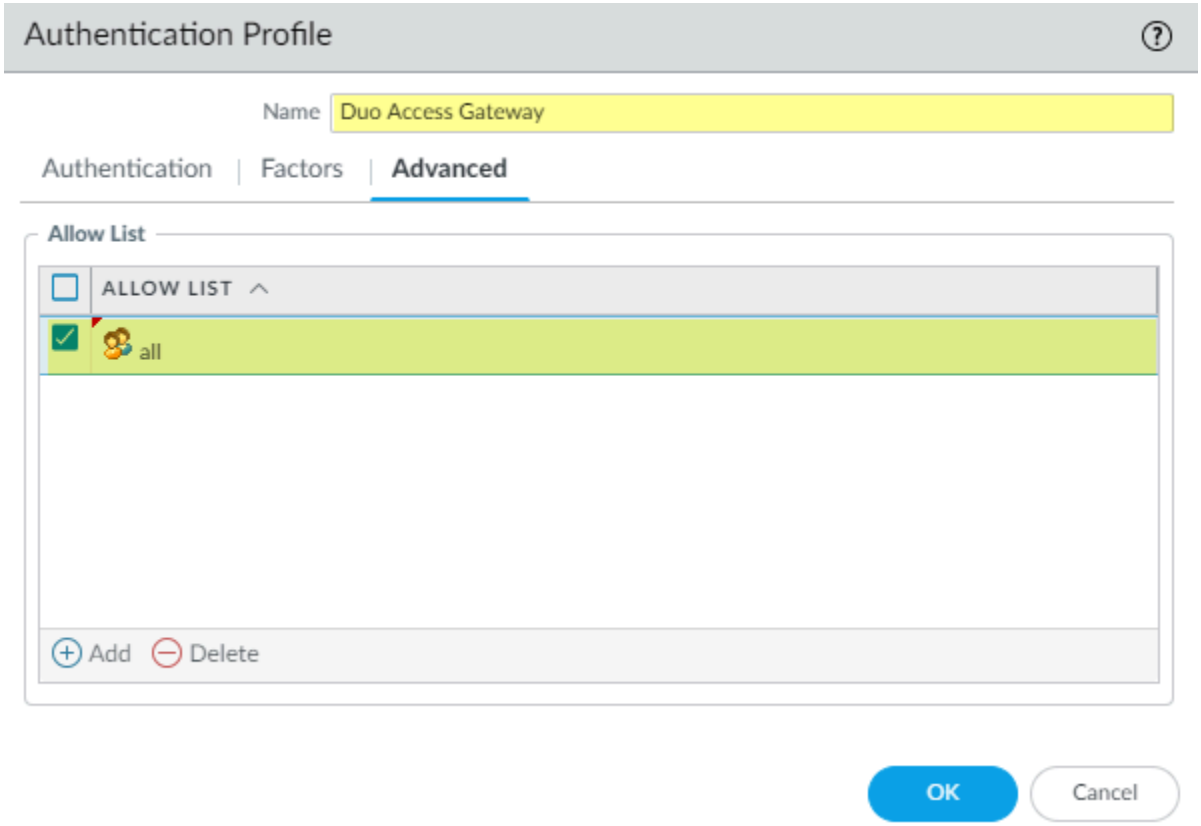
驗證設定檔允許 Duo 作為身分提供者驗證管理員登入認證。

1. **Add**（新增）**Authentication Profile**（驗證設定檔）。
2. 輸入設定檔 **Name**（名稱）。
3. 選取 **SAML** 作為驗證 **Type**（類型）。
4. 選取 **Duo Access Gateway Profile**（**Duo Access Gateway** 設定檔）作為 **IdP Server Profile**（**IdP** 伺服器設定檔）。
5. 選取要用於與 Duo Access Gateway 進行 SAML 通訊的憑證，以獲取 **Certificate for Signing Requests**（用於簽署要求的憑證）。
6. 輸入 **`duo_username`** 作為 **Username Attribute**（使用者名稱屬性）。



7. 選取 **Advanced**（進階）來**Add**（新增）允許清單。
8. 選取 **all**（全部），然後按一下 **OK**（確定）。
9. **Commit**（提交）變更。

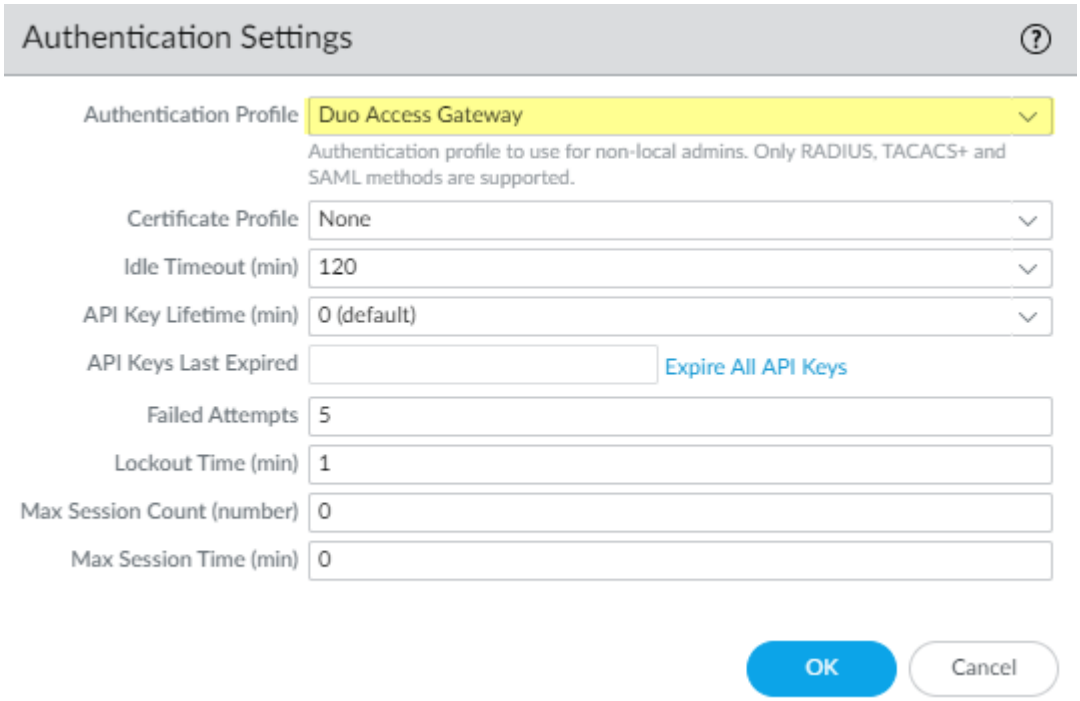
©2024 Palo Alto Networks, Inc.



©2024 Palo Alto Networks, Inc.

STEP 3 | 指定防火牆用於透過 Duo 進行 SAML 驗證的驗證設定。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理），然後編輯 **Authentication Settings**（驗證設定）。
2. 選取 **Duo Access Gateway** 作為 **Authentication Profile**（驗證設定檔），然後按一下 **OK**（確定）。



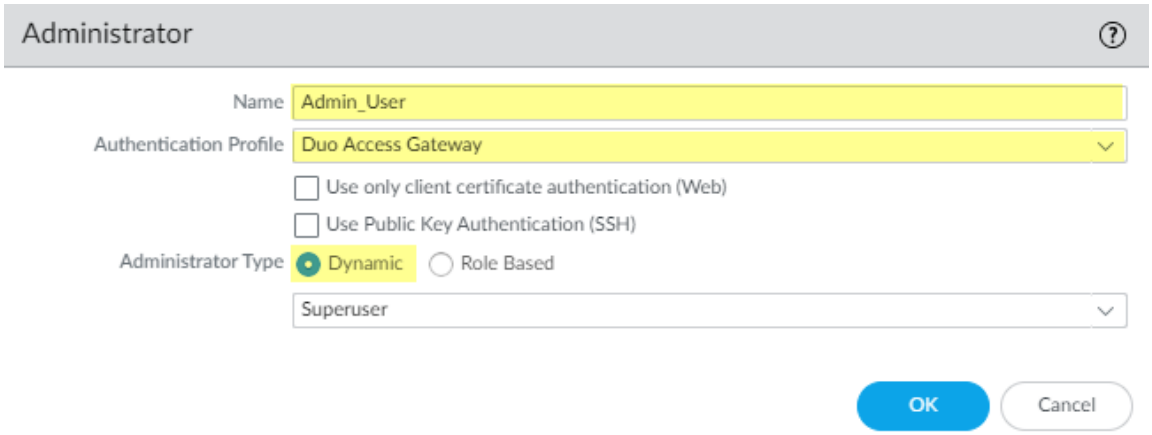
3. **Commit**（提交）您的變更。

©2024 Palo Alto Networks, Inc.

STEP 4 | 為將使用 Duo 向防火牆進行驗證的管理員新增帳戶。

1. 選取 **Device**（裝置） > **Administrators**（管理員），然後 **Add**（新增） 帳戶。
2. 輸入使用者 **Name**（名稱）。
3. 選取 **Duo Access Gateway** 作為 **Authentication Profile**（驗證設定檔）。
4. 選取 **Administrator Type**（管理員類型），然後按一下 **OK**（確定）。

   若要對使用者使用自訂角色，請選取 **Role Based**（以角色為基礎）。否則，選取 **Dynamic**（動態）。若要要求管理員透過 Duo 使用 SSO 進行登入，請將驗證設定檔指派給所有現行管理員。



透過 Duo 驗證 MFA

STEP 1 | 登入防火牆的 Web 介面。

STEP 2 | 選取 **Use Single Sign-on**（使用單一登入）與 **Continue**（繼續）。

STEP 3 | 在 Duo Access Gateway 登入頁面上輸入您的登入認證。

STEP 4 | 選取驗證方法（推送通知、電話或密碼輸入）。

成功進行驗證後，會將您重新導向至防火牆 Web 介面。

©2024 Palo Alto Networks, Inc.

設定 SAML 驗證

若要設定 SAML 單一登入 (SSO) 和單一登出 (SLO)，您必須相互註冊防火牆和 IdP，以啟用它們之間的通訊。若 IdP 提供了包含註冊資訊的中繼資料檔案，您可以將其匯入防火牆，以註冊 IdP 並建立 IdP 伺服器設定檔。該伺服器設定檔定義了如何連線至 IdP 並指定了 IdP 用於簽署 SAML 訊息的憑證。您還可以使用防火牆的憑證簽署 SAML 訊息。為確保防火牆與 IdP 之間的通訊安全，必須使用憑證。

Palo Alto Networks 要求使用 HTTPS，從而確保所有 SAML 交易（而非已加密之 SAML 判斷提示等替代方法）的機密性。為了確保 SAML 事務中所處理之所有訊息的完整性，Palo Alto Networks 要求使用數位憑證以加密簽署所有訊息。

下列程序介紹了如何為使用者和防火牆管理員設定 SAML 驗證。您還可以為 Panorama 管理員設定 SAML 驗證。

SSO 適用於管理員和 *GlobalProtect* 及驗證入口網站一般使用者。*SLO* 適用於管理員和 *GlobalProtect* 一般使用者，但不適用於驗證入口網站一般使用者。

管理員可以使用 *SAML* 來驗證防火牆 *Web* 介面，但不能驗證 *CLI*。

STEP 1 | 取得 IdP 和防火牆將用於簽署 SAML 資訊的憑證。

如果這些憑證未指定金鑰用途屬性，則預設會允許各種用途，包括簽署訊息。在這種情況下，您可以透過任何方式取得憑證。

如果憑證明確指定了金鑰的用途屬性，則其中一個屬性必須是 Digital Signature（數位簽章），而您在防火牆或 Panorama 上產生的憑證中並無此屬性。在這種情況下，您必須匯入憑證：

- 防火牆用於簽署 **SAML** 訊息的憑證—從企業憑證授權單位 (CA) 或協力廠商 CA 匯入憑證。
- **IdP** 用於簽署 **SAML** 訊息的憑證（對於所有部署均為必須）—從 IdP 匯入包含憑證的中繼資料檔案（請參閱下一步）。IdP 憑證限於下列演算法：

  公開金鑰演算法—RSA（1,024 位元或更大）和 ECDSA（所有大小）。FIPS/CC 模式下的防火牆支援 RSA（2,048 位元或更大）和 ECDSA（所有大小）。

  簽章演算法—SHA1、SHA256、SHA384 和 SHA512。FIPS/CC 模式下的防火牆支援 SHA256、SHA384 和 SHA512。

STEP 2 | 新增 SAML IdP 伺服器設定檔。

該伺服器設定檔將在防火牆中註冊 IdP，並定義它們的連線方式。

在此範例中，您將從 IdP 匯入 SAML 中繼資料檔案，以便防火牆能夠自動建立伺服器設定檔並填入連線、註冊和 IdP 憑證資訊。

如果 *IdP* 未提供中繼資料檔案，則選取 ***Device***（裝置） > ***Server Profiles***（伺服器設定檔） > ***SAML Identity Provider***（***SAML*** 識別提供者），然後 ***Add***（新增） 伺服器設定檔，再手動輸入相關資訊（請資訊 *IdP* 管理員以獲取相關值）。

©2024 Palo Alto Networks, Inc.

1. 從 IdP 匯出 SAML 中繼資料檔案到用戶端系統，您可從中將中繼資料檔案上載到防火牆。

   該檔案中指定的憑證必須符合前一步中所列的要求。關於匯出檔案的說明，請參閱 IdP 文件。

2. 在 Panorama™ 上選取 **Device**（裝置） > **Server Profiles**（伺服器設定檔） > **SAML Identity Provider**（**SAML** 識別提供者）或**Panorama** > **Server Profiles**（伺服器設定檔） > **SAML Identity Provider**（**SAML** 識別提供者），並將中繼資料檔案 **Import**（匯入）防火牆。
3. 輸入用來識別伺服器設定檔的 **Profile Name**（設定檔名稱）。
4. **Browse**（瀏覽）至**Identity Provider Metadata**（識別提供者中繼資料）檔案。
5. 選取 **Validate Identity Provider Certificate**（驗證識別提供者憑證）（預設值）以驗證信任鏈以及 IdP 憑證的吊銷狀態（選用）。

   要啟用此選項，憑證授權單位 (CA) 必須簽發您的 IdP 簽署憑證。您必須建立擁有具有簽發 IdP 簽署憑證的 CA 憑證設定檔。在「驗證設定檔」中，選取 SAML 伺服器設定檔和憑證設定檔以驗證 IdP 憑證。

   如果您的 IdP 簽署憑證為自我簽署憑證，則沒有信任鏈；因此，您無法啟用此選項。防火牆始終會根據您設定的識別提供者憑證來驗證 SAML 回應或聲明的簽名，無論您是否啟用**Validate Identity Provider Certificate**（驗證識別提供者憑證）選項。如果您的 IdP 提供自我簽署憑證，請確保您使用的是 PAN-OS 11.0，以減少對 CVE-2020-2021 的接觸。

   驗證憑證以確保其未遭受入侵並提高安全性。

6. 輸入 **Maximum Clock Skew**（最大時鐘誤差），即在防火牆驗證 IdP 訊息的瞬間，IdP 系統時間與 防火牆系統時間的差值（單位為秒，預設值為 60；範圍為 1-900）。若差值超過此值，則驗證失敗。
7. 按一下 **OK**（確定）來儲存伺服器設定檔。
8. 按一下伺服器設定檔名稱，以顯示設定檔組態。確認所匯出的資訊是否正確，並在必要時編輯。
9. 無論您是匯入 IdP 中繼資料檔案還是手動輸入 IdP 資訊，請始終確保 SAML 識別提供者的簽名憑證是您伺服器設定檔的識別提供者憑證，且您的 IdP 會傳送簽署的 SAML 回應、聲明或兩者。

©2024 Palo Alto Networks, Inc.

STEP 3 | 設定驗證設定檔。

此設定檔定義了一組使用者共用的驗證設定。

1. 選取 **Device**（裝置） > **Authentication Profile**（驗證設定檔），然後 **Add**（新增） 設定檔。
2. 輸入用來識別設定檔的 **Name**（名稱）。
3. 將 **Type**（類型）設為 **SAML**。
4. 選取您設定的 **IdP Server Profile**（**IdP** 伺服器設定檔）。
5. 選取 **Certificate for Signing Requests**（用於簽署要求的憑證）。

   防火牆將使用此憑證簽署傳送至 IdP 的訊息。您可以匯入由企業 CA 產生的憑證，也可以使用在防火牆或 Panorama 上產生的根 CA 產生憑證。
6. （選用）**Enable Single Logout**（啟用單一登出）（預設為停用）。
7. 選取防火牆將用於驗證 **Identity Provider Certificate**（識別提供者憑證）的 **Certificate Profile**（憑證設定檔）。
8. 輸入 IdP 訊息用於識別使用者的 **Username Attribute**（使用者名稱屬性）（預設值為 **`username`**）。

   當您預先定義使用者的動態管理員角色時，使用小寫字母指定角色（例如，輸入 ***`superreader`***，而不是 ***`SuperReader`***）。如果您在 *IdP* 識別身分存放區中管理管理員授權，則還要制定 ***Admin Role Attribute***（管理員角色屬性）和***Access Domain Attribute***（存取網域屬性）。
9. 選取 **Advanced**（進階），然後**Add**（新增）允許使用此驗證設定檔進行驗證的使用者和群組。
10. 按一下 **OK**（確定）來儲存驗證設定檔。

STEP 4 | 將驗證設定檔指派給需要驗證的防火牆應用程式。

1. 將驗證設定檔指派給：
   - 您在防火牆上本機管理的管理員帳戶。在此範例中，先設定防火牆管理員帳戶，然後在此程序後期驗證 SAML 組態。
   - 您在 IdP 識別身分存放區中外部管理的管理員帳戶。選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理），編輯 Authentication Settings（驗證設定），然後選取您所設定的 **Authentication Profile**（驗證設定檔）。
   - 用於確保一般使用者透過驗證入口網站存取的服務和應用程式安全的驗證原則規則。請參閱設定驗證原則。
   - 一般使用者存取的 GlobalProtect 入口網站和閘道。
2. **Commit**（提交）您的變更。

   防火牆將驗證您為 SAML IdP 伺服器設定檔指派的 **Identity Provider Certificate**（識別提供者憑證）。

©2024 Palo Alto Networks, Inc.

STEP 5 | 建立 SAML 中繼資料檔案，以在 IdP 上註冊防火牆應用程式（管理存取權、驗證入口網站或 GlobalProtect）。

1. 選取 **Device**（裝置） > **Authentication Profile**（驗證設定檔），然後在您所設定的驗證設定檔的 Authentication（驗證）欄中，按一下 **Metadata**（中繼資料）。
2. 在 **Service**（服務）下拉式清單中選取您要註冊的應用程式：
   - 管理（預設值）—Web 介面的管理存取權。
   - 驗證入口網站—一般使用者透過驗證入口網站存取服務和應用程式。
   - **global-protect**—使用者透過 GlobalProtect 存取服務和應用程式的存取權。
3. （僅限驗證入口網站或 GlobalProtect）對於 **Vsysname Combo**，選取定義了驗證入口網站設定或 GlobalProtect 入口網站的虛擬系統。
4. 根據您將註冊的應用程式，輸入介面、IP 位址或主機名稱：
   - 管理—對於 **Management Choice**（管理選項），選取 **Interface**（介面）（預設值），然後選取要為 Web 介面的管理存取權啟用的介面。預設會選取 MGT 介面的 IP 位址。
   - 驗證入口網站—對於 **IP Hostname**（**IP** 主機名稱），輸入 **Redirect Host**（重新導向主機）的 IP 位址或主機名稱（請參閱 **Device**（裝置） > **User Identification**（使用者識別） > **Authentication Portal Settings**（驗證入口網站設定））。
   - **global-protect**—對於 **IP Hostname**（**IP** 主機名稱），輸入 GlobalProtect 入口網站或閘道的主機名稱或 IP 位址。
5. 按一下 **OK**（確定），將中繼資料檔案儲存至用戶端系統。
6. 將中繼資料檔案匯入 IdP 伺服器，以註冊防火牆應用程式。相關說明，請參閱 IdP 文件。

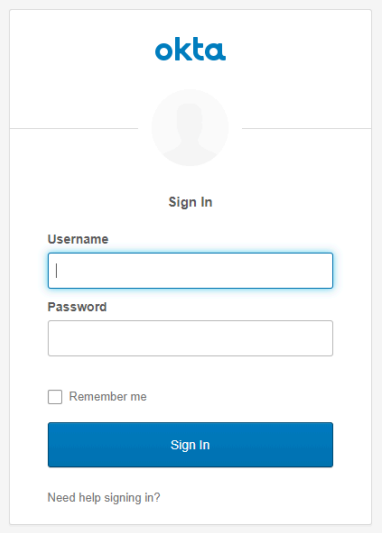
©2024 Palo Alto Networks, Inc.

STEP 6 | 確認使用者是否能使用 SAML SSO 進行驗證。

例如，若要使用本機管理員帳戶確認 SAML 是否可用於存取 Web 介面：

1. 移至防火牆 Web 介面的 URL。
2. 按一下 **Use Single Sign-On**（使用單一登入）。
3. 輸入管理員的使用者名稱。
4. 按一下 **Continue**（繼續）。

   防火牆會將您重新導向，以驗證 IdP，此時會顯示一個登入頁面。例如：



5. 使用 SSO 使用者名稱和密碼登入。

   在 IdP 上成功驗證後，將重新導向回防火牆，此時會顯示 Web 介面。
6. 使用防火牆管理員帳戶要求存取其他 SSO 應用程式。

   成功存取表示 SAML SSO 驗證成功。

 ©2024 Palo Alto Networks, Inc.

設定 Kerberos 單一登入

Palo Alto Networks 防火牆和 Panorama 支援 Kerberos V5 Single Sign-On（單一登入，SSO），以向網頁介面驗證管理員並向驗證入口網站驗證一般使用者。啟用 Kerberos SSO 後，使用者僅需要在首次存取網路時登入（例如登入 Microsoft Windows）。在首次登入之後，使用者便可存取網路中任何以瀏覽器為基礎的服務（例如防火牆網頁介面），而不必再次登入，直到 SSO 工作階段到期為止。

STEP 1 | 建立 Kerberos 金鑰標籤。

金鑰標籤是一個包含了防火牆主體名稱和密碼的檔案，SSO 過程中需要此檔案。在驗證設定檔和順序中設定 Kerberos 時，防火牆首先會檢查 Kerberos SSO 主機名稱。若您提供了主機名稱，則防火牆會搜尋與此主機名稱相符的金鑰標籤作為服務主體名稱，並僅使用該金鑰標籤進行解密。若您未提供主機名稱，防火牆會嘗試驗證順序中的每個金鑰標籤，直至其可以使用 Kerberos 成功進行驗證。

如果 *Kerberos SSO* 主機名稱包含在傳送至防火牆的請求中，則主機名稱必須與 *Keytab* 的服務主體名稱相符；否則不會傳送 *Kerberos* 驗證請求。

1. 登入 Active Directory（主動式目錄 - AD）伺服器並開啟命令提示字元。
2. 輸入以下命令為 GlobalProtect 或驗證入口網站註冊服務主體名稱 (SPN)，其中 *<portal_fqdn>* 和 *<service_account_username>* 是變數。

   setspn -s HTTP/*<portal_fqdn>* *<service_account_username>*
3. 為防火牆建立 Kerberos 帳戶。相關步驟，請參閱 Kerberos 文件。
4. 登入 KDC 並開啟命令提示字元。
5. 輸入以下命令，其中 *<portal_fqdn>*、*<kerberos_realm>*、*<netbios_name>*、*<service_account_username>*、*<password>*、*<f* 和 *<algorithm>* 是變數。

   ktpass /princ HTTP *<portal_fqdn>*@*<kerberos_realm>* /mapuser *<netbios_name><service_account_username>* /pass *<password>*/out *<filename>*.keytab /ptype KRB5_NT_PRINCIPAL /crypto *<algorithm>***

   <kerberos_realm> 值必須全為大寫字元（例如，輸入 ***AD1.EXAMPLE.COM***，而不是 ***ad1.example.com***）。

   如果防火牆處於 *FIPS/CC* 模式，演算法必須為 ***aes128-cts-hmac-sha1-96*** 或 ***aes256-cts-hmac-sha1-96***。否則，您也可以使用 ***des3-cbc-sha1*** 或 ***arcfour-hmac***。若要使用 *Advanced Encryption Standard*（進階加密標準，*AES*）演算法，*KDC* 的功能層級必須為 *Windows Server 2012* 或更新層級，且您必須針對防火牆帳戶啟用 *AES* 加密。

   金鑰標籤中的演算法，必須符合 *TGS* 發行給用戶端之服務票證中的演算法。您的 *Kerberos* 管理員會決定服務票證所使用的演算法。

©2024 Palo Alto Networks, Inc.

STEP 2 | 設定驗證設定檔和順序，以定義由一組使用者共用的 Kerberos 設定和其他驗證選項。

- 輸入 **Kerberos Realm**（**Kerberos** 領域）（通常為使用者的 DNS 網域，但領域為大寫時除外）。
- **Import**（匯入）您為防火牆建立的 **Kerberos Keytab**（**Kerberos** 金鑰標籤）。

STEP 3 | 將驗證設定檔指派給需要驗證的防火牆應用程式。

- Web 介面的管理存取權—設定防火牆管理員帳戶並指派您所設定的驗證設定檔。
- 使用者對服務和應用程式的存取權—將您所設定的驗證設定檔指派給驗證強制物件。在設定物件時，將 **Authentication Method**（驗證方法）設定為 **browser-challenge**（瀏覽器挑戰）。將物件指派給驗證原則規則。關於設定使用者驗證的完整程序，請參閱設定驗證原則。

©2024 Palo Alto Networks, Inc.

設定 Kerberos 伺服器驗證

您可以使用 Kerberos 以透過 Active Directory 網域控制站或 Kerberos V5 相容驗證伺服器原生驗證使用者和防火牆或 Panorama 管理員。這是一種互動式驗證方法，需要使用者輸入使用者名稱和密碼。

若要使用 *Kerberos* 伺服器進行驗證，伺服器必須可在 *IPv4* 位址上進行存取。不支援 *IPv6* 位址。

STEP 1 | 新增 Kerberos 伺服器設定檔。

設定檔定義了防火牆將採用何種方式連線 Kerberos 伺服器。

1. 在 Panorama™ 上選取 **Device**（裝置） > **Server Profiles**（伺服器設定檔） > **Kerberos** 或 **Panorama** > **Server Profiles**（伺服器設定檔） > **Kerberos**，然後 **Add**（新增）伺服器設定檔。
2. 輸入用來識別伺服器設定檔的 **Profile Name**（設定檔名稱）。
3. **Add**（新增）每個伺服器，並指定用於識別伺服器的 **Name**（名稱）、**Kerberos Server**（**Kerberos** 伺服器）的 IPv4 位址或 FQDN，以及用於與伺服器通訊的 **Port**（連接埠）號碼（選填，預設為 88）。

   如果您使用 *FQDN* 位址物件識別伺服器並隨後變更了位址，則必須要提交變更，以便新伺服器位址生效。
4. 按一下 **OK**（確定）以儲存設定檔的變更。

STEP 2 | 將伺服器設定檔指定給驗證設定檔或驗證順序。

驗證設定檔定義了一組使用者共用的驗證設定。

STEP 3 | 將驗證設定檔指派給需要驗證的防火牆應用程式。

- Web 介面的管理存取權—設定防火牆管理員帳戶並指派您所設定的驗證設定檔。
- 使用者對服務和應用程式的存取權—將您所設定的驗證設定檔指派給驗證強制物件，並將該物件指派給驗證原則規則。關於設定使用者驗證的完整程序，請參閱設定驗證原則。

STEP 4 | 確認防火牆是否能夠測試驗證伺服器連線，以驗證使用者。

©2024 Palo Alto Networks, Inc.

設定 TACACS+ 驗證

您可以為使用者以及防火牆或 Panorama 管理員設定 TACACS+ 驗證。您還可以透過定義廠商特定屬性 (VSA) 來使用 TACACS+ 伺服器管理管理員授權（角色與存取網域指派）。對於所有使用者，您必須設定 TACACS+ 伺服器設定檔，定義防火牆或 Panorama 如何連線至伺服器。然後將該伺服器設定檔指派給每一組（需要共用驗證設定的）使用者的驗證設定檔。對驗證設定檔執行的操作視乎於 TACACS+ 伺服器驗證的使用者：

- 使用者—將驗證設定檔指派給驗證強制物件，並將該物件指派給驗證原則規則。完整的程序，請參閱設定驗證原則。
- 在防火牆或 **Panorama** 上本機管理授權的管理員帳戶—將驗證設定檔指派給防火牆管理員或Panorama 管理員帳戶。
- 在 **TACACS+** 伺服器上管理授權的管理員帳戶—下列程序介紹了如何為防火牆管理員設定 TACACS+ 驗證和授權。對於 Panorama 管理員，請參閱為 Panorama 管理員設定 TACACS+ 驗證。

STEP 1 | 新增 TACACS+ 伺服器設定檔。

該設定檔定義了防火牆將採用何種方式連線 TACACS+ 伺服器。

1. 在 Panorama™ 上選取 **Device**（裝置） > **Server Profiles**（伺服器設定檔） > **TACACS+** 或 **Panorama** > **Server Profiles**（伺服器設定檔） > **TACACS+** 並 **Add**（新增） 設定檔。
2. 輸入用來識別伺服器設定檔的 **Profile Name**（設定檔名稱）。
3. （選用）選取 **Administrator Use Only**（僅管理員使用）以將存取權限限制到管理員。
4. 輸入 **Timeout**（逾時）間隔時間（單位為秒），超過此時間後，驗證要求將逾時（預設值為 3；範圍為 1-20）。
5. 選取防火牆將用於驗證 TACACS+ 伺服器的 **Authentication Protocol**（驗證通訊協定）（預設值為 **CHAP**）。

   選取 ***CHAP***（如果 *TACACS+* 伺服器支援此通訊協定）；它比 ***PAP*** 更安全。

6. **Add**（新增）每個 TACACS+ 伺服器，然後輸入下列資訊：
   - 用來識別伺服器的 **Name**（名稱）
   - **TACACS+ Server**（**TACACS+** 伺服器）IP 位址或 FQDN。如果您使用 FQDN 位址物件識別伺服器並隨後變更了位址，則必須要提交變更，以便新伺服器位址生效。
   - **Secret**（密碼）/**Confirm Secret**（確認密碼）（用於加密使用者名稱和密碼的金鑰）
   - 用於驗證要求的伺服器 **Port**（連接埠）（預設值為 49）
7. 按一下 **OK**（確定）來儲存伺服器設定檔。

©2024 Palo Alto Networks, Inc.

STEP 2 | 將 TACACS+ 伺服器設定檔指派給驗證設定檔。

驗證設定檔定義了一組使用者共用的驗證設定。

1. 選取 **Device**（裝置） > **Authentication Profile**（驗證設定檔），然後 **Add**（新增） 設定檔。
2. 輸入用來識別設定檔的 **Name**（名稱）。
3. 將 **Type**（類型）設為 **TACACS+**。
4. 選取您設定的 **Server Profile**（伺服器設定檔）。
5. 選取 **Retrieve user group from TACACS+**（從 **TACACS+** 擷取使用者群組），以從 TACACS+ 伺服器上定義的 VSA 收集使用者群組資訊。

   防火牆將比對這些群組資訊與驗證設定檔的允許清單中指定的群組。
6. 選取 **Advanced**（進階），然後在允許清單中，**Add**（新增）允許使用此驗證設定檔進行驗證的使用者和群組。
7. 按一下 **OK**（確定）來儲存驗證設定檔。

STEP 3 | 將防火牆設定為針對所有管理員使用驗證設定檔。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理），然後編輯 Authentication Settings（驗證設定）。
2. 選取您所設定的 **Authentication Profile**（驗證設定檔），再按一下 **OK**（確定）。

STEP 4 | 設定角色和存取網域，定義管理員的授權設定。

如果您已在 TACACS+ 伺服器上定義 TACACS+ VSA，則您為防火牆上角色和存取網域指定的名稱必須與 VSA 值相符。

1. 如果管理員將使用自訂角色而非預定義（動態）角色，則設定管理員角色設定檔。
2. 如果防火牆有一個以上的虛擬系統，則設定存取網域—選取 **Device**（裝置） > **Access Domain**（存取網域），**Add**（新增）並存取網域，輸入用於識別存取網域的 **Name**（名稱），**Add**（新增）管理員將存取的每個虛擬系統，然後按一下 **OK**（確定）。

STEP 5 | **Commit**（提交）變更，以在防火牆上啟用。

©2024 Palo Alto Networks, Inc.

STEP 6 | 設定 TACACS+ 伺服器以驗證和授權管理員。

關於執行下列步驟的特定說明，請參閱 TACACS+ 伺服器文件：

1. 新增防火牆 IP 位址或主機名稱作為 TACACS+ 用戶端。
2. 新增管理員帳戶。

   若將 ***CHAP*** 選為 ***Authentication Protocol***（驗證通訊協定），則您必須為帳戶定義可反轉的加密密碼。否則，*CHAP* 驗證將失敗。
3. 分別為每個管理員的角色、存取網域和使用者群組定義 TACACS+ VSA。

   當您預先定義使用者的動態管理員角色時，使用小寫字母指定角色（例如，輸入 ***superuser***，而不是 ***SuperUser***）。

STEP 7 | 確認 TACACS+ 伺服器是否對管理員執行驗證和授權。

1. 使用您新增至 TACACS+ 伺服器的管理員帳戶登入防火牆 Web 介面。
2. 確認您是否只能存取允許該管理員關聯的角色存取的 Web 介面頁面。
3. 在 **Monitor**（監控）、**Policies**（原則）和 **Objects**（物件）頁籤中，驗證您是否只能存取允許該管理員關聯的粗存取網域存取的虛擬系統。

©2024 Palo Alto Networks, Inc.

設定 RADIUS 驗證

您可以為使用者以及防火牆或 Panorama 管理員設定 RADIUS 驗證。對於管理員，您可以透過定義廠商特定屬性 (VSA) 來使用 RADIUS 管理驗證（角色與存取網域指派）。您可以使用 RADIUS 來對管理員和使用者實作多因素驗證 (MFA)。若要啟用 RADIUS 驗證，您必須設定 RADIUS 伺服器設定檔，其中定義防火牆或 Panorama 如何連線至伺服器（請參閱下方的步驟 1）。然後將該伺服器設定檔指派給每一組（需要共用驗證設定的）使用者的驗證設定檔（請參閱下方的步驟 5）。對驗證設定檔執行的操作視乎於 RADIUS 伺服器驗證的使用者：

- 使用者—將驗證設定檔指派給驗證強制物件，並將該物件指派給驗證原則規則。完整的程序，請參閱設定驗證原則。

  您還可以透過將驗證設定檔指派給 *GlobalProtect* 入口網站或閘道，設定用戶端系統以傳送 *RADIUS* 廠商特定屬性 *(*VSA*)* 到 *RADIUS* 伺服器。*RADIUS* 管理員隨後將基於這些 *VSA* 執行管理工作。

- 在防火牆或 **Panorama** 上本機管理授權的管理員帳戶—將驗證設定檔指派給防火牆管理員或Panorama 管理員帳戶。
- 在 **RADIUS** 伺服器上管理授權的管理員帳戶—下列程序介紹了如何為防火牆管理員設定 RADIUS 驗證和授權。對於 Panorama 管理員，請參閱為 Panorama 管理員設定 RADIUS 驗證。

©2024 Palo Alto Networks, Inc.

STEP 1 | 新增 RADIUS 伺服器設定檔。

該設定檔定義了防火牆將採用何種方式連線 RADIUS 伺服器。

1. 在 Panorama™ 上選擇 裝置 > 伺服器設定檔 > **RADIUS** 或 **Panorama** > 伺服器設定檔 > **RADIUS** 並 新增 設定檔。
2. 輸入用來識別伺服器設定檔的 **Profile Name**（設定檔名稱）。
3. （選用）選取 **Administrator Use Only**（僅管理員使用）以將存取權限限制到管理員。
4. 輸入 **Timeout**（逾時） 間隔時間（單位為秒），超過此時間後，驗證要求將逾時（預設值為 3；範圍為 1-120）。

   如果您是使用伺服器設定檔將防火牆與 *MFA* 服務整合，則輸入可讓使用者有足夠時間進行驗證的間隔。例如，如果 *MFA* 服務提示輸入一次性密碼 *(OTP)*，使用者需要時間才能在其端點設備上看到 *OTP*，然後在 *MFA* 登入頁面中輸入 *OTP*。
5. 輸入 **Retries**（重試）次數。
6. 選取防火牆將用於驗證 RADIUS 伺服器的 **Authentication Protocol**（驗證通訊協定）（預設值為 **PEAP-MSCHAPv2**）。

   視乎您要使用哪些因素來在多因素驗證 (MFA) 環境中驗證使用者，選取對應的驗證通訊協定：

   - 使用者名稱、密碼與推送（自動觸發頻外要求）：所有驗證通訊協定均支援
   - 推送、密碼、權杖以及 **PIN** 碼（密碼、權杖或 **PIN** 同時提供時）：PAP、採用 GTC 的 PEAP 以及採用 PAP 的 EAP-TTLS 均支援
   - 使用者名稱、密碼、權杖、**PIN** 碼及挑戰回應（密碼、權杖或 **PIN** 碼同時提供時）：PAP 以及採用 GTC 的 PEAP 均支援

   如果您選取 EAP 驗證方法（PEAP-MSCHAPv2、採用 GTC 的 PEAP 或者採用 PAP 的 EAP-TTLS），請確認 RADIUS 伺服器支援傳輸層安全性 (TLS) 1.1 或更高版本，而且 RADIUS 伺服器的根和中繼憑證授權單位 (CA) 包含在與 RADIUS 伺服器設定檔相關的憑

©2024 Palo Alto Networks, Inc.

證設定檔中。如果您選取 EAP 方法，而且未將正確設定的憑證設定檔與 RADIUS 設定檔進行關聯，則驗證會失敗。

7. **Add**（新增）每個 RADIUS 伺服器，然後輸入下列資訊：
   - 用來識別伺服器的 **Name**（名稱）
   - **RADIUS Server**（**RADIUS** 伺服器）IP 位址或 FQDN。如果您使用 FQDN 識別伺服器並隨後變更了位址，則必須要提交變更，以便新伺服器位址生效。
   - **Secret**（密碼）/**Confirm Secret**（確認密碼）是用於加密密碼的金鑰，最長可包含 64 個字元。
   - 用於驗證要求的伺服器 **Port**（連接埠）（預設值為 1812）
8. 按一下 **OK**（確定）來儲存伺服器設定檔。

對於備援，在防火牆要使用的順序中新增多個 RADIUS 伺服器。如果您已選取 EAP 方法，設定驗證順序，以確保使用者將能夠成功回應驗證挑戰。EAP 沒有替代驗證方法：如果使用者在驗證挑戰中失敗，而且您沒有設定允許另一種驗證方法的驗證順序，則驗證會失敗。

STEP 2 | 如果藉助 GlobalProtect 使用 PEAP-MSCHAPv2，請選取 **Allow users to change passwords after expiry**（允許使用者在過期後變更密碼），以允許 GlobalProtect 使用者變更過期密碼進行登入。

STEP 3 | （僅限 PEAP-MSCHAPv2、採用 GTC 的 PEAP 或者採用 PAP 的 EAP-TTLS） 若要在與伺服器進行驗證後建立的外部通道中匿名化使用者的識別資訊，請選取 **Make Outer Identity Anonymous**（匿名化外部識別）。

必須設定 *RADIUS* 伺服器，以便整個鏈結允許匿名使用者進行存取。有些 *RADIUS* 伺服器設定也許無法支援匿名的外部 *ID*，且您也許需要清除此選項。清除後，*RADIUS* 伺服器以純文字傳輸使用者名稱。

STEP 4 | 如果您選取 EAP 驗證方法，請選取憑證設定檔。

©2024 Palo Alto Networks, Inc.

STEP 5 | 將 RADIUS 伺服器設定檔指派給驗證設定檔。

驗證設定檔定義了一組使用者共用的驗證設定。

1. 選取 **Device**（裝置） > **Authentication Profile**（驗證設定檔），然後 **Add**（新增） 設定檔。
2. 輸入用來識別驗證設定檔的 **Name**（名稱）。
3. 將 **Type**（類型）設為 **RADIUS**。
4. 選取您設定的 **Server Profile**（伺服器設定檔）。
5. 選取 **Retrieve user group from RADIUS**（從 **RADIUS** 擷取使用者群組），以從 RADIUS 伺服器上定義的 VSA 收集使用者群組資訊。

   防火牆將比對這些群組資訊與驗證設定檔的允許清單中指定的群組。
6. 選取 **Advanced**（進階），然後在允許清單中，**Add**（新增）允許使用此驗證設定檔進行驗證的使用者和群組。
7. 按一下 **OK**（確定）來儲存驗證設定檔。

STEP 6 | 將防火牆設定為針對所有管理員使用驗證設定檔。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理），然後編輯 Authentication Settings（驗證設定）。
2. 選取您所設定的 **Authentication Profile**（驗證設定檔），再按一下 **OK**（確定）。

STEP 7 | 設定角色和存取網域，定義管理員的授權設定。

如果您已在 RADIUS 伺服器上定義 RADIUS VSA，則您為防火牆上角色和存取網域指定的名稱必須與 VSA 值相符。

1. 如果管理員使用自訂角色而非預定義（動態）角色，則設定管理員角色設定檔。
2. 如果防火牆有一個以上的虛擬系統，則設定存取網域：
   1. 選取 **Device**（裝置） > **Access Domain**（存取網域），**Add**（新增） 並存取網域，然後輸入用於識別存取網域的 **Name**（名稱）。
   2. **Add**（新增）管理員將存取的每個虛擬系統，然後按一下 **OK**（確定）。

STEP 8 | **Commit**（提交）變更，以在防火牆上啟用。

©2024 Palo Alto Networks, Inc.

STEP 9 | 設定 RADIUS 伺服器以驗證和授權管理員。

關於執行下列步驟的特定說明，請參閱 RADIUS 伺服器文件：

1. 新增防火牆 IP 位址或主機名稱作為 RADIUS 用戶端。
2. 新增管理員帳戶。

   若 *RADIUS* 伺服器設定檔將 ***CHAP*** 指定為 ***Authentication Protocol***（驗證通訊協定），則您必須為帳戶定義可反轉的加密密碼。否則，*CHAP* 驗證將失敗。
3. 定義防火牆的廠商代碼 (25461)，然後分別為每個管理員的角色、存取網域和使用者群組定義 RADIUS VSA。

   當您預先定義使用者的動態管理員角色時，使用小寫字母指定角色（例如，輸入 **`superuser`**，而不是 **`SuperUser`**）。

   在 *ACS* 上設定進階廠商選項時，您必須將 ***Vendor Length Field Size***（廠商長度欄位大小）和 ***Vendor Type Field Size***（廠商類型欄位大小）設定為 ***1***。否則，驗證將失敗。
4. 如果您已選取 EAP 方法，防火牆會驗證伺服器而非用戶端。若要確保用戶端有效性，請透過 IP 位址或子網域限制用戶端。

STEP 10 | 確認 RADIUS 伺服器是否對管理員執行驗證和授權。

1. 使用您新增至 RADIUS 伺服器的管理員帳戶登入防火牆 Web 介面。
2. 確認您是否只能存取允許該管理員關聯的角色存取的 Web 介面頁面。
3. 在 **Monitor**（監控）、**Policies**（原則）和 **Objects**（物件）頁籤中，驗證您是否只能存取允許該管理員關聯的粗存取網域存取的虛擬系統。
4. 在 **Monitor**（監控） > **Authentication**（驗證）中，校驗 **Authentication Protocol**（驗證通訊協定）。
5. 使用以下 CLI 命令測試連線以及憑證設定檔的有效性：

```
admin@PA-220 > test authentication authentication-profile
 auth-profile username <username> password <password>
```


©2024 Palo Alto Networks, Inc.

設定 LDAP 驗證

您可以使用 LDAP 驗證透過驗證入口網站存取應用程式或服務的使用者，以及驗證存取 Web 介面的防火牆或 Panorama 管理員。

您還可以連線至 *LDAP* 伺服器，以根據使用者群組定義原則規則。詳細資訊，請參閱對應使用者到群組。

©2024 Palo Alto Networks, Inc.

STEP 1 | 新增 LDAP 伺服器設定檔。

設定檔定義了防火牆將採用何種方式連線 LDAP 伺服器。

1. 在 Panorama™ 上選擇 裝置 > 伺服器設定檔 > **LDAP** 或 **Panorama** > 伺服器設定檔 > **LDAP** 並 新增 伺服器設定檔。
2. 輸入用來識別伺服器設定檔的 **Profile Name**（設定檔名稱）。
3. （僅多重 vsys）選取設定檔可用的**Location**（位置）。
4. （選用）選取 **Administrator Use Only**（僅管理員使用）以將存取權限限制到管理員。
5. **Add**（新增）LDAP 伺服器（最多可新增四個）。對於每個伺服器，輸入 **Name**（名稱）（用於識別伺服器）、**LDAP Server**（**LDAP** 伺服器）IP 位址或 FQDN，以及伺服器 **Port**（連接埠）（預設值為 389）。

   如果您使用 *FQDN* 位址物件識別伺服器並隨後變更了位址，則必須要提交變更，以便新伺服器位址生效。
6. 選取伺服器 **Type**（類型）。
7. 選取 **Base DN**（基礎 **DN**）。

   識別您目錄 Base DN，打開**Active Directory Domains and Trusts**（主動式目錄網域與信任）Microsoft 管理控制台管理單元，並使用頂級網域名稱。
8. 輸入 **Bind DN**（繫結 **DN**）與 **Password**（密碼）以讓驗證服務能驗證防火牆。

   繫結 *DN* 賬號須具有讀取 *LDAP* 目錄的權限。
9. 輸入 **Bind Timeout**（繫結逾時）和**Search Timeout**（搜尋逾時），單位為秒（預設值均為 30）。
10. 輸入 **Retry Interval**（重試間隔）（秒）（預設值為 60）。
11. 啟用 **Require SSL/TLS secured connection**（要求 **SSL/TLS** 安全連線）選項（依預設啟用）。端點使用的協定視乎伺服器連接埠而定：
    - 389（預設）—TLS（特別是裝置會使用 StartTLS 操作，用來升級連接至 TLS 的初始純文字連線。）
    - 636—SSL
    - 任何其他連接埠—裝置首先會嘗試使用 TLS。若目錄伺服器不支援 TLS，則裝置會回復使用 SSL。
12. （選用）為了獲得額外的安全，請啟用 **Verify Server Certificate for SSL sessions**（確認 **SSL** 工作階段的伺服器憑證）選項，讓端點確認目錄伺服器為 SSL/TLS 連線所呈現的憑證。若要啟用驗證，您也必須啟用 **Require SSL/TLS secured connection**（要求 **SSL/TLS** 安全連線）選項。為了順利確認，憑證必須滿足以下條件之一：
    - 位於裝置憑證清單內：**Device**（設備）> **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Device Certificates**（設備憑證）。若有必要，將憑證匯入至裝置。

©2024 Palo Alto Networks, Inc.

- 憑證簽署者位於受信任的憑證授權單位清單中：**Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證） > **Default Trusted Certificate Authorities**（預設的受信任憑證授權單位）。

13. 按一下 **OK**（確定）來儲存伺服器設定檔。

STEP 2 | 指派伺服器設定檔以設定驗證設定檔或順序，以定義各種驗證設定。

STEP 3 | 將驗證設定檔指派給需要驗證的防火牆應用程式。

- **Web** 介面的管理存取權—設定防火牆管理員帳戶並指派您所設定的驗證設定檔。
- 使用者對服務和應用程式的存取權—關於設定使用者驗證的完整程序，請參閱設定驗證原則。

STEP 4 | 確認防火牆是否能夠測試驗證伺服器連線，以驗證使用者。

©2024 Palo Alto Networks, Inc.

驗證伺服器的連線逾時

您可以設定防火牆使用外部驗證服務，驗證存取防火牆或 Panorama 的管理員以及透過驗證入口網站存取服務或應用程式的使用者。為確保防火牆不會因不斷嘗試連線無法連線的驗證伺服器而浪費資源，您可以設定逾時間隔，超過此間隔後，防火牆將停止嘗試連線。在伺服器設定檔中設定逾時，定義防火牆連線驗證伺服器的方式。在選擇逾時值時，您的目標是實現節約防火牆資源與考量正常網路延遲（影響驗證伺服器回應防火牆的速度）之間的平衡。

- 關於設定驗證伺服器逾時的指引
- 修改 PAN-OS Web 伺服器逾時
- 修改驗證入口網站工作階段逾時

關於設定驗證伺服器逾時的指引

以下是一些關於為嘗試連線外部驗證服務的防火牆設定逾時的指引。

- 除了您在伺服器設定檔中為特定伺服器設定的逾時以外，防火牆還有一個全域 PAN-OS Web 伺服器逾時。當防火牆連線至任何外部伺服器以驗證對防火牆 Web 介面或 PAN-OS XML API 的管理存取以及驗證透過驗證入口網站存取應用程式或服務的使用者時，會套用此全域逾時。全域逾時預設為 30 秒（範圍為 3-125）。其值必須等於或大於任何伺服器設定檔允許嘗試連線的總時間。伺服器設定檔中的總時間等於逾時值乘以重試次數再乘以伺服器數。例如，如果某個 RADIUS 伺服器設定檔指定了 3 秒的逾時，重試了 3 次，有 4 個伺服器，則該設定檔允許嘗試連線的總時間為 36 秒 (3 x 3 x 4)。若有必要，修改 PAN-OS Web 伺服器逾時。

  除非驗證失敗，否則不要變更 *PAN-OS Web* 伺服器逾時值。將逾時值設定得過高，可能會降低防火牆的效能，或導致防火牆丟棄驗證要求。您可以檢閱驗證日誌中的驗證失敗資訊。

- 防火牆將套用驗證入口網站工作階段逾時設定，其中定義了使用者能有多長時間來回應驗證入口網站 Web 表單形式的驗證挑戰。當使用者要求與驗證原則規則相符的服務或應用程式時，會顯示此 Web 表單。該工作階段逾時預設為 30 秒（範圍為 1-599999）。其值必須等於或大於 PAN-OS Web 伺服器逾時值。如有必要，修改驗證入口網站工作階段逾時。請注意，增加 PAN-OS Web 伺服器和驗證入口網站工作階段逾時可能會降低防火牆效能，或導致防火牆丟棄驗證要求。

  驗證入口網站工作階段逾時與決定防火牆能將 *IP* 位址到使用者對應保留多長時間的計時器不相關。

- 在驗證順序中，逾時值將會累計。以具有兩個驗證設定檔的驗證順序為範例。一個驗證設定檔為 RADIUS 伺服器設定檔指定了 3 秒逾時、3 次重試和 4 個伺服器。另一個驗證設定檔為 TACACS+ 伺服器設定檔指定了 3 秒逾時和 2 個伺服器。防火牆可嘗試利用該驗證順序驗證使用者帳戶的最長時間為 42 秒：其中，RADIUS 伺服器設定檔為 36 秒，TACACS+ 伺服器設定檔為 6 秒。
- Kerberos 伺服器的逾時不可設定，Kerberos 伺服器設定檔中指定了每個伺服器的逾時為 17 秒。

©2024 Palo Alto Networks, Inc.

- 若要為其他類型伺服器設定逾時及相關設定，請參閱：
  - 新增 MFA 伺服器設定檔。
  - 新增 SAML IdP 伺服器設定檔。
  - 新增 TACACS+ 伺服器設定檔。
  - 新增 RADIUS 伺服器設定檔。
  - 新增 LDAP 伺服器設定檔。

修改 PAN-OS Web 伺服器逾時

PAN-OS Web 伺服器逾時必須等於或大於任何驗證伺服器設定檔中的逾時乘以重試次數再乘以該設定檔中的伺服器數目。

除非驗證失敗，否則不要變更 *PAN-OS Web* 伺服器逾時值。將逾時值設定得過高，可能會降低防火牆的效能，或導致防火牆丟棄驗證要求。您可以檢閱驗證日誌中的驗證失敗資訊。

STEP 1 | 存取防火牆 CLI。

STEP 2 | 透過輸入下列命令來設定 PAN-OS Web 伺服器逾時，其中 <*value*> 為秒數（預設值為 30；範圍為 3 到 125）。

```
> configure # set deviceconfig setting l3-service timeout <value>
 # commit
```

修改驗證入口網站工作階段逾時

驗證入口網站工作階段逾時必須等於或大於 PAN-OS Web 伺服器逾時。詳細資訊，請參閱驗證伺服器的連線逾時。

PAN-OS Web 伺服器和驗證入口網站工作階段的逾時愈高，驗證入口網站回應使用者的速度就愈慢。

STEP 1 | 選取 **Device**（裝置） > **Setup**（設定） > **Session**（工作階段），然後編輯 Session Timeouts（工作階段逾時）。

STEP 2 | 輸入新的 **Authentication Portal**（驗證入口網站） 值（單位為秒，預設值為 30；範圍為 1 至 1,599,999）然後按一下 **OK**（確定）。

STEP 3 | **Commit**（提交）您的變更。

©2024 Palo Alto Networks, Inc.

設定本機資料庫驗證

您可以設定屬於防火牆本機的使用者資料庫，驗證存取防火牆 Web 介面的管理員以及驗證透過驗證入口網站或 GlobalProtect 存取應用程式的一般使用者。執行下列步驟，設定使用本機資料庫的本機驗證。

外部驗證服務一般是本機驗證的首選，因為它們提供了集中管理帳戶的好處。

您還可以設定沒有資料庫的本機驗證，但僅適用於防火牆或 Panorama 管理員。

STEP 1 | 新增使用者帳戶到本機資料庫。

1. 選取 **Device**（裝置） > **Local User Database**（本機使用者資料庫） > **Users**（使用者），然後按一下 **Add**（新增）。
2. 輸入管理員的使用者 **Name**（名稱）。
3. 輸入 **Password**（密碼）並 **Confirm Password**（確認密碼）或輸入 **Password Hash**（確認密碼）。
4. **Enable**（啟用）帳戶（預設會啟用），然後按一下 **OK**（確定）。

STEP 2 | 新增使用者群組到本機資料庫。

如果您的使用者需要群組成員，則需設定。

1. 選取 **Device**（裝置） > **Local User Database**（本機使用者資料庫） > **User Groups**（使用者群組），然後按一下 **Add**（新增）。
2. 輸入用來識別群組的 **Name**（名稱）。
3. **Add**（新增）每一位群組成員使用者，然後按一下 **OK**（確定）。

STEP 3 | 設定驗證設定檔。

驗證設定檔定義了一組使用者共用的驗證設定。將驗證 **Type**（類型）設定為 **Local Database**（本機資料庫）。

STEP 4 | 將驗證設定檔指派給管理員帳戶或用戶的驗證原則規則。

- 管理員—設定防火牆管理員帳戶：

  指定您在此程序前期定義的使用者 **Name**（名稱）。

  指派您為帳戶設定的 **Authentication Profile**（驗證設定檔）。

- 使用者—關於設定使用者驗證的完整程序，請參閱設定驗證原則。

STEP 5 | 確認防火牆是否能夠測試驗證伺服器連線，以驗證使用者。

©2024 Palo Alto Networks, Inc.

設定驗證設定檔和順序

驗證設定檔定義了用於驗證以下管理員和使用者登入認證的驗證服務：存取防火牆 Web 介面的管理員和透過驗證入口網站或 GlobalProtect 存取應用程式的使用者。該服務可能是防火牆提供的本機驗證或者是外部驗證服務。驗證設定檔還定義了 Kerberos 單一登入 (SSO) 等選項。

一些網路針對不同使用者和使用者群組擁有多個資料庫（如 TACACS+ 和 LDAP）。要在此類情況下驗證使用者，需設定驗證順序—這是在登入期間，防火牆用於比對使用者的驗證設定檔的先後順序。防火牆將按順序對照每個設定檔檢查，直至成功驗證使用者。唯有當驗證順序中的所有設定檔皆驗證失敗時，才會拒絕使用者存取。該順序可以指定基於防火牆說支援之驗證服務的驗證設定檔，但多重要素驗證 (MFA) 和 SAML 除外。

STEP 1 | （僅限外部服務）啟用防火牆，以連線至用於驗證使用者的外部伺服器：

1. 設定外部伺服器。相關說明，請參閱伺服器的文件。
2. 為您使用的驗證服務類型設定伺服器設定檔。
   - 新增 RADIUS 伺服器設定檔。

     如果防火牆透過 *RADIUS* 整合 *MFA* 服務，則必須新增 *RADIUS* 伺服器設定檔。在此情況下，*MFA* 服務將提供所有驗證要素。若防火牆透過廠商 *API* 整合 *MFA* 服務，您仍可使用 *RADIUS* 伺服器作為第一個因素，但其他因素需要使用 *MFA* 伺服器設定檔。

   - 新增 MFA 伺服器設定檔。
   - 新增 SAML IdP 伺服器設定檔。
   - 新增 Kerberos 伺服器設定檔。
   - 新增 TACACS+ 伺服器設定檔。
   - 新增 LDAP 伺服器設定檔。

STEP 2 | （僅限本機資料庫驗證）設定屬於伺服器本機的使用者資料庫。

根據屬於防火牆本機的使用者識別身分存放區，為您要設定本機驗證的每個使用者和使用者群組執行下列步驟：

1. 新增使用者帳戶到本機資料庫。
2. （選用）新增使用者帳戶到本機資料庫。

STEP 3 | （僅限 Kerberos SSO）如果 Kerberos 單一登入 (SSO) 是主要驗證服務，則為防火牆建立一個 Kerberos 金鑰標籤。

建立 Kerberos 金鑰標籤。金鑰標籤是一個檔案，包含了防火牆的 Kerberos 帳戶資訊。您的網路必須有 Kerberos 基礎結構才能支援 Kerberos SSO。

©2024 Palo Alto Networks, Inc.

STEP 4 | 設定驗證設定檔。

定義下列之一或兩者：

- **Kerberos SSO**—防火牆會先嘗試 SSO 驗證。如果驗證失敗，再使用指定的驗證 **Type**（類型）。
- 外部驗證或本機資料庫驗證—防火牆會提示使用者輸入登入認證，並使用其外部服務或本機資料庫來驗證使用者。

1. 選取 **Device**（裝置） > **Authentication Profile**（驗證設定檔），然後 **Add**（新增） 驗證設定檔。
2. 輸入用來識別驗證設定檔的 **Name**（名稱）。
3. 選取驗證服務的 **Type**（類型）。
   - 如果您使用多重要素驗證，則所選的類型僅適用於第一個驗證要素。您需要在 **Factors**（要素）頁籤中，為其他 MFA 要素選取服務。
   - 如果您選取 **RADIUS**、**TACACS+**、**LDAP** 或 **Kerberos**，則選取 **Server Profile**（伺服器設定檔）。
   - 如果您選取 **LDAP**，則選取 **Server Profile**（伺服器設定檔），然後定義 **Login Attribute**（登入屬性）。針對 Active Directory，請輸入 **sAMAccountName** 作為值。
   - 如果您選取 **SAML**，則選取 **IdP Server Profile**（**IdP** 伺服器設定檔）。
   - 如果您選取 **Cloud Authentication Service**（雲端驗證服務），請設定雲端識別引擎執行個體與防火牆進行通訊。有關雲端識別引擎的更多資訊，請參閱雲端識別引擎入門指南。
4. 如果您想啟用 Kerberos SSO，請輸入 **Kerberos Realm**（**Kerberos** 領域）（通常為使用者的 DNS 網域，但領域為大寫時除外），並 **Import**（匯入）您為防火牆或 Panorama 建立的 **Kerberos Keytab**（**Kerberos** 金鑰標籤）。
5. （僅限 MFA）選取 **Factors**（要素）、**Enable Additional Authentication Factors**（啟用其他驗證要素），然後 **Add**（新增）您說設定的 MFA 伺服器設定檔。

   防火牆將按照所列順序，從上到下地叫用每個 MFA 服務。
6. 選取 **Advanced**（進階），然後 **Add**（新增）可使用此設定檔驗證的使用者及群組。

   您可以從本機資料庫選取使用者及群組，或者，如果您已設定防火牆對應使用者到群組，從 Active Directory 等基於 LDAP 的目錄服務進行選取。依預設，清單為空，表示使用者無法進行驗證。

   您還可以選取群組對應設定中定義的指定群組。
7. （選用）若要在防火牆向伺服器傳送驗證請求之前修改使用者資訊， 請設定 **Username Modifier**（使用者名稱修改程式）。
   - **%USERDOMAIN%\%USERINPUT%**—如果來源不包含網域（例如，其使用 sAMAccountName），則防火牆會在使用者名稱之前新增您指定的 **User Domain**（使用者網域）。如果來源包含網域，則防火牆會用 **User Domain**（使用者網域）取代該網

©2024 Palo Alto Networks, Inc.

域。如果 **User Domain**（使用者網域） 為空，則防火牆會在傳送請求至驗證伺服器之前，在從來源收到的使用者資訊中移除網域。

LDAP 伺服器不支援在 *sAMAccountName* 中使用反斜線，因此請勿使用此選項對 *LDAP* 伺服器進行驗證。

- **%USERINPUT%**—（預設）防火牆將使用者資訊以從來源收到時的格式傳送至驗證伺服器。
- **%USERINPUT%@%USERDOMAIN%**—如果來源不包含網域，則防火牆會在使用者名稱之後新增 **User Domain**（使用者網域）值。如果來源包含網域，則防火牆會用 **User Domain**（使用者網域）值取代該網域。如果 **User Domain**（使用者網域） 為空，則防火牆會在傳送請求至驗證伺服器之前，在從來源收到的使用者資訊中移除網域。
- 無—如果您手動輸入 **None**（無）：
  - 對於 LDAP 和 Kerberos 伺服器設定檔，防火牆將使用從來源收到的網域選取合適的驗證設定檔，然後在傳送驗證請求至伺服器時移除此網域。這讓您可以在驗證順序中包含 **User Domain**（使用者網域），但在防火牆傳送驗證請求至伺服器之前移除此網域。例如，如果您使用 LDAP 伺服器設定檔且 samAccountName 作為屬性，須使用此選項，確保防火牆不會傳送網域至只需要使用者名稱而不需要網域的驗證伺服器。
  - 對於 RADIUS 伺服器設定檔：
    - 如果來源以 **domain\username** 格式傳送使用者資訊，防火牆將以相同格式傳送使用者資訊至伺服器。
    - 如果來源以 **username@domain** 格式傳送使用者資訊，防火牆會將使用者資訊標準化為 **domain\username** 格式，然後再將其傳送至伺服器。
    - 如果來源僅傳送使用者名稱，防火牆會新增您指定的 **User Domain**（使用者網域），然後再以 **domain\username** 格式將資訊傳送至伺服器。
  - 對於本機資料庫、TACACS+ 和 SAML，防火牆會將使用者資訊以從來源收到時的格式傳送至驗證伺服器。

8. 按一下 **OK**（確定）來儲存驗證設定檔。

©2024 Palo Alto Networks, Inc.

STEP 5 | 設定驗證順序。

如果您希望防火牆嘗試使用多個驗證設定檔來驗證使用者，則需要執行此步驟。防火牆將按從上到下的順序評估設定檔，直到某個設定檔成功驗證使用者。

1. 選取 **Device**（裝置） > **Authentication Sequence**（驗證順序），然後 **Add**（新增） 驗證順序。
2. 輸入用來識別驗證順序的 **Name**（名稱）。

   （選用但推薦）若要加速驗證程序，可 ***Use domain to determine authentication profile***（使用網域決定驗證設定檔）：防火牆會將使用者在登入期間輸入的網域名稱與序列中的驗證設定檔進行比對，然後使用該設定檔驗證使用者。如果防火牆找不到符合項目，或者如果您停用該選項，則防火牆會依從上到下的順序嘗試用設定檔進行驗證。
3. （選用但推薦）為了加快驗證過程並避免在不需要時執行整個驗證序列所帶來的計算負載，您可以讓防火牆 **Exit the sequence on failed authentication**（驗證失敗時退出序列）。當您選擇此選項時，如果使用者在登入時輸入的網域名稱與驗證序列中的任何驗證設定檔中的網域名稱（無論是否標準化）匹配，但驗證過程不成功（例如，無法識別密碼或使用者名稱），則防火牆將停止驗證序列。

   僅當防火牆將網域名稱與序列中的驗證設定檔匹配時，此選項才適用。
4. （選用但推薦）要在套用驗證序列之前標準化使用者在登入期間輸入的網域名稱，請選擇 **Use User-ID domain to determine authentication profile**（使用 **User-ID** 網域決定驗證設定檔）。如果不選擇此選項，則在套用驗證設定檔序列之前，防火牆不會標準化使用者在登入期間輸入的網域名稱。
5. **Add**（新增）驗證設定檔。若要變更設定檔的評估順序，請選取設定檔，並按一下 **Move Up**（上移）或 **Move Down**（下移）。
6. 按一下 **OK**（下移）以儲存驗證順序。

STEP 6 | 將驗證設定檔或順序指派給防火牆管理員的管理帳戶，或指派給使用者驗證原則。

- 管理員—根據管理管理員授權的方式指派驗證設定檔：

  在防火牆上本機管理授權—設定防火牆管理員帳戶。

  SAML、TACACS+ 或 RADIUS 伺服器上受管理的授權—選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理），編輯 Authentication Settings（驗證設定），然後選取 **Authentication Profile**（驗證設定檔）。
- 使用者—關於設定使用者驗證的完整程序，請參閱設定驗證原則。

STEP 7 | 確認防火牆是否能夠測試驗證伺服器連線，以驗證使用者。

©2024 Palo Alto Networks, Inc.

測試驗證伺服器連線

測試驗證功能可以讓您確認防火牆或 Panorama 是否能與驗證設定檔中指定的驗證伺服器通訊、特定使用者的驗證要求是否能成功。您可以測試用於驗證存取 Web 介面的管理員或驗證透過 GlobalProtect 或驗證入口網站存取應用程式的使用者的驗證設定檔。您可以對侯選組態執行驗證測試，以在提交之前驗證組態是否正確。

STEP 1 | 設定驗證設定檔。您無需在測試之前提交驗證設定檔或伺服器設定檔組態。

STEP 2 | 登入防火牆 CLI。

STEP 3 | （多虛擬系統防火牆）定義測試命令將存取的目標虛擬系統。

在多虛擬系統防火牆上需要執行此操作，以便測試驗證命令能夠定位您要測試的使用者。

輸入下列名稱，定義目標虛擬系統：

```
admin@PA-325060> set system setting target-vsys <vsys-name>
```

例如，如果使用者是在 vsys2 中定義，則輸入：

```
admin@PA-3250> set system setting target-vsys vsys2
```

target-vsys 選項視乎於登入工作階段，因此當您登出時，系統會清除此選項。

STEP 4 | 輸入下列命令以測試驗證設定檔：

```
admin@PA-3250> test authentication authentication-
profile <authentication-profile-name> username <username> password
```

例如，若要為名稱為 **bsimpson** 之使用者測試名稱為 **my-profile** 的驗證設定檔，則輸入：

```
admin@PA-3250> test authentication authentication-profile my-
profile username bsimpson password
```

在執行 ***test*** 命令時，驗證設定檔和伺服器設定檔的名稱均區分大小寫。此外，如果驗證設定檔已定義使用者名稱修改程式，您必須輸入此使用者名稱的修改程式。例如，如果您為名為 ***bsimpson*** 的使用者新增使用者名稱修改程式 ***%USERINPUT%@%USERDOMAIN%***，且網域名稱為 ***mydomain.com***，請輸入 ***bsimpson@mydomain.com*** 作為使用者名稱。這可以確保防火牆向驗證伺服器傳送正確的認證。在此範例中，*mydomain.com* 為您在驗證設定檔中的 ***User Domain***（使用者網域）欄位中定義的網域。

©2024 Palo Alto Networks, Inc.

STEP 5 | 檢視測試輸出。

如果已正確設定驗證設定檔，輸出會顯示 `Authentication succeeded`。如果有設定問題，輸出會顯示協助您疑難排解設定的資訊。

輸出結果會根據與您要測試之驗證類型以及問題的類型相關的多個因素而有所不同。例如，*RADIUS* 與 *TACACS+* 使用不同的基礎程式庫，因此針對這兩種類型存在的相同問題將產生不同的錯誤。此外，如果有網路問題，例如在驗證伺服器設定檔中使用錯誤的連接埠或 *IP* 位址，輸出錯誤並非特有。這是因為測試命令無法在防火牆與驗證伺服器之間執行初始交握，以決定關於問題的詳細資訊。

©2024 Palo Alto Networks, Inc.

驗證原則

驗證原則讓您可在使用者可以存取服務和應用程式之前驗證他們。每當使用者要求服務或資源時（例如造訪網頁時），防火牆就會評估驗證原則。根據相符的驗證原則規則，防火牆接下來會提示使用者使用一種或多種方式（因素）進行驗證，例如登入和密碼、語音、簡訊、推送，或一次性密碼 (OTP) 驗證。對於第一個因素，使用者將透過驗證入口網站 Web 表單進行驗證。對於其他因素，使用者將透過多因素驗證 (MFA) 登入頁面進行驗證。

若要為 *GlobalProtect* 實作驗證原則，請參閱設定 GlobalProtect 以協作多因素驗證通知。

使用者驗證所有因素後，防火牆將評估安全性原則，以確定是否允許存取服務或應用程式。

為了降低中斷使用者工作流程的驗證問題的發生頻率，您可以指定一個逾時期間，在此期間內，使用者僅針對首次存取服務和應用程式進行驗證，而不針對以後的存取進行驗證。驗證原則將與驗證入口網站整合，以記錄時間戳記，從而評估逾時並啟用基於使用者的原則和報告。

根據防火牆在驗證期間收集的使用者資訊，User-ID（使用者 ID）將建立一個新的 IP 位址到使用者名稱的對應，或者為該使用者更新現有的對應（如果對應資訊已變更）。防火牆將產生 User-ID（使用者 ID），以記錄新增和更新。防火牆還將為每個與驗證規則相符的要求產生驗證日誌。如果想執行集中監控，可根據 User-ID（使用者 Id）或驗證日誌建立報告，並向任何其他日誌類型一樣，將日誌轉送至 Panorama 或外部服務。

- 驗證時間戳記
- 設定驗證原則

驗證時間戳記

在設定驗證原則規則時，您可以指定一個逾時期間，在此期間內，使用者僅針對首次存取服務和應用程式進行驗證，而不針對以後的存取進行驗證。您的目標是指定一個逾時設定，使對安全服務和應用程式的需求以及減少使用者工作流程中斷次數的需求達到平衡。在使用者進行驗證時，防火牆將記錄首個驗證挑戰（因素）的時間戳記和任何其他多因素驗證 (MFA) 因素的時間戳記。在使用者後續請求與驗證原則相符的服務和應用程式時，防火牆將評估與每個時間戳記相關的規則中指定的逾時。這意味著在逾時過後，防火牆將重新為每個因素簽發驗證挑戰。如果您重新散佈使用者對應和驗證時間戳記，所有防火牆將對所有使用者一致地執行驗證原則逾時設定。

防火牆將單獨記錄每個 *MFA* 廠商的時間戳記。例如，如果您使用 Duo v2 和 *PingID* 伺服器簽發 *MFA* 因素挑戰，防火牆將為針對 *Duo* 因素的回應記錄一個時間戳記，並為針對 *PingID* 因素的回應記錄一個時間戳記。

在逾時期間內，成功驗證通過一項驗證規則的使用者可存取其他規則保護的服務或應用程式。但是，這僅適用於會觸發相同驗證因素的規則。例如，成功驗證通過觸發 TACACS+ 驗證的使用者必須要再次驗證通過觸發 SAML 驗證的規則，即使存取要求在這兩項規則的逾時期間內。

在評估每項驗證規則中的逾時設定以及驗證入口網站設定中定義的全域計時器時（請參閱設定驗證入口網站），防火牆將提示使用者針對先過期的設定進行重新驗證。在重新驗證時，防火牆將記錄

©2024 Palo Alto Networks, Inc.

規則的最新驗證時間戳記，並重設驗證入口網站計時器的時間計數。因此，為了對不同驗證規則啟用不同的逾時期間，需將驗證入口網站計時器設定為大於或等於任意規則內逾時設定的值。

設定驗證原則

執行下列步驟，為透過驗證入口網站存取服務的使用者設定驗證原則。開始前，確保您的安全性原則允許使用者存取需要驗證的服務和 URL 類別。

在設定驗證政策規則之前，確保您瞭解 IPv4 位址集會被視為 IPv6 位址集的子集，原則中對此進行了詳細說明。

STEP 1 | 設定驗證入口網站。若您使用多重要素驗證 (MFA) 服務驗證使用者，則必須將 **Mode**（模式）設定為 **Redirect**（重新導向）。

STEP 2 | 設定防火牆使用以下任何服務來驗證使用者。

- 外部驗證服務—設定伺服器設定檔，以定義防火牆連線至服務的方式。
- 本機資料庫驗證—將每一個使用者帳戶新增至防火牆上的本機使用者資料庫。
- Kerberos 單一登入 (SSO)—為防火牆建立 Kerberos 金鑰標籤。您可以設定防火牆將 Kerberos SSO 用作主要驗證服務，如果 SSO 失敗，再使用外部服務或本機資料庫驗證。

STEP 3 | 為每一組需要使用相同驗證服務和設定的使用者和驗證原則規則設定驗證設定檔和順序。

選取驗證服務的 **Type**（類型）和相關設定：

- 外部服務—選取外部伺服器的 **Type**（類型），然後選取您為其建立的 **Server Profile**（伺服器組態）。
- 本機資料庫驗證—將 **Type**（類型）設定為 **Local Database**（本機資料庫）。在 **Advanced**（進階）設定中，**Add**（新增）您所建立的驗證入口網站使用者和使用者群組。
- **Kerberos SSO**—指定 **Kerberos Realm**（**Kerberos** 領域），然後 **Import**（匯入）**Kerberos Keytab**（**Kerberos** 金鑰標籤）。

©2024 Palo Alto Networks, Inc.

STEP 4 | 設定驗證強制物件。

該物件會將每個驗證設定檔與一種驗證入口網站方法關聯。該方法決定了第一個驗證挑戰（因素）是透明還是需要使用者回應。

1. 選取 **Objects**（物件） > **Authentication**（驗證），然後 **Add**（新增） 物件。
2. 輸入 **Name**（名稱）來識別物件。
3. 為您在驗證設定檔中指定的驗證服務 **Type**（類型）選取 **Authentication Method**（驗證方法）：
   - 瀏覽器挑戰—如果您希望用戶端瀏覽器回應第一個驗證要素而不是讓使用者輸入登入認證，則選取此方法。對於此方法，您必須在驗證設定檔中設定 Kerberos SSO。如果瀏覽器挑戰失敗，防火牆再使用 **web-form**（**Web** 表單）方法。
   - **Web** 表單—如果您希望防火牆向使用者顯示驗證入口網站 Web 表單以輸入登入認證，則選取此方法。
4. 選取您設定的 **Authentication Profile**（驗證設定檔）。
5. 輸入驗證入口網站 Web 表單為提示使用者針對第一個驗證要素進行驗證而顯示的 **Message**（訊息）。
6. 按一下 **OK**（確定）儲存物件。

©2024 Palo Alto Networks, Inc.

STEP 5 | 設定驗證原則規則。

為每一組需要使用相同驗證服務和設定的使用者、服務和 URL 類別建立一個規則。

如果您的驗證原則使用預設的驗證強制物件（如 ***default-browser-challenge***），則防火牆不會套用驗證入口網站逾時。如需要求使用者在驗證入口網站逾時後重新進行驗證，請複製預設驗證物件的規則，並將其移到預設驗證物件的現有規則之前。

1. 選取 **Policies**（原則） > **Authentication**（驗證），然後 **Add**（新增） 規則。
2. 輸入用來識別規則的 **Name**（名稱）。
3. 選取 **Source**（來源），**Add**（新增）特定的區域和 IP 位址，或選取 **Any**（任何）區域或 IP 位址。

   該規則將僅套用於來自於特定 IP 位址或來自於特定區域中介面的流量。
4. 選取 **User**（使用者），然後選取或 **Add**（新增）將套用該規則的來源使用者和使用者群組（預設值為 **any**（任何））。
5. 選取或 **Add**（新增）將套用該規則的 Host Information Profiles（主機資訊設定檔）（預設值為 **any**（任何））。
6. 選取 **Destination**（目的地），**Add**（新增）特定的區域和 IP 位址，或選取 **Any**（任何）區域或 IP 位址。

   這些 IP 位址可以是您要控制存取的資源（例如伺服器）。
7. 選取 **Service/URL Category**（服務/**URL** 類別），然後選取或 **Add**（新增）規則將控制存取的 services and service groups（服務和服務群組）（預設值為 **service-http**）。
8. 選取或 **Add**（新增）規則將控制存取的 URL 類別（預設值為 **any**（任何））。例如，您可以建立自訂 URL 類別，指定最敏感的內部網站。
9. 選取 **Actions**（動作），然後選取您所建立的 **Authentication Enforcement**（驗證強制）物件。
10. 指定 **Timeout**（逾時）期間（以分鐘為單位，預設值為 60），在此期間內防火牆僅提示使用者驗證一次，以便於重複存取服務和應用程式。

    Timeout（逾時）是更嚴格的安全性（兩次出現驗證提示的間隔時間較短）與使用者體驗（兩次出現驗證提示的間隔時間較長）之間的權衡。存取重要系統以及敏感區域（如資料中心）時，通常需要進行更為頻繁的驗證。對於網路周邊以及那些使用者體驗對其至關重要的企業而言，進行驗證的頻率通常較低。
11. 按一下 **OK**（確定）來儲存規則。

STEP 6 | （僅限 MFA ）指定 MFA 登入頁面。

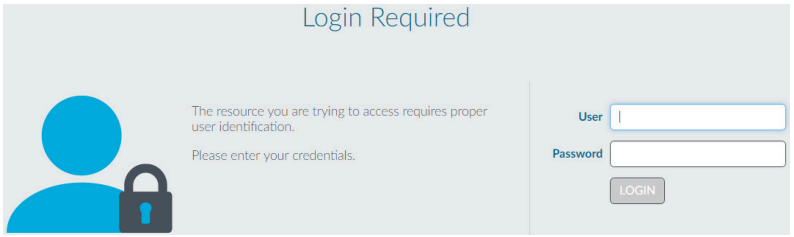
防火牆將顯示此頁面，以便使用者可驗證任何其他 MFA 要素。

 ©2024 Palo Alto Networks, Inc.

STEP 7 | 驗證防火牆是否執行驗證原則。

1. 以您在驗證原則規則中指定的一個來源使用者的身分登入網路。
2. 要求與規則中指定的服務或 URL 類別相符的服務或 URL 類別。

   防火牆將顯示第一個驗證因素的驗證入口網站 Web 表單。例如：



   如果您已設定防火牆使用一個或多個 *MFA* 服務，將驗證其他驗證要素。

3. 結束您所存取之服務或 URL 的工作階段。
4. 對相同的服務或應用程式啟動新工作階段。務必在您於驗證規則中設定的 **Timeout**（逾時）期間內執行此步驟。

   防火牆將允許存取，無需重新驗證。
5. 等待 **Timeout**（逾時）期間過期，然後要求相同的服務或引用程式。

   防火牆將提示您重新驗證。

STEP 8 | （選用）重新散佈資料和驗證時間戳記 到其他執行驗證政策的防火牆，以確保它們對所有使用者一致地套用逾時設定。

©2024 Palo Alto Networks, Inc.

疑難排解驗證問題

當使用者無法對 Palo Alto Networks 防火牆或 Panorama 進行驗證，或驗證程序花費的時間比預期要長時，分析驗證相關資訊可協助您判斷導致失敗或延遲的原因是：

- 使用者行為—例如，使用者在輸入錯誤的認證後遭到鎖定，或大量使用者同時嘗試存取。
- 系統或網路問題—例如，驗證伺服器無法存取。
- 設定問題—例如，驗證設定檔的允許清單並未包含其應包含的所有使用者。

下列 CLI 命令會顯示可協助您疑難排解這些問題的資訊：

工作	命令
顯示與驗證設定檔 (**auth-profile**)、驗證順序 (**is-seq**) 或虛擬系統 (**vsys**) 相關聯的鎖定使用者帳戶數。 若要解鎖使用者，請使用下列命令： **> request authentication [unlock-admin | unlock-user]**	**PA-220> show authentication locked-users { vsys <value> | auth-profile <value> | is-seq {yes | no} {auth-profile | vsys} <value> }**
使用 **debug authentication** 命令可疑難排解驗證事件。 使用 **show** 選項可顯示驗證要求統計資料與目前偵錯層級： • **show** 可顯示驗證服務 (authd) 的目前偵錯層級。 • **show-active-requests** 可顯示對驗證要求、允許清單、鎖定使用者帳戶以及多因素驗證 (MFA) 要求的使用中檢查數。 • **show-pending-requests** 可顯示對驗證要求、允許清單、鎖定使用者帳戶以及 MFA 要求的擱置中檢查數。 • **connection-show** 可顯示所有驗證伺服器或特定通訊協定類型的驗證要求與回應統計資料。 使用 **connection-debug** 選項可啟用或停用驗證偵錯：	**PA-220> debug authentication { on {debug | dump | error | info | warn} | show | show-active-requests | show-pending-requests | connection-show | { connection-id | protocol-type { Kerberos connection-id <value> | LDAP connection-id <value> | RADIUS connection-id <value> | TACACS+ connection-id <value> | } connection-debug-on | { connection-id | debug-prefix | protocol-type { Kerberos connection-id <value> | LDAP connection-id <value> | RADIUS connection-id <value> | TACACS+ connection-id <value> | } connection-debug-off | { connection-id | protocol-type {**

©2024 Palo Alto Networks, Inc.

工作	命令
• 使用 **on** 選項可啟用對 authd 的偵錯，而使用 **off** 選項可予以停用。 • 使用 **connection-debug-on** 選項可啟用對所有驗證伺服器或特定通訊協定類型的偵錯，而使用 **connection-debug-off** 選項可予以停用。	**Kerberos connection-id <value> | LDAP connection-id <value> | RADIUS connection-id <value> | TACACS+ connection-id <value> | } connection-debug-on }**
測試連線以及憑證設定檔的有效性。	`PA-220> test authentication authentication-profile auth-profile username <username>password <password>`
使用 **Monitor**（監控） > **Logs**（日誌） > **Authentication**（驗證）中顯示的 **Authentication ID**（驗證 **ID**）疑難排解特定驗證。	`PA-220> grep <Authentication ID>`

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

憑證管理

下列主題說明 Palo Alto Networks® 防火牆及 Panorama 使用的各種金鑰與憑證，及其取得與管理方式：

金鑰與憑證

Palo Alto Networks 防火牆及 Panorama 使用數位憑證，在安全通訊工作階段中確保雙方之間的信任。各憑證均包含加密金鑰，用於將明文加密或將加密文字解密。各憑證也包含數位簽章，以驗證簽發者的識別。簽發者必須列在驗證方的受信任憑證授權單位 (CA) 清單中。驗證方可選擇性地驗證簽發者是否未撤銷憑證（請參閱憑證撤銷）。

Palo Alto Networks 防火牆及 Panorama 將於下列應用程式中使用憑證：

- 驗證入口網站的使用者驗證、多因素驗證 (MFA) 及防火牆或 Panorama 的 Web 介面存取。
- 驗證 GlobalProtect VPN（遠端使用者對站點或大規模）的裝置。
- 使用網際網路金鑰交換 (IKE) 驗證 IPSec 站點對站點 VPN 的裝置。
- 外部動態清單 (EDL) 驗證。
- User-ID 代理程式與 TS 代理程式存取。
- 將輸入與輸出 SSL 流量解密。

  防火牆會將流量解密以套用原則規則，重新加密後再將流量轉送到最後目的地。對於輸出流量，防火牆會作為正向 Proxy 伺服器，向目的地伺服器建立 SSL/TLS 連線。防火牆為保護本身與用戶端之間的連線安全，因此使用簽署憑證自動產生目的地伺服器憑證的複本。

下表說明　Palo Alto Networks 防火牆及 Panorama 使用的金鑰與憑證。最佳做法是針對每種用途使用不同的金鑰與憑證。

表 **1: Palo Alto Networks** 裝置金鑰**/**憑證

金鑰/憑證用途	說明
管理存取權	如需安全地存取防火牆或 Panorama 管理介面（透過 HTTPS 存取 Web 介面），必須有 MGT 介面的伺服器憑證（如果防火牆或 Panorama 未使用 MGT，則須在資料面板上使用指定的介面），並選擇性地使用憑證驗證管理員。
驗證入口網站	在使用驗證原則識別存取 HTTPS 資源之使用者的部署中，為驗證入口網站介面指定伺服器憑證。如果您設定驗證入口網站以使用憑證來驗證使用者（代替互動式驗證或除了互動式驗證之外），則還要部署用戶端憑證。如需驗證入口網站的詳細資訊，請參閱使用驗證入口網站對應 IP 位址到使用者名稱。
轉送信任	對於輸出 SSL/TLS 流量，如果作為正向 Proxy 的防火牆信任簽署目的地伺服器憑證的 CA，則防火牆會使用轉送信任 CA 憑證來產生要對用戶端出示的目的地伺服器憑證複本。若要設定私密金鑰大小，請參閱設定 Ssl 正向 Proxy 伺服器憑證的金鑰大小。為了增加安全性，可將金鑰存

©2024 Palo Alto Networks, Inc.

金鑰/憑證用途	說明
	放在硬體安全性模組中（詳細資訊，請參閱使用硬體安全性模組保護金鑰）。
轉送不信任	對於輸出 SSL/TLS 流量，如果作為正向 Proxy 的防火牆不信任簽署目的地伺服器憑證的 CA，則防火牆會使用轉送不信任 CA 憑證來產生要對用戶端顯示的目的地伺服器憑證複本。
SSL 輸入檢查	此類金鑰會將輸入 SSL/TLS 流量解密以進行檢查與執行原則。針對此應用程式，請為每個要進行 SSL/TLS 輸入檢查的伺服器，將其私密金鑰匯入防火牆。請參閱設定 SSL 輸入檢查。 從 *PAN-OS 8.0* 開始，防火牆將使用橢圓曲線 *Diffie-Hellman* 暫時 *(ECDHE)* 算法執行嚴格的憑證檢查。這意味著，若防火牆使用中繼憑證，則必須在升級至 *PAN-OS 8.0* 或更新版本後，將憑證從 *Web* 伺服器重新匯入至防火牆，並將伺服器憑證與中繼憑證合併（安裝鏈結憑證）。否則，憑證鏈中包含中繼憑證的 *SSL* 輸入檢查工作階段發生故障。若要安裝鏈結憑證： ***1.*** 在純文字編輯器（例如記事本）中開啟每個憑證 *(.cer)* 檔案。 ***2.*** 將每個憑證端對端貼至頂部的伺服器憑證，且包含下列簽署者。 ***3.*** 將檔案儲存為文字 *(.txt)* 或憑證 *(.cer)* 檔案（檔案名稱不能包含空格）。 ***4.*** 將合併（鏈結）後的憑證匯入到防火牆。
SSL 排除憑證	此類憑證適用於排除進行 SSL/TLS 解密的伺服器。例如，如果您啟用 SSL 解密功能，但您的網路中包含防火牆不應將其流量解密的伺服器 (例如人力資源系統的 Web 服務)，則請將對應的憑證匯入到防火牆上，並將憑證設定為「SSL 排除憑證」。請參閱解密排除項。
GlobalProtect	GlobalProtect 元件之間所有的互動都是透過 SSL/TLS 連線發生的。因此，在部署 GlobalProtect 的過程中，請為所有的 GlobalProtect 入口網站、閘道與 Mobile Security Manager 部署伺服器憑證。亦可選擇性地部署用於驗證使用者的憑證。

©2024 Palo Alto Networks, Inc.

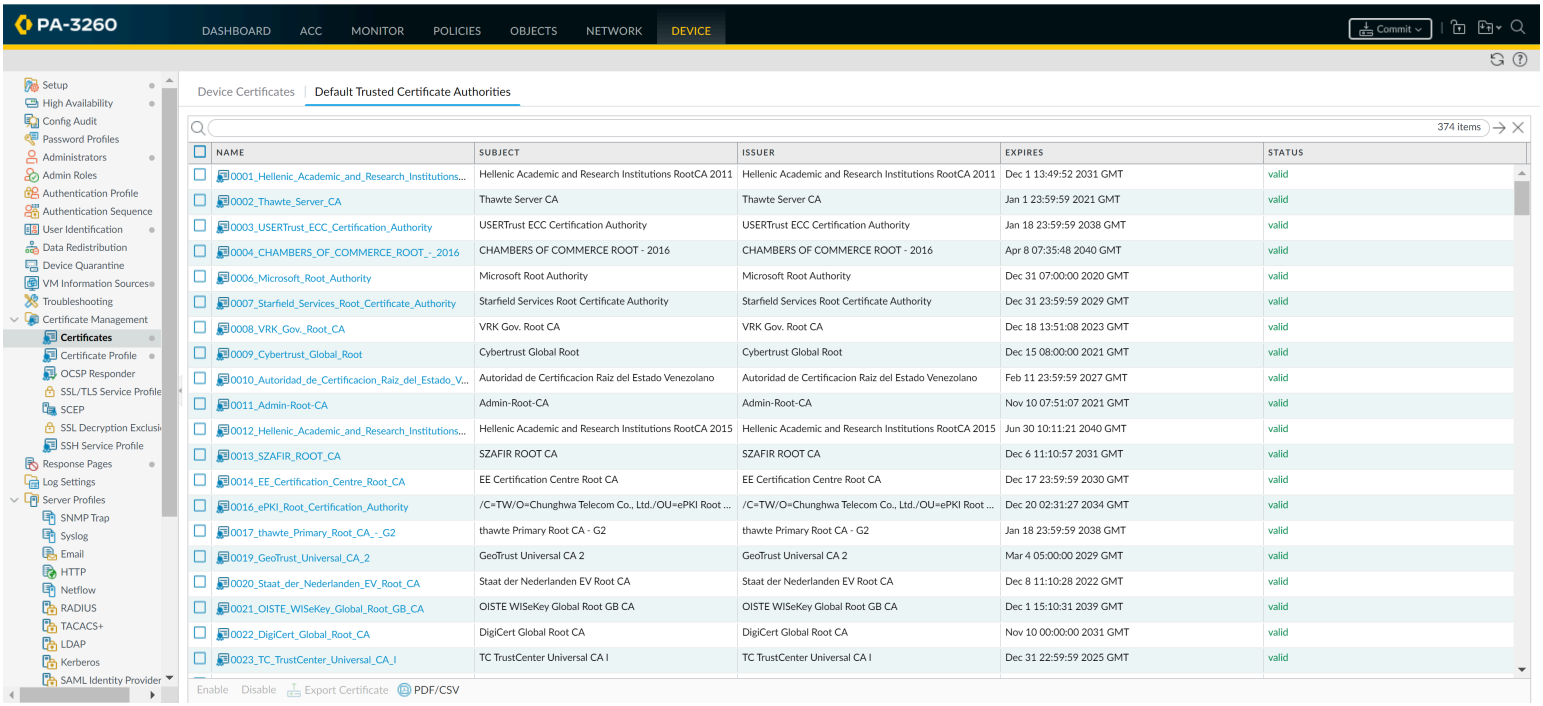
金鑰/憑證用途	說明
	GlobalProtect 大規模 VPN (LSVPN) 功能需要 *CA* 簽署的憑證。
站點對站點 VPN (IKE)	在站點對站點 IPSec VPN 部署中，對等裝置會使用網際網路金鑰交換 (IKE) 閘道建立安全通道。IKE 閘道使用憑證或預先共用的金鑰以互相驗證對等。憑證或金鑰請於定義防火牆的 IKE 閘道時設定與指派。請參閱站點對站點 VPN 概覽。
主要金鑰	防火牆使用主要金鑰加密所有的私密金鑰與密碼。如果您的網路需要一個存放私密金鑰的安全位置，您可以使用存放在硬體安全性模組 (HSM) 上的加密（封裝）金鑰將主要金鑰加密。如需詳細資訊，請參閱使用 HSM 加密主要金鑰。
安全 Syslog	此類憑證可讓防火牆與 Syslog 伺服器之間有安全的連線。請參閱 Syslog 欄位說明。
受信任的根 CA	指定由防火牆信任的 CA 簽發的根憑證。防火牆會使用自我簽署的根 CA 憑證自動簽發其他應用程式的憑證（例如 Ssl 正向 Proxy）。 此外，如果防火牆必須與其他防火牆之間建立安全連線，則簽發其憑證的根 CA 必須列在防火牆上受信任根 CA 的清單中。 （Panorama 管理的防火牆）CA 的 **Trusted Root CA**（受信任的根 **CA**）設定必須設定為範本組態設定的一部分，而不是範本堆疊組態設定的一部分。如果在範本堆疊組態設定過程中為 CA 設定 **Trusted Root CA**（受信任的根 **CA**）設定，則關聯的範本不會繼承 CA 的設定。
裝置間通訊	依預設，Panorama、防火牆及日誌收集器將使用一組預先定義的憑證進行用於管理和日誌轉送的 SSL/TLS 連線。但是，您可以透過將自訂憑證部署給其中裝置的方式增強這些連線。這些憑證還可用於保護 Panorama HA 對等體之間的 SSL/TLS 連線。

©2024 Palo Alto Networks, Inc.

預設受信任憑證授權單位 (CA)

依預設，防火牆信任最常見的以及受信任的授權單位 (CA)。這些受信任的憑證提供者負責簽發防火牆保護網際網路連線所需的憑證。

若要檢視並管理防火牆依預設信任的 CA 清單，可選取 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證） > **Default Trusted Certificate Authorities**（預設受信任憑證授權單位）：



您組織所需的受信任企業 CA 是您可能需額外新增的唯一一個 CA—請參閱取得憑證。

©2024 Palo Alto Networks, Inc.

憑證撤銷

Palo Alto Networks 防火牆及 Panorama 使用數位憑證，在安全通訊工作階段中確保雙方之間的信任。設定防火牆或 Panorama 檢查憑證的撤銷狀態，可提高安全性。某一方若出示的憑證已遭撤銷，則該方不值得信任。若憑證是憑證鏈結的一部分，防火牆或 Panorama 會檢查鏈結中根　CA 憑證外的每個憑證；其無法驗證根　CA 憑證的撤銷狀態。

有各種狀況會讓憑證在到期日前失效。例如名稱改變、主體與憑證授權單位間的關聯改變 (例如員工離職)，以及私密金鑰遭到洩露 (已知或疑似)。在上述狀況下，簽發該憑證的憑證授權單位必須撤銷憑證。

防火牆及 Panorama 支援下列驗證憑證撤銷狀態的方法。如果這兩種方法皆已設定，防火牆或 Panorama 會先嘗試　OCSP 方法；當　OCSP 伺服器無法使用時，才使用　CRL 方法。

- 憑證撤銷清單 (CRL)
- 線上憑證狀態通訊協定　(OCSP)
- 啟用 HTTP Proxy 以進行 OCSP 狀態檢查

在 *PAN-OS* 中，憑證撤銷狀態驗證屬於選用功能。最佳做法就是對憑證設定檔啟用此功能，憑證設定檔會為驗證入口網站、*GlobalProtect*、站台對站台 *IPSec VPN* 及防火牆或 *Panorama* 的網頁介面存取定義使用者與裝置驗證，以驗證憑證未被撤銷。

憑證撤銷清單 (CRL)

每個憑證授權單位 (CA) 都會定期簽發憑證撤銷清單 (CRL) 給公開儲存庫。CRL 會透過序號識別已撤銷的憑證。CA 撤銷憑證後，下一個 CRL 更新便會包含該憑證的序號。防火牆支援採用辨別編碼規則 (DER) 和隱私增強型郵件 (PEM) 格式的 CRL。

Palo Alto Networks 防火牆會為防火牆信任 CA 清單中所列的每個 CA 下載與快取最新簽發的 CRL。快取僅適用於經過驗證的憑證；如果防火牆從未驗證憑證，則防火牆快取不會存放簽發 CA 的 CRL。此外，快取只會存放未過期的 CRL。

如果您設定了多個 *CRL* 分佈點 *(CDP)* 且防火牆無法連接第一個 *CDP*，則防火牆不會檢查剩餘的 *CDP*。若要重新導向無效的 *CRL* 請求，請將 DNS Proxy 設定為替代伺服器。

若要使用 CRL 以驗證用於將輸入與輸出 SSL/TLS 流量解密之憑證的撤銷狀態，請參閱設定用於 SSL/TLS 解密的憑證撤銷狀態驗證。

對於驗證使用者與裝置所使用的憑證，若要使用 CRL 驗證該憑證的撤銷狀態，請設定憑證設定檔並指派給應用程式專有的介面：驗證入口網站、GlobalProtect（遠端使用者對站台或大規模）、站台對站台 IPSec VPN，或 Palo Alto Networks 防火牆或 Panorama 的網頁介面存取。詳細資訊，請參閱設定憑證的驗證撤銷狀態。

©2024 Palo Alto Networks, Inc.

線上憑證狀態通訊協定 (OCSP)

Palo Alto Networks 防火牆可以使用線上憑證狀態通訊協定 (OCSP) 檢查 X.509 數位憑證（SSL/TLS 憑證）的撤銷狀態。使用 OCSP 代替或補充 憑證撤銷清單 (CRL) 的好處是即時憑證狀態回應以及使用更少的網路和用戶端資源。

啟用使用 OCSP 驗證憑證後，防火牆會在建立 SSL/TLS 工作階段時驗證憑證的狀態。首先，驗證用戶端（防火牆）向 OCSP 回應程式（伺服器）傳送 OCSP 要求。該要求包括目標憑證的序號。接下來，OCSP 回應程式使用序號在簽發憑證之 CA 的資料庫中搜尋其撤銷狀態。然後，OCSP 回應程式將憑證狀態（`good`（良好）、`revoked`（已撤銷）或 `unknown`（未知））傳回到用戶端。防火牆會丟棄具有已撤銷憑證的工作階段。

如果您的網路部署包含 *Web Proxy*，則 *OCSP* 要求工作流程會有所不同。*OCSP* 要求和回應將先通過您的 *Proxy* 伺服器。啟用 HTTP Proxy 以進行 OCSP 狀態檢查的程序更詳細地描述了該工作流程。

Palo Alto Networks 防火牆為防火牆的受信任 CA 清單中的每個 CA 下載並快取 OCSP 回應。僅當防火牆已經驗證了憑證時，快取才會包含發證 CA 的 OCSP 回應。快取 OCSP 回應可加快回應時間並最大程度地減少前往回應程式的 OCSP 流量。

下列應用程式使用憑證驗證使用者和裝置：驗證入口網站、GlobalProtect（遠端使用者對站台或大規模）、站台對站台 IPSec VPN，和 Palo Alto Networks 防火牆或 Panorama 的網頁介面存取。要使用 OCSP 驗證對使用者和裝置進行驗證之憑證的撤銷狀態，請執行以下步驟：

如果您的防火牆用作 SSL 正向 Proxy，您將需要設定解密憑證撤銷設定。

- 設定 OCSP 回應程式。
- 啟用防火牆上的 HTTP OCSP 服務（如果您將防火牆設定為 OCSP 回應程式）。
- 建立或取得各應用程式的憑證。
- 為每個應用程式設定憑證設定檔。
- 將憑證設定檔指派給相關的應用程式。

要涵蓋 *OCSP* 回應程式無法使用的狀況，請將 *CRL* 設定為回復方法。詳細資訊，請參閱設定憑證的驗證撤銷狀態。

啟用 HTTP Proxy 以進行 OCSP 狀態檢查

如果您的網路部署包含 Web Proxy，您可以設定線上憑證狀態通訊協定 (OCSP) 來驗證憑證。所有 OCSP 要求和回應都將通過您的 Proxy 伺服器。使用 OCSP 代替或補充 憑證撤銷清單 (CRL) 檢查憑證狀態的好處包括即時狀態回應以及減少網路和用戶端資源的使用。

透過 Web Proxy 驗證 OCSP 憑證的工作流程如下：

1. 驗證用戶端（防火牆）將 OCSP 要求轉送給 Proxy。該要求包含用戶端要驗證的憑證的序號。
2. Proxy 驗證要求並識別頒發憑證的憑證授權單位 (CA) 的 OCSP 回應程式。

©2024 Palo Alto Networks, Inc.

3. Proxy 將 OCSP 要求轉送給回應程式，OCSP 回應者在 CA 資料庫中查找憑證的撤銷狀態。
4. OCSP 回應程式將憑證狀態（`good`（良好）、`revoked`（已撤銷）或 `unknown`（未知））傳送到 Proxy。
5. Proxy 將憑證狀態轉送給用戶端。

以下程序假定您尚未設定 *Web Proxy*。

STEP 1 | 設定 Proxy 伺服器。

1. 前往 **Device**（裝置） > **Setup**（設定） > **Services**（服務），然後編輯服務設定。
2. 編輯 Proxy 伺服器設定。
   - 對於 **Server**（伺服器），輸入 Proxy 伺服器的 IP 位址或主機名稱。
   - 輸入 **Port**（連接埠）。
   - 對於 **User**（使用者），輸入管理員輸入以用於存取 Proxy 伺服器的使用者名稱。
   - 輸入並確認管理員輸入以用於存取Proxy 伺服器的 **Password**（密碼）。

   您還可以使用以下 CLI 命令設定您的 Proxy 伺服器以進行 OCSP 狀態檢查（和 CRL 下載）。
   - **`set deviceconfig system secure-proxy-server <value>`**
   - **`set deviceconfig system secure-proxy-port <1-65535>`**
   - **`set deviceconfig system secure-proxy-user <value>`**
   - **`set deviceconfig system secure-proxy-password <value>`**

STEP 2 | 設定 OCSP 回應程式。

STEP 3 | https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/certificate-management/set-up-verification-for-certificate-revocation-status/configure-revocation-status-verification-of-certificates。

©2024 Palo Alto Networks, Inc.

憑證部署

部署 Palo Alto Networks 防火牆或 Panorama 憑證的最佳方法是：

- 從信任的協力廠商 **CA** 取得憑證—從 VeriSign 或 GoDaddy 等信任的協力廠商憑證簽發單位 (CA) 取得憑證的好處就是終端用戶端已經信任該憑證，因為常用的瀏覽器會在其信任根憑證存放區中包含知名 CA 的根 CA 憑證。因此，對於必須在終端用戶端與防火牆或 Panorama 間建立安全連線的應用程式而言，向終端用戶端信任的 CA 購買憑證可避免必須對終端用戶端預先部署根 CA 憑證的狀況。（如 GlobalProtect 入口網站或 GlobalProtect Mobile Security Manager 等都是此類應用程式。） 但大多數的協力廠商 CA 不會簽發簽署憑證。因此，這類憑證不適用於需要防火牆簽發憑證的應用程式 (例如 SSL/TLS 解密與大規模 VPN)。請參閱從外部 CA 取得憑證。
- 從企業 **CA** 取得憑證—有自己內部 CA 的企業可使用該 CA 簽發防火牆應用程式的憑證，並將這些憑證匯入到防火牆上。好處是終端用戶端或許已經信任企業　CA。您可以產生必要的憑證並匯入防火牆，或在防火牆產生 certificate signing request (憑證簽署要求，CSR) 並傳送至企業 CA 進行簽署。此方法的好處是私密金鑰不會離開防火牆。企業 CA 也可簽發簽署憑證，讓防火牆用來自動產生憑證 (例如為需要 SSL/TLS 解密的 GlobalProtect 大規模 VPN 或站台產生)。請參閱匯入憑證與私密金鑰。
- 產生自我簽署憑證—您可以在防火牆上建立自我簽署根 CA 憑證，並用來自動為其他防火牆應用程式簽發憑證。

如果您使用此方法為需要終端用戶端信任憑證的應用程式產生憑證，則一般使用者會看到發生憑證錯誤訊息，因為根 *CA* 憑證不在其信任根憑證存放區中。若要防止此狀況發生，請將自我簽署的根 *CA* 憑證部署到所有的一般使用者系統上。您可以手動部署憑證或使用中央部署方法，如 *Active Directory* 群組原則物件 *(GPO)*。

©2024 Palo Alto Networks, Inc.

設定憑證撤銷狀態驗證

為了驗證憑證的撤銷狀態，防火牆會使用線上憑證狀態通訊協定 (OCSP) 和/或憑證撤銷清單 (CRL)。如需這些方法的詳細資訊，請參閱憑證撤銷；如果這兩種方法您皆有設定，則防火牆會先嘗試 OCSP，如果 OCSP 回應程式無法使用，則僅會回復為 CRL 方法。如果貴企業有自己的公開金鑰基礎結構 (PKI)，就可以將防火牆設定成作為 OCSP 回應程式。

下列主題說明如何設定防火牆驗證憑證撤銷狀態：

- 設定 OCSP 回應程式
- 設定憑證的驗證撤銷狀態
- 設定用於 SSL/TLS 解密的憑證撤銷狀態驗證

設定 OCSP 回應程式

若要使用線上憑證狀態通訊協定 (OCSP) 來驗證憑證撤銷狀態，您必須設定防火牆存取 OCSP 回應程式（伺服器）。管理 OCSP 回應程式的實體可以是協力廠商憑證授權單位 (CA)。如果貴企業有自己的公開金鑰基礎結構 (PKI)，便可以使用外部 OCSP 回應程式或將防火牆本身設定為 OCSP 回應程式。關於 OCSP 的詳細資訊，請參閱撤銷憑證。

僅當您產生新憑證（***Device***（裝置） > ***Certificate Management***（憑證管理） > ***Certificates***（憑證））時，才設定 *OCSP* 回應程式 Certificate Profile（憑證設定檔）。在產生新憑證時指定 ***OCSP Responder***（***OCSP*** 回應程式），以便防火牆用適當的 *URL* 填充授權單位資訊存取 *(AIA)* 欄位，然後在憑證設定檔中指定新憑證。設定憑證設定檔不會覆寫現有憑證或 *Root CA* 的憑證設定檔。

您可以啟用 *OCSP* 驗證或覆寫 Certificate Profile（憑證設定檔）中憑證的 *AIA* 欄位。憑證設定檔設定確定對防火牆上託管之服務（如 *GlobalProtect*）進行驗證的憑證使用哪些憑證驗證機制。

©2024 Palo Alto Networks, Inc.

STEP 1 | 定義外部 OCSP 回應程式或將防火牆本身設定為 OCSP 回應程式。

1. 選取 **Device**（裝置） > **Certificate Management**（憑證管理） > **OCSP Responder**（**OCSP** 回應程式），再按一下 **Add**（新增）。
2. 輸入用來識別回應程式的 **Name**（名稱）（最多 31 個字元）。名稱區分大小寫。名稱必須是唯一的，且只能使用字母、數字、空格、連字號與底線。
3. 若防火牆具有一個以上的虛擬系統 (vsys)，為憑證選取一個 **Location**（位置）（vsys 或 **Shared**（共用））。
4. 在**Host Name**（主機名稱）欄位中，輸入 OCSP 回應程的主機名稱（建議）或 IP 位址。您可以輸入 IPv4 或 IPv6 位址。PAN-OS 會自動從這個值衍生出 URL 並新增至正在驗證的憑證。

   如果您將防火牆本身設為 OCSP 回應程式，則主機名稱必須解析成防火牆為 OCSP 服務所使用介面中的 IP 位址。
5. 按一下 **OK**（確定）。

STEP 2 | 如果希望防火牆使用 OCSP 回應程式介面的管理介面，請對防火牆啟用 OCSP 通訊。否則，請繼續執行下一步以設定替代介面。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Interfaces**（介面） > **Management**（管理）。
2. 在「網路服務」區段中，選取 **HTTP OCSP** 核取方塊，然後按一下 **OK**（確定）。

STEP 3 | 若要將替代介面用作 OCSP 回應程式介面，請將介面管理設定檔新增至用於 OCSP 服務的介面。

1. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **Interface Mgmt**（介面管理）。
2. 按一下新增以建立新的設定檔，或按一下現有設定檔的名稱。
3. 選取 **HTTP OCSP** 核取方塊，然後按一下確定。
4. 選取 **Network**（網路） > **Interfaces**（介面），然後按一下防火牆將用於 OCSP 服務的介面名稱。在步驟 1 中指定的 OCSP **Host Name**（主機名稱）必須解析為此介面中的 IP 位址。
5. 選取 **Advanced**（進階） > **Other info**（其他資訊），然後選取您設定的介面管理設定檔。
6. 按一下 **OK**（確定）與 **Commit**（提交）。

設定憑證的驗證撤銷狀態

防火牆及 Panorama 使用憑證為驗證入口網站、GlobalProtect、站台對站台 IPSec VPN 及防火牆/Panorama 的網頁介面存取等應用程式驗證使用者與裝置。若要提高安全性，最佳做法是設定防火牆或 Panorama 以驗證用於裝置/使用者驗證的憑證其撤銷狀態。

©2024 Palo Alto Networks, Inc.

STEP 1 | 為每個應用程式設定憑證設定檔。

將一或多個根 CA 憑證指派給該設定檔，然後選取防火牆驗證憑證撤銷狀態的方式。

關於各種應用程式所使用憑證的詳細資訊，請參閱金鑰與憑證

STEP 2 | 將憑證設定檔指派給相關的應用程式。

指派憑證設定檔的步驟會視需要憑證的應用程式而異。

設定用於 SSL/TLS 解密的憑證撤銷狀態驗證

防火牆解密輸入和輸出 SSL/TLS 流量以檢查流量中是否存在威脅。當您建立允許流量的安全性原則規則並將安全性設定檔套用至該規則時，請建立類似的解密原則規則以解密該流量。如果您沒有解密流量，防火牆將無法使用安全性設定檔檢查流量（您不能檢查看不到的內容）。防火牆在轉送流量前會重新加密流量。（請參閱 SSL 輸入檢查和 SSL 正向 Proxy。） 您可以設定防火牆驗證用於解密的憑證其撤銷狀態，如下所述。

啟用 *SSL/TLS* 解密憑證的撤銷狀態驗證會增加工作階段建立程序的時間。如果在工作階段逾時前未完成驗證，第一個存取站台的嘗試可能會失敗。基於這些原因，驗證預設為停用。

STEP 1 | 定義撤銷狀態要求的服務特定逾時間隔。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Session**（工作階段），然後在 Session Features（工作階段功能）區段中選取 **Decryption Certificate Revocation Settings**（解密憑證撤銷設定）。
2. 執行下列一或兩個步驟，這視防火牆要使用線上憑證狀態通訊協定 (OCSP) 或 憑證撤銷清單 (CRL) 方法來驗證憑證撤銷狀態而定。如果這兩種方法防火牆皆已使用，則會先嘗試 OCSP；如果 OCSP 回應程式無法使用，才會嘗試 CRL 方法。
   - 在 CRL 區段中，選取**Enable**（啟用）核取方塊，然後輸入**Receive Timeout**（接收逾時）。過了此間隔後 (1-60 秒)，防火牆會停止等待 CRL 服務的回應。
   - 在 OCSP 區段中，選取**Enable**（啟用）核取方塊，然後輸入**Receive Timeout**（接收逾時）。過了此間隔後 (1-60 秒)，防火牆會停止等待 OCSP 回應程式的回應。

   視您在步驟 2 中指定的 **Certificate Status Timeout**（憑證狀態逾時）值而定，防火牆可能會在上述一個或兩個 **Receive Timeout**（接收逾時）間隔過去之前註冊逾時。

©2024 Palo Alto Networks, Inc.

STEP 2 | 定義撤銷狀態要求的總逾時間隔。

輸入**Certificate Status Timeout**（憑證狀態逾時）。過了此間隔（1-60 秒）後，防火牆會停止等待任何憑證狀態服務的回應，並套用您選擇性在步驟 3 中定義的工作階段封鎖邏輯。**Certificate Status**（憑證狀態逾時）與 OCSP/CRL **Receive Timeout**（接收逾時）有關，如下所述：

- 如果您啟用 OCSP 與 CRL—在經過以下兩個間隔之中較短的間隔後，防火牆會註冊要求逾時：**Certificate Status Timeout**（憑證狀態逾時）值或兩個 **Receive Timeout**（接收逾時）值的彙總。
- 如果您僅啟用 OCSP—在經過以下兩個間隔之中較短的間隔後，防火牆會註冊要求逾時：**Certificate Status**（憑證狀態逾時）值或 OCSP **Receive Timeout**（接收逾時）值。
- 如果您僅啟用 CRL—在經過以下兩個間隔之中較短的間隔後，防火牆會註冊要求逾時：**Certificate Status Timeout**（憑證狀態逾時）值或 CRL **Receive Timeout**（接收逾時）值。

STEP 3 | 定義未知憑證狀態的封鎖行為，或定義撤銷要求逾時。

如果您想要防火牆在 OCSP 或 CRL 服務傳回未知的憑證撤銷狀態時封鎖 SSL/TLS 工作階段，請選取封鎖未知憑證狀態的工作階段核取方塊。否則，防火牆會繼續進行該工作階段。

如果您想要防火牆在註冊要求逾時後封鎖 SSL/TLS 工作階段，請選取封鎖憑證狀態檢查逾時的工作階段核取方塊。否則，防火牆會繼續進行該工作階段。

STEP 4 | 按一下 **OK**（確定）與 **Commit**（提交）。

©2024 Palo Alto Networks, Inc.

設定主要金鑰

每個防火牆和 Panorama 管理伺服器都會有一個預設的主要金鑰，用於加密組態中的所有私密金鑰和密碼，以保護它們（例如用於 Ssl 正向 Proxy 解密的私密金鑰）。

盡快變更預設主要金鑰，以確保您使用唯一主要金鑰進行加密。

在高可用性 (HA) 設定中，您必須在兩個防火牆上使用相同的主要金鑰，因為主要金鑰不會在 HA 對等之間同步。否則，HA 同步將無法正常運作。

如果您使用 Panorama 管理防火牆，則可以在 Panorama 和所有受管理防火牆上設定相同的主要金鑰，或為每個受管理防火牆設定唯一的主要金鑰。對於 HA 設定中的受管理防火牆，您必須為每個 HA 對等設定相同的主要金鑰。如果防火牆由 Panorama™ 管理伺服器管理，請參閱從 Panorama 管理主要金鑰。

務必將主要金鑰儲存在安全位置。您無法復原主要金鑰，還原預設主要金鑰的唯一方法是將防火牆重設為原廠預設設定。

STEP 1 | 備份設定。

STEP 2 | （僅適用於 HA）停用設定同步。

需要執行此步驟才能為防火牆 HA 配對部署新的主要金鑰。

在將新的主要金鑰部署到任何防火牆 HA 配對之前，您必須停用設定同步。對於 Panorama 管理的防火牆，如果您未在部署新的主要金鑰之前停用設定同步，Panorama 將失去與主要防火牆的連線。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般），然後編輯 **Setup**（設定）。
2. 停用（清除）**Enable Config Sync**（啟用設定同步），然後按一下 **OK**（確定）。
3. **Commit**（提交）組態變更。

STEP 3 | 選取 **Device**（裝置） > **Master Key and Diagnostics**（主要金鑰與診斷），然後編輯 Master Key（主要金鑰）區段。

STEP 4 | 如果目前主要金鑰為空白，請為其輸入。

STEP 5 | 按一下新增主要金鑰定義新的主要金鑰，然後按一下確認新主要金鑰。金鑰長度必須剛剛好 16 個字元。

©2024 Palo Alto Networks, Inc.

STEP 6 | 若要指定主要金鑰的 **Lifetime**（存留時間），可輸入金鑰存留 **Days**（天）數及/或 **Hours**（小時）數，超過此時間即過期。

您在目前的金鑰到期之前，必須設定新的主要金鑰。如果主要金鑰到期，防火牆或 Panorama 就會自動以維護模式重新啟動。您必須將防火牆重設為原廠預設設定。

將 ***Lifetime***（存留時間）設定為兩年或更短，具體取決於裝置執行的加密次數。裝置執行的加密次數越多，就應設定越短的 ***Lifetime***（存留時間）。關鍵考慮因素是不要在變更主要金鑰之前用完唯一加密。根據主要金鑰值和初始化向量 *(IV)* 值，每個主要金鑰可以提供最多 2^{32} 個唯一加密。2^{32} 個唯一加密用完後，加密會重複（不再唯一），這會帶來安全性風險。

為主要金鑰設定 ***Time for Reminder***（提醒時間）值（參閱下一步驟），在出現提醒通知時，變更主要金鑰。

STEP 7 | 輸入 **Time for Reminder**（提醒時間），指定防火牆在主要金鑰到期前多少 **Days**（天）及 **Hours**（小時）產生到期警報。防火牆會自動開啟 System Alarms（系統警報）對話方塊來顯示警報。

設定提醒，以便主要金鑰在排程的維護時段內到期之前，您有充足的時間來設定新主要金鑰。當 ***Time for Reminder***（提醒時間）到期且防火牆或 *Panorama* 傳送通知日誌時，變更主要金鑰，不要等到 ***Lifetime***（存留時間）到期。對於分組裝置，追蹤每個裝置（例如，*Panorama* 管理的防火牆和防火牆 *HA* 配對），當群組中任何裝置的提醒值到期時，變更主要金鑰。

為了確保會顯示到期警報，可選取 ***Device***（裝置） > ***Log Settings***（日誌設定），編輯 *Alarm Settings*（警報設定），然後 ***Enable Alarms***（啟用警報）。

STEP 8 | 啟用 **Auto Renew Master Key**（自動更新主要金鑰）以將防火牆設為自動更新主要金鑰。若要設定 **Auto Renew With Same Master Key**（使用相同的主要金鑰自動更新），請指定更新同一

©2024 Palo Alto Networks, Inc.

主要金鑰的 **Days**（天數）和/或 **Hours**（小時數）。金鑰擴展讓防火牆繼續執行並繼續保護網路；如果現有主要金鑰存留時間即將到期，其不能取代主要金鑰設定新金鑰。

自動更新主要金鑰既有好處，也有風險。好處是延長主要金鑰 **Lifetime**（存留時間），防止在存留時間到期之前未能變更主要金鑰。風險是，如果裝置使用主要金鑰執行的加密次數超過主要金鑰可以產生的唯一加密數量（2^{32} 個唯一加密），則加密將重複並帶來安全性風險。

如果主要金鑰到期（您沒有自動更新且沒有及時更換），裝置將進入維護模式。

如果啟用 ***Auto Renew Master Key***（自動更新主要金鑰），請進行設定，以使總時間（存留時間加自動更新時間）不會導致裝置用完唯一加密。例如，如果您認為裝置將在兩年半內耗用完主要金鑰的唯一加密次數，則可以將 ***Lifetime***（存留時間）設定為兩年，將 ***Time for Reminder***（提醒時間）設定為 *60* 天，並將 ***Auto Renew Master Key***（自動更新主要金鑰）設定為 *60-90* 天，以在 ***Lifetime***（存留時間）到期之前提供額外的時間來設定新的主要金鑰。但是，最佳做法仍然是在存留時間到期之前變更主要金鑰，以確保沒有裝置重複加密。

考慮設定主要金鑰以在其存留時間到期後自動更新時，距離下一個可用維護窗口的天數。

STEP 9 | （選用）為了增強安全性，請選取是否使用 **HSM** 加密主要金鑰。如需詳細資訊，請參閱使用 HSM 加密主要金鑰。

STEP 10 | 按一下 **OK**（確定）與 **Commit**（提交）。

STEP 11 | （僅適用於 HA）重新啟用設定同步。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般），然後編輯 **Setup**（設定）。
2. 啟用（核選）**Enable Config Sync**（啟用設定同步），然後按一下 **OK**（確定）。
3. **Commit**（提交）組態變更。

©2024 Palo Alto Networks, Inc.

主要金鑰加密

在實體和虛擬 Palo Alto Networks 裝置上，您可以設定主要金鑰以使用 AES-256-CBC 或 AES-256-GCM（PAN-OS 10.0 中引入）加密演算法來加密金鑰和密碼之類的資料。AES-256-GCM 提供比 AES-256-CBC 更強的加密，可改善您的安全狀態。它還包含一個內建完整性檢查。主要金鑰使用設定的加密演算法對儲存在防火牆和 Panorama 上的敏感資料進行加密。將加密演算法設定為 AES-256-GCM 時，您仍可以透過儲存在 HSM 上的加密金鑰，使用 HSM 來加密主要金鑰。

主要金鑰用於加密資料的預設加密演算法為 AES-256-CBC，與 PAN-OS 10.0 之前主要金鑰使用的演算法相同。AES-256-CBC 是預設的加密層級，因為當您使用 Panorama 管理防火牆時，受管理的防火牆可能使用不同的 PAN-OS 版本，且執行 PAN-OS 11.0 之前 PAN-OS 版本的防火牆不支援 AES-256-GCM。這就是 Panorama 必須使用其受管理裝置可以使用的最低加密層級的原因。例如，如果某些受管理裝置執行 PAN-OS 11.0，而另一些執行早期版本，則 Panorama 必須使用 AES-256-CBC。但是，如果所有受管理裝置都執行 PAN-OS 11.0 或更新版本，則 Panorama 及其所有受管理裝置都可以使用 AES-256-GCM。

在 *Panorama* 及其受管理裝置上使用相同的加密層級，並在防火牆配對上使用相同的加密層級。升級裝置以使用可能最強的加密演算法。如果 *Panorama* 管理的所有裝置都執行 *PAN-OS 10.0*，請在所有裝置上使用 *AES-256-GCM*。使用其他加密層級的受管理或已配對裝置的設定可能變得不同步。

當您將加密演算法變更為 AES-256-GCM 時，裝置將使用 AES-256-GCM 而不是 AES-256-CBC 來加密敏感資料。從一種演算法變更為另一種演算法時，還可以指定是否：

- 使用新演算法重新加密現有已加密資料。
- 現有資料繼續使用舊加密演算法進行加密，新演算法用於新的（未來）加密。

依預設，當您變更加密演算法時，裝置將使用新演算法來重新加密現有的已加密資料以及加密新資料。如果您使用 *Panorama* 管理裝置，則它們可能使用不同版本的 *PAN-OS*，且可能不支援最新的加密演算法。在變更加密演算法或重新加密已加密資料之前，請確保您瞭解 *Panorama* 及其受管理裝置支援的加密演算法。

- 設定主要金鑰加密層級
- 防火牆 HA 配對上的主要金鑰加密
- 主要金鑰加密日誌
- AES-256-GCM 的唯一主要金鑰加密

設定主要金鑰加密層級

設定主要金鑰加密演算法層級，以及是否使用 CLI，以新的加密演算法層級來重新加密所有當前加密的資料。根據關鍵字的順序，您可以變更加密層級，也可以變更加密層級並同時指定是否重新加密以前加密的資料。

©2024 Palo Alto Networks, Inc.

以下可操作的 CLI 命令可以變更加密層級，並以指定的加密層級自動重新加密所有當前加密的資料：

```
admin@PA-NGFW>request encryption-level level <0|1|2>
```

以下可操作 CLI 命令可以變更加密層級，並指定是否以新的加密層級重新加密所有當前加密的資料：

```
admin@PA-NGFW>request encryption-level re-encrypt <yes|no> level <0|1|2>
```

關鍵字	選項
層級	**0** = 使用預設演算法 (AES-256-CBC) 加密資料 **1** = 使用 AES-256-CBC 演算法加密資料 **2** = 使用 AES-256-GCM 演算法加密資料 防火牆使用指定的演算法重新加密所有當前加密的資料並加密新的敏感資料。如果您不想使用新演算法重新加密現有的加密資料，請在命令字串中指定 **re-encrypt no**。這樣可以阻止防火牆自動重新加密防火牆已經加密的資料。 僅當 *Panorama* 及其所有受管理裝置（或 *HA* 配對中的兩個裝置）執行 *PAN-OS 11.0* 或更高版本時使用 *AES-256-GCM*，並設定所有裝置使用 *AES-256-GCM*。使用其他加密層級的受管理或已配對裝置可能變得不同步。
re-encrypt	**no** = 不重新加密當前已加密的資料。防火牆不會重新加密當前已加密的資料。當前加密的資料將仍使用防火牆最初用來加密這些資料的任何演算法進行加密。防火牆僅使用指定演算法加密未來的敏感資料。 **yes** = 使用指定的演算法重新加密當前加密的資料，並使用該演算法加密未來的敏感資料。

使用可操作的 CLI 命令 **show system masterkey-properties** 來驗證裝置上當前設定的加密演算法（層級），例如：

```
admin@PA-NGFW>show system masterkey-properties
```


©2024 Palo Alto Networks, Inc.

```
Master key expires at: unspecified Reminders will begin at:
 unspecified Master key on hsm: no Automatically renew master key
 lifetime:0 Encryption Level:1
```

輸出顯示當前加密層級為 1，即 AES-256-CBC。

如果您降級到 PAN-OS 的早期版本，則裝置會自動將加密演算法還原到降級的 PAN-OS 版本支援的層級，並使用該層級自動重新加密已加密資料，以便裝置可以解密和按需使用資料。例如，如果您的裝置執行 PAN-OS 11.0 並使用 AES-256-GCM 作為加密演算法（在 PAN-OS 的早期版本中不受支援），裝置降級到 PAN-OS 9.1 後，會將已加密資料重新加密到 PAN-OS 9.1 中受支援的 AES-256-CBC 中。

防火牆 HA 配對上的主要金鑰加密

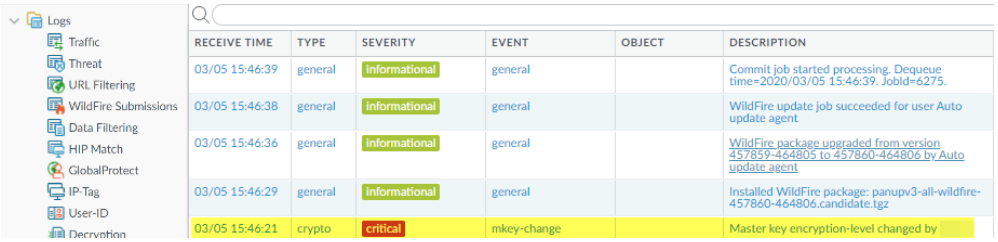
要在防火牆高可用性 (HA) 配對上使用 AES-256-GCM 加密層級，兩個防火牆都必須執行 PAN-OS 10.0，以便兩個防火牆都支援 AES-256-GCM。如果 HA 配對中的任一防火牆執行的版本低於 PAN-OS 10.0，您將無法使用 AES-256-GCM。當兩個防火牆都使用 PAN-OS 10.0 時，兩個防火牆都可以解碼 AES-256-CBC 或 AES-256-GCM 加密金鑰，因此它們可以使用任一加密層級。但是，兩個防火牆應使用相同的加密層級，以避免出現不同步。

在 *HA* 配對的兩個防火牆上使用 *AES-256-GCM* 加密。無論您使用 *AES-256-GCM* 還是 *AES-256-CBC*，請在兩個防火牆上使用相同的演算法。

您無需停用 HA 即可在兩個防火牆都執行 PAN-OS 10.0 的 HA 配對中的防火牆上變更加密層級。

主要金鑰加密日誌

當您變更主要金鑰加密演算法（層級）時，防火牆會產生系統日誌（**Monitor**（監控） > **Logs**（日誌） > **System**（系統））。



要檢視所有主要金鑰加密的系統日誌，請建立一個篩選器，顯示 crypto 類型的所有日誌：**(subtype eq crypto)**。

AES-256-GCM 的唯一主要金鑰加密

在用盡唯一組合之前，主要金鑰只能產生有限數量的唯一加密，且必須重複加密。防火牆使用帶有初始化向量 (IV) 的 AES-256-GCM 加密演算法建立唯一加密。IV 是一個任意數，只能使用一次來建立加密，以確保每個加密都是唯一的。

©2024 Palo Alto Networks, Inc.

使用主要金鑰和 IV 進行的每個加密都必須唯一，以防止偽造攻擊。防火牆滿足唯一性要求，即在兩個或更多不同的輸入資料集上使用相同的 IV 和相同的金鑰建立經過驗證的加密的可能性不超過 2^{32} 種。

當 IV 遍歷其所有唯一值時，IV 值會重複。當 IV 值重複時，使用相同的主要金鑰和重複的 IV 值來加密資料意味著該加密與先前在其他資料上使用的加密相同。在系統用盡唯一加密前變更主要金鑰，以防止防火牆對多個敏感資料使用相同的加密（主要金鑰和 IV 值組合）。唯一加密組合不得重複或重新使用。

要追蹤您何時需要變更主要金鑰，請在每個設備上設定主要金鑰 **Lifetime**（存留時間）和 **Reminder**（提醒）值（**Device**（裝置） > **Master Key and Diagnostics**（主要金鑰和診斷），然後編輯主要金鑰）。根據主要金鑰加密的預期量保守地設定這些值，以確保所有加密都是唯一的，且不會重複或重新使用任何加密組合。

©2024 Palo Alto Networks, Inc.

取得憑證

- 建立自我簽署根 CA 憑證
- 產生憑證
- 匯入憑證與私密金鑰
- 從外部 CA 取得憑證
- 安裝裝置憑證
- 使用 SCEP 部署憑證

建立自我簽署根 CA 憑證

自我簽署根憑證授權單位 (CA) 憑證是憑證鏈結中最上層的憑證。防火牆會使用此憑證自動簽發其他用途的憑證。例如，防火牆針對 GlobalProtect 大規模 VPN 中的 SSL/TLS 解密與衛星簽發憑證。

與防火牆建立安全連線時，遠端用戶端必須信任簽發憑證的根 CA。否則，用戶端瀏覽器將顯示憑證無效的警告，並可能封鎖連線 (取決於安全性設定)。若要防止此狀況發生，在產生自我簽署根 CA 憑證後，將該憑證匯入用戶端系統中。

在 *Palo Alto Networks* 防火牆或 *Panorama* 上，僅當憑證為 *CA* 憑證時，您才能產生自我簽署憑證。

STEP 1 | 選取 **Device**（設備） > **Certificate Management**（憑證管理） > **Certificates**（憑證） > **Device Certificates**（裝置憑證）。

STEP 2 | 若防火牆具有一個以上的虛擬系統 (vsys)，為憑證選取一個 **Location**（位置）（vsys 或 **Shared**（共用））。

STEP 3 | 按一下 **Generate**（產生）。

STEP 4 | 輸入 **Certificate Name**（憑證名稱），例如 **`GlobalProtect_CA`**。名稱區分大小寫，防火牆上最多可使用 63 個字元，Panorama 上最多可使用 31 個字元。名稱必須是唯一的，且只能使用字母、數字、連字號與底線。

STEP 5 | 在 **Common Name**（通用名稱）欄位中輸入 FQDN（建議），或是輸入介面的 IP 位址，您將在該介面上設定使用此憑證的服務。

STEP 6 | 若防火牆具有一個以上的 vsys 且您想讓每個 vsys 都獲得驗證，請選取 **Shared**（共用）核取方塊。

STEP 7 | 將**Signed By**（簽署者）欄位保留空白，以指定憑證為自我簽署。

STEP 8 | （必要）選取 **Certificate Authority**（憑證授權單位）核取方塊。

©2024 Palo Alto Networks, Inc.

STEP 9 | 將 **OCSP Responder**（**OCSP** 回應程式）欄位保留空白，憑證撤銷狀態驗證不適用於根 CA 憑證。

STEP 10 | 按一下產生與提交。

產生憑證

Palo Alto Networks 防火牆及 Panorama 使用憑證驗證數種應用程式中的用戶端、伺服器、使用者與裝置，包括 SSL/TLS 解密、驗證入口網站、GlobalProtect、站點對站點 IPSec VPN 及防火牆/Panorama 網頁介面存取等。針對每種用途產生憑證：詳細資訊，請參閱金鑰與憑證。

若要產生憑證，您必須先建立自我簽署根 CA 憑證或匯入一個（匯入憑證與私密金鑰）以簽署憑證。若要使用線上憑證狀態通訊協定 (OCSP) 驗證憑證撤銷狀態，請在產生憑證之前設定 OCSP 回應程式。

STEP 1 | 選取 **Device**（設備） > **Certificate Management**（憑證管理） > **Certificates**（憑證） > **Device Certificates**（裝置憑證）。

STEP 2 | 若防火牆具有一個以上的虛擬系統 (vsys)，為憑證選取一個 **Location**（位置）（vsys 或 **Shared**（共用））。

STEP 3 | 按一下 **Generate**（產生）。

STEP 4 | 選取 **Local**（本機）（預設）作為 **Certificate Type**（憑證類型），除非您要將 SCEP 憑證部署至 GlobalProtect 端點。

STEP 5 | 輸入 **Certificate Name**（憑證名稱）。名稱區分大小寫，防火牆上最多可使用 63 個字元，Panorama 上最多可使用 31 個字元。名稱必須是唯一的，且只能使用字母、數字、連字號與底線。

STEP 6 | 在 **Common Name**（通用名稱）欄位中輸入 FQDN（建議），或是輸入介面的 IP 位址，您將在該介面上設定使用此憑證的服務。

STEP 7 | 若防火牆具有一個以上的 vsys 且您想讓每個 vsys 都獲得驗證，請選取 **Shared**（共用）核取方塊。

STEP 8 | 在 **Signed By**（簽署者）欄位中，選取將簽發憑證的根 CA 憑證。

STEP 9 | （選用）選取是否要 **Block Private Key Export**（封鎖私密金鑰匯出）。

啟用此設定可防止在您匯出憑證時匯出私密金鑰。

如果啟用此設定，則在匯入憑證到 *Panorama* 或其他防火牆時，必須手動匯入相關聯的私密金鑰。對於由 *Panorama* 管理的防火牆，必須使用私密金鑰才能成功將設定變更推送至您匯入憑證的受管理防火牆。

STEP 10 | （選用）選取 **OCSP Responder**（**OCSP** 回應程式）。

©2024 Palo Alto Networks, Inc.

STEP 11 | 如需金鑰產生 **Algorithm**（演算法），請選取 **RSA**（預設）或 **Elliptical Curve DSA**（橢圓曲線 DSA）(ECDSA)。ECDSA 建議使用於支援的用戶端瀏覽器和作業系統。

執行 *PAN-OS 6.1* 及以前版本的防火牆將刪除任何從 *Panorama™* 推送的 *ECDSA* 憑證，且任何由 *ECDSA* 憑證授權單位 *(CA)* 簽署的 *RSA* 憑證在那些防火牆上將成為無效。

您無法使用硬體安全性模組 (HSM) 來儲存用於 SSL/TLS 解密的 ECDSA 金鑰。

STEP 12 | 選取 **Number of Bits**（位元組數）定義憑證金鑰長度。越多數字越為安全，但也需要較多處理時間。

STEP 13 | 選取 **Digest**（摘要）演算法。安全性最高到最低的選項排列為： **sha512**、**sha384**、**sha256**（預設）、 **sha1** 及**md5**。

在要求仰賴 *TLSv1.2* 之防火牆服務（例如管理員存取 *Web* 介面）時所使用的用戶端憑證不能以 ***sha512*** 作為摘要演算法。這些用戶端憑證必須使用較低的摘要演算法（例如 ***sha384***），或者在您設定 SSL/TLS 服務設定檔時，必須將防火牆服務的 ***Max Version***（最高版本）限定為 ***TLSv1.1***。

STEP 14 | 對於 **Expiration**（到期日期），請輸入憑證的有效天數（預設為 365）。

STEP 15 | （選用）按一下**Add**（新增）並選取 **Certificate Attributes**（憑證屬性），以唯一識別使用憑證的防火牆與服務。

如果您新增 ***Host Name***（主機名稱）（*DNS* 名稱）屬性，最佳做法是讓此名稱符合 ***Common Name***（通用名稱），因為主機名稱會填入憑證的主旨替代名稱 *(SAN)* 欄位，部分瀏覽器要求 *SAN* 指定憑證所保護的網域；此外，與 ***Common Name***（通用名稱）相符的 ***Host Name***（主機名稱）對 *GlobalProtect* 而言為必要。

STEP 16 | 按一下 **Generate**（產生），然後在（裝置憑證）頁面上按一下憑證的（名稱）。

無論防火牆時區如何，裝置始終顯示憑證驗證的相應格林威治標準時間 *(GMT)* 及到期日期/時間。

STEP 17 | 選取與憑證在防火牆上預定用途對應的核取方塊。

例如，若防火牆使用此憑證將系統日誌安全轉送至外部系統日誌伺服器，則要選中 **Certificate for Secure Syslog**（安全系統日誌的憑證）核取方塊。

STEP 18 | 按一下 **OK**（確定）與 **Commit**（提交）。

匯入憑證與私密金鑰

如果貴企業有自己的公開金鑰基礎結構 (PKI)，則可以將憑證與私密金鑰從您企業的憑證授權單位 (CA) 匯入防火牆。企業 CA 憑證 (不同於從信任的第三方 CA 購買的大多數憑證)會自動為 SSL/TLS 解密或大規模 VPN 等應用程式簽發 CA 憑證。

©2024 Palo Alto Networks, Inc.

在 *Palo Alto Networks* 防火牆或 *Panorama* 上，僅當憑證為 *CA* 憑證時，您才能匯入自我簽署憑證。

最佳做法是從企業 *CA* 匯入憑證，而非將自我簽署根 *CA* 憑證匯入至所有用戶端系統，因為用戶端已經與企業 *CA* 間有了信任關係，這能夠簡化部署。

如果您匯入的憑證是憑證鏈結的一部分，最佳做法是匯入整個鏈結。

STEP 1 | 從企業 CA 匯出防火牆用於驗證的憑證與私密金鑰。

匯出私密金鑰時，您必須輸入密碼才能將要傳輸的複雜密碼加密。確定管理系統可存取憑證與金鑰檔案。將金鑰匯入到防火牆時，您必須輸入相同的密碼才能解密。

STEP 2 | 選取 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證） > **Device Certificates**（裝置憑證）。

STEP 3 | 若防火牆具有一個以上的虛擬系統 (vsys)，為憑證選取一個 **Location**（位置）（vsys 或 **Shared**（共用））。

STEP 4 | 按一下 **Import**（匯入）並輸入 **Certificate Name**（憑證名稱）。名稱區分大小寫，防火牆上最多可使用 63 個字元，Panorama 上最多可使用 31 個字元。名稱必須是唯一的，且只能使用字母、數字、連字號與底線。

STEP 5 | 若要讓憑證可供所有虛擬系統使用，請選取共用核取方塊。此核取方塊只有在防火牆支援多個虛擬系統時才會顯示。

STEP 6 | 輸入從 CA 所收到 **Certificate File**（憑證檔案）的路徑與名稱，或按一下 **Browse**（瀏覽）以找到該檔案。

STEP 7 | 選取 **File Format**（檔案格式）：

- 加密的私密金鑰與憑證 **(PKCS12)**—這是預設值，也是最常見的格式，其中的金鑰與憑證是在單一容器內（**Certificate File**（憑證檔案））。如果硬體安全性模組 (HSM) 將存放此憑證的私密金鑰，請選取**Private key resides on Hardware Security Module**（私人金鑰位於硬體安全性模組）核取方塊。
- **Base64** 編碼憑證 **(PEM)**—您必須將金鑰與憑證分開匯入。如果硬體安全性模組 (HSM) 存放此憑證的私密金鑰，則選中 **Private key resides on Hardware Security Module**（將私密金鑰存取於硬體安全性模組）核取方塊，並略過下一步驟。否則，選中 **Import Private Key**（匯入私密金鑰）核取方塊，輸入 **Key File**（金鑰檔案）或 **Browse**（瀏覽）至該檔案，然後繼續執行下一步驟。

（*Panorama* 受管理的防火牆）如果您在產生憑證時啟用了 ***Block Private Key Export***（封鎖私密金鑰匯出）以成功將設定變更從 *Panorama* 管理伺服器推送到受管理的防火牆，則需要 ***Import Private Key***（匯入私密金鑰）。

STEP 8 | 輸入用於加密私密金鑰的密碼，並重新輸入進行確認。

STEP 9 | 按一下 **OK**（確定）。（裝置憑證）頁面會顯示匯入的憑證。

©2024 Palo Alto Networks, Inc.

從外部 CA 取得憑證

從外部憑證授權單位 (CA) 取得憑證的優點就是，私密金鑰不會離開防火牆。若要從外部 CA 取得憑證，請產生憑證簽署要求 (CSR) 並提交到 CA。CA 簽發具備指定屬性的憑證後，請將憑證匯入到防火牆上。CA 可以是知名、公開的 CA 或企業 CA。

若要使用線上憑證狀態通訊協定 (OCSP) 驗證憑證撤銷狀態，可在產生 CSR 之前設定 OCSP 回應程式。

STEP 1 | 從外部 CA 取得憑證。

1. 選取 **Device**（設備） > **Certificate Management**（憑證管理） > **Certificates**（憑證） > **Device Certificates**（裝置憑證）。
2. 若防火牆具有一個以上的虛擬系統 (vsys)，為憑證選取一個 **Location**（位置）（vsys 或 **Shared**（共用））。
3. 按一下 **Generate**（產生）。
4. 輸入 **Certificate Name**（憑證名稱）。名稱區分大小寫，防火牆上最多可使用 63 個字元，Panorama 上最多可使用 31 個字元。名稱必須是唯一的，且只能使用字母、數字、連字號與底線。
5. 在 **Common Name**（通用名稱）欄位中輸入 FQDN（建議），或是輸入介面的 IP 位址，您將在該介面上設定使用此憑證的服務。
6. 若防火牆具有一個以上的 vsys 且您想讓每個 vsys 都獲得驗證，請選取 **Shared**（共用）核取方塊。
7. 在 **Signed By**（簽署者）欄位中，選取 **External Authority (CSR)**（外部授權 **(CSR)**）。
8. 如果適用，請選取 **OCSP** 回應程式。
9. （選用）按一下**Add**（新增）並選取 **Certificate Attributes**（憑證屬性），以唯一識別使用憑證的防火牆與服務。

   如果您新增 ***Host Name***（主機名稱）屬性，應該讓此名稱符合 ***Common Name***（通用名稱）（這對 *GlobalProtect* 而言為必要）。主機名稱會填入憑證的（主旨替代名稱）欄位。
10. 按一下 **Generate**（產生）。**Device Certificates**（裝置憑證）頁籤顯示狀態為 `pending`（擱置中）的 CSR。

STEP 2 | 將 CSR 提交至 CA。

1. 選取 CSR，然後按一下**Export**（匯出）將 .csr 檔案儲存至本機電腦。
2. 將 CSR 上傳至 CA。

©2024 Palo Alto Networks, Inc.

STEP 3 | 匯入憑證。

1. CA 傳送簽署的憑證來回應 CSR 後，請返回**Device Certificates**（裝置憑證）頁籤並按一下**Import**（匯入）。
2. 輸入用於產生 CSR 的**Certificate Name**（憑證名稱）。
3. 輸入 CA 傳送 PEM **Certificate File**（憑證檔案）的路徑與名稱，或**Browse**（瀏覽）至該檔案。
4. 按一下 **OK**（確定）。**Device Certificates**（裝置憑證）頁籤顯示狀態為 `valid`（有效）的憑證。

STEP 4 | 設定憑證。

1. 按一下憑證**Name**（名稱）。
2. 選取與憑證在防火牆上預定用途對應的核取方塊。例如，若防火牆使用此憑證將系統日誌安全轉送至外部系統日誌伺服器，則要選中 **Certificate for Secure Syslog**（安全系統日誌的憑證）核取方塊。
3. 按一下 **OK**（確定）與 **Commit**（提交）。

安裝裝置憑證

您的新世代防火牆可以利用一個或多個 Palo Alto Networks 雲端服務。為此，您必須安裝裝置憑證以透過 Palo Alto Networks 客戶支援入口網站 (CSP) 成功驗證防火牆，以利用這些雲端服務。需要裝置憑證的情況因功能而異，因此，僅在功能的設定文件告訴您需要安裝時才安裝裝置憑證。

您僅需安裝裝置憑證一次。每個使用裝置憑證的功能都將使用安裝在防火牆上的憑證（如果已存在）。

要在防火牆上成功安裝裝置憑證，您的網路必須允許使用以下 FQDN 和連接埠。

FQDN	連接埠
• http://ocsp.paloaltonetworks.com • http://crl.paloaltonetworks.com • http://ocsp.godaddy.com	TCP 80
• https://api.paloaltonetworks.com • http://apitrusted.paloaltonetworks.com • certificatetrusted.paloaltonetworks.com • certificate.paloaltonetworks.com	TCP 443
• *.gpcloudservice.com	TCP 444 和 TCP 443

©2024 Palo Alto Networks, Inc.

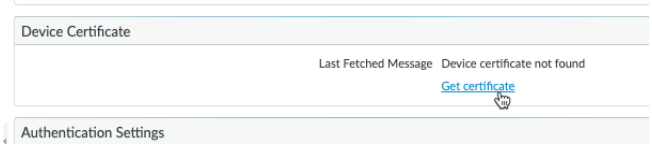
您可以將裝置憑證安裝到由 Panorama 管理的防火牆。如果想要將裝置憑證直接安裝到單個新世代防火牆（也就是說，您不使用 Panorama）：

STEP 1 | 產生一次性密碼 (OTP)。

1. 登入客戶支援入口網站。
2. 選取 **Assets**（資產） > **Device Certificates**（裝置憑證）及 **Generate OTP**（產生 **OTP**）。
3. 對於 **Device Type**（裝置類型），選取 **Generate OTP for Next-Gen Firewalls**（為新世代防火牆產生 **OTP**）。
4. 選取您的 **PAN OS Device**（**PAN OS** 裝置）序號。
5. **Generate OTP**（產生 **OTP**）且複製 OTP。

STEP 2 | 作為管理員使用者登入您的新世代防火牆。

STEP 3 | 選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理） > **Device Certificate**（裝置憑證）和 **Get certificate**（獲取憑證）。



STEP 4 | 貼上您產生的 **One-time Password**（一次性密碼）並按一下 **OK**（確定）。

STEP 5 | 您的新世代防火牆會成功擷取並安裝憑證。

使用 SCEP 部署憑證

如果您的企業 PKI 擁有簡易憑證註冊通訊協定 (SCEP) 伺服器，則可設定 SCEP 設定檔，以自動化唯一用戶端憑證的產生及散佈。SCEP 在該企業 PKI 中動態運作，以便在 SCEP 用戶端請求時產生使用者特定憑證，並將憑證傳送至 SCEP 用戶端。SCEP 用戶端然後以透明方式部署憑證至用戶端裝置。

您可在 GlobalProtect 上使用 SCEP 設定檔，以將使用者特定用戶端憑證指派給各 GlobalProtect 使用者。在此使用案例中，GlobalProtect 入口網站充當企業 PKI 中 SCEP 伺服器的 SCEP 用戶端。此外，還可使用 SCEP 設定檔，將用戶端憑證指派給用於相互驗證的 Palo Alto Networks 裝置，將其他 Palo Alto Networks 裝置用於管理存取以及裝置間通訊。

STEP 1 | 建立 SCEP 設定檔。

1. 選取 **Device**（裝置） > **Certificate Management**（憑證管理） > **SCEP**，然後 **Add**（新增） 新的設定檔。
2. 輸入用來識別 SCEP 設定檔的 **Name**（名稱）。
3. 如果此設定檔適用於具有多重虛擬系統功能的防火牆，請選取一個虛擬系統或 **Shared**（共用）作為設定檔可用的 **Location**（位置）。

©2024 Palo Alto Networks, Inc.

STEP 2 | （選用）為使基於 SCEP 的憑證產生更安全，在 PKI 與各憑證要求的入口網站之間設定 SCEP 質詢回應機制。

在您設定此機制後，其操作不可見，您不必進行進一步輸入。

為了符合美國聯邦資訊處理標準 (FIPS)，請使用 **Dynamic**（動態）SCEP 挑戰，並指定一個使用 HTTPS 的 **Server URL**（伺服器 **URL**）。

選取下列其中一個選項：

- **None**（無） — （預設）SCEP 伺服器在簽發憑證之前，不會質詢入口網站。
- **Fixed**（固定）—在 PKI 基礎結構中，從 SCEP 伺服器取得註冊質詢密碼，然後在密碼欄位輸入密碼。
- **Dynamic**（動態）—輸入使用者名稱和您選擇的密碼（可能是 PKI 管理員的認證）以及入口網站用戶端提交這些認證的 SCEP **Server URL**（伺服器 **URL**）。使用認證向 SCEP 伺服器驗證，以透明方式產生用於每次憑證要求的入口網站 OTP 密碼。（您可以看到螢幕在註冊挑戰密碼是欄位中重新整理後，此 OTP 將根據每個憑證要求變更。） PKI 以透通方式將每個新密碼傳輸至入口網站，其接著使用該密碼用於憑證要求。

STEP 3 | 指定 SCEP 伺服器與入口網站之間的連線設定，以啟用入口網站來請求和接收用戶端憑證。

您可以透過在憑證 **Subject**（主旨）名稱中指定權杖，來包含關於用戶端裝置或使用者的其他資訊。

入口網站包括 CSR 對 SCEP 伺服器要求中的語彙值和主機 ID。

1. 設定入口網站用於連線 PKI 中 SCEP 伺服器的 **Server URL**（伺服器 **URL**）（例如 `http://10.200.101.1/certsrv/mscep/`）。
2. 在 **CA-IDENT Name**（**CA-IDENT** 名稱）欄位中輸入字串（長度最大為 255 個字元），用以識別 SCEP 伺服器。
3. 輸入 SCEP 伺服器所產生之憑證使用的 **Subject**（主旨）名稱。主旨必須是一個格式為 **<attribute>=<value>** 的辨別名稱，且必須包含通用名稱 (CN) 屬性 (CN=**<variable>**)。CN 支援下列動態權杖：
   - `$USERNAME`—使用此權杖讓入口網站能向特定使用者要求憑證。若要在 GlobalProtect 中使用此變數，您也必須啟用群組對應。使用者輸入的使用者名稱必須與使用者群組對應表格中的名稱相符。
   - `$EMAILADDRESS`—使用此權杖以要求與特定電子郵件地址關聯的憑證。若要使用此變數，您也必須啟用群組對應並在伺服器設定檔的郵件網域區段中設定 **Mail Attributes**（郵件屬性）。若 GlobalProtect 無法辨識使用者的電子郵件地址，便會產生唯一的 ID 並以該值填入 CN。
   - `$HOSTID`—若要僅為裝置要求憑證，請指定主機 ID 權杖。當使用者嘗試登入入口網站時，端點會傳送識別資訊，其中包括其主機 ID 值。主機 ID 值隨裝置類型而異，可

 ©2024 Palo Alto Networks, Inc.

以是介面的 GUID (Windows) MAC 位址、Android ID（Android 裝置）、UDID（iOS 裝置）或 GlobalProtect 指派的唯一名稱 (Chrome)。

- `$UDID`—使用 UDID 通用名稱屬性，來根據用戶端的 GlobalProtect 裝置 UDID 或者用於 Palo Alto Networks 裝置間相互驗證的裝置序號請求憑證。

當 GlobalProtect 入口網站將 SCEP 設定推送至代理程式時，主旨名稱的 CN 部分會取代為憑證擁有者的實際值（使用者名稱、主機 ID 或電子郵件地址）（例如，**`O=acme,CN=johndoe`**）。

4. 選取 **Subject Alternative Name Type**（主旨替代名稱類型）：

   為主旨替代名稱類型使用靜態項目。防火牆不會支援動態權杖。例如 ***`$USERNAME`***。

   - **RFC 822 Name**（**RFC 822** 名稱）—在憑證的主旨或主旨替代副檔名輸入電子郵件名稱。
   - **DNS Name**（**DNS** 名稱）—輸入用於評估憑證的 DNS 名稱。
   - **Uniform Resource Identifier**（統一資源識別項）—輸入用戶端從中取得憑證的資源名稱。
   - **None**（無）—請勿指定憑證的屬性。

STEP 4 | （選用）進行憑證密碼設定。

- 選取憑證的金鑰長度（**Number of Bits**（位元數））。

  如果防火牆處於 FIPS-CC 模式，則金鑰產生演算法為 RSA。RSA 金鑰必須為 2,048 位元或更大。

- 選取 **Digest for CSR**（**CSR** 摘要），這會指出憑證簽署請求 (CSR) 的摘要演算法：憑證簽署要求 (CSR)：sha1、sha256 或 sha384。

STEP 5 | （選用）設定允許使用的憑證（簽署或加密）。

- 若要使用此憑證進行簽署，請選取 **Use as digital signature**（用作數位簽章）核取方塊。此選項可讓端點使用憑證中的私密金鑰來驗證數位特徵碼。
- 若要使用此憑證進行加密，請選取 **Use for key encipherment**（用作金鑰加密）核取方塊。此選項可讓用戶端使用憑證中的私密金鑰來加密透過 HTTPS 連線（使用 SCEP 伺服器核發的憑證建立連線）交換的資料。

STEP 6 | （選用）若要確保入口網站連線至正確的 SCEP 伺服器，請輸入 **CA Certificate Fingerprint**（**CA** 憑證指紋）。從 Thumbprint（指紋）欄位的 SCEP 伺服器介面取得該指紋。

1. 為 SCEP 伺服器管理員 UI 輸入 URL（例如 **`http://<hostname or IP>/CertSrv/mscep_admin/`**）。
2. 複製指紋並在 **CA Certificate Fingerprint**（**CA** 憑證指紋）欄位中輸入。

©2024 Palo Alto Networks, Inc.

STEP 7 | 啟用 SCEP 伺服器與防火牆之間的相互 SSL 驗證。這需要符合美國美國聯邦資訊處理標準 (FIPS)。

FIPS-CC 操作顯示於防火牆登入頁面及其狀態列。

選取 SCEP 伺服器的根 **CA Certificate**（**CA** 憑證指紋）。選取 **Client Certificate**（用戶端憑證）來選擇性地在 SCEP 伺服器與防火牆之間啟用相互 SSL 驗證。

STEP 8 | 儲存並提交組態。

1. 按一下 **OK**（確定）以儲存設定並關閉 SCEP 組態。
2. **Commit**（提交）組態。

入口網站嘗試使用 SCEP 設定檔中的設定請求 CA 憑證，並將其儲存至托管入口網站的防火牆。如果成功，CA 憑證將顯示在 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證）中。

STEP 9 | （選用）如果在儲存 SCEP 設定檔之後，入口網站無法取得憑證，您可以手動透過入口網站產生憑證簽署請求 (CSR)。

1. 選取 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證） > **Device Certificates**（裝置憑證），然後按一下 **Generate**（產生）。
2. 輸入 **Certificate Name**（憑證名稱）。此名稱不能包含空格。
3. 選取 **SCEP Profile**（**SCEP** 設定檔），用以提交 CSR 至企業 PKI。
4. 按一下 **OK**（確定），以提交請求並產生憑證。

©2024 Palo Alto Networks, Inc.

匯出憑證與私密金鑰

Palo Alto Networks 建議您使用貴企業的公開金鑰基礎結構 (PKI) 在組織內發行憑證和私密金鑰。然而，若有需要，您也可以從防火牆或 Panorama 匯出憑證和私密金鑰。您可以在下列狀況中使用匯出的憑證和私密金鑰：

- 將憑證式管理員驗證設定為網頁介面
- 啟用 GlobalProtect LSVPN 元件之間的 SSL，以設定面向入口網站及閘道的 GlobalProtect 代理程式/應用程式驗證
- Ssl 正向 Proxy 解密
- 從外部 CA 取得憑證

STEP 1 | 選取 **Device**（設備） > **Certificate Management**（憑證管理） > **Certificates**（憑證） > **Device Certificates**（裝置憑證）。

STEP 2 | 若防火牆具有一個以上的虛擬系統 (vsys)，為憑證選取一個 **Location**（位置）（特定的 vsys 或 **Shared**（共用））。

STEP 3 | 選取憑證，按一下 **Export**（匯出）然後選取 **File Format**（檔案格式）：

- **Base64** 編碼憑證 **(PEM)**—這是預設的格式。這最常見並在網際網路上具有最廣泛的支援。若您希望匯出的檔案包含私密金鑰，請選取 **Export Private Key**（匯出私密金鑰）核取方塊。
- 加密私人金鑰及憑證 **(PKCS12)**—此格式比 PEM 更為安全，但較不常見也較未受到廣泛支援。匯出的檔案會自動包含私密金鑰。
- 二進位編碼憑證 **(DER)**—比起其他格式，有較多作業系統類型支援此格式。您可以僅匯出憑證而非金鑰：請忽略 **Export Private Key**（匯出私密金鑰）核取方塊與複雜密碼欄位。

STEP 4 | 如果 **File Format**（檔案格式）為 PKCS12 或 PEM 且您已選取 **Export Private Key**（匯出私密金鑰）核取方塊，請輸入 **Passphrase**（複雜密碼）然後 **Confirm Passphrase**（確認複雜密碼）來加密私密金鑰。將憑證和金鑰匯入用戶端系統時，您將使用此複雜密碼。

（*Panorama* 受管理的防火牆）如果您在產生或匯入憑證時啟用了 ***Block Private Key Export***（封鎖私密金鑰匯出），請務必 ***Import Private Key***（匯入私密金鑰）并在匯入所匯出的憑證時新增 ***key File***（金鑰檔）。這是成功將設定變更從 *Panorama* 推送到受管理的防火牆（將憑證匯入其中）所必需的。

STEP 5 | 按一下 **OK**（確定）並將憑證/金鑰檔案儲存至您的本機電腦。

©2024 Palo Alto Networks, Inc.

設定憑證設定檔

憑證設定檔為驗證入口網站、多因素驗證 (MFA)、GlobalProtect、站點對站點 IPSec VPN、外部動態清單 (EDL) 驗證、動態 DNS (DDNS)、User-ID 代理程式、TS 代理程式存取及 Palo Alto Networks 防火牆或 Panorama 的網頁介面存取定義使用者與裝置驗證。設定檔會指定要使用哪些憑證、如何驗證憑證撤銷狀態，以及該狀態如何限制存取。為每個應用程式設定憑證設定檔。

最佳做法是為憑證設定檔啟用線上憑證狀態通訊協定 *(OCSP)* 和憑證撤銷清單 *(CRL)* 狀態驗證以驗證憑證未被撤銷。同時啟用 *OCSP* 和 *CRL*，這樣，如果 *OCSP* 伺服器不可用，防火牆可以使用 *CRL*。如需這些方法的詳細資訊，請參閱撤銷憑證。

STEP 1 | 取得您將指派的憑證授權單位 (CA) 憑證。

執行下列其中一個步驟以取得您要指派給設定檔的 CA 憑證。您必須指派至少一個憑證。

- 產生憑證。
- 從您的企業 CA 匯出憑證，然後匯入至防火牆（請參閱 3步驟）。

STEP 2 | 識別憑證設定檔。

1. 選取 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates Profile**（憑證設定檔），再按一下 **Add**（新增）。
2. 輸入用來識別設定檔的 **Name**（名稱）。名稱區分大小寫且必須是唯一的，防火牆上最多可使用 63 個字元，Panorama 上最多可使用 31 個字元，僅包含字母、數字、空格、連字號和底線。
3. 若防火牆具有一個以上的虛擬系統 (vsys)，為憑證選取一個 **Location**（位置）（vsys 或 **Shared**（共用））。

STEP 3 | 指派一或多個憑證。

為每個 CA 憑證執行下列步驟：

1. 在 [CA 憑證] 表格中按一下 **Add**（新增）。
2. 選取 **CA Certificate**（**CA** 憑證）。或者，若要匯入憑證，請按一下 **Import**（匯入）、輸入 **Certificate Name**（憑證名稱）、**Browse**（瀏覽）至您從企業 CA 匯出的 **Certificate File**（憑證檔案），然後按一下 **OK**（確定）。
3. （選用）如果防火牆使用 OCSP 驗證憑證撤銷狀態，請設定下列欄位取代預設行為。對於大多數的部署而言，這些欄位並不適用。
   - 依預設，防火牆使用憑證中的「授權資訊存取」(AIA) 資訊來擷取 OCSP 回應程式資訊。若要覆寫 AIA 資訊，請輸入 **Default OCSP URL**（預設 **OCSP URL**）（開頭為 **`http://`** 或 **`https://`**）。
   - 依預設，防火牆會使用在 **CA** 憑證欄位中選取的憑證來驗證 OCSP 回應。若要使用不同的憑證進行驗證，請在 **OCSP** 驗證 **CA** 憑證欄位中選取所需憑證。
4. 按一下 **OK**（確定）。CA 憑證表格會顯示指派的憑證。

©2024 Palo Alto Networks, Inc.

STEP 4 | 定義驗證憑證撤銷狀態的方法，以及相關的封鎖行為。

1. 選取**Use CRL**（使用 **CRL**）和/或**Use OCSP**（使用 **OCSP**）。如果這兩種方法您皆已選取，防火牆會先嘗試 OCSP，而且只有在 OCSP 回應程式無法使用時才會回復 CRL 方法。
2. 視驗證方法而定，輸入 **CRL Receive Timeout**（CRL 接收逾時）和/或 **OCSP Receive Timeout**（OCSP 接收逾時）。過了此間隔後 (1-60 秒)，防火牆會停止等待 CRL/OCSP 服務的回應。
3. 輸入**Certificate Status Timeout**（憑證狀態逾時）。過了此間隔 (1-60 秒)後，防火牆會停止等待任何憑證狀態服務的回應，並套用任何您定義的工作階段封鎖邏輯。**Certificate Status**（憑證狀態逾時）與 OCSP/CRL **Receive Timeout**（接收逾時）有關，如下所述：
   - 如果您啟用 OCSP 與 CRL—在經過以下兩個間隔之中較短的間隔後，防火牆會註冊要求逾時：**Certificate Status Timeout**（憑證狀態逾時）值或兩個 **Receive Timeout**（接收逾時）值的彙總。
   - 如果您僅啟用 OCSP—在經過以下兩個間隔之中較短的間隔後，防火牆會註冊要求逾時：**Certificate Status**（憑證狀態逾時）值或 OCSP **Receive Timeout**（接收逾時）值。
   - 如果您僅啟用 CRL—在經過以下兩個間隔之中較短的間隔後，防火牆會註冊要求逾時：**Certificate Status Timeout**（憑證狀態逾時）值或 CRL **Receive Timeout**（接收逾時）值。
4. 如果您想要防火牆在 OCSP 或 CRL 服務傳回憑證撤銷狀態為未知時封鎖工作階段，則選取**Block session if certificate status is unknown**（如果憑證狀態未知則封鎖工作階段）。否則，防火牆會允許這些工作階段。
5. 如果您想要防火牆在註冊 OCSP 或 CRL 要求逾時後封鎖工作階段，則選取**Block session if certificate status cannot be retrieved within timeout**（如果無法在逾時內擷取憑證狀態則封鎖工作階段）。否則，防火牆會允許這些工作階段。
6. （僅限 **GlobalProtect**）如果您希望防火牆在用戶端憑證主旨中的序號屬性與 GlobalProtect 應用程式向端點報告的主機 ID 不相符時封鎖工作階段，則選取 **Block sessions if the certificate was not issued to the authenticating device**（如果憑證未簽發給驗證裝置則封鎖工作階段）。

STEP 5 | 按一下 **OK**（確定）與 **Commit**（提交）

©2024 Palo Alto Networks, Inc.

設定 SSL/TLS 服務設定檔

Palo Alto Networks 防火牆及 Panorama 使用 SSL/TLS 服務設定檔來指定憑證及用於 SSL/TLS 服務的允許通訊協定版本。防火牆及 Panorama 會為驗證入口網站、GlobalProtect 入口網站與閘道、管理 (MGT) 介面上的輸入流量、URL 管理員取代功能以及 User-ID™ 系統日誌接聽服務使用 SSL/TLS。透過定義通訊協定版本，您可使用設定檔限制加密套件，可用於確保與要求服務的用戶端進行安全通訊。這會啟用防火牆或 Panorama 以避免載有已知弱點的 SSL/TLS 版本，從而改善網路安全性。如果服務請求包含指定範圍之外的通訊協定版本，則防火牆或 Panorama 將降級或升級支援版本的連線。

在要求防火牆服務的用戶端系統中，憑證信任清單 *(CTL)* 必須包含發出 *SSL/TLS* 服務設定檔所指定之憑證的憑證授權單位 *(CA)* 憑證。否則，使用者在要求防火牆服務時將會看見憑證錯誤。根據預設，大部分的第三方 *CA* 憑證都會顯示在用戶端瀏覽器中。如果企業或防火牆產生的 *CA* 憑證是簽發者，您就必須將該 *CA* 憑證部署至用戶端瀏覽器中的 *CTL*。

STEP 1 | 針對每個所需服務，在防火牆上產生或匯入憑證（請參閱取得憑證）。

在 *SSL/TLS* 服務設定檔中，僅使用已簽署的憑證，而非 *CA* 憑證。

STEP 2 | 選取 **Device**（裝置） > **Certificate Management**（憑證管理） > **SSL/TLS Service Profile**（**SSL/TLS** 服務設定檔）。

STEP 3 | 若防火牆具有多個虛擬系統 (vsys)，請選取可在其中使用設定檔的 **Location**（位置）（vsys 或 **Shared**（位置））。

STEP 4 | 按一下 **Add**（新增），並輸入用來識別設定檔的 **Name**（名稱）。

STEP 5 | 選取您剛剛取得的 **Certificate**（憑證）。

STEP 6 | 定義服務可使用的通訊協定範圍：

- 針對 **Min Version**（最低版本），選取最舊的允許 TLS 版本：**TLSv1.0**（預設）、**TLSv1.1** 或 **TLSv1.2**。
- 針對 **Max Version**（最高版本），選取最新的允許 TLS 版本：**TLSv1.0**、**TLSv1.1**、**TLSv1.2** 或 **Max**（最大）（最新的可用版本）。預設為 **Max**（最大）。

作為最佳做法，請將 ***Min Version***（最低版本）設為 ***TLSv1.2***，並將 ***Max Version***（最高版本）設為 ***Max***（最高）。

在執行 *PAN-OS 8.0* 或更新版本、處於 *FIPS/CC* 模式的防火牆上，***TLSv1.1*** 是最低支援的 *TLS* 版本；不要選 ***TLSv1.0***。

要求倚賴 *TLSv1.2* 的防火牆服務時所使用的用戶端憑證，不可用 *SHA512* 作為摘要演算法。這些用戶端憑證必須使用較低的摘要演算法（例如 *SHA384*），或您必須將防火牆服務的 ***Max Version***（最高版本）限定為 ***TLSv1.1***。

©2024 Palo Alto Networks, Inc.

STEP 7 | 按一下 **OK**（確定）與 **Commit**（提交）。

©2024 Palo Alto Networks, Inc.

設定 SSL 服務設定檔

SSH 服務設定檔可讓您自訂 SSH 參數，以增強指向 Palo Alto Networks 管理和高可用性 (HA) 設備的 SSH 連線的安全性與完整性。依預設，SSH 支援所有密碼、金鑰交換演算法和訊息驗證碼，這讓您的連線易於受到攻擊。在 SSH 服務設定檔中，您可以限制 SSH 伺服器支援的演算法。您還可以產生新的主機金鑰，並為 SSH 工作階段金鑰的重新產生和交換指定資料量、時間和基於封包的臨界值。

根據 SSH 伺服器執行個體，設定管理或 HA SSH 服務設定檔。您可以從防火牆、Panorama™ Web 介面（如果將設定套用至多個防火牆或設備）或 CLI 設定設定檔。

您最多可以設定四個管理和四個 *HA* 伺服器設定檔。

要對收集器群組中的每個專用日誌收集器（日誌收集器模式中的 *M-series* 或 *Panorama* 虛擬設備）使用同一 *SSH* 連線設定，請從 *Panorama* 管理伺服器設定 *SSH* 服務設定檔，將您的變更 ***Commit***（提交）到 *Panorama*，然後將設定 ***Push***（推送）到日誌收集器。您還可以使用 ***set log-collector-group <name> general-setting management ssh*** 命令從 *CLI* 執行這些步驟。

- 建立 SSH 管理設定檔
- 建立 SSH HA 設定檔

建立 SSH 管理設定檔

要為管理連線自訂 SSH 設定，請建立 SSH 管理設定檔。

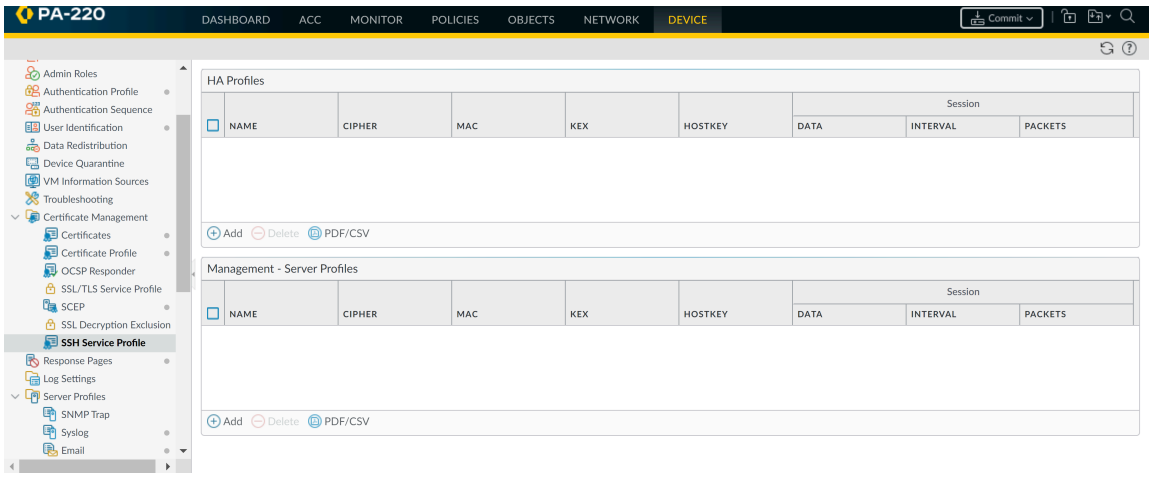
您可以從 *CLI* 設定或更新現有管理設定檔。

©2024 Palo Alto Networks, Inc.

STEP 1 | 建立管理-伺服器設定檔。

1. 選取 **Device**（裝置） > **Certification Management**（憑證管理） > **SSH Service Profile**（**SSH** 服務設定檔）。
2. **Add**（新增）管理-伺服器設定檔。

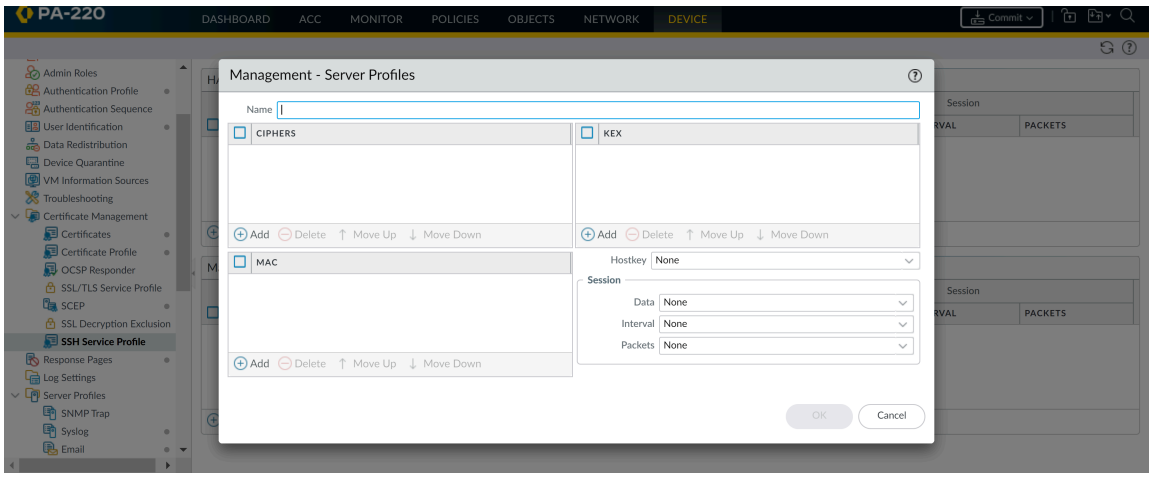
©2024 Palo Alto Networks, Inc.



©2024 Palo Alto Networks, Inc.

3. 輸入用來識別設定檔的 **Name**（名稱）。
4. （選用）**Add**（新增）該設定檔支援的密碼、訊息驗證碼或金鑰交換演算法。
5. （選用）選取 **Hostkey** 和金鑰長度。
6. （選用）為 SSH 工作階段金鑰更新參數輸入值：**Data**（資料）、**Interval**（間隔）和 **Packets**（封包數）。

©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.

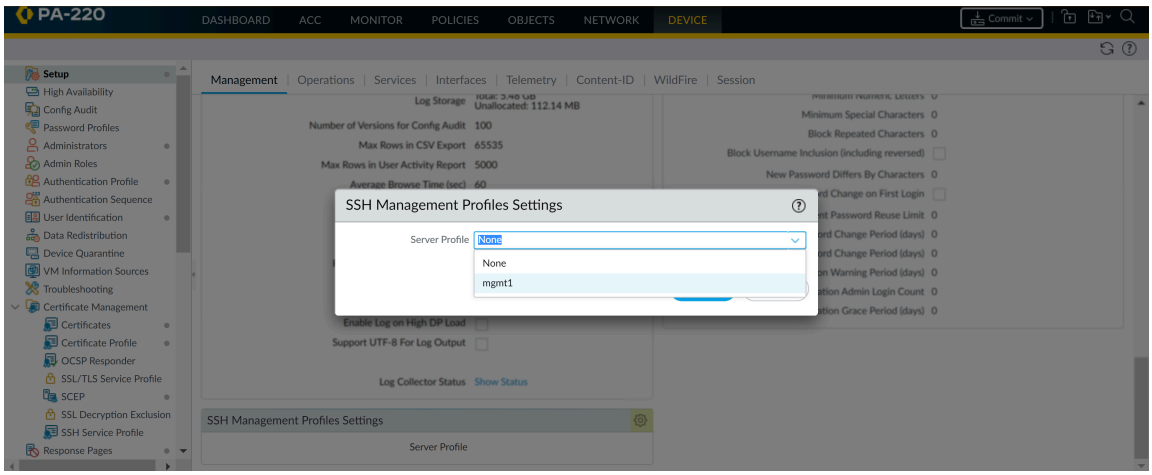
7. 按一下 **OK**（確定）並 **Commit**（交付）變更。

©2024 Palo Alto Networks, Inc.

STEP 2 | 選取要套用的管理設定檔。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理）。
2. 在 SSH 管理設定檔設定下，選取一個現有設定檔。

©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.

3. 按一下 **OK**（確定）並 **Commit**（交付）變更。

STEP 3 | 從 CLI 重新啟動管理 SSH 服務以套用設定檔。

每次套用新設定檔或對使用中的設定檔進行變更時，都需要重新啟動連線。設定變更不會影響作用中的工作階段，新設定檔會套用至之後的連線（或工作階段）。

使用 **`set ssh service-restart mgmt`** CLI 命令。

建立 SSH HA 設定檔

要保護 HA 配對中設備之間的 SSH 通訊，請建立 SSH HA 設定檔。在建立設定檔之前，請在 HA 對等之間建立 HA 連線。要建立 HA 連線，您需要在控制連結連線上啟用加密，將 HA 金鑰匯出至某個網路位置，並在對等上匯入 HA 金鑰。（請參閱設定主動/被動 HA 或設定主動/主動 HA。）

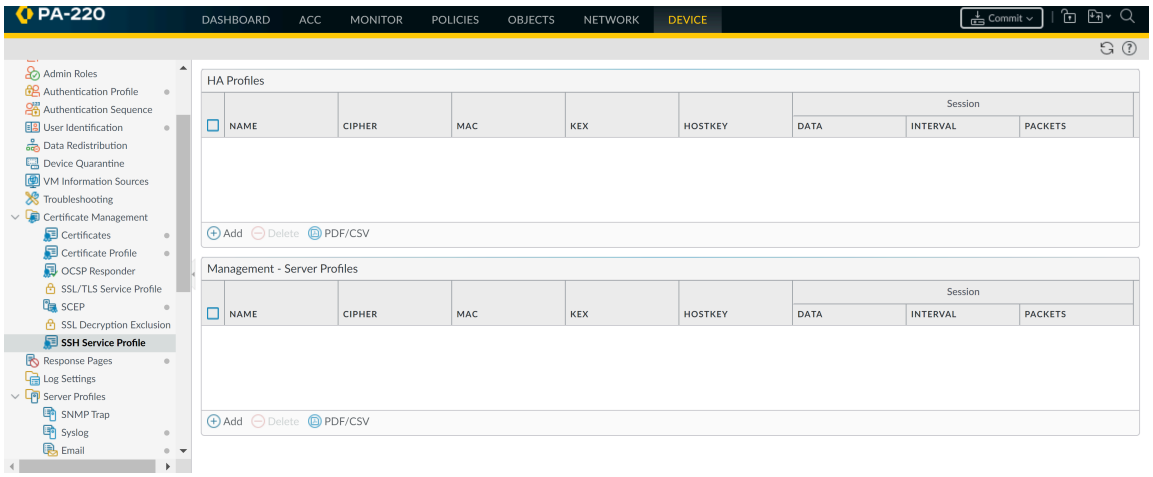
您可以從 *CLI* 設定或更新現有 HA 設定檔。

©2024 Palo Alto Networks, Inc.

STEP 1 | 建立 HA 設定檔。

1. 選取 **Device**（裝置） > **Certification Management**（憑證管理） > **SSH Service Profile**（**SSH** 服務設定檔）。
2. **Add**（新增） HA 設定檔。

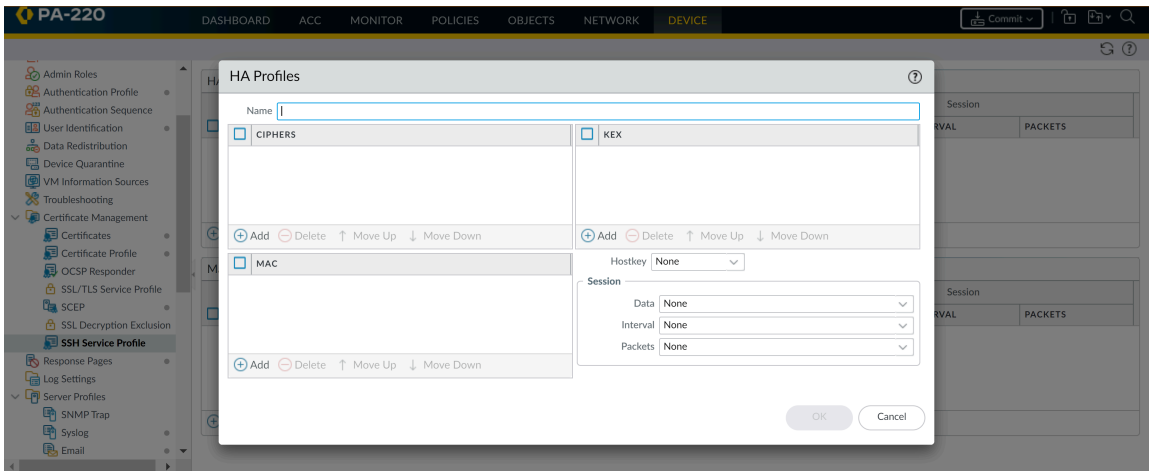
©2024 Palo Alto Networks, Inc.



©2024 Palo Alto Networks, Inc.

3. 輸入用來識別設定檔的 **Name**（名稱）。
4. （選用）**Add**（新增）該設定檔支援的密碼、訊息驗證碼或金鑰交換演算法。
5. （選用）選取 **Hostkey** 和金鑰長度。
6. （選用）為 SSH 工作階段金鑰更新參數輸入值：**Data**（資料）、**Interval**（間隔）和 **Packets**（封包數）。

©2024 Palo Alto Networks, Inc.



©2024 Palo Alto Networks, Inc.

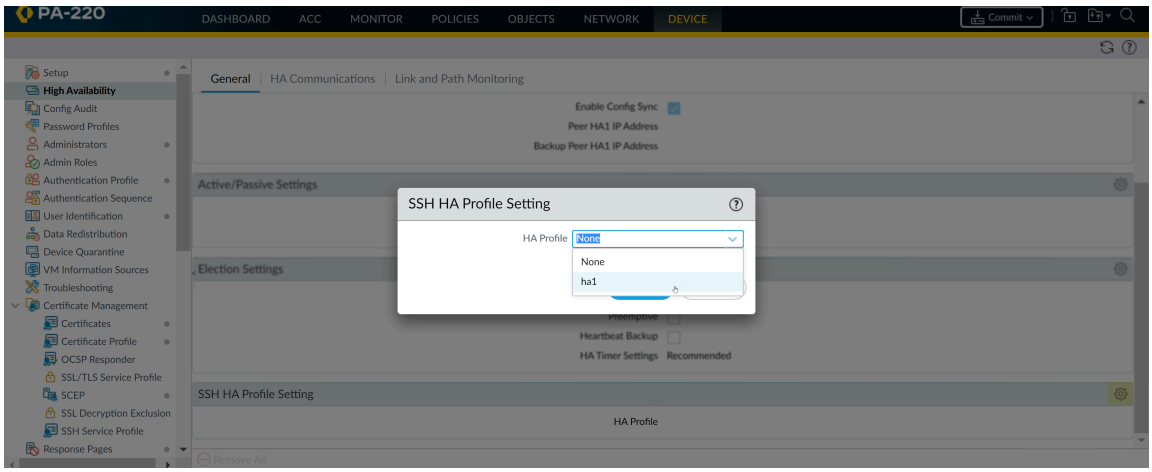
7. 按一下 **OK**（確定）並 **Commit**（交付）變更。

©2024 Palo Alto Networks, Inc.

STEP 2 | 選取要套用的 HA 設定檔。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般）。
2. 在 SSH HA 設定檔設定下，選取一個現有設定檔。

©2024 Palo Alto Networks, Inc.



©2024 Palo Alto Networks, Inc.

3. 按一下 **OK**（確定）並 **Commit**（交付）變更。

STEP 3 | 從 CLI 重新啟動 HA1 SSH 服務以套用設定檔。

每次套用新設定檔或對使用中的設定檔進行變更時，都需要重新啟動連線。設定變更不會影響作用中的工作階段，新設定檔會套用至之後的連線（或工作階段）。

使用 **`set ssh service-restart ha`** CLI 命令。

如果 *HA* 對中的設備之間存在連線，您可以使用以下命令來最大程度地減少 *SSH* 服務重新啟動帶來的停機時間。

- （已設定 *HA1* 備份）*admin@PA-3260>* ***`request high-availability session-reestablish`***
- （未設定 *HA1* 備份或者 *HA1* 備份連結已中斷）*admin@PA-3260>* ***`request high-availability session-reestablish force`***

  如果沒有 *HA1* 備份，可以強制防火牆重新建立 *HA1* 工作階段。但是，這會導致短暫的「核心分裂」情況，*HA* 對等無法相互偵測並因此承擔主動角色。（當設定的 *HA1* 備份沒有效果時，使用 ***`force`*** 選項。）

©2024 Palo Alto Networks, Inc.

取代輸入管理流量的憑證

首次啟動防火牆或 Panorama 時，將會自動產生預設憑證，可存取網頁介面、支援管理 (MGT) 介面的 XML API 以及支援 HTTPS 管理流量的任何其他介面（詳細資訊，請參閱使用介面管理設定檔限制存取）。若要提高輸入管理流量的安全性，用您組織特別簽發的新憑證取代預設憑證。

您無法檢視、修改或刪除預設憑證。

若要保護管理流量，必須設定管理帳戶和驗證。

STEP 1 | 取得將用於驗證管理員用戶端系統防火牆或 Panorama 的憑證。

可使用用戶端系統已經信任的憑證簡化憑證部署。因此，我們建議您從企業憑證授權單位 (CA) 匯入憑證與私密金鑰或從外部 CA 取得憑證；用戶端系統的受信任根憑證儲存區已有保證受信任的相關根 CA 憑證。

如果您在防火牆或 *Panorama* 上產生憑證，管理員將會看到憑證錯誤，因為該根 *CA* 憑證不在用戶端系統的受信任憑證儲存區中。若要防止此狀況發生，請將自我簽署的根 *CA* 憑證部署到所有用戶端系統上。

無論以何種方式取得憑證，我們建議採用 ***sha256*** 的 ***Digest***（摘要）演算法或更高算法，以增強安全性。

STEP 2 | 設定 SSL/TLS 服務設定檔。

選取您剛剛取得的 **Certificate**（憑證）。

若要增強安全性，我們建議您針對輸入管理流量將 ***Min Version***（最低版本）（允許的最早 *TLS* 版本）設定為 ***TLSv1.2***。我們還推薦針對每項防火牆或 *Panorama* 服務使用不同的 *SSL/TLS* 服務設定檔，而非對所有服務重複使用此設定檔。

STEP 3 | 將 SSL/TLS 服務設定檔套用至輸入管理流量。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理），然後編輯 General Settings（一般設定）。
2. 選取您剛才設定的 **SSL/TLS Service Profile**（**SSL/TLS** 服務設定檔）。
3. 按一下 **OK**（確定）與 **Commit**（提交）。

©2024 Palo Alto Networks, Inc.

設定 SSL 正向 Proxy 伺服器憑證的金鑰大小

在 Ssl 正向 Proxy工作階段中回應用戶端時，防火牆會建立目的地伺服器呈現的憑證複本，然後使用該複本與用戶端間建立連線。依預設，防火牆所產生憑證的金鑰大小，與目的地伺服器所呈現的憑證相同。然而，您可以如下所示變更防火牆所產生憑證的金鑰大小。

STEP 1 | 選取 **Device**（裝置） > **Setup**（設定） > **Session**（工作階段），然後在 Decryption Settings（解密設定）區段中按一下 **SSL Forward Proxy Settings**（**Ssl** 正向 **Proxy** 設定）。

STEP 2 | 選取 **Key Size**（金鑰大小）：

- 由目的地主機定義—防火牆會決定根據目的地伺服器憑證，來決定所產生用來與用戶端之間建立 SSL Proxy 工作階段之憑證中的金鑰大小和雜湊演算法。如果目的地伺服器使用 1024 位元 RSA 金鑰，則防火牆會使用 1024 位元 RSA 金鑰產生憑證。如果目的地伺服器使用大於 1,024 位元的金鑰大小（例如 2,048 位元或 4,096 位元），則防火牆會產生使用 2,048 位元 RSA 金鑰的憑證。如果目的地伺服器使用 SHA-1 雜湊演算法，則防火牆會使用 SHA-1 雜湊演算法產生憑證。如果目的地伺服器使用強於 SHA-1 的雜湊演算法，則防火牆會使用 SHA-256 演算法產生憑證。這是預設設定。
- **1024** 位元 **RSA**—防火牆會產生使用 1024 位元 RSA 金鑰與 SHA-256 雜湊演算法的憑證，無論目的地伺服器憑證的金鑰大小為何。從 2013 年 12 月 31 日開始，公開憑證授權單位 (CA) 和受歡迎的瀏覽器針對使用少於 2,048 位元之金鑰的 X.509 憑證，提供有限的支援。未來在向瀏覽器呈現這類金鑰時，視安全性設定而定，瀏覽器可警告使用者或將 SSL/TLS 工作階段整個封鎖。
- **2048** 位元 **RSA**—防火牆會產生使用 1024 位元 RSA 金鑰與 SHA-256 雜湊演算法的憑證，無論目的地伺服器憑證的金鑰大小為何。公開 CA 和受歡迎的瀏覽器支援 2,048 位元金鑰，其提供比 1,024 位元金鑰更佳的安全性。

變更金鑰大小設定會清除目前的憑證快取。

STEP 3 | 按一下 **OK**（確定）與 **Commit**（提交）。

©2024 Palo Alto Networks, Inc.

撤銷與更新憑證

撤銷憑證

有各種狀況會讓憑證在到期日前失效。例如名稱改變、主體與憑證授權單位間的關聯改變 (例如員工離職)，以及私密金鑰遭到洩露 (已知或疑似)。在上述狀況下，簽發該憑證的憑證授權單位 (CA) 必須撤銷憑證。下列工作說明如何撤銷防火牆為其 CA 的憑證。

STEP 1 | 選取 **Device**（設備） > **Certificate Management**（憑證管理） > **Certificates**（憑證） > **Device Certificates**（裝置憑證）。

STEP 2 | 如果防火牆支援多個虛擬系統，則頁籤會顯示 **Location**（位置）下拉式清單。選取憑證所屬的虛擬系統。

STEP 3 | 選取要撤銷的憑證。

STEP 4 | 按一下撤銷。PAN-OS 會立即將憑證狀態設為已撤銷，並將序號新增至線上憑證狀態通訊協定 (OCSP) 回應程式快取或憑證撤銷清單 (CRL)。您不必執行認可。

更新憑證

如果憑證過期或即將過期，您可以重設有效期間。如果外部憑證授權單位 (CA) 已簽署憑證，且防火牆使用線上憑證狀態通訊協定 (OCSP) 驗證憑證撤銷狀態，防火牆會使用 OCSP 回應程式資訊更新憑證狀態（請參閱設定 OCSP 回應程式）。如果防火牆為簽發憑證的 CA，則防火牆會用與舊憑證序號不同但屬性相同的新憑證予以取代。

STEP 1 | 選取 **Device**（設備） > **Certificate Management**（憑證管理） > **Certificates**（憑證） > **Device Certificates**（裝置憑證）。

STEP 2 | 若防火牆具有一個以上的虛擬系統 (vsys)，為憑證選取一個 **Location**（位置）（vsys 或 **Shared**（共用））。

STEP 3 | 選取要更新的憑證，再按一下**Renew**（更新）。

STEP 4 | 輸入**New Expiration Interval**（新過期間隔）（天數）。

STEP 5 | 按一下 **OK**（確定）與 **Commit**（提交）。

©2024 Palo Alto Networks, Inc.

使用硬體安全性模組保護金鑰

硬體安全性模組 (HSM) 是管理數位金鑰的實體裝置。HSM 能夠安全地儲存與產生數位金鑰。同時提供邏輯與實體方法保護這些材料免遭未經授權的使用與潛在對手的危害。

HSM 用戶端已與 Palo Alto Networks 防火牆及 Panorama 整合，能夠增強 SSL/TLS 解密（SSL 正向 Proxy 與 SSL 輸入檢查）中所使用私密金鑰的安全性。此外，您可以使用 HSM 將主要金鑰加密。

下列主題說明如何將 HSM 與防火牆或 Panorama 整合：

- 設定與 HSM 的連線
- 使用 HSM 加密主要金鑰
- 將私密金鑰存放在 HSM 上
- 管理 HSM 部署

設定與 HSM 的連線

HSM 用戶端已與 PA-3200 Series、PA-3400 Series、PA-5200 Series、PA-5400 Series、PA-7000 Series 和 VM-Series 防火牆以及 Panorama 管理伺服器（虛擬設備與 M-Series 設備）整合，可與下列 HSM 廠商搭配使用：

- **nCipher nShield Connect**—支援的用戶端版本視乎 PAN-OS 版本：
  - PAN-OS 11.0 支援用戶端版本 12.40.2（回溯相容至舊版設備的用戶端版本 11.50）。
  - PAN-OS 9.1、9.0 和 8.1 支援用戶端版本 12.30。
  - PAN-OS 8.0 以及較早版本支援用戶端版本 11.62。
- **SafeNet Network**—支援的用戶端版本視乎 PAN-OS 版本：
  - PAN-OS 11.0 支援用戶端版本 5.4.2 和 7.2。
  - PAN-OS 9.1 和 9.0 支援用戶端版本 5.4.2 和 6.3。
  - PAN-OS 8.1 支援用戶端版本 5.4.2 和 6.2.2。
  - PAN-OS 8.0.2 及更新的 PAN-OS 8.0 版本（以及 PAN-OS 7.1.10 及更新的 PAN-OS 7.1 版本）支援用戶端版本 5.2.1、5.4.2 和 6.2.2。

HSM 伺服器版本必須與這些用戶端版本相容。請參閱 HSM 廠商文件中的用戶端-伺服器版本相容表。在防火牆或 Panorama 上，使用以下程序來選取與 SafeNet HSM 伺服器相容的 SafeNet Network 用戶端版本。

升級 *HSM* 伺服器後，下載 *HSM* 伺服器可能不是合適選擇。

- 設定與 SafeNet Network HSM 的連線
- 設定與 nCipher nShield Connect HSM 的連線

©2024 Palo Alto Networks, Inc.

安裝 SafeNet 用戶端 RPM 封包管理員。

1. 選取 **Device**（裝置） > **Setup**（設定） > **HSM**，並 **Select HSM Client Version**（選取 **HSM** 用戶端版本）（Hardware Security Operations（硬體安全性操作）設定）。
2. 根據具體情況為 HSM 伺服器版本選取 **Version 5.4.2**（版本 **5.4.2**）（預設值）或 **7.2**。
3. 按一下 **OK**（確定）。
4. （只在在防火牆上變更 HSM 版本才需執行此步驟）若成功變更版本，防火牆會提示您重新啟動以變更至新 HSM 版本。如果收到提示，請按一下 **Yes**（是）。
5. 如果主要金鑰不在防火牆上，則用戶端版本升級會失敗。**Close**（關閉）訊息並將主要金鑰儲存在防火牆上：
   - 編輯 Hardware Security Module Provider（硬體安全性模組提供者）並停用（清除）**Master Key Secured by HSM**（**HSM** 保護的主要金鑰）選項。
   - 按一下 **OK**（確定）。
   - 選取 **Device**（裝置） > **Master Key and Diagnostics**（主要金鑰與診斷）以編輯 Master Key（主要金鑰）。
   - 輸入 **Current Master Key**（目前主要金鑰）；之後可輸入這一相同金鑰作為 **New Master Key**（新主要金鑰），然後 **Confirm New Master Key**（確認新主要金鑰）。
   - 按一下 **OK**（確定）。
   - 重複前四個步驟以 **Select HSM Client Version**（選取 **HSM** 用戶端版本），然後再次重新啟動。

設定與 SafeNet Network HSM 的連線

若要建立 Palo Alto Networks 防火牆（HSM 用戶端）與 SafeNet Network HSM 伺服器的連線，您必須指定該伺服器的 IP 位址，輸入向伺服器驗證防火牆的密碼，然後向伺服器註冊防火牆。設定 HSM 用戶端前，在 HSM 伺服器上建立用於防火牆的分割區，並確認防火牆上的 SafeNet Network 用戶端版本與您的 SafeNet Network HSM 伺服器相容（請參閱設定與 HSM 的連線）。

在 HSM 和防火牆連線之前，HSM 將根據防火牆 IP 位址驗證防火牆。因此，您必須設定防火牆使用靜態 IP 位址—而不要使用透過 DHCP 指派的動態位址。若在執行階段期間，防火牆 IP 位址發生變更，HSM 上的作業將會停止。

HSM 組態不會在高可用性 *(HA)* 防火牆對等體之間保持同步。因此，您必須在每個對等體上單獨設定 *HSM*。在主動/被動 *HA* 組態中，您必須手動執行一次容錯移轉，以單獨設定並向 *HSM* 驗證每個 *HA* 對等體。首次執行此手動容錯移轉後，不需要使用者操作，容錯移轉就能正常運作。

©2024 Palo Alto Networks, Inc.

STEP 1 | 為每個 SafeNet Network HSM 定義連線設定。

1. 登入防火牆 Web 介面，選取 **Device**（裝置） > **Setup**（設定） > **HSM**。
2. 編輯 Hardware Security Module Provider（硬體安全性模組提供者）設定，然後將 **Provider Configured**（已設定提供者）設定為 **SafeNet Network HSM**。
3. 按照下列步驟 **Add**（新增）每一個 HSM 伺服器。高可用性 (HA) HSM 組態需要至少兩個伺服器；您可擁有至多由 16 個 HSM 伺服器構成的叢集。叢集中的所有 HSM 伺服器必須執行相同的 SafeNet 版本，而且需單獨進行驗證。只有在需在整個叢集中複製金鑰的情況下，方可使用 SafeNet 叢集。或者，您可新增至多 16 個 SafeNet HSM 伺服器以單獨運作。
   1. 輸入 HSM 伺服器的 **Module Name**（模組名稱）（由至多 31 個字元組成的 ASCII 字串）。
   2. 輸入 IPv4 位址，作為 HSM **Server Address**（伺服器位址）。
4. （僅限 HA）選取 **High Availability**（高可用性），指定 **Auto Recovery Retry**（自動復原重試）值（容錯移轉至 HSM HA 對等體伺服器之前，HSM 用戶端嘗試復原其與 HSM 伺服器連線的最大次數；範圍為 0 至 500；預設值為 0），並輸入 **High Availability Group Name**（高可用性群組名稱）（由至多 31 個字元組成的 ASCII 字串）。

   如果設定兩個或更多 *HSM* 伺服器，最佳做法是啟用 ***High Availability***（高可用性）。否則防火牆不會使用其他 *HSM* 伺服器。
5. 按一下 **OK**（確定）並 **Commit**（交付）變更。

STEP 2 | （選用）如果您不希望伺服器透過管理介面（預設）連線，則設定服務路由，以連線至 HSM。

如果您為 *HSM* 設定了服務路由，則執行 *CLI* 命令 ***clear session all*** 會清除所有現有的 *HSM* 工作階段，造成所有 *HSM* 先關閉再重新啟動。*HSM* 需要數秒鐘的時間復原，在這段期間，所有的 *SSL/TLS* 操作都會失敗。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Services**（服務），然後按一下 **Service Route Configuration**（服務路由組態）。
2. **Customize**（自訂）服務路由。預設會啟用 **IPv4** 頁籤。
3. 按一下 Service（服務）欄中的 **HSM**。
4. 為 HSM 選取 **Source Interface**（來源介面）。
5. 按一下 **OK**（確定）並 **Commit**（交付）變更。

©2024 Palo Alto Networks, Inc.

STEP 3 | 設定要對 HSM 驗證的防火牆。

1. 選取 **Device**（裝置） > **Setup**（設定），然後 **Setup Hardware Security Module**（設定硬體安全性模組）。
2. 選取 HSM **Server Name**（伺服器名稱）。
3. 為您的驗證和信任憑證選取 **Automatic**（自動）或 **Manual**（手動）。
4. 輸入管理員密碼對 HSM 驗證防火牆。
5. 按一下 **OK**（確定）。

   防火牆會嘗試向 HSM 驗證，並顯示狀態訊息。
6. 再按一下 **OK**（確定）。

STEP 4 | 將防火牆向 HSM 伺服器註冊為 HSM 用戶端，並將防火牆指派給 HSM 上的某個分割區。

如果 *HSM* 上已註冊具有相同 <*cl-name*> 的防火牆，則您必須先執行 ***client delete -client <cl-name>*** 命令，以移除重複註冊，其中 <*cl-name*> 為您要刪除之已註冊用戶端（防火牆）的名稱。

1. 從遠端系統登入 HSM。
2. 使用 **client register -c *<cl-name>* -ip *<fw-ip-addr>*** CLI 命令註冊防火牆，其中 <*cl-name*> 是您為要在 HSM 上使用的防火牆指派的名稱，<*fw-ip-addr*> 是該防火牆的 IP 位址。
3. 使用 **client assignpartition -c *<cl-name>* -p *<partition-name>*** CLI 命令為防火牆指派分割區，其中 <*cl-name*> 是使用 **client register** 命令為防火牆指派的名稱，<*partition-name*> 是您之前設定要指派給此防火牆的分割區名稱。

STEP 5 | 設定防火牆與 HSM 分割區連接。

1. 選取 **Device**（裝置） > **Setup**（設定） > **HSM**，並重新整理 ( ) 顯示。
2. **Setup HSM Partition**（設定 **HSM** 分割區）（Hardware Security Operations（硬體安全性操作）設定）。
3. 輸入分割區密碼對 HSM 上的分割區驗證防火牆。
4. 按一下 **OK**（確定）。

STEP 6 | （僅限 HA）重複之前的驗證、註冊和分割區連線步驟，為現有 HA 群組新增其他 HSM。

如果要從組態中移除 *HSM*，可重複前面的分割區連線步驟，將已刪除的 *HSM* 從 *HA* 群組中移除。

©2024 Palo Alto Networks, Inc.

STEP 7 | 確認防火牆是否與 HSM 連線、是否已向其驗證。

1. 選取 **Device**（裝置） > **Setup**（設定） > **HSM**，然後檢查驗證和連線狀態：
   - 綠色—防火牆已成功驗證並連線至 HSM。
   - 紅色—防火牆向 HSM 驗證失敗，或與 HSM 的網路連線中斷。
2. 檢視 Hardware Security Module Status（硬體安全性模組狀態）中的下列欄，以判定驗證狀態：
   - 序號—如果防火牆向 HSM 驗證成功，則為 HSM 分割區的序號。
   - 分割區—HSM 上指派給防火牆的分割區名稱。
   - 模組狀態—HSM 連線的目前狀態。如果 Hardware Security Module Status（硬體安全性模組狀態）顯示 HSM，則此值始終為 `Authenticated`。

設定與 nCipher nShield Connect HSM 的連線

您必須設定遠端檔案系統 (RFS) 作為中樞來同步組織中所有使用 nCipher nShield Connect HSM 的防火牆（HSM 用戶端）的關鍵資料。為了確保防火牆上的 nShield Connect 用戶端版本與 nShield Connect 伺服器相容，請參閱設定與 HSM 的連線。

在 HSM 和防火牆連線之前，HSM 將根據防火牆 IP 位址驗證防火牆。因此，您必須設定防火牆以使用靜態 IP 位址，而不要使用透過 DHCP 指派的動態位址。（若在執行階段期間，防火牆 IP 位址發生變更，HSM 上的作業將會停止）。

HSM 組態不會在高可用性 *(HA)* 防火牆對等體之間保持同步。因此，您必須在每個對等體上單獨設定 *HSM*。在主動/被動 *HA* 組態中，您必須手動執行一次容錯移轉，以單獨設定並向 *HSM* 驗證每個 *HA* 對等體。首次執行此手動容錯移轉後，不需要使用者操作，容錯移轉就能正常運作。

Thales/nCipher HSM 不支援 *ECDSA* 憑證。

STEP 1 | 為每個 nCipher nShield Connect HSM 定義連線設定。

1. 登入防火牆 Web 介面，選取 **Device**（裝置） > **Setup**（設定） > **HSM**。
2. 編輯 Hardware Security Module Provider（硬體安全性模組提供者）設定，然後將 **Provider Configured**（已設定提供者）設定為 **nShield Connect**。
3. 按照下列步驟 **Add**（新增）每一個 HSM 伺服器。HA HSM 組態需要兩個伺服器。
   1. 輸入 HSM 伺服器的 **Module Name**（模組名稱）。可以時任何 ASCII 字串，最長 31 個字元。
   2. 輸入 IPv4 位址，作為 HSM **Server Address**（伺服器位址）。
4. 輸入一個 IPv4 位址，作為 **Remote Filesystem Address**（遠端檔案系統位址）。
5. 按一下 **OK**（確定）並 **Commit**（交付）變更。

©2024 Palo Alto Networks, Inc.

STEP 2 | （選用）如果您不希望伺服器透過管理介面（預設）連線，則設定服務路由，以連線至 HSM。

如果您為 *HSM* 設定了服務路由，則執行 *CLI* 命令 ***clear session all*** 會清除所有現有的 *HSM* 工作階段，造成所有 *HSM* 先關閉再重新啟動。*HSM* 需要數秒鐘的時間復原，在這段期間，所有的 *SSL/TLS* 操作都會失敗。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Services**（服務），然後按一下 **Service Route Configuration**（服務路由組態）。
2. **Customize**（自訂）服務路由。預設會啟用 **IPv4** 頁籤。
3. 按一下 Service（服務）欄中的 **HSM**。
4. 為 HSM 選取 **Source Interface**（來源介面）。
5. 按一下 **OK**（確定）並 **Commit**（交付）變更。

STEP 3 | 向 HSM 伺服器註冊防火牆（作為 HSM 用戶端）。

此步驟簡短說明使用 Nshield Connect HSM 前面板介面的程序。如需詳細資訊，請參閱 nCipher 文件。

1. 登入 nCipher nShield Connect HSM 的前面板顯示畫面。
2. 使用右側導覽按鈕，選取 **System**（系統） > **System configuration**（系統組態） > **Client config**（用戶端組態） > **New client**（新用戶端）。
3. 輸入防火牆 IP 位址。
4. 選取 **System**（系統） > **System configuration**（系統組態） > **Client config**（用戶端組態） > **Remote file system**（遠端檔案系統），然後輸入您用來安裝遠端檔案系統的用戶端電腦 IP 位址。

©2024 Palo Alto Networks, Inc.

STEP 4 | 設定 RFS 以接受來自防火牆的連線。

1. 從 Linux 用戶端登入 RFS。
2. 透過執行 **anonkneti *<ip-address>*** CLI 命令，取得電子序號 (ESN) 和 K_{NETI} 金鑰（用於向用戶端驗證 HSM）的雜湊，其中 <*ip-address*> 是 HSM 的 IP 位址。

   例如：

   ```
   anonkneti 192.0.2.1
   ```

   ```
   B1E2-2D4C-E6A2 5a2e5107e70d525615a903f6391ad72b1c03352c
   ```

   在此範例中，`B1E2-2D4C-E6A2` 是 ESN，`5a2e5107e70d525615a903f6391ad72b1c03352c` 是 K_{NETI} 金鑰的雜湊。
3. 從超級使用者帳戶使用下列命令執行 RFS 設定：

   ```
   rfs-setup --force <ip-address> <ESN> <hash-Kneti-key>
   ```

   <*ip-address*> 是 HSM 的 IP 位址，<*ESN*> 是電子序號，<*hash-Kneti-key*> 是 K_{NETI} 金鑰的雜湊。

   下列範例使用此程序中包含的值：

   ```
   rfs-setup --force 192.0.2.1 B1E2-2D4C-E6A2
    5a2e5107e70d525615a903f6391ad72b1c03352c
   ```
4. 使用下列命令在 RFS 上允許 HSM 用戶端提交：

   ```
   rfs-setup --gang-client --write-noauth <FW-IPaddress>
   ```

   其中 <*FW-IPaddress*> 是防火牆 IP 位址。

STEP 5 | 向 HSM 驗證防火牆。

1. 在防火牆 Web 介面中，選取 **Device**（裝置） > **Setup**（設定） > **HSM**，然後 **Setup Hardware Security Module**（設定硬體安全性模組）。
2. 按一下 **OK**（確定）。

   防火牆會嘗試向 HSM 驗證，並顯示狀態訊息。
3. 按一下 **OK**（確定）。

STEP 6 | 選取 **Device**（裝置） > **Setup**（設定） > **HSM** 和 **Synchronize with Remote Filesystem**（與遠端檔案系統同步），同步防火牆與 RFS。

©2024 Palo Alto Networks, Inc.

STEP 7 | 確認防火牆是否與 HSM 連線、是否已向其驗證。

1. 選取 **Device**（裝置） > **Setup**（設定） > **HSM**，然後檢查驗證和連線狀態：
   - 綠色—防火牆已成功驗證並連線至 HSM。
   - 紅色—防火牆向 HSM 驗證失敗，或與 HSM 的網路連線中斷。
2. 檢視 Hardware Security Module Status（硬體安全性模組狀態），以判定驗證狀態。
   - 名稱—HSM 的名稱。
   - **IP** 位址—HSM 的 IP 位址。
   - 模組狀態—HSM 連線的目前狀態:`Authenticated` 或 `NotAuthenticated`。

使用 HSM 加密主要金鑰

主要金鑰用於加密防火牆和 Panorama 上的所有私密金鑰和密碼。如果您具有將私密金鑰存放在安全位置的安全需求，則可以使用存放在 HSM 的加密金鑰來加密主要金鑰。在需要解密防火牆上的密碼或私密金鑰時，防火牆或 Panorama 會要求 HSM 解密主要金鑰。一般而言，HSM 位於高度安全的位置，與防火牆或 Panorama 分開，因此安全性更高。

HSM 使用封裝金鑰加密主要金鑰。為了保持安全性，您必須不定期變更（重新整理）此封裝金鑰。

下列主題先說明如何加密主要金鑰，再說明如何重新整理主要金鑰加密：

- 加密主要金鑰
- 重新整理主要金鑰加密

加密主要金鑰

如果您先前尚未加密防火牆上的主要金鑰，請使用下列程序加密。此程序適用於首次加密金鑰，或者是您在定義新的主要金鑰且您想要將它解密時。如果您想要重新整理先前已加密金鑰上的加密時，請參閱重新整理主要金鑰加密。

STEP 1 | 選取 **Device**（裝置） > **Master Key and Diagnostics**（主要金鑰與診斷）。

STEP 2 | 在 **Master Key**（主要金鑰）欄位中，指定目前用來加密防火牆上所有私密金鑰與密碼的金鑰。

STEP 3 | 如果變更主要金鑰，請輸入新的主要金鑰並確認。

STEP 4 | 選取 **HSM** 核取方塊。

- 存留時間—主要金鑰將於多少天及多少小時之後過期（範圍為 1-730 天）。
- 提醒時間—當使用者收到即將過期的通知時，將於多少天及多少小時後過期（範圍為 1-365 天）。

STEP 5 | 按一下 **OK**（確定）。

©2024 Palo Alto Networks, Inc.

重新整理主要金鑰加密

最佳做法是輪換使用加密所用的封裝金鑰，定期重新整理主要金鑰加密。輪換頻率視乎於應用程式。封裝金鑰存放在 HSM 上。下列命令為 SafeNet Network 和 nCipher nShield Connect HSM 通用。

STEP 1 | 登入防火牆 CLI。

STEP 2 | 使用下列 CLI 命令在 HSM 上輪換主要金鑰的封裝金鑰：

```
> request hsm mkey-wrapping-key-rotation
```

如果主要金鑰在 HSM 上加密，則 CLI 命令會在 HSM 上產生新的封裝金鑰，並使用新的封裝金鑰加密主要金鑰。

如果主要金鑰未在 HSM 上加密，則 CLI 命令將在 HSM 上產生新的封裝金鑰，以供未來使用。

此命令不會刪除舊的封裝金鑰。

將私密金鑰存放在 HSM 上

為了提升安全性，您可針對下列情況使用 HSM 確保用於 SSL/TLS 解密私密金鑰的安全：

- Ssl 正向 Proxy—HSM 可儲存轉送信任憑證的私密金鑰，用於在 SSL/TLS 正向 Proxy 操作中簽署憑證。接著防火牆會將它在此操作期間產生的憑證傳送到 HSM 以進行簽署，再將這些憑證轉送到用戶端。
- SSL 輸入檢查 — HSM 可儲存您要執行 SSL/TLS 輸入檢查的內部伺服器私密金鑰。

如果您使用 DHE 或 ECDHE 金鑰交換演算法啟用 SSL 解密的完美轉送密碼 (PFS) 支援，則可使用 HSM 來儲存用於 SSL 輸入檢查的私密金鑰。您也可使用 HSM 來儲存用於 SSL 正向 Proxy 或 SSL 輸入檢查解密的 ECDSA 金鑰，除非您正在使用 TLSv1.3。對於 TLSv1.3 流量，PAN-OS 僅對於 SSL 正向 Proxy 支援 HSM。它對於 SSL 輸入檢查不支援 HSM。

STEP 1 | 在 HSM 上，匯入或產生用於解密部署的憑證和私密金鑰。

關於在 HSM 上匯入或產生憑證和私密金鑰的說明，請參閱 HSM 文件。

STEP 2 | （僅限 nCipher nShield Connect）將 nCipher nShield 遠端檔案系統中的重要資料同步至防火牆。

與 *SafeNet Network HSM* 的同步會自動進行。

1. 存取防火牆網頁介面並選取 **Device**（裝置） > **Setup**（設定） > **HSM**。
2. 選取 **Synchronize with Remote Filesystem**（與遠端檔案系統同步）（Hardware Security Operations（硬體安全性操作）設定）。

©2024 Palo Alto Networks, Inc.

STEP 3 | 匯入對應至存放於 HSM 金鑰的憑證。

1. 選取 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證） > **Device Certificates**（裝置憑證），然後按一下 **Import**（匯入）。
2. 輸入憑證名稱。
3. **Browse**（瀏覽）至 HSM 上的 **Certificate File**（憑證檔案）。
4. 選取 **File Format**（檔案格式）。
5. 選取 **Private Key resides on Hardware Security Module**（將私密金鑰存取於硬體安全性模組）。
6. 按一下 **OK**（確定）並 **Commit**（交付）變更。

STEP 4 | （僅限轉送信任憑證）啟用憑證以用於 SSL/TLS 正向 Proxy 中。

1. 開啟您在步驟 3 中匯入的憑證進行編輯。
2. 選取 **Forward Trust Certificate**（轉送信任憑證）。
3. 按一下 **OK**（確定）並 **Commit**（交付）變更。

STEP 5 | 確認您已成功匯入憑證至防火牆上。

找到您在步驟 3 中匯入的憑證，並檢查 Key（金鑰）欄中的圖示：

- 鎖定圖示—憑證的私密金鑰在 HSM 上。
- 錯誤圖示—私密金鑰不在 HSM 上，或 HSM 未適當的驗證或連線。

管理 HSM 部署

您可以執行下列工作來管理 HSM 部署：

檢視 HSM 組態設定。

選取 **Device**（設備） > **Setup**（設定） > **HSM**。

顯示詳細的 HSM 資訊。

從 [硬體安全性操作] 區段中選取**Show Detailed Information**（顯示詳細資訊）。

顯示 HSM 伺服器、HSM HA 狀態及 HSM 硬體的相關資訊。

匯出支援檔案。

從硬體安全性操作區段中選取 **Export Support File**（匯出支援檔案）。

當處理防火牆的 HSM 組態問題時，會建立測試檔案以協助客戶支援。

重設 HSM 組態。

從 **Reset HSM Configuration**（硬體安全性操作）區段中選取重設 HSM 組態。

選取此選項會移除所有的 HSM 連線。使用此選項後，必須重複所有的驗證程序。

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

High availability（高可用性）

高可用性 (HA) 是兩個防火牆放在一個群組中或者最多 16 個防火牆放在一個 HA 叢集中的部署，且其設定會進行同步以防止網路上出現單一失敗點。兩個防火牆對等間的活動訊號連線可確保當其中一個對等損壞時能夠無縫容錯移轉。設定 HA 可提供備援能力，並能讓您確保業務連續性。

- HA 概要介紹
- HA 概念
- 設定主動/被動 HA
- 設定主動/主動 HA
- HA 叢集概要介紹
- HA 叢集最佳做法和佈建
- 設定 HA 叢集
- 重新整理 HA1 SSH 金鑰並設定金鑰選項
- HA 防火牆狀態
- 參考：HA 同步
- CLI 速查表 - HA

HA 概要介紹

您可以將兩個 Palo Alto Networks 防火牆設定為 HA 配對，或設定最多 16 個防火牆作為 HA 叢集中的對等成員。叢集中的對等體可以是 HA 配對或獨立防火牆。您可使用 HA 確保替代防火牆可在對等防火牆故障時使用，以減少停機時間。HA 配對或叢集中的防火牆使用防火牆專用或頻內 HA 連接埠，以同步資料（網路、物件和原則設定）以及維護狀態資訊。不會在對等之間共用防火牆特定設定，例如管理介面 IP 位址或管理設定檔、HA 特定組態、日誌資料和 Application Command Center（應用程式控管中心，ACC） 資訊。

針對 HA 配對中的合併應用程式及日誌檢視，您必須使用 Panorama，即 Palo Alto Networks 中央管理系統。請參閱《Panorama 管理者指南》中的內容交換 — 防火牆或 Panorama。請查閱 主動/被動 HA 先決條件 和 主動/主動 HA 先決條件。強烈建議使用 Panorama 佈建 HA 叢集成員。請查閱 HA 叢集最佳做法和佈建。

HA 配對或 HA 叢集中的防火牆發生故障時，對等防火牆隨即接管保護流量的工作，此事件稱之為容錯移轉。觸發容錯移轉的條件如下：

- 一或多個監控介面故障。（連結監控）
- 無法到達防火牆的一或多個指定目的地。(路徑監控)
- 防火牆未回應活動訊號輪詢。（活動訊號輪詢與 Hello 訊息）
- 關鍵晶片或軟體元件發生故障，稱之為封包路徑健康監控。

Palo Alto Networks 防火牆支援與工作階段間的狀態主動/被動或主動/主動可用性，並支援組態同步處理，有極少數例外狀況：

- Azure 的 VM 系列防火牆和 AWS 上的 VM 系列防火牆僅支援主動/被動 HA。

  在 AWS 上，當您使用 Amazon 彈性負載平衡 (ELB) 服務部署防火牆時，其不支援 HA（在本例中，ELB 服務提供容錯移轉功能）。
- Google 雲端平台上的 VM 系列防火牆不支援 HA。

如果您準備設定 HA 叢集，請先瞭解 HA 概念和 HA 叢集概要介紹。

©2024 Palo Alto Networks, Inc.

HA 概念

下列主題提供 HA 在 Palo Alto Networks 防火牆上如何運作的概念資訊：

- HA 模式
- HA 連結及備份連結
- 裝置優先順序及先佔
- 容錯移轉
- 主動/被動 HA 下的 LACP 與 LLDP 預交涉
- 浮動 IP 位址和虛擬 MAC 位址
- ARP 負載共用
- 基於路由的備援
- HA 計時器
- 工作階段擁有者
- 工作階段設定
- 主動/主動 HA 模式中的 NAT
- 主動/主動 HA 模式中的 ECMP

HA 模式

您可以將 HA 配對中的防火牆設定為兩種模式的其中一種：

- 主動/被動—一個防火牆主動管理流量，而另一個則同步並隨時準備在發生故障時轉換為主動狀態。在此模式中，兩個防火牆共用相同的設定，而其中一個則主動管理流量，直到發生路徑、連結、系統或網路故障。主動防火牆故障時，被動防火牆會轉換為主動狀態並無縫接管，同時強制套用相同的原則以維護網路安全性。主動/被動 HA 是在虛擬連線、Layer 2 和 Layer 3 部署中支援。
- 主動/主動 — 配對中的兩個防火牆皆為主動並處理流量，且同步運作以處理工作階段設定與工作階段擁有權。兩個防火牆個別保留工作階段表及路由表，並相互同步。在 Virtual Wire 和 Layer 3 部署中支援主動/主動 HA。

  在主動/主動 HA 模式中，防火牆不支援 DHCP 用戶端。此外，只有主動-主要防火牆可用作 DHCP 轉送。如果主動-次要防火牆接收 DHCP 廣播封包，則可丟棄這些封包。

  主動/主動組態沒有負載平衡流量。雖然您可以透過傳送流量至對等來共用負載，但不會出現負載平衡。在兩個防火牆上載入共用工作階段的方法包括使用 *ECMP*、多個 *ISP* 及負載平衡器。

決定是否使用主動/被動或主動/主動模式時，考慮下列不同情況：

- 主動/被動模式設計簡單；在主動/被動模式中，大幅降低了路由及流量疑難排解的難度。主動/被動模式支援 Layer 2 部署；主動/主動模式則不支援。

©2024 Palo Alto Networks, Inc.

- 主動/主動模式要求採用進階設計理念，這可能導致網路變得更複雜。視乎您實作主動/主動 HA 的方式，可能需要附加組態，例如在兩個防火牆上啟動網路通訊協定，複製 NAT 集區，以及部署浮動 IP 位址來提供適當的容錯轉移。由於兩個防火牆都主動處理流量，防火牆將使用工作階段擁有者的其他理念及工作階段設定來執行 Layer 7 內容檢查。如果每種防火牆需要其自身的路由實例，則建議採用主動/主動模式，並且您需要始終在兩個防火牆之外進行完整、即時的備援。主動/主動模式具有更快的容錯轉移，由於兩個防火牆都主動處理流量，因此相比主動/被動模式可更好地處理尖峰流量。

  在主動/主動模式中，*HA* 配對可臨時處理高於一個防火牆正常處理的流量。然而，這不應成為規範，因為一個防火牆發生故障，可能導致所有流量重新導向至 *HA* 配對中的另一個防火牆。您的設計必須允許另一個防火牆處理最大容量的流量負載（啟用內容檢查）。如果設計超過另一個防火牆的容量，可能會出現高延遲及/或應用程式故障。

如需在主動/被動模式中設定防火牆的詳細資訊，請參閱設定主動/被動 HA。關於在主動/主動模式中設定防火牆的詳細資訊，請參閱設定主動/被動 HA。

在 HA 叢集中，所有成員均被視為作用中；除了叢集中的 HA 配對外，沒有被動防火牆的概念，HA 配對可以在新增到 HA 叢集後保持其主動/被動關係。

HA 連結及備份連結

HA 配對中的防火牆使用 HA 連結來同步資料及維護狀態資訊。某些防火牆型號具有專用 HA 連接埠 (控制連結 (HA1) 與資料連結 (HA2))，而其他型號則需要使用頻內連接埠作為 HA 連結。

- 對於擁有專用 HA 連接埠的防火牆，使用這些連接埠來管理防火牆之間的通訊與同步。如需詳細資訊，請參閱 Palo Alto Networks 防火牆的 HA 連接埠。
- 對於沒有專用 HA 連接埠的防火牆，例如 PA-220 和 PA-220R 防火牆，最佳做法是使用管理連接埠作為 HA1 連接埠，使用資料平面連接埠用作 HA1 備份。

  您可以將資料連接埠設定為專用 *HA* 介面和專用備份 *HA* 介面。對於沒有專用 *HA* 介面的防火牆（如*PA-200*、*PA-400*系列），需要設定一個資料連接埠作為 *HA* 介面。

  設定為 *HA1*、*HA2* 或 *HA3* 介面的資料連接埠可以直接連接到防火牆上的每個 *HA* 介面，也可以透過第二層交換器連接。對於設定為 *HA3* 介面的資料連接埠，您必須啟用巨型框架，因為 *HA3* 訊息超過 *1,500* 個位元組。

HA 叢集中的 HA 對等可以是獨立成員和 HA 配對的組合。HA 叢集成員使用 HA4 連結和 HA4 備份連結來執行工作階段狀態同步。非 HA 配對的叢集成員之間不支援 HA1（控制連結）、HA2（資料連結）和 HA3（封包轉送連結）。

HA 連結及備份連結	說明
控制連結	HA1 連結用於交換 Hello、活動訊號及 HA 狀態資訊，以及管理路由和 User-ID 資訊的平面同步。防火牆也會使用此連結與其對等同步組態變更。HA1 連結為 Layer 3 連結，且需 IP 位址。

©2024 Palo Alto Networks, Inc.

HA 連結及備份連結	說明
	ICMP 用於在 HA 對等體之間交換活動訊號。 適用於 HA1 的連接埠—使用於明碼通訊的 TCP 連接埠 28769 和 28260，或使用於加密通訊的連接埠 28（TCP 上的 SSH）。 若您在 HA1 連結上啟用加密，也可以重新整理 HA1 SSH 金鑰並設定金鑰選項。
資料連結	HA2 連結可用於在 HA 配對中同步防火牆之間的執行階段、轉送表格、IPSec 安全性關聯和 ARP 表格。HA2 連結中的資料流永遠為單一方向性（HA2 保持運作除外）；其流向會從主動或主動主要防火牆流往被動或主動次要防火牆。HA2 連結為 Layer 2 連結，而預設為使用 ether 類型 0x7261。 適用於 HA2 的連接埠 — HA 資料連結可設定為使用 IP（通訊協定編號 99）或 UDP（埠號 29281）作為傳輸用途，並允許 HA 資料連結跨越子網路。
HA1 和 HA2 備份連結	提供 HA1 與 HA2 連結的備援。專用備份連結不可用時，頻內連接埠可用作 HA1 與 HA2 連線的備份連結。設定備份 HA 連結時，請考慮下列方針： • 主要及備份 HA 連結的 IP 位址不得相互重疊。 • HA 備份連結必須在非主要 HA 連結的不同子網路上。 • HA1 備份及 HA2 備份連接埠皆必須在個別實體連接埠上設定。HA1 備份連結使用連接埠 28770 和 28260。 • PA-3200 系列防火牆不支援對 HA1 備份連結使用 IPv6 位址；使用 IPv4 位址。 如果您在 *HA1* 或 *HA1* 備份連結使用頻內連接埠，*Palo Alto Networks* 建議啟用活動訊號備份 *(*在 *MGT* 介面上使用連接埠 *28771)*。
封包轉送連結	除了 HA1 與 HA2 連結，主動/主動部署還需要專用 HA3 連結。防火牆使用此連結在工作階段設定期間及非對稱流量中將封包轉送至對等。HA3 連結為 Layer 2 連結，使用 MAC-in-MAC 封裝。其不支援 Layer 3 定址或解密。PA-7000 系列防火牆可在 NPC 中逐一同步工作階段。在 PA-800 Series、PA-3200 Series、PA-3400 Series、PA-5200 Series 和 PA-5400 Series 防火牆上，您可以將彙總介面設定為 HA3 連結。彙總介面還可提供 HA3 連結備援；您無法為 HA3 連結設定備份連結。在 PA-3200 Series、PA-3400 Series、PA-5200 Series、PA-5400 Series 和 PA-7000 Series 防火牆上，專用 HSCI 連接埠支援 HA3 連結。防火牆可

©2024 Palo Alto Networks, Inc.

HA 連結及備份連結	說明
	將專有封包標頭新增至周遊 HA3 連結的封包，因此該連結上的 MTU 必須大於封包轉送長度。
HA4 連結和 HA4 備份連結	HA4 連結和 HA4 備份連結在具有相同叢集 ID 的所有 HA 叢集成員之間執行工作階段快取同步。叢集成員之間的 HA4 連結透過傳送和接收 Layer 2 保持活動訊息來偵測叢集成員之間的連線失敗情況。在防火牆儀表板上檢視 HA4 和 HA4 備份連結的狀態。

Palo Alto Networks 防火牆的 HA 連接埠

連線高可用性 (HA) 組態中的兩個 Palo Alto Networks® 防火牆時，我們建議您使用用於 HA 連結與備份連結的專用 HA 連接埠。此類專用連接埠包括：用於 HA 控制與同步流量的標示為 HA1、HA1-A 和 HA1-B 的 HA1 連接埠；以及用於 HA 工作階段設定流量的 HA2 與高速機殼互連 (HSCI) 連接埠。PA-5200 系列防火牆配備可為 HA1 流量設定的多用途輔助連接埠（標示為 AUX-1 與 AUX-2）。

此外，您還可為 HA3 設定 HSCI 連接埠，用於在工作階段設定及非對稱流量中將封包轉送至對等防火牆（僅限主動/主動 HA）。HSCI 連接埠可用於 HA2 流量、HA3 流量或者同時用於這兩種流量。

HA1 與 *AUX* 連結可用於同步管理平面上的功能。與使用頻內連接埠相比，使用管理背板上專用的 *HA* 介面更有效率，因為不需要透過資料背板傳遞同步處理封包。

您可以將資料連接埠設定為專用 *HA* 介面和專用備份 *HA* 介面。對於沒有專用 *HA* 介面的防火牆（如*PA-200*、*PA-400*系列），需要設定一個資料連接埠作為 *HA* 介面。

設定為 *HA1*、*HA2* 或 *HA3* 介面的資料連接埠可以直接連接到防火牆上的每個 *HA* 介面，也可以透過第二層交換器連接。對於設定為 *HA3* 介面的資料連接埠，您必須啟用巨型框架，因為 *HA3* 訊息超過 *1,500* 個位元組。

儘可能在 *HA* 配對中的兩個防火牆之間直接連線 *HA* 連接埠（不透過交換器或路由器），以免存在網路問題時出現 *HA* 連結與通訊問題。

使用以下表格瞭解專用 HA 連接埠以及如何連線 HA 連結與備份連結：

©2024 Palo Alto Networks, Inc.

Model	前面板專用連接埠

PA-800 系列防火牆	• **HA1** 與 **HA2**—在兩種 HA 模式中用於 HA1 與 HA2 的乙太網路 10Mbps/100Mbps/1000Mbps 連接埠。
	  • 對於 **HA1** 流量—將第一個防火牆的 HA1 連接埠，直接連線到配對中第二個防火牆的 HA1 連接埠，或者將這兩個連接埠透過交換器或路由器連線在一起。
	  • 對於 **HA2** 流量—將第一個防火牆的 HA2 連接埠，直接連線到配對中第二個防火牆的 HA2 連接埠，或者將這兩個連接埠透過交換器或路由器連線在一起。

PA-1400 系列防火牆	• **HA1-A** 與 **HA1-B**—在兩種 HA 模式中用於 HA1 流量的乙太網路 10Mbps/100Mbps/1000Mbps 連接埠。
	  • 對於 **HA1** 流量—將第一個防火牆的 HA1-A 連接埠，直接連線到配對中第二個防火牆的 HA1-A 連接埠，或者將其透過交換器或路由器連線在一起。
	  • 對於 **HA1-A** 連線的備份—將第一個防火牆的 HA1-B 連接埠，直接連線到配對中第二個防火牆的 HA1-B 連接埠，或者將其透過交換器或路由器連線在一起。
	• **HSCI** — HSCI 連接埠是第一層 SFP+ 介面，用於連線 HA 設定中的兩個 PA-1400 系列防火牆。使用此連接埠用於 HA2 連線、HA3 連線或同時用於兩者。
	  HSCI 連接埠上攜帶的流量為原始 Layer 1 流量，此流量不可路由或交換。因此，您必須直接將 HSCI 連接埠連線在一起（將第一個防火牆的 HSCI 連接埠連線到第二個防火牆的 HSCI 連接埠）。

©2024 Palo Alto Networks, Inc.

Model	前面板專用連接埠

PA-3200 系列防火牆	• **HA1-A** 與 **HA1-B**—在兩種 HA 模式中用於 HA1 流量的乙太網路 10Mbps/100Mbps/1000Mbps 連接埠。
	  • 對於 **HA1** 流量—將第一個防火牆的 HA1-A 連接埠，直接連線到配對中第二個防火牆的 HA1-A 連接埠，或者將其透過交換器或路由器連線在一起。
	  • 對於 **HA1-A** 連線的備份—將第一個防火牆的 HA1-B 連接埠，直接連線到配對中第二個防火牆的 HA1-B 連接埠，或者將其透過交換器或路由器連線在一起。
	  如果防火牆資料面由於故障而重新啟動或手動重新啟動，*HA1-B* 連結也將重新啟動。如果出現此情況，而且 *HA1-A* 連結未連線與設定，則會出現「核心分裂」的情況。因此，我們建議連線並設定 *HA1-A* 連接埠與 *HA1-B* 連接埠，以提供備援並避免出現「核心分裂」問題。
	  您可以透過 *PAN-OS* 或 *Panorama* 將防火牆的 *SFP* 連接埠重新對應為 *HA1-A* 和 *HA1-B* 連接埠。
	• **HSCI**—HSCI 連接埠是 Layer 1 SFP+ 介面，用於連線 HA 組態中的兩個 PA-3200 系列防火牆。使用此連接埠用於 HA2 連線、HA3 連線或同時用於兩者。
	  HSCI 連接埠上攜帶的流量為原始 Layer 1 流量，此流量不可路由或交換。因此，您必須直接將 HSCI 連接埠連線在一起（將第一個防火牆的 HSCI 連接埠連線到第二個防火牆的 HSCI 連接埠）。

PA-3400 Series 防火牆	• **HA1-A** 與 **HA1-B**—在兩種 HA 模式中用於 HA1 流量的乙太網路 10Mbps/100Mbps/1000Mbps 連接埠。
	  • 對於 **HA1** 流量—將第一個防火牆的 HA1-A 連接埠，直接連線到配對中第二個防火牆的 HA1-A 連接埠，或者將其透過交換器或路由器連線在一起。
	  • 對於 **HA1-A** 連線的備份—將第一個防火牆的 HA1-B 連接埠，直接連線到配對中第二個防火牆的 HA1-B 連接埠，或者將其透過交換器或路由器連線在一起。

©2024 Palo Alto Networks, Inc.

Model	前面板專用連接埠
	• **HSCI**—HSCI 連接埠是 Layer 1 SFP+ 介面，用於連線 HA 設定中的兩個 PA-3400 Series 防火牆。使用此連接埠用於 HA2 連線、HA3 連線或同時用於兩者。 HSCI 連接埠上攜帶的流量為原始 Layer 1 流量，此流量不可路由或交換。因此，您必須直接將 HSCI 連接埠連線在一起（將第一個防火牆的 HSCI 連接埠連線到第二個防火牆的 HSCI 連接埠）。 管理介面不能設定為 *HA* 連接埠。

PA-5200 系列防火牆	• **HA1-A** 與 **HA1-B**—在兩種 HA 模式中用於 HA1 流量的乙太網路 10Mbps/100Mbps/1000Mbps 連接埠。
	  • 對於 **HA1** 流量—將第一個防火牆的 HA1-A 連接埠，直接連線到配對中第二個防火牆的 HA1-A 連接埠，或者將其透過交換器或路由器連線在一起。
	  • 對於 **HA1-A** 連線的備份—將第一個防火牆的 HA1-B 連接埠，直接連線到配對中第二個防火牆的 HA1-B 連接埠，或者將其透過交換器或路由器連線在一起。
	• **HSCI**—HSCI 連接埠是 Layer 1 介面，用於連線 HA 組態中的兩個 PA-5200 系列防火牆。使用此連接埠用於 HA2 連線、HA3 連線或同時用於兩者。
	
	PA-5220 防火牆上的 *HSCI* 連接埠是 *QSFP+* 連接埠，*PA-5250*、*PA-5260* 以及 *PA-5280* 防火牆的 *HSCI* 連接埠是 *QSFP28* 連接埠。
	
	HSCI 連接埠上攜帶的流量為原始 Layer 1 流量，此流量不可路由或交換。因此，您必須直接將 HSCI 連接埠連線在一起（將第一個防火牆的 HSCI 連接埠連線到第二個防火牆的 HSCI 連接埠）。

PA-5200 系列防火牆（續）	• **AUX-1** 與 **AUX-2**—輔助 SFP+ 連接埠是多用途連接埠，可為 HA1、管理功能或日誌轉送至 Panorama 而進行設定。若您需針對這些功能之一建立光纖連線，請使用此類連接埠。
	  • 對於 **HA1** 流量—將第一個防火牆的 AUX-1 連接埠，直接連線到配對中第二個防火牆的 AUX-1 連接埠，或者將其透過交換器或路由器連線在一起。
	  • 對於 **AUX-1** 連線的備份—將第一個防火牆的 AUX-2 連接埠，直接連線到配對中第二個防火牆的 AUX-2 連接埠，或者將其透過交換器或路由器連線在一起。

©2024 Palo Alto Networks, Inc.

Model	前面板專用連接埠

PA-5400 Series 防火牆（PA-5410、PA-5420、PA-5430 和 PA-5440）	• **HA1-A** 和 **HA1-B**—SFP/SFP+ 1Gbps/10Gbps 連接埠，用於兩種 HA 模式下的 HA1 流量。
	  • 對於 **HA1** 流量—將第一個防火牆的 HA1-A 連接埠，直接連線到配對中第二個防火牆的 HA1-A 連接埠，或者將其透過交換器或路由器連線在一起。
	  • 對於 **HA1-A** 連線的備份—將第一個防火牆的 HA1-B 連接埠，直接連線到配對中第二個防火牆的 HA1-B 連接埠，或者將其透過交換器或路由器連線在一起。
	• **HSCI**—HSCI 連接埠是 Layer 1 QSFP+ 介面，用於連線 HA 設定中的兩個 PA-5400 Series 防火牆。使用此連接埠用於 HA2 連線、HA3 連線或同時用於兩者。
	HSCI 連接埠上攜帶的流量為原始 Layer 1 流量，此流量不可路由或交換。因此，您必須直接將 HSCI 連接埠連線在一起（將第一個防火牆的 HSCI 連接埠連線到第二個防火牆的 HSCI 連接埠）。
	  • 對於 **HA2** 與 **HA3** 流量—將第一個防火牆的 HSCI-A 連接埠，直接連線到第二個防火牆的 HSCI-A 連接埠。
	  您也可以將防火牆資料連接埠用於 *HA2* 或 *HA3* 流量；但是，這些連接埠不能同時用於 *HA2* 和 *HA3*。

PA-5450 防火牆	• **HA1-A** 和 **HA1-B**—SFP/SFP+ 1Gbps/10Gbps 連接埠，用於兩種 HA 模式下的 HA1 流量。
	  • 對於 **HA1** 流量—將第一個防火牆的 HA1-A 連接埠，直接連線到配對中第二個防火牆的 HA1-A 連接埠，或者將其透過交換器或路由器連線在一起。
	  • 對於 **HA1-A** 連線的備份—將第一個防火牆的 HA1-B 連接埠，直接連線到配對中第二個防火牆的 HA1-B 連接埠，或者將其透過交換器或路由器連線在一起。

©2024 Palo Alto Networks, Inc.

Model	前面板專用連接埠
	• **HSCI-A** 和 **HSCI-B**—HSCI 連接埠是 Layer 1 QSFP+ 介面，用於連線 HA 設定中的兩個 PA-5450 Series 防火牆。使用此類連接埠用於 HA2 連線、HA3 連線或同時用於兩者。 HSCI 連接埠上攜帶的流量為原始 Layer 1 流量，此流量不可路由或交換。因此，必須按下述方式連線此類連接埠： • 對於 **HA2** 與 **HA3** 流量—將第一個防火牆的 HSCI-A 連接埠，直接連線到第二個防火牆的 HSCI-A 連接埠。 • 對於 **HSCI-A** 連線的備份—將第一個防火牆的 HSCI-B 連接埠，直接連線到第二個防火牆的 HSCI-B 連接埠。
PA-7000 系列防火牆	• **HA1-A** 與 **HA1-B**—在兩種 HA 模式中用於 HA1 流量的乙太網路 10Mbps/100Mbps/1000Mbps 連接埠。 • 對於 **HA1** 流量—將第一個防火牆的 HA1-A 連接埠，直接連線到配對中第二個防火牆的 HA1-A 連接埠，或者將其透過交換器或路由器連線在一起。 • 對於 **HA1-A** 連線的備份—將第一個防火牆的 HA1-B 連接埠，直接連線到配對中第二個防火牆的 HA1-B 連接埠，或者將其透過交換器或路由器連線在一起。 您無法在 *NPC* 資料連接埠或管理 *(MGT)* 連接埠上設定 *HA1* 連線。 • **HSCI-A** 與 **HSCI-B**—HSCI 連接埠是 Layer 1 QSFP+介面，用於連線 HA 組態中的兩個 PA-7000 系列防火牆。使用此類連接埠用於 HA2 連線、HA3 連線或同時用於兩者。 HSCI 連接埠上攜帶的流量為原始 Layer 1 流量，此流量不可路由或交換。因此，必須按下述方式連線此類連接埠： • 對於 **HA2** 與 **HA3** 流量—將第一個防火牆的 HSCI-A 連接埠，直接連線到第二個防火牆的 HSCI-A 連接埠。 對於 *HA2* 或 *HA2/HA3* 流量，*PA-7000* 系列防火牆透過一對一的方式同步 *NPC* 中的工作階段。 • 對於 **HSCI-A** 連線的備份—將第一個防火牆的 HSCI-B 連接埠，直接連線到第二個防火牆的 HSCI-B 連接埠。

©2024 Palo Alto Networks, Inc.

Model	前面板專用連接埠
	可以設定 *HA2* 和 *HA2-Backup* 連結使用資料平面介面，而不是 *HSCI* 連接埠。但是，如果這樣設定，*HA2* 和 *HA2-Backup* 連結二者都需要使用資料平面介面。無論 *HA2* 還是 *HA2-Backup*，混合使用資料平面連接埠和 *HSCI* 連接埠都會導致提交失敗。這適用於 *PA-7050-SMC*、*PA-7080-SMC*、*PA-7050-SMC-B* 和 *PA-7080-SMC-B*。

裝置優先順序及先佔

可對主動-被動 HA 配對中的防火牆指定*裝置優先順序*值，以表示喜好的防火牆可擔任主動角色。若要在 HA 配對中使用特定防火牆來主動保護流量，您必須在兩個防火牆上啟用先佔行為並為每個防火牆指定防火牆優先順序。數值較小的防火牆就等於有較高的優先順序，表示將其指定為主動防火牆。另一個防火牆是被動防火牆。

主動-主動 HA 配對也是如此；但是，*裝置 ID* 用於指定裝置優先順序值。同樣地，裝置 ID 中較小數值對應較高優先順序。優先順序較高的防火牆變成主動-主要防火牆，而配對防火牆變成主動-次要防火牆。

依預設，防火牆上的先佔選項為停用，且必須在兩個防火牆上都啟用。啟用後，先佔行為允許優先順序較高（數值較小）的防火牆在容錯移轉後恢復為主動或主動主要。出現先佔行為時，該事件會記錄在系統日誌中。

容錯移轉

一個防火牆發生故障時，HA 配對中的對等（或 HA 叢集中的對等）隨即接管保護流量的工作，此事件稱之為*容錯移轉*。例如，HA 配對中防火牆上的監控公制失敗時，就會觸發容錯移轉。防火牆為偵測防火牆失敗而監控的指標包括：

- 活動訊號輪詢與您好訊息

  防火牆使用您好訊息和活動訊號來驗證對等防火牆可回應及可操作。您好訊息會以設定的 *Hello 間隔*在對等間傳送，以確認另一個對等的狀態。活動訊號是在控制連結上對 HA 對等的 ICMP 偵測，而該對等會回應偵測以建立防火牆間的連線與回應。活動訊號的間隔預設為 1000 毫秒。每 1000 毫秒會傳送一次偵測，如果連續丟失三個活動訊號，則會發生容錯移轉。如需觸發容錯移轉的 HA 計時器的詳細資訊，請參閱 HA 計時器。

- 連結監控

  您可以指定一組防火牆將監控的實體介面（一個連結群組），且防火牆將監控群組中每個連結的狀態（連結開啟或連結關閉）。確定連結群組中的失敗條件：群組中 **Any**（任何）連結關閉或 **All**（全部）連結關閉即構成連結群組失敗（但不一定會發生容錯移轉）。

  您可以建立多個連結群組。因此，您還可以確定一組連結群組的失敗條件：**Any**（任何）連結群組失敗或 **All**（全部）連結群組失敗，可確定何時觸發容錯移轉。預設行為是，當 **Any**（任

©2024 Palo Alto Networks, Inc.

何）連結群組中的 **Any**（任何）連結故障時，防火牆會將 HA 狀態變更為非作用狀態（或主動/主動模式中的暫訂狀態），表示監控物件發生故障。

- 路徑監控

  您可以指定防火牆將監控的 IP 位址的目的地 IP 群組。防火牆使用 ICMP ping 監控從網路到任務關鍵性 IP 位址的完整路徑，以驗證 IP 位址的可連線性。偵測的預設間隔為 200 毫秒。如果連續 10 次 ping（預設值）失敗，則認為 IP 位址無法連線。指定目的地 IP 群組中 IP 位址的失敗條件：群組中 **Any**（任何）IP 位址無法連線或 **All**（全部）IP 位址無法連線。您可以為虛擬介接、VLAN 或虛擬路由器的路徑群組指定多個目的地 IP 群組；指定路徑群組中目的地 IP 群組的失敗條件：**Any**（任何）或 **All**（全部），構成路徑群組失敗。您可以設定多個虛擬介接路徑群組、VLAN 路徑群組和虛擬路由器路徑群組。

  您還可確定全域失敗條件：**Any**（任何）路徑群組失敗或 **All**（全部）路徑群組失敗，可確定何時觸發容錯移轉。預設行為是，當 **Any**（任何）虛擬介接、VLAN 或虛擬路由器路徑群組中的 **Any**（任何）目的地 IP 群組中的 **Any**（任何）IP 位址之一變得無法連線時，防火牆會將 HA 狀態變更為非作用狀態（或主動/主動模式中的暫訂狀態），表示監控物件發生故障。

除了以上容錯移轉觸發程序外，管理員在暫停防火牆時或有先佔狀態時，也會發生容錯移轉。

在 PA-3200 系列、PA-5200 系列和 PA-7000 系列防火牆上，內部健康情況檢查失敗時會發生容錯移轉。此健康檢查無法設定，可用於監控關鍵元件，例如 FPGA 和 CPU。此外，會在導致容錯轉移的任何平台上進行健康檢查。

以下內容描述了作為 HA 叢集成員的 PA-7000 系列防火牆上的網路處理卡 (NPC) 發生失敗時的情況：

- 如果用於保留 HA 叢集工作階段快取的 NPC（其他成員工作階段的複本）關閉，則防火牆將無法運作。發生這種情況時，工作階段散佈裝置（例如負載平衡器）必須偵測到防火牆已關閉，並將工作階段負載散佈給叢集的其他成員。
- 如果一個叢集成員的 NPC 關閉，且該 NPC 上未啟用任何連結監控或路徑監控，則 PA-7000 系列防火牆成員將保持開啟，但容量會降低，因為一個 NPC 已經關閉。
- 如果一個叢集成員的 NPC 關閉，且在該 NPC 上啟用了連結監控或路徑監控，則 PA-7000 系列防火牆將無法運作，且工作階段散佈裝置（例如負載平衡器）必須偵測到防火牆已關閉，並將工作階段負載散佈給叢集的其他成員。

主動/被動 HA 下的 LACP 與 LLDP 預交涉

如果防火牆使用 LACP 或 LLDP，在出現容錯轉移時對這些通訊協定進行預交涉可避免亞秒級容錯轉移。然而，您可以在被動防火牆上啟用介面，以在容錯轉移之前交涉 LACP 與 LLDP。因此，處在被動或非運作 HA 狀態下的防火牆可與使用 LACP 或 LLDP 的相鄰裝置通訊。此類預交涉可加速容錯轉移。

除 VM 系列防火牆以外的所有防火牆型號均支援預交涉組態，具體取決於乙太網路或 AE 介面在 Layer 2、Layer 3 還是 Virtual Wire 部署中。HA 被動防火牆採用下列兩種方式中的一種處理 LACP 與 LLDP 封包：

- 主動—防火牆在介面上進行 LACP 或 LLDP 設定，並各自主動參與 LACP 或 LLDP 預交涉。

©2024 Palo Alto Networks, Inc.

- 被動—在介面上未進行 LACP 或 LLDP 設定，且防火牆不參與通訊協定，但允許防火牆兩側對等各自進行 LACP 或 LLDP 預交涉。

以下表格顯示彙總乙太網路 (AE) 和乙太網路介面上支援哪些部署。

介面部署	**AE** 介面	乙太網路介面
Layer 2 中的 LACP	主動	不受支援
Layer 3 中的 LACP	主動	不受支援
虛擬介接中的 LACP	不受支援	被動
Layer 2 中的 LLDP	主動	主動
Layer 3 中的 LLDP	主動	主動
虛擬介接中的 LLDP	主動	• 如果 LLDP 本身已設定，則為主動。 • 如果 LLDP 本身未設定，則為被動。

在子介面或通道介面上不支援預交涉。

若要設定 LACP 或 LLDP 預交涉，請參閱步驟（選用）如果您的網路使用 LACP 或 LLDP，則啟用主動/被動 HA 的 LACP 和 LLDP 預交涉，以加快容錯移轉。

浮動 IP 位址和虛擬 MAC 位址

在 HA 主動/主動模式的 Layer 3 部署中，您可以指定浮動 IP 位址，如果連結或防火牆發生故障，將會從 HA 防火牆移至其他防火牆。防火牆上的介面擁有浮動 IP 位址，會回應含虛擬 MAC 位址的 ARP 要求。

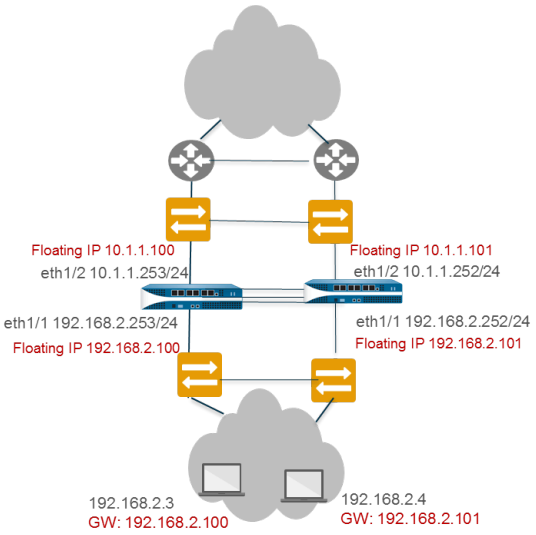
當您需要諸如虛擬路由備援通訊協定 (VRRP) 等功能時建議使用浮動 IP 位址。浮動 IP 位址還可用於實作 VPN 與來源 NAT，在防火牆提供這些服務失敗時，可保持持續連線。

如下圖所示，每個 HA 防火牆介面有其自身的 IP 位址與浮動 IP 位址。介面 IP 位址保持在防火牆本機上，但在防火牆發生故障時，浮動 IP 位址則在防火牆之間移動。您可以設定終端主機將浮動 IP 位址用作其預設閘道，可讓您將負載平衡流量載入至兩個 HA 對等。您還可以使用外部負載平衡器來載入平衡流量。

如果連結或防火牆失敗，或路徑監控事件導致容錯轉移，浮動 IP 位址與虛擬 MAC 位址將移至功能性防火牆。（在下圖中，每個防火牆擁有兩個浮動 IP 位址和虛擬 MAC 位址；如果防火牆失敗，它們則會移動。） 功能性防火牆傳送 Gratuitous ARP 來更新連線交換器的 MAC 表，通知交換器浮動 IP 位址與 MAC 位址擁有權變更情況，以向其自身重新導向流量。

©2024 Palo Alto Networks, Inc.

失敗的防火牆復原後，浮動 IP 與虛擬 MAC 位址預設會移回連結該浮動 IP 且具有裝置 ID [0 或 1] 的防火牆。更具體而言，失敗的防火牆復原後，則會連線。目前的主動防火牆確定防火牆重新連線，並檢查以原生方式處理的浮動 IP 位址是屬於其自身還是其他防火牆。如果浮動 IP 位址以原生方式連接至其他裝置 ID，防火牆將自動返回。（如需此預設行為的替代方案，請參閱使用案例：使用繫結至主動/主要防火牆 的浮動 IP 位址設定主動/主動 HA）



HA 配對中的每個防火牆將建立一個虛擬 MAC 位址，用於具有浮動 IP 位址或 ARP 負載共用 IP 位址的各個介面。

PA-7000、PA-7000b、PA-5400、PA-5200、PA-3200 系列和 CN-Series 防火牆上的虛擬 MAC 位址的格式為 B4-0C-25-xx-xx-xx，其中 B4-0C-25 是供應商 ID（在此情況下是 Palo Alto Networks），接下來的 24 位元表示裝置、群組 ID 與介面 ID，如下所示：

765	4	321076	5432	1076543210
111	Device-ID	Group-ID	0000	Interface-ID

其餘防火牆型號上的虛擬 MAC 位址的格式為 00-1B-17-00-xx-yy，其中 00-1B-17 是供應商 ID（在此情況下是 Palo Alto Networks），00 為固定編號，xx 表示設定 ID 與群組 ID（如下圖所示），yy 為介面 ID：

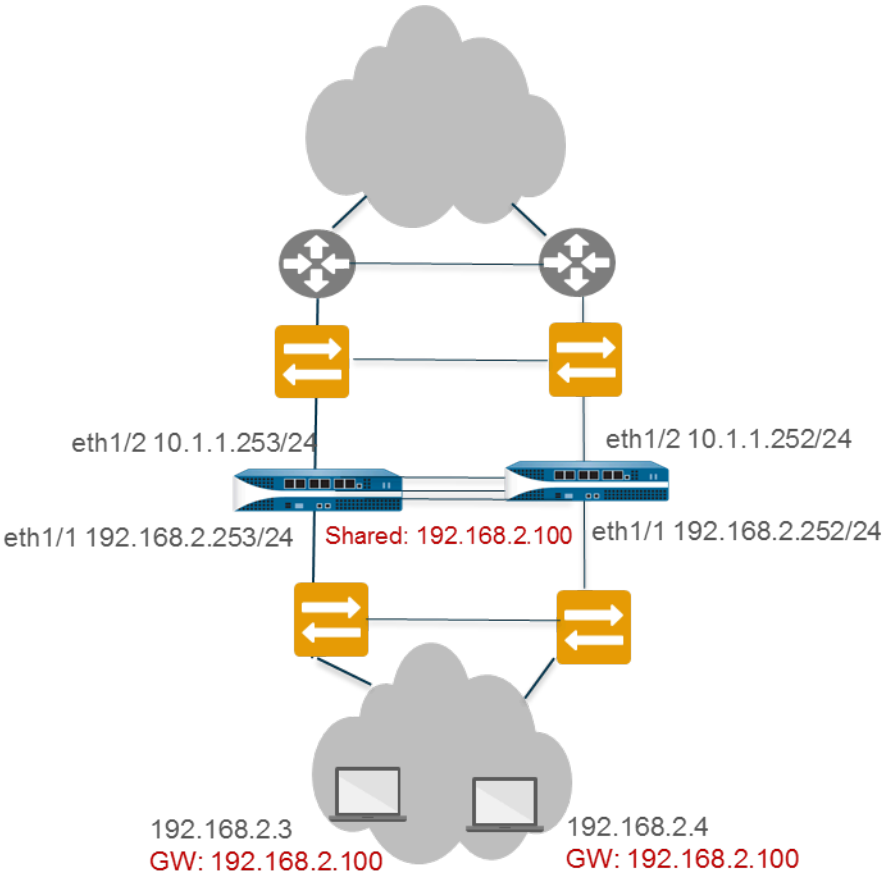
7	6	543210	76543210
Device-ID	0	Group-ID	Interface-ID

新的主動防火牆接管時，它將從各連線介面傳送 Gratuitous ARP，通知連線 Layer 2 交換器虛擬 MAC 位址的新位置。若要設定浮動 IP 位置，請參閱使用案例：使用浮動 IP 位址設定主動/主動 HA。

©2024 Palo Alto Networks, Inc.

ARP 負載共用

在 Layer 3 介面部署與主動/主動 HA 組態中，ARP 負載共用允許防火牆共用 IP 位址並提供閘道服務。僅當防火牆與終端主機之間不存在任何 Layer 3 裝置時（即終端主機使用防火牆作為其預設閘道時），才會使用 APR 負載共用。



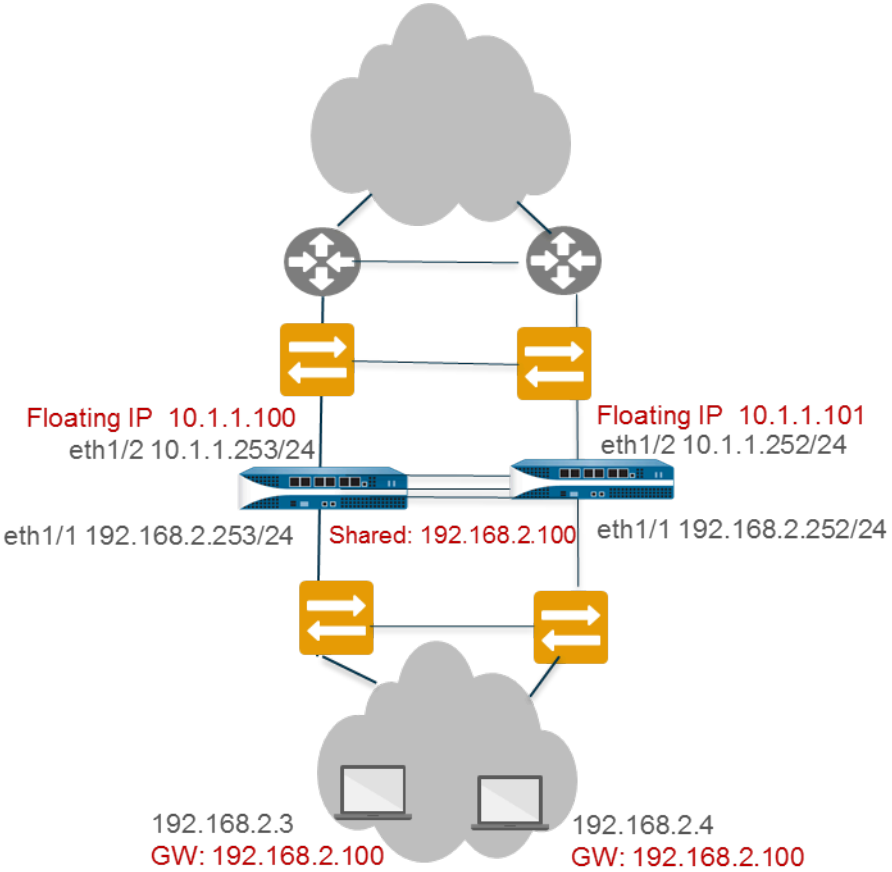
在此類案例中，會以單一閘道 IP 位址設定所有主機。其中一個防火牆透過其虛擬 MAC 位址回應閘道 IP 位址的 ARP 請求。每個防火牆針對共用 IP 位址產生唯一的虛擬 MAC 位址。控制哪個防火牆會對 APR 做出回應的負載共用演算法可以進行設定；透過計算 APR 請求來源 IP 位址的雜湊或模數來確定。

終端主機從閘道收到 APR 請求後，它會擷取 MAC 位址，且主機的所有流量在 ARP 緩衝的存留期間透過回應虛擬 MAC 位址的防火牆路由。APR 緩衝的存留事件視終端主機作業系統而定。

如果連結或防火牆失敗，浮動 IP 位址與虛擬 MAC 位址將移至功能性防火牆。功能性防火牆傳送 Gratuitous ARP 來更新連線交換器的 MAC 表，通知連線交換器從失敗的防火牆向其自身重新導向流量。請參閱使用案例：設定主動/主動 HA（具有 ARP 負載共用）。

您可以在具有浮動 IP 位址的 HA 防火牆 WAN 端設定介面，並在具有共用 IP 位址用於 APR 負載平衡的 HA 防火牆 LAN 端設定介面。例如，下圖顯示上游 WAN 邊緣路由器的浮動 IP 位址，以及 LAN 區段上主機的 ARP 負載共用位址。

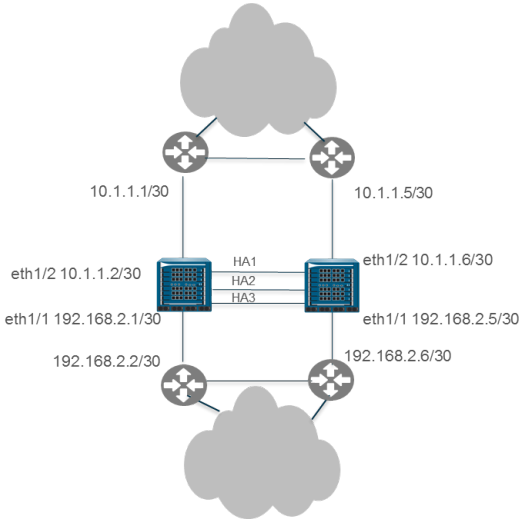
©2024 Palo Alto Networks, Inc.



基於路由的備援

在 Layer 3 介面部署及主動/主動 HA 組態中，防火牆將連線至路由器而非交換器。防火牆使用動態路由通訊協定來確定最佳路徑（非對稱路由）並在 HA 配對間進行負載共用。在此類案例中，浮動 IP 位址沒有必要。如果連結、監控路徑或防火牆失敗，或者如果雙向轉送偵測 (BFD) 偵測到連結失敗，路由通訊協定（RIP、OSPF 或 BGP）將重新路由流量至功能性防火牆。您可以使用唯一的 IP 位址設定各防火牆介面。IP 位址設定時保持在防火牆本機上；防火牆失敗時，它們不會在設定間移動。請參閱使用案例：設定主動/主動 HA（具有基於路由的備援）。

©2024 Palo Alto Networks, Inc.



HA 計時器

高可用性 (HA) 計時器有助於防火牆偵測防火牆失敗及觸發故障復原。若要減少為 HA 對等設定計時器的複雜度，您可以從三個設定檔中進行選取：**Recommended**（建議的）、**Aggressive**（積極）和 **Advanced**（進階）。這些設定檔會自動填入最佳的 HA 計時器值，供特定的防火牆平台啟用更快速的 HA 部署。

為一般的故障復原計時器設定使用 **Recommended**（建議）的設定檔，並為較快速的故障復原計時器設定使用 **Aggressive**（積極）設定檔。**Advanced**（進階）設定檔可讓您自訂計時器值以符合您的網路需求。

下表說明設定檔包含的每個計時器，及跨不同硬體機型的目前預設值（建議/主動）；這些值僅供目前參考之用，後續的版本可能會變更。

影響 *HA* 叢集成員的計時器在 設定 HA 叢集 中進行了介紹。

計時器	說明	**PA-7000** 系列 **PA-5200** 系列 **PA-3200** 系列	**PA-800 Series** **PA-220** **VM-Series**	**Panorama** 虛擬設備 **Panorama M** 系列
監控失敗維持時間（毫秒）	防火牆在路徑監控或連結監控失敗後，將於其間保持使用中狀態的時間間隔。建議使用此設定，以避免由於相鄰裝置偶爾波動所致的 HA 容錯移轉。	0/0	0/0	0/0

©2024 Palo Alto Networks, Inc.

計時器	說明	**PA-7000** 系列 **PA-5200** 系列 **PA-3200** 系列	**PA-800 Series** **PA-220** **VM-Series**	**Panorama** 虛擬設備 **Panorama M** 系列
先佔保留時間（分鐘）	接管成為主動或主動主要防火牆之前，被動或主動次要防火牆將等待的時間。	1/1	1/1	1/1
Heartbeat Interval (ms)	HA 對等交換 ICMP（偵測）形式之活動訊號訊息的頻率。	1000/1000	2000/1000	2000/1000
Promotion Hold Time (ms)	被動防火牆（在主動/被動模式下）或主動次要防火牆（在主動/主動模式中下）在失去與 HA 對等之通訊之後接管成為主動或主動主要防火牆之前，將等待的時間。此保留時間將僅在進行對等失敗宣告之後開始。	2000/500	2000/500	2000/500
Additional Master Hold Up Time (ms)	時間間隔適用於與監控失敗保持時間相同的事件（以毫秒為單位，範圍是 0 至 60000，預設值為 500）。其他時間間隔僅適用於主動/被動模式下的主要防火牆，及適用於主動/主動模式下的主動主要防火牆。建議使用此計時器，以避免兩個防火牆同時遇到相同連結/路徑監控失敗時的容錯移轉。	500/500	500/500	7000/5000
Hello 間隔（毫秒）	傳送以確認其他防火牆上的 HA 是否可正常操作之您好封包間的毫秒時間間隔（範圍為	8000/8000	8000/8000	8000/8000

©2024 Palo Alto Networks, Inc.

計時器	說明	**PA-7000** 系列 **PA-5200** 系列 **PA-3200** 系列	**PA-800 Series** **PA-220** **VM-Series**	**Panorama** 虛擬設備 **Panorama M** 系列
	8,000 至 60,000；預設值為 8,000）。			
擺動最大值	發生以下某種情況時，將計算旗標次數： • 已啟用先佔的防火牆在變更為作用中狀態後 20 分鐘內退出作用中狀態。 • 連結或路徑在正常運行後不能保持開啟 10 分鐘。 如果先佔失敗或出現功能異常迴圈，此值指出在判定防火牆進入暫停狀態前，允許的擺動旗標數上限（範圍為 0 至 16；預設值為 3）。	3/3	3/3	不適用

工作階段擁有者

在 HA 主動/主動組態中，兩個防火牆同時為主動，這意味著封包可在它們之間散佈。此類散佈需要防火牆執行兩項功能：工作階段擁有權與工作階段設定。通常，配對的每個防火牆執行其中一項功能，從而避免可能在非對稱式路由環境中發生競爭條件。

您可以設定工作階段擁有者為從終端主機中接收新工作階段第一個封包的防火牆，或處於主動-主要狀態下的防火牆（主要裝置）。如果設定了主要裝置，但接收第一個封包的防火牆未處於主動-主要狀態，防火牆則會透過 HA3 連結將封包轉送至對等防火牆（工作階段擁有者）。

工作階段擁有者執行所有 Layer 7 處理，例如 App-ID、內容 ID 及工作階段威脅掃描。工作階段擁有者還會針對工作階段產生所有流量日誌。

如果工作階段擁有者失敗，對等防火牆則會稱為工作階段擁有者。現有工作階段容錯轉移至功能性防火牆，且這些工作階段不可進行 Layer 7 處理。防火牆失敗復原後，依預設，所有其失敗前擁有的工作階段將復原至原防火牆；不會繼續進行 Layer 7 處理。

如果將工作階段擁有權設定為主要裝置，工作階段設定也將預設為主要裝置。

©2024 Palo Alto Networks, Inc.

Palo Alto Networks 建議將 *Session Owner*（工作階段擁有者）設為 *First Packet*（第一個封包），將 *Session Setup*（工作階段設定）設為 *IP Modulo*（*IP* 模數），除非在特定使用案例中另行指明。將 *Session Owner*（工作階段擁有者）設為 *First Packet*（第一個封包）會減少 *HA3* 連結上的流量，有助於在對等機間分配資料平面負載。

將 *Session Owner*（工作階段擁有者）和 *Session Setup*（工作階段設定）設為 *Primary Device*（主要裝置）致使主動-主要防火牆執行所有流量處理。出於下列其中一個原因，您可能需要設定此項：

- 您正在進行疑難排解及擷取日誌與 *PCAP*，因此防火牆間的封包處理不會分割。
- 您想要強制執行主動/主動 *HA* 配對，使其運作方式與主動/被動 *HA* 配對類似。請參閱 使用案例：使用繫結至主動/主要防火牆的浮動 IP 位址設定主動/主動 HA。

工作階段設定

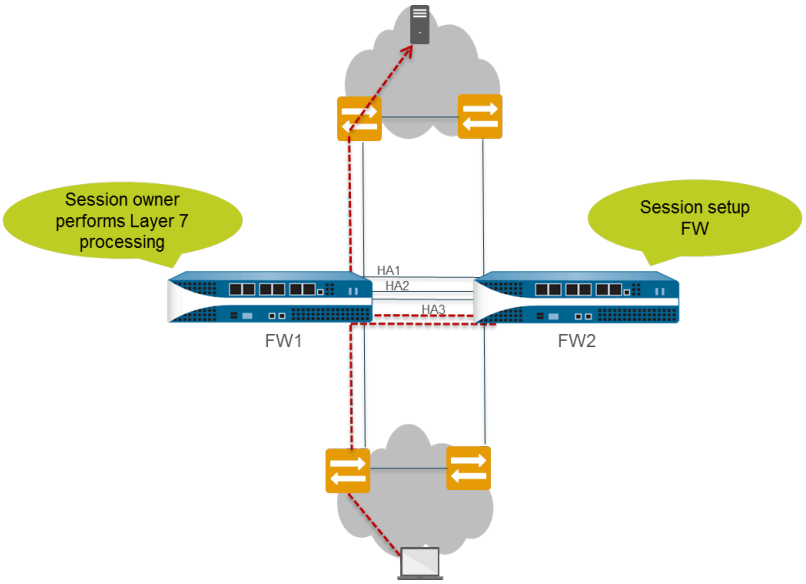
工作階段設定防火牆執行設定新工作階段所需的 Layer 2 至 Layer 4 處理。此外，工作階段設定防火牆還將使用工作階段擁有者的 NAT 集區來執行 NAT。您可以透過選取下列其中一個工作階段設定負載共用選項，確定主動/主動組態中的工作階段設定防火牆。

工作階段設定選項	說明
IP 模數	防火牆根據來源 IP 位址的同位性散佈工作階段設定負載。這是共用工作階段設定的決定性方法。
IP 雜湊	防火牆使用來源雜湊和目的地 IP 位址來散佈工作階段設定責任。
主要裝置	主動-主要防火牆一直設定工作階段；只有一個防火牆執行所有工作階段設定責任。
第一個封包	接收工作階段第一個封包的防火牆執行工作階段設定。

- 如果您想要對工作階段擁有者與工作階段設定責任進行負載共用，則將 *Session Owner*（工作階段擁有者）設為 *First Packet*（第一個封包），將 *Session Setup*（工作階段設定）設為 *IP Modulo*（*IP* 模數）。這些是建議的設定。
- 如果您不需要進行疑難排解或擷取日誌或 *PCAP*，或者如果您希望主動/主動 *HA* 配對與主動/被動 *HA* 配對的運作方式類似，則將工作階段擁有者與工作階段設定均設為主要裝置，以便主動-主要裝置執行所有流量處理。請參閱使用案例：使用繫結至主動/主要防火牆的浮動 *IP* 位址設定主動/主動 *HA*。

©2024 Palo Alto Networks, Inc.

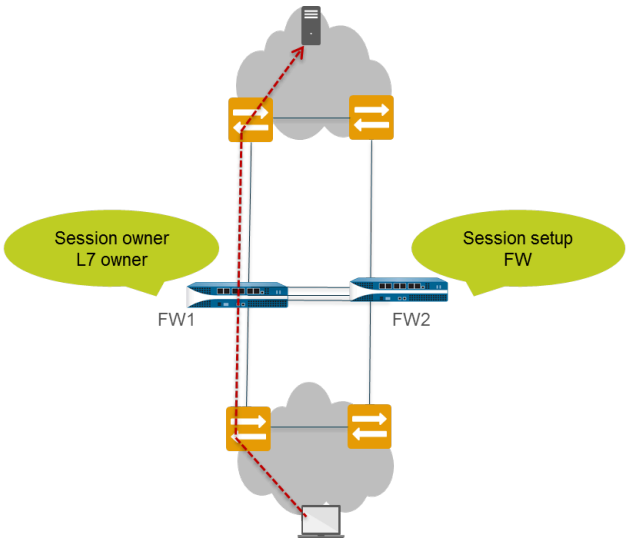
如有必要，防火牆使用 HA3 連結將封包傳送至其對等進行工作階段設定。下圖及文字說明了防火牆 FW1 接收用於新工作階段的封包路徑。紅色虛線表 FW1 轉送封包至 FW2，且 FW2 轉送封包至 HA3 連結上的 FW1。



- 終端主機傳送封包至 FW1。
- FW1 檢查封包的內容以將其比對現有工作階段。如果沒有工作階段相符，FW1 將確定其已接收新工作階段的第一個封包，因此稱為工作階段擁有者（假設 **Session Owner Selection**（工作階段擁有者選取項）設定為 **First Packet**（第一個封包）。
- FW1 使用已設定的工作階段設定負載共用選項來識別工作階段設定防火牆。在此範例中，FW2 設定用於執行工作階段設定。
- FW1 使用 HA3 連結來傳送第一個封包至 FW2。
- FW2 設定工作階段並返回封包至 FW1 進行 Layer 7 處理（如有）。
- FW1 隨後將封包從輸出介面轉送出去到達目的地。

下圖及文字說明了比對現有工作階段的封包路徑：

©2024 Palo Alto Networks, Inc.



- 終端主機傳送封包至 FW1。
- FW1 檢查封包的內容以將其比對現有工作階段。如果工作階段與現有工作階段相符，FW1 將處理封包並將封包從輸出介面轉送出去到達目的地。

主動/主動 HA 模式中的 NAT

在主動/主動 HA 組態中：

- 您必須將各動態 IP (DIP) NAT 規則與動態 IP 及連接埠 (DIPP) NAT 規則繫結至裝置 ID 0 或裝置 ID 1。
- 您必須將各靜態 NAT 規則繫結至裝置 ID 0、裝置 ID 1、兩個裝置 ID 或主動-主要狀態下的防火牆。

因此，當其中一個防火牆建立新工作階段時，裝置 ID **0** 或裝置 ID **1** 繫結將確定用哪條 NAT 規則來比對防火牆。裝置繫結必須包含工作階段擁有者防火牆以產生相符結果。

工作階段設定防火牆執行 NAT 原則比對，但 NAT 規則根據工作階段擁有者進行評估。即會根據連結至工作階段擁有者防火牆的 NAT 規則轉譯工作階段。執行 NAT 原則比對時，防火牆會略過未連結至工作階段擁有者防火牆的所有 NAT 規則。

例如，假設裝置 ID 1 的防火牆是工作階段擁有者，則該工作階段設定防火牆。當防火牆與裝置 ID 1 嘗試將工作階段與 NAT 規則進行比對時，它將略過連結至裝置 0 的所有規則。僅當工作階段擁有者與裝置 ID 在 NAT 規則比對中時，防火牆才會執行 NAT 轉譯。

通常在對等防火牆使用不同的 IP 位址進行轉譯時建立裝置特定的 NAT 規則。

如果其中一個對等防火牆失敗，主動防火牆將繼續處理失敗防火牆同步工作階段的流量，包括 NAT 流量。在來源 NAT 組態中，當一個防火牆失敗時：

- 用作 NAT 規則轉譯 IP 位址的浮動 IP 位址將轉送至繼續存在的防火牆。因此，進行容錯轉移的現有工作階段仍將使用此 IP 位址。

©2024 Palo Alto Networks, Inc.

- 所有新工作階段將使用繼續存在的防火牆自然而然擁有的裝置特定 NAT 規則。即，繼續存在的防火牆僅使用與其裝置 ID 相符的 NAT 規則轉譯新工作階段；它將略過任何繫結至失敗裝置 ID 的 NAT 規則。

如需主動/主動 HA 與 NAT 範例，請參閱：

- 使用案例：使用浮動 IP 位址設定主動/主動 HA（具有來源 DIPP NAT）
- 使用案例：為主動/主動 HA 防火牆設定單獨的來源 NAT IP 位址
- 使用案例：透過目的地 NAT 設定 ARP 負載共用的主動/主動 HA
- 使用案例：透過 Layer 3 中的目的地 NAT 設定 ARP 負載共用的主動/主動 HA

主動/主動 HA 模式中的 ECMP

當主動/主動 HA 對等失敗時，其工作階段將傳送至新的主動/主要防火牆，其將嘗試使用失敗防火牆所用的同一輸出介面。如果防火牆在 ECMP 路徑之間找到此類介面，傳輸的工作階段會採用相同的輸出介面和路徑。無論使用的 ECMP 演算法為何都會發生此行為；需要使用相同的介面。

只有在沒有符合原始輸出介面之 ECMP 路由的情況下，主動-主要防火牆才會選取新的 ECMP 路徑。

如果您未在主動/主動對等上設定相同的介面，主動-主要防火牆會從 FIB 表格中選取下一個最佳路徑。因此，系統可能不會根據 ECMP 演算法來散佈現有工作階段。

©2024 Palo Alto Networks, Inc.

設定主動/被動 HA

主動/被動 HA 先決條件

若要在 Palo Alto Networks 防火牆上設定高可用性，這兩個防火牆都需要符合下列要求：

- 型號相同—配對中的兩個防火牆必須為相同的硬體型號或虛擬機器型號。
- **PAN-OS** 版本相同—兩個防火牆應執行相同的 PAN-OS 版本，且應用程式、URL 及威脅資料庫皆必須為最新狀態。
- 相同的多虛擬系統功能—兩個防火牆必須啟用或停用 **Multi Virtual System Capability**（多虛擬系統功能）。啟用時，每個防火牆需要其自身的多虛擬系統授權。
- 介面類型相同—專用 HA 連結，或設定為 *interface type*（介面類型）HA 的管理連接埠與頻內連接埠組合。
  - 決定 HA 對等間 HA1（控制）連線的 IP 位址。如果兩個裝置為直接連接或連接至相同的交換器，則兩個對等的 HA1 IP 位址必須位於相同的子網路上。

    針對沒有專用 HA 連接埠的防火牆，可使用控制連線的管理連接埠。管理連接埠提供兩防火牆管理平面間的直接通訊連結。但是因為管理連接埠不會在對等間直接連接，因此請確定您有連接這兩個網路介面的路由器。
  - 如果使用 Layer 3 作為 HA2 (資料) 連線的傳輸方式，請決定 HA2 連結的 IP 位址。如果 HA2 連線必須在連接路由器的網路上通訊，請僅使用 Layer 3。HA2 連結的 IP 子網路不得與 HA1 連結的子網路重疊，或與防火牆上指定至資料連接埠的任何其他子網路重疊。
- 授權集相同 — 各防火牆的授權皆為唯一，無法在防火牆間共享。因此，您必須設定相同的防火牆授權。如果兩個防火牆的授權集不同，將無法同步設定資訊，亦無法維持同位檢查以進行無縫容錯移轉。

最佳做法是，若有現有的防火牆，並想要針對 *HA* 用途新增防火牆，且新防火牆具備現有的設定，則在新防火牆上將防火牆重設為原廠預設設定。如此可確保新防火牆具有全新的組態。設定 *HA* 後，您接著可將主要防火牆上的組態，與包含全新組態之最近引進的防火牆維持同步。

©2024 Palo Alto Networks, Inc.

主動/被動 HA 設定方針

若要設定 HA 中的主動 (PeerA) 被動 (PeerB) 配對，您必須將兩個防火牆上的部分選項設定為相同，某些選項設定為不同（不相符）。這些 HA 設定皆未在防火牆之間同步。如需同步/未同步之內容的詳細資料，請參閱參考：HA 同步。

以下檢查清單詳細列出了兩個防火牆必須完全相同的設定：

- 您必須在兩個防火牆上都啟用 HA。
- 您必須在兩個防火牆上設定相同的群組 ID 值。防火牆將使用群組 ID 值為所有已設定的介面建立虛擬 MAC 位址。關於虛擬 MAC 位址的資訊，請參閱「浮動 IP 位址和虛擬 MAC 位址」。新的主動防火牆接管後，將從所連線的每一個介面傳送 Gratuitous ARP 訊息，通知所連線的第 2 層交換器虛擬 MAC 位址的新位置。
- 如果您使用頻內連接埠作為 HA 連結，則必須將 HA1 和 HA2 的介面設定為 HA 類型。
- 在兩個防火牆上，將 HA 模式設定為 Active Passive（主動式被動式）。
- 若有必要，在兩個防火牆上啟用先佔。但是裝置的優先順序值不得相同。
- 如有必要，在兩個防火牆上設定 HA1 連結（用於 HA 對等之間的通訊）上的加密。

©2024 Palo Alto Networks, Inc.

- 請根據目前使用的 HA1 與 HA1 備份連接埠組合，採用下列建議來決定是否應啟用活動訊號備份：

  如果 *HA* 功能（*HA1* 和 *HA1* 備份）設定用於 *DHCP* 定址（***IP Type***（***IP*** 類型）設定為 ***DHCP Client***（***DHCP*** 用戶端），則在管理介面上不受支援。但 *AWS* 和 *Azure* 是例外，其中的管理介面設定為 *DHCP* 用戶端，且支援 *HA1* 與 *HA1* 備份連結。

  - HA1：專用 HA1 連接埠

    HA1 備份：專用 HA1 連接埠

    建議：啟用活動訊號備份
  - HA1：專用 HA1 連接埠

    HA1 備份：頻內連接埠

    建議：啟用活動訊號備份
  - HA1：專用 HA1 連接埠

    HA1 備份：管理連接埠

    建議：不要啟用活動訊號備份
  - HA1：頻內連接埠

    HA1 備份：頻內連接埠

    建議：啟用活動訊號備份
  - HA1：管理連接埠

    HA1 備份：頻內連接埠

    建議：不要啟用活動訊號備份

下表列示了必須在每個防火牆上獨立進行的設定：請參閱參考：HA 同步，瞭解更多關於未在對等間自動同步之其他設定的資訊。

獨立組態設定	**PeerA**	**PeerB**
控制連結	在此防火牆上 (PeerA) 設定的 HA1 連結 IP 位址。	在此防火牆上 (PeerB) 設定的 HA1 連結 IP 位址。
	針對沒有專用 HA 連接埠的防火牆，請使用控制連結的管理連接埠 IP 位址。	
資料連結 資料連結資訊會在啟用 HA 後的防火牆之間同步，	HA2 連結預設使用 Ethernet/Layer 2。 如果使用 Layer 3 連線，請設定此防火牆 (PeerA) 的資料連結 IP 位址。	HA2 連結預設使用 Ethernet/Layer 2。

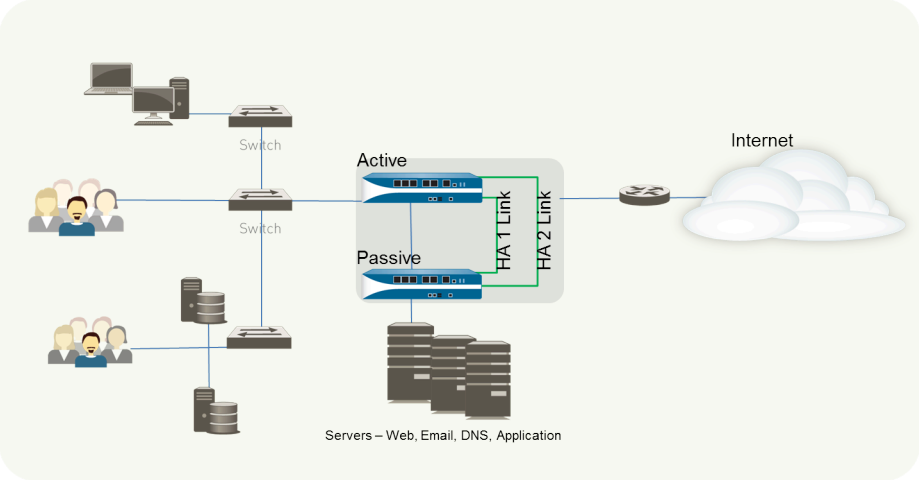
©2024 Palo Alto Networks, Inc.

獨立組態設定	PeerA	PeerB
並在防火牆之間建立控制連結。		如果使用 Layer 3 連線，請設定此防火牆 (PeerB) 的資料連結 IP 位址。
裝置優先順序 (如果啟用先佔，則必須設定)	若要作為主動防火牆，其數值必須小於該防火牆對等體的值。因此如果要將 PeerA 設定為主動防火牆，請保留預設值 100 並增加 PeerB 的值。 如果防火牆具有相同的裝置優先值，則其將 HA1 的 MAC 位址用作連結中斷器。	如果 PeerB 為被動，請將裝置優先值設定為大於 PeerA 上設定值的數值。例如，將此值設定為 110。
連結監控—監控此防火牆上處理重要流量的一或多個實體介面，並定義失敗條件。	選取在此防火牆上要監控的實體介面，並定義觸發容錯移轉的失敗條件（所有或任何）。	請挑選在此防火牆上要監控的實體介面類似設定，並定義觸發容錯移轉的失敗條件（所有或任何）。
路徑監控—監控一或多個防火牆可使用 ICMP偵測確認回應的目的地 IP 位址。	定義容錯移轉條件（全部或任何）、偵測間隔和偵測計數。這在監控其他互連網路裝置可用性方面特別實用。例如，監控連接伺服器的路由器可用性、伺服器主機連線或一些其他位於流量中的重要裝置。 請確定您在監控的節點/裝置不至於無法回應，特別是在承受負載時，因為這可能會造成路徑監控失敗並觸發容錯移轉。	請挑選可監控判斷 PeerB 容錯移轉觸發程序的裝置類似設定或目的地 IP 位址。定義容錯移轉條件（全部或任何）、偵測間隔和偵測計數。

設定主動/被動 HA

下列程序說明如何設定主動/被動部署中的防火牆配對，如下列範例拓撲所述。

©2024 Palo Alto Networks, Inc.



若要設定主動/被動 HA 配對，需先在第一個防火牆上完成下列工作流程，然後在第二個防火牆上重複這些步驟。

STEP 1 | 連接 HA 連接埠以設定防火牆間的實體連線。

- 針對有專用 HA 連接埠的防火牆，請使用乙太網路纜線連接對等體上的專用 HA1 連接埠與 HA2 連接埠。如果防火牆彼此直接連接，請使用跳接纜線。
- 針對沒有專用 HA 連接埠的防火牆，請選取供 HA2 連結和備份 HA1 連結使用的兩個資料介面。然後，請使用乙太網路纜線連接這兩個防火牆上的頻內 HA 介面。

請使用 HA1 連結的管理連接埠，並確保管理連接埠可在您的網路中彼此連接。

STEP 2 | 在管理連接埠上啟用偵測。

啟用偵測可讓管理連接埠交換活動訊號備份資訊。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Interfaces**（介面） > **Management**（管理）。
2. 選取 **Ping** 作為介面上允許的服務。

STEP 3 | 如果防火牆沒有專用的 HA 連接埠，請將資料連接埠設定為可發揮 HA 連接埠的功能。

針對具有專用 HA 連接埠的防火牆，請繼續進行下一步。

1. 選取 **Network**（網路） > **Interfaces**（界面）。
2. 確認在要使用的連接埠上開啟連結。
3. 選取介面並將 **Interface Type**（介面類型）設定為 **HA**。
4. 視需要完成 **Link Speed**（連結速度）及 **Link Duplex**（連結雙工）設定。

©2024 Palo Alto Networks, Inc.

STEP 4 | 設定 HA 模式及群組 ID。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般），然後編輯 Setup（設定）區段。
2. 設定配對的 **Group ID**（群組 **Id**）並選擇設定其並選擇設定其 **Description**（說明）。群組 ID 會唯一識別您網路上的每個 HA 配對。如果您有多個共用相同廣播網域的 HA 配對，請務必為每個配對設定唯一的群組 ID。
3. 將模式設定為 **Active Passive**（主動式被動式）。

STEP 5 | 設定控制連結連線。

此範例說明設定為介面類型 HA 的頻內連接埠。

針對使用管理連接埠作為控制連結的防火牆，將自動填入 IP 位址資訊。

1. 在 **Device**（裝置） > **High Availability**（高可用性） > **HA Communications**（**HA** 通訊）中，編輯 Control Link (HA1)（控制連結 (HA1)）。
2. 選取要當成 HA1 連結使用的 **Port**（連接埠）。
3. 設定 **IPv4/IPv6 Address**（**IPv4/IPv6** 位址）及 **Netmask**（網路遮罩）。

   如果 HA1 介面位於不同子網路，請輸入 **Gateway**（閘道）的 IP 位址。如果防火牆為直接連線或位於同一個 VLAN 中，請勿新增閘道位址。

STEP 6 | （選用）啟用控制連結連線加密。

這通常用於確保兩個防火牆未直接連接時的連結，也就是連接埠連接至交換器或路由器。

1. 從防火牆中匯出 HA 金鑰再匯入對等防火牆。
   1. 選取 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證）。
   2. 選取匯出 **Export HA key**（匯出 **HA** 金鑰）。將 HA 金鑰儲存至對等體可存取的網路位置。
   3. 在對等防火牆上，選取 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證），再選取 **Import HA key**（匯入 **HA** 金鑰） 以瀏覽至金鑰儲存位置，然後將金鑰匯入到對等體。
   4. 第二個防火牆上重複此過程以交換兩個裝置上的 HA 金鑰。
2. 選取 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般），編輯 Control Link (HA1)（控制連結 (HA1)）區段。
3. 選取 **Encryption Enabled**（已啟用加密）。

   如果您啟用了加密，完成設定 *HA* 防火牆之後，您可以重新整理 HA1 SSH 金鑰並設定金鑰選項。

©2024 Palo Alto Networks, Inc.

STEP 7 | 設定備份控制連結連線。

1. 在 **Device**（裝置） > **High Availability**（高可用性） > **HA Communications**（**HA** 通訊）中，編輯 Control Link (HA1 Backup)（控制連結（HA1 備份））。
2. 選取 HA1 備份介面並設定 **IPv4/IPv6 Address**（**IPv4/IPv6** 位址）及 **Netmask**（網路遮罩）。

   PA-3200 系列防火牆不支援對 *HA1* 備份控制連結使用 *IPv6* 位址；使用 *IPv4* 位址。

STEP 8 | 設定防火牆間的資料連結連線 (HA2) 及備份 HA2 連線。

1. 在 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般）中，編輯 Data Link (HA2)（資料連結 (HA2)）區段。
2. 選取要用於資料連結連線的 **Port**（連接埠）。
3. 選取傳輸 方式。預設為 **ethernet**（乙太網路），只有在 HA 配對為直接連接或透過交換器時才有作用。若要透過網路處理資料連結流量，請選取 **IP** 或 **UDP** 作為傳輸模式。
4. 如果使用 IP 或 UDP 作為傳輸模式，請輸入 **IPv4/IPv6 Address**（**IPv4/IPv6** 位址）與 **Netmask**（網路遮罩）。
5. 請確認是否已選取 **Enable Session Synchronization**（啟用工作階段同步）。
6. 選取 **HA2 Keep-alive** 可啟用對 HA 對等體之間 HA2 資料連結的監控。如果根據設定的臨界值（預設為 10000 毫秒）發生故障，將會出現定義的動作。針對主動/被動設定，發生 HA2 保持運作失敗時，會產生重要系統日誌訊息。

   您可以在兩個防火牆都設定 *HA2* 保持運作選項，或僅設定 *HA* 配對中的一個防火牆。如果僅對一個防火牆啟用選項，僅該防火牆會傳送保持運作訊息。發生故障時，會通知另一個防火牆。
7. 編輯 **Data Link (HA2 Backup)**（資料連結（**HA2** 備份））區段，選取介面，然後新增 **IPv4/IPv6 Address**（**IPv4/IPv6** 位址）及 **Netmask**（網路遮罩）。

STEP 9 | 如果您的控制連結使用專用的 HA 連接埠或頻內連接埠，請啟用活動訊號備份。

如果正在使用控制連結的管理連接埠，則無須啟用活動訊號備份。

1. 在 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般） 中，編輯 Election Settings（選取設定）。
2. 選取 **Heartbeat Backup**（活動訊號備份）。

   若要允許在防火牆間傳送活動訊號，您必須確認兩個對等體中的管理連接埠可相互路由傳送。

   啟用活動訊號備份也可讓您避免發生腦分裂 *(split-brain)* 狀況。當 *HA1* 連結中斷而造成防火牆失去活動訊號時，就會發生腦分裂狀況，即使是防火牆仍在運作中。在此狀況下，每個對等體會認為另一個對等體已停擺，並嘗試啟動正在執行的服務，因此造成腦分裂。當活動訊號備份連結啟用時，會防止腦分裂，因為會透過管理連接埠傳輸備援的活動訊號與您好訊息。

©2024 Palo Alto Networks, Inc.

STEP 10 | 設定裝置優先順序及啟用先佔。

此設定只有在想確定特定防火牆是偏好的主動防火牆時才需使用。相關資訊，請參閱裝置優先順序及先佔。

1. 在 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般） 中，編輯 Election Settings（選取設定）。
2. 設定 **Device Priority**（裝置優先順序）中的數值。請確定在要指定較高優先順序的防火牆上設定較小的數值。

   如果兩個防火牆具備相同的防火牆優先順序值，則 *HA1* 控制連結上有最小 *MAC* 位址的防火牆會成為主動防火牆。
3. 選取 **Preemptive**（先佔）。

   您必須在主動與被動防火牆上啟用先佔。

STEP 11 | （選用）修改 HA計時器。

依預設，HA 計時器設定檔是設定為 **Recommended**（建議的）設定檔，並且適用於最近的 HA 部署。

1. 在 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般） 中，編輯 Election Settings（選取設定）。
2. 選取 **Aggressive**（積極）設定檔可更快速觸發容錯移轉；選取 **Advanced**（進階）可定義自訂值，以便在您的設定中觸發容錯移轉。

   若要檢視設定檔包含的個別計時器的預設值，請選取 ***Advanced***（進階）並按一下 ***Load Recommended***（建議的載入）或 ***Load Aggressive***（積極的載入）。畫面將顯示硬體機型的預設值。

©2024 Palo Alto Networks, Inc.

STEP 12 | （選用）修改被動防火牆上 HA 連接埠的連結狀態。

被動連結狀態預設為 ***shutdown***（關閉）。啟用 *HA* 後，主動防火牆 *HA* 連接埠的連結狀態會變為綠色，被動防火牆的連結狀態則為停用並顯示紅色。

將連結狀態設定為 **Auto**（自動）可減少被動防火牆在發生故障時接管需花費的時間，並允許您監控連結狀態。

啟用被動防火牆的連結狀態，保持開啟並反應實體介面上的連線狀態：

1. 在 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般）中，編輯 Active Passive Settings（主動/被動設定）。
2. 將 **Passive Link State**（被動連結狀態）設定為 **Auto**（自動）。

   自動選項可減少被動防火牆在發生容錯移轉時接管需花費的時間。

   雖然介面顯示綠色（代表已連接並開啟），卻持續捨棄所有流量直到觸發容錯移轉。

   修改被動連結狀態時，請確定相鄰裝置不會轉送流量至僅以防火牆連結狀態為基礎的被動防火牆。

STEP 13 | 啟用 HA。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般），然後編輯 Setup（設定）區段。
2. 選取 **Enable HA**（啟用 **HA**）。
3. 選取 **Enable Config Sync**（啟用設定同步）。此設定會啟用主動與被動防火牆之間的設定同步。
4. 在 **Peer HA1 IP Address**（對等 **HA IP** 位址）中輸入指定至對等體控制連結的 IP 位址。

   針對沒有專用 HA 連接埠的防火牆，如果對等體使用 HA1 連結的管理連接埠，請輸入對等體的管理連接埠 IP 位址。
5. 輸入 **Backup HA1 IP Address**（備份對等 **HA IP** 位址）。

©2024 Palo Alto Networks, Inc.

STEP 14 | （選用）如果您的網路使用 LACP 或 LLDP，則啟用主動/被動 HA 的 LACP 和 LLDP 預交涉，以加快容錯移轉。

如果您在主動模式中運作預交涉功能，先啟用 LACP 和 LLDP，再為通訊協定設定 *HA* 預交涉。

1. 確保在步驟 12 中將連結狀態設定為 **Auto**（自動）。
2. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路）。
3. 若要啟用 LACP 主動預交涉：
   1. 在 Layer 2 或 Layer 3 部署中選取 AE 介面。
   2. 選取 **LACP** 頁籤。
   3. 選取 **Enable in HA Passive State**（啟用 **HA** 被動狀態）。
   4. 按一下 **OK**（確定）。

      此外，您無法選取 ***Same System MAC Address for Active-Passive HA***（適用於主動-被動 ***HA*** 的相同系統 ***MAC*** 位址），因為預交涉需要主動與被動防火牆上具有唯一的介面 *MAC* 位址。
4. 若要啟用 LACP 被動預交涉：
   1. 在 Virtual Wire 部署中選取乙太網路介面。
   2. 選取 **Advanced**（進階）頁籤。
   3. 選取 **LACP** 頁籤。
   4. 選取 **Enable in HA Passive State**（啟用 **HA** 被動狀態）。
   5. 按一下 **OK**（確定）。
5. 若要啟用 LLDP 主動預交涉：
   1. 在 Layer 2、Layer 3 或 Virtual Wire 部署中選取乙太網路介面。
   2. 選取 **Advanced**（進階）頁籤。
   3. 選取 **LLDP** 頁籤。
   4. 選取 **Enable in HA Passive State**（啟用 **HA** 被動狀態）。
   5. 按一下 **OK**（確定）。

      如果您想要允許對虛擬介接部署進行 *LLDP* 被動預交涉，請執行步驟 14.e，但不要啟用 *LLDP* 本身。

STEP 15 | 儲存您的組態變更。

按一下 **Commit**（交付）。

©2024 Palo Alto Networks, Inc.

STEP 16 | 完成兩個防火牆的設定後，請確認配對的防火牆為主動/被動 HA。

1. 存取兩個防火牆上的 **Dashboard**（儀表板），然後檢視高可用性 Widget。
2. 在主動防火牆上，按一下 **Sync to peer**（同步處理至對等體）連結。
3. 確認防火牆已配對並同步，如下所示：
   - 在被動防火牆上：本機防火牆狀態應顯示為 **passive**（被動），而執行中設定應顯示為 **synchronized**（已同步）。
   - 在主動防火牆上：本機防火牆狀態應顯示為 **active**（主動），而執行中設定應顯示為 **synchronized**（已同步）。

定義 HA 容錯移轉條件

執行下列工作以使用連結監控或路徑監控定義 容錯移轉 條件，並因此確定哪些事件將造成 HA 配對中的防火牆發生容錯移轉，將保護流量的工作從之前作用中的防火牆傳遞給其 HA 對等。HA 概要介紹中介紹了會造成容錯移轉的條件。

您可以監控每個虛擬路由器、VLAN 或虛擬介接的多個 IP 路徑群組。您可以為每個路徑群組啟用一個或多個 IP 位址，並為每個路徑群組提供自己的對等故障條件。此外，您還可以使用「任何」或「所有」故障檢查來確定作用中防火牆的狀態，從而在路徑群組層級和更廣泛的虛擬路由器或 VLAN 或虛擬介接群組層級上設定這些故障條件。

當您升級到 PAN OS 10.0 時，防火牆會自動將您當前監控的目的地 IP 位址傳輸到新建立的目的地群組，並為該群組提供預設的路徑監控名稱。新的目的地群組會在路徑群組層級保留您之前的容錯移轉條件。

升級到 *PAN-OS 11.0* 之前，請確保刪除主動/主動 *HA* 中的所有 *VLAN* 路徑監控設定，因為 *VLAN* 路徑監控與 *PAN-OS 10.0* 中的主動/主動 *HA* 配對不相容；保留較早的主動/主動 *HA* 設定會導致自動提交失敗。

在啟用路徑監控之前，必須設定虛擬路由器、VLAN 或虛擬介接或這些邏輯網路元件的組合。虛擬路由器和虛擬介接中的路徑監控與主動/主動和主動/被動 HA 部署相容；但是，僅主動/被動配對支援 VLAN 中的路徑監控。

在啟用路徑監控前，還必須：

- 檢查虛擬路由器中目的地 IP 群組的連線性。
- 確保 VLAN（打算為其啟用路徑監控）包括已設定的介面。
- 獲取將用於從適當的目的地 IP 位址接收 ping 的來源 IP 位址。

如果您使用 *SNMPv3* 來監控防火牆，請注意，*SNMPv3* 引擎 *ID* 會在 *HA* 配對之間同步。如需設定關於 *SNMP* 的資訊，請參閱將設陷轉送至 SNMP 管理員。因為引擎 *ID* 是使用防火牆序號所產生的，所以在 *VM* 系列的防火牆上，您必須套用有效的授權，才能取得每個防火牆的唯一引擎 *ID*。

©2024 Palo Alto Networks, Inc.

STEP 1 | 要設定 HA 連結監控，請指定一組實體介面以供防火牆監控（連結開啟或連結關閉）。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） > **Link and Path Monitoring**（連結與路徑監控）。
2. 在「連結監控」區段中，按 **Name**（名稱）**Add**（新增）一個連結群組。
3. 選取 **Enabled**（已啟用）啟用連結群組。
4. 為連結群組中的介面選取 **Failure Condition**（失敗條件）：**Any**（任何）（預設值）或 **All**（全部）。
5. **Add**（新增）要監控的 **Interface**（介面）。
6. 按一下 **OK**（確定）。

STEP 2 | （選用）修改防火牆上設定的連結群組集的失敗條件。

依預設，防火牆會在發生任何監控連結群組失敗時觸發容錯移轉。

1. 編輯 **Link Monitoring**（連結監控）區段。
2. 將 **Failure Condition**（失敗條件）設定為**Any**（任何）（預設值）或 **All**（全部）。
3. 按一下 **OK**（確定）。

STEP 3 | 若要為虛擬介接、VLAN 或虛擬路由器（對於進階路由引擎，則為邏輯路由器）設定 HA 路徑監控，請指定防火牆將執行 ping 作業以驗證網路連線性的目的地 IP 位址。

1. 在 Path Monitoring（路徑監控）區段中，選取 **Add Virtual Wire Path**（新增虛擬介接路徑）、**Add VLAN Path**（新增 **VLAN** 路徑）或 **Add Virtual Router Path**（新增虛擬路由器路徑）（對於進階路由引擎，則為 **Add Logical Router Path**（新增邏輯路由器路徑））。
2. 輸入虛擬介接、VLAN、虛擬路由器路徑群組或邏輯路由器路徑群組的 **Name**（名稱）。
3. （僅限虛擬介接路徑或 VLAN 路徑）輸入 **Source IP**（來源 **IP**）位址以用於透過虛擬介接或 VLAN 來 ping 目的地 IP 位址。
4. 選取 **Enabled**（已啟用）啟用路徑群組。
5. 選取導致此路徑群組失敗的 **Failure Condition**（失敗條件）：**Any**（任何）（預設值），在此路徑群組中一個或多個目的地 IP 群組失敗時發佈失敗，或 **All**（全部），在此路徑群組中的全部目的地 IP 群組失敗時發佈失敗。
6. 輸入以毫秒為單位的 **Ping Interval**（**Ping** 間隔）；傳送 ICMP 訊息至目的地 IP 位址的間隔（範圍為 200 至 60,000；預設值為 200）。
7. 輸入 **Ping Count**（**Ping** 計數），即宣告失敗前必須失敗的 ping 次數（範圍為 3 到 10；預設值為 10）。
8. **Add**（新增）並輸入 **Destination IP Group**（目的地 **IP** 群組）名稱。
9. **Add**（新增）要 ping 的一個或多個 **Destination IP**（目的地 **IP**）位址。
10. 選取 **Enabled**（已啟用）為目的地 IP 群組啟用路徑監控。

©2024 Palo Alto Networks, Inc.

11. 選取導致此目的地 IP 群組失敗的 **Failure Condition**（失敗條件）：**Any**（任何）（預設值），在一個或多個所列 IP 位址無法連線時發佈失敗，或 **All**（全部），在全部所列 IP 位址無法連線時發佈失敗。
12. 按兩下 **OK**（確定）。
13. （僅限 Panorama）選取適當的 Panorama 範本以將路徑監控設定推送到您的設備。

    您只能將虛擬介接、*VLAN* 或虛擬路由器的 *HA* 路徑監控推送至執行 *PAN-OS 10.0* 或更新版本的防火牆。如果您嘗試將設定推送到執行 *PAN-OS 10.0* 之前版本（例如 *9.1.x* 或 *9.0.x*）的防火牆，則提交可能會失敗，或提交可能會從路徑群組中移除目的地 *IP* 位址。

    執行 *PAN-OS 9.1* 及更早版本的受管理防火牆僅支援包含一個目的地 *IP* 群組的 *HA* 路徑群組。

    若要從 *Panorama* 管理執行不同 *PAN-OS* 版本的受管理防火牆的目的地 *IP* 位址，請為執行 *PAN-OS 10.0* 及更新版本的受管理防火牆建立單獨的範本，並為執行 *PAN-OS 9.1* 和更早版本的受管理防火牆建立單獨的範本。如果您建立了多個目的地 *IP* 群組，這可讓您更精確地控制目的地 *IP* 位址設定，並確保受管理的防火牆順利容錯移轉。

STEP 4 | （選用）修改防火牆上設定的路徑群組集的失敗條件。

依預設，防火牆會在發生任何監控路徑群組失敗時觸發容錯移轉。

1. 編輯 **Path Monitoring**（路徑監控）區段。
2. 選取 **Enabled**（已啟用）以在設備上啟用路徑監控。
3. 將 **Failure Condition**（失敗條件）設定為 **Any**（任何）（預設值），以便在監控的一個或多個虛擬路由器、VLAN 或虛擬介接關閉時為此防火牆發佈失敗。選取 **All**（全部）以便在監控的全部虛擬路由器、VLAN 或虛擬介接關閉時為此防火牆發佈失敗。
4. 按一下 **OK**（確定）。

STEP 5 | **Commit**（認可）。

確認容錯移轉

若要測試 HA 設定是否正常運作，可觸發手動容錯移轉，並確認防火牆成功轉換狀態。

STEP 1 | 暫停主動防火牆。

選取 **Device**（裝置）> **High Availability**（高可用性）> **Operational Commands**（操作命令），然後按一下 **Suspend local device**（暫停本機裝置）連結。

STEP 2 | 確認被動防火牆已經以主動身分接管。

在 **Dashboard**（儀表板）上，確認被動防火牆在高可用性 Widget 中的狀態變更為 **active**（主動）。

©2024 Palo Alto Networks, Inc.

STEP 3 | 將暫停的防火牆還原為作用狀態。如果已啟用先佔，請等候幾分鐘後，再確認 **Preemptive**（先佔）結果。

1. 在先前暫停的防火牆上，選取 **Device**（裝置） > **High Availability**（高可用性） > **Operational Commands**（操作命令），然後按一下 **Make local device functional**（讓本機裝置運作）連結。
2. 在 **Dashboard**（儀表板）上的高可用性 Widget 中，確認防火牆已經以主動防火牆的身分接管，且對等防火牆目前為被動狀態。

©2024 Palo Alto Networks, Inc.

設定主動/主動 HA

主動/主動 HA 先決條件

若要在防火牆上設定主動/主動高可用性，這兩個防火牆都需要符合下列要求：

- 型號相同 — 配對中的防火牆必須為相同的硬體型號。
- **PAN-OS** 版本相同 — 防火牆必須執行相同的 PAN-OS 版本，且應用程式、URL 及威脅資料庫皆必須為最新狀態。
- 相同的多虛擬系統功能—兩個防火牆必須啟用或停用 **Multi Virtual System Capability**（多虛擬系統功能）。啟用時，每個防火牆需要其自身的多虛擬系統授權。
- 介面類型相同—專用 HA 連結，或設定為 *interface type*（介面類型）HA 的管理連接埠與頻內連接埠組合。
  - HA 介面必須僅設定靜態 IP 位址，而非從 DHCP 取得的 IP 位址（AWS 可使用 DHCP 位址的情況除外）。決定 HA 對等間 HA1（控制）連線的 IP 位址。如果兩個裝置為直接連接或連接至相同的交換器，則對等的 HA1 IP 位址必須位於相同的子網路上。

    針對沒有專用 HA 連接埠的防火牆，可使用控制連線的管理連接埠。管理連接埠提供兩防火牆管理平面間的直接通訊連結。但是因為管理連接埠不會在對等間直接連接，因此請確定您有連接這兩個網路介面的路由器。
  - 如果使用 Layer 3 作為 HA2 (資料) 連線的傳輸方式，請決定 HA2 連結的 IP 位址。如果 HA2 連線必須在連接路由器的網路上通訊，請僅使用 Layer 3。HA2 連結的 IP 子網路不得與 HA1 連結的子網路重疊，或與防火牆上指定至資料連接埠的任何其他子網路重疊。
  - 每個防火牆都需要 HA3 連結的專用介面。PA-7000 系列、PA-5400 系列、PA-3400 系列、PA-3200 和 PA-1400 系列防火牆均將 HSCI 連接埠用於 HA3。PA-5200 系列防火牆將 HSCI 用於 HA3，或者您可以設定 資料平面連接埠上的彙總介面用於 HA3，以作為備援。在其餘平台上，您可以將資料平面上的彙總介面設定為 HA3 連結用於備援。
- 授權集相同 — 各防火牆的授權皆為唯一，無法在防火牆間共享。因此，您必須設定相同的防火牆授權。如果兩個防火牆的授權集不同，將無法同步設定資訊，亦無法維持同位檢查以進行無縫容錯移轉。

若有現有的防火牆，並想要針對 *HA* 用途新增防火牆，且新防火牆具備現有的設定，則建議您在新防火牆上將防火牆重設為原廠預設設定。如此可確保新防火牆具有全新的組態。設定 *HA* 後，您接著可將主要防火牆上的設定，與包含全新設定之最近引進的防火牆維持同步。此外，您還必須設定本機 *IP* 位址。

©2024 Palo Alto Networks, Inc.

設定主動/主動 HA

以下程序介紹了在主動/主動組態中設定防火牆的基本工作流程。但在開始前，先確定主動/主動使用案例，確保組態範例更貼合特定網路環境。

您可以將資料連接埠設定為專用 *HA* 介面和專用備份 *HA* 介面。對於沒有專用 *HA* 介面的防火牆（如*PA-200*、*PA-400*系列），需要設定一個資料連接埠作為 *HA* 介面。

設定為 *HA1*、*HA2* 或 *HA3* 介面的資料連接埠可以直接連接到防火牆上的每個 *HA* 介面，也可以透過第二層交換器連接。對於設定為 *HA3* 介面的資料連接埠，您必須啟用巨型框架，因為 *HA3* 訊息超過 *1,500* 個位元組。

若要設定主動/主動，首先需在一個對等體上完成下列步驟，然後在第二個對等體上完成這些步驟，以確保您為每個對等體設定了不同的裝置 ID 值（0 或 1）。

STEP 1 | 連接 HA 連接埠以設定防火牆間的實體連線。

對於每種使用案例，防火牆可以是任何硬體型號；選擇與型號對應的 *HA3* 步驟。

- 針對有專用 HA 連接埠的防火牆，請使用乙太網路纜線連接對等體上的專用 HA1 連接埠與 HA2 連接埠。如果防火牆彼此直接連接，請使用跳接纜線。
- 針對沒有專用 HA 連接埠的防火牆，請選取供 HA2 連結和備份 HA1 連結使用的兩個資料介面。然後，請使用乙太網路纜線連接這兩個防火牆上的頻內 HA 介面。請使用 HA1 連結的管理連接埠，並確保管理連接埠可在您的網路中彼此連接。
- HA3：
  - 在 PA-7000 系列防火牆上，將第一個底座的高速機殼互連 (HSCI) (HSCI-A) 連接至第二個底座的 HSCI-A，將第一個底座的 HSCI-B 連接至第二個底座的 HSCI-B。
  - 在 PA-5450 防火牆上，將第一個底座上的 HSCI-A 連線至第二個底座上的 HSCI-A，將第一個底座上的 HSCI-B 連線至第二個底座上的 HSCI-B。
  - 在 PA-5400 Series 防火牆（有一個 HSCI 連接埠）上，將第一個底座上的 HSCI 連接埠連線至第二個底座上的 HSCI 連接埠。
  - 在 PA-5200 系列防火牆（有一個 HSCI 連接埠）上，將第一個底座的 HSCI 連接埠連線至第二個底座的 HSCI 連接埠。您還可以使用 PA-5200 系列防火牆上的 HA3 資料連接埠。
  - 在 PA-3400 Series 防火牆（有一個 HSCI 連接埠）上，將第一個底座上的 HSCI 連接埠連線至第二個底座上的 HSCI 連接埠。
  - 在 PA-3200 系列防火牆（有一個 HSCI 連接埠）上，將第一個底座的 HSCI 連接埠連線至第二個底座的 HSCI 連接埠。
  - 在任何其他型號上，使用 HA3 資料平面介面。

©2024 Palo Alto Networks, Inc.

STEP 2 | 在管理連接埠上啟用偵測。

啟用偵測可讓管理連接埠交換活動訊號備份資訊。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Interfaces**（介面） > **Management**（管理）。
2. 選取 **Ping** 作為介面上允許的服務。

STEP 3 | 如果防火牆沒有專用的 HA 連接埠，請將資料連接埠設定為可發揮 HA 連接埠的功能。

針對具有專用 HA 連接埠的防火牆，請繼續進行下一步。

1. 選取 **Network**（網路） > **Interfaces**（界面）。
2. 確認在要使用的連接埠上開啟連結。
3. 選取介面並將 **Interface Type**（介面類型）設定為 **HA**。
4. 視需要完成 **Link Speed**（連結速度）及 **Link Duplex**（連結雙工）設定。

STEP 4 | 啟用主動/主動 HA 並設定群組 ID。

1. 在 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般）中，編輯 Setup（設定）。
2. 選取 **Enable HA**（啟用 **HA**）。
3. 輸入 **Group ID**（群組 **ID**），在兩個防火牆上必須採用相同設定。防火牆使用群組 ID 來計算虛擬 MAC 位址（範圍是 1-63）。
4. （選用）輸入 **Description**（說明）。
5. 對於 **Mode**（模式），選取 **Active Active**（主動/主動）。

STEP 5 | 在對等防火牆上設定裝置 ID，啟用同步，並識別控制連結

1. 在 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般）中，編輯 Setup（設定）。
2. 按如下方式選取 **Device ID**（裝置 **ID**）：
   - 在設定第一個對等體時，將 **Device ID**（裝置 **ID**）設定為 **0**。
   - 在設定第二個對等體時，將 **Device ID**（裝置 **ID**）設定為 **1**。
3. 選取 **Enable Config Sync**（啟用設定同步）。此設定需要同步兩個防火牆組態（預設會啟用）。
4. 輸入 **Peer HA1 IP Address**（對等 **HA1 IP** 位址），這是對等防火牆上 HA1 控制連結的 IP 位址。
5. （選用）輸入 **Backup Peer HA1 IP Address**（備份對等 **HA1 IP** 位址），這是對等防火牆上備份控制連結的 IP 位址。
6. 按一下 **OK**（確定）。

©2024 Palo Alto Networks, Inc.

STEP 6 | 確定防火牆具有數值較低的裝置 ID 的防火牆是否在復原失敗時先佔主動-主要防火牆。

1. 在 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般） 中，編輯 Election Settings（選取設定）。
2. 選取 **Preemptive**（先佔）可使具有數值較低的裝置 ID 的防火牆在防火牆復原失敗後繼續主動-主要運作。兩個防火牆都必須選取 **Preemptive**（先佔），才能出現先佔行為。

   如果您想要主動-主要角色保留目前的防火牆，則取消選取 **Preemptive**（先佔），直至手動將復原的防火牆設定為主動-主要防火牆。

STEP 7 | 如果您的控制連結使用專用的 HA 連接埠或頻內連接埠，請啟用活動訊號備份。

如果正在使用控制連結的管理連接埠，則無須啟用活動訊號備份。

1. 在 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般） 中，編輯 Election Settings（選取設定）。
2. 選取 **Heartbeat Backup**（活動訊號備份）。

   若要允許在防火牆間傳送活動訊號，您必須確認兩個對等體中的管理連接埠可相互路由傳送。

   啟用活動訊號備份可讓您避免發生腦分裂 *(split-brain)* 狀況。當 *HA1* 連結中斷而造成防火牆失去活動訊號時，就會發生腦分裂狀況，即使是防火牆仍在運作中。在此狀況下，每個對等體會認為另一個對等體已停擺，並嘗試啟動正在執行的服務，因此造成腦分裂。啟用動訊號備份連結可防止腦分裂，因為會透過管理連接埠傳輸備援的活動訊號與您好訊息。

STEP 8 | （選用）修改 HA計時器。

依預設，HA 計時器設定檔是設定為 **Recommended**（建議的）設定檔，並且適用於最近的 HA 部署。

1. 在 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般） 中，編輯 Election Settings（選取設定）。
2. 選取 **Aggressive**（積極）可觸發更快的容錯轉移。選取 **Advanced**（進階）可定義在設定中觸發容錯轉移的自訂值。

   若要檢視設定檔包含的個別計時器的預設值，請選取 ***Advanced***（進階）並按一下 ***Load Recommended***（建議的載入）或 ***Load Aggressive***（積極的載入）。畫面將顯示硬體機型的預設值。

©2024 Palo Alto Networks, Inc.

STEP 9 | 設定控制連結連線。

此範例使用設定為介面類型 HA 的頻內連接埠。

針對使用管理連接埠作為控制連結的防火牆，將自動填入 IP 位址資訊。

1. 在 **Device**（裝置） > **High Availability**（高可用性） > **HA Communications**（**HA** 通訊）中，編輯 Control Link (HA1)（控制連結 (HA1)）。
2. 選取要當成 HA1 連結使用的 **Port**（連接埠）。
3. 設定 **IPv4/IPv6 Address**（**IPv4/IPv6** 位址）及 **Netmask**（網路遮罩）。

   如果 HA1 介面位於不同子網路，請輸入 **Gateway**（閘道）的 IP 位址。如果防火牆為直接連接，請勿新增閘道位址。

STEP 10 | （選用）啟用控制連結連線加密。

這通常用於確保兩個防火牆未直接連接時的連結，也就是連接埠連接至交換器或路由器。

1. 從防火牆中匯出 HA 金鑰再匯入對等防火牆。
   1. 選取 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證）。
   2. 選取匯出 **Export HA key**（匯出 **HA** 金鑰）。將 HA 金鑰儲存至對等體可存取的網路位置。
   3. 在對等防火牆上，選取 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證），再選取 **Import HA key**（匯入 **HA** 金鑰） 以瀏覽至金鑰儲存位置，然後將金鑰匯入到對等體。
2. 在 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般）中，編輯 Control Link (HA1)（控制連結 (HA1)）。
3. 選取 **Encryption Enabled**（已啟用加密）。

   如果您啟用了加密，完成設定 *HA* 防火牆之後，您可以重新整理 HA1 SSH 金鑰並設定金鑰選項。

STEP 11 | 設定備份控制連結連線。

1. 在 **Device**（裝置） > **High Availability**（高可用性） > **HA Communications**（**HA** 通訊）中，編輯 Control Link (HA1 Backup)（控制連結（HA1 備份））。
2. 選取 HA1 備份介面並設定 **IPv4/IPv6 Address**（**IPv4/IPv6** 位址）及 **Netmask**（網路遮罩）。

   PA-3200 系列防火牆不支援對 *HA1* 備份控制連結使用 *IPv6* 位址；使用 *IPv4* 位址。

©2024 Palo Alto Networks, Inc.

STEP 12 | 設定防火牆間的資料連結連線 (HA2) 及備份 HA2 連線。

1. 在 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般） 中，編輯 Data Link (HA2)（資料連結 (HA2)）。
2. 選取要用於資料連結連線的 **Port**（連接埠）。
3. 選取傳輸 方式。預設為 **ethernet**（乙太網路），只有在 HA 配對為直接連接或透過交換器時才有作用。若要透過網路處理資料連結流量，請選取 **IP** 或 **UDP** 作為傳輸模式。
4. 如果使用 IP 或 UDP 作為傳輸模式，請輸入 **IPv4/IPv6 Address**（**IPv4/IPv6** 位址）與 **Netmask**（網路遮罩）。
5. 請確認是否已選取 **Enable Session Synchronization**（啟用工作階段同步）。
6. 選取 **HA2 Keep-alive** 可啟用對 HA 對等體之間 HA2 資料連結的監控。如果根據設定的臨界值（預設為 10000 毫秒）發生故障，將會出現定義的動作。發生 HA2 保持運作失敗時，系統會根據您的組態，產生重要系統日誌訊息或導致資料平面分割。

   您可以在兩個防火牆都設定 *HA2* 保持運作選項，或僅設定 *HA* 配對中的一個防火牆。如果僅對一個防火牆啟用選項，僅該防火牆會傳送保持運作訊息。發生故障時，會通知另一個防火牆。

   分割資料平面會使兩個對等體的資料平面獨立運作，同時保持高可用狀態為主動-主要和主動-次要。如果只有一個防火牆設定為分割資料平面，則分割資料平面也適用於另一個裝置。
7. 編輯 **Data Link (HA2 Backup)**（資料連結（**HA2** 備份））區段，選取介面，然後新增 **IPv4/IPv6 Address**（**IPv4/IPv6** 位址）及 **Netmask**（網路遮罩）。
8. 按一下 **OK**（確定）。

STEP 13 | 設定 HA3 連結進行封包轉送。

1. 在 **Device**（裝置） > **High Availability**（高可用性） > **Active/Active Config**（主動/主動組態）中，編輯 Packet Forwarding（封包轉送）。
2. 對於 **HA3 Interface**（**HA3** 介面），選取想要用於在主動/主動 HA 對等體之間轉送封包的介面。必須為能夠實現 Layer 2 傳輸的專用介面，並設定為 **Interface Type HA**（介面類型 **HA**）。
3. 選取 **VR Sync**（**VR** 同步）以強制 HA 對等體上設定的所有虛擬路由器進行同步。沒有為動態路由通訊協定設定虛擬路由器時選取此選項。必須透過交換式網路將兩個對等體都連線至相同的下一個躍點路由器，且只能使用靜態路由。
4. 選取 **QoS Sync**（**QoS** 同步）可同步所有實體介面上的 QoS 設定檔選取。當兩個對等體的連結速度相似，且需要所有實體介面上的 QoS 設定檔都相同時選取此選項。此設定會影響 **Network**（網路）頁籤上 QoS 設定的同步。無論此設定為何，都會同步 QoS 原則。

©2024 Palo Alto Networks, Inc.

STEP 14 | （選用）修改暫訂保留時間。

1. 在 **Device**（裝置） > **High Availability**（高可用性） > **Active/Active Config**（主動/主動組態）中，編輯 Packet Forwarding（封包轉送）。
2. 對於 **Tentative Hold Time (sec)**（暫訂保留時間）（秒），輸入防火牆在失敗復原後保持暫訂狀態的秒數（範圍是 10-600，預設為 60）。

STEP 15 | 設定工作階段擁有者和工作階段設定。

1. 在 **Device**（裝置） > **High Availability**（高可用性） > **Active/Active Config**（主動/主動組態）中，編輯 Packet Forwarding（封包轉送）。
2. 對於 **Session Owner Selection**（工作階段擁有者選取項），選取下列其中一項：
   - 第一個封包—接收新工作階段第一個封包的防火牆是工作階段擁有者（建議設定）。此設定可最大限度地減少 HA3 中的流量與對等體間的負載共用流量。
   - 主要裝置—處於主動-主要狀態的防火牆為工作階段擁有者。
3. 對於 工作階段設定，選取下列其中一項：
   - **IP Modulo**（**IP** 模數）—防火牆會對封包的來源和目的地 IP 位址執行 XOR 操作，並根據結果選擇將設定工作階段的 HA 對等體。
   - 主要裝置—主動-主要防火牆設定所有工作階段。
   - **First Packet**（第一個封包）—接收新工作階段第一個封包的防火牆執行工作階段設定（建議設定）。

     從工作階段擁有者和工作階段設定的第一個封包開始，然後根據負載散佈情況，您可以變更為其他選項之一。
   - **IP** 雜湊—防火牆使用來源 IP 位址或來源和目的地 IP 位址的組合來散佈工作階段設定責任。
4. 按一下 **OK**（確定）。

STEP 16 | 設定 HA 虛擬位址。

您需要一個虛擬位址來使用浮動 IP 位址和虛擬 MAC 位址或 ARP 負載共用。

1. 在 **Device**（裝置） > **High Availability**（高可用性） > **Active/Active Config**（主動/主動組態） 中，**Add**（新增）一個虛擬位址。
2. 輸入或選取 **Interface**（介面）。
3. 選取 **IPv4** 或 **IPv6** 頁籤，然後按一下 **Add**（新增）。
4. 輸入 **IPv4 Address**（**IPv4** 位址）或 **IPv6 Address**（**IPv6** 位址）。
5. 對於 **Type**（類型）：
   - 選取 **Floating**（浮動）來將虛擬 IP 位址設定為浮動 IP 位址。
   - 選取 **ARP Load Sharing**（**ARP** 負載共用）來將虛擬 IP 位址設定為共用 IP 位址並繼續設定 ARP 負載共用。

©2024 Palo Alto Networks, Inc.

STEP 17 | 設定浮動 IP 位址。

1. 請勿選取 **Floating IP bound to the Active-Primary device**（繫結至主動主要裝置的浮動 **IP**），除非您想要將 HA 配對與主動/被動 HA 配對的運作類似。
2. 對於 **Device 0 Priority**（裝置 **0** 優先順序）與 **Device 1 Priority**（裝置 **1** 優先順序），分別為被設定為「裝置 ID 0」和「裝置 ID 1」的防火牆輸入優先順序。相對優先順序確定哪個對等體擁有您剛才設定的浮動 IP 位址（範圍是 0-255）。具有最低優先值（最高優先順序）的防火牆擁有浮動 IP 位址。
3. 選取 **Failover address if link state is down**（如果連結狀態為中斷則容錯移轉位址），當介面上的連結狀態中斷時，使防火牆使用容錯轉移位址。
4. 按一下 **OK**（確定）。

STEP 18 | 設定 ARP 負載共用。

裝置選取演算法取得哪個 HA 防火牆回應 HA 請求以提供負載共用。

1. 對於 **Device Selection Algorithm**（裝置選取演算法），選取下列其中一項：
   - **IP** 模數—根據 ARP 要求者 IP 位址的同位性來選取將回應 ARP 要求的防火牆。
   - **IP** 雜湊—根據 ARP 要求者 IP 位址的雜湊來選取將回應 ARP 要求的防火牆。
2. 按一下 **OK**（確定）。

STEP 19 | 定義 HA 容錯移轉條件。

STEP 20 | **Commit**（提交）組態。

確定主動/主動使用案例

確定您擁有哪類使用案例，然後選擇相應的步驟來設定主動/主動 HA。

如果您使用 基於路由的備援、浮動 IP 位址和虛擬 MAC 位址或 ARP 負載共用，則選取相應的步驟：

- 使用案例：設定主動/主動 HA（具有基於路由的備援）
- 使用案例：使用浮動 IP 位址設定主動/主動 HA
- 使用案例：設定主動/主動 HA（具有 ARP 負載共用）

如果您想要 Layer 3 主動/主動 HA 部署與主動/被動部署的運作方式類似，請選取下列步驟：

- 使用案例：使用繫結至主動/主要防火牆的浮動 IP 位址設定主動/主動 HA

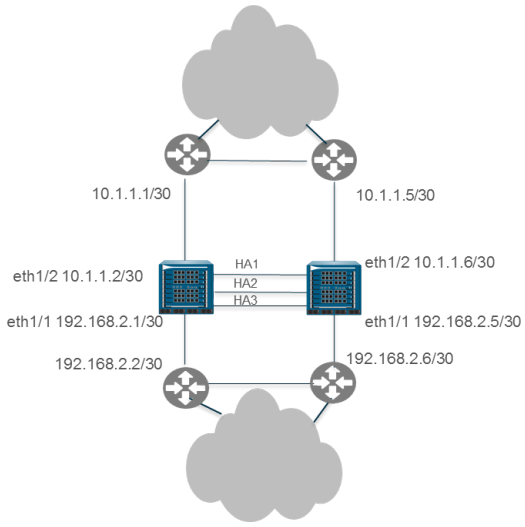
如果您要設定 主動/主動 HA 模式中的 NAT，請參閱下列步驟：

- 使用案例：使用浮動 IP 位址設定主動/主動 HA（具有來源 DIPP NAT）
- 使用案例：為主動/主動 HA 防火牆設定單獨的來源 NAT IP 位址
- 使用案例：透過目的地 NAT 設定 ARP 負載共用的主動/主動 HA
- 使用案例：透過 Layer 3 中的目的地 NAT 設定 ARP 負載共用的主動/主動 HA

©2024 Palo Alto Networks, Inc.

使用案例：設定主動/主動 HA（具有基於路由的備援）

下列 Layer 3 拓撲顯示了主動/主動 HA 環境中的兩個 PA-7050 防火牆使用基於路由的備援。防火牆屬於 OSPF 區域。當連結或防火牆失敗時，OSPF 透過將流量重新導向至功能性防火牆來處理備援。



STEP 1 | 設定主動/主動 HA。

執行步驟 1 到步驟 15。

STEP 2 | 設定 OSPF。

請參閱 OSPF。

STEP 3 | 定義 HA 容錯移轉條件。

定義 HA 容錯移轉條件。

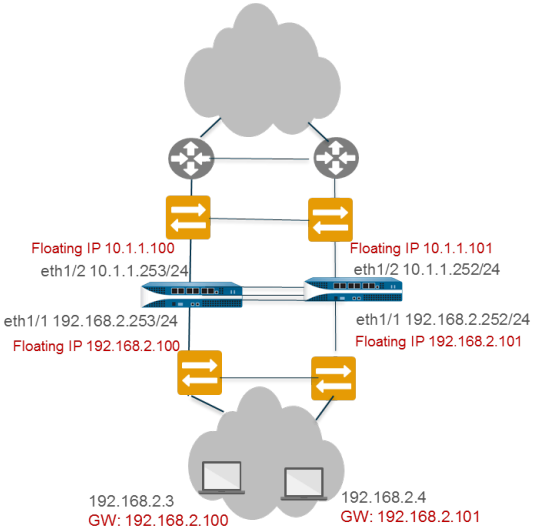
STEP 4 | **Commit**（提交）組態。

STEP 5 | 以相同方式設定對等防火牆，只是在步驟 5 中，如果您為第一個防火牆選取裝置 ID **0**，則為對等防火牆選取裝置 ID **1**。

使用案例：使用浮動 IP 位址設定主動/主動 HA

在此 Layer 3 介面範例中，HA 防火牆將連線至交換器並使用浮動 IP 位址來處理連結或防火牆失敗。每個終端主機均設定了閘道，即 HA 防火牆的其中一個浮動 IP 位址。請參閱浮動 IP 位址和虛擬 MAC 位址。

©2024 Palo Alto Networks, Inc.



STEP 1 | 設定主動/主動 HA。

執行步驟 1 到步驟 15。

STEP 2 | 設定 HA 虛擬位址。

您需要一個虛擬位址來使用浮動 IP 位址和虛擬 MAC 位址。

1. 在 **Device**（裝置） > **High Availability**（高可用性） > **Active/Active Config**（主動/主動組態） 中，**Add**（新增）一個虛擬位址。
2. 輸入或選取 **Interface**（介面）。
3. 選取 **IPv4** 或 **IPv6** 頁籤，然後按一下 **Add**（新增）。
4. 輸入 **IPv4 Address**（**IPv4** 位址）或 **IPv6 Address**（**IPv6** 位址）。
5. 對於 **Type**（類型），選取 **Floating**（浮動）來將虛擬 IP 位址設定為浮動 IP 位址。

STEP 3 | 設定浮動 IP 位址。

1. 請勿選取 **Floating IP bound to the Active-Primary device**（繫結至主動-主要裝置的浮動 **IP**）。
2. 對於 **Device 0 Priority**（裝置 **0** 優先順序）與 **Device 1 Priority**（裝置 **1** 優先順序），分別為被設定為「裝置 ID 0」和「裝置 ID 1」的防火牆輸入優先順序。相對優先順序確定哪個對等體擁有您剛才設定的浮動 IP 位址（範圍是 0 至 255）。具有最低優先值（最高優先順序）的防火牆擁有浮動 IP 位址。
3. 選取 **Failover address if link state is down**（如果連結狀態為中斷則容錯移轉位址），當介面上的連結狀態中斷時，使防火牆使用容錯轉移位址。
4. 按一下 **OK**（確定）。

STEP 4 | 在 PA-7000 系列之外的防火牆上啟用 Jumbo Frame。

執行設定主動/主動 HA 的步驟 19。

 ©2024 Palo Alto Networks, Inc.

STEP 5 | 定義 HA 容錯移轉條件

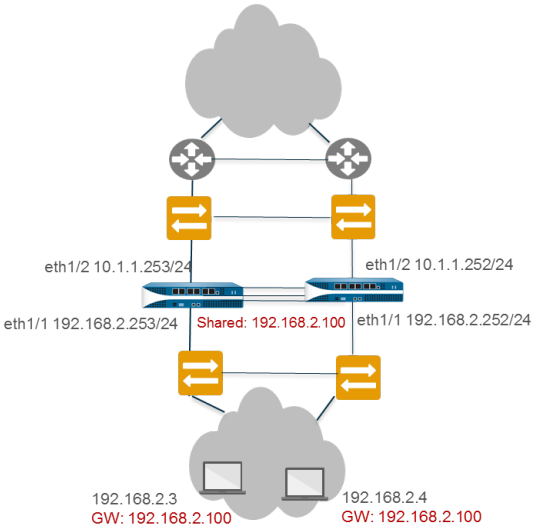
STEP 6 | **Commit**（提交）組態。

STEP 7 | 以相同的方式設定對等防火牆，只是選取另一個裝置 ID。

例如，如果您為第一個防火牆選取裝置 ID **0**，則為對等防火牆選取裝置 ID **1**。

使用案例：設定主動/主動 HA（具有 ARP 負載共用）

在此範例中，Layer 3 部署中的主機需要 HA 防火牆的閘道服務。防火牆設定單一共用 IP 位址，允許 ARP 負載共用。每個終端主機均設定了相同的閘道，即 HA 防火牆的共用 IP 位址。



STEP 1 | 執行設定主動/主動 HA 的步驟 1 到步驟 15。

STEP 2 | 設定 HA 虛擬位址。

虛擬位址是允許 ARP 負載共用的共用 IP 位址。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） > **Active/Active Config**（主動/主動組態） > **Virtual Address**（虛擬位址），然後按一下 **Add**（新增）。
2. 輸入或選取 **Interface**（介面）。
3. 選取 **IPv4** 或 **IPv6** 頁籤，然後按一下 **Add**（新增）。
4. 輸入 **IPv4 Address**（**IPv4** 位址）或 **IPv6 Address**（**IPv6** 位址）。
5. 對於 **Type**（類型），選取 **ARP Load Sharing**（**ARP** 負載共用），允許兩個對等體使用虛擬 IP 位址進行 ARP 負載共用。

©2024 Palo Alto Networks, Inc.

STEP 3 | 設定 ARP 負載共用。

裝置選取演算法取得哪個 HA 防火牆回應 HA 請求以提供負載共用。

1. 對於 **Device Selection Algorithm**（裝置選取演算法），選取下列其中一項：
   - **IP** 模數—根據 ARP 要求者 IP 位址的同位性來選取將回應 ARP 要求的防火牆。
   - **IP** 雜湊—根據 ARP 要求者 IP 位址的雜湊來選取將回應 ARP 要求的防火牆。
2. 按一下 **OK**（確定）。

STEP 4 | 在 PA-7000 系列之外的防火牆上啟用 Jumbo Frame。

STEP 5 | 定義 HA 容錯移轉條件

STEP 6 | **Commit**（提交）組態。

STEP 7 | 以相同的方式設定對等防火牆，只是選取另一個裝置 ID。

例如，如果您為第一個防火牆選取裝置 ID **0**，則為對等防火牆選取裝置 ID **1**。

使用案例：使用繫結至主動/主要防火牆的浮動 IP 位址設定主動/主動 HA

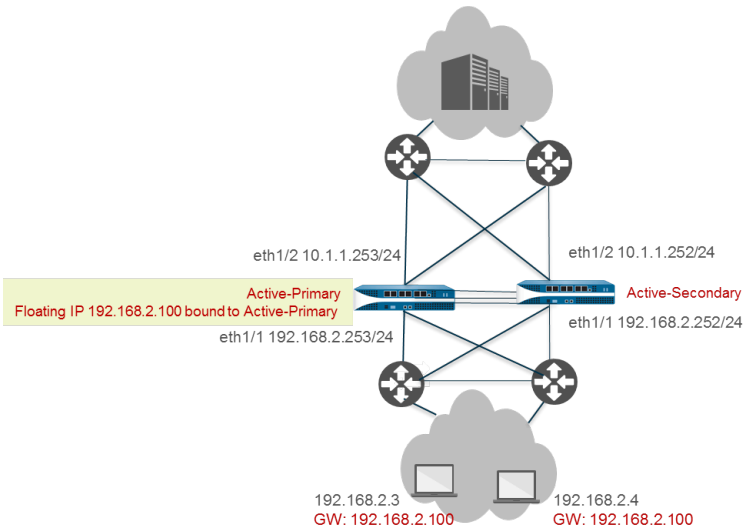
在任務關鍵型資料中心，您可能需要兩個 Layer 3 HA 防火牆來參與路徑監控，以便其可偵測兩個防火牆的上游路徑失敗。此外，您更願意控制 IP 位址是否在其恢復後返回至還原的防火牆，以及返回時間，而非返回其繫結的裝置 ID。（浮動 IP 位址和虛擬 MAC 位址中介紹了該預設行為。）

在此使用案例中，您將控制浮動 IP 位址返回，從而使主動-主要角色移回還原的 HA 對等的時間。主動/主動 HA 防火牆將共用繫結至處於主動-主要狀態的防火牆的單一浮動 IP 位址。由於只有一個浮動 IP 位址，網路流量主要流至單一防火牆，因此該主動/主動部署與主動/被動部署的運作方式類似。

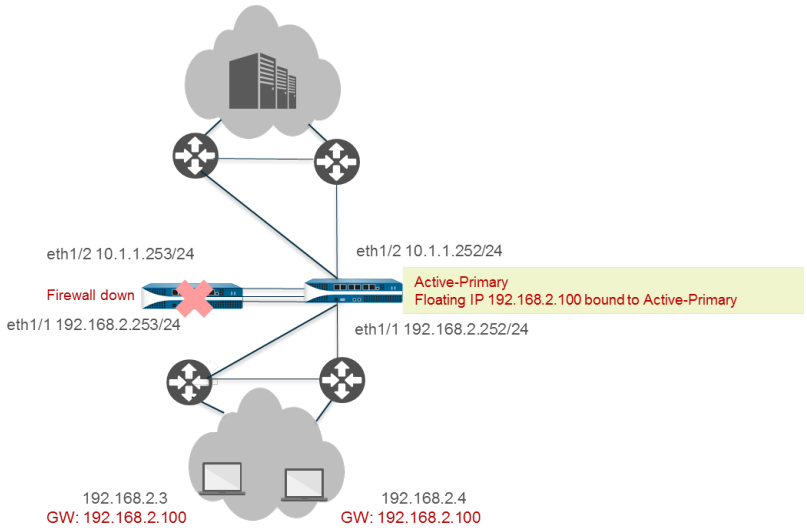
在此使用案例中，Cisco Nexus 7010 交換器具有在 Layer 3 中運作的虛擬 PortChannels (vPC)，連線至防火牆。您必須設定防火牆南北方向的 Layer 3 交換器（路由器對等），優先路由至浮動 IP 位址。即，您必須在設計網路時使路由器對等的路由表具有通向浮動 IP 位址的最佳路徑。此範例使用具有正確公制的靜態路由，以便到浮動 IP 位址的路由使用較低的公制（偏好使用到浮動 IP 位址的路由）並接收流量。使用靜態路由的替換方案是，在設計網路時，將浮動 IP 位址重新散佈至 OSPF 路由通訊協定（如果您使用 OSPF）。

下列拓撲顯示繫結至主動-主要防火牆的浮動 IP 位址，最初為對等 A，防火牆在左側。

©2024 Palo Alto Networks, Inc.



在容錯移轉時，若主動-主要防火牆（對等 A）中斷，且主動-次要防火牆（對等 B）接管主動-主要對等，浮動 IP 位址將移至對等 B（如下圖所示）。對等 B 保持在主動-主要防火牆上，且流量繼續移至對等 B，即使對等 A 復原並變成主動-次要防火牆。您將決定是否再次將對等 A 變成主動-主要防火牆以及時間。



將浮動 IP 位址繫結至主動-主要防火牆，讓您更好地控制防火牆在浮動 IP 位址於不同 HA 防火牆狀態之間變動時透過何種方式確定其擁有權。具有下列優點：

- 您可以設定主動/主動 HA 組態用於兩個防火牆之外的路徑監控，但使防火牆的運作方式與主動/被動 HA 組態類似，因為導向至浮動 IP 位址的流量始終移至主動-主要防火牆。

在兩個防火牆上停用先佔後，具有下列額外優點：

- 如果主動-次要防火牆上下擺動，浮動 IP 位址不會在 HA 防火牆之間來回移動。
- 您可以先檢閱復原防火牆及相鄰元件的功能性，再手動重新導向流量，您可以在方便的中斷時間執行。

©2024 Palo Alto Networks, Inc.

- 您可以掌控哪個防火牆擁有浮動 IP 位址，以便在主動-主要防火牆上保留所有新工作階段及現有工作階段的流量，從而最大限度地減少 HA3 連結上的流量。

- 我們強烈建議您在支援浮動 *IP* 位址的介面上設定 *HA* 連結監控，讓各 *HA* 對等快速偵測連結失敗並容錯轉移至其對等。兩個 *HA* 對等必須具有連結監控功能才能運作。
- 我們強烈建議您設定 *HA* 路徑監控，在路徑失敗時通知各 *HA* 對等，以使防火牆可容錯轉移至其對等。由於浮動 *IP* 位址始終繫結至主動-主要防火牆，當路徑中斷且未啟用路徑監控時，防火牆無法自動容錯轉移至對等。

您無法為浮動 *IP* 位址設定繫結至主動-主要防火牆的 *NAT*。

STEP 1 | 執行設定主動/主動 HA 的步驟 1 到步驟 5。

STEP 2 | （選用）停用先佔。

停用先佔可讓您在復原的防火牆變成主動-主要防火牆時實現完全掌控。

1. 在 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般） 中，編輯 Election Settings（選取設定）。
2. 如果已啟用，則清除 **Preemptive**（先佔）。
3. 按一下 **OK**（確定）。

STEP 3 | 執行設定主動/主動 HA 的步驟 7 到步驟 14。

STEP 4 | 設定工作階段擁有者和工作階段設定。

1. 在 **Device**（裝置） > **High Availability**（高可用性） > **Active/Active Config**（主動/主動組態）中，編輯 Packet Forwarding（封包轉送）。
2. 對於 **Session Owner Selection**（工作階段擁有者選取項），我們建議您選取 **Primary Device**（主要裝置）。處於主動-主要狀態的防火牆為工作階段擁有者。

   或者，對於 **Session Owner Selection**（工作階段擁有者選取項），您可以選取 **First Packet**（第一個封包），對於 **Session Setup**（工作階段設定），則選取 **Primary Device**（主要裝置）或 **First Packet**（第一個封包）。
3. 對於 **Session Setup**（工作階段設定），選取 **Primary Device**（主要裝置）—主動-主要防火牆設定所有工作階段。如果您想要主動/主動組態的運作方式與主動/被動設定類似，則這是建議的設定，因為它將所有活動保持在主動-主要防火牆上。

   此外，您還必須將網路設計為消除移至 *HA* 配對的非對稱流量的可能性。如果您未進行此操作且流量移至主動-次要防火牆，則將 ***Session Owner Selection***（工作階段擁有者選取項）和 ***Session Setup***（工作階段設定）設定為 ***Primary Device***（主要裝置），可使流量周遊 *HA3* 以到達主動-主要防火牆，取得工作階段擁有權及工作階段設定。
4. 按一下 **OK**（確定）。

©2024 Palo Alto Networks, Inc.

STEP 5 | 設定 HA 虛擬位址。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） > **Active/Active Config**（主動/主動組態） > **Virtual Address**（虛擬位址），然後按一下 **Add**（新增）。
2. 輸入或選取 **Interface**（介面）。
3. 選取 **IPv4** 或 **IPv6** 頁籤，然後 **Add**（新增） **IPv4 Address**（**IPv4** 位址）或 **IPv6 Address**（**IPv6** 位址）。
4. 對於 **Type**（類型），選取 **Floating**（浮動）來將虛擬 IP 位址設定為浮動 IP 位址。
5. 按一下 **OK**（確定）。

STEP 6 | 將浮動 IP 位址繫結至主動-主要防火牆。

1. 選取 **Floating IP bound to the Active-Primary device**（繫結至主動主要裝置的浮動 **IP**）。
2. 選取 **Failover address if link state is down**（如果連結狀態為中斷則容錯移轉位址），當介面上的連結狀態中斷時，使防火牆使用容錯轉移位址。
3. 按一下 **OK**（確定）。

STEP 7 | 在 PA-7000 系列之外的防火牆上啟用 Jumbo Frame。

STEP 8 | **Commit**（提交）組態。

STEP 9 | 以相同的方式設定對等防火牆，只是選取另一個裝置 ID。

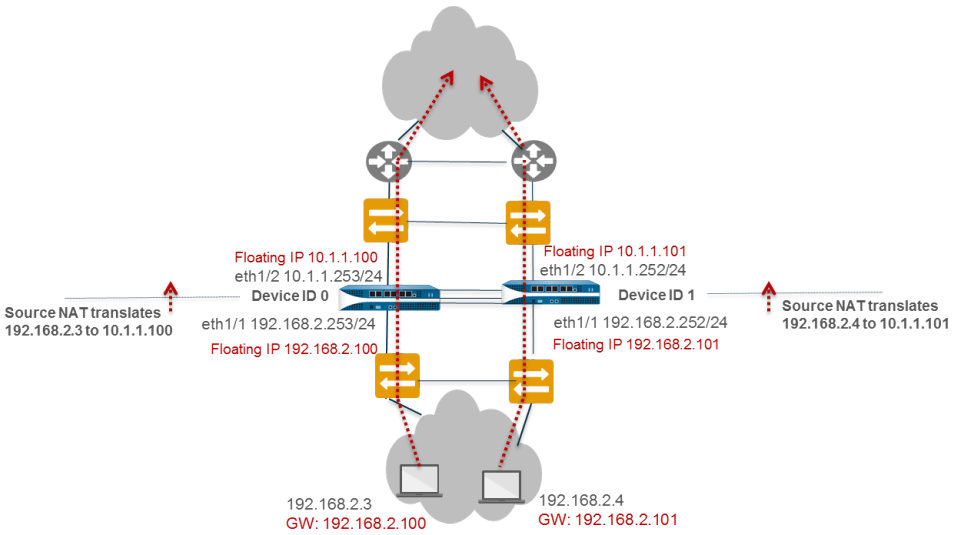
例如，如果您為第一個防火牆選取裝置 ID **0**，則為對等防火牆選取裝置 ID **1**。

使用案例：使用浮動 IP 位址設定主動/主動 HA（具有來源 DIPP NAT）

此 Layer 3 介面範例使用了主動/主動 HA 模式下的 NAT。Layer 2 交換器建立廣播網域以確保使用者可到達防火牆的南北方向的一切位置。

PA-3050-1 具有裝置 ID 0 及其 HA 對等體，PA-3050-2 具有裝置 ID 1。在此使用案例中，NAT 將來源 IP 位址及連接埠編號轉譯為在輸出介面上設定的浮動 IP 位址。每個主機均設定預設閘道位址，這是各防火牆乙太網路 1/1 上的浮動 IP 位址。組態需要兩個來源 NAT 規則，一個繫結至各裝置 ID，但您可在單一防火牆上設定兩個 NAT 規則，且它們將同步至對等防火牆。

©2024 Palo Alto Networks, Inc.



STEP 1 | 在 PA-3050-2（裝置 ID 1）上，執行設定主動/主動 HA 的步驟 1 到步驟 3。

STEP 2 | 啟用主動/主動 HA。

1. 在 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般）中，編輯 Setup（設定）。
2. 選取 **Enable HA**（啟用 **HA**）。
3. 輸入 **Group ID**（群組 **ID**），在兩個防火牆上必須採用相同設定。防火牆使用群組 ID 來計算虛擬 MAC 位址（範圍是 1-63）。
4. 對於 **Mode**（模式），選取 **Active Active**（主動/主動）。
5. 將 **Device ID**（裝置 **ID**）設定為 **1**。
6. 選取 **Enable Config Sync**（啟用設定同步）。此設定需要同步兩個防火牆組態（預設會啟用）。
7. 輸入 **Peer HA1 IP Address**（對等 **HA1 IP** 位址），這是對等防火牆上 HA1 控制連結的 IP 位址。
8. （選用）輸入 **Backup Peer HA1 IP Address**（備份對等 **HA1 IP** 位址），這是對等防火牆上備份控制連結的 IP 位址。
9. 按一下 **OK**（確定）。

STEP 3 | 設定主動/主動 HA。

完成步驟 6 到步驟 14。

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 設定工作階段擁有者和工作階段設定。

1. 在 **Device**（裝置） > **High Availability**（高可用性） > **Active/Active Config**（主動/主動組態）中，編輯 Packet Forwarding（封包轉送）。
2. 對於 **Session Owner Selection**（工作階段擁有者選取項），選取 **First Packet**（第一個封包）—接收新工作階段第一個封包的防火牆是工作階段擁有者。
3. 對於 **Session Setup**（工作階段設定），選取 **IP Modulo**（**IP** 模數）—根據來源 IP 位址的同位性散佈工作階段設定負載。
4. 按一下 **OK**（確定）。

STEP 5 | 設定 HA 虛擬位址。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） > **Active/Active Config**（主動/主動組態） > **Virtual Address**（虛擬位址），然後按一下 **Add**（新增）。
2. 選取 **Interface**（介面） eth1/1。
3. 選取 **IPv4**，然後 **Add**（新增）一個 10.1.1.101 的 **IPv4 Address**（**IPv4** 位址）。
4. 對於 **Type**（類型），選取 **Floating**（浮動）來將虛擬 IP 位址設定為浮動 IP 位址。

STEP 6 | 設定浮動 IP 位址。

1. 請勿選取 **Floating IP bound to the Active-Primary device**（繫結至主動-主要裝置的浮動 **IP**）。
2. 選取 **Failover address if link state is down**（如果連結狀態為中斷則容錯移轉位址），當介面上的連結狀態中斷時，使防火牆使用容錯轉移位址。
3. 按一下 **OK**（確定）。

STEP 7 | 在 PA-7000 系列之外的防火牆上啟用 Jumbo Frame。

STEP 8 | 定義 HA 容錯移轉條件。

STEP 9 | **Commit**（提交）組態。

STEP 10 | 設定對等防火牆 PA-3050-1，採用相同設定，只是要做出下列變更：

- 選取 **Device ID 0**（裝置 **ID 0**）。
- 設定 HA 虛擬位址 10.1.1.100。
- 對於 **Device 1 Priority**（裝置 **1** 優先順序），輸入 255。對於 **Device 0 Priority**（裝置 **0** 優先順序），輸入0。

在此範例中，裝置 ID 0 具有較低的優先值，因此具有較高優先順序；因此，具有裝置 ID 0 (PA-3050-1) 的防火牆擁有浮動 IP 位址 10.1.1.100。

©2024 Palo Alto Networks, Inc.

STEP 11 | 仍然在 PA-3050-1 上，為裝置 ID 0 建立來源 NAT 規則。

1. 選取 **Policies**（原則） > **NAT**，然後按一下 **Add**（新增）。
2. 在此範例中，為規則輸入 **Name**（名稱），將其識別為裝置 ID 0 的來源 NAT。
3. 對於 **NAT Type**（**NAT** 類型），選取 **ipv4**（預設）。
4. 在 **Original Packet**（原始封包）上，對於 **Source Zone**（來源區域），選取 **Any**（任何）。
5. 對於 **Destination Zone**（目的地區域），選取您為外部網路建立的區域。
6. 允許 **Destination Interface**（目的地介面）、**Service**（服務）、**Source Address**（來源位址）及 **Destination Address**（目的地位址）保持設定為 **Any**（任何）。
7. 對於 **Translated Packet**（轉譯的封包），對 **Translation Type**（轉譯類型）選取 **Dynamic IP And Port**（動態 **IP** 和連接埠）。
8. 對於 **Address Type**（位址類型），選取 **Interface Address**（介面位址），在此情況下，轉譯的位址將為介面的 IP 位址。選取 **Interface**（介面）（在此範例中為 eth1/1）和 **IP Address**（**IP** 位址）（浮動 IP 位址為 10.1.1.100）。
9. 在 **Active/Active HA Binding**（主動/主動 **HA** 繫結）頁籤上，對於 **Active/Active HA Binding**（主動/主動 **HA** 繫結），選取 **0** 以將 NAT 規則繫結至裝置 ID 0。
10. 按一下 **OK**（確定）。

STEP 12 | 為裝置 ID 1 建立來源 NAT 規則。

1. 選取 **Policies**（原則） > **NAT**，然後按一下 **Add**（新增）。
2. 在此範例中，為規則輸入 **Name**（名稱），可將其識別為裝置 ID 1 的來源 NAT。
3. 對於 **NAT Type**（**NAT** 類型），選取 **ipv4**（預設）。
4. 在 **Original Packet**（原始封包）上，對於 **Source Zone**（來源區域），選取 **Any**（任何）。對於 **Destination Zone**（目的地區域），選取您為外部網路建立的區域。
5. 允許 **Destination Interface**（目的地介面）、**Service**（服務）、**Source Address**（來源位址）及 **Destination Address**（目的地位址）保持設定為 **Any**（任何）。
6. 對於 **Translated Packet**（轉譯的封包），對 **Translation Type**（轉譯類型）選取 **Dynamic IP And Port**（動態 **IP** 和連接埠）。
7. 對於 **Address Type**（位址類型），選取 **Interface Address**（介面位址），在此情況下，轉譯的位址將為介面的 IP 位址。選取 **Interface**（介面）（在此範例中為 eth1/1）和 **IP Address**（**IP** 位址）（浮動 IP 位址為 10.1.1.101）。
8. 在 **Active/Active HA Binding**（主動/主動 **HA** 繫結）頁籤上，對於 **Active/Active HA Binding**（主動/主動 **HA** 繫結），選取 **1** 以將 NAT 規則繫結至裝置 ID 1。
9. 按一下 **OK**（確定）。

STEP 13 | **Commit**（提交）組態。

©2024 Palo Alto Networks, Inc.

使用案例：為主動/主動 HA 防火牆設定單獨的來源 NAT IP 位址

如果您想要對來源主動/主動 HA 模式中的 NAT使用 IP 位址集區，每個防火牆必須有其自身的集區，隨後繫結至 NAT 規則中的裝置 ID。

位址物件與 NAT 規則保持同步（主動/被動模式與主動/主動模式），因此只需在 HA 配對中設定其中一個防火牆。

此範例設定包含 IP 位址集區 10.1.1.140-10.1.1.150 的位址物件（名稱為 Dyn-IP-Pool-dev0）。此外還設定包含 IP 位址集區 10.1.1.160-10.1.1.170 的位址物件（名稱為 Dyn-IP-Pool-dev1）。第一個位址物件繫結至裝置 ID 0；第二個位址物件繫結至裝置 ID 1。

STEP 1 | 在一個 HA 防火牆上，建立位址物件。

1. 選取 **Objects**（物件）> **Addresses**（位址），然後 **Add**（新增）位址物件 **Name**（名稱），在此範例中為 Dyn-IP-Pool-dev0。
2. 對於 **Type**（類型），選取 **IP Range**（**IP** 範圍），並輸入 10.1.1.140-10.1.1.150 之間的範圍。
3. 按一下 **OK**（確定）。
4. 重複此步驟設定名稱為 Dyn-IP-Pool-dev1 的位址物件，其 **IP Range**（**IP** 範圍）為 10.1.1.160-10.1.1.170。

STEP 2 | 為裝置 ID 0 建立來源 NAT 規則。

1. 選取 **Policies**（原則）> **NAT**，然後 **Add**（新增）具有 **Name**（名稱）的 NAT 原則規則，例如 Src-NAT-dev0。
2. 在 **Original Packet**（原始封包）上，對於 **Source Zone**（來源區域），選取 **Any**（任何）。
3. 對於 **Destination Zone**（目的地區域），選取您想要轉譯來源位址（例如不信任位址）的目的地區域。
4. 在 **Translated Packet**（轉譯封包）上，對於 **Translation Type**（轉譯類型），選取 **Dynamic IP and Port**（動態 **IP** 和連接埠）。
5. 對於 **Translated Address**（轉譯位址），**Add**（新增）您為位址集區（屬於裝置 ID 0）建立的位址物件：Dyn-IP-Pool-dev0。
6. 對於 **Active/Active HA Binding**（主動/主動 **HA** 繫結），選取 **0** 可將 NAT 規則繫結至裝置 ID 0。
7. 按一下 **OK**（確定）。

©2024 Palo Alto Networks, Inc.

STEP 3 | 為裝置 ID 1 建立來源 NAT 規則。

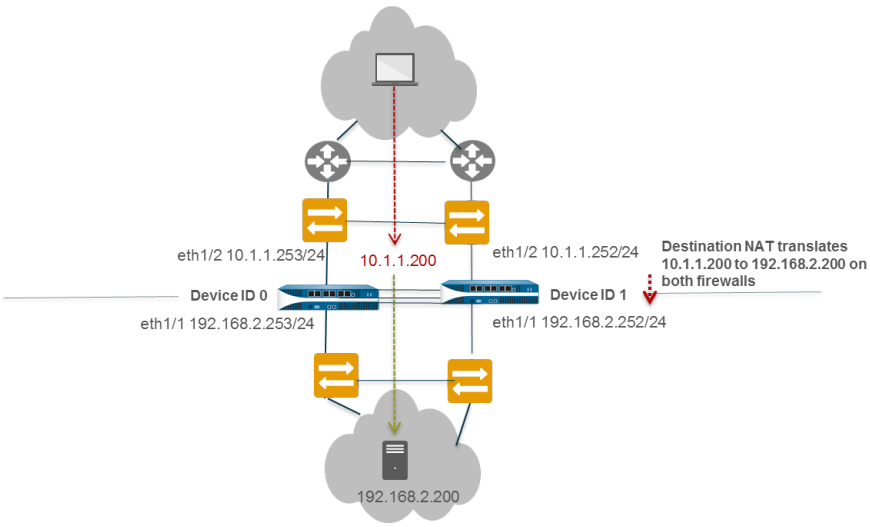
1. 選取 **Policies**（原則）> **NAT**，然後 **Add**（新增）具有 **Name**（名稱）的 NAT 原則規則，例如 Src-NAT-dev1。
2. 在 **Original Packet**（原始封包）上，對於 **Source Zone**（來源區域），選取 **Any**（任何）。
3. 對於 **Destination Zone**（目的地區域），選取您想要轉譯來源位址（例如不信任位址）的目的地區域。
4. 在 **Translated Packet**（轉譯封包）上，對於 **Translation Type**（轉譯類型），選取 **Dynamic IP and Port**（動態 **IP** 和連接埠）。
5. 對於 **Translated Address**（轉譯位址），**Add**（新增）您為位址集區（屬於裝置 ID 1）建立的位址物件。Dyn-IP-Pool-dev1。
6. 對於 **Active/Active HA Binding**（主動/主動 **HA** 繫結），選取 **1** 可將 NAT 規則繫結至裝置 ID 1。
7. 按一下 **OK**（確定）。

STEP 4 | **Commit**（提交）組態。

使用案例：透過目的地 NAT 設定 ARP 負載共用的主動/主動 HA

此 Layer 3 介面範例使用了主動/主動 HA 模式下的 NAT以及與 NAT 進行 ARP 負載共用。兩個 HA 防火牆使用輸入介面 MAC 位址回應 ARP 對目的地 NAT 位址的請求。目的地 NAT 將公共、共用 IP 位址（在本範例中為 10.1.1.200）轉譯為伺服器的私人 IP 位址（在此範例中為 192.168.2.200）。

當 HA 防火牆收到目的地 10.1.1.200 的流量時，兩個防火牆均可回應 ARP 請求，這可能會導致網路不穩定。為了避免潛在問題，透過將目的地 NAT 規則繫結至主動-主要防火牆，將處於主動-主要狀態的防火牆設定為回應 ARP 請求。



STEP 1 | 在 PA-3050-2（裝置 ID 1）上，執行設定主動/主動 HA 的步驟 1 到步驟 3。

©2024 Palo Alto Networks, Inc.

STEP 2 | 啟用主動/主動 HA。

1. 在 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般）中，編輯 Setup（設定）。
2. 選取 **Enable HA**（啟用 **HA**）。
3. 輸入 **Group ID**（群組 **ID**），在兩個防火牆上必須採用相同設定。防火牆使用群組 ID 來計算虛擬 MAC 位址（範圍是 1 至 63）。
4. （選用）輸入 **Description**（說明）。
5. 對於 **Mode**（模式），選取 **Active Active**（主動/主動）。
6. 將 **Device ID**（裝置 **ID**）選為 **1**。
7. 選取 **Enable Config Sync**（啟用設定同步）。此設定需要同步兩個防火牆組態（預設會啟用）。
8. 輸入 **Peer HA1 IP Address**（對等 **HA1 IP** 位址），這是對等防火牆上 HA1 控制連結的 IP 位址。
9. （選用）輸入 **Backup Peer HA1 IP Address**（備份對等 **HA1 IP** 位址），這是對等防火牆上備份控制連結的 IP 位址。
10. 按一下 **OK**（確定）。

STEP 3 | 執行設定主動/主動 HA 的步驟 6 到步驟 15。

STEP 4 | 設定 HA 虛擬位址。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） > **Active/Active Config**（主動/主動組態） > **Virtual Address**（虛擬位址），然後按一下 **Add**（新增）。
2. 選取 **Interface**（介面） eth1/1。
3. 選取 **IPv4**，然後 **Add**（新增）一個 10.1.1.200 的 **IPv4 Address**（**IPv4** 位址）。
4. 對於 **Type**（類型），選取 **ARP Load Sharing**（**ARP** 負載共用），這會將虛擬 IP 位址設定用於兩個對等以進行 ARP 負載共用。

STEP 5 | 設定 ARP 負載共用。

裝置選取演算法取得哪個 HA 防火牆回應 HA 請求以提供負載共用。

1. 對於 **Device Selection Algorithm**（裝置選取演算法），選取 **IP Modulo**（**IP** 模數）。根據 ARP 要求者 IP 位址的同位性來選取將回應 ARP 要求的防火牆。
2. 按一下 **OK**（確定）。

STEP 6 | 在 PA-7000 系列之外的防火牆上啟用 Jumbo Frame。

STEP 7 | 定義 HA 容錯移轉條件。

STEP 8 | **Commit**（提交）組態。

©2024 Palo Alto Networks, Inc.

STEP 9 | 設定對等防火牆，PA-3050-1（裝置 ID 0），採用相同設定，只是步驟 2 中選取 **Device ID 0**（裝置 **ID 0**）。

STEP 10 | 仍然在 PA-3050-1（裝置 ID 0）上，建立目的地 NAT 規則，以便主動-主要防火牆回應 ARP 請求。

1. 選取 **Policies**（原則）> **NAT**，然後按一下 **Add**（新增）。
2. 在此範例中，為規則輸入 **Name**（名稱），將其識別為 Layer 2 ARP 的目的地 NAT 規則。
3. 對於 **NAT Type**（**NAT** 類型），選取 **ipv4**（預設）。
4. 在 **Original Packet**（原始封包）上，對於 **Source Zone**（來源區域），選取 **Any**（任何）。
5. 對於 **Destination Zone**（目的地區域），選取您為外部網路建立的 Untrust（不安全）區域。
6. 允許 **Destination Interface**（目的地介面）、**Service**（服務）、**Source Address**（來源位址）保持設定為 **Any**（任何）。
7. 對於 **Destination Address**（目的地位址）指定 10.1.1.200。
8. 對於 **Translated Packet**（轉譯的封包），來源位址轉譯保持 **None**（無）。
9. 對於 **Destination Address Translation**（目的地位址轉譯），輸入目的地伺服器地私人 IP 位址，在此範例中為 192.168.1.200。
10. 在 **Active/Active HA Binding**（主動/主動 **HA** 繫結）頁籤上，對於 **Active/Active HA Binding**（主動/主動 **HA** 繫結），選取 **primary**（主要），以將 NAT 規則繫結至主動-主要狀態中的防火牆。
11. 按一下 **OK**（確定）。

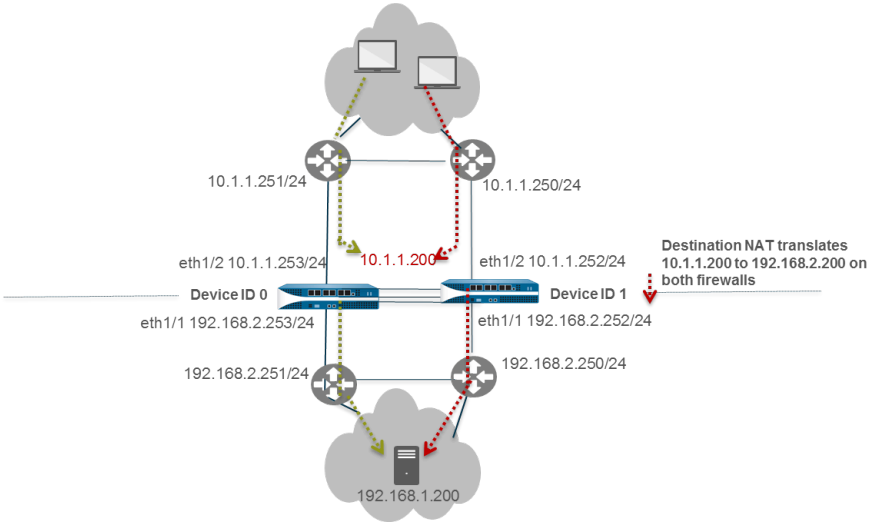
STEP 11 | **Commit**（提交）組態。

使用案例：透過 Layer 3 中的目的地 NAT 設定 ARP 負載共用的主動/主動 HA

此 Layer 3 介面範例使用了主動/主動 HA 模式下的 NAT以及 ARP 負載共用。PA-3050-1 具有裝置 ID 0 及其 HA 對等體，PA-3050-2 具有裝置 ID 1。

在此使用案例中，兩個 HA 防火牆必須回應對目的地 NAT 位址的 ARP 請求。流量可到達不信任區域任何 WAN 路由器的任何防火牆。目的地 NAT 將公開、共用 IP 位址轉譯為伺服器的私人 IP 位址。組態需要將一個目的地 NAT 規則繫結至兩個裝置 ID，以便兩個防火牆皆可回應 APR 請求。

©2024 Palo Alto Networks, Inc.



STEP 1 | 在 PA-3050-2（裝置 ID 1）上，執行設定主動/主動 HA 的步驟 1 到步驟 3。

STEP 2 | 啟用主動/主動 HA。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般） > **Setup**（設定）並編輯。
2. 選取 **Enable HA**（啟用 **HA**）。
3. 輸入 **Group ID**（群組 **ID**），在兩個防火牆上必須採用相同設定。防火牆使用群組 ID 來計算虛擬 MAC 位址（範圍是 1-63）。
4. （選用）輸入 **Description**（說明）。
5. 對於 **Mode**（模式），選取 **Active Active**（主動/主動）。
6. 將 **Device ID**（裝置 **ID**）選為 **1**。
7. 選取 **Enable Config Sync**（啟用設定同步）。此設定需要同步兩個防火牆組態（預設會啟用）。
8. 輸入 **Peer HA1 IP Address**（對等 **HA1 IP** 位址），這是對等防火牆上 HA1 控制連結的 IP 位址。
9. （選用）輸入 **Backup Peer HA1 IP Address**（備份對等 **HA1 IP** 位址），這是對等防火牆上備份控制連結的 IP 位址。
10. 按一下 **OK**（確定）。

STEP 3 | 設定主動/主動 HA。

執行步驟 6 到步驟 15。

©2024 Palo Alto Networks, Inc.

STEP 4 | 設定 HA 虛擬位址。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） > **Active/Active Config**（主動/主動組態） > **Virtual Address**（虛擬位址），然後按一下 **Add**（新增）。
2. 選取 **Interface**（介面） eth1/2。
3. 選取 **IPv4**，然後 **Add**（新增）一個 10.1.1.200 的 **IPv4 Address**（**IPv4** 位址）。
4. 對於 **Type**（類型），選取 **ARP Load Sharing**（**ARP** 負載共用），這會將虛擬 IP 位址設定用於兩個對等以進行 ARP 負載共用。

STEP 5 | 設定 ARP 負載共用。

裝置選取演算法取得哪個 HA 防火牆回應 HA 請求以提供負載共用。

1. 對於 **Device Selection Algorithm**（裝置選取演算法），選取下列其中一項：
   - **IP** 模數—根據 ARP 要求者 IP 位址的同位性來選取將回應 ARP 要求的防火牆。
   - **IP** 雜湊—根據 ARP 要求者的來源 IP 位址和目的地 IP 位址的雜湊來選取將回應 ARP 要求的防火牆。
2. 按一下 **OK**（確定）。

STEP 6 | 在 PA-7000 系列之外的防火牆上啟用 Jumbo Frame。

STEP 7 | 定義 HA 容錯移轉條件。

STEP 8 | **Commit**（提交）組態。

STEP 9 | 設定對等防火牆，PA-3050-1（裝置 ID 0），採用相同設定，指示將 **Device ID**（裝置 **ID**）設定為 **0** 而非 **1**。

©2024 Palo Alto Networks, Inc.

STEP 10 | 仍然在 PA-3050-1（裝置 ID 0）上，建立用於裝置 ID 0 和設定 ID 1 的目的地 NAT 規則。

1. 選取 **Policies**（原則）> **NAT**，然後按一下 **Add**（新增）。
2. 在此範例中，為規則輸入 **Name**（名稱），將其識別為 Layer 3 ARP 的目的地 NAT 規則。
3. 對於 **NAT Type**（**NAT** 類型），選取 **ipv4**（預設）。
4. 在 **Original Packet**（原始封包）上，對於 **Source Zone**（來源區域），選取 **Any**（任何）。
5. 對於 **Destination Zone**（目的地區域），選取您為外部網路建立的 Untrust（不安全）區域。
6. 允許 **Destination Interface**（目的地介面）、**Service**（服務）、**Source Address**（來源位址）保持設定為 **Any**（任何）。
7. 對於 **Destination Address**（目的地位址）指定 10.1.1.200。
8. 對於 **Translated Packet**（轉譯的封包），來源位址轉譯保持 None（無）。
9. 對於 **Destination Address Translation**（目的地位址轉譯），輸入目的地伺服器地私人 IP 位址，在此範例中為 192.168.1.200。
10. 在 **Active/Active HA Binding**（主動/主動 **HA** 繫結）頁籤上，對於 **Active/Active HA Binding**（主動/主動 **HA** 繫結），選取 **both**（兩者），以將 NAT 規則繫結至裝置 ID 0 和裝置 ID 1。
11. 按一下 **OK**（確定）。

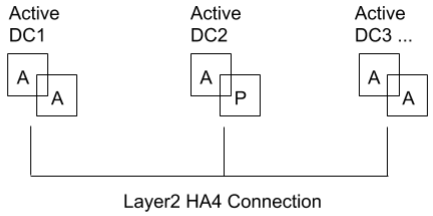
STEP 11 | **Commit**（提交）組態。

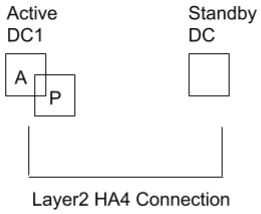
©2024 Palo Alto Networks, Inc.

HA 叢集概要介紹

現在，許多 Palo Alto Networks® 防火牆型號都支援多達 16 個防火牆的高可用性 (HA) 叢集中防火牆之間的工作階段狀態同步。HA 叢集對等同步工作階段，以防止資料中心或水平擴展的防火牆上大型安全性檢查點出現失敗。在網路中斷或防火牆出現故障的情況下，工作階段將容錯移轉到叢集中的其他防火牆。這種同步在以下使用案例中特別有用。

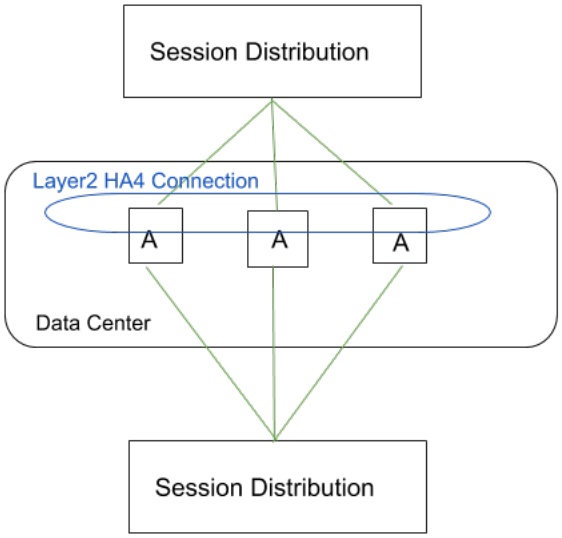
一種使用案例是，HA 對等分佈在多個資料中心中，從而在資料中心之內或之間沒有單一失敗點。第二個多資料中心使用案例是，一個資料中心處於作用中，而另一個資料中心處於待命狀態。





第三個 HA 叢集使用案例是水平擴展，可以將 HA 叢集成員新增到單個資料中心以擴展安全性並確保工作階段的生存能力。

©2024 Palo Alto Networks, Inc.



HA 叢集支援 Layer 3 或虛擬介接部署。叢集中的 HA 對等可以是 HA 配對和獨立叢集成員的組合。在 HA 叢集中，所有成員均被視為作用中；除了 HA 配對外，沒有被動防火牆的概念，HA 配對可以在新增到 HA 叢集後保持其主動/被動關係。

所有叢集成員共用工作階段狀態。當新的防火牆加入 HA 叢集時，將觸發叢集中的所有防火牆同步所有現有工作階段。HA4 和 HA4 備份連線是專用的叢集連結，用於在具有相同叢集 ID 的所有叢集成員之間同步工作階段狀態。叢集成員之間的 HA4 連結能夠偵測叢集成員之間的連線失敗情況。非 HA 配對的叢集成員之間不支援 HA1（控制連結）、HA2（資料連結）和 HA3（封包轉送連結）。

對於尚未進行容錯移轉的普通工作階段，只有作為工作階段擁有者的防火牆才會建立流量日誌。對於進行了容錯移轉的工作階段，新的工作階段擁有者（接收容錯移轉流量的防火牆）將建立流量日誌。

支援 HA 叢集的防火牆型號以及每個叢集支援的最大成員數如下：

防火牆型號	每個叢集支援的成員數
PA-3200 系列	6
PA-3400 Series	6
PA-5200 系列	16
PA-5400 系列	8

©2024 Palo Alto Networks, Inc.

防火牆型號	每個叢集支援的成員數
具有至少一張以下卡的 PA-7000 系列防火牆：PA-7000-100G-NPC、PA-7000-20GQXM-NPC、PA-7000-20GXM-NPC	PA-7080：4 PA-7050：6
VM-300	6
VM-500	6
VM-700	16

公共雲端部署中不支援 HA 叢集。在開始 設定 HA 叢集 之前考慮 HA 叢集最佳做法和佈建。

©2024 Palo Alto Networks, Inc.

HA 叢集最佳做法和佈建

以下是 HA 叢集的佈建要求和最佳做法。

- 佈建要求和最佳做法
  - HA 叢集成員必須是相同的防火牆型號並執行相同的 PAN-OS® 版本。

    升級時，防火牆成員將繼續與不同版本的某個成員同步處理工作階段。
  - 強烈建議採用最佳做法，使用 Panorama 佈建 HA 叢集成員，以使所有設定和原則在所有叢集成員之間保持同步。
  - HA 叢集成員必須獲得相同元件的授權，以確保一致的原則強制執行和內容檢查功能。
  - 授權必須同時到期，以防止授權不符和功能喪失。
  - 所有叢集成員應執行相同版本的動態內容更新，以實現一致的安全性強制執行。
  - HA 叢集成員必須共用相同的區域名稱，以便工作階段成功容錯移轉到另一個叢集成員。例如，假設前往名為 **`internal`** 的輸入區域的工作階段由於連結關閉而被丟棄。為了使這些工作階段容錯移轉到叢集中的 HA 防火牆對等，該對等也必須具有一個名為 **`internal`** 的區域。
  - 用戶端到伺服器和伺服器到用戶端的流程必須在正常（非故障）條件下回到同一防火牆，以便進行安全內容掃描。非對稱流量不會被丟棄，但出於安全目的，無法對其進行掃描。
- 工作階段同步最佳做法
  - 應在資料平面介面上使用專用的 HA 通訊介面。HSCI 介面不用於 HA4。這允許將 HA 配對與叢集工作階段同步分開，以確保工作階段同步獲得最大的頻寬和可靠性。
  - 如果使用資料平面介面，則 HA4 的大小應適當。這樣可以確保叢集成員之間盡可能好的工作階段狀態同步。
  - 最佳做法是為 HA4 通訊連結建立專用的叢集網路，以確保叢集成員之間有足夠的頻寬以及不擁塞的低延遲連線。
  - 設計您的網路並執行流量規劃，以避免可能出現的爭用情況，在這種情況下，在防火牆之間成功同步工作階段之前，網路會將流量從工作階段擁有者引導到叢集成員。Layer 2 HA4 連線必須具有足夠的頻寬和低延遲，以允許 HA 成員之間及時同步。HA4 延遲必須低於對等裝置在叢集成員之間切換流量時引起的延遲。
  - 設計網路以最大程度地減少不對稱流量。工作階段設定需要一個叢集成員來查看完整的 TCP 三向交握。
- 健康情況檢查最佳做法
  - 在叢集中的 HA 配對上，為 HA1、HA2 和 HA4 設定具有 HA 備份通訊連結的主動/被動配對。為 HA1、HA2、HA3 和 HA4 設定具有 HA 備份通訊連結的主動/主動配對。
  - 在所有叢集成員上設定 HA4 備份連結。

©2024 Palo Alto Networks, Inc.

設定 HA 叢集

HA 防火牆設定為叢集的成員之前，瞭解有關 HA 叢集的相關資訊，並遵照 HA 叢集最佳做法和佈建。

STEP 1 | 建立一個介面作為 HA 介面（之後指派為 HA4 連結）。

1. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），然後選取介面；例如，ethernet1/1。
2. 選取 **Interface Type**（介面類型）為 **HA**。
3. 按一下 **OK**（確定）。
4. 重複此步驟以設定另一介面用作 HA4 備份連結。

STEP 2 | 啟用 HA 叢集。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般），然後編輯叢集設定。
2. 啟用叢集參與。
3. 輸入 **Cluster ID**（叢集 **ID**），這是 HA 叢集的唯一數字 ID，其中所有成員都可共用工作階段狀態；範圍為 1 至 99。
4. 輸入簡短有用的 **Cluster Description**（叢集說明）。
5. （選用）變更叢集同步逾時（分鐘），這是當另一個叢集成員（例如，處於未知狀態）阻止叢集完全同步時，本機防火牆在進入作用中狀態之前等待的最大分鐘數；範圍為 0 至 30；預設值為 0。
6. （選用）變更監控失敗維持時間（分鐘），這是一個分鐘數，在該時間段之後，將對失效的連結進行重新測試以查看其是否恢復；範圍為 1 至 60；預設值為 1。
7. 按一下 **OK**（確定）。

STEP 3 | 設定 HA4 連結。

1. 選取 **HA Communications**（**HA** 通訊），並在「叢集連結」區段中，編輯 HA4 區段。
2. 選取您在第一步中設定為 **HA** 介面的介面作為 HA4 連結的 **Port**（連接埠）；例如，ethernet1/1。
3. 輸入本機 HA4 介面的 **IPv4/IPv6 Address**（**IPv4/IPv6** 位址）。
4. 輸入 **Netmask**（網路遮罩）。
5. （選用）變更 **HA4** 保持活動臨界值（毫秒），以指定一個時間範圍，防火牆必須在該時間範圍內從叢集成員接收保持活動，以瞭解該叢集成員正在運作；範圍是 5,000 至 60,000；預設值為 10,000。
6. 按一下 **OK**（確定）。

©2024 Palo Alto Networks, Inc.

STEP 4 | 設定 HA4 備份連結。

1. 編輯 HA4 備份區段。
2. 選取您在第一步中設定為 **HA** 介面的另一個介面作為 HA4 備份連結的 **Port**（連接埠）。
3. 輸入本機 HA4 備份介面的 **IPv4/IPv6 Address**（**IPv4/IPv6** 位址）。
4. 輸入 **Netmask**（網路遮罩）。
5. 按一下 **OK**（確定）。

STEP 5 | 指定 HA 叢集的所有成員，包括本機成員和任何 HA 配對中的兩個 HA 對等。

1. 選取 **Cluster Config**（叢集設定）。
2. （在受支援的防火牆上）**Add**（新增）對等成員的 **Device Serial Number**（裝置序號）。
3. （在 Panorama 上）**Add**（新增）並從下拉式清單中選取一個 **Device**（裝置），然後輸入 **Device Name**（裝置名稱）。
4. 輸入叢集中 HA 對等的 **HA4 IP Address**（**HA4 IP** 位址）。
5. 輸入叢集中 HA 對等的 **HA4 Backup IP Address**（**HA4** 備份 **IP** 位址）。
6. 啟用與您識別的對等進行 **Session Synchronization**（工作階段同步）。
7. （選用）輸入有用的 **Description**（說明），
8. 按一下 **OK**（確定）。
9. 選取裝置，並 **Enable**（啟用）它。

STEP 6 | 使用連結和路徑監控定義 HA 容錯移轉條件。

STEP 7 | **Commit**（認可）。

STEP 8 | （僅限 Panorama）重新整理 HA 叢集中 HA 防火牆的清單。

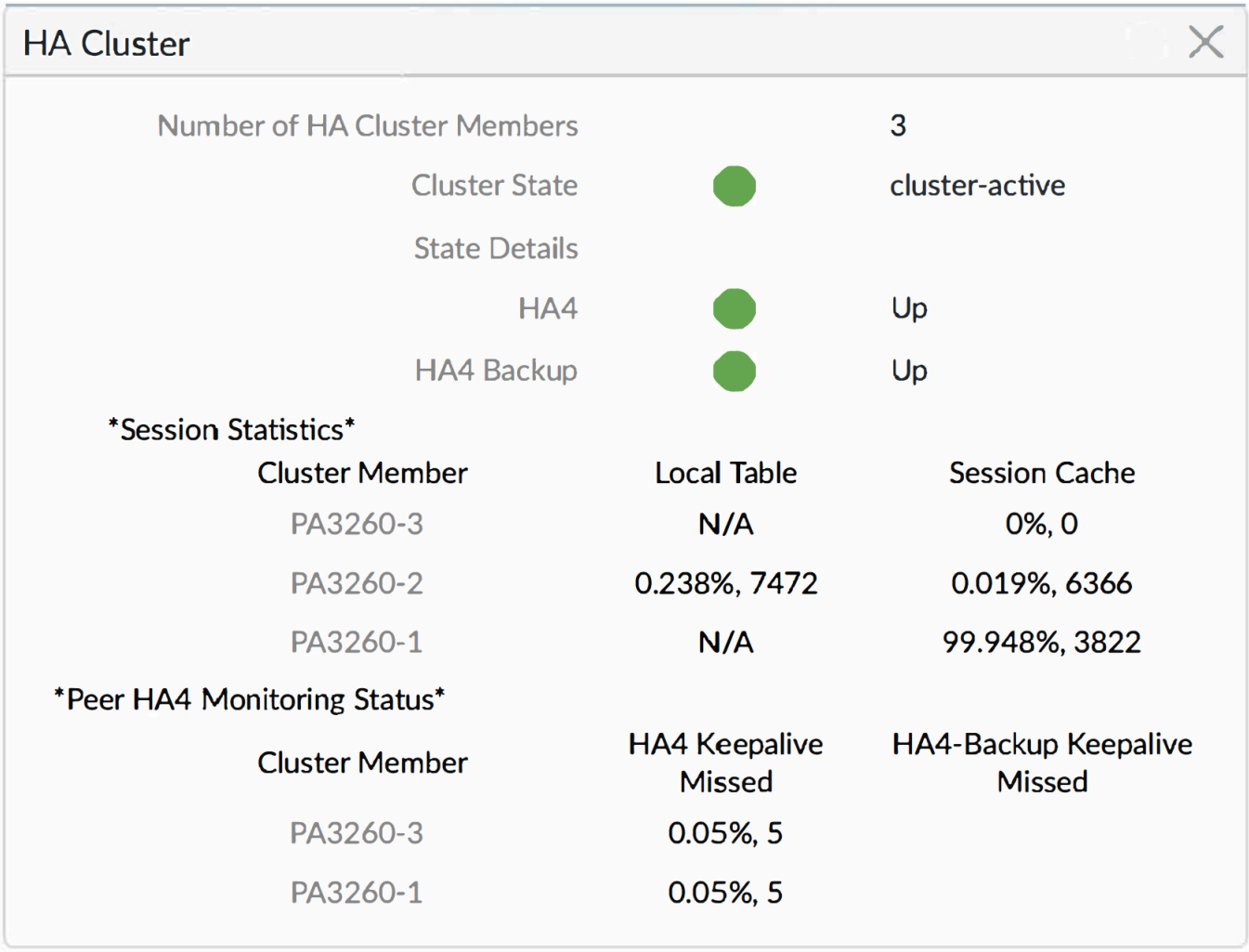
1. 在「範本」下，選取**Device**（裝置） > **High Availability**（高可用性） > **Cluster Config**（叢集設定）。
2. 按一下螢幕底部的 **Refresh**（重新整理）。

STEP 9 | 在 UI 中檢視 HA 叢集資訊。

1. 選取 **Dashboard**（儀表板）。
2. 檢視 HA 叢集欄位。頂部區段顯示叢集狀態和 HA4 連線，提供叢集健康情況概觀。HA4 和 HA4 備份指標如下：綠色表示叢集成員的連結狀態為「開啟」。紅色表示所有叢集成員的連結狀態為「關閉」。黃色表示部分叢集成員的連結狀態為「開啟」，而另一些叢集成員的狀態為「關閉」。灰色表示未設定。中央區段顯示本機工作階段表格和工作階段

©2024 Palo Alto Networks, Inc.

快取表格的容量，這樣您可以監控表格的填充程度，並計劃防火牆升級。下部區段顯示 HA4 和 HA4 備份連結上的通訊錯誤，表示在成員之間同步資訊方面可能存在的問題。



STEP 10 | 存取 CLI 以檢視 HA 叢集和 HA4 連結資訊，以及執行其他 HA 叢集工作。

您可以檢視 *HA* 叢集擺動統計資料。當 *HA* 裝置從暫停變更為正常運作以及從正常運作變更為暫停時，叢集擺動計數會重設。當非運作保持時間到期時，叢集擺動計數也會重設。

©2024 Palo Alto Networks, Inc.

重新整理 HA1 SSH 金鑰並設定金鑰選項

所有 Palo Alto Networks 防火牆都預先設定了 Secure Shell (SSH)，且高可用性 (HA) 防火牆可同時作為 SSH 伺服器和 SSH 用戶端。當您設定主動/被動或主動/主動 HA 時，可以針對 HA 防火牆之間的 HA1（控制連結）連線啟用加密。我們建議您使用加密來保護 HA 對等之間的 HA1 流量，當防火牆位於不同的網站中時尤為如此。在 HA1 控制連結上啟用加密後，您可以使用 CLI 來建立 SSH 服務設定檔並保護 HA 防火牆之間的連線。

SSH 服務設定檔可讓您變更預設主機金鑰類型，為 HA1 控制連結產生一對新的公開和私密 SSH 主機金鑰，並設定其他 SSH HA1 設定。您可以將新主機金鑰和設定的設定套用至防火牆，無需重新啟動 HA 對等。防火牆將重新建立 HA1 工作階段，以便其對等同步設定變更。它還會產生用於重新建立 HA1 和 HA1-backup 工作階段的系統日誌（子類型為 `ha`）。

以下範例顯示在啟用加密後如何為 HA1 設定各種 SSH 設定以及存取 CLI。（請參閱重新整理 SSH 金鑰和為管理介面連線設定金鑰選項，獲取 SSH 管理伺服器設定檔範例。）

您必須啟用加密，且該加密必須在 *HA* 配對上正常運行，然後才能執行以下工作。

如果在 FIPS-CC 模式下設定 *HA1* 控制連結，則必須為工作階段金鑰設定自動金鑰更新參數。

要對收集器群組中的每個專用日誌收集器（日誌收集器模式中的 *M-series* 或 *Panorama* 虛擬設備）使用同一 *SSH* 連線設定，請從 *Panorama* 管理伺服器設定 *SSH* 服務設定檔，將變更 ***Commit***（提交）到 *Panorama*，然後將設定 ***Push***（推送）到日誌收集器。您可以使用 ***set log-collector-group <name> general-setting management ssh*** 命令。

建立 SSH 服務設定以對 HA 防火牆之間的 SSH 連線進行更強的控制。

此範例會建立一個 HA 設定檔，而無需進行任何設定。

1. admin@PA-3250> **configure**
2. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles *<name>***
3. admin@PA-3250# **commit**
4. admin@PA-3250# **exit**
5. 要確認新設定檔已建立並檢視任何現有設定檔的設定：

   admin@PA-3250> **configure**

   admin@PA-3250# **show deviceconfig system ssh profiles**

©2024 Palo Alto Networks, Inc.

（選用）設定 SSH 伺服器以對 HA1 工作階段僅使用指定的加密密碼。

依預設，HA1 SSH 允許所有受支援的密碼來加密 CLI HA 工作階段。當您設定一個或多個密碼時，SSH 伺服器在連線時只會宣告這些密碼，如果 SSH 用戶端（HA 對等體）嘗試使用其他密碼連線，伺服器將終止連線。

1. admin@PA-3250> **configure**
2. admin@PA-3250# **set deviceconfig system ssh profiles ciphers ha-profiles <*name*> ciphers <*cipher*>**

   aes128-cbc—AES 128 位元密碼，帶加密區塊鏈結

   aes128-ctr—AES 128 位元密碼，帶計數器模式

   aes128-gcm—AES 128 位元密碼，帶 GCM（伽羅瓦/計數器模式）

   aes192-cbc—AES 192 位元密碼，帶加密區塊鏈結

   aes192-ctr—AES 192 位元密碼，帶計數器模式

   aes256-cbc—AES 256 位元密碼，帶加密區塊鏈結

   aes256-ctr—AES 256 位元密碼，帶計數器模式

   aes256-gcm—AES 256 位元密碼，帶 GCM
3. admin@PA-3250# **commit**
4. admin@PA-3250# **exit**
5. （已設定 HA1 備份）admin@PA-3250> **request high-availability session-reestablish**
6. （未設定 HA1 備份或 HA1 備份連結中斷）admin@PA-3250> **request high-availability session-reestablish force**

   如果沒有 *HA1* 備份，可以強制防火牆重新建立 *HA1* 工作階段，而此會在 *HA* 對等體之間引發短暫的「腦分裂」狀況。（當設定的 *HA1* 備份沒有效果時，使用 ***force*** 選項。）
7. 要驗證密碼已更新：

   admin@PA-3250> **configure**

   admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles ciphers**

（選用）設定預設主機金鑰類型。

如果您在 HA1 控制連結上啟用了加密，除非變更主機金鑰類型，否則防火牆將使用預設值：RSA 2048。HA1 SSH 連線僅使用預設的主機金鑰類型來驗證 HA 對等體（在 HA 對等體之間建立加密工作階段之前）。您可變更預設主機金鑰類型；可供選擇的主機金鑰類型有 ECDSA 256、384 或 521，或 RSA 2048、3072 或 4096。如果要使用較長的 RSA 金鑰或要使用 ECDSA（而不是 RSA），則須變更預設主機金鑰類型。此範例將預設主機金鑰類型設為

 ©2024 Palo Alto Networks, Inc.

ECDSA 金鑰（256 位元）。還使用新的主機金鑰重新建立 HA1 連線，無需重新啟動 HA 對等體。

1. admin@PA-3250> **configure**
2. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles *<name>* default-hostkey key-type ECDSA key-length 256**
3. admin@PA-3250# **commit**
4. admin@PA-3250# **exit**
5. admin@PA-3250> **request high-availability sync-to-remote ssh-key**

   必須已在 *HA* 防火牆之間建立 *HA* 連線。如果防火牆尚未建立 *HA* 連線，則必須在控制連結連線上啟用加密，將 *HA* 金鑰匯出至網路位置，並在對等體上匯入 *HA* 金鑰。請參閱設定主動/被動 HA 或設定主動/主動 HA。
6. （已設定 HA1 備份）admin@PA-3250> **request high-availability session-reestablish**
7. （未設定 HA1 備份或 HA1 備份連結中斷）admin@PA-3250> **request high-availability session-reestablish force**

   如果沒有 *HA1* 備份，可以強制防火牆重新建立 *HA1* 工作階段，而此會在兩個 *HA* 對等體之間引發短暫的「腦分裂」狀況。（當設定的 *HA1* 備份沒有效果時，使用 ***force*** 選項。）
8. 要確認主機金鑰已更新：

   admin@PA-3250> **configure**

   admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles *<name>* default-hostkey**

©2024 Palo Alto Networks, Inc.

（選用）從為 HA1 控制連結上的 SSH 選取的密碼集中刪除密碼。

在本範例中，刪除了帶 128 位元金鑰的 AES CBC 密碼。

1. admin@PA-3250> **configure**
2. admin@PA-3250# **delete deviceconfig system ssh profiles ha-profiles <*name*> ciphers aes128-cbc**
3. admin@PA-3250# **commit**
4. admin@PA-3250# **exit**
5. （已設定 HA1 備份）admin@PA-3250> **request high-availability session-reestablish**
6. （未設定 HA1 備份或 HA1 備份連結中斷）admin@PA-3250> **request high-availability session-reestablish force**

   如果沒有 *HA1* 備份，可以強制防火牆重新建立 *HA1* 工作階段，而此會在兩個 *HA* 對等體之間引發短暫的「腦分裂」狀況。（當設定的 *HA1* 備份沒有效果時，使用 ***force*** 選項。
7. 要確認密碼已刪除：

   admin@PA-3250> **configure**

   admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles <*name*> ciphers**

©2024 Palo Alto Networks, Inc.

（選用）設定 HA1 SSH 伺服器將支援的工作階段金鑰交換演算法。

依預設，SSH 伺服器（HA 防火牆）向 SSH 用戶端（HA 對等防火牆）宣告所有金鑰交換演算法。

如果使用的是 *ECDSA* 預設金鑰類型，最佳做法是使用 *ECDH* 金鑰演算法。

1. admin@PA-3250> **configure**
2. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles <*name*> kex <*value*>**

   diffie-hellman-group14-sha1—Diffie-Hellman 群組 14，帶 SHA1 雜湊

   ecdh-sha2-nistp256—美國國家標準技術研究所 (NIST) P-256 橢圓曲線 Diffie-Hellman，帶 SHA2-256 雜湊

   ecdh-sha2-nistp384—NIST P-384 橢圓曲線 Diffie-Hellman，帶 SHA2-384 雜湊

   ecdh-sha2-nistp521—NIST P-521 橢圓曲線 Diffie-Hellman，帶 SHA2-521 雜湊
3. admin@PA-3250# **commit**
4. admin@PA-3250# **exit**
5. （已設定 HA1 備份）admin@PA-3250> **request high-availability session-reestablish**
6. （未設定 HA1 備份或 HA1 備份連結中斷）admin@PA-3250> **request high-availability session-reestablish force**

   如果沒有 *HA1* 備份，可以強制防火牆重新建立 *HA1* 工作階段，而此會在兩個 *HA* 對等體之間引發短暫的「腦分裂」狀況。（當設定的 *HA1* 備份沒有效果時，使用 ***force*** 選項。
7. 要確認金鑰交換演算法已更新：

   admin@PA-3250> **configure**

   admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles**

©2024 Palo Alto Networks, Inc.

（選用）設定 HA1 SSH 伺服器將支援的訊息驗證碼 (MAC)。

依預設，伺服器向用戶端宣告所有 MAC 演算法。

1. admin@PA-3250> **configure**
2. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles *<name>* mac *<value>***

   hmac-sha1—MAC，帶 SHA1 加密雜湊

   hmac-sha2-256—MAC，帶 SHA2-256 加密雜湊

   hmac-sha2-512—MAC，帶 SHA2-512 加密雜湊
3. admin@PA-3250# **commit**
4. admin@PA-3250# **exit**
5. （已設定 HA1 備份）admin@PA-3250> **request high-availability session-reestablish**
6. （未設定 HA1 備份或 HA1 備份連結中斷）admin@PA-3250> **request high-availability session-reestablish force**

   如果沒有 *HA1* 備份，可以強制防火牆重新建立 *HA1* 工作階段，而此會在兩個 *HA* 對等體之間引發短暫的「腦分裂」狀況。（當設定了 *HA1* 備份時，使用 ***force*** 選項無效。
7. 要確認 MAC 演算法已更新：

   admin@PA-3250> **configure**

   admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles**

©2024 Palo Alto Networks, Inc.

（選用）為 HA1 SSH 重新產生 ECDSA 或 RSA 主機金鑰，以取代現有金鑰，並使用新金鑰在 HA 對等體之間重新建立 HA1 工作階段，無需重新啟動 HA 對等體。

HA 對等體使用主機金鑰進行相互驗證。此範例重新產生了 ECDSA 256 預設主機金鑰。

重新產生主機金鑰不會變更預設主機金鑰類型。若要重新產生正在使用的預設主機金鑰，則必須在重新產生時指定預設主機金鑰類型和長度。如果重新產生的主機金鑰不是預設主機金鑰類型，則重新產生的不是正在使用的金鑰，因此無效。

1. admin@PA-3250> **configure**
2. admin@PA-3250# **set deviceconfig system ssh regenerate-hostkeys ha key-type ECDSA key-length 256**
3. admin@PA-3250# **commit**
4. admin@PA-3250# **exit**
5. admin@PA-3250> **request high-availability sync-to-remote ssh-key**

   必須已在 *HA* 防火牆之間建立 *HA* 連線。如果防火牆尚未建立 *HA* 連線，則必須在控制連結連線上啟用加密，將 *HA* 金鑰匯出至網路位置，並在對等體上匯入 *HA* 金鑰。請參閱設定主動/被動 HA 或設定主動/主動 HA。
6. （已設定 HA1 備份）admin@PA-3250> **request high-availability session-reestablish**
7. （未設定 HA1 備份或 HA1 備份連結中斷）admin@PA-3250> **request high-availability session-reestablish force**

   如果沒有 *HA1* 備份，可以強制防火牆重新建立 *HA1* 工作階段，而此會在兩個 *HA* 對等體之間引發短暫的「腦分裂」狀況。（當設定的 *HA1* 備份沒有效果時，使用 ***force*** 選項。）

（選用）設定金鑰更新參數，確定 SSH 在 HA1 控制連結上自動對工作階段金鑰進行金鑰更新的時間。

工作階段金鑰用於加密 HA 對等體之間的流量。您可以設定的參數包括資料量 (MB)、時間間隔（秒）和封包計數。在任何一個金鑰更新參數達到其設定值後，SSH 會啟動金鑰交換。

如果不確定所設定的參數是否能在您希望進行金鑰更新時達到其值，您可設定第二個或第三個參數。第一個達到其設定值的參數將提示金鑰更新，然後防火牆將重設所有金鑰更新參數。

1. admin@PA-3250> **configure**
2. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles <*name*> session-rekey data 32**

   金鑰更新在上一次金鑰更新之後傳送一定的資料數量 (MB) 後進行。預設值基於您使用的密碼，範圍是 1GB 至 4GB；範圍為 10MB 至 4,000MB。或者，您可以輸入 **set**

©2024 Palo Alto Networks, Inc.

deviceconfig system ssh profiles ha-profiles *<name>* session-rekey data default 命令，以將資料參數設為正在使用之個別密碼的預設值。

3. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles *<name>* session-rekey interval 3600**

   金鑰更新在上一次金鑰更新之後指定的時間間隔（秒）後進行。依預設，以時間為基礎的金鑰更新為停用狀態（設定為無）。範圍是 10 至 3,600。

4. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles *<name>* session-rekey packets 27**

   金鑰更新在上一次金鑰更新之後傳送所定義的封包數目 (2^n) 後進行。例如，14 設定進行金鑰更新之前最多傳送 2^{14} 個封包。預設值為 2^{28}。範圍是 12 至 27（2^{12} 至 2^{27}）。或者，您可輸入 **set deviceconfig system ssh profiles ha-profiles *<name>* session-rekey packets default**，將封包參數設定為 2^{28}。

   根據流量類型和網路速度選擇金鑰更新參數（*FIPS-CC* 要求除外，如果其適用於您）。不要將參數設得太低，以免影響 *SSH* 效能。

5. admin@PA-3250# **commit**
6. admin@PA-3250# **exit**
7. （已設定 HA1 備份）admin@PA-3250> **request high-availability session-reestablish**
8. （未設定 HA1 備份或 HA1 備份連結中斷）admin@PA-3250> **request high-availability session-reestablish force**

   如果沒有 *HA1* 備份，可以強制防火牆重新建立 *HA1* 工作階段，而此會在兩個 *HA* 對等體之間引發短暫的「腦分裂」狀況。（當設定的 *HA1* 備份沒有效果時，使用 ***force*** 選項。）

9. 要驗證變更：

   admin@PA-3250> **configure**

   admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles *<name>* session-rekey**

透過選取設定檔並重新啟動 HA1 SSH 服務以啟動設定檔。

1. admin@PA-3250> **configure**
2. admin@PA-3250# **set deviceconfig system ssh ha ha-profile *<name>***
3. admin@PA-3250# **commit**
4. admin@PA-3250# **exit**
5. admin@PA-3250> **set ssh service-restart ha**
6. 要確認正在使用正確的設定檔：

   admin@PA-3250> **configure**

   admin@PA-3250# **show deviceconfig system ssh ha**

©2024 Palo Alto Networks, Inc.

HA 防火牆狀態

HA 防火牆可為下列狀態其中一項：

HA 防火牆狀態	發生情況	說明
初始化	A/P 或 A/A	加入 HA 配對時防火牆的瞬時狀態。啟動後，防火牆保持此狀態，直至其發現對等並開始交涉。逾時後，如果 HA 交涉未開始，則防火牆變為主動。
主動	A/P	主動/被動組態中的主動防火牆狀態。
被動	A/P	主動/被動組態中的被動防火牆狀態。被動防火牆可隨時變為主動防火牆，而不會中斷網路。但被動防火牆未處理其他流量： • 如果被動連結狀態設定為自動，被動防火牆將執行路由通訊協定，監控連結及路徑狀態，並且如果分別設定了 LACP 和 LLDP 預交涉，則被動防火牆將會進行 LACP 和 LLDP 預交涉。 • 被動防火牆正在同步流量狀態、執行時物件與組態。 • 被動防火牆正在使用 hello 通訊協定監控主動防火牆的狀態。
主動主要	A/A	在主動/主動組態中，防火牆狀態為連線至 User-ID 代理程式，執行 DHCP 伺服器和 DHCP 轉送，比對 NAT 和 PBF 規則與主動-主要防火牆的裝置 ID。在此狀態下的防火牆可擁有工作階段並設定工作階段。
主動次要	A/A	在主動/主動組態中，防火牆狀態為連線至 User-ID 代理程式，執行 DHCP 伺服器，比對 NAT 和 PBF 規則與主動-主要防火牆的裝置 ID。處於主動-次要狀態的防火牆不支援 DHCP 轉送。在此狀態下的防火牆可擁有工作階段並設定工作階段。
暫訂	A/A	下列其中一項原因導致的防火牆狀態（在主動/主動組態中）： • 防火牆失敗。 • 受監控物件失敗（連結或路徑）。 • 防火牆保持暫停或非運作狀態。 處於暫訂狀態的防火牆與對等工作階段與組態保持同步。 • 在 Virtual Wire 部署中，防火牆因路徑失敗進入暫訂狀態且收到轉送封包時，將會透過 HA3 連結將封包傳送至對等進行處理。對等防火牆將處理封包，並透過 HA3 連結傳回至防火牆

©2024 Palo Alto Networks, Inc.

HA 防火牆狀態	發生情況	說明
		以便從輸出介面傳送出去。此行為保留了 Virtual Wire 部署中的轉送路徑。 • 在 Layer 3 部署中，當處於暫訂狀態中的防火牆收到封包時，它會透過對等防火牆的 HA3 連結將該封包傳送給自己或設定工作階段。視乎網路拓撲，此防火牆會將封包傳送至目的地，或將其傳回處於暫訂狀態的對等進行轉送。 失敗的路徑或連結清除後或失敗的防火牆從暫訂狀態轉換為主動-次要狀態時，將會觸發 **Tentative Hold Time**（暫訂保留時間）並出現路由聚合。防火牆會試著先建立路由相鄰項及填寫其路由表，再處理任何封包。無此計時器，復原防火牆將立即進入主動次要狀態並將無訊息丟棄封包，因為它不會有必要的路由。 當防火牆處於暫停狀態時，在連結開啟後且無法處理傳入封包時，防火牆將會在 **Tentative Hold Time**（暫訂保留時間）內進入暫訂狀態。 可以停用 **Tentative Hold Time range (sec)**（暫訂保留時間）（秒）（0 秒）或者範圍是 10-600；預設為 60。
非運作	A/P 或 A/A	因資料背板或組態不符導致的錯誤狀態，例如只設定一個防火牆進行封包轉送、VR 同步或 QoS 同步。 在主動/被動模式中，所有暫訂狀態列示的原因導致非運作狀態。
已暫停	A/P 或 A/A	裝置已停用，因此不會傳遞資料流量，儘管仍然會進行 HA 通訊，但裝置不會參與 HA 選項處理。若無使用者介入，其無法移動至 HA 運作狀態。

©2024 Palo Alto Networks, Inc.

參考：HA 同步

如果您在 HA 配對中已對兩個對等啟用設定同步處理，則您在對等之一所設定的大部分組態設定都會在提交之後自動同步至另一個對等。若要避免設定衝突，請一律在主動 (主動/被動) 或主動主要 (主動/主動) 對等上進行組態變更，並等到變更已同步至對等後再繼續進行其他組態變更。

僅提交的組態會在 *HA* 對等間保持同步。在進行 *HA* 同步時，不會同步提交佇列中的任何組態。

下列主題說明您必須在各防火牆上獨立進行哪些組態設定（這些裝置不與 HA 對等保持同步）。

- 哪些設定在主動/被動 HA 中不會同步？
- 哪些設定在主動/主動 HA 中不會同步？
- 系統執行時間資訊的同步

哪些設定在主動/被動 HA 中不會同步？

您必須在主動/被動部署中設定每個 HA 配對防火牆的下列設定。這些設定不會由一個對等同步至另一個對等。

組態項目	何者在主動/被動中不會同步？
管理介面設定	所有管理組態設定必須在每個防火牆上個別設定，包括： • **Device**（裝置） > **Setup**（設定） > **Management**（管理） > **General Settings**（一般設定） — 主機名稱、網域、登入橫幅、SSL/TLS 服務設定檔（及相關憑證）、時區、地區設定、日期、時間、緯度、經度。 • **Device**（裝置） > **Setup**（設定） > **Management**（管理） > **Management Interface Settings**（管理介面設定） — IP 類型、IP 位址、網路遮罩、預設閘道、IPv6 位址/首碼長度、預設 IPv6 閘道、速度、MTU 以及服務（HTTP、HTTP OCSP、HTTPS、Telnet、SSH、偵測、SNMP、User-ID、User-ID Syslog Listener-SSL、User-ID Syslog Listener-UDP）
多重 vsys 能力	您必須在配對中的每個防火牆上啟動虛擬系統授權，才能使虛擬系統數目超出 PA-400 系列、PA-3200 系列、PA-3400 系列、PA-5200 系列、PA-5400 系列及 PA-7000 系列防火牆預設提供的基本數目。 您也必須在每個防火牆上啟用 **Multi Virtual System Capability**（多虛擬系統能力）（**Device**（裝置） > **Setup**（設定） > **Management**（管理） > **General Settings**（一般設定））。

©2024 Palo Alto Networks, Inc.

組態項目	何者在主動/被動中不會同步？
Panorama 設定	在每個防火牆上設定下列 Panorama 設定（**Device**（裝置） > **Setup**（設定） > **Management**（管理） > **Panorama Settings**（**Panorama** 設定）。 • **Panorama** 伺服器 • **Disable Panorama Policy and Objects**（停用 **Panorama** 原則與物件）與 **Disable Device and Network Template**（停用裝置與網路範本）
SNMP	裝置 > 設定 > 操作人員 > **SNMP** 設定
服務	裝置 > 設定 > 服務
全域服務路由	裝置 > 設定 > 服務 > 服務路由設定
遙測和威脅情報設定	裝置 > 設定 > 遙測和威脅情報
資料保護	裝置 > 設定 > 內容 **ID** > 管理資料保護
Jumbo 框架	裝置 > 設定 > 工作階段 > 工作階段設定 > 啟用 **Jumbo Frame**
封包緩衝區保護	裝置 > 設定 > 工作階段 > 工作階段設定 > 封包緩衝區保護 網路 > 地區 > 啟用封包緩衝區保護
正向 Proxy 伺服器憑證設定	裝置 > 設定 > 工作階段 > 解密設定 > **SSL** 正向 **Proxy** 設定
HSM 保護的主要金鑰	裝置 > 設定 > **HSM** > 硬體安全性模組提供者 > **HSM** 保護的主要金鑰
日誌匯出設定	裝置 > 已排程的日誌匯出
軟體更新	透過軟體更新，您可以在每個防火牆上個別下載並安裝更新，或是在一個對等體中下載並同步更新至其他對等體。您必須在每個對等體上安裝更新（**Device**（裝置） > **Software**（軟體））。
GlobalProtect 代理程式套件	透過 GlobalProtect 應用程式更新，您可以在每個防火牆上個別下載並安裝更新，或是在一個對等體中下載並同步更新至其他對等體。您必須在每個對等體上單獨啟用（**Device**（裝置） > **GlobalProtect Client**（**GlobalProtect** 用戶端））。

©2024 Palo Alto Networks, Inc.

組態項目	何者在主動/被動中不會同步？
內容更新	透過內容更新，您可以在每個防火牆上個別下載並安裝更新，或是在一個對等體中下載並同步更新至其他對等體。您必須在每個對等體上安裝更新（**Device**（裝置） > **Dynamic Updates**（動態更新））。
授權/訂閱	裝置 > 授權
支援訂閱	裝置 > 支援
主要金鑰	在 HA 配對中每個防火牆上的主要金鑰必須相同，但您必須在每個防火牆上手動輸入（**Device**（裝置） > **Master Key and Diagnostics**（主要金鑰與診斷））。 您必須在兩個對等體上停用組態同步（**Device**（裝置） > **High Availability**（高可用性） > **General**（一般） > **Setup**（設定））並清除 **Enable Config Sync**（啟用組態同步）核取方塊）才能變更主要金鑰，然後在變更金鑰後將其重新啟用。
報告、日誌與儀表板設定	日誌資料、報告以及儀表板資料和設定（欄顯示、Widget）不會在對等體中同步。但是報告組態設定卻會同步。
HA 設定	裝置 > **High availability**（高可用性）
解密	容錯移轉之後，防火牆不支援解密 SSL 工作階段的 HA 同步。
規則使用資料	規則使用資料（如命中數、建立和修改日期）不會在對等體之間同步。您需要登入至每個防火牆以檢視其原則規則命中數資料，或使用 Panorama 檢視 HA 防火牆對等機上的資訊。
僅限透過 SSL 進行裝置管理和 Syslog 通訊的憑證	裝置 > 憑證管理 > 憑證 用於透過 SSL 的裝置管理和 Syslog 通訊的憑證不會與 HA 對等同步。 儘管用於管理介面的憑證不同步（並且可以不同），但對於主動和被動裝置，憑證項目的名稱應該相同。
憑證設定檔中的憑證	裝置 > 憑證管理 > 憑證設定檔
僅用於裝置管理的 SSL/TLS Service Profile（SSL/TLS 服務設定檔）	裝置 > 憑證管理 > **SSL/TLS** 服務設定檔 用於裝置管理的 SSL/TLS 服務設定檔不會與 HA 對等同步。

©2024 Palo Alto Networks, Inc.

組態項目	何者在主動/被動中不會同步？
Device-ID 和 IoT Security	IP 位址到裝置的對應和原則規則建議不會與 HA 對等同步。

哪些設定在主動/主動 HA 中不會同步？

您必須在主動/主動部署中設定每個 HA 配對防火牆的下列設定。這些設定不會由一個對等同步至另一個對等。

組態項目	何者在主動/主動中不會同步？
管理介面設定	您必須在每個防火牆上單獨進行所有管理設定，包括： • **Device**（裝置）> **Setup**（設定）> **Management**（管理）> **General Settings**（一般設定）— 主機名稱、網域、登入橫幅、SSL/TLS 服務設定檔（及相關憑證）、時區、地區設定、日期、時間、緯度、經度。 • **Device**（裝置）> **Setup**（設定）> **Management**（管理）> **Management Interface Settings**（管理介面設定）— IP 位址、網路遮罩、預設閘道、IPv6 位址/首碼長度、預設 IPv6 閘道、速度、MTU 以及服務（HTTP、HTTP OCSP、HTTPS、Telnet、SSH、偵測、SNMP、User-ID、User-ID Syslog Listener-SSL、User-ID Syslog Listener-UDP）
多重 vsys 能力	您必須在配對中的每個防火牆上啟動虛擬系統授權，才能使虛擬系統數目超出 PA-400 系列、PA-3200 系列、PA-3400 系列、PA-5200 系列、PA-5400 系列及 PA-7000 系列防火牆預設提供的基本數目。 您也必須在每個防火牆上啟用 **Multi Virtual System Capability**（多虛擬系統能力）（**Device**（裝置）> **Setup**（設定）> **Management**（管理）> **General Settings**（一般設定））。
Panorama 設定	在每個防火牆上設定下列 Panorama 設定（**Device**（裝置）> **Setup**（設定）> **Management**（管理）> **Panorama Settings**（**Panorama** 設定）。 • **Panorama** 伺服器 • **Disable Panorama Policy and Objects**（停用 **Panorama** 原則與物件）與 **Disable Device and Network Template**（停用裝置與網路範本）
SNMP	裝置 > 設定 > 操作人員 > **SNMP** 設定

©2024 Palo Alto Networks, Inc.

組態項目	何者在主動/主動中不會同步？
服務	裝置 > 設定 > 服務
全域服務路由	裝置 > 設定 > 服務 > 服務路由設定
遙測和威脅情報設定	裝置 > 設定 > 遙測和威脅情報
資料保護	裝置 > 設定 > 內容 **ID** > 管理資料保護
Jumbo 框架	裝置 > 設定 > 工作階段 > 工作階段設定 > 啟用 **Jumbo Frame**
封包緩衝區保護	裝置 > 設定 > 工作階段 > 工作階段設定 > 封包緩衝區保護 網路 > 地區 > 啟用封包緩衝區保護
正向 Proxy 伺服器憑證設定	裝置 > 設定 > 工作階段 > 解密設定 > **SSL** 正向 **Proxy** 設定
HSM 組態	裝置 > 設定 > **HSM**
日誌匯出設定	裝置 > 已排程的日誌匯出
軟體更新	透過軟體更新，您可以在每個防火牆上個別下載並安裝更新，或是在一個對等體中下載並同步更新至其他對等體。您必須在每個對等體上安裝更新（**Device**（裝置） > **Software**（軟體））。
GlobalProtect 代理程式套件	透過 GlobalProtect 應用程式更新，您可以在每個防火牆上個別下載並安裝更新，或是在一個對等體中下載並同步更新至其他對等體。您必須在每個對等體上單獨啟用（**Device**（裝置） > **GlobalProtect Client**（**GlobalProtect** 用戶端））。
內容更新	透過內容更新，您可以在每個防火牆上個別下載並安裝更新，或是在一個對等體中下載並同步更新至其他對等體。您必須在每個對等體上安裝更新（**Device**（裝置） > **Dynamic Updates**（動態更新））。
授權/訂閱	裝置 > 授權
支援訂閱	裝置 > 支援
乙太網路介面 IP 位址	除了 IP 位址外，所有乙太網路介面組態設定皆會同步（**Network**（網路） > **Interface**（介面） > **Ethernet**（乙太網路））。
回送介面 IP 位址	除了 IP 位址外，所有回送介面組態設定皆會同步（**Network**（網路） > **Interface**（介面） > **Loopback**（回送））。

©2024 Palo Alto Networks, Inc.

組態項目	何者在主動/主動中不會同步？
通道介面 IP 位址	除了 IP 位址外，所有通道介面組態設定皆會同步（**Network**（網路） > **Interface**（介面） > **Tunnel**（通道））。
LACP 系統優先順序	每個對等在主動/主動部署中必須有唯一的 LACP 系統 ID（**Network**（網路） > **Interface**（介面） > **Ethernet**（乙太網路） > **Add Aggregate Group**（新增彙總群組） > **System Priority**（系統優先順序））。
VLAN 介面 IP 位址	除了 IP 位址外，所有 VLAN 介面組態設定皆會同步（**Network**（網路） > **Interface**（介面） > **VLAN**）。
虛擬路由器	僅當您啟用 VR 同步處理時，虛擬路由器設定才會同步（**Device**（裝置） > **High Availability**（高可用性） > **Active/Active Config**（主動/主動組態） > **Packet Forwarding**（封包轉送））。是否要這麼做取決於您的網路設定，包括您是否有非對稱路由。
IPSec 通道	IPSec 通道設定同步取決於您是否已設定虛擬位址使用浮動 IP 位址（**Device**（裝置） > **High Availability**（高可用性） > **Active/Active Config**（主動/主動組態） > **Virtual Address**（虛擬位址））。若您已設定浮動 IP 位址，則這些設定將會自動同步。否則，您必須在每個對等上個別設定這些設定。
GlobalProtect 入口網站組態	GlobalProtect 入口網站組態同步取決於您是否已設定虛擬位址使用浮動 IP 位址（**Network**（網路） > **GlobalProtect** > **Portals**（入口網站））。若您已設定浮動 IP 位址，則 GlobalProtect 入口網站組態設定將會自動同步。否則，您必須在每個對等上個別設定入口網站組態。
GlobalProtect 閘道組態	GlobalProtect 閘道組態同步取決於您是否已設定虛擬位址使用浮動 IP 位址（**Network**（網路） > **GlobalProtect** > **Gateways**（閘道））。若您已設定浮動 IP 位址，則 GlobalProtect 閘道組態設定將會自動同步。否則，您必須在每個對等上個別設定閘道設定。
QoS	僅當您啟用 **QoS Sync**（**QoS** 同步）時，QoS 組態才會同步（**Device**（裝置） > **High Availability**（高可用性） > **Active/Active Config**（主動/主動組態） > **Packet Forwarding**（封包轉送））。例如，如果您在每個連結上有不同的頻寬或服務提供者有不同的延遲，則您可能會選擇不同步 QoS 設定。
LLDP	在主動/主動設定中，LLDP 狀態或個別防火牆資料不會同步（**Network**（網路） > **Network Profiles**（網路設定檔） > **LLDP**）。

©2024 Palo Alto Networks, Inc.

組態項目	何者在主動/主動中不會同步？
BFD	在主動/主動設定中，BFD 組態或 BFD 工作階段資料不會同步（**Network**（網路） > **Network Profiles**（網路設定檔） > **BFD Profile**（**BFD** 設定檔））。
IKE 閘道	IKE 閘道設定同步取決於您是否已設定虛擬位址使用浮動 IP 位址（**Network**（網路） > **IKE Gateways**（**IKE** 閘道））。若您已設定浮動 IP 位址，則 IKE 閘道組態設定將會自動同步。否則，您必須在每個對等上個別設定 IKE 閘道設定。
主要金鑰	在 HA 配對中每個防火牆上的主要金鑰必須相同，但您必須在每個防火牆上手動輸入（**Device**（裝置） > **Master Key and Diagnostics**（主要金鑰與診斷））。 您必須在兩個對等體上停用組態同步（**Device**（裝置） > **High Availability**（高可用性） > **General**（一般） > **Setup**（設定））並清除 **Enable Config Sync**（啟用組態同步）核取方塊）才能變更主要金鑰，然後在變更金鑰後將其重新啟用。
報告、日誌與儀表板設定	日誌資料、報告以及儀表板資料和設定（欄顯示、Widget）不會在對等體中同步。但是報告組態設定卻會同步。
HA 設定	• 裝置 > **high availability**（高可用性） • （**Device**（裝置） > **High Availability**（高可用性） > **Active/Active Configuration**（主動/主動組態） > **Virtual Addresses**（虛擬位址）是一個例外，它會執行同步。）
解密	容錯移轉之後，防火牆不支援解密 SSL 工作階段的 HA 同步。
規則使用資料	規則使用資料（如命中數、建立和修改日期）不會在對等體之間同步。您需要登入至每個防火牆以檢視其原則規則命中數資料，或使用 Panorama 檢視 HA 防火牆對等機上的資訊。
僅限透過 SSL 進行裝置管理和 Syslog 通訊的憑證	裝置 > 憑證管理 > 憑證 用於透過 SSL 的裝置管理和 Syslog 通訊的憑證不會與 HA 對等同步。
憑證設定檔中的憑證	裝置 > 憑證管理 > 憑證設定檔
僅用於裝置管理的 SSL/TLS Service Profile（SSL/TLS 服務設定檔）	裝置 > 憑證管理 > **SSL/TLS** 服務設定檔 用於裝置管理的 SSL/TLS 服務設定檔不會與 HA 對等同步。

©2024 Palo Alto Networks, Inc.

組態項目	何者在主動/主動中不會同步？
Device-ID 和 IoT Security	IP 位址到裝置的對應和原則規則建議不會與 HA 對等同步。

系統執行時間資訊的同步

下表彙總了 HA 對等體之間將會同步的系統執行階段資訊。

執行階段資訊	設定已同步？		HA 連結	詳細資訊
	A/P	**A/A**		
管理平面				
使用者至群組對應	是	是	Ha1	
虛擬系統之間的使用者對應	是	是	Ha1	
使用者至 IP 位址對應	是	是	Ha1	在主動/主動設定中，只有主動-主要對等連線至 User-ID 伺服器或代理程式，主動-次要對等不會連線。如果主動-主要對等處於「已暫停」或「離線」狀態，則主動-次要對等會連線至 User-ID 伺服器或代理程式。
DHCP 租期（伺服器）	是	是	Ha1	若 HA 對等體上的 PAN-OS 版本不相符，DHCP 租期（伺服器）組態資訊不會同步。
DNS 快取	否	否。	無	
FQDN 重新整理	否	否。	不適用	
IKE SA [安全性關聯]（階段 1）	否。	否。	不適用	
轉送資訊庫 (FIB)	是	否。	Ha1	

©2024 Palo Alto Networks, Inc.

執行階段資訊	設定已同步？		HA 連結	詳細資訊
	A/P	A/A		
多點傳送 FIB (MFIB)	是	否。	Ha1	
PAN-DB URL 快取	是	否。	Ha1	這會在資料庫備份至磁碟時（每八個小時，當 URL 資料庫版本更新時），或當防火牆重新啟動時進行同步。
內容（手動同步）	是	是	Ha1	
PPPoE、PPPoE 租期	是	是	Ha1	
DHCP 用戶端設定與租期	是	是	Ha1	若 HA 對等體上的 PAN-OS 版本不相符，DHCP 用戶端設定與租期組態資訊不會同步。
在使用者清單中記錄的 SSL VPN	是	是	Ha1	
資料背板				
工作階段表	是	是	HA2	• 主動/被動對等不會同步 ICMP 或主機工作階段資訊。 • 主動/主動對等不會同步主機工作階段、多點

©2024 Palo Alto Networks, Inc.

執行階段資訊	設定已同步？		HA 連結	詳細資訊
	A/P	A/A		
				傳送工作階段或 BFD 工作階段資訊。 主機工作階段是在一個防火牆介面上終止的工作階段，例如對一個防火牆介面或 *GP* 通道執行 *ping* 操作的 *ICMP* 工作階段。
ARP 表	是	否。	HA2	
多點傳送工作階段表格	是	否。	HA2	
芳鄰探索 (ND) 表	是	否。	HA2	
MAC 表	是	否。	HA2	
IPSec SA [安全性關聯]（階段 2）	是	是	HA2	
IPSec 序號（防重播）	是	是	HA2	
DoS 封鎖 IP 清單項目	否	否。	無	
虛擬 MAC	是	是	HA2	
SCTP 關聯	是	否。	HA2	

©2024 Palo Alto Networks, Inc.

監控

為了防止潛在問題發生，並在需要時加速事件回應，防火牆將使用可自訂的資訊報告提供流量和使用者模式情報。防火牆上的儀表板、應用程式控管中心 (ACC)、報告和日誌可讓您監控網路上的活動。您可以監控日誌及篩選資訊，以預先定義或自訂的檢視產生報告。例如，您可以使用預先定義的範本產生使用者活動報告，或分析報告與日誌以判讀網路上的異常行為，並產生流量模式的自訂報告。為了以具有視覺吸引力的方式呈現網路活動，儀錶盤和 ACC 中包含了 Widget、圖表和表格，您可以與它們進行互動以尋找關注的資訊。此外，您可以設定防火牆以透過電子郵件通知、syslog 訊息、SNMP 設陷和 NetFlow 記錄將監控資訊轉送至外部服務。

要對 *PA-410* 使用監控功能，您必須透過 *Panorama* 管理伺服器管理 *PA-410* 防火牆。

使用儀表板

Dashboard（儀錶盤）頁籤 Widget 顯示一般防火牆資訊，例如軟體版本、每個介面的操作狀態、資源使用率，以及威脅、設定與系統日誌中最多 10 個最近的項目。依預設，會顯示所有可用 Widget，但是每位管理員都可視需要移除及新增個別 Widget。按一下重新整理圖示 可更新儀表板或個別 Widget。若要變更自動重新整理間隔，請從下拉式清單中選取間隔（**1 min**（**1** 分鐘）、**2 mins**（**2** 分鐘）、**5 mins**（**5** 分鐘）或 **Manual**（手動））。若要將 Widget 新增至儀錶盤，請按一下 Widget 下拉式清單，選取類別，然後選取 Widget 名稱。若要刪除 Widget，請按一下標題列中的 。下表說明儀錶盤 Widget。

儀錶盤圖表	說明
前幾大應用程式	顯示工作階段最多的應用程式。封鎖大小指示工作階段的相對數量 (將滑鼠游標置於封鎖上可檢視數量)，而顏色指示安全性風險—從綠色 (最低) 到紅色 (最高)。按一下應用程式可檢視其應用程式設定檔。
前幾大高風險應用程式	除顯示工作階段最多的最高風險應用程式以外，其他均與最上層應用程式相似。
一般資訊	顯示防火牆名稱、型號、PAN-OS 軟體版本、應用程式、威脅、URL 篩選定義版本、目前日期與時間，以及從上次重新啟動到現在的時間長度。
介面狀態	指示每個介面的狀態為使用中 (綠色)、關閉 (紅色)，還是未知 (灰色)。
威脅日誌	威脅日誌中顯示最新 10 筆記錄的威脅 ID、應用程式，以及日期與時間。威脅 ID 是惡意軟體描述或違反 URL 篩選設定檔的 URL。
設定日誌	設定日誌中顯示最新 10 筆項目的管理員使用者名稱、用戶端 (Web 或 CLI) 及日期與時間。
資料過濾日誌	資料篩選日誌中會顯示最近 60 分鐘的說明以及日期與時間。
URL 篩選日誌	URL 篩選日誌中會顯示最近 60 分鐘的說明以及日期與時間。
系統日誌	系統日誌中顯示最新 10 筆記錄的描述以及日期與時間。 已安裝組態項目表示已成功提交組態變更。
系統資源	顯示管理 CPU 使用、Data Plane 使用，以及工作連線數量 (顯示透過防火牆建立的工作連線數)。

©2024 Palo Alto Networks, Inc.

儀錶盤圖表	說明
已登入管理員	顯示來源 IP 位址、工作連線類型 (Web 或 CLI)，以及目前登入的每個管理員的工作連線啟動時間。
應用程式監測中心風險係數	顯示過去一週處理之網路流量的平均風險係數 (1 到 5)。值越高表示風險越高。
High availability（高可用性）	如果啟用高可用性 (HA)，則會指示本機與對等防火牆的高可用性狀態—綠色（主動）、黃色（被動）或黑色（其他）。如需 HA 的詳細資訊，請參閱High availability（高可用性）。
鎖定	顯示管理員所用的組態鎖定。

©2024 Palo Alto Networks, Inc.

使用應用程式控管中心

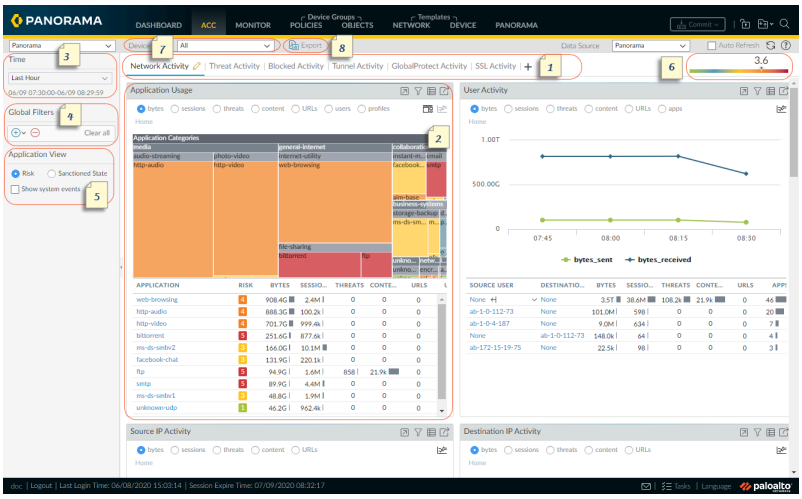
應用程式控管中心 (ACC) 是應用程式、使用者、URL、威脅和在網路中周遊之內容的互動式圖形化摘要。ACC 會使用防火牆日誌以提供流量模式可見度和可執行的威脅資訊。ACC 配置包含網路活動、威脅活動和封鎖的活動之分頁檢視，且每個頁籤都包含適當的 Widget，為網路流量提供更佳的視覺化效果。圖形化呈現可讓您與資料互動並視覺化網路事件之間的關係，以發現異常狀況或增強網路安全性規則的方法。若要個人化網路檢視，您也可以新增自訂頁籤並包含可讓您深入查看重要資訊的 Widget。

ACC 資料（包括 *ACC Widget* 和匯出的 *ACC* 報告）使用您啟用以 ***Log at Session End***（在工作階段結束時記錄）的安全性政策規則資料。如果您希望在 *ACC* 中檢視的某些資料未顯示，請檢視流量和威脅日誌以決定要按需修改的正確安全性政策規則，以便在 *ACC* 中檢視產生的與安全性政策規則相符的所有新日誌。

- ACC—初始概覽
- ACC 頁籤
- ACC Widget (Widget 說明)
- ACC 篩選器
- 與 ACC 互動
- 使用案例：ACC—資訊探索路徑

ACC—初始概覽

讓我們為您快速導覽 ACC。



 ©2024 Palo Alto Networks, Inc.

ACC—初始概覽		
	頁籤	ACC 包含三個預先定義的頁籤，可讓您洞悉網路流量、威脅活動及封鎖的活動。如需各個頁籤的相關資訊，請參閱 ACC 頁籤。
	**Widget**	每個頁籤都包含預設的 Widget 集，可代表與頁籤相關聯的活動/趨勢。Widget 可讓您使用下列篩選器調查資料： • 位元組（傳入和傳出） • 工作階段 • 內容（檔案和資料） • URL 類別 • 威脅（和計數） 如需各個 Widget 的相關資訊，請參閱 ACC Widget。
	時間	每個 Widget 中的圖表或圖形都會提供摘要和歷程檢視。您可選擇自訂範圍或使用預先定義期間，從過去 15 分鐘到過去 90 天，或過去 30 個曆日。選取的時段會套用至 ACC 中的所有頁籤。 用於呈現資料的時段預設為以 15 分鐘為間隔更新的 **Last Hour**（前 **1** 小時）。螢幕上會顯示日期和時間間隔，例如 11:40 時，時間範圍是 01/12 10:30:00-01/12 11:29:59。
	全域過濾器	全域篩選器可讓您設定所有 Widget 和所有頁籤的篩選器。在呈現資料之前，圖表/圖形會先套用選取的篩選器。如需使用篩選器的相關資訊，請參閱 ACC 篩選器。
	應用程式檢視	應用程式檢視可讓您依據在您的網路上使用的認可和不被認可的應用程式來篩選 ACC 檢視，或依據在您的網路上使用之應用程式的風險層級來篩選。綠色指示認可的應用程式，藍色只是不被認可的應用程式，黃色只是被部分認可的應用程式。被部分認可的應用程式是指具有混合認可狀態的應用程式；表示應用程式未被一致地標記為認可，例如其可能在為多個虛擬系統啟用的防火牆中的一個或多

©2024 Palo Alto Networks, Inc.

ACC—初始概覽		
		個虛擬系統上被認可，或者在 Panorama 上的某個裝置群組中的一個或多個防火牆中被認可。
6	風險係數	風險係數（最低 1 到最高 5）會根據網路上使用的應用程式，表示相對風險。風險係數使用各種係數評估相關聯的風險等級，例如應用程式是否可以共用檔案、是否容易遭到濫用或嘗試迴避防火牆，以及透過封鎖的威脅數、受危害的主機數或指向惡意軟體主機/網路的流量，評估威脅活動和惡意軟體係數。
7	來源	用於 ACC 顯示的資料。防火牆和 Panorama 上的選項會有所不同。 在防火牆上，如果已針對多個虛擬系統啟用此項目，您可以使用 **Virtual System**（虛擬系統）下拉式清單，將 ACC 顯示畫面變更為包含來自於所有虛擬系統的資料，或僅包含選取的虛擬系統。 在 Panorama 上，您可以選取 **Device Group**（裝置群組）下拉式清單，將 ACC 顯示畫面變更為包含所有裝置群組中的資料，或僅包含選取的裝置群組。 此外，在 Panorama 上，您可以將 **Data Source**（資料來源）變更為 **Panorama** 資料或 **Remote Device Data**（遠端裝置資料）。只有在所有受管理的防火牆都執行 PAN-OS 7.0.0 或更新版本時，才能使用 **Remote Device Data**（移除裝置資料）。當您篩選特定裝置群組的顯示時，系統會使用 **Panorama** 資料作為資料來源。
8	匯出	您可以將目前選取的頁籤中顯示的 Widget 匯出為 PDF。系統會下載 PDF，並將其儲存至與電腦上的網頁瀏覽器相關聯的下載資料夾。

ACC 頁籤

ACC 包含下列預先定義的頁籤，可讓您檢視網路活動、威脅活動和封鎖的活動。

©2024 Palo Alto Networks, Inc.

頁籤	說明
網路活動	顯示網路上流量和使用者活動的概要，其中包含： • 使用中的前幾名應用程式 • 產生流量的前幾名使用者（可深入查看使用者存取的位元組、內容、威脅或 URL） • 流量比對發生時最常用的安全性規則 此外，您也可依據來源或目的地區域、地區或 IP 位址、輸入或輸出介面和 GlobalProtect 主機資訊（例如，網路上最常用設備的作業系統）來檢視網路活動。
威脅活動	顯示網路上威脅的概要，其專注於主要的威脅：漏洞、間諜軟體、病毒、造訪惡意網域或 URL 的主機、依檔案類型和應用程式排序的熱門 WildFire 提交，以及使用非標準連接埠的應用程式。此頁籤中的受危害的主機 Widget（只有某些平台支援此 Widget）以更佳的視覺化技術補強偵測；其使用來自關聯事件頁籤（**Automated Correlation Engine**（自動關聯引擎） > **Correlated Events**（關聯的事件）的資訊），依來源使用者/IP 位址呈現網路上受危害主機的彙總檢視，並依嚴重性排序。
封鎖的活動	專注於禁止進入網路的流量。此頁籤中的 Widget 可讓您檢視因應用程式名稱、使用者名稱、威脅名稱、封鎖的內容而遭到拒絕的活動，也就是檔案封鎖設定檔封鎖的檔案和資料。其也會列出比對封鎖威脅、內容和 URL 的安全性規則前幾名。
通道活動	顯示防火牆根據您的通道檢查原則所檢查之通道流量的活動。其資訊包括以通道 ID、監控標籤、使用者和通道通訊協定（例如 Generic Routing Encapsulation (GRE)、整合封包無線電服務 (GPRS) 使用者資料通道通訊協定 (GTP-U)）和非加密 IPSec 為基礎的通道使用情形。
GlobalProtect 活動	顯示 GlobalProtect 部署中使用者活動的概要。資訊包括使用者人數、使用者連線次數、使用者連線的閘道、連線失敗次數及失敗原因、驗證方法摘要與使用的 GlobalProtect 應用程式版本及隔離的端點數。 此外，此頁簽顯示已隔離裝置的圖表檢視摘要。使用圖表頂部的切換鍵，按導致 GlobalProtect 隔離裝置的動作、GlobalProtect 隔離裝置的原因、已隔離裝置的位置來檢視已隔離裝置。
SSL 活動	顯示防火牆上 TLS/SSL 解密活動的概要。資訊包括您網路上的成功和失敗解密活動、解密失敗原因（如通訊協定、憑證和版本問題）、TLS 版本、金鑰交換演算法，以及已解密和未解密流量的數量與類型。

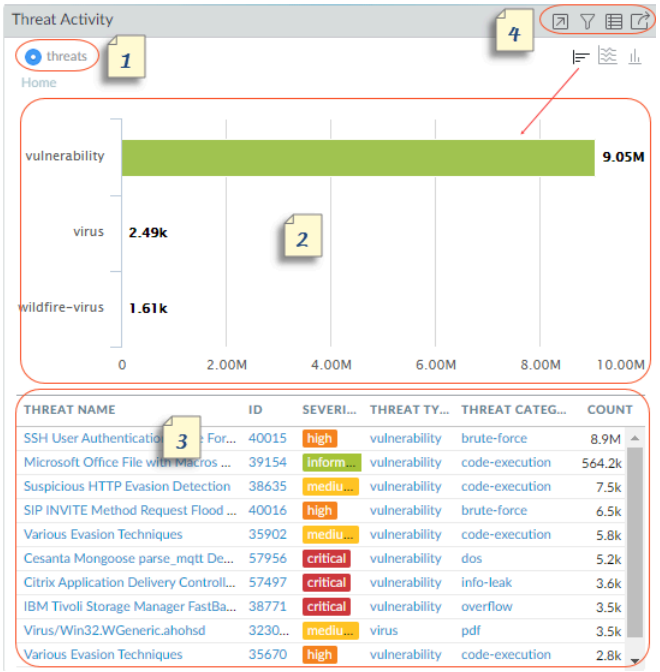
©2024 Palo Alto Networks, Inc.

頁籤	說明
	使用 ACC 資訊評估網路上的解密情況，然後使用 解密日誌 深入挖掘詳細資料。

您也可以 與 ACC 互動，以透過符合您網路監控需求的自訂配置和 Widget 建立自訂頁籤、匯出頁籤並與其他管理員共用。

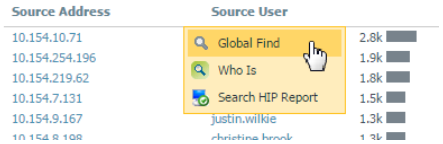
ACC Widget

每個頁籤上的 Widget 均為互動式；您可以設定 ACC 篩選器並深入查看每個表格或圖形的詳細資料，或自訂頁籤中包含的 Widget 以專注於所需資訊。如需各個 Widget 顯示的詳細資訊，請參閱 Widget 描述。



Widget		
1	檢視	您可以依據位元組、工作階段、威脅、計數、內容、URL、惡意、良性、檔案、應用程式、資料、設定檔、物件和使用者來排序資料。每個 Widget 可用的選項有所不同。
2	圖形	圖形顯示選項為樹狀圖、折線圖、橫條圖、堆疊區域圖、堆疊長條圖以及地圖。每個 Widget 可用的選項有所不同；互動體驗也因圖形類型而有所不同。例如，使用非標準連接埠的應用程式 Widget 可讓您在樹狀圖和折線圖之間選擇。

©2024 Palo Alto Networks, Inc.

Widget		
		若要深入至顯示，請按一下圖形。您按一下的區域會成為篩選器，可讓您放大至選取項目並檢視該選取項目更詳細的資訊。
3	表格	圖形下方的表格會提供用於呈現圖形的資料詳細檢視。您可以使用數種方式與表格互動： • 按一下並針對表格中的屬性設定本機篩選器。系統會更新圖形，並使用本機篩選器排序表格。系統一律會同步處理圖形和表格中顯示的資訊。 • 將游標停留在表格中的屬性上，並使用下拉式清單中的可用選項。 
4	動作	最大化檢視—可讓您放大 Widget，在更大的畫面空間中檢視表格，並提供更多可檢視的資訊。 設定本機篩選器—可讓您新增 ACC 篩選器以精簡 Widget 內的顯示內容。您可以使用這些篩選器自訂 Widget；系統會在登入之間保留這些自訂。 跳至日誌—可讓您直接導覽至日誌（**Monitor**（監控）> **Logs**（日誌）> **<log-type>**頁籤）。系統會使用圖形呈現的時段篩選日誌。 若您已設定本機和全域篩選器，日誌查詢會串連時段和篩選器，並僅顯示符合合併篩選器集的日誌。 匯出—可讓您將圖表匯出為 PDF。系統會下載 PDF，並將其儲存至您的電腦。其會儲存於與網頁瀏覽器相關聯的 Downloads（下載）資料夾。

Widget 說明

ACC 上的每個頁籤都包含不同的 Widget 集。

 ©2024 Palo Alto Networks, Inc.

Widget	說明
網路活動—顯示網路上流量和使用者活動的概要。	
應用程式使用方式	表格會顯示網路上所使用的應用程式前十名，且彙總網路上所使用的所有剩餘應用程式並顯示為其他。圖形會依應用程式類別、子類別和應用程式，顯示所有應用程式。您可以使用此 Widget 掃描網路上使用的應用程式，其會告知您使用頻寬、工作階段計數、檔案傳輸、觸發最多威脅和存取 URL 的主要應用程式。 排序屬性：位元組、工作階段、威脅、內容、URL 可用圖表：樹狀圖、區域圖、直條圖、折線圖（圖表視所選屬性排序而異）
使用者活動	顯示網路上最活躍且產生最大流量並耗用網路資源以取得內容的使用者前十名。使用此 Widget 可依位元組、工作階段、威脅、內容 (檔案和模式) 和造訪的 URL 排序，監控使用率前幾名的使用者。 排序屬性：位元組、工作階段、威脅、內容、URL 可用圖表：區域圖、直條圖、折線圖（圖表視所選屬性排序而異）
來源 **IP** 活動	顯示網路上已啟動活動的設備 IP 位址或主機名稱前十名。系統會彙總所有其他設備並顯示為其他。 排序屬性：位元組、工作階段、威脅、內容、URL 可用圖表：區域圖、直條圖、折線圖（圖表視所選屬性排序而異）
目的地 **IP** 活動	顯示網路上使用者存取的目的地 IP 位址或主機名稱前十名。 排序屬性：位元組、工作階段、威脅、內容、URL 可用圖表：區域圖、直條圖、折線圖（圖表視所選屬性排序而異）
來源區域	顯示網路上全球使用者啟動活動的地區前十名（內建或自訂定義地區）。 排序屬性：位元組、工作階段、威脅、內容、URL 可用圖表：地圖、長條圖
目的地區域	顯示網路的世界地圖上使用者存取內容的目的地區域前十名（內建或自訂定義地區）。 排序屬性：位元組、工作階段、威脅、內容、URL 可用圖表：地圖、長條圖

©2024 Palo Alto Networks, Inc.

Widget	說明
GlobalProtect 主機資訊	顯示執行 GlobalProtect 代理程式的主機狀態資訊；主機系統為 GlobalProtect 端點。此資訊來自 HIP 比對日誌中的項目，GlobalProtect 應用程式提交的資料符合您在防火牆上定義的 HIP 物件或 HIP 設定檔時，便會生產生該項目。如果您沒有 HIP 比對日誌，此 Widget 會空白。若要瞭解如何建立 HIP 物件和 HIP 設定檔，並將其作為原則比對規則，請參閱設定基於 HIP 的原則強制執行。 排序屬性：設定檔、物件、作業系統 可用圖表：長條圖
規則使用情況	顯示網路上已允許最多流量的規則前十名。使用此 Widget 可檢視最常用的規則、監控使用率模式，以及評估規則是否可有效保護網路。 排序屬性：位元組、工作階段、威脅、內容、URL 可用圖表：折線圖
輸入介面	顯示最常用於允許流量進入網路的防火牆介面。 排序屬性：位元組、傳送的位元組、收到的位元組 可用圖表：折線圖
輸出介面	顯示最常用於讓流量離開網路的防火牆介面。 排序屬性：位元組、傳送的位元組、收到的位元組 可用圖表：折線圖
來源區域	顯示最常用於允許流量進入網路的區域。 排序屬性：位元組、工作階段、威脅、內容、URL 可用圖表：折線圖
目的地區域	顯示最常用於讓流量離開網路的區域。 排序屬性：位元組、工作階段、威脅、內容、URL 可用圖表：折線圖
威脅活動—顯示網路上威脅的概要	
受危害的主機	顯示在網路上可能受危害的主機。此 Widget 會摘要來自關聯日誌的事件。針對每個來源使用者/IP 位址，其包含觸發比對的關聯物件和比對計數，此為從關聯事件日誌中彙整之比對證據彙總的資訊。如需詳細資訊，請參閱使用自動關聯引擎。

©2024 Palo Alto Networks, Inc.

Widget	說明
	在 PA-5200 系列、PA-7000 系列和 Panorama 上可用。 排序屬性：嚴重性（預設）
造訪惡意 **URL** 的主機	顯示網路上已存取惡意 URL 的主機（IP 位址/主機名稱）頻率。根據 PAN-DB 中的分類，這些 URL 為已知的惡意軟體。 排序屬性：計數 可用圖表：折線圖
解析惡意網域的主機	顯示符合 DNS 特徵碼的前幾名主機；網路上嘗試解析惡意 URL 的主機名稱或網域的主機。系統會從您網路上的 DNS 活動分析收集此資訊。其會利用被動 DNS 監控、在網路上產生的 DNS 流量、在沙箱中看到的活動 (如果您已在防火牆上設定 DNS Sinkhole)，以及可供 Palo Alto Networks 客戶使用的惡意 DNS 來源 DNS 報告。 排序屬性：計數 可用圖表：折線圖
威脅活動	顯示在網路上發現的威脅。此資訊是以防毒、反間諜軟體和漏洞保護設定檔，以及 WildFire 彙報之病毒中的特徵碼比對為基礎。 排序屬性：威脅 可用圖表：長條圖、區域圖、直條圖
按應用程式別的 **WildFire** 活動	顯示產生最多 WildFire 提交的應用程式。此 Widget 會使用來自 WildFire 提交日誌的惡意和良性裁定。 排序屬性：惡意、良性 可用圖表：長條圖、折線圖
按檔案類型分的 **WildFire** 活動	依檔案類型顯示威脅載體。此 Widget 會顯示產生最多 WildFire 提交的檔案類型，並使用來自 WildFire 提交日誌的惡意和良性裁定。如果無法使用此資料，則 Widget 為空白。 排序屬性：惡意、良性 可用圖表：長條圖、折線圖
使用非標準連接埠的應用程式	顯示使用非標準連接埠進入網路的應用程式。如果您已從以連接埠為基礎的防火牆移轉防火牆規則，請使用此資訊建立針對應用程式僅允許使用預設連接埠之流量的原則規則。需要時，可建立例外狀況以允許使用非標準連接埠的流量，或建立自訂應用程式。 排序屬性：位元組、工作階段、威脅、內容、URL

©2024 Palo Alto Networks, Inc.

Widget	說明
	可用圖表：樹狀圖、折線圖
允許應用程式使用非標準連接埠的規則	顯示允許使用非預設連接埠之應用程式的安全性原則規則。圖形會顯示所有規則，而表格會顯示前十名規則並將剩餘規則的資料彙總為其他。 此資訊可讓您評估應用程式是否在連接埠之間轉換或暗中潛入您的網路，以協助您識別網路安全性的漏洞。例如，您可以驗證您是否擁有允許使用（除了應用程式預設連接埠以外）任何連接埠之流量的規則。比如說，例如，您擁有允許使用應用程式預設連接埠之 DNS 流量的規則（連接埠 53 是 DNS 的標準連接埠）。此 Widget 會顯示允許 DNS 流量使用任何連接埠 53 以外的連接埠進入網路的任何規則。 排序屬性：位元組、工作階段、威脅、內容、URL 可用圖表：樹狀圖、折線圖
封鎖的活動—專注於禁止進入網路的流量	
封鎖的應用程式活動	顯示網路上已拒絕的應用程式，且可讓您檢視已排除於網路之外的威脅、內容和 URL。 排序屬性：威脅、內容、URL 可用圖表：樹狀圖、區域圖、直條圖
封鎖的使用者活動	顯示因符合附加至安全性原則的防毒、反間諜軟體、檔案封鎖或 URL 篩選設定檔而被封鎖的使用者要求。 排序屬性：威脅、內容、URL 可用圖表：長條圖、區域圖、直條圖
封鎖的威脅	顯示在網路上已成功拒絕的威脅。已將這些威脅與可透過防火牆上的動態內容更新取得的防毒特徵碼、漏洞特徵碼和 DNS 特徵碼進行比對。 排序屬性：威脅 可用圖表：長條圖、區域圖、直條圖
封鎖的內容	顯示已禁止進入網路的檔案和資料。由於安全性原則已根據檔案封鎖安全性設定檔或資料篩選安全性設定檔中定義的規則拒絕存取，因此已封鎖該內容。 排序屬性：檔案、資料 可用圖表：長條圖、區域圖、直條圖

©2024 Palo Alto Networks, Inc.

Widget	說明
安全性原則封鎖活動	顯示已封鎖或限制流量進入網路的安全性原則規則。由於此 Widget 會顯示已拒絕存取網路的威脅、內容和 URL，您可以將其用於評估原則規則的效益。由於您已在原則中定義的拒絕規則，此 Widget 不會顯示封鎖的流量。 排序屬性：威脅、內容、URL 可用圖表：長條圖、區域圖、直條圖
GlobalProtect 活動—顯示 GlobalProtect 部署中使用者活動的資訊。	
Successful GlobalProtect Connection Activity（**GlobalProtect** 連線活動成功）	顯示所選時段的 GlobalProtect 連接活動的圖表檢視。使用圖表頂部的切換鍵，可以在使用者、入口網站和閘道的連線統計資料以及位置之間進行切換。 排序屬性：使用者、入口網站/閘道、位置 可用圖表：長條圖、折線圖
Unsuccessful GlobalProtect Connection Activity（**GlobalProtect** 連線活動不成功）	顯示所選時段的 GlobalProtect 連接活動不成功的圖表檢視。使用圖表頂部的切換鍵，可以在使用者、入口網站和閘道的連線統計資料以及位置之間進行切換。為了幫助您識別和疑難排解連線問題，您還可以檢視原因圖表或圖形。對於此圖表，ACC 會顯示錯誤、來源使用者、公開 IP 位址和其他資訊，以幫助您快速識別並解決問題。 排序屬性：使用者、入口網站/閘道、原因、位置 可用圖表：長條圖、折線圖
GlobalProtect 部署活動	顯示您部署的圖表檢視摘要。使用圖表頂部的切換鍵，可以透過驗證方法、GlobalProtect 應用程式版本和作業系統版本檢視使用者散佈。 排序屬性：驗證方法、GlobalProtect 應用程式版本、作業系統 可用圖表：長條圖、折線圖
GlobalProtect 隔離活動	顯示已隔離裝置的圖表檢視摘要。使用圖表頂部的切換鍵，按導致 GlobalProtect 隔離裝置的動作、GlobalProtect 隔離裝置的原因、已隔離裝置的位置來檢視已隔離裝置。 排序屬性：動作、原因、位置 可用圖表：長條圖、折線圖
SSL Activity（**SSL** 活動）—顯示有關網路中 SSL/TLS 活動的資訊。	

©2024 Palo Alto Networks, Inc.

Widget	說明
Traffic Activity（流量活動）	按工作階段總數或位元組數顯示 SSL/TLS 活動與非 SSL/TLS 活動之比。
SSL/TLS Activity（**SSL/TLS** 活動）	按 TLS 版本和應用程式或 SNI 顯示成功的 TLS 連線。此 Widget 可幫助您瞭解允許較弱的 TLS 通訊協定版本會帶來多大的風險。識別使用弱通訊協定的應用程式和 SNI 讓您能夠評估每個應用程式和 SNI，並確定是否需要出於業務原因允許對其進行存取。如果您不需要出於業務目的而使用該應用程式，則可以封鎖流量而不是允許它。按一下應用程式或 SNI 以向下鑽研並查看詳細資訊。
Decryption Failure Reasons（解密失敗原因）	按 SNI 顯示解密失敗的原因，如憑證或通訊協定問題。使用此資訊來偵測由解密原則或設定檔設定錯誤或者使用弱通訊協定或演算法的流量引起的問題。按一下失敗原因以向下鑽研並隔離每個 SNI 的工作階段數，或者按一下 SNI 以檢視該 SNI 的失敗。
Successful TLS Version Activity（成功 **TLS** 版本活動）	按工作階段數或位元組數顯示已解密和未解密的流量數。未解密的流量可能會因原則、原則設定錯誤，或因在解密排除清單上而從解密中排除（**Device**（裝置） > **Certificate Management**（憑證管理） > **SSL Decryption Exclusion**（**SSL** 解密排除））。
Successful Key Exchange Activity（成功金鑰交換活動）	按應用程式或按 SNI 顯示每個演算法成功的金鑰交換活動。按一下金鑰交換演算法以僅查看該演算法的活動，或者按一下應用程式或 SNI 以檢視該應用程式或 SNI 的金鑰交換活動。

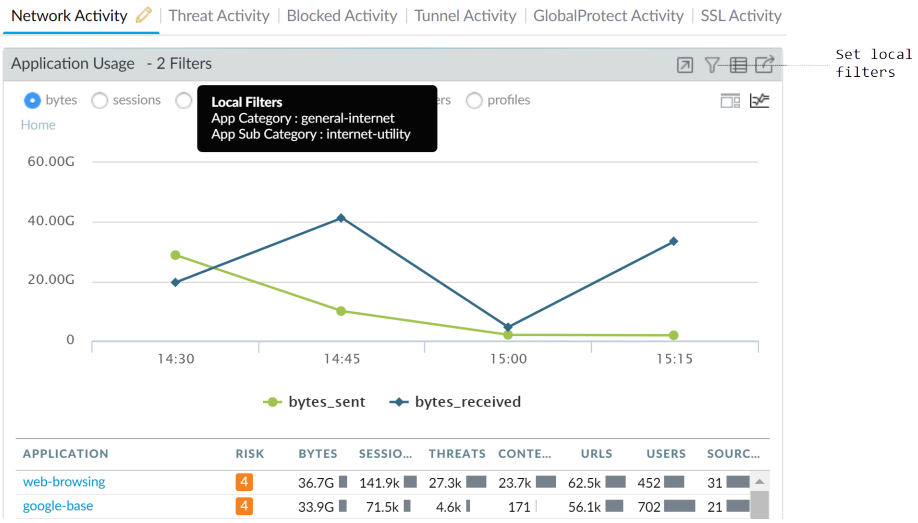
ACC 篩選器

ACC Widget 上的圖形和表格可讓您使用篩選器縮小顯示的資料範圍，從而隔離特定屬性並分析要更仔細檢視的資訊。ACC 支援同時使用 Widget 和全域篩選器。

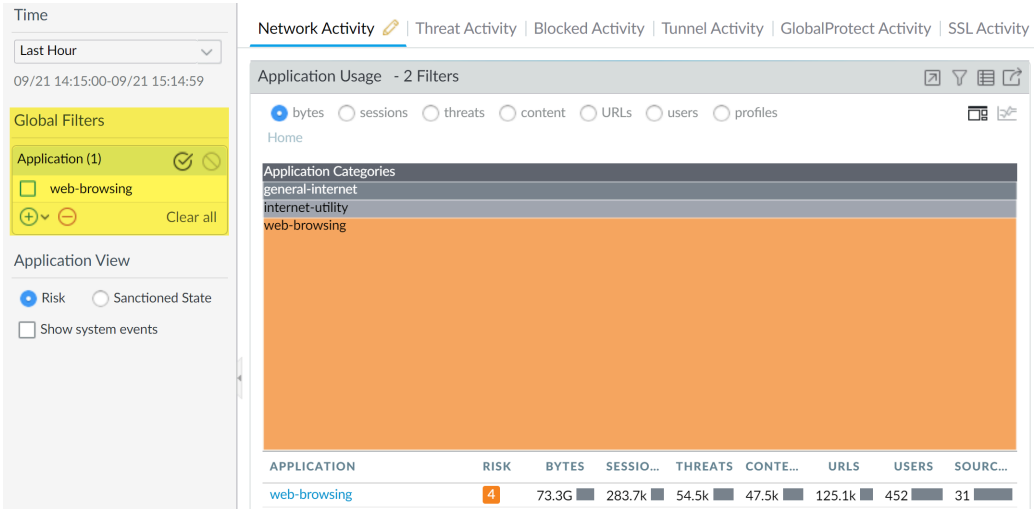
- **Widget** 篩選器—套用 Widget 篩選器，其為特定 Widget 本機的篩選器。Widget 篩選器可讓您與圖形互動並自訂顯示畫面，以深入查看詳細資料並存取要針對特定 Widget 監控的資訊。若要

©2024 Palo Alto Networks, Inc.

建立重新啟動之後仍會維持原狀的 Widget 篩選器，您必須使用 **Set Local Filter**（設定本機篩選器）選項。



- 全域篩選器—全域篩選器會套用至 ACC 中的所有頁籤。全域篩選器可讓您依目前重視的詳細資料轉換顯示畫面，並將無關資訊從目前的顯示畫面中排除。例如，若要檢視與特定使用者和應用程式相關的所有事件，您可以套用使用者名稱和應用程式作為全域篩選器，並僅檢視 ACC 的所有頁籤和 Widget 上與該使用者和應用程式相關的資訊。全域篩選器並非持續性篩選器。



您可以使用三種方式套用全域篩選器：

- 從表格設定全域篩選器—在任何 Widget 中從表格選取屬性，接著將該屬性套用為全域篩選器。
- 新增 **Widget** 篩選器至全域篩選器 — 將游標停留在屬性上，然後按一下屬性右側的箭頭圖示。此選項可讓您增加用於 Widget 中的本機篩選器，並全域套用屬性，以便在 ACC 的所有頁籤上更新顯示。
- **Define a global filter**（定義全域篩選器）—使用 ACC 上的 **Global Filters**（全域篩選器）窗格定義篩選器。

©2024 Palo Alto Networks, Inc.

如需使用這些篩選器的詳細資料，請參閱 與 ACC 互動。

與 ACC 互動

若要自訂並縮小 ACC 顯示畫面，您可新增、刪除匯出及匯入頁籤、新增及刪除 Widget、設定本機和全域過濾器，以及與 Widget 互動。

新增頁籤。

1. 選取頁籤清單旁的 ＋ 圖示。
2. 新增檢視名稱。此名稱將用作頁籤名稱。您可新增最多五個頁籤。

編輯頁籤。

選取頁籤，並按一下頁籤名稱旁的鉛筆圖示以編輯頁籤。例如 Threat Activity 。

編輯頁籤可讓您新增、刪除或重設頁籤中顯示的 Widget。您也可以變更頁籤中的 Widget 配置。

若要將頁籤儲存為預設頁籤，可選取 。

匯出和匯入頁籤。

1. 選取頁籤，並按一下頁籤名稱旁的鉛筆圖示以編輯頁籤。
2. 選取 圖示以將目前的頁籤匯出為 .txt 檔案。您可以與其他管理員共用此 .txt 檔案。
3. 若要將此頁籤作為新頁籤匯入到另一個防火牆上，可選取 ＋ 圖示及頁籤清單，新增名稱，按一下匯入圖示，然後瀏覽以選取 該.txt 檔案。

查看頁籤中包含的 Widget。

1. 選取頁籤並按一下鉛筆圖示以編輯頁籤。
2. 選取 **Add Widgets**（新增 **Widget**）下拉式清單，並確認 Widget 已選中該核取方塊。

©2024 Palo Alto Networks, Inc.

新增 Widget 或 Widget 群組。

1. 新增頁籤或編輯預先定義頁籤。
2. 選取 新增 **Widget**，接著選取對應您想新增 Widget 的核取方塊。您最多可選取 12 個 Widget。
3. （選用）若要建立 2 欄配置，請選取**Add Widget Group**（新增 Widget 群組）。您可將 Widget 拖放至 2 欄顯示中。當您將 Widget 拖曳至配置時，將向您顯示預留位置以放置 Widget。

   您無法命名 *Widget* 群組。

刪除頁籤或 Widget 群組/Widget。

1. 若要刪除自訂頁籤，請選取頁籤並按一下 X 圖示。 Custom_threat_user_activity

   您無法刪除預先定義的頁籤。

2. 若要刪除 Widget 群組/Widget，請編輯頁籤，然後在工作區區段中，按一下右方的 [X] 圖示。您無法復原刪除項目。

重設頁籤中的預設 Widget。

在預先定義的頁籤（例如 **Blocked Activity**（封鎖的活動）頁籤）上，您可以刪除一或多個 Widget。若要重設配置以包含頁籤的預設 Widget 集，請編輯頁籤並按一下 **Reset View**（重設檢視）。

放大區域圖、直條圖或折線圖中的詳細資料。

觀看如何使用放大功能。

按一下並拖曳要放大之圖形中的區域。例如，放大折線圖時，其會觸發重新查詢且防火牆會針對選取的時段擷取資料。這不只是單純的放大功能。

使用表格下拉式清單尋找屬性的詳細資訊。

1. 將游標停留在表格中的屬性上以查看下拉式清單。
2. 按一下下拉式清單以檢視可用的選項。
   - **Global Find**（全域尋找）—使用全域搜尋來搜尋防火牆或 Panorama 管理伺服器以參考候選設定中任意位置的屬性（使用者名稱/IP 位址、物件名稱、政策規則名稱、威脅 ID 或應用程式名稱）。
   - 值—顯示威脅 ID、應用程式名稱或位址物件的詳細資料。
   - 誰—針對 IP 位址執行網域名稱（*WHOIS*）查閱。查閱會查詢儲存已註冊使用者或網際網路資源獲指派者的資料庫。
   - 搜尋 **HIP** 報告—使用使用者名稱或 IP 位址尋找 HIP 比對報告中的相符項目。

©2024 Palo Alto Networks, Inc.

設定 Widget 篩選器。

您也可以按一下（圖表下方）表格中的屬性，以將其套用為 *Widget* 篩選器。

1. 選取 Widget 並按一下圖示。
2. 按一下 圖示以新增要套用的篩選器。
3. 按一下 **Apply**（套用）。這些過濾器在重新啟動之後仍會維持原狀。

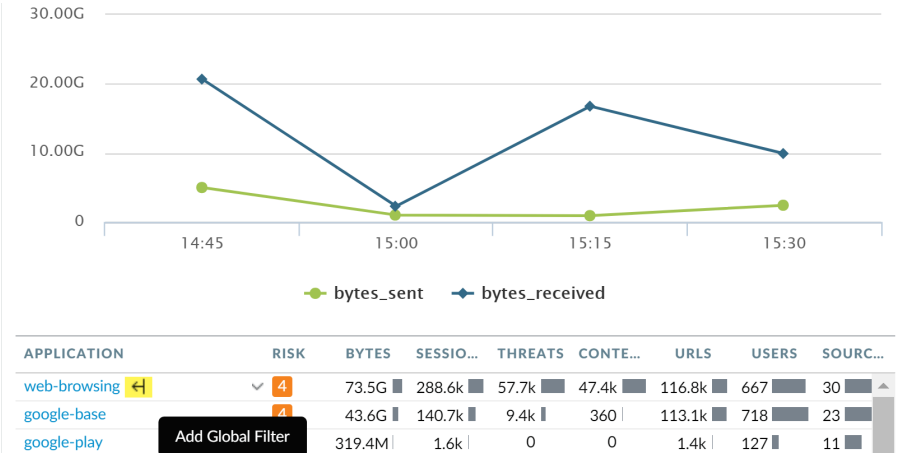
Widget 名稱旁邊會表示使用中的 *Widget* 篩選器。

否定 Widget 篩選器

1. 按一下 圖示以顯示 (設定本機篩選器) 對話方塊。
2. 新增篩選器，然後按一下 否定圖示。

從表格設定全域過濾器。

將游標停留在圖表下表格的屬性上，然後按一下屬性右側的箭頭圖示。



使用全域篩選器窗格設定全域篩選器。

觀看運作中的全域篩選器。

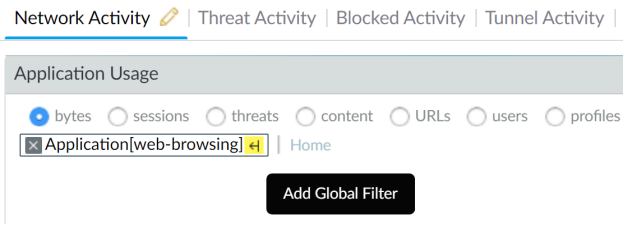
1. 找到 ACC 左側的 **Global Filters**（全域篩選器）窗格。

2. 按一下 圖示以檢視可套用的篩選器清單。

©2024 Palo Alto Networks, Inc.

將 Widget 篩選器提升為全域篩選器。

1. 在 Widget 中的任何表格上，按一下屬性連結。這會將屬性設定為 Widget 篩選器。
2. 若要將篩選器提升為全域篩選器，請選取篩選器右方的箭頭。



移除過濾器。

按一下 圖示以移除篩選器。

- 針對全域篩選器：其位於全域篩選器窗格中。
- 針對 Widget 篩選器：按一下 圖示以顯示（設定本機篩選器）對話方塊，然後選取篩選器並按一下 圖示。

清除所有篩選器。

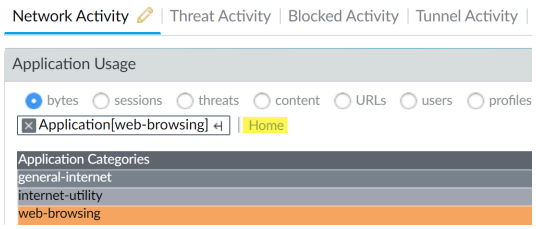
- 針對全域篩選器：按一下（全域篩選器）下的 **Clear All**（全部清除）按鈕。
- 針對 Widget 篩選器：選取 Widget 並按一下圖示。然後按一下（設定本機篩選器）對話方塊中的 **Clear All**（全部清除）按鈕。

查看使用中的篩選器。

- 針對全域篩選器：全域篩選器下的左窗格會顯示已套用全域篩選器的數量。
- 針對 Widget 篩選器：Widget 名稱旁會顯示套用於 Widget 的本機篩選器數量。若要檢視篩選器，請按一下 圖示。

重設 Widget 上的顯示畫面。

- 如果您設定 Widget 篩選器或深入查看圖形，請按一下 **Home**（首頁）連結，以重設 Widget 中的顯示畫面。



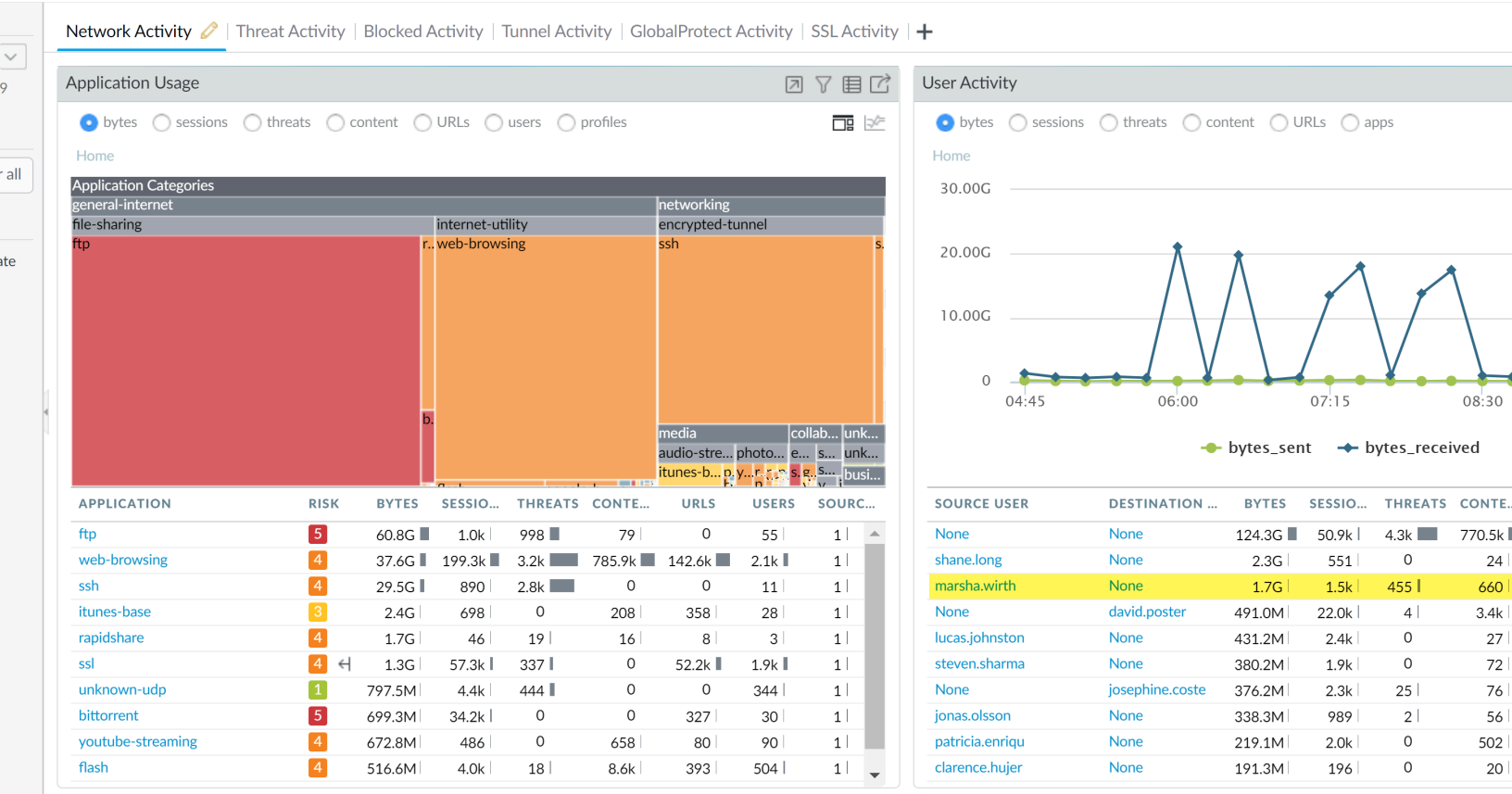
 ©2024 Palo Alto Networks, Inc.

使用案例：ACC—資訊探索路徑

ACC 具有大量的資訊，可供您作為分析網路流量的起點。讓我們看一下使用 ACC 發現所需事件的範例。此範例說明您可以如何使用 ACC 來確保合法使用者可為其動作承擔責任、偵測和追蹤未經授權的活動，以及偵測和診斷網路上受危害的主機和具有漏洞的系統。

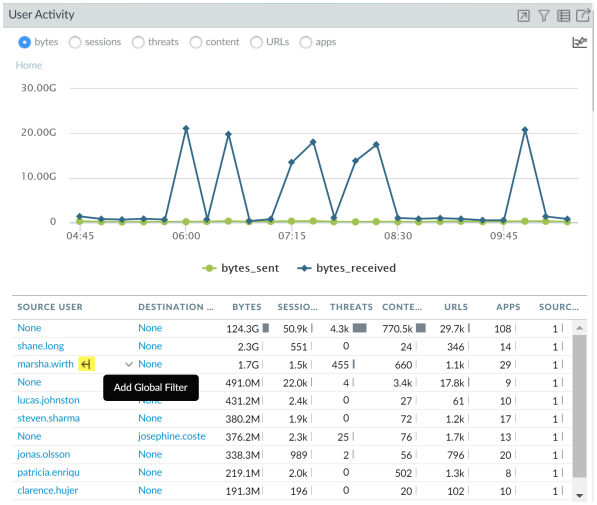
ACC 中的 Widget 和篩選器可讓您根據需要或關注的事件，分析資料和篩選檢視。您可以追蹤引起您注意的事件，直接將頁籤匯出為 PDF、存取原始日誌，以及儲存要追蹤之活動的個人化檢視。這些功能可讓您監控活動和開發原則和對策，以強化您的網路來抵禦惡意活動。在本節中，您將在不同頁籤之間 與 ACC 互動 Widget、使用 Widget 篩選器深入查看資訊、使用全域篩選器轉換 ACC 檢視，以及匯出 PDF 與事件回應或 IT 團隊共用。

在 **ACC** > **Network Activity**（網路活動）頁籤中，您一眼就能看到 Application Usage（應用程式使用率）和 User Activity（使用者活動）Widget。使用者活動 Widget 顯示使用者 Marsha Wirth 在過去一小時內已傳輸 154MB 的資料。此傳輸量幾乎已超過網路上任何其他使用者的六倍。若要查看過去幾個小時的趨勢，請將**Time**（時間）週期擴展至 **Last 6 Hrs**（前 **6** 小時），現在 Marsha 的活動已涵蓋 1,500 個工作階段中的 1.7GB，且已觸發 455 個威脅特徵碼。



由於 Marsha 已傳輸大量資料，因此我們將其使用者名稱套用為全域篩選器（ACC 篩選器），並將 ACC 中的所有檢視轉換為 Marsha 的流量活動。

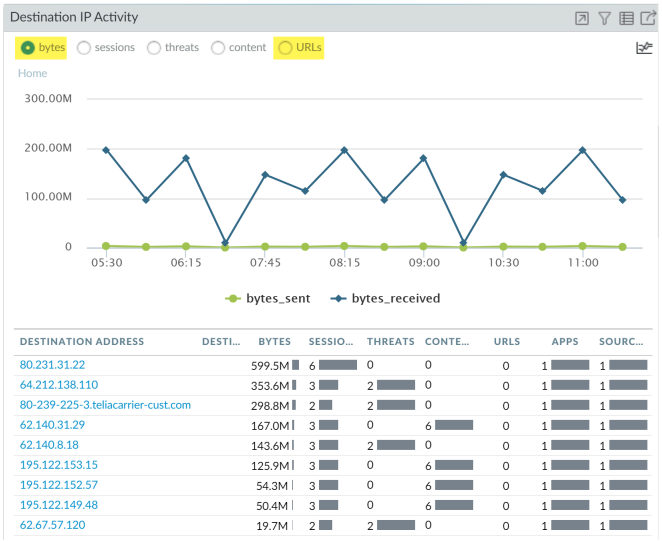
©2024 Palo Alto Networks, Inc.



（應用程式使用率）頁籤現在顯示 Martha 最常用的應用程式是 rapidshare，其為屬於檔案共用 URL 類別的瑞士檔案共享網站。為了進一步調查，請將 rapidshare 新增為全域篩選器，並在 rapidshare 內容中檢視 Marsha 的活動。

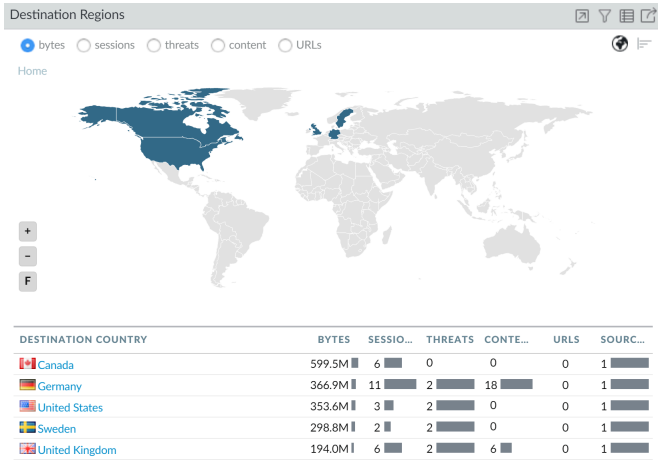
請考慮您是否想要核准在公司內部使用 *rapidshare*。您是否應該允許上傳至此網站？是否需要透過 *QoS* 原則限制頻寬？

若要檢視已與 Marsha 通訊的 IP 位址，請核取 **Destination IP Activity**（目的地 **IP** 活動）Widget，並依位元組和 URL 檢視資料。



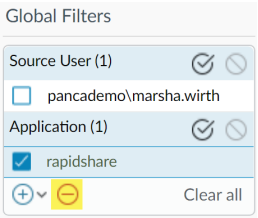
若要瞭解與 Marsha 通訊的國家，請排序 **Destination Regions**（目的地區域）Widget 中的 **sessions**（工作階段）。

©2024 Palo Alto Networks, Inc.

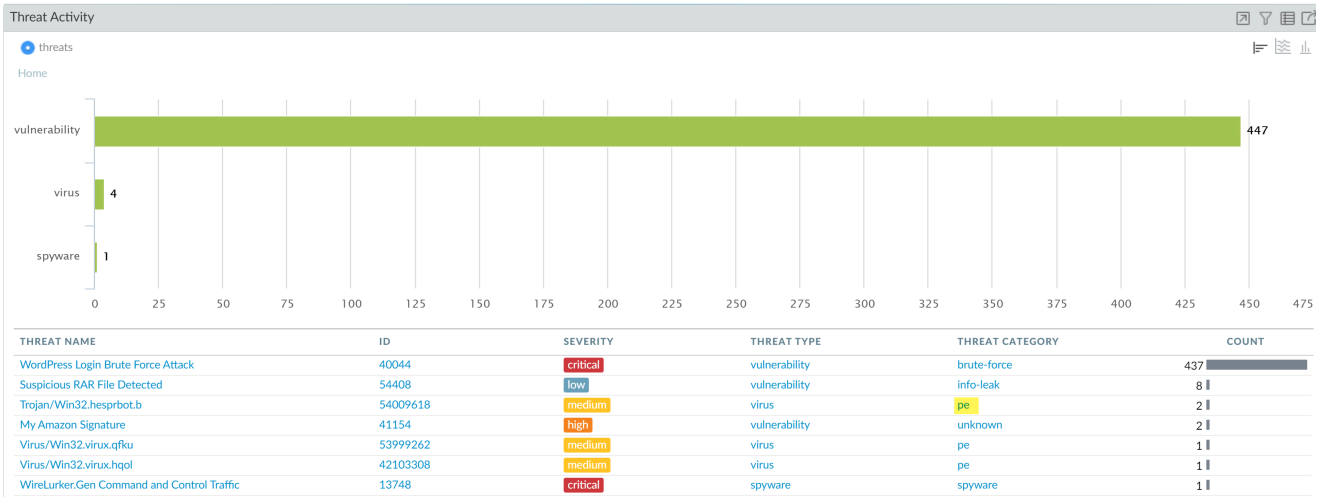


從這些資料中，您可以確認您網路上的使用者 Marsha 已在加拿大、德國、瑞典、英國和美國建立工作階段。她在每個目的地國家的工作階段中記錄了 2 個威脅。

為了從威脅的觀點查看 Marsha 的活動，請移除 rapidshare 的全域篩選器。



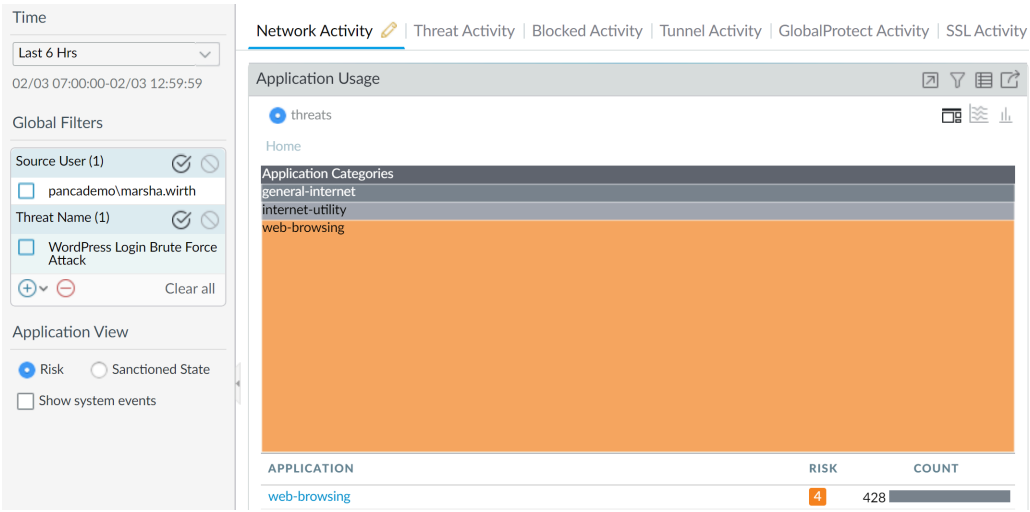
在 **Threat Activity**（威脅活動）頁籤的 **Threat Activity**（威脅活動）Widget 中檢視威脅。Widget 顯示其活動已觸發暴力密碼破解、資訊洩漏、可攜式可執行檔 (PE) 和間諜軟體威脅類別中的 452 個漏洞比對。許多漏洞都具有關鍵嚴重性。



若要進一步深入查看每個漏洞，請按一下圖形並縮小調查範圍。每次按一下時，系統都會在 Widget 上自動套用本機篩選器。

©2024 Palo Alto Networks, Inc.

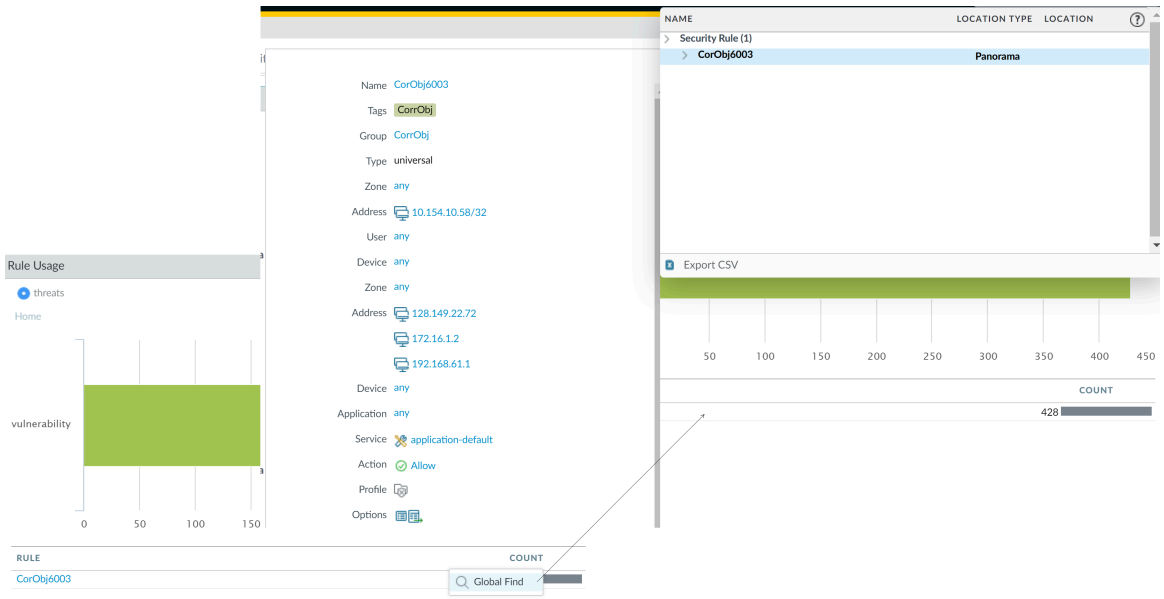
若要依名稱調查每個威脅，您可以建立一個全域篩選器，例如 **WordPress** 登入暴力密碼破解攻擊。然後檢視 **Network Activity**（網路活動）頁籤中的 **User Activity widget**（使用者活動 **Widget**）。系統會自動篩選頁籤以針對 Marsha 顯示威脅活動（請注意螢幕擷取畫面中的全域篩選器）。



請注意，imap 應用程式已透過電子郵件觸發此 Microsoft 指令碼執行漏洞。現在您可以證實 Martha 具有 IE 漏洞和電子郵件附件漏洞，且其電腦可能需要修補。現在您可以導覽至 **Blocked Activity**（封鎖的活動）頁籤中的 **Blocked Threats**（封鎖的威脅）Widget，以查看已封鎖多少漏洞。

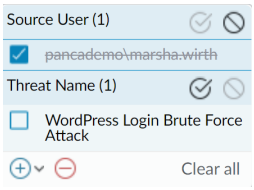
或者，您可以查看 **Network Activity**（網路活動）頁籤上的 **Rule Usage**（規則使用率）Widget，以探索有多少漏洞讓其進入您的網路，以及哪個安全性規則允許此流量進入，並使用 **Global Find**（全域尋找）功能直接導覽至安全性規則。

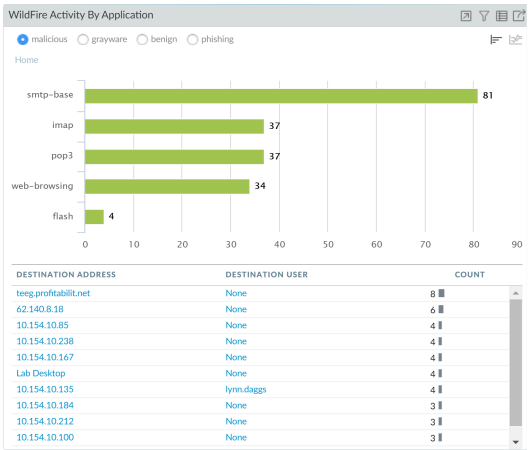
©2024 Palo Alto Networks, Inc.



然後，深入探究使用 web-browsing 攻擊目標目的地的攻擊者。請考慮修改安全性原則規則，以限制這些惡意 IP 位址，或更確切地定義哪些 IP 位址可以存取您的網路資源。

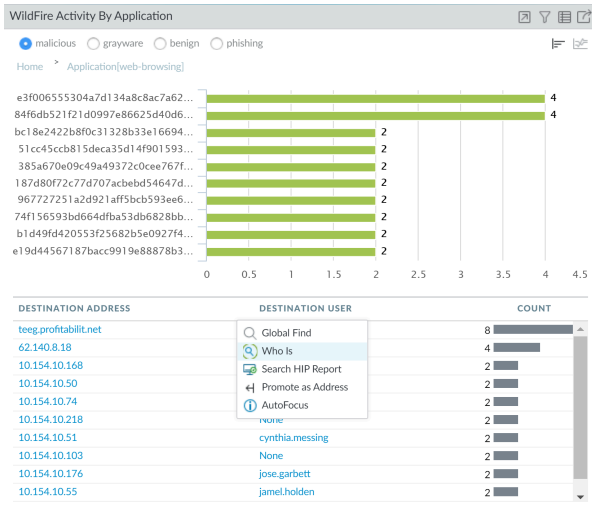
若要檢閱是否已在 web-browsing 中記錄任何威脅，可在 **Threat Activity**（威脅活動）頁籤的 **WildFire Activity by Application**（按應用程式分的 **WildFire** 活動）Widget 中查看 Marsha 的活動。您可以確認 Marsha 並未進行任何惡意活動，但若要確認所有其他使用者都未受到 web-browsing 應用程式的危害，請否定將 Marsha 作為全域篩選器，並尋找在 web-browsing 中觸發威脅的其他使用者。





在圖形中按一下 imap 的長條，然後深入查看與應用程式相關聯的輸入威脅。若要找到 IP 位址註冊的項目，請將遊標停留在攻擊者 IP 位址上，然後在下拉式清單中，選取 **Who Is**（誰）連結。

©2024 Palo Alto Networks, Inc.



由於來自此 IP 位址的工作階段計數較多，因此可查看 **Blocked Activity**（封鎖的活動）頁籤中的 **Blocked Content**（封鎖的內容）和 **Blocked Threats**（封鎖的威脅）是否有與此 IP 位址相關的事件。**Blocked Activity**（封鎖的活動）頁籤可讓您驗證網路上的主機受危害時，原則規則是否可有效封鎖內容或威脅。

使用 ACC 上的 **Export PDF**（匯出 **PDF**）功能匯出目前的檢視（建立資料快照），並將其傳送至事件回應團隊。若要直接從 Widget 中檢視威脅日誌，您也可以按一下 圖示以跳至日誌；系統會自動產生查詢，且螢幕上只會顯示相關日誌（例如，在**Monitor**（監控）> **Logs**（日誌）> **Threat Logs**（威脅日誌）中）。

您現在已使用 ACC 檢閱網路資料/趨勢，以尋找產生最多流量的應用程式或使用者，以及多少應用程式應該為網路上發現的威脅承擔責任。您已識別產生流量的應用程式和使用者、判斷應用程式是否使用預設連接埠和允許流量進入網路的原則規則，以及判斷威脅是否已橫向散佈於網路。您也已識別與網路上的主機通訊的目的地 IP 位址的地理位置。且可使用從調查得出結論建立目標導向的原則，以保護網路上的使用者。

©2024 Palo Alto Networks, Inc.

使用 App-Scope 報告

App Scope 報告提供可見度與分析工具，以協助指出有問題的行為、協助您瞭解應用程式使用情況與使用者活動的異動、知道佔用最多網路頻寬的使用者與應用程式，並識別網路威脅。

透過 App Scope 報告，您可以快速發現是否有任何異常或非預期的行為。各報告均會提供使用者可自訂的動態網路視窗；將滑鼠移到圖表上方，再按一下圖表的行或軸，即可在 ACC 上開啟特定應用程式、應用程式類別、使用者或來源的詳細資訊。**Monitor**（監控） > **App Scope** 上的 App Scope 圖表可讓您：

- 切換圖例中的屬性，便能只檢視您要檢閱的圖表詳細資料。資料可自圖表中加以包含或排除，讓您更密切地變更規模與檢閱詳細資料。
- 按一下長條圖中的屬性，可在 ACC 中深入到相關的工作階段。在任何長條圖上按一下應用程式名稱、應用程式類別、威脅名稱、威脅類別、來源 IP 位址或目的地 IP 位址，可在 ACC 中篩選屬性並檢視相關的工作階段。
- 將圖表或地圖匯出為 PDF 或影像。如需攜帶及離線檢視，您可以將圖表與影像匯出為 PDF 或 PNG 影像。

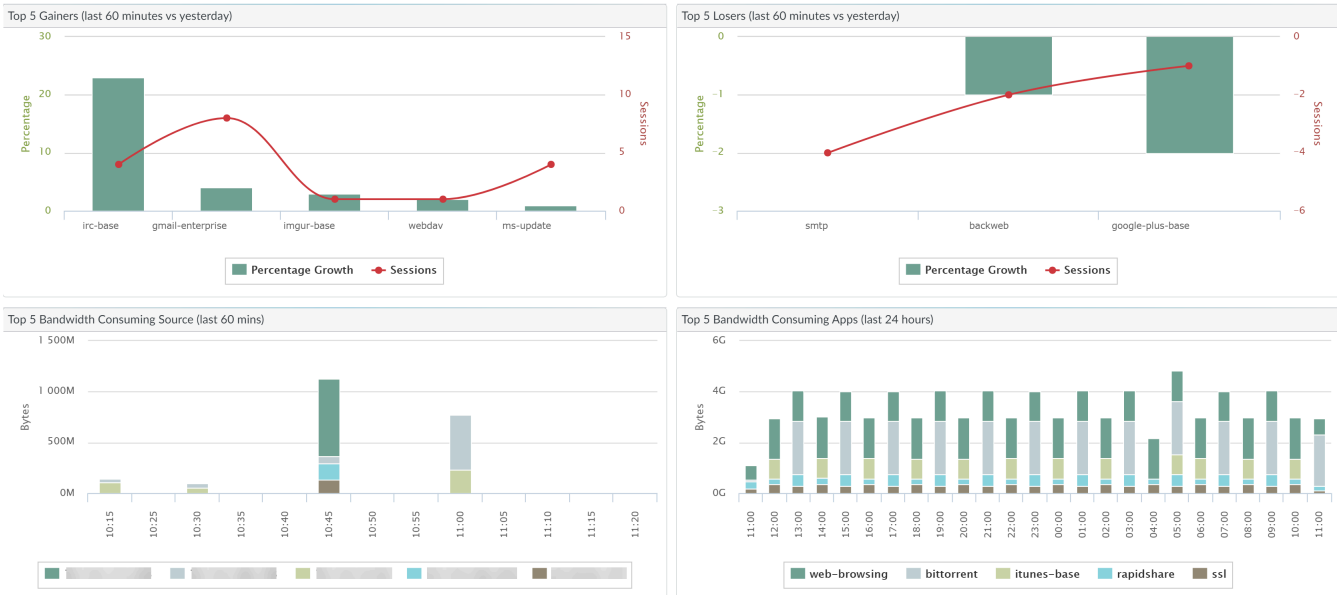
以下為可用的 App Scope 報告：

- 摘要報告
- 異動監控報告
- 威脅監控報告
- 威脅地圖報告
- 網路監控報告
- 流量地圖報表

摘要報告

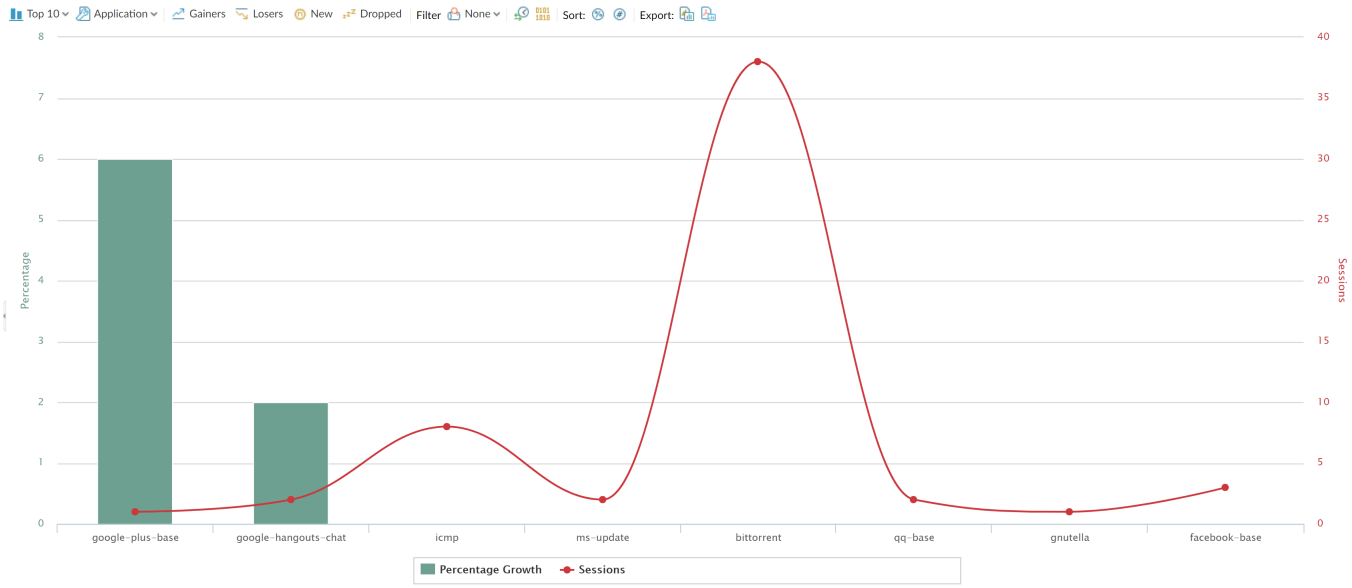
App Scope 摘要報告**Monitor**（監控） > **App Scope** > **Summary**（摘要））可顯示前五名的成長項目、衰退項目，以及頻寬消耗應用程式、應用程式類別、使用者和來源的圖表。

©2024 Palo Alto Networks, Inc.



異動監控報告

App Scope 異動監控報告（**Monitor**（監控） > **App Scope** > **Change Monitor**（異動監控））會顯示指定時段內的異動。例如，下列圖表顯示與過去 24 小時期間相比較，在前一個小時內都在使用的前幾名應用程式。前幾名的應用程式是由工作階段數量所決定，並按百分比排序。



異動監控報告包含下列按鈕與選項。

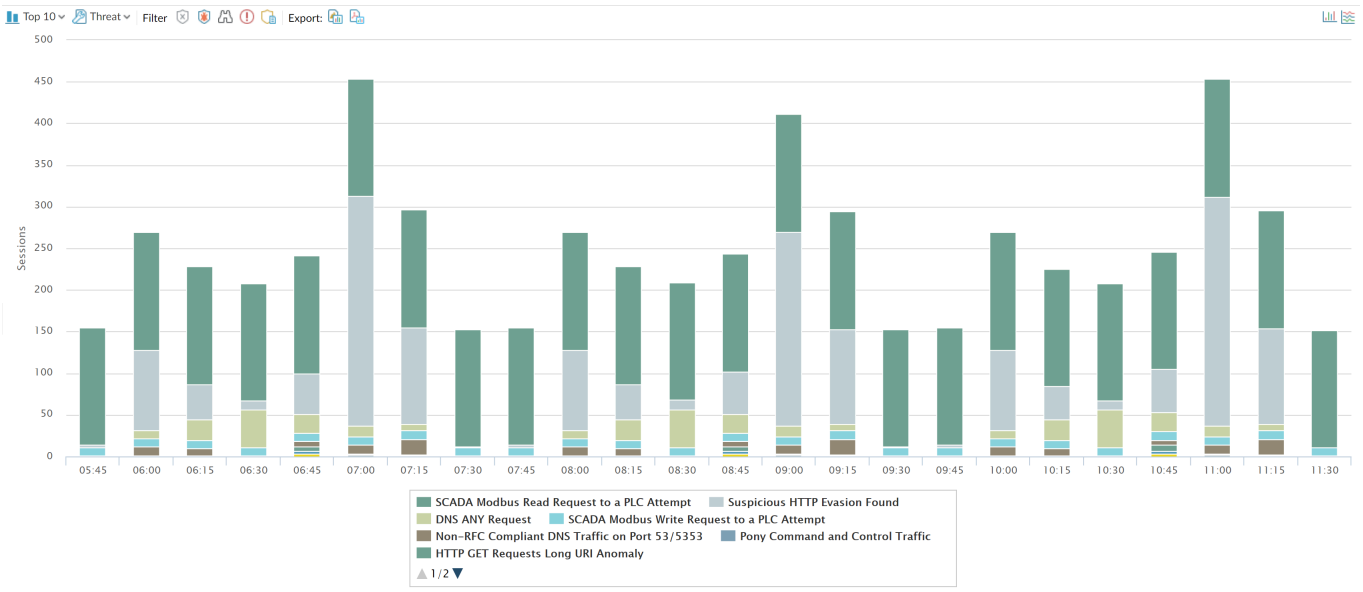
按鈕	說明
前 **10** 位	決定在圖表中包含最高排名，記錄的數量。

©2024 Palo Alto Networks, Inc.

按鈕	說明
應用程式	決定報告的項目類型：應用程式、應用程式類別、來源或目的地。
獲利者	顯示在測量過程中增加的項目測量。
失敗者	顯示在測量過程中減少的項目測量。
新增	顯示在測量過程中新增的項目測量。
已丟棄	顯示在測量過程中終止的項目測量。
篩選	套用篩選器以僅顯示所選項目。None（無）會顯示所有項目。
	決定顯示工作階段還是位元組資訊。
排序	決定按百分比還是粗略的成長率排序項目。
匯出	將圖形匯出為 .png 影像或 PDF。
比較	指定進行異動測量的時段。

威脅監控報告

App Scope 威脅監控報告（**Monitor**（監控） > **App Scope** > **Threat Monitor**（威脅監控））會顯示所選時段內前幾名的威脅計數。例如，下圖即顯示過去 6 個小時的前 10 名威脅類型。



©2024 Palo Alto Networks, Inc.

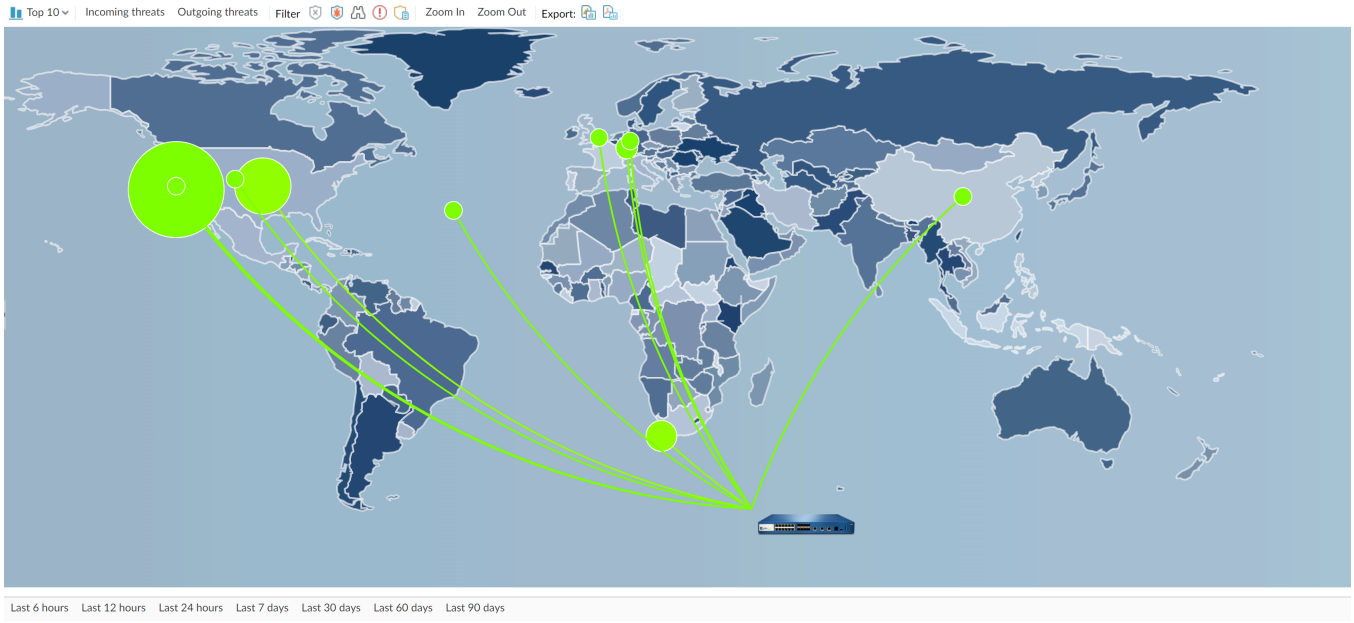
每個威脅類型都用顏色分類，如圖表下面的圖例所示。威脅監控報告包括下列按鈕與選項。

按鈕	說明
前 **10** 位	決定在圖表中包含最高排名，記錄的數量。
威脅	決定測量的項目類型：威脅、威脅類別、來源或目的地。
篩選	套用篩選器以僅顯示所選項目類型。
	決定將資訊顯示在堆疊式欄圖表還是堆疊式區域圖表中。
匯出	將圖形匯出為 .png 影像或 PDF。
	指定進行測量的時段。

威脅地圖報告

App Scope 威脅地圖報告（**Monitor**（監控） > **App Scope** > **Threat Map**（威脅地圖））會顯示威脅的地理視圖，包含嚴重性。每個威脅類型都用顏色分類，如圖表下面的圖例所示。

防火牆使用地理位置來建立威脅地圖。如果您未在防火牆上指定地理位置座標（**Device**（裝置） > **Setup**（設定） > **Management**（管理） 的 General Settings（一般設定）區段），則防火牆會位於威脅地圖畫面底端。



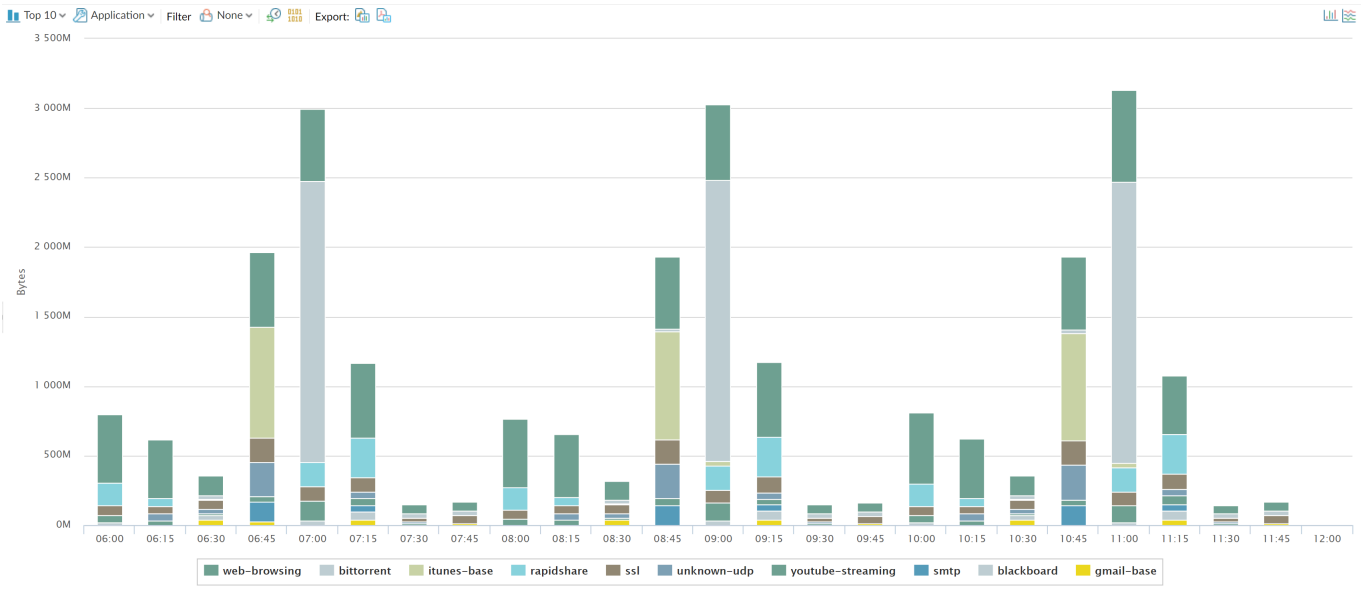
威脅地圖報告包括下列按鈕與選項。

 ©2024 Palo Alto Networks, Inc.

按鈕	說明
前 **10** 位	決定在圖表中包含最高排名，記錄的數量。
連入威脅	顯示連入的威脅。
傳出威脅	顯示連出的威脅。
篩選器	套用篩選器以僅顯示所選項目類型。
放大和縮小	放大和縮小地圖。
匯出	將圖形匯出為 .png 影像或 PDF。
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days Last 90 d	選擇進行分析的時間區段。

網路監控報告

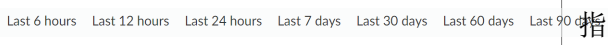
App Scope 網路監控報告（**Monitor**（監控） > **App Scope** > **Network Monitor**（網路監控））會顯示指定時段內用於不同網路功能的頻寬。每個網路服務應用都用顏色分類，如圖表下面的圖例所示。例如，下列影像顯示以工作階段資訊為基礎的過去 7 天應用程式頻寬。



網路監控報告包括下列按鈕與選項。

按鈕	說明
前 **10** 位	決定在圖表中包含最高排名，記錄的數量。

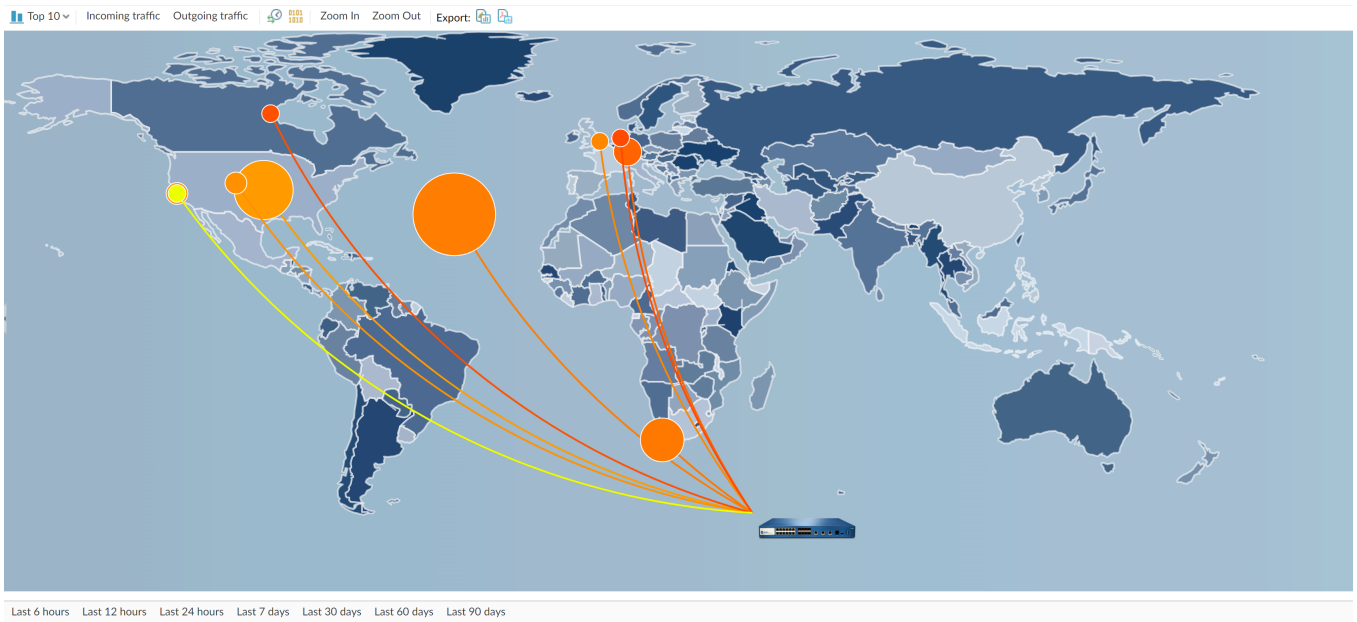
©2024 Palo Alto Networks, Inc.

按鈕	說明
應用程式	決定報告的項目類型：應用程式、應用程式類別、來源或目的地。
篩選	套用篩選器以僅顯示所選項目。**None**（無）會顯示所有項目。
	決定顯示工作階段還是位元組資訊。
匯出	將圖形匯出為 .png 影像或 PDF。
	決定將資訊顯示在堆疊式欄圖表還是堆疊式區域圖表中。
	指示進行異動測量的時段。

流量地圖報表

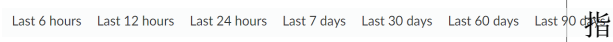
App Scope 流量地圖（**Monitor**（監控） > **App Scope** > **Traffic Map**（流量地圖））報告會根據工作階段或流量顯示流量的地理視圖。

防火牆使用地理位置來建立流量地圖。如果您未在防火牆上指定地理位置座標（**Device**（裝置） > **Setup**（設定） > **Management**（管理） 的 General Settings（一般設定）區段），則防火牆會位於流量地圖畫面底端。



每個流量類型都用顏色分類，如圖表下面的圖例所示。流量地圖報告包括下列按鈕與選項。

©2024 Palo Alto Networks, Inc.

按鈕	說明
前 **10** 位	決定在圖表中包含最高排名，記錄的數量。
連入威脅	顯示連入的威脅。
連出威脅	顯示連出的威脅。
	決定顯示工作階段還是位元組資訊。
放大和縮小	放大和縮小地圖。
匯出	將圖形匯出為 .png 影像或 PDF。
	指示進行異動測量的時段。

 ©2024 Palo Alto Networks, Inc.

使用自動關聯引擎

自動關聯引擎是可使用防火牆上的日誌，偵測到網路上可執行事件的分析工具。引擎會建立一系列的相關威脅事件之間的關聯，結合這些事件後便可表示網路上可能受危害的主機或某些其他更高層次的結論。其可指出風險區域（例如受網路上危害的主機），可讓您評估風險並採取行動以防止網路資源遭到入侵。自動關聯引擎會使用關聯物件分析日誌中的模式，並在發生相符時產生關聯的事件。

下列型號支援自動關聯引擎：

- *Panorama—M* 系列裝置和虛擬裝置
- *PA-7000* 系列防火牆
- *PA-5400* 系列防火牆
- *PA-5200 Series* 防火牆
- *PA-3400* 系列防火牆
- *PA-3200* 系列防火牆

- 自動關聯引擎概念
- 檢視關聯物件
- 判讀關聯的事件
- 使用 ACC 中之受危害的主機 Widget

自動關聯引擎概念

自動關聯引擎會使用關聯物件分析日誌中的模式，並在發生相符時產生關聯的事件。

- 關聯物件
- 關聯的事件

關聯物件

關聯物件為定義檔案，可指定要比對的模式、用於執行查閱的資料來源，以及要尋找這些模式的時段。模式為條件的布林結構，其可查詢防火牆上的下列資料來源（或日誌）：應用程式統計資料、流量、流量摘要、威脅、資料篩選和 URL 篩選。每個模式都具有嚴重性評等，以及定義的時間限制內模式比對必須發生的次數臨界值，超過此值時才能表示發生惡意活動。符合比對條件時，便會記錄關聯的事件。

關聯物件可以連線至隔離的網路事件，並尋找表示發生更嚴重事件的模式。這些物件會識別可疑的流量模式和網路異常狀況，包含可疑的 IP 活動、已知的命令與控制項活動、已知的漏洞入侵或 Botnet 活動，關聯時，表示網路上的主機非常可能已受危害。Palo Alto Networks 威脅研究團隊會

©2024 Palo Alto Networks, Inc.

定義和開發關聯物件，並為防火牆和 Panorama 提供每週動態更新。若要取得新的關聯物件，防火牆必須具有威脅防止授權。Panorama 需要支援授權才能取得更新。

在關聯物件中定義的模式可以是靜態或動態模式。包含 WildFire 中所觀測模式的關聯物件是動態物件，且可建立將 WildFire 偵測到的惡意軟體模式，與網路上惡意軟體目標主機所啟動之命令與控制項活動或 Panorama 上設陷保護端點所發現的活動關聯。例如，主機將檔案提交至 WildFire 雲端且裁定為惡意時，關聯物件會在網路上尋找出現在雲端中觀察到之相同行為的其他主機或用戶端。如果惡意軟體樣本已執行 DNS 查詢，並瀏覽至惡意軟體網域，則關聯物件會剖析日誌中是否具有類似事件。主機上的活動符合雲端中的分析時，便會記錄高嚴重性關聯事件。

關聯的事件

關聯物件中定義的模式和臨界值符合網路上的流量模式時，便會記錄關聯的事件。若要 判讀關聯的事件 並檢視事件的圖形顯示，請參閱 使用 ACC 中之受危害的主機 Widget。

檢視關聯物件

您可以檢視防火牆上目前可用的關聯物件。

STEP 1 | 選取 **Monitor**（監控） > **Automated Correlation Engine**（自動關聯引擎） > **Correlation Objects**（關聯物件）。清單中的所有物件都預設為啟用。

	TITLE	CATEGORY	STATE	DESCRIPTION
☐	Multiple User from One Endpoint MFA Credential Theft	credential-theft-abuse	active	This correlation object detects multiple account abuse from a possibly compromised endpoint
☐	WildFire C2	compromised-host	active	This correlation object detects hosts that have exhibited command-and-control (C2) network behavior corresponding to malware detected by WildFire elsewhere on your network.
☐	WildFire and Traps ESM Correlated C2	compromised-host	active	This correlation object detects hosts that have received malware detected by WildFire or executed malware as seen by Traps, and have also exhibited command- and-control (C2) network behavior corresponding to the detected malware.
☐	Single Account and Endpoint MFA Credential Theft	credential-theft-abuse	active	This correlation object detects activity from a possibly compromised user account from a single endpoint
☐	Compromise Activity Sequence	compromised-host	active	This correlation object detects a host involved in a sequence of activity indicating remote compromise, starting with scanning or probing activity, progressing to exploitation, and concluding with network contact to a known malicious domain.
☐	Exploit Kit Activity	compromised-host	active	This object detects probable exploit kit activity targeted at a host on the network. Exploit kits are identified by a vulnerability exploit or exploit kit landing page signature, combined with either a malware download signature or a known command-and-control signature.
☐	Single Account 1 FA Multiple Endpoints Credential Timeouts	credential-theft-abuse	active	This correlation object detects timed out attempts of first factor authentications from multiple endpoints using a single user account
☐	Beacon Detection	compromised-host	active	This correlation object detects likely compromised hosts based on activity that resembles command-and-control (C2) beaconing, such as repeated visits to recently registered domains or dynamic DNS domains, repeated file downloads from the same location, generation of unknown traffic, etc.
☐	Single Account and Endpoint MFA Credential Timeout	credential-theft-abuse	active	This correlation object detects timedout MFA authentication attempts from a single endpoint using single account
☐	Multiple Endpoint MFA Credential Timeout Abuse	credential-theft-abuse	active	This correlation object detects timed out second factor authentications from multiple endpoints using a single user account
☐	Multiple Endpoint MFA Credential Abuse	credential-theft-abuse	active	This correlation object detects activity from multiple endpoints using a single user account
☐	Exploit Kit Delivering XOR obfuscated malware	compromised-host	active	This correlation object detects exclusive-or (XOR) obfuscated malware downloaded to a host. XOR obfuscation is a technique to evade detection by encrypting portions of a file in order to hide malicious code. This correlation object specifically identifies XOR obfuscated malware that is delivered to the host by an exploit kit. While the Exploit Kit Activity object detects exploit kits combined with either a malware download signature or a known command-and-control signature, this object is provided to specifically detect an event where XOR obfuscation malware inserted on a host by an exploit kit and to distinguish such an event from other exploit kit activities.
☐	Single Account 1 FA Credential Abuse	credential-theft-abuse	active	This correlation object detects timed out first factor authentications from an endpoint using a single user account

STEP 2 | 通視每個關聯物件的詳細資料。每個物件都會提供下列資訊：

- 名稱和 標題—名稱和標題將指示關聯物件偵測到的活動類型。名稱欄在檢視中預設為隱藏。若要檢視物件定義，請取消隱藏該欄並按一下名稱連結。
- **ID**—用於識別關聯物件的唯一號碼；此欄也預設為隱藏。這些 ID 位於 6000 系列中。
- 類別—網路、使用者或主機所受威脅或傷害類型的分類。目前所有物件都會識別網路上受危害的主機。
- **State**（狀態）—表示關聯物件為啟用（使用中）或停用（非使用中）。清單中的所有物件都預設為啟用，因此都為使用中。由於這些物件是以威脅情報資料為基礎，且由 Palo Alto

©2024 Palo Alto Networks, Inc.

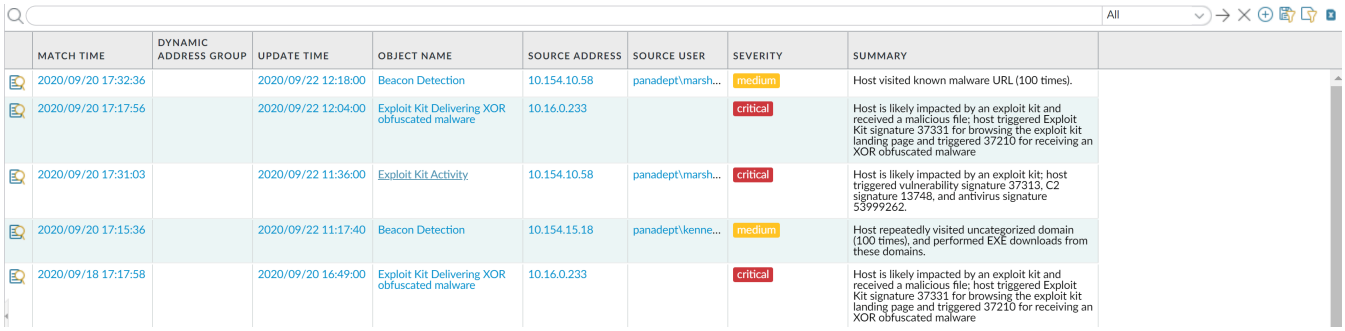
Networks 威脅研究團隊所定義，因此您必須讓這些物件保持為使用中狀態才能追蹤和偵測網路上的惡意活動。

- 說明—指定防火牆或 Panorama 將分析日誌的比對條件。其說明要進行比對以識別惡意活動或可疑主機行為之加速或升級的一系列條件。例如，**Compromise Lifecycle**（危害生命週期）物件偵測以三步驟升級涉及完整攻擊生命週期主機，從掃描或探查活動開始，發展為入侵，然後以與已知惡意網域聯繫的網路結束。

如需詳細資訊，請參閱自動關聯引擎概念與使用自動關聯引擎。

判讀關聯的事件

您可以檢視和分析針對 **Monitor**（監控） > **Automated Correlation Engine**（自動關聯引擎） > **Correlated Events**（關聯的事件） 頁籤中每個關聯的事件產生的日誌。



MATCH TIME	DYNAMIC ADDRESS GROUP	UPDATE TIME	OBJECT NAME	SOURCE ADDRESS	SOURCE USER	SEVERITY	SUMMARY
2020/09/20 17:32:36		2020/09/22 12:18:00	Beacon Detection	10.154.10.58	panadept\marsh...	medium	Host visited known malware URL (100 times).
2020/09/20 17:17:56		2020/09/22 12:04:00	Exploit Kit Delivering XOR obfuscated malware	10.16.0.233		critical	Host is likely impacted by an exploit kit and received a malicious file; host triggered Exploit Kit signature 37331 for browsing the exploit kit landing page and triggered 37210 for receiving an XOR obfuscated malware
2020/09/20 17:31:03		2020/09/22 11:36:00	Exploit Kit Activity	10.154.10.58	panadept\marsh...	critical	Host is likely impacted by an exploit kit; host triggered vulnerability signature 37313, C2 signature 13748, and antivirus signature 53999262.
2020/09/20 17:15:36		2020/09/22 11:17:40	Beacon Detection	10.154.15.18	panadept\kenne...	medium	Host repeatedly visited uncategorized domain (100 times), and performed EXE downloads from these domains.
2020/09/18 17:17:58		2020/09/20 16:49:00	Exploit Kit Delivering XOR obfuscated malware	10.16.0.233		critical	Host is likely impacted by an exploit kit and received a malicious file; host triggered Exploit Kit signature 37331 for browsing the exploit kit landing page and triggered 37210 for receiving an XOR obfuscated malware

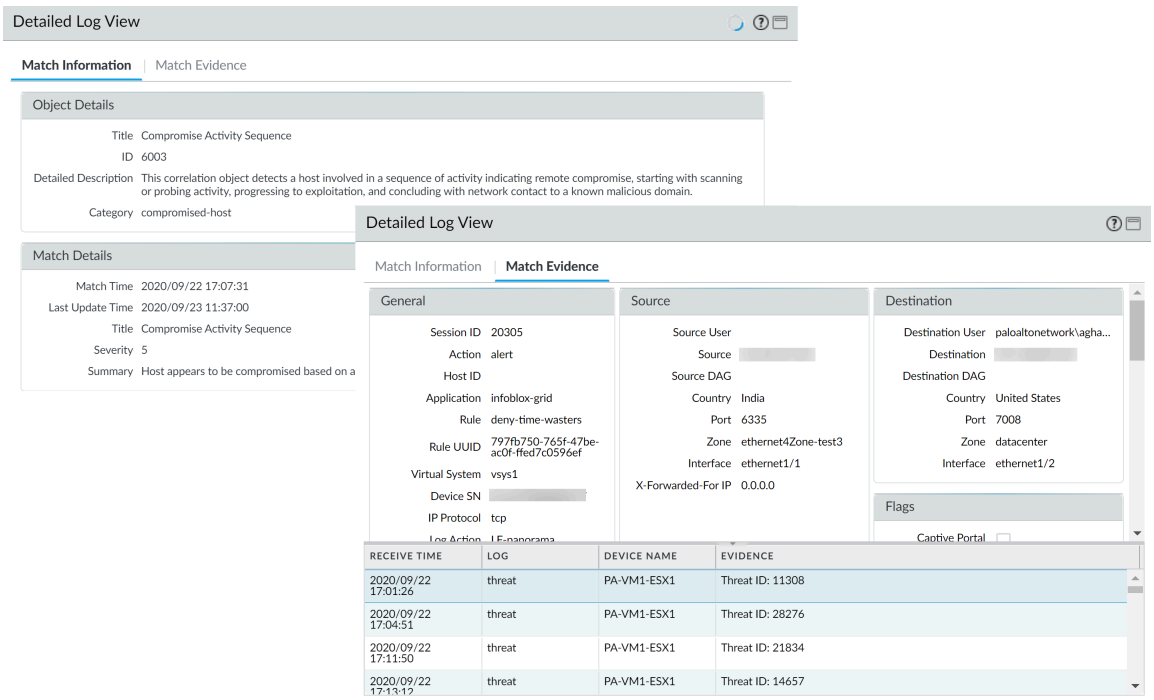
關聯的事件 包含下列詳細資料：

欄位	說明
比對時間	關聯物件觸發比對的時間。
更新時間	事件上次更新比對證據的時間。防火牆收集關聯物件中定義之模式或事件順序的證據時，系統會更新關聯的事件日誌上的時間戳記。
物件名稱	觸發比對的關聯物件名稱。
來源位址	網路上流量來源使用者/裝置的 IP 位址。
來源使用者	如果已啟用 使用者-ID，則為來自目錄伺服器的使用者和使用者群組資訊。
severity	表示比對急迫性和影響的評等。嚴重性等級可表示損害範圍或升級模式，以及發生頻率。由於關聯物件主要用於偵測威脅，因此關聯的事件一般與識別網路上的受危害主機相關，而嚴重性具有下列意涵：

©2024 Palo Alto Networks, Inc.

欄位	說明
若要設定防火牆或 *Panorama*，以針對所需的嚴重性等級使用電子郵件、*SNMP* 或 *syslog* 訊息傳送警示，請參閱 使用外部服務進行監控。	• 關鍵—根據表示升級模式的關聯事件，確認主機已受危害。例如，主機收到 WildFire 裁定為惡意的檔案，且該檔案出現在 WildFire 沙箱中針對該惡意檔案觀察到的命令與控制項活動時，便會記錄關鍵事件。 • 高—表示根據多個威脅事件的關聯，主機非常可能已受危害，例如在網路上隨處偵測到的惡意軟體與從特定主機產生的命令與控制項活動相符。 • 中—表示根據對一或多個可疑事件的偵測，主機可能已受危害，例如重複造訪建議指令碼化之命令與控制項活動的已知惡意 URL。 • 低 — 表示根據對一或多個可疑事件的偵測，主機可能已受危害，例如造訪惡意 URL 或動態 DNS 網域。 • 資訊—偵測到在彙總後可能對識別可疑活動有用的事件，但事件本身不一定具有重大意義。
Summary	概述關聯事件所收集證據的說明。

按一下 圖示可查看詳細的日誌檢視，其包含所有比對證據：

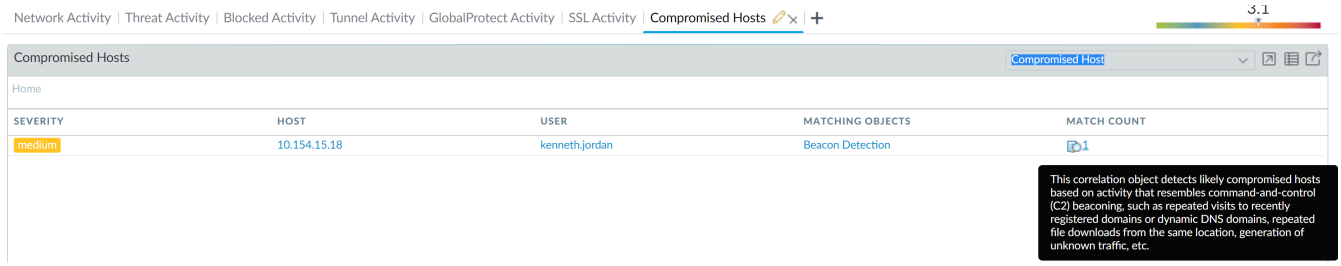


 ©2024 Palo Alto Networks, Inc.

頁籤	說明
比對資訊	物件詳細資料：呈現觸發比對的 關聯物件 資訊。
	比對詳細資料：比對詳細資料摘要，包括比對時間、在比對證據上的上次更新時間、事件嚴重性以及事件摘要。
比對證據	呈現所有證實關聯事件的證據。它列出各工作階段所收集證據的詳細資訊。

使用 ACC 中之受危害的主機 Widget

ACC > Threat Activity（威脅活動）上受危害的主機 Widget 會彙總關聯的事件，並將其依嚴重性排序。其會顯示觸發事件的來源 IP 位址/使用者、相符的關聯物件和物件相符次數。使用比對計數連結跳至比對證據詳細資料。



如需詳細資料，請參閱使用自動關聯引擎與使用應用程式控管中心。

©2024 Palo Alto Networks, Inc.

獲得封包擷取

所有 Palo Alto Networks 防火牆都可讓您執行在防火牆上周遊管理介面和網路介面之流量的封包擷取 (pcaps)。對資料平面執行封包擷取時，您可能需要停用硬體卸載以確保防火牆擷取所有流量。

封包擷取需要大量 *CPU*，且可能導致防火牆效能降級。請只在需要時使用此功能，並確保在收集到所需封包之後關閉此功能。

- 封包擷取的類型
- 停用硬體卸載
- 執行自訂封包擷取
- 執行威脅封包擷取
- 執行應用程式封包擷取
- 針對管理介面執行封包擷取

封包擷取的類型

根據需要執行的動作，您可以啟用以下不同類型的封包擷取：

- 自訂封包擷取—防火牆會針對所有流量或根據您定義的篩選器針對特定流量擷取封包。例如，您可以將防火牆設定為僅擷取進入或離開特定來源、目的地 IP 位址或連接埠的封包。然後您可以使用封包擷取來疑難排解網路相關問題或收集應用程式屬性，以讓您編寫自訂應用程式特徵碼或向 Palo Alto Networks 要求應用程式特徵碼。請參閱 執行自訂封包擷取。
- 威脅封包擷取—防火牆會在偵測到病毒、間諜軟體或漏洞時擷取封包。您在防毒軟體、反間諜軟體及弱點保護安全性設定檔中啟用此功能。檢視或匯出封包擷取的連結會顯示在威脅日誌的第二欄中。這些封包擷取提供威脅內容資訊以協助您判斷攻擊是否成功，或進一步瞭解攻擊者採用的方式。如果您認為其為誤判或誤否定，您也可以將此類型的 pcap 提交至 Palo Alto Networks 以重新分析威脅。請參閱 執行威脅封包擷取。
- 應用程式封包擷取—防火牆會根據您定義的特定應用程式和篩選器擷取封包。檢視或匯出封包擷取的連結會顯示在符合封包擷取規則之流量的威脅日誌第二欄中。請參閱 執行應用程式封包擷取。
- 管理介面封包擷取—防火牆在管理介面 (MGT) 上擷取封包。疑難排解周遊介面的服務（例如，外部驗證服務 的防火牆管理驗證、軟體和內容更新、日誌轉送、與 SNMP 伺服器通訊，以及 GlobalProtect 和驗證入口網站的驗證要求）時，封包擷取非常實用。請參閱 針對管理介面執行封包擷取。
- **GTP** 事件封包擷取—防火牆擷取單一 GTP 事件，例如 GTP-in-GTP、一般使用者 IP 詐騙和異常 GTP 訊息，以便行動網路營運商能夠更輕鬆地進行 GTP 疑難排解。在行動網路保護設定檔中啟用封包擷取。

©2024 Palo Alto Networks, Inc.

停用硬體卸載

由資料平面 CPU 負責擷取通過 Palo Alto Networks 防火牆網路資料連接埠的流量封包。若要擷取通過管理介面的流量，必須針對管理介面執行封包擷取，在此種情況下，在管理平面上執行封包擷取。

在資料平面上執行封包擷取時，與防火牆、丟棄以及輸出擷取階段相比，輸入階段中封包擷取篩選器的使用方式會有所不同。輸入階段使用封包擷取篩選器，將與篩選器相符的單個封包複製到擷取檔案。在封包剖析檢查中失敗的封包在擷取前會予以丟棄。防火牆、丟棄以及輸出擷取階段使用相同的封包擷取篩選器，標記所有與篩選器相符的新工作階段。由於各個工作階段（如在工作階段表格中記錄的一樣）會識別用戶端至伺服器的連線以及伺服器至用戶端的連線，因此任何與旗標工作階段相符的任一方向上的流量，將會複製到防火牆階段以及傳輸階段的擷取檔案。同樣地，任何與旗標工作階段相符的任一方向上的丟棄流量（接收後的階段）將會複製到丟棄階段的擷取檔案。

在配備網路處理器的防火牆型號上，與 Palo Alto Networks 預先確定的特定準則相符的流量，可能會進行卸載，由網路處理器進行處理。此類卸載流量不會傳送至資料平面 CPU，因此不會進行擷取。若要擷取卸載流量，必須使用 CLI 關閉硬體卸載功能。

常見的可能會卸載的流量類型包括非解密 SSL 與 SSH 流量（加密後無法進行有效檢查，是否超出初始 SSL/SSH 工作階段設定）、網路通訊協定（例如 OSPF、BGP、RIP）以及與應用程式取代原則相符的流量。系統無法卸載某些類型的流量，例如 ARP、所有非 IP 流量、IPSec 以及 VPN 工作階段。系統無法卸載單個 SYN、FIN 以及 RST 封包（即使是包含已卸載工作階段流量的此類封包），此類封包經網路處理器識別後，始終會通向資料平面 CPU。

下列防火牆支援硬體卸載：*PA-3200* 系列、*PA-5200* 系列、*PA-5450* 和 *PA-7000* 系列防火牆。

停用硬體卸載可能會增加資料平面 *CPU* 使用率。如果資料平面 *CPU* 使用率已非常高，停用硬體卸載之前，您可能需要排程維護窗口。

STEP 1 | 執行下列 CLI 命令以停用硬體卸載：

```
admin@PA-7050>set session offload no
```

STEP 2 | 防火牆擷取所需流量之後，請執行下列 CLI 命令以啟用硬體卸載：

```
admin@PA-7050>set session offload yes
```

執行自訂封包擷取

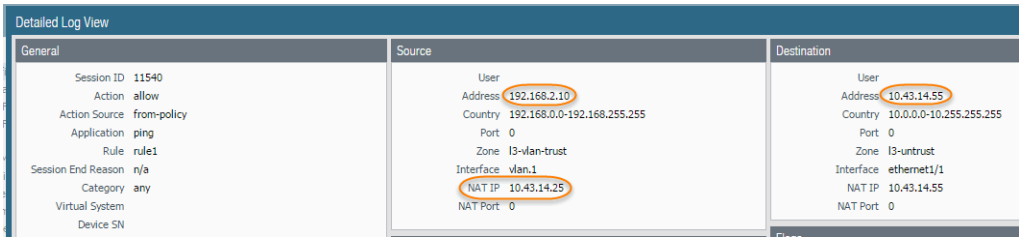
自訂封包擷取可讓您定義防火牆擷取的流量。若要確保擷取所有流量，您可能需要停用硬體卸載。

STEP 1 | 在您開始執行封包擷取之前，請識別要擷取的流量屬性。

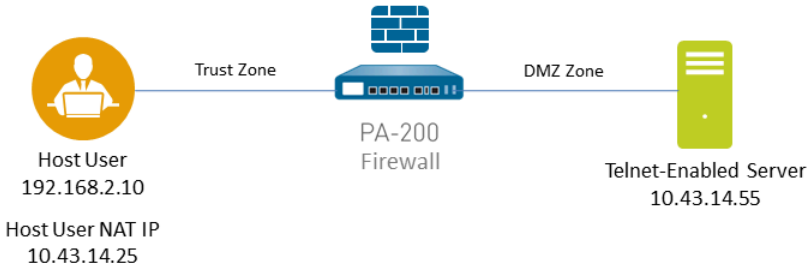
例如，若要決定兩個系統之間流量的來源 IP 位址、來源 NAT IP 位址和目的地 IP 位址，請執行從來源系統到目的地系統的 ping。ping 完成之後，請前往 **Monitor**（監控） > **Traffic**（流

©2024 Palo Alto Networks, Inc.

量），並找到兩個系統的流量日誌。按一下位於日誌第一欄的 **Detailed Log View**（詳細記錄檢視）圖示，並記下來源位址、來源 NAT IP 和目的地位址。



在下列範例介紹了如何使用封包擷取，對從信任區域中之使用者到 DMZ 區域中之伺服器的 Telnet 連線問題進行疑難排解。



 ©2024 Palo Alto Networks, Inc.

STEP 2 | 設定封包擷取篩選器，讓防火牆僅擷取所需流量。

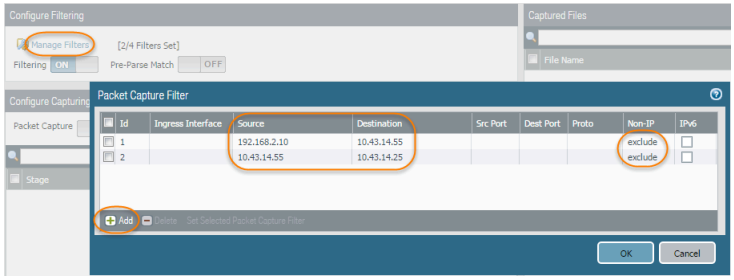
使用這些篩選器可讓您在封包擷取中輕鬆找到所需的資訊，並減少防火牆獲得封包擷取所需的處理能力。若要擷取所有流量，請勿定義篩選器並將篩選器選項保留為關閉。

例如，如果您已在防火牆上設定 NAT，則必須套用兩個篩選器。第一個篩選器會篩選指向目的地 IP 位址的預先 NAT 來源 IP 位址，而第二個篩選器會篩選從目的地伺服器到來源 NAT IP 位址的流量。

1. 選取 **Monitor**（監控） > **Packet Capture**（封包擷取）。
2. 按一下視窗底端的 **Clear All Settings**（清除所有設定）以清除任何現有擷取設定。
3. 按一下 **Manage Filters**（管理篩選器），然後按一下 **Add**（新增）。
4. 選取 **Id** 1，然後在 **Source**（來源）欄位中輸入所需來源 IP 位址，並在 **Destination**（目的地）欄位中輸入目的地 IP 位址。

   例如，輸入來源 IP 位址 **192.168.2.10** 和目的地 IP 位址 **10.43.14.55**。若要進一步篩選擷取，請將 **Non-IP**（非 **IP**）設定為 **exclude**（排除）非 IP 流量，例如廣播流量。
5. **Add**（新增）第二個篩選器，然後選取 **Id** 2。

   例如，在 **Source**（來源）欄位中輸入 **10.43.14.55**，然後在 **Destination**（目的地）欄位中輸入 **10.43.14.25**。在 **Non-IP**（非 **IP**）下拉式功能表中，選取 **exclude**（排除）。



6. 按一下 **OK**（確定）。

STEP 3 | 將 **Filtering**（篩選）設定為 **On**（開啟）。

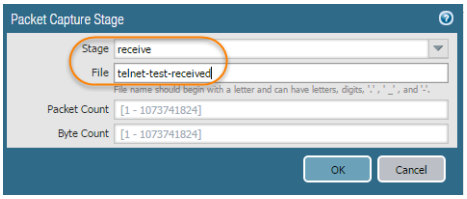
©2024 Palo Alto Networks, Inc.

STEP 4 | 指定觸發封包擷取的流量階段，以及要用於儲存擷取內容的檔案名稱。針對每個階段的定義，按一下封包擷取頁面上的 **Help**（說明）圖示。

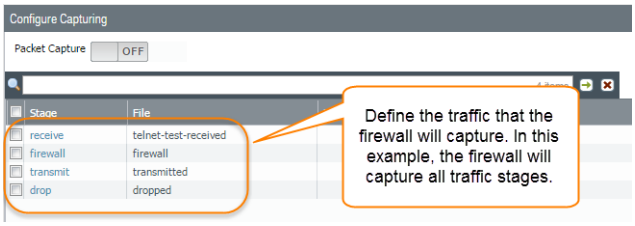
例如，若要設定所有封包擷取階段和定義每個階段的檔案名稱，請執行下列程序：

1. 將 **Stage**（階段）**Add**（新增）至封包擷取設定，並針對產生的封包擷取定義 **File**（檔案）名稱。

   例如，選取 **receive**（接收）作為 **Stage**（階段），然後將 **File**（檔案）名稱設定為 telnet-test-received。

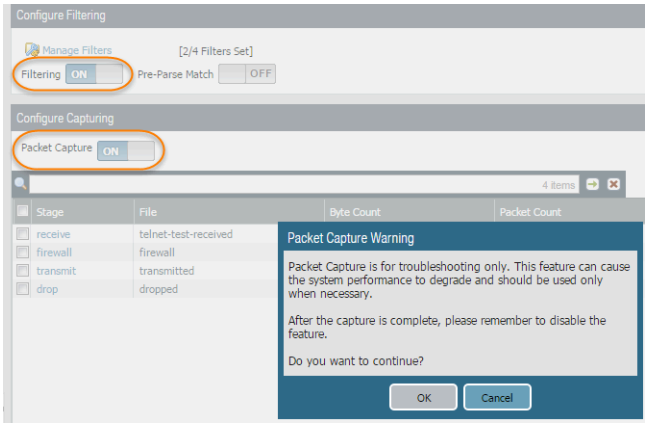


2. 繼續 **Add**（新增）每個要擷取的 **Stage**（階段）（**receive, firewall**（接收、防火牆）、**transmit**（傳輸）和 **drop**（丟棄）），然後為每個階段設定唯一 **File**（檔案）名稱。



STEP 5 | 將 **Packet Capture**（封包擷取）設定為 **ON**（開啟）。

防火牆或裝置將警告您系統效能可能會降低；按一下 **OK**（確定）以確認警告。如果您定義篩選器，封包擷取應該會稍微影響效能，但防火牆擷取要分析的資料之後，您應該一律 **Off**（關閉）封包擷取。



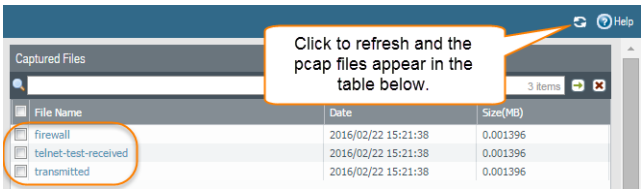
 ©2024 Palo Alto Networks, Inc.

STEP 6 | 產生符合已定義之篩選器的流量。

針對此範例，請從來源系統（192.168.2.10）執行下列命令，以產生從來源系統到已啟用 Telnet 之伺服器的流量：

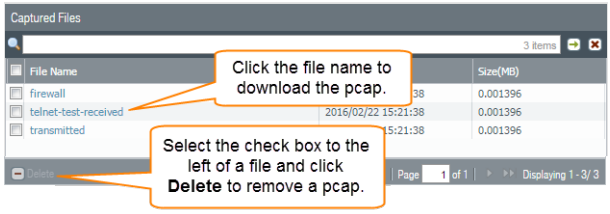
```
telnet 10.43.14.55
```

STEP 7 | **OFF**（關閉）封包擷取，然後按一下重新整理圖示以查看封包擷取檔案。



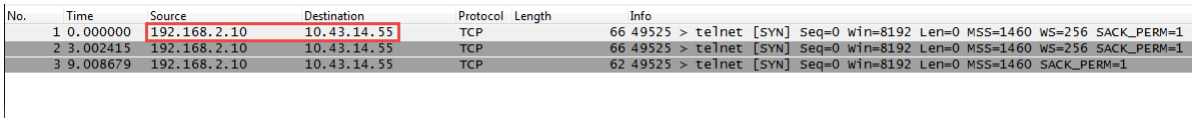
請注意，在此狀況下沒有丟棄的封包，因此防火牆不會建立丟棄階段的檔案。

STEP 8 | 按一下（檔案名稱）欄中的檔案名稱以下載封包擷取。



STEP 9 | 使用網路封包分析器檢視封包擷取檔案。

在此範例中，received.pcap 封包擷取會顯示從來源系統 192.168.2.10 到已啟用 Telnet 之伺服器 10.43.14.55 的失敗 Telnet 工作階段。來源系統已將 Telnet 要求傳送至伺服器，但伺服器並未回應。在此範例中，伺服器可能未啟用 Telnet，因此請查看伺服器。



STEP 10 | 在目的地伺服器 (10.43.14.55) 上啟用 Telnet 服務，並開啟封包擷取以執行新的封包擷取。

STEP 11 | 產生會觸發封包擷取的流量。

再次執行從來源系統到已啟用 Telnet 之伺服器的 Telnet 工作階段

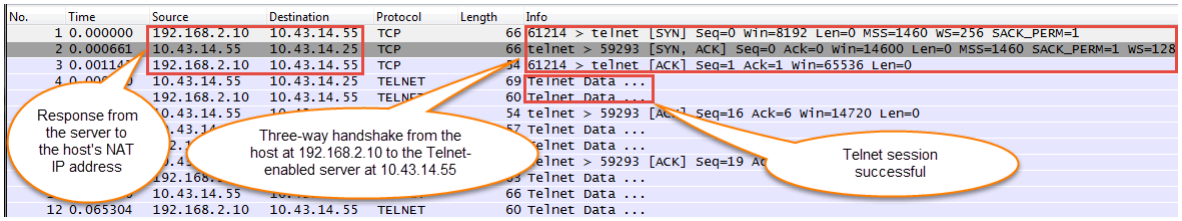
```
telnet 10.43.14.55
```

 ©2024 Palo Alto Networks, Inc.

STEP 12 | 下載並開啟 received.pcap 檔案，然後使用網路封包分析器檢視該檔案。

現在下列封包擷取會顯示從主機使用者 192.168.2.10 到已啟用 Telnet 之伺服器 10.43.14.55 的成功 Telnet 工作階段。

您也會看到 *NAT* 位址 *10.43.14.25*。伺服器回應時，其也會回應 *NAT* 位址。如主機和伺服器之間的三方交握所表示，您可以看到工作階段已成功，然後您會看到 *Telnet* 資料。



執行威脅封包擷取

若要設定防火牆以在偵測到威脅時執行封包擷取 (pcap)，請針對防毒、反間諜軟體和漏洞保護安全性設定檔啟用封包擷取。

STEP 1 | 在安全性設定檔中啟用封包擷取選項。

某些安全性設定檔可讓您定義單一封包擷取或延伸擷取。如果您選擇延伸擷取，請定義擷取長度。這可讓防火牆擷取更多封包，以提供與威脅相關的其他內容。

如果對給定威脅的動作為允許，則防火牆不會觸發威脅日誌，且不會擷取封包。如果動作為警示，您可以將封包擷取設定為單一封包或延伸擷取。所有封鎖動作（丟棄、封鎖和重設動作）都會擷取單一封包。裝置上的內容套件確定預設動作。

1. 選取 **Objects**（物件） > **Security Profiles**（安全性設定檔），然後針對支援的設定檔啟用封包擷取選項，如下所示：
   - 防毒—選取自訂防毒設定檔，然後在 **Antivirus**（防毒）頁籤中，選取 **Packet Capture**（封包擷取）核取方塊。
   - 反間諜軟體 — 選取自訂反間諜軟體設定檔，按一下 **Signature Policies**（特徵碼政策）、**Signature Exceptions**（特徵碼例外）或 **DNS Policies**（**DNS** 政策）頁簽，在封

©2024 Palo Alto Networks, Inc.

包擷取下拉式清單中，選擇 **single-packet**（單一封包）或 **extended-capture**（延伸擷取）。

> ***Signature Policies***（特徵碼政策）封包擷取適用於跨指定類別或匹配威脅名稱的多個特徵碼，而 ***Signature Exceptions***（特徵碼例外）封包擷取適用於特定特徵碼。

- 漏洞保護—選取自訂弱點保護設定檔，然後在 **Rules**（規則）頁籤中，按一下 **Add**（新增）以新增規則或選取現有規則。將 **Packet Capture**（封包擷取）設定為 **single-packet**（單一封包）或 **extended-capture**（延伸擷取）。

> 如果設定檔具有已定義的特徵碼例外狀況，請按一下 ***Exceptions***（例外）頁籤，然後在 ***Packet Capture***（封包擷取）欄中，針對特徵碼設定 ***single-packet***（單一封包）或 ***extended-capture***（延伸擷取）。

2. （選用）如果您已針對任何設定檔選取 **extended-capture**（延伸擷取），請定義延伸封包擷取長度。
   1. 選取 **Device**（裝置） > **Setup**（設定） > **Content-ID**，然後編輯 Content-ID Settings（Content-ID 設定）。
   2. 在 **Extended Packet Capture Length**（**packets**）（延伸封包擷取長度（封包））區段中，指定防火牆擷取的封包數（範圍是 1-50；預設值是 5）。
   3. 按一下 **OK**（確定）。

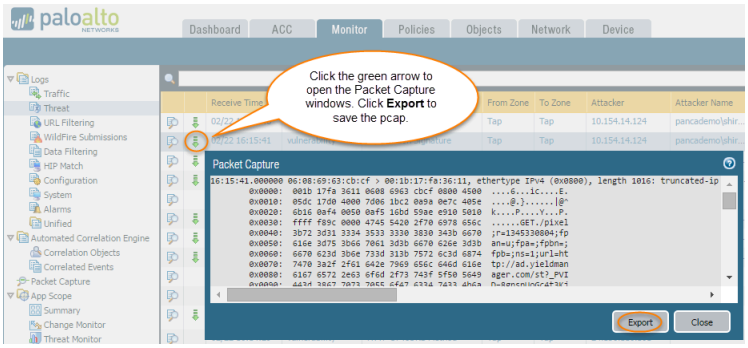
STEP 2 | 將（已啟用封包擷取的）安全性設定檔新增至安全性原則規則。

1. 選取 **Policies**（原則） > **Security**（安全性），然後選取規則。
2. 選取 **Actions**（動作）頁籤。
3. 在（設定檔設定）區段中，選取已啟用封包擷取的設定檔。

   例如，按一下 **Antivirus**（防毒）下拉式清單，然後選取已啟用封包擷取的設定檔。

STEP 3 | 從威脅日誌檢視/匯出封包擷取。

1. 選取 **Monitor**（監控） > **Logs**（日誌） > **Threat**（威脅）。
2. 在所需的日誌項目中，按一下第二欄中的綠色封包擷取圖示 。直接檢視封包擷取或將其 **Export**（匯出）至您的系統。



 ©2024 Palo Alto Networks, Inc.

執行應用程式封包擷取

下列主題說明您可以用於設定防火牆以執行應用程式封包擷取的兩種方法：

- 針對未知應用程式執行封包擷取
- 執行自訂應用程式封包擷取

針對未知應用程式執行封包擷取

Palo Alto Networks 防火牆會針對包含防火牆無法識別之應用程式的工作階段，自動產生封包擷取。一般而言，系統只會將沒有 App-ID 特徵碼的市售應用程式、網路上的內部或自訂應用程式，或潛在威脅分類為未知流量（tcp、udp 或 non-syn-tcp）。您可以使用這些封包擷取來收集與未知應用程式相關的更多內容，或使用該資訊來分析流量或潛在威脅。您也可以透過安全性原則控制自訂或未知的應用程式，或編寫自訂應用程式特徵碼，然後根據自訂特徵碼建立安全性原則，以管理自訂或未知的應用程式。如果該應用程式為市售應用程式，您可以將封包擷取提交至 Palo Alto Networks 以建立 App-ID 特徵碼。

STEP 1 | 確認已啟用未知應用程式封包擷取（此選項依預設已啟用）。

1. 若要檢視未知應用程式擷取設定，請執行下列 CLI 命令：

```
admin@PA-220>show running application setting | match “Unknown
 capture”
```

2. 如果未知擷取設定選項已關閉，請將其啟用：

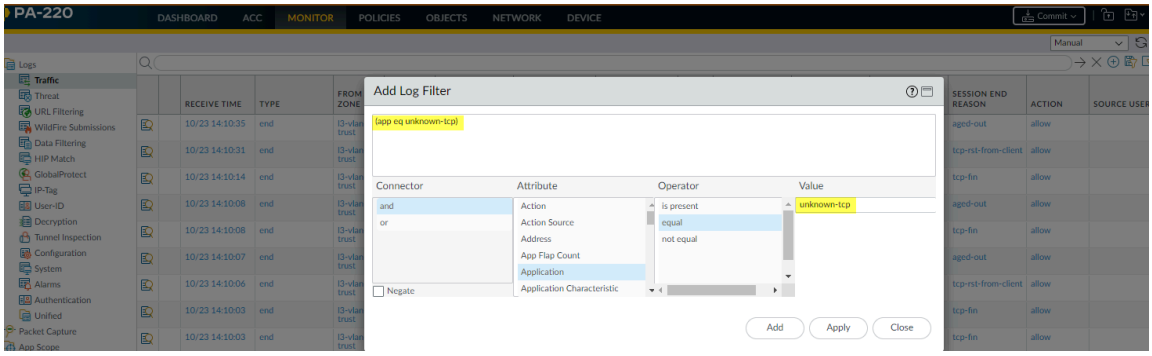
```
admin@PA-220>set application dump-unknown yes
```

STEP 2 | 篩選流量日誌以找到未知的 TCP 和 UDP 應用程式。

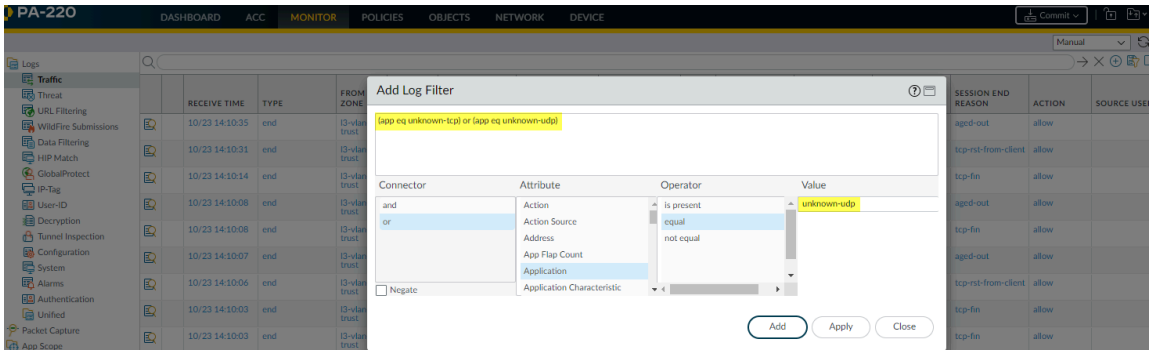
1. 選取**Monitor**（監控） > **Logs**（日誌） > **Traffic**（流量）。
2. 按一下 **Add Filter**（新增篩選器），建立篩選器的未知 TCP 部分（**Connector**（連接器）= “and”，**Attribute**（屬性）= “Application”，**Operator**（運算子）= “equal”，然

©2024 Palo Alto Networks, Inc.

後輸入“unknown-tcp”作為 **Value**（值）），然後按一下 **Add**（新增）以新增查詢到篩選器。

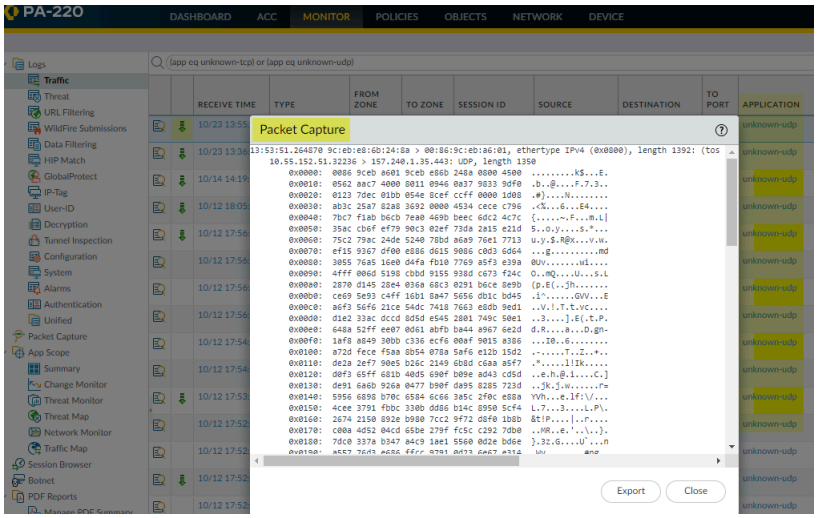


3. 建立篩選器的未知 UDP 部分（**Connector**（連接器）= “or”，**Attribute**（屬性）= “Application”，**Operator**（運算子）= “equal”，然後輸入“unknown-udp”作為 **Value**（值）），然後按一下 **Add**（新增）以新增查詢到篩選器。



4. 按一下 **Apply**（套用）以替換日誌螢幕查詢欄位中的篩選器。

STEP 3 | 按一下查詢欄位旁邊的 **Apply Filter**（套用篩選器）箭頭以執行篩選器，然後按一下封包擷取圖示 以檢視封包擷取或將其 **Export**（匯出）至您的本機系統。



©2024 Palo Alto Networks, Inc.

執行自訂應用程式封包擷取

您可以設定 Palo Alto Networks 防火牆以根據您定義的應用程式名稱和篩選器獲得封包擷取。然後您可以使用封包擷取疑難排解與控制應用程式相關的問題。設定應用程式封包擷取時，您必須使用 App-ID 資料庫中定義的應用程式名稱。您可使用 Applipedia 或透過防火牆網頁介面的 **Objects**（物件）> **Applications**（應用程式），檢視所有 App-ID 應用程式的清單。

STEP 1 | 使用終端機模擬應用程式（例如 PuTTY）時，請啟動防火牆的 SSH 工作階段。

STEP 2 | 開啟應用程式封包擷取並定義篩選器。

```
admin@PA-220>set application dump on application <application-name>
 rule <rule-name>
```

例如，若要針對 linkedin-base 應用程式擷取符合名為 Social Networking Apps 之安全性規則的封包，請執行下列 CLI 命令：

```
admin@PA-220>set application dump on application linkedin-base rule
 "Social Networking Apps"
```

您也可以套用其他篩選器，例如來源 *IP* 位址和目的地 *IP* 位址。

STEP 3 | 檢視封包擷取輸出，以確保已套用正確的篩選器。輸出在您啟用封包擷取後顯示。

以下輸出確認針對符合 Social Networking Apps 規則之流量的應用程式擷取篩選現在基於 linkedin-base 應用程式進行。

```
Application setting:
Application cache              : yes
Supernode                      : yes
Heuristics                     : yes
Cache Threshold                : 16
Bypass when exceeds queue limit: no
Traceroute appid               : yes
Traceroute TTL threshold       : 30
Use cache for appid            : no
Use simple appsigs for ident   : yes
Use AppID cache on SSL/SNI     : no
Unknown capture                : on
Max. unknown sessions          : 5000
Current unknown sessions       : 7
Application capture            : on
Max. application sessions      : 5000
Current application sessions   : 0
Application filter setting:
    Rule                       : Social Networking Apps
    From                       : any
    To                         : any
    Source                     : any
    Destination                : any
    Protocol                   : any
    Source Port                : any
    Dest. Port                 : any
    Application                : linkedin-base

Current APPID Signature
   Memory Usage                : 16768  KB (Actual 16440  KB)
      TCP 1 C2S                : regex 11898  states
      TCP 1 S2C                : regex 4549   states
      UDP 1 C2S                : regex 4234   states
      UDP 1 S2C                : regex 1605   states

Alternate APPID Signature
   Memory Usage                : 16768  KB (Actual 16425  KB)
      TCP 1 C2S                : regex 11878  states
      TCP 1 S2C                : regex 4549   states
      UDP 1 C2S                : regex 4233   states
      UDP 1 S2C                : regex 1604   states
```

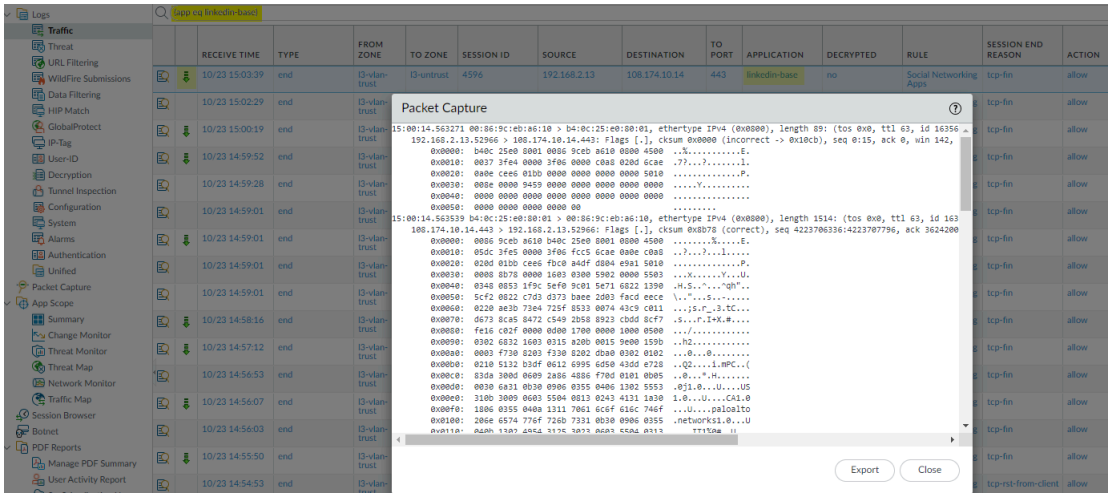
STEP 4 | 從 Web 瀏覽器存取 linkedin.com 並執行一些 LinkedIn 工作以產生 LinkedIn 流量，然後執行以下 CLI 命令以關閉應用程式封包擷取：

```
admin@PA-220>set application dump off
```


©2024 Palo Alto Networks, Inc.

STEP 5 | 檢視/匯出封包擷取。

1. 登入防火牆上的網頁介面，然後選取 **Monitor**（監控） > **Logs**（日誌） > **Traffic**（流量）。
2. 在感興趣的日誌項目中，按一下綠色封包擷取圖示 。
3. 直接檢視封包擷取或將其 **Export**（匯出）至您的電腦。下列螢幕擷取畫面顯示 linkedin-base 封包擷取。



針對管理介面執行封包擷取

tcpdump CLI 命令可讓您擷取在 Palo Alto Networks 防火牆上周遊管理介面（MGT）的封包。

每個平台都具有 ***tcpdump*** 擷取的預設位元組數。*PA-220* 防火牆會從每個封包和任何截斷的項目擷取 *68* 位元組的資料。*PA-7000* 系列防火牆和 *VM* 系列防火牆會從每個封包擷取 *96* 個位元組的資料。若要定義 ***tcpdump*** 擷取的封包數，請使用 ***snaplen***（貼齊長度）選項（範圍 *0-65535*）。將 ***snaplen*** 設定為 *0* 會造成防火牆使用擷取整個封包所需的最大長度。

STEP 1 | 使用終端機模擬應用程式（例如 PuTTY）時，請啟動防火牆的 SSH 工作階段。

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 若要針對 MGT 介面開始執行封包擷取，請執行下列命令：

```
admin@PA-220>tcpdump filter “<filter-option> <IP-address>” snaplen
 length
```

例如，若要擷取管理員驗證使用 RADIUS 的防火牆時產生的流量，請篩選 RADIUS 伺服器的目的地 IP 位址（在此範例中為 10.5.104.99）：

```
admin@PA-220>tcpdump filter “dst 10.5.104.99” snaplen 0
```

您也可以篩選 src（來源 IP 位址）、host 和 net，以及排除內容。例如，若要針對子網路進行篩選，並排除所有 SCP、SFTP 和 SSH 流量（這些流量使用連接埠 22），請執行下列命令：

```
admin@PA-220>tcpdump filter “net 10.5.104.0/24 and not port 22”
 snaplen 0
```

每次 ***tcpdump*** 執行封包擷取時，都會將內容儲存於名為 *mgmt.pcap* 的檔案。每次執行 ***tcpdump*** 時，系統都會覆寫此檔案。

STEP 3 | 所需流量周遊 MGT 介面之後，請按下 Ctrl + C 以停止擷取。

STEP 4 | 執行下列命令以檢視封包擷取：

```
admin@PA-220> view-pcap mgmt-pcap mgmt.pcap
```

下列輸出顯示從 MGT 連接埠 (10.5.104.98) 到 RADIUS 伺服器 (10.5.104.99) 的封包擷取：

```
09:55:29.139394 IP 10.5.104.98.43063 > 10.5.104.99.radius:RADIUS,
 Access Request (1), id:0x00 length:89 09:55:29.144354 arp reply
 10.5.104.98 is-at 00:25:90:23:94:98 (oui Unknown) 09:55:29.379290
 IP 10.5.104.98.43063 > 10.5.104.99.radius:RADIUS, Access Request
 (1), id:0x00 length:70 09:55:34.379262 arp who-has 10.5.104.99
 tell 10.5.104.98
```


©2024 Palo Alto Networks, Inc.

STEP 5 | （選用）使用 SCP （或 TFTP）從防火牆匯出封包擷取。例如，若要使用 SCP 匯出封包擷取，請執行下列命令：

```
admin@PA-220>scp export mgmt-pcap from mgmt.pcap
 to <username@host:path>
```

例如，若要將 pcap 匯出至已啟用 SCP 的伺服器 10.5.5.20 中名為 temp-SCP 的暫存資料夾，請執行下列 CLI 命令：

```
admin@PA-220>scp export mgmt-pcap from mgmt.pcap to
 admin@10.5.5.20:c:/temp-SCP
```

在 SCP 伺服器上輸入帳戶的登入名稱和密碼，以讓防火牆將封包擷取複製到已啟用 SCP 的伺服器中的 c:\temp-SCP 資料夾。

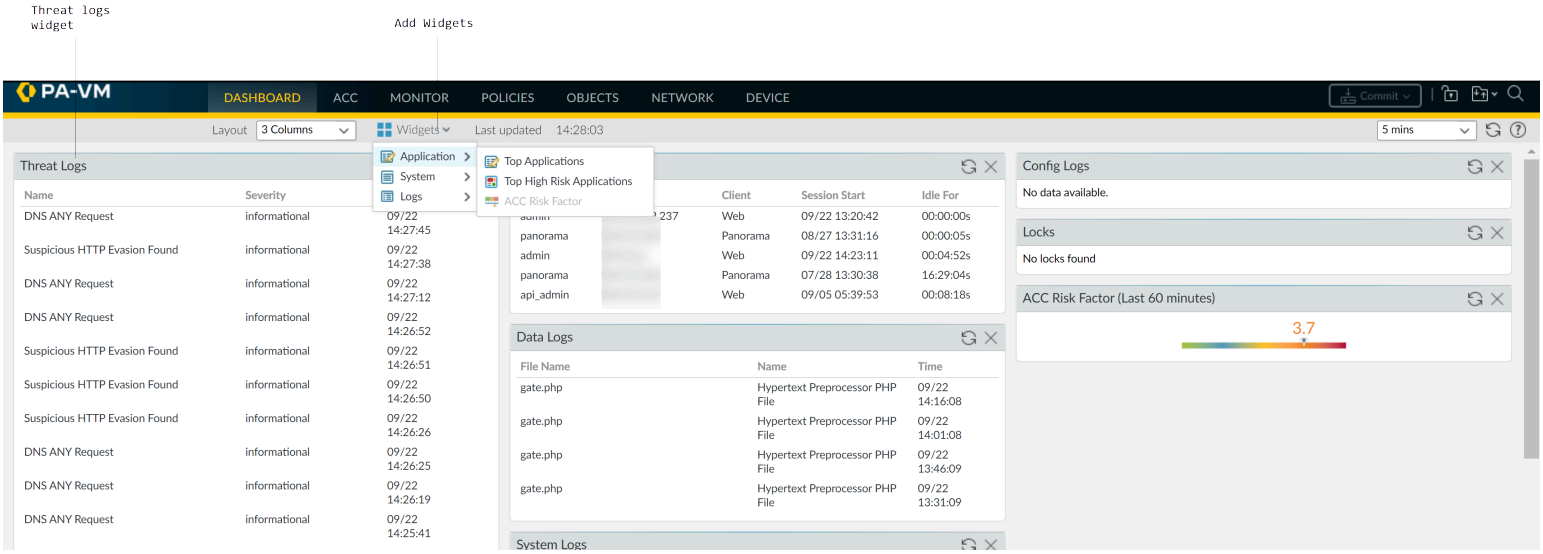
STEP 6 | 您現在可以使用網路封包分析器（例如 Wireshark）檢視封包擷取檔案。

©2024 Palo Alto Networks, Inc.

監控應用程式及威脅

所有 Palo Alto Networks 的新世代防火牆都配備 App-ID 技術，不論使用何種通訊協定、加密或規避行為，其都可識別在您網路上周遊的應用程式。接著您可使用應用程式控管中心來監控應用程式。ACC 會以圖形方式摘要來自各種日誌資料庫的資料，以反白顯示在您網路上周遊的應用程式、該程式的使用者及其潛在的安全性影響。ACC 會使用 App-ID 執行的連續流量分類進行動態更新；如果應用程式變更連接埠或行為，App-ID 將持續監控流量，並在 ACC 中顯示結果。其他 URL 類別、威脅及資料的可見度可提供完整且全面的網路活動圖。您可以使用 ACC 非常快速地深入瞭解周遊網路的流量，然後將此資訊轉換為更詳實的安全性原則

您也可以使用儀表板來監控網路。



檢閱內容傳送網路基礎結構，檢查防火牆上記錄的事件是否會造成安全性風險。AutoFocus 情報摘要顯示了與網路中、在全域範圍內的日誌關聯的屬性、活動或行為，以及與它們關聯的 WildFire 裁定與 AutoFocus 標籤。透過作用中 AutoFocus 訂閱，您可使用此資訊來建立追蹤網路上的特定威脅的自訂 AutoFocus 警示。

©2024 Palo Alto Networks, Inc.

檢視和管理日誌

日誌是一個自動產生、帶時間戳記的檔案，為防火牆上的系統事件以及防火牆監控的網路流量事件提供稽核記錄。日誌項目包含構件，即與記錄事件關聯的屬性、活動或行為，例如應用程式類型或攻擊者的 IP 位址。每種日誌類型會記錄單獨事件類型的資訊。例如，防火牆會產生一個威脅日誌，其中記錄防火牆上符合間諜軟體、漏洞或病毒特徵碼或符合為連接埠掃描或主機掃描活動所設臨界值的 DoS 攻擊的流量。

- 日誌類型與嚴重性等級
- 檢視日誌
- 篩選器日誌
- 匯出日誌
- 設定日誌儲存配額和到期時間
- 排程將日誌匯出至 SCP 或 FTP 伺服器

日誌類型與嚴重性等級

您可以在 **Monitor**（監控） > **Logs**（日誌）頁面中檢視以下日誌類型。

- 流量日誌
- 威脅日誌
- URL 篩選日誌
- WildFire 提交日誌
- 資料過濾日誌
- 關聯日誌
- 通道檢查日誌
- 設定日誌
- 系統日誌
- HIP 比對日誌
- GlobalProtect 日誌
- IP-Tag 日誌
- User-ID 日誌
- 解密日誌
- 警告日誌
- 驗證日誌
- 統一日誌

©2024 Palo Alto Networks, Inc.

流量日誌

流量日誌會顯示一個有關每個工作階段開始與結束的項目。每個項目都包括以下資訊：日期與時間；來源與目的地區域、來源和目的地動態位址群組、位址與連接埠；應用程式名稱；套用至流量的安全性規則；規則動作（允許、拒絕或丟棄）；輸入和輸出介面；位元組數；以及工作階段結束原因。

僅當流量符合的規則包括動態位址群組時，動態位址群組才會出現在日誌中。如果一個 *IP* 位址出現在多個動態位址群組中，則防火牆在日誌中最多顯示五個動態位址群組以及來源 *IP* 位址

Type（類型）欄表示項目是否關於工作階段開始或結束。Action（動作）欄表示防火牆是否允許、拒絕或丟棄工作階段。丟棄表示封鎖流量的安全性規則指定任何應用程式，而拒絕則表示規則識別特定應用程式。如果防火牆在識別應用程式之前丟棄流量，例如當規則丟棄特定服務的所有流量時，應用程式欄會顯示「不可應用」。

按一下項目旁邊的 以檢視有關工作階段的其他詳細資訊，例如 ICMP 項目是否在相同來源與目的地之間彙總多個工作階段（在此情況下，Count（計數）欄值將大於一）。

當 *PAN-OS 11.0* 中引入的解密日誌停用時，防火牆會傳送 *HTTP/2* 日誌作為流量日誌。但是，啟用解密日誌時，防火牆將 *HTTP/2* 日誌作為通道檢查日誌傳送（停用解密日誌時，*HTTP/2* 日誌作為流量日誌傳送），因此您需要查看通道檢查日誌而不是流量日誌來瞭解 *HTTP/2* 事件。

威脅日誌

威脅日誌會在流量符合附加至防火牆上安全性規則的安全性設定檔之一時顯示項目。每個項目包括以下資訊：日期與時間；威脅類型（例如病毒或間諜軟體）；威脅說明或 URL（名稱欄）；來源與目的地區域、位址、來源和目的地動態位址群組以及連接埠；應用程式名稱；警報動作（例如允許或封鎖）；以及嚴重性等級。

僅當流量符合的規則包括動態位址群組時，動態位址群組才會出現在日誌中。如果一個 *IP* 位址出現在多個動態位址群組中，則防火牆在日誌中最多顯示五個動態位址群組以及來源 *IP* 位址

若要查看個別威脅日誌項目的更多詳細資訊：

- 按一下威脅項目旁邊的 以檢視以下詳細資訊，例如項目是否在相同來源與目的地之間彙總多個相同類型的威脅（在此情況下，Count（計數）欄值將大於一）。
- 若您將防火牆設定為執行封包擷取，按一下項目旁的 以存取所擷取的封包。

下表摘要威脅嚴重性等級：

©2024 Palo Alto Networks, Inc.

severity	說明
嚴重	嚴重的威脅，例如影響廣泛部署軟體的預設安裝、導致入侵伺服器控管帳戶及攻擊者可廣泛取得攻擊指令碼。攻擊者通常不需要任何特殊驗證認證或有關個別受害者的知識，也不需要操控目標執行任何特殊功能。
高	可能變為重要等級，但具有可減輕攻擊之因素的威脅；例如，難以攻擊、不會導致權限提升或沒有大型受害集區。 裁定為惡意且動作設定為允許的 WildFire 提交日誌項目都會記錄為「高」。
中	帶來輕微影響的次要威脅，例如不會影響目標的 DoS 攻擊或需要攻擊者與受害者位於相同 LAN 的入侵行為，只會影響非標準設定或不重要的應用程式，或提供極其有限的存取權。 • 基於現有 WildFire 特徵碼嚴重性，裁定為惡意的威脅日誌項目和封鎖或警示動作會記錄為記錄為「中等」。
低	對組織基礎結構影響極小的警告等級威脅。這些威脅通常需要本機或實體系統存取權，具經常可能導致隱私受損或 DoS 問題和資訊洩漏。 • 資料篩選設定檔相符部分會記錄為 (低)。 • 裁定為灰色軟體的 WildFire 提交日誌項目和任何動作都會記錄為「低」。
僅供參考	未產生立即威脅的可疑事件，但會報告以讓您注意可能存在的深入問題。 • URL 篩選日誌項目都會記錄為「資訊」。 • 裁定為良性的 WildFire 提交日誌項目和任何動作都會記錄為「資訊」。 • 裁定為良性的 WildFire 提交日誌項目和設定為封鎖和轉送的動作都會記錄為「資訊」。 • 具有任何裁定的日誌項目和設定為封鎖的動作會記錄為「資訊」。

URL 篩選日誌

URL 篩選日誌（**Monitor**（監控） > **Logs**（日誌） > **URL Filtering**（**URL** 篩選））顯示流向安全性政策規則中監控的 URL 類別的流量的全面資訊。為每個工作階段記錄的內容或屬性包括 `receive time, category, URL, from zone, to zone, source, and source user`。您可以自訂日誌檢視，以便僅顯示您最感興趣的屬性。在以下情況下，防火牆會產生 URL 篩選日誌項目：

- 流量與安全性政策規則比對，並將 URL 類別作為比對規則。該規則對流量執行以下動作之一：`deny, drop, or reset (client, server, both)`。
- 流量與附加了 URL 篩選設定檔的安全性政策規則比對。設定檔中類別的 Site Access（網站存取）設定為 `alert, block, continue, or override`。

©2024 Palo Alto Networks, Inc.

依預設，設定為 ***allow***（允許）的類別不會產生 *URL* 篩選日誌項目。例外是設定日誌轉送。

如果您希望防火牆記錄流向您允許但希望取得更多可見性的類別的流量，請在您的 *URL* 篩選設定檔中將這些類別的 ***Site Access***（網站存取）設定為 ***alert***（警示）。

WildFire 提交日誌

防火牆會根據 WildFire 分析設定檔設定（**Objects**（物件） > **Security Profiles**（安全性設定檔） > **WildFire Analysis**（**WildFire** 分析））將範例（檔案和電子郵件連結）轉送至 WildFire 雲端以進行分析。防火牆會在 WildFire 對範例完成靜態與動態分析後針對其轉送的每個範例產生 WildFire 提交日誌項目。WildFire 提交日誌項目包含了針對範例的防火牆動作（允許或封鎖）以及針對所提交之範例以及範例嚴重性等級的 WildFire 裁定。

下表彙總 WildFire 裁定：

裁定	說明
良性	表示項目已收到良性的 WildFire 分析裁定。分類為良性的檔案安全無虞，且不會出現任何惡意行為。
Grayware	表示項目已收到灰色軟體的 WildFire 分析裁定。分類為灰色軟體的檔案造成直接的安全性威脅，但可能會顯示其他干擾行為。灰色軟體包含廣告軟體、間諜軟體和瀏覽器協助程式物件 (BHO)。
網路釣魚	指示 WildFire 為連結指派了網路釣魚的分析裁定。網路釣魚裁定表示該連結將使用者導向到的網站顯示了認證網路釣魚活動。
惡意的	表示項目已收到惡意的 WildFire 分析裁定。歸類為惡意的範例可產生安全性威脅。惡意軟體包含病毒、C2（命令和控制）、蠕蟲、木馬程式、遠端存取工具 (RAT)、Rootkit 和 Botnet。針對已識別為惡意軟體的範例，WildFire 雲端會產生和散佈特徵碼以防日後暴露。 在 *WildFire* 分析報告和依賴於 *WildFire* 分析資料的其他 *Palo Alto Networks* 產品中，*C2* 樣本被分類為 *C2*；然而，防火牆會轉譯該裁定並將其分類為惡意。

資料過濾日誌

資料篩選日誌會顯示安全性規則的項目，可協助防止機敏資訊（例如信用卡號碼）離開受防火牆保護的區域。如需定義資料篩選設定檔的相關資訊，請參閱 資料篩選。

此日誌也顯示檔案封鎖設定檔的資訊。例如，若規則封鎖 .exe 檔案，日誌會顯示封鎖的檔案。

©2024 Palo Alto Networks, Inc.

關聯日誌

關聯物件 中定義的模式和閾值符合網路上的流量模式時，防火牆會記錄關聯的事件。若要 判讀關聯的事件 並檢視事件的圖形顯示，請參閱 使用 ACC 中之受危害的主機 Widget。

下表摘要關聯日誌嚴重性等級：

severity	說明
嚴重	根據表示升級模式的關聯事件，確認主機已受危害。例如，主機收到 WildFire 裁定為惡意的檔案，且該檔案出現在 WildFire 沙箱中針對該惡意檔案觀察到的命令與控制項活動時，便會記錄關鍵事件。
高	表示根據多個威脅事件的關聯，主機非常可能已受危害，例如在網路上隨處偵測到的惡意軟體與從特定主機產生的命令與控制項活動相符。
中	表示根據對一或多個可疑事件的偵測，主機可能已受危害，例如重複造訪建議指令碼化之命令與控制項活動的已知惡意 URL。
低	表示根據對一或多個可疑事件的偵測，主機可能已受危害，例如造訪惡意 URL 或動態 DNS 網域。
僅供參考	偵測到在彙總後可能對識別可疑活動有用的事件；每個事件本身不一定具有重大意義。

通道檢查日誌

通道檢查日誌與通道工作階段的流量日誌相似；它們會顯示非加密通道工作階段的項目。為了防止重複計數，防火牆僅儲存流量日誌中的內部流程，並將通道工作階段傳送至通道檢查日誌。通報檢查日誌項目包括接收時間（收到日誌的日期和時間）、通道 ID、監控標籤、工作階段 ID、套用於通道工作階段的安全性原則、工作階段中的位元組數、上層工作階段 ID（通道工作階段的工作階段 ID）、來源位址、來源使用者和來源區域、目的地位址、目的地使用者以及目的地區域。

當 *PAN-OS 11.0* 中引入的解密日誌啟用時，防火牆將 *HTTP/2* 日誌作為通道檢查日誌傳送（停用解密日誌後，*HTTP/2* 日誌將作為流量日誌傳送），因此您需要查看通道檢查日誌而不是流量日誌來瞭解 *HTTP/2* 事件。在這種情況下，您還必須啟用通道內容檢查來獲取 *HTTP/2* 流量的 *App-ID*。

按一下 Detailed Log（詳細日誌）檢視表，可檢視條目的詳細資料，例如使用的通道通訊協定以及指示是否已檢查通道內容的標幟。只有具有上層工作階段才會設定通道檢查標幟，這意味著該工作階段在於通道內的通道中（兩層封裝）。通道的第一個外部標頭將不會設定通道檢查標幟。

©2024 Palo Alto Networks, Inc.

設定日誌

組態日誌會顯示關於對防火牆組態進行變更的項目。每個項目都包括日期與時間、管理員使用者名稱、管理員進行變更所在位置的 IP 位址、用戶端類型（Web、CLI 或 Panorama）、執行的命令類型、命令狀態（無論命令成功還是失敗）、組態路徑，以及變更之前和之後的值。

系統日誌

系統日誌會顯示防火牆上每個系統事件的項目。每個項目都包括日期與時間、事件嚴重性以及事件描述。下表摘要系統日誌嚴重性等級。如需系統日誌訊息及其對應嚴重性等級的部分清單，請參閱系統日誌事件。

severity	說明
嚴重	硬體故障，包括高可用性 (HA) 容錯移轉及連結失效。
高	嚴重問題，包含與外部裝置的連線中斷，例如 LDAP 與 RADIUS 伺服器。
中	中等級通知，例如防毒套件升級。
低	低等級嚴重性通知，例如使用者密碼變更。
僅供參考	登入/登出、管理者名稱或密碼變更、任何設定失敗及其他嚴重性等級未涵蓋的其他所有事件。

HIP 比對日誌

GlobalProtect 主機資訊設定檔 (HIP) 比對可用於收集存取網路的終端裝置的安全性狀態的相關資訊（例如它們是否已啟用磁碟加密）。防火牆可以根據遵守您定義的以 HIP 為基礎的安全性規則來允許或拒絕特定主機。HIP 比對日誌會顯示符合您為規則所設定的 HIP 物件或 HIP 設定檔的流量。

GlobalProtect 日誌

GlobalProtect 日誌會顯示以下與 GlobalProtect 有關的日誌：

- GlobalProtect 系統日誌。

  GlobalProtect 驗證事件日誌保留在**Monitor**（監控） > **Logs**（日誌） > **System**（系統）內； 但是，GlobalProtect 日誌的 **Auth Method**（驗證方法）欄會顯示用於登入的驗證方法。
- LSVPN/衛星事件。
- GlobalProtect 入口網站和閘道日誌。
- 無用戶端 VPN 日誌。

©2024 Palo Alto Networks, Inc.

IP-Tag 日誌

Ip-tag 日誌顯示來源 IP 位址如何及何時在防火牆上註冊或取消註冊，及防火牆對位址套用哪些標籤。此外，每個日誌項目都會顯示設定的逾時（設定時）和 IP 位址至標籤對應資訊的來源，例如 User-ID 代理程式 VM 資訊來源和自動標記。如需詳細資訊，請參閱如何動態註冊 IP 位址與標籤。

User-ID 日誌

使用者-ID 日誌會顯示 IP 位址至使用者名稱對應和 驗證時間戳記的相關資訊，例如對應資訊的來源以及使用者的驗證時間。您可以使用此資訊來協助解決 User-ID 和驗證問題。例如，如果防火牆對使用者套用了錯誤的原則規則，您可以檢視日誌來確認該使用者是否對應到正確的 IP 位址，以及群組關聯是否正確。

解密日誌

Decryption Logs（解密日誌）在依預設顯示不成功 TLS 交握的項目，如果在解密原則中啟用，則還可以顯示成功 TLS 交握的項目。如果您啟用成功交握的項目，確保您擁有用於日誌的系統資源（日誌空間）。

解密日誌包含大量資訊，可幫助您 疑難排解和監控解密，然後解決問題。您可以在日誌中啟用 62 欄不同類型的資訊，還可以選取任何單個日誌（，放大鏡），並在單個「詳細資料」檢視中查看詳細資料。您可以檢視憑證、加密套件和錯誤資訊，例如：主體通用名稱、簽發者通用名稱、根通用名稱、根狀態、憑證金鑰類型和大小、憑證開始和結束日期、憑證序號、憑證指紋、TLS 版本、金鑰交換演算法、加密演算法、交涉的 EC 曲線、驗證演算法、SNI、Proxy 類型、錯誤資訊（密碼、HSM、資源、繼續、通訊協定、功能、憑證、版本）和錯誤索引（可以透過查找此代碼獲取更多錯誤資訊）。

警告日誌

警報是防火牆產生的訊息，指示特定類型的時間數目（例如加密與解密失敗）已超過為該時間類型設定的臨界值。若要啟用警報並設定警報臨界值，請選取 **Device**（裝置） > **Log Settings**（日誌設定）並編輯警報設定。

產生警報時，防火牆會建立警報日誌，並開啟 [系統警報] 對話方塊以顯示警報。在您 **Close**（關閉）對話方塊後，您可以按一下 Web 介面底部的 **Alarms**（警報）（ ）可隨時重新開啟。若要防止防火牆自動開啟特定警報的對話方塊，請選取 Unacknowledged Alarms（未確認警報）清單中的警報，然後 **Acknowledge**（確認）該警報。

驗證日誌

驗證日誌顯示當使用者嘗試存取網路資源，而其存取權受到 驗證原則 規則控制時，所發生之驗證事件的相關資訊。您可以使用此資訊來協助疑難排解存取問題，以及視需要來調整驗證原則。與關聯物件搭配使用時，您也可以使用驗證日誌來識別網路上的可疑活動，例如暴力攻擊。

您也可以設定驗證規則設定以記錄逾時事件。這些逾時值與使用者需要只驗證一次資源就可以重複存取該項資源的時段有關。查看逾時的相關資訊可協助您決定是否要加以調整以及該如何調整（如需詳細資訊，請參閱 驗證時間戳記）。

©2024 Palo Alto Networks, Inc.

系統日誌會記錄與 *GlobalProtect* 有關以及與管理員的 *Web* 介面存取有關的驗證事件。

統一日誌

統一日誌為來自流量、威脅、URL 篩選、WildFire 提交以及單一檢視中顯示的資料篩選日誌的項目。利用統一日誌檢視，可在一個位置調查及篩選來自不同日誌類型的最新項目，而不是分別搜尋每個日誌類型。按一下篩選區域中的 Effective Queries（有效查詢）（ ）以選取將在統一日誌檢視中顯示項目的日誌類型。

統一日誌檢視只顯示日誌中您有權查看的日誌。例如，若管理員沒有檢視 WildFire 提交日誌的權限，在檢視統一日誌時，則不會看到 WildFire 提交日誌項目。管理角色類型定義這些權限。

在 *AutoFocus* 中設定遠端搜尋以在防火牆上執行針對性搜尋時，統一日誌檢視中會顯示搜尋結果。

檢視日誌

您可以使用表格格式檢視防火牆上的不同日誌類型。依預設，防火牆會在本機儲存所有日誌檔案並自動產生組態與系統日誌。若要瞭解有關觸發建立其他類型日誌項目的更多資訊，請參閱日誌類型與嚴重性等級。

若要把防火牆設定成將日誌作為 syslog 訊息、電子郵件通知或簡易網路管理通訊協定 (SNMP) 設陷轉送，使用外部服務進行監控。

STEP 1 | 選取要檢視的日誌類型。

1. 選取 **Monitor**（監控）> **Logs**（日誌）。
2. 從清單中選取日誌類型。

   防火牆只會顯示您有權查看的日誌。例如，若您的管理帳戶無權檢視 *WildFire* 提交日誌，則在您存取日誌頁面時，防火牆不會顯示該日誌類型。管理角色類型定義這些權限。

STEP 2 | （選用）自訂日誌欄顯示。

1. 按一下欄標頭右側的箭頭，然後選取 **Columns**（欄）。
2. 選取要在清單中顯示的欄。日誌會自動更新以符合您選取的項目。

©2024 Palo Alto Networks, Inc.

STEP 3 | 檢視有關日誌項目的詳細資訊。

- 按一下望遠鏡 ( ) 以查看特定的日誌項目。Detailed Log View（詳細日誌檢視）包含有關工作階段的來源與目的地的更多資訊，以及與日誌項目相關的工作階段清單。
- （僅限威脅日誌）按一下項目旁邊的 以存取威脅的本機封包擷取功能。若要啟用本機封包擷取，請參閱獲得封包擷取。
- （僅限流量、威脅、URL 篩選、WildFire 提交、資料篩選和統一日誌）檢視日誌項目的 AutoFocus 威脅資料。

  1. 啟用 AutoFocus。

     在 *Panorama* 中啟用 *AutoFocus*，以檢視所有 *Panorama* 日誌項目的 *AutoFocus* 威脅資料，包括來自未連接至 *AutoFocus* 和/或執行 *PAN-OS 7.0* 及更早版本的防火牆的日誌項目（***Panorama*** > ***Setup***（設定） > ***Management***（管理） > ***AutoFocus***）。

  2. 將游標暫留在 IP 位址、URL、使用者代理程式、威脅名稱（子類型：僅病毒和 Wildfire 病毒）、檔案名稱或 SHA-256。
  3. 按一下下拉式清單 ( )，然後選取 **AutoFocus**。
  4. 內容傳送網路基礎結構。

接下來的步驟...

- 篩選器日誌.
- 匯出日誌。
- 設定日誌儲存配額和到期時間.

篩選器日誌

每個日誌都具有一個篩選器區域，您可在此區域為顯示哪些日誌項目設定準則。篩選日誌的功能有利專注於防火牆上具有特定內容或屬性的事件。依與個別日誌項目關聯的構件篩選日誌。

例如，按規則 UUID 進行篩選，可以讓您更輕鬆地找到您想要尋找的特定規則，即使在許多名稱類似的規則中。若您的規則集非常大且包含許多規則，使用規則的 UUID 作為篩選條件可以突出顯示您需要尋找的特定規則，無需導覽結果頁面。

STEP 1 | （僅限統一日誌）選取要在統一日誌顯示中顯示的日誌類型。

1. 按一下 Effective Queries（有效查詢）（ ）。
2. 從清單中選取一種或多種日誌類型（**traffic**（流量）、**threat**（威脅）、**url**、**data**（資料）和 **wildfire**）。
3. 按一下 **OK**（確定）。統一日誌會更新為僅顯示您選取的日誌類型的項目。

©2024 Palo Alto Networks, Inc.

STEP 2 | 向篩選器欄位新增一個篩選器。

如果構件的值與運算式（例如 ***has*** 或 ***in***）相符，則用引號括住該值，避免出現語法錯誤。例如，如果您依目的地國家篩選，則將 *IN* 用作 *Value*（值）來指定 *INDIA*，將篩選輸入為 ***(dstloc eq “IN”)***。

- 按一下日誌項目中的一個或多個構件（例如與流量和攻擊者的 IP 位址關聯的應用程式類型）。例如，按一下日誌項目的來源 **10.0.0.25** 和目的地 **web-browsing**（網頁瀏覽），以僅顯示日誌中包含兩個構件的項目（AND 搜尋）。
- 若要指定構件以新增至篩選器欄位，請按一下 Add Filter（新增篩選器）( )。
- 若要新增先前儲存的篩選器，按一下 Load Filter（載入篩選器）( )。

STEP 3 | 將篩選器套用至日誌。

按一下 Apply Filter（套用篩選器）( )。日誌會重新整理，以僅顯示與目前篩選器相符的日誌項目。

STEP 4 | （選用）儲存常用的篩選器。

1. 按一下 Save Filter（儲存篩選器）( )。
2. 輸入篩選器的 **Name**（名稱）。
3. 按一下 **OK**（確定）。您可以按一下 Load Filter（載入篩選器）( )，以檢視儲存的篩選器。

接下來的步驟...

- 檢視日誌。
- 匯出日誌。

匯出日誌

您可以將日誌類型的內容匯出至逗號分隔值 (CSV) 格式的報告。依預設，報告包含多達 2,000 行日誌項目。

STEP 1 | 指定要在報告中顯示的列數。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理），然後編輯 Logging and Reporting Settings（日誌記錄與報告設定）。
2. 按一下 **Log Export and Reporting**（日誌匯出與報告）頁籤。
3. 編輯 **Max Rows in CSV Export**（**CSV** 匯出中的最大列數）的數目（多達 1048576 列）。
4. 按一下 **OK**（確定）。

©2024 Palo Alto Networks, Inc.

STEP 2 | 下載日誌。

1. 按一下 Export to CSV（匯出至 CSV）( )。會出現一個顯示下載狀態的進度列。
2. 下載完成後，按一下 **Download file**（下載檔案）以將日誌複本儲存至本機資料夾。如需下載的日誌中的欄標頭的說明，請參閱Syslog 欄位說明。

接下來的步驟...

排程將日誌匯出至 SCP 或 FTP 伺服器。

設定日誌儲存配額和到期時間

防火牆會自動刪除超過到期期間的日誌。即使您並未設定到期期間，防火牆到達日誌類型的儲存配額時，其仍會自動偵測該類型中較舊的日誌以產生空間。

若要手動刪除日誌，可選取 ***Device***（裝置） > ***Log Settings***（日誌設定），然後在 *Manage Logs*（管理日誌）區段中，按一下連結以依類型清除日誌。

STEP 1 | 選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理），然後編輯 Logging and Reporting Settings（日誌記錄與報告設定）。

STEP 2 | 選取 **Log Storage**（日誌儲存）並為每種日誌類型輸入 **Quota (%)**（配額 **(%)**）。當您變更百分比值時，對話方塊會重新整理以顯示對應的絕對值（配額 GB/MB 欄）。

STEP 3 | 輸入各日誌類型的 **Max Days**（最大天數）（到期日期）（範圍為 1-2000）。欄位預設為空白，表示日誌永不到期。

防火牆會在高可用性 *(HA)* 端點之間同步處理到期期間。由於只有主動 *HA* 端點會產生日誌，因此除非發生容錯移轉且被動端點開始產生日誌，否則其不會具有要刪除的日誌。

STEP 4 | 按一下 **OK**（確定）與 **Commit**（提交）。

排程將日誌匯出至 SCP 或 FTP 伺服器

您可以排程將流量、威脅、URL 篩選、資料篩選、HIP 比對和 WildFire 提交日誌匯出至安全複製 (SCP) 伺服器或檔案傳輸通訊協定 (FTP) 伺服器。請針對要匯出的每個日誌類型執行此工作。

您可以從 CLI 使用安全複本 (SCP) 命令，將整個日誌資料庫匯出至 *SCP* 伺服器，並將其匯入至其他防火牆。由於日誌資料庫太大，因此無法在不支援這些選項的下列平台上實際執行匯出或匯入：*PA-7000* 系列防火牆（所有 *PAN-OS* 發行版本）、在 *Panorama 6.0* 或更新版本上執行的 *Panorama* 虛擬裝置以及 *Panorama M* 系列裝置（所有 *Panorama* 發行版本）。

STEP 1 | 選取 **Device**（裝置） > **Scheduled Log Export**（已排程日誌匯出），然後按一下 **Add**（新增）。

STEP 2 | 輸入已排程日誌匯出的 **Name**（名稱），然後將其 **Enable**（啟用）。

 ©2024 Palo Alto Networks, Inc.

STEP 3 | 選取要匯出的 **Log Type**（日誌類型）。

STEP 4 | 選取每日的 **Scheduled Export Start Time**（已排程的匯出開始時間）。24 小時制 (00:00 - 23:59) 的選項以 15 分鐘為增量。

STEP 5 | 選取要用於匯出日誌的 **Protocol**（通訊協定）：**SCP**（安全）或 **FTP**。

STEP 6 | 輸入伺服器的 **Hostname**（主機名稱）或 IP 位址。

STEP 7 | 輸入 **Port**（連接埠）號碼。依預設，FTP 使用連接埠 21，SCP 使用連接埠 22。

STEP 8 | 輸入要儲存所匯出日誌的 **Path**（路徑）或目錄。

STEP 9 | 輸入要存取伺服器的 **Username**（使用者名稱），並視需要輸入 **Password**（密碼）（及 **Confirm Password**（確認密碼））。

STEP 10 | （僅限 FTP）如果您想使用 FTP 被動模式，則選取 **Enable FTP Passive Mode**（啟用 **FTP** 被動模式）；在此模式中，防火牆會透過 FTP 伺服器啟動資料連線。依預設，防火牆會使用 FTP 主動模式；在此模式中，FTP 伺服器會透過防火牆啟動資料連線。根據 FTP 伺服器支援的項目和網路需求來選擇模式。

STEP 11 | （僅限 SCP）按一下 **Test SCP server connection**（測試 **SCP** 伺服器連線）。將顯示一個快顯視窗，要求您輸入純文字 **Password**（密碼），然後輸入 **Confirm Password**（確認密碼），以測試 SCP 伺服器連線並啟用資料的安全傳輸。

在您輸入並確認 SCP 伺服器密碼之前，防火牆不會建立和測試 SCP 伺服器連線。如果防火牆在 HA 設定中，為每個 HA 對等執行此步驟，讓每個 HA 對等可以成功連線至 SCP 伺服器。如果防火牆可成功連線至 SCP 伺服器，則會建立並上傳名為 `ssh-export-test.txt` 的測試檔。

如果您使用 *Panorama* 範本來設定日誌匯出排程，在將範本設定認可至防火牆後，必須執行此步驟。認可範本後，登入每個防火牆、開啟日誌匯出排程，然後按一下 ***Test SCP server connection***（測試 ***SCP*** 伺服器連線）。

STEP 12 | 按一下 **OK**（確定）與 **Commit**（提交）。

 ©2024 Palo Alto Networks, Inc.

監控封鎖清單

有兩種方式可讓防火牆將 IP 位址放入封鎖清單：

- 為漏洞保護設定檔設定封鎖 IP 連線的規則，並將設定檔套用至您對區域套用的安全性原則。
- 為 DoS 保護原則規則設定保護動作和分類 DoS 保護設定檔，指定最大速率（每秒連線數）。當輸入封包與 DoS 保護原則相符並超過最大速率時，如果您指定了封鎖持續時間和分類原則規則以包含來源 IP 位址，防火牆會將攻擊性 IP 位址放入封鎖清單。

在上述情況中，防火牆將在這些封包使用 CPU 或封包緩衝資源之前，自動封鎖硬體中的流量。如果攻擊流量超過硬體的封鎖能力，則防火牆會使用軟體中的 IP 封鎖機制來封鎖流量。

防火牆將根據漏洞保護設定檔或 DoS 保護原則規則自動建立硬體封鎖清單項目；規則中的來源位址是硬體封鎖清單中的來源 IP 位址。

封鎖清單中的項目在 Type（類型）欄中指示了是被硬體 (hw) 還是軟體 (sw) 封鎖。畫面底部顯示：

- **Total Blocked IPs**（封鎖的 **IP** 總數）以及防火牆支援封鎖的 IP 位址數目。
- 防火牆已使用封鎖清單容量的百分比。

若要檢視封鎖清單上某個位址的詳細資料，將滑鼠暫留在來源 IP 位址上，然後按一下向下箭頭連結。按一下 Who Is 連結，將顯示 Network Solutions Who Is 功能，提供位址資訊。

如需設定漏洞保護設定檔的詳細資訊，請自訂暴力密碼破解特徵碼的動作與觸發條件。如需封鎖清單與 DoS 保護設定檔的詳細資訊，請參閱對新工作階段流量的 DoS 保護。

©2024 Palo Alto Networks, Inc.

檢視和管理報告

防火牆的報告功能可讓您掌握網路的脈動、驗證原則，並將工作重心放在維護網路安全性上，讓您的使用者能有安全的狀態並具備生產力。

- 報告類型
- 檢視報告
- 設定報告的到期時間和執行時間
- 停用預先定義的報告
- 自訂報告
- 產生自訂報告
- 產生 Botnet 報告
- 產生 SaaS 應用程式使用情況報告
- 管理 PDF 摘要報告
- 產生使用者/群組活動報告
- 管理報告群組
- 排程以電子郵件傳遞報告
- 管理報告儲存容量

報告類型

防火牆包括預先定義的報告，您可以依原狀使用、建立符合您特定資料與可執行工作之需求的自訂報告，或結合預先定義報告與自訂報告以編譯您需要的資訊。防火牆提供下列類型的報告：

- 預先定義的報告—允許您檢視網路流量的快速摘要。一組預先定義的報告，分成四種類別—應用程式、流量、威脅與 URL 篩選。請參閱 檢視報告。
- 使用者或群組活動報告—允許您針對特定的使用者或使用者群組排程或建立「依需求報告」。報告包括 URL 類別，以及針對各個使用者計算的預估瀏覽時間。請參閱 產生使用者/群組活動報告。
- 自訂報告—建立和排程自訂報告，藉由篩選要包含的條件和欄，顯示您真正要查看的資訊。您也可以包括查詢建立器，以深入考察取得更具體的報告資料。請參閱 產生自訂報告。
- **PDF** 摘要報告—最多可將來自威脅、應用程式、趨勢、流量、URL 篩選等類別的 18 個預先定義或自訂報告/圖表彙總為 PDF 文件。請參閱 管理 PDF 摘要報告。
- **Botnet** 報告—可以讓您使用行為式機制來識別網路中潛在的受 Botnet 感染的主機。請參閱 產生 Botnet 報告。
- 報告群組—將自訂報告與預先定義的報告合併至報告群組、編譯成 PDF 檔並以電子郵件傳送給一或多個收件者。請參閱 管理報告群組。

您可視需要或依週期性排程來產生報告，並可排程以電子郵件傳送報告。

©2024 Palo Alto Networks, Inc.

檢視報告

防火牆提供超過 40 種各式各樣的預先定義報告，並每天產生這些報告。您可以直接在防火牆上檢視這些報告。您也可以檢視自訂報告和摘要報告。

系統約分配 200 MB 的儲存區，以供將報告儲存在防火牆上。此限制僅可對 PA-7000 與 PA-5200 系列防火牆進行重新設定。對於所有其他防火牆型號，您可以設定報告的到期時間和執行時間，以允許防火牆刪除超過該期間的報告。請記住，即使您並未設定到期期間，防火牆到達其儲存限制時，其仍會自動刪除較舊的報告以產生空間。另一個節約使用防火牆上系統資源的方法是停用預先定義的報告。對於長期保留報告，您可以匯出報告（如下所述）或排程以電子郵件傳遞報告。

不同於其他報告，您無法在防火牆上儲存使用者/群組活動報告。您必須隨選產生使用者/群組活動報告，或排程以電子郵件傳遞報告。

STEP 1 | （僅限 VM-50、VM-50 Lite 和 PA-200 防火牆）啟用產生預先定義報告。

依預設，預先定義報告會在 *VM-50*、*VM-50 Lite* 和 *PA-200* 防火牆上停用以節省資源。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理），然後編輯 **Logging and Reporting**（記錄與報告）。
2. 選取 **Pre-Defined Reports**（預先定義報告）並啟用（核取）**Pre-Defined Reports**（預先定義報告）。
3. 核取（啟用）您想要產生的預先定義報告並按一下 **OK**（確定）
4. **Commit**（提交）組態變更。
5. 存取防火牆 CLI 以啟用預先定義報告。

   此步驟對本機預先定義報告和從 Panorama™ 管理伺服器推送的預先定義報告為必需。

   ```
   admin> debug predefined-default enable
   ```

STEP 2 | 選取 **Monitor**（監控） > **Reports**（報告）。

報告在頁面右側分組成數個區段（類型）：**Custom Reports**（自訂報告）、**Application Reports**（應用程式報告）、**Traffic Reports**（流量報告）、**Threat Reports**（威脅報告）、**URL Filtering Reports**（**URL** 篩選報告）與 **PDF Summary Reports**（**PDF** 摘要報告）。

STEP 3 | 選取要檢視的報告。報告頁面然後會顯示前一天的報告。

若要檢視其他天的報告，請在頁面右下角行事曆中選取一個日期，然後選取報告。若您在另一個區段選取報告，日期選取會重設至目前日期。

STEP 4 | 若要離線檢視報告，您可以將報告匯出成 PDF、CSV 或 XML 格式。按一下頁面底端的 **Export to PDF**（匯出為 **PDF**）、**Export to CSV**（匯出為 **CSV**）或 **Export to XML**（匯出為 **XML**），然後列印或儲存檔案。

©2024 Palo Alto Networks, Inc.

設定報告的到期時間和執行時間

到期時間和執行時間是套用於所有 報告類型 的全域設定。執行新報告後，防火牆會自動刪除超過到期時間的報告。

STEP 1 | 選取 **Device**（裝置） > **Setup**（裝置） > **Management**（管理），編輯 Logging and Reporting Settings（日誌記錄與報告設定），然後選取 **Log Export and Reporting**（日誌匯出與報告）頁籤。

STEP 2 | 將 **Report Runtime**（報告執行時間）設定為 24 小時制的整點（預設為 02:00；範圍為 00:00 [午夜] 到 23:00）。

STEP 3 | 輸入 **Report Expiration Period**（報告到期時間）天數（預設值為不過期；範圍為 1-2000）。

您無法變更防火牆針對儲存報告而配置的儲存空間，其預先定義為約 *200 MB*。即使您並未設定 ***Report Expiration Period***（報告到期期間），防火牆到達儲存上限時，其仍會自動刪除較舊的報告以產生空間。

STEP 4 | 按一下 **OK**（確定）與 **Commit**（提交）。

停用預先定義的報告

防火牆包含約 40 個預先定義的報告，其每日都會自動產生這些報告。如果您不使用某些或所有這些項目，則可以停用所選的報告以節約使用防火牆上的系統資源。

請確定所有報告群組或 PDF 摘要報告都不包含您將停用的預先定義報告。否則防火牆呈現的 PDF 摘要報告或報告群組中不會有任何資料。

STEP 1 | 選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理），然後編輯 Logging and Reporting Settings（日誌記錄與報告設定）。

STEP 2 | 選取 **Pre-Defined Reports**（預先定義的報告）頁籤，然後針對要停用的每個報告清除核取方塊。若要停用所有預先定義的報告，請按一下 **Deselect All**（取消全選）。

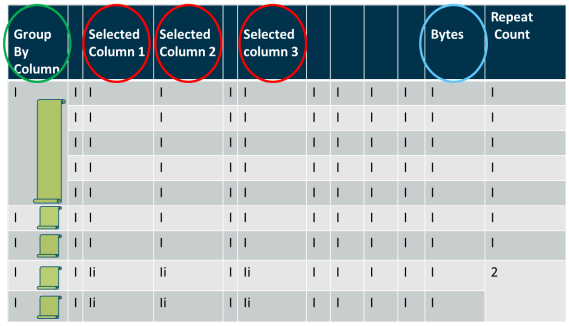
STEP 3 | 按一下 **OK**（確定）與 **Commit**（提交）。

自訂報告

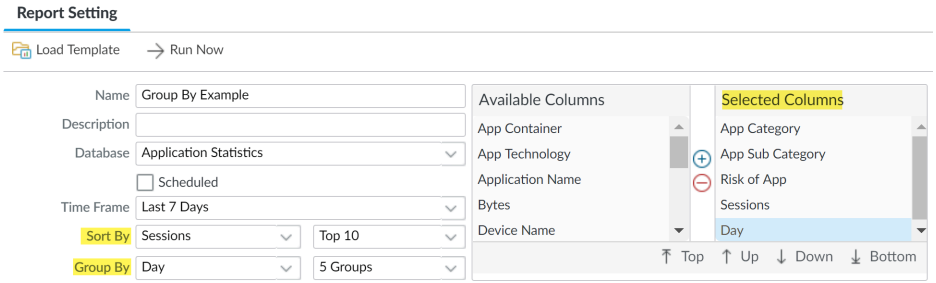
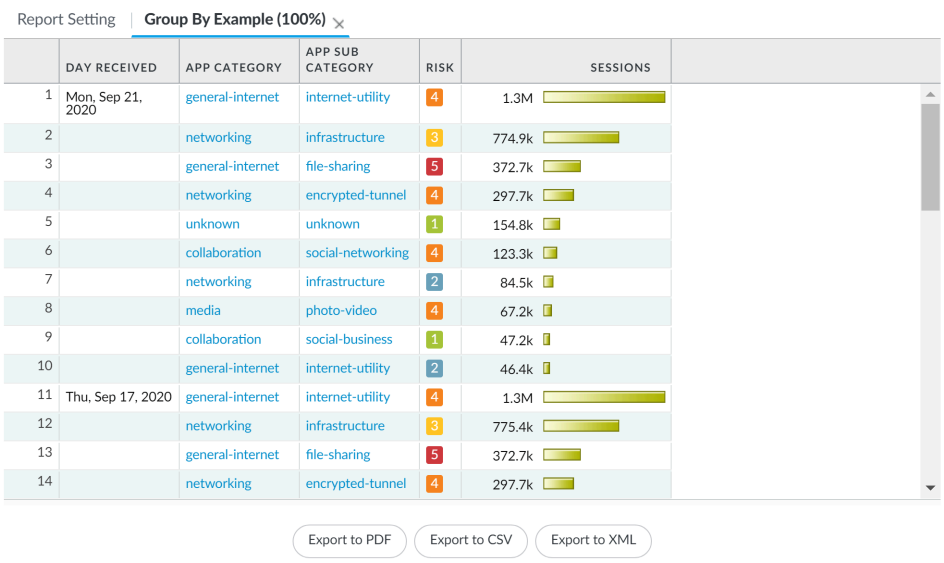
為了建立針對性自訂報告，您必須考慮您想要擷取並分析的屬性或關鍵資訊，例如威脅，以及最佳資訊分類方法，例如按規則 UUID 分組，以便您查看適用於每個威脅類型的規則。此考量可引導您在自訂報告中進行下列選擇：

選擇	說明
Database	您可以根據下列任何資料庫類型產生報告：

©2024 Palo Alto Networks, Inc.

選擇	說明
	• 摘要資料庫 — 這些資料庫可供應用程式統計資料、流量、威脅、URL 篩選以及通道檢查日誌使用。防火牆每 15 分鐘就會彙總詳細日誌。若要縮短產生報告時的回應事件，防火牆將壓縮資料：重複的工作階段將被分鐘，並增加重複計數器的計數，摘要中將不會包含某些屬性（欄）。 • 詳細日誌 — 這些資料庫將逐項列出日誌，並列出每個日誌項目的全部屬性（欄）。 以詳細日誌為基礎的報告所需的執行時間很長，除非絕對需求，否則不建議使用。
屬性	要作為比對規則的欄。屬性為報告中可供選擇的欄。從 **Available Columns**（可用欄）清單中，您可以新增用於比對資料及彙總詳細資料的選擇準則（**Selected Columns**（已選取的欄））。
排序方式/群組方式	**Sort By**（排序方式）與 **Group By**（群組方式）準則可讓您在報告中組織/分隔資料；可用的排序與群組屬性會視所選的資料來源而異。 (排序方式) 選項可指定用於彙總的屬性。如果您未選取作為排序方式的屬性，報告會傳回前 N 個結果，不進行任何的彙總。 (群組方式) 選項可讓您選取屬性並作為群組資料的錨點；報告中所有的資料會以前 5 個、10 個、25 個或 50 個群組的方式顯示。例如，您選取 (小時) 作為 (群組依據) 選擇，並要顯示 24 小時的前 25 個群組時，系統將會產生 24 小時每一小時的報告結果。報告的第一欄會是小時，下一組欄將是您所選其餘的報告欄。
	下例說明產生報告時，**Selected Columns**（已選取的欄）與 **Sort By**（排序方式）/**Group By**（分組方式）準則如何一起運作：  加上紅色圈 (上方) 的欄表示所選的欄，亦即您比對用來產生報告的屬性。系統會剖析資料來源中的每個日誌項目，並對照這些欄進行比對。如果選取的欄在多個工作階段中有相同的值，系統會將這些工作階段彙總，並增加重複計數 (或工作階段)。

©2024 Palo Alto Networks, Inc.

選擇	說明
	加上藍色圈的欄表示所選的排序順序。指定排序順序（**Sort By**（排序方式））時，會依照所選的屬性排序（與彙總）資料。 加上綠色圈的欄表示 **Group By**（分組方式）選項，作報告的錨點。**Group By**（分組方式）欄作為篩選前　N 個群組的比對準則。接著，針對前 N 名的每個群組，報告會列舉所有其他選取欄的值。
	例如，如果報告有下列選項：  輸出會如下顯示：  報告會依據 **Day**（日）錨定，並依 **Sessions**（工作階段）排序。其會列出 **Last 7 Days**（過去 **7** 天）時間範圍內流量最大的 5 天（**5 Groups**（**5** 個群組））。系統會針對所選欄—**App Category**（應用程式類別）、**App Subcategory**（應用程式子類別）及 **Risk**（風險）—的每一天，依照 **Top 5**（前 **5** 名）工作階段列舉資料。
時間範圍	您想要分析資料的日期範圍。您可以定義自訂範圍，或選取範圍從過去 15 分鐘到過去 30 天的時段。報告可以依需要執行，或排程為以每天或每週的週期執行。

©2024 Palo Alto Networks, Inc.

選擇	說明
查詢建立器	查詢建立器允許您定義特定的查詢，以進一步調整所選的屬性。它允許您使用 **AND** 與 **OR** 運算子及比對準則，在報告中只顯示您想要看到的項目，並可讓您包括或排除符合或不符合報告中查詢的資料。查詢可讓您在報告中產生更聚焦的定序資料。

產生自訂報告

您可以設定防火牆即時（視需要）或依排程（每晚）產生的自訂報告。若要瞭解可用於建立針對性自訂報告的選項，請參閱自訂報告。

防火牆產生排程的自訂報告後，如果修改了報告設定以變更未來的輸出，則會有使該報告過去的結果變為無效的風險。如果需要修改已排程報告的設定，最佳做法是建立新報告。

STEP 1 | 選取 **Monitor**（監控） > **Manage Custom Reports**（管理自訂報告）.

STEP 2 | 按一下 **Add**（新增），然後輸入報告的 **Name**（名稱）。

若要使報告以預先定義的範本為基礎，請按一下載入範本並選擇範本。接著您可以編輯範本並另存成自訂報告。

STEP 3 | 選取要用於產生報告的 **Database**（資料庫）。

每次您建立自訂報告時，會自動建立日誌檢視報告。此報告將顯示用來建立自訂報告的日誌。日誌檢視報告會使用與自訂報告相同的名稱，但在報告名稱上加上 *(*日誌檢視*)* 的字詞。

建立報告群組時，您可以包含日誌檢視報告與自訂報告。如需詳細資訊，請參閱管理報告群組。

STEP 4 | 選取已排程核取方塊可在每晚執行報告。然後您可以在側邊的 **Reports**（報告）欄中檢視報告。

若要使用儲存在 *Panorama*™ 管理伺服器上 *Cortex Data Lake* 中的日誌產生計劃的自訂報告，必須在 *Panorama* 上安裝雲端服務外掛程式 *1.8* 或更新版本。

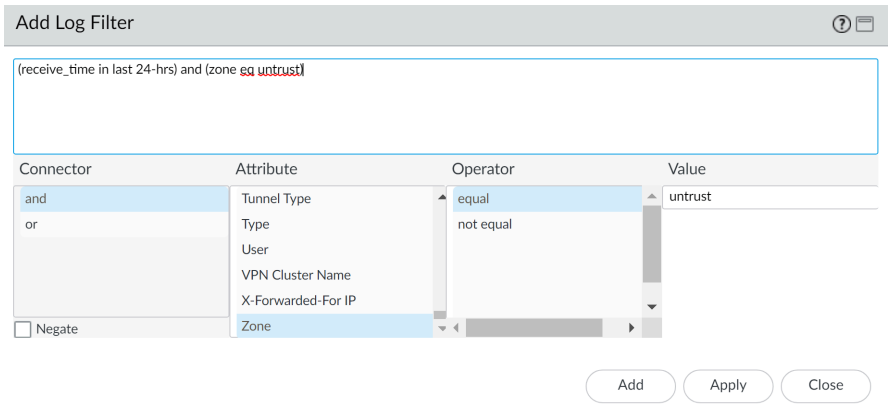
STEP 5 | 定義篩選規則。選取 **Time Frame**（時間範圍）、**Sort By**（排序方式）順序、**Group By**（分組方式）偏好設定，再選取報告中必須顯示的欄。

©2024 Palo Alto Networks, Inc.

STEP 6 | （選用）若要進一步調整選取準則，請選取 **Query Builder**（查詢建立器）屬性。若要建立報告查詢，請指定下列項目並按一下 **Add**（新增）。視需要重複操作來建構完整查詢。

- **Connector**—選擇連接器 (and/or) 來優先處理您要新增的表示式。
- 否定—選取此核取方塊可將查詢解譯為否定。例如，如果您選擇比對最近 24 小時內的項目，且/或源自於不信任的區域開始，則否定選項會造成比對不是過去 24 小時且/或不源自不信任區域的項目。
- **Attribute**（屬性）—選擇資料元素。可用選項視選擇的資料庫而定。
- **Operator**（運算子）—選擇準則以決定是否套用屬性（例如 =）。可用選項視選擇的資料庫而定。
- **Value**（值）—指定要比對的屬性值。

例如，下圖（以 `Traffic Log` 資料庫為基礎）顯示了如果在過去 24 小時內收到流量日誌項目且來自不信任區域時的相符查詢。



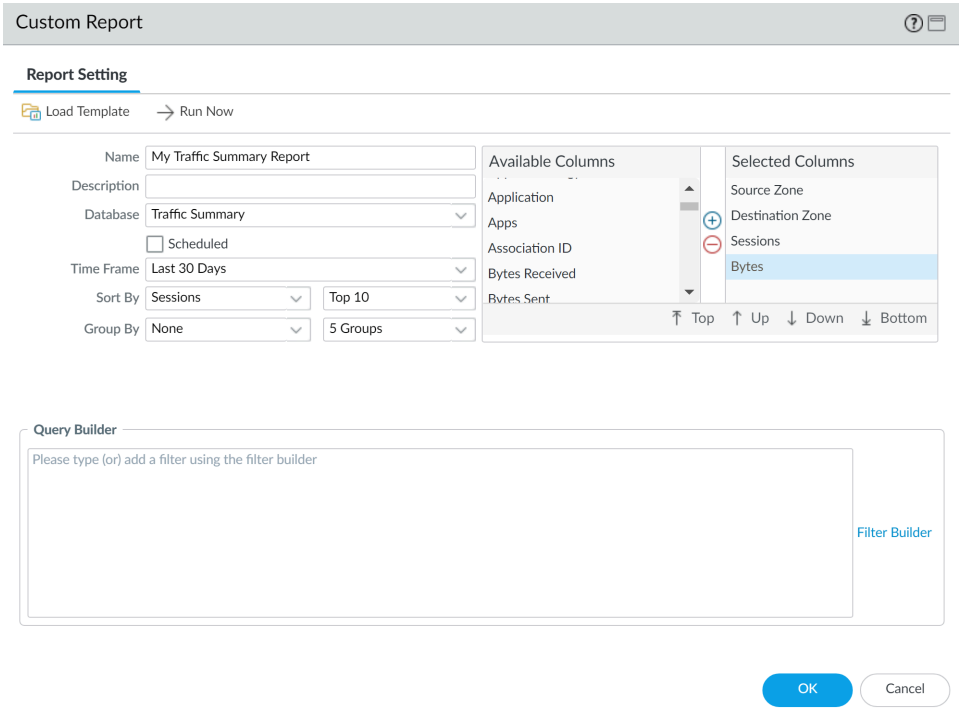
STEP 7 | 若要測試報告設定，請選取 **Run Now**（立即執行）。修改欲變更報告中顯示的資訊時所需要的設定。

©2024 Palo Alto Networks, Inc.

STEP 8 | 按一下 **OK**（確定）以儲存自訂報告。

自訂報告範例

如果您想要設定一個簡單的報告，在報告中您會使用過去 30 天的流量摘要資料庫，並依照前 10 個工作階段排序資料，再將這些工作階段依照星期幾分組成 5 個群組。您可以如下所示設定自訂報告：



報告的 PDF 輸出如下所示：

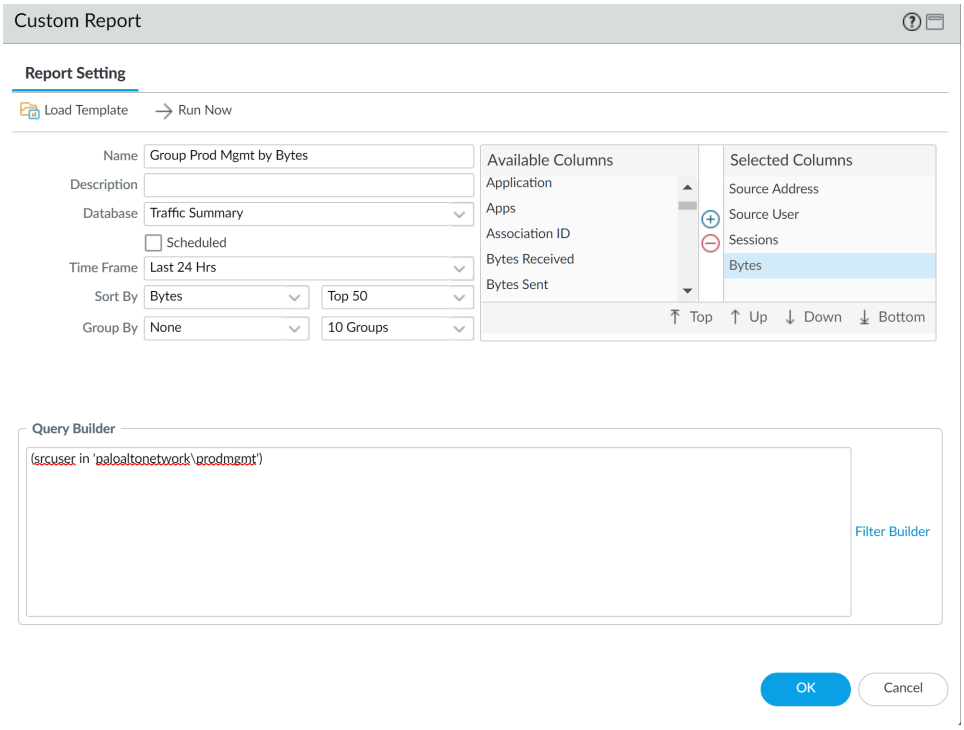
My Traffic Summary Report

ca1demo.paloaltonetworks.com : 2016/01/25 10:34:39 - 2016/02/24 10:34:38

Source Zone	Destination Zone	App Category	Application	Sessions	Bytes
Tap	Tap	general-internet	web-browsing	74.54 M	2.47 T
Tap	Tap	networking	dns	52.03 M	28.93 G
Tap	Tap	networking	ssl	18.01 M	678.13 G
Tap	Tap	general-internet	bittorrent	9.80 M	1.62 T
Tap	Tap	general-internet	google-base	4.48 M	168.99 G
Tap	Tap	unknown	insufficient-data	4.45 M	31.30 G
Tap	Tap	collaboration	facebook-base	4.09 M	99.14 G
Tap	Tap	networking	ntp	4.07 M	3.29 G
Tap	Tap	collaboration	blackboard	2.84 M	186 G
Tap	Tap	collaboration	smtp	1.92 M	172.57 G
Tap	Tap	networking	icmp	1.36 M	320.49 M
Tap	Tap	general-internet	gnutella	1.17 M	17.84 G
Tap	Tap	collaboration	myspace-base	1.10 M	35.22 G
Tap	Tap	general-internet	ping	1.06 M	86.21 M
Tap	Tap	general-internet	flash	1.01 M	168.14 G

現在，如果您想要使用查詢建立器產生自訂報告，來表示使用者群組內耗用量最高的前名網路資源，您可以如下所示設定報告：

 ©2024 Palo Alto Networks, Inc.



報告會依位元組排序顯示產品管理使用者群組內的前幾名使用者。

產生 Botnet 報告

Botnet 報告可讓您使用啟發學習法和行為式機制來識別網路中潛在的受惡意軟體或 Botnet 感染的主機。若要評估 Botnet 活動和受感染的主機，防火牆會建立威脅、URL 和資料篩選日誌中使用者和網路活動資料與 PAN-DB、已知動態 DNS 網域提供者和最近 30 天註冊網域中的惡意軟體 URL 清單之間的關聯。您可以設定報告以識別造訪這些網站的主機，以及與網路聊天 (IRC) 伺服器通訊的主機，或使用未知應用程式的主機。惡意軟體通常會使用動態 DNS 以避免 IP 封鎖，而 IRC 伺服器通常會使用 Bot 自動化運作。

防火牆需要威脅防止和 *URL* 篩選授權才能使用 *Botnet* 報告。您可以 使用自動關聯引擎，以根據 *Botnet* 報告使用的指標及其他指標監控可疑活動。但是，*Botnet* 報告唯一使用新註冊網域作為指標的工具。

- 設定 Botnet 報告
- 判讀 Botnet 報告輸出

設定 Botnet 報告

您可以排程或視需要執行 Botnet 報告。由於行為式偵測需要在時間範圍內對多個日誌進行流量關聯，因此防火牆每 24 小時會產生一次排程的 Botnet 報告。

©2024 Palo Alto Networks, Inc.

STEP 1 | 定義表示可能的 Botnet 活動之流量類型。

1. 選取 **Monitor**（監控） > **Botnet**（殭屍網路），然後按一下頁面右側的 **Configuration**（組態）。
2. **Enable**（啟用）並定義報告中將包含的各類 HTTP 流量的 **Count**（計數）。

   Count（計數）值代表每個流量類型必須發生的事件數下限，事件數超過此值時，報告才能以較高的信任分數（較可能受 Botnet 感染）列出相關聯的主機。如果事件數少於 **Count**（計數），則報告會顯示較低的信任分數或（針對特定流量類型）不顯示主機項目。例如，如果您針對 **Malware URL visit**（惡意軟體 **URL** 造訪），將 **Count**（計數）設定為三，則相較於造訪已知惡意軟體 URL 少於三次的主機，造訪三或更多次的主機會具有較高的分數。如需詳細資料，請參閱 判讀 Botnet 報告輸出。
3. 定義決定報告是否包含與涉及未知 TCP 或未知 UDP 應用程式之流量相關聯之主機的臨界值。
4. 選取 **IRC** 核取方塊以包含涉及 IRC 伺服器的流量。
5. 按一下 **OK**（確定）以儲存報告組態。

STEP 2 | 排程或視需要執行報告。

1. 按一下頁面右側的 **Report Setting**（報告設定）。
2. 在 **Test Run Time Frame**（測試執行階段範圍）下拉式清單中選取報告的時間間隔。
3. 選取要在報告中包含的 **No. of Rows**（列數）。
4. （選用）**Add**（新增）查詢至「查詢建立器」，按照來源/目的地 IP 位址、使用者或區域等屬性篩選報告輸出。

   例如，如果您事先知道從 IP 位址 10.3.3.15 啟動的流量不包含潛在 Botnet 活動，則可以將 **`not (addr.src in 10.0.1.35)`** 新增為查詢，以從報告輸出中排除該主機。如需詳細資料，請參閱 判讀 Botnet 報告輸出。
5. 選取 **Scheduled**（已排程）以每日執行報告，或按一下 **Run Now**（立即執行）以立即執行報告。
6. 按一下 **OK**（確定）與 **Commit**（提交）。

判讀 Botnet 報告輸出

Botnet 報告會針對與您在設定報告時定義為可疑的流量相關聯的每台主機顯示一行。報告會針對每台主機顯示 1 到 5 的信任分數，以表示受 Botnet 感染的可能性，其中 5 表示最可能受到感染。分數會對應至威脅嚴重性等級：1 是資訊、2 是低、3 是中、4 是高，而 5 是關鍵。防火牆會根據下列項目決定分數：

- 流量類型—較可能涉及 Botnet 活動的特定 HTTP 流量類型。例如，如果您將造訪已知惡意軟體 URL 和瀏覽至 IP 網域這兩種活動定義為可疑活動，則相較於瀏覽至 IP 網域而非 URL 的主機，報告會將較高的信任分數指派給造訪已知惡意軟體 URL 的主機。
- 事件數—根據您 設定 Botnet 報告 時定義的閾值（**Count**（計數）值），與較多可疑事件相關聯的主機會具有較高的信賴分數。

©2024 Palo Alto Networks, Inc.

- 可執行的下載項目—報告會將較高的信任分數指派給下載可執行檔的主機。可執行檔是許多感染中的一部分，且與其他類型的可疑流量結合時，可協助您設定調查受危害主機的優先順序。

檢閱報告輸出時，您可能會發現防火牆用於評估 Botnet 活動的來源（例如，PAN-DB 中的惡意軟體 URL 清單）具有漏洞。您可能也會發現這些來源會識別您認為安全的流量。若要彌補這兩種狀態，您可以在 設定 Botnet 報告 時新增查詢篩選器。

產生 SaaS 應用程式使用情況報告

SaaS 應用程式使用情況 PDF 報告分成兩部分，可讓您輕鬆依據風險與認可狀態探索 SaaS 應用程式活動。認可應用程式是您正式核准用於網路上的應用程式。SaaS 應用程式在 **Objects**（物件） > **Applications**（應用程式）中的應用程式詳細資訊頁面具有 SaaS=yes 的特性；所有其他應用程式皆視為非 SaaS。若要表示您已經認可 SaaS 或非 SaaS 應用程式，則必須使用名為 Sanctioned（已認可）的預先定義的標籤來標記它。防火牆與 Panorama 會將無此預先定義標籤的任何應用程式，視為不可在網路上使用。

- 報告的第一部分顯示報告時段中有關網路中 SaaS 應用程式的重要發現，並對認可與非認可應用程式進行對比，依據使用情況、合規性以及資料傳輸的認可狀態列出前幾名應用程式。為協助您識別與探索高風險應用程式使用情況的範圍，報告中的風險性應用程式這一部分會列出存在以下不利裝載特性的 SaaS 應用程式：獲得的憑證、過去的資料外洩情況、支援以 IP 為主的限制、財務可行性與服務條款。此外，還可檢視認可與非認可 SaaS 應用程式在以下方面的對比情況：網路上使用的應用程式總數、這些應用程式所耗用的頻寬以及、使用這些應用程式的使用者數目、使用最多 SaaS 應用程式的前幾名使用者群組，以及透過認可與非認可 SaaS 應用程式傳輸最大資料量的前幾名使用者群組。報告第一部分還著重介紹了依據所用應用程式的最大數目、使用者數目、每個應用程式子類別中傳輸的資料量（位元組數）標準按順序排列的前幾名 SaaS 應用程式子類別。
- 報告第二部分專門講述 SaaS 或非 SaaS 應用程式在報告第一部分所列之每個應用程式子類別方面的詳細瀏覽資訊。對於子類別中的每個應用程式，還包括以下相關資訊：傳輸資料方面排前幾名的使用者、被封鎖或警示方面排前幾名的檔案類型；以及每個應用程式面臨的幾大威脅。此外，報告這個部分還統計了防火牆提交進行 WildFire 分析的每個應用程式的範例，以及確定為良性和惡意的範例數目。

使用這個報告中的見解，可整合業務關鍵及核准的 SaaS 應用程式清單，並強制執行相關原則來控制會產生不必要的惡意軟體傳播及資料洩露風險的非認可應用程式以及具風險的應用程式。

預先定義的 *SaaS* 應用程式使用情況報告仍可用作每日檢視報告，列出指定天網路上執行之前 *100* 名的 *SaaS* 應用程式（意味著具有 *SaaS* 應用程式特性：*SaaS=yes*）。此報告不提供已指定為認可的應用程式的可見性，而提供網路上所有使用中 *SaaS* 應用程式的可見性。

©2024 Palo Alto Networks, Inc.

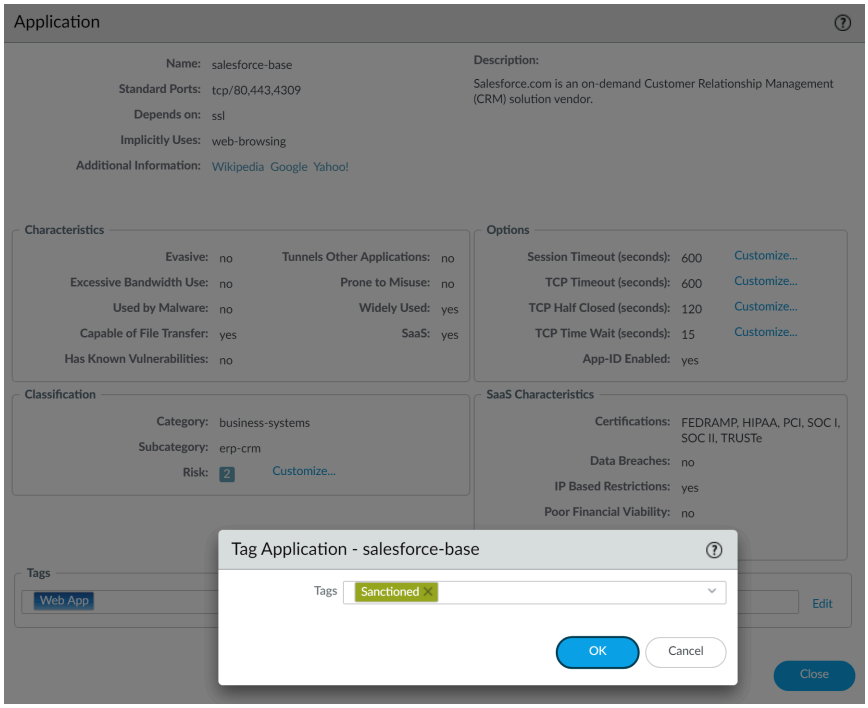
STEP 1 | 將您核准用於網路上的應用程式標記為 Sanctioned（已認可）。

如需產生準確且資訊詳盡的報告，您需要在擁有多個虛擬系統的防火牆以及屬於 *Panorama* 上某個裝置群組的防火牆上對認可應用程式採用一致的標記。若相同的應用程式在一個虛擬系統上被標記為認可，在另一個系統或 *Panorama* 上卻被標記為不被認可；應用程式在上級裝置群組中被標記為不被任可，在下級裝置群組中卻被標記為不被認可（反之亦然），則 *SaaS* 應用程式使用情況報告會將該應用程式報告為部分認可，並將會產生重疊的結果。

範例：若 Box 在 vsys1 上被認可，Google Drive 在 vsys2 上被認可，則 vsys1 中的 Google Drive 使用者將被計為不被認可的 SaaS 應用程式使用者，vsys2 中的 Box 使用者被計為不被認可的 SaaS 應用程式使用者。報告中的重要發現會強調在擁有兩個認可應用程式及兩個不被認可應用程式的網路上，共發現兩個獨特的 SaaS 應用程式。

1. 選取 **Objects**（物件）> **Applications**（應用程式）。
2. 按一下應用程式 **Name**（名稱）以編輯應用程式，然後選取標記區段的 **Edit**（編輯）。
3. 從 **Tags**（標籤）下拉式清單選取 **Sanctioned**（已認可）。

   必須使用預先定義的 **Sanctioned**（已認可）標籤 (Sanctioned)。若您使用任何其他標籤來表示您已認可某個應用程式，防火牆將無法識別該標籤，並且報告也會不準確。



4. 按一下 **OK**（確定）和 **Close**（關閉）以結束所有開啟的對話方塊。

©2024 Palo Alto Networks, Inc.

STEP 2 | 設定 SaaS 應用程式使用情況報告。

1. 選取 **Monitor**（監控） > **PDF Reports**（**PDF** 報告） > **SaaS Application Usage**（**SaaS** 應用程式使用情況）。
2. 按一下 **Add**（新增），輸入 **Name**（名稱），然後選取報告的 **Time Period**（時段）（預設值為 **Last 7 Days**（過去 **7** 天））。

   依預設，報告包有關前幾名 *SaaS* 及非 *SaaS* 應用程式子類別的詳細資訊，令報告頁數及檔案大小都會很大。若您要減小檔案大小並將頁數限制為 *10* 頁，可清除 ***Include detailed application category information in report***（在報告中包括詳細的應用程式類別資訊）核取方塊。
3. 選擇是否希望報告**Include logs from**（包含下列來源的日誌）：

   在 *PAN-OS 10.0.2* 和之後的版本中，根據 *Cortex* 資料湖中的日誌產生的報告僅支援包含來自 ***Selected Zone***（所選區域）的日誌。

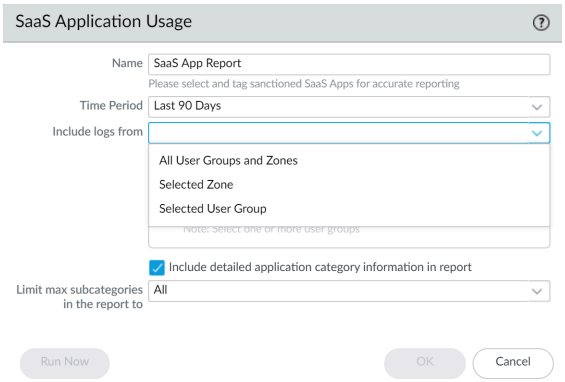
   - **All User Groups and Zones**（所有使用者群組及區域）—報告將包含日誌中可用的所有安全性區域和使用者群組資料。

     如果您要在報告中包含特定使用者群組，則選取 **Include user group information in the report**（在報告中包含使用者群組資訊），然後按一下 **manage groups**（管理群組）連結以選取您要包含的群組。您必須新增 1 到 25 個（上限）使用者群組，以便防火牆或 Panorama 能夠在日誌中篩選出選定的使用者群組。如果您選取了要包含的群組，報告會將所有使用者群組彙總到一個名稱為 Others（其他）的群組。
   - 選定區域—報告將篩選指定安全性區域的資料，並僅包含該區域的資料。

     如果您要在報告中包含特定使用者群組，則選取 **Include user group information in the report**（在報告中包含使用者群組資訊），然後按一下 **manage groups for selected zone**（管理選定區域的群組）連結，以選取您要在報告中包含的該區域內的使用者群組。您必須新增 1 到 25 個（上限）使用者群組，以便防火牆或 Panorama 能夠在日誌中篩選出該安全性區域內的選定使用者群組。如果您選取了要包含的群組，報告會將所有使用者群組彙總到一個名稱為 Others（其他）的群組。

 ©2024 Palo Alto Networks, Inc.

- **Selected User Group**（選定使用者群組）—報告將僅篩選指定使用者群組的資料，並僅包含選定使用者群組的 SaaS 應用程式使用情況資訊。



4. 選擇是要在報告中包含所有應用程式子類別（預設），還是將報告中的最大子類別數目限制為前 10、15、20 或 25 個類別（預設為所有子類別）。
5. 按一下 **Run Now**（立即執行），以視需要產生過去 7 天或 30 天的報告。由於報告在新的頁籤開啟，需確保快顯封鎖程式已停用。
6. 按一下 **OK**（確定）儲存您的變更。

STEP 3 | 排程以電子郵件傳遞報告。

過去 90 天的報告必須要排程電子郵件傳送。

在 PA-220R 和 PA-800 防火牆上，SaaS 應用程式使用情況將作為電子郵件中的 PDF 附件來傳送。反之，電子郵件則包括必須按一下才可在網頁瀏覽器中開啟報告的連結。

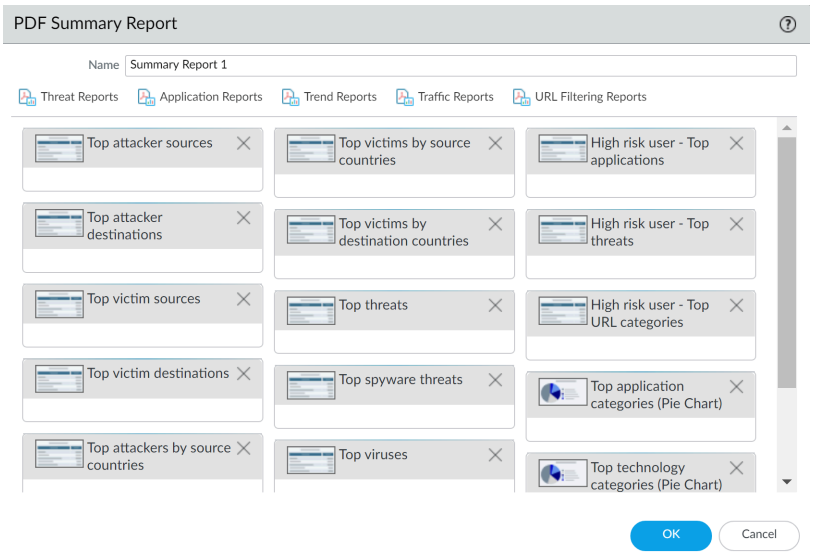
管理 PDF 摘要報告

PDF 摘要報告包括從現有報告收集的資訊，這些報告以每個類別中的前 5 個 (而非前 50 個) 資料為基礎。報告也包括其他報告中不可用的趨勢圖表。

©2024 Palo Alto Networks, Inc.

STEP 1 | 設定 **PDF** 摘要報告。

1. 選取 **Monitor**（監控） > **PDF Reports**（**PDF** 報告） > **Manage PDF Summary**（管理 **PDF** 摘要）。
2. 按一下 **Add**（新增），然後輸入報告的 **Name**（名稱）。
3. 使用每個報告群組的下拉式清單，並選取一或多個元素以設計 PDF 摘要報告。您可以包含最多 18 個報告元素。



在 *PDF* 摘要報告的「預先定義的 *Widgets*」欄中，選取 ***Top Threats***（威脅排序）顯示為攻擊排序。

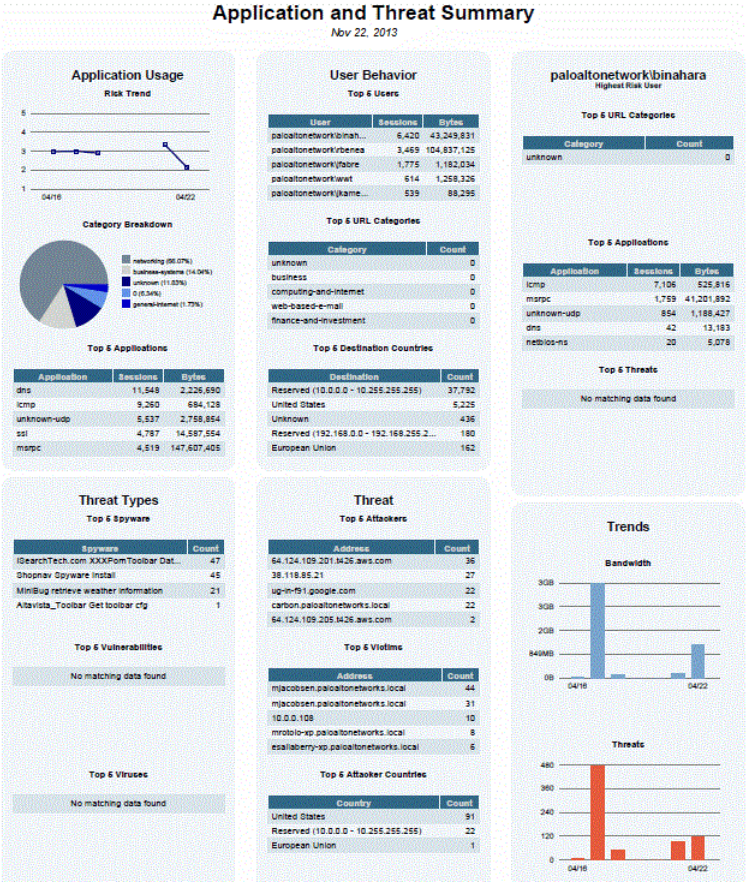
- 若要移除報告中的元素，請按一下 **x** 圖示，或清除適當報告群組其下拉式清單中的選擇。
- 若要重新排列報告，請將元素圖示拖放至報告中的其他區域。

4. 按一下**OK**（確定）儲存報告。
5. **Commit**（提交）變更。

©2024 Palo Alto Networks, Inc.

STEP 2 | 檢視報告。

若要下載與檢視 PDF 摘要報告，請參閱檢視報告。



以下摘要部分引用以下 *PDF* 摘要報告元素：

- ***Top 5 Attacks***（前五大攻擊）—引用威脅排名元素。
- ***Top 5 Threats***（前五大威脅）—引用高風險使用者- 威脅排名元素。
- 威脅排名報告—引用來自威脅排名元素中威脅的完整清單。

產生使用者/群組活動報告

使用者/群組活動報告會摘要個別使用者或使用者群組的 Web 活動。除了僅包含於使用者活動報告的 **Browsing Summary by URL Category**（**URL** 類別的瀏覽摘要）和 **Browse time calculations**（瀏覽時間計算）外，這兩個報告包含相同的資訊。

您必須在防火牆上設定 使用者-ID 才能存取使用者和使用者群組清單。

©2024 Palo Alto Networks, Inc.

STEP 1 | 設定使用者/群組活動報告的瀏覽次數和日誌數。

只有在您想變更預設值時才需要此項目。

1. 選取 **Device**（裝置） > **Setup**（裝置） > **Management**（管理），編輯 Logging and Reporting Settings（日誌記錄與報告設定），然後選取 **Log Export and Reporting**（日誌匯出與報告） 頁籤。
2. 針對 **Max Rows in User Activity Report**（使用者活動報告中的最大列數），輸入詳細使用者活動報告支援的最大列數（範圍是 1-1048576，預設值是 5000）。這會決定報告分析的日誌數。
3. 以秒數輸入 **Average Browse Time**（平均瀏覽時間），其為您預估使用者會用於瀏覽網頁的時間（範圍是 0-300，預設值是 60）。系統會將在平均瀏覽時間過去之後所做的任何要求都視為新瀏覽活動。計算會使用容器頁面（在 URL 篩選日誌中記錄）作為基礎，並忽略在第一個要求的時間（開始時間）與平均瀏覽時間之間載入的任何新網頁。例如，如果您將 **Average Browse Time**（平均瀏覽時間）設定為兩分鐘且使用者開啟網頁並檢視該頁面五分鐘，則該頁面的瀏覽時間仍將為兩分鐘。之所以會如此，是因為防火牆無法判斷使用者檢視指定頁面的時間。平均瀏覽時間計算會忽略分類為網路廣告與內容傳遞網路的網站。
4. 針對 **Page Load Threshold**（頁面載入臨界值），以秒數輸入頁面元素載入頁面的預估時間（預設值是 20）。系統會將在第一個頁面載入與頁面載入臨界值之間發生的任何要求假設為頁面元素。而將在頁面載入臨界值以外發生的任何要求假設為使用者按一下頁面內的連結。
5. 按一下 **OK**（確定）儲存您的變更。

STEP 2 | 產生使用者/群組活動報告。

1. 選取 **Monitor**（監控） > **PDF Reports**（**PDF** 報告） > **User Activity Report**（使用者活動報告）。
2. 按一下 **Add**（新增），然後輸入報告的 **Name**（名稱）。
3. 建立報告：
   - 使用者活動報告—選取 **User**（使用者），然後輸入使用者的 **Username**（使用者名稱）或 **IP address**（**IP** 位址）（IPv4 或 IPv6）。
   - 群組活動報告—選取 **Group**（群組），然後選取使用者群組的 **Group Name**（群組名稱）。
4. 選取用於產生報告的 **Time Period**（時段）。
5. （選用）選中 **Include Detailed Browsing**（包含詳細瀏覽）核取方塊（預設為清除），以在報告中包含詳細的 URL 日誌。

   詳細瀏覽資訊可能包含所選使用者或使用者群組的大量日誌 (數千個日誌)，並可能產生極大的報告。
6. 若要依需要執行報告，請按一下 **Run Now**（立即執行）。
7. 若要儲存報告設定，請按一下 **OK**（確定）。您無法在防火牆上儲存使用者/群組活動報告的輸出。若要排程以電子郵件傳遞報告，請參閱 排程以電子郵件傳遞報告。

©2024 Palo Alto Networks, Inc.

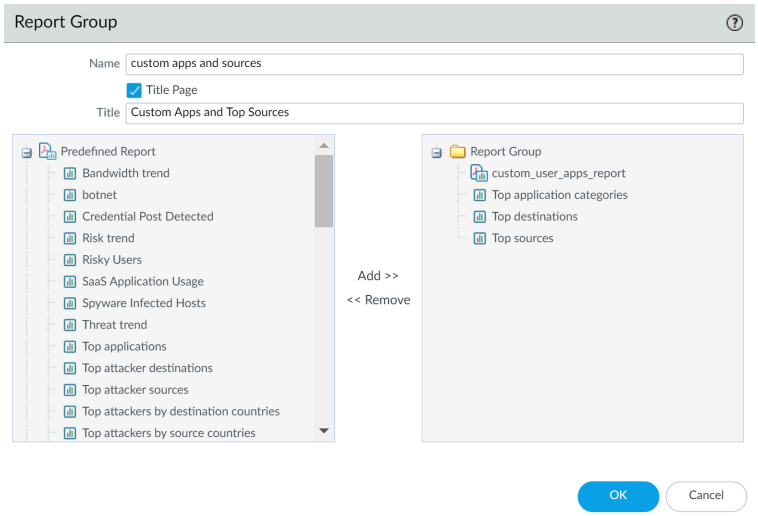
管理報告群組

報告群組可讓您建立系統可視作單一彙總 PDF 報告的報告集（包含可選標題頁面以及所有組成的報告），進行編譯與傳送。

設定報告群組。

您必須設定 **Report Group**（報告群組）才能以電子郵件傳送報告。

1. 建立電子郵件伺服器設定檔。
2. 定義 **Report Group**（報告群組）。報告群組會將預先定義的報告、PDF 摘要報告、自訂報告及日誌檢視報告編譯為單一 PDF。
   1. 選取 **Monitor**（監控） > **Report Group**（報告群組）。
   2. 按一下 **Add**（新增），然後輸入報告群組的 **Name**（名稱）。
   3. （選用）選取 **Title Page**（標題頁面），並新增 PDF 輸出的 **Title**（標題）。
   4. 從左欄中選取報告，然後按一下 **Add**（新增），將每個報告都移至右側的報告群組中。



   Log View（日誌檢視）報告是您每次建立自訂報告時自動建立的報告類型，使用的名稱與自訂報告相同。此報告將顯示建立自訂報告內容所用的日誌。

   若要包含日誌檢視資料，在建立報告群組時，您可以在 **Custom Reports**（自訂報告）清單下新增自訂報告，然後從 **Log View**（日誌檢視）清單中選取相符的報告名稱，以新增日誌檢視報告。報告將包括自訂報告資料，以及用來建立自訂報告的日誌資料。
   5. 按一下 **OK**（確定）以儲存設定。
   6. 若要使用報告群組，請參閱排程報告以進行電子郵件傳送。

©2024 Palo Alto Networks, Inc.

排程以電子郵件傳遞報告

您可以排程每天傳遞報告，或在每週的指定日期傳遞。排程報告於 2:00 AM 開始執行，產生所有排程的報告後，便開始用電子郵件傳遞。

STEP 1 | 選取 **Monitor**（監控） > **PDF Reports**（**PDF** 報告） > **Email Scheduler**（電子郵件排程器），然後按一下 **Add**（新增）。

STEP 2 | 輸入用來識別排程的 **Name**（名稱）。

STEP 3 | 選取要用電子郵件傳遞的 **Report Group**（報告群組）。若要設定報告群組，請參閱管理報告群組。

STEP 4 | 對於 **Email Profile**（電子郵件設定檔），選取電子郵件伺服器設定檔以用於傳遞報告，或按一下 **Email Profile**（電子郵件設定檔）連結以建立電子郵件伺服器設定檔。

STEP 5 | 在週期性中選取產生及傳送報告的頻率。

STEP 6 | **Override Email Addresses**（覆寫電子郵件位址）允許您將此報告只傳送至此欄位中指定的收件者。當您將收件者新增至該欄位時，防火牆不會將報告傳送至在電子郵件伺服器設定檔中設定的收件者。此選項適用於報告需要管理員或電子郵件伺服器設定檔中所定義收件者以外的人員注意時。

STEP 7 | 按一下 **OK**（確定）與 **Commit**（提交）。

管理報告儲存容量

依預設，防火牆包含 200MB 專用儲存空間，用於儲存其產生的報告。在某些情況下，特別是對於 PA-7000 系列和 PA-5200 系列防火牆，可能需要增加可用報告儲存空間的容量，以便成功產生新的報告。

STEP 1 | 存取防火牆 CLI。

STEP 2 | 確認防火牆目前的報告儲存容量：

命令輸出顯示報告儲存容量大小（位元組）。在此程序中，防火牆的預設報告儲存容量為 200MB。

```
admin@ISP-CONDOR-B(active)> request report-storage-size show

209715200
```


©2024 Palo Alto Networks, Inc.

STEP 3 | 擴展報告儲存容量量，確認防火牆上是否有足夠的儲存空間進行配置：

```
admin> show system disk-space
```

```
admin@ISP-CONDOR-B(active)> show system disk-space

Filesystem      Size  Used Avail Use% Mounted on
/dev/root        12G  8.9G  2.0G  83% /
none            7.9G   52K  7.9G   1% /dev
/dev/sda5        16G  8.5G  5.9G  59% /opt/pancfg
/dev/sda6        12G  5.8G  5.0G  54% /opt/panrepo
tmpfs           7.9G  247M  7.6G   4% /dev/shm
/dev/sda8        22G  8.7G   12G  43% /opt/panlogs
tmpfs            12M     0   12M   0% /opt/pancfg/mgmt/lcaas/ssl/private
```

STEP 4 | 視需要增加報告儲存容量：

例如，我們將報告儲存容量大小增加到 1GB。

```
admin> request report-storage-size set size <0-4>
```

```
admin@ISP-CONDOR-B(active)> request report-storage-size set size 1

cfg.report-storage-size-gb: 1
```

STEP 5 | 確認報告儲存容量是否已增加到上一步所設定的數量：

```
admin> request report-storage-size show
```

```
admin@ISP-CONDOR-B(active)> request report-storage-size show

1073741824
```

 ©2024 Palo Alto Networks, Inc.

檢視原則規則使用情況

檢視安全性、NAT、QoS、基於原則的轉送 (PBF)、解密、通道檢查、應用程式取代、驗證或 DoS 保護規則與流量相符的次數，以促使防火牆原則保持最新狀態，因為您的環境和安全性需進行變更。若要防止攻擊者利用過度佈建的存取（例如伺服器被解除，或者當您不再需要服務的暫時存取時），請使用原則規則命中數資料來識別並移除未使用的規則。

原則規則使用情況資料使您驗證規則增加以及規則變更情況，並可監控使用規則的時間範圍。例如，從以連接埠為基礎的規則移轉至以應用程式為基礎的規則時，您建立以應用程式為基礎的規則（優先順序高於以連接埠為基礎的規則），並檢查與以連接埠為基礎的規則相符的流量。移轉後，憑藉命中數資料，透過確認流量是否與以應用程式為基礎的規則（而非與以連接埠為基礎的規則）相符，可幫助您判斷是否可安全移除以連接埠為基礎的規則。原則規則命中數資料，有助於您判斷規則對於存取執行是否有效。

您可重設規則命中數資料，以驗證現有規則或衡量規則在指定時期內的使用情況。原則規則命中數資料未儲存在防火牆或 Panorama 中，因此在您重設（清除）命中數後，資料將不再可用。

篩選原則規則庫後，管理員可以採取動作直接從原則最佳化工具中刪除、停用、啟用和標記原則規則。例如，您可以篩選未使用的規則，然後標記它們以進行檢閱，從而確定可以安全地刪除它們還是將其保留在規則庫中。透過讓管理員能夠直接從原則最佳化工具中採取動作，可以減少進一步幫助簡化規則生命週期管理並確保防火牆沒有被過度佈建所需的管理負荷。

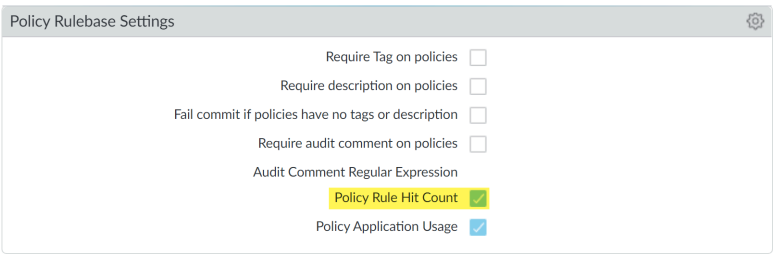
規則命中數資料不會在高可用性 *(HA)* 部署中的防火牆之間進行同步，因此您需登入各個防火牆檢視各防火牆的原則規則命中數資料，或使用 *Panorama* 檢視 *HA* 防火牆對等機上的資訊。

使用安全性原則規則最佳化以確定移轉或清除規則的優先順序時，政策規則使用情況資料也可能有用。

STEP 1 | 啟動 Web 介面.

STEP 2 | 確認是否已啟用 **Policy Rule Hit Count**（原則規則命中數）。

1. 導覽至 Policy Rulebase Settings（原則規則庫設定）（ **Device**（裝置） > **Setup**（設定） > **Management**（管理））。
2. 確認是否已啟用 **Policy Rule Hit Count**（原則規則命中數）。



STEP 3 | 選取 **Policies**（原則）。

©2024 Palo Alto Networks, Inc.

STEP 4 | 檢視各原則規則的規則使用情況：

- 命中數—流量與您在原則規則中定義的準則相符的次數。重新啟動、資料平面重新啟動以及升級後，仍然會存在，除非您手動重設或重新命名規則。
- 最後一次命中—流量與規則相符的最近的時間戳記。
- 第一次命中—流量與此規則相符的首個實例。
- 修改—原則規則上次修改的日期與時間。
- 建立—原則規則建立的日期與時間。

如果規則建立時 *Panorama* 執行 *PAN-OS 8.1* 並已啟用原則規則命中數設定，第一次命中日期與時間將用作升級至 *PAN-OS 9.0* 時的建立日期與時間。如果規則在 *PAN-OS 8.1* 防火牆中建立並已停用原則規則命中數設定，或如果規則在 *Panorama* 執行 *PAN-OS 8.0* 或更早版本時建立，為原則規則建立日期將為您成功升級*Panorama*至 *PAN-OS 9.0* 的日期與時間

		Source				Rule Usage				
NAME	T...	Z...	A...	U...		HIT COUNT	LAST HIT	FIRST HIT	MODIFIED	CREATED
Video	n...	a...	a...	a...		2424328	2020-09-22 11:33:00	2019-07-30 10:12:57	2020-07-27 13:27:16	2019-07-30 09:50
Video Streaming	n...	a...	a...	a...		14337228	2020-09-22 16:26:58	2019-07-30 10:12:57	2020-07-27 13:27:16	2019-07-30 09:50
Scavenger	n...	a...	a...	a...		321760616	2020-09-22 16:27:10	2019-07-30 10:12:57	2020-07-27 13:27:16	2019-07-30 09:50
Web Traffic	n...	a...	a...	a...		1509584361	2020-09-22 16:27:10	2019-07-30 10:12:02	2020-07-27 13:27:16	2019-07-30 09:50
iperf	n...	a...	a...	a...		5	2019-10-15 14:54:31	2019-10-11 13:08:28	2020-07-27 13:27:16	2019-07-30 09:50

STEP 5 | 在原則最佳化工具對話框中，檢視 **Rule Usage**（規則使用率）篩選器。

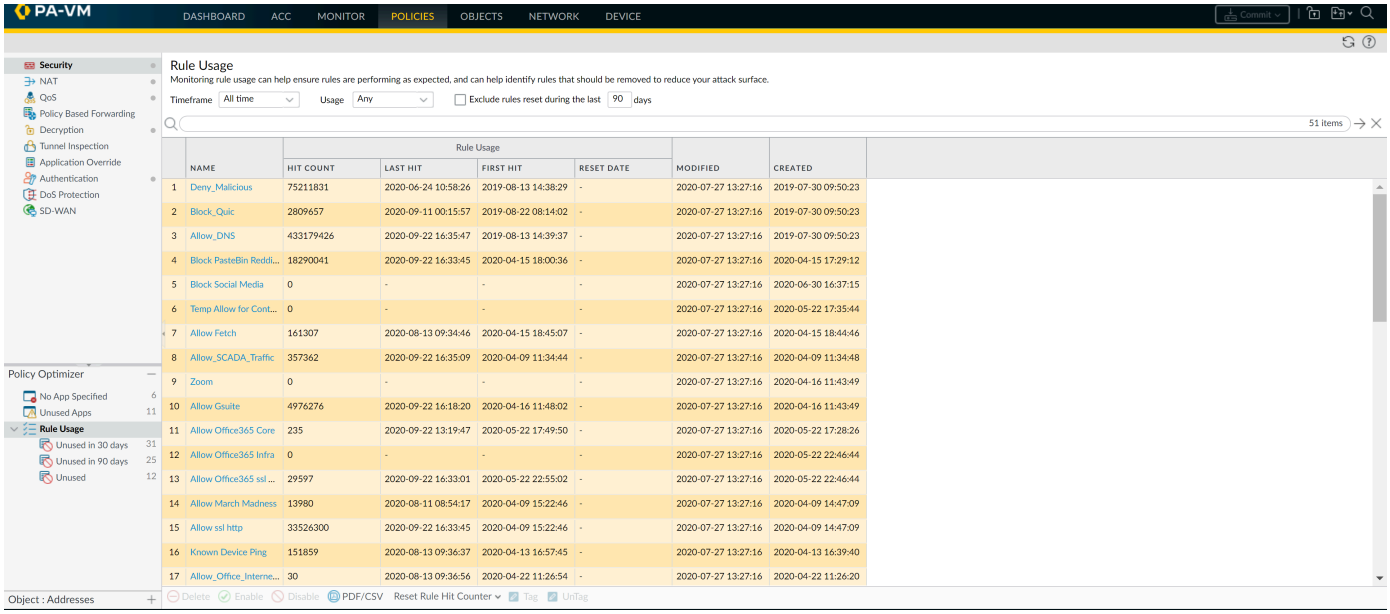
STEP 6 | 篩選所選規則庫中的規則。

使用規則使用情況篩選器評估指定時段內的規則使用情況。例如，為 *30* 天內未使用的規則篩選所選的規則庫。您還可評估具有其他規則屬性的規則使用情況，例如建立與修改日期使您能夠篩選要檢視的正確規則集。您可以使用此資料幫助管理您的規則生命週期，並確定是否需要移除規則以減少網路受攻擊面。

1. 選取要篩選的 **Timeframe**（時間範圍），或指定 **Custom**（自訂）時間範圍。
2. 選取要篩選的規則 **Usage**（使用情況）。
3. （選用）如果您重設了任何規則的規則使用情況資料，請檢查 **Exclude rules reset during the last <*number of days*> days**（排除最近 **<*number of days*>** 天內重設的規則），並確定

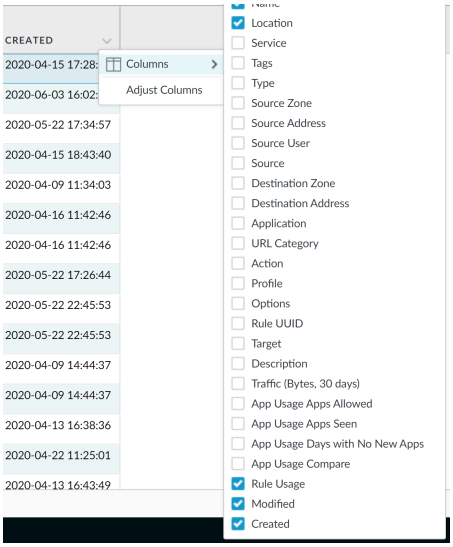
©2024 Palo Alto Networks, Inc.

根據自重設規則以來指定的天數排除規則的時間。僅在您指定天數之前重設的規則包含在篩選結果內。



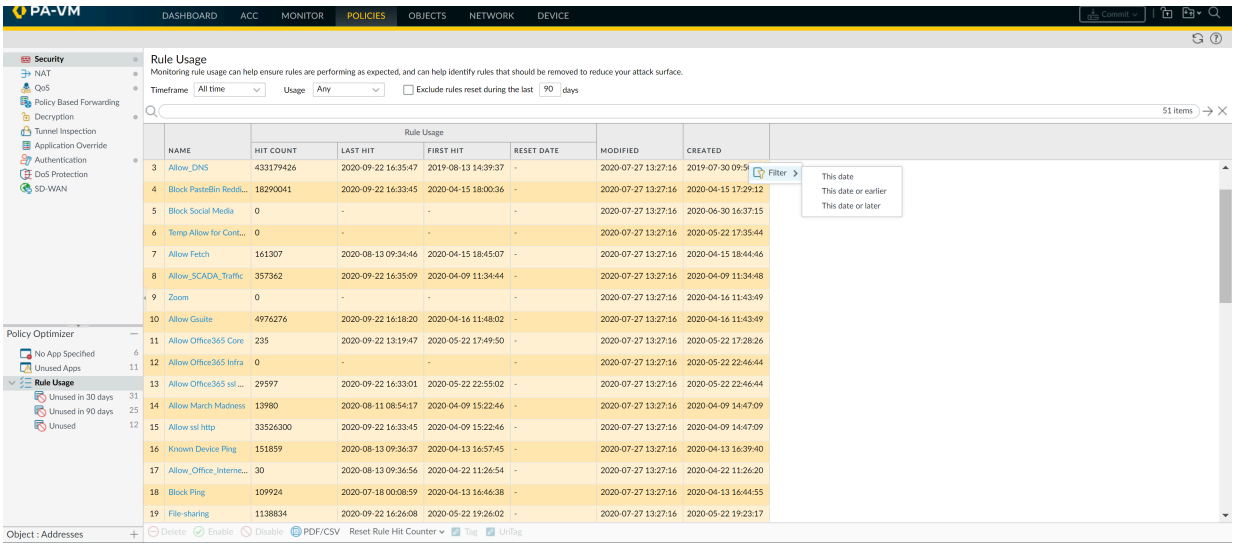
4. （選用）指定基於規則資料的搜尋篩選器

1. 將游標停留在欄標頭和 **Columns**（欄）上。
2. 新增您想要顯示或用於篩選器的任何其他欄。



3. 將游標停留在要在 **Filter**（篩選器）上進行篩選的欄資料上。針對包含日期的資料，選取使用 **This date**（此日期）、**This date or earlier**（此日期或更高）或 **This date or later**（此日期或更遲）進行篩選。
4. **Apply Filter**（套用篩選器）（→）。

©2024 Palo Alto Networks, Inc.



STEP 7 | 對一個或多個未使用的原則規則採取動作。

1. 選取一個或多個未使用的原則規則。
2. 執行下列其中一個動作：
   - 刪除—刪除一個或多個所選原則規則。
   - 啟用—在停用狀態下啟用一個或多個所選原則規則。
   - 停用—停用一個或多個所選原則規則。
   - 標記—將一個或多個群組標籤套用至一個或多個所選原則規則。群組標籤必須已經存在才可標記原則規則。
   - 取消標記—從一個或多個所選原則規則中移除一個或多個群組標籤。
3. **Commit**（提交）您的變更。

©2024 Palo Alto Networks, Inc.

使用外部服務進行監控

使用外部服務監控防火牆可讓您收到重要事件的警示、透過專用的長期儲存空間封存系統上的監控資訊，以及與協力廠商安全性監控工具整合。下列為使用外部服務的一些常見案例：

- 如需立即獲取有關重要系統事件或威脅的通知，您可使用 SNMP 監控統計資料、將設陷轉送至 SNMP 管理員或者設定電子郵件警示。
- 用於直接向任何暴露 API 的協力廠商服務傳送基於 HTTP 的 API 要求，以自動執行工作流量或動作。例如，您可以轉送符合所定義準則的日誌，以對 ServiceNow 建立發生票證，而不依賴外部系統將 syslog 訊息或 SNMP 設陷轉換成 HTTP 要求。您可以修改 HTTP 要求中的 URL、HTTP 標頭、參數以及裝載，以根據防火牆日誌中的屬性觸發相應動作。請參閱將日誌轉送至 HTTP(S) 目的地。
- 針對長期日誌儲存和集中化防火牆監控，您可以設定 Syslog 監控，將日誌資料傳送至 syslog 伺服器。這可與 Splunk 或 ArcSight 等協力廠商安全性監控工具整合。
- 針對周遊防火牆介面之 IP 流量的監控統計資料，您可以設定 NetFlow 匯出以檢視 NetFlow 收集器中的統計資料。

您可以設定日誌轉送（從防火牆直接轉送至外部服務，或從防火牆轉送至 Panorama），然後設定 Panorama 將日誌轉送至伺服器。決定轉送日誌的目的地時，請參閱日誌轉送選項以瞭解要考慮的因素。

您無法在 *Panorama* 上彙總 *NetFlow* 記錄；您必須將其從防火牆直接傳送至 *NetFlow* 收集器。

©2024 Palo Alto Networks, Inc.

設定日誌轉送

在使用多個防火牆控制和分析網路流量的環境中，任意一個防火牆只能針對其所監控的流量顯示日誌和報告。因為登入多個防火牆可能使監控變得異常繁重，您可以將所有防火牆的日誌轉送至 Panorama 或外部服務，以更高效地對網路活動實施全域監控。如果您 使用外部服務進行監控，防火牆會自動將日誌轉換成必要的格式：syslog 訊息、SNMP 設陷、電子郵件通知或 HTTP 有效負載，以將日誌詳細資料傳送至 HTTP(S) 伺服器。如果組織中的某些團隊能夠透過僅監控與其業務相關的日誌提高效率，您可以根據任何日誌屬性（例如威脅類型或來源使用者）建立轉送篩選器。例如，負責調查惡意軟體攻擊的安全性操作分析員可能僅對屬性設定為 wildfire-virus 的威脅日誌感興趣。

依預設，日誌透過管理介面轉送，除非您設定專門的服務路由來轉送日誌。轉送日誌的最大日誌記錄大小為 4,096 個位元組。日誌記錄大小超過最大值的轉送日誌將被截斷為 4,096 個位元組，未超過日誌記錄大小最大值的日誌則不會。

只有支援的日誌欄位才支援日誌轉送。轉送包含不受支援的日誌欄位或偽欄位的日誌會導致防火牆崩潰。

您可以將日誌直接從防火牆轉送至外部服務或從防火牆轉送至 *Panorama*，然後設定 Panorama 將日誌轉送至服務。決定轉送日誌的目的地時，請參閱日誌轉送選項以瞭解要考慮的因素。

您可以從 CLI 使用安全複本 (SCP) 命令，將整個日誌資料庫匯出至 *SCP* 伺服器，並將其匯入至其他防火牆。由於日誌資料庫太大，因此無法在不支援這些選項的 *PA-7000* 系列防火牆上實際執行匯出或匯入。您也可以使用所有平台上的網頁介面來檢視和管理報告，但只能以每個日誌類型為單位，無法匯出整個日誌資料庫。

STEP 1 | 針對每個將收到日誌資訊的外部服務設定伺服器設定檔。

您可以使用單獨的設定檔，將按照日誌屬性篩選的不同日誌集合傳送至不同的伺服器。若要增加可用性，請在單一設定檔中定義多個伺服器。

設定一或多個下列伺服器設定檔：

- （對 SMTP over TLS 為必需）如果尚未建立，則請為電子郵件伺服器建立憑證設定檔。
- 2若要啟用 SNMP 管理員（設陷伺服器）以判讀防火牆設陷，您必須將 Palo Alto Networks 支援的 MIB 載入至 SNMP 管理員，並視需要對其進行編譯。如需詳細資訊，請參閱 SNMP 管理軟體文件。
- 如果 syslog 伺服器要求進行用戶端驗證，您還必須 5
- 設定 HTTP 伺服器設定檔（請參閱 將日誌轉送至 HTTP/S 目的地）。

©2024 Palo Alto Networks, Inc.

STEP 2 | 建立日誌轉送設定檔。

設定檔中定義了流量、威脅、WildFire 提交、URL 篩選、資料篩選、通道及驗證日誌的目的地。

1. 選取 **Objects**（物件） > **Log Forwarding**（日誌轉寄），然後 **Add**（新增） 設定檔。
2. 輸入用來識別設定檔的 **Name**（名稱）。

   若要讓防火牆將設定檔自動指派給新的安全性規則和區域，請輸入 **`default`**。如果您不想要預設設定檔，或想要覆寫現有的預設設定檔，將該設定檔指派給安全性規則和區域時，請輸入可協助您識別設定檔的 **Name**（名稱）。

   如果不存在名為 ***`default`*** 的日誌轉送設定檔，雖然您可以變更選項，但在新的安全性規則（***Log Forwarding***（日誌轉送）欄位）和新的安全性地區（***Log Setting***（日誌設定）欄位）中，設定檔選項會預設為 ***None***（無）。
3. **Add**（新增）一個或多個比對清單設定檔。

   這些設定檔指定了日誌查詢篩選器、轉送目的地以及標記等自動動作。對於每個比對清單設定檔：

   1. 輸入用來識別設定檔的 **Name**（名稱）。
   2. 選取 **Log Type**（日誌類型）。
   3. 在 **Filter**（篩選器）下拉式清單中選取 **Filter Builder**（篩選器產生器）。指定下列選項，然後 **Add**（篩選器產生器）每項查詢：
      - **Connector**（連接器）邏輯（And/Or）
      - 日誌 **Attribute**（屬性）
      - **Operator**（運算子），用於定義包含或排除邏輯
      - 用於比對的查詢屬性 **Value**（值）
   4. 若您要將日誌轉送至日誌收集器或 Panorama 管理伺服器，請選取 **Panorama**。
   5. 對於您要用於監控的每種類型的外部服務（SNMP、電子郵件、Syslog 和 HTTP），**Add**（新增）一個或多個伺服器設定檔。
4. （選用，僅限 GlobalProtect）如果您使用具有安全性原則的日誌轉送設定檔來自動隔離使用 GlobalProtect 的裝置，請在 **Built-in Actions**（內建動作）區域選取 **Quarantine**（隔離）。
5. 按一下 **OK**（新增）以儲存日誌轉送設定檔。

©2024 Palo Alto Networks, Inc.

STEP 3 | 將日誌轉送設定檔指派給原則規則和網路區域。

安全性、嚴重和 DoS 保護規則支援日誌轉送。在此範例中，將設定檔指派給安全性規則。

針對要觸發日誌轉送的每個規則執行下列步驟：

1. 選取 **Policies**（原則） > **Security**（安全性），然後編輯規則。
2. 選取 **Actions**（動作）頁籤，然後選取所建立的 **Log Forwarding**（日誌轉送）設定檔。
3. 將 **Profile Type**（設定檔類型）設定為 **Profiles**（設定檔）或 **Group**（群組），然後選取相應的安全性設定檔或 **Group Profile**（群組設定檔）以觸發日誌產生和轉送：
   - 威脅日誌—流量必須符合指派給規則的任何安全性設定檔。
   - WildFire 提交日誌 — 流量必須符合指派給規則的 WildFire 分析設定檔。
4. 對於流量日誌，選取 **Log At Session Start**（開始時的日誌）及/或 **Log At Session End**（結束時的日誌）。

   Log At Session Start（工作階段開始時記錄）比僅在工作階段結束時記錄會耗用更多的資源。在大多數情況下，您只能 **Log At Session End**（工作階段結束時記錄）。啟用 **Log At Session Start**（工作階段開始時記錄）和 **Log At Session End**（工作階段結束時記錄）僅用於疑難排解、長期通道工作階段（例如 GRE 通道）（除非您在工作階段開始時記錄，否則您無法在 ACC 中看到這些工作階段），並獲得對營運技術/工業控制系統 (OT/ICS) 工作階段的可見性（這些工作階段也是長期工作階段）。
5. 按一下 **OK**（確定）來儲存規則。

STEP 4 | 設定系統、組態、關聯性、GlobalProtect、HIP 比對和 User-ID 日誌的目的地。

Panorama 會根據其收到的防火牆日誌而非彙總來自防火牆的關聯日誌，來產生關聯日誌。

1. 請選取 **Device**（裝置） > **Log Settings**（日誌設定）。
2. 對於防火牆將轉送的每種日誌類型，請參閱步驟新增一個或多個比對清單設定檔。

©2024 Palo Alto Networks, Inc.

STEP 5 | （僅限具有日誌處理卡的 PA-7000 Series 防火牆）設定日誌卡介面以執行日誌轉送。

從 *PAN OS 10.1* 開始，您不能再使用管理介面或服務路由轉送系統日誌和其他管理平面日誌。從具有執行 *PAN-OS 10.1* 或更新版本之 *LPC* 的 *PA-7000* 系列防火牆轉送系統日誌的唯一方法是設定日誌卡介面

1. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），然後按一下 **Add Interface**（新增介面）。
2. 選取 **Slot**（插槽）和 **Interface Name**（介面名稱）。
3. 將 **Interface Type**（介面名稱）設定為 **Log Card**（日誌卡）。
4. 輸入 **IP Address**（**IP** 位址）、**Default Gateway**（預設閘道）和（僅適用於 IPv4）**Netmask**（網路遮罩）。
5. 選取 **Advanced**（進階），然後指定 **Link Speed**（連結速度）、**Link Duplex**（連結雙工）與 **Link State**（連結狀態）。

   這些欄位預設為 ***auto***，其指定防火牆根據連接自動決定值。但是，任何連接的最小建議 ***Link Speed***（連結速度）為 ***1000 (Mbps)***。
6. 按一下 **OK**（確定）儲存您的變更。

©2024 Palo Alto Networks, Inc.

STEP 6 | （僅適用於 PA-5450 防火牆）設定日誌介面以執行日誌轉送。

如果您使用管理介面將日誌轉送到 *Panorama* 或 *Cortex Data Lake*，則不需要此步驟。依預設，管理介面處理日誌轉送，不需要設定日誌介面。

- （PAN-OS 10.2.0 和 10.2.1）依預設，管理介面處理日誌轉送，除非您設定了特定的服務路由用於日誌轉送。
- （PAN-OS 10.2.2 及更新版本）依預設，管理介面處理日誌轉送，除非您設定了日誌介面或特定的服務路由用於日誌轉送。如果設定並提交了日誌介面，則所有內部記錄、CDL、SNMP、HTTP 和 Syslog 都將由日誌介面轉送。

所有服務（例如 *SNMP*、*HTTP* 和 *Syslog*）都透過管理或資料介面進行路由。如果您為服務指定了特定的服務路由，則該服務路由優先於透過介面進行的日誌轉送。

確保您正在設定的日誌介面與管理介面不在同一個子網路中。在同一子網路中設定兩個介面可能會導致連線問題，並導致將錯誤的介面用於日誌轉送。

依預設，日誌連接埠（*LOG-1* 和 *LOG-2*）配套用作 *LAG*（連結彙總群組）。若要利用這兩個連接埠，必須將其連接到 *LAG* 感知交換機。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理）。
2. 選取 **Log Interface**（日誌介面）頂部功能表列上的設定齒輪。
3. 填寫 **IP Address**（**IP** 位址）、**Netmask**（網路遮罩）和 **Default Gateway**（預設閘道）欄位。

   如果您的網路使用 IPv6，請填寫 **IPv6 Address**（**IPv6** 位址）和 **IPv6 Default Gateway**（**IPv6** 預設閘道）欄位。

   當日誌介面設定了 *IP* 位址時，防火牆和 *Panorama* 之間的通訊會自動從由管理介面（預設）處理切換為由日誌介面處理。
4. 指定 **Link Speed**（連結速度）、**Link Duplex**（連結雙工）和 **Link State**（連結狀態）。

   這些欄位預設為 ***auto***，其指定防火牆根據連接自動決定值。
5. 按一下 **OK**（確定）儲存您的變更。

©2024 Palo Alto Networks, Inc.

STEP 7 | 認可並驗證變更。

1. **Commit**（提交）您的變更。
2. 確認您設定的日誌目的地已收到防火牆日誌：
   - Panorama—如果防火牆將日誌轉送至處於 Panorama 模式的 Panorama 裝置或轉送至 M 系列裝置，您必須設定收集器群組，Panorama 才會收到日誌。然後您可以驗證日誌轉送。
   - 電子郵件伺服器—確認指定收件者已透過電子郵件通知的形式收到日誌。
   - Syslog 伺服器—請參閱 syslog 伺服器文件以確認其將透過 syslog 訊息形式接收日誌。
   - SNMP 管理員—使用 SNMP 管理員探索 MIB 和物件 以驗證其以 SNMP 設陷形式接收日誌。
   - HTTP 伺服器—將日誌轉送至 HTTP/S 目的地。

©2024 Palo Alto Networks, Inc.

設定電子郵件警示

您可以設定系統、設定、HIP 比對、關聯、威脅、WildFire 提交和流量日誌的電子郵件警示。您可以使用個別設定檔，將每個日誌類型的電子郵件通知傳送至不同的伺服器。若要增加可用性，請在單一設定檔中定義多個伺服器（最多四個）。

最佳做法是設定傳輸層安全性 *(TLS)*，要求防火牆在將電子郵件轉送到伺服器之前對電子郵件伺服器進行驗證。這有助於防止惡意活動，如可用於傳送垃圾郵件或惡意軟體的簡易郵件傳輸通訊協定 *(SMTP)* 轉送，以及可用於網路釣魚攻擊的電子郵件詐騙。

STEP 1 | （對 SMTP over TLS 為必需）如果尚未建立，則請為電子郵件伺服器建立憑證設定檔。

STEP 2 | 選取 **Device**（裝置） > **Server Profiles**（伺服器設定檔） > **Email**（電子郵件）。

STEP 3 | **Add**（新增）電子郵件伺服器設定檔並輸入 **Name**（名稱）。

STEP 4 | 從顯示的唯讀視窗中，**Add**（新增）電子郵件伺服器並輸入 **Name**（名稱）。

STEP 5 | 若防火牆具有多個虛擬系統 (vsys)，請選取可在其中使用設定檔的 **Location**（位置）（vsys 或 **Shared**（共用））。

STEP 6 | （選用）輸入 **Email Display Name**（電子郵件顯示名稱，用於指定顯示在電子郵件 From（寄件者）欄位中的名稱。

STEP 7 | 輸入防火牆傳送電子郵件的電子郵件地址 **From**（寄件者）。

STEP 8 | 輸入防火牆傳送電子郵件的電子郵件地址 **To**（收件者）。

STEP 9 | （選用）如果您想要將電子郵件傳送到第二個帳戶，請輸入 **Additional Recipient**（其他收件者）的地址。您只能新增一位其他收件者。針對多位收件者，新增通訊群組清單的電子郵件地址。

STEP 10 | 輸入用於傳送電子郵件的電子郵件閘道的 IP 位址或主機名稱。

STEP 11 | 選取用於連線至電子郵件伺服器的通訊協定的 **Type**（類型）：

- **Unauthenticated SMTP**（未經驗證的 **SMTP**）—使用 SMTP 無需驗證連線到電子郵件伺服器。預設 **Port**（連接埠）為 25，但是您可以選擇指定其他連接埠。此通訊協定不會提供與 SMTP over TLS 相同的安全性，但如果您選取此通訊協定，則會跳過下一步驟。
- **SMTP over TLS**—（推薦）使用 TLS，以要求進行驗證才可連線到電子郵件伺服器。繼續下一步驟以設定 TLS 驗證。

©2024 Palo Alto Networks, Inc.

STEP 12 | （僅限 SMTP over TLS）設定防火牆以使用 TLS 驗證連線到電子郵件伺服器。

1. （選用）指定用於連線到電子郵件伺服器的 **Port**（連接埠）（預設值為 587）。
2. **TLS Version**（**TLS** 版本）—指定 TLS 版本（**1.1** 或 **1.2**）。

   Palo Alto Networks 強烈推薦使用最新 *TLS* 版本。

3. 為防火牆和電子郵件伺服器選取驗證方法：
   - **Auto**（自動）—允許防火牆和電子郵件伺服器確定驗證方法。
   - **Login**（登入）—使用者名稱和密碼使用 Base64 編碼，並將其分開傳輸。
   - **Plain**（純文字）—使用者名稱和密碼使用 Base64 編碼，並將其一起傳輸。
4. 選取一個 **Certificate Profile**（憑證設定檔）以對電子郵件伺服器進行驗證。
5. 輸入傳送電子郵件之帳戶的 **Username**（使用者名稱）和 **Password**（密碼），然後 **Confirm Password**（確認密碼）。
6. （選用）要確認防火牆能夠成功對電子郵件伺服器進行驗證，您可以 **Test Connection**（測試連線）。

STEP 13 | 按一下 **OK**（確定）以儲存電子郵件伺服器設定檔。

STEP 14 | （選用）選取**Custom Log Format**（自訂日誌格式）頁籤，然後自訂電子郵件訊息的格式。如需為各種日誌類型建立自訂格式的詳細資訊，請參閱《常見事件格式組態指南》。

STEP 15 | 設定流量、威脅和 WildFire 提交日誌的電子郵件警示。

1. 參閱建立日誌轉送設定檔。
   1. 選取 **Objects**（物件） > **Log Forwarding**（日誌轉送），按一下 **Add**（新增），然後輸入用來識別設定檔的 **Name**（名稱）。
   2. 針對每個日誌類型和嚴重性等級或 WildFire 裁定，選取電子郵件伺服器設定檔，然後按一下 **OK**（確定）。
2. 參閱將日誌轉送設定檔指派給原則規則和網路區域。

STEP 16 | 設定系統、設定、HIP 比對和關聯日誌的電子郵件警示。

1. 請選取 **Device**（裝置） > **Log Settings**（日誌設定）。
2. 針對系統和關聯日誌，按一下每個嚴重性等級，選取 **Email**（電子郵件）伺服器設定檔，然後按一下 **OK**（確定）。
3. 針對設定和 HIP 比對日誌，按一下（編輯）圖示，選取 **Email**（電子郵件）伺服器設定檔，然後按一下 **OK**（確定）。
4. 按一下 **Commit**（交付）。

©2024 Palo Alto Networks, Inc.

使用 Syslog 進行監控

系統日誌是標準日誌傳輸機制，可彙總不同網路裝置日誌資料（例如路由器、防火牆、印表機），將不同廠商的資料彙總為封存、分析及報告的中央儲存庫。Palo Alto Networks 防火牆可以轉送其針對外部 syslog 伺服器產生的所有日誌類型。您可以使用 TCP 或 TLS（僅限 TLSv1.2）執行可靠且安全的日誌轉送，或使用 UDP 執行非安全轉送。

- 設定 Syslog 監控
- Syslog 欄位說明
- Syslog 嚴重性參考手冊

設定 Syslog 監控

若要使用 Syslog 監控 Palo Alto Networks 防火牆，可建立 Syslog 伺服器設定檔，然後將其指派給每個日誌類型的日誌設定。（選用）您可以設定在 syslog 訊息中使用的標頭格式，並針對 TLSv1.2 上的 syslog 啟用用戶端驗證。

對於 CEF 格式的 syslog 事件收集，您必須編輯預設 *syslog* 設定。*CEF syslog* 事件收集不支援預設 *syslog* 監控設定。

©2024 Palo Alto Networks, Inc.

STEP 1 | 設定系統日誌伺服器設定檔。

您可以使用個別設定檔，將每個日誌類型的 *syslog* 傳送至不同的伺服器。若要增加可用性，請在單一設定檔中定義多個伺服器（最多四個）。

1. 選取 **Device**（裝置） > **Server Profiles**（伺服器設定檔） > **Syslog**。
2. 按一下 **Add**（新增），然後輸入設定檔的 **Name**（名稱）。
3. 若防火牆具有多個虛擬系統 (vsys)，請選取可在其中使用設定檔的 **Location**（位置）（vsys 或 **Shared**（共用））。
4. 針對每個 syslog 伺服器，按一下 **Add**（新增），然後輸入防火牆連線至該伺服器所需的資訊：
   - 名稱—伺服器設定檔的唯一名稱。
   - **Syslog** 伺服器—系Syslog 伺服器的 IP 位址或完全合格網域名稱 (FQDN)。

     如果您設定了 *FQDN* 並使用 ***UDP*** 傳輸，若防火牆無法解析 *FQDN*，則會使用 *FQDN* 的現有 *IP* 位址解析作為 ***Syslog Server***（***Syslog*** 伺服器）位址。
   - **Transport**（傳輸）—選取 **TCP**、**UDP** 或 **SSL** (TLS) 作為與 Syslog 伺服器通訊的通訊協定。對於 **SSL**，防火牆僅支援 TLSv1.2。
   - 連接埠—傳送 syslog 訊息的連接埠號碼（預設為連接埠 514 上的 UDP）；您必須在防火牆及 Syslog 伺服器上使用相同的連接埠號碼。
   - 格式—選取要使用的 syslog 訊息格式：**BSD**（預設值）或 **IETF**。傳統上，UDP 上為 **BSD** 格式，TCP 或 SSL/TLS 上則為 **IETF** 格式。
   - 裝置—選取 Syslog 標準值（預設值是 **LOG_USER**），以在 Syslog 伺服器實作中計算優先順序 (PRI) 欄位。選取對應如何將 PRI 欄位用於管理 syslog 訊息的值。
5. （選用）若要自訂防火牆所傳送 syslog 訊息的格式，請選取 **Custom Log Format**（自訂日誌格式）頁籤。如需為各種日誌類型建立自訂格式的詳細資訊，請參閱《常見事件格式組態指南》。
6. 按一下 **OK**（確定）來儲存伺服器設定檔。

©2024 Palo Alto Networks, Inc.

STEP 2 | 設定流量、威脅和 WildFire 提交日誌的 syslog 轉送。

1. 設定防火牆以轉送日誌。有關更多資訊，請參閱步驟建立日誌轉送設定檔。
   1. 選取 **Objects**（物件） > **Log Forwarding**（日誌轉送），按一下 **Add**（新增），然後輸入用來識別設定檔的 **Name**（名稱）。
   2. 針對每個日誌類型和嚴重性等級或 WildFire 裁定，選取 **Syslog** 伺服器設定檔，然後按一下 **OK**（確定）。
2. 將日誌轉送設定檔指派給安全性原則以觸發日誌產生和轉送。有關更多資訊，請參閱步驟將日誌轉送設定檔指派給原則規則和網路區域。
   1. 選取 **Policies**（原則） > **Security**（安全性），然後選取原則規則。
   2. 選取 **Actions**（動作）頁籤，然後選取所建立的 **Log Forwarding**（日誌轉送）設定檔。
   3. 對於流量日誌，選取**Log at Session Start**（工作階段開始時的日誌）並**Log At Session End**（工作階段結束時的日誌）中的一個或兩個，然後按一下 **OK**（確定）。

   如需設定日誌轉送設定檔和將設定檔指派給政策規則的詳細資訊，請參閱設定日誌轉送。

STEP 3 | 設定系統、設定、HIP 比對和關聯日誌的 syslog 轉送。

1. 請選取 **Device**（裝置） > **Log Settings**（日誌設定）。
2. 針對系統和關聯日誌，按一下每個嚴重性等級，選取 **Syslog** 伺服器設定檔，然後按一下 **OK**（確定）。
3. 針對組態、HIP 比對和關聯日誌，編輯此區段，選取 **Syslog** 伺服器設定檔，然後按一下 **OK**（確定）。

STEP 4 | （選用）設定 syslog 訊息的標頭格式。

日誌資料包含產生日誌之防火牆的唯一識別碼。選擇標頭格式可在某些安全性資訊與事件管理 (SIEM) 伺服器的日誌資料上更有彈性地進行篩選與報告作業。

這是全域設定，且會套用至在防火牆上設定的所有 Syslog 伺服器設定檔。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理），然後編輯 Logging and Reporting Settings（日誌記錄與報告設定）。
2. 選取 **Log Export and Reporting**（日誌匯出與報告）頁籤，然後選取 Syslog HOSTNAME Format（Syslog 主機名稱格式）：
   - **FQDN**（預設）—串連在傳送防火牆上定義的主機名稱與網域名稱。
   - 主機名稱—使用在傳送防火牆上定義的主機名稱。
   - **ipv4** 位址—使用用於傳送日誌之防火牆介面的 IPv4 位址。依預設，此為 MGT 介面。
   - **ipv6** 位址—使用用於傳送日誌之防火牆介面的 IPv6 位址。依預設，此為 MGT 介面。
   - 無—讓主機名稱欄位在防火牆上保持未設定。沒有傳送日誌的防火牆識別碼。
3. 按一下 **OK**（確定）儲存您的變更。

©2024 Palo Alto Networks, Inc.

STEP 5 | 建立憑證以保護 TLSv1.2 上的 syslog 通訊。

只有在 syslog 伺服器使用用戶端驗證時才需要此項目。Syslog 伺服器會使用憑證確認已授權防火牆與 Syslog 伺服器通訊。

請確保符合下列條件：

- 傳送防火牆必須有可用的私密金鑰；金鑰不得位於硬體安全性模組 (HSM)。
- 憑證的主體與簽發者絕對不能相同。
- Syslog 伺服器和傳送防火牆必須具有相同的信任憑證授權單位 (CA) 所簽署的憑證。或者，您可以在防火牆上產生自我簽署憑證、從防火牆匯出憑證，並將其匯入至 Syslog 伺服器。
- 只要信任鏈中的每個憑證都指定了這些延伸中的一個或兩個，就可以使用線上憑證狀態通訊協定　(OCSP) 或使用憑證撤銷清單 (CRL) 驗證透過 TLS 與 Syslog 伺服器進行的連線。但是，您無法繞過 OCSP 或 CRL 故障，因此必須確保憑證鏈有效，並且可以使用 OCSP 或 CRL 驗證每個憑證。

1. 選取 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證） > **Device Certificates**（裝置憑證），然後按一下 **Generate**（產生）。
2. 輸入憑證的名稱。
3. 在 **Common Name**（通用名稱）欄位中，輸入將日誌傳送至 syslog 伺服器的防火牆 IP 位址。
4. 在 **Signed by**（簽署者）中，選取信任的 CA，或 Syslog 伺服器及傳送防火牆都信任的自我簽署 CA。

   憑證不可以是 **Certificate Authority**（憑證授權單位）或 **External Authority**（外部授權）（憑證簽署要求[CSR]）。
5. 按一下 **Generate**（產生）。防火牆會產生憑證和金鑰配對。
6. 按一下憑證名稱以對其進行編輯，選取 **Certificate for Secure Syslog**（安全 **Syslog** 的憑證）核取方塊，然後按一下 **OK**（確定）。

STEP 6 | 提交變更並檢閱 Syslog 伺服器上的日誌。

1. 按一下 **Commit**（交付）。
2. 若要檢閱日誌，請參閱 syslog 管理軟體文件。您還可以檢閱 Syslog 欄位描述。

©2024 Palo Alto Networks, Inc.

STEP 7 | （選用）設定防火牆以在 FQDN 重新整理時終止與 syslog 伺服器的連線。

當您使用 FQDN 設定 syslog 伺服器設定檔時，依預設，防火牆會在 FQDN 名稱發生變更時保持與 syslog 伺服器的連線。

例如，您已將現有 syslog 伺服器替換為使用不同 FQDN 名稱的新 syslog 伺服器。如果您希望防火牆連線到使用新 FQDN 名稱的 syslog 伺服器，您可以將防火牆設定為自動終止其與舊 syslog 伺服器的連線，並與使用新 FQDN 名稱的新 syslog 伺服器建立連線。

1. 登入防火牆 CLI。
2. 設定防火牆以在 FQDN 重新整理時終止與 syslog 伺服器的連線。

```
admin> set syslogng fqdn-refresh yes
```

Syslog 欄位說明

下列主題會列出 Palo Alto Networks 防火牆可以轉送至外部伺服器之每個日誌類型的標準欄位，以及嚴重性等級、自訂格式和逸出序列。為了促進剖析，因此使用逗號作為分隔符號；每個欄位都是逗號分隔值 (CSV) 字串。FUTURE_USE 標籤會套用到該防火牆目前未實作的欄位。

WildFire 提交日誌是威脅日誌的子類型，且使用相同的 *syslog* 格式。

- 流量日誌欄位
- 威脅日誌欄位
- URL 篩選日誌欄位
- 資料篩選日誌欄位
- HIP 比對日誌欄位
- GlobalProtect 日誌欄位
- IP-Tag 日誌欄位
- User-ID 日誌欄位
- 解密日誌欄位
- 通道檢查日誌欄位
- SCTP 日誌欄位
- 組態日誌欄位
- 驗證日誌欄位
- 系統日誌欄位
- 關聯的事件日誌欄位
- GTP 日誌欄位
- 自訂日誌/事件格式

 ©2024 Palo Alto Networks, Inc.

- 逸出順序

流量日誌欄位

格式：FUTURE_USE、接收時間、序號、類型、威脅/內容類型、FUTURE_USE、產生時間、來源位址、目的地位址、NAT 來源 IP、NAT 目的地 IP、規則名稱、來源使用者、目的地使用者、應用程式、虛擬系統、來源區域、目的地區域、輸入介面、輸出介面、日誌動作、FUTURE_USE、工作階段 ID、重複計數、來源連接埠、目的地連接埠、NAT 來源連接埠、NAT 目的地連接埠、旗標、通訊協定、動作、位元組、已傳送位元組數、已接收位元組數、封包、開始時間、經過時間、類別、FUTURE_USE、序號、動作旗標、來源國家/地區、目的地國家/地區、FUTURE_USE、已傳送封包數、已接收封包數、工作階段結束原因、裝置群組階層層級 1、裝置群組階層層級 2、裝置群組階層層級 3、裝置群組階層層級 4、虛擬系統名稱、裝置名稱、動作來源、來源 VM UUID、目的地 VM UUID、通道 ID/IMSI、監控標籤/IMEI、上層工作階段 ID、上層開始時間、通道類型、SCTP 關聯 ID、SCTP 區塊、傳送的 SCTP 區塊數、接收的 SCTP 區塊數、規則 UUID、HTTP/2 連線、應用程式擺動計數、政策 ID、連結交換器、SD-WAN 叢集、SD-WAN 裝置類型、SD-WAN 叢集類型、SD-WAN 網站、動態使用者群組名稱、XFF 位址、來源裝置類別、來源裝置設定檔、來源裝置型號、來源裝置廠商、來源裝置作業系統系列、來源裝置作業系統版本、來源主機名稱、來源 Mac 位址、目的地裝置類別、目的地裝置設定檔、目的地裝置型號、目的地裝置廠商、目的地裝置作業系統系列、目的地裝置作業系統版本、目的地主機名稱、目的地 Mac 位址、容器 ID、POD 命名空間、POD 名稱、來源外部動態清單、目的地外部動態清單、主機 ID、序號、來源動態位址群組、目的地動態位址群組、工作階段擁有者、高解析度時間戳記、A 切片服務類型、A 切片差分器、應用程式子類別、應用程式類別、應用程式技術、應用程式風險、應用程式特性、應用程式容器、通道應用程式、應用程式 SaaS、應用程式認可狀態、卸載、流類型、叢集名稱

欄位名稱	說明
接收時間（receive_time 或 cef-formatted-receive_time）	在管理平面接收日誌的時間。
序號 (serial)	產生日誌之防火牆的序號。
類型 (type)	指定日誌類型；值為 TRAFFIC。
威脅/內容類型 (subtype)	流量日誌的子類型；值有開始、結束、丟棄與拒絕 • 開始—開始的工作階段 • 結束—結束的工作階段 • 丟棄—識別應用程式前丟棄的工作階段，且沒有允許工作階段的規則。 • 拒絕—識別應用程式後丟棄的工作階段，且有要封鎖的規則或沒有允許工作階段的規則。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
產生時間（time_generated 或 cef-formatted-time_generated）	在資料層上產生日誌的時間。
來源位址 (src)	原始工作階段來源 IP 位址。
目的地位址 (dst)	原始工作階段目的地 IP 位址。
NAT 來源 IP (natsrc)	如果已執行來源 NAT，則為後續 NAT 來源 IP 位址。
NAT 目的地 IP (natdst)	如果已執行目的地 NAT，則為後續 NAT 目的地 IP 位址。
規則名稱 (rule)	工作階段符合的規則名稱。
來源使用者 (srcuser)	啟動工作階段之使用者的使用者名稱。
目的地使用者 (dstuser)	將工作階段指定至之使用者的使用者名稱。
應用程式 (app)	與工作階段相關聯的應用程式。
虛擬系統 (vsys)	與工作階段相關聯的虛擬系統。
來源區域 (from)	工作階段的來源區域。
目的地區域 (to)	將工作階段指定至的區域。
輸入介面 (inbound_if)	工作階段的來源介面。
輸出介面 (outbound_if)	將工作階段指定至的介面。
日誌動作 (logset)	套用至工作階段的日誌轉送設定檔。
工作階段 ID (sessionid)	套用至每個工作階段的內部數字識別碼。
重複計數 (repeatcnt)	在 5 秒鐘內看到的有相同來源 IP、目的地 IP、應用程式與子類型的工作階段數。
來源連接埠 (sport)	工作階段使用的來源連接埠。
目的地連接埠 (dport)	工作階段使用的目的地連接埠。
NAT 來源連接埠 (natsport)	後續 NAT 來源連接埠。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
NAT 目的地連接埠 (natdport)	後續 NAT 目的地連接埠。
標幟 (flags)	32 位元欄位提供工作階段詳細資訊；您可以透過 AND 有記錄值的值解碼此欄位： • 0x80000000—工作階段有封包擷取 (PCAP) • 0x40000000—已啟用選項，允許用戶端使用多條路徑連線到目的地主機 • 0x20000000—指示是否已提交樣本以使用 WildFire 公共或私人雲端通道進行分析 • 0x10000000—偵測到一般使用者提交的企業認證 • 0x08000000—流量的來源在允許清單上，且不受偵察保護 • 0x02000000—IPv6 工作階段 • 0X01000000—解密 SSL 工作階段 (SSL Proxy) • 0x00800000—透過 URL 篩選拒絕工作階段 • 0x00400000—工作階段已執行 NAT 轉譯 • 0x00200000—透過驗證入口網站擷取工作階段的使用者資訊 • 0x00100000—應用程式流量位於非標準目的地連接埠 • 0x00080000—Proxy 中的 X-Forwarded-For 值在來源使用者欄位中 • 0x00040000—日誌對應至 http proxy 工作階段內的交易 (Proxy 交易) • 0x00020000—用戶端到伺服器的流量符合基於原則的轉送 • 0x00010000—伺服器到用戶端的流量符合基於原則的轉送 • 0x00008000—工作階段是容器頁面存取（容器頁面） • 0x00002000—工作階段暫時符合規則，以進行隱含應用程式相依性處理。適用於 PAN-OS 5.0.0 及以上版本。 • 0x00000800—對稱傳回用於轉送此工作階段的流量 • 0x00000400—解密的流量透過鏡像連接埠傳送出純文字 • 0x00000100—檢查外部通道的有效負載
IP 通訊協定 (proto)	與工作階段相關聯的 IP 通訊協定。
動作 (action)	針對工作階段採取的動作；可能的值為： • 允許—原則已允許工作階段

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
	• 拒絕—原則已拒絕工作階段 • 丟棄—無訊息丟棄工作階段 • 丟棄 ICMP—無訊息丟棄工作階段，並將 ICMP 無法連線訊息傳送至主機或應用程式 • 重設兩者—已終止工作階段，並將 TCP 重設傳送至連線的兩端 • 重設用戶端—已終止工作階段，並將 TCP 重設傳送至用戶端 • 重設伺服器—已終止工作階段，並將 TCP 重設傳送至伺服器
位元組 (bytes)	工作階段的位元組（傳輸與接收）總數。
傳送的位元組 (bytes_sent)	工作階段之用戶端至伺服器方向上的位元組數。
收到的位元組 (bytes_received)	工作階段之伺服器至用戶端方向上的位元組數。
封包數 (packets)	工作階段的封包（傳輸與接收）總數。
開始時間 (start)	工作階段開始的時間。
經過時間 (elapsed)	工作階段經過的時間。
類別 (category)	與工作階段相關聯的 URL 類別（如果適用）。
序號 (seqno)	依序遞增的 64 位元日誌項目識別碼；每個日誌類型有一個唯一編號空間。
動作旗標 (actionflags)	指示是否將日誌轉送至 Panorama 的位元欄位。
來源國家 (srcloc)	私人位址的來源國家/地區或內部地區；最大長度為 32 位元組。
目的地國家 (dstloc)	私人位址的目的地國家或內部地區。最大長度為 32 位元組。
已傳送的封包數 (pkts_sent)	工作階段之用戶端至伺服器封包數。
已接收的封包 (pkts_received)	工作階段之伺服器至用戶端封包數。
工作階段結束原因 (session_end_reason)	工作階段終止的原因。若有多個終止原因，此欄位只會顯示最高優先順序的原因。以下按優先順序的順序 (第一個最高) 顯示可能的工作階段結束原因值：

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
	• threat—防火牆偵測到與重設、丟棄或封鎖 (IP 位址) 動作相關聯的威脅。 • policy-deny—工作階段符合包含拒絕或丟棄動作的安全性規則。 • decrypt-cert-validation—當工作階段使用用戶端驗證或當工作階段使用任何條件（已到期、不受信任的發行者、未知狀態或狀態驗證逾時）的伺服器憑證時，工作階段會因將防火牆設定為封鎖 SSL 轉送代理程式解密或 SSL 輸入檢查 而終止。伺服器憑證產生以下類型的嚴重錯誤警示時也會顯示此工作階段的結束原因：bad_certificate、unsupported_certificate、certificate_revoked、access_de 或 no_certificate_RESERVED（僅限 SSLv3）。 • decrypt-unsupport-param—當工作階段使用不支援的通訊協定版本、加密或 SSH 演算法時，此工作階段會因將防火牆設定為封鎖 SSL 轉送代理程式解密或 SSL 輸入檢查時而終止。工作階段產生 unsupported_extension、unexpected_message 或 handshake_failure 類型的嚴重錯誤警示時，會顯示此工作階段結束原因。 • decrypt-error—當防火牆資源或硬體安全性模組 (HSM) 不可用時，此工作階段會因將防火牆設定為封鎖 SSL 轉送代理程式解密或 SSL 輸入檢查而終止。當將防火牆設定為封鎖發生 SSL 錯誤或產生嚴重錯誤警示（為 decrypt-cert-validation 和 decrypt-unsupport-param 結束原因所列之警示以外）的 SSL 流量時，也會顯示此工作階段結束原因。 • tcp-rst-from-client—用戶端將 TCP 重設傳送至伺服器。 • tcp-rst-from-server—伺服器將 TCP 重設傳送至用戶端。 • resources-unavailable—因系統資源限制而丟棄工作階段。例如，工作階段可能已超出每個流程所允許的順序紊亂封包數，或全域順序紊亂封包佇列。 • tcp-fin—連線中的兩個主機會傳送 TCP FIN 訊息來關閉工作階段。
	• tcp-reuse—工作階段重複使用，且防火牆關閉先前的工作階段。 • decoder—解碼器偵測到通訊協定中的新連線 (例如 HTTP-Proxy) 並結束先前的連線。 • aged-out—工作階段已逾期。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明

	• unknown—此值適用於下列情況：
	  • 上述原因未涵蓋的工作階段結束狀況 (例如，`clear session all` 命令)。
	  • 比 PAN-OS 6.1 版更舊的版本不支援工作階段結束原因欄位，以這些版本產生的日誌在升級至 PAN-OS 目前版本後或在將日誌載入到防火牆後，此值將為 **unknown**。
	  • 在 Panorama 中，從防火牆中針對不支援工作階段結束原因的 PAN-OS 版本所接收的日誌將具有值 **unknown**。
	• n/a—此值適用於流量日誌類型不是 **end** 時。

設備群組階層（dg_hier_level_1 到 dg_hier_level_4）	一系列的識別號碼，可表示設備群組在設備群組階層中的位置。產生日誌的防火牆（或虛擬系統）會在裝置群組階層中包含每個上階項目的識別號碼。此結構不包含共用設備群組（層級 0）。 如果日誌值為 12、34、45 或 0，這表示該日誌是由屬於裝置群組 45 且其上階項目為 34 和 12 的防火牆（或虛擬系統）所產生。若要檢視對應至值 12、34 或 45 的設備群組名稱，請使用下列其中一個方法： API 查詢： `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
虛擬系統名稱 (vsys_name)	與工作階段相關聯的虛擬系統名稱；只在已針對多個虛擬系統啟用的防火牆上有效。
設備名稱 (device_name)	已記錄工作階段的防火牆主機名稱。
動作來源 (action_source)	指定是否要針對已在應用程式或原則中定義的應用程式，採取允許或封鎖動作。動作包含針對工作階段允許、拒絕、丟棄、重設伺服器、重設用戶端或重設兩者。
來源 VM UUID (src_uuid)	在 VMware NSX 環境中識別來賓虛擬機器的來源通用唯一識別碼。
目的地 VM UUID (dst_uuid)	在 VMware NSX 環境中識別來賓虛擬機器的目的地通用唯一識別碼。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
通道 ID/IMSI (tunnelid/imsi)	國際行動用戶識別 (IMSI) 是為 GSM/UMTS/EPS 系統內每個行動用戶分配的唯一號碼。IMSI 必須僅由十進位數字 (0-9) 組成，允許的最大位數為 15 位。
監控標籤/IMEI (monitortag/imei)	國際行動裝置識別 (IMEI) 是為每個行動站裝置分配的唯一 15 或 16 位號碼。
上層工作階段 ID (parent_session_id)	此工作階段通道所在的工作階段 ID。僅適用於內部通道（若有兩層通道）或內部內容（若僅有一層通道）。
上層開始時間 (parent_start_time)	上層通道工作階段開始的年/月/日 時：分：秒。
通道類型 (tunnel)	通道的類型，例如 GRE 或 IPSec。
SCTP 關聯 ID (assoc_id)	識別兩個 SCTP 端點間關聯所對應的所有連線的號碼。
SCTP 區塊 (chunks)	為關聯所傳送與接收的 SCTP 區塊的總和。
傳送的 SCTP 區塊 (chunks_sent)	為關聯所傳送的 SCTP 區塊數。
接收的 SCTP 區塊 (chunks_received)	為關聯所接收的 SCTP 區塊數。
規則 UUID (rule_uuid)	永久識別規則的 UUID。
HTTP/2 連線 (http2_connection)	透過顯示以下一個值來確定流量是否使用了 HTTP/2 連線： • 上層工作階段 ID—HTTP/2 連線 • 0—SSL 工作階段
應用程式擺動計數 (link_change_count)	工作階段期間發生的連結擺動次數。
原則 ID (policy_id)	SW-WAN 原則的名稱。
連結交換器 (link_switches)	最多包含四個連結擺動項目，每個項目包含連結名稱、連結標籤、連結類型、實體介面、時間戳記、讀取的位元組、寫入的位元組、連結健康情況和連結擺動原因。
SD-WAN 叢集 (sdwan_cluster)	SW-WAN 叢集的名稱。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
SD-WAN 裝置類型 (sdwan_device_type)	裝置類型（中樞或分支）。
SD-WAN 叢集類型 (sdwan_cluster)	叢集類型（網狀或中樞 - 支點）。
SD-WAN 網站 (sdwan_site)	SW-WAN 網站的名稱。
動態使用者群組名稱 (dynusergroup_name)	包含啟動工作階段的使用者的動態使用者群組名稱。
XFF 位址 (xff_ip)	要求網頁之使用者的 IP 位址或要求周遊之倒數第二個裝置的 IP 位址。如果要求通過一個或多個 Proxy、負載平衡器或其他上游裝置，則防火牆將顯示最新裝置的 IP 位址。 基於不同的設備實施，*XFF* 欄位可能包含非 *IP* 位址值。
來源裝置類別 (src_category)	Device-ID 識別為流量來源的裝置的類別。
來源裝置設定檔 (src_profile)	Device-ID 識別為流量來源的裝置的裝置設定檔。
來源裝置型號 (src_model)	Device-ID 識別為流量來源的裝置的型號。
來源裝置廠商 (src_vendor)	Device-ID 識別為流量來源的裝置的廠商。
來源裝置作業系統系列 (src_osfamily)	Device-ID 識別為流量來源的裝置的作業系統類型。
來源裝置作業系統版本 (src_osversion)	Device-ID 識別為流量來源的裝置的作業系統版本。
來源主機名稱 (src_host)	Device-ID 識別為流量來源的裝置的主機名稱。
來源 MAC 位址 (src_mac)	Device-ID 識別為流量來源的裝置的 MAC 位址。
目的地裝置類別 (dst_category)	Device-ID 識別為流量目的地的裝置的類別。
目的地裝置設定檔 (dst_profile)	Device-ID 識別為流量目的地的裝置的裝置設定檔。
目的地裝置型號 (dst_model)	Device-ID 識別為流量目的地的裝置的型號。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
目的地裝置廠商 (dst_vendor)	Device-ID 識別為流量目的地的裝置的廠商。
目的地裝置作業系統系列 (dst_osfamily)	Device-ID 識別為流量目的地的裝置的作業系統類型。
目的地裝置作業系統版本 (dst_osversion)	Device-ID 識別為流量目的地的裝置的作業系統版本。
目的地主機名稱 (dst_host)	Device-ID 識別為流量目的地的裝置的主機名稱。
目的地 MAC 位址 (dst_mac)	Device-ID 識別為流量目的地的裝置的 MAC 位址。
容器 ID (container_id)	部署應用程式 POD 之 Kubernetes 節點上 PAN-NGFW pod 的容器 ID。
POD 命名空間 (pod_namespace)	受保護應用程式 POD 的命名空間。
POD 名稱 (pod_name)	受保護的應用程式 POD。
來源外部動態清單 (src_edl)	包含流量來源 IP 位址的外部動態清單的名稱。
目的地外部動態清單 (dst_edl)	包含流量目的地 IP 位址的外部動態清單的名稱。
主機 ID (hostid)	GlobalProtect 為識別主機所指派的唯一 ID。
使用者裝置序列號 (serialnumber)	使用者電腦或裝置的序列號。
來源動態位址群組 (src_dag)	原始工作階段來源動態位址群組。
目的地動態位址群組 (dst_dag)	原始目的地來源動態位址群組。
工作階段擁有者 (session_owner)	高可用性叢集中的原始高可用性 (HA) 對等工作階段擁有者，在 HA 容錯移轉時會從中同步工作階段表格資料。
高解析度時間戳記 (high_res_timestamp)	在管理平面接收日誌的時間（毫秒）。 此新欄位的格式為 YYYY-MM-DDThh:ss:sssTZD： • **YYYY**—四位數表示年份 • **MM**—二位數表示月份 • **DD**—二位數表示當月的日期（01 到 31）

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
	• **T**—時間戳記開始的指標 • **hh**—兩位數表示小時（使用 24 小時制，00 到 23） • **mm**—兩位數表示分鐘（00 到 59） • **ss**—兩位數表示秒鐘（00 到 60） • **sss**—一位或多位數表示毫秒 • **TZD**—時區指示項（+hh:mm 或 -hh:mm） 對於從執行 *PAN-OS 10.0* 和後續版本的受管理防火牆接收的日誌，支援高解析度時間戳記。從執行 *PAN-OS 9.1* 及早前版本的防火牆接收的日誌顯示 `1969-12-31T16:00:00:000-8:00` 時間戳記，而不論接收日誌的時間如何。
A 切片服務類型 (nsdsai_sst)	網路切片 ID 的 A 切片服務類型。
A 切片差分器 (nsdsai_sd)	網路切片 ID 的 A 切片差分器。
應用程式子類別 (subcategory_of_app)	應用程式設定屬性中指定的應用程式子類別。
應用程式類別 (category_of_app)	應用程式設定屬性中指定的應用程式類別。值為： • 業務系統 • 協同作業 • 一般網際網路 • 媒體 • 網路 • saas
應用程式技術 (technology_of_app)	應用程式設定屬性中指定的應用程式技術。值為： • browser-based • client-server • network-protocol • peer-to-peer
應用程式風險 (risk_of_app)	與應用程式關聯的風險層級（1 = 最低，5 = 最高）。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
應用程式特性 (characteristic_of_app)	應用程式適用特性的逗號分隔清單
應用程式容器 (container_of_app)	應用程式的父應用程式。
通道應用程式 (tunneled_app)	通道應用程式的名稱。
應用程式 SaaS (is_saas_of_app)	如果是 SaaS 應用程式，則顯示 `1` ，如果不是 SaaS 應用程式，則顯示 `0`。
應用程式認可狀態 (sanctioned_state_of_app)	如果應用程式受認可，則顯示 `1`，如果應用程式不受認可，則顯示 `0`。
已卸載 (offloaded)	如果已卸載流量，則顯示 `1`；如果未卸載流量，則顯示 `0`。
流類型 (flow_type)	標識用於流量的 Proxy 類型。如果使用 Proxy，則顯示 `Explicit Proxy`（明確 `Proxy`）或 `Transparent Proxy`（透明 `Proxy`）。如果未使用 Proxy，則顯示 `NonProxyTraffic`。
叢集名稱 (cluster_name)	CN-Series 防火牆叢集的名稱。

威脅日誌欄位

格式：FUTURE_USE、接收時間、序號、類型、威脅/內容類型、FUTURE_USE、產生時間、來源位址、目的地位址、NAT 來源 IP、NAT 目的地 IP、規則名稱、來源使用者、目的地使用者、應用程式、虛擬系統、來源區域、目的地區域、輸入介面、輸出介面、日誌動作、FUTURE_USE、工作階段 ID、重複計數、來源連接埠、目的地連接埠、NAT 來源連接埠、NAT 目的地連接埠、旗標、IP 通訊協定、動作、URL/檔案名稱、威脅 ID、類別、嚴重性、方向、序號、動作旗標、來源位置、目的地位置、FUTURE_USE、內容類型、PCAP_ID、檔案摘要、雲端、URL 索引、使用者代理程式、檔案類型、X-Forwarded-For、轉介者、寄件者、主旨、收件者、報告 ID、裝置群組階層層級 1、裝置群組階層層級 2、裝置群組階層層級 3、裝置群組階層層級 4、虛擬系統名稱、裝置名稱、FUTURE_USE、來源 VM UUID、目的地 VM UUID、HTTP 方法、通道 ID/IMSI、監控標籤/IMEI、上層工作階段 ID、上層開始時間、通道類型、威脅類別、內容版本、FUTURE_USE、SCTP 關聯 ID、有效負載通訊協定 ID、HTTP 標頭、URL 類別清單、規則 UUID、HTTP/2 連線、動態使用者群組名稱、XFF 位址、來源裝置類別、來源裝置設定檔、來源裝置型號、來源裝置廠商、來源裝置作業系統系列、來源裝置作業系統版本、來源主機名稱、來源 MAC 位址、目的地裝置類別、目的地裝置設定檔、目的地裝置型號、目的地裝置廠商、目的地裝置作業系統系列、目的地裝置作業系統版本、目的地主機名稱、目的地 MAC 位址、容器 ID、POD 命名空間、POD 名稱、來源外部動態清單、目的地外部動態清單、主機 ID、序號、網域 EDL、來源動態位址群組、目的地動態位址群組、部分雜湊、高解析度時間戳記、原因、理由、A

©2024 Palo Alto Networks, Inc.

切片服務類型、應用程式子類別、應用程式類別、應用程式技術、應用程式風險、應用程式特性、應用程式容器、應用程式 SaaS、通道應用程式、應用程式認可狀態、雲端報告 ID

欄位名稱	說明
接收時間（receive_time 或 cef-formatted-receive_time）	在管理平面接收日誌的時間。
序號 (Serial #)	產生日誌之防火牆的序號。
類型 (type)	指定日誌類型；值為 THREAT。
威脅/內容類型 (subtype)	威脅日誌的子類型。值包括以下項： • 資料—符合資料篩選設定檔的資料模式。 • 檔案—符合檔案封鎖設定檔的檔案類型。 • 流量—透過區域保護設定檔偵測到的流量。 • 封包—區域保護設定檔觸發的以封包為基礎的攻擊保護。 • 掃描—透過區域保護設定檔偵測到的掃描。 • 間諜軟體—透過反間諜軟體設定檔偵測到的間諜軟體。 • url—URL 篩選日誌。 • ml-virus—病毒由 WildFire 內嵌 ML 透過防毒設定檔偵測到。 • 病毒—透過防毒軟體設定當偵測到的病毒。 • 漏洞—透過漏洞保護設定當偵測到的漏洞入侵。 • wildfire—防火牆依 WildFire 分析設定檔將檔案提交至 WildFire 時產生的 WildFire 裁定，WildFire 提交日誌中會記錄裁定（惡意軟體、網路釣魚、灰色軟體或良性，取決於您記錄的內容）。 • wildfire 病毒—透過防毒軟體設定當偵測到的病毒。
產生時間（time_generated 或 cef-formatted-time_generated）	在資料層上產生日誌的時間。
來源位址 (src)	原始工作階段來源 IP 位址。
目的地位址 (dst)	原始工作階段目的地 IP 位址。
NAT 來源 IP (natsrc)	如果已執行來源 NAT，則為後續 NAT 來源 IP 位址。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
NAT 目的地 IP (natdst)	如果已執行目的地 NAT，則為後續 NAT 目的地 IP 位址。
規則名稱 (rule)	工作階段符合的規則名稱。
來源使用者 (srcuser)	啟動工作階段之使用者的使用者名稱。
目的地使用者 (dstuser)	將工作階段指定至之使用者的使用者名稱。
應用程式 (app)	與工作階段相關聯的應用程式。
虛擬系統 (vsys)	與工作階段相關聯的虛擬系統。
來源區域 (from)	工作階段的來源區域。
目的地區域 (to)	將工作階段指定至的區域。
輸入介面 (inbound_if)	工作階段的來源介面。
輸出介面 (outbound_if)	將工作階段指定至的介面。
日誌動作 (logset)	套用至工作階段的日誌轉送設定檔。
工作階段 ID (sessionid)	套用至每個工作階段的內部數字識別碼。
重複計數 (repeatcnt)	在 5 秒鐘內看到的有相同來源 IP、目的地 IP、應用程式與內容/威脅類型的工作階段數。
來源連接埠 (sport)	工作階段使用的來源連接埠。
目的地連接埠 (dport)	工作階段使用的目的地連接埠。
NAT 來源連接埠 (natsport)	後續 NAT 來源連接埠。
NAT 目的地連接埠 (natdport)	後續 NAT 目的地連接埠。
標幟 (flags)	32 位元欄位提供工作階段詳細資訊；您可以透過 AND 有記錄值的值解碼此欄位： • 0x80000000—工作階段有封包擷取 (PCAP) • 0x40000000—已啟用選項，允許用戶端使用多條路徑連線到目的地主機

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
	• 0x20000000—檔案已提交給 WildFire 進行裁定 • 0x10000000—偵測到一般使用者提交的企業認證 • 0x08000000—流量的來源在允許清單上，且不受偵察保護 • 0x02000000—IPv6 工作階段 • 0X01000000—解密 SSL 工作階段 (SSL Proxy) • 0x00800000—透過 URL 篩選拒絕工作階段 • 0x00400000—工作階段已執行 NAT 轉譯 • 0x00200000—透過驗證入口網站擷取工作階段的使用者資訊 • 0x00100000—應用程式流量位於非標準目的地連接埠 • 0x00080000—Proxy 中的 X-Forwarded-For 值在來源使用者欄位中 • 0x00040000—日誌對應至 http proxy 工作階段內的交易（Proxy 交易） • 0x00020000—用戶端到伺服器的流量符合基於原則的轉送 • 0x00010000—伺服器到用戶端的流量符合基於原則的轉送 • 0x00008000—工作階段是容器頁面存取（容器頁面） • 0x00002000—工作階段暫時符合規則，以進行隱含應用程式相依性處理。適用於 PAN-OS 5.0.0 及以上版本。 • 0x00000800—對稱傳回用於轉送此工作階段的流量 • 0x00000400—解密的流量透過鏡像連接埠傳送出純文字 • 0x00000010—檢查外部通道的有效負載
IP 通訊協定 (proto)	與工作階段相關聯的 IP 通訊協定。
動作 (action)	針對工作階段採取的動作；值有（警示）、（允許）、（拒絕）、（丟棄）、（丟棄所有封包）、（重設用戶端）、（重設伺服器）、（重設兩者）、（封鎖 url）。 • 警示—偵測到威脅或 URL 但未封鎖 • 允許—流量偵測警示 • 拒絕—流量偵測機制啟動，並根據組態拒絕流量 • 丟棄—偵測到威脅並丟棄關聯的工作階段 • 重設用戶端—偵測到威脅，並將 TCP RST 傳送到用戶端 • 重設伺服器—偵測到威脅，並將 TCP RST 傳送到伺服器 • 重設兩者—偵測到威脅，並將 TCP RST 傳送到用戶端與伺服器

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
	• 封鎖 url—已封鎖 URL 要求，因為它符合設為封鎖的 URL 類別 • 封鎖-ip—偵測到威脅，而且用戶端 IP 已封鎖 • 隨機丟棄—偵測到流量，而且封包已隨機丟棄 • sinkhole—DNS sinkhole 已啟動 • syncookie 已傳送—syncookie 警示 • 封鎖-繼續（僅 URL 子類型）—HTTP 請求遭到封鎖並重新導向至繼續頁面，其中包含確認繼續的按鈕 • 繼續（僅 URL 子類型）—回應封鎖-繼續 URL 繼續頁面，表明允許執行封鎖-繼續請求 • 封鎖-取代（僅 URL 子類型）—HTTP 請求遭到封鎖並重新導向至管理員取代頁面，要求防火牆管理員提供密碼以繼續 • 取代-鎖定（僅 URL 子類型）—來源 IP 的管理員取代密碼嘗試失敗次數過多。封鎖-取代重新導向頁面現在已封鎖 IP • 取代（僅 URL 子類型）—回應封鎖-取代頁面，並提供正確密碼，請求已獲允許 • 封鎖（僅 Wildfire）—檔案已遭到防火牆封鎖並已上傳至 Wildfire
URL/檔案名稱 (misc)	具有變動長度的欄位。檔案名稱最多包含 63 個字元。URL 最多包含 1023 個字元 子類型為 URL 時的實際 URI 子類型為檔案時的檔案名稱或檔案類型 子類型為病毒時的檔案名稱 子類型為 Wildfire 病毒時的檔案名稱 子類型為 WildFire 時的檔案名稱 子類型為漏洞時的 URL 或檔案名稱（如果適用） Threat Category（威脅類型）為 `domain-edl` 時的 URL 偵測到主機標頭不相符項（由唯一威脅 ID 86467 識別）時的欺騙性 SNI 網域。
威脅/內容名稱 (threatid)	已知和自訂威脅的 Palo Alto Networks 識別碼。這是某些子類型的描述字串，後面加上以括號括住的 64 位元數字識別碼： • 8000 - 8099—掃描偵測 • 8500 - 8599—流量偵測 • 9999—URL 篩選日誌

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
	• 10000 - 19999—間諜軟體打電話回家偵測 • 20000 - 29999—間諜軟體下載偵測 • 30000 - 44999—漏洞利用偵測 • 52000 - 52999—檔案類型偵測 • 60000 - 69999—資料篩選偵測 如果 Domain EDL（網域 EDL）欄位已填寫，那麼此欄位會填入相同的值。 之前版本中使用的病毒偵測、*WildFire* 特徵碼摘要以及 *DNS C2* 特徵碼的威脅 *ID* 範圍將被永久性的全域唯一 *ID* 取代。請參閱威脅/內容類型（子類型）和威脅類別 *(thr_category)* 欄位名稱，以建立更新報告、篩選威脅日誌以及 *ACC* 活動。
類別 (category)	針對 URL 子類型，其為 URL 類別；針對 WildFire 子類型，其為「惡意軟體」、「網路釣魚」「灰色軟體」或「良性」的檔案裁定；針對其他子類型，該值為「any」（任何）。
嚴重性 (severity)	與威脅相關聯的嚴重性；值有（資訊）、（低）、（中）、（高）、（重要）。
方向 (direction)	表示攻擊的方向，為用戶端到伺服器或伺服器到用戶端： • 0—表示威脅方向為用戶端到伺服器 • 1—表示威脅方向為伺服器到用戶端
序號 (seqno)	依序遞增的 64 位元日誌項目識別碼。每個日誌類型有一個唯一編號空間。
動作旗標 (actionflags)	指示是否將日誌轉送至 Panorama 的位元欄位。
來源國家 (srcloc)	私人位址的來源國家或內部地區。最大長度為 32 位元組。
目的地國家 (dstloc)	私人位址的目的地國家或內部地區。最大長度為 32 位元組。
內容類型 (contenttype)	僅當子類型是 URL 時可用。 HTTP 回應資料的內容類型。最大長度 32 位元組。
PCAP ID (pcap_id)	封包擷取 (pcap) ID 是 64 位元未帶正負號的整數，用於標示 ID，以將威脅 pcap 檔案與作為流量一部分的延伸 pcaps 產生關聯。所有的

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
	威脅日誌皆將包含為 0 的 pcap_id (關聯的 pcap)，或參照延伸 pcap 檔案的 ID。
檔案摘要 (filedigest)	僅適用於 WildFire 子類型；所有其他的類型不會使用此欄位 filedigest 字串會顯示所傳送要由 WildFire 服務進行分析的檔案二進位雜湊。
雲端 (cloud)	僅適用於 WildFire 子類型；所有其他的類型不會使用此欄位。 雲端字串會顯示 WildFire 裝置 (私人) 或 WildFire 雲端 (公共) 的 FQDN，您可以在其中上傳檔案以供分析。
URL 索引 (url_idx)	用於 URL 篩選和 WildFire 子類型。 應用程式使用 TCP 保持活動，在一段時間長度內保持連線開啟時，該工作階段的所有日誌項目都具有單一工作階段 ID。在此狀況下，當您擁有包含多個 URL 實體的單一威脅日誌（和工作階段 ID）時，url_idx 是可讓您在單一工作階段內建立每個日誌項目順序之關聯的計數器。 例如，若要瞭解防火牆轉送至 WildFire 進行分析的檔案 URL，請從 WildFire 提交日誌中找到工作階段 ID 和 url_idx，並在 URL 篩選日誌中搜尋相同的工作階段 ID 和 url_idx。符合工作階段 ID 和 url_idx 的日誌項目會包含轉送至 WildFire 的檔案 URL。
使用者代理程式 (user_agent)	僅適用於 URL 篩選子類型；所有其他的類型不會使用此欄位。 (使用者代理程式) 欄位會指定使用者用來存取 URL 的網頁瀏覽器，例如 Internet Explorer。此資訊是在 HTTP 要求中傳送給伺服器。
檔案類型 (filetype)	僅適用於 WildFire 子類型；所有其他的類型不會使用此欄位。 指定防火牆為了 WildFire 分析而轉送的檔案類型。
X-Forwarded-For (xff)	僅適用於 URL 篩選子類型；所有其他的類型不會使用此欄位。 HTTP 標頭中的 X 轉送針對欄位包含要求網頁的使用者其 IP 位址。它允許您識別使用者的 IP 位址，這在您的網路上有 Proxy 伺服器會將使用者 IP 位址取代為該伺服器在封包標頭中來源 IP 位址欄位內的位址時，特別的有用。 基於不同的設備實施，*XFF* 欄位可能包含非 *IP* 位址值。
轉介者 (referer)	僅適用於 URL 篩選子類型；所有其他的類型不會使用此欄位。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
	HTTP 標頭中的 (參照位址) 欄位包含網頁的 URL 可將使用者連結至其他網頁；它是將使用者重新導向 (轉介) 至正在要求之網頁的來源。
寄件者 (sender)	指定電子郵件寄件者的名稱。
主旨 (subject)	指定電子郵件的主旨。
收件者 (recipient)	指定電子郵件收件者的名稱。
報告 ID (reportid)	僅適用於資料篩選和 WildFire 子類型；所有其他的類型不會使用此欄位。 識別防火牆、WildFire 雲端或 WildFire 設備上的分析要求。
設備群組階層（dg_hier_level_1 到 dg_hier_level_4）	一系列的識別號碼，可表示設備群組在設備群組階層中的位置。產生日誌的防火牆（或虛擬系統）會在裝置群組階層中包含每個上階項目的識別號碼。此結構不包含共用設備群組（層級 0）。 如果日誌值為 12、34、45 或 0，這表示該日誌是由屬於裝置群組 45 且其上階項目為 34 和 12 的防火牆（或虛擬系統）所產生。若要檢視對應至值 12、34 或 45 的設備群組名稱，請使用下列其中一個方法： API 查詢： `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
虛擬系統名稱 (vsys_name)	與工作階段相關聯的虛擬系統名稱；只在已針對多個虛擬系統啟用的防火牆上有效。
設備名稱 (device_name)	已記錄工作階段的防火牆主機名稱。
來源 VM UUID (src_uuid)	在 VMware NSX 環境中識別來賓虛擬機器的來源通用唯一識別碼。
目的地 VM UUID (dst_uuid)	在 VMware NSX 環境中識別來賓虛擬機器的目的地通用唯一識別碼。
HTTP 方法 (http_method)	僅適用於 URL 篩選日誌。描述 Web 要求中使用的 HTTP 方法。僅記錄下列方法：Connect、Delete、Get、Head、Options、Post、Put。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
通道 ID/IMSI (tunnel_id/imsi)	國際行動用戶識別 (IMSI) 是為 GSM/UMTS/EPS 系統內每個行動用戶分配的唯一號碼。IMSI 必須僅由十進位數字 (0-9) 組成，允許的最大位數為 15 位。
監控標籤/IMEI (monitortag/imei)	國際行動裝置識別 (IMEI) 是為每個行動站裝置分配的唯一 15 或 16 位號碼。
上層工作階段 ID (parent_session_id)	此工作階段通道所在的工作階段 ID。僅適用於內部通道（若有兩層通道）或內部內容（若僅有一層通道）。
上層工作階段開始時間 (parent_start_time)	上層通道工作階段開始的年/月/日 時：分：秒。
通道類型 (tunnel)	通道的類型，例如 GRE 或 IPSec。
威脅類別 (thr_category)	描述了用於分類各種威脅特徵碼的威脅類別。 如果網域外部動態清單產生了此日誌，則 `domain-edl` 會填入此欄位。
內容版本 (contentver)	產生日誌時，防火牆上的應用程式和威脅版本。
SCTP 關聯 ID (assoc_id)	識別兩個 SCTP 端點間關聯所對應的所有連線的號碼。
裝載通訊協定 ID (ppid)	資料區塊的資料部分中有效負載的通訊協定 ID。
HTTP 標頭 (http_headers)	表明防火牆 URL 日誌項目中插入的 HTTP 標頭。
URL 類別清單 (url_category_list)	列出防火牆用於執行政策的 URL 篩選類別。
規則 UUID (rule_uuid)	永久識別規則的 UUID。
HTTP/2 連線 (http2_connection)	透過顯示以下一個值來確定流量是否使用了 HTTP/2 連線： • TCP 連線工作階段 ID—工作階段是 HTTP/2 • 0—工作階段不是 HTTP/2
動態使用者群組名稱 (dynusergroup_name)	包含啟動工作階段的使用者的動態使用者群組名稱。
XFF 位址 (xff_ip)	要求網頁之使用者的 IP 位址或要求周遊之倒數第二個裝置的 IP 位址。如果要求通過一個或多個 Proxy、負載平衡器或其他上游裝置，則防火牆將顯示最新裝置的 IP 位址。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
	基於不同的設備實施，*XFF* 欄位可能包含非 *IP* 位址值。
來源裝置類別 (src_category)	Device-ID 識別為流量來源的裝置的類別。
來源裝置設定檔 (src_profile)	Device-ID 識別為流量來源的裝置的裝置設定檔。
來源裝置型號 (src_model)	Device-ID 識別為流量來源的裝置的型號。
來源裝置廠商 (src_vendor)	Device-ID 識別為流量來源的裝置的廠商。
來源裝置作業系統系列 (src_osfamily)	Device-ID 識別為流量來源的裝置的作業系統類型。
來源裝置作業系統版本 (src_osversion)	Device-ID 識別為流量來源的裝置的作業系統版本。
來源主機名稱 (src_host)	Device-ID 識別為流量來源的裝置的主機名稱。
來源 MAC 位址 (src_mac)	Device-ID 識別為流量來源的裝置的 MAC 位址。
目的地裝置類別 (dst_category)	Device-ID 識別為流量目的地的裝置的類別。
目的地裝置設定檔 (dst_profile)	Device-ID 識別為流量目的地的裝置的裝置設定檔。
目的地裝置型號 (dst_model)	Device-ID 識別為流量目的地的裝置的型號。
目的地裝置廠商 (dst_vendor)	Device-ID 識別為流量目的地的裝置的廠商。
目的地裝置作業系統系列 (dst_osfamily)	Device-ID 識別為流量目的地的裝置的作業系統類型。
目的地裝置作業系統版本 (dst_osversion)	Device-ID 識別為流量目的地的裝置的作業系統版本。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
目的地主機名稱 (dst_host)	Device-ID 識別為流量目的地的裝置的主機名稱。
目的地 MAC 位址 (dst_mac)	Device-ID 識別為流量目的地的裝置的 MAC 位址。
容器 ID (container_id)	部署應用程式 POD 之 Kubernetes 節點上 PAN-NGFW pod 的容器 ID。
POD 命名空間 (pod_namespace)	受保護應用程式 POD 的命名空間。
POD 名稱 (pod_name)	受保護的應用程式 POD。
來源外部動態清單 (src_edl)	包含流量來源 IP 位址的外部動態清單的名稱。
目的地外部動態清單 (dst_edl)	包含流量目的地 IP 位址的外部動態清單的名稱。
主機 ID (hostid)	GlobalProtect 為識別主機所指派的唯一 ID。
使用者裝置序列號 (serialnumber)	使用者電腦或裝置的序列號。
網域 EDL (domain_edl)	包含流量網域名稱的外部動態清單的名稱。
來源動態位址群組 (src_dag)	原始工作階段來源動態位址群組。
目的地動態位址群組 (dst_dag)	原始目的地來源動態位址群組。
部分雜湊 (partial_hash)	機器學習部分雜湊。
高解析度時間戳記 (high_res timestamp)	在管理平面接收日誌的時間（毫秒）。 此新欄位的格式為 YYYY-MM-DDThh:ss:sssTZD： • **YYYY**—四位數表示年份 • **MM**—二位數表示月份 • **DD**—二位數表示當月的日期（01 到 31） • **T**—時間戳記開始的指標

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
	• **hh**—兩位數表示小時（使用 24 小時制，00 到 23） • **mm**—兩位數表示分鐘（00 到 59） • **ss**—兩位數表示秒鐘（00 到 60） • **sss**—一位或多位數表示毫秒 • **TZD**—時區指示項（+hh:mm 或 -hh:mm） 對於從執行 *PAN-OS 11.0* 和更新版本的受管理防火牆接收的日誌，支援高解析度時間戳記。從執行 *PAN-OS 9.1* 及早前版本的防火牆接收的日誌顯示 `1969-12-31T16:00:00:000-8:00` 時間戳記，而不論接收日誌的時間如何。
原因 (reason)	資料篩選動作的原因。
理由 (justification)	資料篩選動作的理由。
A 切片服務類型 (nssai_sst)	網路切片 ID 的 A 切片服務類型。
應用程式子類別 (subcategory_of_app)	應用程式設定屬性中指定的應用程式子類別。
應用程式類別 (category_of_app)	應用程式設定屬性中指定的應用程式類別。值為： • 業務系統 • 協同作業 • 一般網際網路 • 媒體 • 網路 • saas
應用程式技術 (technology_of_app)	應用程式設定屬性中指定的應用程式技術。值為： • browser-based • client-server • network-protocol • peer-to-peer

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
應用程式風險 (risk_of_app)	與應用程式關聯的風險層級（1 = 最低，5 = 最高）。
應用程式特性 (characteristic_of_app)	應用程式適用特性的逗號分隔清單
應用程式容器 (container_of_app)	應用程式的父應用程式。
通道應用程式 (tunneled_app)	通道應用程式的名稱。
應用程式 SaaS (is_saas_of_app)	如果是 SaaS 應用程式，則顯示 `1` ，如果不是 SaaS 應用程式，則顯示 `0`。
應用程式認可狀態 (sanctioned_state_of_app)	如果應用程式受認可，則顯示 `1`，如果應用程式不受認可，則顯示 `0`。
雲端報告 ID (cloud_reportid)	(PAN-OS 10.2.0) 防火牆傳送的 DLP 雲端服務掃描檔案存在的 32 個字元的唯一 ID。 （PAN-OS 10.2.1 及更新版本）防火牆傳送的 DLP 雲端服務掃描檔案存在的 67 個字元的唯一 ID。 系統會針對 DLP 雲端服務已掃描並產生雲端報告 ID 的檔案，顯示相同的雲端報告 ID。
叢集名稱 (cluster_name)	CN-Series 防火牆叢集的名稱。
流類型 (flow_type)	標識用於流量的 Proxy 類型。如果使用 Proxy，則顯示 `Explicit Proxy`（明確 `Proxy`）或 `Transparent Proxy`（透明 `Proxy`）。如果未使用 Proxy，則顯示 `NonProxyTraffic`。

URL 篩選日誌欄位

格式：FUTURE_USE、接收時間、序號、類型、威脅/內容類型、FUTURE_USE、產生時間、來源位址、目的地位址、NAT 來源 IP、NAT 目的地 IP、規則名稱、來源使用者、目的地使用者、應用程式、虛擬系統、來源區域、目的地區域、輸入介面、輸出介面、日誌動作、FUTURE_USE、工作階段 ID、重複計數、來源連接埠、目的地連接埠、NAT 來源連接埠、NAT 目的地連接埠、旗標、IP 通訊協定、動作、URL/檔案名稱、威脅 ID、類別、嚴重性、方向、序號、動作旗標、來源國家/地區、目的地國家/地區、FUTURE_USE、內容類型、PCAP_ID、檔案摘要、雲端、URL 索引、使用者代理程式、檔案類型、X-Forwarded-For、轉介者、寄件者、主旨、收件者、報告 ID、裝置群組階層層級 1、裝置群組階層層級 2、裝置群組階層層級 3、裝置群組階層層級 4、虛

©2024 Palo Alto Networks, Inc.

擬系統名稱、裝置名稱、FUTURE_USE、來源 VM UUID、目的地 VM UUID、HTTP 方法、通道 ID/IMSI、監控標籤/IMEI、上層工作階段 ID、上層開始時間、通道類型、威脅類別、內容版本、FUTURE_USE、SCTP 關聯 ID、有效負載通訊協定 ID、HTTP 標頭、URL 類別清單、規則 UUID、HTTP/2 連線、動態使用者群組名稱、XFF 位址、來源裝置類別、來源裝置設定檔、來源裝置型號、來源裝置廠商、來源裝置作業系統系列、來源裝置作業系統版本、來源主機名稱、來源 MAC 位址、目的地裝置類別、目的地裝置設定檔、目的地裝置型號、目的地裝置廠商、目的地裝置作業系統系列、目的地裝置作業系統版本、目的地主機名稱、目的地 MAC 位址、容器 ID、POD 命名空間、POD 名稱、來源外部動態清單、目的地外部動態清單、主機 ID、序號、網域 EDL、來源動態位址群組、目的地動態位址群組、部分雜湊、高解析度時間戳記、原因、理由、A 切片服務類型、應用程式子類別、應用程式類別、應用程式技術、應用程式風險、應用程式特性、應用程式容器、通道應用程式、應用程式 SaaS、應用程式認可狀態、雲端報告 ID、叢集名稱、流類型

欄位名稱	說明
接收時間（receive_time 或 cef-formatted-receive_time）	在管理平面接收日誌的時間。
序號 (Serial #)	產生日誌之防火牆的序號。
類型 (type)	指定日誌類型；值為 THREAT。
威脅/內容類型 (subtype)	威脅日誌的子類型；值為 URL。
產生時間（time_generated 或 cef-formatted-time_generated）	在資料層上產生日誌的時間。
來源位址 (src)	原始工作階段來源 IP 位址。
目的地位址 (dst)	原始工作階段目的地 IP 位址。
NAT 來源 IP (natsrc)	如果已執行來源 NAT，則為後續 NAT 來源 IP 位址。
NAT 目的地 IP (natdst)	如果已執行目的地 NAT，則為後續 NAT 目的地 IP 位址。
規則名稱 (rule)	工作階段符合的規則名稱。
來源使用者 (srcuser)	啟動工作階段之使用者的使用者名稱。
目的地使用者 (dstuser)	將工作階段指定至之使用者的使用者名稱。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
應用程式 (app)	與工作階段相關聯的應用程式。
虛擬系統 (vsys)	與工作階段相關聯的虛擬系統。
來源區域 (from)	工作階段的來源區域。
目的地區域 (to)	將工作階段指定至的區域。
輸入介面 (inbound_if)	工作階段的來源介面。
輸出介面 (outbound_if)	將工作階段指定至的介面。
日誌動作 (logset)	套用至工作階段的日誌轉送設定檔。
工作階段 ID (sessionid)	套用至每個工作階段的內部數字識別碼。
重複計數 (repeatcnt)	在 5 秒鐘內看到的有相同來源 IP、目的地 IP、應用程式與內容/威脅類型的工作階段數。
來源連接埠 (sport)	工作階段使用的來源連接埠。
目的地連接埠 (dport)	工作階段使用的目的地連接埠。
NAT 來源連接埠 (natsport)	後續 NAT 來源連接埠。
NAT 目的地連接埠 (natdport)	後續 NAT 目的地連接埠。
標幟 (flags)	32 位元欄位提供工作階段詳細資訊；您可以透過 AND 有記錄值的值解碼此欄位： • 0x80000000—工作階段有封包擷取 (PCAP) • 0x40000000—已啟用選項，允許用戶端使用多條路徑連線到目的地主機 • 0x20000000—檔案已提交給 WildFire 進行裁定 • 0x10000000—偵測到一般使用者提交的企業認證 • 0x08000000—流量的來源在允許清單上，且不受偵察保護 • 0x02000000—IPv6 工作階段 • 0X01000000—解密 SSL 工作階段 (SSL Proxy) • 0x00800000—透過 URL 篩選拒絕工作階段

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
	• 0x00400000—工作階段已執行 NAT 轉譯 • 0x00200000—透過驗證入口網站擷取工作階段的使用者資訊 • 0x00100000—應用程式流量位於非標準目的地連接埠 • 0x00080000—Proxy 中的 X-Forwarded-For 值在來源使用者欄位中 • 0x00040000—日誌對應至 http proxy 工作階段內的交易（Proxy 交易） • 0x00020000—用戶端到伺服器的流量符合基於原則的轉送 • 0x00010000—伺服器到用戶端的流量符合基於原則的轉送 • 0x00008000—工作階段是容器頁面存取（容器頁面） • 0x00002000—工作階段暫時符合規則，以進行隱含應用程式相依性處理。適用於 PAN-OS 5.0.0 及以上版本。 • 0x00000800—對稱傳回用於轉送此工作階段的流量 • 0x00000400—解密的流量透過鏡像連接埠傳送出純文字 • 0x00000010—檢查外部通道的有效負載
IP 通訊協定 (proto)	與工作階段相關聯的 IP 通訊協定。
動作 (action)	針對工作階段執行的動作；值為 alert（警示）、allow（允許）、block-url（封鎖 URL）、block-continue（封鎖-繼續）、continue（繼續）、block-override（封鎖-取代）、override-lockout（取代-鎖定）和 override（取代）。 • 警示—偵測到威脅或 URL 但未封鎖 • 封鎖 url—已封鎖 URL 要求，因為它符合設為封鎖的 URL 類別 • block-continue（封鎖-繼續）—HTTP 要求遭到封鎖並重新導向至繼續頁面，其中包含確認繼續的按鈕 • continue（繼續）—回應封鎖-繼續 URL 繼續頁面，表明允許執行封鎖-繼續要求 • block-override（封鎖-取代）—HTTP 要求遭到封鎖並重新導向至管理員取代頁面，要求防火牆管理員提供密碼以繼續 • override-lockout（取代-鎖定）—來源 IP 的管理員取代密碼嘗試失敗次數過多。封鎖-取代重新導向頁面現在已封鎖 IP • override（取代）—回應封鎖-取代頁面，並提供正確密碼，要求已獲允許
URL/檔案名稱 (misc)	具有變動長度的欄位。URL 最多包含 1023 個字元。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
	子類型為 URL 時的實際 URI。 Threat Category（威脅類別）為 `domain-edl` 時的 URL。
威脅/內容名稱 (threatid)	已知和自訂威脅的 Palo Alto Networks 識別碼。這是某些子類型的描述字串，後面加上以括號括住的 64 位元數字識別碼： • 8000 - 8099—掃描偵測 • 8500 - 8599—流量偵測 • 9999—URL 篩選日誌 • 10000 - 19999—間諜軟體打電話回家偵測 • 20000 - 29999—間諜軟體下載偵測 • 30000 - 44999—漏洞利用偵測 • 52000 - 52999—檔案類型偵測 • 60000 - 69999—資料篩選偵測 如果 Domain EDL（網域 EDL）欄位已填寫，則此欄位會填入相同的值。 之前版本中使用的病毒偵測、*WildFire* 特徵碼摘要以及 *DNS C2* 特徵碼的威脅 *ID* 範圍將被永久性的全域唯一 ID 取代。請參閱威脅/內容類型（子類型）和威脅類別 *(thr_category)* 欄位名稱，以建立更新報告、篩選威脅日誌以及 *ACC* 活動。
類別 (category)	針對 URL 子類型，其為 URL 類別；針對 WildFire 子類型，其為「惡意軟體」、「網路釣魚」「灰色軟體」或「良性」的檔案裁定；針對其他子類型，該值為「any」（任何）。
嚴重性 (severity)	與威脅相關聯的嚴重性；值有（資訊）、（低）、（中）、（高）、（重要）。
方向 (direction)	表示攻擊的方向： • 用戶端到伺服器 • 伺服器到用戶端
序號 (seqno)	依序遞增的 64 位元日誌項目識別碼。每個日誌類型有一個唯一編號空間。
動作旗標 (actionflags)	指示是否將日誌轉送至 Panorama 的位元欄位。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
來源國家 (srcloc)	私人位址的來源國家或內部地區。最大長度為 32 位元組。
目的地國家 (dstloc)	私人位址的目的地國家或內部地區。最大長度為 32 位元組。
內容類型 (contenttype)	HTTP 回應資料的內容類型。最大長度 32 位元組。
PCAP ID (pcap_id)	封包擷取 (pcap) ID 是 64 位元未帶正負號的整數，用於標示 ID，以將威脅 pcap 檔案與作為流量一部分的延伸 pcaps 產生關聯。所有的威脅日誌皆將包含為 0 的 pcap_id (關聯的 pcap)，或參照延伸 pcap 檔案的 ID。
檔案摘要 (filedigest)	僅適用於 WildFire 子類型；所有其他的類型不會使用此欄位 filedigest 字串會顯示所傳送要由 WildFire 服務進行分析的檔案二進位雜湊。
雲端 (cloud)	僅適用於 WildFire 子類型；所有其他的類型不會使用此欄位。 雲端字串會顯示 WildFire 裝置 (私人) 或 WildFire 雲端 (公共) 的 FQDN，您可以在其中上傳檔案以供分析。
URL 索引 (url_idx)	應用程式使用 TCP 保持活動，在一段時間長度內保持連線開啟時，該工作階段的所有日誌項目都具有單一工作階段 ID。在此狀況下，當您擁有包含多個 URL 實體的單一威脅日誌（和工作階段 ID）時，url_idx 是可讓您在單一工作階段內建立每個日誌項目順序之關聯的計數器。 例如，若要瞭解防火牆轉送至 WildFire 進行分析的檔案 URL，請從 WildFire 提交日誌中找到工作階段 ID 和 url_idx，並在 URL 篩選日誌中搜尋相同的工作階段 ID 和 url_idx。符合工作階段 ID 和 url_idx 的日誌項目會包含轉送至 WildFire 的檔案 URL。
使用者代理程式 (user_agent)	(使用者代理程式) 欄位會指定使用者用來存取 URL 的網頁瀏覽器，例如 Internet Explorer。此資訊是在 HTTP 要求中傳送給伺服器。
檔案類型 (filetype)	僅適用於 WildFire 子類型；所有其他的類型不會使用此欄位。 指定防火牆為了 WildFire 分析而轉送的檔案類型。
X-Forwarded-For (xff)	HTTP 標頭中的 X 轉送針對欄位包含要求網頁的使用者其 IP 位址。它允許您識別使用者的 IP 位址，這在您的網路上有 Proxy 伺服器會將使用者 IP 位址取代為該伺服器在封包標頭中來源 IP 位址欄位內的位址時，特別的有用。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
	基於不同的設備實施，*XFF* 欄位可能包含非 *IP* 位址值。
轉介者 (referer)	HTTP 標頭中的 (參照位址) 欄位包含網頁的 URL 可將使用者連結至其他網頁；它是將使用者重新導向 (轉介) 至正在要求之網頁的來源。
寄件者 (sender)	指定電子郵件寄件者的名稱。
主旨 (subject)	指定電子郵件的主旨。
收件者 (recipient)	指定電子郵件收件者的名稱。
報告 ID (reportid)	僅適用於資料篩選和 WildFire 子類型；所有其他的類型不會使用此欄位。 識別防火牆、WildFire 雲端或 WildFire 設備上的分析要求。
設備群組階層（dg_hier_level_1 到 dg_hier_level_4）	一系列的識別號碼，可表示設備群組在設備群組階層中的位置。產生日誌的防火牆（或虛擬系統）會在裝置群組階層中包含每個上階項目的識別號碼。此結構不包含共用設備群組（層級 0）。 如果日誌值為 12、34、45 或 0，這表示該日誌是由屬於裝置群組 45 且其上階項目為 34 和 12 的防火牆（或虛擬系統）所產生。若要檢視對應至值 12、34 或 45 的設備群組名稱，請使用下列其中一個方法： API 查詢： `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
虛擬系統名稱 (vsys_name)	與工作階段相關聯的虛擬系統名稱；只在已針對多個虛擬系統啟用的防火牆上有效。
設備名稱 (device_name)	已記錄工作階段的防火牆主機名稱。
來源 VM UUID (src_uuid)	在 VMware NSX 環境中識別來賓虛擬機器的來源通用唯一識別碼。
目的地 VM UUID (dst_uuid)	在 VMware NSX 環境中識別來賓虛擬機器的目的地通用唯一識別碼。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
HTTP 方法 (http_method)	描述 Web 要求中使用的 HTTP 方法。僅記錄下列方法：Connect、Delete、Get、Head、Options、Post、Put。
通道 ID/IMSI (tunnel_id/imsi)	國際行動用戶識別 (IMSI) 是為 GSM/UMTS/EPS 系統內每個行動用戶分配的唯一號碼。IMSI 必須僅由十進位數字 (0-9) 組成，允許的最大位數為 15 位。
監控標籤/IMEI (monitortag/imei)	國際行動裝置識別 (IMEI) 是為每個行動站裝置分配的唯一 15 或 16 位號碼。
上層工作階段 ID (parent_session_id)	此工作階段通道所在的工作階段 ID。僅適用於內部通道（若有兩層通道）或內部內容（若僅有一層通道）。
上層工作階段開始時間 (parent_start_time)	上層通道工作階段開始的年/月/日 時：分：秒。
通道類型 (tunnel)	通道的類型，例如 GRE 或 IPSec。
威脅類別 (thr_category)	描述了用於分類各種威脅特徵碼的威脅類別。 如果網域外部動態清單產生了此日誌，則 `domain-edl` 會填入此欄位。
內容版本 (contentver)	產生日誌時，防火牆上的應用程式和威脅版本。
SCTP 關聯 ID (assoc_id)	識別兩個 SCTP 端點間關聯所對應的所有連線的號碼。
裝載通訊協定 ID (ppid)	資料區塊的 資料部分中有效負載的通訊協定 ID 。
HTTP 標頭 (http_headers)	表明防火牆 URL 日誌項目中插入的 HTTP 標頭。
URL 類別清單 (url_category_list)	列出防火牆用於執行政策的 URL 篩選類別。
規則 UUID (rule_uuid)	永久識別規則的 UUID。
HTTP/2 連線 (http2_connection)	透過顯示以下一個值來確定流量是否使用了 HTTP/2 連線： • TCP 連線工作階段 ID—工作階段是 HTTP/2 • 0—工作階段不是 HTTP/2

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
動態使用者群組名稱 (dynusergroup_name)	包含啟動工作階段的使用者的動態使用者群組名稱。
XFF 位址 (xff_ip)	要求網頁之使用者的 IP 位址或要求周遊之倒數第二個裝置的 IP 位址。如果要求通過一個或多個 Proxy、負載平衡器或其他上游裝置，則防火牆將顯示最新裝置的 IP 位址。 基於不同的設備實施，*XFF* 欄位可能包含非 *IP* 位址值。
來源裝置類別 (src_category)	Device-ID 識別為流量來源的裝置的類別。
來源裝置設定檔 (src_profile)	Device-ID 識別為流量來源的裝置的裝置設定檔。
來源裝置型號 (src_model)	Device-ID 識別為流量來源的裝置的型號。
來源裝置廠商 (src_vendor)	Device-ID 識別為流量來源的裝置的廠商。
來源裝置作業系統系列 (src_osfamily)	Device-ID 識別為流量來源的裝置的作業系統類型。
來源裝置作業系統版本 (src_osversion)	Device-ID 識別為流量來源的裝置的作業系統版本。
來源主機名稱 (src_host)	Device-ID 識別為流量來源的裝置的主機名稱。
來源 MAC 位址 (src_mac)	Device-ID 識別為流量來源的裝置的 MAC 位址。
目的地裝置類別 (dst_category)	Device-ID 識別為流量目的地的裝置的類別。
目的地裝置設定檔 (dst_profile)	Device-ID 識別為流量目的地的裝置的裝置設定檔。
目的地裝置型號 (dst_model)	Device-ID 識別為流量目的地的裝置的型號。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
目的地裝置廠商 (dst_vendor)	Device-ID 識別為流量目的地的裝置的廠商。
目的地裝置作業系統系列 (dst_osfamily)	Device-ID 識別為流量目的地的裝置的作業系統類型。
目的地裝置作業系統版本 (dst_osversion)	Device-ID 識別為流量目的地的裝置的作業系統版本。
目的地主機名稱 (dst_host)	Device-ID 識別為流量目的地的裝置的主機名稱。
目的地 MAC 位址 (dst_mac)	Device-ID 識別為流量目的地的裝置的 MAC 位址。
容器 ID (container_id)	部署應用程式 POD 之 Kubernetes 節點上 PAN-NGFW pod 的容器 ID。
POD 命名空間 (pod_namespace)	受保護應用程式 POD 的命名空間。
POD 名稱 (pod_name)	受保護的應用程式 POD。
來源外部動態清單 (src_edl)	包含流量來源 IP 位址的外部動態清單的名稱。
目的地外部動態清單 (dst_edl)	包含流量目的地 IP 位址的外部動態清單的名稱。
主機 ID (hostid)	GlobalProtect 為識別主機所指派的唯一 ID。
使用者裝置序列號 (serialnumber)	使用者電腦或裝置的序列號。
網域 EDL (domain_edl)	包含流量網域名稱的外部動態清單的名稱。
來源動態位址群組 (src_dag)	原始工作階段來源動態位址群組。
目的地動態位址群組 (dst_dag)	原始目的地來源動態位址群組。
部分雜湊 (partial_hash)	機器學習部分雜湊。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
高解析度時間戳記 (high_res timestamp)	在管理平面接收日誌的時間（毫秒）。 此新欄位的格式為 YYYY-MM-DDThh:ss:sssTZD： • **YYYY**—四位數表示年份 • **MM**—二位數表示月份 • **DD**—二位數表示當月的日期（01 到 31） • **T**—時間戳記開始的指標 • **hh**—兩位數表示小時（使用 24 小時制，00 到 23） • **mm**—兩位數表示分鐘（00 到 59） • **ss**—兩位數表示秒鐘（00 到 60） • **sss**—一位或多位數表示毫秒 • **TZD**—時區指示項（+hh:mm 或 -hh:mm） 對於從執行 *PAN-OS 10.1* 和更高版本的受管理防火牆接收的日誌，支援高解析度時間戳記。從執行 *PAN-OS 9.1* 及早前版本的防火牆接收的日誌顯示 `1969-12-31T16:00:00:000-8:00` 時間戳記，而不論接收日誌的時間如何。
原因 (reason)	URL 篩選動作的原因。
理由 (justification)	URL 篩選動作的理由。
A 切片服務類型 (nssai_sst)	網路切片 ID 的 A 切片服務類型。
應用程式子類別 (subcategory_of_app)	應用程式設定屬性中指定的應用程式子類別。
應用程式類別 (category_of_app)	應用程式設定屬性中指定的應用程式類別。值為： • 業務系統 • 協同作業 • 一般網際網路 • 媒體 • 網路 • saas

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
應用程式技術 (technology_of_app)	應用程式設定屬性中指定的應用程式技術。值為： • browser-based • client-server • network-protocol • peer-to-peer
應用程式風險 (risk_of_app)	與應用程式關聯的風險層級（1 = 最低，5 = 最高）。
應用程式特性 (characteristic_of_app)	應用程式適用特性的逗號分隔清單
應用程式容器 (container_of_app)	應用程式的父應用程式。
通道應用程式 (tunneled_app)	通道應用程式的名稱。
應用程式 SaaS (is_saas_of_app)	如果是 SaaS 應用程式，則顯示 `yes`，如果不是 SaaS 應用程式，則顯示 `no`。
應用程式認可狀態 (sanctioned_state_of_app)	如果應用程式受認可，則顯示 `yes`，如果應用程式不受認可，則顯示 `no`。
雲端報告 ID (cloud_reportid)	(PAN-OS 10.2.0) 防火牆傳送的 DLP 雲端服務掃描檔案存在的 32 個字元的唯一 ID。 （PAN-OS 10.2.1 及更新版本）防火牆傳送的 DLP 雲端服務掃描檔案存在的 67 個字元的唯一 ID。 系統會針對 DLP 雲端服務已掃描並產生雲端報告 ID 的檔案，顯示相同的雲端報告 ID。
叢集名稱 (cluster_name)	CN-Series 防火牆叢集的名稱。
流類型 (flow_type)	標識用於流量的 Proxy 類型。如果使用 Proxy，則顯示 `Explicit Proxy`（明確 `Proxy`）或 `Transparent Proxy`（透明 `Proxy`）。如果未使用 Proxy，則顯示 `NonProxyTraffic`。

©2024 Palo Alto Networks, Inc.

資料篩選日誌欄位

格式：FUTURE_USE、接收時間、序號、類型、威脅/內容類型、FUTURE_USE、產生時間、來源位址、目的地位址、NAT 來源 IP、NAT 目的地 IP、規則名稱、來源使用者、目的地使用者、應用程式、虛擬系統、來源區域、目的地區域、輸入介面、輸出介面、日誌動作、FUTURE_USE、工作階段 ID、重複計數、來源連接埠、目的地連接埠、NAT 來源連接埠、NAT 目的地連接埠、旗標、IP 通訊協定、動作、URL/檔案名稱、威脅 ID、類別、嚴重性、方向、序號、動作旗標、來源國家/地區、目的地國家/地區、FUTURE_USE、內容類型、PCAP_ID、檔案摘要、雲端、URL 索引、使用者代理程式、檔案類型、X-Forwarded-For、轉介者、寄件者、主旨、收件者、報告 ID、裝置群組階層層級 1、裝置群組階層層級 2、裝置群組階層層級 3、裝置群組階層層級 4、虛擬系統名稱、裝置名稱、FUTURE_USE、來源 VM UUID、目的地 VM UUID、HTTP 方法、通道 ID/IMSI、監控標籤/IMEI、上層工作階段 ID、上層開始時間、通道類型、威脅類別、內容版本、FUTURE_USE、SCTP 關聯 ID、有效負載通訊協定 ID、HTTP 標頭、URL 類別清單、規則 UUID、HTTP/2 連線、動態使用者群組名稱、XFF 位址、來源裝置類別、來源裝置設定檔、來源裝置型號、來源裝置廠商、來源裝置作業系統系列、來源裝置作業系統版本、來源主機名稱、來源 MAC 位址、目的地裝置類別、目的地裝置設定檔、目的地裝置型號、目的地裝置廠商、目的地裝置作業系統系列、目的地裝置作業系統版本、目的地主機名稱、目的地 MAC 位址、容器 ID、POD 命名空間、POD 名稱、來源外部動態清單、目的地外部動態清單、主機 ID、序號、網域 EDL、來源動態位址群組、目的地動態位址群組、部分雜湊、高解析度時間戳記、原因、理由、A 切片服務類型、應用程式子類別、應用程式類別、應用程式技術、應用程式風險、應用程式特性、應用程式容器、通道應用程式、應用程式 SaaS、應用程式認可狀態、雲端報告 ID、叢集名稱、流類型

欄位名稱	說明
接收時間（receive_time 或 cef-formatted-receive_time）	在管理平面接收日誌的時間。
序號 (Serial #)	產生日誌之防火牆的序號。
類型 (type)	指定日誌類型；值為 THREAT。
威脅/內容類型 (subtype)	威脅日誌的子類型；值是資料、dlp、dlp 非檔案、檔案。
產生時間（time_generated 或 cef-formatted-time_generated）	在資料層上產生日誌的時間。
來源位址 (src)	原始工作階段來源 IP 位址。
目的地位址 (dst)	原始工作階段目的地 IP 位址。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
NAT 來源 IP (natsrc)	如果已執行來源 NAT，則為後續 NAT 來源 IP 位址。
NAT 目的地 IP (natdst)	如果已執行目的地 NAT，則為後續 NAT 目的地 IP 位址。
規則名稱 (rule)	工作階段符合的規則名稱。
來源使用者 (srcuser)	啟動工作階段之使用者的使用者名稱。
目的地使用者 (dstuser)	將工作階段指定至之使用者的使用者名稱。
應用程式 (app)	與工作階段相關聯的應用程式。
虛擬系統 (vsys)	與工作階段相關聯的虛擬系統。
來源區域 (from)	工作階段的來源區域。
目的地區域 (to)	將工作階段指定至的區域。
輸入介面 (inbound_if)	工作階段的來源介面。
輸出介面 (outbound_if)	將工作階段指定至的介面。
日誌動作 (logset)	套用至工作階段的日誌轉送設定檔。
工作階段 ID (sessionid)	套用至每個工作階段的內部數字識別碼。
重複計數 (repeatcnt)	在 5 秒鐘內看到的有相同來源 IP、目的地 IP、應用程式與內容/威脅類型的工作階段數。
來源連接埠 (sport)	工作階段使用的來源連接埠。
目的地連接埠 (dport)	工作階段使用的目的地連接埠。
NAT 來源連接埠 (natsport)	後續 NAT 來源連接埠。
NAT 目的地連接埠 (natdport)	後續 NAT 目的地連接埠。
標幟 (flags)	32 位元欄位提供工作階段詳細資訊；您可以透過 AND 有記錄值的值解碼此欄位： • 0x80000000—工作階段有封包擷取 (PCAP)

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
	• 0x40000000—已啟用選項，允許用戶端使用多條路徑連線到目的地主機 • 0x20000000—檔案已提交給 WildFire 進行裁定 • 0x10000000—偵測到一般使用者提交的企業認證 • 0x08000000—流量的來源在允許清單上，且不受偵察保護 • 0x02000000—IPv6 工作階段 • 0X01000000—解密 SSL 工作階段 (SSL Proxy) • 0x00800000—透過 URL 篩選拒絕工作階段 • 0x00400000—工作階段已執行 NAT 轉譯 • 0x00200000—透過驗證入口網站擷取工作階段的使用者資訊 • 0x00100000—應用程式流量位於非標準目的地連接埠 • 0x00080000—Proxy 中的 X-Forwarded-For 值在來源使用者欄位中 • 0x00040000—日誌對應至 http proxy 工作階段內的交易（Proxy 交易） • 0x00020000—用戶端到伺服器的流量符合基於原則的轉送 • 0x00010000—伺服器到用戶端的流量符合基於原則的轉送 • 0x00008000—工作階段是容器頁面存取（容器頁面） • 0x00002000—工作階段暫時符合規則，以進行隱含應用程式相依性處理。適用於 PAN-OS 5.0.0 及以上版本。 • 0x00000800—對稱傳回用於轉送此工作階段的流量 • 0x00000400—解密的流量透過鏡像連接埠傳送出純文字 • 0x00000010—檢查外部通道的有效負載
IP 通訊協定 (proto)	與工作階段相關聯的 IP 通訊協定。
動作 (action)	針對工作階段採取的動作；值有（警示）、（允許）、（拒絕）、（丟棄）、（丟棄所有封包）、（重設用戶端）、（重設伺服器）、（重設兩者）、（封鎖 url）。 • 警示—偵測到但未封鎖包含相符資料的流量 • 允許（僅限 dlp 子類型）—洪水偵測警示 • 封鎖（僅適用於 dlp 和 WildFire 子類型）—包含偵測到但遭到封鎖的相符資料的流量 • 封鎖-繼續（僅適用於 dlp 子類型）—包含遭到封鎖並重新導向至繼續頁面（其中包含確認繼續的按鈕）的相符資料的流量

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
	• 繼續（僅適用於 dlp 子類型）—回應封鎖-繼續頁面（其表明允許封鎖-繼續要求繼續執行） • 拒絕（僅適用於 dlp 子類型）—洪水偵測機制已啟動並根據設定拒絕流量
URL/檔案名稱 (misc)	具有變動長度的欄位。檔案名稱最多包含 63 個字元。 子類型為 dlp 時的檔案名稱 Threat Category（威脅類別）為 `domain-edl` 時的 URL。
威脅/內容名稱 (threatid)	已知和自訂威脅的 Palo Alto Networks 識別碼。這是某些子類型的描述字串，後面加上以括號括住的 64 位元數字識別碼： • 8000 – 8099—掃描偵測 • 8500 – 8599—流量偵測 • 9999—URL 篩選日誌 • 10000 – 19999—間諜軟體打電話回家偵測 • 20000 – 29999—間諜軟體下載偵測 • 30000 – 44999—漏洞利用偵測 • 52000 – 52999—檔案類型偵測 • 60000 – 69999—資料篩選偵測 如果 Domain EDL（網域 EDL）欄位已填寫，那麼此欄位會填入相同的值。 之前版本中使用的病毒偵測、*WildFire* 特徵碼摘要以及 *DNS C2* 特徵碼的威脅 *ID* 範圍將被永久性的全域唯一 ID 取代。請參閱威脅/內容類型（子類型）和威脅類別 *(thr_category)* 欄位名稱，以建立更新報告、篩選威脅日誌以及 *ACC* 活動。
類別 (category)	針對 URL 子類型，其為 URL 類別；針對 WildFire 子類型，其為「惡意軟體」、「網路釣魚」「灰色軟體」或「良性」的檔案裁定；針對其他子類型，該值為「any」（任何）。
嚴重性 (severity)	與威脅相關聯的嚴重性；值有（資訊）、（低）、（中）、（高）、（重要）。
方向 (direction)	表示攻擊的方向： • 用戶端到伺服器

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
	• 伺服器到用戶端
序號 (seqno)	依序遞增的 64 位元日誌項目識別碼。每個日誌類型有一個唯一編號空間。
動作旗標 (actionflags)	指示是否將日誌轉送至 Panorama 的位元欄位。
來源國家 (srcloc)	私人位址的來源國家或內部地區。最大長度為 32 位元組。
目的地國家 (dstloc)	私人位址的目的地國家或內部地區。最大長度為 32 位元組。
內容類型 (contenttype)	僅當子類型是 URL 時可用。 HTTP 回應資料的內容類型。最大長度 32 位元組。
PCAP ID (pcap_id)	封包擷取 (pcap) ID 是 64 位元未帶正負號的整數，用於標示 ID，以將威脅 pcap 檔案與作為流量一部分的延伸 pcaps 產生關聯。所有的威脅日誌皆將包含為 0 的 pcap_id (關聯的 pcap)，或參照延伸 pcap 檔案的 ID。
檔案摘要 (filedigest)	僅適用於 WildFire 子類型；所有其他的類型不會使用此欄位 filedigest 字串會顯示所傳送要由 WildFire 服務進行分析的檔案二進位雜湊。
雲端 (cloud)	僅適用於 WildFire 子類型；所有其他的類型不會使用此欄位。 雲端字串會顯示 WildFire 裝置 (私人) 或 WildFire 雲端 (公共) 的 FQDN，您可以在其中上傳檔案以供分析。
URL 索引 (url_idx)	用於 URL 篩選和 WildFire 子類型。 應用程式使用 TCP 保持活動，在一段時間長度內保持連線開啟時，該工作階段的所有日誌項目都具有單一工作階段 ID。在此狀況下，當您擁有包含多個 URL 實體的單一威脅日誌（和工作階段 ID）時，url_idx 是可讓您在單一工作階段內建立每個日誌項目順序之關聯的計數器。 例如，若要瞭解防火牆轉送至 WildFire 進行分析的檔案 URL，請從 WildFire 提交日誌中找到工作階段 ID 和 url_idx，並在 URL 篩選日誌中搜尋相同的工作階段 ID 和 url_idx。符合工作階段 ID 和 url_idx 的日誌項目會包含轉送至 WildFire 的檔案 URL。
使用者代理程式 (user_agent)	僅適用於 URL 篩選子類型；所有其他的類型不會使用此欄位。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
	(使用者代理程式) 欄位會指定使用者用來存取 URL 的網頁瀏覽器，例如 Internet Explorer。此資訊是在 HTTP 要求中傳送給伺服器。
檔案類型 (filetype)	指定防火牆為了分析而轉送的檔案類型。
X-Forwarded-For (xff)	僅適用於 URL 篩選子類型；所有其他的類型不會使用此欄位。 HTTP 標頭中的 X 轉送針對欄位包含要求網頁的使用者其 IP 位址。它允許您識別使用者的 IP 位址，這在您的網路上有 Proxy 伺服器會將使用者 IP 位址取代為該伺服器在封包標頭中來源 IP 位址欄位內的位址時，特別的有用。
轉介者 (referer)	僅適用於 URL 篩選子類型；所有其他的類型不會使用此欄位。 HTTP 標頭中的 (參照位址) 欄位包含網頁的 URL 可將使用者連結至其他網頁；它是將使用者重新導向 (轉介) 至正在要求之網頁的來源。
寄件者 (sender)	指定電子郵件寄件者的名稱。
主旨 (subject)	指定電子郵件的主旨。
收件者 (recipient)	指定電子郵件收件者的名稱。
報告 ID (reportid)	識別防火牆、WildFire 雲端或 WildFire 設備上的分析要求。
設備群組階層（dg_hier_level_1 到 dg_hier_level_4）	一系列的識別號碼，可表示設備群組在設備群組階層中的位置。產生日誌的防火牆（或虛擬系統）會在裝置群組階層中包含每個上階項目的識別號碼。此結構不包含共用設備群組（層級 0）。 如果日誌值為 12、34、45 或 0，這表示該日誌是由屬於裝置群組 45 且其上階項目為 34 和 12 的防火牆（或虛擬系統）所產生。若要檢視對應至值 12、34 或 45 的設備群組名稱，請使用下列其中一個方法： API 查詢： `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
虛擬系統名稱 (vsys_name)	與工作階段相關聯的虛擬系統名稱；只在已針對多個虛擬系統啟用的防火牆上有效。
設備名稱 (device_name)	已記錄工作階段的防火牆主機名稱。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
來源 VM UUID (src_uuid)	在 VMware NSX 環境中識別來賓虛擬機器的來源通用唯一識別碼。
目的地 VM UUID (dst_uuid)	在 VMware NSX 環境中識別來賓虛擬機器的目的地通用唯一識別碼。
HTTP 方法 (http_method)	僅適用於 URL 篩選日誌。描述 Web 要求中使用的 HTTP 方法。僅記錄下列方法：Connect、Delete、Get、Head、Options、Post、Put。
通道 ID/IMSI (tunnel_id/imsi)	國際行動用戶識別 (IMSI) 是為 GSM/UMTS/EPS 系統內每個行動用戶分配的唯一號碼。IMSI 必須僅由十進位數字 (0-9) 組成，允許的最大位數為 15 位。
監控標籤/IMEI (monitortag/imei)	國際行動裝置識別 (IMEI) 是為每個行動站裝置分配的唯一 15 或 16 位號碼。
上層工作階段 ID (parent_session_id)	此工作階段通道所在的工作階段 ID。僅適用於內部通道（若有兩層通道）或內部內容（若僅有一層通道）。
上層工作階段開始時間 (parent_start_time)	上層通道工作階段開始的年/月/日 時：分：秒。
通道類型 (tunnel)	通道的類型，例如 GRE 或 IPSec。
威脅類別 (thr_category)	描述了用於分類各種威脅特徵碼的威脅類別。 如果網域外部動態清單產生了此日誌，則 `domain-edl` 會填入此欄位。
內容版本 (contentver)	產生日誌時，防火牆上的應用程式和威脅版本。
SCTP 關聯 ID (assoc_id)	識別兩個 SCTP 端點間關聯所對應的所有連線的號碼。
裝載通訊協定 ID (ppid)	資料區塊的 資料部分中有效負載的通訊協定 ID 。
HTTP 標頭 (http_headers)	表明防火牆 URL 日誌項目中插入的 HTTP 標頭。
URL 類別清單 (url_category_list)	列出防火牆用於執行原則的 URL 篩選類別。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
規則 UUID (rule_uuid)	永久識別規則的 UUID。
HTTP/2 連線 (http2_connection)	透過顯示以下一個值來確定流量是否使用了 HTTP/2 連線： • TCP 連線工作階段 ID—工作階段是 HTTP/2 • 0—工作階段不是 HTTP/2
動態使用者群組名稱 (dynusergroup_name)	包含啟動工作階段的使用者的動態使用者群組名稱。
XFF 位址 (xff_ip)	要求網頁之使用者的 IP 位址或要求周遊之倒數第二個裝置的 IP 位址。如果要求通過一個或多個 Proxy、負載平衡器或其他上游裝置，則防火牆將顯示最新裝置的 IP 位址。
來源裝置類別 (src_category)	Device-ID 識別為流量來源的裝置的類別。
來源裝置設定檔 (src_profile)	Device-ID 識別為流量來源的裝置的裝置設定檔。
來源裝置型號 (src_model)	Device-ID 識別為流量來源的裝置的型號。
來源裝置廠商 (src_vendor)	Device-ID 識別為流量來源的裝置的廠商。
來源裝置作業系統系列 (src_osfamily)	Device-ID 識別為流量來源的裝置的作業系統類型。
來源裝置作業系統版本 (src_osversion)	Device-ID 識別為流量來源的裝置的作業系統版本。
來源主機名稱 (src_host)	Device-ID 識別為流量來源的裝置的主機名稱。
來源 MAC 位址 (src_mac)	Device-ID 識別為流量來源的裝置的 MAC 位址。
目的地裝置類別 (dst_category)	Device-ID 識別為流量目的地的裝置的類別。
目的地裝置設定檔 (dst_profile)	Device-ID 識別為流量目的地的裝置的裝置設定檔。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
目的地裝置型號 (dst_model)	Device-ID 識別為流量目的地的裝置的型號。
目的地裝置廠商 (dst_vendor)	Device-ID 識別為流量目的地的裝置的廠商。
目的地裝置作業系統系列 (dst_osfamily)	Device-ID 識別為流量目的地的裝置的作業系統類型。
目的地裝置作業系統版本 (dst_osversion)	Device-ID 識別為流量目的地的裝置的作業系統版本。
目的地主機名稱 (dst_host)	Device-ID 識別為流量目的地的裝置的主機名稱。
目的地 MAC 位址 (dst_mac)	Device-ID 識別為流量目的地的裝置的 MAC 位址。
容器 ID (container_id)	部署應用程式 POD 之 Kubernetes 節點上 PAN-NGFW pod 的容器 ID。
POD 命名空間 (pod_namespace)	受保護應用程式 POD 的命名空間。
POD 名稱 (pod_name)	受保護的應用程式 POD。
來源外部動態清單 (src_edl)	包含流量來源 IP 位址的外部動態清單的名稱。
目的地外部動態清單 (dst_edl)	包含流量目的地 IP 位址的外部動態清單的名稱。
主機 ID (hostid)	GlobalProtect 為識別主機所指派的唯一 ID。
使用者裝置序列號 (serialnumber)	使用者電腦或裝置的序列號。
網域 EDL (domain_edl)	包含流量網域名稱的外部動態清單的名稱。
來源動態位址群組 (src_dag)	原始工作階段來源動態位址群組。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
目的地動態位址群組 (dst_dag)	原始目的地來源動態位址群組。
部分雜湊 (partial_hash)	機器學習部分雜湊。
高解析度時間戳記 (high_res timestamp)	在管理平面接收日誌的時間（毫秒）。 此新欄位的格式為 YYYY-MM-DDThh:ss:sssTZD： • **YYYY**—四位數表示年份 • **MM**—二位數表示月份 • **DD**—二位數表示當月的日期（01 到 31） • **T**—時間戳記開始的指標 • **hh**—兩位數表示小時（使用 24 小時制，00 到 23） • **mm**—兩位數表示分鐘（00 到 59） • **ss**—兩位數表示秒鐘（00 到 60） • **sss**—一位或多位數表示毫秒 • **TZD**—時區指示項（+hh:mm 或 -hh:mm） 對於從執行 *PAN-OS 10.1* 和更高版本的受管理防火牆接收的日誌，支援高解析度時間戳記。從執行 *PAN-OS 9.1* 及早前版本的防火牆接收的日誌顯示 `1969-12-31T16:00:00:000-8:00` 時間戳記，而不論接收日誌的時間如何。
原因 (reason)	資料篩選動作的原因。
理由 (justification)	資料篩選動作的理由。
A 切片服務類型 (nssai_sst)	網路切片 ID 的 A 切片服務類型。
應用程式子類別 (subcategory_of_app)	應用程式設定屬性中指定的應用程式子類別。
應用程式類別 (category_of_app)	應用程式設定屬性中指定的應用程式類別。值為： • 業務系統 • 協同作業 • 一般網際網路

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
	• 媒體 • 網路 • saas
應用程式技術 (technology_of_app)	應用程式設定屬性中指定的應用程式技術。值為： • browser-based • client-server • network-protocol • peer-to-peer
應用程式風險 (risk_of_app)	與應用程式關聯的風險層級（1 = 最低，5 = 最高）。
應用程式特性 (characteristic_of_app)	應用程式適用特性的逗號分隔清單
應用程式容器 (container_of_app)	應用程式的父應用程式。
通道應用程式 (tunneled_app)	通道應用程式的名稱。
應用程式 SaaS (is_saas_of_app)	如果是 SaaS 應用程式，則顯示 `yes`，如果不是 SaaS 應用程式，則顯示 `no`。
應用程式認可狀態 (sanctioned_state_of_app)	如果應用程式受認可，則顯示 `yes`，如果應用程式不受認可，則顯示 `no`。
雲端報告 ID (cloud_reportid)	(PAN-OS 10.2.0) 防火牆傳送的 DLP 雲端服務掃描檔案存在的 32 個字元的唯一 ID。 （PAN-OS 10.2.1 及更新版本）防火牆傳送的 DLP 雲端服務掃描檔案存在的 67 個字元的唯一 ID。 系統會針對 DLP 雲端服務已掃描並產生雲端報告 ID 的檔案，顯示相同的雲端報告 ID。
叢集名稱 (cluster_name)	CN-Series 防火牆叢集的名稱。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
流類型 (flow_type)	標識用於流量的 Proxy 類型。如果使用 Proxy，則顯示 `Explicit Proxy`（明確 `Proxy`）或 `Transparent Proxy`（透明 `Proxy`）。如果未使用 Proxy，則顯示 `NonProxyTraffic`。

HIP 比對日誌欄位

格式：FUTURE_USE、接收時間、序號、類型、威脅/內容類型、FUTURE_USE、產生時間、來源使用者、虛擬系統、電腦名稱、作業系統、來源位址、HIP、重複計數、HIP 類型、FUTURE_USE、FUTURE_USE、序號、動作旗標、裝置群組階層 1、裝置群組階層 2、裝置群組階層 3、裝置群組階層 4、虛擬系統名稱、裝置名稱、虛擬系統 ID、IPv6 來源位址、主機 ID、使用者裝置序號、裝置 MAC 位址、高解析度時間戳記、叢集名稱

欄位名稱	說明
接收時間（receive_time 或 cef-formatted-receive_time）	在管理平面接收日誌的時間。
序號 (serial)	產生日誌之防火牆的序號。
類型 (type)	指定日誌類型；值為 HIP-MATCH。
威脅/內容類型 (subtype)	HIP 比對日誌的子類型：未使用。
產生時間（time_generated 或 cef-formatted-time_generated）	在資料層上產生日誌的時間。
來源使用者 (srcuser)	啟動工作階段之使用者的使用者名稱。
虛擬系統 (vsys)	與 HIP 比對日誌相關聯的虛擬系統。
電腦名稱 (machinename)	使用者電腦的名稱。
作業系統 (os)	安裝在使用者電腦或裝置 (或用戶端系統) 上的作業系統。
來源位址 (src)	來源使用者的 IP 位址。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
HIP (matchname)	HIP 物件或設定檔的名稱。
重複計數 (repeatcnt)	符合 HIP 設定檔的次數。
HIP 類型 (matchtype)	HIP 欄位是表示 HIP 物件還是 HIP 設定檔。
序號 (seqno)	依序遞增的 64 位元日誌項目識別碼；每個日誌類型有一個唯一編號空間。
動作旗標 (actionflags)	指示是否將日誌轉送至 Panorama 的位元欄位。
設備群組階層（dg_hier_level_1 到 dg_hier_level_4）	一系列的識別號碼，可表示設備群組在設備群組階層中的位置。產生日誌的防火牆（或虛擬系統）會在裝置群組階層中包含每個上階項目的識別號碼。此結構不包含共用設備群組（層級 0）。 如果日誌值為 12、34、45 或 0，這表示該日誌是由屬於裝置群組 45 且其上階項目為 34 和 12 的防火牆（或虛擬系統）所產生。若要檢視對應至值 12、34 或 45 的設備群組名稱，請使用下列其中一個方法： API 查詢： `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
虛擬系統名稱 (vsys_name)	與工作階段相關聯的虛擬系統名稱；只在已針對多個虛擬系統啟用的防火牆上有效。
設備名稱 (device_name)	已記錄工作階段的防火牆主機名稱。
虛擬系統 ID (vsys_id)	虛擬系統在 Palo Alto Networks 防火牆上的唯一識別碼。
IPv6 系統位址 (srcipv6)	使用者電腦或裝置的 IPv6 位址。
主機 ID (hostid)	GlobalProtect 為識別主機所指派的唯一 ID。
使用者裝置序列號 (serialnumber)	使用者電腦或裝置的序列號。
裝置 MAC 位址 (mac)	使用者電腦或裝置的 MAC 位址。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
高解析度時間戳記 (high_res _timestamp)	在管理平面接收日誌的時間（毫秒）。 此新欄位的格式為 YYYY-MM-DDThh:ss:sssTZD： • **YYYY**—四位數表示年份 • **MM**—二位數表示月份 • **DD**—二位數表示當月的日期（01 到 31） • **T**—時間戳記開始的指標 • **hh**—兩位數表示小時（使用 24 小時制，00 到 23） • **mm**—兩位數表示分鐘（00 到 59） • **ss**—兩位數表示秒鐘（00 到 60） • **sss**—一位或多位數表示毫秒 • **TZD**—時區指示項（+hh:mm 或 -hh:mm） 對於從執行 *PAN-OS 11.0* 和更新版本的受管理防火牆接收的日誌，支援高解析度時間戳記。從執行 *PAN-OS 9.1* 及早前版本的防火牆接收的日誌顯示 `1969-12-31T16:00:00:000-8:00` 時間戳記，而不論接收日誌的時間如何。
叢集名稱 (cluster_name)	CN-Series 防火牆叢集的名稱。

GlobalProtect 日誌欄位

格式：FUTURE_USE、接收時間、序號、類型、威脅/內容類型、FUTURE_USE、產生時間、虛擬系統、事件 ID、階段、驗證方法、通道類型、來源使用者、來源區域、電腦名稱、公開 IP、公開 IPv6、私人 IP、私人 IPv6、主機 ID、序號、用戶端版本、用戶端作業系統、用戶端作業系統版本、重複計數、原因、錯誤、說明、狀態、位置、登入時間、連線方式、錯誤代碼、入口網站、序號、動作旗標、高解析度時間戳記、選取類型、回應時間、優先順序、嘗試的閘道、閘道、裝置群組階層層級 1、裝置群組階層層級 2、裝置群組階層層級 3、裝置群組階層層級 4、虛擬系統名稱、裝置名稱、虛擬系統 ID、叢集名稱

欄位名稱	說明
接收時間 (receive_time)	在管理平面接收日誌的時間。
序列號 (serial)	產生日誌之防火牆的序號。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
類型 (type)	指定日誌類型；值為 GLOBALPROTECT。
威脅/內容類型 (subtype)	威脅日誌的子類型。值包括以下項： • 資料—符合資料篩選設定檔的資料模式。 • 檔案—符合檔案封鎖設定檔的檔案類型。 • 流量—透過區域保護設定檔偵測到的流量。 • 封包—區域保護設定檔觸發的以封包為基礎的攻擊保護。 • 掃描—透過區域保護設定檔偵測到的掃描。 • 間諜軟體—透過反間諜軟體設定檔偵測到的間諜軟體。 • url—URL 篩選日誌。 • 病毒—透過防毒軟體設定當偵測到的病毒。 • 漏洞—透過漏洞保護設定當偵測到的漏洞入侵。 • wildfire—防火牆依 WildFire 分析設定檔將檔案提交至 WildFire 時產生的 WildFire 裁定，WildFire 提交日誌中會記錄裁定（惡意、網路釣魚、灰色軟體或良性，取決於您記錄的內容）。 • wildfire 病毒—透過防毒軟體設定當偵測到的病毒。
產生時間 (time_generated)	在資料平面上產生日誌的時間。
虛擬系統 (vsys)	與工作階段相關聯的虛擬系統。
事件 ID (eventid)	顯示事件名稱的字串。
階段 (stage)	顯示連線階段的字串（例如，`before-login`、`login` 或 `tunnel`）。
驗證方法 (auth_method)	顯示驗證類型的字串，如 `LDAP`、`RADIUS` 或 `SAML`。
通道類型 (tunnel_type)	通道的類型（SSLVPN 或 IPSec）。
來源使用者 (srcuser)	啟動工作階段之使用者的使用者名稱。
來源地區 (srcregion)	啟動工作階段之使用者的地區。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
電腦名稱 (machinename)	使用者電腦的名稱。
公共 IP (public_ip)	啟動工作階段之使用者的公開 IP 位址。
公開 IPv6 (public_ipv6)	啟動工作階段之使用者的公開 IPv6 位址。
私人 IP (private_ip)	啟動工作階段之使用者的私人 IP 位址。
私人 IPv6 (private_IPv6)	啟動工作階段之使用者的私人 IPv6 位址。
主機 ID (hostid)	GlobalProtect 為了識別主機所指派的唯一 ID。
序列號 (serialnumber)	使用者電腦或裝置的序列號。
用戶端版本 (client_ver)	用戶端的 GlobalProtect 應用程式版本。
用戶端作業系統 (client_os)	用戶端裝置的作業系統類別（例如，Windows 或 Linux）。
用戶端作業系統版本 (client_os_ver)	用戶端裝置的作業系統版本。
重複計數 (repeatcnt)	GlobalProtect 在過去五秒內偵測到具有相同來源 IP 位址、目的地 IP 位址、應用程式以及子類型的工作階段。
原因 (reason)	顯示隔離原因的字串。
錯誤 (error)	顯示在任何事件中發生錯誤的字串。
說明 (opaque)	發生的任何事件的其他資訊。
狀態 (status)	事件的狀態（成功或失敗）。
位置 (location)	顯示管理員定義的 GlobalProtect 入口網站或閘道的位置的字串。
登入時間 (login_duration)	使用者連線至 GlobalProtect 閘道（從登入到登出）的時間長度，以秒為單位。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
連線方式 (connect_method)	顯示 GlobalProtect 應用程式連線到閘道的方式（例如，`on-demand` 或 `user-logon`）的字串。
錯誤代碼 (error_code)	與發生的任何錯誤相關聯的整數。
入口網站 (portal)	GlobalProtect 入口網站或閘道的名稱。
序號 (seqno)	依序遞增的 64 位元日誌項目識別碼；每個日誌類型有一個唯一編號空間。
動作旗標 (actionflags)	指示是否將日誌轉送至 Panorama 的位元欄位。
閘道選取方法 (selection_type)	選取用於連線至閘道的連線方法。 • 手動—您希望 GlobalProtect 應用程式手動連線至閘道。 • 偏好—您希望 GlobalProtect 應用程式連線至偏好閘道。 • 自動—基於指派到閘道的優先順序和回應時間自動連線到 **Best Available**（最佳可用）閘道。
SSL 回應時間 (response_time)	通道設定期間在端點上測量的所選閘道的 SSL 回應時間（以毫秒為單位）。
閘道優先順序 (priority)	閘道的優先順序，GlobalProtect 應用程式可基於最高 (1)、高 (2)、中等 (3)、低 (4) 或最低 (5) 的順序連線至閘道。
嘗試的閘道 (attempted_gateways)	為每個閘道連線嘗試收集的欄位，包括閘道名稱、SSL 回應時間和優先順序（請參閱多個閘道組態中的閘道優先順序）。每個欄位項目都使用逗號分隔，例如 `g82-gateway,12,3`。每個閘道項目都使用分號分隔，例如 `g83-gateway,10,2;g84-gateway,-1,1`。
閘道名稱 (gateway)	閘道的名稱，在入口網站設定上指定。
設備群組階層（dg_hier_level_1 到 dg_hier_level_4）	一系列的識別號碼，可表示設備群組在設備群組階層中的位置。產生日誌的防火牆（或虛擬系統）會在裝置群組階層中包含每個上階項目的識別號碼。此結構不包含共用設備群組（層級 0）。 如果日誌值為 12、34、45 或 0，這表示該日誌是由屬於裝置群組 45 且其上階項目為 34 和 12 的防火牆（或虛擬系統）所產生。若要檢視對應至值 12、34 或 45 的設備群組名稱，請使用下列其中一個方法：

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
	API 查詢： `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
虛擬系統名稱 (vsys_name)	與工作階段相關聯的虛擬系統名稱；只在已針對多個虛擬系統啟用的防火牆上有效。
設備名稱 (device_name)	已記錄工作階段的防火牆主機名稱。
虛擬系統 ID (vsys_id)	虛擬系統在 Palo Alto Networks 防火牆上的唯一識別碼。
叢集名稱 (cluster_name)	CN-Series 防火牆叢集的名稱。

IP-Tag 日誌欄位

格式：FUTURE_USE、接收時間、序號、類型、威脅/內容類型、FUTURE_USE、產生時間、虛擬系統、來源 IP、標籤名稱、事件 ID、重複計數、逾時、資料來源名稱、資料來源類型、資料來源子類型、序號、動作旗標、裝置群組階層 1、裝置群組階層 2、裝置群組階層 3、裝置群組階層 4、虛擬系統名稱、裝置名稱、虛擬系統 ID、高解析度時間戳記、叢集名稱

欄位名稱	說明
接收時間（receive_time 或 cef-formatted-receive_time）	在管理平面接收日誌的時間。
序號 (serial)	產生日誌之防火牆的序號。
類型 (type)	指定日誌類型；值為 IPTAG。
威脅/內容類型 (subtype)	HIP 比對日誌的子類型；未使用。
產生時間（time_generated 或 cef-formatted-time_generated）	在資料層上產生日誌的時間。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
虛擬系統 (vsys)	與 HIP 比對日誌相關聯的虛擬系統。
來源 IP (src)	來源使用者的 IP 位址。
標籤名稱 (tag_name)	與來源 IP 位址對應的標籤。
事件 ID (event_id)	顯示事件名稱的字串。
重複計數 (repeatcnt)	在 5 秒鐘內看到的有相同來源 IP、目的地 IP、應用程式與子類型的工作階段數。
逾時 (timeout)	來源 IP 位址的 IP 位址至標籤對應到期前的時間。
資料來源名稱 (datasourcename)	收集對應資訊的來源名稱。
資料來源類型 (datasource_type)	收集對應資源的來源。
資料來源子類型 (datasource_subtype)	用於在資料來源中識別 IP 位址至使用者名稱對應對應的機制。
序號 (seqno)	依序遞增的 64 位元日誌項目識別碼。每個日誌類型有一個唯一編號空間。
動作旗標 (actionflags)	指示是否將日誌轉送至 Panorama 的位元欄位。
設備群組階層（dg_hier_level_1 到 dg_hier_level_4）	一系列的識別號碼，可表示裝置群組在裝置群組階層中的位置。產生日誌的防火牆（或虛擬系統）會在裝置群組階層中包含每個上階項目的識別號碼，但未包括在該結構的共用裝置群組（層級 0）除外。 如果日誌值為 12、34、45 和 0，這表示該日誌是由屬於裝置群組 45 且其上階項目為 34 和 12 的防火牆（或虛擬系統）所產生。若要檢視對應至值 12、34，或 45 的裝置群組名稱，請使用下列其中一個方法： API 查詢： `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
虛擬系統名稱 (vsys_name)	與工作階段相關聯的虛擬系統名稱；只在已針對多個虛擬系統啟用的防火牆上有效。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
設備名稱 (device_name)	已記錄工作階段的防火牆主機名稱。
虛擬系統 ID (vsys_id)	虛擬系統在 Palo Alto Networks 防火牆上的唯一識別碼。
高解析度時間戳記 (high_res timestamp)	在管理平面接收日誌的時間（毫秒）。 此新欄位的格式為 YYYY-MM-DDThh:ss:sssTZD： • **YYYY**—四位數表示年份 • **MM**—二位數表示月份 • **DD**—二位數表示當月的日期（01 到 31） • **T**—時間戳記開始的指標 • **hh**—兩位數表示小時（使用 24 小時制，00 到 23） • **mm**—兩位數表示分鐘（00 到 59） • **ss**—兩位數表示秒鐘（00 到 60） • **sss**—一位或多位數表示毫秒 • **TZD**—時區指示項（+hh:mm 或 -hh:mm） 對於從執行 *PAN-OS 11.0* 和更新版本的受管理防火牆接收的日誌，支援高解析度時間戳記。從執行 *PAN-OS 9.1* 及早前版本的防火牆接收的日誌顯示 `1969-12-31T16:00:00:000-8:00` 時間戳記，而不論接收日誌的時間如何。
叢集名稱 (cluster_name)	CN-Series 防火牆叢集的名稱。

User-ID 日誌欄位

格式：FUTURE_USER、接收時間、序號、類型、威脅/內容類型、FUTURE_USE、產生時間、虛擬系統、來源 IP、使用者、資料來源名稱、事件 ID、重複計數、逾時臨界值、來源連接埠、目的地連接埠、資料來源、資料來源類型、序號、動作旗標、裝置群組階層 1、裝置群組階層 2、裝置群組階層 3、裝置群組階層 4、虛擬系統名稱、裝置名稱、虛擬系統 ID、因素類型、因素完成時間、因素號碼、使用者群組標幟、基於來源的使用者、標籤名稱、高解析度時間戳記、原始資料來源、FUTURE_USE、叢集名稱

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
接收時間（receive_time 或 cef-formatted-receive_time）	在管理平面接收日誌的時間。
序號 (serial)	產生日誌之防火牆的序號。
類型 (type)	指定日誌類型；值為 USERID。
威脅/內容類型 (subtype)	User-ID 日誌的子類型；值是 login、logout、register-tag 和 unregister-tag。 • 登入—使用者已登入。 • 登出—使用者已登出。 • register-tag—指示為使用者註冊的一個或多個標籤。 • unregister-tag—指示為使用者取消註冊的一個或多個標籤。
產生時間（time_generated 或 cef-formatted-time_generated）	在資料層上產生日誌的時間。
虛擬系統 (vsys)	與組態日誌相關聯的虛擬系統。
來源 IP (ip)	原始工作階段來源 IP 位址。
使用者 (user)	用於識別使用者。
資料來源名稱 (datasourcename)	用於傳送 IP（連接埠）-使用者對應的 User-ID 來源。
事件 ID (eventid)	顯示事件名稱的字串。
重複計數 (repeatcnt)	在 5 秒鐘內看到的有相同來源 IP、目的地 IP、應用程式與子類型的工作階段數。
逾時臨界值 (timeout)	超過此逾時後，將清除 IP/使用者對應。
來源連接埠 (beginport)	工作階段使用的來源連接埠。
目的地連接埠 (endport)	工作階段使用的目的地連接埠。
資料來源 (datasource)	收集對應資源的來源。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
資料來源類型 (datasourcetype)	用於在資料來源中識別 IP/使用者對應的機制。
序號 (seqno)	產生日誌之防火牆的序號。
動作旗標 (actionflags)	指示是否將日誌轉送至 Panorama 的位元欄位。
設備群組階層（dg_hier_level_1 到 dg_hier_level_4）	一系列的識別號碼，可表示設備群組在設備群組階層中的位置。產生日誌的防火牆（或虛擬系統）會在裝置群組階層中包含每個上階項目的識別號碼。此結構不包含共用設備群組（層級 0）。 如果日誌值為 12、34、45 或 0，這表示該日誌是由屬於裝置群組 45 且其上階項目為 34 和 12 的防火牆（或虛擬系統）所產生。若要檢視對應至值 12、34 或 45 的設備群組名稱，請使用下列其中一個方法： API 查詢：`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
虛擬系統名稱 (vsys_name)	與工作階段相關聯的虛擬系統名稱；只在已針對多個虛擬系統啟用的防火牆上有效。
設備名稱 (device_name)	已記錄工作階段的防火牆主機名稱。
虛擬系統 ID (vsys_id)	虛擬系統在 Palo Alto Networks 防火牆上的唯一識別碼。
因素類型 (factortype)	在顯示多因素驗證時，用於驗證使用者的廠商。
因素完成時間 (factorcompletiontime)	驗證完成時間。
因素號碼 (factorno)	指示是使用主要驗證 (1) 還是額外驗證（2、3）。
使用者群組標識 (ugflags)	顯示使用者群組在使用者群組對應期間是否已找到。支援的值包括： • 已找到使用者群組—表示使用者是否可以對應至群組。 • 重複使用者—表示是否在使用者群組中找到了重複使用者。如果未找到使用者群組，則顯示 `N/A`。
使用者來源 (userbysource)	顯示通過 IP 位址-使用者名稱對應從來源接收的使用者名稱。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
標籤名稱 (tag_name)	與動態使用者群組（其與使用者對應的使用者群組關聯）關聯的標籤的名稱。
高解析度時間戳記 (high_res timestamp)	在管理平面接收日誌的時間（毫秒）。 此新欄位的格式為 YYYY-MM-DDThh:ss:sssTZD： • **YYYY**—四位數表示年份 • **MM**—二位數表示月份 • **DD**—二位數表示當月的日期（01 到 31） • **T**—時間戳記開始的指標 • **hh**—兩位數表示小時（使用 24 小時制，00 到 23） • **mm**—兩位數表示分鐘（00 到 59） • **ss**—兩位數表示秒鐘（00 到 60） • **sss**—一位或多位數表示毫秒 • **TZD**—時區指示項（+hh:mm 或 -hh:mm） 對於從執行 *PAN-OS 11.0* 和更新版本的受管理防火牆接收的日誌，支援高解析度時間戳記。從執行 *PAN-OS 9.1* 及早前版本的防火牆接收的日誌顯示 *`1969-12-31T16:00:00:000-8:00`* 時間戳記，而不論接收日誌的時間如何。
原始資料來源（origindatasource）	User-ID 對應的來源。
叢集名稱 (cluster_name)	CN-Series 防火牆叢集的名稱。

解密日誌欄位

格式：FUTURE_USE、接收時間、序號、類型、威脅/內容類型、設定版本、產生時間、來源位址、目的地位址、NAT 來源 IP、NAT 目的地 IP、規則、來源使用者、目的地使用者、應用程式、虛擬系統、來源區域、目的地區域、輸入介面、輸出介面、日誌動作、記錄時間、工作階段 ID、重複計數、來源連接埠、目的地連接埠、NAT 來源連接埠、NAT 目的地連接埠、旗標、IP 通訊協定、動作、通道、FUTURE_USE、FUTURE_USE、來源 VM UUID、目的地 VM UUID、規則的 UUID、用戶端到防火牆的階段、防火牆到伺服器的階段、TLS 版本、金鑰交換演算法、加密演算法、雜湊演算法、政策名稱、橢圓曲線、錯誤索引、根狀態、鏈結狀態、Proxy 類型、憑證序號、指紋、憑證開始日期、憑證結束日期、憑證版本、憑證大小、通用名稱長度、簽發者通用名稱長度、根通用名稱長度、SNI 長度、憑證旗標、主體通用名稱、簽發者主體通用名稱、根主體通用名稱、伺服器名稱指示、錯誤、容器 ID、POD 命名空間、POD 名稱、來源外部動態清單、目的地外

©2024 Palo Alto Networks, Inc.

部動態清單、來源動態位址群組、目的地動態位址群組、高解析度時間戳記、來源裝置類別、來源裝置設定檔、來源裝置型號、來源裝置廠商、來源裝置作業系統系列、來源裝置作業系統版本、來源主機名稱、來源 Mac 位址、目的地裝置類別、目的地裝置設定檔、目的地裝置型號、目的地裝置廠商、目的地裝置作業系統系列、目的地裝置作業系統版本、目的地主機名稱、目的地 Mac 位址、序號、動作旗標、裝置群組階層層級 1、裝置群組階層層級 2、裝置群組階層層級 3、裝置群組階層層級 4、虛擬系統名稱、裝置名稱、虛擬系統 ID、應用程式子類別、應用程式類別、應用程式技術、應用程式風險、應用程式特性、應用程式容器、應用程式 SaaS、應用程式認可狀態、叢集名稱

欄位名稱	說明
接收時間（receive_time 或 cef-formatted-receive_time）	在管理平面接收日誌的時間。
序號 (serial)	產生日誌之防火牆的序號。
類型 (type)	指定日誌類型；值為 DECRYPTION。
威脅/內容類型 (subtype)	不在解密日誌中使用。
設定版本 (config_ver)	軟體版本。
產生時間 (time_generated)	在資料層上產生日誌的時間。
來源位址 (src)	原始工作階段來源 IP 位址。
目的地位址 (dst)	原始工作階段目的地 IP 位址。
NAT 來源 IP (natsrc)	如果已執行來源 NAT，則為後續 NAT 來源 IP 位址。
NAT 目的地 IP (natdst)	如果已執行目的地 NAT，則為後續 NAT 目的地 IP 位址。
規則 (rule)	控制工作階段流量的安全性原則規則。
來源使用者 (srcuser)	啟動工作階段之使用者的使用者名稱。
目的地使用者 (dstuser)	將工作階段指定至之使用者的使用者名稱。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
應用程式 (app)	與工作階段相關聯的應用程式。
虛擬系統 (vsys)	與工作階段相關聯的虛擬系統。
來源區域 (from)	工作階段的來源區域。
目的地區域 (to)	將工作階段指定至的區域。
輸入介面 (inbound_if)	工作階段的來源介面。
輸出介面 (outbound_if)	將工作階段指定至的介面。
日誌動作 (logset)	套用至工作階段的日誌轉送設定檔。
記錄時間 (time_received)	收到日誌的時間。
工作階段 ID (sessionid)	套用至每個工作階段的內部數字識別碼。
重複計數 (repeatcnt)	在 5 秒鐘內看到的有相同來源 IP、目的地 IP、應用程式與內容/威脅類型的工作階段數。
來源連接埠 (sport)	工作階段使用的來源連接埠。
目的地連接埠 (dport)	工作階段使用的目的地連接埠。
NAT 來源連接埠 (natsport)	後續 NAT 來源連接埠。
NAT 目的地連接埠 (natdport)	後續 NAT 目的地連接埠。
標幟 (flags)	32 位元欄位提供工作階段詳細資訊；您可以透過 AND 有記錄值的值解碼此欄位： • 0x80000000—工作階段有封包擷取 (PCAP) • 0x40000000—已啟用選項，允許用戶端使用多條路徑連線到目的地主機 • 0x20000000—檔案已提交給 WildFire 進行裁定 • 0x10000000—偵測到一般使用者提交的企業認證

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
	• 0x08000000—流量的來源在允許清單上，且不受偵察保護 • 0x02000000—IPv6 工作階段 • 0X01000000—解密 SSL 工作階段 (SSL Proxy) • 0x00800000—透過 URL 篩選拒絕工作階段 • 0x00400000—工作階段已執行 NAT 轉譯 • 0x00200000—透過驗證入口網站擷取工作階段的使用者資訊 • 0x00100000—應用程式流量位於非標準目的地連接埠 • 0x00080000—Proxy 中的 X-Forwarded-For 值在來源使用者欄位中 • 0x00040000—日誌對應至 http proxy 工作階段內的交易 (Proxy 交易) • 0x00020000—用戶端到伺服器的流量符合基於原則的轉送 • 0x00010000—伺服器到用戶端的流量符合基於原則的轉送 • 0x00008000—工作階段是容器頁面存取（容器頁面） • 0x00002000—工作階段暫時符合規則，以進行隱含應用程式相依性處理。適用於 PAN-OS 5.0.0 及以上版本。 • 0x00000800—對稱傳回用於轉送此工作階段的流量 • 0x00000400—解密的流量透過鏡像連接埠傳送出純文字 • 0x00000100—檢查外部通道的有效負載
IP 通訊協定 (proto)	與工作階段相關聯的 IP 通訊協定。
動作 (action)	針對工作階段採取的動作；可能的值為： • 允許—原則已允許工作階段 • 拒絕—原則已拒絕工作階段 • 丟棄—無訊息丟棄工作階段 • 丟棄 ICMP—無訊息丟棄工作階段，並將 ICMP 無法連線訊息傳送至主機或應用程式 • 重設兩者—已終止工作階段，並將 TCP 重設傳送至連線的兩端 • 重設用戶端—已終止工作階段，並將 TCP 重設傳送至用戶端 • 重設伺服器—已終止工作階段，並將 TCP 重設傳送至伺服器
通道 (tunnel)	通道類型。
來源 VM UUID (src_uuid)	在 VMware NSX 環境中的來賓虛擬機器的來源通用唯一識別碼。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
目的地 VM UUID (dst_uuid)	在 VMware NSX 環境中的來賓虛擬機器的目的地通用唯一識別碼。
規則 UUID (rule_uuid)	永久識別規則的 UUID。
用戶端到防火牆的階段 (hs_stage_c2f)	從用戶端到防火牆的 TLS 交握的階段，例如，Client Hello、Server Hello、憑證、用戶端/伺服器金鑰交換等。
防火牆到伺服器的階段 (hs_stage_f2s)	從防火牆到伺服器的 TLS 交握的階段。
TLS 版本 (tls_version)	用於工作階段的 TLS 通訊協定的版本。
金鑰交換演算法 (tls_keyxchg)	用於工作階段的金鑰交換演算法。
加密演算法 (tls_enc)	用於加密工作階段資料的演算法，例如 AES-128-CBC、AES-256-GCM 等。
雜湊演算法 (tls_auth)	用於工作階段的驗證演算法，例如 SHA、SHA256、SHA384 等。
原則名稱 (policy_name)	與工作階段關聯的解密原則的名稱。
橢圓曲線 (ec_curve)	用戶端和伺服器交涉的橢圓密碼曲線，用於使用 ECDHE 加密套件的連線。
錯誤索引 (err_index)	發生的錯誤的類型：密碼、資源、繼續、版本、通訊協定、憑證、功能或 HSM。
根狀態 (root_status)	跟憑證的狀態，例如，受信任、不受信任、未受檢查。
鏈結狀態 (chain_status)	鏈結是否受信任。值為： • 未受檢查 • 不受信任 • 受信任 • 不完整
Proxy 類型 (proxy_type)	解密 Proxy 類型，例如，正向（表示正向 Proxy）、輸入（表示輸入檢查）、不解密（表示不解密的流量）、GlobalProtect 等。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
憑證序號 (cert_serial)	憑證的唯一識別碼（由憑證簽發者產生）。
憑證指紋 (fingerprint)	x509 二進位格式的憑證雜湊。
憑證開始日期 (notbefore)	憑證變得有效的時間（憑證在此時間之前無效）。
憑證結束日期 (notafter)	憑證到期的時間（憑證在此時間之後變得無效）。
憑證版本 (cert_ver)	憑證版本（V1、V2 或 V3）。
憑證大小 (cert_size)	憑證金鑰大小。
通用名稱長度 (cn_len)	主體通用名稱的長度。
簽發者通用名稱長度 (issuer_len)	簽發者通用名稱的長度。
根通用名稱長度 (rootcn_len)	根通用名稱的長度。
SNI 長度 (sni_len)	伺服器名稱指示（主機名稱）的長度。
憑證旗標 (cert_flags)	憑證旗標可以返回七個值： • 工作階段已繼續 (b_resume_session) • 憑證（主體）通用名稱已截斷 (b_cert_cn_truncated) • 簽發者通用名稱已截斷 (b_issuer_cn_truncated) • 根通用名稱已截斷 (b_issuer_cn_truncated) • 伺服器名稱指示 (SNI) 已截斷 (b_sni_truncated) • 憑證類型、RSA 或 ECDSA (b_cert_type) • 未使用 (padding3)
主體通用名稱 (cn)	網域名稱（憑證保護的伺服器的名稱）。
簽發者通用名稱 (issuer_cn)	驗證憑證內容的組織的名稱。
根通用名稱 (root_cn)	根憑證授權單位的名稱。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
伺服器名稱指示 (sni)	用戶端嘗試聯絡的伺服器的主機名稱。使用 SNI 讓伺服器能夠託管多個網站，並在同一 IP 位址和 TCP 連接埠上顯示多個憑證，因為每個網站都有唯一的 SNI。
錯誤 (error)	顯示事件中所發生錯誤的字串。
容器 ID (container_id)	當防火牆在雲端容器中執行時，用於標識容器的唯一英數字元字串。
POD 命名空間 (pod_namespace)	Kubernetes pod 命名空間的名稱。
POD 名稱 (pod_name)	Kubernetes pod 的名稱。
來源外部動態清單 (src_edl)	包含流量來源 IP 位址的外部動態清單的名稱。
目的地外部動態清單 (dst_edl)	包含流量目的地 IP 位址的外部動態清單的名稱。
來源動態位址群組 (src_dag)	Device-ID 識別為流量來源的動態位址群組。
目的地動態位址群組 (dst_dag)	Device-ID 識別為流量目的地的動態位址群組。
高解析度時間戳記 (high_res _timestamp)	在管理平面接收日誌的時間（毫秒）。 此欄位的格式為 YYYY-MM-DDThh:ss:sssTZD： • **YYYY**—四位數表示年份 • **MM**—二位數表示月份 • **DD**—二位數表示當月的日期（01 到 31） • **T**—時間戳記開始的指標 • **hh**—兩位數表示小時（使用 24 小時制，00 到 23） • **mm**—兩位數表示分鐘（00 到 59） • **ss**—兩位數表示秒鐘（00 到 60） • **sss**—一位或多位數表示毫秒 • **TZD**—時區指示項（+hh:mm 或 -hh:mm）

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
	對於從執行 *PAN-OS 11.0* 和更新版本的受管理防火牆接收的日誌，支援高解析度時間戳記。從執行 *PAN-OS 9.1* 及早前版本的防火牆接收的日誌顯示 `1969-12-31T16:00:00:000-8:00` 時間戳記，而不論接收日誌的時間如何。
來源裝置類別 (src_category)	Device-ID 識別為流量來源的裝置的類別。
來源裝置設定檔 (src_profile)	Device-ID 識別為流量來源的裝置的裝置設定檔。
來源裝置型號 (src_model)	Device-ID 識別為流量來源的裝置的型號。
來源裝置廠商 (src_vendor)	Device-ID 識別為流量來源的裝置的廠商。
來源裝置作業系統系列 (src_osfamily)	Device-ID 識別為流量來源的裝置的作業系統類型。
來源裝置作業系統版本 (src_osversion)	Device-ID 識別為流量來源的裝置的作業系統版本。
來源主機名稱 (src_host)	Device-ID 識別為流量來源的裝置的主機名稱。
來源 MAC 位址 (src_mac)	Device-ID 識別為流量來源的裝置的 MAC 位址。
目的地裝置類別 (dst_category)	Device-ID 識別為流量目的地的裝置的類別。
目的地裝置設定檔 (dst_profile)	Device-ID 識別為流量目的地的裝置的裝置設定檔。
目的地裝置型號 (dst_model)	Device-ID 識別為流量目的地的裝置的型號。
目的地裝置廠商 (dst_vendor)	Device-ID 識別為流量目的地的裝置的廠商。
目的地裝置作業系統系列 (dst_osfamily)	Device-ID 識別為流量目的地的裝置的作業系統類型。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
目的地裝置作業系統版本 (dst_osversion)	Device-ID 識別為流量目的地的裝置的作業系統版本。
目的地主機名稱 (dst_host)	Device-ID 識別為流量目的地的裝置的主機名稱。
目的地 MAC 位址 (dst_mac)	Device-ID 識別為流量目的地的裝置的 MAC 位址。
序號 (seqno)	依序遞增的 64 位元日誌項目識別碼；每個日誌類型有一個唯一編號空間。
動作旗標 (actionflags)	指示是否將日誌轉送至 Panorama 的位元欄位。
設備群組階層（dg_hier_level_1 到 dg_hier_level_4）	一系列的識別號碼，可表示設備群組在設備群組階層中的位置。產生日誌的防火牆（或虛擬系統）會在裝置群組階層中包含每個上階項目的識別號碼。此結構不包含共用設備群組（層級 0）。 如果日誌值為 12、34、45 或 0，這表示該日誌是由屬於裝置群組 45 且其上階項目為 34 和 12 的防火牆（或虛擬系統）所產生。若要檢視對應至值 12、34 或 45 的設備群組名稱，請使用下列其中一個方法： API 查詢： `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
虛擬系統名稱 (vsys_name)	與工作階段相關聯的虛擬系統名稱；只在已針對多個虛擬系統啟用的防火牆上有效。
設備名稱 (device_name)	已記錄工作階段的防火牆主機名稱。
虛擬系統 ID (vsys_id)	虛擬系統在 Palo Alto Networks 防火牆上的唯一識別碼。
應用程式子類別 (subcategory_of_app)	應用程式設定屬性中指定的應用程式子類別。
應用程式類別 (category_of_app)	應用程式設定屬性中指定的應用程式類別。值為： • 業務系統 • 協同作業 • 一般網際網路

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
	• 媒體 • 網路 • saas
應用程式技術 (technology_of_app)	應用程式設定屬性中指定的應用程式技術。值為： • browser-based • client-server • network-protocol • peer-to-peer
應用程式風險 (risk_of_app)	與應用程式關聯的風險層級（1 = 最低，5 = 最高）。
應用程式特性 (characteristic_of_app)	應用程式適用特性的逗號分隔清單
應用程式容器 (container_of_app)	應用程式的父應用程式。
應用程式 SaaS (is_saas_of_app)	如果是 SaaS 應用程式，則顯示 `1` ，如果不是 SaaS 應用程式，則顯示 `0`。
應用程式認可狀態 (sanctioned_state_of_app)	如果應用程式受認可，則顯示 `1`，如果應用程式不受認可，則顯示 `0`。
叢集名稱 (cluster_name)	CN-Series 防火牆叢集的名稱。

通道檢查日誌欄位

格式：FUTURE_USE、接收時間、序號、類型、子類型、FUTURE_USE、產生時間、來源位址、目的地位址、NAT 來源 IP、NAT 目的地 IP、規則名稱、來源使用者、目的地使用者、應用程式、虛擬系統、來源區域、目的地區域、輸入界面、輸出介面、日誌動作、FUTURE_USE、工作階段 ID、重複計數、來源連接埠、目的地連接埠、NAT 來源連接埠、NAT 目的地連接埠、標幟、通訊協定、動作、嚴重性、序號、動作旗標、來源位置、目的地位置、裝置群組階層層級 1、裝置群組階層層級 2、裝置群組階層層級 3、裝置群組階層層級 4、虛擬系統名稱、裝置名稱、通道 ID/IMSI、監控標籤/IMEI、上層工作階段 ID、上層開始時間、通道、位元組數、傳送的位元組數、接收的位元組數、封包數、傳送的封包數、接收的封包數、最大封裝、未知通訊協定、嚴格檢查、通道片段、建立的工作階段數、關閉的工作階段數、工作階段結束原因、動作來源、開始時間、經過時間、通道檢查規則、遠端使用者 IP、遠端使用者 ID、規則 UUID、PCAP ID、動態使用者群組、來源外部動態清單、目的地外部動態清單、高解析度時間戳記、A 切片差分器、A 切片服務類

©2024 Palo Alto Networks, Inc.

型、PDU 工作階段 ID、應用程式子類別、應用程式類別、應用程式技術、應用程式風險、應用程式特性、應用程式容器、應用程式 SaaS、應用程式認可狀態、叢集名稱

欄位名稱	說明
接收時間（receive_time 或 cef-formatted-receive_time）	在管理平面接收日誌的月份、日期和時間。
序號 (serial)	產生日誌之防火牆的序號。
類型 (type)	與工作階段相關的日誌類型：START（開始）或 END（結束）。
威脅/內容類型 (subtype)	流量日誌的子類型；值有開始、結束、丟棄與拒絕 • 開始—開始的工作階段 • 結束—結束的工作階段 • 丟棄—識別應用程式前丟棄的工作階段，且沒有允許工作階段的規則。 • 拒絕—識別應用程式後丟棄的工作階段，且有要封鎖的規則或沒有允許工作階段的規則。
產生時間（time_generated 或 cef-formatted-time_generated）	在資料層上產生日誌的時間。
來源位址 (src)	工作階段中封包的來源 IP 位址。
目的地位址 (dst)	工作階段中封包的目的地 IP 位址。
NAT 來源 IP (natsrc)	如果已執行來源 NAT，則為後續 NAT 來源 IP 位址。
NAT 目的地 IP (natdst)	如果已執行目的地 NAT，則為後續 NAT 目的地 IP 位址。
規則名稱 (rule)	對工作階段使用的安全性原則規則名稱。
來源使用者 (srcuser)	工作階段中封包的來源使用者 ID。
目的地使用者 (dstuser)	工作階段中封包的目的地使用者 ID。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
應用程式 (app)	工作階段中使用的通道通訊協定。
虛擬系統 (vsys)	與工作階段相關聯的虛擬系統。
來源區域 (from)	工作階段中封包的來源區域。
目的地區域 (to)	工作階段中封包的目的地區域。
輸入介面 (inbound_if)	工作階段的來源介面。
輸出介面 (outbound_if)	將工作階段指定至的介面。
日誌動作 (logset)	套用至工作階段的日誌轉送設定檔。
工作階段 ID (sessionid)	所記錄之工作階段的 ID。
重複計數 (repeatcnt)	在 5 秒鐘內看到的有相同來源 IP、目的地 IP、應用程式與子類型的工作階段數。
來源連接埠 (sport)	工作階段使用的來源連接埠。
目的地連接埠 (dport)	工作階段使用的目的地連接埠。
NAT 來源連接埠 (natsport)	後續 NAT 來源連接埠。
NAT 目的地連接埠 (natdport)	後續 NAT 目的地連接埠。
標幟 (flags)	32 位元欄位提供工作階段詳細資訊；您可以透過 AND 有記錄值的值解碼此欄位： • 0x80000000—工作階段有封包擷取 (PCAP) • 0x02000000—IPv6 工作階段 • 0x01000000—SSL 工作階段已解密 (SSL Proxy) • 0x00800000—已透過 URL 篩選拒絕工作階段 • 0x00400000—工作階段已執行 NAT 轉譯 (NAT) • 0x00200000—透過驗證入口網站擷取工作階段的使用者資訊 • 0x00080000—Proxy 中的 X-Forwarded-For 值在來源使用者欄位中

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
	• 0x00040000—日誌對應至 http proxy 工作階段內的交易（Proxy 交易） • 0x00008000—工作階段是容器頁面存取（容器頁面） • 0x00002000—工作階段暫時符合規則，以進行隱含應用程式相依性處理。適用於 PAN-OS 5.0.0 及以上版本。 • 0x00000800—對稱傳回用於轉送此工作階段的流量
IP 通訊協定 (proto)	與工作階段相關聯的 IP 通訊協定。
動作 (action)	針對工作階段採取的動作；可能的值為： • 允許—原則已允許工作階段 • 拒絕—原則已拒絕工作階段 • 丟棄—無訊息丟棄工作階段 • 丟棄 ICMP—無訊息丟棄工作階段，並將 ICMP 無法連線訊息傳送至主機或應用程式 • 重設兩者—已終止工作階段，並將 TCP 重設傳送至連線的兩端 • 重設用戶端—已終止工作階段，並將 TCP 重設傳送至用戶端 • 重設伺服器—已終止工作階段，並將 TCP 重設傳送至伺服器
嚴重性 (severity)	與事件相關聯的嚴重性；值有資訊、低、中、高、重要。
序號 (seqno)	依序遞增的 64 位元日誌項目識別碼；每個日誌類型有一個唯一編號空間。PA-7000 系列防火牆不支援此欄位。
動作旗標 (actionflags)	指示是否將日誌轉送至 Panorama 的位元欄位。
來源位置 (srcloc)	私人位址的來源國家/地區或內部地區；最大長度為 32 位元組。
目的地位置 (dstloc)	私人位址的目的地國家或內部地區。最大長度為 32 位元組。
設備群組階層（dg_hier_level_1 到 dg_hier_level_4）	一系列的識別號碼，可表示設備群組在設備群組階層中的位置。產生日誌的防火牆（或虛擬系統）會在裝置群組階層中包含每個上階項目的識別號碼。此結構不包含共用設備群組（層級 0）。 如果日誌值為 12、34、45 或 0，這表示該日誌是由屬於裝置群組 45 且其上階項目為 34 和 12 的防火牆（或虛擬系統）所產生。若要檢視對應至值 12、34 或 45 的設備群組名稱，請使用下列其中一個方法：

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
	API 查詢： `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
虛擬系統名稱 (vsys_name)	與工作階段相關聯的虛擬系統名稱；只在已針對多個虛擬系統啟用的防火牆上有效。
設備名稱 (device_name)	已記錄工作階段的防火牆主機名稱。
通道 ID (tunnelid)	被檢查的通道 ID 或行動用戶的國際行動用戶識別 (IMSI) ID。
監控頁籤 (monitortag)	您為通道檢查原則規則設定的監控名稱或行動裝置的國際行動裝置識別 (IMSI) ID。
上層工作階段 ID (parent_session_id)	此工作階段通道所在的工作階段 ID。僅適用於內部通道（若有兩層通道）或內部內容（若僅有一層通道）。
上層開始時間 (parent_start_time)	上層通道工作階段開始的年/月/日 時：分：秒。
通道類型 (tunnel)	通道的類型，例如 GRE 或 IPSec。
位元組 (bytes)	工作階段中的位元組數。
傳送的位元組 (bytes_sent)	工作階段之用戶端至伺服器方向上的位元組數。
收到的位元組 (bytes_received)	工作階段之伺服器至用戶端方向上的位元組數。
封包數 (packets)	工作階段的封包（傳輸與接收）總數。
已傳送的封包數 (pkts_sent)	工作階段之用戶端至伺服器封包數。
已接收的封包 (pkts_received)	工作階段之伺服器至用戶端封包數。
最大封裝 (max_encap)	防火牆因封包數超出通道檢查原則規則（如果超出最高通道檢查規則層級，則丟棄封包）中設定的封裝層級書上限而丟棄的封包數。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
未知通訊協定 (unknown_proto)	防火牆因封包內包含未知通訊協定，而按照通道檢查原則規則（如果通道內有未知通訊協定，則丟棄封包）啟用的設定丟棄的封包數。
嚴格檢查 (strict_check)	防火牆由於封包內的通道通訊協定標頭與不符合關於通道通訊協定的 RFC 要求，而按照通道檢查原則規則（**Drop packet if tunnel protocol fails strict header check**如果通道通訊協定未通過嚴格標頭檢查，則丟棄封包）啟用的設定丟棄的封包數。
通道片段 (tunnel_fragment)	防火牆由於分割錯誤而丟棄的封包數。
建立的工作階段數 (sessions_created)	所建立的內部工作階段數。
關閉的工作階段數 (sessions_closed)	已完成/已關閉的工作階段數。
工作階段結束原因 (session_end_reason)	工作階段終止的原因。若有多個終止原因，此欄位只會顯示最高優先順序的原因。以下按優先順序的順序 (第一個最高) 顯示可能的工作階段結束原因值： • threat—防火牆偵測到與重設、丟棄或封鎖 (IP 位址) 動作相關聯的威脅。 • policy-deny—工作階段符合包含拒絕或丟棄動作的安全性規則。 • decrypt-cert-validation—當工作階段使用用戶端驗證或當工作階段使用任何條件（已到期、不受信任的發行者、未知狀態或狀態驗證逾時）的伺服器憑證時，工作階段會因將防火牆設定為封鎖 SSL 轉送代理程式解密或 SSL 輸入檢查 而終止。伺服器憑證產生以下類型的嚴重錯誤警示時也會顯示此工作階段的結束原因：bad_certificate、unsupported_certificate、certificate_revoked、access_denied 或 no_certificate_RESERVED（僅限 SSLv3）。 • decrypt-unsupport-param—當工作階段使用不支援的通訊協定版本、加密或 SSH 演算法時，此工作階段會因將防火牆設定為封鎖 SSL 轉送代理程式解密或 SSL 輸入檢查時而終止。工作階段產生 unsupported_extension、unexpected_message 或 handshake_failure 類型的嚴重錯誤警示時，會顯示此工作階段結束原因。 • decrypt-error—當防火牆資源或硬體安全性模組 (HSM) 不可用時，此工作階段會因將防火牆設定為封鎖 SSL 轉送代理程式解密或 SSL 輸入檢查而終止。當將防火牆設定為封鎖發生 SSH 錯誤或產生嚴重錯誤警示（為 decrypt-cert-validation 和 decrypt-unsupport-param 結束

©2024 Palo Alto Networks, Inc.

欄位名稱	說明

	原因所列之警示以外）的 SSL 流量時，也會顯示此工作階段結束原因。
	• tcp-rst-from-client—用戶端將 TCP 重設傳送至伺服器。
	• tcp-rst-from-server—伺服器將 TCP 重設傳送至用戶端。
	• resources-unavailable—因系統資源限制而丟棄工作階段。例如，工作階段可能已超出每個流程所允許的順序紊亂封包數，或全域順序紊亂封包佇列。
	• tcp-fin—連線中的一部或兩部主機會傳送 TCP FIN 訊息來關閉工作階段。
	• tcp-reuse—工作階段重複使用，且防火牆關閉先前的工作階段。
	• decoder—解碼器偵測到通訊協定中的新連線 (例如 HTTP-Proxy) 並結束先前的連線。
	• aged-out—工作階段已逾期。
	• unknown—此值適用於下列情況：
	  • 上述原因未涵蓋的工作階段結束狀況 (例如，`clear session all` 命令)。
	  • 比 PAN-OS 6.1 版更舊的版本不支援工作階段結束原因欄位，以這些版本產生的日誌在升級至 PAN-OS 目前版本後或在將日誌載入到防火牆後，此值將為 `unknown`。
	  • 在 Panorama 中，從防火牆中針對不支援工作階段結束原因的 PAN-OS 版本所接收的日誌將具有值 `unknown`。
	• n/a—此值適用於流量日誌類型不是 **end** 時。

動作來源 (action_source)	指定是否要針對已在應用程式或原則中定義的應用程式，採取允許或封鎖動作。動作包含針對工作階段允許、拒絕、丟棄、重設伺服器、重設用戶端或重設兩者。
開始時間 (start)	工作階段開始的年/月/日 時：分：秒。
經過時間 (elapsed)	工作階段經過的時間。
通道檢查規則 (tunnel_insp_rule)	與純文字通道流量相符的通道檢查規則的名稱。
遠端使用者 IP (remote_user_ip)	遠端使用者的 IPv4 或 IPv6 位址。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
遠端使用者 ID (remote_user_id)	遠端使用者的 IMSI 識別碼以及一個 IMEI 識別碼或一個 MSISDN 識別碼（如有）。
安全性規則 UUID (rule_uuid)	永久識別規則的 UUID。
PCAP ID (pcap_id)	定義防火牆上的 pcap 檔案的位置之唯一封包擷取 ID。
動態使用者群組名稱 (dynusergroup_name)	包含啟動工作階段的使用者的動態使用者群組名稱。
來源外部動態清單 (src_edl)	包含流量來源 IP 位址的外部動態清單的名稱。
目的地外部動態清單 (dst_edl)	包含流量目的地 IP 位址的外部動態清單的名稱。
高解析度時間戳記 (high_res timestamp)	在管理平面接收日誌的時間（毫秒）。 此新欄位的格式為 YYYY-MM-DDThh:ss:sssTZD： • **YYYY**—四位數表示年份 • **MM**—二位數表示月份 • **DD**—二位數表示當月的日期（01 到 31） • **T**—時間戳記開始的指標 • **hh**—兩位數表示小時（使用 24 小時制，00 到 23） • **mm**—兩位數表示分鐘（00 到 59） • **ss**—兩位數表示秒鐘（00 到 60） • **sss**—一位或多位數表示毫秒 • **TZD**—時區指示項（+hh:mm 或 -hh:mm） 對於從執行 *PAN-OS 11.0* 和更新版本的受管理防火牆接收的日誌，支援高解析度時間戳記。從執行 *PAN-OS 9.1* 及早前版本的防火牆接收的日誌顯示 *`1969-12-31T16:00:00:000-8:00`* 時間戳記，而不論接收日誌的時間如何。
A 切片差分器 (nssai_sd)	網路切片 ID 的 A 切片差分器。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
A 切片服務類型 (nssai_sd)	網路切片 ID 的 A 切片服務類型。
PDU 工作階段 ID (pdu_session_id)	通道內 L4 區段集合的工作階段 ID。
應用程式子類別 (subcategory_of_app)	應用程式設定屬性中指定的應用程式子類別。
應用程式類別 (category_of_app)	應用程式設定屬性中指定的應用程式類別。值為： • 業務系統 • 協同作業 • 一般網際網路 • 媒體 • 網路 • saas
應用程式技術 (technology_of_app)	應用程式設定屬性中指定的應用程式技術。值為： • browser-based • client-server • network-protocol • peer-to-peer
應用程式風險 (risk_of_app)	與應用程式關聯的風險層級（1 = 最低，5 = 最高）。
應用程式特性 (characteristic_of_app)	應用程式適用特性的逗號分隔清單
應用程式容器 (container_of_app)	應用程式的父應用程式。
應用程式 SaaS (is_saas_of_app)	如果是 SaaS 應用程式，則顯示 `1` ，如果不是 SaaS 應用程式，則顯示 `0`。
應用程式認可狀態 (sanctioned_state_of_app)	如果應用程式受認可，則顯示 `1`，如果應用程式不受認可，則顯示 `0`。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
叢集名稱 (cluster_name)	CN-Series 防火牆叢集的名稱。

SCTP 日誌欄位

格式：FUTURE_USE、接收時間、序號、類型、FUTURE_USE、FUTURE_USE、產生時間、來源位址、目的地位址、FUTURE_USE、FUTURE_USE、規則名稱、FUTURE_USE、FUTURE_USE、FUTURE_USE、虛擬系統、來源區域、目的地區域、輸入介面、輸出介面、日誌動作、FUTURE_USE、工作階段 ID、重複計數、來源連接埠、目的地連接埠、FUTURE_USE、FUTURE_USE、FUTURE_USE、FUTURE_USE、IP 通訊協定、動作、裝置群組階層 1、裝置群組階層 2、裝置群組階層 3、裝置群組階層 4、虛擬系統名稱、裝置名稱、序號、FUTURE_USE、SCTP 關聯 ID、裝載通訊協定 ID、嚴重性、SCTP 區塊類型、FUTURE_USE、SCTP 驗證標籤 1、SCTP 驗證標籤 2、SCTP 原因代碼、直徑 App ID、直徑指令代碼、直徑 AVP 代碼、SCTP 串流 ID、SCTP 關聯結束原因、Op 代碼、SCCP 呼叫方 SSN、SCCP 呼叫方全域碼、SCTP 篩選器、SCTP 區塊、傳送的 SCTP 區塊、接收的 SCTP 區塊、封包數、傳送的封包數、接收的封包數、規則 UUID、高解析度時間戳記

欄位名稱	說明
接收時間（receive_time 或 cef-formatted-receive_time）	在管理平面接收日誌的時間。
序號 (serial)	產生日誌之防火牆的序號。
類型 (type)	指定日誌類型；值為 SCTP。
產生時間（time_generated 或 cef-formatted-time_generated）	在資料層上產生日誌的時間。
來源位址 (src)	原始工作階段來源 IP 位址。
目的地位址 (dst)	原始工作階段目的地 IP 位址。
規則名稱 (rule)	對工作階段使用的安全性原則規則名稱。
虛擬系統 (vsys)	與工作階段相關聯的虛擬系統。
來源區域 (from)	工作階段的來源區域。
目的地區域 (to)	將工作階段指定至的區域。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
輸入介面 (inbound_if)	工作階段的來源介面。
輸出介面 (outbound_if)	將工作階段指定至的介面。
日誌動作 (logset)	套用至工作階段的日誌轉送設定檔。
工作階段 ID (sessionid)	套用至每個工作階段的內部數字識別碼。
重複計數 (repeatcnt)	在 5 秒鐘內看到的有相同來源 IP、目的地 IP、應用程式與子類型的工作階段數。
來源連接埠 (sport)	工作階段使用的來源連接埠。
目的地連接埠 (dport)	工作階段使用的目的地連接埠。
IP 通訊協定 (proto)	與工作階段相關聯的 IP 通訊協定。
動作 (action)	針對工作階段採取的動作；可能的值為： • 允許—原則已允許工作階段 • 拒絕—原則已拒絕工作階段
設備群組階層（dg_hier_level_1 到 dg_hier_level_4）	一系列的識別號碼，可表示設備群組在設備群組階層中的位置。產生日誌的防火牆（或虛擬系統）會在裝置群組階層中包含每個上階項目的識別號碼。此結構不包含共用設備群組（層級 0）。 如果日誌值為 12、34、45 或 0，這表示該日誌是由屬於裝置群組 45 且其上階項目為 34 和 12 的防火牆（或虛擬系統）所產生。若要檢視對應至值 12、34 或 45 的設備群組名稱，請使用下列其中一個方法： API 查詢： `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
虛擬系統名稱 (vsys_name)	與工作階段相關聯的虛擬系統名稱；只在已針對多個虛擬系統啟用的防火牆上有效。
設備名稱 (device_name)	已記錄工作階段的防火牆主機名稱。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
序號 (seqno)	依序遞增的 64 位元日誌項目識別碼；每個日誌類型有一個唯一編號空間。
SCTP 關聯 ID (assoc_id)	套用至各 SCTP 關聯的內部 56 位元數字邏輯識別碼。
裝載通訊協定 ID (ppid)	識別已觸發此事件的資料區塊中的裝載通訊協定 ID (PPID)。PPID 由 Internet Assigned Numbers Authority (IANA) 指派。
嚴重性 (severity)	與事件相關聯的嚴重性；值有資訊、低、中、高、重要。
SCTP 區塊類型 (sctp_chunk_type)	描述區塊中包含的資訊類型，例如控制或資料。
SCTP 事件類型 (sctp_event_type)	定義將 SCTP 保護設定檔套用至 SCTP 流量時各 SCTP 區塊或封包觸發的事件。此外，它還由 SCTP 關聯之開始或結束而觸發。
SCTP 驗證標籤 1 (verif_tag_1)	由端點 1 使用，啟動關聯以驗證接收的 SCTP 封包是否屬於目前的 SCTP 關聯，並驗證端點 2。
SCTP 驗證標籤 2 (verif_tag_2)	由端點 2 使用，驗證接收的 SCTP 封包是否屬於目前的 SCTP 關聯，並驗證端點 1。
SCTP 原因代碼 (sctp_cause_code)	由端點傳送至同一 SCTP 關聯的其他端點，指定錯誤狀態的原因。
直徑 App ID (diam_app_id)	觸發事件的資料區塊中的直徑應用程式。直徑應用程式 ID 由 Internet Assigned Numbers Authority (IANA) 指派。
直徑指令代碼 (diam_cmd_code)	觸發事件的資料區塊中的直徑指令代碼。直徑指令代碼由 Internet Assigned Numbers Authority (IANA) 指派
直徑 AVP 代碼 (diam_avp_code)	觸發事件的資料區塊中的直徑 AVP 代碼。
SCTP 串流 ID (stream_id)	攜帶觸發事件的資料區塊之串流的 ID。
SCTP 關聯結束原因 (assoc_end_reason)	對關聯終止進行分析。如果終止因多個原因而引起，則會顯示優先順序最高的原因。可能的工作階段結束原因（優先順序呈遞減方式）包括： • shutdown-from-endpoint（最高）—端點傳送出 SHUTDOWN

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
	• abort-from-endpoint—端點傳送出 ABORT • 未知（最低）—關聯已過時，或者先前的原因未涵蓋關聯終止原因（例如，clear session all 命令）。
Op 代碼 (op_code)	識別觸發事件之資料區塊中應用程式層 SS7 通訊協定（例如 MAP 或 CAP）的作業碼。
SCCP 呼叫方 SSN (sccp_calling_ssn)	觸發事件之資料區塊中的信號連接控制部分 (SCCP) 呼叫方子系統編號 (SSN)。
SCCP 呼叫方全域碼 (sccp_calling_gt)	觸發事件之資料區塊中的信號連接控制部分 (SCCP) 呼叫方全域碼 (GT)。
SCTP 篩選器 (sctp_filter)	與 SCTP 區塊相符的篩選器名稱。
SCTP 區塊 (chunks)	關聯的區塊（傳輸與接收）總數。
傳送的 SCTP 區塊 (chunks_sent)	關聯的端點 1（啟動關聯）-至-端點 2 區塊的數目。
接收的 SCTP 區塊 (chunks_received)	關聯的端點 2-至-端點 1 區塊（啟動關聯）的數目。
封包數 (packets)	工作階段的封包（傳輸與接收）總數。
已傳送的封包數 (pkts_sent)	工作階段之用戶端至伺服器封包數。
已接收的封包 (pkts_received)	工作階段之伺服器至用戶端封包數。
規則 UUID (rule_uuid)	永久識別規則的 UUID。
高解析度時間戳記 (high_res_timestamp)	在管理平面接收日誌的時間（毫秒）。 此新欄位的格式為 YYYY-MM-DDThh:ss:sssTZD： • **YYYY**—四位數表示年份 • **MM**—二位數表示月份 • **DD**—二位數表示當月的日期（01 到 31） • **T**—時間戳記開始的指標 • **hh**—兩位數表示小時（使用 24 小時制，00 到 23） • **mm**—兩位數表示分鐘（00 到 59） • **ss**—兩位數表示秒鐘（00 到 60）

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
	• **sss**—一位或多位數表示毫秒 • **TZD**—時區指示項（+hh:mm 或 -hh:mm） 對於從執行 *PAN-OS 11.0* 和更新版本的受管理防火牆接收的日誌，支援高解析度時間戳記。從執行 *PAN-OS 9.1* 及早前版本的防火牆接收的日誌顯示 `1969-12-31T16:00:00:000-8:00` 時間戳記，而不論接收日誌的時間如何。

驗證日誌欄位

格式：FUTURE_USE、接收時間、序號、類型、威脅/內容類型、FUTURE_USE、產生時間、虛擬系統、來源 IP、使用者、標準化使用者、物件、驗證政策、重複計數、驗證 ID、廠商、日誌動作、伺服器設定檔、說明、用戶端類型、事件類型、因素號碼、序號、動作旗標、裝置群組階層 1、裝置群組階層 2、裝置群組階層 3、裝置群組階層 4、虛擬系統名稱、裝置名稱、虛擬系統 ID、驗證通訊協定、規則 UUID、高解析度時間戳記、來源裝置類別、來源裝置設定檔、來源裝置型號、來源裝置廠商、來源裝置作業系統系列、來源裝置作業系統版本、來源主機名稱、來源 Mac 位址、區域、FUTURE_USE、使用者代理程式、工作階段 ID、叢集名稱

欄位名稱	說明
接收時間（receive_time 或 cef-formatted-receive_time）	在管理平面接收日誌的時間。
序號 (serial)	產生日誌之裝置的序號。
類型 (type)	指定日誌類型；值為 AUTHENTICATION。
威脅/內容類型 (subtype)	系統日誌的子類型，是指產生日誌的系統精靈；值包括 crypto、dhcp、dnsproxy、dos、general、global-protect、ha、hw、nat、ntpd、pbf、port、pppoe、ras、routing、satd、sslmgr、sslvpn、filtering、vpn。
產生時間（time_generated 或 cef-formatted-time_generated）	在資料層上產生日誌的時間。
虛擬系統 (vsys)	與工作階段相關聯的虛擬系統。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
來源 IP (ip)	原始工作階段來源 IP 位址。
使用者 (user)	被驗證的使用者。
標準化使用者 (normalize_user)	被驗證的使用者名稱的標準化版本（例如在使用者名稱中附加網域名稱）。
物件 (object)	與系統事件關聯之物件的名稱。
驗證原則 (authpolicy)	在允許存取受保護資源之前，為進行驗證而叫用的原則。
重複計數 (repeatcnt)	在 5 秒鐘內看到的有相同來源 IP、目的地 IP、應用程式與子類型的工作階段數。
驗證 ID (authid)	在主要驗證和額外（多因素）驗證中指定的唯一 ID。
廠商 (vendor)	提供額外因素驗證的廠商。
日誌動作 (logset)	套用至工作階段的日誌轉送設定檔。
伺服器設定檔 (serverprofile)	驗證時使用的驗證伺服器。
描述 (desc)	其他驗證資訊。
用戶端類型 (clienttype)	用於完成驗證的用戶端類型（例如驗證入口網站）。
事件類型 (event)	驗證結果。
因素號碼 (factorno)	指示是使用主要驗證 (1) 還是額外驗證（2、3）。
序號 (seqno)	依序遞增的 64 位元日誌項目識別碼。每個日誌類型有一個唯一編號空間。
動作旗標 (actionflags)	指示是否將日誌轉送至 Panorama 的位元欄位。
設備群組階層（dg_hier_level_1 到 dg_hier_level_4）	一系列的識別號碼，可表示設備群組在設備群組階層中的位置。產生日誌的防火牆（或虛擬系統）會在裝置群組階層中包含每個上階項目的識別號碼。此結構不包含共用設備群組（層級 0）。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
	如果日誌值為 12、34、45 或 0，這表示該日誌是由屬於裝置群組 45 且其上階項目為 34 和 12 的防火牆（或虛擬系統）所產生。若要檢視對應至值 12、34 或 45 的設備群組名稱，請使用下列其中一個方法： API 查詢： `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
虛擬系統名稱 (vsys_name)	與工作階段相關聯的虛擬系統名稱；只在已針對多個虛擬系統啟用的防火牆上有效。
設備名稱 (device_name)	已記錄工作階段的防火牆主機名稱。
虛擬系統 ID (vsys_id)	虛擬系統在 Palo Alto Networks 防火牆上的唯一識別碼。
驗證通訊協定 (authproto)	表明伺服器所使用的驗證通訊協定。例如，採用 GTC 的 PEAP。
規則 UUID (rule_uuid)	永久識別規則的 UUID。
高解析度時間戳記 (high_res _timestamp)	在管理平面接收日誌的時間（毫秒）。 此新欄位的格式為 YYYY-MM-DDThh:ss:sssTZD： • **YYYY**—四位數表示年份 • **MM**—二位數表示月份 • **DD**—二位數表示當月的日期（01 到 31） • **T**—時間戳記開始的指標 • **hh**—兩位數表示小時（使用 24 小時制，00 到 23） • **mm**—兩位數表示分鐘（00 到 59） • **ss**—兩位數表示秒鐘（00 到 60） • **sss**—一位或多位數表示毫秒 • **TZD**—時區指示項（+hh:mm 或 -hh:mm） 對於從執行 *PAN-OS 11.0* 和更新版本的受管理防火牆接收的日誌，支援高解析度時間戳記。從執行 *PAN-OS 9.1* 及早前版本的防火牆接收的日誌顯示 *1969-12-31T16:00:00.000-8:00* 時間戳記，而不論接收日誌的時間如何。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
來源裝置類別 (src_category)	Device-ID 識別為流量來源的裝置的類別。
來源裝置設定檔 (src_profile)	Device-ID 識別為流量來源的裝置的裝置設定檔。
來源裝置型號 (src_model)	Device-ID 識別為流量來源的裝置的型號。
來源裝置廠商 (src_vendor)	Device-ID 識別為流量來源的裝置的廠商。
來源裝置作業系統系列 (src_osfamily)	Device-ID 識別為流量來源的裝置的作業系統類型。
來源裝置作業系統版本 (src_osversion)	Device-ID 識別為流量來源的裝置的作業系統版本。
來源主機名稱 (src_host)	Device-ID 識別為流量來源的裝置的主機名稱。
來源 MAC 位址 (src_mac)	Device-ID 識別為流量來源的裝置的 MAC 位址。
區域 (region)	流量來源地理區域。
使用者代理程式 (user_agent)	來自 HTTP 要求標頭 `User-Agent` 的字串。
工作階段 ID (sessionid)	唯一識別流量工作階段的字串。
叢集名稱 (cluster_name)	CN-Series 防火牆叢集的名稱。

組態日誌欄位

格式：FUTURE_USE、接收時間、序號、類型、子類型、FUTURE_USE、產生時間、主機、虛擬系統、命令、管理員、用戶端、結果、設定路徑、變更前詳細資料、變更後詳細資料、序號、動作旗標、裝置群組階層 1、裝置群組階層 2、裝置群組階層 3、裝置群組階層 4、虛擬系統名稱、裝置名稱、裝置群組、稽核註解、FUTURE_USE、高解析度時間戳記

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
接收時間（receive_time 或 cef-formatted-receive_time）	在管理平面接收日誌的時間。
序號 (serial)	產生日誌之裝置的序號。
類型 (type)	指定日誌類型；值為 CONFIG。
威脅/內容類型 (subtype)	組態日誌的子類型；未使用。
產生時間（time_generated 或 cef-formatted-time_generated）	在資料層上產生日誌的時間。
主機 (host)	用戶端電腦的主機名稱或 IP 位址
虛擬系統 (vsys)	與組態日誌相關聯的虛擬系統
命令 (cmd)	管理員所執行的命令；值有 add、clone、commit、delete、edit、move、rename、set。
管理員 (admin)	執行設定之管理員的使用者名稱
用戶端 (client)	管理員所使用的用戶端；值有 Web 與 CLI
結果 (result)	組態動作的結果，值有 (已提交)、(已成功)、(已失敗) 及 (未經授權)
設定路徑 (path)	簽發組態命令的路徑，長度最多 512 個位元組
變更前詳細資料 (before-change-detail)	此欄位僅在自訂日誌中；未採用預設的格式。 其包含組態變更前的完整 xpath。
變更後詳細資料 (after-change-detail)	此欄位僅在自訂日誌中；未採用預設的格式。 其包含組態變更後的完整 xpath。
序號 (seqno)	依序遞增的 64 位元日誌項目識別碼；每個日誌類型有一個唯一編號空間。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
動作旗標 (actionflags)	指示是否將日誌轉送至 Panorama 的位元欄位。
設備群組階層（dg_hier_level_1 到 dg_hier_level_4）	一系列的識別號碼，可表示設備群組在設備群組階層中的位置。產生日誌的防火牆（或虛擬系統）會在裝置群組階層中包含每個上階項目的識別號碼。此結構不包含共用設備群組（層級 0）。 如果日誌值為 12、34、45 或 0，這表示該日誌是由屬於裝置群組 45 且其上階項目為 34 和 12 的防火牆（或虛擬系統）所產生。若要檢視對應至值 12、34 或 45 的設備群組名稱，請使用下列其中一個方法： API 查詢： `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
虛擬系統名稱 (vsys_name)	與工作階段相關聯的虛擬系統名稱；只在已針對多個虛擬系統啟用的防火牆上有效。
設備名稱 (device_name)	已記錄工作階段的防火牆主機名稱。
裝置群組 (dg_id)	防火牆所屬的裝置群組（如果由 Panorama™ 管理伺服器進行管理）。
稽核註解 (comment)	原則規則設定變更中輸入的稽核註解。
高解析度時間戳記 (high_res _timestamp)	在管理平面接收日誌的時間（毫秒）。 此新欄位的格式為 YYYY-MM-DDThh:ss:sssTZD： • **YYYY**—四位數表示年份 • **MM**—二位數表示月份 • **DD**—二位數表示當月的日期（01 到 31） • **T**—時間戳記開始的指標 • **hh**—兩位數表示小時（使用 24 小時制，00 到 23） • **mm**—兩位數表示分鐘（00 到 59） • **ss**—兩位數表示秒鐘（00 到 60） • **sss**—一位或多位數表示毫秒 • **TZD**—時區指示項（+hh:mm 或 -hh:mm）

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
	對於從執行 *PAN-OS 10.0* 和後續版本的受管理防火牆接收的日誌，支援高解析度時間戳記。從執行 *PAN-OS 9.1* 及早前版本的防火牆接收的日誌顯示 `1969-12-31T16:00:00:000-8:00` 時間戳記，而不論接收日誌的時間如何。

系統日誌欄位

格式：FUTURE_USE、接收時間、序號、類型、內容/威脅類型、FUTURE_USE、產生時間、虛擬系統、事件 ID、物件、FUTURE_USE、FUTURE_USE、模組、嚴重性、描述、序號、動作旗標、裝置群組階層 1、裝置群組階層 2、裝置群組階層 3、裝置群組階層 4、虛擬系統名稱、裝置名稱、FUTURE_USE、FUTURE_USE、高解析度時間戳記

欄位名稱	說明
接收時間（receive_time 或 cef-formatted-receive_time）	在管理平面接收日誌的時間。
序號 (serial)	產生日誌之防火牆的序號。
類型 (type)	指定日誌類型；值為 SYSTEM。
內容/威脅類型 (subtype)	系統日誌的子類型，是指產生日誌的系統精靈；值包括 crypto、dhcp、dnsproxy、dos、general、global-protect、ha、hw、nat、ntpd、pbf、port、pppoe、ras、routing、satd、sslmgr、sslvpn、filtering、vpn。
產生時間（time_generated 或 cef-formatted-time_generated）	在資料層上產生日誌的時間。
虛擬系統 (vsys)	與組態日誌相關聯的虛擬系統。
事件 ID (eventid)	顯示事件名稱的字串。
物件 (object)	與系統事件關聯之物件的名稱。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
模組 (module)	只有在子類型欄位值為 general 時，此欄位才有效。 它會提供子系統產生日誌的其他相關資訊；值有 general、management、auth、ha、upgrade、chassis。
嚴重性 (severity)	與事件相關聯的嚴重性；值有資訊、低、中、高、重要。
說明 (opaque)	事件的詳細說明，最多 512 個位元組。
序號 (seqno)	依序遞增的 64 位元日誌項目識別碼；每個日誌類型有一個唯一編號空間。
動作旗標 (actionflags)	指示是否將日誌轉送至 Panorama 的位元欄位。
設備群組階層（dg_hier_level_1 到 dg_hier_level_4）	一系列的識別號碼，可表示設備群組在設備群組階層中的位置。產生日誌的防火牆（或虛擬系統）會在裝置群組階層中包含每個上階項目的識別號碼。此結構不包含共用設備群組（層級 0）。 如果日誌值為 12、34、45 或 0，這表示該日誌是由屬於裝置群組 45 且其上階項目為 34 和 12 的防火牆（或虛擬系統）所產生。若要檢視對應至值 12、34 或 45 的設備群組名稱，請使用下列其中一個方法： API 查詢： `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
虛擬系統名稱 (vsys_name)	與工作階段相關聯的虛擬系統名稱；只在已針對多個虛擬系統啟用的防火牆上有效。
設備名稱 (device_name)	已記錄工作階段的防火牆主機名稱。
高解析度時間戳記 (high_res _timestamp)	在管理平面接收日誌的時間（毫秒）。 此新欄位的格式為 YYYY-MM-DDThh:ss:sssTZD： • **YYYY**—四位數表示年份 • **MM**—二位數表示月份 • **DD**—二位數表示當月的日期（01 到 31） • **T**—時間戳記開始的指標 • **hh**—兩位數表示小時（使用 24 小時制，00 到 23） • **mm**—兩位數表示分鐘（00 到 59）

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
	• **ss**—兩位數表示秒鐘（00 到 60） • **sss**——一位或多位數表示毫秒 • **TZD**—時區指示項（+hh:mm 或 -hh:mm） 對於從執行 *PAN-OS 11.0* 和更新版本的受管理防火牆接收的日誌，支援高解析度時間戳記。從執行 *PAN-OS 9.1* 及早前版本的防火牆接收的日誌顯示 *1969-12-31T16:00:00.000-8:00* 時間戳記，而不論接收日誌的時間如何。

關聯的事件日誌欄位

格式：FUTURE_USE、接收時間、序號、類型、內容/威脅類型、FUTURE_USE、產生時間、來源位址。來源使用者、虛擬系統、類別、嚴重性、裝置群組階層 1、裝置群組階層 2、裝置群組階層 3、裝置群組階層 4、虛擬系統名稱、裝置名稱、虛擬系統 ID、物件名稱、物件 ID、辨識項

欄位名稱	說明
接收時間（receive_time 或 cef-formatted-receive_time）	在管理平面接收日誌的時間。
序號 (serial)	產生日誌之裝置的序號。
類型 (type)	指定日誌類型；值為 CORRELATION。
內容/威脅類型 (subtype)	系統日誌的子類型，是指產生日誌的系統精靈；值包括 crypto、dhcp、dnsproxy、dos、general、global-protect、ha、hw、nat、ntpd、pbf、port、pppoe、ras、routing、satd、sslmgr、sslvpn、filtering、vpn。
產生時間（time_generated 或 cef-formatted-time_generated）	在資料層上產生日誌的時間。
來源位址 (src)	啟動事件之使用者的 IP 位址。
來源使用者 (srcuser)	啟動事件之使用者的使用者名稱。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
虛擬系統 (vsys)	與組態日誌相關聯的虛擬系統。
類別 (category)	網路、使用者或主機所受威脅或傷害類型的摘要。
嚴重性 (severity)	與事件相關聯的嚴重性；值有資訊、低、中、高、重要。
設備群組階層（dg_hier_level_1 到 dg_hier_level_4）	一系列的識別號碼，可表示設備群組在設備群組階層中的位置。產生日誌的防火牆（或虛擬系統）會在裝置群組階層中包含每個上階項目的識別號碼。此結構不包含共用設備群組（層級 0）。 如果日誌值為 12、34、45 或 0，這表示該日誌是由屬於裝置群組 45 且其上階項目為 34 和 12 的防火牆（或虛擬系統）所產生。若要檢視對應至值 12、34 或 45 的設備群組名稱，請使用下列其中一個方法： API 查詢： `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
虛擬系統名稱 (vsys_name)	與工作階段相關聯的虛擬系統名稱；只在已針對多個虛擬系統啟用的防火牆上有效。
設備名稱 (device_name)	已記錄工作階段的防火牆主機名稱。
虛擬系統 ID (vsys_id)	虛擬系統在 Palo Alto Networks 防火牆上的唯一識別碼。
物件名稱 (objectname)	比對的關聯物件名稱。
物件 ID (object_id)	與系統事件關聯之物件的名稱。
證據 (evidence)	表示主機根據關聯物件中定義的條件比對的次數的概述。例如，主機造訪已知惡意軟體 URl（19 次）。

GTP 日誌欄位

格式：FUTURE_USE、接收時間、序號、類型、威脅/內容類型、FUTURE_USE、產生時間、來源位址、目的地位址、FUTURE_USE、FUTURE_USE、規則名稱、FUTURE_USE、FUTURE_USE、應用程式、虛擬系統、來源區域、目的地區域、輸入介面、輸出介面、日誌動作、FUTURE_USE、工作階段 ID、FUTURE_USE、來源連接埠、目的地連接埠、FUTURE_USE、FUTURE_USE、FUTURE_USE、通訊協定、動作、GTP 事件類型、MSISDN、存取點名稱、無線存取技術、GTP 訊息類型、一般使用者 IP 位址、通道端點識別碼 1、通道端點識別碼 2、GTP 介面、GTP 原因、嚴重性、伺服國家 MCC、伺服網路 MNC、

©2024 Palo Alto Networks, Inc.

區域代碼、基站 ID、GTP 事件代碼、FUTURE_USE、FUTURE_USE、來源位置、目的地位置、FUTURE_USE、FUTURE_USE、FUTURE_USE、FUTURE_USE、FUTURE_USE、FUTURE_USE、FUTU
通道 ID/IMSI、監控標籤/
IMEI、FUTURE_USE、FUTURE_USE、FUTURE_USE、FUTURE_USE、FUTURE_USE、FUTURE_USE、FU
開始時間、經過時間、通道檢查規則、遠端使用者 IP、遠端使用者 ID、規則 UUID、PCAP ID、高解析度時間戳記、A 切片服務類型、A 切片差分器、應用程式子類別、應用程式類別、應用程式技術、應用程式風險、應用程式特性、應用程式容器、應用程式 SaaS、應用程式認可狀態

欄位名稱	說明
接收時間（receive_time 或 cef-formatted-receive_time）	在管理平面接收日誌的月份、日期和時間。
序號 (serial)	產生日誌之防火牆的序號。
類型 (type)	指定日誌類型；值為 GTP。
威脅/內容類型 (subtype)	流量日誌的子類型；值有開始、結束、丟棄與拒絕 • 開始—開始的工作階段 • 結束—結束的工作階段 • 丟棄—識別應用程式前丟棄的工作階段，且沒有允許工作階段的規則。 • 拒絕—識別應用程式後丟棄的工作階段，且有要封鎖的規則或沒有允許工作階段的規則。
產生時間（time_generated 或 cef-formatted-time_generated）	在資料層上產生日誌的時間。
來源位址 (src)	工作階段中封包的來源 IP 位址。
目的地位址 (dst)	工作階段中封包的目的地 IP 位址。
規則名稱 (rule)	對工作階段使用的安全性原則規則名稱。
應用程式 (app)	工作階段中使用的通道通訊協定。
虛擬系統 (vsys)	與工作階段相關聯的虛擬系統。
來源區域 (from)	工作階段中封包的來源區域。
目的地區域 (to)	工作階段中封包的目的地區域。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
輸入介面 (inbound_if)	工作階段的來源介面。
輸出介面 (outbound_if)	將工作階段指定至的介面。
日誌動作 (logset)	套用至工作階段的日誌轉送設定檔。
工作階段 ID (sessionid)	所記錄之工作階段的 ID。
來源連接埠 (sport)	工作階段使用的來源連接埠。
目的地連接埠 (dport)	工作階段使用的目的地連接埠。
IP 通訊協定 (proto)	與工作階段相關聯的 IP 通訊協定。
動作 (action)	針對工作階段採取的動作；可能的值為： • 允許—原則已允許工作階段 • 拒絕—原則已拒絕工作階段
GTP 事件類型 (event_type)	定義將 GTP 保護設定檔中的檢查套用至 GTP 流量時 GTP 訊息所觸發的事件。開始或結束 GTP 工作階段時也會觸發。
MSISDN (msisdn)	與行動用戶關聯的服務身份識別號碼，由國家/地區代碼、國家目的地代碼及訂閱者號碼構成。由十進位數字 (0-9) 組成，最多 15 位。
存取點名稱 (apn)	參考行動網路中的封包資料網路資料閘道 (PGW)/ 閘道 GPRS 支援節點。由強制 APN 網路識別碼和可選 APN 營運商識別碼構成。
無線存取技術 (rat)	用於無線存取的技術類型。例如 EUTRAN、WLAN、Virtual、HSPA Evolution、GAN 和 GERAN。
GTP 訊息類型 (msg_type)	指示 GTP 訊息的類型。
終端 IP 位址 (end_ip_adr)	PGW/GGSN 分配的行動用戶 IP 位址。
通道端點識別碼 1 (teid1)	用於識別網路節點中的 GTP 通道。TEID1 是 GTP 訊息中的第一個 TEID。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
通道端點識別碼 2 (teid2)	用於識別網路節點中的 GTP 通道。TEID2 是 GTP 訊息中的第二個 TEID。
GTP 介面 (gtp_interface)	從其接收 GTP 訊息的 3GPP 介面。
GTP 原因 (cause_code)	日誌回應（其中包含了資訊元素，提供了關於網路節點接受或拒絕 GTP 要求的資訊）中的 GTP 原因值。
嚴重性 (severity)	與事件相關聯的嚴重性；值有資訊、低、中、高、重要。
伺服網路 MCC (mcc)	提供核心網路的營運商的行動業務國家/地區代碼。
伺服網路 MNC (mnc)	提供核心網路的營運商的行動網路代碼。
區域代碼 (area_code)	公眾行動電話網路 (PLMN) 中的區域。
Cell ID (cell_id)	區域內的基站代碼。
GTP 事件代碼 (event_code)	描述 GTP 事件的事件代碼。
來源位置 (srcloc)	私人位址的來源國家/地區或內部地區；最大長度為 32 位元組。
目的地位置 (dstloc)	私人位址的目的地國家/地區或內部地區；最大長度為 32 位元組。
通道 ID/IMSI (imsi)	國際行動用戶識別 (IMSI) 是為 GSM/UMTS/EPS 系統內每個行動用戶分配的唯一號碼。IMSI 必須僅由十進位數字 (0-9) 組成，允許的最大位數為 15 位。
監控標籤/IMEI (imei)	國際行動裝置識別 (IMEI) 是為每個行動站裝置分配的唯一 15 或 16 位號碼。
開始時間 (start)	工作階段開始的時間。
經過時間 (elapsed)	工作階段經過的時間。
通道檢查規則 (tunnel_insp_rule)	與純文字通道流量相符的通道檢查規則的名稱
遠端使用者 IP (remote_user_ip)	遠端使用者所使用的 IPv4 或 IPv6 位址。

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
遠端使用者 ID (remote_user_id)	遠端使用者的 IMSI 識別碼，如果有，則為一個 IMEI 識別碼和/或一個 MSISDN 識別碼。
規則 UUID (rule_uuid)	規則的通用唯一 ID。
PCAP ID (pcap_id)	唯一的封包擷取 ID，用於尋找防火牆上儲存的 pcap 檔案。
高解析度時間戳記 (high_res_timestamp)	在管理平面接收日誌的時間（毫秒）。 此新欄位的格式為 YYYY-MM-DDThh:ss:sssTZD： • **YYYY**—四位數表示年份 • **MM**—二位數表示月份 • **DD**—二位數表示當月的日期（01 到 31） • **T**—時間戳記開始的指標 • **hh**—兩位數表示小時（使用 24 小時制，00 到 23） • **mm**—兩位數表示分鐘（00 到 59） • **ss**—兩位數表示秒鐘（00 到 60） • **sss**—一位或多位數表示毫秒 • **TZD**—時區指示項（+hh:mm 或 -hh:mm） 對於從執行 *PAN-OS 11.0* 和更新版本的受管理防火牆接收的日誌，支援高解析度時間戳記。從執行 *PAN-OS 9.1* 及早前版本的防火牆接收的日誌顯示 `1969-12-31T16:00:00:000-8:00` 時間戳記，而不論接收日誌的時間如何。
A 切片服務類型 (nsdsai_sst)	網路切片 ID 的 A 切片服務類型。
A 切片差分器 (nsdsai_sd)	網路切片 ID 的 A 切片差分器。
應用程式子類別 (subcategory_of_app)	應用程式設定屬性中指定的應用程式子類別。
應用程式類別 (category_of_app)	應用程式設定屬性中指定的應用程式類別。值為： • 業務系統 • 協同作業 • 一般網際網路 • 媒體

©2024 Palo Alto Networks, Inc.

欄位名稱	說明
	• 網路 • saas
應用程式技術 (technology_of_app)	應用程式設定屬性中指定的應用程式技術。值為： • browser-based • client-server • network-protocol • peer-to-peer
應用程式風險 (risk_of_app)	與應用程式關聯的風險層級（1 = 最低，5 = 最高）。
應用程式特性 (characteristic_of_app)	應用程式適用特性的逗號分隔清單
應用程式容器 (container_of_app)	應用程式的父應用程式。
應用程式 SaaS (is_saas_of_app)	如果是 SaaS 應用程式，則顯示 `1` ，如果不是 SaaS 應用程式，則顯示 `0`。
應用程式認可狀態 (sanctioned_state_of_app)	如果應用程式受認可，則顯示 `1`，如果應用程式不受認可，則顯示 `0`。
應用程式子類別 (subcategory_of_app)	應用程式設定屬性中指定的應用程式子類別。

Syslog 嚴重性

syslog 嚴重性是根據日誌類型與內容所設定的。

日誌類型/嚴重性	Syslog 嚴重性
流量	資訊
設定	資訊
威脅/系統—資訊	資訊
威脅/系統—低	通知

©2024 Palo Alto Networks, Inc.

日誌類型/嚴重性	Syslog 嚴重性
威脅/系統—中	警告
威脅/系統—高	警告
威脅/系統—重要	嚴重

自訂日誌/事件格式

為了促進與外部日誌剖析系統整合，防火牆允許您自訂日誌格式，並允許您新增自訂的 *Key*：*Value* 屬性配對。自訂訊息格式可在 **Device**（裝置） > **Server Profiles**（伺服器設定檔） > **Syslog** > **Syslog Server Profile**（**Syslog** 伺服器設定檔） > **Custom Log Format**（自訂日誌格式） 下設定。

若要採用與 ArcSight 常見事件格式 (CEF) 相容的日誌格式，請參閱《常見組態指南》。

逸出順序

包含逗號或用雙引號括出雙引號的任何欄位。此外，如果雙引號出現在欄位內部，則可在其之前加上另一個雙引號將它逸出。若要保持回溯相容，一律以雙引號括出威脅日誌中的（雜項）欄位。

Syslog 嚴重性參考

按嚴重性分類的 syslog 訊息參考：

- 低嚴重性系統日誌訊息
- 告知性嚴重性系統日誌訊息
- 中等嚴重性系統日誌訊息
- 高嚴重性系統日誌訊息
- 嚴重嚴重性系統日誌訊息

告知性系統日誌訊息

電子日誌

日誌標籤：

- audit
- auth
- bfd
- clusterd
- ddns
- debug

 ©2024 Palo Alto Networks, Inc.

- dhcp
- dns-security
- dnsproxy
- dynamic-updates
- fips
- general
- hw
- ipv6nd
- lacp
- lldp
- monitoring
- nat
- ntpd
- panorama-check
- pbf
- port
- pppoe
- ras
- resctrl
- routing
- satd
- sched-push
- sdwan
- ssh
- sslmgr
- syslog
- tls
- url-filtering
- userid
- vm
- vpn
- wildfire
- wildfire-appliance

 ©2024 Palo Alto Networks, Inc.

audit

事件 ID	說明
api	<cmd>
cli	<cmd>
cli	<config command>
api	<config command>
gnmi	<config command>
gui-op	<config command>

auth

事件 ID	說明
cas-message	（設定檔 id：<id>）<message>
auth-fail	時鐘與位於「<name>」的 KDC 伺服器上的時鐘不匹配（代碼：<id>）
auth-fail	KDC 伺服器「<name>」上不存在使用者「<name>」（代碼：<id>）
auth-fail	錯誤的領域：「<name>」（代碼：<id>）
auth-fail	使用者名稱和密碼不匹配，預驗證失敗（代碼：<id>）
	Kerberos 錯誤：<error>（代碼：<id>）
auth-fail	驗證使用者「<name>」時，krb5_verify_init_creds() 偵測到 KDC 詐騙攻擊（krb5 錯誤代碼：<id>）
auth-success	管理員 <name> 帳戶已復還 - 鎖定計時器已過期。
user-password-change-success	驗證使用者「<name>」<remotehost> 時，使用了一種不太安全的驗證方法 <proto>。請移轉到 PEAP 或 EAP-TTLS。驗證設定檔

©2024 Palo Alto Networks, Inc.

事件 ID	說明
	「<name>」，vsys「<name>」，伺服器設定檔「<name>」，伺服器位址「<ip>」
auth-fail	使用者「<name>」的憑證驗證失敗。<error>
auth-success	已為使用者「<user>」驗證憑證。<error> 驗證設定檔「<name>」，vsys「<id>」，回覆訊息「<msg>」來自：<name>。
user-password-change-success	已為使用者「<name>」驗證 Kerberos SSO。領域「<name>」，EAP 外部身分「<name>」，內部身分「<name>」，驗證設定檔「<name>」，vsys「<id>」，伺服器設定檔「<name>」，伺服器位址「<addr>」，管理員角色「<name>」，存取網域「<name>」，回覆訊息「<msg>」來自：<name>。
auth-success	已為使用者「<name>」驗證 Kerberos SSO。領域「<name>」，EAP 外部身分「<name>」，內部身分「<name>」，驗證設定檔「<name>」，vsys「<id>」，伺服器設定檔「<name>」，伺服器位址「<addr>」，管理員角色「<name>」，存取網域「<name>」，回覆訊息「<msg>」來自：<name>。
user-password-change-success	已為使用者「<name>」驗證 SAML SSO。領域「<name>」，EAP 外部身分「<name>」，內部身分「<name>」，驗證設定檔「<name>」，vsys「<id>」，伺服器設定檔「<name>」，伺服器位址「<addr>」，管理員角色「<name>」，存取網域「<name>」，回覆訊息「<msg>」來自：<name>。
auth-success	已為使用者「<name>」驗證 SAML SSO。領域「<name>」，EAP 外部身分「<name>」，內部身分「<name>」，驗證設定檔「<name>」，vsys「<id>」，伺服器設定檔「<name>」，伺服器位址「<addr>」，管理員角色「<name>」，存取網域「<name>」，回覆訊息「<msg>」來自：<name>。
user-password-change-success	已為使用者「<name>」驗證 CAS SSO。領域「<name>」，EAP 外部身分「<name>」，

©2024 Palo Alto Networks, Inc.

事件 ID	說明
	內部身分「<name>」，驗證設定檔「<name>」，vsys「<id>」，伺服器設定檔「<name>」，伺服器位址「<addr>」，管理員角色「<name>」，存取網域「<name>」，回覆訊息「<msg>」來自：<name>。
auth-success	已為使用者「<name>」驗證 CAS SSO。領域「<name>」，EAP 外部身分「<name>」，內部身分「<name>」，驗證設定檔「<name>」，vsys「<id>」，伺服器設定檔「<name>」，伺服器位址「<addr>」，管理員角色「<name>」，存取網域「<name>」，回覆訊息「<msg>」來自：<name>。
user-password-change-success	已為使用者「<name>」驗證。領域「<name>」，EAP 外部身分「<name>」，內部身分「<name>」，驗證設定檔「<name>」，vsys「<id>」，伺服器設定檔「<name>」，伺服器位址「<addr>」，管理員角色「<name>」，存取網域「<name>」，回覆訊息「<msg>」來自：<name>。
auth-success	已為使用者「<name>」驗證。領域「<name>」，EAP 外部身分「<name>」，內部身分「<name>」，驗證設定檔「<name>」，vsys「<id>」，伺服器設定檔「<name>」，伺服器位址「<addr>」，管理員角色「<name>」，存取網域「<name>」，回覆訊息「<msg>」來自：<name>。
cas-client-redirect	用戶端「<name>」已重新導向至「<url>」，auth_session_id 為「<id>」
cas-token-received	從「<url>」接收到來自用戶端「<name>」的 CAS 權杖，auth_session_id 為「<id>」
cas-token-parse-error	無法剖析來自「<url>」的用戶端「<host>」的 CAS 權杖，auth_session_id 為「<id>」：<message>
cas-token-validated	已驗證來自「<url>」的用戶端「<name>」的 CAS 權杖，auth_session_id 為「<id>」，使用者名稱為「<name>」

©2024 Palo Alto Networks, Inc.

事件 ID	說明
cas-mfa-info	來自「<url>」的用戶端「<name>」的 MFA 資訊，auth_session_id 為「<id>」，使用者名稱為「<name>」：<info>
saml-client-redirect	對於驗證設定檔「<profile>」，用戶端「<name>」已重新導向至「<url>」
saml-idp-activity	從用戶端「<name>」接收到來自「<name>」的 SAML 判斷提示
saml-signature-validated	SAML 判斷提示：已根據使用者「<name>」的 IdP 憑證（主旨「<name>」）驗證特徵碼
idp-initiated-log-out-success	從「<name>」為使用者「<name>」發起 SAML 單一登出，驗證設定檔：「<name>」，虛擬系統：「<name>」，伺服器設定檔：「<name>」，IdP 實體 ID：「<id>」
sp-initiated-log-out-success	從「<name>」為使用者「<name>」發起 SAML 單一登出，驗證設定檔：「<name>」，虛擬系統：「<name>」，伺服器設定檔：「<name>」，IdP 實體 ID：「<id>」
auth-fail	伺服器憑證：「<name>」無效，其名稱與主機名稱「<name>」不匹配
auth-fail	伺服器憑證：「<name>」對伺服器「<name>」無效：<error>

bfd

事件 ID	說明
session-state-change	對於到介面 <name> 上的芳鄰 <name> 的 BFD 工作階段 <name>，BFD 狀態變更為 <name>。通訊協定：<name>

clusterd

事件 ID	說明
cluster-cfg-mode	叢集節點模式已變更。

©2024 Palo Alto Networks, Inc.

事件 ID	說明
cluster-config-p1-success	叢集精靈設定載入階段 1 成功。
cluster-config-p1-abort	叢集精靈設定載入階段 1 已中止。
cluster-config-p2-success	叢集精靈設定載入階段 2 成功。
cluster-self-join	本機節點已加入叢集：
cluster-service-ready	叢集服務已準備就緒。
cluster-service-up	叢集服務啟動：
cluster-split-brain-enter	叢集進入核心分裂模式。
cluster-split-brain-leave	叢集離開核心分裂模式。
cluster-engine-start	將為以下物件啟動叢集引擎：
cluster-daemon-start	叢集精靈已準備就緒。
cluster-daemon-exit	叢集精靈已退出。
cluster-daemon-init	叢集精靈正在初始化。

ddns

事件 ID	說明
ddns-remove	主機 <host> 到 <label> 的介面 <name> DDNS 設定已移除。請手動從 DDNS 服務提供者中移除。

debug

事件 ID	說明
packet-diag-log	已啟用 Packet-diag 日誌記錄
packet-diag-log	已停用 Packet-diag 日誌記錄

dhcp

©2024 Palo Alto Networks, Inc.

事件 ID	說明
if-update-ok	DHCP <desc>：介面 <name>，dhcp 伺服器：<name>
if-release-trigger	DHCP <name>：介面 <name>，IP <ip> 網路遮罩 <mask> dhcp 伺服器：<name>
if-renew-trigger	DHCP <name>：介面 <name>，IP <ip> 網路遮罩 <mask> dhcp 伺服器：<name>
if-update-fail	DHCP 用戶端無法清除介面 <name> 上的 IP 位址，原因為：更新介面/路由表時出錯
if-update-fail	DHCP 用戶端無法取得介面 <name> 上的 IP 位址，原因為：更新介面/路由表時出錯
if-update-fail	DHCP 用戶端無法取得介面 <name> 上的 IP 位址，原因為：從對等進行 HA 同步後更新介面/路由表時出錯
if-release-trigger	<dhcp_log_event>
if-renew-trigger	<dhcp_log_event>
if-update-ok	<dhcp_log_event>
if-rcv-nak	<dhcp_log_event>
if-duplicate-ip-intf	<dhcp_log_event>
if-duplicate-ip-remote	<dhcp_log_event>
if-update-fail	DHCP 用戶端無法取得介面 <name> 上的 IP 位址，原因為：更新介面/路由表時出錯
if-update-fail	DHCP 用戶端無法清除介面 <name> 上的 IP 位址，原因為：更新介面/路由表時出錯
relay-on	DHCP 轉送開啟
relay6-on	DHCPv6 轉送開啟
lease-end	DHCP 租用已結束
lease-start	DHCP 租用已開始

©2024 Palo Alto Networks, Inc.

事件 ID	說明
server-auto-probe-off	DHCP 伺服器自動探查已完成
server-auto-probe-on	DHCP 伺服器自動探查已完成
server-on	DHCP 伺服器自動探查已完成
if-inherit	介面 <name> 上的 DHCP 伺服器從動態介面 <name> 繼承以下值：<server>
if-update-fail	DHCP 用戶端無法取得介面索引 <num> 上的 IP 位址，原因為：更新介面/路由表時出錯

dns-security

事件 ID	說明
PAN_ELOG_EVENT_DNSSEC_CACHE_SUCCESS	從檔案儲存區成功初始化 DNS 特徵碼。

dnsproxy

事件 ID	說明
if-add	介面 <name> 已新增到 DNS Proxy 物件：<obj>
if-del	介面 <name> 已從 DNS Proxy 物件 <obj> 刪除
if-inherit	DNS Proxy 物件 <name> 從動態介面 <name> 繼承以下值：主要 DNS：<name> 次要 DNS：<name>
cache-cleared	已清除所有 DNS Proxy 快取項目
object-enable	Dnsproxy 物件 <name> 已啟用。
object-enable	Dnsproxy 物件 <name> 已停用。

dynamic-updates

事件 ID	說明
palo-alto-networks-message	<message>

fips

©2024 Palo Alto Networks, Inc.

事件 ID	說明
fips-selftest	FIPS 模式自檢 <description> ..... 失敗
fips-selftest	FIPS-CC 模式自檢 <description> ..... 失敗
fips-selftest	已成功啟用 FIPS 模式

general

事件 ID	說明
general	已從「<name>」擷取 CRL，其中 crl_next_update = <name>
general	插槽 s<num>：應用程式 Pod '<namespace> : <name>:<interface>' 使用介面 eth<num< and eth<num>
general	插槽 s<num>：應用程式 Pod '<namespace> : <name>:<interface>' 釋放介面 eth<num< and eth<num>
general	<name> 的機器學習引擎已啟動
general	重新連接到 MLAV 雲端，啟用所有機器學習引擎
general	<type> 作業已成功還原。完成時間=<time>。JobId=<id>使用者：<name>
wf-real-time-enabled	WildFire 即時功能已啟用
general	Evtmgr：Client=<id>[<devid>] msg=<msg> code=<num> socket <num>
general	向 <name> 伺服器發出的要求成功

hw

事件 ID	說明
fan-removed	風扇托架 #<num> 已移除
fan-inserted	風扇托架 #<num> 已插入

©2024 Palo Alto Networks, Inc.

事件 ID	說明
ps-inserted	電源 #<num> 已插入
熱失效	I2C 故障：強制風扇控制器以最大速度執行。\n"將節點 [force] 設定為 pan_true\n
熱失效	I2C 連線已還原。強制風扇恢復其正常速度。\n"將節點 [force] 設定為 pan_false\n
熱失效	I2C 連線已還原。強制風扇恢復其正常速度。\n"將節點 [force] 設定為 pan_false\n
slot-up	插槽 <id> (<model>) 偵測到工作階段分配政策不再是 ingress-slot。啟用 DPC。
bootstrap-success	啟動程序已成功完成 "sw-version: <version>; app-version: <version>; threat-version: <version>
bootstrap-media-prep-success	<username>：使用搭售包 <file> 成功準備 USB

ipv6nd

事件 ID	說明
duplicated-IPv6-address-found	介面 <name> 上 IPv6 位址 <address> 重複。

lacp

事件 ID	說明
lacp-up	LACP 介面 <name> 已移動至 AE 群組 <name>。

lldp

事件 ID	說明
mib changed	更新：LLDP更新：在本機介面 <index> 上傳送了TLV <name> 的更新：
mib changed	更新：在本機介面 <name> 上收到變更

monitoring

 ©2024 Palo Alto Networks, Inc.

事件 ID	說明
deviating-device	偏離的裝置：<name>，序號：<serial>，物件：<name> <nest>，指標：<name>，值：<value>

無

事件 ID	說明
無	建立稽核日誌
無	test file

nat

事件 ID	說明
fqdn-add	Vsys <id> NAT 規則 <name> FQDN <key> 新增 IP 項目 <ip>
fqdn-del	Vsys <id> NAT 規則 <name> FQDN <key> 刪除 IP 項目 <ip>

ntpd

事件 ID	說明
sync	NTP 同步到伺服器 <address>
time-learn	從 <time> 獲悉 NTP 時間； 新時間是：<time>，舊時間是 <time>
restart	已執行 NTP 重新啟動同步
time-learn	已獲悉 NTP 時間；新時間是：<time>

panorama-check

事件 ID	說明
panorama-check-test	JobId=<id>: <message>

©2024 Palo Alto Networks, Inc.

事件 ID	說明
panorama-check-skip	JobId=<id>:由於 IP 已變更，跳過 <name>/<name> 的連線檢查。
panorama-check-skip	JobId=<id>:由於 panorama 未主動連接，跳過 <name> 的連線檢查。
panorama-check-auto-revert	<type> 作業已成功還原。完成時間=<time>。JobId=<id>使用者：<name>

pbf

事件 ID	說明
nh-up	Vsys <id> PBF 規則 <name> nexthop 為 UP
nh-down	Vsys <id> PBF 規則 <name> nexthop 為 DOWN
nh-down	Vsys <id> PBF 規則 <name> 為 Bypassed
nh-up	Vsys <id> PBF 規則 <name> 為 Normal
pbf-fqdn-change	Vsys <id> PBF 規則 <name> nexthop FQDN <key> IPv4 已從 <ip> 變更為 <ip>
pbf-fqdn-change	Vsys <id> PBF 規則 <name> nexthop FQDN <key> IPv6 已從 <ip> 變更為 <ip>

port

事件 ID	說明
link-change	連接埠 HSCI：開啟 <type> 雙工
link-change	連接埠 HSCI：關閉 <type> 雙工
link-change	連接埠 HA1-b：開啟 <type> 雙工
link-change	連接埠 HA1-b：關閉 <type> 雙工
link-change	連接埠 HA2：開啟 <type> 雙工
link-change	連接埠 HA2：關閉 <type> 雙工

©2024 Palo Alto Networks, Inc.

事件 ID	說明
sdwan-link-change	連接埠 <port>：開啟 <type> 雙工
link-change	連接埠 <port>：關閉 <type> 雙工
sdwan-link-change	ethernet<num>/<num>:開啟 <type> 雙工
link-change	ethernet<num>/<num>:關閉 <type> 雙工
sdwan-link-change	連接埠 <port>：MAC 開啟
link-change	連接埠 <port>：MAC 關閉
nonsupp-forced	ethernet<num>/<num>：嘗試強制模式 <type> 不受支援，使用 autoneg
link-change	連接埠 MGT：開啟 <type>
link-change	連接埠 <interface>：開啟 <type>
link-change	連接埠 <interface>：關閉 <type>

pppoe

事件 ID	說明
connect-fail	為介面 <name> 上的使用者 <name> 連接 PPPoE 工作階段失敗。原因：<reason>
connect	對於介面 <name> 上的使用者 <name>，PPPoE 工作階段已連接到 AC：<name>，mac 位址：<mac>，工作階段 id：<id>，交涉的 IP 位址：<ip>
if-update-fail	已針對介面上的使用者 <name> 連接 PPPoE 工作階段：<name>，但更新介面/路由表失敗。
connect-fail	為介面 <name> 上的使用者 <name> 連接 PPPoE 工作階段失敗。原因：未收到 PPPoE 報價
initiate	已為介面 <name> 上的使用者 <name> 啟動 PPPoE 工作階段

©2024 Palo Alto Networks, Inc.

事件 ID	說明
connect-fail	為介面 <name> 上的使用者 <name> 連接 PPPoE 工作階段失敗。原因：未收到 PPPoE 確認
terminate	對於介面 <name> 上的使用者 <name>，到 AC <name> 的 PPPoE 工作階段已終止，mac 位址：<mac>，工作階段 id：<id>
terminate	對於介面 <name> 上的使用者 <name>，到 AC <name> 的 PPPoE 工作階段已終止，mac 位址：<mac>，工作階段 id：<id>

ras

事件 ID	說明
rasmgr-config-p1-success	RASMGR 精靈設定載入階段 1 成功。
rasmgr-config-p1-abort	RASMGR 精靈設定載入階段 1 已中止。
rasmgr-config-p2-success	RASMGR 精靈設定載入階段 2 成功。
rasmgr-ha-full-sync-done	RASMGR 精靈同步所有使用者資訊到 HA 對等已結束。
rasmgr-ha-full-sync-done	RASMGR 精靈同步所有使用者資訊到 HA 對等已結束。
rasmgr-flow-full-sync-start	RASMGR 精靈同步所有使用者資訊到流程已開始。
rasmgr-daemon-exit	RASMGR 精靈已退出。
rasmgr-daemon-init	RASMGR 精靈正在初始化。
rasmgr-daemon-start	RASMGR 精靈已準備就緒。

resctrl

事件 ID	說明
mem-usage-normal	記憶體使用量正常

©2024 Palo Alto Networks, Inc.

routing

事件 ID	說明
routed-OSPF-stop-helper-mode	OSPF 已停止用於重新啟動芳鄰的協助程式模式。重新啟動芳鄰路由器 ID <name> 芳鄰 IP 位址 <ip>。原因：<reason>
routed-ECMP	在虛擬路由器 <name> 中，ECMP 最大路徑已變更為 <num>。
routed-ECMP	在虛擬路由器 <name> 中啟用了 ECMP 。
routed-ECMP	在虛擬路由器 <name> 中停用了 ECMP 。
routed-config-p1-success	路由精靈設定載入階段 1 成功。
routed-config-p2-success	路由精靈設定載入階段 2 成功。
routed-static-fqdn-changed	路由靜態 fqdn 對應已變更
routed-bgp-fqdn-changed	路由的 BGP fqdn 對應已變更
routed-ECMP	在邏輯路由器 <name> 中，ECMP 最大路徑已變更為 <num>。
routed-ECMP	在邏輯路由器 <name> 中啟用了 ECMP 。
routed-ECMP	在邏輯路由器 <name> 中停用了 ECMP 。
routed-ECMP	在邏輯路由器 <name> 中，ECMP 負載平衡演算法已變更為 <name>。
routed-ECMP	在邏輯路由器 <name> 中啟用了 ECMP 對稱傳回。
routed-ECMP	在邏輯路由器 <name> 中停用了 ECMP 對稱傳回。
routed-ECMP	在邏輯路由器 <name> 中啟用了 ECMP 嚴格來源路徑。
routed-ECMP	在邏輯路由器 <name> 中停用了 ECMP 嚴格來源路徑。
routed-fib-sync-peer-backup	當對等裝置變為被動時，FIB HA 同步開始。

©2024 Palo Alto Networks, Inc.

事件 ID	說明
routed-fib-sync-self-master	當本機裝置成為主要裝置時，FIB HA 同步開始。
routed-fib-sync-peer-backup	當對等裝置變為被動時，FIB HA 同步開始。
routed-fib-sync-self-master	當本機裝置成為主要裝置時，FIB HA 同步開始。
routed-daemon-init	路由精靈正在初始化。
routed-daemon-start	路由精靈已準備就緒。
routed-daemon-exit	路由精靈已退出。
routed-BGP-refresh-sent	ROUTE REFRESH 訊息已傳送到 BGP 對等。
routed-BGP-ribin-recalc	由於匯入政策的變更，正在重新計算 RIB-In。
routed-BGP-peer-enter-established	BGP 對等工作階段進入已建立狀態。
routed-BGP-peer-mp-extension-negotiate	BGP 對等 MP 延伸交涉。
routed-IGMP-wrong-version	錯誤的 IGMP 查詢版本
routed-OSPF-neighbor-full	OSPF 與芳鄰建立完全鄰接關係。
routed-OSPF-neighbor-2dir	OSPF 與芳鄰建立雙向通訊。
routed-OSPF-neighbor-full	OSPF 與芳鄰建立完全鄰接關係。
routed-OSPF-start-graceful-restart	OSPF 已開始非失誤性重新啟動。
routed-OSPF-stopped-graceful-restart	OSPF 已停止非失誤性重新啟動。
routed-OSPF-start-helper_node	OSPF 已啟動用於重新啟動芳鄰的協助程式模式。
routed-OSPF-not-help	OSPF 未協助重新啟動芳鄰。
routed-OSPF-start-graceful-restart	OSPF 已開始非失誤性重新啟動。
routed-PIM-new-dr-elected	PIM 選出了新的 DR
routed-PIM-neighbor-discovered	PIM 發現了一個新芳鄰

©2024 Palo Alto Networks, Inc.

事件 ID	說明
routed-PIM-neighbor-disappeared	PIM 芳鄰消失了
routed-RIP-peer-add	發現了 RIP 對等。

satd

事件 ID	說明
satd-config-p1-success	SATD 精靈設定載入階段 1 成功。
satd-config-p1-abort	SATD 精靈設定載入階段 1 已中止。
satd-config-p2-success	SATD 精靈設定載入階段 2 成功。
satd-portal-connect-started	GlobalProtect 衛星到入口網站的連線已啟動。
satd-gateway-connect-started	GlobalProtect 衛星到閘道的連線已啟動。
satd-flow-full-sync-start	SATD 精靈將所有閘道資訊同步到流程已開始。
satd-ha-full-sync-done	SATD 精靈將所有閘道資訊同步到 HA 對等已結束。
satd-daemon-init	SATD 精靈正在初始化。
satd-daemon-start	SATD 精靈已準備就緒。
satd-daemon-exit	SATD 精靈已退出。

sched-push

事件 ID	說明
sched-skip	在被動 panorama 上跳過推送排程 <name>
sched-exec	已排程在 <num> 作業中移除推送排程 <name>Jobids：<ids>

sdwan

 ©2024 Palo Alto Networks, Inc.

事件 ID	說明
sdwan-vif-status-up	<vif> 已開始，狀態為啟動。FW is Active
sdwan-vif-status-up	<vif> 已開始，狀態為啟動。FW 為非作用中狀態。
sdwan-vif-status-up	<vif> 啟動
sdwan-vif-status-down	<vif> 關閉

ssh

事件 ID	說明
ssh-default-hostkey-changed	預設 MGMT SSH 主機金鑰設定為長度為 <length> 的 ECDSA 金鑰。
ssh-default-hostkey-changed	預設 MGMT SSH 主機金鑰設定為長度為 <length> 的 RSA 金鑰
ssh-default-hostkey-changed	預設 MGMT SSH 主機金鑰設定為 all。
ssh-default-hostkey-changed	預設 HA SSH 主機金鑰設定為長度為 <length> 的 ECDSA 金鑰。
ssh-default-hostkey-changed	預設 HA SSH 主機金鑰設定為長度為 <length> 的 RSA 金鑰。
ssh-default-hostkey-changed	為類型為 ECDSA 且長度為 <length> 的 HA 設定預設主機金鑰時出錯
ssh-default-hostkey-changed	為類型為 ECDSA 且長度為 <length> 的 MGMT 設定預設主機金鑰時出錯
ssh-default-hostkey-changed	為類型為 RSA 且長度為 <length> 的 HA 設定預設主機金鑰時出錯
ssh-default-hostkey-changed	為類型為 RSA 且長度為 <length> 的 MGMT 設定預設主機金鑰時出錯
ssh-hostkey-regenerated	已為 ECDSA 類型且長度為 <num> 的 HA 產生 SSH 主機金鑰

©2024 Palo Alto Networks, Inc.

事件 ID	說明
ssh-hostkey-regenerated	已為 ECDSA 類型且長度為 <num> 的 MGMT 產生 SSH 主機金鑰
ssh-hostkey-regenerated	已為 RSA 類型且長度為 <num> 的 HA 產生 SSH 主機金鑰
ssh-hostkey-regenerated	已為 RSA 類型且長度為 <num> 的 MGMT 產生 SSH 主機金鑰
ssh-session-rekey-params-changed	MGMT SSH 集的新重設金鑰參數。
ssh-session-rekey-params-changed	HA SSH 集的新重設金鑰參數。
ssh-session-rekey-params-changed	為 MGMT SSH 設定重設金鑰參數時出錯。
ssh-session-rekey-params-changed	為 HA SSH 設定重設金鑰參數時出錯。
ssh-ciphers-changed	已將 MGMT SSH 的密碼設定為預設值。
ssh-ciphers-changed	已將 HA SSH 的密碼設定為預設值。
ssh-ciphers-changed	為 MGMT SSH 設定密碼時出錯。
ssh-ciphers-changed	為 HA SSH 設定密碼時出錯。
ssh-macs-changed	已將 MGMT SSH 的 Macs 設定為預設值。
ssh-macs-changed	已將 HA SSH 的 Macs 設定為預設值。
ssh-macs-changed	為 MGMT SSH 設定 macs 時出錯。
ssh-macs-changed	為 HA SSH 設定 macs 時出錯。
ssh-kexs-changed	已將 MGMT SSH 的 Kexs 設定為預設值。
ssh-kexs-changed	已將 HA SSH 的 Kexs 設定為預設值。
ssh-kexs-changed	為 MGMT SSH 設定 kexs 時出錯。
ssh-kexs-changed	為 HA SSH 設定 kexs 時出錯。

sslmgr

©2024 Palo Alto Networks, Inc.

事件 ID	說明
ca-session-establishment-success	目的地位址 <addr>，目的地連接埠 <num>，來源位址 <addr>，來源連接埠 <num>
ca-session-establishment-failed	無法取得 CRL %s
ca-session-establishment-failed	CRL <name> 的金鑰用法 cRLSign 檢查失敗
ca-session-establishment-success	"成功取得 CRL <name>
ca-session-establishment-success	對 <name> 的 CRL 請求成功
ca-session-establishment-success	對「<host>」的 OCSP 要求成功。\n目的地位址：<addr>，目的地連接埠：<port>，來源位址：<addr>，來源連接埠 <port>\n
ca-session-establishment-failed	對「<host>」的 OCSP 要求失敗。\n目的地位址：<addr>，目的地連接埠：<port>，來源位址：<addr>，來源連接埠 <port>\n
ca-session-establishment-failed	<open_ssl_error>
sslmgr-ha-not-full-sync	SSLMGR 精靈不同步到 HA 對等。
sslmgr-ha-not-full-sync	SSLMGR 精靈不同步到 HA 對等。
sslmgr-ha-not-full-sync	SSLMGR 精靈不同步到 HA 對等。
sslmgr-cert-ocsp-verify-failed	SSLMGR 憑證 ocsp 驗證失敗。
sslmgr-config-p1-success	SSLMGR 精靈設定載入階段 1 成功。
sslmgr-config-p2-success	SSLMGR 精靈設定載入階段 2 成功。
sslmgr-daemon-start	SSLMGR 精靈已準備就緒。
sslmgr-satellite-info-deleted	SSLMGR 衛星資訊已刪除
sslmgr-cert-status-deleted	SSLMGR 憑證狀態已刪除。
sslmgr-cert-status-revoked	SSLMGR 憑證狀態已撤銷。
sslmgr-satellite-info-deleted	SSLMGR 衛星資訊已刪除
sslmgr-cert-status-revoked	SSLMGR 憑證狀態已撤銷。

©2024 Palo Alto Networks, Inc.

事件 ID	說明
sslmgr-scep-ca-cert-failed	SSLMGR 匯入 SCEP CA 憑證失敗。
sslmgr-scep-cert-failed	SSLMGR 產生 SCEP 憑證失敗。
sslmgr-scep-cert-failed	SSLMGR 產生 SCEP 憑證失敗。
sslmgr-scep-cert-failed	SSLMGR 產生 SCEP 憑證失敗。
sslmgr-satellite-info-updated	SSLMGR 衛星資訊已更新
sslmgr-cert-gen-failed	SSLMGR 產生憑證失敗。
sslmgr-ha-full-sync	SSLMGR 精靈同步到 HA 對等。
sslmgr-ha-full-sync	SSLMGR 精靈同步到 HA 對等。
sslmgr-ha-full-sync	SSLMGR 精靈同步到 HA 對等。
ca-session-establishment-success	目的地位址 <addr>，目的地連接埠 <port>，來源位址 <addr>，來源連接埠 <port>

syslog

事件 ID	說明
syslog-conn-status	<syslog-ng message>

tls

事件 ID	說明
panos-auth-success	<name> 伺服器 CN：<name> - [<name>] 連線已成功建立。
tls-session-disconnected	裝置 <name> 已與伺服器終端連線
panorama-auth-success	<reason> PAN-OS 版本：<version> Panorama 版本：<version>用戶端 ID：<ip> 伺服器 IP：<ip> 用戶端 CN：<name>
panorama-auth-success	<reason> WildFire 版本：<version> Panorama 版本：<version>用戶端 ID：<ip> 伺服器 IP：<ip> 用戶端 CN：<name>

©2024 Palo Alto Networks, Inc.

事件 ID	說明
certificate-renewal	用戶端憑證到期時間不到 30 天。從 scep 伺服器擷取新憑證

url-filtering

事件 ID	說明
failed-to-lock-update	無法鎖定 URL 資料庫更新過程#也許另一個執行個體正在執行。
download-url-database-success	Brightcloud URL 資料庫已成功下載
revert-url-database-success	URL 篩選資料庫已從版本 <ver> 還原為版本 <ver>
url-database-is-latest	URL 篩選資料庫版本 <ver> 已經是最新版本
failed-to-lock-download	無法鎖定 URL 資料庫更新過程。另一個執行個體可能正在執行。
download-url-database-success	PAN-DB 已成功下載
load-success	PAN-DB 已成功初始啟動
failed-to-lock-download	PAN-DB 下載：失敗。
downloading-url-database	正在下載完整的 BrightCloud URL 資料庫。這可能需要很長時間。
downloading-url-database	正在下載完整的 BrightCloud URL 資料庫。這可能需要很長時間。
proxy-connection-failure	無法連線至 Proxy 伺服器。"請檢查 Proxy 使用者名稱和密碼是否正確。
receive-data-failure	無法從「<server>:<port>」接收資料以下載 BrightCloud URL 資料庫
proxy-connection-failure	無法連線至 Proxy 伺服器。"請檢查 Proxy 使用者名稱和密碼是否正確。
proxy-connection-failure	無法連接到 Proxy 伺服器「<server>:<port>」以下載 BrightCloud URL 資料庫

©2024 Palo Alto Networks, Inc.

事件 ID	說明
proxy-connection-failure	無法連接到 Proxy 伺服器「<server>:<port>」以下載 BrightCloud URL 資料庫
connection-success	已連接到 Brightcloud 更新伺服器 <name>
cloud-election	雲端選擇：<name> IP：<ip> 已選擇，已進行保持運作測試 <num>。
url-engine-stopped	PAN-DB 引擎已停止。
url-engine-starts	PAN-DB 引擎已啟動。
url-engine-stopped	URL 篩選引擎已停止...
ha-sync-failure	無法將 URL 與 HA 對等同步。
starts-from-empty-seed	以空白 SEED 開始。
starts-from-backup-seed	以備份 seed 開始。
starts-from-empty-seed	以空白 SEED 開始。
ha-sync-success	已成功將 PAN-DB 同步到對等。
ha-sync-success	PAN-DB 與 HA 的同步開始於 <seconds>。
url-backup-seed-success	PAN-DB 備份已成功完成。
upgrade-url-database-success	PAN-DB 已升級至版本 <version>。
ha-sync-success	URL 廠商匹配並設定為「PAN-DB」。
ha-sync-failure	未將檔案同步到對等，因為模式不是主動-被動 (<mode>)。
ha-sync-failure	未將檔案同步到對等，因為本機狀態不是主動 (<mode>)。
ha-sync-failure	不接受來自對等本機狀態的檔案不是被動 (<mode>)。
ha-sync-failure	未將檔案同步到對等，因為對等狀態不是被動 (<mode>)。

©2024 Palo Alto Networks, Inc.

userid

事件 ID	說明
connect-agent	重新分配代理程式 <name><id>)：已連接到 <host>，狀態 <status>，版本 <num>
connect-client	CMS 重新分配用戶端已連接到全域收集器：<devid> vsys <id>
connect-client	重新分配用戶端已連接到收集器 <name>：<client>，vsys <id>
connect-ldap-sever	ldap cfg <name> 已連接到伺服器 <server>
connect-ldap-sever	ldap cfg <name> 已連接到伺服器 <server>
connect-agent	<agent> <name>(vsys<id>)：已連接到 <name>，狀態 <status>，版本 <version>
connect-client	User-ID 用戶端已連接到收集器 <name>："IP <ip> 連接埠 <num> vsys <num>
disconnect-client	User-ID 用戶端已與收集器 <name> 中斷連線："IP <ip> 連接埠 <num> vsys_id <num>
disconnect-client	User-ID 用戶端已與收集器 <name> 中斷連線："IP <ip> 連接埠 <num> vsys_id <num>
connect-client	User-ID 用戶端已連接到收集器 <name>：<conn_id> vsys_id <id>
disconnect-client	User-ID 用戶端與收集器 <name> 中斷連線：<conn_id> vsys_id <id>
connect-agent	<agent_desc> <name>(vsys<id>)：已連接到 <name>，版本 <id>
agent-read-log-error	<name> 失敗 <num> 次
agent-get-domain-error	<name> 請檢查 Pan-Agent 記錄檔案，以獲取實際的不正確 DC IP 位址
agent-get-groups-error	<name> 失敗 <num> 次
agent-get-config-error	<name> 失敗 <num> 次

©2024 Palo Alto Networks, Inc.

事件 ID	說明
agent-get-users-error	<name> 失敗 <num> 次
agent-no-domain	<name> 失敗 <num> 次
disconnect-syslog	User-ID Syslog Proxy：用戶端 <name>：已中斷連線 <addr>
connect-syslog	User-ID Syslog Proxy：用戶端 <name>(vsys<id>)：已連線 <addr>
disconnect-syslog	User-ID Syslog Proxy：用戶端 <name>：已中斷連線 <addr>
disconnect-syslog	User-ID Syslog Proxy：用戶端 <name>：已中斷連線 <addr>
connect-agent	Pan-TS-Agent <name> 已中斷連線：IP <ip> 連接埠 <num> vsys<num>
disconnect-agent	PAN-Agent <name> 已中斷連線：IP <ip> 連接埠 <num> vsys<id>
agent-status-failure	<num> 次嘗試獲取狀態失敗，連線可能已斷開或裝置與 pan-agent 之間的通訊協定不匹配
disconnect-agent	User-ID-Agent <name> 已中斷連線：IP <ip> 連接埠 <num> vsys<id>
disconnect-agent	User-ID-Agent <name> 已中斷連線：<conn_str> vsys<id>
agent-event	User-ID-Agent <name> 事件：<type>，名稱 <name>，狀態 <status>，vsys<id>
agent-status-failure	<num> 次嘗試獲取狀態失敗，連線可能已斷開或裝置與 pan-agent 之間的通訊協定不匹配
connect-server-monitor	請將伺服器監控 (<name>) 傳輸通訊協定從 WMI 變更為 WinRM，以獲得更好的效能
connect-server-monitor	User-ID 伺服器監控器 <name>(vsys<id>)：已連接到 <host>
connect-server-monitor	伺服器監控器 <name>(vsys<id>) 已連接

©2024 Palo Alto Networks, Inc.

事件 ID	說明
connect-vm-info-source	vm-info-source <name>(vsys<id>)：已連接到 <host>，狀態 <status>
connect-vm-info-source	vm-info-source <name>(vsys<id>)：已連接到 <host>，狀態 <status>
connect-vm-info-source	vm-info-source <name>(vsys<id>)：已連接到 <host>，狀態 <status>，版本 <version>
disconnect-vm-info-source	vm-info-source <name>(vsys<id>)：已與 <host> 中斷連線，狀態 <status>，版本 <version>

vm

事件 ID	說明
dvf-init-succeed	VMware dvfilter 初始化成功

vpn

事件 ID	說明
vpnctl-ike-rekey-event	[<name>]: <davici_name>:<value,
vpnctl-child-updown-event	[<name>]: <davici_name>:<value,
vpnctl-child-rekey-event	[<name>]: <davici_name>:<value,
vpnctl-ike-updown-event	連線失敗，對等 <remote_host>，重試 <conn_try>
keymgr-daemon-init	KEYMGR 精靈正在初始化。
keymgr-daemon-start	KEYMGR 精靈已準備就緒。
keymgr-daemon-exit	KEYMGR 精靈已退出。
keymgr-flow-full-sync-done	KEYMGR 將所有 IPSec SA 同步到流程已結束。
ike-fqdn-change	IKE fqdn 對應已變更
ike-config-p1-success	IKE 精靈設定載入階段 1 成功。

©2024 Palo Alto Networks, Inc.

事件 ID	說明
ike-config-p1-abort	IKE 精靈設定載入階段 1 已中止。
ike-config-p2-success	IKE 精靈設定載入階段 2 成功。
ike-nego-p1-fail-psk	IKE 階段 1 交涉失敗，可能是由於預先共用金鑰不匹配。
ike-nego-p1-fail-psk	IKE 階段 1 交涉失敗，可能是由於預先共用金鑰不匹配。
ike-nego-p1-fail-common	IKE phase-1 negotiation is failed_COMM
ike-nego-p1-fail-common	IKE phase-1 negotiation is failed_COMM
ike-nego-p1-fail-common	IKE phase-1 negotiation is failed_COMM
ikev2-nego-child-ts-bad	處理流量選擇器時，IKEv2 子 SA 交涉失敗。
ikev2-nego-child-ts-bad	處理流量選擇器時，IKEv2 子 SA 交涉失敗。
ikev2-send-p1-delete	IKEv2 IKE SA 刪除訊息已傳送到對等。
ike-nego-p1-fail-common	IKE phase-1 negotiation is failed_COMM
ikev2-nego-use-v1	IKEv1 在 IKEv2 偏好模式中使用。
ike-nego-p2-stale-p1	正在刪除可能過時的階段 1 SA。
ike-nego-p1-start	IKE 階段 1 交涉已開始
ike-nego-p1-fail	IKE 階段 1 交涉失敗
ike-nego-p1-succ	IKE 階段 1 交涉成功
ike-nego-p1-delete	IKE 階段 1 SA 已刪除
ike-nego-p1-expire	IKE 階段 1 SA 已過期
ike-nego-p2-start	IKE 階段 2 交涉已開始
ike-nego-p2-fail	IKE 階段 2 交涉失敗
ike-nego-p2-succ	IKE 階段 2 交涉成功
ipsec-key-install	IPSec 金鑰已安裝。

©2024 Palo Alto Networks, Inc.

事件 ID	說明
ipsec-key-delete	IPSec 金鑰已刪除。
ipsec-key-expire	IPSec 金鑰存留期已過期。
ike-nego-p2-proxy-id-bad	處理 Proxy ID 時，IKE 階段 2 交涉失敗。
ike-nego-p2-proxy-id-bad	處理 Proxy ID 時，IKE 階段 2 交涉失敗。
ike-nego-p2-no-p1	收到 IKE 階段 2 交涉要求，但未找到階段 1 SA。
ike-nego-p2-p1-not-ready	收到 IKE 階段 2 交涉要求，但沒有可用的作用中階段 1 SA。
ike-nego-p2-proposal-bad	IKE phase-2 negotiation failed when processing SA payload.
ike-nego-p1-fail-common	IKE phase-1 negotiation is failed_COMM
ike-nego-p1-psk-idtype	IKE phase-1 negotiation is failed.使用預先共用金鑰時
ike-nego-p1-fail-psk	IKE 階段 1 交涉失敗，可能是由於預先共用金鑰不匹配。
ike-nego-p1-fail-psk	IKE 階段 1 交涉失敗，可能是由於預先共用金鑰不匹配。
ike-recv-notify	已收到 IKE 通訊協定通知訊息：
ike-recv-p1-delete	從對等接收到 IKE 通訊協定階段 1 SA 刪除訊息。
ike-recv-p2-delete	從對等接收到 IKE 通訊協定 IPSec SA 刪除訊息。
ike-send-p1-delete	IKE 通訊協定階段 1 SA 刪除訊息已傳送給對等。
ike-send-p2-delete	IKE 通訊協定 IPSec SA 刪除訊息已傳送給對等。
ike-send-notify	IKE 通訊協定通知訊息已傳送：

©2024 Palo Alto Networks, Inc.

事件 ID	說明
ike-send-notify	IKE 通訊協定通知訊息已傳送：
ike-send-notify	IKE 通訊協定通知訊息已傳送：
ike-nego-p2-dup-rekey	偵測到重複的階段 2 重設金鑰要求
ike-nego-p1-cert-succ	IKE 憑證驗證成功。
ike-nego-p1-fail-psk	IKE 階段 1 交涉失敗，可能是由於預先共用金鑰不匹配。
ikev2-nego-cert-succ	IKEv2 憑證驗證成功。
ikev2-nego-fail-psk	IKEv2 SA 交涉失敗，可能是由於預先共用金鑰不匹配。
ikev2-send-p2-delete	IKEv2 IPSec SA 刪除訊息已傳送到對等。
ikev2-nego-child-fail	IKEv2 子 SA 交涉失敗
ikev2-nego-child-fail	IKEv2 子 SA 交涉失敗
ikev2-nego-child-fail	IKEv2 子 SA 交涉失敗
ikev2-nego-child-fail	IKEv2 子 SA 交涉失敗
ikev2-nego-stale-p2	正在刪除可能過時的 IKEv2 子 SA。
ikev2-nego-fail-common	IKEv2 SA 交涉失敗。
ike-recv-notify	已收到 IKE 通訊協定通知訊息：
ikev2-recv-p1-delete	從對等接收到 IKEv2 IKE SA 刪除訊息。
ikev2-recv-p2-delete	從對等接收到 IKEv2 IPSec SA 刪除訊息。
ikev2-nego-ike-fail	IKEv2 IKE SA 交涉失敗
ikev2-nego-ike-start	IKEv2 IKE SA 交涉已啟動
ikev2-nego-ike-fail	IKEv2 IKE SA 交涉失敗
ikev2-nego-ike-succ	IKEv2 IKE SA 交涉成功
ikev2-nego-ike-delete	IKEv2 IKE SA 已刪除

©2024 Palo Alto Networks, Inc.

事件 ID	說明
ikev2-nego-ike-expire	IKEv2 IKE SA 已過期
ikev2-nego-child-start	IKEv2 子 SA 交涉已啟動
ikev2-nego-child-fail	IKEv2 子 SA 交涉失敗
ikev2-nego-child-succ	IKEv2 子 SA 交涉成功
ipsec-key-install	IPSec 金鑰已安裝。
ipsec-key-delete	IPSec 金鑰已刪除。
ipsec-key-expire	IPSec 金鑰存留期已過期。
ikev2-nego-use-v1	IKEv1 在 IKEv2 偏好模式中使用。
ike-daemon-init	IKE 精靈正在初始化。
ike-daemon-start	IKE 精靈已準備就緒。
ike-daemon-exit	IKE 精靈已退出。

wildfire

事件 ID	說明
wildfire-no-policy	WildFire <name> 通道停用。<name> 通道沒有作用中的 WildFire 分析設定檔。
wildfire-auth-failed	無法向憑證授權單位驗證 SSL 對等的憑證

wildfire-appliance

事件 ID	說明
cluster-mode-change	叢集模式已變更為 stand_alone
cluster-mode-change	叢集模式已變更為 controller
cluster-mode-change	叢集模式已變更為 worker
cluster-mode-change	叢集模式已變更為 unknown

©2024 Palo Alto Networks, Inc.

事件 ID	說明
cluster-engine-role	叢集引擎作為 controller 啟動。

Slog

- 風扇托架丟失，如果不更換，系統將在 <num> 秒鐘內斷電。
- <entry> 在啟動時不存在
- 使用 Force 釋放插槽 <id>，uid <id>
- 使用 Non-force 釋放插槽 <id>，uid <id>
- Get registration with uid <id> sw_ver <version> slot <id> dp_ip <ip>
- 已為 uid <uid> <id> 配置插槽 %d
- 裝置憑證將在 15 天或更短時間內到期
- 已成功從 Palo Alto Networks 擷取裝置憑證
- Logd failed to send disconnect to configd for (<id>)
- Logd blocking customerid (<id>)
- Logd Unblocking customerid (<id>)
- Logd failed to send disconnect to configd for (<name>)]
- 為群組對應觸發 AddrObjRefresh 提交
- 清除 mongodb 資料大小（<num> 個記錄）以使資料大小低於限制 <num>
- 已從對等裝置下載 GlobalProtect 資料檔案版本 <version>
- 名稱解析花費太長時間，停用報告 <name> 的名稱查閱
- 名稱解析花費太長時間，停用報告 <name> 的名稱
- 已在其中一個群組對應設定中變更主要使用者屬性
- <host> 的網頁驗證入口用戶端憑證驗證失敗。沒有憑證。
- <host< 的網頁驗證入口用戶端憑證驗證失敗。憑證不屬於憑證設定檔鏈
- <host> 的 OSCP/CRL 網頁驗證入口用戶端憑證驗證失敗。
- <host> 的網頁驗證入口用戶端憑證尚未啟用。
- <host> 的網頁驗證入口用戶端憑證已過期。
- <host> 的網頁驗證入口用戶端憑證驗證成功
- 對於 <host> vsys<id> 上的使用者 <name>，<type> 驗證成功
- 對於 <addr> vsys<id> 上的使用者 <user>，<type> 已從工作階段 Cookie 更新
- 對於 <addr> vsys<id> 上的使用者 <user>，<type> NTLM 驗證失敗
- 對於 <addr> vsys<id> 上的使用者 <user>，<type> NTLM 驗證成功
- 對於 <ip> vsys<id> 上的使用者 <user>，<type> 驗證失敗（無效）

©2024 Palo Alto Networks, Inc.

- 對於 <ip> vsys<id> 上的使用者 <name>，<type> 驗證失敗
- 對於 <ip> vsys<id> 上的使用者 <name>，<type> 驗證成功
- Logd 從 http 服務收到錯誤回應代碼 (<num>) msg size <num> customerid <id> logtype <name> num_rec <num>
- <serial> 插槽 <id>的 Logdb 降級已開始。
- 在 <num> 天 <num> 小時 <num> 分鐘 <num> 秒內完成了 <serial> 插槽 <id> 上的 Logdb 降級。
- <serial> 插槽 <num> 的 Logdb 移轉已開始。
- <serial> 插槽 <num> 的 Logdb 移轉已暫停。
- <serial> 插槽 <id> 的 Logdb 移轉已被放棄。
- <serial> 插槽 <id> 的 Logdb 移轉已完成。
- 測試電子郵件已成功傳送至 <name>，用於電子郵件設定檔 <name>
- <host> 的 OSCP/CRL 用戶端憑證驗證失敗。
- <host> 的用戶端憑證驗證成功。
- <host> 的用戶端憑證驗證失敗。未偵測到 https。
- <host> 的用戶端憑證驗證失敗。未偵測到 https。
- 建立系統日誌
- 建立自訂系統日誌
- 叢集成員 <id>，已成功為 <name> 更新 <name>，並使用 jobid <id> 推送加入佇列
- 叢集成員 <id>，已成功為 <name> 刪除 <name>，並使用 jobid <id> 推送加入佇列
- 成功連接到 %s:%s:%d
- 連接到 %s:%s:%d 失敗
- dsc 服務已啟動
- 標識用戶端收到格式錯誤的政策建議。
- 標識用戶端收到政策建議錯誤：%v。
- 標識用戶端收到 %v 政策建議。
- 標識用戶端無法獲取政策建議。
- Icd HA 狀態從 %d 變更為 %d
- Icd HA better 狀態從 %d 變更為 %d
- 無法擷取來源位址，出現錯誤 %d"
- iot-eal 服務已啟動
- icd 服務已啟動
- 與 %s 的 gRPC 連線已斷開，錯誤：%v
- 與 %s 的 gRPC 連線已建立，%s -> %s

 ©2024 Palo Alto Networks, Inc.

- "與 %s 的 gRPC 連線已斷開，錯誤：%s"
- Cloud Appid 功能已停用
- Cloud Appid 功能已啟用
- Cloud Appid %s task[%d] 已完成，新雲端版本：%s, %s",
- Cloud Appid %s task[%d] 失敗：%v
- 雲端應用程式：%s 資料丟失了一些檔案，%d -> %d
- 雲端應用程式：檢查並還原 %s 資料，類型 %d。

低嚴重性系統日誌訊息

電子日誌

- audit
- auth
- dns-security
- dynamic-updates
- routing
- vpn

audit

事件 ID	說明
cli	<cmd>
api	<cmd>
cli	<config command>
api	<config command>
gnmi	<config command>
gui-op	<config command>

auth

事件 ID	說明
cas-message	（設定檔 id：<id>）<message>
saml-out-of-band-message	客戶端「<name>」收到頻外 SAML 訊息：<message>

©2024 Palo Alto Networks, Inc.

dns-security

事件 ID	說明
PAN_ELOG_EVENT_DNSSEC_CACHE_FAIL	從檔案儲存區初始化 DNS 特徵碼失敗，以空白快取開始。

dynamic-updates

事件 ID	說明
palo-alto-networks-message	<message>

routing

事件 ID	說明
routed-config-p1-failed	路由精靈設定載入階段 1 失敗。
routed-BGP-peer-failed	BGP 對等工作階段失敗，可能會重新啟動。
routed-BGP-peer-restarted	已啟動 BGP 對等的非失誤性重新啟動。
routed-BGP-peer-restart-failed	BGP 對等的非失誤性重新啟動失敗。
routed-RTM-bad-route	無效的動態路由被拒絕：
routed-OSPF-LSA-chksum-invalid	OSPF 收到的 LSA 具有無效的總和檢查碼。
routed-OSPF-LSA-chksum-invalid	OSPF 收到的 LSA 具有無效的總和檢查碼。
routed-OSPF-LSA-chksum-failed	由於記憶體損壞，OSPF LSA 總和檢查碼產生失敗。
routed-OSPF-LSA-chksum-failed	由於記憶體損壞，OSPF LSA 總和檢查碼產生失敗。
routed-OSPF-md5chksum-bad	OSPF 封包因不正確的 MD5 總和檢查碼而被丟棄。
routed-OSPF-authtype-bad	OSPF 封包因意外的驗證類型而被丟棄。
routed-OSPF-password-bad	OSPF 封包因不正確的簡單密碼而被丟棄。

©2024 Palo Alto Networks, Inc.

事件 ID	說明
routed-OSPF-chksum-bad	OSPF 封包因不正確的 OSPF 總和檢查碼而被丟棄。
routed-OSPF-sequence-bad	OSPF 封包因不正確的序號而被丟棄。
routed-OSPF-hello-hello-intval-bad	OSPF hello 封包因 hello 間隔不匹配而被丟棄。
routed-OSPF-hello-dead-intval-bad	OSPF hello 封包因 dead 間隔不匹配而被丟棄。
routed-OSPF-hello-netmask-bad	OSPF hello 封包因網路遮罩不匹配而被丟棄。
routed-OSPF-hello-area-type-bad	OSPF hello 封包因區域類型不匹配而被丟棄。
routed-PIM-interface-state-changed	PIM 介面狀態已變更
routed-RIP-authtype-bad	RIP 封包因意外的驗證類型而被丟棄。
routed-RIP-auth-failed	RIP 封包因驗證失敗而被丟棄。
routed-RIP-md5length-bad	RIP 封包因 MD5 摘要長度不正確而被丟棄。
routed-RIP-md5length-bad	RIP 封包因 MD5 摘要長度不正確而被丟棄。
routed-RIP-auth-failed	RIP 封包因驗證失敗而被丟棄。

vpn

事件 ID	說明
ike-nego-p1-dpd-dn	IKE 階段 1 SA 被 DPD 確定為關閉。
ikev2-nego-ike-dpd-dn	IKEv2 IKE SA 被 DPD 確定為關閉。

Slog

- 檢查 DB uid 失敗，忽略重新註冊。傳回代碼：<num>
- 已重新交涉交換器網狀架構到網路處理器連結。
- 部署檔案「<file>」的 SCP 成功

©2024 Palo Alto Networks, Inc.

中嚴重性系統日誌訊息

電子日誌

日誌標籤：

- auth
- ddns
- dhcp
- dns-security
- dynamic-updates
- fips
- general
- hw
- nat
- ntpd
- port
- routing
- satd
- syslog
- url-filtering
- userid
- wildfire

auth

事件 ID	說明
cas-message	（設定檔 id：<id>）<message>
auth-fail	由於特殊字元，具有使用者名稱「<name>」的 <type> 無效
auth-fail	為 uid <uid> <id> 配置的插槽 <id>
auth-fail	管理員 <name> 未能通過驗證 <num> 次 — 已達到失敗驗證嘗試的閾值。
auth-fail	由於驗證嘗試失敗次數過多，管理員 <name> 的帳戶被停用。

©2024 Palo Alto Networks, Inc.

事件 ID	說明
auth-success	已為使用者「<name>」驗證憑證。<error>
auth-fail	使用者「<user>」憑證驗證失敗。<error> 驗證設定檔「<name>」，vsys「<id>」，回覆訊息「<msg>」來自：<name>。
auth-fail	使用者「<name>」驗證失敗。領域「<name>」，EAP 外部身分「<name>」，內部身分「<name>」，驗證設定檔「<name>」，vsys「<id>」，伺服器設定檔「<name>」，伺服器位址「<addr>」，管理員角色「<name>」，存取網域「<name>」，回覆訊息「<msg>」來自：<name>。
user-password-change-failed	使用者「<name>」驗證失敗。領域「<name>」，EAP 外部身分「<name>」，內部身分「<name>」，驗證設定檔「<name>」，vsys「<id>」，伺服器設定檔「<name>」，伺服器位址「<addr>」，管理員角色「<name>」，存取網域「<name>」，回覆訊息「<msg>」來自：<name>。
auth-fail	使用者「<name>」Kerberos SSO 驗證失敗。領域「<name>」，EAP 外部身分「<name>」，內部身分「<name>」，驗證設定檔「<name>」，vsys「<id>」，伺服器設定檔「<name>」，伺服器位址「<addr>」，管理員角色「<name>」，存取網域「<name>」，回覆訊息「<msg>」來自：<name>。
user-password-change-failed	使用者「<name>」Kerberos SSO 驗證失敗。領域「<name>」，EAP 外部身分「<name>」，內部身分「<name>」，驗證設定檔「<name>」，vsys「<id>」，伺服器設定檔「<name>」，伺服器位址「<addr>」，管理員角色「<name>」，存取網域「<name>」，回覆訊息「<msg>」來自：<name>。
auth-fail	使用者「<name>」SAML SSO 驗證失敗。領域「<name>」，EAP 外部身分「<name>」，內部身分「<name>」，驗證設定檔「<name>」，vsys「<id>」，伺服器設定檔「<name>」，伺服器位址「<addr>」，管理

©2024 Palo Alto Networks, Inc.

事件 ID	說明
	員角色「<name>」，存取網域「<name>」，回覆訊息「<msg>」來自：<name>。
user-password-change-failed	使用者「<name>」SAML SSO 驗證失敗。領域「<name>」，EAP 外部身分「<name>」，內部身分「<name>」，驗證設定檔「<name>」，vsys「<id>」，伺服器設定檔「<name>」，伺服器位址「<addr>」，管理員角色「<name>」，存取網域「<name>」，回覆訊息「<msg>」來自：<name>。
auth-fail	使用者「<name>」CAS SSO 驗證失敗。領域「<name>」，EAP 外部身分「<name>」，內部身分「<name>」，驗證設定檔「<name>」，vsys「<id>」，伺服器設定檔「<name>」，伺服器位址「<addr>」，管理員角色「<name>」，存取網域「<name>」，回覆訊息「<msg>」來自：<name>。
user-password-change-failed	使用者「<name>」CAS SSO 驗證失敗。領域「<name>」，EAP 外部身分「<name>」，內部身分「<name>」，驗證設定檔「<name>」，vsys「<id>」，伺服器設定檔「<name>」，伺服器位址「<addr>」，管理員角色「<name>」，存取網域「<name>」，回覆訊息「<msg>」來自：<name>。

ddns

事件 ID	說明
ddns-unsupported	主機 <host> 到 <label> (<label>) 的介面 <name> DDNS 設定正在使用不受支援的 DDNS 服務提供者。請轉換為受支援的服務。

dhcp

事件 ID	說明
ip-already-in-use	ip 位址已在使用中
server-no-free-ip	DHCP 伺服器 IP 集區不足

©2024 Palo Alto Networks, Inc.

dns-security

事件 ID	說明
PAN_ELOG_EVENT_DNSSEC_DNS_CLOUD_QUERY_TIMEOUT	DNS 安全性雲端查詢逾時。

dynamic-updates

事件 ID	說明
palo-alto-networks-message	<message>

fips

事件 ID	說明
fips-entropy-rtciid	發生 RTC-IID 錯誤 - 正在嘗試復原...
fips-entropy-rtciid	RTC-IID - 讀取記錄失敗

general

事件 ID	說明
general	CAS 權杖簽署憑證「<name>」無效，錯誤訊息「<msg>」
general	PANDB：驗證或用戶端憑證失敗。
general	PANDB：用戶端憑證已過期或尚未生效。
general	PANDB：裝置用戶端憑證不可用。
general	PANDB：憑證和有效負載中的序號不匹配。
general	PANDB：用戶端憑證已過期。
general	PANDB：用戶端憑證已撤銷。
general	PANDB：原因 - 簽發者未知或者憑證鏈不完整或不正確。
general	MLAV：用戶端憑證已過期或尚未生效。
general	MLAV：裝置用戶端憑證不可用。

©2024 Palo Alto Networks, Inc.

事件 ID	說明
general	MLAV：憑證和有效負載中的序號不匹配。
general	MLAV：用戶端憑證已過期。
general	MLAV：用戶端憑證已撤銷。
general	MLAV：原因 - 簽發者未知或者憑證鏈不完整或不正確。
general	WFRTSIG：驗證或用戶端憑證失敗。
general	WFRTSIG：用戶端憑證已過期或尚未生效。
general	WFRTSIG：裝置用戶端憑證不可用。
general	WFRTSIG：憑證和有效負載中的序號不匹配。
general	WFRTSIG：用戶端憑證已過期。
general	WFRTSIG：用戶端憑證已撤銷。
general	WFRTSIG：原因 - 簽發者未知或者憑證鏈不完整或不正確。
general	伺服器憑證 <name> 無效，其名稱與伺服器 <server> 不匹配
general	伺服器憑證 <name> 對伺服器 <name> 無效：<error>
general	插槽 s<num>：現在無法提供應用程式 Pod '<name> : <namespace>: <interface>'；全部 <num> 個連接埠（<num> 個 pod）都在使用中，等待連接埠可用性（用於 <name>）。
general	無法連接到 wildfire-realtime cloud，請在 30 秒後重試。
general	CONFIG_UPDATE_INC :對 DP 的增量更新失敗，請嘗試 commit force 最新設定
general	向 <name> 伺服器發出的要求傳回 HTTP 回應代碼：<code>

©2024 Palo Alto Networks, Inc.

hw

事件 ID	說明
slot-up	插槽 <id> (PA-7000/5400-100G-NPC) ctd-mode 為 AHO

nat

事件 ID	說明
fallback_report	在 vsys <id> 上，NAT 規則 <name> 中有 <num> 個 NAT DIPP 遞補

ntpd

事件 ID	說明
auth	NTP 與伺服器 <addr> 的同步失敗，驗證類型 autokey
auth	NTP 與伺服器 <addr> 的同步失敗，驗證類型 autokey

port

事件 ID	說明
invalid-module	<name>：需要 SFP+ 模組。
invalid-module	<buf>：需要光纖或銅質 SFP 模組。

routing

事件 ID	說明
routed-static-fqdn-changed	路由靜態 fqdn 對應已變更
routed-static-fqdn-changed	路由靜態 fqdn 對應已變更
routed-BGP-peer-mp-extension-negotiate	BGP 對等 MP 延伸交涉。MP-EXTENSION 交涉到對等名稱：<name>，對等 IP：<ip> 成功"

©2024 Palo Alto Networks, Inc.

事件 ID	說明
routed-BGP-peer-enter-established	BGP 對等工作階段進入已建立狀態。對等名稱：<name>，對等 IP：<ip>
routed-BGP-refresh-sent	ROUTE REFRESH 訊息已傳送到 BGP 對等。對等名稱：<name>，對等 IP：<ip>。
routed-BGP-ribout-recalc	由於匯出政策的變更，正在重新計算 RIB-Out。對等名稱：<name>，對等 IP：<ip>。
routed-BGP-ribin-recalc	由於匯入政策的變更，正在重新計算 RIB-In。對等名稱：<name>，對等 IP：<ip>。

satd

事件 ID	說明
satd-portal-gateway-duplicate	GlobalProtect 入口網站設定重複的閘道。

syslog

事件 ID	說明
syslog-conn-status	<syslog-ng message>

url-filtering

事件 ID	說明
dynamic-url-connection-down	動態 URL 連線不可用，請檢查 service.brightcloud.com (<ip>) 是否可連線
connection-failure	無法連接到 Brightcloud 更新伺服器：無法擷取來源 IP 位址
url-download-failure	在雲端上找不到 URL 雲端清單檔案。
cloud-election	雲端選擇：無法選擇雲端
url-cloud-connection-failure	<num> 次連續嘗試后與雲端開啟連線失敗。
error-msg-from-cloud	來自雲端的錯誤訊息。要求無效。

©2024 Palo Alto Networks, Inc.

事件 ID	說明
error-msg-from-cloud	來自雲端的錯誤訊息。要求無效。
error-msg-from-cloud	來自雲端的錯誤狀態
startup-failure	PAN-DB 引擎啟動失敗。
update-version-failure	更新版本 <version> 失敗。
update-version-failure	更新版本 <version> 失敗。
update-version-failure	更新版本 <version> 失敗。
update-version-failure	更新版本 <version> 失敗。
update-version-failure	更新版本 <version> 失敗。
starts-from-empty-seed	無法載入 URL 種子資料庫，從空白資料庫開始。
ha-sync-failure	無法啟動檔案同步到對等：<error>
url-backup-seed-failure	備份 PAN-DB 失敗
engine-startup-failure	可以在沒有 URL 篩選的情況下執行###
ha-sync-failure	無法將新的HA URL 檔案上傳到 RAM，開始載入舊的 URL 檔案。
starts-from-empty-seed	無法將舊 URL 檔案上傳到 RAM，從空白檔案開始。
engine-startup-failure	在沒有 URL 篩選的情況下執行###
ha-sync-failure	無法從對等 (<name>:<name>) 完全接收檔案：<error>

userid

事件 ID	說明
connect-ldap-sever-failure	ldap cfg <name> 無法連線到伺服器 <server>：<error>

©2024 Palo Alto Networks, Inc.

事件 ID	說明
get-ldap-data-failure	ldap cfg <name> 無法從伺服器 <server> 獲取資訊
connect-ldap-sever-failure	ldap cfg <name> 無法連線到伺服器 <server>：<error>
get-ldap-data-failure	ldap cfg <name> 無法從伺服器 <name> 獲取資訊

wildfire

事件 ID	說明
wildfire-conn-success	已成功註冊到 <description> <name>

Slog

- 佇列「<name>」達到浮水印限制 <num>
- 已移除使用的驗證金鑰「<name>」
- 已移除過期的驗證金鑰「<name>」
- 已刪除驗證金鑰「<name>」
- 已建立驗證金鑰「<name>（計數：<num>，存留時間：< num> 秒，類型：「<type>，Serial-Count：<num>）
- SCP out 部署檔案失敗：「<file>」(rc: <num>)
- SCP out 部署中繼檔失敗：「<file>」(rc: <num>)
- SCP in 部署中繼檔失敗：「<file>」(rc: <num>)
- SCP in 部署檔案失敗：「<file>」(rc: <num>)
- 無法存取威脅資料庫
- 無法將範例上傳到雲端。
- 註冊到雲端失敗。
- 已建立新的裝置憑證「<name>」
- 已建立新憑證「<name>」
- 郵件傳送：<status>
- Tor 狀態已選中並變更為：<name>。
- 無法使用電子郵件設定檔 <name> 傳送測試電子郵件。

©2024 Palo Alto Networks, Inc.

高系統日誌訊息

電子日誌

日誌標籤：

- auth
- bfd
- clusterd
- dhcp
- dns-security
- dynamic-updates
- fips
- general
- globalprotect
- hw
- iot
- ipv6nd
- lldp
- port
- resctrl
- routing
- tls
- url-filtering
- userid
- wildfire

auth

事件 **ID**	訊息
saml-certificate-error	SAML IdP實體 Id 憑證「<name>」未設定，但要求在 IdP 伺服器設定檔「<name>」中對其進行驗證
saml-certificate-error	無法在 vsys <id> 上獲取憑證設定
saml-certificate-error	在 vsys <id> 中找不到 <name> 的憑證

©2024 Palo Alto Networks, Inc.

事件 ID	訊息
saml-certificate-error	無法在實體 ID「<name>」的 IdP 憑證「<name>」中驗證特徵碼
saml-certificate-error	無法在伺服器設定檔「<profile>」中為 IdP 實體 id「<name>」的公開金鑰「<key>」構建 CredentialResolver
saml-certificate-error	無法在伺服器設定檔「<profile>」中為 IdP 實體 id「<id>」的公開金鑰「<key>」轉換一行緩衝區
saml-certificate-error	使用者「<name>」是從 IdP「<name>」的 SAML SSO 回應中擷取的，它不具有在驗證設定檔「<profile>」的伺服器設定檔「<profile>」中設定的憑證
saml-certificate-error	SAML 驗證設定檔「<name>」中的要求簽署憑證（物件名稱：<name>）已過期
saml-certificate-error	IdP 伺服器設定檔「<name>」中 SAML IdP 實體 ID「<name>」的憑證（物件名稱：<name>）已過期
saml-certificate-error	IdP「<name>」沒有憑證，而傳入的 SAML 訊息具有沒有 X509Certificate 的特徵碼
saml-certificate-error	SAML 判斷提示 IdP 憑證「<name>」（用於伺服器設定檔「<name>」）<reason>
saml-certificate-error	SAML 無憑證設定檔設定為檢查 IdP 憑證「<name>」（在伺服器設定檔「<name>」中）的撤銷狀態
saml-certificate-error	沒有為 IdP「<id>」設定 IdP 憑證，傳入訊息中沒有 x509 憑證，無法驗證特徵碼
saml-certificate-error	使用者「<name>」的 SAML <type> 失敗 - 伺服器設定檔「<name>」的 IdP「<id>」憑證「<name>」已過期
saml-certificate-error	來自 IdP「<name>」（驗證設定檔「<name>」）的 SAML <type> 由未知簽署者「<name>」簽署並已被拒絕

©2024 Palo Alto Networks, Inc.

事件 ID	訊息
saml-certificate-error	SAML <type> 失敗 - SAML 驗證設定檔「<name>」的要求簽署憑證「<name>」已過期
saml-certificate-error	SAML 簡單簽署 SAML 訊息失敗（簽署憑證物件：「<name>」）
saml-certificate-error	SAML 簽署 SAML 訊息失敗（簽署憑證物件：「<name>」）
saml-certificate-error	驗證從 IdP「<id>」收到的 SAML 訊息特徵碼時失敗，因為 SAML 訊息中的憑證與 IdP 伺服器設定檔「<profile>」上設定的 IDP 憑證不匹配。（SP：「<type>」），（用戶端 IP：<ip>），（vsys：<id>），（authd id：<id>），（使用者：<name>）
saml-message-parse-error	來自「<name>」的 SAML 判斷提示格式錯誤
saml-message-parse-error	無法將 SAML 訊息有效負載轉換為 xml 樹狀結構
saml-message-parse-error	SAML 判斷提示：InResponseToID "<id>" != OriginalReqID "<id>"
saml-message-parse-error	來自 IdP「<name>」的 SAML 訊息沒有判斷提示
saml-message-parse-error	來自「<name>」的 SAML SSO 回應沒有 usernameattribute 和 saml:Subject NameID 欄位
saml-message-parse-error	username: entered "<name>" != returned "<name>" from IdP "<name>" -> reject SAML auth due to security concerns
saml-message-parse-error	來自「<name>」的 SAML SLO 要求訊息格式錯誤
saml-message-parse-error	SAML 訊息不是 V2.0 的
saml-message-parse-error	SAML 訊息沒有 IssueInstant
saml-message-parse-error	來自 IdP「<id>」的 SAML 訊息沒有 Issuer 節點

©2024 Palo Alto Networks, Inc.

事件 ID	訊息
saml-message-parse-error	來自 IdP「<id>」的 SAML 訊息具有空白 Issuer 節點值
saml-message-parse-error	SAML IdP entityID: parsed "<id>" != configured "<id>"
saml-message-parse-error	SAML SLO 要求訊息沒有特徵碼，但啟用了 validate-idp-certificate
saml-message-parse-error	SAML 訊息沒有 NameID
saml-message-parse-error	SAML 訊息沒有 SessionIndex
saml-message-parse-error	來自「<name>」的 SAML SLO 回應訊息格式錯誤
saml-message-parse-error	SAML SLO：InResponseToID "<name>" != OriginalReqID "<id>"
saml-message-parse-error	SAML SLO 回應狀態：received "<name>" != "urn:oasis:names:tc:SAML:2.0:status:Success"
saml-message-parse-error	SAML SLO 訊息沒有狀態
saml-message-parse-error	SAML 訊息不是版本 2.0
saml-message-parse-error	來自 IdP「<name>」的 SAML 訊息沒有 NameID
saml-message-parse-error	來自 IdP「<name>」SSO 的 SAML 訊息：InResponseToID "<id>" != OriginalReqID "<id>"
saml-message-parse-error	來自 IdP「<name>」的 SAML 訊息沒有主旨
saml-message-parse-error	來自 IdP「<name>」（伺服器設定檔「<name>」）的 SAML 訊息是在未來建立的 (not_before "<time>" - max_clock_skew <num> > now <time>)
saml-message-parse-error	來自 IdP「<name>」（伺服器設定檔「<name>」）的 SAML 訊息已經過期 (not_on_or_after "<time>" + max_clock_skew <num> <= now <time>)

©2024 Palo Alto Networks, Inc.

事件 ID	訊息
saml-message-parse-error	來自 IdP「<name>」的 SAML 訊息沒有條件
saml-message-parse-error	來自 IdP「<name>」的 SAML 訊息沒有 AuthnInstant
saml-message-parse-error	來自 IdP「<name>」的 SAML 訊息沒有 SessionIndex
saml-message-parse-error	來自 IdP「<name>」的 SAML 訊息沒有 AuthnStatement
saml-message-parse-error	來自 IdP「<name>」的 SAML 訊息：擷取 AttributeStatement 時出錯
saml-message-parse-error	無法根據 IdP「<name>」的憑證驗證特徵碼
saml-message-parse-error	對於使用者「<name>」，SAML 訊息沒有來自 IdP「<name>」的特徵碼，其憑證「<name>」在驗證設定檔「<name>」的伺服器設定檔「<name>」中設定
saml-message-parse-error	無法驗證來自 IdP「<name>」的訊息中的 SAML 特徵碼
cas-message	（設定檔 id：<id>）<message>
general	裝置憑證不可用，無法在 vsys「<name>」上啟用雲端驗證設定檔「<name>」
cas-token-invalidated	無法驗證來自「<url>」的用戶端「<name>」的 CAS 權杖，auth_session_id 為「<id>」，使用者名稱為「<name>」
cas-certificate-warning	區域「<name>」中的 CAS 憑證「<name>」已過期
cas-certificate-warning	裝置憑證「<name>」已過期
cas-certificate-warning	區域「<name>」中的 CAS 憑證「<name>」將在 <num> 天后到期
cas-certificate-warning	裝置憑證「<name>」將在 <num> 天后到期

©2024 Palo Alto Networks, Inc.

事件 ID	訊息
saml-certificate-warning	SAML 判斷提示：已根據使用者「<name>」的 IdP 憑證（主旨「<name>」）驗證特徵碼
saml-certificate-warning	SAML 驗證設定檔「<name>」中 IdP 伺服器設定檔「<name>」的憑證「<name>」已過期
saml-certificate-warning	SAML 驗證設定檔「<name>」中的要求簽署憑證「<name>」已過期
saml-certificate-warning	SAML 驗證設定檔「<name>」中 IdP 伺服器設定檔「<name>」的憑證「<name>」將在 <num> 天後到期
saml-certificate-warning	SAML 驗證設定檔「<name>」中的要求簽署憑證「<name>」將在 %d day%s 後到期
cas-certificate-error	裝置憑證「<name>」已過期 <num> 秒

bfd

事件 ID	訊息
admin-down	對於到介面 <name> 上的芳鄰 <name> 的 BFD 工作階段 <name>，BFD 管理關閉。通訊協定：<proto>
expired-time	對於到介面 <name> 上的芳鄰 <name> 的 BFD 工作階段 <name>，BFD 控制偵測時間已過期。通訊協定：<name>
neighbor-down	對於到介面 <name> 上的芳鄰 <name> 的 BFD 工作階段 <name>，BFD 芳鄰已發出工作階段關閉訊號。通訊協定：<name>
session-state-change	對於到介面 <name> 上的芳鄰 <name> 的 BFD 工作階段 <name>，BFD 狀態變更為 <name>。通訊協定：<name>
admin-down	對於到介面 <name> 上的芳鄰 <name> 的 BFD 工作階段 <name>，BFD 管理關閉。通訊協定：<name>

©2024 Palo Alto Networks, Inc.

事件 ID	訊息
admin-down	對於到介面 <name> 上的芳鄰 <name> 的 BFD 工作階段 <name>，BFD 管理關閉。通訊協定：<name>
admin-down	對於到介面 <name> 上的芳鄰 <name> 的 BFD 工作階段 <name>，BFD 管理關閉。通訊協定：<name>

clusterd

事件 ID	訊息
cluster-daemon-cfg-giveup	叢集精靈無法從 cfgagent 獲取最後的 cfg。重試次數不足。
cluster-other-ip-incompatible	對等節點 IP 與當前叢集介面 IP 不相容

dhcp

事件 ID	訊息
if-update-fail	DHCP <desc>：介面 <name>，dhcp 伺服器：<name>
if-update-fail	DHCP <name>：介面 <name>，IP <ip> 網路遮罩 <mask> dhcp 伺服器：<name>

dns-security

事件 ID	訊息
PAN_ELOG_EVENT_DNSSEC_DNS_CLOUD_CONNECTION_NOHOST	DNS 安全性雲端服務 DNS 解析失敗。
PAN_ELOG_EVENT_DNSSEC_DNS_CLOUD_CONNECTION_NOROUTE	DNS 安全性雲端服務網路連線失敗。
PAN_ELOG_EVENT_DNSSEC_DNS_CLOUD_CONNECTION_REFUSED	DNS 安全性雲端服務連線被拒絕。
PAN_ELOG_EVENT_DNSSEC_DNS_CLOUD_DOWN	DNS 安全性雲端服務不可用。

dynamic-updates

©2024 Palo Alto Networks, Inc.

事件 ID	訊息
palo-alto-networks-message	<message>

fips

事件 ID	訊息
fips-zeroization	檔案歸零錯誤：<error>
fips-zeroization	Ram 歸零錯誤

general

事件 ID	訊息
general	對 CURLOPT_WRITEDATA 設定 fd = <id> 時出錯（代碼：<id>；訊息：<msg>）
general	從「<name>」擷取 CRL 時出錯（代碼：<id>；訊息：<msg>）（curl 逾時設定：<num> 秒）
general	從「<name>」載入 CRL 時出錯
general	
general	剖析 CRL 失敗 <name>（原因：<reason>）
general	向伺服器「<url>」發出的要求傳回 HTTP 回應代碼：<id>
general	向伺服器「<url>」發出的要求傳回 HTTP 回應代碼：<id>
general	<name> 的機器學習引擎已停止，請更新您的內容
general	MLAV 雲端錯誤，所有機器學習引擎都已停止
bootstrap-failure	無法處理來自啟動載入裝置 <name> 的註冊，因為在要求中找不到 vm-auth-key。
bootstrap-failure	無法處理來自啟動載入裝置 <name> 的註冊，因為 vm-auth-key <name> 無效。

©2024 Palo Alto Networks, Inc.

事件 ID	訊息
tac-login	來自 <ip> 的 <name> 的 TAC 偵錯存取失敗

globalprotect

事件 ID	訊息
globalprotectgateway-invalid-license	GlobalProtect 訂閱授權已過期。請登入客戶支援入口網站啟用授權，以繼續使用 GlobalProtect 功能。

hw

事件 ID	訊息
bootstrap-license-failure	無法使用驗證碼 <id> 安裝授權
slot-unsupported	當工作階段分發政策設定為 ingress-slot 時，不會使用插槽 <id> (<model>)。工作階段分發政策必須設定為除 ingress-slot 之外的某個值。
bootstrap-license-failure	無法為檔案 <name> 安裝授權金鑰
bootstrap-license-failure	無法使用驗證碼 <name> 安裝授權
bootstrap-content-failure	iot 映像無效。無法獲取檔案 <name> 的主要版本、次要版本和摘要
bootstrap-content-failure	映像無效。無法獲取檔案 <name> 的主要版本、次要版本和摘要
bootstrap-content-failure	映像無效。無法獲取檔案 <name> 的主要版本、次要版本和摘要
bootstrap-content-failure	映像無效。無法獲取檔案 <name> 的主要版本、次要版本和摘要
bootstrap-content-failure	無法為檔案 <name> 排程內容安裝作業
bootstrap-content-failure	無法安裝內容。<error>

iot

©2024 Palo Alto Networks, Inc.

事件 ID	訊息
ha-queue-full	HA 佇列已滿

ipv6nd

事件 ID	訊息
inconsistent-ra-message-received	從介面 <name> 上的位址 <ip> 收到不一致的路由器公告。

lldp

事件 ID	訊息
tooManyNeighbors 計時器已清除	對於介面 <index> 上的 <xx>:<xx>:<xx>:<xx>:<xx>:<xx>，TooManyNeighbors 錯誤已清除
tx error	對於 TLV <index> 的介面 <index> 上的 <xx>:<xx>:<xx>:<xx>:<xx>:<xx>，收到錯誤
rx error	對於 TLV <index> 的介面 <index> 上的 <xx>:<xx>:<xx>:<xx>:<xx>:<xx>，收到錯誤
芳鄰過多	達到最大 MIB 大小：對於介面 <index> 上的 <xx>:<xx>:<xx>:<xx>:<xx>:<xx>，LLDP 芳鄰新增失敗

port

事件 ID	訊息
link-change	連接埠 MGT：關閉 <type>

resctrl

事件 ID	訊息
mem-limit-exceeded	超出記憶體限制。cgroup_name <name> memsw_limit_in_bytes <num> memsw_usage_in_bytes <num>

routing

 ©2024 Palo Alto Networks, Inc.

事件 ID	訊息
routed-BGP-peer-left-established	BGP 對等工作階段離開已建立狀態。對等名稱：<name>，對等 IP：<ip>
routed-BGP-peer-restarted	已啟動 BGP 對等的非失誤性重新啟動。對等名稱：<name>，對等 IP：<ip>
routed-BGP-peer-prefix-exceeded	BGP 對等公告的首碼超過最大允許首碼。對等名稱：<name>，對等 IP：<ip>
route-table-capacity	已達到路由表容量。
routed-BGP-peer-left-established	BGP 對等工作階段離開已建立狀態。
routed-OSPF-neighbor-down	與芳鄰的 OSPF 鄰接關係已關閉。
routed-RIP-peer-del	RIP 對等消失。

tls

事件 ID	訊息
tls-X509-validation-failed	<name> 伺服器憑證驗證失敗。目的地位址：<address>，原因：<reason>
tls-X509-validation-failed	<name> 伺服器憑證驗證失敗

url-filtering

事件 ID	訊息
url-download-failure	PAN-DB 雲端清單載入失敗（錯誤：<error>）。
url-download-failure	從主要雲端下載雲端清單失敗。
url-cloud-connection-failure	URL 雲端清單為空。"無法啟動雲端連線。
url-cloud-connection-failure	無法開啟檔案 /opt/pancfg/opt/pan/content/pan/urlcloud_list.txt. errno=<error>
url-cloud-connection-failure	無法向雲端傳送更新要求
url-cloud-connection-failure	雲端未就緒，未經處理的免費 <num> 要求。

©2024 Palo Alto Networks, Inc.

事件 ID	訊息
url-cloud-connection-failure	雲端未就緒，在過去 <num> 分鐘內沒有來自雲端的更新。
url-cloud-connection-failure	雲端連線：雲端未就緒
update-version-failure	更新 DP 失敗，更新版本 <name>
update-version-failure	更新版本 <version> 失敗。
update-version-failure	更新版本 <version> 失敗。
update-version-failure	更新版本 <version> 失敗。
update-version-failure	更新版本 <version> 失敗。
seed-out-of-sync	PAN-DB sw <version> 與雲端 sw <version> 不相容，需要升級 sw###
url-cloud-connection-failure	無法建立雲端連線代理程式。

userid

事件 ID	訊息
connect-agent-failure	User-ID 代理程式對等的憑證 RSA 公開金鑰大小小於 2048 位元
connect-agent-failure	User-ID 代理程式 X509_verify_cert 傳回錯誤 <id>，錯誤 = '<error>'
connect-agent-failure	User-ID 代理程式伺服器憑證已撤銷/無效
connect-agent-failure	User-ID 代理程式憑證名稱驗證失敗
connect-agent-failure	重新分配代理程式 <name>(vsys<id>)：<status> 詳細資訊：關閉與代理程式的連線
user-group-count	<num> 的使用者群組計數超過閾值 <num>
connect-vm-info-source-failure	vm-info-source <name>(vsys<id>)：連接至 <host> 失敗，狀態 <message>
connect-agent-failure	<agent> <name>(vsys<id>): <status> 詳細資料：<details>

©2024 Palo Alto Networks, Inc.

事件 ID	訊息
HA-queue-full	HA 佇列已滿
HA-queue-full	CFG HA 佇列已滿
connect-agent-failure	User-ID 代理程式對等的憑證 RSA 公開金鑰大小小於 2048 位元
connect-agent-failure	User-ID 代理程式 X509_verify_cert 傳回錯誤 <num> 錯誤 = '<error>'
connect-agent-failure	User-ID 代理程式憑證名稱驗證失敗
connect-agent-failure	User-ID 代理程式伺服器憑證已撤銷/無效
connect-agent-failure	User-ID 代理程式對等的憑證 RSA 公開金鑰大小小於 2048 位元
connect-agent-failure	User-ID 代理程式 X509_verify_cert 傳回錯誤 <num> 錯誤 = '<error>'
connect-agent-failure	User-ID 代理程式憑證名稱驗證失敗
connect-agent-failure	User-ID 代理程式伺服器憑證已撤銷/無效
connect-agent-failure	User-ID 代理程式伺服器憑證已撤銷/無效
connect-agent-failure	User-ID 代理程式對等的憑證 RSA 公開金鑰大小小於 2048 位元
connect-agent-failure	User-ID 代理程式 X509_verify_cert 傳回錯誤 <num>，錯誤 = '<error>'
connect-agent-failure	User-ID 代理程式憑證名稱驗證失敗
connect-server-monitor-failure	User-ID 伺服器監控 <name>(vsys<id>) <status>
connect-server-monitor	User-ID WinRM 伺服器監控 <name>(vsys<id>)：憑證 RSA 公開金鑰大小小於 2048 位元
connect-server-monitor	User-ID WinRM X509_verify_cert 傳回錯誤 <num> 錯誤 = '<error>'
connect-server-monitor	User-ID WinRM 憑證名稱驗證失敗

©2024 Palo Alto Networks, Inc.

事件 ID	訊息
connect-server-monitor	User-ID WinRM 伺服器憑證已撤銷/無效
connect-server-monitor-failure	伺服器監控 <name>(vsys<id>)：連線失敗，<error>
connect-vm-info-source-failure	vm-info-source <name>(vsys<id>)：連接至 <host> 失敗，狀態 <status>
connect-vm-info-source-failure	vm-info-source <name>(vsys<id>)：連接至 <host> 失敗，狀態 <status>
connect-vm-info-source-failure	vm-info-source <name>(vsys<id>)：連接至 GCE 失敗，狀態 <status>
connect-vm-info-source-failure	vm-info-source <name>(vsys<id>)：連接至 <host> 失敗，狀態 <status>

wildfire

事件 ID	訊息
wildfire-auth-failed	WildFire 無法擷取決策。驗證或用戶端憑證失敗。
wildfire-auth-failed	WildFire 無法傳送查詢。驗證或用戶端憑證失敗。
wildfire-disabled-by-cloud	WildFire 無法傳送查詢。用戶端憑證已過期或尚未生效。
wildfire-auth-failed	WildFire 無法傳送查詢。"驗證或用戶端憑證失敗。
wildfire-invalid-cloud-info	WildFire <name> 通道註冊收到無效的雲端資訊。varrcvr.log 中的詳細資料。
wildfire-no-license	由於 WildFire 授權無效，WildFire <name> 通道註冊失敗。
wildfire-wrong-cloud-type	WildFire 註冊失敗。<name> 通道不允許雲端類型 <type> (<name>)。
wildfire-auth-failed	WildFire 註冊失敗。驗證或用戶端憑證失敗。

©2024 Palo Alto Networks, Inc.

事件 ID	訊息
wildfire-auth-failed	WildFire 註冊失敗。憑證和有效負載中的序號不匹配。
wildfire-no-policy	WildFire <name> 通道停用。"無效的 <name> 雲端伺服器設定「<name>」。

Slog

- 智慧卸載中的 GRPC 狀態 DEADLINE_EXCEEDED
- PA-5220 的 40G（連接埠 <num>）不支援插入的 100G QSFP28 模組"（廠商「<name>」；部件「<name>」；id「<id>」）。
- 啟動時未找到有效的資料平面連接埠。
- 無法在資料平面中安裝 SSL 輸入憑證。
- 偵測到記憶體錯誤。
- <name>偵測到磁碟機錯誤。
- 空間不足，無法將內容載入 SHM
- device-server HA 佇列已滿
- GlobalProtect 資料檔案版本 <version> 安裝版本失敗
- 由於日誌轉送失敗，磁碟上的提示數已超過 <num>。
- 已建立 CSR 憑證「<name>」
- 刪除憑證「<name>」
- 已建立 CA 憑證「<name>」
- 已為裝置「<name>」簽署憑證「<name>」
- 已為裝置「<name>」簽署更新憑證「<name>」
- SC3 裝置憑證狀態已重設#
- 已嘗試修復磁碟分割 <name>如果遇到任何問題，建議更新此磁碟分割
- 已達到每日封包擷取限制（目錄 <name> 限制 <num>）。
- 無法獲取區域的執行個體/網域
- 無法獲取區域的屬性：%s instance:%s
- 無法獲取所有區域
- dsc HA 狀態從 %d 變更為 %d
- DPI：EAL 訊息格式變更為 Json[prev: %d]
- DPI：EAL 訊息格式變更為 protobuf[prev: %d]

©2024 Palo Alto Networks, Inc.

嚴重系統日誌訊息

電子日誌

日誌標籤：

- auth
- bfd
- crypto
- dhcp
- dynamic-updates
- fips
- general
- gre
- hw
- ipv6nd
- lacp
- panorama-check
- pbf
- raid
- routing
- satd
- sdwan
- tls
- url-filtering
- userid
- uuid
- vm
- vpn
- wildfire-appliance

auth

事件 ID	訊息
auth-server-down	3 次嘗試繫結回 binddn 失敗：basedn: <name> ; binddn: <name> ; bind_timelimit <num> ; ip: <ip> ; uri: <url>

©2024 Palo Alto Networks, Inc.

事件 ID	訊息
edl-cli-auth-failure	EDL 伺服器憑證驗證失敗。關聯的外部動態清單已被移除，這可能會影響您的政策。EDL 名稱：<name>，EDL 來源 URL：<url>，CN：<name>，原因：<reason>
auth-server-up	<name> 驗證伺服器 <name> 啟動###
auth-server-down	<name> 驗證伺服器 <name> 關閉###
create-admin-acct-error	無法為管理員使用者建立本機使用者帳戶：<name>
auth-success	驗證使用者「<name>」<remotehost> 時，使用了一種不太安全的驗證方法 <proto>。請移轉到 PEAP 或 EAP-TTLS。驗證設定檔「<name>」，vsys「<name>」，伺服器設定檔「<name>」，伺服器位址「<ip>」
user-password-change-failed	驗證使用者「<name>」<remotehost> 時，使用了一種不太安全的驗證方法 <proto>。請移轉到 PEAP 或 EAP-TTLS。驗證設定檔「<name>」，vsys「<name>」，伺服器設定檔「<name>」，伺服器位址「<ip>」

bfd

事件 ID	訊息
session-state-change	對於到介面 <name> 上的芳鄰 <name> 的 BFD 工作階段 <name>，BFD 狀態變更為 <name>。通訊協定：<name>
forward-plane-reset	對於到介面 <name> 上的芳鄰 <name> 的 BFD 工作階段 <name>，BFD 轉送平面已重設。通訊協定：<name>

crypto

事件 ID	訊息
mkey-expiry-reminder	主要金鑰將在 <num> 天 <num> 小時 <num> 分 <num> 秒後到期

©2024 Palo Alto Networks, Inc.

事件 ID	訊息
mkey-expiry	主要金鑰已過期。已啟用自動更新主要金鑰存留期。將存留期延長 <num> 天 <num> 小時
mkey-expiry	主要金鑰現已過期
cert-expiry	共用憑證 <name> 和相應的金鑰已過期
cert-expiry	憑證 <name> 和 vsys <num> 中的相應金鑰已過期
HSM-state-change	HSM 連線已啟動。伺服器 <ip>
HSM-state-change	HSM 連線已關閉。伺服器 <ip>
HSM-state-change	HSM 連線已關閉。
deploy-mkey-change	已嘗試在 <num> 台裝置上部署主要金鑰工作
private-key-export	私密金鑰 <entry> 已由使用者 <name> 匯出
mkey-change	主要金鑰已由 <name> 變更。
mkey-change	<name> 變更主要金鑰失敗
mkey-change	主要金鑰加密層級已由 <name> 變更
mkey-change	<name> 變更主要金鑰加密層級失敗

dhcp

事件 ID	訊息
if-clear	DHCP 用戶端清除了介面 <name> 上的 IP 位址，原因為：設定已移除
if-clear	DHCP 用戶端清除了介面 <name> 上的 IP 位址，原因為：租用到期
if-clear	DHCP 用戶端清除了介面 <name> 上的 IP 位址，原因為：發行觸發程序
if-clear	DHCP 用戶端清除了介面 <name> 上的 IP 位址，原因為：所有要求重試次數都已耗盡。

©2024 Palo Alto Networks, Inc.

事件 ID	訊息
if-clear	DHCP 用戶端清除了介面 <name> 上的 IP 位址，原因為：來自伺服器的 NAK
if-clear	DHCP 用戶端清除了介面 <name> 上的 IP 位址，原因為：由於內部錯誤啟動發布。請檢查重複的 IP 或重疊的子網路。
if-clear	DHCP 用戶端清除了介面 <name> 上的 IP 位址，原因為：<reason>

dynamic-updates

事件 ID	訊息
palo-alto-networks-message	<message>

fips

事件 ID	訊息
fips-selftest	FIPS 模式自檢 <description> ..... 成功
fips-selftest	FIPS-CC 模式自檢 <description> ..... 成功
fips-selftest	FIPS-CC 自檢失敗。進入錯誤狀態。
fips-selftest	FIPS-CC 自檢失敗。進入錯誤狀態。
fips-entropy-rtciid	RTC-IID 持續失敗 - 正在重新啟動...
fips-selftest-timeout	FIPS 故障。<description> 失敗。
fips-selftest-integ	FIPS 故障。<description> 失敗。
fips-selftest-drng	FIPS 故障。<description> 失敗。
fips-selftest-ndrng	FIPS 故障。<description> 失敗。
fips-selftest-sha	FIPS 故障。<description> 失敗。
fips-selftest-hmac	FIPS 故障。<description> 失敗。
fips-selftest-aes	FIPS 故障。<description> 失敗。

©2024 Palo Alto Networks, Inc.

事件 ID	訊息
fips-selftest-des	FIPS 故障。<description> 失敗。
fips-selftest-rsa	FIPS 故障。<description> 失敗。
fips-selftest-dsa	FIPS 故障。<description> 失敗。
fips-selftest-dh-parameter	FIPS 故障。<description> 失敗。
fips-selftest-dh	FIPS 故障。<description> 失敗。
fips-selftest-cmac	FIPS 故障。<description> 失敗。
fips-selftest-drbg	FIPS 故障。<description> 失敗。
fips-selftest-ecdsa	FIPS 故障。<description> 失敗。
fips-selftest-ecdh	FIPS 故障。<description> 失敗。
fips-selftest-timeout	FIPS-CC 故障。<description> 失敗。
fips-selftest-integ	FIPS-CC 故障。<description> 失敗。
fips-selftest-drng	FIPS-CC 故障。<description> 失敗。
fips-selftest-ndrng	FIPS-CC 故障。<description> 失敗。
fips-selftest-sha	FIPS-CC 故障。<description> 失敗。
fips-selftest-hmac	FIPS-CC 故障。<description> 失敗。
fips-selftest-aes	FIPS-CC 故障。<description> 失敗。
fips-selftest-des	FIPS-CC 故障。<description> 失敗。
fips-selftest-rsa	FIPS-CC 故障。<description> 失敗。
fips-selftest-dsa	FIPS-CC 故障。<description> 失敗。
fips-selftest-dh-parameter	FIPS-CC 故障。<description> 失敗。
fips-selftest-dh	FIPS-CC 故障。<description> 失敗。
fips-selftest-cmac	FIPS-CC 故障。<description> 失敗。
fips-selftest-drbg	FIPS-CC 故障。<description> 失敗。

©2024 Palo Alto Networks, Inc.

事件 ID	訊息
fips-selftest-ecdsa	FIPS-CC 故障。<description> 失敗。
fips-selftest-ecdh	FIPS-CC 故障。<description> 失敗。
fips-selftest-core	<num> 的 <num> 資料平面處理器核心驗證失敗。

general

事件 ID	訊息
general	插槽 s<num>：檢查/修復磁碟區「appinfo」路徑未找到預期的目錄。

gre

事件 ID	訊息
tunnel-recur-routing	通道 intf: <name> 由於遞迴路由而正在關閉
tunnel-status-down	通道 <name> 由於通道監控失敗而正在關閉
tunnel-status-up	通道 <name> 正在啟動

hw

事件 ID	訊息
fan-failure	風扇托盤 #<num> 上的警報
ps-failure	電源 #<num> 上的報警
內容引擎故障	CE10 初始化失敗。
內容引擎故障	CA1 初始化失敗。
insufficient-power	DP 電源狀態不良，正在關閉系統#
insufficient-power	CP 電源狀態不良#

ipv6nd

©2024 Palo Alto Networks, Inc.

事件 ID	訊息
duplicated-IPv6-address-found	介面 <name> 上 IPv6 位址 <address> 重複。已在介面上停用 IPv6。
duplicated-IPv6-address-found	介面 <name> 上 IPv6 位址 <address> 重複。位址已停用。

lacp

事件 ID	訊息
lacp-up	LACP 介面 <name> 已移動至 AE 群組 <name>。
nego-fail	LACP 介面 <name> 已從 AE 群組 <name. Selection state <state> 移出
lost-connectivity	LACP 介面 <name> 已從 AE 群組 <name> 移出（失去已現有對等的連線。最後連接的對等連接埠號 <port>）
unresponsive	LACP 介面 <name> 已從 AE 群組 <name> 移出（對等未回應新 LACP 連線）
speed-duplex	LACP 介面 <name> 已從 AE 群組 <name> 移出。選取狀態 <state>
link-down	LACP 介面 <name> 已從 AE 群組 <name> 移出。選取狀態 <state>
link-down	LACP 介面 <name> 已從 AE 群組 <name> 移出（連結狀態被手動設定為關閉）
nego-fail	LACP 介面 <name> 已從 AE 群組 <name> 移出。選取狀態 <state>
lacp-down	LACP 介面 <name> 已從 AE 群組 <name> 移出。選取狀態 <state>

panorama-check

©2024 Palo Alto Networks, Inc.

事件 ID	訊息
panorama-check-test	<name> 的 Panorama 連線能力檢查失敗。原因：<reason>
panorama-check-test	<name> 的 Panorama 連線能力檢查失敗。原因：<reason>

pbf

事件 ID	訊息
pbf-fqdn-down	沒有針對 IPv4 解析 Vsys <id> PBF 規則 <name> nexthop FQDN <key>
pbf-fqdn-down	沒有針對 IPv6 解析 Vsys <id> PBF 規則 <name> nexthop FQDN <key>
pbf-fqdn-down	Vsys <id> PBF 規則 <name> nexthop FQDN <key> 解析 IP <ip> 與介面 IP 不在同一子網路中。它不會用作 FQDN nexthop。

raid

事件 ID	訊息
pair-disappeared	沒有可用的記錄 Raid 磁碟對通知 HA
pair-detected	沒有可用的記錄 Raid 磁碟對通知 HA

routing

事件 ID	訊息
routed-static-fqdn-down	路由的靜態 fqdn 對應未解析
routed-bgp-fqdn-down	路由的 BGP fqdn 對應未解析
path-monitor-recovery	具有下一個躍點 <name> 的靜態路由目的地 <ip> 的路徑監控已復原。路由已還原。
path-monitor-failure	具有下一個躍點 <name> 的靜態路由目的地 <ip> 的路徑監控失敗。路由已移除。

©2024 Palo Alto Networks, Inc.

satd

事件 ID	訊息
satd-portal-connect-failed	GlobalProtect 衛星連線到入口網站失敗。
satd-gateway-connect-failed	GlobalProtect 衛星連線到閘道失敗。

sdwan

事件 ID	訊息
sdwan-vif-status-up	<vif> 啟動
sdwan-vif-status-down	<vif> 關閉

tls

事件 ID	訊息
panos-auth-failure	RADIUS 伺服器認證失敗。伺服器：<name>；CRL/OCSP 失敗，<reason>
tls-edl-auth-failure	EDL 伺服器憑證驗證失敗。將使用關聯的外部動態清單的本機複本，因此不會影響您的政策。EDL 名稱：<name>，EDL 來源 URL：<url>，CN：<name>，原因：<reason>
tls-edl-auth-failure	EDL 伺服器憑證驗證失敗。關聯的外部動態清單已被移除，這可能會影響您的政策。EDL 名稱：<name>，EDL 來源 URL：<url>，CN：<name>，原因：CRL/OCSP 檢查失敗，<reason>
panos-auth-failure	<name> 伺服器 CN：<name> 未能建立連線，原因為 <error>
panorama-auth-failure	用戶端驗證失敗 <error> PPAN-OS 版本：<version> Panorama 版本：<version>用戶端 ID：<ip> 伺服器 IP：<ip> 用戶端憑證 CN：<name>
panorama-auth-failure	用戶端身分檢查失敗。PAN-OS 版本：<version> Panorama 版本：<version> 用

©2024 Palo Alto Networks, Inc.

事件 ID	訊息
	戶端 IP：<ip> 伺服器 IP：<ip> 用戶端憑證 CN：<name>
tls-X509-ocsp-crl-check-failed	連線到 HTTP 伺服器 (<host>) 失敗，原因為伺服器憑證「<name>」是 <reason>
tls-X509-validation-failed	HTTP 伺服器憑證驗證失敗。主機：<host>，CN：<name>，原因：<reason>
mfa-auth-failure	MFA 伺服器認證失敗。伺服器：<name>；CRL/OCSP 失敗，<reason>
mfa-auth-failure	MFA：伺服器憑證驗證失敗。對等：「<name>」Vsys：<id> (<id>:<error>)
panorama-auth-failure	用戶端驗證失敗 <error> 用戶端 IP：<ip>:<port>伺服器 IP：<ip>:<port>用戶端憑證 CN：<name>
tls-X509-ocsp-crl-check-failed	連線到 EMAIL 伺服器 (<host>) 失敗，原因為伺服器憑證「<subject>」是 <reason>
tls-X509-validation-failed	EMAIL 伺服器憑證驗證失敗。主機：<host>，CN：<name>，原因：<reason>

url-filtering

事件 ID	訊息
no-url-database	沒有 URL 資料庫#請從「動態更新頁面」下載一個
seed-out-of-sync	PAN-DB 種子不同步。需要下載新種子###
startup-failure	構建 URL 資料庫失敗#

userid

事件 ID	訊息
registered-ip-max-platform-limit-exceeded	已達到平台的最大註冊 IP 數（<num>)

©2024 Palo Alto Networks, Inc.

事件 ID	訊息
registered-ip-update-failure	自 <num> 秒前開始，無法整合已註冊 IP 位址的更新
registered-ip-update-failure	無法同步已註冊 IP 位址的更新
registered-ip-update-failure	在經過 <num> 次重試後，NSX 對 ip-tag 對應的初始同步請求失敗。建議從 panorama 手動同步。
registered-ip-update-failure	無法同步已註冊 IP 位址的更新
registered-user-max-platform-limit-exceeded	達到註冊使用者總數的限制 (<num>)
agent-version-mismatch	裝置需要通訊協定版本 <num>，但 <name> 僅支援版本 <num>

uuid

事件 ID	訊息
policy-rule-uuid-modified	政策規則 UUID 透過使用「為所選命名設定重新產生規則 UUID」選項載入進行修改

vm

事件 ID	訊息
dvf-init-fail	VMware dvfilter init failed <status> <id>
dvf-init-fail	VMware dvfilter init dev failed <status> devId <id> status <id>

vpn

事件 ID	訊息
ikev2-nego-cert-id-mismatch	IKEv2 SA 交涉失敗。
ike-nego-p1-fail-common	IKE phase-1 negotiation is failed_COMM
ikev2-nego-ike-fail	IKEv2 IKE SA 交涉失敗
tunnel-status-up	通道 <name>（id：<id>，對等：<peer>）啟動

©2024 Palo Alto Networks, Inc.

事件 ID	訊息
tunnel-status-down	通道 <name>（id：<id>，對等：<peer>）關閉
tunnel-status-up	通道 <name> 啟動
tunnel-status-down	通道 <name> 關閉

wildfire-appliance

事件 ID	訊息
cluster-entered-split-brain	叢集進入核心分裂模式。
cluster-entered-split-brain	叢集離開核心分裂模式。
cluster-entered-split-brain	叢集離開核心分裂模式。

Slog

- 底座主機警報：已清除
- 底座主機警報：<name>
- 風扇托架 <id>，風扇 <id> 失敗#
- 風扇區域 <id> 失敗，正在關閉#
- 風扇托架 <id>，風扇 <id> 失敗#
- 風扇區域 <id> 失敗，正在關閉#
- 由於缺少風扇托架，系統正在自行關閉。
- 沒有可用的 Raid 磁碟對，正在重新啟動#
- 插槽 <id> 上的高溫警報
- 正在因溫度過高而關閉系統。
- 正在因插槽 <id> 溫度過高而關閉系統。
- 正在因溫度過高而關閉插槽 <id>。
- SW 版本不匹配，MP 軟體版本 <version>，DP 軟體版本 <version>
- 釋放插槽失敗。
- 插槽配置失敗
- 已成功更新裝置憑證
- 已成功移除裝置憑證
- 偵測到記憶體不足情況，終止程序 <id>
- 裝置憑證狀態：<num>。無法更新

©2024 Palo Alto Networks, Inc.

- LP shmgr 記憶體對應不同步
- 智慧型流量卸載授權已過期
- 使用者 ID 管理器已重設。需要提交才能重新初始化使用者 ID
- 流量和日誌記錄已還原
- 由於未匯出的日誌，流量和日誌記錄暫停
- 由於 traffic-stop-on-logdb-full 功能已啟用，流量和日誌記錄已暫停
- <name> 日誌的稽核儲存區已滿。在釋放磁碟空間之前，不會接受新的流量工作階段
- 最短保留期（<num> 天）違反 segnum：<num> 類型：<name>

©2024 Palo Alto Networks, Inc.

SNMP 監控和設陷

下列主題會說明 Palo Alto Networks 防火牆、Panorama 和 WF-500 裝置如何實作 SNMP 以及設定 SNMP 監控和設陷傳遞的程序。

- SNMP 支援
- 使用 SNMP 管理員探索 MIB 和物件
- 啟用防火牆保護網路元素的 SNMP 服務
- 使用 SNMP 監控統計資料
- 將設陷轉送至 SNMP 管理員
- 支援的 MIB

SNMP 支援

您可以使用 SNMP 管理員，監控防火牆、Panorama 或 WF-500 裝置及其處理之流量的事件導向警示和操作統計資料。統計資料和設陷可協助您識別資源限制、系統變更或失敗，以及惡意軟體攻擊。您可以透過設陷形式轉送日誌資料來設定警示，並在回應來自 SNMP 管理員的 GET 訊息（要求）時傳送統計資料。每個設陷和統計資料都具有物件識別碼 (OID)。在載入至 SNMP 管理員以進行監控的管理資訊庫 (MIB) 中，其會以階層的方式組織相關 OID。

當事件觸發 *SNMP* 設陷產生（例如介面關閉）時，防火牆、*Panorama* 虛擬裝置、*M* 系列裝置及 *WF-500* 裝置會透過更新相應的 *SNMP* 物件（例如介面 *MIB*）而非等待每十秒鐘發生的所有物件的定期更新來作出回應。這可確保，*SNMP* 管理員在輪詢物件以確認事件時顯示最新資訊。

防火牆、Panorama 和 WF-500 裝置支援 SNMP 版本 2c 和版本 3。請根據網路中其他設備支援的版本和網路安全性需求，決定要使用的版本。相較於 SNMPv2c，SNMPv3 是更安全且具有更精確的系統統計資料存取控制。下表摘要每個版本的安全性功能。您需選取版本並設定使用 SNMP 監控統計資料以及將設陷轉送至 SNMP 管理員時的安全性功能。

SNMP版本	驗證	訊息隱私	訊息完整性	**MIB** 存取細微性
SNMPv2c	社群字串	無 (純文字)	否	設備上所有 MIB 的 SNMP 社群存取
SNMPv3	EngineID、使用者名稱和驗證密碼（密碼的 SHA 雜湊）	SNMP 訊息 AES（128、192 或 256）加密的私人密碼	是	根據包含或排除特定 OID 檢視的使用者存取

©2024 Palo Alto Networks, Inc.

SNMP 實作中介紹了一種部署，其中防火牆將設陷轉送至 SNMP 管理員，並同時將日誌轉送至日誌收集器。或者，您可以設定日誌收集器以將防火牆設陷轉送至 SNMP 管理員。關於這些部署的詳細資訊，請參閱集中日誌記錄與報告中的日誌轉送選項。在所有部署中，SNMP 管理員會直接從防火牆、Panorama 或 WF-500 裝置中取得統計資料。雖然如果針對這些功能使用個別管理員更適合您的網路，您可以透過此方法使用管理員，但在此範例中，單一 SNMP 管理員會同時收集設陷和統計資料。

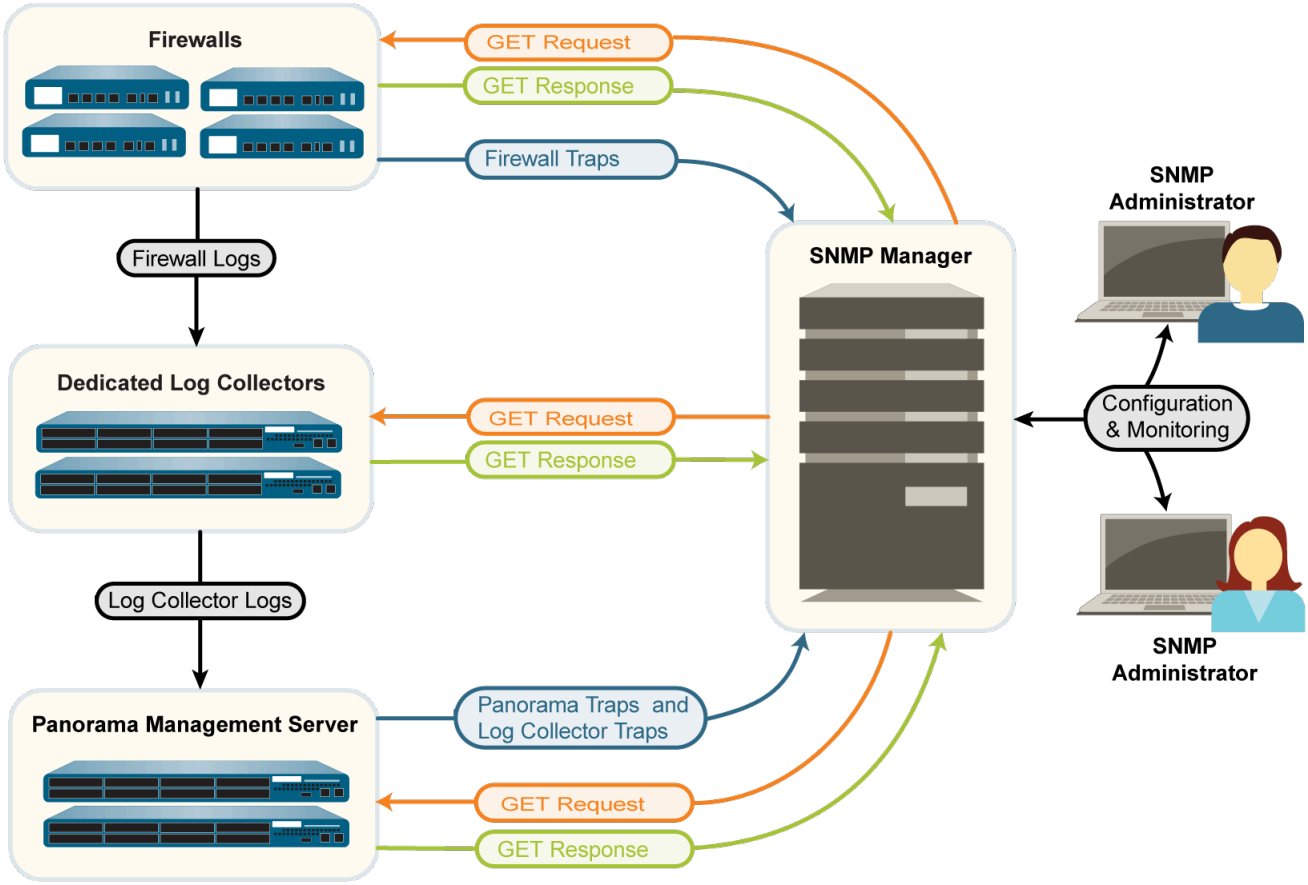


圖 **2: SNMP** 實作

使用 SNMP 管理員探索 MIB 和物件

若要使用 SNMP 監控 Palo Alto Networks 防火牆、Panorama 或 WF-500 裝置，您必須先將支援的 MIB 載入至 SNMP 管理員，並確定哪些物件識別碼 (OID) 對應於要監控之系統統計資料和設陷。下列主題提供如何在 SNMP 管理員中尋找 OID 和 MIB 的概要。如需執行這些工作的特定步驟，請參閱 SNMP 管理軟體。

- 識別包含已知 OID 的 MIB
- 執行 MIB
- 識別系統統計資料或設陷的 OID

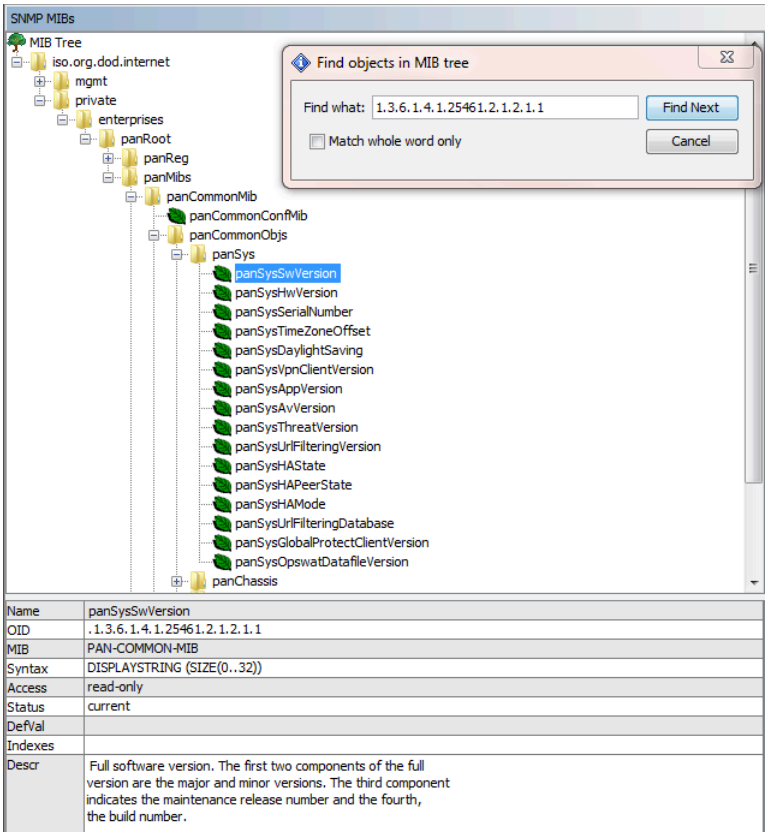
©2024 Palo Alto Networks, Inc.

識別包含已知 OID 的 MIB

如果您已知道特定 SNMP 物件（統計資料或設陷）的 OID，且想知道類似物件的 OID 以進行監控，則可以探索包含已知 OID 的 MIB。

STEP 1 | 將所有 支援的 MIB 載入至 SNMP 管理員。

STEP 2 | 搜尋整個 MIB 樹狀結構中是否存在已知 OID。搜尋結果會顯示 OID 的 MIB 路徑，以及 OID 的相關資訊（例如，名稱、狀態和說明）。然後您可以在相同 MIB 中選取其他 OID 以查看其相關資訊。

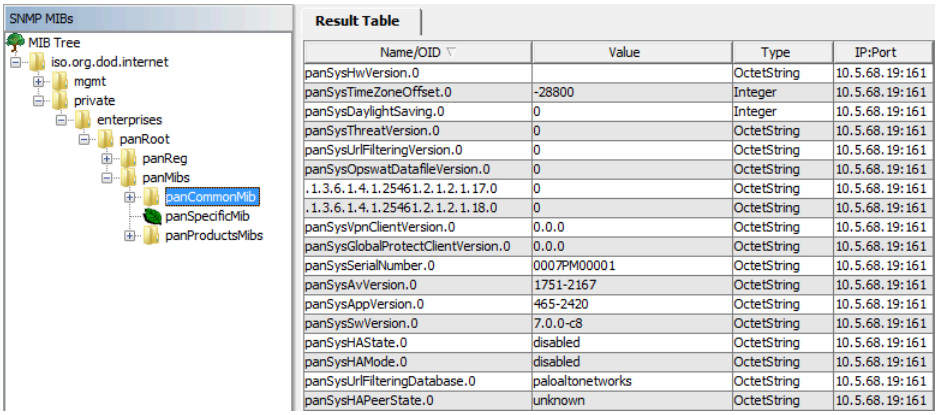


STEP 3 | （選用）執行 MIB以顯示其所有物件。

執行 MIB

如果您想查看可監控的 SNMP 物件（統計資料和設陷），則顯示特定 MIB 的所有物件非常實用。若要執行此操作，請將支援的 MIB 載入至 SNMP 管理員，並執行需要的 MIB。若要列出 Palo Alto Networks 防火牆、Panorama 或 WF-500 裝置支援的設陷，請執行 panCommonEventEventsV2 MIB。在下列範例中，執行PAN-COMMON-MIB.my 會針對特定統計資料，顯示下列 OID 及其值的清單：

©2024 Palo Alto Networks, Inc.



識別系統統計資料或設陷的 OID

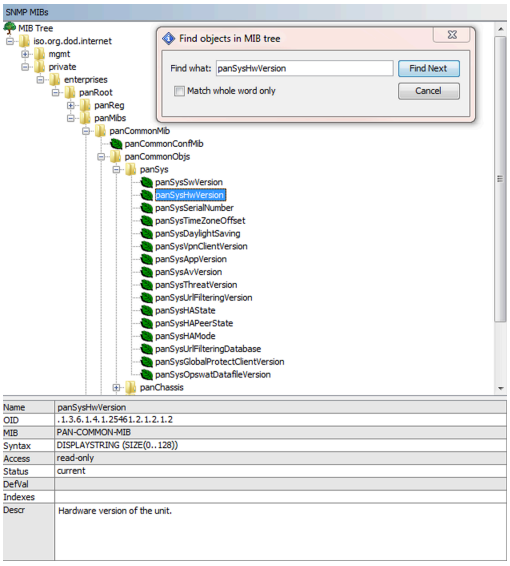
若要使用 SNMP 管理員監控 Palo Alto Networks 防火牆、Panorama 或 WF-500 裝置，您必須知道要監控之系統統計資料和設陷的 OID。

STEP 1 | 檢閱受支援的 MIB 以判斷包含所需統計資料類型的 MIB。例如，PAN-COMMON-MIB.my 中包含了硬體版本資訊。panCommonEventEventsV2 MIB 包含 Palo Alto Networks 防火牆、Panorama 或 WF-500 裝置支援的所有設陷。

STEP 2 | 在文字編輯器中開啟 MIB，並執行關鍵字搜尋。例如，使用 **Hardware version** 作為在 PAN-COMMON-MIB 中識別 panSysHwVersion 物件的搜尋字串：

```
panSysHwVersion OBJECT-TYPE SYNTAX DisplayString (SIZE(0..128))
 MAX-ACCESS read-only STATUS current DESCRIPTION "Hardware version
 of the unit." ::= {panSys 2}
```

STEP 3 | 在 MIB 瀏覽器中，搜尋 MIB 樹狀結構中是否存在已識別的物件名稱以顯示其 OID。例如，panSysHwVersion 物件具有 1.3.6.1.4.1.25461.2.1.2.1.2 的 OID。



 ©2024 Palo Alto Networks, Inc.

啟用防火牆保護網路元素的 SNMP 服務

如果您會使用簡易網路管理通訊協定 (SNMP) 監控或管理 Palo Alto Networks 防火牆的安全性地區中的網路元素 (例如，交換器和路由器)，則必須建立安全性規則以允許這些元素的 SNMP 服務。

您不需要安全性規則即可啟用 *Palo Alto Networks* 防火牆、*Panorama* 或 *WF-500* 裝置的 *SNMP* 監控。如需詳細資料，請參閱 使用 SNMP 監控統計資料。

STEP 1 | 建立應用程式群組。

1. 選取 **Objects**（物件） > **Application Group**（應用程式群組），然後按一下 **Add**（新增）。
2. 輸入用來識別應用程式群組的 **Name**（名稱）。
3. 按一下 **Add**（新增），輸入 **snmp**，然後從 **snmp-trap**（**SNMP** 設陷）下拉式清單中選取 **snmp**。
4. 按一下 **OK**（確定）以儲存應用程式群組。

STEP 2 | 建立安全性規則以允許 SNMP 服務。

1. 選取 **Policies**（原則） > **Security**（安全性），然後按一下 **Add**（新增）。
2. 在 **General**（一般）頁籤中，輸入規則的 **Name**（名稱）。
3. 在規則的 **Source**（來源）和 **Destination**（目的地）頁籤中，按一下 **Add**（新增），然後輸入流量的 **Source Zone**（來源區域）和 **Destination Zone**（目的地區域）。
4. 在 **Applications**（應用程式）頁籤中，按一下 **Add**（新增），輸入您剛剛建立的應用程式群組名稱，然後從下拉式清單中選取該項目。
5. 在 **Actions**（動作）頁籤中，確認已將 **Action**（動作）設定為 **Allow**（允許），然後按一下 **OK**（確定）和 **Commit**（提交）。

使用 SNMP 監控統計資料

簡易網路管理通訊協定 (SNMP) 管理員從 Palo Alto Networks 防火牆收集的統計資料可協助您衡量網路的健康情況（系統和連線）、識別資源限制和監控流量或處理負載。該統計資料包含介面狀態（正常或故障）、使用中的使用者工作階段、同時工作階段、工作階段使用率、溫度和系統執行時間等資訊。

您無法設定 *SNMP* 管理員以控制 *Palo Alto Networks* 防火牆（使用 *SET* 訊息），只能收集這些裝置的統計資料（使用 *GET* 訊息）。如需針對 *Palo Alto Networks* 防火牆實作 *SNMP* 的詳細資訊，請參閱 SNMP 支援。

©2024 Palo Alto Networks, Inc.

STEP 1 | 設定 SNMP 管理員以取得防火牆的統計資料。

下列步驟提供在 SNMP 管理員上執行之工作的概要。如需特定步驟，請參閱 SNMP 管理員文件。

1. 若要啟用 SNMP 管理員解釋防火牆統計資料，為 Palo Alto Networks 防火牆載入支援的 MIB，並在必要時將其編譯。
2. 針對 SNMP 管理員監控的每個防火牆，定義防火牆的連線設定（IP 位址和連接埠）和驗證設定（SNMPv2c 社群字串或 SNMPv3 EngineID/使用者名稱/密碼）。

   所有 *Palo Alto Networks* 防火牆均使用連接埠 *161*。

   SNMP 管理員可以針對多個防火牆，使用相同或不同的連線和驗證設定。該設定必須與在防火牆上設定 SNMP 時定義的設定相符（請參閱步驟 3）。例如，如果您使用 SNMPv2c，您在設定防火牆時定義的社群字串，必須與您針對該防火牆在 SNMP 管理員中定義的社群字串相符。
3. 決定要監控之統計資料的物件識別碼 (OID)。例如，若要監控防火牆的工作階段使用率百分比，MIB 瀏覽器會顯示此統計資料對應至 PAN-COMMON-MIB.my 中的 OID 1.3.6.1.4.1.25461.2.1.2.3.1.0。詳細資訊，請參閱使用 SNMP 管理程式探索 MIB 和物件。
4. 設定 SNMP 管理員以監控所需 OID。

STEP 2 | 在防火牆介面上啟用 SNMP 流量。

此為會收到來自 SNMP 管理員之統計資料要求的介面。

PAN-OS 不會在高可用性 *(HA)* 組態中同步處理防火牆的管理 *(MGT)* 介面設定。您必須針對每個 *HA* 端點設定介面。

請在防火牆網頁介面中執行此步驟。

- 若要在 MGT 介面上啟用 SNMP 流量，請選取 **Device**（裝置） > **Setup**（設定） > **Interfaces**（介面），編輯 **Management**（管理） 介面，選取 **SNMP**，然後按一下 **OK**（確定） 和 **Commit**（提交）。
- 若要在任何其他介面上啟用 SNMP 流量，請為 SNMP 服務建立介面管理設定檔，並將設定檔指派給接收 SNMP 要求的介面。介面類型必須是 Layer 3 乙太網路。

©2024 Palo Alto Networks, Inc.

STEP 3 | 設定防火牆以回應來自 SNMP 管理員的統計資料要求。

PAN-OS 不會在高可用性 *(HA)* 組態中同步處理防火牆的 *SNMP* 回應設定。您必須針對每個 *HA* 端點設定這些設定。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作），然後在 Miscellaneous（雜項）區段中，按一下 **SNMP Setup**（**SNMP** 設定）。
2. 選取 SNMP **Version**（版本），然後設定驗證值，如下所示。關於版本的詳細資訊，請參閱 SNMP 支援。
   - **V2c**—輸入 **SNMP Community String**（SNMP 社群字串），其可識別 SNMP 管理員社群和監控的裝置，並作為社群成員彼此驗證的密碼。

     最佳做法是不使用預設社群字串 ***public***；其為已知的字串，因此並不安全。
   - **V3**—建立至少一個 SNMP 檢視群組和一個使用者。當防火牆轉送設陷，且 SNMP 管理員取得防火牆統計資料時，使用者帳戶和檢視會提供驗證、隱私和存取控制。
     - 檢視 — 每個檢視都具有一組配對的 OID 和 Bitwise 遮罩：OID 會指定 MIB，而遮罩 (使用十六進位格式) 會指定 MIB 之中 (包含相符) 或之外 (排除相符) 的可存取物件。在第一個清單中按一下 **Add**（新增）並輸入檢視群組的 **Name**（名稱）。對於群組內的各個檢視，按一下 **Add**（新增）並和設定檢視 **Name**（名稱）、**OID**，相符 **Option**（選項）（**include**（包括）或 **exclude**（排除）），和 **Mask**（遮罩）。
     - 使用者—在第二個清單中按一下 **Add**（新增），在 **Users**（使用者）下方輸入使用者名稱，從下拉式清單中選取 **View**（檢視）群組，輸入用於驗證 SNMP 管理員的驗證密碼（**Auth Password**（驗證密碼），然後輸入用於加密傳送至 SNMP 管理員之 SNMP 訊息的私用密碼（**Priv Password**（私用密碼））。
3. 按一下 **OK**（確定）與 **Commit**（提交）。

STEP 4 | 在 SNMP 管理員中監控防火牆統計資料。

詳細資料，請參閱 SNMP 管理員文件。

監控與防火牆介面相關的統計資料時，您必須比對 *SNMP* 管理員中的介面索引與防火牆網頁介面中的介面名稱。如需詳細資訊，請參閱 SNMP 管理員和 NetFlow 收集器中的防火牆介面識別碼。

將設陷轉送至 SNMP 管理員

簡易網路管理通訊協定 (SNMP) 設陷可在需要立即注意的系統事件（Palo Alto Networks 防火牆發生硬體或軟體故障或變更）或威脅（符合防火牆安全性規則的流量）發生時，傳送警示給您。

若要查看 *Palo Alto Networks* 防火牆支援的設陷清單，請使用 *SNMP* 管理員存取 *panCommonEventEventsV2 MIB*。詳細資訊，請參閱使用 SNMP 管理程式探索 MIB 和物件。

如需 *Palo Alto Networks* 防火牆如何實作 *SNMP* 的詳細資訊，請參閱 SNMP 支援。

©2024 Palo Alto Networks, Inc.

STEP 1 | 啟用 SNMP 管理員以判讀收到的設陷。

為 Palo Alto Networks 防火牆載入受支援的 MIB，如有必要，對其進行編譯。如需特定步驟，請參閱 SNMP 管理員文件。

STEP 2 | 設定 SNMP 設陷伺服器設定檔。

設定檔會定義防火牆如何存取 SNMP 管理員（設陷伺服器）。您可以針對每個設定檔，定義最多四個 SNMP 管理員。

（選用）針對不同的日誌類型、嚴重性等級和 *WildFire* 裁定，設定個別 *SNMP* 設陷伺服器設定檔。

1. 登入防火牆 Web 介面。
2. 選取 **Device**（裝置） > **Server Profiles**（伺服器設定檔） > **SNMP Trap**（**SNMP** 設陷）。
3. 按一下 **Add**（新增），然後輸入設定檔的 **Name**（名稱）。
4. 若防火牆具有多個虛擬系統 (vsys)，請選取可在其中使用設定檔的 **Location**（位置）（vsys 或 **Shared**（共用））。
5. 選取 SNMP **Version**（版本），然後設定驗證值，如下所示。關於版本的詳細資訊，請參閱 SNMP 支援。
   - **V2c**—針對每個伺服器，按一下 **Add**（新增），然後輸入伺服器 **Name**（名稱）、IP 位址（**SNMP Manager**（**SNMP** 管理員））和 **Community String**（社群字串）。社群字串可識別 SNMP 管理員社群和監控的裝置，並作為社群成員彼此驗證的密碼。

     最佳做法是不使用預設社群字串 ***public***；其為已知的字串，因此並不安全。
   - **V3**—針對每個伺服器，按一下 **Add**（新增），然後輸入伺服器 **Name**（名稱）、IP 位址（**SNMP Manager**（**SNMP** 管理員））、SNMP **User**（使用者）帳戶（這必須與在 SNMP 管理員中定義的使用者名稱相符）、用於唯一識別防火牆的 **EngineID**（您可以將欄位保留空白以使用防火牆序號）、用於驗證伺服器的驗證密碼（**Auth Password**（驗證密碼））和用於加密傳送至伺服器之 SNMP 訊息的私人密碼（**Priv Password**（私人密碼））。
6. 按一下 **OK**（確定）來儲存伺服器設定檔。

 ©2024 Palo Alto Networks, Inc.

STEP 3 | 組態日誌轉送。

1. 設定流量、威脅和 WildFire 設陷的目的地：
   1. 建立日誌轉送設定檔。針對每個日誌類型和嚴重性等級或 WildFire 裁定，選取 **SNMP Trap**（**SNMP** 設陷）伺服器設定檔。
   2. 將日誌轉送設定檔指派給原則規則和網路區域。這些規則和區域會觸發設陷產生和轉送。
2. 設定系統、組態、User-ID、HIP 比對和關聯日誌的目的地。針對每個日誌（設陷）類型和嚴重性等級，選取 **SNMP Trap**（**SNMP** 設陷）伺服器設定檔。
3. 按一下 **Commit**（交付）。

STEP 4 | 在 SNMP 管理員中監控設陷。

請參閱 SNMP 管理員文件。

監控與防火牆介面相關的設陷時，您必須比對 *SNMP* 管理員中的介面索引與防火牆網頁介面中的介面名稱。如需詳細資訊，請參閱 SNMP 管理員和 NetFlow 收集器中的防火牆介面識別碼。

支援的 MIB

下表列出了 Palo Alto Networks 防火牆、Panorama 或 WF-500 裝置支援的簡易網路管理協定 (SNMP) 管理資訊庫 (MIB)。您必須將這些 MIB 載入至 SNMP 管理員，才能監控 MIB 中定義的物件（系統統計資料和設陷）。詳細資訊，請參閱使用 SNMP 管理程式探索 MIB 和物件。

MIB 類型	支援的 **MIB**
標準—網際網路工程任務推動小組 (IETF) 會維護大部分的標準 MIB。您可以從 IETF 網站下載 MIB。 *Palo Alto Networks* 防火牆、*Panorama* 或 *WF-500* 裝置不支援所有這些 *MIB* 中的所有物件 *(OID)*。請參閱「受支援的 *MIB*」連結以取得受支援 *OID* 的概要。	MIB-II IF-MIB HOST-RESOURCES-MIB ENTITY-MIB ENTITY-SENSOR-MIB ENTITY-STATE-MIB IEEE 802.3 LAG MIB LLDP-V2-MIB.my BFD-STD-MIB

©2024 Palo Alto Networks, Inc.

MIB 類型	支援的 MIB
企業—您可以從 Palo Alto Networks 技術文件入口網站下載企業 MIB。	PAN-COMMON-MIB.my PAN-GLOBAL-REG-MIB.my PAN-GLOBAL-TC-MIB.my PAN-LC-MIB.my PAN-PRODUCT-MIB.my PAN-ENTITY-EXT-MIB.my PAN-TRAPS.my

MIB-II

MIB-II 可在以 TCP/IP 為基礎的網路中，提供網路管理通訊協定的物件識別碼 (OID)。使用此 MIB 可監控系統和介面的一般資訊。例如，您可以透過介面類型（ifType 物件）分析頻寬使用率的趨勢，以決定防火牆是否需要更多該類型的介面以容納流量中的高點。

Palo Alto Networks 防火牆、Panorama 或 WF-500 裝置僅支援下列物件群組：

物件群組	說明
系統	提供硬體型號、系統執行時間、FQDN 和實體位置等系統資訊。
介面	提供類型、目前頻寬（速度）、操作狀態（例如，正常或故障）和已捨棄的封包等實體與邏輯介面的統計資料。邏輯介面支援包含 VPN 通道、彙總群組、Layer 2 子介面、Layer 3 子介面、回送介面和 VLAN 介面。

RFC 1213 已定義此 MIB。

IF-MIB

IF-MIB 支援MIB-II中定義項目外的介面類型（實體與邏輯）和較大計數器 (64K)。使用此 MIB 可監控 MIB-II 不提供的介面統計資料。例如，若要監控 PA-5200 Series 防火牆的 10G 介面等高速介面 (大於 2.2Gps) 的目前頻寬，您必須查看 IF-MIB 中的 ifHighSpeed 物件，而非 MIB-II 中的 ifSpeed 物件。評估網路容量時，IF-MIB 統計資料非常實用。

Palo Alto Networks 防火牆、Panorama 或 WF-500 裝置僅支援 IF-MIB 中的 ifXTable，其可提供多點傳送數、傳輸和接收的廣播封包數、介面是否處於混合式模式，以及介面是否具有實體連接器等介面資訊。

RFC 2863 已定義此 MIB。

©2024 Palo Alto Networks, Inc.

HOST-RESOURCES-MIB

HOST-RESOURCES-MIB 可提供主機電腦資源的資訊。使用此 MIB 可監控 CPU 和記憶體使用率統計資料。例如，查看目前的 CPU 負載 (hrProcessorLoad object) 可協助您疑難排解防火牆上的效能問題。

Palo Alto Networks 防火牆、Panorama 或 WF-500 裝置支援下列物件群組：

物件群組	說明
hrDevice	提供 CPU 負載、儲存容量和分割區大小等資訊。hrProcessorLoad OID 可提供處理封包的平均核心。 對於具有多個資料平面 (DP) 的 PA-7000 和 PA-5200 系列防火牆，您可以監控單個資料平面處理器使用率。設定使用率達到每個 DP 處理器的特定臨界值時發出警示，以避免服務可用性問題。
hrSystem	提供系統執行時間、目前的使用者工作階段數和目前的處理程序數等資訊。
hrStorage	提供使用的儲存量等資訊。

RFC 2790 已定義此 MIB。

ENTITY-MIB

ENTITY-MIB 可提供多個邏輯與實體元件的 OID。使用此 MIB 可判斷系統上裝載的實體元件（例如，風扇和溫度感測器），並查看型號和序號等相關資訊。您也可以使用這些元件的索引號碼，判斷其在 ENTITY-SENSOR-MIB 和 ENTITY-STATE-MIB 中的操作狀態。

Palo Alto Networks 防火牆、Panorama 或 WF-500 裝置僅支援 entPhysicalTable 群組的部分：

object	說明
entPhysicalIndex	包含磁碟插槽和磁碟機的單一命名空間。
entPhysicalDescr	元件說明。
entPhysicalVendorType	可用時的 sysObjectID（請參閱 PAN-PRODUCT-MIB.my）（底座和模組物件）。
entPhysicalContainedIn	包含此元件的元件 entPhysicalIndex 值。
entPhysicalClass	底座 (3)、插槽容器 (5)、電源供應器 (6)、風扇 (7)、每個溫度或其他環境的感測器 (8)，以及每個線路卡的模組 (9)。

©2024 Palo Alto Networks, Inc.

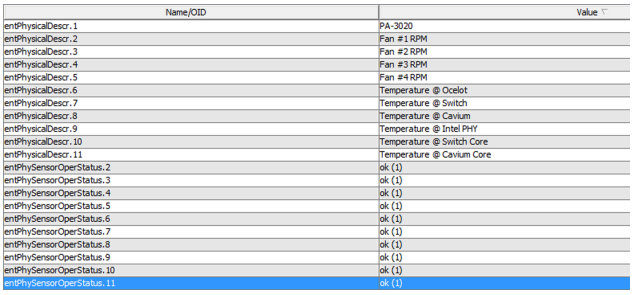
object	說明
entPhysicalParentRelPos	此子元件在其同層級元件之間的相對位置。系統將同層級元件定義為 entPhysicalEntry 元件，其會共用每個 entPhysicalContainedIn 和 entPhysicalClass 物件的相同實例值。
entPhysicalName	只有在管理 (MGT) 介面允許命令線路卡時才支援此項目。
entPhysicalHardwareRev	元件的廠商特定硬體修訂。
entPhysicalFirwareRev	元件的廠商特定韌體修訂。
entPhysicalSoftwareRev	元件的廠商特定軟體修訂。
entPhysicalSerialNum	元件的廠商特定序號。
entPhysicalMfgName	元件製造商名稱。
entPhysicalMfgDate	元件製造日期。
entPhysicalModelName	磁碟型號。
entPhysicalAlias	網路管理員針對元件指定的別名。
entPhysicalAssetID	網路管理員針對元件指定之使用者指派的資產追蹤識別碼。
entPhysicalIsFRU	表示元件是否為現場可更換單元 (FRU)。
entPhysicalUris	元件的通用語言裝置識別碼 (CLEI) 號碼 (例如，URN:CLEI:CNME120ARA)。

RFC 4133 已定義此 MIB。

ENTITY-SENSOR-MIB

ENTITY-SENSOR-MIB 可新增 ENTITY-MIB 定義項目外的網路裝置實體感測器支援。將此 MIB 與 ENTITY-MIB 串聯使用可監控系統實體元件的操作狀態（例如，風扇和溫度感測器）。例如，若要疑難排解環境條件造成的問題，您可以將實體索引從 ENTITY-MIB（entPhysicalDescr 物件）對應至 ENTITY-SENSOR-MIB 中的操作狀態值 (entPhysSensorOperStatus 物件)。在下列範例中，PA-3020 防火牆的所有風扇和溫度感測器都正常運作：

©2024 Palo Alto Networks, Inc.



Name/OID	Value
entPhysicalDescr.1	PA-3020
entPhysicalDescr.2	Fan #1 RPM
entPhysicalDescr.3	Fan #2 RPM
entPhysicalDescr.4	Fan #3 RPM
entPhysicalDescr.5	Fan #4 RPM
entPhysicalDescr.6	Temperature @ Ocelot
entPhysicalDescr.7	Temperature @ Switch
entPhysicalDescr.8	Temperature @ Cavium
entPhysicalDescr.9	Temperature @ Intel PHY
entPhysicalDescr.10	Temperature @ Switch Core
entPhysicalDescr.11	Temperature @ Cavium Core
entPhySensorOperStatus.2	ok (1)
entPhySensorOperStatus.3	ok (1)
entPhySensorOperStatus.4	ok (1)
entPhySensorOperStatus.5	ok (1)
entPhySensorOperStatus.6	ok (1)
entPhySensorOperStatus.7	ok (1)
entPhySensorOperStatus.8	ok (1)
entPhySensorOperStatus.9	ok (1)
entPhySensorOperStatus.10	ok (1)
entPhySensorOperStatus.11	ok (1)

不同平台上的相同 *OID* 可能會參考不同的感測器。針對目標平台使用 *ENTITY-MIB* 可比對值與說明。

Palo Alto Networks 防火牆、Panorama 或 WF-500 裝置僅支援 entPhySensorTable 群組的部分。支援部分視平台而異，並且僅支援熱（溫度單位攝氏）和風扇（單位 RPM）感測器。

RFC 3433 已定義 ENTITY-SENSOR-MIB。

ENTITY-STATE-MIB

ENTITY-STATE-MIB 可提供 ENTITY-MIB 定義項目以外的實體元件狀態資訊，包含以底座為基礎的平台中元件的管理和操作狀態。將此 MIB 與 ENTITY-MIB 串聯使用可監控 PA-7000 Series 或 PA-5450 防火牆元件的操作狀態（例如，線路卡、風扇托架和電源供應器）。例如，若要疑難排解威脅日誌的日誌轉送問題，您可以將日誌處理卡 (LPC) 索引從 ENTITY-MIB（entPhysicalDescr 物件）對應至 ENTITY-STATE-MIB 中的操作狀態值（entStateOper 物件）。操作狀態值使用數字表示狀態：1 為未知、2 為已停用、3 為已啟用，而 4 為測試中。PA-7000 Series 和 PA-5450 防火牆是唯一支援此 MIB 的 Palo Alto Networks 防火牆。

RFC 4268 已定義 ENTITY-STATE-MIB。

IEEE 802.3 LAG MIB

使用 IEEE 802.3 LAG MIB 來監控已啟用連結彙總控制通訊協定（彙總介面群組中的 LACP）之彙總群組的狀態。防火牆記錄 LACP 事件時，其也會產生對疑難排解非常實用的設陷。例如，設陷可讓您知道防火牆和 LACP 端點之間的流量是否因失去連線或不相符的介面速度和雙工值而中斷。

PAN-OS 會針對 LACP 實作下列 SNMP 表格。

dot3adTablesLastChanged 物件表示最近變更 *dot3adAggTable*、*dot3adAggPortListTable* 和 *dot3adAggPortTable* 的時間。

表格	說明
彙總設定表格 (dot3adAggTable)	此表格包含與防火牆相關聯之所有彙總群組的資訊。每個彙總群組都具有一個項目。 某些表格物件具有限制，如 dot3adAggIndex 物件所述。此索引是本機系統指派給彙總群組的唯一識別碼。其可在包含物件的次級管理物件之間，識別彙總群組實例。識別碼是唯讀項目。

©2024 Palo Alto Networks, Inc.

表格	說明
	ifTable MIB（介面項目清單）不支援邏輯介面，因此其沒有彙總群組項目。
彙總連接埠清單表格 (dot3adAggPortListTable)	此表格列出與防火牆中每個彙總群組相關聯的連接埠。每個彙總群組都具有一個項目。 dot3adAggPortListPorts 屬性會列出與彙總群組相關聯的一組完整連接埠。在清單中設定的每個位元都代表連接埠成員。針對非底座平台，此為 64 位元值。針對底座平台，該值是八個 64 位元項目的陣列。
彙總連接埠表格 (dot3adAggPortTable)	此表格包含與防火牆中彙總群組相關聯之所有連接埠的 LACP 設定資訊。每個連接埠都具有一個項目。該表格沒有與彙總群組無關之連接埠的項目。
LACP 統計資料表格 (dot3adAggPortStatsTable)	此表格包含與防火牆中彙總群組相關聯之所有連接埠的連結彙總資訊。每個連接埠都具有一列。該表格沒有與彙總群組無關之連接埠的項目。

IEEE 802.3 LAG MIB 包含下列 LACP 相關設陷：

設陷名稱	說明
panLACPLostConnectivityTrap	端點失去防火牆的連線。
panLACPUnresponsiveTrap	端點未回應防火牆。
panLACPNegoFailTrap	LACP 與端點交涉失敗。
panLACPSpeedDuplexTrap	防火牆上的連結速度和雙工設定與端點不相符。
panLACPLinkDownTrap	彙總群組中的介面故障。
panLACPLacpDownTrap	已從彙總群組中移除介面。
panLACPLacpUpTrap	已將介面新增至彙總群組。

針對 MIB 定義，請參閱 IEEE 802.3 LAG MIB。

LLDP-V2-MIB.my

使用 LLDP-V2-MIB 可監控連結層探索通訊協定 (LLDP) 事件。例如，您可以查看 lldpV2StatsRxPortFramesDiscardedTotal 物件以查看因任何原因而丟棄的 LLDP 框架數。Palo Alto

©2024 Palo Alto Networks, Inc.

Networks 防火牆會使用 LLDP 探索鄰近設備及其功能。LLDP 讓疑難排解變得更容易，尤其是虛擬線部署，因為在此部署中 ping 或路徑追蹤無法偵測到防火牆。

Palo Alto Networks 防火牆支援下列物件以外的所有 LLDP-V2-MIB 物件：

- 下列 lldpV2Statistics 物件：
  - lldpV2StatsRemTablesLastChangeTime
  - lldpV2StatsRemTablesInserts
  - lldpV2StatsRemTablesDeletes
  - lldpV2StatsRemTablesDrops
  - lldpV2StatsRemTablesAgeouts
- 下列 lldpV2RemoteSystemsData 物件：
  - lldpV2RemOrgDefInfoTable 表格
  - 在 lldpV2RemTable 表格中：lldpV2RemTimeMark

RFC 4957 已定義此 MIB。

BFD-STD-MIB

使用雙向轉送偵測 (BFD) MIB，監控並接收兩個轉送引擎（介面、資料連結或實際引擎）之間雙向路徑的故障警示。例如，您可檢查 bfdSessState 物件以查看轉送引擎之間 BFD 工作階段的狀態。在 Palo Alto Networks 實作中，其中一個轉向引擎是防火牆介面，另一個是已設定的相臨 BFD 對等。

RFC 7331 已定義此 MIB。

PAN-COMMON-MIB.my

使用 PAN-COMMON-MIB 可監控下列 Palo Alto Networks 防火牆、Panorama 或 WF-500 裝置資訊：

物件群組	說明
panSys	包含系統軟體/硬體版本、動態內容版本、序號、HA 模式/狀態和全域計數器等物件。 全域計數器包含拒絕服務 (DoS)、IP 分散、TCP 狀態和已丟棄封包的相關計數器。追蹤這些計數器可讓您監控因 DoS 攻擊、系統或連線失敗，或是資源限制而產生的流量異常。PAN-COMMON-MIB 支援防火牆的全域計數器，但不支援 Panorama 的全域計數器。
panChassis	底座類型和 M 系列裝置模式（Panorama 或日誌收集器）。
panSession	工作階段使用率資訊。例如，防火牆上或特定虛擬系統上使用中工作階段的總數。

©2024 Palo Alto Networks, Inc.

物件群組	說明
panMgmt	從防火牆到 Panorama 管理伺服器的連線狀態。
panGlobalProtect	以百分比表示的 GlobalProtect 閘道使用率、允許的通道上限和使用中通道數。
panLogCollector	記錄每個日誌收集器的統計資料，包括日誌記錄速率、日誌配額、磁碟使用情況、保留期間、日誌備援（啟用或停用）、從防火牆轉送至日誌收集器的狀態、從日誌收集器轉送至外部服務的狀態，以及防火牆與日誌收集器連線的狀態。
panDeviceLogging	記錄每個防火牆的統計資料，包括日誌記錄速率、磁碟使用情況、保留期間、從各防火牆轉送至 Panorama 和外部伺服器的狀態，以及防火牆與日誌收集器連線的狀態。

PAN-GLOBAL-REG-MIB.my

PAN-GLOBAL-REG-MIB.my 包含 Palo Alto Networks 企業 MIB 模組之各種子樹狀結構的全域最上層 OID 定義。此 MIB 不包含可讓您監控的物件，其僅供其他 MIB 參考。

PAN-GLOBAL-TC-MIB.my

PAN-GLOBAL-TC-MIB.my 會定義 Palo Alto Networks 企業 MIB 模組中物件文字值的慣例（例如，字元長度和允許的字元）。所有 Palo Alto Networks 產品都會使用這些慣例。此 MIB 不包含可讓您監控的物件，其僅供其他 MIB 參考。

PAN-LC-MIB.my

PAN-LC-MIB.my 包含日誌收集器（處於日誌收集器模式的 M-Series 裝置）實作之受管理物件的定義。使用此 MIB 可監控日誌收集器上每個邏輯磁碟（最多四個）的日誌記錄速率、日誌資料庫儲存持續時間（單位天數）和磁碟使用率（單位 MB）。例如，您可以使用此資訊決定是否應該新增更多日誌收集器，或將日誌轉送至外部伺服器（例如，syslog 伺服器）以進行封存。

PAN-PRODUCT-MIB.my

PAN-PRODUCT-MIB.my 定義所有 Palo Alto Networks 產品的 sysObjectID OID。此 MIB 不包含可讓您監控的物件，其僅供其他 MIB 參考。

PAN-ENTITY-EXT-MIB.my

將 PAN-ENTITY-EXT-MIB.my 與 ENTITY-MIB 串聯使用可監控 PA-7000 Series 或 PA-5450 防火牆實體元件的電源使用率（例如，風扇托架和電源供應器），該防火牆是唯有的兩個支援此 MIB 的 Palo Alto Networks 防火牆。例如，疑難排解日誌轉送問題時，若要查看日誌處理卡 (LPC) 的電源使用率：您可以將 LPC 索引從 ENTITY-MIB（entPhysicalDescr 物件）對應至 PAN-ENTITY-EXT-MIB（panEntryFRUModelPowerUsed 物件）中的值。

©2024 Palo Alto Networks, Inc.

PAN-TRAPS.my

使用 PAN-TRAPS.my 可查看所有產生的設陷及其相關資訊（例如，說明）的完整清單。如需 Palo Alto Networks 防火牆、Panorama 或 WF-500 裝置支援的設陷清單，請參閱 PAN-COMMON-MIB.my **panCommonEvents** > **panCommonEventsEvents** > **panCommonEventEventsV2** 物件。

©2024 Palo Alto Networks, Inc.

將日誌轉送至 HTTP/S 目的地

防火牆和 Panorama™ 可將日誌轉送至 HTTP/S 伺服器。您可以選擇轉送所有日誌或特定日誌，以在發生事件時，對基於外部的 HTTP 服務觸發相應動作。當轉送日誌到 HTTP 伺服器時，請設定防火牆直接向協力廠商服務傳送 HTTP 型 API 要求，以根據防火牆日誌中的屬性觸發相應動作。您可以設定防火牆與任何暴露 API 的 HTTP 型服務協作，且您還可以修改 HTTP 要求中的 URL、HTTP 標頭、參數和承載來符合您的整合需求。

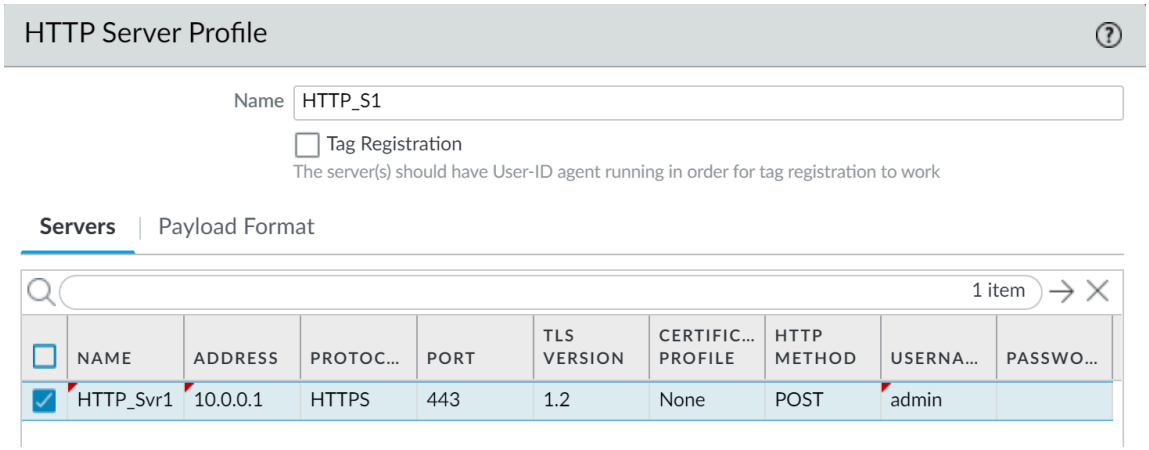
STEP 1 | 設定 HTTP 伺服器設定檔，以將日誌轉送至 HTTP/S 目的地。

HTTP 伺服器設定檔允許您指定伺服器存取方式並定義以何種格式轉送日誌到 HTTP/S 目的地。依預設，防火牆將使用管理連接埠轉送這些日誌。但是，您可以在 **Device**（裝置） > **Setup**（設

©2024 Palo Alto Networks, Inc.

定） > **Services**（服務） > **Service Route Configuration**（服務路由設定）中指派不同的來源介面及 IP 位址。

1. 選取 **Device**（裝置） > **Server Profiles**（伺服器設定檔） > **HTTP**，然後 **Add**（新增） 新的設定檔。
2. 為伺服器設定檔指定名稱，並選取**Location**（位置）。該設定檔可由所有虛擬系統 **Shared**（共用），也可以屬於特定虛擬系統。
3. **Add**（新增）各個伺服器的詳細資訊。每個設定檔最多可以有四個伺服器。
4. 輸入 **Name**（名稱）及 IP **Address**（位址）。
5. 選取 **Protocol**（通訊協定）（**HTTP**或**HTTPS**）。預設 **Port**（連接埠） 為 80 或 443；但您可以修改連接埠號，以與 HTTP 伺服器接聽的連接埠相符。
6. 選取伺服器支援的 **TLS Version**（**TLS** 版本）—**1.0**、**1.1**或**1.2**（預設值）。
7. 選取 **Certificate Profile**（憑證設定檔）以用於與伺服器建立 TLS 連線。
8. 選取協力廠商服務支援的 **HTTP Method**（**HTTP** 方法）—**DELETE**、**GET**、**POST**（預設值），或**PUT**。
9. （選用）必要時，輸入 **Username**（使用者名稱）及 **Password**（密碼），以向伺服器驗證。
10. （選用）選取 **Test Server Connection**（測試伺服器連線），以驗證防火牆與 HTTP/S 伺服器之間的網路連線。



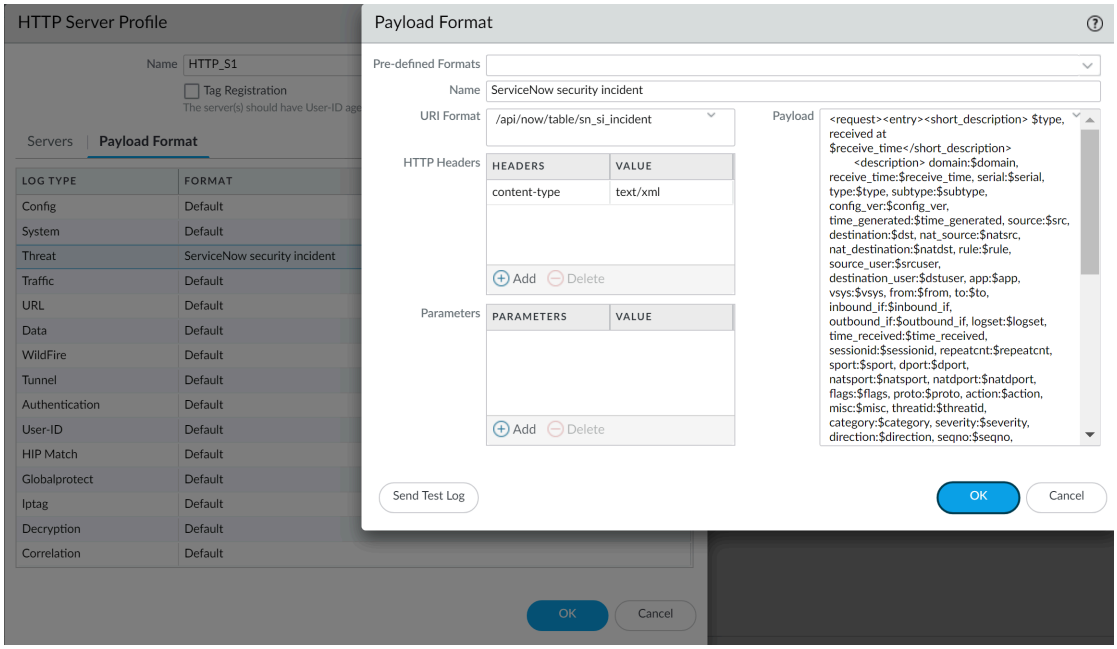
STEP 2 | 選取 HTTP 要求的 **Payload Format**（裝載格式）。

1. 為您要定義 HTTP 要求格式的每個日誌類型選取 **Log Type**（日誌類型）連結。
2. 選取 **Pre-defined Formats**（預先定義的格式）（可透過內容更新）或建立自訂格式。

   如果您建立自訂格式，**URI** 會是 HTTP 服務上的資源端點。防火牆會將 URI 附加至您稍早定義的 IP 位址，以建構 HTTP 要求的 URL。請確保 URI 與承載格式符合您第三方廠商

©2024 Palo Alto Networks, Inc.

要求的語法。您可以在 HTTP 標頭、參數-值配對以及要求裝載中，使用選取的日誌類型上支援的任何屬性。

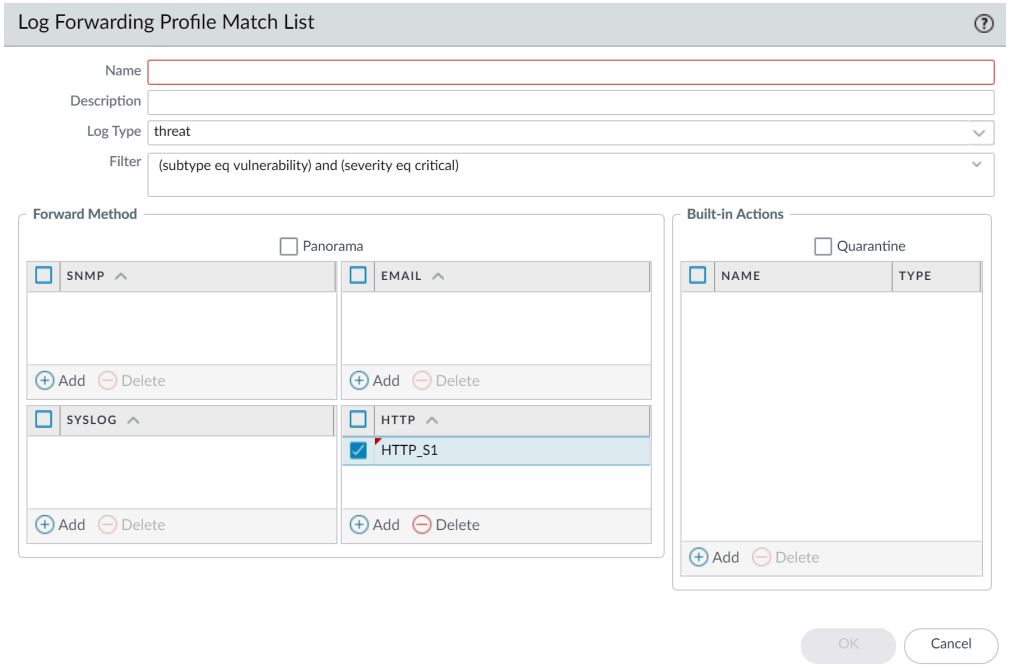


3. **Send Test Log**（傳送測試日誌）以驗證 HTTP 伺服器是否能接收要求。若您已互動方式傳送測試日誌，防火牆將使用原格式，不會用防火牆日誌中的值取代變數。若 HTTP 伺服器傳送 404 回應，則提供參數值，以便伺服器能夠成功處理要求。

©2024 Palo Alto Networks, Inc.

STEP 3 | 針對防火牆向 HTTP 伺服器轉送日誌的時間，定義比對準則，並附加您將使用的 HTTP 伺服器設定檔。

1. 選取您要觸發工作流程的日誌類型：
   - 針對與使用者活動相關的日誌（例如，Traffic（流量）、威脅（Threat）或 Authentication logs（驗證日誌）），新增日誌轉送（**Objects**（物件）> **Log Forwarding Profile**（日誌轉送設定檔））。
   - 針對與系統事件相關的日誌，例如組態日誌或系統日誌，選取 **Device**（裝置）> **Log Settings**（日誌設定）。
2. 選取日誌類型，然後使用 **Filter Builder**（篩選器產生器）來定義比對準則。
3. **Add**（新增）HTTP 伺服器設定檔，以將日誌轉送至 HTTP 目的地。



 ©2024 Palo Alto Networks, Inc.

NetFlow 監控

NetFlow 是業界標準的通訊協定，防火牆可將其用於匯出有關進入其介面之 IP 流量的統計資料。防火牆會將統計資料匯出成 NetFlow 收集器中的 NetFlow 欄位。NetFlow 收集器是您用於分析網路流量的伺服器，可滿足安全性、管理、會計與疑難排解等用途。所有 Palo Alto Networks 防火牆都支援 NetFlow 第 9 版。防火牆僅支援單向 NetFlow，而非雙向。防火牆會執行介面所有 IP 封包上的 NetFlow 處理，且不支援範例 NetFlow。您可以將 Layer 3、Layer 2、虛擬介接、旁接、VLAN、回送及通道介面的 NetFlow 記錄匯出。針對彙總乙太網路子介面，您可以將資料在群組內流過的個別子介面的記錄匯出。若要識別 NetFlow 收集器中的防火牆介面，請參閱SNMP 管理員和 NetFlow 收集器中的防火牆介面識別碼。防火牆支援標準與企業（PAN-OS 特定）NetFlow 範本，可供 NetFlow 收集器用來解譯 NetFlow 欄位。

- 設定 NetFlow 匯出
- NetFlow 範本

設定 NetFlow 匯出

若要使用 NetFlow 收集器分析進入防火牆介面的網路流量，可按下列步驟設定 NetFlow 記錄匯出。

STEP 1 | 建立 NetFlow 伺服器設定檔。

設定檔定義了哪些 NetFlow 收集器將接收匯出的記錄並指定了匯出參數。

1. 選取 **Device**（裝置） > **Server Profiles**（伺服器設定檔） > **NetFlow**，然後 **Add**（新增）設定檔。
2. 輸入用來識別設定檔的 **Name**（名稱）。
3. 根據 NetFlow 收集器的需求，以 **Minutes**（分鐘）（預設值為 30）和 **Packets**（封包數）（匯出的記錄—預設值為 20）指定防火牆重新整理 NetFlow Templates（NetFlow 範本）的速率。防火牆會在超過任何臨界值後重新整理範本。
4. 指定 **Active Timeout**（主動式逾時），即防火牆匯出記錄的頻率（以分鐘為單位，預設值是 5）。
5. 如果要讓防火牆匯出 App-ID 與 User-ID 欄位，可選取 **PAN-OS Field Types**（**PAN-OS** 欄位類型）。
6. **Add**（新增）將要接收記錄的 NetFlow 收集器（每個設定檔最多兩個）。對於每個收集器，指定下列設定：
   - 用來識別憑證的 **Name**（名稱）。
   - **NetFlow Server**（**NetFlow** 伺服器）主機名稱或 IP 位址。
   - 存取 **Port**（連接埠）（默認為 2055）.
7. 按一下 **OK**（確定）來儲存設定檔。

©2024 Palo Alto Networks, Inc.

STEP 2 | 將 NetFlow 伺服器設定檔指派給您要分析之流量進入的防火牆介面。

在此範例中，您會將設定檔指派給現有的乙太網路介面。

1. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），然後按一下要編輯的介面名稱。

   您可以將 *Layer 3*、*Layer 2*、虛擬介接、旁接、*VLAN*、回送及通道介面的 *NetFlow* 記錄匯出。針對彙總乙太網路介面，您可以將資料在群組內流過的個別子介面的記錄匯出。

2. 選取您設定的 NetFlow 伺服器設定檔（**NetFlow Profile**（**NetFlow** 設定檔）），然後按一下 **OK**（確定）。

STEP 3 | （**PA-7000** 系列、**PA-5400** 系列和 **PA-5200** 系列防火牆要求）為防火牆用於傳送 NetFlow 記錄的介面設定服務路由。

您可以使用管理 (MGT) 介面，從 PA-7000 系列、PA-5400 系列和 PA-5200 系列防火牆傳送 NetFlow 記錄。對於其他防火牆型號，服務路由為可選項。對於所有防火牆，傳送 NetFlow 記錄的介面不必與防火牆為其收集記錄的介面相同。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Services**（服務）。
2. （帶有多個虛擬系統的防火牆）選取以下任何選項：
   - 全域—如果服務路由適用於防火牆上的所有虛擬系統，則選取此選項。
   - 虛擬系統—如果服務路由適用於特定虛擬系統，則選取此選項。將 **Location**（位置）設定為虛擬系統。
3. 選取 **Service Route Configuration**（服務路由組態），然後進行自訂。
4. 選取介面使用的通訊協定（**IPv4** 或 **IPv6**）。若有必要，您可以為這兩種通訊協定設定服務路由。
5. 按一下 Service（服務）欄中的 **Netflow**。
6. 選取 **Source Interface**（來源介面）。

   Any（任何）、***Use default***（使用預設值）和 ***MGT*** 介面選項不適用於從 *PA-7000* 系列、*PA-5400* 系列或 *PA-5200* 系列防火牆傳送 *NetFlow* 記錄。

7. 選取 **Source Address**（來源位址）（IP 位址）。
8. 按兩下 **OK**（確定）儲存您的變更。

STEP 4 | **Commit**（提交）您的變更。

©2024 Palo Alto Networks, Inc.

STEP 5 | 在 NetFlow 收集器中監控防火牆流量。

請參閱 NetFlow 收集器文件。

監控統計資料時，您必須比對 *NetFlow* 收集器中的介面索引與防火牆網頁介面中的介面名稱。如需詳細資訊，請參閱 SNMP 管理員和 NetFlow 收集器中的防火牆介面識別碼。

若要對 NetFlow 傳送問題進行疑難排解，可使用操作 CLI 命令 **debug log-receiver netflow statistics**。

NetFlow 範本

NetFlow 收集器會使用範本解碼防火牆匯出的欄位。防火牆會根據匯出的資料類型來選取範本：IPv4 或 IPv6 流量、含或不含 NAT，以及含標準或企業特定（PAN-OS 特定）的欄位。防火牆會定期重新整理範本以重新評估要使用哪個範本（以免匯出資料的類型變更），並將任何變更套用至所選範本中的欄位。在設定 NetFlow 匯出時，根據 NetFlow 收集器所需的日誌匯出時間間隔和數量設定重新整理速率。防火牆會在超過任何臨界值後重新整理範本。

Palo Alto Networks 防火牆支援下列 NetFlow 範本：

範本	ID
IPv4 標準版	256
IPv4 企業版	257
IPv6 標準版	258
IPv6 企業版	259
IPv4 含 NAT 標準版	260
IPv4 含 NAT 企業版	261
IPv6 含 NAT 標準版	262
IPv6 含 NAT 企業版	263

下表列出防火牆可傳送的 NetFlow 欄位，以及可定義這些欄位的範本：

©2024 Palo Alto Networks, Inc.

值	欄位	說明	範本
1	IN_BYTES	長度為 N * 8 位元的傳入計數器，代表與 IP 流量相關聯的位元組數。N 預設為 4。	所有範本
2	IN_PKTS	長度為 N * 8 位元的傳入計數器，代表與 IP 流量相關聯的封包數。N 預設為 4。	所有範本
4	PROTOCOL	IP 通訊協定位元	所有範本
5	TOS	進入輸入介面時的服務類型位元組設定。	所有範本
6	TCP_FLAGS	此流量中所有 TCP 旗標的總計。	所有範本
7	L4_SRC_PORT	TCP/UDP 來源連接埠號碼 (例如 FTP、Telnet 或等同項目)。	所有範本
8	IPV4_SRC_ADDR	IPv4 來源位址。	IPv4 標準版 IPv4 企業版 IPv4 含 NAT 標準版 IPv4 含 NAT 企業版
10	INPUT_SNMP	輸入介面索引。值長度預設為 2 位元組，但可能為更大的值。關於 Palo Alto Networks 防火牆如何產生介面索引的詳細資料，請參閱 SNMP 管理員和 NetFlow 收集器中的防火牆介面識別碼。	所有範本
11	L4_DST_PORT	TCP/UDP 目的地連接埠號碼 (例如 FTP、Telnet 或等同項目)。	所有範本
12	IPV4_DST_ADDR	IPv4 目的地位址。	IPv4 標準版 IPv4 企業版 IPv4 含 NAT 標準版 IPv4 含 NAT 企業版

©2024 Palo Alto Networks, Inc.

值	欄位	說明	範本
14	OUTPUT_SNMP	輸出介面索引。值長度預設為 2 位元組，但可能為更大的值。關於 Palo Alto Networks 防火牆如何產生介面索引的詳細資料，請參閱 SNMP 管理員和 NetFlow 收集器中的防火牆介面識別碼。	所有範本
21	LAST_SWITCHED	當交換此流量的最後一個封包時的系統執行時間，以毫秒為單位。	所有範本
22	FIRST_SWITCHED	當交換此流量的第一個封包時的系統執行時間，以毫秒為單位。	所有範本
27	IPV6_SRC_ADDR	IPv6 來源位址。	IPv6 標準版 IPv6 企業版 IPv6 含 NAT 標準版 IPv6 含 NAT 企業版
28	IPV6_DST_ADDR	IPv6 目的地位址	IPv6 標準版 IPv6 企業版 IPv6 含 NAT 標準版 IPv6 含 NAT 企業版
32	ICMP_TYPE	網際網路控制訊息通訊協定 (ICMP) 封包類型。這會彙報為： ICMP 類型 * 256 + ICMP 指令碼	所有範本
61	DIRECTION	流量方向： • 0 = ingress • 1 = egress	所有範本
148	flowId	在觀察網域內唯一的流量識別碼。如果系統未報告如 IP 位址與連接埠號碼等流量金鑰，或在另一個記錄中報告，您可以使用此資訊元素區分不同的流量。flowID 與流量與	所有範本

©2024 Palo Alto Networks, Inc.

值	欄位	說明	範本
		威脅日誌中的工作階段 ID 欄位對應。	
233	firewallEvent	指示防火牆事件： • 0 = 忽略（無效）—未使用。 • 1 = 已建立流程—NetFlow 資料記錄用於建立新流程。 • 2 = 已刪除流程—NetFlow 資料記錄用於結束新流程。 • 3 = 已拒絕流程—NetFlow 資料記錄指示防火牆原則拒絕了流程。 • 4 = 流程警示—未使用。 • 5 = 流程更新—NetFlow 資料記錄被傳送用於長期流程，即持續時間長於 NetFlow 伺服器設定檔中設定的 **Active Timeout**（啟用超時）期間。	所有範本
225	postNATSourceIPv4Address	此資訊元素的定義與 sourceIPv4Address 的定義相同，但不同處為其會報告防火牆在封包周遊介面之後的網路位址轉譯期間產生的修改值。	IPv4 含 NAT 標準版 IPv4 含 NAT 企業版
226	postNATDestinationIPv4Address	此資訊元素的定義與 destinationIPv4Address 的定義相同，但不同處為其會報告防火牆在封包周遊介面之後的網路位址轉譯期間產生的修改值。	IPv4 含 NAT 標準版 IPv4 含 NAT 企業版
227	postNAPTSourceTransportPort	此資訊元素的定義與 sourceTransportPort 的定義相同，但不同處為其會報告防火牆在封包周遊介面之後的網路位址連接埠轉譯期間產生的修改值。	IPv4 含 NAT 標準版 IPv4 含 NAT 企業版
228	postNAPTDestinationTransportPort	此資訊元素的定義與 destinationTransportPort 的定義相同，但不同處為其會報告防火牆在	IPv4 含 NAT 標準版 IPv4 含 NAT 企業版

©2024 Palo Alto Networks, Inc.

值	欄位	說明	範本
		封包周遊介面之後的網路位址連接埠轉譯期間產生的修改值。	
281	postNATSourceIPv6Address	此資訊元素定義與 sourceIPv6Address 的資訊元素定義相同，但不同處為其會報告防火牆在封包周遊介面之後的 NAT64 網路位址轉譯期間產生的修改值。請參閱 RFC 2460 以取得 IPv6 標頭中來源位址欄位的定義。請參閱 RFC 6146 以瞭解 NAT64 規格。	IPv6 含 NAT 標準版 IPv6 含 NAT 企業版
282	postNATDestinationIPv6Address	此資訊元素定義與 destinationIPv6Address 的資訊元素定義相同，但不同處為其會報告防火牆在封包周遊介面之後的 NAT64 網路位址轉譯期間產生的修改值。請參閱 RFC 2460 以取得 IPv6 標頭中目的地位址欄位的定義。請參閱 RFC 6146 以瞭解 NAT64 規格。	IPv6 含 NAT 標準版 IPv6 含 NAT 企業版
346	privateEnterpriseNumber	這是可識別 Palo Alto Networks 的唯一私用企業號碼：25461。	IPv4 企業版 IPv4 含 NAT 企業版 IPv6 企業版 IPv6 含 NAT 企業版
56701	App-ID	App-ID 識別的應用程式名稱。此名稱最多為 32 個位元組。	IPv4 企業版 IPv4 含 NAT 企業版 IPv6 企業版 IPv6 含 NAT 企業版
56702	使用者-ID	User-ID 識別的使用者名稱。此名稱最多為 64 個位元組。	IPv4 企業版 IPv4 含 NAT 企業版 IPv6 企業版 IPv6 含 NAT 企業版

©2024 Palo Alto Networks, Inc.

SNMP 管理員和 NetFlow 收集器中的防火牆介面識別碼

當您使用 NetFlow 收集器（請參閱 NetFlow 監控）或 SNMP 管理員（請參閱 SNMP 監控及設陷）監控 Palo Alto Networks 防火牆時，介面索引（SNMP ifindex 物件）會識別包含特定流量的介面（請參閱 SNMP 管理員中的介面索引）。相對地，防火牆網頁介面會使用介面名稱作為識別碼（例如，ethernet1/1），而非索引。若要瞭解您在 NetFlow 收集器或 SNMP 管理員中看到的統計資料適用於哪個防火牆介面，您必須具備比對介面索引與介面名稱的能力。

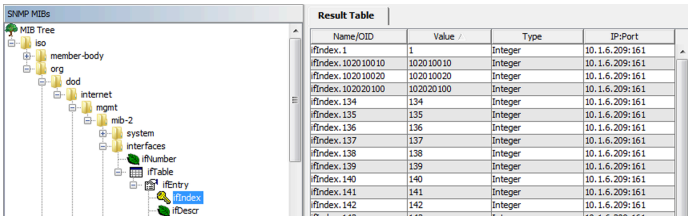


圖 **3: SNMP** 管理員中的介面索引

您可以透過瞭解防火牆用於計算索引的公式來比對索引與名稱。公式視平台和介面類型為實體或邏輯而異。

實體介面索引的範圍為 1-9999，防火牆計算此範圍的方式如下所示：

防火牆平台	計算	範例介面索引
VM-Series	管理連接埠個數 + 實體連接埠位移 • 管理連接埠個數—1，此為常數。 • 實體連接埠位移—這是實體連接埠號碼。	VM-100 防火牆，Eth1/4 = 1（管理連接埠個數） + 4（實體連接埠） = **5**
PA-220、PA-220R、PA-800 系列	管理連接埠個數 + 實體連接埠位移 • 管理連接埠個數—5，此為常數。 • 實體連接埠位移—這是實體連接埠號碼。	PA-5200 Series 防火牆，Eth1/4 = 5（管理連接埠個數） + 4（實體連接埠） = **9**
PA-3200 系列、PA-5200 系列	管理連接埠個數 + 實體連接埠位移 • 管理連接埠個數—4，此為常數。	PA-5200 Series 防火牆，Eth1/4 = 4（管理連接埠個數） + 4（實體連接埠） = **8**

©2024 Palo Alto Networks, Inc.

防火牆平台	計算	範例介面索引
	• 實體連接埠位移—這是實體連接埠號碼。	
PA-7000 系列	（連接埠數上限 * 插槽） + 實體連接埠位移 + 管理連接埠個數 • 連接埠數上限—64，此為常數。 • 插槽—這是網路介面卡的底座插槽數。 • 實體連接埠位移—這是實體連接埠號碼。 • 管理連接埠個數—5，此為常數。	PA-7000 系列防火牆，Eth3/9 = [64（連接埠數上限）* 3（插槽）] + 9（實體連接埠） + 5（管理連接埠個數）= **206**

所有平台的邏輯介面索引是 9 位數的數字，防火牆計算此數字的方式如下所示：

介面類型	範圍	數字 **9**	數字 **7-8**	數字 **5-6**	數字 **1-4**	範例介面索引
Layer 3 子介面	101010001-199999999	類型：1	介面插槽：1-9 (01-09)	介面連接埠：1-9 (01-09)	子介面：尾碼 1-9999 (0001-9999)	Eth1/5.22 = 100000000 (類型) + 100000 (插槽) + 50000 (連接埠) + 22 (尾碼) = **101050022**
Layer 2 子介面	101010001-199999999	類型：1	介面插槽：1-9 (01-09)	介面連接埠：1-9 (01-09)	子介面：尾碼 1-9999 (0001-9999)	Eth2/3.6 = 100000000 (類型) + 200000 (插槽) + 30000 (連接埠) + 6 (尾碼) = **102030006**
Vwire 子介面	101010001-199999999	類型：1	介面插槽：1-9 (01-09)	介面連接埠：1-9 (01-09)	子介面：尾碼 1-9999 (0001-9999)	Eth4/2.312 = 100000000 (類型) + 400000 (插槽) + 20000 (連接埠) + 312 (尾碼) = **104020312**
VLAN	200000001-200009999	類型：2	00	00	VLAN 尾碼：1-9999 (0001-9999)	VLAN.55 = 200000000 (類型) + 55 (尾碼) = **200000055**

©2024 Palo Alto Networks, Inc.

介面類型	範圍	數字 **9**	數字 **7-8**	數字 **5-6**	數字 **1-4**	範例介面索引
回送	300000001-300009999	類型：3	00	00	回送尾碼：1-9999 (0001-9999)	Loopback.55 = 300000000 (類型) + 55 (尾碼) = **300000055**
通道	400000001-400009999	類型：4	00	00	通道尾碼：1-9999 (0001-9999)	Tunnel.55 = 400000000 (類型) + 55 (尾碼) = **400000055**
彙總群組	500010001-500089999	類型：5	00	AE 尾碼：1-8 (01-08)	子介面：尾碼 1-9999 (0001-9999)	AE5.99 = 500000000 (類型) + 50000 (AE 尾碼) + 99 (尾碼) = **500050099**

©2024 Palo Alto Networks, Inc.

監控收發機

您可以監控實體設備或裝置中收發機的狀態，以簡化安裝和疑難排解。透過收發機監控（也稱為數位光學監控 (DOM)），您可以檢視傳輸偏置電流、發射功率、接收功率、收發機溫度和電源電壓等診斷資訊。請參閱以下支援收發機監控的裝置清單。

- PA-415 防火牆
- PA-445 防火牆
- PA-800 Series
- PA-1400 系列
- PA-3200 系列
- PA-3400 Series
- PA-5200 系列
- PA-5400 系列
- PA-7000 系列

使用命令列介面執行收發機監控。參閱以下表格獲取所有可用的 CLI 命令。

如果在不相容的收發機上執行命令，則 *CLI* 將為無法讀取的任何診斷資訊返回「不適用」。

CLI	定義
`show transceiver <interface name>`	檢視指定收發機的摘要以及每個診斷的值。 範例： `admin@PA-7080> show transceiver ethernet11/25` CLI 將返回溫度、電壓、電流、發射功率和接收功率的值。
`show transceiver-detail <interface name>`	接收更詳細的收發機規範，包括廠商資訊和連結長度。CLI 還將提供更詳細的診斷資訊。
`show transceiver all`	檢視所有作用中收發機的清單以及每個診斷的摘要。

©2024 Palo Alto Networks, Inc.

CLI	定義
`show transceiver-detail all`	獲取裝置中每個收發機的全方位詳細資料。

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

使用者-ID

與 IP 位址相反，使用者身分識別是有效安全性基礎結構的構成元件。知道是誰在網路上使用每個應用程式以及誰可能傳輸了威脅或正在傳輸檔案，可以強化安全性原則並減少事件回應次數。User-ID™ 是 Palo Alto Networks 防火牆的一項標配功能，可以讓您利用各種存放庫中儲存的使用者資訊。下列主題詳細介紹了 User-ID 及其設定方法：

User-ID 概要介紹

User-ID™ 允許您使用多種方法識別網路上的所有使用者，以確保您可以識別各個位置使用各種存取方法和作業系統（包括 Microsoft Windows、Apple iOS、Mac OS、Android 和 Linux®/UNIX）的使用者。瞭解使用者是哪些人而不僅僅是他們的 IP 位址，可以實現：

- 可見性—更好地監控使用者使用應用程式的情況，讓您可以更清晰地瞭解網路活動。當您發現網路上有陌生或不熟悉的應用程式時，User-ID 的作用將非常明顯。您的安全性團隊可使用 ACC 或日誌檢視器來識別該應用程式、使用者、頻寬和工作階段消耗情況、應用程式流量的來源及目的地，以及任何相關的威脅。
- 原則控制—將使用者資訊與安全性原則規則繫結，有助於安全地啟用在網路中周遊的應用程式，確保僅處於業務需求而要存取該應用程式的使用者才有存取權。例如，某些應用程式，例如提供人力資源服務（例如工作日或現時服務）存取權限的 SaaS 應用程式，必須提供給網路上任何已知的使用者。但是，對於更敏感的應用程式，您可透過確保僅有需求的使用者才可以存取這些應用程式來減少攻擊面。例如，雖然 IT 支援人員可能對存取遠端桌面應用程式具有合法需求，但大多數使用者沒有。
- 記錄、報告、鑑識—如果發生安全性事件，基於使用者資訊而非僅 IP 位址的鑑識分析和報告能夠提供該事件更詳細的資訊。例如，您可以使用預先定義的「使用者/群組活動」報告，來查看各使用者或使用者群組的 Web 活動摘要，或使用「SaaS 應用程式使用情況」報告來查看哪些使用者透過非認可 SaaS 應用程式傳輸的資料最多。

若要強制執行使用者與群組原則，防火牆必須可將封包中收到的 IP 位址對應至使用者名稱。User-ID 提供許多可收集這項使用者識別資訊的機制。例如，User-ID 代理程式可監控伺服器日誌中的登入事件，以及從驗證服務中接聽 syslog 訊息。若要識別代理程式未對應之 IP 位址的對應，您可以設定驗證原則將 HTTP 要求重新導向至「驗證入口網站」登入。您可以針對您的環境定制使用者對應機制，甚至還可以在不同的網站使用不同的機制，以確保隨時為各個位置的使用者安全地啟用應用程式存取。

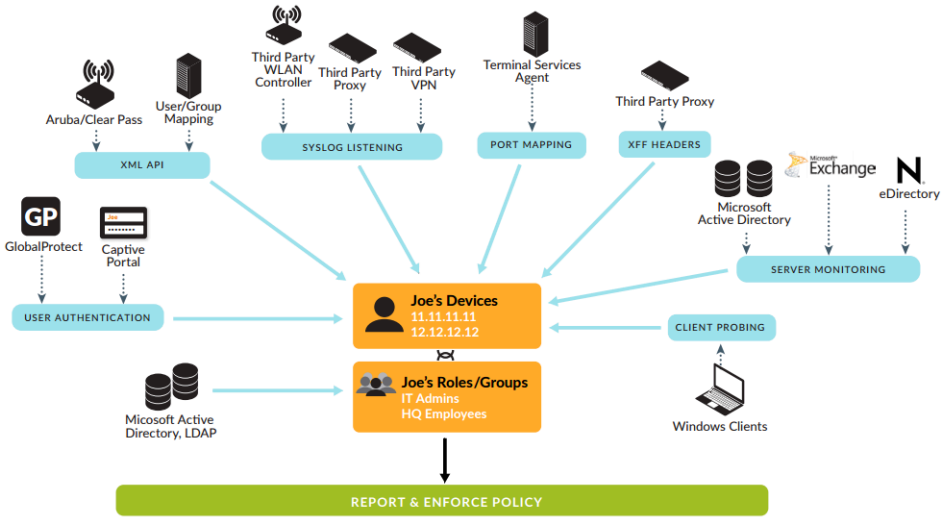


圖 **4:** 使用者**-ID**

©2024 Palo Alto Networks, Inc.

若要啟用基於使用者與群組的原則強制，防火牆必須要有可用的使用者及其對應群組成員的清單，供您在定義原則規則時選取群組。防火牆將透過直接連線 LDAP 目錄伺服器或利用 XML API 與目錄伺服器整合，以收集群組對應資訊。

如需 User-ID 運作方式的相關資訊，請參閱 User-ID 概念，如需設定 User-ID 的指示，請參閱啟用 User-ID。

User-ID 不適用於在防火牆將 *IP* 位址對應至使用者名稱之前必須對使用者的來源 *IP* 位址進行 *NAT* 轉譯的環境。

©2024 Palo Alto Networks, Inc.

User-ID 概念

- 群組對應
- 使用者識別

群組對應

若要根據使用者或群組定義原則規則，請先建立 LDAP 伺服器設定檔，以定義防火牆對您的目錄伺服器進行連接和驗證的方式。防火牆支援多種目錄伺服器，其中包括 Microsoft Active Directory (AD)、Novell eDirectory 和 Sun ONE 目錄伺服器。伺服器設定檔也可定義防火牆將如何搜尋目錄以擷取群組清單和對應的成員清單。若您使用並非防火牆原生支援的目錄伺服器，可以使用 XML API 整合群組對應功能。然後，您可以建立群組對應設定以 將使用者對應至群組 和 啟用使用者與群組原則。

根據群組成員資格（而不是個別使用者）來定義原則規則，將可簡化管理作業，因為您無須在每次有新使用者新增至群組時更新規則。在設定群組對應時，您可以限定哪些群組將可在原則規則中使用。您可以指定已存在於目錄服務中的群組，或根據 LDAP 篩選器來定義自訂群組。定義自訂群組可能會比在 LDAP 伺服器上建立新群組或變更現有群組來得快，且不需要 LDAP 管理員操作。User-ID 會將符合篩選器的所有 LDAP 目錄使用者對應至自訂群組。例如，您可能希望有安全性原則能允許行銷部門的承包商存取社交網路網站。如果沒有該部門的 Active Directory 群組存在，您可以設定一個 LDAP 篩選器，以比對將 LDAP 屬性「部門」設為「行銷」的使用者。以使用者群組為基礎的日誌查詢和報告，將會包含自訂群組。

使用者識別

瞭解使用者及群組名稱只是其中一步。防火牆也需要瞭解哪個 IP 位址對應至哪個使用者，以便能適當地強制執行安全性規則。User-ID 概要介紹說明用於在網路上識別使用者與群組的不同方法，並顯示使用者對應與群組對應如何一起合作，以啟用基於使用者與群組的安全性執行與可見度。下列主題說明不同的使用者識別方法：

- 伺服器監控
- 連接埠對應
- Syslog
- XFF 標頭
- 使用者名稱標頭插入
- 驗證原則和驗證入口網站
- GlobalProtect
- XML API
- 用戶端探測

©2024 Palo Alto Networks, Inc.

伺服器監控

當伺服器監控 User-ID 代理程式時—無論是在您網路中的網域伺服器上執行的 Windows 代理程式，或在防火牆上執行的整合了 PAN-OS 的 User-ID 代理程式—會監控指定 Microsoft Exchange Server、網域控制站或 Novell eDirectory 伺服器安全性事件日誌中的登入事件。例如，在 AD 環境中，您可以設定 User-ID 代理程式監控 Kerberos 票證授予或更新的安全性日誌、Exchange 伺服器存取 (如已設定) 及檔案和列印服務連線。若要在安全性日誌中記錄這些事件，則必須設定 AD 網域才能成功記錄帳戶登入事件。此外，由於使用者可以登入網域中的任何伺服器，因此您必須為所有伺服器設定伺服器監控，才能擷取所有的使用者登入事件。如需詳細資訊，請參閱使用 User-ID 代理程式設定使用者對應或使用 PAN-OS 整合的 User-ID 代理程式設定使用者對應。

連接埠對應

在擁有多重使用者系統的環境中 (例如 Microsoft Terminal Server 或 Citrix 環境)，許多使用者都共用相同的 IP 位址。在此情況下，使用者與 IP 位址的對應程序便需要各用戶端來源連接埠的知識。若要執行此類對應，您必須在 Windows/Citrix 終端機伺服器上安裝 Palo Alto Networks 終端機服務代理程式，干預指定來源連接埠至各使用者的處理程序。對於不支援終端機服務代理程式的終端機伺服器（例如 Linux 終端機伺服器），您可以使用 XML API，從登入和登出事件中將使用者對應資訊傳送至 User-ID。如需設定詳細資料，請參閱設定終端伺服器使用者的使用者識別。

XFF 標頭

如果您在網路使用者與防火牆之間部署了 Proxy 伺服器，防火牆會將 Proxy 伺服器 IP 位址視為 Proxy 所轉送 HTTP/HTTPS 流量中的來源 IP 位址，而非要求內容之用戶端的 IP 位址。在許多狀況下，Proxy 伺服器會將 X-Forwarded-For (XFF) 標頭新增到包含用戶端（已請求內容或發起請求）實際 IPv4 或 Ipv6 位址的流量封包。在此類情況下，您可將防火牆設定為從 XFF 中擷取一般使用者 IP 位址，從而使 User-ID 可將 IP 位址對應至使用者名稱。透過這一點，您可將 XFF 值用於原則和記錄來源使用者，以便能夠執行以使用者為基礎的原則，為 Proxy 伺服器後的使用者安全啟用 Web 應用程式的存取。

使用者名稱標頭插入

當您使用 Palo Alto Networks 設定次要執行裝置以強制執行基於使用者的原則時，次要裝置可能沒有來自防火牆的 IP 位址至使用者名稱對應。將使用者身份傳輸到下游裝置可能需要部署其他裝置（例如 Proxy），或對使用者的體驗產生負面影響（例如，使用者須登入多次）。您可以動態地將網域和使用者名稱新增到使用者傳出流量的 HTTP 標頭中，從而允許您在 Palo Alto Networks 防火牆中使用的任何次要裝置以接收使用者的資訊並執行基於使用者的原則。透過將使用者名稱和網域插入流量標頭中來包括使用者身份，啟用執行基於使用者的原則，而不會對使用者的體驗或其他基礎架構的部署造成負面影響。

驗證原則和驗證入口網站

在某些情況下，User-ID 代理程式無法使用服務器監控或其他方式將 IP 位址對應至使用者名稱（例如，如果使用者未登入或使用了網域伺服器不支援的作業系統，例如 Linux）。在其他情況下，您可能希望使用者在存取敏感應用程式時進行驗證，而無論 User-ID 代理程式使用何種方式執行使用者對應。對於所有這些情況，您可以參閱設定驗證原則和使用驗証入口網站將 IP 位址對應至使用

©2024 Palo Alto Networks, Inc.

者名稱。任何與驗證原則規則相符的 Web 流量（HTTP 或 HTTPS）會提示使用者透過驗證入口網站進行驗證。您可以使用以下驗證入口網站驗證方法：

- 瀏覽器挑戰—使用 Kerberos 單一登入（如果您想減少使用者必須回應的登入提示數量）。
- Web 表單—使用多因素驗證、SAML 單一登入、Kerberos、TACACS+、RADIUS、LDAP 或 本機驗證。
- 用戶端憑證驗證。

Syslog

您的環境可能已有驗證使用者的網路服務。這些服務包括無線控制器、802.1x 裝置、Apple Open Directory 伺服器、Proxy 伺服器或其他網路存取控制 (NAC）機制。您可以設定這些服務傳送包含登入和登入事件資訊的 syslog 訊息，並設定 User-ID 代理程式剖析這些訊息。User-ID 代理程式剖析登入事件，以對應 IP 位址到使用者名稱，並剖析登出事件，以刪除過期的對應。刪除過期對應在 IP 位址指派經常變更的環境中會特別有用。

整合了 PAN-OS 的 User-ID 代理程式和基於 Windows 的 User-ID 代理程式均使用 Syslog 剖析設定檔來剖析 syslog 訊息。在服務以不同格式傳送訊息的環境中，您可以為每種格式建立自訂設定檔，並為每個 syslog 傳送程式關聯多個設定檔。如果您使用整合了 PAN-OS 的 User-ID 代理程式，則可以使用 Palo Alto Networks 透過應用程式內容更新提供的預先定義 Syslog 剖析設定檔。

Syslog 訊息必須符合下列準則才可供 User-ID 代理程式進行剖析：

- 每個訊息都必須是單行文字字串。允許用於分行的分隔符號為換行字元 (**\n**) 或歸位字元加上換行字元 (**\r\n**)。
- 個別訊息的大小上限為 8,000 個位元組。
- 透過 UDP 傳送的訊息必須包含在單一封包中；透過 SSL 傳送的日誌訊息可跨越多個封包。單一封包可包含多個訊息。

如需設定詳細資料，請參閱設定 User-ID 以監控用於使用者對應的 Syslog 傳送程式。

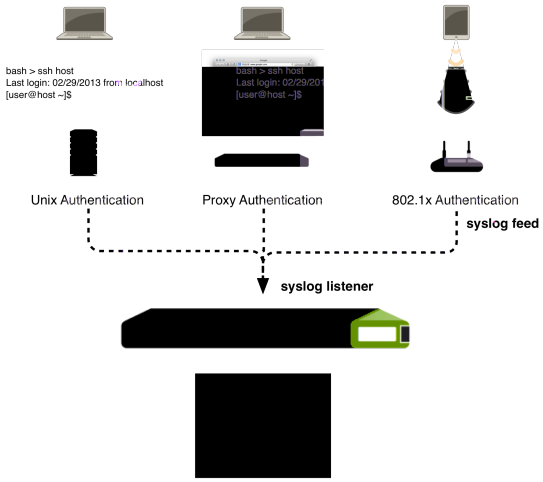


圖 **5: User-ID** 與 **Syslog** 整合

©2024 Palo Alto Networks, Inc.

GlobalProtect

針對行動或漫遊使用者，GlobalProtect 端點會為防火牆直接提供使用者對應資訊。在此狀況下，每個 GlobalProtect 使用者在其端點上均具備所執行的應用程式，其需要使用者輸入登入認證，才能透過 VPN 存取防火牆。接著此登入資訊會新增至防火牆的 User-ID 使用者識別表，以提供可見度，並執行使用者安全性原則。由於 GlobalProtect 使用者必須驗證以取得網路存取權，因此 IP 位址對使用者名稱的對應為明確已知。在敏感的環境中，亦即您必須是某種身分的使用者才能存取應用程式或服務，如此才是最佳的解決方案。如需設定 GlobalProtect 的詳細資訊，請參閱《GlobalProtect 管理者指南》。

XML API

驗證入口網站和其他標準使用者對應方法可能不適用於某些類型的使用者存取。例如，標準方法無法新增連接自第三方 VPN 解決方案的使用者或連接至啟用了 802.1x 的無線網路的使用者的對應。對於此類情況，可以使用 PAN-OS XML API 來擷取登入事件並將其傳送至整合了 PAN-OS 的 User-ID 代理程式。如需詳細資料，請參閱 使用 XML API 將使用者對應傳送至 User-ID。

用戶端探測

Palo Alto Networks 強烈建議停用用戶端探查，因為這不是在高安全性網路中獲取 *User-ID* 資訊的推薦方法。

Palo Alto Networks 不建議使用用戶端探查，因為存在以下潛在風險：

- 由於用戶端探查信任從端點報告的資料，因此在設定錯誤時可能會使您面臨安全性風險。如果您在外部非受信任介面上啟用它，會造成代理程式在您的網路外部傳送包含機密資訊（例如 User-ID 代理程式服務帳戶的使用者名稱、網域名稱和密碼雜湊）的用戶端探查。如果您未正確設定服務帳戶，則攻擊者可能會利用認證滲透網路以獲得進一步存取權限。
- 用戶端探查設計用于大部分使用者位于內部網路中 Windows 工作站上的舊版網路，但並不適用于如今在各種裝置和作業系統上支援漫游和行動使用者群體的現代網路。
- 用戶端探查可產生大量的網路流量（基於所對應之 IP 位址的總數）。

相反，Palo Alto Networks 強烈建議使用以下替代方法進行使用者對應：

- 使用更孤立且更受信任的來源（如網域控制器及與 Syslog 或 XML API 整合），以便安全地從任何裝置類型或作業系統擷取使用者對應資訊。
- 設定驗證原則和驗證入口網站，以確保您只允許授權使用者存取。

User-ID 代理程式支援 WMI 探查，它使用 PAN-OS 整合式 User-ID 代理程式或 Windows User-ID 代理程式。

在 Microsoft Windows 環境中，您可以設定 User-ID 代理程式以使用 Windows Management Instrumentation (WMI) Probing 來定期探查用戶端系統，從而驗證現有使用者對應是否仍然有效或者取得未對應之 IP 位址的使用者名稱。

如果選擇在受信任區域啟用探查，代理程式將定期探查各個已知 IP 位址 (預設為每 20 分鐘，但可進行設定) 以確認相同的使用者仍為登入狀態。此外，當防火牆遭遇無使用者對應的 IP 位址時，將傳送位址至代理程式以立即探查。

©2024 Palo Alto Networks, Inc.

有關詳細資訊，請參閱使用 Windows User-ID 代理程式設定使用者對應或使用 PAN-OS 整合式 User-ID 代理程式設定使用者對應。

©2024 Palo Alto Networks, Inc.

啟用 User-ID

與 IP 位址相反，使用者身分識別是有效安全性基礎結構的構成元件。知道是誰在網路上使用每個應用程式以及誰可能傳輸了威脅或正在傳輸檔案，可以強化安全性原則並減少事件回應次數。User-ID 允許您利用各種存放庫中儲存的使用者資訊實現可見性、基於使用者和群組的原則控制，並改進日誌記錄、報告及鑑識：

STEP 1 | 在包含需要使用者存取控制來傳送要求的使用者來源區域中啟用 User-ID。

請僅在受信任的區域上啟用 *User-ID*。如果您在外部不受信任的區域（例如網際網路）上啟用 *User-ID* 和用戶端探查，則探查可能會傳送至您受保護的網路以外，而導致 *User-ID* 代理程式服務帳戶名稱、網域名稱和加密密碼雜湊等資訊的揭露，進而讓攻擊者得以對受保護的服務和應用程式進行未經授權的存取。

1. 選取 **Network**（網路） > **Zones**（區域），然後按一下區域 **Name**（名稱）。
2. **Enable User Identification**（啟用使用者識別），然後 **OK**（確定）。

STEP 2 | 為 User-ID 代理程式建立專用服務帳戶。

最佳做法是建立一個服務帳戶，提供支援您所啟用之 *User-ID* 選項的必要權限集合，以減小服務帳戶萬一洩露時的受攻擊面。

如果您計劃針對使用者登入和登出事件，使用基於 Windows 的 User-ID 代理程式或整合了 PAN-OS 的 User-ID 代理程式來監控網域控制站、Microsoft Exchange 伺服器或 Windows 用戶端，這是必需的。

STEP 3 | 將使用者對應至群組。

這可以讓防火牆連線至 LDAP 目錄並擷取群組對應資訊，以便您可以在建立原則時選取使用者名稱和群組名稱。

STEP 4 | 將 IP 位址對應至使用者。

最佳做法是，不要將用戶端探查用作高安全性網路上的使用者對應方法。用戶端探查可產生大量的網路流量，並可能在錯誤設定時導致安全性威脅。

執行此操作的方法視乎於使用者的位置、使用的系統類型以及網路上的哪些系統在收集使用者的登入和登出事件。您必須設定一個或多個 User-ID 代理程式以啟用使用者對應：

- 使用 User-ID 代理程式設定使用者對應。
- 使用整合 PAN-OS 的 User-ID 代理程式設定使用者對應。
- 設定 User-ID 以監控用於使用者對應的 Syslog 傳送程式。
- 設定終端伺服器使用者的使用者對應。
- 使用 XML API 將使用者對應傳送至 User-ID。
- 在 HTTP 標頭中插入使用者名稱.

©2024 Palo Alto Networks, Inc.

STEP 5 | 指定使用者對應要包含及排除的網路。

最佳做法是指定 *User-ID* 要包含及排除的網路。這可以讓您確保僅探查受信任的資產，不會意外建立不需要的使用者對應。

指定要包含及排除的網路的方式，取決於您是在使用基於 Windows 的 User-ID 代理程式還是在使用整合了 PAN-OS 的 User-ID 代理程式。

STEP 6 | 設定驗證原則和驗證入口網站。

在使用者要求與驗證原則規則相符的服務、應用程式或 URL 類別時，防火牆將使用驗證入口網站驗證使用者。根據驗證期間收集的使用者資訊，防火牆將建立新使用者對應或更新現有對應。驗證期間收集的對應資訊將覆寫透過其他 User-ID 方法收集的資訊。

1. 設定驗證入口網站。
2. 設定驗證原則。

STEP 7 | 啟用基於使用者與群組的原則執行。

盡可能根據群組而非使用者建立規則。如此您就不需要在每次變更使用者庫時，即必須持續更新您的規則（需要提交）。

設定 User-ID 後，您即可在定義安全性規則來源或目的地時選取使用者名稱或群組名稱：

1. 選取 **Policies**（原則） > **Security**（安全性），然後 **Add**（新增） 新規則或按一下現有規則名稱進行編輯。
2. 選取 **User**（使用者），以下列其中一種方式，在規則中指定要比對的使用者及群組：
   - 若要選取特定的使用者或群組指定為比對準則，則在 Source User（來源使用者）區段中按一下 **Add**（新增），以顯示由防火牆群組對應功能發現的使用者和群組清單。選取使用者或群組以新增規則。
   - 若要比對已驗證或尚未驗證的任何使用者，而且您不需要瞭解特定的使用者或群組名稱，請從 Source User（來源使用者）清單上方的下拉式清單選取 **known-user**（已知使用者）或 **unknown**（未知）。
3. 視需要設定剩餘的規則，然後按一下 **OK**（確定）以儲存。如需安全性規則中其他欄位的詳細資訊，請參閱設定基本安全性原則。

©2024 Palo Alto Networks, Inc.

STEP 8 | 建立安全性原則規則，以在受信任區域內安全地啟用 User-ID，並防止 User-ID 流量從網路中輸出。

遵循最佳做法網際網路閘道安全性原則，以確保僅在代理程式（Windows 代理程式及整合了 PAN-OS 的代理程式）正在監控服務並向防火牆散佈對應的區域中允許 User-ID 應用程式 (`paloalto-userid-agent`)。具體而言：

- 允許 `paloalto-userid-agent` 應用程式在代理程式所在區域以及受監控伺服器所在區域之間（最好是在裝載應用程式和受監控伺服器的特定系統之間）執行。
- 允許 `paloalto-userid-agent` 應用程式在代理程式和需要使用者對應的防火牆之間，以及在重新散佈使用者對應的防火牆和接受它們所重新散佈之資訊的防火牆之間執行。
- 拒絕在任何外部區域執行 `paloalto-userid-agent` 應用程式，例如網際網路區域。

STEP 9 | 設定防火牆從 X-Forwarded-For (XFF) 標頭取得使用者 IP 位址。

當防火牆位於網際網路與 Proxy 伺服器之間時，防火牆所發現之封包中的 IP 位址將用於 Proxy 伺服器而非使用者。若要實現使用者 IP 位址的可見性，設定防火牆使用 XFF 標頭進行使用者對應。此用此選項後，防火牆將比對 IP 位址與原則中引用的使用者名稱，以針對相關使用者及群組啟用控制和可見性。如需詳細資訊，請參閱識別透過 Proxy 伺服器連線的使用者。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Content-ID**，然後編輯 X-Forwarded-For 標頭設定。
2. 選取 **X-Forwarded-For Header in User-ID**（在 **User-ID** 中使用 **X-Forwarded-For** 標頭）。

   選取 ***Strip-X-Forwarded-For Header***（***Strip-X-Forwarded-For Header*** 標頭）不會針對原則規則中的使用者屬性停用 *XFF* 標頭；防火牆僅在將它用於使用者屬性之後才會將 *XFF* 值調整為零。
3. 按一下 **OK**（確定）儲存您的變更。

STEP 10 | 如果使用高可用性 (HA) 設定，請啟用同步。

最佳做法是，始終為 *HA* 設定啟用 ***Enable Config Sync***（啟用設定同步） 選項，以確保群組對應和使用者對應在主動和被動的防火牆之間同步。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般），然後編輯 Setup（設定）區段。
2. 選取 **Enable HA**（啟用 **HA**）。
3. 選取 **Enable Config Sync**（啟用設定同步）。
4. 輸入 **Peer HA1 IP Address**（對等 **HA1 IP** 位址），這是對等防火牆上 HA1 控制連結的 IP 位址。
5. （選用）輸入 **Backup Peer HA1 IP Address**（備份對等 **HA1 IP** 位址），這是對等防火牆上備份控制連結的 IP 位址。
6. 按一下 **OK**（確定）。

 ©2024 Palo Alto Networks, Inc.

STEP 11 | Commit（提交）您的變更。

Commit（提交）變更以將其啟用。

STEP 12 | 確認 User-ID 組態。

設定使用者對應及群組對應後，確認組態是否正常工作，是否可以安全地啟用和監控使用者和群組對應用程式和服務的存取。

 ©2024 Palo Alto Networks, Inc.

將使用者對應至群組

根據使用者群組成員資格（而不是個別使用者）來定義原則規則，將可簡化管理作業，因為您無須在每次有群組成員身份發生變更時更新規則。每個防火牆或 Panorama 可以跨所有原則參考的不同使用者群組之數目會依型號而有所不同。如需詳細資訊，請參閱「相容性矩陣」。

使用下列程序，可讓防火牆連接到您的 LDAP 目錄並擷取群組對應資訊。然後，您可以啟用基於使用者和基於群組的原則。

以下是在 *Active Directory* 環境中使用群組對應的最佳做法：

- 如果您只有一個網域，則您只需要一個帶有 *LDAP* 伺服器設定檔的群組對應組態，即可以最佳連線能力將防火牆連接到網域控制器。您最多可新增四個網域控制站到 *LDAP* 伺服器，以用作備援。請注意，對於單個網域，您無法透過新增多個群組對應組態到該網域的方式，超出單個網域四個備援網域控制站的限制。
- 如果您有多個網域和/或多個樹系，則必須建立帶有 *LDAP* 伺服器設定檔的群組對應組態，以將防火牆連線至每個網域/樹系中的網域伺服器。採取步驟以確保使用者名稱在分開的樹系中為唯一。
- 如果具有萬用群組，請您建立一個 *LDAP* 伺服器設定檔以連線到用於 *SSL* 的 *3268* 或*3269* 連接埠上的通用類別目錄伺服器的根網域，然後建立另一個 *LDAP* 伺服器設定檔以連線到 *389* 連接埠上的根網域控制器。這有助於確保使用者和群組資訊可用於所有網域和子網域。
- 使用群組對應前，為以使用者為基礎的安全性原則設定 ***Primary Username***（主要使用者名稱），因為此屬性將在原則組態、日誌以及報告中識別使用者。

STEP 1 | 新增 LDAP 伺服器設定檔。

此設定檔會定義防火牆將如何連接到它要從中收集群組對應資訊的目錄伺服器。

如果您建立使用同一基本識別名稱 *(DN)* 或 *LDAP* 伺服器的多個群組對應設定，則群組對應設定不能包含重疊的群組（例如，一個群組對應設定的包含清單不能包含也在另一群組對應設定中的群組）。

1. 選取 **Device**（裝置） > **Server Profiles**（伺服器設定檔） > **LDAP**，然後 **Add**（新增） 伺服器設定檔。
2. 輸入用來識別伺服器設定檔的 **Profile Name**（設定檔名稱）。
3. **Add**（新增）LDAP 伺服器。您可將多達四台伺服器新增至此設定檔，但它們必須屬於相同的 **Type**（類型）。對於每個伺服器，輸入 **Name**（名稱）（用於識別伺服器）、**LDAP Server**（**LDAP** 伺服器）IP 位址或 FQDN，以及伺服器 **Port**（連接埠）（預設值為 389）。

©2024 Palo Alto Networks, Inc.

4. 選取伺服器 **Type**（類型）。

   根據您的選擇（例如 **active-directory**），防火牆會在群組對應組態中自動填入正確的 LDAP 屬性。但是，如果您已自訂 LDAP 結構描述，則可能需要修改預設設定。

5. 對於 **Base DN**（基準 **DN**），輸入您要讓防火牆從中開始搜尋使用者和群組資訊之 LDAP 樹狀目錄位置的辨別名稱 (DN)。

6. 對於 **Bind DN**（繫結 **DN**）、**Password**（密碼）和 **Confirm Password**（確認密碼），輸入要繫結至 LDAP 樹狀目錄的驗證認證。

   Bind DN（繫結 **DN**）可以是完整 LDAP 名稱（例如 `cn=administrator,cn=users,dc=acme,dc=local`）或使用者主體名稱（例如 `administrator@acme.local`）。

7. 輸入 **Bind Timeout**（繫結逾時）和**Search Timeout**（搜尋逾時），單位為秒（預設值均為 30）。

8. 按一下 **OK**（確定）來儲存伺服器設定檔。

STEP 2 | 在群組對應組態中進行伺服器設定。

1. 選取 **Device**（裝置） > **User Identification**（使用者識別） > **Group Mapping Settings**（群組對應設定）。

2. **Add**（新增）群組對應組態。

3. 輸入唯一的 **Name**（名稱）以識別群組對應組態。

4. 選取您剛剛建立的 LDAP **Server Profile**（伺服器設定檔）。

5. （選用）指定 **Update Interval**（更新間隔）（以秒為單位）。根據防火牆應該多久檢查一次 LDAP 來源以獲取群組對應設定的更新，輸入一個值（範圍為 60—86400，預設值為 3600）。如果 LDAP 來源包含許多群組，則值太低可能不會留出足夠的時間來對應所有群組。

6. （選用）依預設，**User Domain**（使用者網域）欄位為空白：防火牆會自動偵測 Active Directory (AD) 伺服器的網域名稱。若您輸入值，它將取代防火牆從 LDAP 來源擷取的任何網域名稱。對於大多數設定，如果需要輸入值，請輸入 NetBIOS 網域名稱（例如，**`example`** ，而不是 **`example.com`**）。

   如果使用通用類別目錄，則輸入值將替換該伺服器中所有使用者和群組的網域名稱，包括來自其他網域中的使用者和群組。

7. （選用）若要篩選防火牆為群組對應追蹤的群組，請在群組物件區段中，輸入 **Search Filter**（搜尋篩選器）（LDAP 查詢）以及 **Object Class**（物件類別）（群組定義）。

8. （選用）若要篩選防火牆為群組對應追蹤的使用者，請在使用者物件區段中，輸入 **Search Filter**（搜尋篩選器）（LDAP 查詢）以及 **Object Class**（物件類別）（使用者定義）。

9. 確保傳群組對應組態 **Enabled**（已啟用）（預設值）。

©2024 Palo Alto Networks, Inc.

STEP 3 | （選用） 定義要為使用者與群組對應收集的使用者與群組屬性。若您想依據目錄屬性而非網域對應使用者，則需要執行此步驟。

1. 如果您的 User-ID 來源僅傳送使用者名稱，而且使用者名稱在整個組織內為唯一，請選取 **Device**（裝置） > **User Identification**（使用者識別） > **User Mapping**（使用者對應） > **Setup**（設定），並 **Edit**（編輯）Setup（設定）區段，以 **Allow matching usernames without domains**（允許比對沒有網域的使用者名稱），從而允許防火牆檢查在群組對應過程中從 LDAP 伺服器收集的唯一使用者名稱是否與原則相關的使用者相符，並避免取代來源設定檔中的網域。

   啟用此選項前，為包含收集對應的 *User-ID* 來源（例如 GlobalProtect 或驗證入口網站）之 *LDAP* 群組設定群組對應。提交變更後，*User-ID* 來源會填入沒有網域的使用者名稱。僅在群組對應過程中收集的使用者名稱可在沒有網域的情況下進行比對。如果您的 *User-ID* 來源以多種格式傳送使用者資訊，而且您啟用此選項，請驗證防火牆所收集的屬性擁有唯一首碼。若您啟用此選項，為確保正確識別使用者，群組對應的所有屬性均應為唯一。如果使用者名稱不是唯一，防火牆會在偵錯日誌中記錄錯誤。

2. 選取 **Device**（裝置） > **User Identification**（使用者識別） > **Group Mapping Settings**（使用者對應設定） > **Add**（新增） > **User and Group Attributes**（使用者與群組屬性） > **User Attributes**（使用者屬性），並輸入您想為使用者識別收集的 **Directory Attribute**（目錄屬性）。指定 **Primary Username**（主要使用者名稱）以識別防火牆上的使用者並在報告與日誌中表示使用者，這些報告與日誌將覆寫防火牆從 User-ID 來源收到的任何其他格式。

   當您選取 Server Profile（伺服器設定檔） **Type**（類型）時，防火牆將自動填入使用者與群組屬性值。根據 User-ID 的來源所傳送的使用者資訊，您可能需設定正確屬性：

   - 使用者主體名稱 **(UPN)**：**`userPrincipalName`**
   - **NetBios** 名稱：**`sAMAccountName`**
   - 電子郵件 **ID**：該電子郵件的目錄屬性
   - 多種格式：啟用 User-ID 來源前，先從使用者目錄擷取使用者對應屬性。

   如果您沒有指定主要使用者名稱，防火牆將針對各伺服器設定檔類型使用以下預設值：

屬性	Active Directory	Novell eDirectory 或 Sun ONE Directory Server
主要使用者名稱	`sAMAccountName`	`uid`
電子郵件	`mail`	`mail`
備選使用者名稱 1	`userPrincipalName`	無。
群組名稱	`name`	`cn`
群組成員	`member`	`member`

©2024 Palo Alto Networks, Inc.

3. （選用）指定 **E-Mail**（電子郵件）地址格式以及至多三種 **Alternate Username**（替代使用者名稱）格式。
4. 選取 **Device**（裝置） > **User Identification**（使用者識別） > **Group Mapping Settings**（使用者對應設定） > **Add**（新增） > **User and Group Attributes**（使用者與群組屬性） > **Group Attributes**（使用者屬性），並指定 **Group Name**（群組名稱）、**Group Member**（群組成員）以及 **E-Mail**（電子郵件）地址格式。

   必須先提交，防火牆才會從 LDAP 伺服器中收集目錄屬性。

STEP 4 | 限定哪些群組將可在原則規則中使用。

只有在要將原則規則限定於特定群組時，才須執行。對於每個群組對應組態，**Group Include List**（群組包含清單） 和 **Custom Group**（自訂群組）清單中的項目總數不能超過 640 個。每個項目可以是單一群組或群組清單。根據預設，如果未指定群組，則所有群組都可在原則規則中使用。

您所建立的任何自訂群組，都可在驗證設定檔的允許清單中使用（設定驗證設定檔和順序）。

1. 從目錄服務中新增現有的群組：
   1. 選取 **Group Include List**（群組包含清單）。
   2. 選取您希望在原則規則中顯示的可用群組，然後將其新增 (⊕) 至 Included Groups（包含的群組）。
2. 如果您的原則規則要以不符合現有使用者群組的使用者屬性作為基礎，請根據 LDAP 篩選器建立自訂群組：
   1. 選取 **Custom Group**（自訂群組），然後 **Add**（新增）群組。
   2. 輸入群組 **Name**（名稱）；此名稱在現行防火牆或虛擬系統的群組對應組態中必須是唯一的。

      如果該 **Name**（名稱）與現有 AD 群組網域的辨別名稱 (DN) 具有相同的值，防火牆將在該名稱的所有參照中使用自訂群組（例如在原則和日誌中）。
   3. 指定多達 2,048 個 UTF-8 字元的 **LDAP Filter**（**LDAP** 篩選器），然後按一下 **OK**（確定）。

      防火牆不會驗證 LDAP 篩選器，因此您必須自行確認其正確性。

      若要盡可能降低對 *LDAP* 目錄伺服器的效能影響，在篩選器中應一律使用索引屬性。
3. 按一下 **OK**（確定）儲存您的變更。

   必須先提交，自訂群組才可在原則和物件中使用。

©2024 Palo Alto Networks, Inc.

STEP 5 | **Commit**（提交）您的變更。

必須先提交，才可在原則和物件中使用自訂群組，防火牆才能從 LDAP 伺服器中收集屬性。

將防火牆設定為從 *LDAP* 伺服器擷取群組對應資訊後，但在依據其所擷取的群組設定原則前，最佳做法為等待防火牆重新整理群組對應快取或手動重新整理快取。若要驗證您目前可在原則中使用的群組，請存取防火牆 CLI 並執行 ***show user group*** 命令。若要確定防火牆下次會在何時重新整理群組對應快取，請執行 ***show user group-mapping statistics*** 命令並查看 *Next Action*。若要手動重新整理快取，請執行 ***debug user-id refresh group-mapping all*** 命令。

©2024 Palo Alto Networks, Inc.

STEP 6 | 驗證使用者與群組對應是否已正確識別使用者。

1. 選取 **Device**（裝置） > **User Identification**（使用者識別） > **Group Mapping**（群組對應） > **Group Include List**（群組包含清單），以確認防火牆已擷取所有群組。
2. 若要驗證所有使用者屬性是否已正確擷取，請使用以下 CLI 命令：

   ```
   show user user-attributes user all
   ```

   會為所有使用者顯示使用者主體名稱 (UPN)、主要使用者名稱、電子郵件屬性以及任何設定的替代使用者名稱的標準化格式：

   ```
   admin@PA-VM-8.1> show user user-attributes user all
   ```

   ```
   Primary: nam\sam-user Email: sam-user@nam.com
   ```

   ```
   Alt User Names:1) nam.com\sam-user
   ```

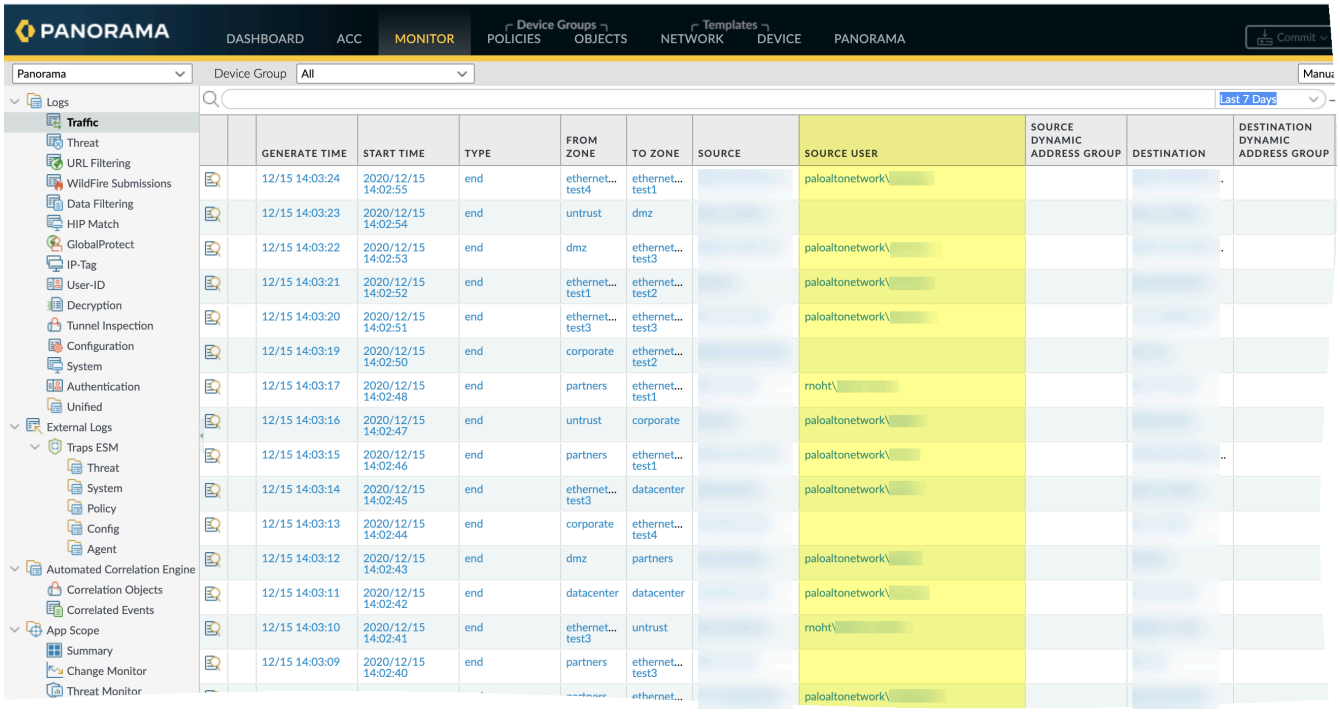
   ```
   2) nam\sam-user-upn
   ```

   ```
   3) sam-user-upn@nam.local
   ```

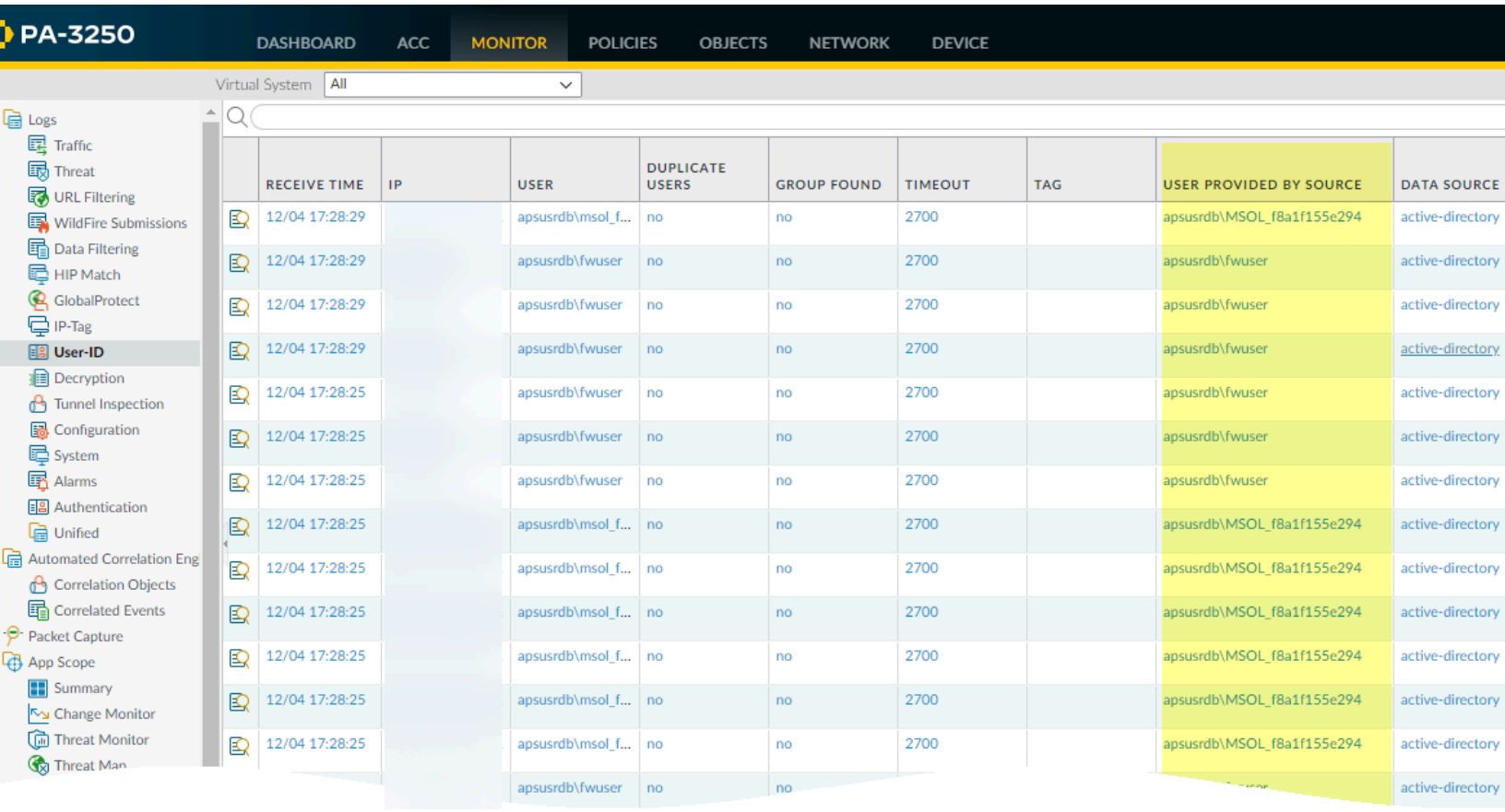
   ```
   4) sam-user@nam.com
   ```

3. 驗證 **Source User**（來源使用者）欄（在 **Monitor**（監控） > **Logs**（日誌） > **Traffic**（流量）下）中是否正確顯示使用者名稱。

©2024 Palo Alto Networks, Inc.



4. 驗證 **User Provided by Source**（由來源提供的使用者）欄（在 **Monitor**（監控） > **Logs**（日誌） > **User-ID**下）中，使用者是否對應至正確的使用者名稱。



©2024 Palo Alto Networks, Inc.

將 IP 位址對應至使用者

User-ID 提供許多將 IP 位址對應到使用者名稱的方法。在您開始設定使用者對應之前，先考量使用者將從哪裡登入、他們將存取哪些服務以及您需要控制存取哪些應用程式和資料。這將能告知您哪些類型的代理程式或整合能讓您最有效地識別使用者。

制定好計畫後，便可以開始根據需要，使用下列一種或多種方法設定使用者對應，以針對應用程式和資源啟用基於使用者的存取和可見性：

- 如果您的使用者具有未登入網域伺服器的用戶端系統（例如，使用者執行未登入網域的 Linux 用戶端），您可以使用驗證入口網站對應 IP 位址到使用者名稱。結合使用驗證入口網站和驗證原則還能確保所有使用者都需要經過驗證才能存取最敏感的應用程式和資料。
- 若要在使用者登入您的 Exchange 伺服器、網域控制器、eDirectory 伺服器或 Windows 用戶端時對應使用者，您必須設定 User-ID 代理程式：
  - 使用 PAN-OS 整合的 User-ID 代理程式設定使用者對應
  - 使用 User-ID 代理程式設定使用者對應
- 如果您的用戶端在 Windows 環境中執行多使用者系統，例如 Microsoft Terminal Server 或 Citrix Metaframe Presentation Server 或 XenApp，則設定 Palo Alto Networks 終端機伺服器 (TS) 代理程式進行使用者對應。對於不在 Windows 上執行的多使用者系統，您可以使用 PAN-OS XML API 從終端機伺服器擷取使用者對應。
- 要從驗證使用者的現有網路服務（如無線控制器、802.1x 裝置、Apple Open Directory 伺服器、Proxy 伺服器或其他網路存取控制 (NAC）機制）取得使用者對應，則設定 User-ID 以監控用於使用者對應的 Syslog 傳送程式。

  您只能在防火牆上設定 *Windows* 代理程式或整合了 *PAN-OS* 的 *User-ID* 代理程式中的一種來從網路服務接聽驗證 *syslog* 訊息，因為只有整合了 *PAN-OS* 的代理程式才支援在 *TLS* 上接聽 *syslog*，因此它是首選組態。
- 若要將使用者名稱和網域包括在傳出流量的標頭中，以便網路中的其他裝置可以識別使用者，並強制執行基於使用者的政策，您可以在 HTTP 標頭中插入使用者名稱。
- 若要在虛擬系統之間共享 User-ID 對應，您可以將虛擬系統設為 User-ID 中樞。
- 對於無法使用其他方法對應的其他用戶端，您可以使用 XML API 將使用者對應傳送至 User-ID。
- 大規模網路可能擁有數百個防火牆可查詢使用者和群組對應的資訊來源，並可擁有多個根據對應資訊強制執行原則的防火牆。先彙總對應資訊再由 User-ID 代理程式收集，如此可以為網路簡化 User-ID 管理。您也可以透過將某些防火牆設定成重新散佈對應資訊，來減少防火牆和資訊來源在查詢過程中使用的資源。如需詳細資訊，請參閱在大規模網路中部署 User-ID。

©2024 Palo Alto Networks, Inc.

為 User-ID 代理程式建立專用服務帳戶

若要使用基於 Windows 的 User-ID 代理程式或整合了 PAN-OS 的 User-ID 代理程式，在使用者登入 Exchange 伺服器、網域控制站、eDirectory 伺服器或 Windows 用戶端時對應他們，請在代理程式將監控的每個網域的網域控制站上為 User-ID 代理程式建立專用的服務帳戶。

User-ID 代理程式基於安全性事件日誌對應使用者。要確保 User-ID 代理程式可成功對應使用者，請確認對應的來源可為稽核登入、稽核 Kerberos 驗證服務和稽核 Kerberos 服務票證操作事件產生日誌。至少，來源必須可為以下事件產生日誌：

- 登入成功 (4624)
- 驗證票證已授權 (4768)
- 服務票證已授權 (4769)
- 授權的票證已更新 (4770)

該服務帳戶所需的權限視乎於您計劃使用的使用者對應方法和設定。例如，如果您使用的是整合了 PAN-OS 的 User-ID 代理程式，則該服務帳戶需要伺服器操作員權限，以監控使用者工作階段。如果您使用的是基於 Windows 的 User-ID 代理程式，則該服務帳戶不需要伺服器操作員權限，以監控使用者工作階段。為了降低 User-ID 服務帳戶洩露的風險，務必為該帳戶設定確保代理程式所需的必要權限集。

- 如果您在支援的 Windows 伺服器上安裝基於 Windows 的 User-ID 代理程式，請為 Windows User-ID 代理程式設定服務帳戶。
- 如果您在防火牆上使用整合了 PAN-OS 的 User-ID 代理程式，請為整合了 PAN-OS 的 User-ID 代理程式設定服務帳戶。

User-ID 提供了很多安全收集使用者資訊的方法。一些舊功能（用於僅需對應連接本機網路的 *Windows* 電腦上使用者的環境），需要具有特殊權限的服務帳戶。如果具有特殊權限之服務帳戶洩露，可能會導致網路遭受攻擊。最佳做法是避免使用這些舊功能，例如用戶端探查和工作階段監控，它們需要一些特殊權限，一旦帳戶洩漏將引發威脅。

為 Windows User-ID 代理程式建立服務帳戶

為 Windows User-ID 代理程式建立專用的 Active Directory (AD) 服務帳戶，以存取其為收集使用者對應而監控的服務和主機。您必須在代理程式將監控的每個網域中建立服務帳戶。啟用服務帳戶所需的權限後，使用 Windows User-ID 代理程式設定使用者對應。

以下工作流程詳細介紹了所需的全部權限，並針對需要可能引起威脅之權限的 *User-ID* 功能提供了指南，以便您自行決定如何最好地識別使用者而不會破壞整體安全性。

©2024 Palo Alto Networks, Inc.

STEP 1 | 為 User-ID 代理程式建立 AD 服務帳戶。

您必須在代理程式將監控的每個網域中建立服務帳戶。

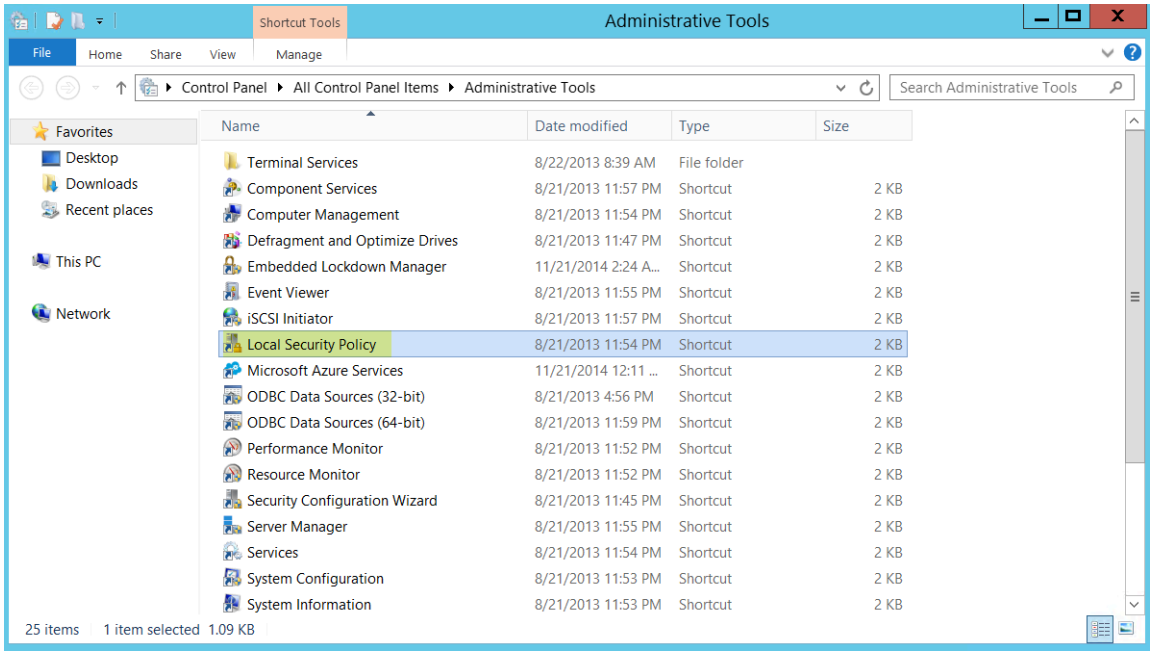
1. 登入網域控制站。
2. 以滑鼠右鍵按一下 Windows 圖示 ( )，**Search**（搜尋）**Active Directory Users and Computers**，然後啟動該應用程式。
3. 在導覽窗格中，開啟網域樹狀結構，以滑鼠右鍵按一下 **Managed Service Accounts**（受管理服務帳戶），然後選取 **New**（新建） > **User**（使用者）。
4. 輸入使用者的 **First Name**（名字）、**Last Name**（姓氏）及 **User logon name**（使用者登入名稱），然後按一下 **Next**（下一步）。
5. 輸入 **Password**（密碼），然後 **Confirm Password**（確認密碼），再按一下 **Next**（下一步）和 **Finish**（完成）。

©2024 Palo Alto Networks, Inc.

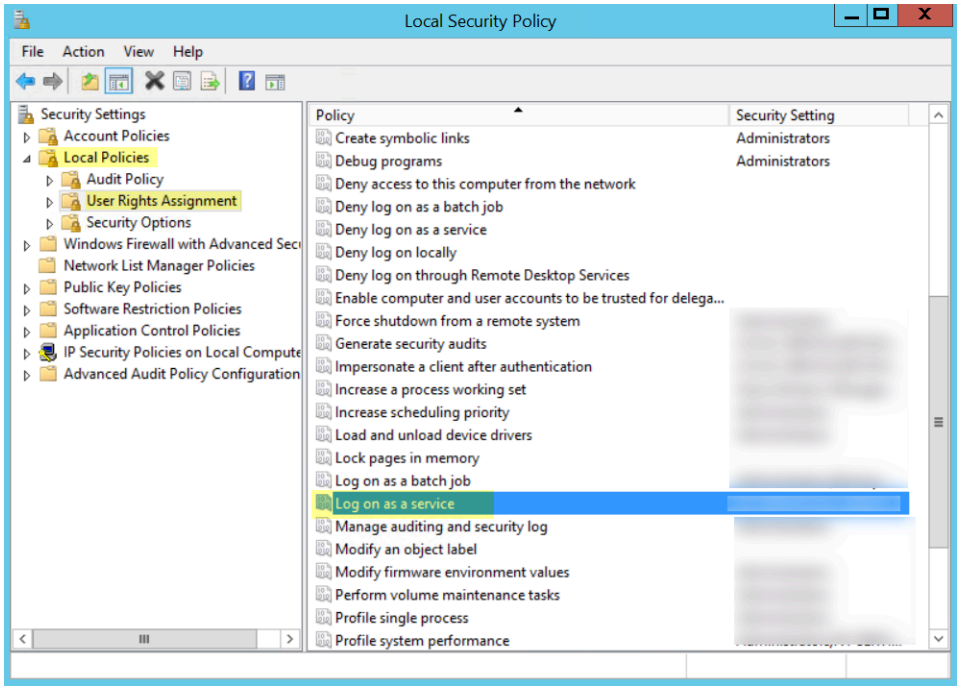
STEP 2 | 設定本機或群組原則，以允許服務帳戶作為服務登入。

僅作為代理程式主機的 Windows 伺服器本機需要作為服務登入的權限。

- 若要在本機指派權限：

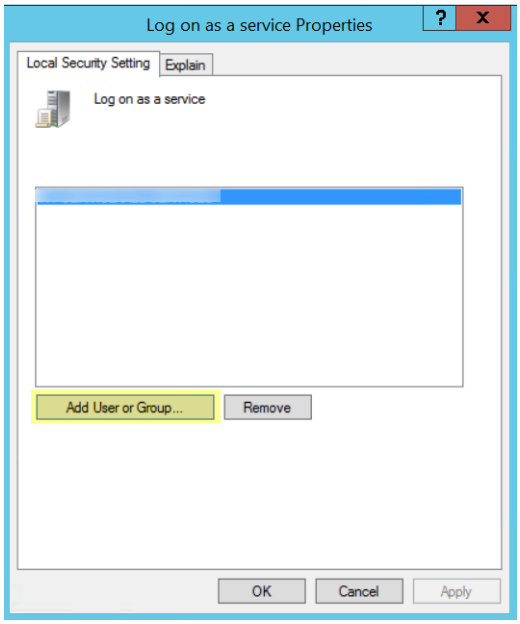
1. 選取 **Control Panel**（控制台） > **Administrative Tools**（管理工具） > **Local Security Policy**（本機安全性原則）。
2. 

3. 選取 **Local Policies**（本機原則） > **User Rights Assignment**（使用者權限指派） > **Log on as a service**（作為服務登入）。

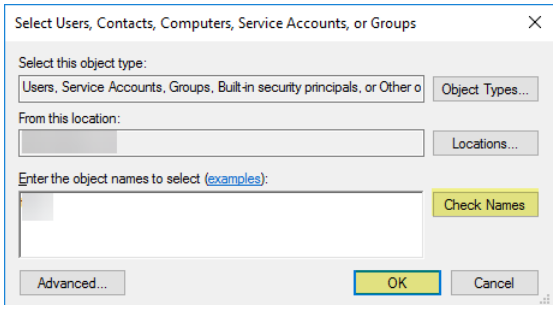


 ©2024 Palo Alto Networks, Inc.

4. **Add User or Group**（新增使用者或群組）以新增服務帳戶。



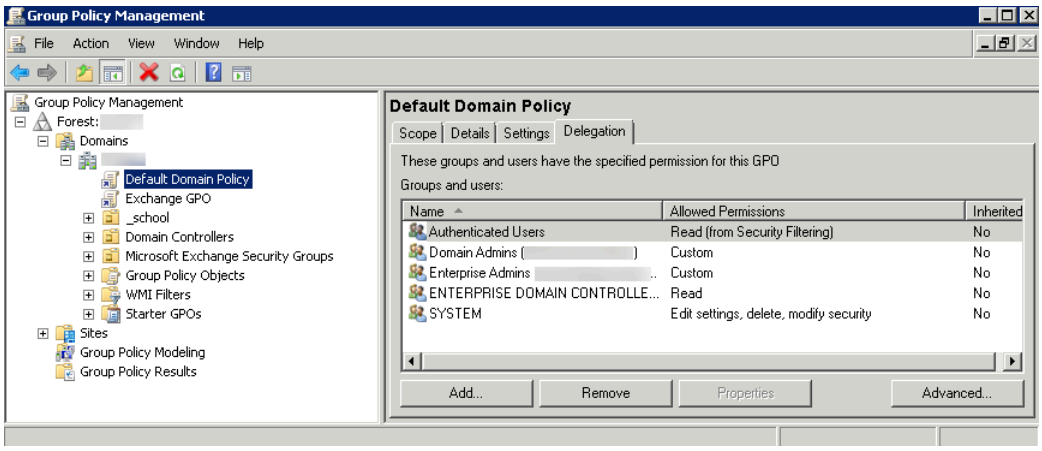
5. 以 **domain\username** 格式 **Enter the object names to select**（輸入要選取的物件名稱）（服務帳戶名稱），然後按一下 **OK**（確定）。



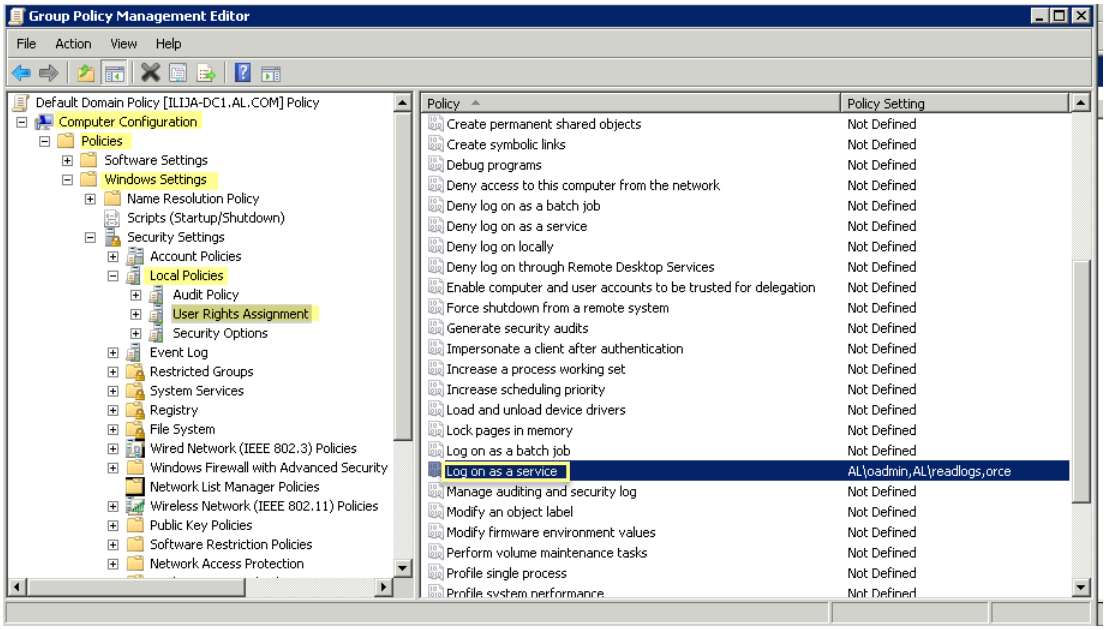
- 要在多個伺服器上安裝 Windows User-ID 代理程式時設定群組原則，請使用群組原則管理編輯器。

1. 在作為代理程式主機的 Windows 伺服器上，選取 **Start**（開始） > **Group Policy Management**（群組政策管理） > **<your domain>** > **Default Domain Policy**（預設網域政策） > **Action**（動作） > **Edit**（編輯）。

 ©2024 Palo Alto Networks, Inc.



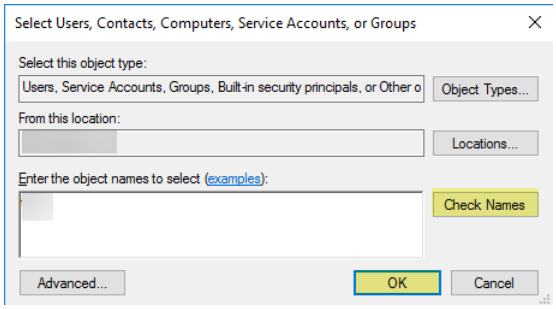
2. 選取 **Computer Configuration**（電腦組態） > **Policies**（原則） > **Windows Settings**（**Windows** 設定） > **Security Settings**（安全性設定） > **Local Policies**（本機原則） > **User Rights Assignment**（使用者權限指派）。



3. 用滑鼠右鍵按一下 **Log on as a service**（作為服務登入），然後選取 **Properties**（屬性）。
4. **Add User or Group**（新增使用者或群組）以新增服務帳戶使用者名稱或內建群組，然後按兩次 **OK**（確定）。

依預設，管理員擁有此權限。

©2024 Palo Alto Networks, Inc.



STEP 3 | 如果要使用 WMI 收集使用者資料，則為服務帳戶指派 DCOM 權限以便其可以在受監控伺服器上使用 WMI 查詢。

1. 選取 **Active Directory Users and Computers**（**Active Directory** 使用者和電腦） > **<your domain>** > **Builtin**（內建） > **Distributed COM Users**（分散式 **COM** 使用者）。
2. 用滑鼠右鍵按一下 **Properties**（屬性） > **Members**（成員） > **Add**（新增） 並輸入服務帳戶名稱。

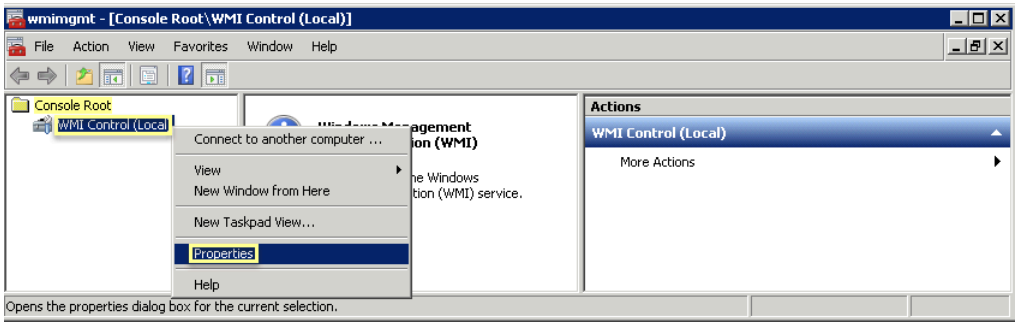
 ©2024 Palo Alto Networks, Inc.

STEP 4 | 如果您計劃使用 WMI 探查，則允許帳戶在要探查的用戶端系統上讀取 CIMV2 命名空間並指派所需權限。

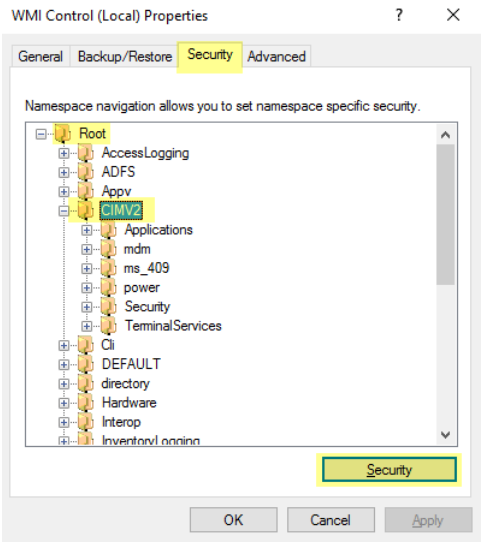
請勿在高安全性網路上啟用用戶端探查。用戶端探查可產生大量的網路流量，並可能在錯誤設定時導致安全性威脅。反之，從更多隔離與受信任來源收集使用者對應資訊，例如網域控制器及透過與 *Syslog* 或 *XML API* 整合，可帶來額外好處，讓您能夠安全地從任何裝置類型或作業系統而非僅有 *Windows* 用戶端擷取使用者對應資訊。

在 User-ID 代理程式探查使用者對應資訊的每個用戶端系統上執行此工作：

1. 以滑鼠右鍵按一下 Windows 圖示 ( )，**Search**（搜尋）**`wmimgmt.msc`**，然後啟動 WMI Management Console（WMI 管理主控台）。
2. 在主控台樹狀結構中，以滑鼠右鍵按一下 **WMI Control**（**WMI** 控制），然後選取 **Properties**（屬性）。



3. 選取 **Security**（安全性）頁籤，再選取 **Root**（根） > **CIMV2**，然後按一下 **Security**（安全性）按鈕。

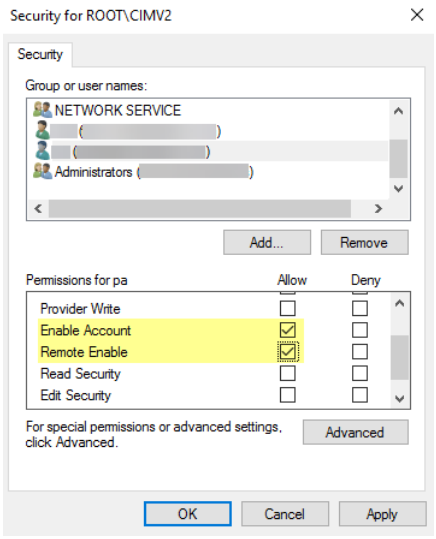


4. **Add**（新增）您所建立的服務帳戶名稱，**Check Names**（檢查名稱）以驗證項目是否正確，然後按一下 **OK**（確定）。

 ©2024 Palo Alto Networks, Inc.

您可能必須要變更 ***Locations***（位址）或按一下 ***Advanced***（進階）以查詢帳戶名稱。詳細資訊，請參閱對話方塊的說明。

5. 在 **<Username>** 區段的 Permissions（權限）中，**Allow**（允許）**Enable Account**（啟用帳戶）以及 **Remote Enable**（遠端啟用）權限。



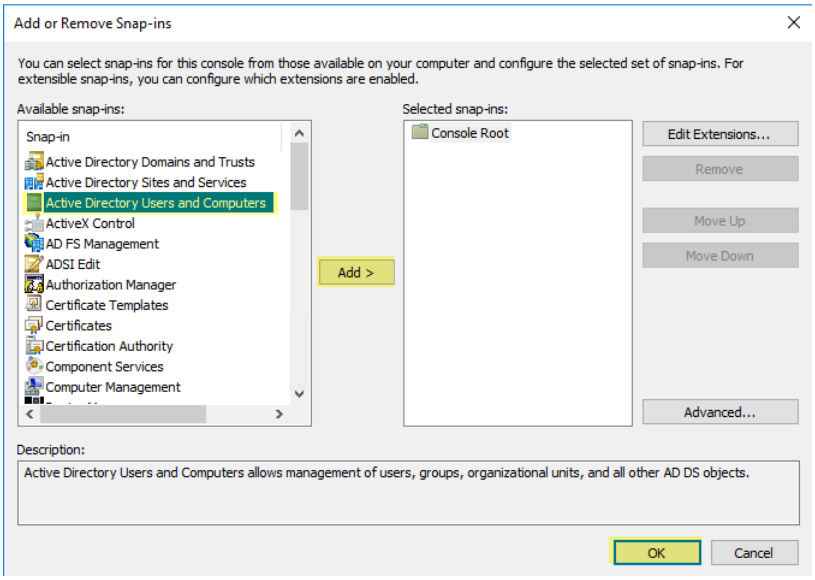
6. 按兩下 **OK**（確定）。
7. 使用本機使用者與群組 MMC 嵌入式管理單元 (lusrmgr.msc)，在將要探查的系統中將服務帳戶新增至本機分散式元件物件模型 (DCOM) 使用者與遠端桌面使用者群組。

STEP 5 | 若要使用 伺服器監控 識別使用者，則新增服務帳戶至事件日誌讀取器內建群組，以允許服務帳戶讀取安全性日誌事件。

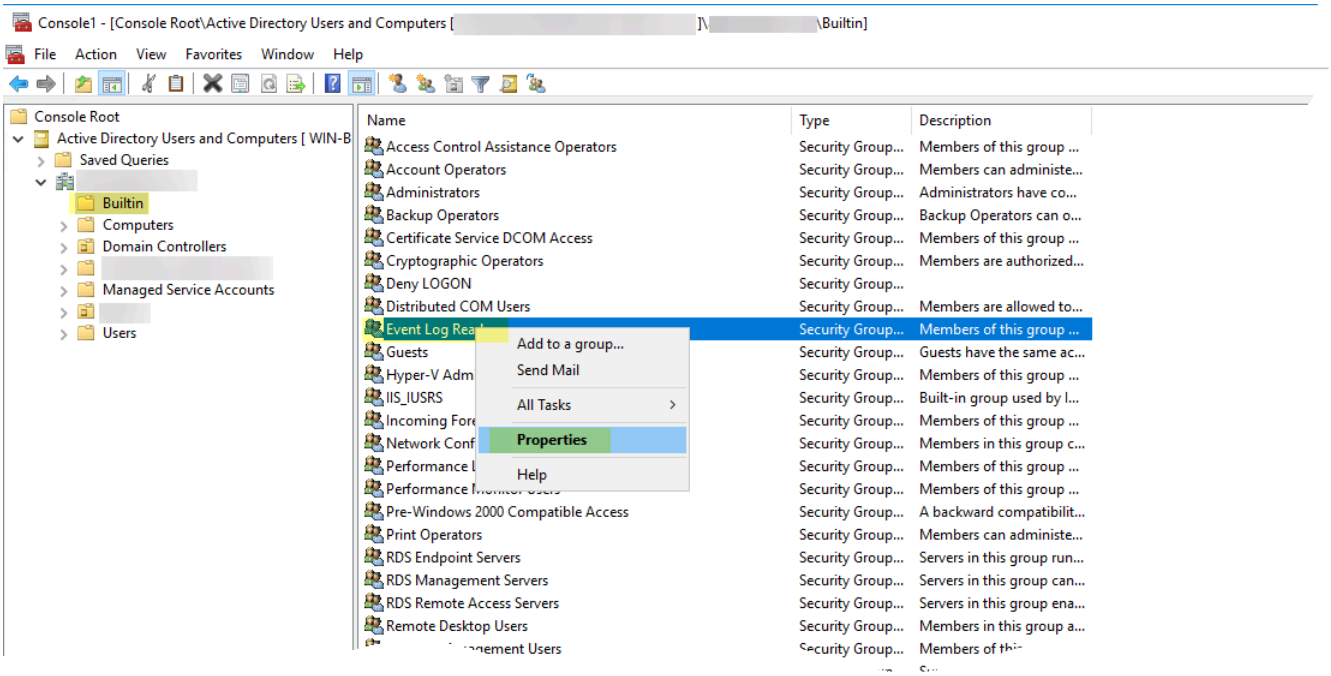
1. 在包含您希望 User-ID 代理程式讀取之日誌的網域控制站或 Exchange 伺服器上，或者在從 Windows 日誌轉送接收事件的成員伺服器上，選取**Start**（啟動）> **Run**（執行），輸入 **MMC**。
2. 選取 **File**（檔案）> **Add/Remove Snap-in**（新增/移除嵌入式管理單元）> **Active Directory Users and Computers**（**Active Directory** 使用者和電腦）> **Add**（新增），然後

©2024 Palo Alto Networks, Inc.

按一下 **OK**（確定）以執行 MMC，然後啟動Active Directory 使用者和電腦嵌入式管理單元。

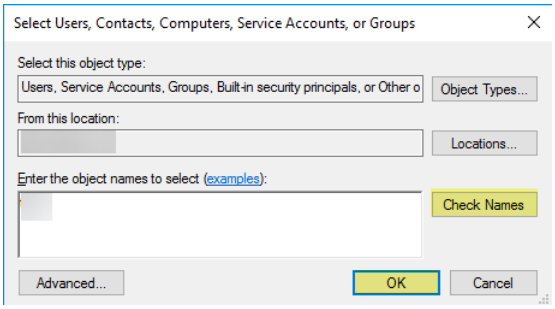


3. 導覽至網域的 Builtin 資料夾，用滑鼠右鍵按一下 **Event Log Readers**（事件日誌讀取器）群組，然後選取**Properties**（屬性） > **Members**（成員）。



4. **Add**（新增）服務帳戶的名稱，然後按一下 **Check Names**（檢查名稱）驗證您是否有正確的物件名稱。

©2024 Palo Alto Networks, Inc.



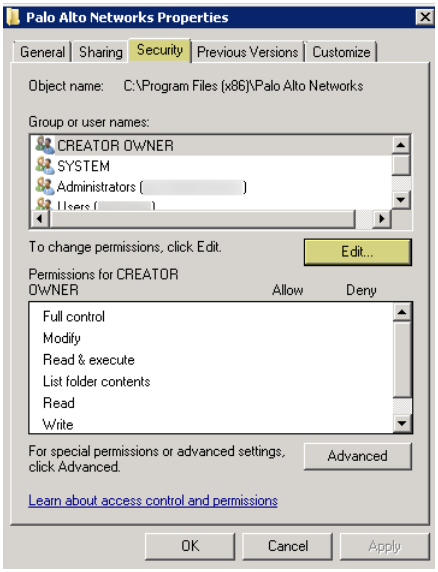
5. 按兩下 **OK**（確定）以儲存設定。
6. 確認內建事件日誌讀取器群組將服務帳戶列為成員（**Event Log Readers**（事件日誌讀取器） > **Properties**（屬性） > **Members**（成員））。

©2024 Palo Alto Networks, Inc.

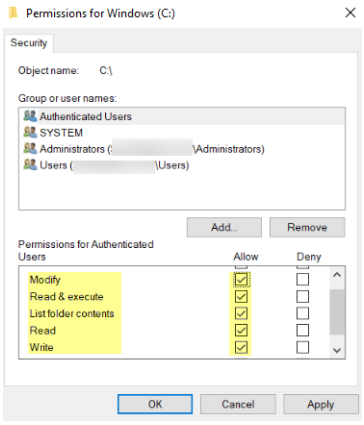
STEP 6 | 為安裝資料夾指派帳戶權限，使服務帳戶可以存取代理程式的安裝資料夾，進而讀取組態並寫入日誌。

只有在您為 User-ID 代理程式設定的服務帳戶既不是 User-ID 代理程式伺服器主機的網域管理員，也不是本機管理員時，才需執行此步驟。

1. 在 Windows 檔案總管中導覽至 **`C:\Program Files(x86)\Palo Alto Networks`**，在資料夾上按一下滑鼠右鍵，然後選取 **Properties**（屬性）。
2. 在 **Security**（安全性）頁籤上按一下 **Edit**（編輯）。



3. **Add**（新增）User-ID 代理程式服務帳戶，並 **Allow**（允許）**Modify**（修改）、**Read & execute**（讀取與執行）、**List folder contents**（清單資料夾內容）、**Read**（讀取）及**Write**（寫入）權限，然後按一下 **OK**（確定）儲存帳戶設定。

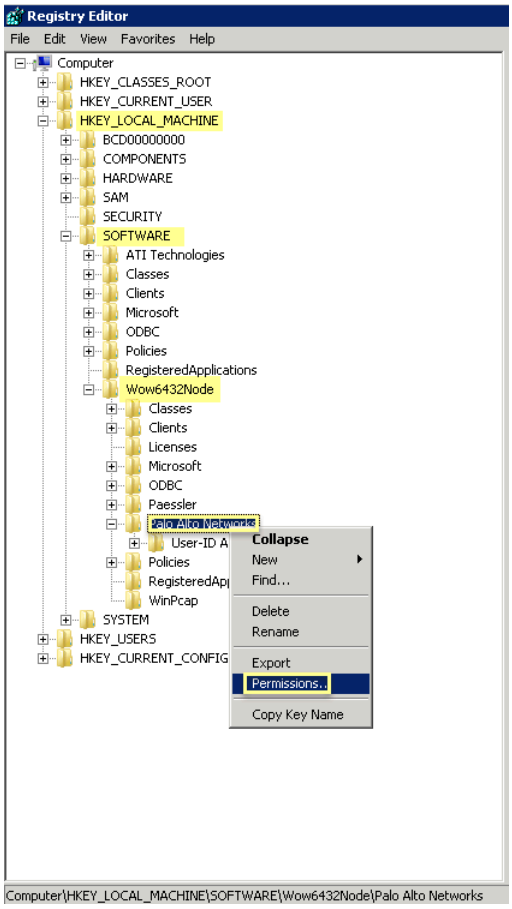


如果您不想設定個別權限，可改為 ***Allow***（允許）***Full Control***（完整控制）權限。

©2024 Palo Alto Networks, Inc.

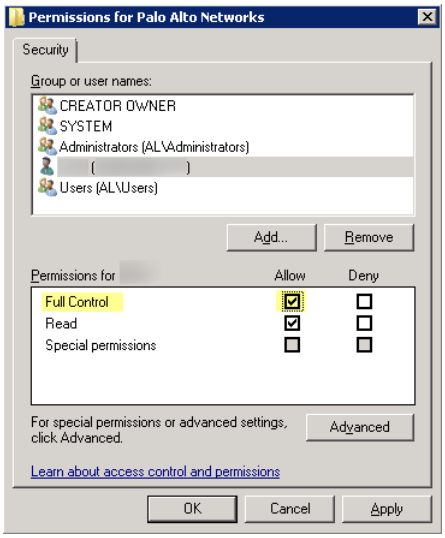
STEP 7 | 若要允許代理程式進行組態變更（例如，選取不同的日誌記錄層級時），將服務帳戶權限授予 User-ID 代理程式登錄子樹系。

1. 選取 **Start**（啟動）> **Run**（執行），然後輸入 **`regedt32`** 並導覽至下列其中一個位置的 Palo Alto Networks 子樹系：
   - **32** 位元系統—`HKEY_LOCAL_MACHINE\Software\Palo Alto Networks`
   - **64** 位元系統—`HKEY_LOCAL_MACHINE\Software\WOW6432Node\PaloAlto Networks`
2. 在 **Palo Alto Networks** 節點上按一下右鍵，然後選取 **Permissions**（權限）。



3. 將 **Full Control**（完整控制）權限指派給 User-ID 服務帳戶，然後按一下 **OK**（確定）儲存設定。

 ©2024 Palo Alto Networks, Inc.



STEP 8 | 停用不需要的服務帳戶權限。

為了減小帳戶洩漏時的受攻擊面，務必確保 User-ID 服務帳戶僅具有必要的帳戶權限集合。

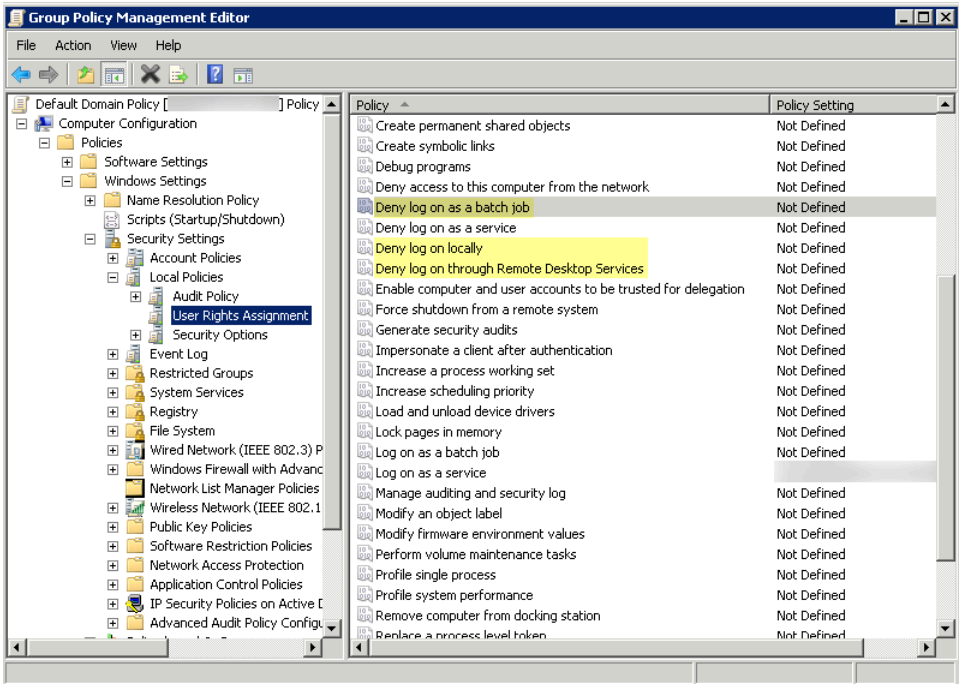
為了確保 User-ID 帳戶僅具有必要的權限，在帳戶上拒絕下列權限。

- 拒絕 **User-ID** 服務帳戶的互動式登入—由於 User-ID 服務帳戶不需要讀取或剖析 Active Directory 安全性事件日誌的權限，因此無需以互動方式登入伺服器或網域系統。您可以使用群組原則或受管理服務帳戶限制此權限（詳細資訊，請參閱 Microsoft TechNet）。

  1. 選取 **Policy Management Editor**（群組政策管理編輯器） > **Default Domain Policy**（預設網域政策） > **Computer Configuration**（電腦設定） > **Policies**（政策） > **Windows Settings**（**Windows** 設定） > **Security Settings**（安全性設定） > **User Rights Assignment**（使用者權限指派）。
  2. 在 **Deny log on as a batch job**（拒絕作為批次工作登入）、**Deny log on locally**（拒絕本機登入）和 **Deny log on through Remote Desktop Services**（拒絕透過遠端桌面服務登入）中，用滑鼠右鍵按一下 **Properties**（屬性）。

 ©2024 Palo Alto Networks, Inc.

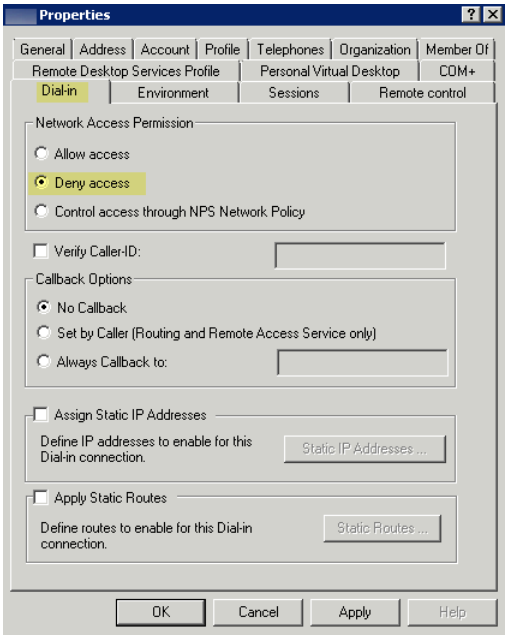
3. 選取 **Define these policy settings**（定義這些政策設定）> **Add User or Group**（新增使用者或群組）並新增服務帳戶名稱，然後按一下 **OK**（確定）。



- 拒絕遠端存取 **User-ID** 服務帳戶—這可以防止攻擊者利用帳戶從外部存取您的網路。

  1. 選取 **Start**（啟動）> **Run**（執行），輸入 **MMC**，然後選取 **File**（檔案）> **Add/Remove Snap-in**（新增/移除嵌入式管理單元）> **Active Directory Users and Computers**（**Active Directory** 使用者和電腦）> **Users**（使用者）。
  2. 用滑鼠右鍵按一下服務帳戶名稱，然後選取 **Properties**（屬性）。
  3. 選取 **Dial-in**（撥入），然後 **Deny**（拒絕）**Network Access Permission**（網路存取權限）。

©2024 Palo Alto Networks, Inc.



STEP 9 | 在下一步中，使用 Windows User-ID 代理程式設定使用者對應。

為整合了 PAN-OS 的 User-ID 代理程式設定服務帳戶

為整合了 PAN-OS 的 User-ID 代理程式建立專用的 Active Directory (AD) 服務帳戶，以存取其為收集使用者對應而監控的服務和主機。您必須在代理程式將監控的每個網域中建立服務帳戶。啟用服務帳戶所需的權限後，使用整合 PAN-OS 的 User-ID 代理程式設定使用者對應。

以下工作流程詳細介紹了所需的全部權限，並針對需要可能引起威脅之權限的 *User-ID* 功能提供了指南，以便您自行決定如何最好地識別使用者而不會破壞整體安全性。

STEP 1 | 為 User-ID 代理程式建立 AD 服務帳戶。

您必須在代理程式將監控的每個網域中建立服務帳戶。

1. 登入網域控制站。
2. 以滑鼠右鍵按一下 Windows 圖示 ( )，**Search**（搜尋）**Active Directory Users and Computers**，然後啟動該應用程式。
3. 在導覽窗格中，開啟網域樹狀結構，以滑鼠右鍵按一下 **Managed Service Accounts**（受管理服務帳戶），然後選取 **New**（新建）> **User**（使用者）。
4. 輸入使用者的 **First Name**（名字）、**Last Name**（姓氏）及 **User logon name**（使用者登入名稱），然後按一下 **Next**（下一步）。
5. 輸入 **Password**（密碼），然後 **Confirm Password**（確認密碼），再按一下 **Next**（下一步）和 **Finish**（完成）。

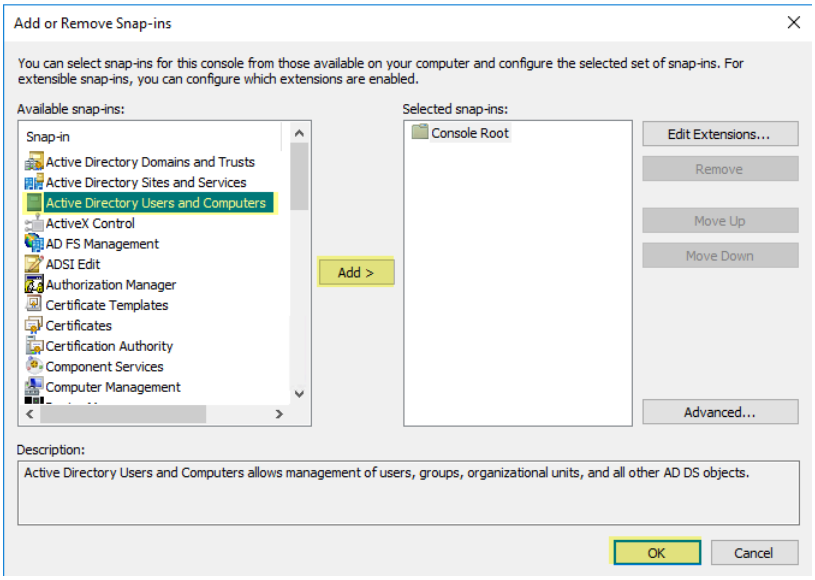
©2024 Palo Alto Networks, Inc.

STEP 2 | 若要使用 伺服器監控 識別使用者，則新增服務帳戶至事件日誌讀取器內建群組，以允許服務帳戶讀取安全性日誌事件。

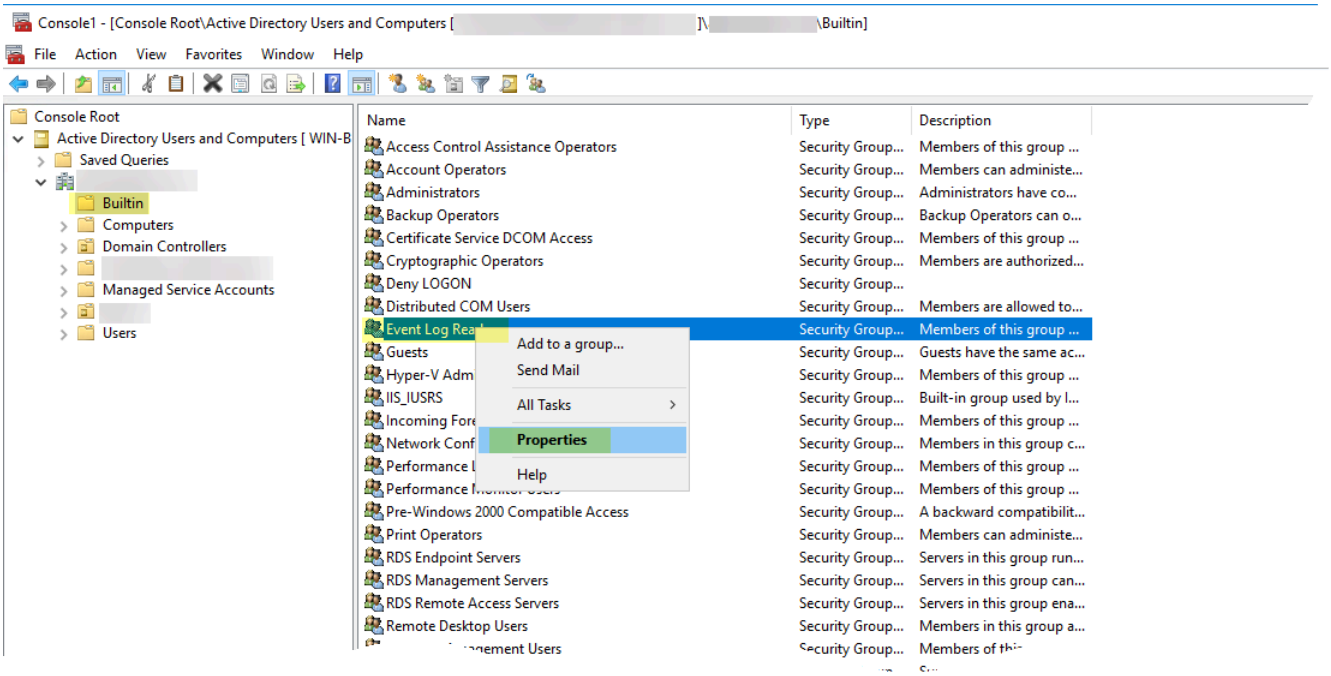
1. 在包含您希望 User-ID 代理程式讀取之日誌的網域控制站或 Exchange 伺服器上，或者在從 Windows 日誌轉送接收事件的成員伺服器上，選取**Start**（啟動） > **Run**（執行），輸入 **`MMC`**。
2. 選取 **File**（檔案） > **Add/Remove Snap-in**（新增/移除嵌入式管理單元） > **Active Directory Users and Computers**（**Active Directory** 使用者和電腦） > **Add**（新增），然後

 ©2024 Palo Alto Networks, Inc.

按一下 **OK**（確定）以執行 MMC，然後啟動Active Directory 使用者和電腦嵌入式管理單元。

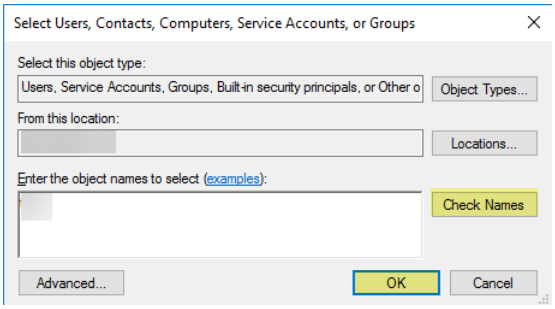


3. 導覽至網域的 Builtin 資料夾，用滑鼠右鍵按一下 **Event Log Readers**（事件日誌讀取器）群組，然後選取**Properties**（屬性） > **Members**（成員）。



4. **Add**（新增）服務帳戶的名稱，然後按一下 **Check Names**（檢查名稱）驗證您是否有正確的物件名稱。

©2024 Palo Alto Networks, Inc.



5. 按兩下 **OK**（確定）以儲存設定。
6. 確認內建事件日誌讀取器群組將服務帳戶列為成員（**Event Log Readers**（事件日誌讀取器） > **Properties**（屬性） > **Members**（成員））。

STEP 3 | 如果要使用 WMI 收集使用者資料，則為服務帳戶指派 DCOM 權限以便其可以在受監控伺服器上使用 WMI 查詢。

1. 選取 **Active Directory Users and Computers**（**Active Directory** 使用者和電腦） > **<your domain>** > **Builtin**（內建） > **Distributed COM Users**（分散式 **COM** 使用者）。
2. 用滑鼠右鍵按一下 **Properties**（屬性） > **Members**（成員） > **Add**（新增） 並輸入服務帳戶名稱。

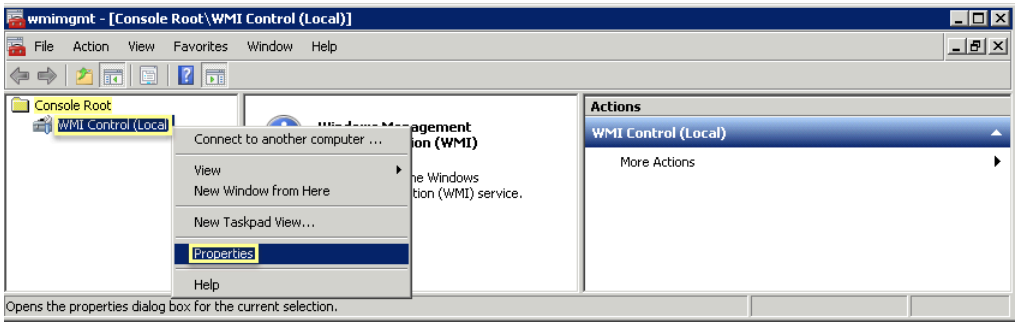
 ©2024 Palo Alto Networks, Inc.

STEP 4 | 如果您計劃使用 WMI 探查，請允許服務帳戶在要探查的用戶端系統上讀取您想要監控的網域控制器上的 CIMV2 命名空間並指派所需權限。

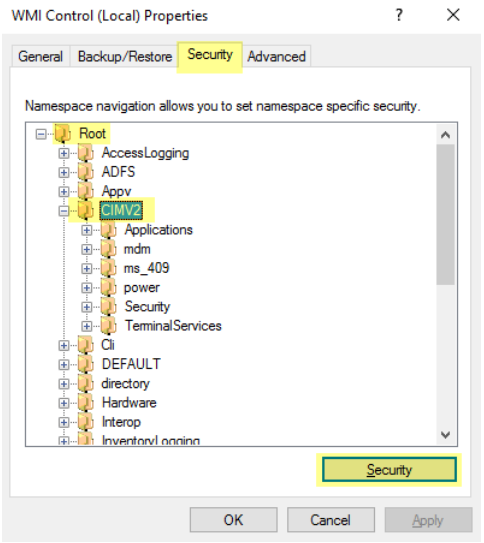
請勿在高安全性網路上啟用用戶端探查。用戶端探查可產生大量的網路流量，並可能在錯誤設定時導致安全性威脅。反之，從更多隔離與受信任來源收集使用者對應資訊，例如網域控制器及透過與 *Syslog* 或 *XML API* 整合，可帶來額外好處，讓您能夠安全地從任何裝置類型或作業系統而非僅有 *Windows* 用戶端擷取使用者對應資訊。

在 User-ID 代理程式探查使用者對應資訊的每個用戶端系統上執行此工作：

1. 以滑鼠右鍵按一下 Windows 圖示 ( )，**Search**（搜尋）**`wmimgmt.msc`**，然後啟動 WMI Management Console（WMI 管理主控台）。
2. 在主控台樹狀結構中，以滑鼠右鍵按一下 **WMI Control**（**WMI** 控制），然後選取 **Properties**（屬性）。



3. 選取 **Security**（安全性）頁籤，再選取 **Root**（根） > **CIMV2**，然後按一下 **Security**（安全性）按鈕。

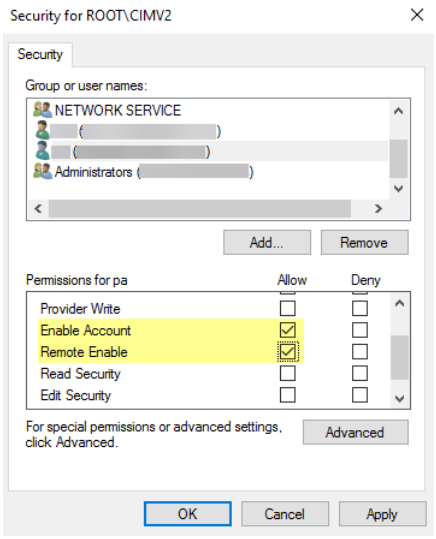


4. **Add**（新增）您所建立的服務帳戶名稱，**Check Names**（檢查名稱）以驗證項目是否正確，然後按一下 **OK**（確定）。

 ©2024 Palo Alto Networks, Inc.

您可能必須要變更 ***Locations***（位址）或按一下 ***Advanced***（進階）以查詢帳戶名稱。詳細資訊，請參閱對話方塊的說明。

5. 在 **<Username>** 區段的 Permissions（權限）中，**Allow**（允許）**Enable Account**（啟用帳戶）以及 **Remote Enable**（遠端啟用）權限。



6. 按兩下 **OK**（確定）。
7. 使用本機使用者與群組 MMC 嵌入式管理單元 (lusrmgr.msc)，在將要探查的系統中將服務帳戶新增至本機分散式元件物件模型 (DCOM) 使用者與遠端桌面使用者群組。

STEP 5 | （不建議）若要允許代理程式監控使用者工作階段以對 Windows 伺服器輪詢使用者對應資訊，則為服務帳戶指派伺服器操作員權限。

由於此群組還具有關閉和重新啟動伺服器的權限，因此僅在必須監控使用者工作階段時才將帳戶指派給此群組。

1. 選取 **Active Directory Users and Computers**（**Active Directory** 使用者和電腦） > **<your domain>** > **Builtin**（內建） > **Server Operators Group**（伺服器操作員群組）。
2. 用滑鼠右鍵按一下 **Properties**（屬性） > **Members**（成員） > **Add**（新增） 以新增服務帳戶名稱

STEP 6 | 停用不需要的服務帳戶權限。

為了減小帳戶洩漏時的受攻擊面，務必確保 User-ID 服務帳戶僅具有必要的帳戶權限集合。

為了確保 User-ID 帳戶僅具有必要的權限，在帳戶上拒絕下列權限：

- 拒絕 **User-ID** 服務帳戶的互動式登入—由於 User-ID 服務帳戶不需要讀取或剖析 Active Directory 安全性事件日誌的權限，因此無需以互動方式登入伺服器或網域系統。您可以使用群組原則或受管理服務帳戶限制此權限（詳細資訊，請參閱 Microsoft TechNet）。

  1. 選取 **Policy Management Editor**（群組政策管理編輯器） > **Default Domain Policy**（預設網域政策） > **Computer Configuration**（電腦設定） > **Policies**（政策） > **Windows**

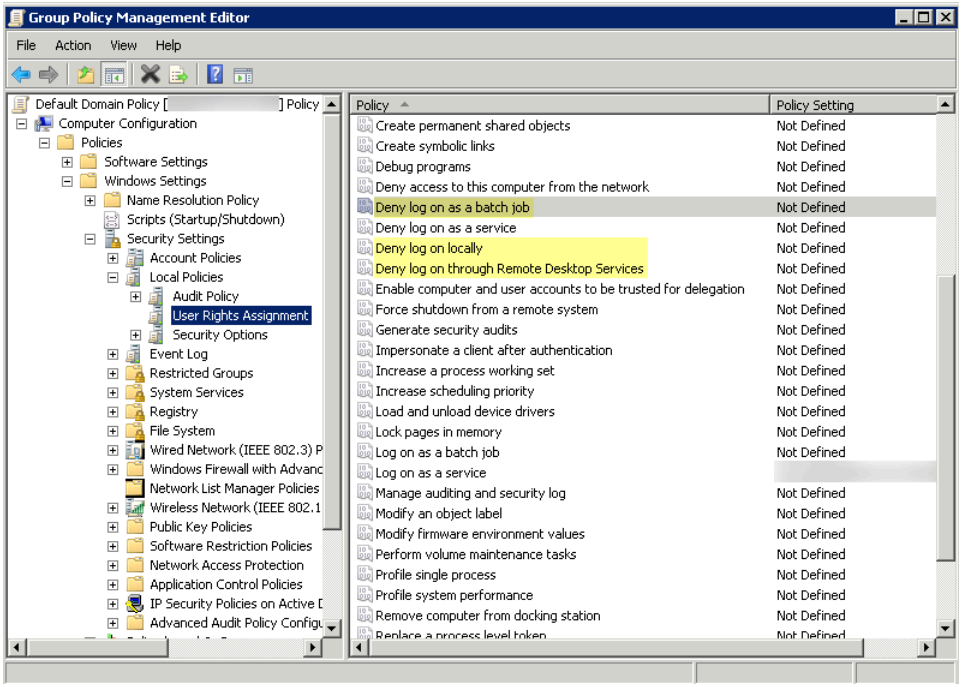
©2024 Palo Alto Networks, Inc.

Settings（**Windows** 設定） > **Security Settings**（安全性設定） > **User Rights Assignment**（使用者權限指派）。

2. 在 **Deny log on as a batch job**（拒絕作為批次工作登入）、**Deny log on locally**（拒絕本機登入）和 **Deny log on through Remote Desktop Services**（拒絕透過遠端桌面服務登入）中，用滑鼠右鍵按一下 **Properties**（屬性），選取 **Define these policy settings**（定義

©2024 Palo Alto Networks, Inc.

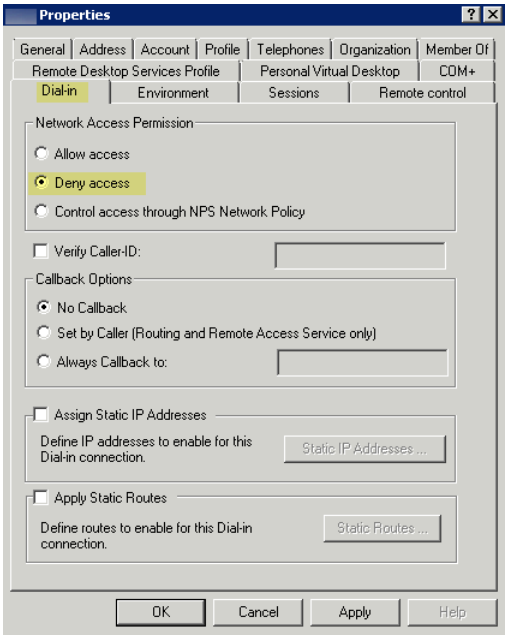
這些政策設定）> **Add User or Group**（新增使用者或群組）並新增服務帳戶名稱，然後按一下 **OK**（確定）。



- 拒絕遠端存取 **User-ID** 服務帳戶—這可以防止攻擊者利用帳戶從外部存取您的網路。

  1. **Start**（啟動）> **Run**（執行），輸入 **MMC**，然後選取 **File**（檔案）> **Add/Remove Snap-in**（新增/移除嵌入式管理單元）> **Active Directory Users and Computers**（**Active Directory** 使用者和電腦）> **Users**（使用者）。
  2. 用滑鼠右鍵按一下服務帳戶名稱，然後選取 **Properties**（屬性）。
  3. 選取 **Dial-in**（撥入），然後 **Deny**（拒絕）**Network Access Permission**（網路存取權限）。

©2024 Palo Alto Networks, Inc.



STEP 7 | 在下一步中，使用整合 PAN-OS 的 User-ID 代理程式設定使用者對應。

使用 User-ID 代理程式設定使用者對應

在大多數情況下，您主要的網路使用者皆需登入您監控的網域服務。對於這些使用者，Palo Alto Networks User-ID 代理程式會監控伺服器的登入事件，並執行 IP 位址對使用者名稱的對應。您設定 User-ID 代理程式的方式視環境大小及網域伺服器的位置而定。最佳做法是找到將監控之伺服器附近的 User-ID 代理程式（亦即受監控之伺服器與 Windows User-ID 代理程式不應互相跨越 WAN 連結）。這是因為大多數的使用者對應流量都發生在代理程式和監控伺服器之間，只有極少部分的流量 (從上次更新之後的使用者對應差異) 是從代理程式到防火牆。

下列主題說明如何安裝與設定 User-ID 代理程式，以及如何設定防火牆從代理程式擷取使用者識別資訊：

- 安裝基於 Windows 的 User-ID 代理程式
- 為使用者對應設定 Windows User-ID 代理程式

安裝基於 Windows 的 User-ID 代理程式

下列程序顯示如何將 User-ID 代理程式安裝在網域中的成員伺服器上，並設定具備必要權限的服務帳戶。如果您正在升級，則安裝程式會自動移除舊版，因此建議在執行安裝程式前，最好能先備份 config.xml 檔案。

關於安裝 *Windows User-ID* 代理程式的系統要求資訊，以及受支援伺服器作業系統版本資訊，請參閱 User-ID 代理程式版本資訊和 Palo Alto Networks 相容性矩陣。

©2024 Palo Alto Networks, Inc.

STEP 1 | 為 User-ID 代理程式建立專用的 Active Directory 服務帳戶，以存取其為收集使用者對應而監控的服務和主機。

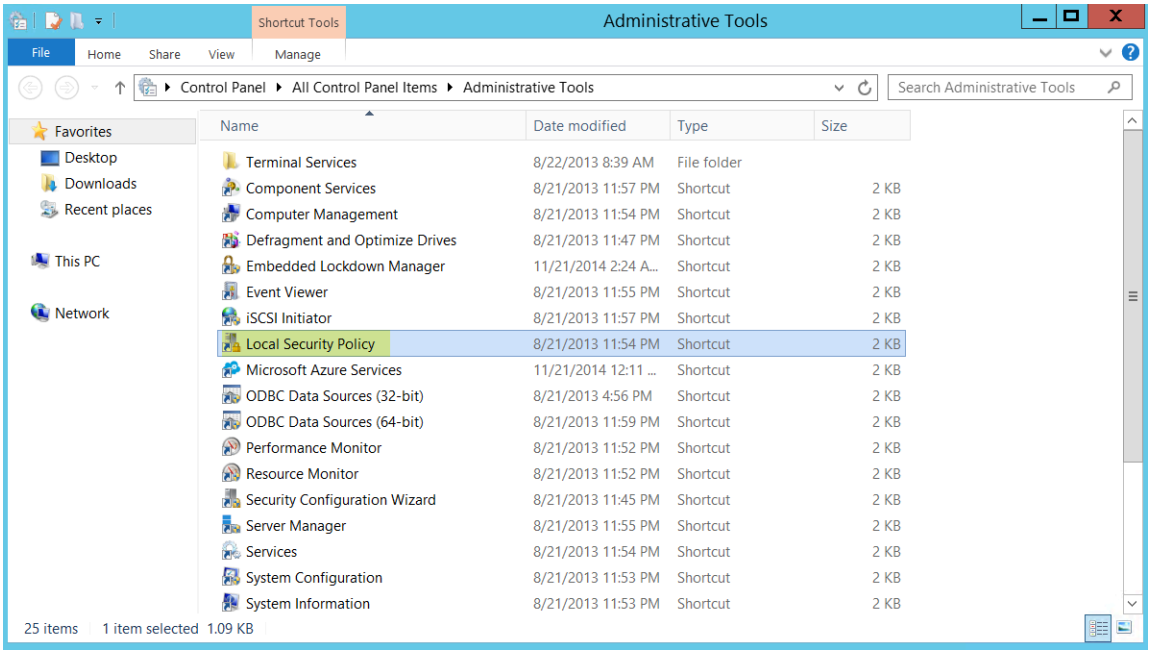
為 User-ID 代理程式建立專用服務帳戶，並為 Windows User-ID 代理程式授與必要權限。

1. 透過設定本機或群組原則，允許服務帳戶作為服務登入。

   1. 要在多個伺服器上安裝基於 Windows 的 User-ID 代理程式時設定群組政策，請為作為代理程式主機的 Windows 伺服器選取 **Group Policy Management**（群組政策管理） > **Default Domain Policy**（預設網域政策） > **Computer Configuration**（電腦組態） > **Policies**（政策） > **Windows Settings**（**Windows** 設定） > **Security Settings**（安全性設定） > **Local Policies**（本機政策） > **User Rights Assignment**（使用者權限指派）。
   2. 用滑鼠右鍵按一下 **Log on as a service**（作為服務登入），然後選取 **Properties**（屬性）。
   3. 新增服務帳戶使用者名稱或內建群組（依預設，管理員具有此權限）。

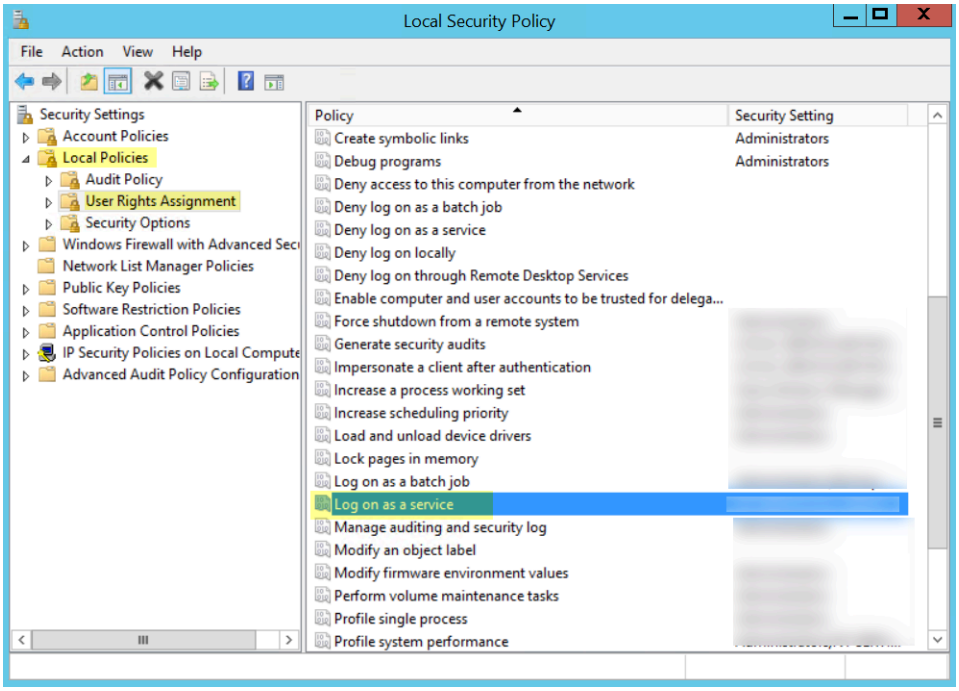
   作為代理程式主機的 *Windows* 伺服器僅本機需要作為服務登入的權限。如果您只使用一個 *User-ID* 代理程式，則可以使用下列指示在代理程式主機上本機授與權限。

   1. 若要在本機指派權限，請選取 **Control Panel**（控制台） > **Administrative Tools**（管理工具） > **Local Security Policy**（本機安全性政策）。

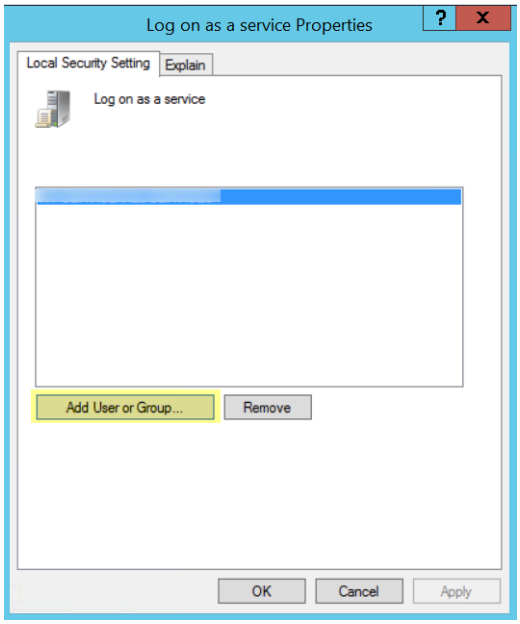


©2024 Palo Alto Networks, Inc.

2. 選取 **Local Policies**（本機政策） > **ser Rights Assignment**（使用者權限指派） > **Log on as a service**（作為服務登入）。

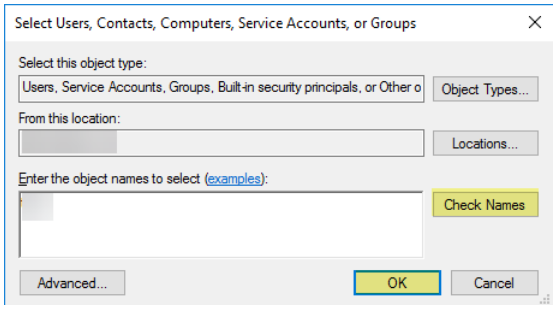


3. **Add User or Group**（新增使用者或群組）以新增服務帳戶。



©2024 Palo Alto Networks, Inc.

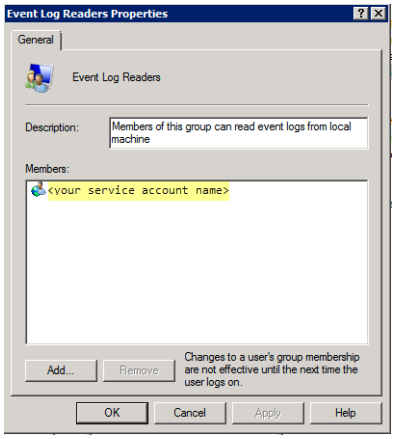
4. 在 **Enter the object names to select**（輸入要選取的物件名稱）輸入欄位中以 **domain\username** 格式輸入服務帳戶名稱，然後按一下 **OK**（確定）。



若要確認服務帳戶名稱有效，請 **Check Names**（檢查名稱）。

2. 若要使用伺服器監控識別使用者，則新增服務帳戶至事件日誌讀取器內建群組，以啟用讀取安全性日誌事件的權限。

   1. 在包含您希望 User-ID 代理程式讀取之日誌的網域控制站或 Exchange 伺服器上，或者在從 Windows 日誌轉送接收事件的成員伺服器上，執行 MMC 並啟動 Active Directory 使用者和電腦嵌入式管理單元。
   2. 導覽至網域的 Builtin 資料夾，用滑鼠右鍵按一下 **Event Log Reader**（事件日誌讀取器）群組，然後選取 **Add to Group**（新增至群組）開啟屬性對話方塊。
   3. 按一下 **Add**（新增），輸入您設定　User-ID 服務使用的服務帳戶名稱，然後按一下 **Check Names**（檢查名稱）驗證您是否有正確的物件名稱。
   4. 按兩下 **OK**（確定）以儲存設定。
   5. 確認內建事件日誌讀取器群組將服務帳戶列為成員。

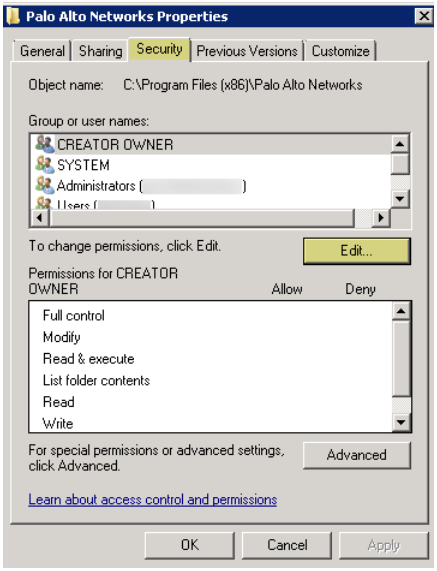


3. 為安裝資料夾指派帳戶權限，使服務帳戶可以存取代理程式的安裝資料夾，進而讀取組態並寫入日誌。

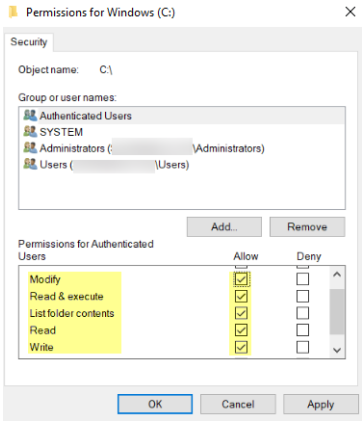
   只有在您為 User-ID 代理程式設定的服務帳戶既不是 User-ID 代理程式伺服器主機的網域管理員，也不是本機管理員時，才需執行此步驟。

©2024 Palo Alto Networks, Inc.

1. 在 Windows 檔案總管中導覽至 **`C:\Program Files(x86)\Palo Alto Networks`**（對於 32 位元系統），在資料夾上按一下滑鼠右鍵，然後選取 **Properties**（屬性）。
2. 在 **Security**（安全性）頁籤上按一下 **Edit**（編輯）。



3. **Add**（新增） User-ID 代理程式服務帳戶，並將可 **Modify**（修改）、**Read & execute**（讀取與執行）、**List folder contents**（清單資料夾內容）、**Read**（讀取）及 **Write**（寫入）的權限指派給此帳戶，然後按一下 **OK**（確定）儲存帳戶設定。



若要允許服務帳戶存取 *User-ID* 代理程式的登錄金鑰，則 ***Allow***（允許）***Full Control***（完整控制）權限。

4. 將服務帳戶權限授予 User-ID 代理程式登錄子樹系：
   1. 執行 **`regedt32`** 並導覽至以下位置的 Palo Alto Networks 子樹系：`HKEY_LOCAL_MACHINE\Software\Palo Alto Networks`。
   2. 在 Palo Alto Networks 節點上按一下右鍵，然後選取**Permissions**（權限）。
   3. 將 **Full Control**（完整控制）權限指派給 User-ID 服務帳戶，然後按一下 **OK**（確定）儲存設定。

©2024 Palo Alto Networks, Inc.

STEP 2 | 決定安裝 User-ID 代理程式的位置。

User-ID 代理程式使用 Microsoft 遠端程序呼叫 (MSRPC) 查詢網域控制站與 Exchange 伺服器日誌。在初始連線中，代理程式會傳輸日誌中最近的 50,000 個事件，以對應使用者。在每一次後續連線中，代理程式會附加時間戳記傳輸事件（晚於上次與網域控制站通訊的時間）。因此，請一律在每個具有要監控伺服器的網站上安裝一或多個 User-ID 代理程式。

- 您必須將 User-ID 代理程式安裝在執行支援作業系統的系統上：請參閱相容性矩陣中的「作業系統 (OS) 相容性 User-ID 代理程式」。系統還必須滿足最低要求（參閱 User-ID 代理程式版本資訊）。
- 確定要用來主控 User-ID 代理程式的系統，是待監控伺服器所屬之相同網域的成員。
- 最佳做法是，將 User-ID 代理程式安裝在接近待監控伺服器的位置上：由於 User-ID 代理程式與待監控伺服器之間的流量比 User-ID 代理程式與防火牆之間的流量多，因此讓代理程式接近待監控伺服器可最佳化頻寬使用。
- 為確保最為全面地對應使用者，必須監控所有為要對應的使用者處理驗證的網域控制站。您可能需要安裝多個 User-ID 代理程式，才能有效監控所有的資源。
- 若使用 User-ID 代理程式進行認證偵測，則必須將其安裝在唯讀網域控制站 (RODC) 上。最佳做法是，為此目的部署單獨的代理程式。請勿使用 RODC 上安裝的 User-ID 代理程式來將 IP 位址對應至使用者。用於認證偵測的 User-ID 代理程式安裝程式名稱為 UaCredInstall64-x.x.x.msi。

STEP 3 | 下載 User-ID 代理程式安裝程式。

安裝與防火牆上所執行 *PAN-OS* 版本相同的 *User-ID* 代理程式版本。如果沒有與 *PAN-OS* 版本相符的 *User-ID* 版本，則安裝與 *PAN-OS* 版本最接近的最新版本。

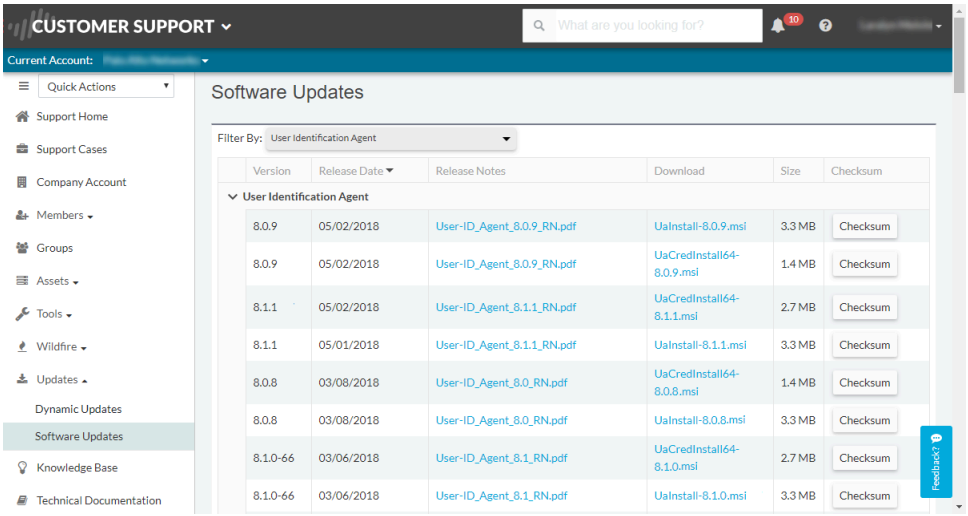
1. 登入 Palo Alto Networks 客戶支援入口網站。
2. 選取 **Updates**（更新） > **Software Updates**（軟體更新）。
3. 將 **Filter By**（篩選依據）設定為 **User Identification Agent**（使用者識別代理程式），然後選取要從相應 Download（下載）欄中安裝之 User-ID 代理程式的版本。檔案名稱使用

©2024 Palo Alto Networks, Inc.

下列格式：`UaInstall-x.x.x.msi`（其中 x 表示版本號碼）。例如，若要下載 10.0 版 User-ID 代理程式，請選取 **UaInstall-10.0.0-0.msi**。

如果您使用 User-ID 代理程式防止認證網路釣魚，請改為下載 `UaCredInstall64-x.x.x.msi` 檔案。如果您使用 User-ID 進行認證偵測，請僅下載並安裝 `UaCredInstall64-x.x.x.msi`。

4. 將檔案儲存在您計劃安裝代理程式的系統上。



STEP 4 | 以管理員身分執行安裝程式。

1. 開啟 Windows **Start**（開始）功能表，以滑鼠右鍵按一下 **Command Prompt**（命令提示）程式，然後選取 **Run as administrator**（以系統管理員身分執行）。
2. 從命令列中執行您下載的 .msi 檔案。例如，如果您將 .msi 檔案儲存在桌面上，可以輸入下列命令：

```
C:\Users\administrator.acme>cd Desktop
C:\Users\administrator.acme\Desktop>UaInstall-6.0.0-1.msi
```

3. 依照安裝提示使用預設設定安裝代理程式。依預設，代理程式會安裝到 **`C:\Program Files(x86)\Palo Alto Networks`**，但您可以 **Browse**（瀏覽）至其他位置。
4. 安裝完成時，按一下 **Close**（關閉）將設定視窗 關閉。

STEP 5 | 以管理員身分啟動 User-ID 代理程式應用程式。

開啟 Windows **Start**（啟動）功能表，以滑鼠右鍵按一下 **User-ID Agent**（**User-ID** 代理程式）程式，然後選取 **Run as administrator**（以管理員身分執行）。

必須以管理員身分執行 *User-ID* 代理程式應用程式才能安裝應用程式，提交組態變更或解除安裝應用程式。

©2024 Palo Alto Networks, Inc.

STEP 6 | （選用）變更 User-ID 代理程式登入時使用的服務帳戶。

依預設，代理程式會使用安裝 .msi 檔案時使用的管理員帳戶。若要將帳戶變更為受限帳戶：

1. 選取 **User Identification**（使用者識別） > **Setup**（設定），然後按一下 **Edit**（編輯）。
2. 選取 **Authentication**（驗證）頁籤，然後在 **User name for Active Directory**（**Active Directory** 使用者名稱）欄位中輸入您要 User-ID 代理程式使用的服務帳戶名稱。
3. 輸入指定帳戶的 **Password**（密碼）。
4. **Commit**（提交）變更至 User-ID 代理程式組態，以使用服務帳戶認證重新啟動服務。

STEP 7 | （選用）指派您自己的憑證，以使 Windows User-ID 代理程式和防火牆相互驗證。

1. 使用以下方法之一獲取 Windows User-ID 代理程式的憑證。上傳採用隱私權增強式郵件 (PEM) 格式的伺服器憑證，以及伺服器憑證的加密金鑰。
   - 產生憑證並將其匯出，以上傳至 Windows User-ID 代理程式。
   - 從企業憑證授權單位 (CA) 匯出憑證，並將其上傳至 Windows User-ID 代理程式。
2. 新增伺服器憑證到 Windows User-ID 代理程式。
   1. 在 Windows User-ID 代理程式上，選取 **Server Certificate**（伺服器憑證），然後按一下 **Add**（新增）。
   2. 輸入從 CA 接收的憑證檔案的路徑與名稱，或瀏覽該憑證檔案。
   3. 輸入私密金鑰複雜密碼。
   4. 按一下 **OK**（確定），再按一下 **Commit**（提交）。
3. 上傳憑證到防火牆，以驗證 Windows User-ID 代理程式的識別資訊。
4. 為用戶端裝置（防火牆或 Panorama）設定憑證設定檔。
   1. 選取 **Device**（裝置） > **Certificates Management**（憑證管理） > **Certificate Profile**（憑證設定檔）。
   2. 設定憑證設定檔。

      您只能為 *Windows User-ID* 代理程式和終端機伺服器 *(TS)* 代理程式指派一個憑證設定檔。因此，憑證設定檔中必須包含簽發了已上傳至所連線 *User-ID* 和 *TS* 代理程式之憑證的所有憑證授權單位。
5. 在防火牆上指派憑證設定檔。
   1. 選取 **Device**（裝置） > **User Identification**（使用者識別） > **Connection Security**（連線安全性），然後按一下編輯按鈕。
   2. 選取您在上一步中設定的 **User-ID Certificate Profile**（**User-ID** 憑證設定檔）。
   3. 按一下 **OK**（確定）。
6. **Commit**（提交）您的變更。

©2024 Palo Alto Networks, Inc.

STEP 8 | 防止認證網路釣魚。

若要使用基於 Windows 的 User-ID 代理程式偵測認證提交和防止認證網路釣魚，則必須在基於 Windows 的 User-ID 代理程式上安裝 User-ID 認證服務。您只能在唯讀網域控制站 (RODC) 上安裝此附加元件。

為使用者對應設定 Windows User-ID 代理程式

Palo Alto Networks Windows User-ID 代理程式是一種 Windows 服務，可連線至您網路上的伺服器—例如，Active Directory 伺服器、Microsoft Exchange 伺服器及 Novell eDirectory 伺服器—並監控日誌中的登入事件。代理程式會使用此資訊將 IP 位址對應至使用者名稱。Palo Alto Networks 防火牆會連線至 User-ID 代理程式以擷取此使用者識別資訊，能夠依使用者名稱檢視使用者活動，而非依 IP 位址，並能執行使用者與群組安全性。

如需 *User-ID* 代理程式支援的伺服器作業系統版本資訊，請參閱 User-ID 代理程式版本資訊中的「*User-ID* 代理程式作業系統相容性」。

STEP 1 | 定義 User-ID 代理程式會監控的伺服器，以收集 IP 位址對應使用者的資訊。

User-ID 代理程式可監控多達 100 台伺服器，其中多達 50 台可以是 syslog 寄件者。

為收集所有必要的對應項目，*User-ID* 代理程式必須連接至所有使用者登入的伺服器，以便監控所有伺服器上含登入事件的安全性日誌檔案。

1. 開啟 Windows **Start**（開始）功能表，然後選取 **User-ID Agent**（**User-ID** 代理程式）。
2. 選取 **User Identification**（使用者識別）> **Discovery**（探索）。
3. 在畫面的伺服器 區段中，按一下新增。
4. 輸入待監控伺服器的名稱及伺服器位址。網路位址可為 FQDN 或 IP 位址。
5. 選取 **Server Type**（伺服器類型）（**Microsoft Active Directory**、**Microsoft Exchange**、**Novell eDirectory** 或 **Syslog Sender**（系統日誌寄件者）），然後按一下 **OK**（確定）以儲存伺服器項目。針對每個要監控的伺服器重複此步驟。
6. （選用）若要讓 Windows User-ID 代理程式使用 DNS 查閱自動探索網路上的網域控制器，請按一下 **Auto Discover**（自動探索）。如果您有希望 Windows User-ID 代理程式探索的新網域控制器，則每次您要探索新的網域控制器時，按一下 **Auto Discover**（自動探索）。

   自動探索只會尋找本機網域中的網域控制器；您必須手動新增 *Exchange* 伺服器、*eDirectory* 伺服器及 *syslog* 寄件者。
7. （選用）若要調整防火牆輪詢所設定伺服器以取得對應資訊的頻率，可選取 **User Identification**（使用者識別）> **Setup**（設定），然後 **Edit**（編輯）Setup（設定）區段。

©2024 Palo Alto Networks, Inc.

在伺服器監控頁籤上，修改伺服器日誌監控頻率（秒數）欄位。在含舊版網域控制站或高延遲連結的環境中，將此欄位中的值增大至 5 秒。

確保未選取 ***Enable Server Session Read***（啟用伺服器工作階段讀取）。此設定需要 *User-ID* 代理程式具有 *Active Directory* 帳戶與伺服器運算子權限，以便讀取所有使用者工作階段。您需使用 *syslog* 或 *XML API* 整合來監控擷取所有裝置類型與作業系統之登入及登出事件的來源（而非僅 *Windows*），例如無線控制器及網路存取控制 *(NAC)*。

8. 按一下 **OK**（確定）以儲存設定。

STEP 2 | 指定 Windows User-ID 代理程式應在 User-ID 中包括或排除的子網路。

依預設，User-ID 會對應存取您所監控之伺服器的所有使用者。

最佳做法是指定 *User-ID* 中要包括和排除的網路，確保代理程式僅與內部資源通訊，防止對應未經授權的使用者。您只應在組織內部使用者登入的子網路上啟用 *User-ID*。

1. 選取 **User Identification**（使用者識別） > **Discovery**（探索）。
2. **Add**（新增）項目到所設定網路的包含/排除清單，然後輸入項目 **Name**（名稱），再輸入子網路的 IP 位址範圍，作為 **Network Address**（網路位址）。
3. 選擇是包括還是排除網路：
   - 包括指定網路—如果您要將使用者對應限制於僅限登入指定子網路的使用者，則選取此選項。例如，如果要包括 10.0.0.0/8，則代理程式將對應此子網路上的使用者，並排除所有其他使用者。如果您希望代理程式對應其他子網路中的使用者，則必須重複上述步驟，將其他網路新增至清單。
   - 排除特定網路—只有在您希望代理程式排除您新增的要包含之子網路的子集合時，才選取此選項。例如，如果要包括 10.0.0.0/8 並排除 10.2.50.0/22，代理程式將對應 10.0.0.0/8 的所有子網路（10.2.50.0/22 除外）上的使用者，並將排除 10.0.0.0/8 之外的所有子網路。

     如果您新增「排除」設定檔而不新增任何「包括」設定檔，*User-ID* 代理程式將排除所有子網路，而不只是您新增的子網路。
4. 按一下 **OK**（確定）。

©2024 Palo Alto Networks, Inc.

STEP 3 | （選用）如果您將代理程式設定為連線至 Novell eDirectory 伺服器，則必須指定代理程式應如何搜尋目錄。

1. 選取 **User Identification**（使用者識別） > **Setup**（設定），然後按一下視窗 Setup（設定）區段中的 **Edit**（編輯）。
2. 選取 **eDirectory** 頁籤並完成下列欄位：
   - **Search Base**—指定代理程式查詢的起點或根內容，例如：`dc=domain1,dc=example, dc=com`。
   - 繫結辨別名稱—用於繫結目錄的帳戶，例如：`cn=admin,ou=IT, dc=domain1, dc=example, dc=com`。
   - 繫結密碼—繫結帳戶密碼。代理程式會將加密的密碼儲存在設定檔案中。
   - 搜尋篩選器—使用者項目的搜尋查詢（預設值為 `objectClass=Person`）。
   - 伺服器網域首碼—用來唯一識別使用者的首碼。只有在有重疊命名空間時才需要，例如兩個不同目錄中，不同的使用者擁有相同的名稱時。
   - 使用 **SSL**—選取此核取方塊可使用 eDirectory 連結的 SSL。
   - 驗證伺服器憑證—選取此核取方塊可在使用 SSL 時驗證 eDirectory 伺服器憑證。

STEP 4 | （強烈建議）停用用戶端探查。

Palo Alto Networks 強烈建議在高安全性網路上停用用戶端探查。如果設定不當，用戶端探查可能會構成安全性威脅。有關更多資訊，請參閱用戶端探查。

1. 在 **Client Probing**（用戶端探查）頁籤上，取消選取 **Enable WMI Probing**（啟用 **WMI** 探查）核取方塊（如果已啟用）。

   Palo Alto Network 強烈建議您從孤立和受信任的來源（如網域控制器或與 Syslog 或 XML API 的整合）收集使用者對應資訊，以便安全地從任何裝置類型或作業系統擷取使用者對應資訊。

   如果您必須啟用用戶端探查，請在 ***Client Probing***（用戶端探查）頁籤上選取 ***Enable WMI Probing***（啟用 ***WMI*** 探查）核取方塊。然後，為各探查用戶端的 *Windows* 防火牆新增遠端管理例外，以確保 *Windows* 防火牆允許用戶端探查。每個探查的用戶端 *PC* 都必須在 *Windows* 防火牆中允許連接埠 *139*，同時必須啟用檔案與印表機共用服務。

STEP 5 | 儲存組態。

按一下 **OK**（確定）以儲存 User-ID 代理程式設定，然後按一下 **Commit**（提交）以重新啟動 User-ID 代理程式並載入新設定。

©2024 Palo Alto Networks, Inc.

STEP 6 | （選用）定義一組您不需提供 IP 位址對使用者名稱對應的使用者，例如自助服務機帳戶。

使用標題 `ignore_user_list` 在代理程式主機上將 `ignore-user` 清單儲存為文字文件，然後使用 .txt 副檔名將其儲存至代理程式安裝所在之網域伺服器上的 User-ID Agent 資料夾。

列出待忽略使用者帳戶清單；您可新增至清單的帳戶數量沒有限制。每個使用者帳戶名稱必須各自為一行。例如：

```
SPAdmin SPInstall TFSReport
```

您可將星號用作萬用字元來比對多個使用者名稱，但只能用作項目中的最後一個字元。例如，`corpdomain\it-admin*` 會比對 `corpdomain` 網域中使用者名稱以字串 `it#admin` 開頭的所有管理員。您也可以使用 `ignore-user` 清單來識別您想要使用驗證入口網站執行驗證的使用者。

新增項目到「忽略使用者」清單後，您必須中斷到服務的連線，然後重新建立連線。

STEP 7 | 設定要與 User-ID 代理程式連線的防火牆。

防火牆只能連線至一個基於 *Windows* 的 *User-ID* 代理程式，該代理程式將使用 *User-ID* 認證服務附加元件偵測公司認證提交。關於如何使用此服務的更多詳細資訊，請參閱使用 Windows User-ID 代理程式設定認證偵測。

在每個您要連線至 User-ID 代理程式的防火牆上完成下列步驟，以接收使用者識別：

1. 選取 **Device**（裝置） > **Data Redistribution**（資料重新散佈） > **Agents**（代理程式），然後按一下 **Add**（新增）。
2. 輸入代理程式的 **Name**（名稱）。
3. 使用 **Host and Port**（主機和連接埠）新增代理程式。
4. 輸入安裝 User-ID 代理程式之 Windows **Host**（主機）的 IP 位址。
5. 輸入代理程式用來接聽使用者對應要求的 **Port**（連接埠）號碼 (1-65535)。此值必須符合 User-ID 代理程式上所設定的值。依預設，在防火牆與新版 User-ID 代理程式上連接埠設為 5007。然而，某些舊版 User-ID 代理程式支援使用連接埠 2010 為預設值。
6. 選取 **IP User Mappings**（**IP** 使用者對應）作為 **Data type**（資料類型）。
7. 確定設定為 **Enabled**（已啟用），然後按一下 **OK**（確定）。
8. **Commit**（提交）變更。
9. 確認 **Connected status**（連線狀態）是否顯示為已連線（綠燈）。

©2024 Palo Alto Networks, Inc.

STEP 8 | 確認 User-ID 代理程式已成功將 IP 位址對應至使用者名稱，且防火牆可連線至代理程式。

1. 啟動 **User Identification**（連線狀態）並選取使用者識別。
2. 確認代理程式狀態顯示 **Agent is running**（代理程式執行中）。如果代理程式未執行，請按一下 **Start**（啟動）。
3. 若要確認 User-ID 代理程式可連接至監控的伺服器，請確定各伺服器的狀態均為 **Connected**（已連線）。
4. 若要確認防火牆可連線至 User-ID 代理程式，請確定各個已連線裝置的狀態均為 **Connected**（已連線）。
5. 若要確認 User-ID 代理程式會將 IP 位址對應至使用者名稱，請選取 **Monitoring**（監控），並確定已填入對應表格。您也可以 **Search**（搜尋）特定使用者，或 **Delete**（刪除）清單中的使用者識別。

使用 PAN-OS 整合的 User-ID 代理程式設定使用者對應

下列程序說明如何在防火牆上設定 PAN-OS® 整合式 User-ID™ 代理程式以進行 IP 位址對使用者名稱的對應。整合式 User-ID 代理程式執行的工作與基於 Windows 的代理程式相同。

STEP 1 | 為 User-ID 代理程式建立 Active Directory 服務帳戶，以存取防火牆為收集使用者對應資訊而監控的服務和主機。

為 User-ID 代理程式建立專用服務帳戶。

©2024 Palo Alto Networks, Inc.

STEP 2 | 定義防火牆為收集使用者對應資訊而監控的伺服器。

在每個防火牆總共最多 100 台受監控伺服器的範圍內，客易為任何虛擬系統定義不超過 50 個 Syslog 寄件者。

若要收集所有必要的對應項目，防火牆必須連線到使用者登入的所有伺服器，讓防火牆可以監控所有伺服器上含有登入事件的安全性日誌檔案。

1. 選取 **Device**（裝置） > **User Identification**（使用者識別） > **User Mapping**（使用者對應）。
2. **Add**（新增）一個伺服器（Server Monitoring（伺服器監控）區段）。
3. 輸入用來識別伺服器的 **Name**（名稱）。
4. 選取伺服器的類型。
   - **Microsoft Active Directory**
   - **Microsoft Exchange**
   - **Novell eDirectory**
   - 系統日誌寄件者
5. （僅限 Microsoft Active Directory 和 Microsoft Exchange）選取要用於監控伺服器上安全性日誌和工作階段資訊的 **Transport Protocol**（傳輸通訊協定）。
   - **WMI**—防火牆和受監控伺服器使用 Windows Management Instrumentation (WMI) 進行通訊。
   - **WinRM-HTTP**—防火牆和受監控伺服器使用 Kerberos 進行相互驗證，受監控伺服器使用交涉的 Kerberos 工作階段金鑰加密與防火牆之間的通訊。
   - **WinRM-HTTPS**—防火牆和受監控伺服器使用 HTTPS 進行通訊，並使用基本驗證或 Kerberos 進行相互驗證。

   如果您選取 Windows Remote Management (WinRM) 選項，則必須使用 WinRM 設定伺服器監控。
6. （僅限 Microsoft Active Directory、Microsoft Exchange 和 Novell eDirectory）輸入伺服器的 **Network Address**（網路位址）。

©2024 Palo Alto Networks, Inc.

如果您使用帶 Kerberos 的 WinRM，則必須輸入完全合格網域名稱 *(FDQN)*。如果您要使用帶基本驗證的 WinRM 或使用 ***WMI*** 監控伺服器，可以輸入 *IP* 位址或 *FQDN*。

若要使用 *WMI* 監控伺服器，請指定 *IP* 位址、服務帳戶名稱（如果監控中的伺服器都在同一網域中），或完全合格網域名稱 *(FQDN)*。如果指定 *FQDN*，請使用 *\sAMAccountName* 格式的下層 *(DLN)* 登入名稱，而不是 *FQDN\sAMAccountName* 格式。例如，使用 ***example\user.services***，而不是 ***example.com\user.services***。如果指定 *FQDN*，防火牆將嘗試使用 *Kerberos* 進行驗證，而 *Kerberos* 不支援 *WMI*。

7. （僅限 Syslog 傳送端）如果您選取 **Syslog Sender**（**Syslog** 傳送端）作為伺服器 **Type**（類型），將整合了 PAN-OS 的 User-ID 代理程式設定為 Syslog 接聽程式。
8. （僅限 Novell eDirectory）請確保您選取的 **Server Profile**（伺服器設定檔）**Enabled**（已啟用）並按一下 **OK**（確定）。
9. （選用）設定防火牆使用 DNS 查閱自動**Discover**（探索）您網路上的網域控制器。

自動探索功能僅適用於網域控制器；您必須手動新增要監控的 *Exchange* 伺服器或 *eDirectory* 伺服器。

STEP 3 | （選用）指定防火牆對 Windows 伺服器輪詢對應資訊的頻率。此為上一個查詢結束與下一個查詢開始之間的間隔。

如果網域控制器正在處理多個請求，查詢之間的延遲可能會超過指定值。

1. **Edit**（編輯） **Palo Alto Networks User ID Agent Setup**（**Palo Alto Networks User ID** 代理程式設定）。
2. 選取 **Server Monitor**（伺服器監控）頁籤，然後指定以秒為單位的 **Server Log Monitor Frequency**（伺服器日誌監控頻率）（範圍為 1-3600；預設值為 2）。在含舊版網域控制站或高延遲連結的環境中，將此頻率設定為最少 5 秒。

確保未啟用 ***Enable Session***（啟用工作階段）選項。此選項要求 *User-ID* 代理程式具有 *Active Directory* 帳戶與伺服器運算子權限，以便讀取所有使用者工作階段。您需使用 *Syslog* 或 *XML API* 整合來監控擷取所有裝置類型與作業系統之登入及登出事件的來源（而非僅 *Windows*），例如無線控制器及網路存取控制 *(NAC)* 裝置。

3. 按一下 **OK**（確定）儲存您的變更。

©2024 Palo Alto Networks, Inc.

STEP 4 | 指定整合了 PAN-OS 的 User-ID 代理程式應在使用者對應中包括或排除的子網路。

依預設，User-ID 會對應存取您所監控之伺服器的所有使用者。

最佳做法是指定 *User-ID* 中要包括和排除（可選）的網路，確保代理程式僅與內部資源通訊，防止對應未經授權的使用者。您只應在組織內部使用者登入的子網路上啟用使用者對應。

1. 選取 **Device**（裝置） > **User Identification**（使用者識別） > **User Mapping**（使用者對應）。
2. **Add**（新增）一個項目到 **Include/Exclude Networks**（包括/排除網路），然後為該項目輸入一個 **Name**（名稱）。確保項目已 **Enabled**（啟用）。
3. 輸入 **Network Address**（網路位址），然後選擇是要包括還是排除：
   - **Include**（包括）—選取此選項以將使用者對應限制於僅限登入指定子網路的使用者。例如，如果要包括 10.0.0.0/8，則代理程式將對應此子網路上的使用者，並排除所有其他使用者。如果您希望代理程式對應其他子網路中的使用者，則必須重複上述步驟，將其他網路新增至清單。
   - **Exclude**（排除）—選取此選項以設定代理程式排除您新增的要包含之子網路的子集合。例如，如果要包括 10.0.0.0/8 並排除 10.2.50.0/22，代理程式將對應除 10.2.50.0/22 之外 10.0.0.0/8 所有子網路上的使用者，並將排除 10.0.0.0/8 之外的所有子網路。

     如果您新增「排除」設定檔而不新增任何「包括」設定檔，*User-ID* 代理程式將排除所有子網路，而不只是您新增的子網路。
4. 按一下 **OK**（確定）。

STEP 5 | 為防火牆將用於使用存取 Windows 資源的帳戶設定網域認證。對監控 Exchange 伺服器與網域控制器，以及 WMI 探查來說這是必要動作。

1. **Edit**（編輯）**Palo Alto Networks User-ID Agent Setup**（**Palo Alto Networks User-ID** 代理程式設定）。
2. 選取 **Server Monitor Account**（伺服器監控帳戶）頁籤，然後輸入 User-ID 代理程式用來探查用戶端和監控伺服器之服務帳戶的 **User Name**（使用者名稱）和 **Password**（密碼）。使用 **`domain\username`** 語法輸入使用者名稱。
3. 如果您使用 WinRM 監控伺服器，可設定防火牆以對您所監控之伺服器進行驗證。
   - 如果您要使用帶基本驗證的 WinRM，請在伺服器上啟用 WinRM，設定基本驗證，然後指定服務帳戶 **Domain’s DNS Name**（網域的 **DNS** 名稱）。
   - 如果您要使用帶 Kerberos 的 WinRM，請設定 Kerberos 伺服器設定檔（若尚未設定），然後選取 **Kerberos Server Profile**（**Kerberos** 伺服器設定檔）。

©2024 Palo Alto Networks, Inc.

STEP 6 | （選用，但不建議）設定 WMI 探查。

請勿在高安全性網路上啟用 *WMI* 探查。用戶端探查可產生大量的網路流量，並可能在錯誤設定時導致安全性威脅。

1. 在 **Client Probing**（用戶端探查）頁籤上，**Enable Probing**（啟用探查）。
2. （選用）指定 **Probe Interval**（探查間隔），以定義上一個探查要求結束與下一個要求開始之間的間隔（分鐘）。

   如有必要，增加該值以確保 User-ID 代理程式有足夠的時間探查所有學習到的 IP 位址（範圍為 1 到 1440；預設值為 20）。

   如果要求負載很高，則觀察到的要求之間延遲可能會大大超過指定的時間間隔。
3. 按一下 **OK**（確定）。
4. 為各探查用戶端的 Windows 防火牆新增允端管理例外，以確定 Windows 防火牆允許用戶端探查。

STEP 7 | （選用）定義一組您不需 IP 位址對使用者名稱對應的使用者帳戶，例如自助服務機帳戶。

在 *User-ID* 代理程式防火牆（而不是用戶端防火牆）上定義忽略使用者清單。如果您在用戶端防火牆上定義忽略使用者清單，清單中的使用者在重新散佈時仍然會進行對應。

在 **Ignore User List**（忽略使用者清單）頁籤上，**Add**（新增）您想要從使用者對應中排除的每個使用者名稱。您也可以使用忽略使用者清單來識別想要使用驗證入口網站強制驗證的使用者。您可將星號用作萬用字元來比對多個使用者名稱，但只能用作項目中的最後一個字元。例如，**`corpdomain\it-admin*`** 會比對 `corpdomain` 網域中使用者名稱以字串 `it#admin` 開頭的所有管理員。您可新增最多 5,000 個從使用者對應中排除的項目。

STEP 8 | 啟動組態變更。

按一下 **OK**（確定）與 **Commit**（提交）。

STEP 9 | 確認組態。

1. 存取防火牆 CLI。
2. 輸入下列操作命令：

   ```
   > show user server-monitor state all
   ```
3. 在 Web 介面的 **Device**（裝置）> **User Identification**（使用者識別）> **User Mapping**（使用者對應）頁籤中，確認為其設定伺服器監控的各伺服器狀態為已`Connected`（連線）。

©2024 Palo Alto Networks, Inc.

使用 WinRM 設定伺服器監控

您可設定整合 PAN-OS 的 User-ID 代理程式以使用 Windows Remote Management (WinRM) 來監控伺服器。監控伺服器事件以將使用者事件對應至 IP 位址時，使用 WinRM 通訊協定可提高速度、效率和安全性。整合 PAN-OS 的 User-ID 代理程式支援 Windows 伺服器 2012 Active Directory 和 Microsoft Exchange 伺服器 2012 或兩者更新版本上的 WinRM 通訊協定。

使用 WinRM 設定伺服器監控有三種方式：

- 設定 WinRM over HTTPS 與基本驗證—防火牆使用 User-ID 代理程式之服務帳戶的使用者名稱和密碼對受監控伺服器進行驗證且使用 User-ID 憑證設定檔對受監控伺服器進行驗證。
- 設定 WinRM over HTTP 與 Kerberos—防火牆和受監控伺服器使用 Kerberos 進行相互驗證且受監控伺服器使用交涉的 Kerberos 工作階段金鑰加密與防火牆之間的通訊。
- 設定 WinRM over HTTPS 與 Kerberos—防火牆和受監控伺服器使用 HTTPS 進行通訊，並使用 Kerberos 進行相互驗證。

設定 WinRM over HTTPS 與基本驗證

當您設定 WinRM 以使用 HTTPS 和基本驗證時，防火牆將使用 SSL 在安全通道中傳輸服務帳戶的認證。

STEP 1 | 使用要監控的伺服器之遠端管理使用者和 CIMV2 權限設定服務帳戶。

STEP 2 | 在監控的 Windows 伺服器上，從 Windows 伺服器的憑證中取得指紋，用於 WinRM 並啟用 WinRM。

確保使用具有管理員權限的帳戶在要監控的伺服器上設定 *WinRM*。作為安全性的最佳做法，此帳戶不應與步驟 *1* 中的服務帳戶相同。

1. 確認憑證是否已安裝在本機電腦憑證存放區中（**Certificates (Local Computer)**（憑證（本機電腦））> **Personal**（個人）> **Certificates**（憑證））。

   如果您沒有看到本機電腦憑證存放區，請啟動 Microsoft 管理主控台（**Start**（啟動）> **Run**（執行）> **MMC**），並新增憑證嵌入式管理單元（**File**（檔案）> **Add/Remove**

©2024 Palo Alto Networks, Inc.

Snap-in（新增/移除嵌入式管理單元）> **Certificates**（憑證）> **Add**（新增）> **Computer account**（電腦帳戶）> **Next**（下一步）> **Finish**（完成））。

2. 開啟憑證並選取 **General**（一般）> **Details**（詳細資料）> **Show:**（顯示：）**<All>**。
3. 選取 **Thumbprint**（指紋）並複製。
4. 若要讓防火牆使用 WinRM 連線至 Windows 伺服器，請輸入以下命令：**`winrm quickconfig`**。
5. 輸入 **`y`** 確認變更，然後確認輸出顯示 `WinRM service started`。

   如果 WinRM 已啟用，輸出將顯示 `WinRM service is already running on this machine.`。系統將提示您確認任何其他必要的組態變更。
6. 若要確認 WinRM 是否在使用 HTTPS 進行通訊，請輸入以下命令：**`winrm enumerate winrm/config/listener`**，確認後，輸出將顯示 `Transport = HTTPS`。

   依預設，WinRM/HTTPS 使用連接埠 5986。
7. 在 Windows 伺服器命令提示字元中，輸入以下命令：**`winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="<hostname>";CertificateThumbprint="Certificate Thumbprint"}`**，其中 *hostname* 是 Windows 伺服器的主機名稱，*Certificate Thumbprint* 是從憑證中複製的值。

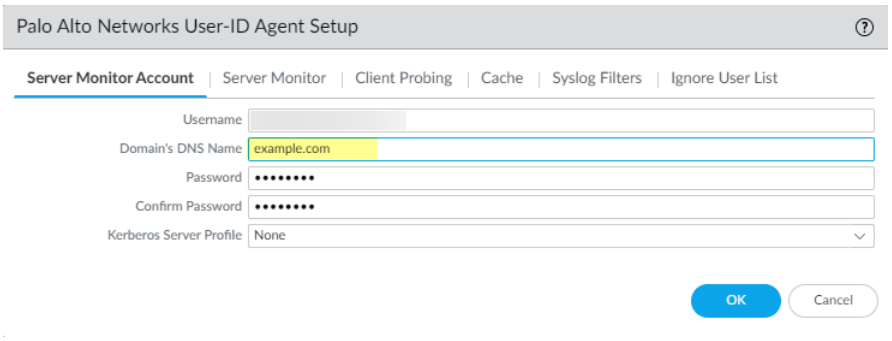
   使用命令提示（而非 *Powershell*），並移除憑證指紋中的任何空格以確保 *WinRM* 能驗證憑證。
8. 在 Windows 伺服器命令提示中，輸入以下命令：

   ```
   c:\> winrm set winrm/config/client/auth @{Basic="true"}
   ```
9. 輸入下列命令：**`winrm get winrm/config/service/Auth`** 並確認 `Basic = true`。

©2024 Palo Alto Networks, Inc.

STEP 3 | 在整合 PAN-OS 的 User-ID 代理程式和受監控伺服器之間啟用基本驗證。

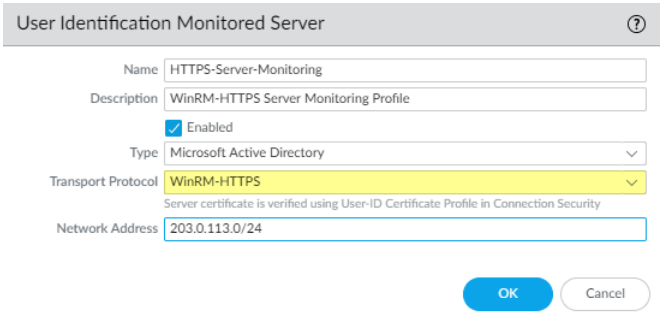
1. 選取 **Device**（裝置）> **User Identification**（使用者識別）> **User Mapping**（使用者對應）> **Palo Alto Networks User-ID Agent Setup**（**Palo Alto Networks User-ID** 代理程式設定）> **Server Monitor**（伺服器監控）。
2. 以 **`domain\username`**（網域\使用者名稱）格式，輸入 User-ID 代理程式將用於監控伺服器之服務帳戶的 **User Name**（使用者名稱）。
3. 輸入伺服器監控帳戶的 **Domain's DNS Name**（網域的 **DNS** 名稱）。



4. 輸入服務帳戶的 **Password**（密碼）並 **Confirm Password**（確認密碼）。
5. 按一下 **OK**（確定）

STEP 4 | 為整合了 PAN-OS 的 User-ID 代理程式設定伺服器監控。

1. 選取 Microsoft 伺服器 **Type**（類型）（**Microsoft Active Directory** 或 **Microsoft Exchange**）。
2. 選取 **Win-RM-HTTPS** 作為 **Transport Protocol**（傳輸通訊協定），以透過 HTTPS 使用 Windows Remote Management (WinRM) 來監控伺服器安全日誌和工作階段資訊。

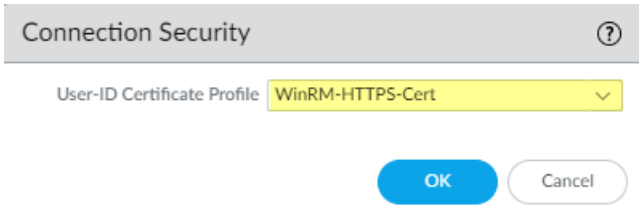


3. 輸入伺服器的 IP 位址或 FQDN **Network Address**（網路位址）。

©2024 Palo Alto Networks, Inc.

STEP 5 | 若要讓整合 PAN-OS 的 User-ID 代理程式使用 WinRM-HTTPS 與受監控伺服器進行通訊，請確認您已成功將 Windows 伺服器用於 WinRM 的服務憑證之根憑證匯入到防火牆，並將憑證與 User-ID 憑證設定檔相關聯。

1. 選取 **Device**（裝置） > **User Identification**（使用者識別） > **Connection Security**（連線安全性）。
2. 按一下 **Edit**（編輯）。
3. 選取要用於 **User-ID Certificate Profile**（**User-ID** 憑證設定檔）的 Windows 伺服器憑證。



4. 按一下 **OK**（確定）。

STEP 6 | **Commit**（提交）您的變更。

STEP 7 | 確認各受監控伺服器的狀態是否為已連線（**Device**（裝置） > **User Identification**（使用者識別） > **User Mapping**（使用者對應））。

設定 WinRM over HTTP 與 Kerberos

當您設定 WinRM over HTTP 與 Kerberos 時，防火牆和受監控伺服器將使用 Kerberos 進行相互驗證，受監控伺服器使用交涉的 Kerberos 工作階段金鑰加密與防火牆之間的通訊。

帶 *Kerberos* 的 *WinRM* 支援 *aes128-cts-hmac-sha1-96* 和 *aes256-cts-hmac-sha1-96* 密碼。如果要監控的伺服器使用 *RC4*，則必須下載 *Windows* 更新並在要監控之伺服器的登錄設定中停用 *Kerberos* 的 *RC4*。

STEP 1 | 使用要監控的伺服器之遠端管理使用者和 CIMV2 權限設定服務帳戶。

©2024 Palo Alto Networks, Inc.

STEP 2 | 確認您正在監控的 Windows 伺服器上已啟用 WinRM。

確保使用具有管理員權限的帳戶在要監控的伺服器上設定 *WinRM*。作為安全性的最佳做法，此帳戶不應與步驟 *1* 中的服務帳戶相同。

1. 若要讓防火牆使用 WinRM 連線至 Windows 伺服器，請輸入以下命令：**`winrm quickconfig`**。
2. 輸入 **`y`** 確認變更，然後確認輸出顯示 `WinRM service started`。

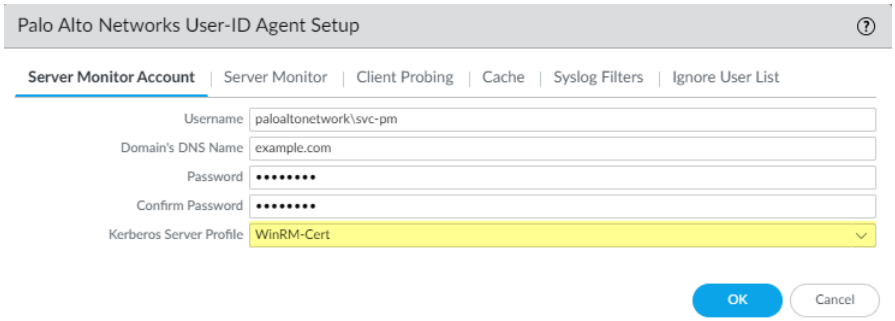
   如果 WinRM 已啟用，輸出將顯示 `WinRM service is already running on this machine.`。系統將提示您確認任何其他必要的組態變更。
3. 若要確認 WinRM 是否在使用 HTTPS 進行通訊，請輸入以下命令：**`winrm enumerate winrm/config/listener`**，確認後，輸出將顯示 `Transport = HTTPS`。

   依預設，WinRM/HTTP 使用連接埠 5985。
4. 輸入下列命令：**`winrm get winrm/config/service/Auth`** 並確認 `Kerberos = true`。

STEP 3 | 讓整合 PAN-OS 的 User-ID 代理程式和受監控伺服器使用 Kerberos 進行驗證。

1. 如果您在初始設定期間未執行此動作，請設定日期和時間 (NTP) 設定，以確保成功進行 Kerberos 交涉。
2. 在防火牆上設定 Kerberos 伺服器設定檔以對伺服器進行驗證，從而監控安全性日誌和工作階段資訊。
3. 選取 **Device**（裝置） > **User Identification**（使用者識別） > **User Mapping**（使用者對應） > **Palo Alto Networks User-ID Agent Setup**（**Palo Alto Networks User-ID** 代理程式設定） > **Server Monitor**（伺服器監控）。
4. 以 **`domain\username`**（網域\使用者名稱）格式，輸入 User-ID 代理程式將用於監控伺服器之服務帳戶的 **User Name**（使用者名稱）。
5. 輸入伺服器監控帳戶的 **Domain's DNS Name**（網域的 **DNS** 名稱）。

   Kerberos 使用網域名稱尋找服務帳戶。
6. 輸入服務帳戶的 **Password**（密碼）並 **Confirm Password**（確認密碼）。
7. 選取在步驟 3.2 中設定的 **Kerberos Server Profile**（**Kerberos** 伺服器設定檔）。

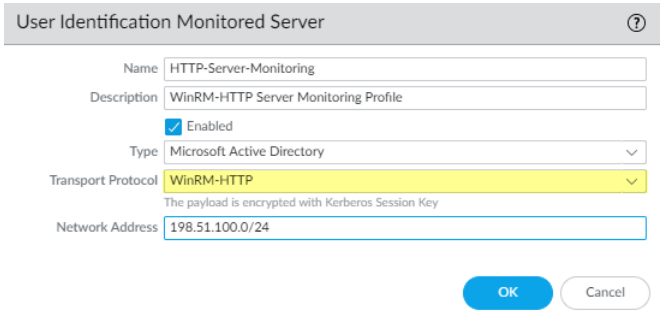


8. 按一下 **OK**（確定）。

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 為整合了 PAN-OS 的 User-ID 代理程式設定伺服器監控。

1. 設定 Microsoft 伺服器類型（**Microsoft Active Directory** 或 **Microsoft Exchange**）。
2. 選取 **WinRM-HTTP** 作為 **Transport Protocol**（傳輸通訊協定），以透過 HTTP 使用 Windows Remote Management (WinRM) 來監控伺服器的安全日誌和工作階段資訊。



3. 輸入伺服器的 FQDN **Network Address**（網路位址）。

   如果您使用的是 Kerberos，則網路位址必須為完全合格網域名稱 (FDQN)。

STEP 5 | **Commit**（提交）您的變更。

STEP 6 | 確認各受監控伺服器的狀態是否為已連線（**Device**（裝置） > **User Identification**（使用者識別） > **User Mapping**（使用者對應））。

設定 WinRM over HTTPS 與 Kerberos

當您設定 WinRM over HTTPS 與 Kerberos 時，防火牆和受監控伺服器將使用 HTTPS 進行通訊，並使用 Kerberos 進行相互驗證。

帶 *Kerberos* 的 *WinRM* 支援 *aes128-cts-hmac-sha1-96* 和 *aes256-cts-hmac-sha1-96* 密碼。如果要監控的伺服器使用 *RC4*，則必須下載 *Windows* 更新並在要監控之伺服器的登錄設定中停用 *Kerberos* 的 *RC4*。

STEP 1 | 使用要監控的伺服器之遠端管理使用者和 CIMV2 權限設定服務帳戶。

STEP 2 | 在監控的 Windows 伺服器上，從 Windows 伺服器的憑證中取得指紋，用於 WinRM 並啟用 WinRM。

確保使用具有管理員權限的帳戶在要監控的伺服器上設定 *WinRM*。作為安全性的最佳做法，此帳戶不應與步驟 *1* 中的服務帳戶相同。

1. 確認憑證是否已安裝在本機電腦憑證存放區中（**Certificates (Local Computer)**（憑證（本機電腦）） > **Personal**（個人） > **Certificates**（憑證））。

   如果您沒有看到本機電腦憑證存放區，請啟動 Microsoft 管理主控台（**Start**（啟動） > **Run**（執行） > **MMC**），並新增憑證嵌入式管理單元（**File**（檔案） > **Add/Remove**

©2024 Palo Alto Networks, Inc.

Snap-in（新增/移除嵌入式管理單元）> **Certificates**（憑證）> **Add**（新增）> **Computer account**（電腦帳戶）> **Next**（下一步）> **Finish**（完成））。

2. 開啟憑證並選取 **General**（一般）> **Details**（詳細資料）> **Show:**（顯示：）**<All>**。
3. 選取 **Thumbprint**（指紋）並複製。
4. 若要讓防火牆使用 WinRM 連線至 Windows 伺服器，請輸入以下命令：**`winrm quickconfig`**。
5. 輸入 **`y`** 確認變更，然後確認輸出顯示 `WinRM service started`。

   如果 WinRM 已啟用，輸出將顯示 `WinRM service is already running on this machine.`。系統將提示您確認任何其他必要的組態變更。
6. 若要確認 WinRM 是否在使用 HTTPS 進行通訊，請輸入以下命令：**`winrm enumerate winrm/config/listener`**。然後確認輸出顯示 `Transport = HTTPS` 。

   依預設，WinRM/HTTPS 使用連接埠 5986。
7. 在 Windows 伺服器命令提示字元中，輸入以下命令：**`winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="<hostname>";CertificateThumbprint="Certificate Thumbprint"}`**，其中 *hostname* 是 Windows 伺服器的主機名稱，*Certificate Thumbprint* 是從憑證中複製的值。

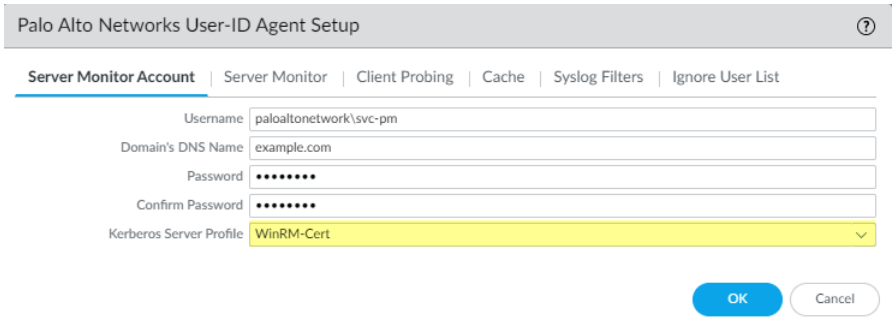
   使用命令提示（而非 *Powershell*），並移除憑證指紋中的任何空格以確保 *WinRM* 能驗證憑證。
8. 輸入下列命令：**`winrm get winrm/config/service/Auth`** 並確認 `Basic = false` 和 `Kerberos= true`。

©2024 Palo Alto Networks, Inc.

STEP 3 | 讓整合 PAN-OS 的 User-ID 代理程式和受監控伺服器使用 Kerberos 進行驗證。

1. 如果您在初始設定期間未執行此動作，請設定日期和時間 (NTP) 設定，以確保成功進行 Kerberos 交涉。
2. 在防火牆上設定 Kerberos 伺服器設定檔以對伺服器進行驗證，從而監控安全性日誌和工作階段資訊。
3. 選取 **Device**（裝置） > **User Identification**（使用者識別） > **User Mapping**（使用者對應） > **Palo Alto Networks User-ID Agent Setup**（**Palo Alto Networks User-ID** 代理程式設定） > **Server Monitor**（伺服器監控）。
4. 以 **`domain\username`**（網域\使用者名稱）格式，輸入 User-ID 代理程式將用於監控伺服器之服務帳戶的 **User Name**（使用者名稱）。
5. 輸入伺服器監控帳戶的 **Domain's DNS Name**（網域的 **DNS** 名稱）。

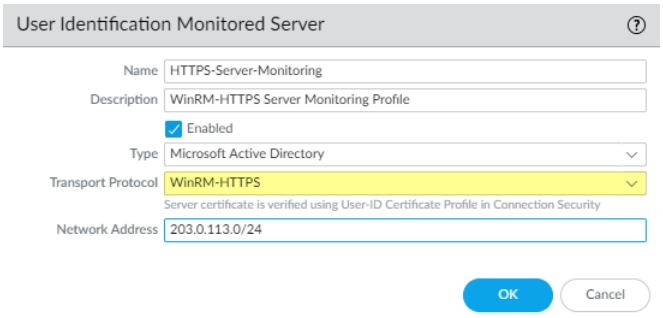
   Kerberos 使用網域名稱尋找服務帳戶。
6. 輸入服務帳戶的 **Password**（密碼）並 **Confirm Password**（確認密碼）。
7. 選取在步驟 3.2 中建立的 **Kerberos Server Profile**（**Kerberos** 伺服器設定檔）。



8. 按一下 **OK**（確定）。

STEP 4 | 為整合了 PAN-OS 的 User-ID 代理程式設定伺服器監控。

1. 設定 Microsoft 伺服器類型（**Microsoft Active Directory** 或 **Microsoft Exchange**）。
2. 選取 **Win-RM-HTTPS** 作為 **Transport Protocol**（傳輸通訊協定），以透過 HTTPS 使用 Windows Remote Management (WinRM) 來監控伺服器安全日誌和工作階段資訊。



3. 輸入伺服器的 FQDN **Network Address**（網路位址）。

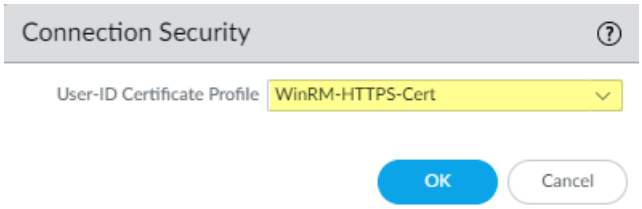
   如果您使用的是 Kerberos，則網路位址必須為完全合格網域名稱 (FDQN)。

 ©2024 Palo Alto Networks, Inc.

STEP 5 | 若要讓整合 PAN-OS 的 User-ID 代理程式使用 WinRM-HTTPS 與受監控伺服器進行通訊，請確認您已成功將 Windows 伺服器用於 WinRM 的服務憑證之根憑證匯入到防火牆，並將憑證與 User-ID 憑證設定檔相關聯。

防火牆會使用同一憑證來驗證所有受監控伺服器。

1. 選取 **Device**（裝置） > **User Identification**（使用者識別） > **Connection Security**（連線安全性）。
2. 按一下 **Edit**（編輯）。
3. 選取要用於 **User-ID Certificate Profile**（**User-ID** 憑證設定檔）的 Windows 伺服器憑證。



4. 按一下 **OK**（確定）。
5. **Commit**（提交）您的變更。

STEP 6 | 確認各受監控伺服器的狀態是否為已連線（**Device**（裝置） > **User Identification**（使用者識別） > **User Mapping**（使用者對應））。

設定 User-ID 以監控用於使用者對應的 Syslog 傳送程式

若要從驗證使用者的現有網路服務取得 IP 位址至使用者名稱對應，您可以設定 PAN-OS 整合式 User-ID 代理程式或基於 Windows 的 User-ID 代理程式，以剖析來自這些服務的 Syslog 訊息。若要將使用者對應保持更新，您還可以設定 User-ID 代理程式，以剖析登出事件的 syslog 訊息，從而使防火牆自動刪除過期的對應。

- 將整合了 PAN-OS 的 User-ID 代理程式設定為 Syslog 接聽程式
- 將 Windows User-ID 代理程式設定為 syslog 接聽程式

將整合了 PAN-OS 的 User-ID 代理程式設定為 Syslog 接聽程式

若要設定整合了 PAN-OS 的 User-ID 代理程式，以建立新使用者對應並透過 syslog 監控移除已過期的對應，首先要定義 Syslog 剖析設定檔。User-ID 代理程式將使用這些設定檔，在 syslog 訊息中尋找登入和登入事件。在 *syslog* 傳送程式（用於驗證使用者的網路服務）以不同格式傳送 syslog 訊息的環境中，需為每種 syslog 格式設定一個設定檔。Syslog 訊息必須符合特定準則才可供 User-ID 代理程式進行剖析（請參閱 Syslog）。此程序使用了採用下列格式的範例：

- 登入事件—`[Tue Jul 5 13:15:04 2016 CDT] Administrator authentication success User:johndoe1 Source:192.168.3.212`
- 登出事件—`[Tue Jul 5 13:18:05 2016CDT] User logout successful User:johndoe1 Source:192.168.3.212`

©2024 Palo Alto Networks, Inc.

設定 Syslog 剖析設定檔後，指定由 User-ID 代理程式監控的 syslog 傳送程式。

STEP 1 | 判定您的特定 syslog 傳送程式是否有預先定義的 Syslog 剖析設定檔。

Palo Alto Networks 會透過應用程式內容更新來提供一些預先定義的設定檔。預先定義的設定檔對防火牆是全域的，但自訂設定檔僅適用於單一虛擬系統。

在所指定的內容版本中，任何新的 *Syslog* 剖析設定檔都將連同用於定義篩選器的特定 *regex* 一起記錄在對應的版本資訊中。

1. 安裝最新的應用程式或應用程式及威脅更新。
   1. 選取 **Device**（裝置） > **Dynamic Updates**（動態更新），再選取 **Check Now**（立即檢查）。
   2. **Download**（下載）並 **Install**（安裝）任何新的更新。
2. 確定可用的預先定義 Syslog 剖析設定檔：
   1. 選取 **Device**（裝置） > **User Identification**（使用者識別） > **User Mapping**（使用者對應），然後在 Server Monitoring（伺服器對應）區段中按一下 **Add**（新增）。
   2. 將 **Type**（類型）設定為 **Syslog Sender**（**Syslog** 傳送程式），然後在 Filter（篩選）區段中按一下 **Add**（更新）。如果您需要的 Syslog 剖析設定檔可用，則跳過定義自訂設定檔的步驟。

STEP 2 | 定義自訂 Syslog 剖析設定檔，以建立和刪除使用者對應。

每個設定檔會篩選 syslog 訊息，以識別登入事件（建立使用者對應）或登出（刪除使用者對應），但沒有任何設定檔可同時執行這兩個工作。

1. 檢閱 syslog 傳送程式產生的 syslog 訊息，以識別登入和登出事件的語法。這讓您在建立 Syslog 剖析設定檔時能夠定義符合模式。

   在檢閱 *syslog* 訊息時，還需確定它們是否包含了網域名稱。如果未包含而使用者對應又需要網域名稱，則在此程序後面的步驟中定義 *User-ID* 代理程式監控的 *syslog* 傳送程式時，輸入 ***Default Domain Name***（預設網域名稱）。
2. 選取 **Device**（裝置） > **User Identification**（使用者識別） > **User Mapping**（使用者對應），然後編輯 Palo Alto Networks User-ID Agent Setup（Palo Alto Networks User-ID 代理程式設定）。
3. 選取 **Syslog Filters**（**Syslog** 篩選器），然後 **Add**（新增）Syslog 剖析設定檔。
4. 輸入用於識別 **Syslog Parse Profile**（新增）的名稱。
5. 選取剖析 **Type**（類型），以在 syslog 訊息中尋找登入或登出事件：
   - **Regex** 識別碼—規則運算式。
   - 欄位識別碼—文字字串。

   下列步驟介紹了如何設定這些剖析類型。

©2024 Palo Alto Networks, Inc.

STEP 3 | （僅限 **Regex** 識別碼剖析）定義 regex 符合模式。

如果 *syslog* 訊息中包含獨立空格或定位點作為分隔符號，則使用 **`\s`**（表示空格）和 **`\t`**（表示定位點）。

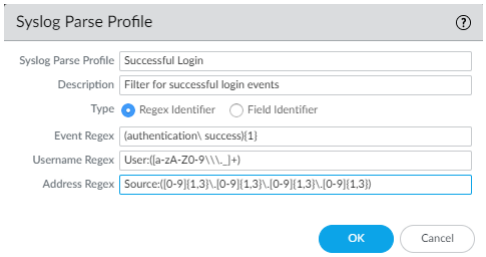
1. 為您要尋找的事件類型輸入 **Event Regex**（事件 Regex）：
   - 登入事件—對於範例訊息，regex **`(authentication\ success){1}`** 將擷取字串 `authenticationsuccess` 的第一個 **`{1}`** 執行個體。
   - 登出事件—對於範例訊息，regex **`(logout\ successful){1}`** 將擷取字串 `logoutsuccessful` 的第一個 **`{1}`** 執行個體。

   空格前面的反斜線 (\) 是標準的 regex 逸出字元，指示 regex 引擎不要將空格視為特殊字元。
2. 輸入 **Username Regex**（使用者名稱 **Regex**），以識別使用者名稱的開頭。

   在範例訊息中，regex **`User:([a-zA-Z0-9\\\._]+)`** 將比對 `User:johndoe1`，並將 `johndoe1` 識別為使用者名稱。
3. 輸入 **Address Regex**（位址 Regex），以識別 syslog 訊息的 IP 位址部分。

   在範例訊息中，規則運算式 **`Source:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})`** 將比對 IPv4 位址 `Source:192.168.3.212`。

   以下範例為使用 regex 識別登入事件的完整 Syslog 剖析設定檔：



4. 按兩下 **OK**（確定）以儲存設定檔。

©2024 Palo Alto Networks, Inc.

STEP 4 | （僅限欄位識別碼剖析）定義字串符合模式。

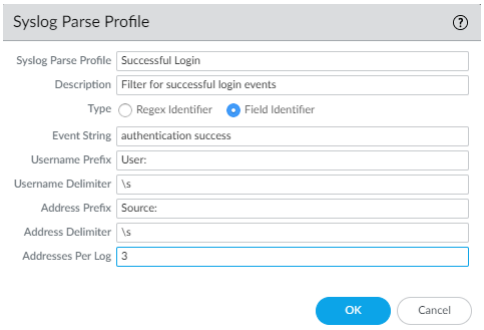
1. 為您要尋找的事件類型輸入 **Event String**（事件字串）。
   - 登入事件—對於範例訊息，字串 `authentication success` 表示登入事件。
   - 登出事件—對於範例訊息，字串 `logoutsuccessful` 表示登出事件。
2. 輸入 **Username Prefix**（使用者名稱首碼）來識別 syslog 訊息中使用者名稱欄位的開頭。此欄位不支援 \s（用於空格）或 \t（用於頁籤）之類的 regex 運算式。

   在範例訊息中，`User:` 表示使用者名稱欄位的開頭。
3. 輸入指示 syslog 訊息中使用者名稱欄位結尾的 **Username Delimiter**（使用者名稱分隔符號）。使用 **`\s`** 可表示獨立空格（如範例訊息所示），使用 **`\t`** 則可表示定位點。
4. 輸入 **Address Prefix**（位址首碼）來識別 Syslog 訊息中 IP 位址欄位的開頭。此欄位不支援 \s（用於空格）或 \t（用於頁籤）之類的 regex 運算式。

   在範例訊息中，`Source:` 表示位址欄位的開頭。
5. 輸入指示 syslog 訊息中 IP 位址欄位結尾的 **Address Delimiter**（位址分隔符號）。

   例如，輸入 **`\n`** 可指出要以分行符號作為分隔符號。

   以下範例為使用字串比對識別登入事件的完整 Syslog 剖析設定檔：



6. 按兩下 **OK**（確定）以儲存設定檔。

 ©2024 Palo Alto Networks, Inc.

STEP 5 | 指定防火牆將監控的 syslog 傳送程式。

在每個防火牆總共最多 100 台受監控伺服器的範圍內，客易為任何虛擬系統定義不超過 50 個 Syslog 寄件者。

若收到的 syslog 訊息並非來自此清單上的傳送程式，防火牆將一律捨棄。

1. 選取 **Device**（裝置） > **User Identification**（使用者識別） > **User Mapping**（使用者對應），然後 **Add**（新增） 項目到 Server Monitoring（伺服器對應）清單。
2. 輸入用來識別傳送程式的 **Name**（名稱）。
3. 確保傳送程式設定檔 **Enabled**（已啟用）（預設值）。
4. 將 **Type**（類型）設為 **Syslog Sender**（**Syslog** 傳送程式）。
5. 輸入 syslog 傳送程式的 **Network Address**（網路位址）（IP 位址）。
6. 選取 **SSL**（預設值）或 **UDP** 作為 **Connection Type**（連線類型）。

   要選取防火牆用於接收 *syslog* 訊息的 *TLS* 憑證，請選取 ***Device***（裝置） > ***User Identification***（使用者識別） > ***User Mapping***（使用者對應） > ***Palo Alto Networks User-ID Agent Setup***（***Palo Alto Networks User-ID*** 代理程式設定）。***Edit***（編輯）設定並選取 ***Server Monitor***（伺服器監控），然後選取包含您希望防火牆用於接收 *syslog* 訊息的 *TLS* 憑證的 ***Syslog Service Profile***（***Syslog*** 服務設定檔）。

   PAN-OS 整合式 *User-ID* 代理程式僅透過 *SSL* 與 *UDP* 接受 *syslog*。不過，您在使用 *UDP* 接收 *syslog* 訊息時必須多加留意，因為它並不是可靠的通訊協定，因此無法驗證從受信任的 *syslog* 傳送程式傳送的訊息。雖然您可以將 *syslog* 訊息限定於特定的來源 *IP* 位址，但攻擊者仍可偽造 *IP* 位址，而可能得以將未經授權的 *syslog* 訊息插入防火牆中。

   由於流量已加密，一律使用 *SSL* 來接聽 *syslog* 訊息（*UDP* 以明文傳送流量）。如果您必須使用 *UDP*，請確定 *syslog* 傳送程式和用戶端皆位於專用的安全網路上，以防止不受信任的主機傳送 *UDP* 流量至防火牆。

   當有使用中的 SSL 連線時，使用 SSL 連線的 syslog 傳送程式只會顯示已連線的狀態。使用 UDP 的系統日誌寄件者不會顯示狀態值。
7. 對於傳送程式支援的每種 syslog 格式，**Add**（新增）Syslog 剖析設定檔到 Filter（篩選器）清單。選取每個設定檔將識別的 **Event Type**（事件類型）：**login**（登入）（預設）或 **logout**（登出）。
8. （選用）如果 syslog 訊息中不包含網域資訊但使用者對應需要網域名稱，則輸入 **Default Domain Name**（登出），將其附加至對應。
9. 按一下 **OK**（確定）以儲存設定。

 ©2024 Palo Alto Networks, Inc.

STEP 6 | 在防火牆用於收集使用者對應的介面上啟用 syslog 接聽程式服務。

1. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **Interface Mgmt**（介面管理），然後編輯現有介面管理設定檔，或 **Add**（新增） 新設定檔。
2. 根據在 Server Monitoring（伺服器監控）清單中為 syslog 傳送程式定義的通訊協定，選取 **User-ID Syslog Listener-SSL**（**User-ID Syslog** 接聽程式 **SSL**）或 **User-ID Syslog Listener-UDP**（**User-ID Syslog** 接聽程式 **UDP**）或二者。

   接聽連接埠（*UDP* 為 *514*，*SSL* 為 *6514*）不可設定；只能透過管理服務啟用。
3. 按一下 **OK**（確定）來儲存介面管理設定檔。

   即使在介面上的 *User-ID syslog* 接聽程式服務啟用後，介面仍將僅接受來自在受 *User-ID* 監控之伺服器組態中有對應項目的傳送程式的 *syslog* 連線。如果連線或訊息來自於未在清單中的傳送程式，防火牆將一律捨棄。
4. 將介面管理設定檔指派給防火牆用於收集使用者對應的介面：
   1. 選取 **Network**（網路） > **Interfaces**（介面），然後編輯介面。
   2. 選取 **Advanced**（進階） > **Other info**（其他資訊），然後選取您剛新增的介面 **Management Profile**（管理設定檔），再按一下 **OK**（確定）。
5. **Commit**（提交）您的變更。

STEP 7 | 確認在使用者登入和登出時，防火牆是否新增和刪除使用者對應。

您可以使用 CLI 命令來查看關於 *syslog* 傳送程式、*syslog* 訊息和使用者對應的其他資訊。

1. 登入受監控 syslog 傳送程式將為其產生登入和登出事件訊息的用戶端系統。
2. 登入防火牆 CLI。
3. 確認防火牆是否已將登入使用者名稱對應到用戶端 IP 位址：

```
> show user ip-user-mapping ip <ip-address> IP
 address:    192.0.2.1 (vsys1) User:          localdomain
\username From:          SYSLOG
```

4. 登出用戶端系統。
5. 確認防火牆是否已偵測使用者對應：

```
> show user ip-user-mapping ip <ip-address> No matched record
```

將 Windows User-ID 代理程式設定為 syslog 接聽程式

若要設定基於 Windows 的 User-ID 代理程式，以建立新使用者對應並透過 syslog 監控移除已過期的對應，首先要定義 Syslog 剖析設定檔。User-ID 代理程式將使用這些設定檔，在 syslog 訊息中尋找登入和登入事件。在 *syslog* 傳送程式（用於驗證使用者的網路服務）以不同格式傳送 syslog 訊息

©2024 Palo Alto Networks, Inc.

的環境中，需為每種 syslog 格式設定一個設定檔。Syslog 訊息必須符合特定準則才可供 User-ID 代理程式進行剖析（請參閱 Syslog）。此程序使用了採用下列格式的範例：

- 登入事件—`[Tue Jul 5 13:15:04 2016 CDT] Administrator authentication success User:johndoe1 Source:192.168.3.212`
- 登出事件—`[Tue Jul 5 13:18:05 2016 CDT] User logout successful User:johndoe1 Source:192.168.3.212`

設定 Syslog 剖析設定檔後，指定由 User-ID 代理程式監控的 syslog 傳送程式。

Windows User-ID 代理程式僅過 *TCP* 與 *UDP* 接受 *syslog*。不過，您在使用 *UDP* 接收 *syslog* 訊息時必須多加留意，因為它並不是可靠的通訊協定，因此無法驗證從受信任的 *syslog* 傳送程式傳送的訊息。雖然您可以將 *syslog* 訊息限定於特定的來源 *IP* 位址，但攻擊者仍可偽造 *IP* 位址，而可能得以將未經授權的 *syslog* 訊息插入防火牆中。最佳做法是使用 *TCP*，而不要使用 *UDP*。無論哪種情況下，都要確保 *syslog* 轉送程式和用戶端皆位於專用的安全 *VLAN* 上，以防止不受信任的主機傳送 *syslog* 至 *User-ID* 代理程式。

STEP 1 | 如果您還未部署基於 Windows 的 User-ID 代理程式，則進行部署。

1. 安裝 Windows 型 User-ID 代理程式。
2. 設定要與 User-ID 代理程式連線的防火牆。

STEP 2 | 定義自訂 Syslog 剖析設定檔，以建立和刪除使用者對應。

每個設定檔會篩選 syslog 訊息，以識別登入事件（建立使用者對應）或登出（刪除使用者對應），但沒有任何設定檔可同時執行這兩個工作。

1. 檢閱 syslog 傳送程式產生的 syslog 訊息，以識別登入和登出事件的語法。這讓您在建立 Syslog 剖析設定檔時能夠定義符合模式。

   在檢閱 *syslog* 訊息時，還需確定它們是否包含了網域名稱。如果未包含而使用者對應又需要網域名稱，則在此程序後面的步驟中定義 *User-ID* 代理程式監控的 *syslog* 傳送程式時，輸入 ***Default Domain Name***（預設網域名稱）。
2. 開啟 Windows **Start**（開始）功能表，然後選取 **User-ID Agent**（**User-ID** 代理程式）。
3. 選取 **User Identification**（使用者識別）> **Setup**（設定），然後 **Edit**（編輯）Setup（設定）。
4. 選取 **Syslog**，**Enable Syslog Service**（啟用 **Syslog** 服務），然後 **Add**（新增）Syslog 剖析設定檔。
5. 輸入 **Profile Name**（設定檔名稱）及 **Description**（說明）。
6. 選取剖析 **Type**（類型），以在 syslog 訊息中尋找登入和登出事件：
   - **Regex**—規則運算式。
   - 欄位—文字字串。

   下列步驟介紹了如何設定這些剖析類型。

©2024 Palo Alto Networks, Inc.

STEP 3 | （僅限 **Regex** 剖析）定義 regex 符合模式。

如果 syslog 訊息中包含獨立空格或定位點作為分隔符號，則使用 **\s**（表示空格）和 **\t**（表示定位點）。

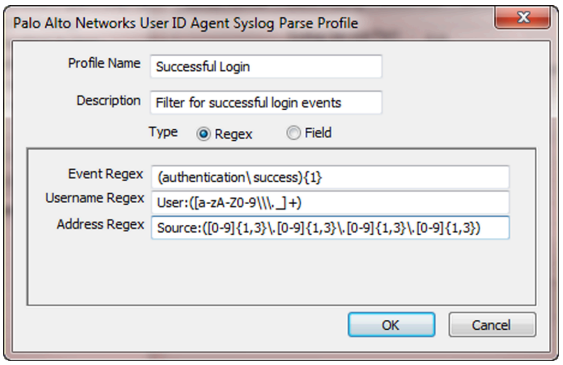
1. 為您要尋找的事件類型輸入 **Event Regex**（事件 Regex）：
   - 登入事件—對於範例訊息，**regex (authentication\ success){1}** 將擷取字串 `authentication success` 的第一個 **{1}** 實例。
   - 登出事件—對於範例訊息，regex **(logout\ successful){1}** 將擷取字串 `logout successful` 的第一個 **{1}** 實例。

   空格前面的反斜線是標準的 regex 逸出字元，指示 regex 引擎不要將空格視為特殊字元。
2. 輸入 **Username Regex**（使用者名稱 **Regex**），以識別使用者名稱的開頭。

   在範例訊息中，regex **User:([a-zA-Z0-9\\\._]+)** 將比對 `User:johndoe1`，並將 `johndoe1` 識別為使用者名稱。
3. 輸入 **Address Regex**（位址 Regex），以識別 syslog 訊息的 IP 位址部分。

   在範例訊息中，規則運算式 **Source:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})** 將比對 IPv4 位址 `Source:192.168.3.212`。

   以下範例為使用 regex 識別登入事件的完整 Syslog 剖析設定檔：



4. 按兩下 **OK**（確定）以儲存設定檔。

©2024 Palo Alto Networks, Inc.

STEP 4 | （僅限欄位識別碼剖析）定義字串符合模式。

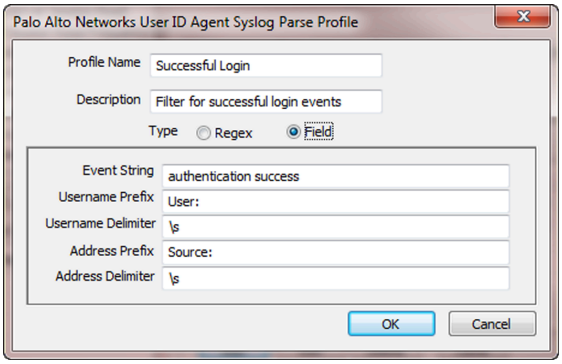
1. 為您要尋找的事件類型輸入 **Event String**（事件字串）。
   - 登入事件—對於範例訊息，字串 `authentication success` 表示登入事件。
   - 登出事件—對於範例訊息，字串 `logout successful` 表示登出事件。
2. 輸入 **Username Prefix**（使用者名稱首碼）來識別 syslog 訊息中使用者名稱欄位的開頭。此欄位不支援 \s（用於空格）或 \t（用於頁籤）之類的 regex 運算式。

   在範例訊息中，`User:` 表示使用者名稱欄位的開頭。
3. 輸入指示 syslog 訊息中使用者名稱欄位結尾的 **Username Delimiter**（使用者名稱分隔符號）。使用 **`\s`** 可表示獨立空格（如範例訊息所示），使用 **`\t`** 則可表示定位點。
4. 輸入 **Address Prefix**（位址首碼）來識別 Syslog 訊息中 IP 位址欄位的開頭。此欄位不支援 \s（用於空格）或 \t（用於頁籤）之類的 regex 運算式。

   在範例訊息中，`Source:` 表示位址欄位的開頭。
5. 輸入指示 syslog 訊息中 IP 位址欄位結尾的 **Address Delimiter**（位址分隔符號）。

   例如，輸入 **`\n`** 可指出要以分行符號作為分隔符號。

   以下範例為使用字串比對識別登入事件的完整 Syslog 剖析設定檔：



6. 按兩下 **OK**（確定）以儲存設定檔。

©2024 Palo Alto Networks, Inc.

STEP 5 | 指定 User-ID 代理程式將監控的 syslog 傳送程式。

在 User-ID 代理程式可監控的總共最多 100 台各類伺服器中，多達 50 台可以是 syslog 寄件者。

若收到的 syslog 訊息並非來自此清單上的傳送程式，User-ID 代理程式會一律將其捨棄。

1. 選取 **User Identification**（使用者識別） > **Discovery**（探索），然後 **Add**（新增） 項目到 Servers（伺服器）清單。
2. 輸入用來識別傳送程式的 **Name**（名稱）。
3. 輸入 syslog 傳送程式的 **Server Address**（伺服器位址）（IP 位址或 FQDN）。
4. 將 **Server Type**（伺服器位址）設為 **Syslog Sender**（**Syslog** 傳送程式）。
5. （選用）如果您要取代 syslog 訊息使用者名稱中的目前網域，或者如果您的 syslog 訊息不包含網域，要在使用者名稱前面加上網域，則輸入 **Default Domain Name**（預設網域名稱）。
6. 對於傳送程式支援的每種 syslog 格式，**Add**（新增）Syslog 剖析設定檔到 Filter（篩選器）清單。選取您設定每個設定檔要識別的 **Event Type**（事件類型）—**login**（登入）（預設）或 **logout**（登入），然後按一下 **OK**（確定）。
7. 按一下 **OK**（確定）以儲存設定。
8. 將變更 **Commit**（提交）至 User-ID 代理程式組態。

©2024 Palo Alto Networks, Inc.

STEP 6 | 確定在使用者登入和登出時，User-ID 代理程式是否新增和刪除使用者對應。

您可以使用 CLI 命令來查看關於 *syslog* 傳送程式、*syslog* 訊息和使用者對應的其他資訊。

1. 登入受監控 syslog 傳送程式將為其產生登入和登出事件訊息的用戶端系統。
2. 確定 User-ID 代理程式是否已將登入使用者名稱對應到用戶端 IP 位址：
   1. 在 User-ID 代理程式中，選取 **Monitoring**（監控）。
   2. 在篩選欄位輸入使用者名稱或 IP 位址，**Search**（搜尋），然後確認清單中是否顯示了對應。
3. 確定防火牆是否收到了來自 User-ID 代理程式的使用者對應：
   1. 登入防火牆 CLI。
   2. 執行下列命令：

      ```
      > show user ip-user-mapping ip <ip-address>
      ```

      若防火牆收到了使用者對應，輸出將類似於：

      ```
      IP address:    192.0.2.1 (vsys1) User:          localdomain
      \username From:          SYSLOG
      ```
4. 登出用戶端系統。
5. 確定 User-ID 代理程式是否已移除使用者對應：
   1. 在 User-ID 代理程式中，選取 **Monitoring**（監控）。
   2. 在篩選欄位輸入使用者名稱或 IP 位址，**Search**（搜尋），然後確認清單中是否顯示對應。
6. 確認防火牆是否已偵測使用者對應：
   1. 存取防火牆 CLI。
   2. 執行下列命令：

      ```
      > show user ip-user-mapping ip <ip-address>
      ```

      若防火牆刪除了使用者對應，輸出將類似於：

      ```
      No matched record
      ```

使用驗證入口網站將 IP 位址對應到使用者名稱

當使用者啟動與 驗證原則 規則相符的 Web 流量（HTTP 或 HTTPS）時，防火牆會提示使用者透過驗證入口網站進行驗證。這可以確保您能準確知道誰在存取最敏感的應用程式和資料。根據驗證期

©2024 Palo Alto Networks, Inc.

間收集的使用者資訊，防火牆將建立新的 IP 位址到使用者名稱對應，或者為該使用者更新現有的對應。這種使用者對應方法適用於防火牆無法透過監控伺服器等其他方式瞭解對應情況的環境。例如，您可能有一些未登入受監控網域伺服器的使用者，例如 Linux 用戶端上的使用者。

- 驗證入口網站驗證方式
- 驗證入口網站模式
- 設定驗證入口網站

驗證入口網站驗證方式

驗證入口網站使用以下方法來驗證 Web 要求與驗證原則規則相符的使用者：

驗證方法	說明
Kerberos SSO	防火牆會使用 Kerberos 單一登入 (SSO)，以透明方式從瀏覽器取得使用者認證。若要使用此方法，您的網路必須要有 Kerberos 基礎結構，包括具有驗證伺服器和票證授予服務的金鑰發佈中心 (KDC)。防火牆必須有 Kerberos 帳戶。 如果 Kerberos SSO 驗證失敗，防火牆會回復至 Web 表單或用戶端憑證驗證，具體視乎於您的驗證原則和驗證入口網站設定。
Web 表單	防火牆會將網頁要求重新導向至網頁表單進行驗證。對於這種方法，您可以設定驗證原則使用多重要素驗證 (MFA)、SAML、Kerberos、TACACS+、RADIUS 或 LDAP 驗證。雖然使用者必須手動輸入登入認證，但此方法可適用於所有瀏覽器和作業系統。
用戶端憑證驗證	防火牆會提示瀏覽器提供有效的用戶端憑證來驗證使用者。若要使用此方法，您必須提供各使用者系統用戶端憑證，並安裝用於發行防火牆憑證受信任的憑證授權單位 CA 憑證。

驗證入口網站模式

驗證入口網站模式會定義防火牆如何擷取網頁要求以進行驗證：

模式	說明
透明	防火牆會根據驗證原則來攔截瀏覽器流量，並模擬原始目的地 URL，發行 HTTP 401 用以呼叫驗證。但是，由於防火牆沒有目的地 URL 的實際憑證，因此瀏覽器會在使用者嘗試存取安全的網站時顯示憑證錯誤。因此，只能在確實有必要時使用此模式，例如 Layer 2 或 Virtual Wire 部署。

©2024 Palo Alto Networks, Inc.

模式	說明
重新導向	防火牆會攔截未知的 HTTP 或 HTTPS 工作階段，並使用 HTTP 302 重新導向，將其重新導向至防火牆上的 Layer 3 介面，以執行驗證。這是系統偏好的模式，因為此模式提供更出色的使用者體驗 (無憑證錯誤)。然而，此模式需要其他的 Layer 3 設定。另一項重新導向模式的優勢在於，該模式提供工作階段 Cookie，這可讓使用者持續瀏覽驗證的網站，而無需在每次逾時到期時重新對應。這對在 IP 位址間漫遊的使用者（例如，從企業 LAN 到無線網路）特別實用，因為只要工作階段維持開啟，他們就不需要在 IP 位址變更時重新驗證。 如果您使用 Kerberos SSO，則必須使用重新導向模式，因為瀏覽器只會提供認證給信任的網站。如果您使用 多因素驗證 來對驗證入口網站使用者進行驗證，還需要重新導向模式。

設定驗證入口網站

下列程序介紹了如何透過設定整合了 PAN-OS 的 User-ID 代理程式來設定驗證入口網站，以將符合驗證原則規則的 Web 要求重新導向至防火牆介面（重新導向主機）。

SSL 輸入檢查不支援驗證入口網站重新導向。要使用驗證入口網站重新導向和解密，您必須使用 SSL 正向 Proxy。

根據敏感性，使用者透過驗證入口網站存取的應用程式需要不用的驗證方法和設定。為了適應所有驗證需求，您可以使用預設和自訂的驗證強制物件。每個物件均會將一個驗證規則與一個驗證設定檔和一種驗證入口網站驗證方法關聯起來。

- 預設驗證強制物件—如果您要將多個驗證規則與同一個全域驗證設定檔關聯，則使用預設物件。您必須在設定驗證入口網站之前，先設定此驗證設定檔，然後在驗證入口網站設定中指派它。對於需要多因素驗證 (MFA) 的驗證規則，您不能使用預設的驗證強制物件。
- 自訂驗證強制物件—為每個需要非全域驗證設定檔的驗證規則使用自訂物件。需要 MFA 的驗證規則必須使用自訂物件。若要使用自訂物件，在設定驗證原則時，要建立驗證設定檔，並在設定驗證入口網站之後，將這些設定檔指派給相應物件。

請注意，只有在使用者透過驗證入口網站 Web 表單或 Kerberos SSO 驗證時，才需要驗證設定檔。除了這些方法以外，下列程序還介紹了如何實作用戶端憑證驗證。

如果您在不使用其他 *User-ID* 功能（使用者對應及群組對應）的情況下使用驗證入口網站，則不需要設定 *User-ID* 代理程式。

©2024 Palo Alto Networks, Inc.

STEP 1 | 設定防火牆將用於傳入 Web 要求、驗證使用者，以及與目錄伺服器通訊以將使用者名稱對應至 IP 位址的介面。

防火牆連線至驗證伺服器或 User-ID 代理程式時，依據預設，它會使用管理介面。作為最佳做法，透過設定服務路由隔離管理網路，以連線至驗證伺服器或 User-ID 代理程式。

1. （僅限 MGT 介面）選取 **Device**（裝置） > **Setup**（設定） > **Interfaces**（介面），編輯 **Management**（管理） 介面，選取 **User- ID**，然後按一下 **OK**（確定）。
2. （僅限非 MGT 介面）將介面管理設定檔指派給防火牆將用來傳入 Web 要求和與目錄伺服器通訊的 Layer 3 介面。您必須 Interface Management（介面管理）設定檔中啟用 **Response Pages**（回應頁面）和 **User ID**（使用者 **ID**）。
3. （僅限非 MGT 介面）為防火牆將用來驗證使用者的介面設定服務路由。如果防火牆有多個虛擬系統 (vsys)，則服務路由可以是全域或 vsys 專用的。服務必須包含 **LDAP**，並且可能包含：
   - **Kerberos**、**RADIUS**、**TACACS+** 或 多因素驗證—為您使用的任何驗證服務設定服務路由。
   - **UID** 代理程式—僅當您啟用基於使用者和群組的原則時設定此服務。
4. （僅限重新導向模式）建立將 Layer 3 介面上的 IP 位址對應至重新導向主機的 DNS 位址 (A) 記錄。如果您要使用 Kerberos SSO，則還必須新增會執行相同對應的 DNS 指標 (PTR) 記錄。

如果您的網路不支援從任何防火牆介面對目錄伺服器進行存取，則必須使用 Windows User-ID 代理程式設定使用者對應。

STEP 2 | 請確實設定網域名稱系統 (DNS) 來解析您的網域控制站位址。

若要確認解析正確，請 Ping 伺服器 FQDN。例如：

```
admin@PA-220> ping host dc1.acme.com
```


©2024 Palo Alto Networks, Inc.

STEP 3 | 將用戶端設定為信任驗證入口網站憑證。

重新導向模式的必要項目—以透明的方式重新導向使用者，而不顯示憑證錯誤。您可以產生自我簽署憑證，會匯入外部憑證授權單位 (CA) 所簽署的憑證。

若要使用自我簽署憑證，請建立根 CA 憑證，然後用它來簽署您要用於驗證入口網站的憑證：

1. 選取 **Device**（設備）> **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Device Certificates**（裝置憑證）。
2. 建立自我簽署根 CA 憑證或匯入 CA 憑證（請參閱匯入憑證與私密金鑰）。
3. 產生憑證以用於驗證入口網站。請確實設定下列欄位：
   - 通用名稱—為 Layer 3 介面輸入內部網路主機的 DNS 名稱。
   - 簽署者—選取您剛剛建立或匯入的 CA 憑證。
   - 憑證屬性—按一下 **Add**（新增），針對 **Type**（類型）選取 **IP**，針對 **Value**（值）則輸入防火牆要將要求重新導向到之 Layer 3 介面的 IP 位址。
4. 設定 SSL/TLS 服務設定檔。將您剛剛建立的驗證入口網站憑證指派給設定檔。

   如果您不指派 *SSL/TLS* 服務設定檔，依據預設，防火牆會使用 *TLS 1.2*。若要使用不同的 *TLS* 版本，請為您要使用的 *TLS* 版本設定 *SSL/TLS* 服務設定檔。
5. 將用戶端設定為信任該憑證：
   1. 匯出 CA 憑證（您剛剛建立或匯入的）。
   2. 將憑證當成信任的 CA 匯入至所有用戶端瀏覽器；方式是手動設定瀏覽器，或新增憑證至 Active Directory 群組原則物件 (GPO) 中的信任根。

STEP 4 | （選用）設定用戶端憑證驗證。

您不需要對用戶端憑證驗證使用驗證設定檔或順序。如果您同時設定驗證設定檔/順序和憑證驗證，使用者必須同時使用兩者進行驗證。

1. 請使用根 CA 憑證，為將透過驗證入口網站進行驗證的每個使用者產生用戶端憑證。在此情況下，CA 通常是您的企業 CA，而不是防火牆。
2. 以 PEM 格式匯出 CA 憑證至防火牆可存取的系統。
3. 匯入 CA 憑證到防火牆：請參閱匯入憑證與私密金鑰。匯入之後，請按一下匯入的憑證、選取 **Trusted Root CA**（信任的根 **CA**），然後按一下 **OK**（確定）。
4. 設定憑證設定檔。
   - 在 **Username Field**（使用者名稱欄位）下拉式清單中，選取包含 User-ID 資訊的憑證欄位。
   - 在 **CA Certificates**（**CA** 憑證）清單中，按一下 **Add**（新增），然後選取您剛匯入的 CA 憑證。

©2024 Palo Alto Networks, Inc.

STEP 5 | （選用）為 Apple Captive Network Assistant 設定驗證入口網站。

僅在將驗證入口網站與 Apple Captive Network Assistant (CNA) 搭配使用時，才需要執行此步驟。若要將驗證入口網站與 CNA 搭配使用，請執行以下步驟。

1. 確認您是否已為重新導向主機指定了 FQDN（而不僅僅是 IP 位址）。
2. 選取 SSL/TLS 服務設定檔，可使用指定 FQDN 之公開簽署的憑證。
3. 輸入下列命令以調整驗證入口網站支援的要求數：**set deviceconfig setting ctd cap-portal-ask-requests *<threshold-value>***

   依預設，防火牆為驗證入口網站設有速率限制臨界值，用於將要求數限制為每兩秒發出一個要求。CNA 傳送多個可能超出此限制的要求，這可能會導致 TCP 重設和 CNA 錯誤。建議的臨界值為 5（預設值為 1）。該值表示每兩秒最多容許 5 個要求。視所處環境而定，您可能需要設定其他值。若目前值不足以處理要求數，請增加該值。

STEP 6 | 設定驗證入口網站設定。

1. 選取 **Device**（裝置） > **User Identification**（使用者識別） > **Authentication Portal Settings**（驗證入口網站設定），然後編輯設定。
2. 啟用驗證入口網站（預設為已啟用）。
3. 指定 **Timer**（計時器），這是使用者透過驗證入口網站進行驗證後，防火牆為使用者保留 IP 位址到使用者名稱對應的最長時間，以分鐘為單位（預設值為 60；範圍為

 ©2024 Palo Alto Networks, Inc.

1-1440）。**Timer**（計時器）過期後，防火牆將移除對應以及任何用於評估驗證原則規則中 **Timeout**（逾時）值的相關驗證時間戳記。

在評估驗證入口網站 ***Timer***（計時器）和每個驗證原則規則中 ***Timeout***（逾時）值時，防火牆將提示使用者針對最先過期的設定進行重新驗證。重新驗證後，防火牆將重設驗證入口網站 ***Timer***（計時器）的時間計數，並為使用者記錄新的驗證時間戳記。因此，為了對不同驗證規則啟用不同的 ***Timeout***（逾時）期間，需將驗證入口網站 ***Timer***（計時器）設定為大於或等於任意規則 ***Timeout***（逾時）設定的值。

4. 選取您為透過 TLS 的重新導向要求建立的 **SSL/TLS Service Profile**（SSL/TLS 服務設定檔）。請參閱設定 SSL/TLS 服務設定檔。
5. 選取 **Mode**（模式）（在此範例中為 **Redirect**（重新導向））。
6. （僅限重新導向模式）指定 **Redirect Host**（重新導向主機），其是一個內部網路主機名稱（在其名稱中沒有句點的主機名稱），會在防火牆上解析為 Web 要求將被重新導向到的 Layer 3 介面的 IP 位址。

   如果使用者透過 Kerberos 單一登入 (SSO) 進行驗證，**Redirect Host**（重新導向主機）必須與 Kerberos 金鑰標籤中指定的主機名稱相同。
7. 選取要使用的回復驗證方法：
   - 若要使用用戶端憑證驗證，請選取您所建立的 **Certificate Profile**（憑證設定檔）。
   - 若要為互動式或 SSO 驗證使用全域設定，則選取您所設定的 **Authentication Profile**（驗證設定檔）。
   - 若要為互動式或 SSO 驗證使用特定驗證原則規則設定，則在設定驗證原則時，將驗證設定檔指派給驗證強制物件。
8. 按一下 **OK**（確定），然後 **Commit**（提交）驗證入口網站設定。

STEP 7 | 接下來的步驟...

在您設定驗證原則規則（以在使用者要求服務或應用程式時觸發驗證）之前，防火牆不會向使用者顯示驗證入口網站 Web 表單。

設定終端伺服器使用者的使用者識別

個別的終端機伺服器使用者似乎有相同的 IP 位址，因此 IP 位址對使用者名稱的對應已不足以識別特定的使用者。為在 Windows 終端機伺服器上識別特定的使用者，Palo Alto Networks 終端機伺服器代理程式（TS 代理程式）會將某個範圍的連接埠配置給每個使用者。接著，TS 代理程式會通知每個連線的防火牆所配置的連接埠範圍，這會讓防火牆建立 IP 位址-連接埠-使用者對應表，並啟用使用者與群組安全性原則執行。對於非 Windows 終端機伺服器，請設定 PAN-OS XML API 擷取使用者識別資訊。以下值適用於此兩種方法：

- 預設連接埠：1025 到 65534
- 各使用者區塊大小：200
- 多重使用者系統數目上限：2,500

©2024 Palo Alto Networks, Inc.

關於 TS 代理程式支援的終端機伺服器資訊及各防火牆型號支援的 TS 代理程式數目，請參閱 Palo Alto Networks Compatibility Matrix（Palo Alto Networks 相容性矩陣）和 Product Comparison Tool（產品比較工具）。

下列各節說明終端機伺服器使用者的使用者識別：

- 設定 Palo Alto Networks 終端機伺服器 (TS) 代理程式進行使用者對應
- 使用 PAN-OS XML API 從終端機伺服器擷取使用者識別

設定 Palo Alto Networks 終端機伺服器 (TS) 代理程式進行使用者對應

使用下列程序在終端機伺服器上安裝和設定 TS 代理程式。若要對應所有使用者，您必須在使用者登入的所有終端機伺服器上安裝 TS 代理程式。

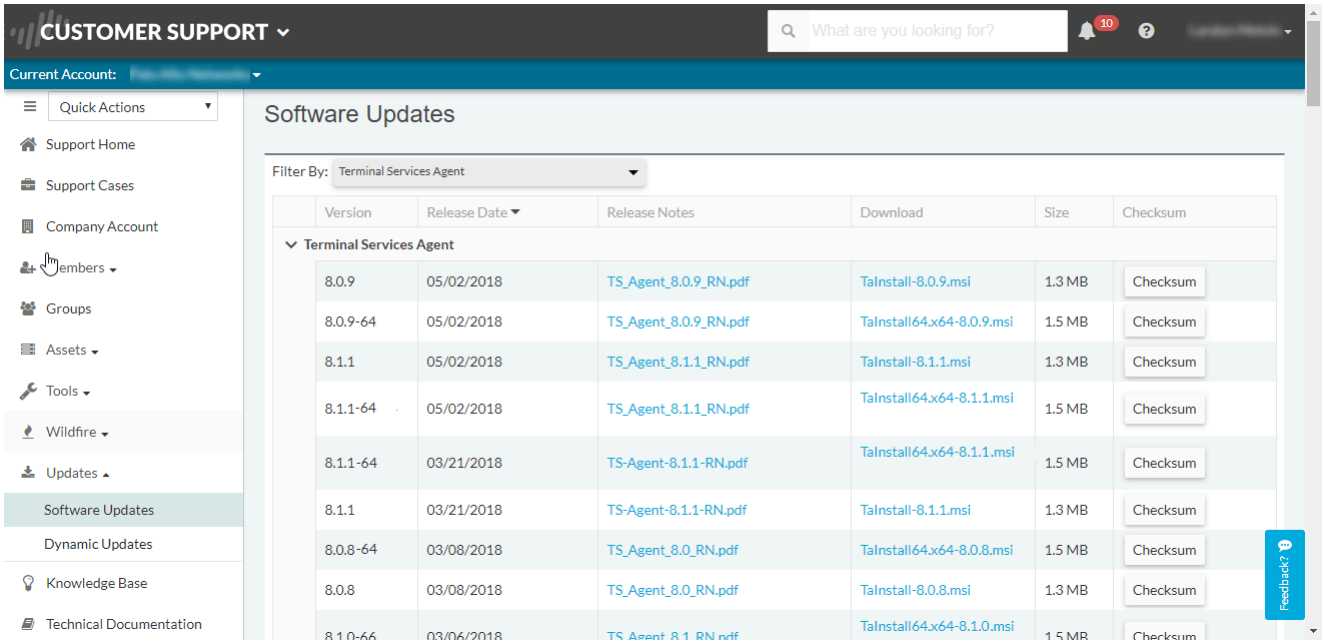
如果您使用的是 *TS* 代理程式 *7.0* 版或更高版本，請停用 *TS* 代理程式主機上的任何 *Sophos* 防毒軟體。否則，防毒軟體將覆寫 *TS* 代理程式分配的來源連接埠。

如需預設值、範圍和其他規範的相關資訊，請參閱 設定終端伺服器使用者的使用者識別。如需 *TS* 代理程式支援的終端機伺服器的資訊及各防火牆型號支援的 *TS* 代理程式數目，請參閱 Palo Alto Networks 相容性矩陣。

©2024 Palo Alto Networks, Inc.

STEP 1 | 下載 TS 代理程式安裝程式。

1. 登入 Palo Alto Networks 客戶支援入口網站。
2. 選取 **Updates**（更新） > **Software Updates**（軟體更新）。
3. 將 **Filter By**（篩選依據）設定為 **Terminal Services Agent**（終端機服務代理程式），然後選取要從相應 Download（下載）欄中安裝之代理程式的版本。例如，下載 TS 代理程式，選取**TaInstall-9.0.msi**。
4. 將 `TaInstall.x64-x.x.x-xx.msi` 或 `TaInstall-x.x.x-xx.msi` 檔案（確保根據 Windows 系統執行的是 32 位元或 64 位元作業系統選取適當的版本）儲存在您計劃安裝代理程式的系統上。



STEP 2 | 以管理員身分執行安裝程式。

1. 開啟 Windows **Start**（開始）功能表，以滑鼠右鍵按一下 **Command Prompt**（命令提示）程式，然後 **Run as administrator**（以系統管理員身分執行）。
2. 從命令列中執行您下載的 .msi 檔案。例如，如果您將 `TaInstall-9.0.msi` 檔案儲存在桌面上，然後可以輸入下列命令：

```
C:\Users\administrator.acme>cd Desktop
```


©2024 Palo Alto Networks, Inc.

```
C:\Users\administrator.acme\Desktop>TaInstall-9.0.0-1.msi
```

3. 依照安裝提示使用預設設定安裝代理程式。設定將代理程式安裝在 `C:\ProgramFiles\Palo Alto Networks\Terminal Server Agent` 中。

   為確保連接埠分配正確，您必須使用預設的終端機伺服器代理程式安裝資料夾位置。

4. 安裝完成時，**Close**（關閉）設定對話框。

   如果您正要升級的 *TS* 代理程式版本有比現有安裝更新的驅動程式，安裝精靈會提示您在升級之後重新啟動系統。

STEP 3 | 為配置到使用者的 TS 代理程式定義連接埠範圍。

System Source Port Allocation Range（系統來源連接埠配置範圍）與 ***System Reserved Source Ports***（系統預留來源連接埠）可指定配置到非使用者工作階段的連接埠範圍。確定在這些欄位中的值未與您為使用者流量指定的連接埠重疊。這些值只能透過編輯對應的 *Windows* 登錄設定來變更。*TS* 代理程式不會為工作階段 *0* 發出的網路流量分配連接埠。

1. 開啟 Windows **Start**（開始）功能表，然後選取 **Terminal Server Agent**（終端機伺服器代理程式）以啟動終端機伺服器代理程式應用程式。
2. 設定（側功能表）代理程式。
3. 輸入 **Source Port Allocation Range**（來源連接埠配置範圍）（預設值是 20,000 至 39,999）。這是 TS 代理程式將配置給使用者識別的完整連接埠號碼範圍。您指定的連接埠範圍不能重疊 **System Source Port Allocation Range**（系統來源連接埠配置範圍）。
4. （選用）如果在來源連接埠範圍內有您不想要 TS 代理程式配置給使用者工作階段的連接埠或連接埠範圍，請將這些連接埠指定為 **Reserved Source Ports**（預留來源連接埠）。若要包含多個範圍，請使用逗號隔開，且不加空格，（例如：**`2000-3000,3500,4000-5000`**）。
5. 指定登入終端機伺服器（**Port Allocation Start Size Per User**（各使用者的連接埠配置起始大小））時要配置給每個個別使用者的連接埠數目；預設值是 200 。
6. 指定 **Port Allocation Maximum Size Per User**（各使用者的連接埠配置大小限制），這是終端機伺服器代理程式可配置給個別使用者的連接埠數目上限。
7. 指定使用者用盡所有配置的連接埠時是否繼續處理使用者的流量。**Fail port binding when available ports are used up**（可用的連接埠已耗盡而無法繫結）的選項依預設會啟用，這表示當所有連接埠均用盡時，應用程式便無法傳送流量。若要讓使用者在連接埠用盡時繼續使用應用程式，請停用（清除）此選項，但如果按此操作，則可能無法使用 User-ID 識別此流量。
8. 如果終端機伺服器在您嘗試將其關閉時停止回應，請啟用 **Detach agent driver at shutdown**（關機時分離代理程式驅動程式）選項。

©2024 Palo Alto Networks, Inc.

STEP 4 | （選用）指派您自己的憑證，以使 TS 代理程式和防火牆相互驗證。

1. 從企業 PKI 取得 TS 代理程式憑證，或在防火牆上產生一個。伺服器的私密金鑰必須加密，且憑證必須以 PEM 檔案格式上傳。執行以下某項工作以上傳憑證：
   - Generate a Certificate（產生憑證）並匯出。
   - 從企業憑證授權單位 (CA) 匯出憑證。
2. 新增伺服器憑證到 TS 代理程式。
   1. 在 TS 代理程式上，選取 **Server Certificate**（伺服器憑證），然後 **Add**（新增）新的憑證。
   2. 輸入從 CA 接收的憑證檔案的路徑與名稱，或瀏覽該憑證檔案。
   3. 輸入私密金鑰密碼。
   4. 按一下 **OK**（確定）。
   5. **Commit**（提交）您的變更。

   TS 代理程式在連接埠 *5009* 上使用自我簽署憑證，具有以下資訊：簽發者：*CN*=終端伺服器代理程式，*OU*=工程，*O*=*Palo Alto Networks*，*L*=聖塔克拉拉，*S*=加利福尼亞州，*C*=美國主體：*CN*=終端伺服器代理程式，*OU*=工程，*O*=*Palo Alto Networks*，*L*=聖塔克拉拉，*S*=加利福尼亞州，*C*=美國
3. 為防火牆設定並指派憑證設定檔。
   1. 選取 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates Profile**（憑證設定檔） 以 設定憑證設定檔 。

      您只能為 *Windows User-ID* 代理程式和 *TS* 代理程式指派一個憑證設定檔。因此，憑證設定檔中必須包含簽發了已上傳至所連線 *Windows User-ID* 和 *TS* 代理程式之憑證的所有憑證授權單位。
   2. 選取 **Device**（裝置） > **User Identification**（使用者識別） > **Connection Security**（連線安全性）。
   3. 編輯 (⚙) 和選取上一步中設定的憑證設定檔作為**User-ID Certificate Profile**（**User-ID** 憑證設定檔）。
   4. 按一下 **OK**（確定）。
   5. **Commit**（提交）您的變更。

©2024 Palo Alto Networks, Inc.

STEP 5 | 設定要與終端機伺服器代理程式連線的防火牆。

在每個您要連線至終端機伺服器代理程式的防火牆上完成下列步驟，以接收使用者對應：

1. 選取 **Device**（裝置） > **User Identification**（使用者識別） > **Terminal Server Agents**（終端機伺服器代理程式），然後 **Add**（新增）新的 TS 代理程式。
2. 輸入終端機伺服器代理程式的 **Name**（名稱）。
3. 輸入安裝終端機伺服器代理程式之 Windows **Host**（主機）的主機名稱或 IP 位址。

   主機名稱或 IP 位置必須解析為靜態 IP 位址。如果變更現有主機名稱，提交變更時，TS 代理程式將重設，以解析新主機名稱。如果主機名稱解析為多個 IP 位址，TS 代理程式將使用清單中的第一個位址。
4. （選用）輸入任何可顯示為傳出流量來源 IP 位址的 **Alternative IP Addresses**（替代 **IP** 位址）之主機名稱或 IP 位址。

   主機名稱或 IP 位置必須解析為靜態 IP 位址。您可輸入最多 8 個 IP 位址或主機名稱。
5. 輸入代理程式 用來接聽使用者識別要求的連接埠號碼。此值必須符合終端機伺服器代理程式上設定的值。依預設，在防火牆與代理程式上連接埠設為 5009。如果您在防火牆變更連接埠，則也必須變更終端機伺服器代理程式 **Configure**（設定）對話的 **Listening Port**（接聽連接埠）到同樣的連接埠。
6. 請確定組態為已啟用，然後按一下 **OK**（確定）。
7. **Commit**（提交）您的變更。
8. 確認 **Connected status**（連線狀態）是否顯示為已連線（綠燈）。

STEP 6 | 確認終端機伺服器代理程式已成功將 IP 位址對應至使用者名稱，且防火牆可連線至代理程式。

1. 開啟 Windows **Start**（開始）功能表，然後選取 **Terminal Server Agent**（終端機伺服器代理程式）。
2. 確保 [連線清單] 中各防火牆的 **Connection Status**（連線狀態）為 `Connected`（已連線），以確認防火牆可連線。
3. 驗證終端機伺服器代理程式成功將連接埠範圍對應至使用者名稱（側功能表中的 **Monitoring**（監控）），並確認對應表格已填寫。

©2024 Palo Alto Networks, Inc.

STEP 7 | （僅限 Windows 2012 R2 伺服器） 在 Microsoft Internet Explorer 中為使用瀏覽器的每個使用者停用增強保護模式。

此工作對於其他瀏覽器（例如 Google Chrome 或 Mozilla Firefox）而言並不必要。

若要為所有使用者停用增強保護模式，請使用 Local Security Policy（本機安全性原則）。

在 Windows Server 上執行以下步驟：

1. 啟動 Internet Explorer。
2. 選取 **Settings**（設定） > **Internet options**（網際網路選項） > **Advanced**（進階），然後捲動至 Security（安全性）區段。
3. 停用（清除）**Enable Enhanced Protected Mode**（啟用增強保護模式）。
4. 按一下 **OK**（確定）。

在 *Internet Explorer* 中，*Palo Alto Networks* 建議您不要停用保護模式（與增強保護模式有所差別）。

使用 PAN-OS XML API 從終端機伺服器擷取使用者識別

PAN-OS XML API 使用標準 HTTP 要求來傳送和接收資料。直接從 cURL 之類的命令行公用程式，或使用支援 RESTful 服務的任何指令碼或應用程式架構，即可進行 API 呼叫。

若要讓非 Windows 終端機伺服器將使用者識別資訊直接傳送至防火牆，請建立指令碼以擷取使用者登入與登出事件，並將這些事件用於輸入至 PAN-OS XML API 要求格式。接著定義機制以使用 cURL 或 wget 並提供防火牆的 API 金鑰進行安全通訊，藉此將 XML API 要求提交至防火牆。若要從終端機伺服器等多重使用者系統中建立使用者識別，則必須使用下列其中一種 API 訊息：

- **<multiusersystem>**—在防火牆上設定 XML API 多重使用者系統設定。此訊息允許定義終端機伺服器 IP 位址 (這將是該終端機伺服器上所有使用者的來源位址)。此外，**<multiusersystem>** 設定訊息會指定要配置用於使用者對應的來源連接埠號碼範圍，以及登入時配置給每個使用者的連接埠數（稱為區塊大小）。如果您要使用預設的來源連接埠配置範圍 (1025-65534) 與區塊大小 (200)，您不必將 **<multiusersystem>** 設定事件傳送至防火牆。相反地，防火牆會在收到第一個使用者登入事件訊息時用預設定自動產生 XML API 多重使用者系統設定。
- **<blockstart>**—搭配 **<login>** 與 **<logout>** 訊息使用，以指示配置給使用者的來源連接埠開始號碼。接著防火牆會使用區塊大小來判定連接埠號碼的實際範圍，以對應至登入訊息中的 IP 位址與使用者名稱。例如，**<blockstart>** 值是 13200，為多重使用者系統設定的區塊大小是 300，配置給使用者的實際來源連接埠範圍是 13200 至 13499。由使用者所啟動的各連線，均應使用所配置範圍內的唯一來源連接埠號碼，讓防火牆能夠根據其 IP 位址-連接埠-使用者對應來識別使用者，以執行使用者與群組安全性規則。當使用者用盡所有配置的連接埠時，終端機伺服器必須傳送新的 **<login>** 訊息，以為使用者配置新的連接埠範圍，讓防火牆能夠更新 IP 位址-連接埠-使用者對應。此外，一個使用者名稱可以同時有多個已對應連接埠區塊。防火牆若收到含 **<blockstart>** 參數的 **<logout>** 訊息，便會將對應的 IP 位址-連接埠-使用者對應從其對應表格中移除。防火牆收到的 **<logout>** 訊息若含使用者名稱與 IP 位址，但

©2024 Palo Alto Networks, Inc.

不含 **<blockstart>**，便會將該使用者從其表格中移除。另外，防火牆若收到僅含 IP 位址的 **<logout>** 訊息，便會移除多重使用者系統及其關聯的所有對應。

終端機伺服器要傳送給防火牆的 *XML* 檔案可包含多種訊息類型，且這些訊息在檔案內不必有特定的順序。但在收到含多種訊類型的 *XML* 檔案時，防火牆將以下列順序處理這些檔案：先是多重使用者系統要求、接著為登入，最後是登出。

以下列工作流程為例，說明如何使用 PAN-OS XML API 將非 Windows 終端機伺服器的使用者識別傳送至防火牆。

STEP 1 | 產生 API 金鑰，用於驗證防火牆與終端機伺服器間的 API 通訊。若要產生金鑰，您必須提供管理帳戶的登入認證；API 可供所有管理員使用 (包括已啟用 XML API 權限的角色相關管理員)。

密碼中的任何特殊字元均必須以 *URL*/百分比加密。

從瀏覽器登入防火牆。接著開啟新的瀏覽器視窗，並輸入下列 URL，藉此為防火牆產生 API 金鑰：

```
https://<Firewall-IPaddress>/api/?
type=keygen&user=<username>&password=<password>
```

其中 **<Firewall-IPaddress>** 是防火牆的 IP 位址或 FQDN，**<username>** 與 **<password>** 是防火牆上管理使用者帳戶的認證。例如：

```
https://10.1.2.5/api/?type=keygen&user=admin&password=admin
```

防火牆會以包含金鑰的訊息回應，例如：

```
<response status="success">    <result>
       <key>k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg=</key>
    </result> </response>
```


©2024 Palo Alto Networks, Inc.

STEP 2 | （選用）產生一則設定訊息，終端機伺服器會傳送此訊息，以指定終端機伺服器代理程式使用的各使用者連接埠範圍與連接埠區塊大小。

如果終端機伺服器代理程式不傳送設定訊息，防火牆會在收到第一個登入訊息時，使用下列預設設定建立終端機服務代理程式組態：

- 預設連接埠：1025 到 65534
- 各使用者區塊大小：200
- 多重使用者系統數目上限：1,000

以下顯示範例設定訊息：

```
<uid-message> <payload> <multiusersystem> <entry ip="10.1.1.23"
 startport="20000"          endport="39999" blocksize="100/"> </
multiusersystem> </payload> <type>update</type> <version>1.0</
version> </uid-message>
```

其中 `entry ip` 會指定指派給終端機伺服器使用者的 IP 位址，`startport` 與 `endport` 會指定將連接埠指派給個別使用者時使用的連接埠範圍，`blocksize` 則指定要指派給每個使用者的連接埠數目。區塊大小上限為 4000，每個多重使用者系統最多可配置 1000 個區塊。

如果您定義自訂區塊大小和/或連接埠範圍，請記住您必須設定值，讓範圍中的每個連接埠都能獲得配置，沒有漏缺或未使用的連接埠。例如，如果您設定一個 1000-1499 的連接埠範圍，您應將區塊大小設為 100，而非 200。這是因為如果您設為 200，範圍結尾可能會有未使用的連接埠。

STEP 3 | 建立將擷取登入事件的指令碼，並建立要傳送至防火牆的 XML 輸入檔案。

確定指令碼會指派界限固定的連接埠號碼範圍，不會有重疊的連接埠。例如，如果連接埠範圍為 1000-1999，則區塊大小為 200，可接受的 blockstart 值為 1000、1200、1400、1600 或 1800。無法接受 blockstart 值為 1001、1300 或 1850，因為範圍中會有一些未使用的連接埠號碼。

終端機伺服器傳送至防火牆的登入事件承載可包含多個登入事件。

以下顯示 PAN-OS XML 登入事件的輸入檔案格式：

```
<uid-message> <payload> <login> <entry name="acme\jjaso"
 ip="10.1.1.23" blockstart="20000"> <entry name="acme\jparker"
 ip="10.1.1.23" blockstart="20100"> <entry name="acme\ccrisp"
 ip="10.1.1.23" blockstart="21000"> </login> </payload>
 <type>update</type> <version>1.0</version> </uid-message>
```

防火牆將使用此資訊填入使用者對應表格。根據從上例中所擷取的對應，如果防火牆收到來源位址與連接埠為 10.1.1.23:20101 的封包，會將要求對應至使用者 jparker 以執行原則。

每個多重使用者系統最多可配置 *1,000* 個連接埠區塊。

©2024 Palo Alto Networks, Inc.

STEP 4 | 建立將擷取登出事件的指令碼，並建立將傳送至防火牆的 XML 輸出檔案。

收到含 `blockstart` 參數的 `logout` 事件訊息時，防火牆會移除對應的 IP 位址-連接埠-使用者對應。如果 `logout` 訊息包含使用者名稱與 IP 位址，但未包含 `blockstart` 參數，防火牆會移除使用者所有的對應。如果 `logout` 訊息僅含 IP 位址，則防火牆會移除多重使用者系統及所有關聯的對應。

以下顯示 PAN-OS XML 登出事件的輸入檔案格式：

```
<uid-message> <payload> <logout> <entry name="acme\jjaso"
 ip="10.1.1.23" blockstart="20000"> <entry name="acme\ccrisp"
 ip="10.1.1.23"> <entry ip="10.2.5.4"> </logout> </payload>
 <type>update</type> <version>1.0</version> </uid-message>
```

您也可以使用下列 *CLI* 命令清除防火牆中的多重使用者系統項目：***clear xml-api multiusersystem***

STEP 5 | 確定您建立的指令碼包含方法可動態執行：使用 XML API 配置的連接埠區塊範圍會符合指派給終端機伺服器上使用者的實際來源連接埠，以及當使用者登出或連接埠配置變更時會移除對應。

方法就是使用 netfilter NAT 規則根據 UID 將使用者工作階段隱藏透過 XML API 配置的特定連接埠範圍之後。例如，若要確定 user ID 為 jjaso 的使用者對應至 10.1.1.23:20000-20099 的來源網路位址轉譯 (SNAT) 值，則您建立的指令碼應包括下列內容：

```
[root@ts1 ~]# iptables -t nat -A POSTROUTING -m owner --uid-owner
 jjaso -p tcp -j SNAT --to-source 10.1.1.23:20000-20099
```

同樣地，您建立的指令碼也應確保當使用者登出或連接埠配置變更時，IP 表格路由組態會動態移除 SNAT 對應：

```
[root@ts1 ~]# iptables -t nat -D POSTROUTING 1
```


©2024 Palo Alto Networks, Inc.

STEP 6 | 定義如何將包含設定、登入及登出事件的 XML 輸入檔案封裝至 wget 或 cURL 訊息，以傳輸至防火牆。

若要使用 **wget** 將檔案套用至防火牆：

```
> wget --post file <filename> “https://<Firewall-IPaddress>/api/?type=user-id&key=<key>&file-name=<input_filename.xml>&client=wget&vsys=<VSYS_name>”
```

例如，使用 wget 在 10.2.5.11 使用 k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg 金鑰將名為 login.xml 的輸入檔案傳送至防火牆的語法如下所示：

```
> wget --post file login.xml “https://10.2.5.11/api/?type=user-id&key=k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg&file-name=login.xml&client=wget&vsys=vsys1”
```

若要使用 **cURL** 將檔案套用至防火牆：

```
> curl --form file=@<filename> https://<Firewall-IPaddress>/api/?type=user-id&key=<key>&vsys=<VSYS_name>
```

例如，使用 cURL 在 10.2.5.11 使用 k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg 金鑰將名為 login.xml 的輸入檔案傳送至防火牆的語法如下所示：

```
> curl --form file@login.xml “https://10.2.5.11/api/?type=user-id&key=k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg&vsys=vsys1”
```

STEP 7 | 確認防火牆成功從終端機伺服器接收登入事件。

透過開啟 SSH 對防火牆的連線，然後執行下列 CLI 命令來驗證設定：

若要確認終端機伺服器是否正透過 **XML** 連線至防火牆：

```
admin@PA-5250> show user xml-api multiusersystem Host Vsys
 Users Blocks ----------------------------------------
 10.5.204.43   vsys1      5         2
```

若要確認防火牆是否正透過 **XML** 從終端機伺服器接收對應：

```
admin@PA-5250> show user ip-port-user-mapping all Global max host
 index 1, host hash count 1 XML API Multi-user System 10.5.204.43
 Vsys 1, Flag 3 Port range:20000 - 39999 Port size: start 200;
 max 2000 Block count 100, port count 20000 20000-20199: acme
\administrator Total host:1
```

使用 XML API 將使用者對應傳送至 User-ID

User-ID 提供許多現成即用的方法來獲得使用者對應資訊。但是，您可能擁有擷取了使用者資訊但無法原生地與 User-ID 整合的應用程式或裝置。例如，您可能擁有無標準使用者對應方法支援的

 ©2024 Palo Alto Networks, Inc.

自訂、內部開發的應用程式或裝置。在此類情況下，可以使用 PAN-OS XML API 來建立自訂指令碼，以將資料傳送至整合了 PAN-OS 的 User-ID 代理程式或直接傳送至防火牆。PAN-OS XML API 使用標準 HTTP 要求來傳送和接收資料。直接從 cURL 之類的命令列公用程式，或使用支援 POST 和 GET 要求的任何指令碼或應用程式架構，進行 API 呼叫。

若要讓非外部系統將使用者對應資訊傳送至整合了 PAN-OS 的 User-ID 代理程式，可建立指令碼以擷取使用者登入與登出事件，並將這些事件用於輸入傳送至 PAN-OS XML API 要求。接著定義機制以將 XML API 要求提交至防火牆（例如使用 cURL），然後使用防火牆的 API 金鑰來進行安全通訊。如需詳細資訊，請參閱 PAN-OS XML API 用法指南。

©2024 Palo Alto Networks, Inc.

啟用使用者與群組原則

啟用 User-ID 後，您將能夠設定對特定使用者和群組套用的安全性原則。基於使用者的原則控制還可以包含應用程式資訊（包括其所屬的類別和子類別、基礎技術或者應用程式特性）。您可以定義原則規則，以根據使用者或使用者群組啟用應用程式（輸出或輸入方向）。

基於使用者的原則範例包括：

- 僅允許 IT 部門在標準連接埠上使用 SSH、Telnet 和 FTP 等工具。
- 僅允許技術支援服務群組使用 Slack。
- 允許所有使用者讀取 Facebook，但禁止使用 Facebook 應用程式並僅限行銷部門員工發佈帖文。

©2024 Palo Alto Networks, Inc.

為具有多個帳戶的使用者啟用原則

如果組織中有某個使用者具有多項責任，該名使用者可能會有多個使用者名稱（帳戶），分別具有不同的權限來存取特定的服務集，但所有的使用者名稱共用相同的 IP 位址（使用者的用戶端系統）。不過，在強制執行原則時，User-ID 代理程式只能將任何一個 IP 位址（或終端機伺服器使用者的 IP 位址和連接埠範圍）對應至一個使用者名稱，且您無法預測代理程式會對應哪個使用者名稱。若要對使用者所有的使用者名稱進行存取控制，您必須調整規則、使用者群組和 User-ID 代理程式。

例如，假設防火牆有一項規則允許使用者名稱 corp_user 存取電子郵件，且有一項規則允許使用者名稱 admin_user 存取 MySQL 伺服器。使用者以來自相同用戶端 IP 位址的使用者名稱進行登入。如果 User-ID 代理程式將此 IP 位址對應至 corp_user，則無論使用者以 corp_user 還是 admin_user 進行登入，防火牆都會將該使用者識別為 corp_user，並允許存取電子郵件，而不是 MySQL 伺服器。另一方面，如果 User-ID 代理程式將 IP 位址對應至 admin_user，則無論登入為何，防火牆一律會將使用者識別為 admin_user，並允許存取 MySQL 伺服器，而不是電子郵件。下列步驟說明如何在此範例中強制執行這兩項規則。

STEP 1 | 為需要不同存取權限的每個服務設定一個使用者群組。

在此範例中，每個群組分別用於一個服務（電子郵件或 MySQL 伺服器）。不過，為每一組需要相同權限的服務設定一個群組，是很常見的（例如，一個群組用於所有的基本使用者服務，一個群組用於所有的管理服務）。

如果您的組織已有可存取使用所需服務的使用者群組，請直接將用於低限制服務的使用者名稱新增至這些群組。在此範例中，與 MySQL 伺服器相較，電子郵件伺服器需要較低限制的存取權，而 corp_user 是存取電子郵件的使用者名稱。因此，您將 corp_user 新增至一個可存取電子郵件的群組 (corp_employees)，以及一個可存取 MySQL 伺服器的群組 (network_services)。

如果將使用者名稱新增至特定線有群組會違反您的組織實務準則，您可以根據 LDAP 篩選器來建立自訂群組。在此範例中，假設 network_services 是自訂群組，而您將其設定如下：

1. 選取 **Device**（裝置） > **User Identification**（使用者識別） > **Group Mapping Settings**（群組對應設定），然後 **Add**（新增）具有唯一 **Name**（名稱） 的群組對應組態。
2. 選取 LDAP **Server Profile**（伺服器設定檔），並確保 **Enabled**（已啟用）核取方塊已啟用。
3. 選取 **Custom Group**（自訂群組）頁籤，然後 **Add**（新增）自訂群組作為 **Name**（名稱）。
4. 指定與 corp_user 的 LDAP 篩選屬性相符的 **LDAP Filter**（**LDAP** 篩選），然後按一下 **OK**（確定）。
5. 按一下 **OK**（確定）與 **Commit**（提交）。

稍後，如果低限制服務的群組中有其他使用者獲得可存取高限制服務的其他使用者名稱，您可以將這些使用者名稱新增至高限制服務的群組。此案例比相反的情況更為常見；使用者若可存取限制較多的服務，通常已可存取限制較少的服務。

©2024 Palo Alto Networks, Inc.

STEP 2 | 請根據您剛設定的群組，設定用來控制使用者存取的規則。

如需詳細資訊，請參閱啟用基於使用者與群組的原則執行。

1. 設定可讓 corp_employees 群組存取電子郵件的安全性規則。
2. 設定可讓 network_services 群組存取 MySQL 伺服器的安全性規則。

STEP 3 | 設定 User-ID 代理程式的忽略清單。

這可以確保 User-ID 代理程式將用戶端 IP 位址對應到的使用者名稱，僅限於為您剛建立的規則指派的群組成員。忽略清單必須包含不屬於這些群組之使用者的所有使用者名稱。

在此範例中，您將 admin_user 新增至 Windows 型 User-ID 代理程式的忽略清單，以確定會將用戶端 IP 位址對應至 corp_user。這可以確保無論使用者是以 corp_user 還是 admin_user 的身分登入，防火牆都會將使用者識別為 corp_user，並同時套用您所設定的兩項規則，因為 corp_user 是規則所參考之群組的成員。

1. 建立 `ignore_user_list.txt` 檔案。
2. 開啟檔案，然後新增 admin_user。

   如果您稍後新增其他使用者名稱，每個名稱都必須位於個別的行上。
3. 將檔案儲存至代理程式安裝所在之網域伺服器上的 User-ID 代理程式資料夾。

> 如果您使用整合了 *PAN-OS* 的 *User-ID* 代理程式，請參閱使用整合 PAN-OS 的 User-ID 代理程式設定使用者對應，以瞭解如何設定忽略清單。

STEP 4 | 為受限的服務設定端點驗證。

這可以讓端點驗證使用者的認證，並保有為具有多個使用者名稱的使用者啟用存取權的能力。

在此範例中，您已設定防火牆規則，讓屬於 network_services 群組成員的 corp_user 能夠將服務要求傳送至 MySQL 伺服器。現在，您必須設定 MySQL 伺服器，使其藉由提示使用者輸入已授權的使用者名稱 (admin_user) 來回應任何未經授權的使用者名稱（例如 corp_user）。

> 如果使用者以 *admin_user* 的身分登入網路，該使用者將可直接存取 *MySQL* 伺服器，而不會再看見 *admin_user* 認證的提示。

在此範例中，corp_user 和 admin_user 都具有電子郵件帳戶，因此電子郵件伺服器不會再提供其他認證的提示，無論使用者在登入網路時所輸入的使用者名稱為何。

現在，防火牆已可為具有多個使用者名稱的使用者強制執行規則。

©2024 Palo Alto Networks, Inc.

確認 User-ID 組態

設定使用者及群組對應、在安全性原則中啟用 User-ID 並設定到驗證原則後，您應該驗證 User-ID 是否正常工作。

STEP 1 | 存取防火牆 CLI。

STEP 2 | 確認群組對應有效。

在 CLI 中，輸入下列操作命令：

```
> show user group-mapping statistics
```

STEP 3 | 確認使用者對應有效。

如果您使用 PAN-OS 整合式 User-ID 代理程式，您可使用下列命令來從 CLI 中確認：

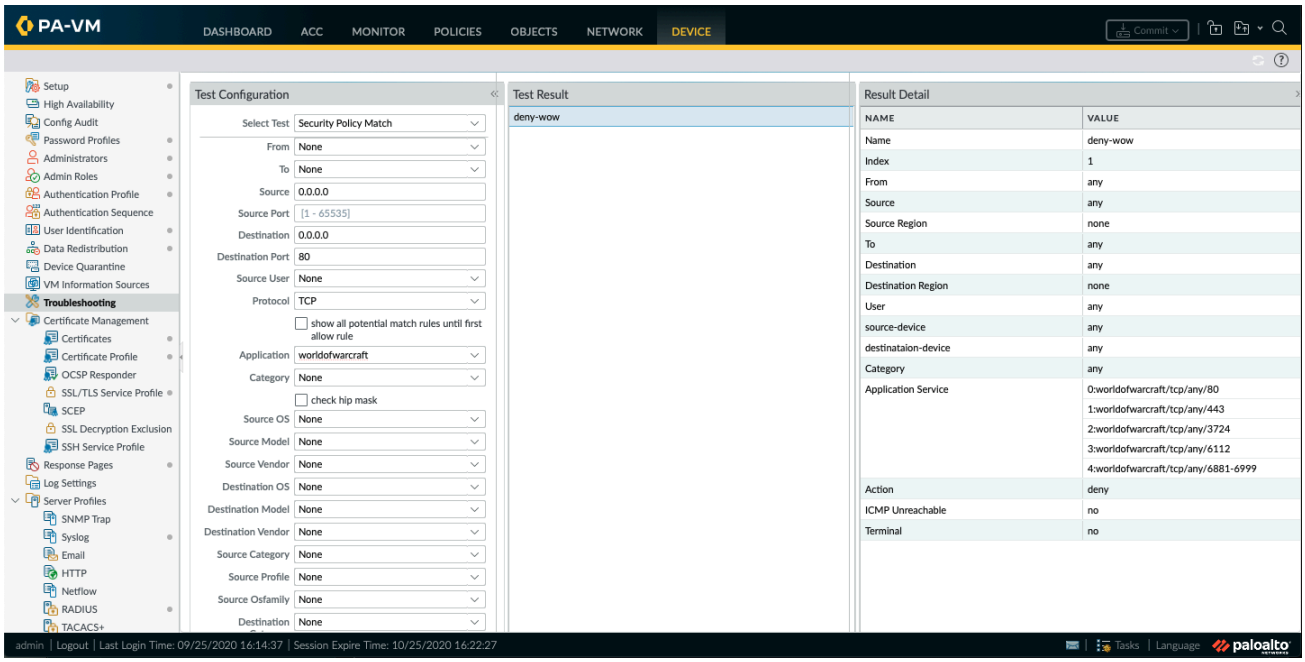
```
> show user ip-user-mapping-mp all
 IP              Vsys  From  User         Timeout (sec)
 ------------------------------------------------------
 192.168.201.1 vsys1 UIA   acme\george            210
 192.168.201.11 vsys1 UIA   acme\duane             210
 192.168.201.50 vsys1 UIA   acme\betsy             210
 192.168.201.10 vsys1 UIA   acme\administrator     210
 192.168.201.100 vsys1 AD    acme\administrator     748 Total:5
 users *:WMI probe succeeded
```


©2024 Palo Alto Networks, Inc.

STEP 4 | 測試安全性原則規則。

- 在啟用 User-ID 區域中的機器中，嘗試存取網站及應用程式，以測試在原則中定義的規則並確保允許和拒絕的流量與預期相同。
- 您還可以對執行中的組態進行疑難排解，以確定原則是否已正確設定。例如，假設您已設定封鎖使用者玩魔獸世界的規則，則您可按如下方式測試原則：

1. 選取 **Device**（裝置） > **Troubleshooting**（疑難排解），然後從 Select Test（選取測試）下拉式清單中選取 **Security Policy Match**（安全性原則比對）。
2. 輸入 **`0.0.0.0`** 作為來源與目的地 IP 位址。這將對任何來源與目的地 IP 位址執行原則比對測試。
3. 輸入目的地連接埠。
4. 輸入通訊協定。
5. **Execute**（執行）安全性原則比對測試。



©2024 Palo Alto Networks, Inc.

STEP 5 | 測試驗證原則及驗證入口網站設定。

1. 由相同的區域中，前往非目錄成員的機器，例如 Mac OS 系統，然後嘗試 Ping 區域外部的系統。偵測應不需驗證就能執行。
2. 在同一電腦上，開啟瀏覽器並導覽至目的地區域中符合您所定義之驗證規則的網站。驗證入口網站 Web 表單應顯示並提示您提供登入認證。
3. 使用正確認證登入並確認已將您重新導向至所需的頁面。
4. 您也可使用操作命令 **test authentication-policy-match** 測試驗證原則，如下所示：

```
> test authentication-policy-match from corporate to internet
 source 192.168.201.10 destination 8.8.8.8  Matched rule:
 'authentication portal' action: web-form
```

STEP 6 | 驗證日誌檔案會顯示使用者名稱。

選取日誌頁面（例如 **Monitor**（監控） > **Logs**（日誌） > **Traffic**（流量）），然後確認來源使用者欄會顯示使用者名稱。

STEP 7 | 確認報告會顯示使用者名稱。

1. 選取 **Monitor**（監控） > **Reports**（報告）。
2. 選取報告使用者名稱的報告類型。例如，拒絕應用程式報表（來源使用者）欄應顯示嘗試存取應用程式的使用者清單。

©2024 Palo Alto Networks, Inc.

在大規模網路中部署 User-ID

大規模網路可擁有數百個資訊來源，防火牆會查詢這些來源以將 IP 位址對應至使用者名稱並將使用者名稱對應至使用者群組。先彙總使用者對應及群組對應資訊再由 User-ID 代理程式收集，如此可以減少必要代理程式數目，從而為網路簡化 User-ID 管理。

大規模網路也可擁有使用對應資訊來強制執行原則的許多防火牆。您可以將某些防火牆設定成透過重新散佈而非直接查詢來獲取對應資訊，以此減少防火牆和資訊來源在查詢過程中使用的資源。重新散佈還讓防火牆可以在使用者依賴本機資源進行驗證（例如區域目錄服務）但需要存取遠端服務和應用程式（例如全域資料中心應用程式）時，強制執行以使用者為基礎的原則。

如果您設定驗證原則，則防火牆還必須重新散佈與使用者針對驗證挑戰的回應關聯的驗證時間戳記。防火牆將使用時間戳記來評估驗證原則規則的逾時。在逾時期間內，已成功驗證的使用者可以在稍後要求服務和應用程式，無需再次驗證。重新散佈時間戳記將允許您對每個使用者強制執行一致的逾時設定，即使最初授予使用者存取權的防火牆與後來控制該使用者的存取權的防火牆並不相同。

若您已設定多個虛擬系統，則可以透過選取一個虛擬系統作為 User-ID 中心點在虛擬系統之間共享 IP 位址到使用者名稱對應資訊。

- 為許多對應資訊來源部署 User-ID
- 重新散佈資料和驗證時間戳記
- 在虛擬系統之間共享 User-ID 對應

為許多對應資訊來源部署 User-ID

您可以使用 Windows 日誌轉送和通用類別目錄伺服器，簡化 Microsoft Active Directory (AD) 網域控制器或 Exchange 伺服器的大規模網路中的使用者對應和群組對應。這些方法透過先彙總對應資訊再由 User-ID 代理程式收集，如此減少必要代理程式數目，從而簡化 User-ID 管理。

- Windows 日誌轉送和通用類別目錄伺服器
- 規劃大規模的 User-ID 部署
- 設定 Windows 日誌轉送
- 為許多對應資訊來源設定 User-ID

Windows 日誌轉送和通用類別目錄伺服器

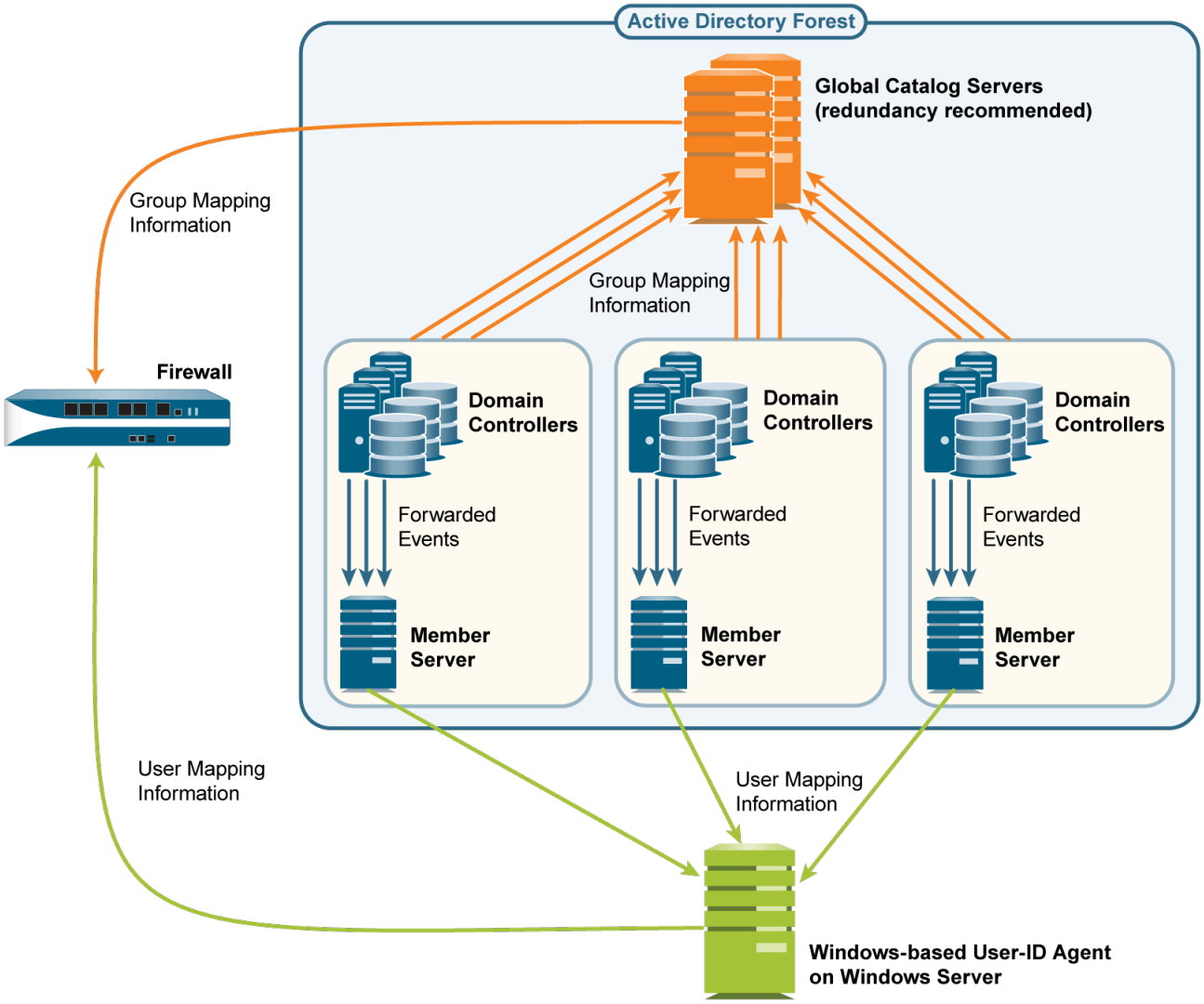
由於每個 User-ID 代理程式可監控多達 100 台伺服器，因此防火牆需要有多個 User-ID 代理程式，來監控具有數百個 AD 網域控制器或 Exchange 伺服器的網路。要建立及管理眾多的 User-ID 代理程式會有大量的管理負荷，尤其是在難以追蹤新網域控制站的大範圍網路中。Windows 日誌轉送可讓您減少所需監控的伺服器數目，進而減少所需管理的 User-ID 代理程式數目，而盡可能減輕管理負荷。當您設定 Windows 日誌轉送時，會有多個網域控制站將其登入事件匯出至 User-ID 代理程式從中收集使用者對應資訊的單一網域成員。

©2024 Palo Alto Networks, Inc.

您可以為 *Windows Server 2012* 和 *2012 R2* 等版本設定 *Windows* 日誌轉送。*Windows* 日誌轉送不適用於非 *Microsoft* 伺服器。

若要在大規模的網路中收集對應資訊，您可以設定防火牆，使其查詢從網域控制器接收帳戶資訊的通用類別目錄伺服器。

下圖說明防火牆使用 Windows 型 User-ID 代理程式的大規模網路中的使用者對應和群組對應。請參閱規劃大規模的 User-ID 部署以確認此部署是否適合您的網路。



規劃大規模的 User-ID 部署

在決定是否要將 Windows 日誌轉送和通用類別目錄伺服器用於您的 User-ID 實作時，請向您的系統管理員確認：

©2024 Palo Alto Networks, Inc.

- 網域控制站將登入事件轉送至成員伺服器所需的頻寬。此頻寬是網域控制站的登入速率 (每分鐘的登入數) 與每個登入事件的位元組大小相乘的積。

  網域控制站不會轉送全部的安全性日誌；它們只會轉送使用者對應程序的每個登入所需的事件：Windows Server 2012 和 MS Exchange 的四個事件。

- 下列網路元素是否支援必要頻寬：
  - 網域控制站—必須支援與轉送事件相關聯的負載處理。
  - 成員伺服器—必須支援與接收事件相關聯的負載處理。
  - 連線—網域控制站、成員伺服器和通用類別目錄伺服器的地理位置分布 (本機或遠端) 是要素之一。一般而言，遠端分布支援較少頻寬。

設定 Windows 日誌轉送

若要設定 Windows 日誌轉送，您必須要有在 Windows 伺服器上設定群組原則的管理權限。在所有 *Windows* 事件收集器（從網域控制站收集登入事件的成員伺服器）上設定 Windows 日誌轉送。以下是工作概覽；如需特定步驟，請參閱 Windows Server 文件。

STEP 1 | 在每個 Windows 事件收集器上，啟用事件收集、將網域控制站新增為事件來源，並設定事件收集查詢（訂閱）。您在訂閱中指定的事件會隨著網域控制站平台而不同：

- **Windows Server 2012**（包括 **R2**）以及 **2016** 或 **MS Exchange**—必要事件的事件 ID 為 4768（授予驗證票證）、4769（授予服務票證）、4770（更新已授予的票證）和 4624（登入成功）。

  若要盡快轉送事件，請在設定訂閱時選取 ***Minimize Latency***（最小化延遲）。

User-ID 代理程式在 Windows 事件收集器上監控安全性日誌（並非預設的事件轉送位置）。請在各個 Windows 事件收集器上執行以下步驟，以將事件記錄路徑變更為安全性日誌。

1. 開啟 Event Viewer（事件檢視器）。
2. 在 **Security**（安全性）日誌上按一下滑鼠右鍵，然後選取 **Properties**（屬性）。
3. 複製 **Log path**（日誌路徑）（預設為 **`%SystemRoot%\System32\Winevt\Logs\security.evtx`**），然後按一下 **OK**（確定）。
4. 在 **Forwarded Events**（轉送的事件）資料夾上按一下滑鼠右鍵，並選取 **Properties**（屬性）。
5. 貼上從 **Security**（安全性）日誌中複製的值，取代預設 **Log path**（日誌路徑）(**`%SystemRoot%\System32\Winevt\Logs\ForwardedEvents.evtx`**)，然後按一下 **OK**（確定）。

STEP 2 | 設定群組原則，以啟用網域控制器上的 Windows 遠端管理 (WinRM)。

STEP 3 | 設定群組原則，以啟用網域控制器上的 Windows 事件轉送。

©2024 Palo Alto Networks, Inc.

為許多對應資訊來源設定 User-ID

STEP 1 | 請在會收集登入事件的成員伺服器上設定 Windows 日誌轉送。

設定 Windows 日誌轉送。此步驟需要在 Windows 伺服器上設定群組原則的管理權限。

STEP 2 | 安裝 Windows 型 User-ID 代理程式。

在可存取成員伺服器的 Windows 伺服器上安裝基於 Windows 的 User-ID 代理程式。確定要用來主控 User-ID 代理程式的系統，是待監控伺服器所屬之相同網域的成員。

STEP 3 | 設定 User-ID 代理程式，以從成員伺服器收集使用者對應資訊。

1. 啟動 Windows 型 User-ID 代理程式。
2. 選取 **User Identification**（使用者識別） > **Discovery**（探索），然後為從網域控制器接收事件的每個成員伺服器執行下列步驟：
    1. 在伺服器區段中，按一下 **Add**（新增），然後輸入用來識別成員伺服器的 **Name**（名稱）。
    2. 在 **Server Address**（伺服器位址）欄位中，輸入成員伺服器的 FQDN 或 IP 位址。
    3. 針對 **Server Type**（伺服器類型），請選取 **Microsoft Active Directory**。
    4. 按一下 **OK**（確定）以儲存伺服器項目。
3. 設定其餘的 User-ID 代理程式設定（請參閱 為使用者對應設定基於 Windows 的 User-ID 代理程式）。
4. 如果 User-ID 來源提供多種格式的使用者名稱，請在將使用者對應至群組時指定 **Primary Username**（主要使用者名稱）的格式。

    主要使用者名稱是識別防火牆中使用者的使用者名稱，並在報告與日誌中表示使用者，無論 User-ID 來源提供何種格式。

STEP 4 | 設定 LDAP 伺服器設定檔，以指定防火牆如何連接到通用類別目錄伺服器 (最多四個) 取得群組對應資訊。

若要改善可用性，請以至少兩個通用類別目錄伺服器作為備援。

您只能收集萬用群組的群組對應資訊，無法收集本機網域群組（子網域）的。

1. 選取 **Device**（裝置） > **Server Profiles**（伺服器設定檔） > **LDAP**，按一下 **Add**（新增），再輸入設定檔的 **Name**（名稱）。
2. 在伺服器區段中，針對每個通用類別目錄，按一下 **Add**（新增），並輸入伺服器 **Name**（名稱）、IP 位址（**LDAP Server**（**LDAP** 伺服器）），以及 **Port**（**LDAP** 伺服器）。如需純文字或啟動傳輸層安全性 (Start TLS) 連線，請使用 **Port**（連接埠）3268。如需透過 SSL 的 LDAP 連線，請使用 **Port**（連接埠）3269。如果連線會使用 Start TLS 或

©2024 Palo Alto Networks, Inc.

透過 SSL 的 LDAP，請選取 **Require SSL/TLS secured connection**（需要 **SSL/TLS** 安全連線）核取方塊。

3. 在 **Base DN**（基準 **DN**）欄位中，輸入防火牆將在通用類別目錄伺服器中開始搜尋群組對應資訊之處的辨別名稱 (DN)，例如 `DC=acbdomain,DC=com`。
4. 針對 **Type**（類型），選取 **active-directory**。

STEP 5 | 設定 LDAP 伺服器設定檔，以指定防火牆如何連接到包含網域對應資訊的伺服器（多達四個）。

User-ID 會使用這項資訊將 DNS 網域名稱對應至 NetBIOS 網域名稱。此對應可確保原則規則中有一致的網域/使用者名稱參考。

若要改善可用性，請以至少兩個伺服器作為備援。

這些步驟與您在上一步 中為通用類別目錄建立的 LDAP 伺服器相似，差別在於下列欄位：

- **LDAP** 伺服器—輸入包含網域對應資訊之網域控制器的 IP 位址。
- 連接埠—如需純文字或 Start TLS 連線，請使用 **Port**（連接埠）389。如需透過 SSL 的 LDAP 連線，請使用 **Port**（連接埠） 636。如果連線會使用 Start TLS 或透過 SSL 的 LDAP，請選取 **Require SSL/TLS secured connection**（需要 **SSL/TLS** 安全連線）核取方塊。
- 基準 **DN**—選取防火牆將在網域控制器中開始搜尋網域對應資訊之處的 DN。其值必須以下列字串開頭：`cn=partitions`、`cn=configuration`（例如，`cn=partitions,cn=configuration,DC=acbdomain,DC=com`）。

STEP 6 | 為您所建立的每個 LDAP 伺服器設定檔建立群組對應設定。

1. 選取 **Device**（裝置） > **User Identification**（使用者識別） > **Group Mapping Settings**（群組對應設定）。
2. 按一下 **Add**（新增），然後輸入 **Name**（名稱），以識別群組對應設定。
3. 選取 LDAP **Server Profile**（伺服器設定檔），並確定 **Enabled**（已啟用）核取方塊已選取。

   如果通用類別目錄和網域對應伺服器所參考的群組超過您的安全性規則所需要的，請設定 ***Group Include List***（群組包含清單）和/或 ***Custom Group***（自訂群組）清單，以限制 *User-ID* 會執行對應的群組。
4. 按一下 **OK**（確定）與 **Commit**（提交）。

在 HTTP 標頭中插入使用者名稱

當您使用 Palo Alto Networks 設定次要執行設備以強制執行基於使用者的原則時，次要設備可能沒有來自防火牆的 IP 位址至使用者名稱對應。將使用者資訊傳輸到下游設備可能需要部署其他設備（例如 Proxy），或對使用者的體驗產生負面影響（例如，使用者須登入多次）。透過在 HTTP 標頭中共用使用者的身分，您可以強制執行基於使用者的原則，而不會負面影響使用者的體驗或部署其他基礎結構。

©2024 Palo Alto Networks, Inc.

設定此功能時，將 URL 設定檔套用於安全性原則，然後提交變更，防火牆：

1. 在來源使用者的群組對應中，使用主要使用者名稱的格式填入使用者和網域值。
2. 使用 Base64 對這些資訊進行編碼。
3. 將 Base64 編碼的標頭新增到有效負載中。
4. 將流量路由到下游設備。

如果僅在使用者存取特定網域時要包括使用者和網域，請設定網域清單，且僅當清單中的網域與 HTTP 要求的 Host 標頭匹配時，防火牆才能插入標頭。

為了與下游設備共用使用者資訊，您須首先啟用 User-ID 並設定群組對應。

若要在標頭中包含使用者名稱和網域，則防火牆需要使用者的 *IP* 位址至使用者名稱對應。如果使用者未對應，則防火牆會為標頭中的網域和使用者名稱在 *Base64* 編碼中插入 *unknown*。

若要在 HTTPS 流量的標頭中包含使用者名稱和網域，必須首先建立解密設定檔來解密 HTTPS 流量。

此功能支援正向 *Proxy* 解密流量。

STEP 1 | Create（建立）或編輯 **URL** 篩選設定檔。

如果該網域的 *URL* 篩選設定檔動作為 ***block***（封鎖），則防火牆不會插入標頭。

STEP 2 | 建立或編輯使用預先定義類型的 HTTP 標頭插入項目。

您可以針對每個設定檔，定義最多五個標頭。

STEP 3 | 選取 **Dynamic Fields**（動態欄位） 作為標題 **Type**（類型）。

STEP 4 | **Add**（新增）您要在其中插入標頭的 **Domains**（網域） 。當使用者存取清單中的網域時，防火牆會插入指定的標頭。

STEP 5 | **Add**（新增）新的 **Header**（標頭）或選取 **X-Authenticated-User** 以進行編輯。

©2024 Palo Alto Networks, Inc.

STEP 6 | 選取標頭 **Value**（值）格式（**`($domain)\($user)`** 或 **`WinNT://($domain)/($user)`**）或使用 **`($domain)`** 和 **`($user)`** 動態語彙基元輸入自己的格式（例如，UserPrincipalName 的**`($user)@($domain)`**）。

每個值請勿多次使用同一個動態語彙基元（***`($user)`*** 或 ***`($domain)`***）。

每個值最多可包含 512 個字元。防火牆使用群組對應設定檔中的主要使用者名稱填入 **`($user)`** 和 **`($domain)`** 動態語彙基元。例如：

- 如果主要使用者名稱是 sAMAccountName，則 **`($user)`** 的值是 sAMAccountName，而 **`($domain)`** 的值則是 NetBios 網域名稱。
- 如果主要使用者名稱是 UserPrincipalName，則 **`($user)`** 是使用者帳戶名稱（首碼），而 **`($domain)`** 則是網域名稱系統 (DNS)。

STEP 7 | （選用）選取 **Log**（日誌），以針對標頭插入啟用日誌記錄。

STEP 8 | 將 URL 篩選設定檔套用至 HTTP 或 HTTPS流量的安全性原則規則。

STEP 9 | 選取兩次 **OK**（確定）以確認 HTTP 標頭設定。

STEP 10 | **Commit**（提交）您的變更。

STEP 11 | 確認防火牆在 HTTP 標頭中包含使用者名稱和網域。

- 使用 **`show user user-ids all`** 命令以驗證群組對應是否正確。
- 使用 **`show counter global name ctd_header_insert`** 命令以檢視防火牆插入的 HTTP 標頭的數量。
- 如果您在步驟 7 中設定了日誌記錄，請檢查 logs（日誌）中是否插入了 Base64 編碼的有效負載（例如，**`c corpexample\testuser`** 將在日誌中顯示為 **`Y29ycGV4YW1wbGVcdGVzdHVzZXI=`**）。

重新散佈資料和驗證時間戳記

在大型網路中，您可以透過設定部分防火牆透過重新散佈來收集對應資訊，以簡化資源使用，而不必設定所有防火牆直接查詢對應資訊來源。

您可重新分配透過終端機伺服器 *(TS)* 代理程式以外的任何方法收集的使用者對應資訊。您無法重新分配群組對應或 HIP 比對資訊。

如果您使用 *Panorama* 來管理防火牆和彙總防火牆日誌，則您可以設定 *Panorama* 來管理 User-ID 重新散佈。使用 *Panorama* 比在防火牆之間建立額外的連線來重新散佈 *User-ID* 資訊更為簡單。

©2024 Palo Alto Networks, Inc.

如果您設定驗證原則，防火牆必須要重新散佈使用者驗證存取應用程式和服務時產生的驗證時間戳記。防火牆將使用時間戳記來評估驗證原則規則的逾時。在逾時期間內，已成功驗證的使用者可以在稍後要求服務和應用程式，無需再次驗證。重新散佈時間戳記能讓您對網路中的所有防火牆強制執行一致的逾時設定。

防火牆將共用同一重新散佈流程中的資料和驗證時間戳記；您不必為每個資訊類型單獨設定重新散佈。

- 用於資料重新散佈的防火牆部署
- 設定資料重新散佈

用於資料重新散佈的防火牆部署

在大型網路中，您可以透過設定部分防火牆透過重新散佈來收集資料，以簡化資源使用，而不必設定所有防火牆直接查詢資料來源。資料重新散佈還會提供細微性，允許您僅將指定的資訊類型重新散佈給選取的裝置。您還可以使用子網路和範圍篩選 IP 使用者對應或 IP 標籤對應，以確保防火牆僅收集執行原則所需的對應。

資料重新散佈可以是單向的（代理程式將資料提供給用戶端），也可以是雙向的，即代理程式和用戶端可以同時傳送和接收資料。

要重新散佈資料，可以使用以下架構類型：

- 用於單個區域的中樞和支點架構：

  要在防火牆之間重新散佈資料，最佳做法是使用中樞和支點架構。在此設定中，中樞防火牆從 Windows User-ID 代理程式、Syslog 伺服器、網域控制器或其他防火牆等來源收集資料。設定重新散佈用戶端防火牆以從中樞防火牆收集資料。

  例如，中樞（包含一對 VM-50 以獲取復原能力）可以連線到 User-ID 來源以獲取使用者對應。然後，當使用使用者對應強制執行原則的用戶端防火牆連線到中樞以接收資料時，中樞將能夠重新散佈使用者對應。

- 用於多個區域的多中樞和支點架構：

  如果您在多個區域部署了防火牆，且希望將資料散佈到所有這些區域的防火牆，以便無論使用者在哪裡登入，都可以一致地執行原則，則可以對多個區域使用多中樞和支點架構。

  先在每個區域設定一個防火牆以從來源收集資料。該防火牆充當進行重新散佈的本機中樞。該防火牆從該區域的所有來源收集資料，以便可以將其重新散佈到用戶端防火牆。接下來，設定用戶端防火牆以連線到其區域和所有其他區域的重新散佈中樞，以便用戶端防火牆具有來自所有中樞的所有資料。

  最佳做法是，如果防火牆需要同時傳送和接收資料，請在區域內啟用雙向重新散佈。例如，如果防火牆充當遠端使用者的 GlobalProtect 閘道，且充當本機使用者的分支防火牆，則防火牆必須將其為遠端使用者收集的使用者對應傳送到中樞防火牆，同時從中樞防火牆接收本機使用者的使用者對應。

©2024 Palo Alto Networks, Inc.

- 階層式架構：

  要重新散佈資料，您還可以使用階層式架構。例如，要重新散佈 User-ID 資訊之類的資料，可以分層組織重新散佈順序，其中每層具有一個或多個防火牆。在底層中，整合了 PAN-OS 的 User-ID 代理程式在防火牆上執行，基於 Windows 的 User-ID 代理程式將在對應 IP 位址到使用者名稱的 Windows 伺服器上執行。每個較高層都有防火牆從下方一層中最多 100 個 從新分配點接收對應資訊和驗證時間戳記。頂層防火牆將彙總來自於所有層的對應資訊和時間戳記。此部署提供了相關選項，為所有使用者（在頂層的防火牆中）設定原則，並為對應網域（有較低層防火牆提供伺服）中的使用者子集設定區域或功能特定的原則。

  在此場景中，三層防火牆將對應和時間戳記從本機辦公室重新散佈至區域辦公室，然後再傳送至全域資料中心。彙總所有資訊的資料中心防火牆，會將這些資訊與其他資料中心防火牆共用，以便它們都可強制執行原則，並為整個網路中的使用者產生報告。僅有底層防火牆使用 User-ID 代理程式來查詢目錄伺服器。

  User-ID 代理程式查詢的資訊來源，不會計入順序中十個躍點的上限。但是，向防火牆轉送對應資訊的 Windows User-ID 代理程式需計入在內。另外，在本範例中，最頂層具有兩個躍點：第一個躍點彙總一個資料中心防火牆中的資訊，第二個躍點則將這些資訊與其他資料中心防火牆共用。

設定資料重新散佈

設定資料重新散佈前：

- ☐ 規劃重新散佈架構。需考慮的一些因素包括：
  - 哪些防火牆將對所有資料類型強制執行原則？哪些防火牆將針對一個資料子集強制執行特定於區域或職能部門的原則？
  - 重新散佈順序需要多少個躍點來彙總所有資料？使用者對應的最大允許躍點數為十，IP 位址到使用者名稱對應和 IP 位址到標籤對應的最大允許躍點數為一。
  - 您如何將查詢使用者對應資訊來源的防火牆數目減到最少？查詢防火牆數目越少，防火牆和來源上的處理負載越少。
- ☐ 設定重新散佈代理程式從中取得資料以重新散佈到其用戶端的資料來源：
  - 來自 PAN-OS 整合 User-ID 代理程式或基於 Windows 的 User-ID 代理程式的使用者對應
  - 動態位址群組的 IP 位址至標籤對應
  - 動態使用者群組的使用者名稱至標籤對應
  - 基於 HIP 的政策執行的 GlobalProtect
  - 裝置隔離的資料 （僅限 Panorama）
- ☐ 設定驗證原則。

資料重新散佈包括：

- 提供資訊的重新散佈代理程式
- 接收資訊的重新散佈用戶端

©2024 Palo Alto Networks, Inc.

按資料重新散佈順序在防火牆上執行下列步驟。

STEP 1 | 在重新散佈用戶端防火牆上，設定防火牆、Panorama 或 Windows User-ID 代理程式作為資料重新散佈代理程式。

1. 選取 **Device**（裝置）> **Data Redistribution**（資料重新散佈）> **Agents**（代理程式）。
2. **Add**（新增）重新散佈代理程式，並輸入 **Name**（名稱）。
3. 確認該代理程式 **Enabled**（已啟用）。

STEP 2 | 使用其 **Serial Number**（序號）或其 **Host and Port**（主機和連接埠）新增代理程式。

- 要使用序號新增代理程式，請選取您想要用作重新散佈代理程式的防火牆的 **Serial Number**（序號）。
- 若要使用代理程式的主機和連接埠資訊新增代理程式：
  1. 輸入 **Host**（主機）的資訊。
  2. 選取主機是否是 **LDAP Proxy**。
  3. 輸入 **Port**（連接埠）（預設值為 5007，範圍為 1—65535）。
  4. （僅限多個虛擬系統）輸入 **Collector Name**（收集器名稱）以確定您想要使用哪個虛擬系統作為重新散佈代理程式。
  5. （僅限多個虛擬系統）輸入並確認您想要用作重新散佈代理程式的虛擬系統的 **Collector Pre-Shared Key**（收集器預先共用金鑰）。

STEP 3 | 選取一個或多個 **Data Type**（資料類型）以供代理程式進行重新散佈。

- **IP User Mappings**（**IP** 使用者對應）—User-ID 的 IP 位址到使用者名稱對應。
- **IP Tags**（**IP** 標籤）—動態位址群組的 IP 位址到標籤對應。
- **User Tags**（使用者標籤）—動態使用者群組的使用者名稱到標籤對應。
- **HIP**—來自 GlobalProtect 的主機資訊設定檔 (HIP) 資料，其中包含 HIP 物件和設定檔。
- **Quarantine List**（隔離清單）—GlobalProtect 識別為已隔離的裝置。

STEP 4 | （僅限多虛擬系統）設定一個虛擬系統作為可以重新散佈資料的收集器。

如果防火牆接收資料，但不重新散佈，則跳過此步驟。

您可以在不同防火牆或同一防火牆上的虛擬系統之間重新散佈資訊。在以上兩種情況下，每個虛擬系統都計為重新散佈順序中的一個躍點。

1. 選取 **Device**（裝置）> **Data Redistribution**（資料重新散佈）> **Collector Settings**（收集器設定）。
2. 編輯 **Data Redistribution Agent Setup**（資料重新散佈代理程式設定）。
3. 輸入 **Collector Name**（收集器名稱）和 **Pre-Shared Key**（預先共用金鑰），以將該防火牆或虛擬系統識別為 User-ID 代理程式。
4. 按一下 **OK**（確定）儲存您的變更。

©2024 Palo Alto Networks, Inc.

STEP 5 | （選用，但推薦）設定要在資料重新散佈中包括的網路以及要從資料重新散佈中排除的網路。

重新散佈 IP 位址到標籤對應或 IP 位址到使用者名稱對應時，可以包括或排除網路和子網路。

最佳做法是始終指定要包括和排除的網路，以確保代理程式僅與內部資源進行通訊。

1. 選取 **Device**（裝置） > **Data Redistribution**（資料重新散佈） > **Include/Exclude Networks**（包括/排除網路）。
2. **Add**（新增）一個項目並輸入 **Name**（名稱）。
3. 確認該項目 **Enabled**（已啟用）。
4. 選取想要 **Include**（包括）還是 **Exclude**（排除）項目。
5. 輸入項目的 **Network Address**（網路位址）。
6. 按一下 **OK**（確定）。

STEP 6 | 設定防火牆將用於向其他防火牆查詢 User-ID 資訊的服務路由。

如果防火牆僅從基於 Windows 的 User-ID 代理程式接收使用者對應資訊，或直接從資訊來源（例如目錄伺服器）而非其他防火牆接收，則跳過此步驟。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Services**（服務）。
2. （僅限包含多個虛擬系統的防火牆）選取 **Global**（全域）（適用於防火牆範圍內的服務路由）或 **Virtual Systems**（虛擬系統）（適用於虛擬系統特定的服務路由），然後設定服務路由。
3. 按一下 **Service Route Configuration**（服務路由組態），選取 **Customize**（自訂），然後根據您的網路通訊協定選取 **IPv4** 或 **IPv6**。若您的網路支援此兩者，則為兩種通訊協定設定服務路由。
4. 選取 **UID Agent**（**UID** 代理程式），然後選取 **Source Interface**（來源介面）和 **Source Address**（來源位址）。
5. 按兩下 **OK**（確定）以儲存服務路由。

STEP 7 | 允許防火牆在其他防火牆查詢要重新散佈的資料時回應。

如果防火牆接收資料，但不重新散佈，則跳過此步驟。

設定介面管理設定檔，啟用 **User-ID** 服務，並將設定檔指派給防火牆介面。

©2024 Palo Alto Networks, Inc.

STEP 8 | （選用，但推薦）使用企業 PKI 中的自訂憑證來建立從重新散佈用戶端到重新散佈代理程式的唯一信任鏈結。

1. 在重新散佈用戶端防火牆上，建立自訂 SSL 憑證設定檔以用於傳出連線。
2. 選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理） > **Secure Communication Settings**（安全通訊設定）。
3. **Edit**（編輯）設定。
4. 選取 **Customize Secure Server Communication**（自訂安全伺服器通訊）選項。
5. 選取在子步驟 1 中建立的 **Certificate Profile**（憑證設定檔）。
6. 按一下 **OK**（確定）。
7. 為 **Data Redistribution**（資料重新散佈）**Customize Communication**（自訂通訊）。
8. **Commit**（提交）您的變更。
9. 輸入以下 CLI 命令以確認憑證設定檔 (`SSL config`) 使用 `Custom certificates`：**`show redistribution agent state <agent-name>`**（其中 <*agent-name*> 是重新散佈代理程式或 User-ID 代理程式的名稱）。

STEP 9 | （選用，但推薦）使用企業 PKI 中的自訂憑證來建立從重新散佈代理程式到重新散佈用戶端的唯一信任鏈結。

1. 在重新散佈代理程式防火牆上，為防火牆建立一個自訂 SSL/TLS 服務設定檔以用於傳入連線。
2. 選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理） > **Secure Communication Settings**（安全通訊設定）。
3. **Edit**（編輯）設定。
4. 選取 **Customize Secure Server Communication**（自訂安全伺服器通訊）選項。
5. 選取您在步驟 1 中建立的 **SSL/TLS Service Profile**（**SSL/TLS** 服務設定檔）。
6. 按一下 **OK**（確定）。
7. **Commit**（提交）您的變更。
8. 輸入以下 CLI 命令以確認憑證設定檔 (`SSL config`) 使用自訂憑證：**`show redistribution service status`**。

©2024 Palo Alto Networks, Inc.

STEP 10 | 確認代理程式將資料正確重新散佈到用戶端。

1. 檢視代理程式統計資料（**Device**（裝置） > **Data Redistribution**（資料重新散佈） > **Agents**（代理程式）），然後選取 **Status**（狀態）以檢視重新散佈代理程式的活動摘要，如用戶端防火牆接收的對應數量。
2. 確認 **Connected**（已連線）狀態為 **yes**（是）。
3. 在代理程式上，存取 CLI 並輸入以下 CLI 命令以檢查重新散佈的狀態：**`show redistribution service status`**。
4. 在代理程式上，輸入以下 CLI 命令以檢視重新散佈用戶端：**`show redistribution service client all`**。
5. 在用戶端上，輸入以下 CLI 命令以檢查重新散佈的狀態：**`show redistribution service client all`**。
6. 確認 User-ID 日誌（ **Monitor**（監控） > **Logs**（日誌） > **User-ID**）中的 **Source Name**（來源名稱），以確認防火牆從重新散佈代理程式接收對應。
7. 在用戶端上，檢視 IP-Tag 日誌（**Monitor**（監控） > **Logs**（日誌） > **IP-Tag**）以確認用戶端防火牆接收資料。
8. 在用戶端上，輸入以下 CLI 命令並驗證防火牆接收對應的來源 `From`（來源）是 `REDIST`：**`show user ip-user-mapping all`**。

STEP 11 | （選用）要對資料重新散佈進行疑難排解，請啟用路徑追蹤選項。

啟用路徑追蹤選項後，接收資料的防火牆會將其 IP 位址附加到 `<route>` 欄位，這是資料周遊的所有防火牆 IP 位址的清單。此選項要求重新散佈路由中的所有 PAN-OS 裝置都使用 PAN-OS 版本 10.0。如果重新散佈路由中的 PAN-OS 裝置使用 PAN-OS 9.1.x 或更早版本，則路徑追蹤資訊會在該裝置上終止。

1. 在來源源自的重新散佈代理程式上，輸入以下 CLI 命令：**`debug user-id test cp-login traceroute yes ip-address <ip-address> user <username>`**（其中 ***`<ip-address>`*** 是您想要驗證的 IP 位址至使用者名稱對應的 IP 位址，***`<username>`*** 是您想要驗證的 IP 位址至使用者名稱對應的使用者名稱）。
2. 在您設定了路徑追蹤的防火牆的用戶端上，輸入以下 CLI 命令驗證防火牆重新散佈資料：**`show user ip-user-mapping all`**。

   防火牆會顯示建立對應的時間戳記 (`SeqNumber`) 以及使用者是否擁有 GlobalProtect（`GP` 使用者）。

```
admin > show user ip-user-mapping-mp ip 192.0.2.0 IP
 address:192.0.2.0 (vsys1) User: jimdoe From:REDIST
 Timeout:889s Created:11s ago Origin:198.51.100.0
 SeqNumber:15895329682-67831262 GP User:No Local HIP:No Route
 Node 0:198.51.100.0 (vsys1) Route Node 1:198.51.100.1 (vsys1)
```


©2024 Palo Alto Networks, Inc.

在虛擬系統之間共享 User-ID 對應

若要在有多個虛擬系統時簡化 User-ID™ 來源組態，您可在單一虛擬系統上設定 User-ID 來源以與防火牆上的所有其他虛擬系統共用 IP 位址至使用者名稱對應和使用者名稱至群組對應。

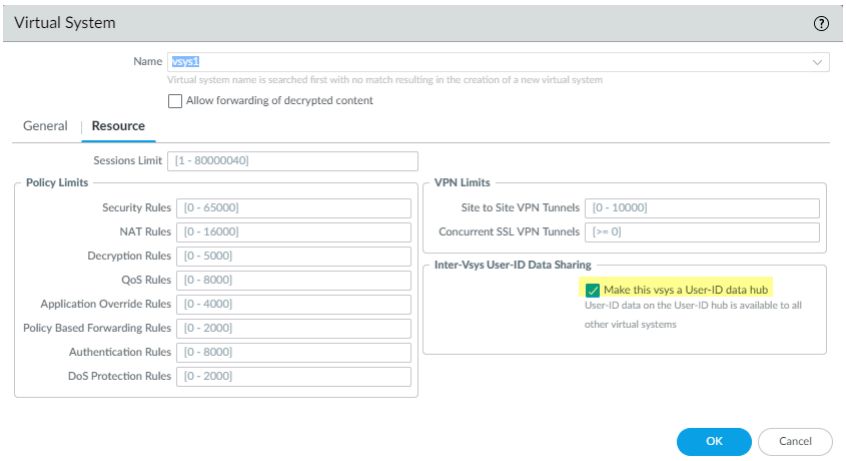
將單一虛擬系統設為 *User-ID* 中心點後，不再需要在多個虛擬系統上設定來源，從而簡化使用者對應，特別是在流量基於使用者嘗試存取的資源需要通過多個虛擬系統時（例如，在學術網路環境下，學生需要存取由不同虛擬系統管理的不同科系）。

為了對應使用者或群組，防火牆將使用本機虛擬系統上的對應表，並對該使用者或群組套用原則。如果防火牆在使用者流量的來源虛擬系統上找不到該使用者或群組的對應，則防火牆會查詢中心點，以擷取該使用者的 IP 位址至使用者名稱資訊或該群組的群組對應資訊。如果防火牆同時在 User-ID 中心點與本機虛擬系統上找到了對應，則防火牆會使用在本機取得的對應。如果本機防火牆上的對應與虛擬系統中心點上的對應不同，則防火牆會使用本機對應。

設定 User-ID 中心點後，當虛擬系統需要識別使用者以執行基於使用者的原則或要在日誌或報告中顯示使用者名稱時，虛擬系統可使用 User-ID 中心上的對應表格，但來源在本機不可用。當您選取中心點時，防火牆會保留其他虛擬系統上的對應，因此我們建議合併中心點的 User-ID 來源。但是，如果您不想共用特定來源的對應，可以設定要執行使用者或群組對應的個別虛擬系統。

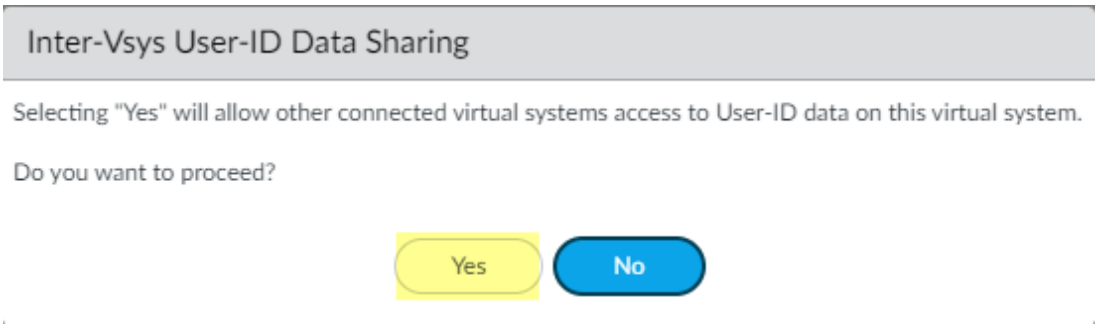
STEP 1 | 指定虛擬系統作為 User-ID 中心點。

1. 選取 **Device**（裝置） > **Virtual Systems**（虛擬系統），然後選取合併 User-ID 來源的虛擬系統。
2. 在 **Resource**（資源）頁籤上，**Make this vsys a User-ID data hub**（將此 **vsys** 設為 **User-ID** 資料中心），然後按一下 **Yes**（是）以確認。然後按一下 **OK**（確定）。

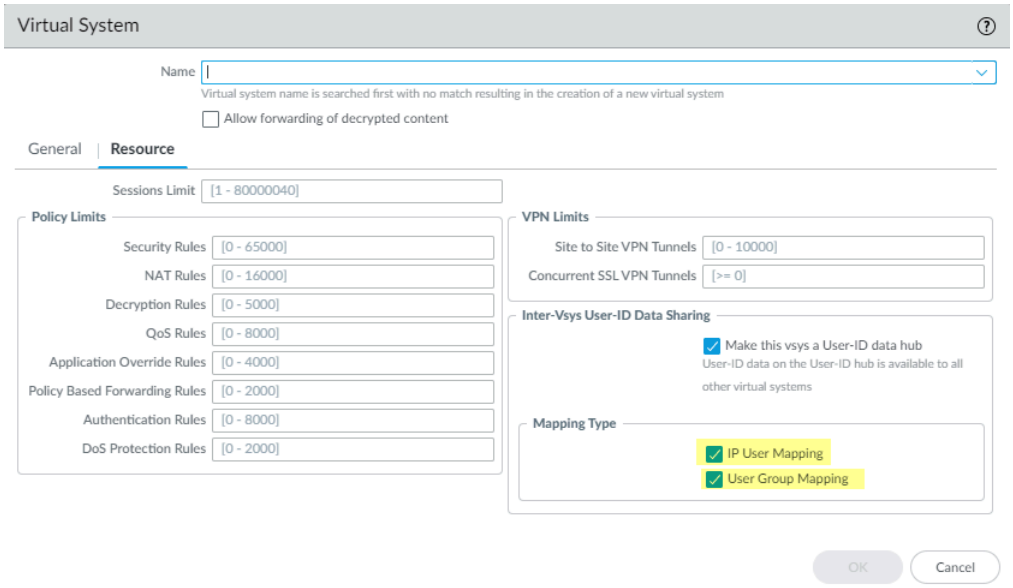


 ©2024 Palo Alto Networks, Inc.

STEP 2 | 按一下 **Yes**（是）以確認。



STEP 3 | 選取您要共用的 **Mapping Type**（對應類型），然後按一下 **OK**（確定）。



- **IP** 使用者對應—與其他虛擬系統共用 IP 位址至使用者名稱對應資訊。
- 使用者群組對應—與其他虛擬系統共用群組對應資訊。

您必須選取至少一個對應類型。

©2024 Palo Alto Networks, Inc.

STEP 4 | 合併 User-ID 來源並將其移轉要用作 User-ID 中心點的虛擬系統。

合併 User-ID 組態可以簡化操作。透過設定中心點以監控伺服器並連線至先前受其他虛擬系統監控代理程式，中心點可以統一收集使用者對應資訊，而無需每個虛擬系統單獨收集。如果您不想共用特定虛擬系統的對應，可在不會用作中心點的虛擬系統上設定這些對應。

跨虛擬系統和防火牆使用相同的主要使用者名稱格式。

1. 移除任何不必要或已過期的來源。
2. 識別用於基於 Windows 代理程式或整合式代理程式的所有設定，以及使用 XML API 傳送使用者對應的任何來源，並將其複製至要用作 User-ID 中心點之虛擬系統。

   在中心點，您可設定目前在虛擬系統上設定的任何 *User-ID* 來源。但是，終端機伺服器代理程式的 *IP* 位址與連接埠到使用者名稱對應資訊不會在 *User-ID* 中心點與連線的虛擬系統之間共用。
3. 指定 User-ID 代理程式應在對應中包括或排除的子網路。
4. 定義 **Ignore User List**（忽略使用者清單）。
5. 在所有其他虛擬系統上，移除 User-ID 中心點上的任何來源。

STEP 5 | **Commit**（提交）變更以啟用 User-ID 中心點並開始收集合併來源的對應。

STEP 6 | 確認 User-ID 中心點正在對應使用者和群組。

1. 使用 **`show user ip-user-mapping all`** 命令顯示 IP 位址至使用者名稱對應及提供對應的虛擬系統。
2. 使用 **`show user user-id-agent statistics`** 命令顯示用作 User-ID 中心點的虛擬系統。
3. 使用下列 CLI 命令確認中心點正在共用群組對應：
   - `show user group-mapping statistics`
   - `show user group-mapping state all`
   - `show user group list`
   - `show user group name` *<group-name>*

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

App-ID

為了讓您網路上的應用程式安全無虞，Palo Alto Networks 新一代的防牆針對應用程式與 Web 層面提供 App-ID 與 URL 篩選，全面防禦各種法律、規定、生產力與資源使用方面的風險。

App-ID 提供網路上應用程式的可見度，讓您能夠瞭解應用程式的運作狀態，並瞭解其行為特性及相關風險。能夠如此地瞭解應用程式，您便能建立與執行安全性原則規則，以啟用、檢查及形成所需的應用程式，並封鎖不想要的應用程式。當您定義原則規則以允許流量時，無須任何額外的設定，App-ID 便會開始分類流量。

新的以及已修改的 App-ID 作為應用程式與威脅內容更新的一部分予以發行—請遵循應用程式和威脅內容更新的最佳做法，無縫地將您的應用程式與威脅特徵碼保持最新狀態。

- App-ID 概要介紹
- 簡化的 App-ID 原則規則
- App-ID 和 HTTP/2 檢查
- 管理自訂或未知的應用程式
- 管理新的以及已修改的 App-ID
- 在原則中使用應用程式物件
- 在預設連接埠上安全啟用應用程式
- 含隱含支援的應用程式
- 安全性原則規則最佳化
- App-ID 雲端引擎
- SaaS App-ID 原則建議
- 應用程式層級閘道
- 停用 SIP 應用程式層級閘道 (ALG)
- 使用 HTTP 標頭管理 SaaS 應用程式存取
- 為舊版應用程式維持自訂逾時

App-ID 概要介紹

App-ID 是 Palo Alto Networks 防火牆獨家提供的流量分類系統，已取得專利，功能為判斷應用程式的身分，無論該應用程式使用何種連接埠、通訊協定、加密（SSH 或 SSL）或任何其他的規避行為。App-ID 將多種分類機制—應用程式特徵碼、應用程式通訊協定解碼及啟發學習法—套用至您的網路流量串流，以正確識別應用程式。

以下是 App-ID 如何識別在您網路中周遊的應用程式：

- 對照原則比對流量，以檢查網路上是否允許該流量。
- 將特徵碼套用到允許的流量上，以根據唯一的應用程式屬性與相關的交易特性來識別應用程式。特徵碼也會判斷該應用程式是否一直使用其預設的連接埠，或是使用非標準的連接埠。如果原則允許流量，便會掃描流量中是否有威脅，並進一步分析，以更精確地識別應用程式。
- 如果 App-ID 判斷出加密技術（SSL 或 SSH）正在使用中，並有適當的解密政策規則，則會將工作階段解密，並再次將應用程式特徵碼套用到解密的流量上。
- 接著使用已知通訊協定的解碼器來套用其他的內容式特徵碼，以偵測其他可能在通訊協定內部形成通道的應用程式（例如在 HTTP 間使用的 Yahoo!即時通訊)。解碼器會驗證流量是否遵循通訊協定規則，此外也支援如 SIP 與 FTP 等應用程式的 NAT 周遊與開啟動態針孔。
- 對於特別規避及無法透過進階特徵碼與通訊協定分析的應用程式，會使用啟發式或行為式分析來判斷應用程式的身分。

識別出應用程式時，原則檢查功能會決定如何處理應用程式，例如封鎖、允許與掃描威脅、檢查未經授權的檔案傳輸與資料模式，或使用 QoS 形成。

在設定應用程式覆寫政策規則之前，您應該瞭解 IPv4 位址集會被視為 IPv6 位址集的子集，原則中對此進行了詳細說明。

©2024 Palo Alto Networks, Inc.

簡化的 App-ID 原則規則

使用單個原則規則安全地啟用具有共同屬性的一組應用程式（例如，為您的使用者提供對 Web 應用程式的廣泛存取權限，或安全地啟用所有企業 VoIP 應用程式）。Palo Alto Networks 承擔研究具有共同屬性的應用程式的工作，並透過動態內容更新中的標籤進行傳遞。這會：

- 最大程度減少錯誤和節約時間。
- 幫助您建立原則，自動更新以處理新發布的應用程式。
- 使用原則最佳化工具簡化向基於 App-ID 的規則的轉換。

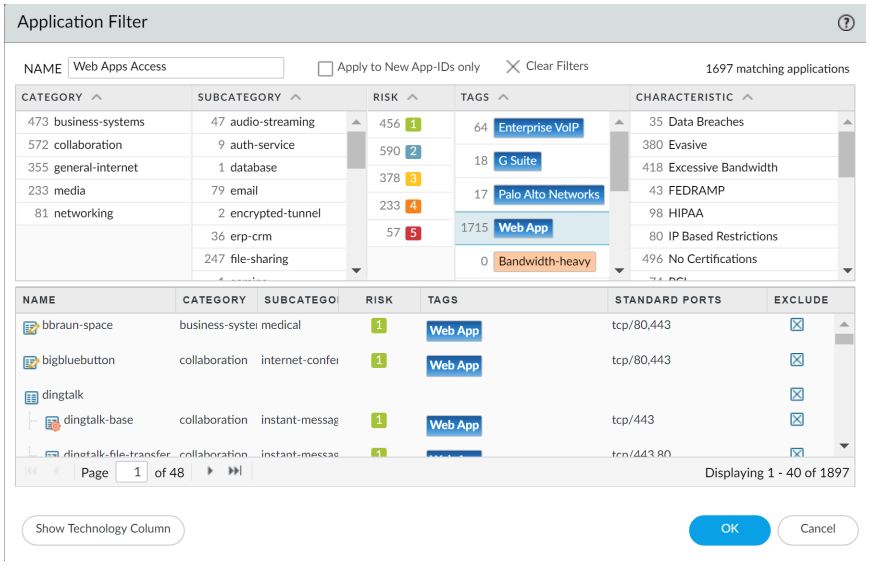
然後，防火牆可以使用基於標籤的應用程式篩選器動態執行新的和更新的 App-ID，而無需在新增新應用程式時檢閱或更新原則規則。如果您選擇從特定標籤中排除應用程式，則新的內容更新將遵循這些排除。您還可以使用自己的標籤基於原則要求定義應用程式類型。

- 使用標籤建立應用程式篩選器
- 建立基於自訂標籤的應用程式篩選器

使用標籤建立應用程式篩選器

STEP 1 | 使用一個或多個標籤建立應用程式篩選器。

如果您選擇多個標籤，應用程式須匹配包含在篩選器中的所有標籤。



STEP 2 | （選用）透過選取 **Exclude**（排除）欄中的核取方塊，從您的篩選器中排除標籤。

STEP 3 | 建立安全性原則規則，然後在 **Application**（應用程式）頁籤上 **Add**（新增）新的應用程式篩選器。

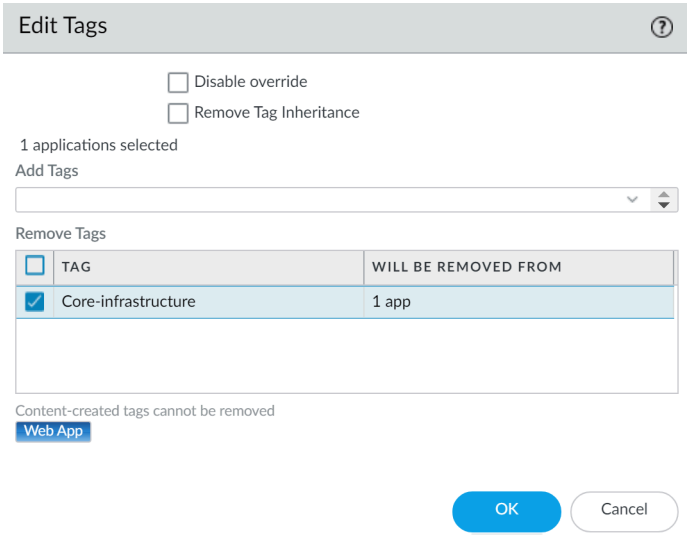
STEP 4 | **Commit**（提交）您的變更。

©2024 Palo Alto Networks, Inc.

建立基於自訂標籤的應用程式篩選器

STEP 1 | 建立一個自訂標籤並套用至 App-ID。

1. （選用）從應用程式中移除標籤。
2. 篩選或搜尋應用程式，然後選取特定應用程式以移除標籤。
3. **Edit Tags**（編輯標籤）並選取要移除的標籤。

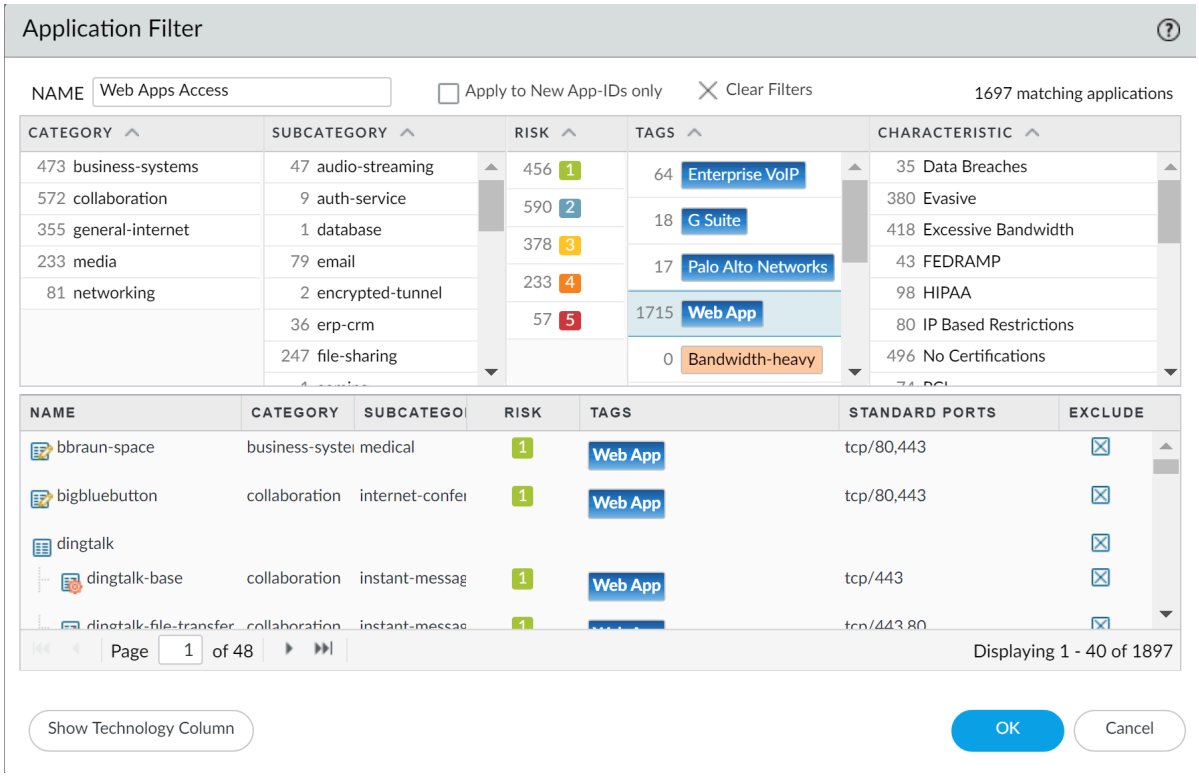


4. 按一下 **OK**（確定）。

©2024 Palo Alto Networks, Inc.

STEP 2 | 使用一個或多個標籤建立應用程式篩選器。

如果您選擇多個標籤，應用程式須匹配包含在篩選器中的所有標籤。



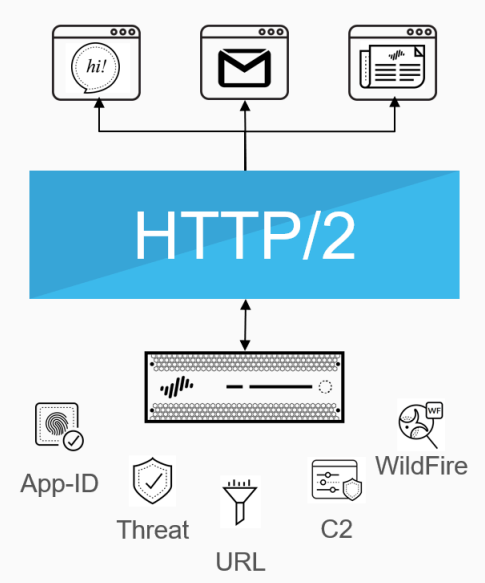
STEP 3 | 建立安全性原則規則，然後在 **Application**（應用程式）頁籤上 **Add**（新增）新的應用程式篩選器。

STEP 4 | **Commit**（提交）您的變更。

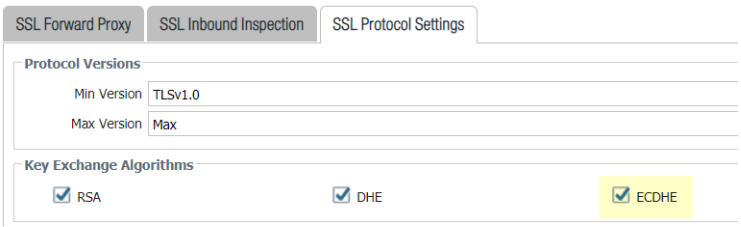
©2024 Palo Alto Networks, Inc.

App-ID 和 HTTP/2 檢查

您現在可以安全啟用透過 HTTP/2 執行的應用程式，無需在防火牆上進行任何其他組態。隨著越來越多的網站繼續採用 HTTP/2，防火牆可以對流量逐個執行安全性原則及所有威脅檢查和防禦功能。透過洞悉 HTTP/2 流量，您便可保護透過 HTTP/2 提供服務的 Web 伺服器，並透過提高 HTTP/2 服務的速度和資源效率，讓使用者獲益。



啟用 SSL 解密時，防火牆預設處理和檢查 HTTP/2 流量。若要 HTTP/2 檢查正常進行，必須啟用防火牆以將 ECDHE（橢圓曲線 Diffie-Hellman）用作 SSL 工作階段的金鑰交換演算法。ECDHE 預設為啟用，但您可透過選取 **Objects**（物件） > **Decryption**（解密） > **Decryption Profile**（解密設定檔） > **SSL Decryption**（**SSL** 解密） > **SSL Protocol Settings**（**SSL** 通訊協定設定），確認其是否已啟用。



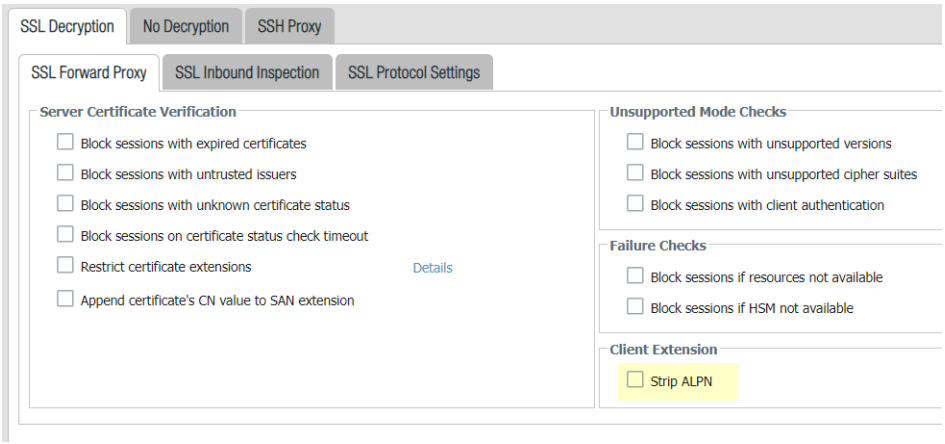
當啟用 *PAN-OS 11.0* 中引入的解密日誌時，您必須啟用通道內容檢查以獲取 *HTTP/2* 流量的 *App-ID*。

您可針對目標流量或在全域範圍內停用 HTTP/2 檢查：

©2024 Palo Alto Networks, Inc.

針對目標流量停用 HTTP/2 檢查。

您需要指定值，以便防火牆移除應用程式層通訊協定交涉 (ALPN) TLS 延伸中包含的任何值。ALPN 用於保護 HTTP/2 連線安全—當沒有為此 TLS 延伸指定任何值時，防火牆會將 HTTP/2 流量降級為 HTTP/1.1 或將其分類為未知 TCP 流量。



1. 選取 **Objects**（物件） > **Decryption**（解密） > **Decryption Profile**（解密設定檔） > **SSL Decryption**（**SSL** 解密） > **SSL Forward Proxy**（**SSL** 正向代理程式），然後選取 **Strip ALPN**（除去 **ALPN**）。
2. 附加解密設定檔至解密原則（**Policies**（原則） > **Decryption**（解密）），以對與該原則相符的流量關閉 HTTP/2 檢查。
3. **Commit**（提交）您的變更。

在全域範圍內停用 HTTP/2 檢查。

使用下列 CLI 命令：`set deviceconfig setting http2 enable no` 並 **Commit**（提交）變更。防火牆會將 HTTP/2 流量分類為未知 TCP 流量。

©2024 Palo Alto Networks, Inc.

管理自訂或未知的應用程式

Palo Alto Networks 每週提供應用程式更新，以識別新的 App-ID 特徵碼。依預設，一律啟用防火牆上的 App-ID，您不需要啟用一系列的特徵碼就能識別已知的應用程式。一般而言，在 ACC 與流量日誌中唯一會被歸類為未知流量—tcp、udp 或 non-syn-tcp—的應用程式是尚未新增至 App-ID 的市售應用程式、您網路上的內部或自訂應用程式，或是潛在威脅。

有時基於下列原因，防火牆會將應用程式彙報為身分未知：

- 資料不完整—發生交握，但在逾時之前沒有傳送任何資料封包。
- 資料不充足—發生交握之後有一或多個資料封包；但是，沒有交換足夠的資料封包來識別應用程式。

您可以選擇下列方式處理未知的應用程式：

- 建立安全性原則以透過未知 TCP、未知 UDP，或來源區域、目的地區域以及 IP 位址的組合，來控制未知應用程式。
- 向 Palo Alto Networks 要求 App-ID—如果您想要檢查與控制在您網路中周遊的應用程式是否有任何未知的流量，您可以記錄封包擷取。如果封包擷取顯示是市售的應用程式，您可以將此封包擷取提交至 Palo Alto Networks 進行 App-ID 開發。如果是內部應用程式，您可以建立自訂 App-ID 和/或定義應用程式取代原則。
- 使用特徵碼 建立自訂應用程式並將其附加到安全性政策，或建立自訂應用程式並定義自訂逾時。避免建立應用程式覆寫政策，因為它們會繞過第七層應用程式處理和威脅檢查，而是使用安全性較低的具狀態第四層檢查。請使用自訂逾時，以便您可以在第七層控制和檢查應用程式流量。

  自訂應用程式允許您自訂內部應用程式的定義（其特徵、類別和子類別、風險、連接埠和逾時），以及執行精細的政策控制並協助消除網路上未識別的流量。建立自訂應用程式也可讓您在 **ACC** 與流量日誌中正確識別應用程式，且有助於稽核/舉報您網路上的應用程式。要建立自訂應用程式，指定能唯一標識應用程式的特徵碼與模式，並附加到允許或拒絕應用程式的安全性政策規則。

  例如，如果您建立一個會在主機標頭 *www.mywebsite.com* 上觸發的自訂應用程式，則會先將封包識別為網頁瀏覽，再將封包比對成為您的自訂應用程式 (其父應用程式為網頁瀏覽)。由於父應用程式是網頁瀏覽，因此會在 Layer-7 檢查自訂應用程式，並掃描內容與弱點。

©2024 Palo Alto Networks, Inc.

管理新的以及已修改的 App-ID

新的以及已修改的 App-ID 作為應用程式與威脅內容更新的一部分傳送至防火牆。雖然新的以及已修改的 App-ID 可讓防火牆日益精準地執行安全性原則，但是因安裝內容更新版本而可能導致的安全性原則執行變更，會影響應用程式可用性。為此，您需考慮如何能夠以最佳方式部署內容更新，從而能夠在可用時獲取最新威脅防禦，並調整安全性原則以充分利用新的以及已修改的 App-ID。

下列選項可以讓您評估新 App-ID 對現有原則強制執行造成的影響、停用 (及啟用) App-ID，以及無縫更新原則規則以保護新識別之應用程式的安全並對其強制執行：

- 最佳併入新的以及已修改的 App-ID 的工作流程
- 查看內容發行版本中的新的以及已修改的 App-ID
- 查看新的以及已修改的 App-ID 會如何影響安全性原則
- 確保允許關鍵新 App-ID
- 監控新 App-ID
- 停用及啟用 App-ID

您還可以利用 簡化的 App-ID 原則規則，它使用內容更新中提供的應用程式標籤。

最佳併入新的以及已修改的 App-ID 的工作流程

請參照此主工作流程，先設定應用程式與威脅內容更新，然後以最佳方式將新的以及已修改的 App-ID 併入安全性原則。部署內容更新所需的一切內容皆在此提供。

STEP 1 | 依據商業需求部署應用程式與威脅內容更新。

瞭解應用程式與威脅內容更新的運作原理，並將組織識別為任務關鍵性或安全性優先組織。瞭解這兩項中的哪一個對您的業務最為重要，有助於您如何以最佳方式部署內容更新以及採用最佳做法，以滿足商業需求。您可能會想要混合採用兩種方式，可能視乎防火牆部署（資料中心或周邊）或者辦公室位置（遠端或總部）而定。

STEP 2 | 依據組織的網路安全性與應用程式可用性要求檢閱並採用應用程式和威脅內容更新的最佳做法。

STEP 3 | 設定安全性原則規則，以始終允許可能會對整個網路產生影響的新 App-ID，例如驗證或軟體開發應用程式。

新 App-ID 特性僅與最新內容發行版本中引入的 App-ID 相符。在安全性原則中使用時，您有一個月的時間來依據新 App-ID 調整安全性原則，同時確保關鍵類別 App-ID 的持續可用性（確保允許關鍵新 App-ID）。

STEP 4 | 將排程設定為部署應用程式與威脅內容更新；這包括可選擇延遲新 App-ID 的安裝，直到您有時間來對安全性原則作出必要更新（使用 **New App-ID Threshold**（新 **App-ID** 臨界值））。

©2024 Palo Alto Networks, Inc.

STEP 5 | 設定內容更新安裝排程後，您將需定期登記並查看內容發行版本中的新的以及已修改的 App-ID。

STEP 6 | 之後您可查看新的以及已修改的 App-ID 會如何影響安全性原則，並按需調整安全性原則。

STEP 7 | 監控新 App-ID，以瞭解網路中的新 App-ID 活動，以便作好充分準備，對安全性原則執行最行之有效的更新。

查看內容發行版本中的新的以及已修改的 App-ID

對於已下載和安裝的內容更新，您可查看更新所包含的新的以及已修改的 App-ID 清單。會提供完整的應用程式詳細資訊，重要的是，可對整個網路產生影響的應用程式的更新（例如 LDAP 或 IKE）會標上明顯的旗標，作為對原則檢閱的建議。對於已修改的 App-ID，應用程式詳細資訊還會說明覆蓋範圍目前得到擴充或變得更加精確的程度。

STEP 1 | 選取 **Device**（裝置） > **Dynamic Updates**（動態更新），然後選取 **Check Now**（立即檢查），以重新整理可用內容更新的清單。

STEP 2 | 對於已下載或目前已安裝的內容發行版本，按一下 **Actions**（動作）欄中的 **Review Apps**（檢閱應用程式）連結，檢視此發行版本中新識別與已修改應用程式的詳細資訊：

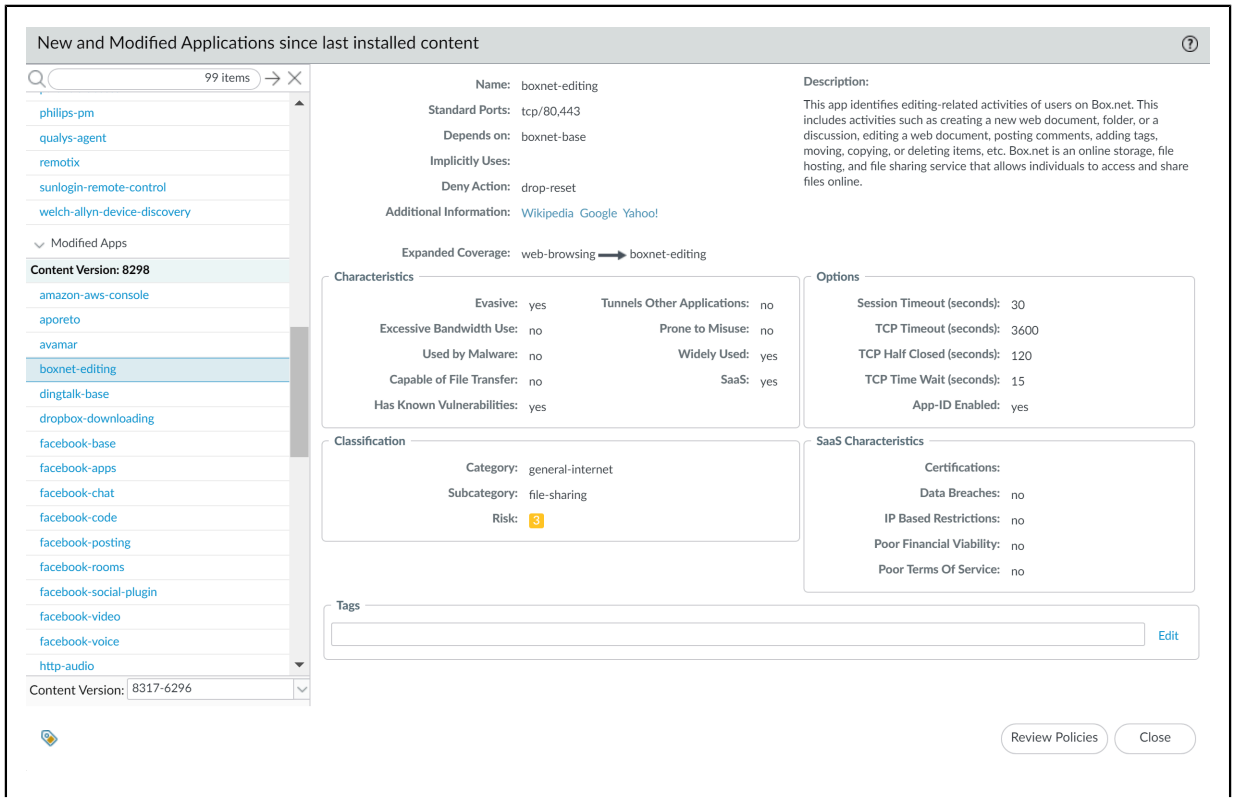
Applications and Threats **Last checked:** 2020/09/23 01:02:02 PDT **Schedule:** Every Wednesday at 01:02 (Download only)

8292-6181	panupv2-all-apps-8292-6181	Apps	Full	47 MB		2020/07/13 11:46:39 PDT	✓ previously		Revert	Release Notes
8317-6296	panupv2-all-apps-8317-6296	Apps	Full	48 MB		2020/09/08 17:55:10 PDT		✓	Review Policies Review Apps	Release Notes
8320-6309	panupv2-all-contents-8320-6309	Apps, Threats	Full	56 MB	192cfd8c2ff0058c188d0...	2020/09/14 18:13:54 PDT			Download	Release Notes
8320-6310	panupv2-all-contents-8320-6310	Apps, Threats	Full	57 MB	2436f79a8f02aeef37b82...	2020/09/15 10:19:15 PDT			Download	Release Notes
8321-6311	panupv2-all-contents-8321-6311	Apps, Threats	Full	56 MB	d3ac74a854c08527869cf...	2020/09/15 13:44:29 PDT			Download	Release Notes
8321-6312	panupv2-all-contents-8321-6312	Apps, Threats	Full	57 MB	a4275ee394b5d942c09e...	2020/09/15 14:26:20 PDT			Download	Release Notes

 ©2024 Palo Alto Networks, Inc.

STEP 3 | 檢閱此內容發行版本自上次內容版本開始所引入或修改的 App-ID。

單獨列出新的以及已修改的 App-ID。針對各個 App-ID 提供完整的應用程式詳細資訊，Palo Alto Networks 預見其會對整個網路產生影響的 App-ID 會標上旗標，作為對原則檢閱的建議。



您可使用以下新 App-ID 詳細資訊來評估可能對原則執行產生的影響：

- 取決於—列出此 App-ID 依賴的應用程式特徵碼，以唯一識別應用程式。如果停用 **Depends On**（取決於）欄位中所列的其中一個應用程式特徵碼，則也會停用所依賴的 App-ID。
- 先前識別為—列出在安裝新 App-ID 之前與應用程式相符的 App-ID，以唯一識別應用程式。
- **App-ID Enabled**（**App-ID** 已啟用）—所有 App-ID 都會在下載內容發行版本時顯示為已啟用，除非您選擇先手動停用 App-ID 特徵碼，然後再安裝內容更新。

對於已修改的 App-ID，詳細資訊涵蓋以下內容：**Expanded Coverage**（擴充的範圍）、**Remove False Positive**（移除誤報）以及應用程式中繼資料變更。Expanded Coverage（擴充的範圍）以及 Remove False Positive（移除誤報）欄位均表明應用程式覆蓋範圍的變化情況（更為全面或已縮小），時鐘圖示表明中繼資料變更，其中已更新特定的應用程式詳細資訊。

STEP 4 | 依據您的結果，按一下 **Review Policies**（檢閱原則）以查看新的以及已修改的 App-ID 會對安全性原則執行產生何種影響：查看新的以及已修改的 App-ID 會如何影響安全性原則。

©2024 Palo Alto Networks, Inc.

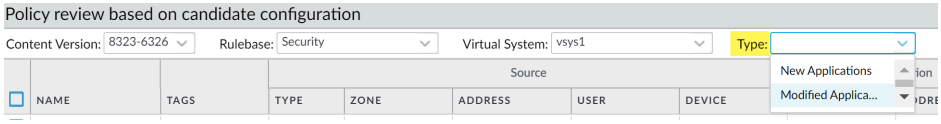
查看新的以及已修改的 App-ID 會如何影響安全性原則

新分類以及已修改的 App-ID 會變更防火牆執行流量的方式。執行內容更新原則檢閱，以查看新的以及已修改的 App-ID 會如何影響安全性原則，並輕鬆作出必要調整。可為已下載內容和已安裝內容執行內容更新原則檢閱。

STEP 1 | 請選取 **Device**（裝置） > **Dynamic Updates**（動態更新）。（裝置 > 動態更新）.

STEP 2 | 查看內容發行版本中的新的以及已修改的 App-ID，詳細瞭解內容發行版本所引入或修改的各個 App-ID。

STEP 3 | 對於已下載或目前已安裝的內容發行版本，按一下 Action（動作）欄中的 **Review Policies**（檢閱原則）。**Policy review based on candidate configuration**（根據候選組態檢閱原則）對話方塊可讓您根據 **Content Version**（內容版本）進行篩選，並檢視在特定發行中導入的新的或已修改的 App-ID（您也可以根據 **Rulebase**（規則庫）、**Virtual System**（虛擬系統）與 **Application**（應用程式）篩選新 App-ID 對原則的影響）。



STEP 4 | 從 **Application**（應用程式）下拉式清單中選取新 App-ID，以檢視目前執行應用程式的原則規則。顯示的規則取決於在安裝新 App-ID 之前與應用程式相符的 App-ID（檢視應用程式詳細資訊，以查看在新 App-ID 之前將應用程式 **Previously Identified As**（先前識別為）之應用程式特徵碼的清單）。

STEP 5 | 使用原則檢閱中提供的詳細資訊，來計劃安裝 App-ID 時要生效的原則規則更新，或者若目前已安裝包含 App-ID 的內容發行版本，所作變更會立即生效。

您可 **Add app to selected policies**（將應用程式新增至已選原則）或 **Remove app from selected policies**（從已選原則中移除應用程式）。

確保允許關鍵新 App-ID

新 App-ID 會導致針對新識別為屬於特定應用程式的流量之原則執行出現變更。為減輕對安全性原則執行的影響，可使用安全性原則規則中的 **New App-ID**（新 **App-ID**）特性，從而使規則始終執行最新導入的 App-ID，而不會要求您在安裝新 App-ID 時變更設定。新 App-ID 特性始終僅與最近安裝的內容發行版本中的新 App-ID 相符。安裝新的內容發行版本時，新 App-ID 特性會自動開始僅與此內容發行版本中的新 App-ID 相符。

您可選擇執行所有新的 App-ID，或者將安全性原則規則的目標設為執行特定類型的可能會對整個網路產生影響或產生決定性影響的新 App-ID（例如，僅執行驗證或軟體開發應用程式）。將安全性原則規則設為 **Allow**（允許），以確保即使 App-ID 發行促使關鍵應用程式的覆蓋範圍更為廣泛或精確，防火牆仍可繼續允許其通過。

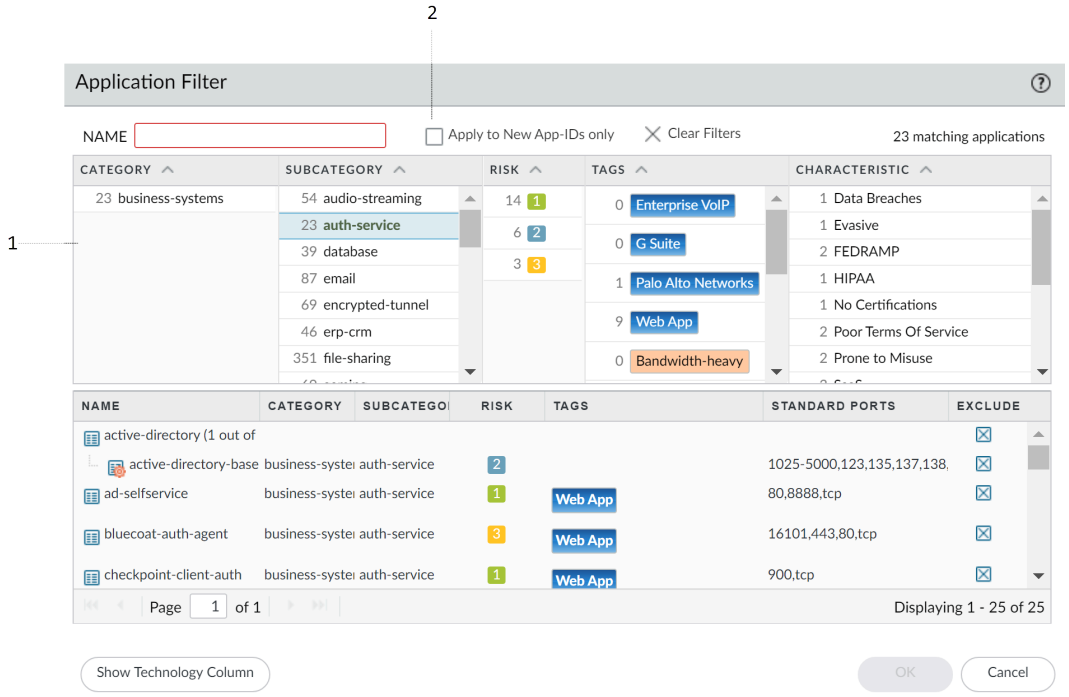
©2024 Palo Alto Networks, Inc.

新 App-ID 每月發行一次，因此允許最新 App-ID 的原則規則會為您預留一個月的時間（或者如果防火牆未依據排程安裝內容更新，則直到下一次手動安裝內容），來評估新分類的應用程式會對安全性原則執行產生何種影響並作出必要調整。

STEP 1 | 選取 **Objects**（物件） > **Application Filters**（應用程式篩選器），並 **Add**（新增） 新的應用程式篩選器。

STEP 2 | 依據子類別或特性定義您要確保持續可用性的新應用程式的類型。例如，選取類別「驗證服務」，以確保允許所有已知會執行或支援驗證的新安裝的應用程式。

STEP 3 | 僅在限制要在安裝後立即予以允許的新應用程式類型後，選取 **Apply to New App-IDs only**（僅套用至新 **App-ID**）。



STEP 4 | 選取 **Policies**（原則） > **Security**（安全性），並新增或編輯設定為允許相符流量的安全性原則規則。

STEP 5 | 選取 **Application**（應用程式），並將新 **Application Filter**（應用程式篩選器）作為比對準則新增至原則規則。

STEP 6 | 按一下 **OK**（確定）和 **Commit**（提交），以儲存變更。

STEP 7 | 為繼續調整安全性原則以應對新 App-ID 所引進的執行變更：

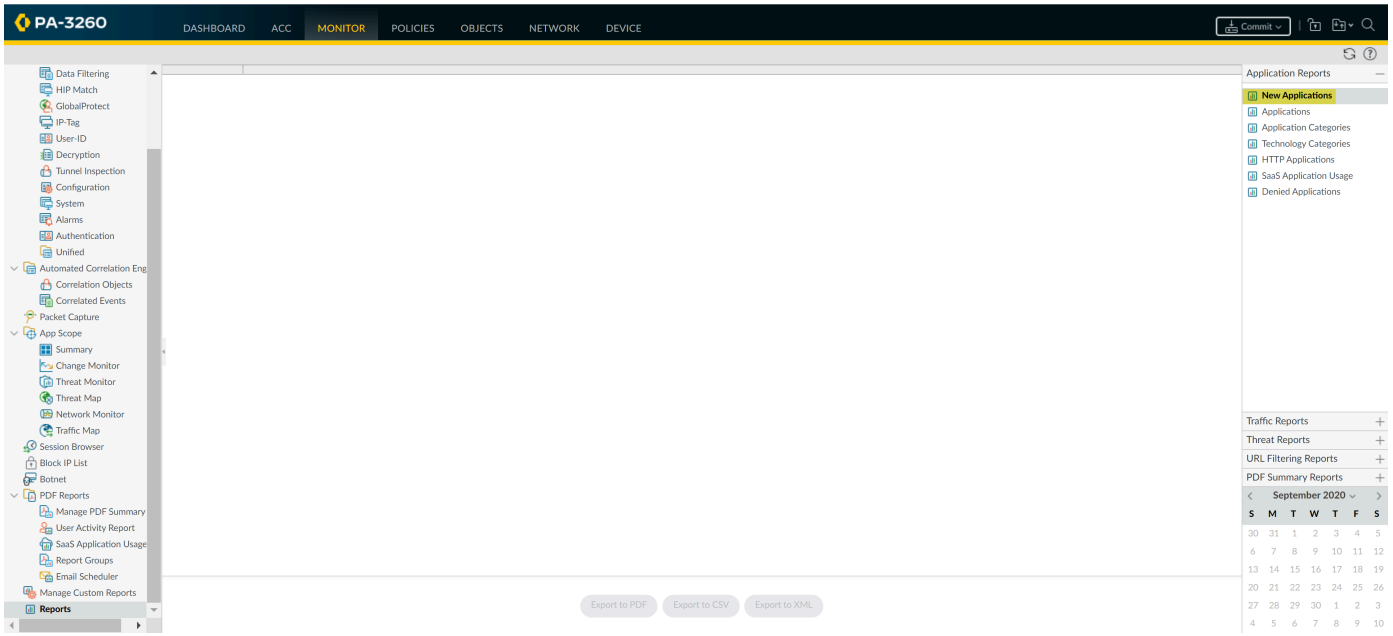
- 監控新 App-ID—監控新 App-ID 活動並獲取報告。
- 查看內容發行版本中的新的以及已修改的 App-ID—查看新安裝的 App-ID 對現有安全性原則規則產生何種影響。

©2024 Palo Alto Networks, Inc.

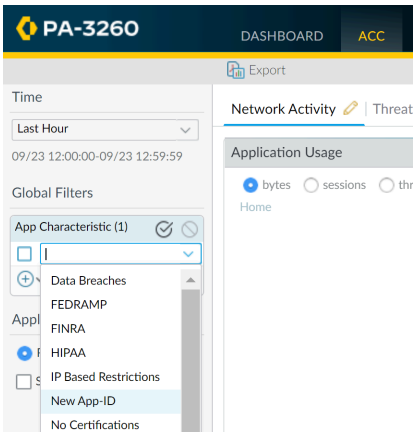
監控新 App-ID

透過 **New App-ID**（新 **App-ID**）特性，您可監控網路中的新應用程式，以便能夠更加充分地評估可能需對安全性原則執行的更新。在 ACC 中使用新 App-ID 特性，來獲取網路中新應用程式的可見度，並產生對新分類應用程式活動進行詳細說明的報告。獲取到的資訊，可幫助您作出正確決策，恰當更新安全性原則，以執行最新分類的 App-ID。無論是在 ACC 上使用還是用於產生報告（或者用於確保允許關鍵新 App-ID），新 App-ID 特性始終僅與最近安裝的內容發行版本中的新 App-ID 相符。安裝新的內容發行版本時，新 App-ID 特性會自動開始僅與此內容發行版本中的新 App-ID 相符。

產生報告，其中包含特定針對新應用程式（僅在最新內容發行版本中引入的應用程式）的詳細資訊。



使用 ACC 監控新應用程式活動：選取 **ACC**，在 **Global Filters**（全域篩選器）下方，選取 **Application**（應用程式） > **Application Characteristics**（應用程式特性） > **New App-ID**（新 **App-ID**）。



©2024 Palo Alto Networks, Inc.

停用及啟用 App-ID

若您想立即受益於最新的威脅防禦，可停用內容發行版本所導入的所有 App-ID，並計劃之後啟用 App-ID，而且您可針對特定應用程式停用 App-ID。

參考 App-ID 的原則規則只會比對並強制執行以所啟用 App-ID 為基礎的流量。

某些 App-ID 無法停用，且僅允許已啟用的狀態。無法停用的 App-ID 包括由其他 App-ID（例如 unknown-tcp）隱含使用的應用程式特徵碼。停用基礎 App-ID 會導致取決於此基礎 App-ID 的 App-ID 同時停用。例如，停用 facebook-base 將停用其他所有 Facebook App-ID。

停用內容發行中的或已排程內容更新的所有 App-ID。

雖然此選項可透過允許您之後啟用 App-ID 來保護您免受威脅攻擊，但是 Palo Alto Networks 建議您設定安全性原則規則以暫時允許新 App-ID 而非定期停用 App-ID。此規則將始終僅允許最新內容發行版本中所導入的新 App-ID。由於包含新 App-ID 的內容更新每月僅發行一次，因此您有時間來評估新 App-ID 並按需調整安全性原則來涵蓋新 App-ID，從而始終可確保關鍵應用程式的可用性不會受到影響。

- 若要停用在內容發行版本中導入的所有新 App-ID，可選取 **Device**（裝置） > **Dynamic Updates**（動態更新），然後 **Install**（安裝） 應用程式與威脅內容發行版本。在出現提示時，選取 **Disable new apps in content update**（在內容更新時停用新應用程式）。選取核取方塊以停用應用程式並繼續安裝內容更新。
- 在 **Device**（裝置） > **Dynamic Updates**（動態更新）頁面上，選取 **Schedule**（排程）。針對內容版本的下載與安裝，選擇 **Disable new apps in content update**（在內容更新時停用新應用程式）。

一次停用一個應用程式或多個應用程式的 App-ID。

- 若要快速停用單一應用程式或同時停用多個應用程式，可按一下 **Objects**（物件） > **Applications**（應用程式）。選取一或多個應用程式核取方塊並按一下 **Disable**（停用）。
- 若要檢閱單一應用程式的詳細資訊，然後停用該應用程式的 App-ID，可選取 **Objects**（物件） > **Applications**（應用程式），然後 **Disable App-ID**（停用 **App-ID**）。您可以使用此步驟來停用擱置中的 App-ID（在此情況下，包含 App-ID 的內容發行已下載到防火牆，但尚未安裝）或已安裝的 App-ID。

啟用 App-ID。

選取 **Objects**（物件） > **Applications**（應用程式），啟用您之前停用的 App-ID。選取一或多個應用程式核取方塊並按一下 **Enable**（啟用），或開啟特定應用程式的詳細資訊並按一下 **Enable App-ID**（啟用 **App-ID**）。

©2024 Palo Alto Networks, Inc.

在原則中使用應用程式物件

使用應用程式物件定義安全原則處理應用程式的方式。

- 建立應用程式群組
- 建立應用程式篩選器
- 建立自訂應用程式
- 解析應用程式相依項

建立應用程式群組

應用程式群組是一種物件，包含您想在原則中以類似方式處理的應用程式。應用程式群組可用來啟用對您明確批准可在組織內使用之應用程式的存取。將認可應用程式分組，可以簡化規則庫的管理。當您支援的應用程式中發生變更時，可以僅更新受影響的應用程式群組，而不必更新各個原則規則。

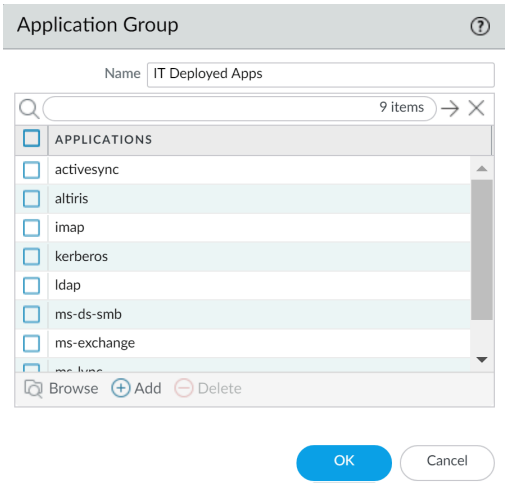
在決定如何分組應用程式時，請考慮您打算如何強制執行對已獲批准之應用程式的存取，並建立符合每個原則目標的應用程式群組。例如，您可能擁有僅允許 IT 管理員存取的一些應用程式，以及想使其可供組織中任何已知使用者使用的其他應用程式。在此情況下，您會為每個原則目標建立單獨的應用程式群組。雖然您通常只想啟用對預設連接埠上應用程式的存取，但可能會想分組對此而言是例外的應用程式，並以單獨的規則強制執行對這些應用程式的存取。

STEP 1 | 選取 **Objects**（物件） > **Application Groups**（應用程式群組）。

STEP 2 | **Add**（新增）群組，並為它設定具描述性的 **Name**（名稱）。

STEP 3 | （選用）選取**Shared**（共用）在共用的位置中建立物件，藉此在 Panorama 中作為共用物件存取，或在多虛擬系統防火牆中的所有虛擬系統之間使用。

STEP 4 | **Add**（新增）您想置於群組中的應用程式，然後按一下 **OK**（確定）。



©2024 Palo Alto Networks, Inc.

STEP 5 | **Commit**（提交）組態。

建立應用程式篩選器

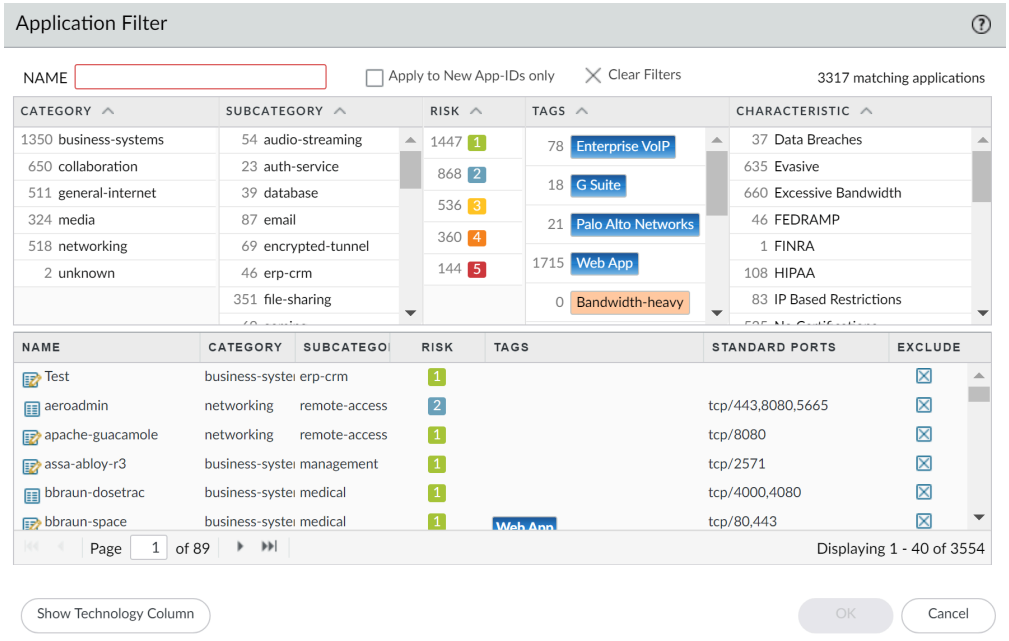
應用程式篩選器是一種物件，可根據您定義的應用程式屬性動態分組應用程式，其中包括類別、子類別、技術、風險係數與特性。當您想安全啟用對並未明確批准，但想讓使用者能夠存取之應用程式的存取時，這很有用。例如，您可能想讓員工選擇他自己的辦公程式（例如 Evernote、Google Docs 或 Microsoft Office 365）來執行業務。若要安全啟用這些類型的應用程式，您可以建立比對類別 **business-systems** 與子類別 **office-programs** 的應用程式篩選器。當新應用程式辦公程式出現，且建立新的 App-ID 時，這些新應用程式將自動符合您定義的篩選器；您不必對原則規則庫進行其他任何變更，便可安全啟用符合您針對篩選器定義之屬性的任何應用程式。

STEP 1 | 選取 **Objects**（物件） > **Application Filters**（應用程式篩選器）。

STEP 2 | **Add**（新增）篩選器，並為它設定具描述性的 **Name**（名稱）。

STEP 3 | （選用）選取**Shared**（共用）在共用的位置中建立物件，藉此在 Panorama 中作為共用物件存取，或在多虛擬系統防火牆中的所有虛擬系統之間使用。

STEP 4 | 從 Category（類別）、Subcategory（子類別）、Technology（技術）、Risk（風險）、Characteristic（特性）和 Tags（標籤）區段選取屬性值，來定義篩選器。（標籤可以簡化安全性政策規則的建立和維護）。當您選取值時，請注意，對話方塊底部的相符應用程式清單的範圍會縮小。當您調整篩選器屬性以符合您要安全啟用的應用程式類型時，請按一下 **OK**（確定）。



STEP 5 | **Commit**（提交）組態。

©2024 Palo Alto Networks, Inc.

建立自訂應用程式

若要安全啟用應用程式，您必須針對所有流量、所有連接埠、所有時段進行分類。使用 App-ID 時，通常在 ACC 與流量日誌中唯一會被歸類為未知流量—tcp、udp 或 non-syn-tcp—的應用程式是尚未新增至 App-ID 的市售應用程式、您網路上的內部或自訂應用程式，或是潛在威脅。

如果您看到還沒有 *App-ID* 的商業應用程式的未知流量，您可以在此提交新 *App-ID* 的要求：http://researchcenter.paloaltonetworks.com/submit-an-application/。

若要確保您的內部自訂應用程式未顯示為未知流量，請建立自訂應用程式。然後，您可以透過這些應用程式運用精確原則控制，來縮小您網路上無法識別之流量的範圍，並因此縮小攻擊面。建立自訂應用程式也可讓您在 ACC 與流量日誌中正確識別應用程式，其可讓您稽核/舉報您網路上的應用程式。

若要建立自訂應用程式，您必須定義應用程式屬性：其特性、類別及子類別、風險、連接埠、逾時等。此外，您必須定義防火牆可用來比對流量本身的特徵碼或值（特徵碼）。最後，您可以將自訂應用程式附加至允許或拒絕應用程式的安全性原則 (或將其新增至應用程式群組，或將其與應用程式篩選器比對)。您也可以建立自訂應用程式，來識別時下關注的暫時應用程式，例如世界盃足球賽或「三月的瘋狂」的 ESPN3-Video。

為了能收集正確的資料來建立自訂應用程式特徵碼，您必須清楚瞭解封包擷取及如何形成資料包。如果特徵碼的建立過於廣泛，您可能會不小心涵蓋其他類似的流量；如果特徵碼的定義過於狹隘，則未嚴格符合模式的流量便能規避偵測。

自訂應用程式會存放在防火牆上另外的資料庫中，此資料庫不受到每週 *App-ID* 更新的影響。

從內容版本 *609* 開始，能夠讓防火牆偵測在通訊協定內部可能形成通道的應用程式的支援應用程式通訊協定解碼器將包含：*FTP*、*HTTP*、*IMAP*、*POP3*、*SMB* 以及 *SMTP*。

以下是如何建立自訂應用程式的基本範例。

STEP 1 | 收集您將用來編寫自訂特徵碼之應用程式的相關資訊。

若要執行此操作，您必須瞭解應用程式，並瞭解如何控制其存取權。例如，您可能想要限制使用者可在應用程式中執行的操作（例如上傳、下載或即時串流）。或者，您可能想要允許應用程式，但強制執行 QoS 原則。

- 擷取應用程式封包，使您可以尋找以其為基礎建立自訂應用程式特徵碼之應用程式的唯一特性。執行此操作的一種方式是，在用戶端系統上執行通訊協定分析器（例如 Wireshark），

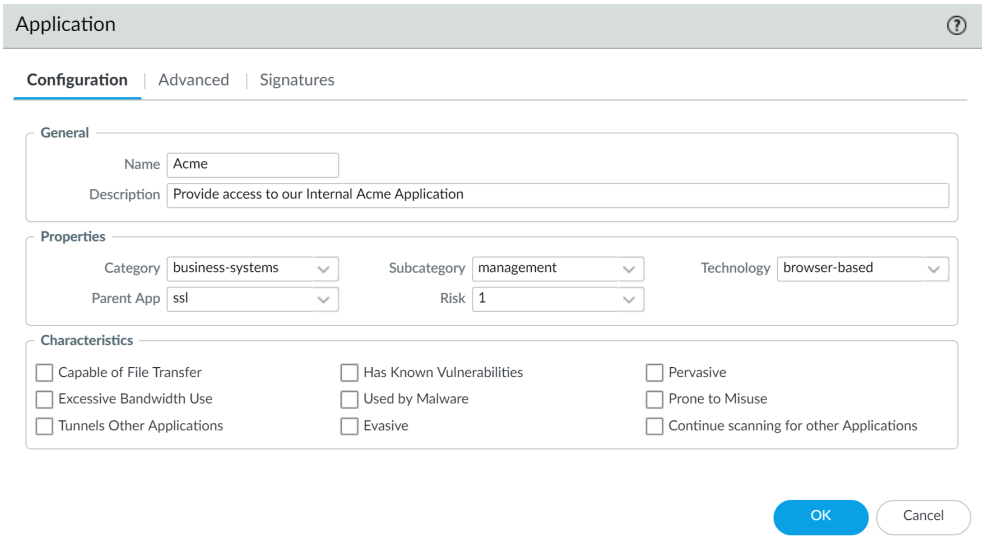
©2024 Palo Alto Networks, Inc.

來擷取用戶端與伺服器之間的封包。在應用程式中執行不同的動作（例如上傳與下載），以使您能夠在產生的封包擷取（PCAP）中找到每種類型的工作階段。

- 由於防火牆預設會獲得所有未知流量的封包擷取，因此，如果防火牆處於用戶端與伺服器之間，您可以直接從流量日誌檢視未知流量的封包擷取。
- 使用封包擷取以在封包內容（您可用來建立將唯一符合應用程式流量的特徵碼）中尋找特徵碼或值。例如，在 HTTP 回應或要求標頭、URI 路徑或主機名稱中尋找字串特徵碼。如需您可以用來建立應用程式特徵碼之不同字串內容，與您可以尋找封包中對應值之位置的相關資訊，請參閱建立自訂威脅特徵碼。

STEP 2 | 新增自訂應用程式。

1. 選取 **Objects**（物件） > **Applications**（應用程式），然後按一下 **Add**（新增）。
2. 在 **Configuration**（組態）頁籤上，為將協助其他管理員瞭解您建立應用程式之原因的自訂應用程式，輸入 **Name**（名稱）與 **Description**（說明）。
3. （選用）選取**Shared**（共用）在共用的位置中建立物件，藉此在 Panorama 中作為共用物件存取，或在多虛擬系統防火牆中的所有虛擬系統之間使用。
4. 定義應用程式屬性與特性。



STEP 3 | 定義有關應用程式的詳細資訊，例如基礎通訊協定、應用程式執行所在的連接埠號碼、逾時值，以及您要對流量執行的任何掃描類型。

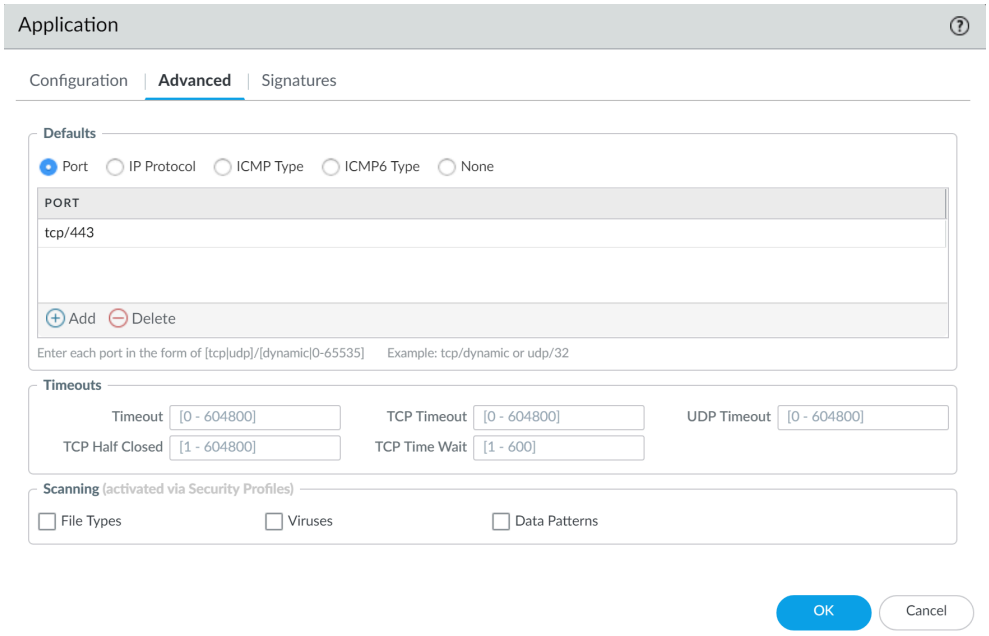
在 **Advanced**（進階）頁籤上，定義將允許防火牆識別應用程式通訊協定的設定：

- 指定應用程式使用的預設連接埠或通訊協定。
- 指定工作階段逾時值。如果您未指定逾時值，將使用預設逾時值。
- 指出您打算對應用程式流量執行的任何類型的其他掃描。

例如，若要建立透過 SSL 執行的自訂 TCP 式應用程式，但使用連接埠 4443（而非 SSL 的預設連接埠 443），您需要指定連接埠號碼。透過為自訂應用程式新增連接埠號碼，您可以建立使

©2024 Palo Alto Networks, Inc.

用應用程式預設連接埠，而非在防火牆上開啟其他連接埠的原則規則。如此可改善您的安全狀態。



STEP 4 | 定義防火牆將用來比對流量與新應用程式的條件。

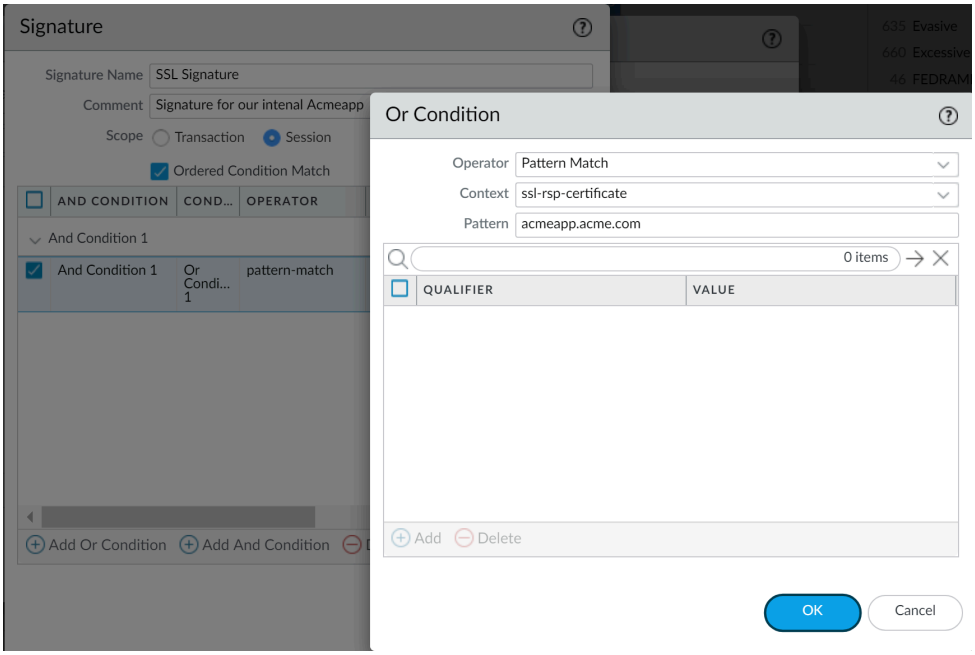
您將使用從封包擷取收集的資訊來指定防火牆可用來比對應用程式流量中特徵碼的唯一字串內容值。

1. 在 **Signatures**（特徵碼）頁籤中，按一下 **Add**（新增），定義 **Signature Name**（特徵碼名稱），並選擇性地定義 **Comment**（註解），來提供您要如何使用此特徵碼的相關資訊。
2. 指定特徵碼的 **Scope**（範圍）：其比對完整 **Session**（工作階段）還是單一 **Transaction**（交易）。
3. 按一下 **Add And Condition**（新增 **And** 條件）或 **Add Or Condition**（新增 **Or** 條件），指定定義特徵碼的條件。
4. 選取 **Operator**（運算子），定義您將使用之比對條件的類型：**Pattern Match**（模式相符）或 **Equal To**（等於）。
   - 如果您選取 **Pattern Match**（模式相符），請選取 **Context**（內容），然後使用規則運算式定義 **Pattern**（模式），來比對所選內容。或者，按一下 **Add**（新增），定義限定詞/值配對。**Qualifier**（限定詞）清單是您選擇的 **Context**（內容）專有的清單。
   - 如果您選取 **Equal To**（等於），請選取 **Context**（內容），然後使用規則運算式定義封包標頭中位元組的 **Position**（位置），來比對所選內容。選擇 **first-4bytes**（第一個 **4**

©2024 Palo Alto Networks, Inc.

位元組）或 **second-4bytes**（第二個 **4** 位元組）。為 **Mask**（遮罩）（例如 0xffffff00）與 **Value**（值）（例如 0xaabbccdd）定義 4 位元組十六進位值。

例如，如果您為其中一個內部應用程式建立自訂應用程式，您可以使用 **ssl-rsp-certificate Context**（**ssl-rsp-certificate** 內容），為伺服器中 SSL 交涉的憑證回應訊息定義特徵碼比對，並建立 **Pattern**（模式）來比對訊息中伺服器的 commonName，如下所示：



5. 針對每個相符條件重複步驟 4.c 和 4.d。
6. 如果防火牆嘗試比對特徵碼定義的順序很重要，請確保已選取 **Ordered Condition Match**（排序的條件比對）核取方塊，然後指定順序條件，使其以適當順序進行評估。選取條件或群組，並按一下 **Move Up**（上移）或 **Move Down**（下移）。您無法將條件從一個群組移至另一個群組。
7. 按一下 **OK**（確定）儲存特徵碼定義。

STEP 5 | 儲存應用程式。

1. 按一下 **OK**（確定）儲存自訂應用程式定義。
2. 按一下 **Commit**（交付）。

STEP 6 | 確認流量如預期一樣符合自訂應用程式。

1. 選取 **Policies**（原則）> **Security**（安全性），然後 **Add**（新增） 安全性原則規則，以允許新應用程式。
2. 從防火牆與應用程式之間的用戶端系統執行應用程式，然後檢查流量日誌（**Monitor**（監控）> **Traffic**（流量），確保您能夠看到與新應用程式相符的流量（且根據您的原則規則進行處理）。

©2024 Palo Alto Networks, Inc.

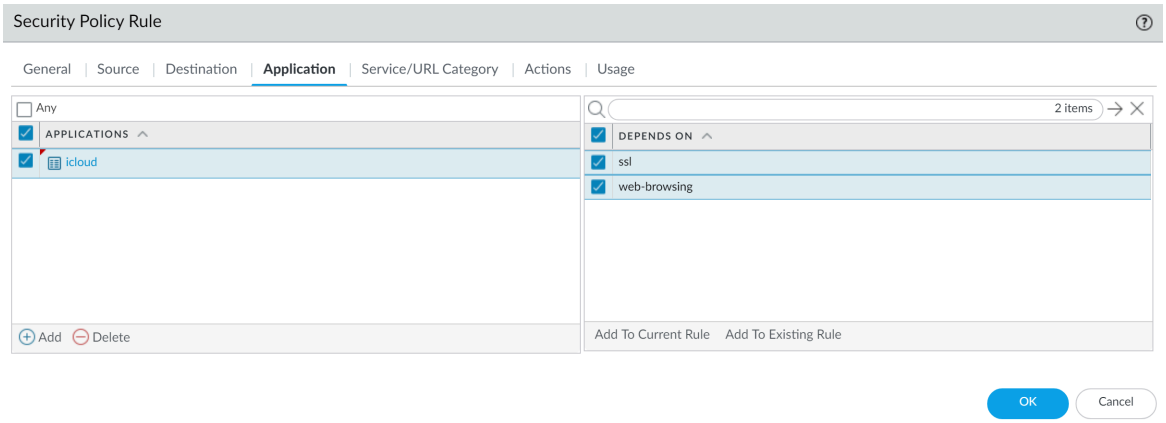
解析應用程式相依項

當建立新的安全原則規則並執行提交時，您可以看到應用程式相依項。當原則未包括所有應用程式相依項時，您可以直接存取關聯的安全原則規則以新增所需的應用程式。

STEP 1 | 建立安全性原則規則。

STEP 2 | 指定規則將允許或封鎖的應用程式。

1. 在 **Applications**（應用程式）頁籤上，**Add**（新增）您要安全啟用的 **Application**（應用程式）。您可以選取多個應用程式，或者可使用應用程式群組或應用程式篩選器。
2. 檢視所選應用程式相依項，然後 **Add To Current Rule**（新增到當前規則）或 **Add To Existing Rule**（新增到現有規則）。

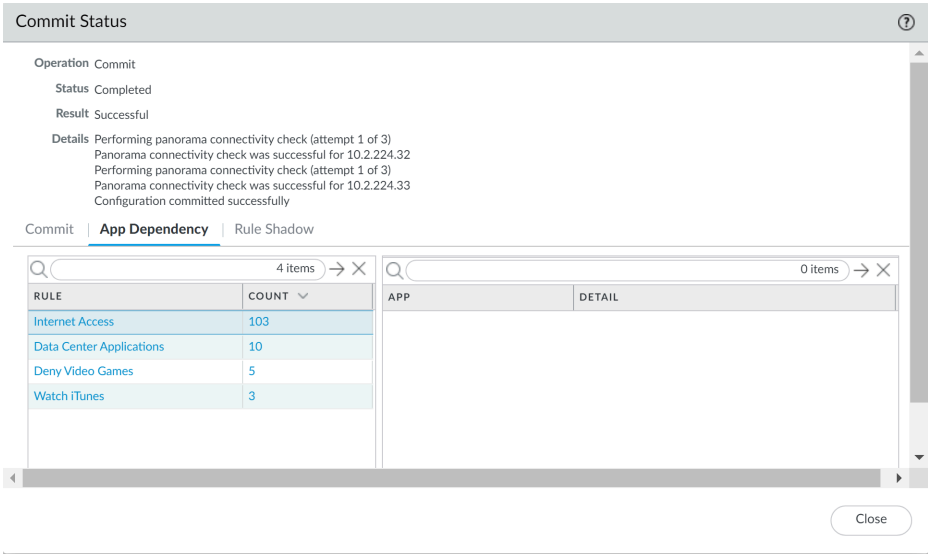


3. 如果新增到現有規則，請選取規則，然後按一下 **OK**（確定）。

©2024 Palo Alto Networks, Inc.

STEP 3 | 按一下 **OK**（確定）並 **Commit**（交付）變更。

1. 檢閱 **App Dependency**（應用程式相依性） 頁籤中的任何提交警告。



2. 選取 **Count**（數目） 以檢視不包括的應用程式相依項。
3. 選取 **Rule**（規則）名稱以開啟原則並新增相依項。

   解決任何相依的應用程式，否則其將繼續在提交時產生警告。

4. 按一下 **OK**（確定）並 **Commit**（交付）變更。

 ©2024 Palo Alto Networks, Inc.

在預設連接埠上安全啟用應用程式

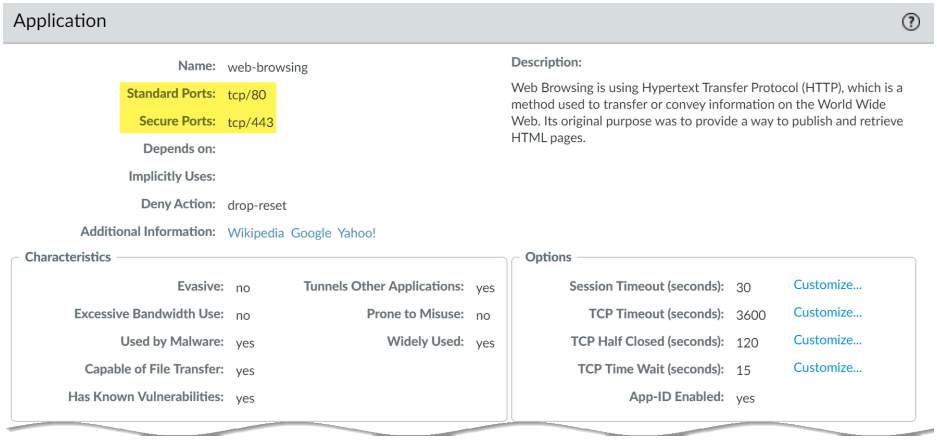
在異常連接埠上執行的應用程式可以指示，攻擊者試圖繞過傳統的基於連接埠的保護功能。應用程式預設是 Palo Alto Networks 防火牆的一個功能，讓您能夠輕鬆防止此類規避並在最常用的連接埠上啟用應用程式。應用程式預設是基於應用程式的安全性原則之最佳做法—能夠減少管理負荷，並消除基於連接埠的原則帶來的安全漏洞：

- **Less overhead**（減少負荷）—根據您的業務需求寫入簡單的基於應用程式的安全性原則規則，無需搜尋和維護應用程式至連接埠對應。我們為所有具有 App-ID 的應用程式定義了預設連接埠。
- **Stronger security**（強大的安全性）—讓應用程式僅在其預設連接埠上執行是一種安全性最佳做法。當應用程式異常執行時，應用程式預設可以幫助您確保重要應用程式可用，不影響安全性。

  此外，應用程式使用的預設連接埠有時取決於應用程式是加密的，還是明文的。基於連接埠的原則要求開啟應用程式可能用於加密的所有預設連接埠。開啟連接埠會帶來安全性漏洞，而攻擊者可以利用這些漏洞繞過安全性原則。但是，應用程式預設能夠區分加密和明文應用程式流量。這表示無論其是否加密，都可以執行應用程式的預設連接埠。

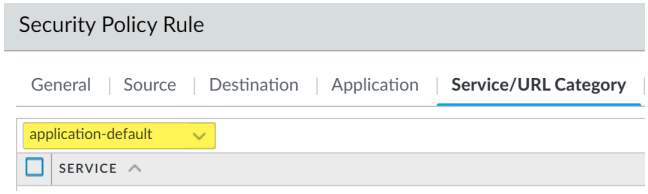
  例如，如果不開啟應用程式預設，您需要開啟連接埠 80 和 443 以啟用網頁瀏覽流量—您將在兩個連接埠上同時允許明文和加密網頁瀏覽流量。開啟應用程式預設後，防火牆將嚴格地僅在連接埠 80 上執行明文網頁瀏覽流量，並僅在連接埠 443 上執行 SSL 通道流量。

若要查看應用程式預設使用的連接埠，您可造訪 Applipedia 或選取 **Objects**（物件） > **Applications**（應用程式）。應用程式詳細資訊包括應用程式的標準連接埠—採用明文時最常使用的連接埠。對於網頁瀏覽、SMTP、FTP、LDAP、POP3 及 IMAP，詳細資訊還包括應用程式的安全連接埠—加密時應用程式使用的連接埠。



選取 **Policy**（原則） > **Security**（安全性） 並新增或修改規則以僅在其預設連接埠上執行應用程式：

©2024 Palo Alto Networks, Inc.



將應用程式預設用作基於應用程式的安全性原則的一部分並採用 *SSL* 解密是一種最佳做法。此外，如果您的現有安全性原則規則可以控制網頁瀏覽流量且 ***Service***（服務）設為 *service-http* 和 *service-https*，應更新這些規則才能使用應用程式預設。

©2024 Palo Alto Networks, Inc.

含隱含支援的應用程式

當建立原則以允許特定的應用程式時，您也必須確定允許任何該應用程式所依賴的其他應用程式。在許多情況下，您不必為讓流量流動而明確允許存取其所依賴的應用程式，因為防火能夠確定依賴項並隱含地允許依賴項。此隱含支援也會套用到以 HTTP、SSL、MS-RPC 或 RTSP 為基礎的自訂應用程式。如果防火牆無法及時判斷出其所依賴的應用程式，您就必須在定義原則時明確允許該類應用程式。您可以在基於應用程式的安全性原則工作流程中使用以下某種方法來確定依賴項：

- 原則最佳化工具
- 使用標籤建立應用程式篩選器
- 建立基於自訂標籤的應用程式篩選器
- 解析應用程式相依項

還可視需要使用 Applipedia（應用程式百科）。

下表列出防火牆隱含支援的應用程式（截至內容更新 595）。

應用程式	隱含支援
360-safeguard-update	http
apple-update	http
apt-get	http
as2	http
avg-update	http
avira-antivir-update	http, ssl
blokus	rtmp
bugzilla	http
clubcooee	http
corba	http
cubby	http, ssl
dropbox	ssl
esignal	http

©2024 Palo Alto Networks, Inc.

應用程式	隱含支援
evernote	http, ssl
ezhelp	http
facebook	http, ssl
facebook-chat	jabber
facebook-social-plugin	http
fastviewer	http, ssl
forticlient-update	http
good-for-enterprise	http, ssl
google-cloud-print	http, ssl, jabber
google-desktop	http
google-talk	jabber
google-update	http
gotomypc-desktop-sharing	citrix-jedi
gotomypc-file-transfer	citrix-jedi
gotomypc-printing	citrix-jedi
hipchat	http
iheartradio	ssl, http, rtmp
infront	http
instagram	http, ssl
issuu	http, ssl
java-update	http
jepptech-updates	http
kerberos	rpc

©2024 Palo Alto Networks, Inc.

應用程式	隱含支援
kik	http, ssl
lastpass	http, ssl
logmein	http, ssl
mcafee-update	http
megaupload	http
metatrader	http
mocha-rdp	t_120
mount	rpc
ms-frs	msrpc
ms-rdp	t_120
ms-scheduler	msrpc
ms-service-controller	msrpc
nfs	rpc
oovoo	http, ssl
paloalto-updates	ssl
panos-global-protect	http
panos-web-interface	http
pastebin	http
pastebin-posting	http
pinterest	http, ssl
portmapper	rpc
prezi	http, ssl
rdp2tcp	t_120

©2024 Palo Alto Networks, Inc.

應用程式	隱含支援
renren-im	jabber
roboform	http, ssl
salesforce	http
stumbleupon	http
supremo	http
symantec-av-update	http
trendmicro	http
trillian	http, ssl
twitter	http
whatsapp	http, ssl
xm-radio	rtsp

©2024 Palo Alto Networks, Inc.

安全性原則規則最佳化

原則最佳化工具提供了一個簡單的工作流程，可將傳統安全性原則規則庫移轉至基於 App-ID 的規則庫，透過減少攻擊面和監控應用程式以便安全啟用，來提高安全性。原則最佳化工具可以識別基於連接埠的規則，方便您將其轉換為基於應用程式的允許規則，或將基於連接埠的規則中的應用程式新增至現有的基於應用程式的規則，而不影響應用程式可用性。其還可識別過度佈建之基於 App-ID 的規則（設有未使用應用程式的 App-ID 規則）。原則最佳化工具可以幫助您確定優先移轉哪些基於連接埠的規則、識別允許未使用應用程式之基於應用程式的規則，及分析規則使用特性，如命中數。

將基於連接埠的規則轉換為基於應用程式的規則，可提高網路安全性，因為您選取了要允許的應用程式並拒絕了所有其他應用程式，因此可以從網路中消除不必要的流量和潛在的惡意流量。結合將應用程式流量限制在其預設連接埠（將服務設為 **application-default**（應用程式預設）），轉換為基於應用程式的規則還可防止規避應用程式在非標準連接埠上執行。

您可將此功能用於：

- 執行 PAN-OS 版本 9.0 且已啟用 App-ID 的防火牆。
- 執行 PAN-OS 版本 9.0 的 Panorama。您無需升級 Panorama 管理的防火牆也可使用 **Policy Optimizer**（原則最佳化工具）功能。但是，若要使用 **Rule Usage**（規則使用方式）功能（監控原則規則使用方式），受管理防火牆必須執行 PAN-OS 8.1 或更新版本。如果受管理防火牆連線至日誌收集器，則這些日誌收集器也必須執行 PAN-OS 版本 9.0。具有日誌處理卡 (LPC) 的受管理 PA-7000 系列防火牆也可以執行 PAN-OS 8.1（或更高版本）。
- 為獲取 Cortex Data Lake 相容性，Panorama 應執行 PAN-OS 10.0.3 或更新版本，並安裝雲端服務外掛程式 2.0 Innovation 或更新版本。

> 政策最佳化工具僅適用於 *Panorama* 管理的防火牆的 *Cloud Services* 外掛程式插件和 *Cortex Data Lake*，不支援與 *Panorama* 管理的 *Prisma Access* 一起使用。

PA-7000 系列防火牆支援兩種日誌記錄卡：*PA-7000* 系列防火牆日誌處理卡 *(LPC)* 和高效能的 *PA-7000* 系列防火牆日誌轉送卡 *(LFC)*。與 *LPC* 不同，*LFC* 沒有用於在本機儲存日誌的磁碟。*LFC* 會將所有日誌轉送至一個或多個外部日誌記錄系統中，例如 *Panorama* 或 *syslog* 伺服器。如果使用 *LFC*，原則最佳化工具的應用程式使用資訊不會顯示在防火牆上，因為流量日誌沒有在本機儲存。如果使用 *LPC*，因為流量日誌儲存在本機防火牆上，所以原則最佳化工具的應用程式使用資訊會顯示在防火牆上。

使用此功能以：

- 將基於連接埠的規則移轉至基於應用程式的規則—使用原則最佳化工具識別基於連接埠的規則並列出與各規則相符的應用程式，無需瀏覽流量日誌及手動將應用程式與基於連接埠的規則對應，以便您可以選取要允許的應用程式並將其安全啟用。將傳統的基於連接埠的規則轉換為基於應用程式的允許規則支援您的業務應用程式，並讓您能夠封鎖與惡意活動相關的任何應用程式。

©2024 Palo Alto Networks, Inc.

- 識別過度佈建之基於應用程式的規則—這些規則過於寬泛，允許網路上未使用的應用程式，會增加攻擊面以及無意間允許惡意流量的風險。

  從安全性政策規則中移除未使用的應用程式，以減少攻擊面，並保持規則庫乾淨。不要允許沒有人在網路上使用的應用程式。

- 將 **App-ID** 雲端引擎 **(ACE)** 應用程式新增到安全性原則規則—如果您擁有 SaaS 安全性內嵌訂閱，則可以使用原則最佳化工具的新應用程式檢視器管理安全性原則中的雲端傳遞 App-ID。ACE 文件介紹了如何使用原則最佳化工具來瞭解並控制雲端傳遞 App-ID 。

  本區段中的原則最佳化工具範例未顯示新應用程式檢視器，因為其描述的是沒有 *SaaS* 安全性內嵌訂閱的防火牆。

若要將組態從傳統防火牆移轉至 *Palo Alto Networks* 裝置，請參閱移轉至基於應用程式的原則之最佳做法。

您不能在 **Security**（安全性） > **Policies**（原則）中對安全性原則規則排序，因為排序可能會變更規則庫中規則的順序。但是，在 **Polices**（政策） > **Security**（安全性） > **Policy Optimizer**（政策最佳化工具）下，政策最佳化工具提供的排序選項不會影響規則順序，以便您可以對規則排序，以確定轉換或清除規則的優先順序。您可以按過去 30 天內的流量、規則上看見的應用程式數量、沒有新應用程式的天數及允許的應用程式數量（針對過度佈建的規則），對規則進行排序。

您還能以其他方式使用原則最佳化工具，包括驗證預先生產規則並對現有規則進行疑難排解。請注意，原則最佳化工具僅接受 **Log at Session End**（工作階段結束時記錄），而忽略 **Log at Session Start**（工作階段啟動時記錄），以避免計算防火牆上的瞬時應用程式。

由於資源限制，*VM-50 Lite* 虛擬防火牆不支援原則最佳化工具。

- 原則最佳化工具概念
- 從基於連接埠的安全性原則規則移轉至基於 App-ID 的安全性原則規則
- 規則複製移轉使用案例：Web 瀏覽和 SSL 流量
- 新增應用程式至現有規則
- 透過未使用的應用程式識別安全性原則規則
- 應用程式使用統計資料的高可用性
- 如何停用原則最佳化工具

原則最佳化工具概念

檢閱以下主題以詳細瞭解此功能的支援情況：

- 排序和篩選安全性原則規則
- 清除應用程式使用資料

©2024 Palo Alto Networks, Inc.

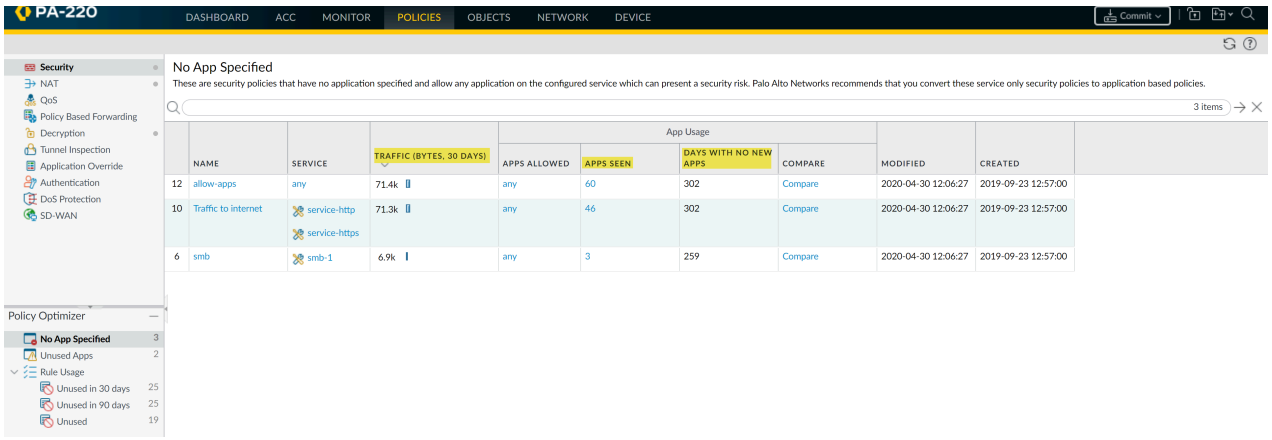
排序和篩選安全性原則規則

您可以篩選安全性原則規則，查看基於連接埠的規則，這些規則上未設定應用程式（**Policies**（原則） > **Security**（安全性） > **Policy Optimizer**（原則最佳化工具） > **No App Specified**（未指定應用程式））。您也可以篩選以查看設定了應用程式但流量僅與部分設定的應用程式相符的規則—該規則為過度佈建，且包含規則上未看到的應用程式（**Policies**（原則） > **Security**（安全性） > **Policy Optimizer**（原則最佳化工具） > **Unused Apps**（未使用的應用程式））。此外，如果您有 SaaS 安全性內嵌授權，則可以使用新應用程式檢視器來篩選看到新 App-ID 雲端引擎 (ACE) 應用程式的規則（請參閱 ACE 文件以瞭解如何操作）。您可以根據不同類型的統計資料，對篩選出的原則規則進行排序，協助確定優先將哪些規則從基於連接埠的規則，轉換為基於應用程式的規則，或者首先清除哪些規則。

您不能在 ***Policies***（原則） > ***Security***（安全性） 中對規則進行篩選或排序，因為這會變革規則庫中原則規則的順序。篩選並排序 ***Policies***（原則） > ***Security***（安全性） > ***Policy Optimizer***（原則最佳化工具） > ***No App Specified***（未指定應用程式）、***Policies***（原則） > ***Security***（安全性） > ***Policy Optimizer***（原則最佳化工具） > ***Unused Apps***（未使用的應用程式）和 ***Policies***（原則） > ***Security***（安全性） > ***Policy Optimizer***（原則最佳化工具） > ***New App Viewer***（新應用程式檢視器）（如果您有 *SaaS* 內嵌安全性訂閱）不會變更規則庫中規則的順序。

您可以按一下數個欄標頭，根據應用程式使用統計資料排序規則。此外，您可以檢視原則規則使用情況，幫助找到並移除未使用的規則，以降低安全性風險，並讓您的政策規則庫井井有條。規則使用方式追蹤讓您能夠快速驗證新規則增加的部分，以及規則變更，並監控操作和疑難排解工作的規則使用狀況。

©2024 Palo Alto Networks, Inc.



- **Traffic (Bytes, 30 days)**（流量（位元組，**30** 天））—過去 30 天內規則上看見的流量。依據預設，在 30 天期間設定目前與清單頂部大多數流量相符的規則（時間範圍越長，越應關注留在清單頂部的舊規則，因為累積總量很大，即使可能不再看到很多流量）。按一下以反轉順序。
- **Apps Seen**（看見的應用程式）—設定在頂部看見最多或最少應用程式的規則。防火牆絕不會自動清除應用程式資料。

  防火牆大約每小時更新一次 ***Apps Seen***（看見的應用程式）。但如果存在大量應用程式流量或大量規則，則更新可能需要一個多小時。將應用程式新增至規則後，請至少等候一小時，再執行「流量日誌」，以查看應用程式的日誌資訊。
- **Days with No New Apps**（沒有新應用程式的天數）—設定自上一個新應用程式與頂部規則相符以來的最多或最少天數的規則。
- （僅限**Unused Apps**（未使用的應用程式）） **Apps Allowed**（允許的應用程式）—設定在頂部規則上設定最多或最少應用程式的規則。

應用程式使用方式統計資料僅計算符合以下條件的規則的應用程式：

- 規則的 Action（動作）必須為 **Allow**（允許）。

 ©2024 Palo Alto Networks, Inc.

- 規則的 Log Setting（日誌設定）必須為 **Log at Session End**（在工作階段結束時記錄）（這是預設日誌設定）。略過 **Log at Session Start**（在工作階段開始時記錄）的規則，以防止計算瞬態應用程式。
- 有效流量必須與規則相符。例如，如果工作階段在足夠的流量通過防火牆以識別應用程式之前結束，則不會對其進行計數。以下流量類型無效，因此不計入 Policy Optimizer（原則最佳化程式）統計資料：
  - 資料不足
  - 不適用
  - 非 SYN-TCP
  - 不完整

  您可以篩選流量日誌（**Monitor**（監控） > **Logs**（日誌） > **Traffic**（流量），以查看識別為其中一種類型的流量。例如，若要查看識別為不完整的所有流量，請使用篩選器 **`(app eq incomplete)`**。

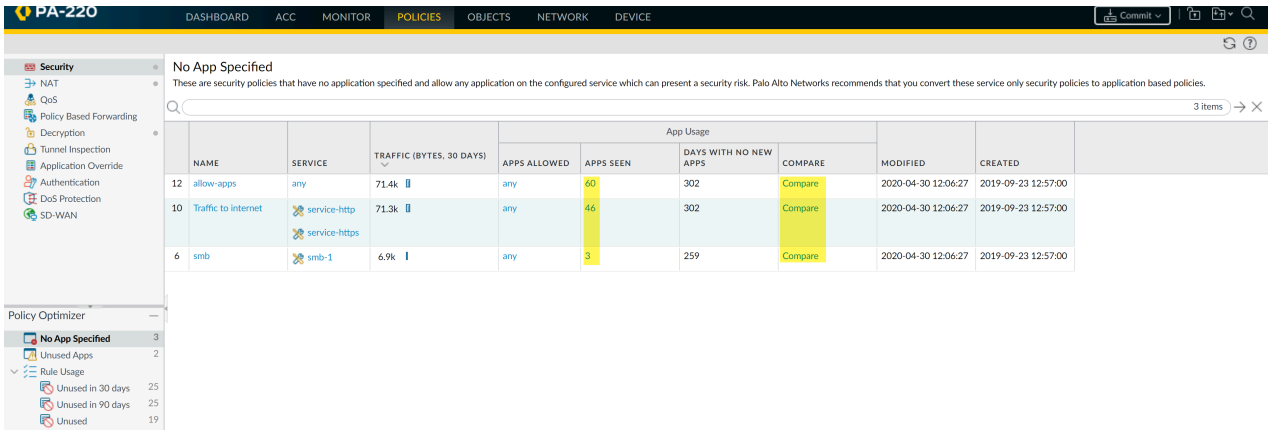
如果不符合這些標準，則不會將應用程式計入 **Apps Seen**（看見的程式）等統計資料，不會影響 **Days with No New Apps**（沒有新應用程式的天數）等統計資料，並且不會出現在應用程式清單中。

防火牆不會追蹤 *interzone-default* 和 *intrazone-default* 安全性原則規則的應用程式使用方式統計資料。

如果規則的 *UUID* 發生變更，則該規則的應用程式使用方式統計資料將會重設，因為 *UUID* 變更會使防火牆將規則視為不同的（新）規則。

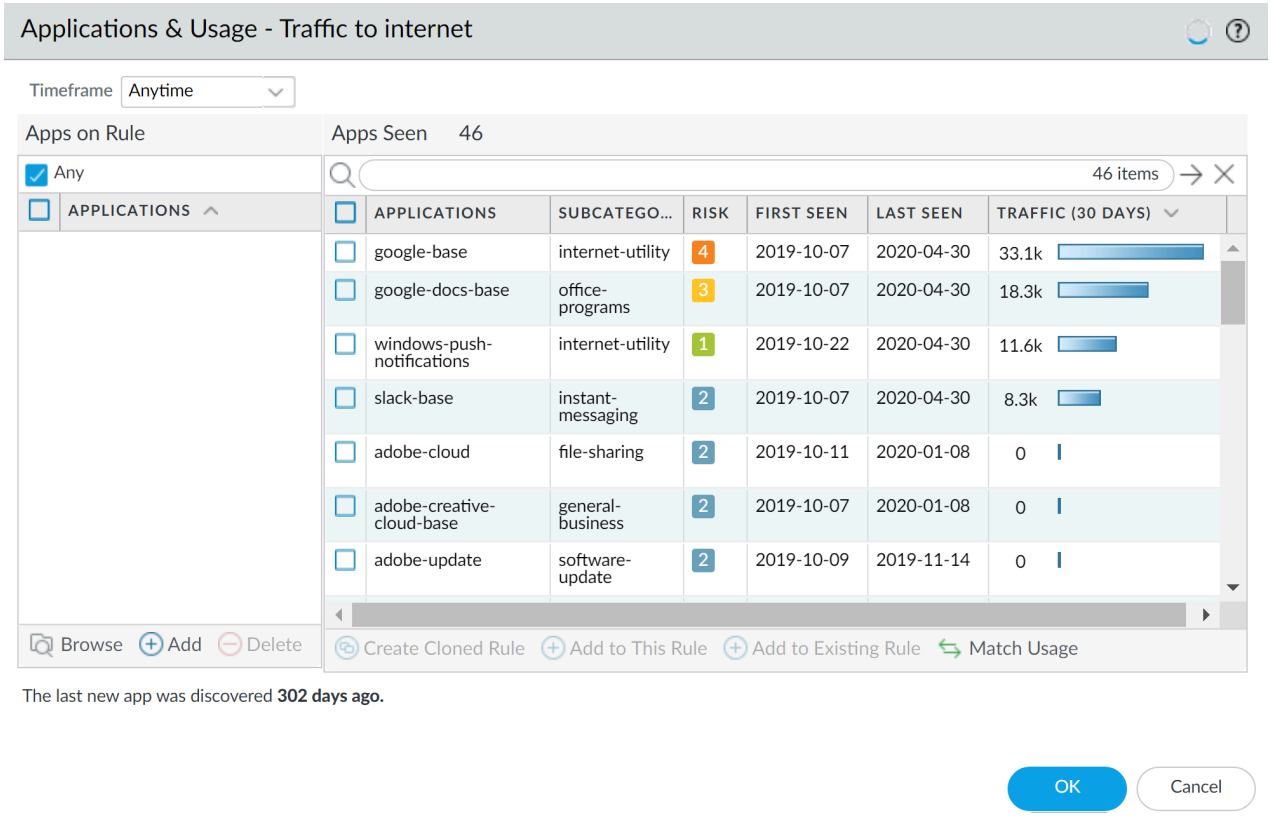
若要查看規則上顯示的應用程式並進行排序，請在規則列中按一下 **Compare**（比較），或按一下 **Apps Seen**（看見的應用程式）中的編號。

©2024 Palo Alto Networks, Inc.



針對在 **Policies**（原則） > **Security**（安全性） > **Policy Optimizer**（原則最佳化程式） > **No App Specified**（未指定應用程式）和 **Policies**（原則） > **Security**（安全性） > **Policy Optimizer**（原則最佳化程式） > **Unused Apps**（未使用的應用程式） 中看見的規則，按一下 **Compare**（比較）或 **Apps Seen**（看見的應用程式）編號，顯示 **Applications & Usage**（應用程式與使用方式），這可讓您查看在規則上看見的應用程式，以及對其進行排序。**Applications & Usage**（應用程式與使用方式）即您從基於連接埠的安全性原則規則移轉至基於 App-ID 的安全性原則規則以及從規則中移除未使用的應用程式的地方。

 ©2024 Palo Alto Networks, Inc.



您可以按照全部六項 **Apps Seen**（看見的應用程式）統計資料（**Apps Seen**（看見的應用程式），對看見應用程式進行排序，其不會即時更新，需要一小時或更長時間來更新，視乎流量和規則數量而定。

- **Applications**（應用程式）—按應用程式名稱的字母順序排列。如果為規則的服務設定特定連接埠或連接埠範圍（服務不能是 **any**（任何）），並且具有應用程式標準（應用程式預設）連接埠，設定的連接埠與應用程式預設連接埠不相符，則在應用程式旁邊會出現一個黃色的三角形警告圖示。
- **Subcategory**（子類別）—按應用程式子類別的字母順序排列，從應用程式內容中繼資料衍生。
- **Risk**（風險）—根據應用程式的風險評等。
- **First Seen**（最先看見）—在規則上看到應用程式的第一天。時間戳記解決方案僅為當天（不是每小時）。
- **Last Seen**（最後看見）—在規則上看到應用程式的最後一天。時間戳記解決方案僅為當天（不是每小時）。
- **Traffic (30 days)**（流量（**30** 天））—在過去 30 天內與規則相符的流量（位元組）為預設排序方法。

©2024 Palo Alto Networks, Inc.

設定 **Timeframe**（時間範圍） 以顯示特定時間段的統計資料—**Anytime**（任何時間）、**Past 7 days**（過去 **7** 天）、**Past 15 days**（過去 **15** 天）或 **Past 30 days**（過去 **30** 天）。

Traffic (30 days)（流量（*30* 天）） 始終僅顯示最近 *30* 天的流量（以位元組為單位）。變更 ***Timeframe***（時間範圍） 不會變更 ***Traffic (30 days)***（流量（*30* 天））位元組測量期間。

按一下欄標題會對顯示進行排序，然後再次按一下同一欄則會反轉順序。例如，按一下 **Risk**（風險）可將應用程式由低風險至高風險排序。再次按一下 **Risk**（風險）可將應用程式由高風險至低風險排序。

防火牆不會為原則最佳化工具即時報告應用程式使用統計資料，因此這不會取代執行報告。

- 防火牆約每小時更新一次 **Apps Allowed**（允許的應用程式）、**Apps Seen**（看見的應用程式），以及在 **Applications & Usage**（應用程式與使用方式）中列示的應用程式，而不是即時更新。如果存在大量流量或大量規則，則更新可能需要更長時間。將應用程式新增至規則後，請至少等候一小時，再執行「流量日誌」，以查看應用程式的日誌資訊。

  防火牆大約每小時更新一次 **Apps Seen**（看見的應用程式）。但如果存在大量應用程式流量或大量規則，則更新可能需要一個多小時。將應用程式新增至規則後，請至少等候一小時，再執行「流量日誌」，以查看應用程式的日誌資訊。
- 防火牆每天在午夜裝置時間更新一次 **Days with No New Apps**（沒有新應用程式的天數），以及 **Applications & Usage**（應用程式與使用方式） 上的 **First Seen**（最先看見） 和 **Last Seen**（最後看見）。
- 對於看見的大量應用程式規則，處理應用程式使用方式統計資料可能需要更長時間。
- 對於包含大量有許多應用程式的規則的安全性原則規則庫，處理應用程式使用方式統計資料可能需要更長時間。
- 對於由 Panorama 管理的防火牆，應用程式使用方式資料僅對 Panorama 推送至防火牆的規則可見，而非針對在個別防火牆上進行本機設定的規則。

清除應用程式使用資料

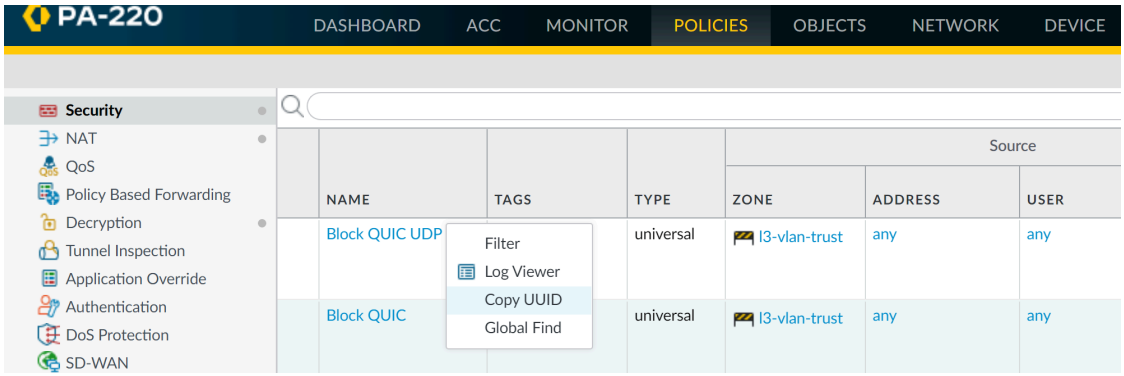
您可使用 CLI 命令清除個別安全性原則規則的應用程式使用資料並重設 **Apps Seen**（看見的應用程式）及其他應用程式使用資料。

©2024 Palo Alto Networks, Inc.

STEP 1 | 找到您想要清除其應用程式使用資料的安全性原則規則之 UUID。

有兩種方法可以在 CN 中找到 UUID：

- 在 **Policies**（原則） > **Security**（安全性） 中，從 **Rule UUID**（規則 **UUID**） 欄複製 UUID。
- 在 **Policies**（原則） > **Security**（安全性）中，選取規則 **Name**（名稱）下拉式功能表中的 **Copy UUID**（複製 **UUID**）。



STEP 2 | 從 UI 切換至 CLI。

使用您在 UI 中擷取的 UUID 清除規則的應用程式使用資料：

```
admin@PA-VM>clear policy-app-usage-data ruleuuid <uuid-value>
```

貼上或輸入規則的 UUID 作為值，並執行命令以清除規則的應用程式使用資料。

從基於連接埠的安全性原則規則移轉至基於 App-ID 的安全性原則規則

當您從舊有防火牆轉換為 Palo Alto Networks 新一代防火牆時，會繼承大量基於連接埠的規則，這會允許連接埠上的任何應用程式，導致增加攻擊面，因為任何應用程式都可以使用開放連接埠。原則最佳化程式可識別在任何舊有基於連接埠的安全性原則規則中看到的所有應用程式，並提供一個簡單的工作流程，用於選取要在該規則上允許的應用程式。將基於連接埠的規則移轉至基於應用程式的規則，以減少攻擊面並安全地啟用網絡上的應用程式。使用原則最佳化程式在新增應用程式時維護規則庫。

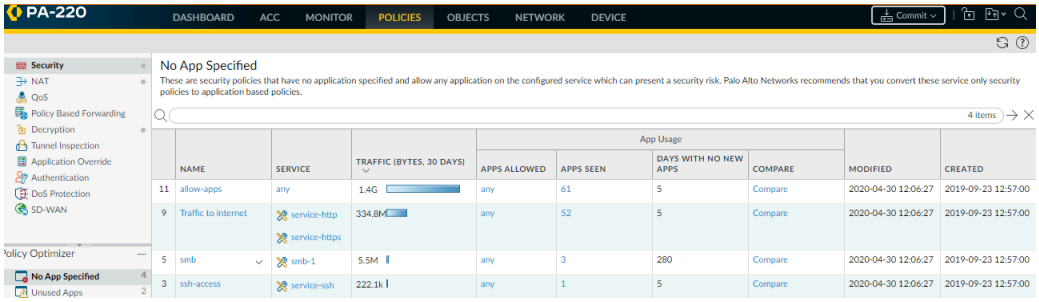
一次性將一些基於連接埠的規則移轉至基於應用程式的規則，並按優先級方式執行。逐步轉換比一次性移轉大型規則庫更安全，並且更容易確保新的基於應用程式的規則來控制必要的應用程式。使用 ***Policy Optimizer***（原則最佳化程式）來確定首先要轉換規則的優先級。

若要將組態從傳統防火牆移轉至 *Palo Alto Networks* 裝置，請參閱移轉至基於應用程式的原則之最佳做法。

©2024 Palo Alto Networks, Inc.

STEP 1 | 識別基於連接埠的規則。

基於連接埠的規則沒有設定（允許的）應用程式。**Policies**（原則） > **Security**（安全性） > **Policy Optimizer**（原則最佳化程式） > **No App Specified**（未指定應用程式） 顯示所有基於連接埠的規則（**Apps Allowed**（允許的應用程式） 為 **any**（任何））。



STEP 2 | 優先考慮要先轉換的基於連接埠的規則。

Policies（原則） > **Security**（安全性） > **Policy Optimizer**（原則最佳化程式） > **No App Specified**（未指定應用程式） 讓您能夠 對規則排序，而不影響其在規則庫中的順序，並提供其他資訊，協助您根據業務目標和風險承受能力確定轉換規則的優先級。

- **Traffic (Bytes, 30 days)**（流量（位元組，**30** 天））—（按一下以排序。） 目前與清單頂部大多數流量相符的規則。這是預設的排序。
- **Apps Seen**（看見的應用程式）—（按一下以排序。） 與基於連接埠的規則相符的大量合法應用程式可能表明，您應將其取代為嚴謹定義應用程式、使用者、來源和目的地的多個基於應用程式的規則。例如，若基於連接埠的規則控制不同裝置集上不同使用者群組的多個應用程式流量，請建立單獨的規則，將應用程式與其合法使用者和裝置配對，以減少攻擊面並提高可見性。（按一下 **Apps Seen**（看見的應用程式）數量或 **Compare**（比較），即會顯示符合規則的應用程式。）

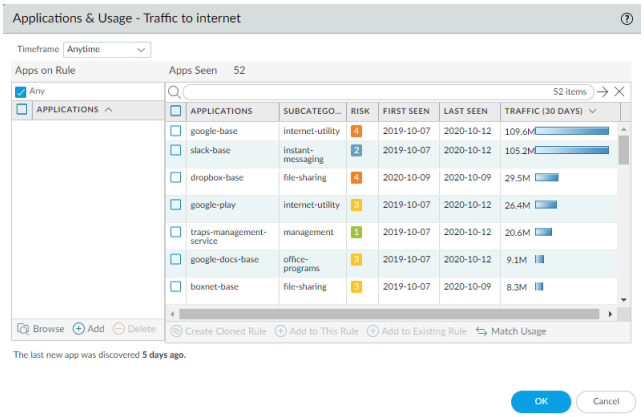
  防火牆大約每小時更新一次 ***Apps Seen***（看見的應用程式）。但如果存在大量應用程式流量或大量規則，則更新可能需要一個多小時。將應用程式新增至規則後，請至少等候一小時，再執行「流量日誌」，以查看應用程式的日誌資訊。
- **Days with No New Apps**（沒有新應用程式的天數）—（按一下以排序。） 當基於連接埠的規則上看見的應用程式穩定後，您可以更加確信規則是成熟的，轉換不會意外地排除合法應用程式，並且沒有更多新應用程式符合規則。**Created**（已建立）和 **Modified**（已修改）日期可協助您評估規則的穩定性，因為最近未修改的舊規則也可能更穩定。
- **Hit Count**（命中數）—顯示所選時間範圍內具有最多相符項的規則。您可排除重設命中計數器的規則，並指定排除時間（天）。排除最近重設命中計數器的規則，可以防止顯示命中數低於預期的規則出現錯誤，因為您不知道計數器已重設。

  您還可以將 ***Hit Count***（命中數）用於檢視原則規則使用情況，協助識別和移除未使用的規則，以降低安全性風險並使您的規則庫保持井然有序。

 ©2024 Palo Alto Networks, Inc.

STEP 3 | 從最高優先級規則開始，檢閱基於連接埠的規則上的 **Apps Seen**（看見的應用程式）。

在 **No Apps Specified**（未指定應用程式）上，按一下 **Compare**（比較）或 **Apps Seen**（看見的應用程式）中的數字，開啟 **Applications & Usage**（應用程式與使用方式），其中列出了應用程式在指定的 **Timeframe**（時間範圍）與基於連接埠的規則相符的應用程式數量、每個應用程式的 **Risk**（風險）、**First Seen**（最先看見）的日期、**Last Seen**（最後看見）的日期，以及過去 30 天的流量。



您可以在過去 7 天、15 天或 30 天或基於規則的生命週期內（**Anytime**（任何時間）），檢閱基於連接埠的規則上的 **Apps Seen**（看見的應用程式）。對於移轉規則，**Anytime**（任何時間）提供與規則相符的應用程式的最完整評估。

您可以搜尋並篩選 **Apps Seen**（看見的應用程式），但請注意，更新 **Apps Seen**（看見的應用程式）需要一個小時或更長時間。您還可以按一下欄標題，對 **Apps Seen**（看見的應用程式）排序。例如，您可以按一下 **Traffic (30 days)**（流量（**30** 天），將具有最新流量的應用程式置於清單頂部，或按一 下**Subcategory**（子類別），按子類別整理應用程式。

First Seen（最先看見）和 ***Last Seen***（最後看見）的測量間隔為一天，因此在您定義規則的當天，這兩欄中的日期是相同的。在防火牆看見應用程式流量的第二天，您會看到日期的差異。

©2024 Palo Alto Networks, Inc.

STEP 4 | 複製或新增應用程式至規則，以指定要在規則上允許的應用程式。

在 **Applications & Usage**（應用程式與使用方式）上，使用以下方法之一，將基於連接埠的規則轉換為基於應用程式的規則：

- 複製規則—保留基於連接埠的原始規則，並將複製的基於應用程式的規則直接置於規則庫中。
- 新增應用程式至規則—使用新的基於應用程式的規則取代基於連接埠的原始規則，並刪除原始規則。

如果您有現有的基於應用程式的規則，且想要將應用程式從基於連接埠的規則移轉到基於應用程式的規則，您可以新增應用程式至現有規則，而不是複製新規則或透過向其新增應用程式來轉換基於連接埠的規則。

某些應用程式會間隔出現在網路上，例如，季度或年度事件。若歷程記錄不足以擷取其最新活動，則這些應用程式可能不會顯示在 ***Applications & Usage***（應用程式與使用方式）畫面上。

複製規則或將應用程式新增至規則時，原始規則的其他任何內容都不會變更。除了新增至規則中的應用程式之外，原始規則的組態保持不變。例如，若原始規則的服務允許 ***Any***（任何）應用程式或指定特定服務，則需將服務變更為 ***Application-Default***（應用程式預設），以將允許的應用程式限制為其新規則的預設連接埠。

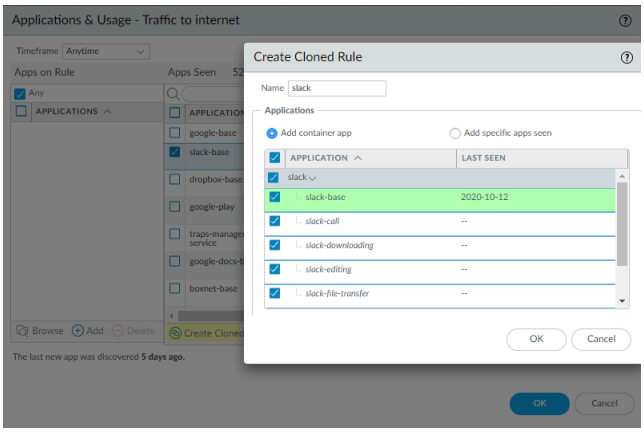
複製是移轉規則最安全的方法，尤其是當 **Applications & Usage**（應用程式和使用方式）顯示多個與該規則相符的眾所周知的應用程式時（規則複製移轉使用案例：Web 瀏覽和 SSL 流量提供了此情況的範例）。複製會保留基於連接埠的原始規則，並將其置於複製的基於應用程式的規則之下，從而消除因與複製規則不相符的流量流入基於連接埠的規則而遺失應用程式可用性的

©2024 Palo Alto Networks, Inc.

風險。當合法應用程式的流量未在合理的時間段內命中基於連接埠的規則時，您可以將其刪除以完成該規則的移轉。

若要複製基於連接埠的規則：

1. 在 **Apps Seen**（看見的應用程式）中，勾選複製規則中所需每個應用程式旁邊的核取方塊。請注意，更新 **Apps Seen**（看見的應用程式）需要一個小時或更長時間。
2. 按一下 **Create Cloned Rule**（建立複製規則）。在 **Create Cloned Rule**（建立複製規則）對話方塊中，**Name**（命名）複製規則（在此範例中為「Slack」），並視需在同一容器和應用程式相依項中新增其他應用程式。例如，若要透過選取基於 Slack 的應用程式來複製規則：



綠色文字是要複製的選定應用程式。容器應用程式 **(slack)** 位於灰色列中。以斜體列出的應用程式是規則中未看見的應用程式，但與所選應用程式位於同一容器中。在規則上看見的個別應用程式採用普通字型。依據預設，所有應用程式都包含在複製規則中（**Add Container App**（新增容器應用程式），該項可新增容器中的所有應用程式，預設已選定），以協助防止規則今後被中斷。

3. 若要允許容器中的所有應用程式，請選取 **Add container app**（新增容器應用程式）。這也會「在未來驗證」規則，因為當應用程式新增至容器應用程式時，其會自動新增至規則中。

   若要限制存取容器中的某些個別應用程式，請取消選中您不希望使用者存取的每個個別應用程式旁邊的方塊。這亦會取消選中容器應用程式，因此若您希望稍後在容器中允許新的應用程式，則必須單獨新增這些應用程式。

   若取消選中容器應用程式，則會取消選中所有應用程式，然後您要手動選取要包含在複製規則中的應用程式。
4. 如果應用程式相依性列示在應用程式下面的方塊中（本示例中沒有），則將其保留為選中。您選取的應用程式需要這些應用程式相依性才可執行。常見相依性包括 **ssl** 和 **web-browsing**。
5. 按一下 **OK**（確定），將新的基於應用程式的規則直接新增至規則庫中基於連接埠的規則上方。
6. **Commit**（提交）組態。

複製規則並 **Commit**（提交）組態時，您為複製規則選取的應用程式，將從基於連接埠的原始規則的 **Apps Seen**（看見的應用程式） 清單中移除。例如，若基於連接埠的規則具有 16 個

 ©2024 Palo Alto Networks, Inc.

Apps Seen（看見的應用程式），並且您為複製規則選取了兩個單獨的應用程式和一個相依應用程式，複製後，基於連接埠的規則將顯示 13 個 **Apps Seen**（看見的應用程式），因為已從基於連接埠的規則中移除了三個選定的應用程式 (16-3 = 13)。複製規則在 **Apps on Rule**（規則上的應用程式）中顯示三個新增的應用程式。

使用容器應用程式建立複製規則的方式略有不同。例如，基於連接埠的規則有 16 個 **Apps Seen**（看見的應用程式），您可以為複製規則選取一個個別應用程式和一個容器應用程式。容器應用程式有五個單獨的應用程式，並有一個相依應用程式。複製後，複製規則顯示七個 **Apps on Rule**（規則上的應用程式）—個別應用程式、容器應用程式中的五個個別應用程式，以及容器應用程式的相依應用程式。但是，在基於連接埠的原始規則中，**Apps Seen**（看見的應用程式） 顯示 13 個應用程式，因為只有個別應用程式、容器應用程式和容器應用程式的相依應用程式從基於連接埠的規則中移除。

相較於複製，將應用程式新增至基於連接埠的規則會將規則取代為產生的基於應用程式的規則。將應用程式新增至規則比複製更簡單，但風險更大，因為您可能無意中錯過應當在規則上的應用程式，並且基於連接埠的原始規則不再出現在規則庫中來擷取意外遺漏。不過，將應用程式新增至基於連接埠的規則，且該規則僅適用於少數眾所周知的應用程式，則會將規則快速

©2024 Palo Alto Networks, Inc.

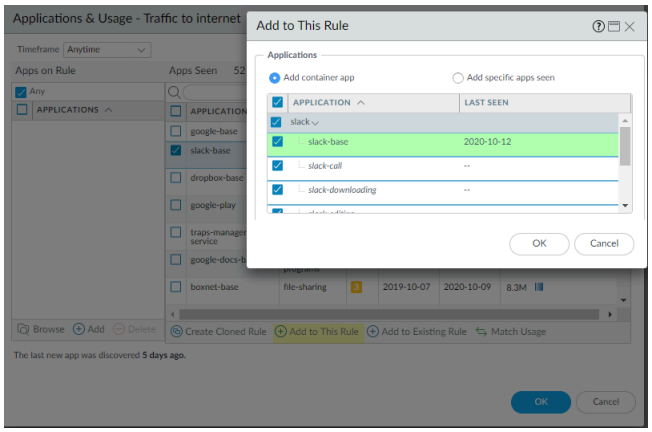
移轉至基於應用程式的規則。例如，對於僅控制 TCP 連接埠 22 流量的基於連接埠的規則，唯一合法的應用程式是 SSH，因此將規則新增至應用程式是安全的。

使用傳統安全性原則規則的 ***Application***（應用程式）標籤新增應用程式，不會變更 ***Apps Seen***（看見的應用程式）或 ***Apps on Rule***（規則上的應用程式）。若要保留準確的應用程式使用方式資訊，在將基於連接埠的規則取代為基於應用程式的規則時，使用 ***Apps Seen***（看見的應用程式）中的 ***Add to This Rule***（新增至此規則）或 ***Match Usage***（與使用方式相符）（或創建複製規則，或改為將應用程式新增至現有的基於應用程式的規則）來新增應用程式。

有三種方法可以透過新增應用程式（**Add to This Rule**（新增至此規則以及 **Apps Seen**（看見的應用程式） 中的 **Match Usage**（與使用方式相符） 和 **Apps on Rule**（規則上的應用程式） 中的 **Add**（新增））， 將基於連接埠的規則取代為基於應用程式的規則：

- **Apps Seen**（看見的應用程式） 中的 **Add to This Rule**（新增至此規則）（符合規則的應用程式）。請注意，更新 **Apps Seen**（看見的應用程式）需要一個小時或更長時間。

  1. 在規則上選取 **Apps Seen**（看見的應用程式）中的應用程式。
  2. 按一下 **Add to This Rule**（新增至此規則）。在 **Add to This Rule**（新增至此規則）對話方塊中，視需在同一容器應用程式和應用程式相依項中新增其他應用程式。例如，若為規則新增 slack-base：



與 **Create Cloned Rule**（建立複製規則）對話方塊類似，**Add to This Rule**（新增至此規則）中的綠色文字是要新增至規則的選定應用程式。容器應用程式 **(slack)** 位於灰色列中。以斜體列出的應用程式是規則中未看見的應用程式，但與所選應用程式位於同一容器中。在規則上看見的個別應用程式採用普通字型。依據預設，所有應用程式都包含在複

©2024 Palo Alto Networks, Inc.

製規則中（**Add Container App**（新增容器應用程式），該項可新增容器中的所有應用程式，預設已選定），以協助防止規則今後被中斷。

3. 若要允許容器中的所有應用程式，請選取 **Add container app**（新增容器應用程式）。這也會「在未來驗證」規則，因為當應用程式新增至容器應用程式時，其會自動新增至規則中。

   若要限制存取容器中的某些個別應用程式，請取消選中您不希望使用者存取的每個個別應用程式旁邊的方塊。這亦會取消選中容器應用程式，因此若您希望稍後在容器中允許新的應用程式，則必須單獨新增這些應用程式。

   若取消選中容器應用程式，則會取消選中所有應用程式，然後您要手動選取要包含在複製規則中的應用程式。

4. 如果應用程式相依性列示在應用程式下面的方塊中（本示例中沒有），則將其保留為選中。您選取的應用程式需要這些應用程式相依性才可執行。

5. 按一下 **OK**（確定），將基於連接埠的規則取代為新的基於應用程式的規則。

Add to This Rule（新增至此規則）並 **Commit**（提交）組態後，您未新增的應用程式將從 **Apps Seen**（看見的應用程式）中刪除，因為新的基於應用程式的應用程式規則不再允許他們。例如，若規則有 16 個 **Apps Seen**（看見的應用程式），並且將三個應用程式 **Add to This Rule**（新增至此規則），則產生的新規則僅顯示 **Apps Seen**（看見的應用程式）中新增的三個應用程式。

Add to This Rule（新增至此規則）與容器應用程式的工作方式略有不同。例如，基於連接埠的規則有 16 個 **Apps Seen**（看見的應用程式），您可以選取一個個別應用程式和一個容器應用程式以新增至新的規則。容器應用程式有五個單獨的應用程式，並有一個相依應用程式。將應用程式新增至規則後，新的規則顯示七個 **Apps on Rule**（規則上的應用程式）—個別應用程式、容器應用程式中的五個個別應用程式，以及容器應用程式的相依應用程式。但是，**Apps Seen**（看見的應用程式） 顯示 13 個應用程式，因為個別應用程式、容器應用程式和容器應用程式的相依應用程式從清單中移除。

- 只需按一下（**Match Usage**（與使用方式相符）），即可將規則中的所有 **Apps Seen**（看見的應用程式）一次性新增至規則中。

  基於連接埠的規則允許任何應用程式，因此 ***Apps Seen***（看見的應用程式）可能包含不需要或不安全的應用程式。僅當規則看見少量具有合法業務用途的眾所周知的應用程式時，才使用 ***Match Usage***（與使用方式相符）轉換規則。一個很好的範例是 *TCP* 連接埠 *22*，其應只允許 *SSH* 流量，因此若 *SSH* 是在開啟連接埠 *22* 的基於連接埠的規則上看見的唯一應用程式，則可以安全地 ***Match Usage***（與使用方式相符）。

  1. 在 **Apps Seen**（看見的應用程式）中，按一下 **Match Usage**（與使用方式相符）。請注意，更新 **Apps Seen**（看見的應用程式）需要一個小時或更長時間。**Apps Seen**（看見的應用程式）中的所有應用程式都會復製到 **Apps on Rule**（規則上的應用程式）中。
  2. 按一下 **OK**（確定），建立基於應用程式的規則，並取代基於連接埠的規則。

- 若您知道規則所需的應用程式，則可在 **Apps on Rule**（規則上的應用程式）中手動 **Add**（新增）應用程式。不過，此方法相當於使用傳統安全性原則規則的 **Application**（應用程式）標

©2024 Palo Alto Networks, Inc.

籤新增應用程式，並且不會變更 **Apps Seen**（看見的應用程式）或 **Apps on Rule**（規則上的應用程式）。若要保留準確的應用程式使用方式資訊，使用 **Apps Seen**（看見的應用程式）中的 **Add to This Rule**（新增至此規則）、**Create Cloned Rule**（建立複製規則）或 **Match Usage**（與使用方式相符）來轉換規則。

1. 在 **Apps on Rule**（規則上的應用程式）中，**Add**（新增）（或 **Browse**（瀏覽）) 應用程式，以選取要新增至規則的應用程式。這相當於在 **Application**（應用程式）標籤上新增應用程式。
2. 按一下 **OK**（確定）將應用程式新增至規則，並將基於連接埠的規則取代為新的基於應用程式的規則。

由於此方法相當於使用 ***Application***（應用程式） 標籤來新增應用程式，因此不會彈出新增應用程式相依項的對話方塊。

STEP 5 | 對於每項基於應用程式的規則，將 **Service**（服務）設定為 **application-default**（應用程式預設）。

若業務需求要求您允許特定用戶端和伺服器之間的非標準連接埠上的應用程式（例如，內部自訂應用程式），則將該異常限制為僅包含所需的應用程式、來源和目的地。請考慮重寫自訂應用程式，以便其使用應用程式預設連接埠。

STEP 6 | **Commit**（提交）組態。

STEP 7 | 監控規則。

- 複製規則—監控基於連接埠的原始規則，以確保基於應用程式的規則與所需的流量相符。若您要允許的應用程式與基於連接埠的規則相符，請將其新增至基於應用程式的規則，或複製其他基於應用程式的規則。當只有您在網路上不需要的應用程式在一段合理的時間內與基於連接埠的規則相符時，複製規則是穩健的（其會擷取您要控制的所有應用程式流量），並且您可以安全地將其移除。
- 新增應用程式的規則—由於您只將具有少量眾所周知應用程式的、基於連接埠的規則直接轉換為基於應用程式的規則，因此在大多數情況下，規則從一開始就是可靠的。監控轉換後的規則以查看預期流量是否與規則相符—若流量少於預期，則該規則可能不允許所有必要的應用程式。若流量超出預期，則該規則可能允許不需要的流量。聆聽使用者的意見反應—若使用者無法存取業務用途所需的應用程式，則該規則（或其他規則）可能過於緊張。

規則複製移轉使用案例：Web 瀏覽和 SSL 流量

允許在 TCP 連接埠 80（HTTP Web 瀏覽）和 443（HTTPS SSL）上進行 Web 存取的基於連接埠的規則，無法控制哪些應用程式使用這些開放的連接埠。Web 應用程式眾多，因此允許 Web 流量的一般規則允許成千上萬的應用程式，其中許多是您不希望在網路上執行的。

該使用案例說明了如何將基於連接埠的原則（允許所有 Web 應用程式）移轉至基於應用程式的原則（僅允許所需應用程式），因此您可以安全地啟用您選擇允許的應用程式。對於看見大量應用程式的規則，相較於將應用程式新增至規則，複製基於連接埠的原始規則更安全，因為新增會取代基於連接埠的規則，因此如果您無意中忘記新增關鍵應用程式，則會影響應用程式可用性。如果採用

©2024 Palo Alto Networks, Inc.

Match Usage（與使用方式相符），這也會取代基於連接埠的規則，您將允許規則看見的所有應用程式，這可能是危險的，尤其是對於 Web 瀏覽流量。

複製規則會保留基於連接埠的原始規則，並將複製規則直接置於規則庫中基於連接埠的規則上方，以便您可以監控規則。複製還允許您將看見許多不同應用程式的規則（例如基於連接埠的 Web 流量規則）拆分為多個基於應用程式的規則，以便您可以區別處理不同的應用程式群組。如果您確定要允許複製規則（或規則）中允許的所有應用程式，則可移除基於連接埠的規則。

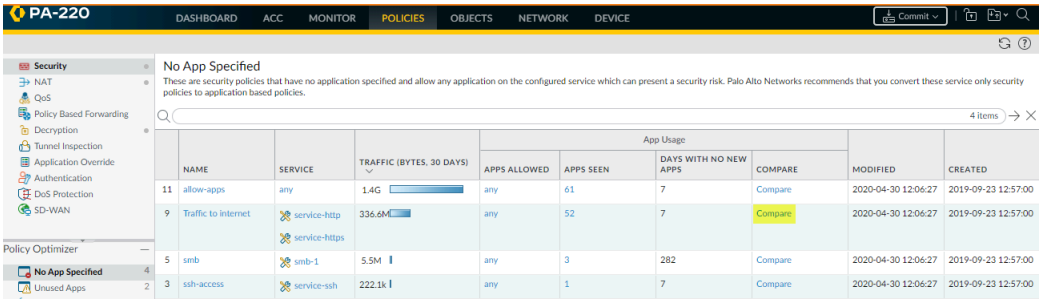
此範例複製了基於連接埠的 Web 流量規則，以便為基於 Web 的檔案共用流量（基於連接埠的規則中看見的應用程式流量的子集）建立基於應用程式的規則。

請範例不適用於使用新應用程式檢視器複製 *App-ID* 雲端引擎 *(ACE)* 應用程式（請參閱 ACE 文件獲取執行此操作的範例）；*ACE* 需要 SaaS 安全性內嵌授權。

STEP 1 | 導覽至 **Policies**（原則） > **Security**（安全性） > **Policy Optimizer**（原則最佳化程式） > **No App Specified**（未指定應用程式），以監視基於連接埠的規則。

STEP 2 | 對於您要移轉的規則，按一下 **Compare**（比較）。

在此範例中，允許 Web 存取的基於連接埠的規則被稱為網際網路流量。

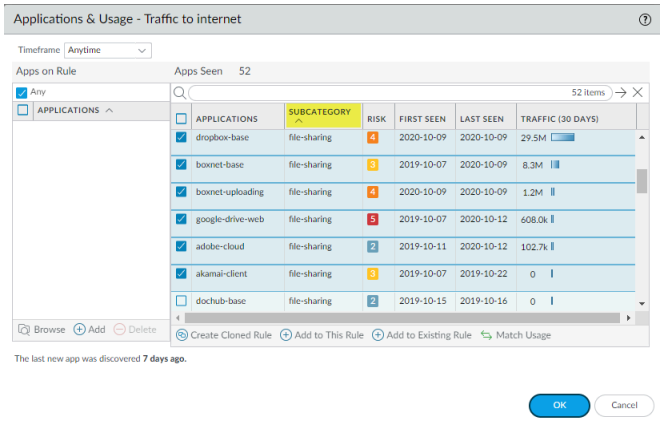


©2024 Palo Alto Networks, Inc.

STEP 3 | 使用排序選項，從 **Apps Seen**（看見的應用程式）中審查並選取您要允許的應用程式。

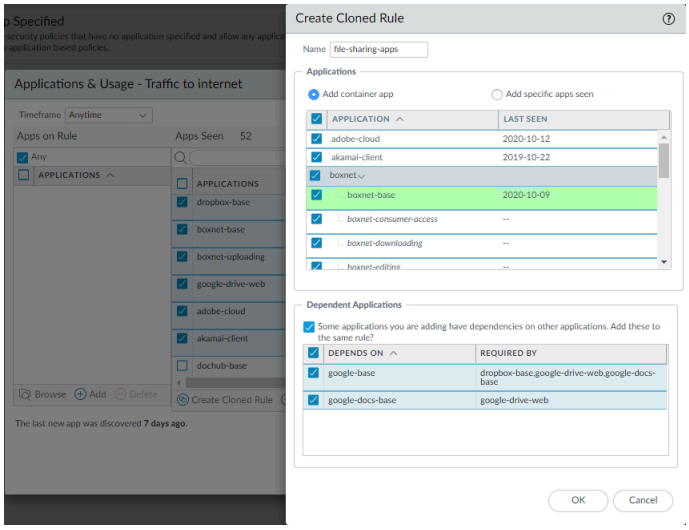
> ***Apps Seen***（看見的應用程式）數量約每小時更新一次，因此如果您沒有看到預期的應用程式數量，請於約一小時後再次查看。視乎防火牆的負載，這些欄位可能需要超過一小時才會更新。

例如，按一下 **Subcategory**（子類別）對應用程式進行排序，捲動至檔案共用子類別，然後選取您要允許的應用程式。或者，您可以篩選（搜尋）檔案共用應用程式。



STEP 4 | 按一下 **Create Cloned Rule**（建立複製規則）和 **Name**（命名）複製的規則（在本範例中為 file-sharing-apps）。

Create Cloned Rule（建立複製規則）以綠色陰影顯示選取的應用程式，以灰色陰影顯示容器應用程式，以*斜體*顯示規則上尚未看見的容器中的個別應用程式，以及在普通文本字型顯示規則上已經看見的個別應用程式。捲動瀏覽 **Applications**（應用程式），會顯示所有容器應用程式及其個別應用程式。



Create Cloned Rule（建立複製規則）還會顯示所選應用程式的相依應用程式。在此範例中，所選的一些應用程式需要（**Required By**（要求者））google-base 和 google-docs-base 應用程式才可以執行。

©2024 Palo Alto Networks, Inc.

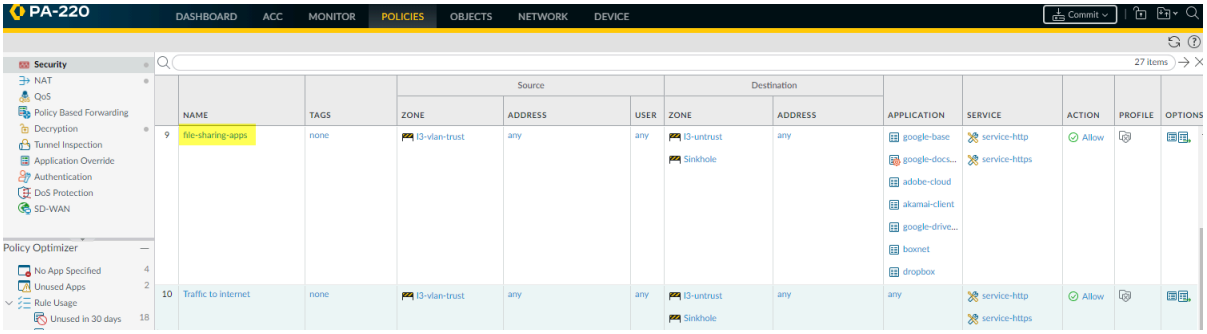
STEP 5 | 在複製規則中選取所需的應用程式。

對於您不想包含的應用程式，請取消選中相應的方塊，該方塊也會取消選中容器應用程式。若不包含容器應用程式，則當新應用程式新增至容器時，它們不會自動新增至規則中。

若取消選中容器應用程式，則會取消選中容器中的所有個別應用程式，並且必須手動選取要新增的應用程式。

STEP 6 | 按一下 **OK**（確定）來建立複製規則。。

STEP 7 | 在 **Policies**（原則） > **Security**（安全性）中，複製規則 (file-sharing-apps) 將插入基於連接埠的原始規則（網際網路流量）上方的規則庫中。



STEP 8 | 按一下規則名稱以編輯複製規則，該規則將繼承基於連接埠的原始規則的屬性。

STEP 9 | 在 **Service/URL Category**（服務/URL 類別）標籤上，從 **Service**（服務） 中刪除 service-http 和 service-https。

這會將 **Service**（服務）變更為 **application-default**（應用程式預設），從而阻止應用程式使用非標準連接埠並進一步減少攻擊面。

若業務需求要求您允許特定用戶端和伺服器之間的非標準連接埠上的應用程式（例如，內部自訂應用程式），則將該異常限制為僅包含所需的應用程式、來源和目的地。請考慮重寫自訂應用程式，以便其使用應用程式預設連接埠。

STEP 10 | 在 **Source**（來源）、**User**（使用者）和 **Destination**（目的地）上，加強規則，僅在正確的位置（區域、子網路）套用於適當的使用者）。

例如，您可能決定將 Web 檔案共用活動限制為僅出於業務原因需要在整個 Web 上共用檔案的使用者群組。

STEP 11 | 按一下 **OK**（確定）。

STEP 12 | **Commit**（提交）組態。

STEP 13 | 對基於連接埠的 Web 存取規則中的其他應用程序類別重複此程序，直至基於應用程序的規則僅允許您希望在網路上允許的應用程序。

若要允許的流量在足夠長的時間內停止命中基於連接埠的原始規則，以確信不再需要基於連接埠的規則，則可以從規則庫中移除基於連接埠的規則。

©2024 Palo Alto Networks, Inc.

新增應用程式至現有規則

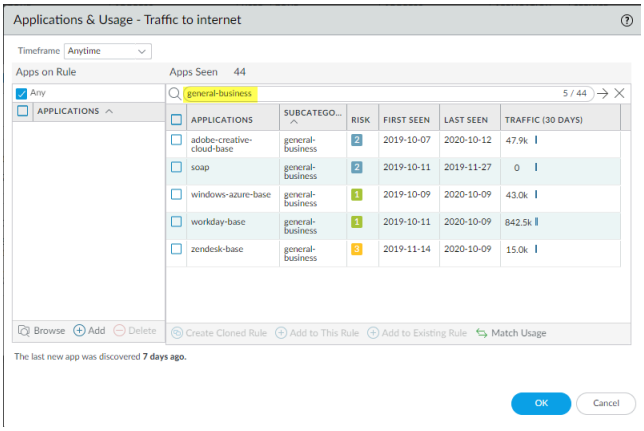
在某些情況下，您可能希望將在以連接埠為基礎的規則上獲知（看見）的應用程式新增至現有的規則中。例如，管理員可能會從允許網際網路存取的以連接埠為基礎的規則（連接埠 80/443 規則），為一般業務 Web 應用程式建立複製之以應用程式為基礎的規則。之後，管理員會注意到，以連接埠為基礎的網際網路存取規則可以看見更多一般業務應用程式，並希望將其中的部分或全部新增至複製之以應用程式為基礎的規則（針對同一類型的應用程式複製另一個以應用程式為基礎的規則會建立不必要的規則，並使規則庫複雜化）。

此範例假定用於控制一般業務流量之基於應用程式的安全性政策規則已存在，或者已從基於連接埠的網際網路存取規則中將其複製，類似於 規則複製移轉使用案例：Web 瀏覽和 SSL 流量。在該範例中，我們從基於連接埠的網際網路存取規則複製了一個基於應用程式的規則，並將新規則的服務變更為應用程式預設值，以防止基於 Web 的應用程式使用非標準連接埠。

除了新增應用程式到現有基於應用程式的規則外，您還可以新增應用程式到現有基於連接埠的規則。這會針對您新增到規則的應用程式將基於連接埠的規則轉換為基於應用程式的規則。如果您執行此操作，請轉到規則並將服務變更為應用程式預設值，以防止應用程式使用非標準連接埠（另外，規則上設定的服務可能與應用程式不符）。

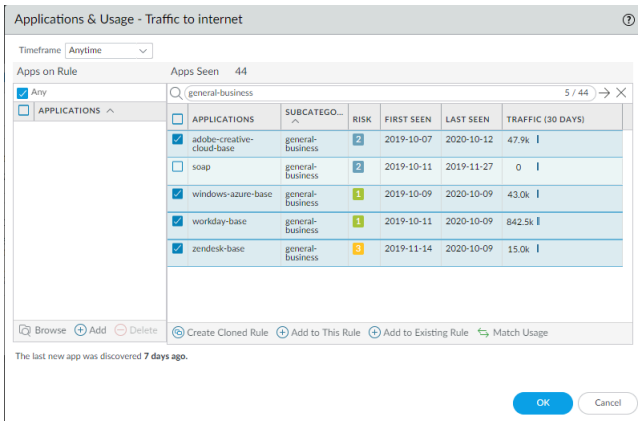
請範例不適用於使用新應用程式檢視器新增 *App-ID* 雲端引擎 *(ACE)* 應用程式到現有規則（請參閱 ACE 文件獲取執行此操作的範例）；*ACE* 需要 SaaS Security Inline（SaaS 安全性內嵌）授權。

STEP 1 | 檢查基於連接埠的網際網路存取規則，可發現規則已看見一般業務應用程式，且您需要允許一些此類應用程式用於業務目的。

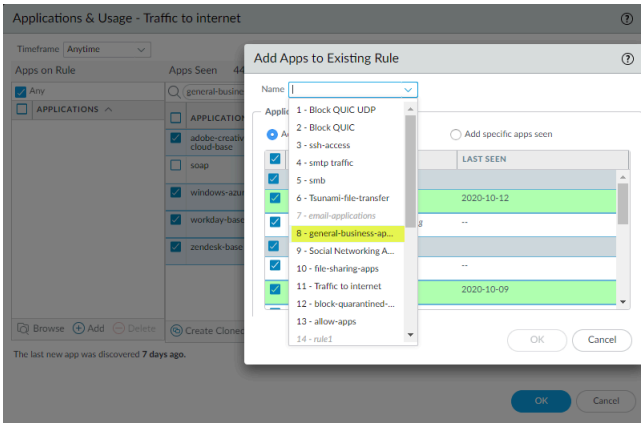


 ©2024 Palo Alto Networks, Inc.

STEP 2 | 選取您想要新增到現有規則的一般業務應用程式。



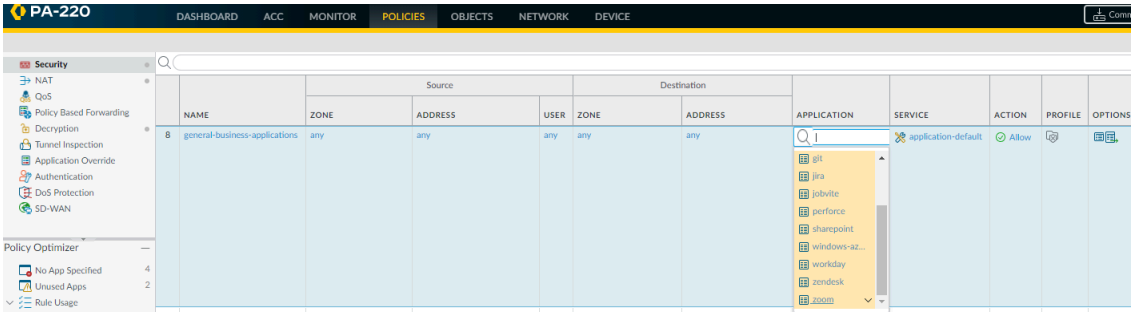
STEP 3 | 按一下 **Add to Existing Rule**（新增至現有規則）並選取要向其新增應用程式的規則之 **Name**（名稱），在本範例中，為 **general-business-applications**（一般業務應用程式）。



STEP 4 | 在 **Add Apps to Existing Rule**（新增應用程式至現有規則）中按一下 **OK**（確定），以將所選應用程式新增到 **general-business-applications**（一般業務應用程式）規則。

STEP 5 | 在 **Applications & Usage**（應用程式與使用方式）中按一下 **OK**（確定）。

STEP 6 | 更新後的規則現在可以控制規則上的原始應用程式及您剛才新增的應用程式。



 ©2024 Palo Alto Networks, Inc.

透過未使用的應用程式識別安全性原則規則

如果您有基於應用程式的安全性原則規則允許大量應用程式，則可移除未使用的應用程式（從未在規則上看到的應用程式）以收緊規則，使其僅允許在符合規則的流量中實際看到的應用程式。最佳做法是，從安全性原則規則中識別並移除未使用的應用程式，以減少攻擊面，從而提高網路安全性。

STEP 1 | 識別具有未使用應用程式的安全性原則規則。

Policies（原則） > **Security**（安全性） > **Policy Optimizer**（原則最佳化工具） > **Unused Apps**（未使用的應用程式）顯示設定有不符合規則之應用程式（在規則上未看到）的、基於應用程式的規則。這意味著這些規則允許您可能未在網路中使用的應用程式（或另一個規則遮蔽了該規則，因此您預計符合該規則的流量會與規則庫中較早的規則相符）。

Apps Allowed（允許的應用程式）和 ***Apps Seen***（看見的應用程式）數量大約每小時更新一次，因此如果您在規則上設定應用程式後，看到的 ***Apps Allowed***（允許的應用程式）數量沒有預期中多，請在大約一小時後重新查看。視乎防火牆的負載，這些欄位可能需要超過一小時才會更新。

STEP 2 | 確定優先修改哪些設有未使用應用程式的規則。

Policies（原則） > **Security**（安全性） > **Policy Optimizer**（原則最佳化工具） > **Unused Apps**（未使用的應用程式） 讓您 排序規則，而不影響其在規則庫中的順序，並提供其他資訊，幫助您根據業務目標和風險容忍能力確定清除規則的優先順序。

- **Apps Allowed**（允許的應用程式）（允許清單上的應用程式數量）和 **Apps Seen**（看見的應用程式）（規則上實際看見的允許的應用程式數）之間的差值顯示各規則上設定但並未實際看見的應用程式數量，這表示過度佈建規則的程度。按一下 **Apps Allowed**（允許的應用程式）以按規則中允許的應用程式數量排序，按一下 **Apps Seen**（看見的應用程式）以按規則上實際看見的應用程式數量排序。
- **Days with No New Apps**（沒有新應用程式的天數）（按一下以排序）顯示自上次新應用程式命中規則以來的天數。這表示規則成熟的可能性，且不會看見任何尚未看見的應用程式。**Days with No New Apps**（沒有新應用程式的天數）越長，新應用程式命中規則的可能性就越小，而您知道規則允許的所有應用程式的可能性就越大。
- **Created**（建立）和 **Modified**（修改）日期還有助於確定規則是否足夠成熟，以瞭解規則中未看見的應用程式是否會在以後看見，或規則是否已看見所有預計會命中規則的應用程式。規則 **Modified**（修改）後的時間越長，規則成熟的可能性就越大。（如果 **Created**（建立）和 **Modified**（修改）日期相同，表示規則未經過修改。）

©2024 Palo Alto Networks, Inc.

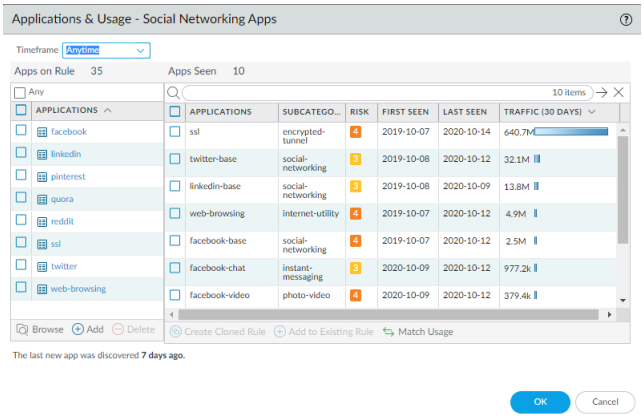
- **Hit Count**（命中數）—顯示所選時間範圍內具有最多相符項的規則。您可排除重設命中計數器的規則，並指定排除時間（天）。排除最近重設命中計數器的規則，可以防止顯示命中數低於預期的規則出現錯誤，因為您不知道計數器已重設。

  您還可使用 ***Hit Count***（命中數）以檢視原則規則使用情況。

您還可按一下 **Traffic (Bytes, 30 days)**（流量 （位元組，**30** 天）），以按規則過去 30 天看見的流量排序。使用此資訊確定優先修改哪些規則。例如，您可優先處理 **Apps Allowed**（允許的應用程式）和 **Apps Seen**（看見的應用程式）之間差異最大且 **Days with No New Apps**（沒有新應用程式的天數）最大的規則，因為這些規則擁有的未使用應用程式數量最多且最成熟。

STEP 3 | 檢閱規則上 **Apps Seen**（看見的應用程式）。

在 **Unused Apps**（未使用的應用程式）上，按一下 **Compare**（比較）或 **Apps Seen**（看見的應用程式）欄中的數字，以開啟 **Applications & Usage**（應用程式與使用情況），其顯示規則上設定的應用程式（**Apps on Rule**（規則上的應用程式））與規則上 **Apps Seen**（看見的應用程式）。

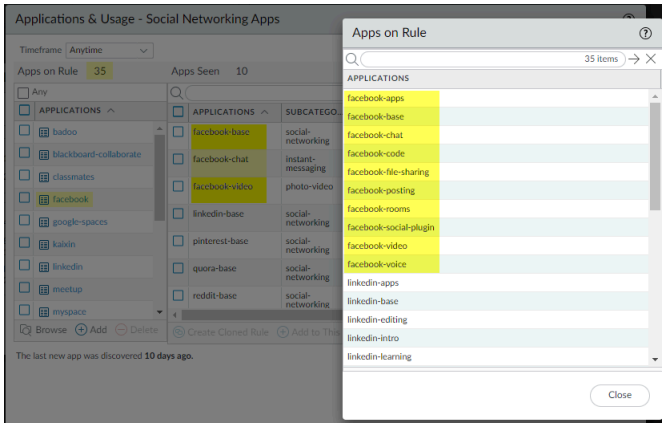


- **Apps Seen**（看見的應用程式）旁邊的數字（本範例中為 10）表示符合規則的應用程式數量。請記住，防火牆更新 **Apps Seen**（看見的應用程式）至少需要一小時。
- **Apps on Rule**（規則上的應用程式）旁邊的數字（本範例中為 35）表示規則上設定的應用程式數量，其透過對容器應用程式中各應用程式進行計數計算得出（但不是容器應用程式本身—如果在規則上設定容器應用程式，規則將允許容器應用程式的個別應用程式）。因為 **Applications**（應用程式）清單僅顯示您在規則上手動設定的應用程式，當您在規則上設定容器應用程式時，**Applications**（應用程式）將僅顯示容器應用程式，而不顯示容器中的個別應用程式（除非也在規則上手動設定個別應用程式）。基於此原因，**Apps on Rule**（規則上的應用程式）數量可能與 **Applications**（應用程式）清單中看到的應用程式數量不同。
- 按一下 **Apps on Rule**（規則上的應用程式）旁邊的數字查看規則上所有個別應用程式。

  此範例規則具有 10 個 **Apps Seen**（看見的應用程式）（符合規則的應用程式），但允許 35 個 **Apps on Rule**（規則上的應用程式）。規則上設定了 **facebook** 容器應用程式，該規則查看來自個別應用程式 facebook-base、facebook-chat 和 facebook-video（**Apps Seen**（看見的應用程式））的流量。當您按一下 **Apps on Rule**（規則上的應用程式）數字時，**Apps on**

©2024 Palo Alto Networks, Inc.

Rule（規則上的應用程式）對話方塊顯示允許的個別應用程式，但不顯示容器應用程式本身。



您將無法從快顯對話方塊中新增或刪除應用程式。

將規則上 **Apps Seen**（看見的應用程式） 與 **Apps on Rule**（規則上的應用程式）進行比較。如果規則上的應用程式未使用（您沒有看到應用程式或您在 **Apps Seen**（看見的應用程式）的允許容器中沒有看到應用程式），則考慮將該應用程式從規則上移除以減少攻擊面。將定期使用的應用程式納入考量，例如用於季度或年度事件的應用程式，因為如果不在一個足夠長的時間範圍內進行檢查的話，這類應用程式可能看起來像沒有使用過一樣。**Timeframe**（時間範圍）讓您可為規則上 **Apps Seen**（看見的應用程式）選取時間範圍。選取 **Anytime**（任何時間）以查看在規則生命週期內看到的每個應用程式。根據 **No App Specified**（無指定的應用程式）對話方塊中的 **Created**（建立）或 **Modified**（修改）日期及定期事件之間的時間，規則在防火牆上的時間可能不夠長，無法查看所有定期使用的應用程式。

STEP 4 | 從規則中移除未使用應用程式。

在 **Apps on Rule**（規則上的應用程式）中 **Delete**（刪除）（或 **Add**（新增））應用程式以手動移除（或新增）應用程式，或 **Match Usage**（比對使用）以在規則上新增 **Apps Seen**（看見的應用程式），或一鍵刪除規則上沒有看見相符流量的應用程式。

若要從規則中手動移除應用程式，請從 **Apps on Rule**（規則上的應用程式）中選取應用程式，並將其 **Delete**（刪除）。在將其從規則上移除前，請確保定期事件不需要任何此類應用程式。（您還可以在安全性原則規則的 **Application**（應用程式）頁簽上新增或刪除應用程式。）

Match Usage（比對使用）可將規則上 **Apps Seen**（看見的應用程式）移至 **Apps on Rule**（規則上的應用程式），然後從規則中移除所有未使用的應用程式。

您可將規則從 ***Policies***（政策） > ***Security***（安全性）及從 ***No App Specified***（無指定的應用程式）複製到從基於連接埠的安全性原則規則移轉至基於 App-ID 的安全性原則規則。您無法從 ***Unused Apps***（未使用的應用程式）開始複製規則。

STEP 5 | **Commit**（提交）組態。

©2024 Palo Alto Networks, Inc.

STEP 6 | 監控更新的規則並傾聽使用者回饋，以確保更新的規則允許您要允許的應用程式，避免無意中封鎖定期使用的應用程式。

> ***Apps Allowed***（允許的應用程式） 和 ***Apps Seen***（看見的應用程式）數量大約每小時更新一次。當您從規則中移除所有未使用的應用程式後，規則將仍保留在 ***Policies***（規則） > ***Security***（安全性） > ***Policy Optimzer***（規則最佳化工具） > ***Unused Apps***（未使用的應用程式）中，直至防火牆更新顯示。當防火牆更新顯示且 ***Apps Allowed***（允許的應用程式）數量與 ***Apps Seen***（看見的應用程式）數量相同時，規則將不再顯示於 ***Unused Apps***（未使用的應用程式）畫面中。但是，根據防火牆的負載，更新這些欄位可能會超過一小時。

應用程式使用統計資料的高可用性

將兩個防火牆設為高可用性 (HA) 配對時，應用程式使用統計資料位於產生應用程式流量日誌的防火牆本機上。檢視應用程式使用統計資料的位置也在一定程度上取決於 HA 組態：

- 主動/被動—主動裝置產生應用程式使用統計資料。如果被動裝置沒有偵測到使用者流量，則僅主動裝置顯示應用程式使用統計資料。如果被動裝置偵測到使用者流量，則被動裝置僅顯示其偵測到的流量之應用程式使用統計資料。

  進行容錯轉移時，應用程式使用統計資料僅以新主動裝置產生的流量日誌為基礎（裝置在容錯轉移之前為被動狀態）。
- 主動/主動—擁有工作階段的裝置會為該工作階段產生流量日誌，因此僅擁有工作階段的裝置才會提供工作階段的應用程式使用統計資料。如果一個主動裝置擁有工作階段，另一個主動裝置不會顯示該工作階段的應用程式使用統計資料。

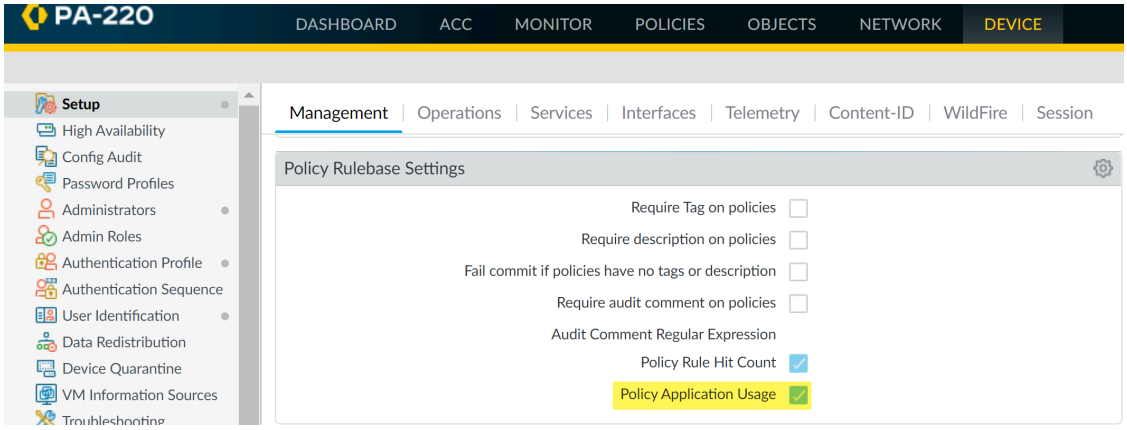
如何停用原則最佳化工具

依預設會啟用原則最佳化工具。政策最佳化工具提供多種功能，方便您輕鬆從基於連接埠的安全性原則規則移轉至基於 App-ID 的安全性原則規則和透過未使用的應用程式識別安全性原則規則，並移除規則中未使用的應用程式，但您可在必要時將其停用。

STEP 1 | 導覽至 **Device**（裝置） > **Setup**（設定） > **Management**（管理） > **Policy Rulebase Settings**（原則規則庫設定）。

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 選取 **Policy Application Usage**（原則應用程式使用方式）核取方塊以啟用此功能，取消選取該核取方塊以停用此功能。



 ©2024 Palo Alto Networks, Inc.

App-ID 雲端引擎

App-ID 雲端引擎 (ACE) 服務可讓防火牆或 Panorama 從雲端為 Palo Alto Networks 內容更新團隊沒有提供具體預先定義 App-ID 的應用程式下載 App-ID。ACE 為應用程式提供特定的 App-ID，否則防火牆會將其標識為 ssl 或 web-browsing。在安全性政策規則中使用 ACE App-ID 來瞭解雲端應用程式並對其進行控制。使用政策最佳化工具在安全性政策中新增和管理應用程式。您不能在任何其他類型的原則規則中使用 ACE App-ID。ACE：

- 大大增加了已知 App-ID 的數量，以識別和控制更多雲端應用程式，並且隨著 ACE 為應用程式定義新的 App-ID，ACE App-ID 在防火牆上變得可用。
- 加快新 App-ID 到防火牆的可用性和傳遞速度。
- 透過在安全性原則規則中使用應用程式篩選器，加快並自動將應用程式新增至安全性原則。
- 大幅增加對之前識別為 ssl 或 web-browsing 之應用程式的可見性。

ACE 需要 SaaS 安全性內嵌訂閱。每個使用 *ACE* 的設備都必須安裝有效的裝置憑證。

支援 *PAN-OS 10.1* 或更高版本的所有硬體平台都支援 *ACE*，您想要在其上使用 *ACE* 的所有設備都需要安裝 *PAN-OS 10.1* 或更高版本。*Panorama* 無法將基於 *ACE* 的原則或物件推送並提交到沒有安裝 *SaaS* 安全性內嵌授權的防火牆或執行的 *PAN-OS* 版本低於 *10.1* 的防火牆。

ACE 在美國、亞太地區和歐盟 *GCP* 地區受支援。系統會根據您的 *CDL* 地區自動選取區域。

確認防火牆使用適用於您所在區域的正確內容雲端 *FQDN*（***Device***（裝置） > ***Setup***（設定） > ***Content-ID***（內容 ***ID***） > ***Content Cloud Setting***（內容雲端設定）），並視需要變更 *FQDN*：

- 美國—***hawkeye.services-edge.paloaltonetworks.com***
- 歐盟—***eu.hawkeye.services-edge.paloaltonetworks.com***
- 亞太地區—***apac.hawkeye.services-edge.paloaltonetworks.com***

包括流量有效負載在內的 *ACE* 資料會傳送至所選區域的伺服器。如果您指定了所在區域之外的內容雲端 *FQDN*（例如，如果您位於歐盟區域，但指定了亞太地區的 *FQDN*），則可能會違反您所在國家或組織的隱私權和法律規定。

預先定義的內容傳遞 App-ID 每月會提供一次新的應用程式，您需要先分析新 App-ID，然後再安裝它們，以瞭解它們可能對安全性政策規則所做的變更。每月一次的節奏和分析需求會減慢原則中採用新 App-ID 的速度。儘管 Palo Alto Networks 將繼續透過每月內容更新提供您需要檢閱的新

©2024 Palo Alto Networks, Inc.

App-ID，但 ACE 會透過為初始識別為以下兩種類型之一的應用程式提供隨選 App-ID，從而提高新 App-ID 的採用：

- **ssl**—加密 SSL 流量是迄今為止最常見的網路流量類型，大多數專家聲稱它超過總流量的 90%。如果您沒有或無法解密該流量，防火牆通常只能將其識別為 ssl，而不是實際的基礎應用程式。
- **web-browsing** — 防火牆無法專門識別某些未加密 (web-browsing) 流量，因為每月內容交付的 App-ID 更新跟不上每天開發的所有新應用程式。

ACE 提供對這些應用程式的具體標識，讓您能夠瞭解這些應用程式並在安全性政策中適當控制這些應用程式。

ACE App-ID 不會識別其他類型的公用應用程式，也不會識別私人和自訂應用程式。*ACE App-ID* 目錄不包含預先定義、內容提供的 *App-ID*。內容提供的 *App-ID* 仍然會在每月內容更新中送達。

當防火牆遇到 ssl 或 web-browsing 流量時，防火牆會將有效負載傳送到 ACE 進行分析。如果它與 ACE 資料庫中的 App-ID 匹配，則 ACE 會將 App-ID 傳回至要求的防火牆。如果 ACE 沒有與流量相符的 App-ID，ACE 會將有效負載傳送至機器學習 (ML) 引擎。ML 引擎會分析有效負載，並與人類內容團隊一起開發新的 App-ID。開發完成時，ML 引擎會將新的 App-ID 上傳到 ACE 資料庫，要求的防火牆（以及任何其他防火牆）可以下載 App-ID 並在安全性原則中使用它。

由於從 *ACE* 擷取已知應用程式可能需要幾分鐘時間，如果必須開發新 *App-ID* 則需要更長的時間，因此雲端應用程式偵測不會內嵌在防火牆上。防火牆不會等待裁定來處理應用程式流量。防火牆將流量作為 *ssl* 或 *web-browsing* 進行處理，直到它從 *ACE* 收到 *App-ID* 並且您在安全性政策中使用它。

如果您在啟用 *ACE* 之後降級防火牆或 *Panorama*，且 *ACE* 雲端 *App-ID* 仍在安全性原則規則或應用程式群組中使用，則降級會失敗。失敗原因會列出需要從設定中移除才可降級的物件。從設定中移除這些物件並 ***Commit***（提交）設定，然後降級將成功。

- 準備部署 App-ID 雲端引擎
- 啟用或停用 App-ID 雲端引擎
- App-ID 雲端引擎處理和政策使用
- 新應用程式檢視器（原則最佳化工具）
- 使用原則最佳化工具將應用程式新增到應用程式篩選器
- 使用原則最佳化工具將應用程式新增到應用程式群組
- 使用原則最佳化工具將應用程式直接新增到規則
- 更換 RMA 防火牆 (ACE)
- 授權到期或停用 ACE 的影響
- 由於雲端內容回復而提交失敗
- 對 App-ID 雲端引擎進行疑難排解

©2024 Palo Alto Networks, Inc.

準備部署 App-ID 雲端引擎

在防火牆能夠使用 App-ID 雲端引擎 (ACE) 之前，需要執行幾項必備的裝載工作。您可以在獨立防火牆上部署 ACE，或使用 Panorama 在受管理防火牆上部署 ACE。

在防火牆可以使用 ACE 為先前識別為 ssl 或 web-browsing 流量的流量提供具體 App-ID 之前，PAN-OS 管理員和 SaaS 安全性管理員必須合作，以便：

- 在將使用 ACE 的每個設備上安裝有效的裝置憑證，包括管理 ACE 防火牆的 Panorama 設備。（PAN-OS 管理員。）
- 在將使用 ACE 的每個防火牆上啟動 SaaS 安全性內嵌。Panorama 不需要授權。（SaaS 安全性管理員。）
- 設定在防火牆與 ACE 之間通訊的服務路由。（PAN-OS 管理員。）
- 在管理將使用 ACE 之防火牆的 Panorama 設備上啟用 ACE。（PAN-OS 管理員。）

  在防火牆上，*ACE* 預設會在啟動 *SaaS* 安全性內嵌之後啟用。

- 建立允許 ACE 流量的安全性原則規則。（PAN-OS 管理員。）
- 設定從防火牆到 Cortex Data Lake (CDL) 的日誌轉送。（PAN-OS 管理員。）

在下列程序的適當步驟中，*PAN-OS* 管理員應當通知 *SaaS* 安全性管理員，部署已就緒，可啟動 *SaaS* 安全性內嵌。啟動 *SaaS* 安全性內嵌之後，*SaaS* 安全性內嵌管理員應當通知 *PAN-OS* 管理員，部署已準備好在 *PAN-OS* 裝置上完成。管理員之間的通訊對於順利完成部署至關重要。

需求：

- 獨立防火牆、Panorama 設備和受管理防火牆必須執行 PAN-OS 11.0 或更新版本。
- 所有 ACE 防火牆都必須購買 SaaS 安全性內嵌授權。Panorama 不需要授權即可管理 ACE 防火牆或將 ACE 設定推送至受管理防火牆。
- 視乎您的位置，所有 ACE 設備都必須能夠連線至美國、亞太地區或歐盟 GCP 區域（會根據您的 CDL 區域自動選取區域）。

  確認防火牆使用適用於您所在區域的正確內容雲端 FQDN（**Device**（裝置） > **Setup**（設定） > **Content-ID**（內容 **ID**） > **Content Cloud Setting**（內容雲端設定）），並視需要變更 FQDN：

  - 美國—**hawkeye.services-edge.paloaltonetworks.com**
  - 歐盟—**eu.hawkeye.services-edge.paloaltonetworks.com**
  - 亞太地區—**apac.hawkeye.services-edge.paloaltonetworks.com**

  包括流量有效負載在內的 ACE 資料會傳送至所選區域的伺服器。如果您指定了所在區域之外的內容雲端 FQDN（例如，如果您位於歐盟區域，但指定了亞太地區的 FQDN），則可能會違反您所在國家或組織的隱私權和法律規定。

©2024 Palo Alto Networks, Inc.

PAN-OS 管理員完成程序的前兩個步驟，然後交給 SaaS 安全性內嵌管理員進行啟動（步驟 3）。啟動後，SaaS 安全性內嵌管理員將剩餘程序交回給 PAN-OS 管理員，以便在 PAN-OS 裝置上完成。

STEP 1 | 使防火牆和 Panorama（如果使用）上線。（PAN-OS 管理員。）

STEP 2 | 在個別防火牆上安裝裝置憑證，以便它們可以使用雲端服務或使用 Panorama 為受管理防火牆安裝裝置憑證。（PAN-OS 管理員。）

將下一個步驟交給 *SaaS* 安全性管理員。

STEP 3 | 在將使用 ACE 的每個防火牆上啟動 SaaS 安全性內嵌。啟動後會在防火牆上啟用 ACE。（SaaS 安全性管理員。）

Panorama 不需要 *SaaS* 安全性內嵌授權來管理使用 *ACE* 的防火牆。只有受管理的防火牆需要授權，您必須按下一步所示手動擷取。

將其餘步驟交給 *PAN-OS* 管理員。

STEP 4 | 在每個防火牆上擷取 SaaS 安全性內嵌授權（Panorama 不需要授權），並確認已啟動該授權。（PAN-OS 管理員。）

SaaS 安全性管理員的啟動會為防火牆設定授權，因此您不必前往客戶支援入口網站或獲取驗證碼。

1. 移至 **Device**（裝置）> **Licenses**（授權）> **License Management**（授權管理），然後選取 **Retrieve license keys from license server**（從授權伺服器擷取授權金鑰）以擷取授權。
2. 請檢查 **Device**（裝置）> **Licenses**（授權），以確保 SaaS 安全性內嵌授權處於作用中狀態。

STEP 5 | 設定資料服務（資料平面）服務路由，讓防火牆可以與 App-ID 雲端引擎通訊。（PAN-OS 管理員。）

您可以將此設定從 *Panorama* 推送至受管理防火牆。*Panorama* 和受管理防火牆都必須執行 *PAN-OS 11.0* 或更新版本。

依預設，防火牆會使用管理介面做為資料服務服務路由的來源介面，但建議您按照此步驟中的後續操作，設定具有雲端服務連線能力的資料平面介面作為資料服務的 **Source Interface**（來源介面）和 **Source Address**（來源位址）。

防火牆上的問題在於，如果在管理介面上設定了明確的 Proxy，且您將其用於資料服務服務路由，則管理介面只能連線至管理雲端應用程式和特徵碼的知識雲端服務 (KCS)。在管理介面上設定了明確的 Proxy 時，它無法連線至偵測雲端服務 (DCS)，該服務會根據現有的 ACE App-ID 來檢查應用程式有效負載並提供裁定。KCS 和 DCS 是 ACE 雲端中的服務。如果管理介面設定

©2024 Palo Alto Networks, Inc.

了明確的 Proxy，您無法將它用於 ACE 的資料服務服務路由，因為它無法連線到所有服務。在這種情況下，您必須使用防火牆上的資料平面介面來連線到資料服務。

Panorama 預設使用管理連接埠來連線到 *KCS*，且不會連線到 *DCS*。

要在資料平面介面上設定服務路由，而不是使用預設管理介面，請執行以下操作：

1. 選取 **Device**（裝置） > **Setup**（設定） > **Services**（服務），然後在 **Service Features**（服務功能）中選取 **Service Route Configuration**（服務路由設定）。
2. **Customize**（自訂）服務路由。
3. 選取 **IPv4** 通訊協定。
4. 按一下「服務」欄中的 **Data Services**（資料服務）開啟 **Service Route Source**（服務路由來源）對話方塊。
5. 選取 **Source Interface**（來源介面）和 **Source Address**（來源位址）（這些不能是管理介面）。

   來源介面必須具有網際網路連線。最佳做法是使用具有雲端服務連線能力的資料平面介面。請參閱設定介面和建立位址物件以獲取有關建立來源介面和位址的更多資訊。
6. 按一下 **OK**（確定）以設定來源介面和位址。
7. 按一下 **OK**（確定）以設定服務路由設定。
8. 選取 **Policies**（原則） > **Security**（安全性），然後新增 Security policy rule（安全性原則規則），該規則允許來自您之前在本程序中指定的來源介面的流量進入 KCS 和 DCS 服務的 FQDN 位址，這些位址為：**`kcs.ace.tpcloud.paloaltonetworks`**（所有區域的 KCS 服務）和 **`hawkeye.services-edge.paloaltonetworks.com`**（美國區域 DCS 服務）、**`eu.hawkeye.services-edge.paloaltonetworks.com`**（歐盟區域 DCS 服務）或 **`apac.hawkeye.services-edge.paloaltonetworks.com`**（亞太區域 DCS 服務）。

   還需在新的或現有安全性原則規則中新增並允許以下兩個 FQDN：用於憑證驗證的 **`ocsp.paloaltonetworks.com`** 和 **`crl.paloaltonetworks.com`**。

   最後，新增或修改安全性原則規則，透過允許下列三個應用程式來允許 ACE 流量：**`paloalto-ace`**、**`paloalto-ace-kcs`** 和 **`paloalto-dlp-service`**。

STEP 6 | 確保可從防火牆上存取 hawkeye.services-edge.paloaltonetworks.com 和 kcs.ace.tpcloud.paloaltonetworks，以及可從 Panorama 裝置上存取 kcs.ace.tpcloud.paloaltonetworks。（PAN-OS 管理員。）

執行操作命令 `admin@fw1> show cloud-appid connection-to-cloud`。其輸出會告知您連線是否正常運作，以及授權是否已安裝。

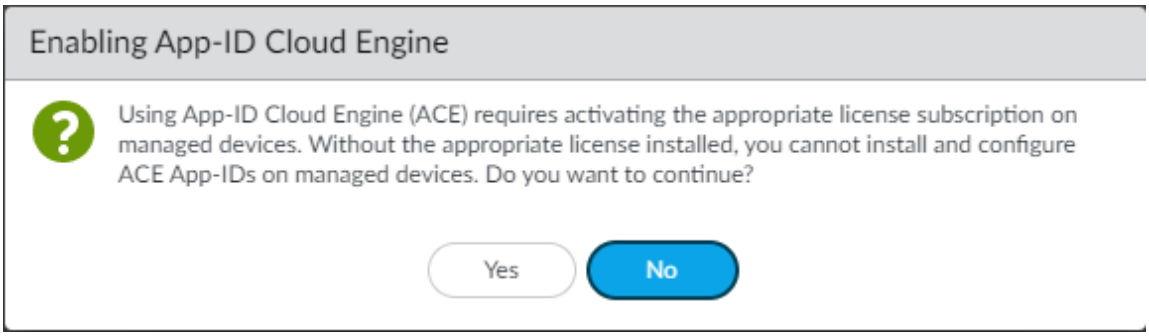
©2024 Palo Alto Networks, Inc.

STEP 7 | （僅限 Panorama）在任何管理已啟用 ACE 之防火牆的 Panorama 設備上啟用 ACE。（PAN-OS 管理員。）

在 Panorama 上，ACE 預設為停用。

如果您將 *ACE* 設定推送至沒有已啟用 *ACE* 之防火牆的受管理群組（群組中的部分或所有防火牆未啟用 *ACE*），則推送會失敗。

1. 導覽至 **Panorama** > **Setup**（設定) > **ACE** > **Settings**（設定）。
2. 按一下編輯 ( )，然後取消選取 **Disable App-ID Cloud Engine**（停用 **App-ID** 雲端引擎）。
3. 按一下 **OK**（確定）。
4. 會顯示 **Enable App-ID Cloud Engine**（啟用 **App-ID** 雲端引擎）對話方塊。



按一下 **Yes**（是） 以啟用 ACE。

5. **Commit**（提交）變更。

STEP 8 | 等待下載 App-ID 目錄。（PAN-OS 管理員。）

內容提供的 App-ID 不到四千個。下載 ACE 目錄之後，您會在防火牆上看到數以千計的應用程式，並且可以透過檢查 **Objects**（物件） > **Applications**（應用程式） 或使用操作 CLI 命令 `show cloud-appid cloud-app-data application all` 來確認，以查看新的 App-ID。

STEP 9 | （僅限 Panorama）將所需的設定推送到受管理防火牆。（PAN-OS 管理員。）

STEP 10 | 設定日誌轉送至 Cortex Data Lake (CDL)，並在安全性原則規則中使用正確的日誌轉送設定檔啟用日誌轉送。（PAN-OS 管理員。）

需要到 CDL 的 SaaS 安全性內嵌連線才能獲取 *SaaS* 可視性以及支援 SaaS App-ID 原則建議。至少，您必須將流量日誌和 *URL* 日誌轉送至 *CDL*，*SaaS* 安全性內嵌才能正常運作。

啟用或停用 App-ID 雲端引擎

App-ID 雲端引擎 (ACE) 在 Panorama 上預設停用，並在安裝 SaaS 安全性內嵌授權的防火牆上預設啟用。您必須在管理啟用 ACE 之防火牆的 Panorama 設備上啟用 ACE。

©2024 Palo Alto Networks, Inc.

要啟用或停用 ACE：

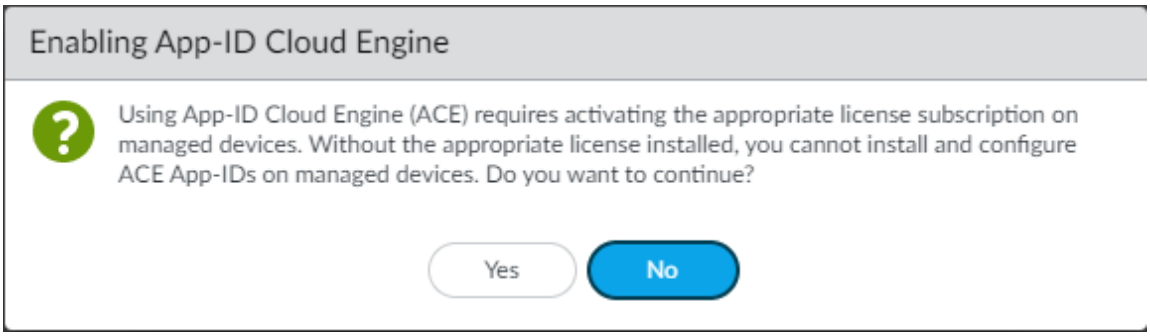
STEP 1 | 導覽到防火牆上的 **Device**（裝置） > **Setup**（設定） > **ACE** > **Settings**（設定），或導覽到 Panorama 上的 **Panorama** > **Setup**（設定） > **ACE** > **Settings**（設定）。

STEP 2 | 按一下編輯 ()，然後取消選取 **Disable App-ID Cloud Engine**（停用 **App-ID** 雲端引擎）以啟用 ACE 或選取 **Disable App-ID Cloud Engine**（停用 **App-ID** 雲端引擎）以停用 ACE。

ACE 預設為停用。

STEP 3 | 按一下 **OK**（確定）。

STEP 4 | （僅當啟用 ACE 時）如果您啟用 ACE，則會顯示 **Enable App-ID Cloud Engine**（啟用 **App-ID** 雲端引擎）對話方塊。



如果防火牆或 Panorama 管理的防火牆安裝了 SaaS 安全性內嵌授權，則按一下 **Yes**（是）以啟用 ACE。

STEP 5 | **Commit**（提交）變更。

App-ID 雲端引擎處理和政策使用

當防火牆下載 App-ID 雲端引擎 (ACE) App-ID，務必要瞭解防火牆如何處理 ACE App-ID，以及當相同應用程式同時存在基於內容的預先定義 App-ID 時，防火牆如何處理 ACE App-ID。Palo Alto Networks 內容團隊開發了基於內容的預先定義 App-ID，並透過應用程式內容更新使用修改後的新 App-ID 進行更新（更新需要有效的支援合約）。

ACE 需要 SaaS 安全性內嵌授權。不支援 ACE 的防火牆僅擁有基於內容的預先定義 App-ID。ACE App-ID 目錄不包含基於內容的 App-ID。

您只能在安全性原則規則中使用 *ACE App-ID*。您不能在任何其他類型的原則規則中使用 *ACE App-ID*。

- 當防火牆首次連線到 ACE 時，防火牆會下載可用的 ACE App-ID 目錄，您可以在安全性政策中使用這些 App-ID。防火牆不下載完整的應用程式簽名，只下載目錄。即使防火牆上從未看到過

©2024 Palo Alto Networks, Inc.

應用程式，該目錄也允許您在安全性政策中指定 ACE App-ID。ACE 定期將目錄更新推送到防火牆，以便防火牆能夠存取最新的 ACE App-ID。

如果到達防火牆的應用程式被識別為 ssl 或 web-browsing，且防火牆沒有其特徵碼，則防火牆會將有效負載傳送到 ACE。如果 ACE 具有匹配的 App-ID，則 ACE 會將完整的特徵碼傳送回防火牆。如果流量與任何 ACE 特徵碼都不符，則 ACE 會將有效負載傳送到機器學習 (ML) 引擎。ML 引擎會分析有效負載，並與人類內容團隊一起開發新的 App-ID。ML 引擎將新的 App-ID 傳送到 ACE，要求防火牆可以下載它並在安全性原則中使用。

由於從 *ACE* 擷取 *App-ID* 可能需要幾分鐘時間，如果必須開發新 *App-ID* 則需要更長的時間，因此雲端應用程式偵測不會內嵌在防火牆上。防火牆不會等待裁定來處理應用程式流量。防火牆將流量作為 *ssl* 或 *web-browsing* 進行處理，直到它從 *ACE* 收到 *App-ID* 並且您在安全性政策中使用它。

- 當防火牆從 ACE 請求 App-ID 時，防火牆會繼續根據當前規則庫處理流量，直到它從 ACE 收到 App-ID 並且 App-ID 被套用到安全性政策中。
- 防火牆處理 ACE App-ID 的方式與它處理內容更新交付之 App-ID 的方式有所不同。在將新的 ACE App-ID 安裝到防火牆上之前，您不必檢查其對安全性政策的影響，因為防火牆會根據您的現有安全性政策處理新 ACE App-ID。您現有的安全性政策規則將控制新的 ACE App-ID，直到您在安全性政策中明確使用 ACE App-ID。例如：

  1. 應用程式僅被識別為「ssl」，並且您有一個安全性原則規則允許 SSL 流量，則 ssl 規則會允許該應用程式。
  2. 防火牆看到標識為 ssl 的應用程式並將有效負載傳送到 ACE。
  3. ACE 識別實際應用程式。如果應用程式存在於 ACE 資料庫中，則 ACE 會將其 App-ID 傳送到防火牆。如果它是沒有 ACE App-ID 的新應用程式，那麼 ACE 會將有效負載轉送給 ML 引擎。在 ML 引擎和人類內容團隊指派 App-ID 並將其傳送到 ACE 之前，防火牆不會接收 App-ID。
  4. 允許 ssl 流量的規則仍然允許新識別的應用程式，即使其 App-ID 不再是「ssl」。（但是，如果您在安全性原則中使用新的 ACE App-ID，該原則將控制流量。同樣，之前被識別為 web-browsing 的流量繼續遵守控制 web browsing 流量的安全性政策規則，直到您在安全性政策中使用 ACE App-ID。）

     此行為的例外狀況是，另一個安全性政策規則已經指定了由 ACE 提供給流量的 App-ID。具有具體 App-ID 的安全性原則規則優先於 ssl App-ID 不太具體的規則。例如，如果防火牆將應用程式識別為 ssl 並將有效負載傳送到 ACE 以獲取精確 App-ID。ACE 傳回 App-ID「app-abc」。防火牆已有允許 App-ID「app-abc」的安全性政策規則，因此應用程式的流量現在與該規則匹配。

     如果指定實際 App-ID 的規則是封鎖規則，則即使存在允許 ssl 流量的規則，應用程式也會被封鎖。具有更具體（詳盡）App-ID 的規則是防火牆作為依據採取動作的規則。

在您明確新增 ACE App-ID 至安全性政策規則之前，防火牆會使用在應用程式擁有 ACE App-ID 之前控制這些應用程式的相同規則來控制它們，並將其識別為 ssl 或 web-browsing 流量。例如，如果防火牆看到被識別為 web-browsing 的應用程式，然後收到該流量的 ACE App-ID，但您沒有在安全性政策規則中使用該 ACE App-ID，則防火牆仍然使用控制 web-browsing 流

©2024 Palo Alto Networks, Inc.

量的規則控制該流量——如果您封鎖 web-browsing 流量，則該流量被封鎖，如果您允許 web-browsing 流量，則允許該流量。

- 防火牆會快取一些資訊，以便防火牆可以避免反覆向雲端傳送資料並要求裁定。如果防火牆正在等待 ACE 的裁定，則防火牆不會兩次轉送相同的應用程式資料。
- 在防火牆上，特定的容器應用程式及其功能應用程式要麼全部是基於雲端的 App-ID，要麼全部是基於內容的 App-ID。一種 App-ID 傳遞方法定義了容器應用程式及其所有功能應用程式。
- 如果基於雲端、內容提供和使用者定義的自訂 App-ID 名稱重疊，優先順序為：
  1. 自訂 **App-ID** — 這些 App-ID 優先權高於所有其他 App-ID。如果防火牆嘗試下載具有相同 App-ID 的 ACE 應用程式，則提交將失敗，因為同一防火牆上的兩個應用程式不能具有相同的 App-ID。

     在這種情況下，您可以重新命名自訂應用程式，或者如果自訂應用程式與 ACE 應用程式為同一應用程式，您可以刪除自訂應用程式並使用 ACE 應用程式。
  2. 基於內容的預先定義 **App-ID**—這些 App-ID 優先於 ACE 雲端 App-ID 定義。
  3. **ACE** 雲端 **App-ID**—自訂和基於內容的 App-ID 優先於 ACE App-ID 定義。
- 如果 App-ID 與容器應用程式相符，則防火牆會下載容器應用程式的 App-ID 及其所有功能應用程式。例如，如果防火牆擷取 facebook 容器應用程式，它還會擷取 facebook-base、facebook-chat、facebook-post 等。
- 當您採取以下任何動作將 ACE App-ID 新增到安全性政策規則時，防火牆不再將應用程式流量與 ssl 或 web-browsing 規則進行匹配，而是將應用程式流量與控制特定 App-ID 的規則進行匹配：
  - 建立應用程式篩選器，以便自動將 ACE App-ID 新增到安全性原則。

    使用應用程式篩選器自動將 *ACE App-ID* 新增到安全性原則規則。當新 *App-ID* 與應用程式篩選器相符時，防火牆會自動將其新增到篩選器。當您在安全性原則規則中使用該應用程式篩選器時，該規則會控制自動新增到篩選器中的新 *App-ID* 的應用程式流量。應用程式篩選器是您的「輕鬆按鈕」，用於自動保護 *ACE App-ID*，以便以最少的努力獲得最大的應用程式可見性和控制權。
  - 將 ACE App-ID 新增到應用程式群組。
  - 使用政策最佳化工具將 ACE App-ID 新增到複製的規則或現有規則中，或新增到現有的應用程式篩選器或應用程式群組。您可以使用原則最佳化工具直接從原則最佳化工具中建立新的應用程式篩選器和應用程式群組。使用原則最佳化工具的排序和篩選工具，為要執行的規則設定優先順序，並評估有多少 ACE App-ID 與這些規則相符。
  - 將 ACE App-ID 直接新增到新的或現有安全性原則規則。

  當您直接、使用應用程式篩選器或使用應用程式群組將雲端 App-ID 新增到安全性原則規則時，該規則將控制應用程式。
- 當您建立應用程式篩選器時，請從篩選器中排除 ssl 和 web-browsing。ssl 和 web-browsing 結合起來與所有基於瀏覽器的雲端應用程式相符，因此包含 ssl 和 web-browsing 的應用程式篩選器與所有基於瀏覽器的雲端應用程式相符。

©2024 Palo Alto Networks, Inc.

- 主動/被動高可用性：
  - 主動防火牆將 ACE 目錄同步到被動防火牆，以便它們具有相同的目錄。
  - 被動防火牆在成為主動防火牆之前不會啟動與 ACE 的連線。
- 主動/主動高可用性：每個裝置分別擷取目錄和特徵碼，因此目錄和特徵碼不會同步。但是，如果目錄在對等上不同步，且安全性原則規則中引用了 ACE App-ID，則提交將失敗。如果對等 HA 防火牆的目錄不同步，請等待幾分鐘，以便更新到達裝置並再次實現同步。
- 如果發生以下情況，Panorama 會提交全部/推送故障到受管理防火牆：
  - 受管理防火牆沒有有效的 SaaS 安全性內嵌授權，因此沒有 ACE 目錄。在這種情況下，請從推送的設定中移除 ACE 物件，然後重試。
  - 受管理防火牆和 ACE 之間的連線會中斷，推送的設定包括不在防火牆上 ACE 目錄中的應用程式。在這種情況下，檢查防火牆與 ACE 雲端的連線，並在必要時重新建立連線，以便防火牆可以更新其目錄。

    CLI 操作命令 `show cloud-appid connection-to-cloud` 提供雲端連線狀態和 ACE 雲端伺服器 URL。
  - Panorama 上的 ACE 目錄和受管理防火牆上的 ACE 目錄不同步，這導致推送的設定包含不在防火牆目錄中的 ACE 應用程式。如果防火牆和 ACE 之間的連線為啟動，則過時的目錄將在未來幾分鐘內自動更新並解決問題。（請等待五分鐘，然後重試。）

    您可以使用 *CLI* 命令 *`debug cloud-appid cloud-manual-pull check-cloud-app-data`* 手動更新目錄。
- 一些安全性設定檔（如檔案封鎖、防毒、WildFire 和 DLP 設定檔）可以指定應用程式作為設定檔的一部分。安全性設定檔中僅支援內容提供的 App-ID。安全性設定檔中不支援 ACE App-ID。ACE App-ID 僅用於安全性原則規則。
- 由於 ACE App-ID 僅受安全性原則支援，因此在應用程式覆寫、基於原則的轉送 (PBF)、QoS 或 SD-WAN 原則規則中不受支援。

在應用程式覆寫或 *PBF* 規則設定中，您看不到 *ACE App-ID*。但是，*ACE App-ID* 在 *QoS* 和 *SD-WAN* 原則規則設定中可見（能夠選取），且可能存在於套用至規則的應用程式群組或應用程式篩選器中。如果您在這些規則中使用 *ACE App-ID*，則該原則不會控制應用程式流量，且對應用程式流量沒有影響—即使 *ACE App-ID* 新增到規則中，該規則也不會套用至 *ACE App-ID* 流量。

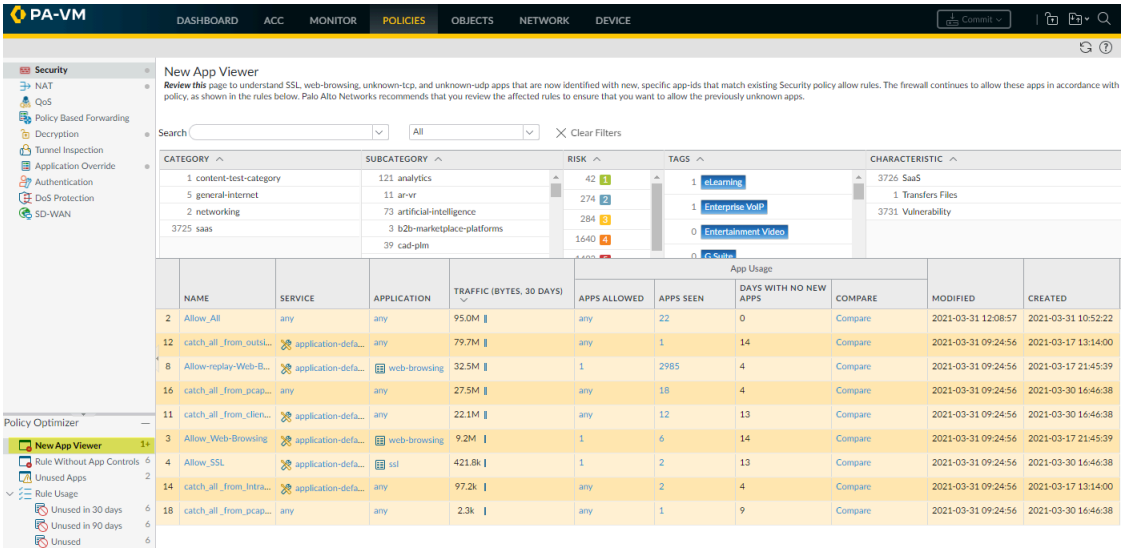
新應用程式檢視器（原則最佳化工具）

原則最佳化工具**New App Viewer**（新應用程式檢視器）顯示與從 ACE 下載的雲端 App-ID 相符的安全性原則規則。使用政策最佳化工具管理新識別的應用程式並將其新增到複製的規則或現有規則中。選擇 **Policies**（政策）> **Security**（安全性），然後在介面的 **Policy Optimizer**（政策最佳化工具）中選擇 **New App Viewer**（新應用程式檢視器）。

螢幕的上半部分類似於 **Objects**（物件）> **Application Filters**（應用程式篩選器）。它以類似的方式運作並篩選螢幕下半部分顯示的安全性原則規則。您可以按類別、子類別等篩選允許應用程式的

規則。只有與螢幕下半部分所列規則上的新應用程式相符的類別和子類別可用於篩選，因此您不必浪費時間篩選不在其中的應用程式。

篩選規則時，只有包含篩選出的應用程式的規則才會顯示在螢幕下半部分。其應用程式不在篩選器中的規則會從清單中移除。（您可以透過移除篩選器再次看到它們。）



按一下 **Apps Seen**（看見的應用程式）欄中的數字以開啟 **Applications & Usage**（應用程式與使用方式）對話方塊，以變更防火牆處理安全性原則中基於雲端的應用程式的方式。使用應用程式篩選器、應用程式群組、原則最佳化工具將 ACE App-ID 新增到安全性原則規則，或直接將 ACE App-ID 新增到規則。在您採取以下動作之一來控制雲端傳遞的 App-ID 之前，防火牆會繼續將流量視為 ssl 或web-browsing 流量，並使用現有的 ssl 或 web-browsing 安全性政策規則控制應用程式。

使用原則最佳化工具將應用程式新增到應用程式篩選器

將來自 App-ID 雲端引擎 (ACE) 的 App-ID 新增到應用程式篩選器，以自動將雲端 App-ID 新增到安全性政策。當新 ACE App-ID 與應用程式篩選器相符時，防火牆會自動將其新增到篩選器。當您在安全性原則規則中使用應用程式篩選器時，該規則會在新 ACE App-ID 到達防火牆並新增到篩選器中時自動控制它們。

ACE 為之前識別為 *ssl* 或 *web-browsing* 的應用程式提供 *App-ID*。

使用應用程式篩選器是最佳做法，因為它們：

- 可改善您的安全狀態。應用程式篩選器會自動將新的 ACE App-ID 新增到您專門設計用於處理特定類型應用程式流量的安全性政策規則，而不是將流量與更通用的 ssl 或 web-browsing 規則進行比對。
- 節省時間。防火牆管理員可以設定應用程式篩選器來處理不同類型的流量，因此新增新 ACE App-ID 到原則是一個自動化過程，無需管理員採取更多操作。

©2024 Palo Alto Networks, Inc.

當您建立應用程式篩選器時，請從篩選器中排除 *ssl* 和 *web-browsing*。*ssl* 和 *web-browsing* 結合起來與所有基於瀏覽器的雲端應用程式相符，因此包含 *ssl* 和 *web-browsing* 的應用程式篩選器與所有基於瀏覽器的雲端應用程式相符。

使用政策最佳化工具將 ACE App-ID 新增到應用程式篩選器中，並將篩選器套用至安全性政策規則。

STEP 1 | 移至 **Policies**（原則） > **Security**（安全性），然後選取 **Policy Optimizer**（原則最佳化工具） > **New App Viewer**（新應用程式檢視器）。

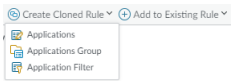
如果防火牆識別到具有 ACE App-ID 的流量，則左側導覽視窗中的 **New App Viewer**（新應用程式檢視器）旁邊會顯示一個數字，表明有多少規則匹配 ACE App-ID。此螢幕會顯示符合雲端 App-ID 的安全性原則規則。

STEP 2 | 按一下安全性政策規則的 **Apps Seen**（看見的應用程式）中的數字，即可檢視與 **Applications & Usage**（應用程式與使用情況）對話方塊中的規則相符的雲端傳遞應用程式。

STEP 3 | 選取您要新增至現有或新應用程式篩選器的應用程式。

您可以按子類別、風險、過去 30 天看到的流量或者應用程式第一次或最後上線時間對應用程式來對 **Apps Seen**（看見的應用程式）中的應用程式進行排序和篩選。

STEP 4 | 依據您要處理應用程式的方式，從 **Create Cloned Rule**（建立複製的規則）或 **Add to Existing Rule**（新增至現有規則）中選取 **Application Filter**（應用程式篩選器）。



您可以使用 ***Create Cloned Rule***（建立複製的規則）複製的應用程式數目上限為 *1,000* 個應用程式。如果您想要移至另一規則的應用程式超過 *1,000* 個，請改用 ***Add to Existing Rule***（新增至現有規則）。如果您要將應用程式移至新規則，僅需先建立規則（***Policies***（原則） > ***Security***（安全性）），然後使用原則最佳化工具將其新增至該規則即可。

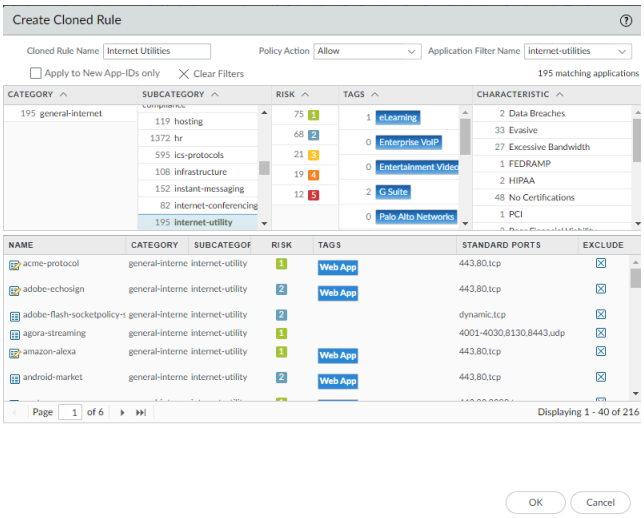
STEP 5 | 選擇或建立應用程式篩選器。使用原則最佳化工具建立應用程式篩選器與使用 **Objects**（物件） > **Application Filters**（應用程式篩選器）建立應用程式篩選器的過程幾乎完全相同——

©2024 Palo Alto Networks, Inc.

二者使用相同的篩選工具和選項。此步驟向您展示如何先使用政策最佳化工具建立複製版本，然後新增到現有規則。

建立複製的規則：

1. 輸入 **Cloned Rule Name**（複製的規則之名稱）（複製的規則之名稱，此名稱會立即顯示在安全性原則規則庫中，位於原始規則的上方）。
2. 選取 **Policy Action**（原則動作）（允許或拒絕）。
3. 從功能表中選取 **Application Filter Name**（應用程式篩選器名稱）或輸入新應用程式篩選器的名稱。
4. 選取篩選器應 **Apply to New App-IDs only**（僅套用至新 **App-ID**）還是應套用至所有 App-ID。
5. 使用類別、子類別、風險、標籤和特性值來篩選要新增到應用程式篩選器的應用程式類型。防火牆會自動將符合篩選器條件的新應用程式新增到應用程式篩選器。

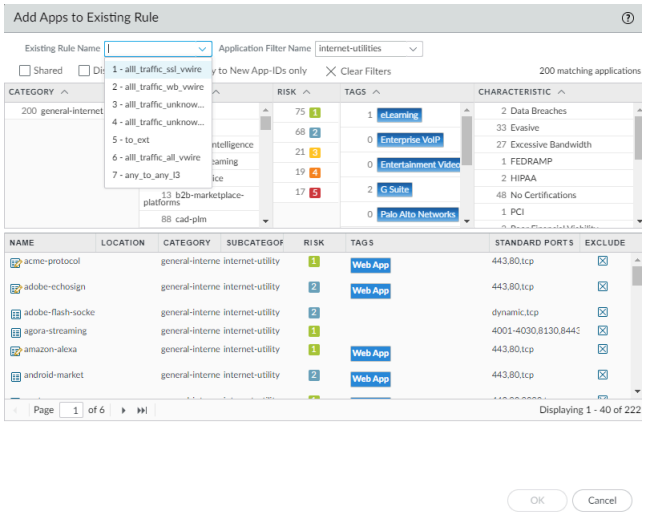


6. 按一下 **OK**（確定）將應用程式新增到新的或現有應用程式篩選器。防火牆包括您在應用程式篩選器中第 3 步中選取的應用程式。
7. **Commit**（提交）變更。

新增到現有規則：

1. 選取 **Existing Rule Name**（現有規則名稱），將選取的應用程式新增到應用程式篩選器中的現有規則。
2. 從功能表中選取 **Application Filter Name**（應用程式篩選器名稱）或輸入新應用程式篩選器的名稱。
3. 選取應用程式篩選器是否 **Shared**（共用）、是否要 **Disable override**（停用覆寫）篩選器的應用程式特性，以及篩選器應 **Apply to New App-IDs only**（僅套用至新 **App-ID**）還是應套用至所有 App-ID。
4. 使用類別、子類別、風險、標籤和特性值來篩選要新增到應用程式篩選器的應用程式類型。防火牆會自動將符合篩選器條件的新應用程式新增到應用程式篩選器。

©2024 Palo Alto Networks, Inc.



5. 按一下 **OK**（確定）將應用程式新增到新的或現有應用程式篩選器。防火牆包括您在應用程式篩選器中第 3 步中選取的應用程式。
6. **Commit**（提交）變更。

使用原則最佳化工具將應用程式新增到應用程式群組

將 App-ID 雲端引擎 (ACE) 中的 App-ID 新增到新的或現有應用程式群組，並使用安全性政策規則中的應用程式群組控制安全性政策中的雲端 App-ID。

ACE 為之前識別為 ssl 或 web-browsing 的應用程式提供 App-ID。

使用 Policy Optimizer（政策最佳化工具）將 ACE App-ID 新增到應用程式群組中，將群組套用至安全性政策規則，並控制安全性政策中的 ACE App-ID。

STEP 1 | 移至 **Policies**（原則） > **Security**（安全性），然後選取 **Policy Optimizer**（原則最佳化工具） > **New App Viewer**（新應用程式檢視器）。

如果防火牆或 Panorama 已下載 ACE App-ID，則左側導覽視窗中的 **New App Viewer**（新應用程式檢視器）旁邊會顯示一個數字。此螢幕會顯示符合已下載雲端 App-ID 的安全性原則規則。

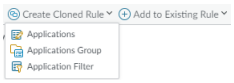
STEP 2 | 按一下安全性原則規則的 **Apps Seen**（看見的應用程式）中的數字，即可查看與 **Applications & Usage**（應用程式與使用情況）對話方塊中的規則相符的雲端傳遞應用程式。

STEP 3 | 選取您要新增至現有或新應用程式群組的應用程式。

您可以按子類別、風險、過去 30 天看到的流量或者應用程式第一次或最後上線時間對應用程式來對 **Apps Seen**（看見的應用程式）中的應用程式進行排序和篩選。

©2024 Palo Alto Networks, Inc.

STEP 4 | 依據您要處理應用程式的方式，從 **Create Cloned Rule**（建立複製的規則）或 **Add to Existing Rule**（新增至現有規則）中選取 **Application Group**（應用程式群組）。



您可以使用 ***Create Cloned Rule***（建立複製的規則）複製的應用程式數目上限為 *1,000* 個應用程式。如果您想要移至另一規則的應用程式超過 *1,000* 個，請改用 ***Add to Existing Rule***（新增至現有規則）。如果您要將應用程式移至新規則，僅需先建立規則（***Policies***（原則） > ***Security***（安全性）），然後使用原則最佳化工具將其新增至該規則即可。

STEP 5 | 為複製的或現有規則選取或建立應用程式群組。使用原則最佳化工具建立應用程式群組與使用 **Objects**（物件） > **Application Groups**（應用程式群組）建立應用程式群組相似。

建立複製的規則：

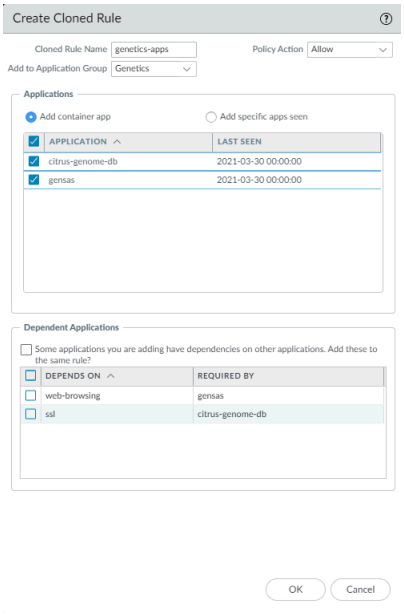
1. 輸入 **Cloned Rule Name**（複製的規則之名稱）（複製的規則之名稱，此名稱會立即顯示在安全性原則規則庫中，位於原始規則的上方）。
2. 選取 **Policy Action**（原則動作）（允許或拒絕）。
3. 在 **Add to Application Group**（新增至應用程式群組）中，選取要新增您在第 3 步中選取之應用程式的應用程式群組。
4. 選取 **Add container app**（新增容器應用程式）（預設）或僅 **Add specific apps seen**（新增看見的特定應用程式）。

   當您新增容器應用程式時，也會新增該容器中的所有功能應用程式，包括尚未在防火牆上看到的功能應用程式。例如，如果您新增「Facebook」容器應用程式，則還會新增 facebook-base、facebook-chat、facebook-posting 等，以及未來新增到該容器的任何應用程式。容器應用程式及其功能應用程式受到您向其新增應用程式群組之安全性原則規則的約束。選取容器應用程式本質上是面向未來的，並會自動化容器應用程式的安全性，讓您不必手動將該容器中的新應用程式新增至您的安全性原則。

   只新增看到的特定應用程式，意味著只有您選取的應用程式才會新增至應用程式群組。如果相同容器應用程式中的新應用程式到達防火牆，則應用程式群組不會控制它們，您必須手動決定如何處理新的應用程式。
5. 在某些情況下，您想要放置到應用程式群組中的應用程式需要（依賴）其他應用程式才能運作。在這些情況下，**Create Cloned Rule**（建立複製的規則）對話方塊會包含 **Dependent**

©2024 Palo Alto Networks, Inc.

Applications（相依應用程式），您可以在其中選取是否要將這些應用程式新增至複製的規則。將相依應用程式新增至規則，以確保選取的應用程式正常運作。



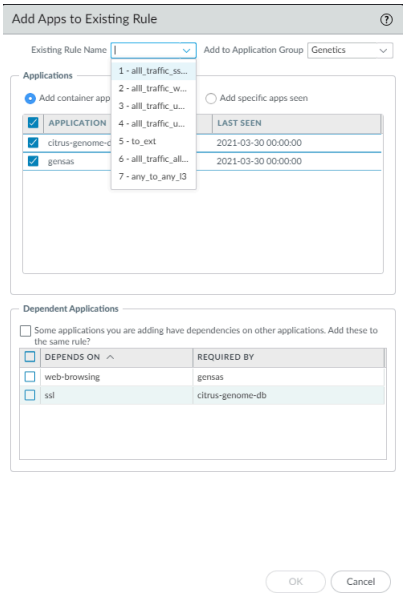
6. 按一下 **OK**（確定）將應用程式新增到新的或現有應用程式群組。
7. **Commit**（提交）變更。

將應用程式新增至現有規則：

1. 選取 **Existing Rule Name**（現有規則名稱），將選取的應用程式新增到應用程式群組中的現有規則。
2. 在 **Add to Application Group**（新增至應用程式群組）中選取應用程式群組，或輸入新應用程式群組的名稱。
3. 與複製規則一樣，您可以選擇 **Add container app**（新增容器應用程式）還是 **Add specific apps seen**（新增看見的特定應用程式）。新增容器應用程式會新增容器中的所有功能應用程式，以及未來新增至該容器的任何應用程式。只新增特定應用程式則只會新增選取的特定應用程式。
4. 與複製規則一樣，在某些情況下，您想要放置到應用程式群組中的應用程式需要（依賴）其他應用程式才能運作。在這些情況下，**Add Apps to Existing Rule**（新增應用程式至現有規則）對話方塊會包含 **Dependent Applications**（相依應用程式），您可以在其中選取是否要

©2024 Palo Alto Networks, Inc.

將這些應用程式新增至複製的規則。將相依應用程式新增至規則，以確保選取的應用程式正常運作。



5. 按一下 **OK**（確定）將應用程式新增到新的或現有應用程式群組。
6. **Commit**（提交）變更。

使用原則最佳化工具將應用程式直接新增到規則

您可以使用政策最佳化工具將 App-ID 雲端引擎 (ACE) App-ID 直接新增到規則中。不過，請考慮使用應用程式篩選器，在 ACE App-ID 到達防火牆時自動將其新增至安全性原則，而不是手動新增它們。

ACE 為之前識別為 *ssl* 或 *web-browsing* 的應用程式提供 *App-ID*。

STEP 1 | 移至 **Policies**（原則） > **Security**（安全性），然後選取 **Policy Optimizer**（原則最佳化工具） > **New App Viewer**（新應用程式檢視器）。

如果防火牆或 Panorama 已下載 ACE App-ID，則左側導覽視窗中的 **New App Viewer**（新應用程式檢視器）旁邊會顯示一個數字。此螢幕會顯示符合已下載雲端 App-ID 的安全性原則規則。

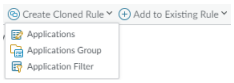
STEP 2 | 按一下安全性政策規則的 **Apps Seen**（看見的應用程式）中的數字，即可檢視與 **Applications & Usage**（應用程式與使用情況）對話方塊中的規則相符的雲端傳遞應用程式。

STEP 3 | 選取您要新增至現有或複製的安全性原則規則的應用程式。

您可以按子類別、風險、過去 30 天看到的流量或者應用程式第一次或最後上線時間對應用程式來對 **Apps Seen**（看見的應用程式）中的應用程式進行排序和篩選。

©2024 Palo Alto Networks, Inc.

STEP 4 | 依據您要處理應用程式的方式，從 **Create Cloned Rule**（建立複製的規則）或 **Add to Existing Rule**（新增至現有規則）中選取 **Applications**（應用程式）。



您可以使用 ***Create Cloned Rule***（建立複製的規則）複製的應用程式數目上限為 *1,000* 個應用程式。如果您想要移至另一規則的應用程式超過 *1,000* 個，請改用 ***Add to Existing Rule***（新增至現有規則）。如果您要將應用程式移至新規則，僅需先建立規則（***Policies***（原則） > ***Security***（安全性）），然後使用原則最佳化工具將其新增至該規則即可。

STEP 5 | 將選取的應用程式新增至複製的規則或現有規則。

建立複製的規則：

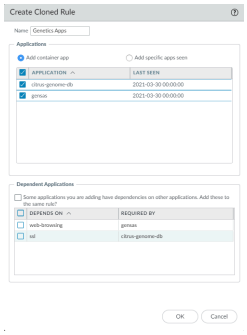
1. 輸入 **Name**（名稱）（複製的規則之名稱，此名稱會立即顯示在安全性原則規則庫中，位於原始規則的上方）。複製的規則與原始規則具有相同的動作（允許或拒絕）。
2. 選取 **Add container app**（新增容器應用程式）（預設）或僅 **Add specific apps seen**（新增看見的特定應用程式）。

   當您新增容器應用程式時，也會新增該容器中的所有功能應用程式，包括尚未在防火牆上看到的功能應用程式。例如，如果您新增「Facebook」容器應用程式，則還會新增 facebook-base、facebook-chat、facebook-posting 等，以及未來新增到該容器的任何應用程式。容器及其功能應用程式受到您正在複製的安全性原則規則的約束。選取容器應用程式本質上是面向未來的，並會自動化容器應用程式的安全性，讓您不必手動將該容器中的新應用程式新增至您的安全性原則。

   只新增看到的特定應用程式，意味著只有您選取的應用程式會新增至複製的規則。如果相同容器應用程式中的新應用程式到達防火牆，則複製的規則不會控制它們，您必須手動決定如何處理新的應用程式。
3. 在某些情況下，您想要新增至規則的應用程式需要（依賴）其他應用程式才能運作。在這些情況下，**Create Cloned Rule**（建立複製的規則）對話方塊會包含 **Dependent**

©2024 Palo Alto Networks, Inc.

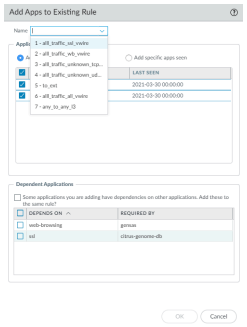
Applications（相依應用程式），您可以在其中選取是否要將這些應用程式新增至複製的規則。將相依應用程式新增至規則，以確保選取的應用程式正常運作。



4. 按一下 **OK**（確定），將應用程式新增至複製的規則。
5. **Commit**（提交）變更。

將應用程式新增至現有規則：

1. 選取要向其新增所選應用程式的現有規則的 **Name**（名稱）。
2. 與複製規則以新增應用程式一樣，您可以選擇 **Add container app**（新增容器應用程式）還是 **Add specific apps seen**（新增看見的特定應用程式）。新增容器應用程式會新增容器中的所有功能應用程式，以及未來新增至該容器的任何應用程式。只新增特定應用程式則只會新增選取的特定應用程式。
3. 與複製規則一樣，某些情況下，您想要新增至規則的應用程式需要（依賴）其他應用程式才能運作。在這些情況下，**Add Apps to Existing Rule**（新增應用程式至現有規則）對話方塊會包含 **Dependent Applications**（相依應用程式），您可以在其中選取是否要將這些應用程式新增至複製的規則。將相依應用程式新增至規則，以確保選取的應用程式正常運作。



4. 按一下 **OK**（確定），將應用程式新增至現有規則。
5. **Commit**（提交）變更。

更換 RMA 防火牆 (ACE)

當存在退貨授權 (RMA) 時，若要還原受管理防火牆上的設定，程序為：

- 檢閱開始 RMA 防火牆更換前。
- 在 Panorama 上，將舊防火牆的序號替換為新防火牆的序號。

©2024 Palo Alto Networks, Inc.

- 在防火牆 CLI 中，檢查以確保防火牆已在線上並連線到知識服務，以便防火牆可以下載雲端應用程式目錄：

  1. 存取防火牆 CLI。
  2. 在操作模式下，檢查雲端 App-ID 連線：

     ```
     admin@vm1> show cloud-appid connection-to-cloud
     ```

     如果防火牆已連線到雲端，顯示命令會返回：

     ```
     ACE Cloud server: kcs.ace.tpcloud.paloaltonetworks.com:443Cloud
     connection: connected
     ```

     還會顯示有關連線的資訊。如果防火牆未連線到雲端，請檢查 DNS 服務是否正常運作，並檢查是否有任何其他與網路相關的連線問題。

- 在防火牆連線到 App-ID 雲端後，更換後還原防火牆設定。

授權到期或停用 ACE 的影響

如果您在防火牆上啟用 App-ID 雲端引擎 (ACE)、下載 ACE App-ID 到防火牆，然後在物件（例如應用程式篩選器）和安全性原則規則中使用這些 App-ID，則您需要瞭解如果 SaaS 安全性內嵌授權到期或停用 ACE，會發生什麼。停用 ACE 和 SaaS 安全性內嵌授權到期都會影響下載的 ACE App-ID、ACE App-ID 的目錄、控制 ACE App-ID 的安全性原則規則以及包含 ACE App-ID 的物件。除非另有說明，否則影響是相同的：

- ACE App-ID 會保留在防火牆上，但防火牆會停止強制執行安全性原則中的 ACE App-ID。

  控制 ACE App-ID 的安全性原則規則不再控制 ACE App-ID，即使它們在規則中可見。在防火牆上啟用 ACE 之前由 ssl 或 web-browsing 規則所控制的流量會再次由這些規則控制，直到您更新並啟動 SaaS 安全性內嵌授權和/或重新啟用 ACE 或者變更這些規則為止。

- 根據 ACE App-ID 執行安全性原則規則會在授權到期後 4-6 小時內停止（基於定期檢查授權狀態的計時器）。

  當您在防火牆上提交停用 ACE 後，根據 ACE App-ID 執行安全性原則規則會立即停止。

  > 停用 *ACE* 會隨著您提交變更而立即停止基於 *ACE App-ID* 執行安全性原則規則，即使 *SaaS* 安全性內嵌授權仍然有效且在作用中。

- ACE App-ID 的目錄會保留在防火牆和 Panorama 上，但雲端引擎不再更新目錄。
- 從防火牆到 ACE 的連線不再運作。如果您重新啟用 ACE 或更新 SaaS 安全性內嵌授權，可能需要一些時間來下載所有目錄更新。
- 如果 SaaS 安全性內嵌授權到期，ACE 服務會在 4-6 小時內停止運作。

  > *Panorama* 不需要 *SaaS* 安全性內嵌授權，因此 *Panorama* 上沒有授權到期。不過，當受管理防火牆上的授權到期時，如果從 *Panorama* 推送至這些防火牆的設定在安全性原則或應用程式群組中包含 *ACE* 設定，則推送會失敗。

- 應用程式篩選器和應用程式群組之類的物件不會發生變更，但您放置在這些物件中的任何 ACE App-ID 都不再強制執行，即使 ACE App-ID 仍然可見。

©2024 Palo Alto Networks, Inc.

- 如果您使用 SaaS 原則建議，防火牆將無法再提取 SaaS 原則建議，因此 SaaS 管理員無法將新的原則建議推送到防火牆。在授權到期前下載的原則建議會保留在設定中，但不會強制執行（與當授權到期或停用 ACE 時，使用 ACE App-ID 設定的安全性原則之行為相同）。

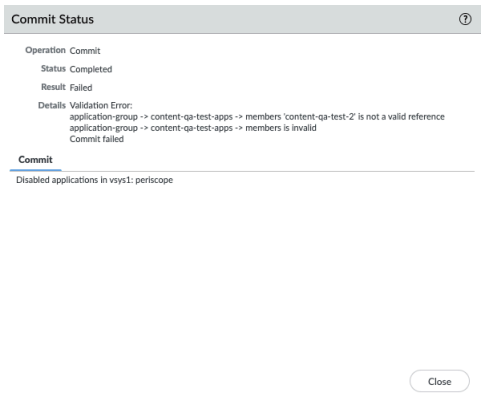
由於雲端內容回復而提交失敗

儘管這種情況極不可能發生，但由於中繼資料不良或應用程式問題，ACE App-ID 有可能需要回復（還原）。如果 ACE 必須還原 App-ID，且您已在安全性原則規則（直接或在應用程式群組中）中使用這些 App-ID，則在從安全性原則規則和物件中移除這些應用程式之前，提交動作將失敗。

如果有必要回復 App-ID，ACE 會從 ACE 目錄中還原所有最近傳遞的基於雲端的 App-ID、特徵碼、中繼資料、類別、子類別和標籤。從目錄中移除 App-ID 會將其從防火牆中移除，因此，當 App-ID 在安全性原則中使用時，提交動作會失敗。

如果您沒有使用 *ACE* 在安全性原則中必須回復的應用程式，則不會對設定產生影響，提交動作將會成功。

當您在 ACE 內容回復後嘗試提交設定時，提交失敗訊息會列出 ACE 已還原的應用程式，如此範例中的驗證錯誤所示：



要解決問題，您必須從安全性原則規則中移除列出的應用程式，無論這些應用程式是直接新增到規則還是透過應用程式群組新增到規則。如果應用程式在應用程式群組中使用，請將其從應用程式群組中移除。

在此範例中，`content-qa-test-2` 是已還原的應用程式，而該應用程式在應用程式群組 `content-qa-test-apps` 中被引用。在從應用程式群組中移除 `content-qa-test-2` 後，提交動作成功。

對 App-ID 雲端引擎進行疑難排解

本主題提供 App-ID 雲端引擎 (ACE) 的一般疑難排解資訊。

©2024 Palo Alto Networks, Inc.

- 若要檢查設備是否具有有效的 SaaS 安全性內嵌授權，請執行操作 CLI 命令 `show cloud-appid connection-to-cloud`。如果存在問題，命令會返回以下訊息：

  `ACE Error:License check failed.Check if SaaS license is installed and activeCloud connection: failed`

  此外，輸出會顯示上次成功連線的時間，例如：`Last successful gRPC connection:2021-05-20 16:00:00 -0800 PDT`

  如果已安裝授權且與 ACE 的連線良好，則命令會返回 ACE 雲端伺服器連線的 URL 和狀態 `Cloud connection: connected`，以及裝置憑證的連線統計資料和狀態，包括憑證有效日期。

- Panorama 提交所有/推送到受管理防火牆失敗。檢查是否存在以下任何條件並修復它們：
  - 受管理防火牆是否具有有效的 SaaS 安全性內嵌授權？如果沒有，那麼它們沒有 ACE 目錄，且提交所有/推送操作會失敗。視您是否希望受管理防火牆處理 ACE App-ID，從推送的設定中移除 ACE 物件並重試，或在受管理防火牆上安裝有效的 SaaS 安全性內嵌授權，等候下載目錄。

    內容提供的 *App-ID* 不到四千個。下載 *ACE* 目錄之後，您會在防火牆上看到數以千計的應用程式，並且可以透過檢查 ***Objects***（物件）> ***Applications***（應用程式）或使用操作 *CLI* 命令 *`show cloud-appid cloud-app-data application all`* 來確認，以查看新的 *App-ID*。

  - 受管理防火牆和 ACE 之間的連線是否已中斷？檢查與 ACE 雲端的連線，並視需要還原連線。

    CLI 操作命令 `show cloud-appid connection-to-cloud` 提供雲端連線狀態和 ACE 雲端伺服器 URL。

  - Panorama 上的 ACE 目錄和受管理防火牆上的 ACE 目錄不同步，這導致推送的設定包含不在防火牆目錄中的 ACE 應用程式。如果防火牆和 ACE 之間的連線為啟動，則過時的目錄將在未來幾分鐘內自動更新並解決問題。（請等待五分鐘，然後重試。）

    您還可以執行 *CLI* 操作命令 *`debug cloud-appid cloud-manual-pull check-cloud-app-data`* 以手動更新目錄。

  - 是否所有防火牆都執行 PAN-OS 11.0 或更新版本？（不允許將引用 ACE 應用程式和物件的設定推送至執行版本低於 PAN-10 11.0 的防火牆。）

- 在具有 ACE 設定的 HA 配對（主動/主動或主動/被動）中，如果您執行操作命令 `show session all` 或 `show session id <id>`，ACE 應用程式的輸出可能會顯示全域 App-ID 號碼，而不是應用程式名稱。僅當其資料平面具有雲端應用程式資料時，防火牆才會顯示應用程式名稱。如果沒有，則防火牆會改為顯示應用程式的全域 App-ID 號碼。
- 若要重設至 ACE 的連線（gRPC 連線），請執行 CLI 操作命令 `debug cloud-appid reset connection-to-cloud`。
- 使用 CLI 操作命令 `show cloud-appid cloud-app-data application` 檢視下載至設備的 ACE 應用程式。您可以按 App-ID 或應用程式名稱檢視所有下載的應用程式或個別應用程式。

©2024 Palo Alto Networks, Inc.

- 使用 CLI 操作命令 `show cloud-appid signature-dp pending-request` 檢視 ACE App-ID 的擱置中要求。輸出包括防火牆將要求傳送至 ACE 的次數（嘗試次數）。十一次嘗試之後，傳送操作逾時。
- CLI 操作命令 `show cloud-appid` 有更多實用選項：

```
admin@PAN-ACE-VM-1> show cloud-appid ? > app-objects-in-policy
 Show application-filter/application-groups referred in policy >
 app-to-filtergroup-mapping Show application to matched filter and
 groups > application Show Application info for UI > application-
filter Show cloud apps in application-filters > application-group
 Show cloud apps in application-groups > cloud-app-data Show cloud
 application, container and metadata > connection-to-cloud Show
 gRPC connection status to cloud application server > ha-info Show
 statistics of cloud application high availability > overlap-appid
 Show duplicated applications in predefined content > signature-
dp Show cloud signatures and applications used on DP > task Show
 task on management-plane > transaction Show cloud application
 transaction > version Show Cloud-AppID version
```

- 若要檢視 ACE 的全域計數器，請執行 CLI 操作命令 `show counter global filter value all category cad`（`cad` 表示「cloud app-identification」）。
- 若要檢視 ACE、DLP 和 IoT 等服務與共用記憶體和安全性用戶端往來的位元組和封包統計資料，請執行操作命令 `show ctd-agent statistics`。
- 如果您發現使用者介面中和 CLI 中與應用程式篩選器相符的應用程式數目之間有差異，這是因為防火牆在使用者介面中和 CLI 中計算相符應用程式的方式如下：
  - 當您在 **Objects**（物件）> **Application Filters**（應用程式篩選器）中查看應用程式篩選器時，防火牆會顯示 ACE 目錄中所有相符的應用程式，不論防火牆是否實際看到這些應用程式並下載其 App-ID，該數目包括所有這些應用程式。
  - 當您使用 `show cloud-appid application-filter` 操作命令查看 CLI 中的應用程式篩選器時，防火牆只會顯示防火牆已下載 ACE App-ID 的相符應用程式數目。

  基於這個原因，對於相同的應用程式篩選器，使用者介面顯示的相符應用程式數可能會多於 CLI。

  當您在使用者介面和 *CLI* 中查看應用程式群組時，也會出現相同情況。

- ACE App-ID 僅針對安全性原則受支援。任何其他原則類型都不支援 ACE App-ID。

  不過，當您設定 QoS 或 SD-WAN 原則時，會顯示 ACE App-ID（可選取），且可能會出現在套用至規則的應用程式群組或應用程式篩選器中，但是將它們新增至 QoS 或 SD-WAN 原則並不會對應用程式流量產生影響。（QoS 和 SD-WAN 原則不會控制應用程式流量。）

©2024 Palo Alto Networks, Inc.

SaaS App-ID 原則建議

SaaS 應用程式的快速增加，導致很難為所有這些應用程式指派特定的 App-ID、瞭解並控制這些應用程式。允許 ssl、web-browsing 或「任何」應用程式的安全性原則規則，可能會允許未經認可的 SaaS 應用程式，從而為您的網路帶來安全風險。若要瞭解並在防火牆上控制這些應用程式，SaaS 安全性管理員可以向 PAN-OS 防火牆管理員建議由 App-ID 雲端引擎 (ACE) 提供的具有特定 SaaS App-ID 的安全性政策規則。PAN-OS 管理員可以在具有 SaaS 安全性內嵌訂閱的防火牆上匯入這些規則。

SaaS 原則建議需要 SaaS 安全性內嵌訂閱。使用 *SaaS* 原則建議引擎的每個設備都需要產生並安裝有效的裝置憑證，或使用 Panorama 來產生並安裝有效的裝置憑證。

需要 SaaS 安全性內嵌至 *Cortex Data Lake (CDL)* 的連線才可獲取 *SaaS* 可視性。設定日誌轉送至 *CDL*，並在安全性原則規則中使用正確的日誌轉送設定檔啟用日誌轉送。至少，您必須將流量日誌和 *URL* 日誌轉送至 *CDL*，*SaaS* 安全性內嵌才能正常運作。

支援 *PAN-OS 10.1* 或更高版本的所有硬體平台都支援 *SaaS* 原則建議，您想要在其上使用 *SaaS* 原則建議的所有設備都需要安裝 *PAN-OS 10.1* 或更高版本。*Panorama* 無法將 *SaaS* 原則建議推送並提交到沒有安裝 *SaaS* 安全性內嵌授權的防火牆或執行的 *PAN-OS* 版本低於 *10.1* 的防火牆。

- *SaaS* 安全性管理員指南介紹了 SaaS 安全性管理員建立安全性原則規則建議並將其推送到防火牆的程序。
- *PAN-OS* 管理員指南介紹了 PAN-OS 管理員如何從 SaaS 安全性管理員處匯入和管理原則建議。

SaaS 安全性管理員會建立新規則，將應用程式、使用者和群組新增至規則，以及設定規則動作。規則動作可以是允許或封鎖；不允許對推送的規則執行其他動作。然後，SaaS 安全性管理員會將規則推送至適當的設備，且規則會顯示在防火牆介面中（**Device**（裝置） > **Policy Recommendation**（原則建議） > **SaaS**）。

PAN-OS 管理員會評估建議的規則，並決定是否要在防火牆上實作。如果 PAN-OS 管理員選擇實作規則，則管理員會將規則匯入到防火牆上，並在防火牆規則庫中選取要放置原則規則的位置。當 PAN-OS 管理員匯入原則建議時，防火牆會自動建立必要的 HIP 設定檔、標籤和應用程式群組（PAN-OS 管理員不需要手動執行）。

如果 *SaaS* 安全性管理員將安全性設定檔與原則建議一起推送，且這些設定檔未存在於防火牆上，則防火牆匯入將失敗。如果設定檔已經存在於防火牆上，則匯入會成功。

如果 SaaS 安全性管理員更新原則規則建議，則 PAN-OS 管理員會看到更新並將其匯入防火牆。如果 SaaS 安全性管理員刪除原則規則建議，則 PAN-OS 管理員會看到該動作，並從防火牆安全性原則規則庫中刪除該規則。

©2024 Palo Alto Networks, Inc.

如果 *SaaS* 安全性內嵌授權到期，則防火牆將不再提取 *SaaS* 原則建議，因此您不會看到新建議。不過，您已匯入的安全性原則規則會繼續運作。

如果您停用 *ACE*，則防火牆將不再接收新的雲端應用程式特徵碼和 *App-ID*，且防火牆無法匯入基於新 *ACE App-ID* 的 *SaaS* 原則建議。

ACE 部署程序（連線至雲端、安裝裝置憑證、在 SaaS 安全性入口網站上啟動授權並將其推送至 Panorama 和防火牆等）也會設定 SaaS 原則建議。

將所有設備更新到最新的安全威脅內容更新。

會為此新功能新增的使用者介面包括：

- **Device**（裝置） > **Policy Recommendation**（原則建議） > **SaaS** 顯示來自 SaaS 管理員的原則建議，並可讓防火牆管理員匯入、更新、移除及控制建議的 SaaS 原則。該頁面顯示包括 SaaS 管理員為原則設定的應用程式群組。
- 基於角色的介面存取（**Device**（裝置） > **Admin Roles**（管理員角色））的 **Web UI** 頁籤上有用於 SaaS 原則建議權限的新選項：**Device**（裝置） > **Policy Recommendation**（原則建議） > **SaaS**。
- SaaS 原則建議會自動標記 **SaaSSecurityRecommended**，這會顯示在介面的 **Tags**（標籤）欄中。

您可以匯入和更新 SaaS 管理員推送的 SaaS 原則建議，並移除 SaaS 管理員已刪除的 SaaS 原則建議。

- 匯入 SaaS 原則建議
- 匯入更新的 SaaS 原則建議
- 移除已刪除的 SaaS 原則建議

匯入 SaaS 原則建議

當 SaaS 安全性管理員將安全性原則規則建議推送到 PAN-OS 防火牆時，PAN-OS 防火牆管理員可以匯入防火牆上的這些規則，以便瞭解和控制原則建議中的應用程式。

請參閱 *SaaS* 安全性管理員指南，瞭解 SaaS 管理員的原則建議和推動程序。此程序向 PAN-OS 管理員展示如何匯入原則建議。

如果 *SaaS* 安全管理員將安全性設定檔與原則建議一起推送，且這些設定檔未存在於防火牆上，則防火牆匯入將失敗。如果設定檔已經存在於防火牆上，則匯入會成功。

STEP 1 | 防火牆上的 **Device**（裝置） > **Policy Recommendation**（原則建議） > **SaaS**和 Panorama 上的 **Panorama** > **Policy Recommendation**（原則建議） > **SaaS** 顯示由 SaaS 管理員推送的所有 SaaS 原則建議。將原則建議從 Panorama 推送至受管理防火牆。

STEP 2 | 重新整理 ( ) **Device**（裝置） > **Policy Recommendation**（原則建議） > **SaaS**（或 **Panorama** > **Policy Recommendation**（原則建議） > **SaaS**）以確保 SaaS 原則建議為最新。

©2024 Palo Alto Networks, Inc.

每次將原則建議從 *Panorama* 推至受管理防火牆時，都重新整理 ( ) 防火牆上的頁面，以確保建議為最新。

新推送的原則建議顯示在螢幕頂部。**Active Recommendations**（作用中推薦）顯示值 **active**（作用中），且 **New Updates Available**（新更新可用）顯示值 **Yes**（是）。

STEP 3 | 選取新的原則建議。

一次匯入一個原則建議。**Applications**（應用程式）欄為每個原則建議顯示一個應用程式群組。按一下群組名稱以查看該群組中的應用程式。

Device（裝置）欄顯示 SaaS 管理員為規則設定的來源裝置。來源裝置前有術語「SaaS」。來源裝置可以是：

- MCD—受管理的合規裝置
- MNCD—受管理的不合規裝置
- UMCD—不受管理的合規裝置
- UMNCD—不受管理的不合規裝置

例如，**SaaS - MCD** 表示受管理的合規來源裝置。

STEP 4 | 匯入原則規則。

在 **Import Policy Rule**（匯入原則規則）對話方塊中：

- **Name**（名稱）—為匯入的規則命名，表明規則的意圖。

  如果您指定已存在於安全性原則規則庫中的規則名稱，則匯入的規則會覆寫現有規則。

- **After Rule**（前置規則）—選取要將匯入的規則放置在其後面的規則。考慮防火牆的規則庫以及新規則對現有規則可能產生什麼影響。如果您不選取規則（未選取規則），則規則將放在安全性原則規則庫的頂部。在某些情況下，這並不是您想要放置規則的位置。例如，您可能希望某些特定的封鎖規則始終位於規則庫的頂部，如封鎖 QUIC 通訊協定。留意所匯入規則的意圖，並小心不要影響現有規則。

Description（說明）來自 SaaS 管理員建立規則時輸入的說明。您可以變更它或保持不變。

匯入過程會自動為原則建議中的應用程式建立應用程式群組。應用程式群組的名稱源自 *SaaS* 安全管理員為規則提供的名稱。防火牆還會自動建立 *SaaS* 管理員套用至規則的任何 *HIP* 設定檔和標籤。

STEP 5 | 按一下 **OK**（確定）以匯入規則並將其新增到安全性原則規則庫中，放置到在 **After Rule**（前置規則）中選取的位置。

STEP 6 | 當您看到狀態訊息「您已成功更新安全性原則規則」時，請按一下 **OK**（確定）。

Location（位置）欄現在顯示防火牆上的規則位置 (vsys)，對應 SaaS 管理員向其推送了規則的 vsys。

©2024 Palo Alto Networks, Inc.

STEP 7 | 確認匯入的原則規則位於安全性原則規則庫（**Security**（安全性） > **Policies**（原則））中的指定位置，且防火牆已建立關聯物件。

例如，檢查安全性原則規則，確認：

- 規則的 **Source Device**（來源裝置）已填寫，且在 **Source**（來源）頁籤上顯示規則的來源裝置。
- 應用程式群組填入規則的 **Application**（應用程式）頁籤。
- 關聯設定檔已附加到規則（**Actions**（動作）頁籤）。

還要確認：

- **Objects**（物件） > **Applications Group**（應用程式群組）顯示匯入的應用程式群組。
- **Objects**（物件） > **GlobalProtect** > **HIP Objects**（**HIP** 物件）和 **Objects**（物件） > **GlobalProtect** > **HIP Profiles**（**HIP** 設定檔）顯示 SaaS 安全性管理員透過規則推送的 HIP 資訊。

匯入更新的 SaaS 原則建議

當 SaaS 安全性管理員將安全性原則規則建議推送到 PAN-OS 防火牆（或 Panorama）時，PAN-OS 防火牆管理員可以匯入這些規則，以便瞭解和控制原則建議中的應用程式。但是，如果 SaaS 管理員更新了規則，例如新增或移除了應用程式，則該規則還需要在防火牆上進行更新。

如果 *SaaS* 安全性管理員推送新的或更新的應用程式群組、*HIP* 設定檔或標籤，則防火牆會自動建立或更新這些物件。如果 *SaaS* 安全管理員將安全性設定檔與原則建議更新一起推送，且這些設定檔未存在於防火牆上，則防火牆匯入將失敗。如果設定檔已經存在於防火牆上，則匯入會成功。

STEP 1 | 重新整理 ( ) **Device**（裝置） > **Policy Recommendation**（原則建議） > **SaaS**（或 **Panorama** > **Policy Recommendation**（原則建議） > **SaaS**）以確保您看到 SaaS 管理員推送到防火牆的所有最新 SaaS 原則建議。

STEP 2 | 查看 **New Updates Available**（新更新可用）。

如果 **New Updates Available**（新更新可用）欄中的值為 **No**（否），則表示規則沒有更新。如果值為 **Yes**（是），則表示 SaaS 管理員已將規則的更新推送至防火牆。此外，**Active Recommendations**（作用中建議）顯示值 **active**（作用中）。

STEP 3 | 按一下 **Applications**（應用程式）欄中的應用程式群組名稱，查看規則控制之應用程式的更新清單。

STEP 4 | 選取要更新的原則建議。

一次只更新一個原則建議。

©2024 Palo Alto Networks, Inc.

STEP 5 | 按一下 **Import Policy Rule**（匯入原則規則）以匯入原則（如果該規則沒有更新，此選項呈現灰色，無法選取）。

會顯示 **Import Policy Rule**（匯入原則規則）對話方塊。**Name**（名稱）已填入，不能變更，因為該規則已匯入。對話方塊中的 **After Rule**（前置規則）也無法變更，但如果您想變更規則在安全性原則規則庫中的位置，您可以按照變更任何安全性原則規則位置的相同方法在 **Policies**（原則）> **Security**（安全性）中進行。您可以變更 **Description**（說明）或保持不變。

STEP 6 | 按一下 **OK**（確定）。

STEP 7 | 在 **Confirm Change**（確認變更）中按一下 **Yes**（是）以匯入更新的規則（如果您不想匯入變更的規則，則按一下 **No**（否））。

防火牆會自動對應用程式群組、HIP 設定檔和與規則相關的標籤進行任何變更。

移除已刪除的 SaaS 原則建議

當 SaaS 安全性管理員將安全性原則規則建議推送到 PAN-OS 設備時，PAN-OS 管理員可以匯入這些規則，以便瞭解和控制原則建議中的應用程式。不過，如果 SaaS 安全性管理員刪除該規則，您也應當從 PAN-OS 設備中刪除該規則。

當 SaaS 安全性管理員刪除一條規則時，**Active Recommendation**（作用中建議）欄會顯示值 **removed**（已移除）（對於有效規則，值為 **active**（作用中））。

STEP 1 | 選取 SaaS 安全管理員 **removed**（已移除）的規則（一次只能選取一個規則進行移除）。

Import Policy Rule（匯入原則規則）選項會呈現灰色，因為無法再匯入該規則。

STEP 2 | 按一下 **Remove Recommendation Mapping**（移除建議對應）。

這會移除防火牆上安全性原則規則的本機對應。例如，將刪除到位置、使用者和規則的對應。**Remove Recommendation Mapping**（移除建議對應）對話方塊會顯示規則的位置，讓您知道移除規則的位置。

STEP 3 | 按一下 **OK**（確定）。

STEP 4 | 在 **Confirm Change**（確認變更）對話方塊中，按一下 **Yes**（是）從原則建議資料庫中移除規則。

此動作只會從原則建議規則清單中移除規則。它不會將規則從安全性原則規則庫中移除。您必須手動從規則庫中移除規則。

STEP 5 | 會顯示 **Status**（狀態）對話方塊，確認原則建議對應已移除，但您仍然需要從安全性原則規則庫中移除該規則。

STEP 6 | 移至 **Policies**（原則）> **Security**（安全性），然後從安全性原則規則庫中刪除規則。

©2024 Palo Alto Networks, Inc.

應用程式層級閘道

Palo Alto Networks 防火牆不會依連接埠與通訊協定分類流量，而是使用 App-ID 技術根據唯一屬性與交易特性來識別應用程式。但由於某些應用程式需要防火牆動態開啟針孔，才能建立連線、判定工作階段參數，及交涉將用於傳輸資料連接埠；這些應用程式會使用應用層的承載來傳達應用程式開啟資料連線所在的 TCP 或 UDP 連接埠。對於這類應用程式，防火牆會作為應用程式層級閘道（ALG），並限時開啟針孔以專門傳輸資料或控制流量。防火牆也會視需要執行承載的 NAT 重新寫入。

- 閘道管理者路由模式下不支援 *H.323*（*H.225* 和 *H.248*）*ALG*。
- 當防火牆作為工作階段初始通訊協定 *(SIP)* 的 *ALG* 時，依預設它會在承載上執行 *NAT*，並為媒體連接埠開啟動態針孔。在某些狀況下，視您環境中使用的 *SIP* 應用程式而定，*SIP* 端點會有 *NAT* 智慧內嵌在其用戶端中。在此狀況下，您必須停用 *SIP ALG* 功能才能防止防火牆修改訊號工作階段。當 *SIP ALG* 停用時，如果 *App-ID* 判斷工作階段為 *SIP*，則不會轉譯承載，也不會開啟動態針孔。請參閱停用 SIP 應用程式層級閘道 (ALG)。

使用動態 *IP* 及連接埠 *(DIPP) NAT* 時，*Palo Alto Networks* 防火牆 *ALG* 解碼器需要在 *SIP* 標頭（「聯絡人」和「透過」欄位）下組合 *IP* 和連接埠（傳送者地址和傳送者連接埠），以便據此轉譯提到的標頭並打開預測工作階段。

下表列出了 Ipv4、NAT、IPv6、NPTv6 和 NAT64 ALG，並用核取記號指示了該 ALG 是否支援每種通訊協定（例如 SIP）。

App-ID	IPv4	NAT	IPv6	NPTv6	NAT64
SIP	✓	✓	✓	—	—
SCCP	✓	✓	✓	—	—
MGCP	✓	✓	—	—	—
FTP	✓	✓	✓	✓	—
RTSP	✓	✓	✓	✓	—
MySQL	✓	✓	—	—	—
Oracle/SQLNet/TNS	✓	✓	✓	✓	—
RPC	✓	✓	—	—	—

©2024 Palo Alto Networks, Inc.

App-ID	IPv4	NAT	IPv6	NPTv6	NAT64
RSH	✓	✓	—	—	—
UNIStim	✓	✓	—	—	—
H.225	✓	✓	—	—	—
H.248	✓	✓	—	—	—

©2024 Palo Alto Networks, Inc.

停用 SIP 應用程式層級閘道 (ALG)

Palo Alto Networks 防火牆會使用工作階段初始通訊協定 (SIP) 應用程式層級閘道 (ALG) 開啟 NAT 已啟用之防火牆中的動態針孔。但是某些應用程式—如 VoIP—已有 NAT 智慧內嵌於用戶端應用程式中。在這些狀況下，防火牆上的 SIP ALG 會干涉到訊號工作階段，並造成用戶端應用程式停止運作。

有一個解決此問題的方法，就是為 SIP 定義應用程式取代原則，但使用此方法會停用 App-ID 與威脅偵測功能。另一個更好的方法就是停用 SIP ALG，這不會停用 App-ID 或威脅偵測。

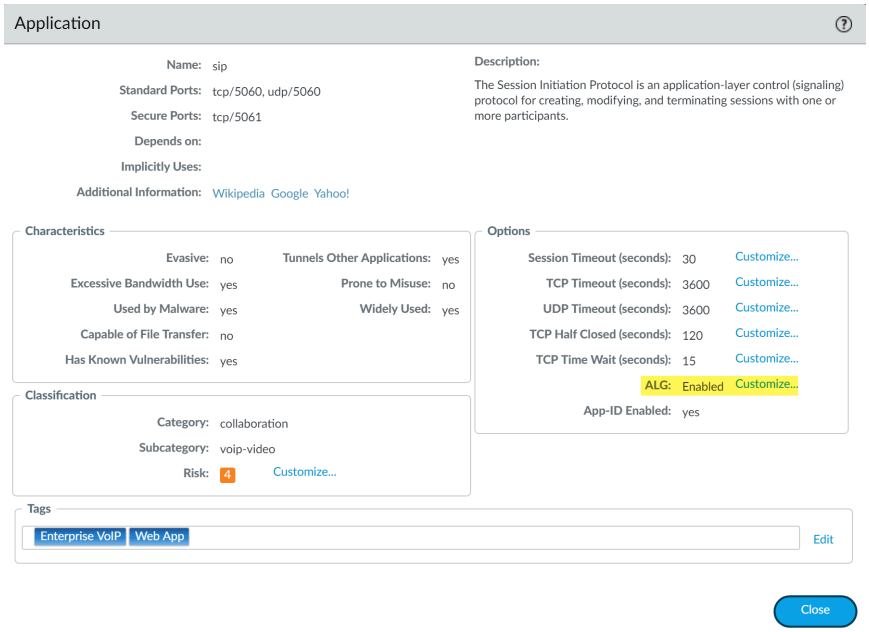
下列程序說明如何停用 SIP ALG。

STEP 1 | 選取 **Objects**（物件） > **Applications**（應用程式）。

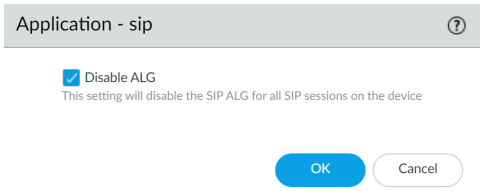
STEP 2 | 選取 **sip** 應用程式。

您可以在搜尋 方塊中輸入 sip，以協助尋找 **sip** 應用程式。

STEP 3 | 在 [應用程式] 對話方塊的 [選項] 區段中，為 **ALG** 選取 **Customize...**（自訂...）。



STEP 4 | 選取 Application - sip（應用程式 - sip） 對話方塊中的 **Disable ALG**（停用 **ALG**）核取方塊，並按一下 **OK**（確定）。



STEP 5 | 關閉 [應用程式] 對話方塊，然後提交變更。

©2024 Palo Alto Networks, Inc.

使用 HTTP 標頭管理 SaaS 應用程式存取

您的使用者可能會透過對 SaaS 應用程式的非認可使用來向網路外部傳輸機密資訊，通常以存取應用程式的消費者版本而實施。但是，如果您需為特定個人或組織允許此類應用程式企業版本的存取，就不能完全封鎖 SaaS 應用程式。

您可使用自訂 HTTP 標頭禁止 SaaS 消費者帳戶，同時允許特定的企業帳戶。許多 SaaS 應用程式根據特定 HTTP 標頭中包含的資訊允許或禁止應用程式的存取。您可使用預先定義的類型建立 HTTP 標頭插入項目，來管理熱門 SaaS 應用程式的存取，例如 Google G Suite 與 Microsoft Office 365。Palo Alto Networks® 使用內容更新來維持特定於這些應用程式的預先定義的規則集，以及新增新的預先定義的規則集。

此外，如果您要管理 SaaS 應用程式的存取，您還可建立自訂 HTTP 標頭插入項目，這些應用程式使用 HTTP 標頭來限制服務存取，而且 Palo Alto Networks 未為其提供預先定義的規則集。

請注意，商業 SaaS 應用程式始終使用 SSL，因此需進行解密以執行 HTTP 標頭插入。若流量尚未透過上游防火牆解密，可將防火牆設定為採用 SSL 正向 Proxy 解密來解密流量。

您無需使用 *URL* 篩選授權即可使用此功能。

若要瞭解如何使用 HTTP 標頭管理 SaaS 應用程式，請參閱以下內容：

- 瞭解 SaaS 自訂標頭
- 預先定義的 SaaS 應用程式類型所使用的網域
- 使用預先定義的類型建立 HTTP 標頭插入項目
- 建立自訂 HTTP 標頭插入項目

瞭解 SaaS 自訂標頭

開始前，請確保您瞭解將針對正在管理的 SaaS 應用程式所使用的自訂 HTTP 標頭。您需瞭解使用這些標頭可實現的目標，以及需指定哪些資訊以實現目標。

請注意，使用自訂標頭的 SaaS 應用程式並不總是使用這些標頭來控制帳戶類型的存取。例如，Palo Alto Networks® 為 YouTube 自訂標頭提供預先定義的支援，這些標頭確定網路使用者是否可存取受限內容。

此外，您還需閱讀要控制其存取的 SaaS 應用程式的文件，以便您瞭解需為此應用程式使用哪些標頭。

©2024 Palo Alto Networks, Inc.

以下限制適用於 *HTTP* 標頭插入：

- 標頭名稱字元長度：*100.*
- 標頭值字元長度：*16K*。

請注意，某些 *SaaS* 應用程式可能會定義自訂標頭名稱，或將超出該等限制的值指派給其自訂標頭。這些情況應該很少見，但如果 *SaaS* 應用程式確實超過了一個或兩個的字元長度限制，則您的新世代防火牆將無法成功管理對該 *SaaS* 應用程式的存取。

以下表格列出了可為 SaaS 應用程式使用的標頭，Palo Alto Networks 已為這些應用程式提供預先定義的支援；每個標頭還包含連結，該連結提供特定於此標頭的詳細資訊。

應用程式	標頭	如需詳細資訊
Dropbox	`X-Dropbox-allowed-Team-Ids`	www.dropbox.com/help/business/network-control 您可允許認可企業版 Dropbox 帳戶的存取。此標頭的值為商業帳戶的團隊 ID，您可透過 Dropbox 管理員主控台的網路控制區段獲取此 ID。此外，您還必須透過相同位置啟用此功能。 如需管理此標頭的詳細資訊，並詳細瞭解如何啟用 Dropbox 用戶端以便能夠解密其流量，請聯絡您的 Dropbox 帳戶代表。
Google G Suite	`X-GooGApps-Allowed-Domains`	support.google.com/a/answer/1668854?hl=en 您可允許透過您的網域存取特定 Google 帳戶。您向此標頭指定的值為您的網域及子網域。 要為 Google 應用程式成功插入標頭，您還必須：

©2024 Palo Alto Networks, Inc.

應用程式	標頭	如需詳細資訊
		1. 建立包含以下類別和 URL 的 SSL 解密設定檔： • business-and-economy • computer-and-internet-info • content-delivery-networks • internet-communications-and-telephony • low-risk • online-storage-and-backup • search-engine • web-based-email • drive.google.com • *.google.com • *.googleusercontent.com • *.gstatic.com 2. HTTP/2 當前不支援 HTTP 標頭插入。要插入標頭，請使用適當解密設定檔中的除去 **ALPN** 功能將 HTTP/2 連線降級為 HTTP/1.1。如需詳細資訊，請參閱 App-ID 和 HTTP/2 檢查。 3. 建立規則以封鎖快速 UDP 網際網路連線 (QUIC) App-ID 並將其置於安全性原則頂部，因為防火牆對此通訊協定不支援標頭插入。當您進行標頭插入時，應用程式會還原到使用 HTTP/2 over TLS，這是防火牆在上一步中處理的。
Microsoft Office 365	`Restrict-Access-To-Tenants` `Restrict-Access-Context`	docs.microsoft.com/en-us/azure/active-directory/active-directory-tenant-restrictions 您向 `Restrict-Access-To-Tenants` 提供要允許使用者存取的租用戶清單。您可使用任何在租用戶中註冊的網域來識別此清單中的租用戶。 您向 `Restrict-Access-Context` 提供設定租用戶限制的目錄 ID。您可在 Azure 入口網站中找到目錄 ID。以管理員身份登入，

©2024 Palo Alto Networks, Inc.

應用程式	標頭	如需詳細資訊
		並選取 **Azure Active Directory**，然後選取 **Properties**（屬性）。
YouTube	`YouTube-Restrict`	support.google.com/a/answer/6214622?hl=en 您向此標頭提供有關希望使用者能夠檢視之視訊類型的資訊。您可指定 **Strict**（嚴格）或 **Moderate**（適中）設定。請參閱 support.google.com/a/answer/6212415 獲取有關這些不同設定的詳細資料。

預先定義的 SaaS 應用程式類型所使用的網域

SaaS 應用程式使用 HTTPS，將自訂標頭插入此流量，自訂標頭必須進行解密處理。若您使用防火牆提供的正向 Proxy 解密來解密自訂標頭，必須透過識別與流量相關的網域來識別您要解密的特定 HTTPS 流量。下表列出了各 SaaS 應用程式的相關網域，Palo Alto Networks® 已為這些應用程式提供預先定義的規則。

應用程式	網域
Dropbox	`*.dropbox.com`
G Suite	`*.google.com` `gmail.com`

Microsoft Office 365	`login.microsoftonline.com`
	`login.microsoft.com`
	`login.windows.net`

YouTube	`www.youtube.com`
	`m.youtube.com`
	`youtubei.googleapis.com`
	`youtube.googleapis.com`
	`www.youtube-nocookie.com`

©2024 Palo Alto Networks, Inc.

使用預先定義的類型建立 HTTP 標頭插入項目

STEP 1 | 如果沒有上游裝置已解密 HTTPS 流量，則使用設定 SSL 正向 Proxy 設定解密。

> 如果您為 *Dropbox* 設定 *SSL* 解密，還必須將您的 *Dropbox* 用戶端設定為允許 *SSL* 流量。這些程序特定於 *Dropbox* 且歸其私有— 若要獲取這些程序，請聯絡您的 *Dropbox* 帳戶代表。

1. 為您正在管理的 SaaS 應用程式 **Add**（新增）自訂 URL 類別（**Objects**（物件） > **Custom Objects**（自訂物件） > **URL Category**（**URL** 類別））。
2. 指定類別的 **Name**（名稱）。
3. **Add**（新增）您管理的 SaaS 應用程式特定的網域，或在標題中插入使用者名稱和網域的網域。請參閱預先定義的 SaaS 應用程式類型所使用的網域，獲取針對各個預先定義的 SaaS 應用程式所使用的網域清單。有關設定防火牆以在 HTTP 標頭中包含使用者名稱和網域的更多資訊，請參見 在 HTTP 標頭中插入使用者名稱。

   每個網域名稱最多可達 254 字元，且每個項目最多可定義 50 個網域。網域清單支援萬用字元（例如`*.example.com`）。最佳做法是，不要巢狀萬用字元（例如`*.*.*`），且不要在同一 URL 設定檔中重疊網域。
4. 對於 SaaS 應用程式管理，建立解密原則規則，按照此程序操作時，執行以下設定：
   - 在 **Service/URL Category**（服務/**URL** 類別）頁籤中，**Add**（新增）您在上一步中建立的 **URL Category**（**URL** 類別）。
   - 在 **Options**（選項）頁籤中，確保將 **Action**（動作）設為 **Decrypt**（解密），並將 **Type**（類型）設為 **SSL Forward Proxy**（**SSL** 正向 **Proxy**）。

STEP 2 | 編輯或新增 URL 篩選器。

STEP 3 | 在 **URL Filtering Profile**（**URL** 篩選設定檔）對話方塊中選取 **HTTP Header Insertion**（**HTTP** 標頭插入）。

STEP 4 | **Add**（新增）項目。

1. 為此項目指定 **Name**（名稱）（最多 100 個字元）。
2. 選取預先定義的 **Type**（類別）。

   此值會填入 **Domains**（網域）以及 **Headers**（標頭）清單。
3. 對於各個 **Header**（標頭），輸入 **Value**（值）。

   每個標頭值最多可以包含 16K 個字元。
4. （選用）選取 **Log**（日誌），以針對標頭插入活動啟用日誌記錄。

   不會記錄允許流量，因此不會記錄允許流量的標頭插入。
5. 按一下 **OK**（確定）儲存您的變更。

©2024 Palo Alto Networks, Inc.

STEP 5 | **Add**（新增） 或編輯 Security Policy（安全性原則）規則（**Policies**（原則） > **Security**（安全性））以包含 HTTP 標頭插入 URL 篩選設定檔。

- 對於 SaaS 應用程式管理，透過此規則，使用者可存取為其設定此標頭插入規則的 SaaS 應用程式。
- 要將使用者名稱和網域包含在 HTTP 標頭中，請將 URL 篩選設定檔套用至 HTTP 或 HTTPS 流量的安全原則規則。
  1. 選擇您在步驟 2 中編輯或建立的 URL 篩選設定檔（**Actions**（動作） > **URL Filtering**（**URL** 篩選））。
  2. 按一下 **OK**（確定）以儲存，然後 **Commit**（提交）變更。

STEP 6 | 確認防火牆已正確插入標頭。

- 對於 SaaS 應用程式管理，請從端點確認對 SaaS 應用程式的存取會按您預期的方式工作。
  1. 嘗試存取您預計能夠存取的帳戶或內容。如果您無法存取 SaaS 帳戶或內容，則表示設定未運作。
  2. 嘗試存取您預計會遭到封鎖的帳戶或內容。如果您能存取 SaaS 帳戶或內容，則表示設定未運作。
  3. 若上述兩個步驟均按預計方式運作，則可檢視日誌（若您已在步驟 4.4 中設定記錄），而且您應該能夠看到記錄的 HTTP 標頭插入活動。

建立自訂 HTTP 標頭插入項目

STEP 1 | 如果沒有上游裝置已解密 HTTPS 流量，則設定 SSL 正向 Proxy。

1. 為您正在管理的 SaaS 應用程式 **Add**（新增）自訂 URL 類別（**Objects**（物件） > **Custom Objects**（自訂物件） > **URL Category**（**URL** 類別））。
2. 指定類別的 **Name**（名稱）。
3. 針對您正在管理的 SaaS 應用程式 **Add**（新增）網域。
4. 建立解密原則規則，按照此程序操作時，執行以下設定：
   - 在 **Service/URL Category**（服務/**URL** 類別）頁籤中，**Add**（新增）您在上一步中建立的 **URL Category**（**URL** 類別）。
   - 在 **Options**（選項）頁籤中，確保將 **Action**（動作）設為 **Decrypt**（解密），並將 **Type**（類型）設為 **SSL Forward Proxy**（**SSL** 正向 **Proxy**）。

STEP 2 | 編輯或新增 URL 篩選器。

STEP 3 | 在 URL Filtering Profile（URL 篩選設定檔）對話方塊中選取 **HTTP Header Insertion**（**HTTP** 標頭插入）。

©2024 Palo Alto Networks, Inc.

STEP 4 | **Add**（新增）項目。

1. 為此項目指定 **Name**（名稱）。
2. 將 **Custom**（自訂）選為 **Type**（類型）。
3. 將網域 **Add**（新增）至 **Domains**（網域）清單。

   您可新增至多 50 個網域，每個網域名稱可擁有至多 256 個字元；支援萬用字元（例如 *.example.com）。

   當此清單中的網域與 *HTTP* 請求的主機標頭中的網域相符時，會產生 *HTTP* 標頭插入。
4. 將標頭 **Add**（新增）至 **Headers**（標頭）清單。

   您可新增至多 5 個標頭，每個標頭可擁有至多 100 個字元但不得包含任何空格。
5. 對於各個標頭，輸入 **Value**（值）。

   每個標頭值最多可以包含 16K 個字元。
6. （選用）標頭的 **Log**（日誌）插入活動。
7. 按一下 **OK**（確定）儲存您的變更。

STEP 5 | **Add**（新增） 或編輯安全性政策規則（**Policies**（政策） > **Security**（安全性）），透過此規則，使用者可存取為其設定此標頭插入規則的 SaaS 應用程式。

1. 選擇您在步驟 2 中編輯或建立的 URL 篩選設定檔（**Actions**（動作） > **URL Filtering**（**URL** 篩選））。
2. 按一下 **OK**（確定）以儲存，然後 **Commit**（提交）變更。

STEP 6 | 驗證對 SaaS 應用程式的存取是否按預計方式運作。透過連線至您網路的端點：

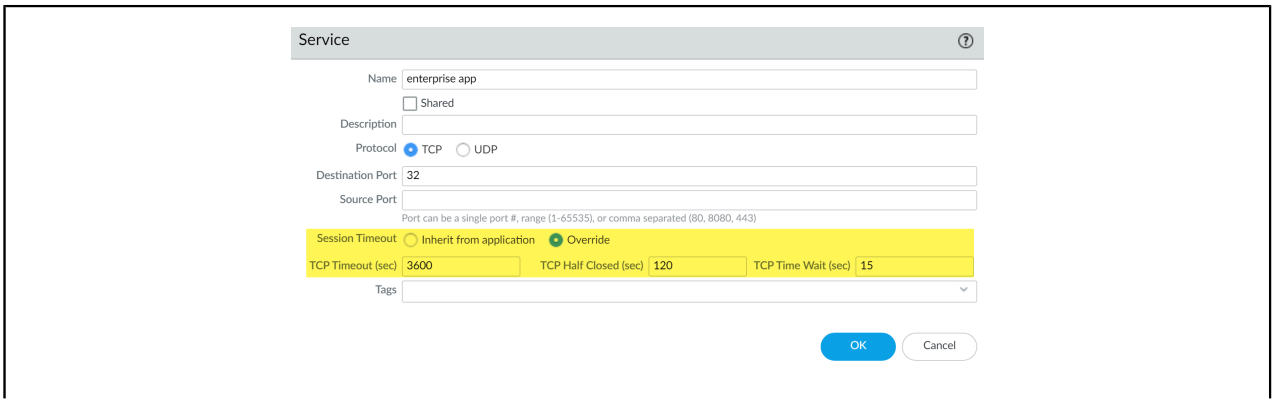
1. 嘗試存取您預計能夠存取的帳戶或內容。如果您無法存取 SaaS 帳戶或內容，則組態未運作。
2. 嘗試存取您預計會遭到封鎖的帳戶或內容。如果您能存取 SaaS 帳戶或內容，則組態未運作。
3. 若上述兩個步驟均按預計方式運作，則可檢視日誌（若您已在步驟 4.6 中組態日誌記錄），而且您應該能夠看到記錄的 HTTP 標頭插入活動。

©2024 Palo Alto Networks, Inc.

為資料中心應用程式維持自訂逾時

從以連接埠為基礎的政策移至以應用程式為基礎的政策時，為應用程式輕鬆維持自訂逾時。使用此方法而不是透過取代 App-ID（會遺失應用程式可見度）或者建立自訂 App-ID（耗時且需進行研究）來維持自訂逾時。

若要開始使用，請作為服務物件的一部分執行自訂逾時設定：



然後，將服務物件新增至政策規則，將自訂逾時套用至執行規則的應用程式。

以下步驟說明了如何將自訂逾時套用至應用程式；若要將自訂逾時套用至使用者群組，您可按照相同的步驟操作，但請確保將服務物件新增至對想向其套用逾時的使用者強制執行的安全性政策規則。

STEP 1 | 選取 **Objects**（物件） > **Services**（服務）以新增或修改服務物件。

此外，您還可在為安全性原則規則定義比對準則時建立服務物件：選取 **Policies**（原則） > **Security**（安全性） > **Service/URL Category**（服務/URL 類別），並 **Add**（新增）新服務物件，將其套用至規則所管理的應用程式流量。

STEP 2 | 選取服務要使用的通訊協定（TCP 或 UDP）。

STEP 3 | 輸入服務使用的目的地連接埠號碼或連接埠號碼範圍。

STEP 4 | 為服務定義工作階段逾時。

- **Inherit from application**（從應用程式繼承）（預設）—沒有套用任何以服務為基礎的逾時；而套用應用程式逾時。
- 取代—為此服務定義自訂工作階段逾時。

©2024 Palo Alto Networks, Inc.

STEP 5 | 若您選擇取代應用程式逾時並定義自訂工作階段逾時，則繼續：

- 輸入 **TCP Timeout**（**TCP** 逾時）值，以秒為單位設定 TCP 工作階段在資料傳輸已開始後可維持開啟的時間上限。當超出這個時間時，工作階段關閉。值的範圍是 1 - 604800，預設值為 3600 秒。
- 輸入 **TCP Half Closed**（**TCP** 半關閉）值，設定在接收第一個 FIN 封包和接收第二個 FIN 封包或 RST 封包之間，工作階段在工作階段表格中停留的時間長度上限（以秒為單位）。如果計時器到期，就會關閉工作階段。值的範圍是 1 - 604800，預設值為 120 秒。
- 輸入 **TCP Wait Time**（**TCP** 等待時間）值，設定在接收第二個 FIN 封包或 RST 封包之後，工作階段在工作階段表格中停留的時間長度上限（以秒為單位）。當計時器到期，就會關閉工作階段。值的範圍是 1 - 600，預設值為 15秒。

STEP 6 | 按一下 **OK**（確定）來儲存服務物件。

STEP 7 | 選取 **Policies**（原則） > **Security**（安全性）並 **Add**（新增）或修改原則規則，以管理您要控制的應用程式流量。

STEP 8 | 選取 **Service/URL Category**（服務/**URL** 類別），並將您剛剛建立的服務物件 **Add**（新增）至安全性原則規則。

STEP 9 | 按一下 **OK**（確定）並 **Commit**（交付）變更。

©2024 Palo Alto Networks, Inc.

Device-ID

Device-ID 概要介紹

根據 2020 年 Unit 42 物聯網威脅報告，普通企業中 30% 的聯網裝置是物聯網。這是一個不斷增長的風險領域，存在許多被惡意使用者利用的可能性。此外，在識別這些裝置後，如何避免其受諸如過時的作業軟體之類漏洞的侵害？使用防火牆上的 Device-ID™，您可以獲取網路上事件的裝置背景資訊，取得針對這些裝置的政策規則建議，基於裝置編寫政策規則，以及根據這些建議強制執行安全性政策。

與 User-ID 提供基於使用者的政策規則和 App-ID 提供基於應用程式的政策規則的方法相似，Device-ID 提供基於裝置的政策規則，而不論其 IP 位址或位置如何變更。透過提供裝置的可追蹤性並將網路事件與特定裝置相關聯，Device-ID 可讓您獲取背景資訊，瞭解事件與裝置的關係，以及新增與裝置相關聯而不是與使用者、位置或 IP 位址（這些會隨著時間而變更）相關聯的政策規則。您可以在安全性、解密、服務品質 (QoS) 和驗證政策中使用 Device-ID。

為了讓 Device-ID 功能在防火牆上可用，您必須購買 IoT Security 訂閱並在執行 IoT Security 裝載程序期間選取防火牆。有兩種類型的 IoT Security 訂閱：

- IoT Security 訂閱
- IoT Security – 不需要 Data Lake (DRDL) 訂閱

對於第一種訂閱，防火牆將資料日誌傳送到記錄服務，該服務將它們串流到 IoT Security 進行分析，並串流到 Cortex Data Lake 執行個體進行存儲。Data Lake 執行個體可以是新的，也可以是現存的。對於第二種訂閱，防火牆將資料日誌傳送到記錄服務，該服務將它們串流到 IoT Security 進行分析，但不會串流到 Cortex Data Lake 執行個體進行存儲。請務必注意，IoT Security 和 IoT Security (DRDL) 訂閱在 IoT Security 和 Device-ID 方面提供相同的功能。

為了允許連接到 IoT Security，防火牆需要裝置授權；為了允許連接到記錄服務，需要記錄服務授權。在連接到 IoT Security 和記錄服務時，防火牆還需要裝置憑證來驗證自身。

如果您在防火牆上使用 PAN-OS 版本 8.1.0 到 PAN-OS 9.1.x，則 IoT Security 授權會為您的裝置提供裝置分類、行為分析和威脅分析。如果使用 PAN-OS 10.0 或更高版本，則可以使用 Device-ID 獲取 IP 位址到裝置的對應，以檢視網路事件的裝置背景資訊，使用 IoT Security 來獲取這些裝置的原則規則建議，並在報告和 ACC 中獲得裝置的可視性。

您可以在使用 *PAN-OS 10.0* 或更高版本的任何 *Panorama* 或防火牆上建立基於裝置的安全性原則。要實施安全性原則，裝置必須具有有效的 *IoT Security* 授權。

為識別和分類裝置，IoT Security 應用程式將使用防火牆上日誌、網路通訊協定和工作階段中的中繼資料。但不包括與裝置識別無關的私人或敏感資訊或資料。中繼資料還構成了裝置預期行為的基礎，然後為原則規則建議建立標準，定義了允許該裝置使用的流量和通訊協定。

當防火牆從 IoT Security 中匯入安全性政策規則建議和 IP 位址到裝置對應時，防火牆會將其裝置憑證傳送到邊緣伺服器以對其自身進行驗證。該邊緣伺服器透過傳送自己的憑證來向防火牆驗證自身。防火牆使用線上憑證狀態通訊協定 (OCSP) 來驗證伺服器的憑證，方法是針對在 TCP 連接埠 80 上使用 HTTP 的以下網站進行檢查：

- o.lencr.org

©2024 Palo Alto Networks, Inc.

- c.lencr.org

當 Panorama 從 IoT Security 中匯入原則規則建議時，Panorama 會執行相同的檢查來驗證邊緣伺服器的憑證。

IoT Security 使用已有的 Palo Alto Networks 防火牆對網路中的裝置進行識別和分類後，您不必實施新裝置或第三方解決方案，Device-ID 可利用此資料將裝置與政策規則進行比對，並為網路事件提供裝置背景資訊。透過防火牆或 Panorama 提供的對流量、應用程式、使用者、裝置和威脅的可視性，您可以立即將網路事件追溯到單個裝置，並獲取保護這些裝置的安全性原則規則建議。

除 *VM-50* 系列、*VM-200* 和 *CN* 系列外，所有支援 *PAN-OS 10.0* 的防火牆平台還支援 *Device-ID* 和 *IoT Security* 。

裝置有六個層級的分類（也稱為屬性）：

屬性	範例
類別	印表機
Profile	`Sharp` 印表機
型號	`MX-6070N`
作業系統版本	`ThreadX 5`
OS Family 作業系統系列	`ThreadX RTOS`
廠商	`SHARP Corporation`

為獲取針對網路中裝置的原則規則建議，防火牆會觀察流量以產生增強型應用程式日誌 (EAL)。然后防火牆將 EAL 轉送到記錄服務。IoT Security 接收來自記錄服務的日誌以進行分析，提供 IP 位址到裝置的對應，並為您的裝置產生最新的政策規則建議。使用 IoT Security，您可以檢閱這些政策規則建議並為這些裝置建立安全性政策規則集。在 IoT Security 中啟動政策規則後，將其匯入防火牆或 Panorama 並提交您的安全性政策。

要識別具有動態指派網路設定的裝置，防火牆必須能夠觀察網路上的 DHCP 廣播和單點傳送流量。IoT Security 還支援靜態 IP 裝置。防火牆能夠觀察到的流量越多，則針對該裝置的原則規則建議就越準確，且針對該裝置的 IP 位址到裝置的對應也越迅速、越準確。當裝置傳送 DHCP 流量以取得其網路設定時，防火牆會觀察到此類型的要求，並產生 EAL 以傳送到記錄服務，在其中，IoT Security 會存取它們以進行分析。

要觀察 *L2* 介面上的流量，必須為該介面設定 *VLAN*。透過允許防火牆將介面視為 *DHCP* 轉送的 *L3* 介面，其可以觀察到 *DHCP* 廣播流量，而不會影響流量或效能。

©2024 Palo Alto Networks, Inc.

由於防火牆需要基於裝置的流量偵測裝置，然後對這些裝置強制實施安全性原則，因此防火牆既充當感應器從裝置收集中繼資料，又充當實施程式對裝置強制實施安全性原則。IoT Security 會在新裝置傳送 DHCP 流量後立即自動偵測到它們，並在第一週內識別出 95# 的裝置。

每個應用程式都有一個單獨的建議，當您在 IoT Security 中啟用其安全性政策規則集時，通常會自動將該建議推送到防火牆或 Panorama。將政策規則建議匯入安全性政策規則庫後，防火牆或 Panorama 會建立至少兩個物件以根據建議定義裝置行為：

- 一個來源裝置物件，用於識別流量來源的裝置設定檔
- 一個或多個目的地物件，用於識別流量的允許目的地，可以是裝置設定檔、IP 位址或完全合格網域名稱 (FQDN)

如果防火牆或 Panorama 上已經存在任何裝置物件，則防火牆或 Panorama 將更新裝置物件，而不是建立新的裝置物件。您可以在安全性、驗證、解密和服務品質 (QoS) 政策規則中使用這些裝置物件。

此外，防火牆為每個規則指派兩個標籤：

- 一個識別來源裝置，包括類別（如 `NetworkDevice - TrendNet`）。
- 一個表明該規則是 IoT 原則規則建議 (`IoTSecurityRecommended`)。

由於防火牆指派到規則的標籤是當對應變得不同步時還原對應的唯一方法，因此請勿編輯或移除它們。

為了最佳部署和操作 Device-ID，我們建議以下最佳做法：

- 在位於網路中央的防火牆上部署 Device-ID。例如，如果在大環境中，請在 IP 位址管理 (IPAM) 裝置上游的防火牆上部署 Device-ID。如果在小環境中，請在充當 DHCP 伺服器的防火牆上部署 Device-ID。更多部署建議，請參見 IoT Security 部署設計指南。
- 在初始部署期間，請允許 Device-ID 從您的網路收集中繼資料，時間為至少十四天。如果裝置沒有每日使用，則識別程序可能需要較長時間。
- 按照從最重要到最不重要裝置的順序，建立基於裝置的政策規則。考量以下事項來對其進行優先排序：
  1. 類別（安全的聯網裝置優先）
  2. 重要裝置（例如伺服器或 MRI 機器）
  3. 特定於環境的裝置（例如火災警報器和標記閱讀器）
  4. 面向消費者的 IoT 裝置（例如智慧型手錶或智慧型喇叭）
- 僅針對內部區域基於每個區域啟用 Device-ID。

©2024 Palo Alto Networks, Inc.

準備部署 Device-ID

若要讓您的網路為部署 Device-ID 做準備，請完成以下前置部署工作，以使防火牆能夠產生增強型應用程式日誌 (EAL)，並透過日誌記錄服務將其傳送到 IoT Security，以進行處理和分析。

STEP 1 | 如果您尚未在防火牆或 Panorama 上安裝裝置憑證，請安裝。

裝置憑證會在連線至記錄服務和 IoT Security 時驗證防火牆。

如果您使用 *Panorama* 來管理多個防火牆，*Palo Alto Networks* 強烈建議將*Device-ID* 部署中的所有防火牆升級到 *PAN-OS 10.0* 或更高版本。如果您建立了一個將 ***Device***（裝置）用作比對準則的規則，且 *Panorama* 將該規則推至使用 *PAN-OS 9.1* 或更早版本的防火牆，則防火牆會忽略 ***Device***（裝置）比對準則，因為它不受支援，這可能會導致政策規則流量比對的問題。

STEP 2 | 在防火牆上安裝裝置授權和記錄服務授權。

若要執行此操作，請按一下 **Device**（裝置） > **Licenses**（授權），然後在 **License Management**（授權管理）區段中選取 **Retrieve license keys from license server**（從授權伺服器擷取授權金鑰）。這會在防火牆上安裝記錄服務和 IoT Security 的授權。

記錄服務授權允許防火牆連線至記錄服務。

裝置授權允許防火牆連線至 IoT Security。

STEP 3 | （僅限 L2 介面）為每個 L2 介面建立一個 VLAN 介面，以便防火牆能夠觀察 DHCP 廣播流量。

©2024 Palo Alto Networks, Inc.

STEP 4 | （選用）設定服務路由以便為 Device-ID 和 IoT Security 允許必要的流量。

依預設，防火牆使用管理介面。要使用其他介面，請完成下列步驟。

1. 如有必要，請設定要用作所需 IoT Security 通訊之來源介面的資料介面。
2. 選擇 **Device**（裝置） > **Setup**（設定） > **Services**（服務） > **Service Route Configuration**（服務路由設定），然後選擇 **Customize**（自訂）。
3. 在 IPv4 頁簽上，選擇 **Data Services**（資料服務），然後選擇要用作來源介面的資料介面。

   其 IP 位址會自動填入「來源位址」欄位。此服務路由用於將增強的應用程式日誌 (EAL) 轉送到日誌記錄服務。

   Device-ID 和 *IoT Security* 不支援 *IPv6*。
4. 按一下 **OK**（確定）。
5. 按一下 **IoT**，選擇與來源介面相同的資料介面，然後按一下 **OK**（確定）。

   此服務路由用於從 IoT Security 中提取 IP 位址到裝置的對應和政策建議。
6. 按一下 **Palo Alto Networks Services**（**Palo Alto Networks** 服務），選擇相同的資料介面，然後按一下 **OK**（確定）。

   此服務路由用於將除 EAL 之外的其他日誌轉送到日誌記錄服務，以及用於從更新伺服器提取裝置字典檔案。
7. 按一下 **OK**（確定）儲存組態變更。

©2024 Palo Alto Networks, Inc.

STEP 5 | （選用）如果在上一步中建立了服務路由，請新增安全性政策規則，允許防火牆使用 IoT Security 所需的服務。

1. 選取 **Policies**（政策） > **Security**（安全性） > **+ Add**（新增）。
2. 在 General（一般）頁簽上，輸入安全性政策規則的名稱，然後選擇 **interzone**（區域間）作為規則類型。
3. 在 Source（來源）頁簽上，選擇 **Any**（任何）作為來源區域，然後 **Add 127.168.0.0/16**（新增 **127.168.0.0/16**）作為來源位址。
4. 在 Destination（目的地）頁簽上，**Add**（新增）具有 IoT Security 的目的地區域，然後為您的區域 **Add**（新增）邊緣服務 FQDN 作為目的地位址。
5. 在 Application（應用程式）頁簽上，**Add paloalto-iot-security**（新增 **paloalto-iot-security**）。

   防火牆使用此應用程式從 IoT Security 中提取 IP 位址到裝置的對應和政策建議。
6. 在 Actions（動作）頁簽上，選擇 **Allow**（允許），然後按一下 **OK**（確定）。
7. 如果您有一個內部網路政策規則，該規則允許日誌記錄服務和更新伺服器所在區域中的所有內部網路流量，則可以使用該規則允許防火牆將日誌轉送到日誌記錄服務並從更新伺服器提取字典檔案。

   否則，請建立一個內部網路政策規則，允許防火牆將這三個應用程式傳送到日誌記錄服務，並從同一區域中防火牆介面的 IP 位址更新伺服器：

   paloalto-shared-services，用於將 EAL 和工作階段日誌轉送到日誌記錄服務

   paloalto-logging-service，用於將 EAL 以外的其他日誌轉送到日誌記錄服務

   paloalto-updates，用於從更新伺服器提取裝置字典檔案

STEP 6 | 如果網際網路與 Panorama 以及 Panorama 管理的新世代防火牆之間存在協力廠商防火牆，請確保它允許 Device-ID 和 IoT Security 的必要流量。

用途	位址	TCP 連接埠
（PAN-OS 10.0.3 版及更新版本）接收區域 FQDN，可允許新世代防火牆從 IoT Security 擷取 IP 位址至裝置對應和政策規則建議。	**enforcer.iot.services-edge.paloaltonetworks.com**	443
（PAN-OS 10.0.0 版及更新版本）允許新世代防火牆接收來自 IoT Security 的政策規則建議和 IP 位址至裝置對應。	美國 **iot.services-edge.paloaltonetworks.com** 加拿大 **ca.iot.services-edge.paloaltonetworks.com**	443

©2024 Palo Alto Networks, Inc.

用途	位址	TCP 連接埠
	歐盟地區 **eu.iot.services-edge.paloaltonetworks.com** 亞太地區 **apac.iot.services-edge.paloaltonetworks.com** 日本 **jp.iot.services-edge.paloaltonetworks.com** 澳大利亞 **au.iot.services-edge.paloaltonetworks.com**	
（PAN-OS 10.0.0 版及更新版本）允許新世代防火牆從更新伺服器下載裝置字典檔案。	**updates.paloaltonetworks.com**	443
（PAN-OS 10.0.0 版及更新版本）允許 Panorama 將日誌查詢傳送到記錄服務。	美國 **iot.services-edge.paloaltonetworks.com** 加拿大 **ca.iot.services-edge.paloaltonetworks.com** 歐盟地區 **eu.iot.services-edge.paloaltonetworks.com** 亞太地區 **apac.iot.services-edge.paloaltonetworks.com** 日本 **jp.iot.services-edge.paloaltonetworks.com** 澳大利亞	443

©2024 Palo Alto Networks, Inc.

用途	位址	TCP 連接埠
	au.iot.services-edge.paloaltonetworks.com	
（IoT Security 訂閱 + Cortex Data Lake）將日誌轉送到 Cortex Data Lake。	請參閱 Cortex Data Lake 所需的 TCP 連接埠和 FQDN。	

依預設，*PAN-OS 10.0.0* 版至 *10.0.2* 版連線到美洲地區中的邊緣服務 *FQDN (iot.services-edge.paloaltonetworks.com)*。要使執行這些 *PAN-OS* 版本的防火牆連接到其他區域中的邊緣服務 *FQDN*，您必須手動設定它（請參閱下一步中的 *FQDN*）。對於 *PAN-OS 10.0.3* 版及更新版本，防火牆會根據 *IoT Security* 裝載程序期間設定的地區，自動探索要使用的正確 *FQDN*。無需手動設定。

STEP 7 | 如果網際網路與新世代防火牆之間存在協力廠商防火牆（沒有 Panorama），請確保它允許 Device-ID 和 IoT Security 的必要流量。

用途	位址	TCP 連接埠
（PAN-OS 10.0.3 版及更新版本）接收區域 FQDN，可允許新世代防火牆從 IoT Security 擷取 IP 位址至裝置對應和政策規則建議。	**enforcer.iot.services-edge.paloaltonetworks.com**	443
（PAN-OS 10.0.0 版及更新版本）允許新世代防火牆接收來自 IoT Security 的政策規則建議和 IP 位址至裝置對應。	美國 **iot.services-edge.paloaltonetworks.com** 加拿大 **ca.iot.services-edge.paloaltonetworks.com** 歐盟地區 **eu.iot.services-edge.paloaltonetworks.com** 亞太地區 **apac.iot.services-edge.paloaltonetworks.com** 日本 **jp.iot.services-edge.paloaltonetworks.com**	443

©2024 Palo Alto Networks, Inc.

用途	位址	TCP 連接埠
	澳大利亞 **au.iot.services-edge.paloaltonetworks.com**	
（PAN-OS 10.0.0 版及更新版本）允許新世代防火牆從更新伺服器下載裝置字典檔案。	**updates.paloaltonetworks.com**	443
（IoT Security 訂閱 + Cortex Data Lake）將日誌轉送到 Cortex Data Lake。	請參閱 Cortex Data Lake 所需的 TCP 連接埠和 FQDN。	

©2024 Palo Alto Networks, Inc.

STEP 8 | 設定防火牆以觀察 DHCP 流量並為其產生日誌，然後轉送日誌以便由 IoT Security 進行處理和分析。

- 如果防火牆作為 DHCP 伺服器：
  1. 啟用增強型應用程式記錄。
  2. 建立一個 Palo Alto Networks 雲端服務的增強型應用程式日誌，以將日誌轉送到日誌記錄服務進行處理。
  3. 啟用 **DHCP Broadcast Session**（**DHCP** 廣播工作階段）選項（**Device**（裝置） > **Setup**（設定） > **Session**（工作階段） > **Session Settings**（工作階段設定））。

     PA-5450 和 *PA-7000* 系列上的 *PAN-OS 11.0.1* 以及執行任何版本的 *PAN-OS 11.0* 的所有其他防火牆都支援此設定。
  4. 建立安全性政策規則以允許 **dhcp** 作為 **Application**（應用程式）類型。
- 如果防火牆不是 DHCP 伺服器，請設定一個介面作為 DHCP 轉送代理程式，以便防火牆能夠為其從用戶端接收的 DHCP 流量產生 EAL。
- 如果 DHCP 伺服器與防火牆介面位於同一網路區段，請在 DHCP 伺服器前面部署虛擬介接介面，以確保防火牆為初始 DHCP 交換中的所有封包產生 EAL，同時對效能的影響最小。
  1. 設定具有相應區域的虛擬介接介面，並啟用 **Multicast Firewalling**（多點傳送防火牆）選項（**Network**（網路） > **Virtual Wires**（虛擬介接） > **Add**（新增））。
  2. 設定一條規則，以允許流量出入虛擬介接區域之間的 DHCP 伺服器。該政策必須允許伺服器當前觀察到的所有現有流量，並使用與其餘規則相同的日誌轉送設定檔。
  3. 要允許 DHCP 伺服器在將 IP 位址作為租用指派到新要求之前檢查 IP 位址是否處於作用中，請設定一條規則以允許從 DHCP 伺服器 ping 子網路的其餘部分。
  4. 設定一條規則，以允許與不轉送日誌以進行流量匹配的 DHCP 伺服器之間的所有其他流量往來。
  5. 設定 DHCP 伺服器主機以使用第一個虛擬介接介面，設定網路交換器使用第二個虛擬介接介面。為最大程度地減少纜線，您可以在交換基礎結構中使用隔離的 VLAN，而不是將 DHCP 伺服器主機直接連線到防火牆。
- 如果您想使用旁接介面來瞭解由於網路的當前設定或拓撲而防火牆通常無法觀察到的 DHCP 流量，最佳做法是使用以下設定。
  1. 設定旁接介面和相應的區域。
  2. 設定一條規則以比對使用與其餘規則相同的日誌轉送設定檔的 DHCP 流量。
  3. 要最大程度地減少防火牆上的工作階段負載，請設定一條規則以丟棄所有其他流量。
  4. 將旁接介面連線到網路交換器上的連接埠鏡像。
- 如果要收集有關其網路流量對防火牆不可見的裝置的資料，請使用以下一個或兩個選項：
  - 使用封裝式遠端交換連接埠分析器 (ERSPAN)，透過一般路由封裝 (GRE) 通道，傳送鏡像流量（來自網路交換機）至防火牆。
  - 設定 DHCP 伺服器以將其包含 IP 位址到 MAC 位址繫結的伺服器日誌傳送到防火牆。

©2024 Palo Alto Networks, Inc.

STEP 9 | 將日誌轉送設定檔套用於您的安全性政策規則。

將 IoT Security 的 Palo Alto Networks 雲端服務的增強型應用程式日誌 套用至您的規則（或更新現有設定檔或建立新的設定檔），以將必要的日誌類型轉送至記錄服務。

©2024 Palo Alto Networks, Inc.

設定 Device-ID

完成以下工作以將 IP 位址到裝置的對應和原則規則建議從 IoT Security 匯入到您的防火牆或 Panorama。

如果您使用 *Panorama* 來管理多個防火牆，*Palo Alto Networks* 強烈建議將*Device-ID* 部署中的所有防火牆升級到 *PAN-OS 10.0* 或更高版本。如果您建立了一個將 ***Device***（裝置）用作比對準則的規則，且 *Panorama* 將該規則推送至使用 *PAN-OS 9.1* 或更早版本的防火牆，則防火牆會忽略 ***Device***（裝置）比對準則，因為它不受支援，這可能會導致原則規則流量比對的問題。

STEP 1 | 在中樞上啟用 IoT Security 授權。

1. 按照電子郵件中收到的指示啟用您的 IoT Security 授權。
2. 初始化您的 IoT Security 應用程式。如需詳細資訊，請參閱開始使用 IoT Security 和 IoT Security 最佳做法。

STEP 2 | 在 IoT Security 中定義安全性政策規則集。

1. 為來源裝置物件 **Create**（建立）一套新的原則規則。

   有關在 IoT Security 中建立安全性政策規則建議的資訊，請參閱建議安全性政策。

2. **Activate**（啟用）安全性政策規則集。

   當您啟用政策規則集時，IoT Security 透過將政策規則集名稱與每個規則中的應用程式名稱連接起來，自動產生政策規則名稱。然後它會自動將規則集推送到 Panorama 和所有訂閱了 IoT Security 服務的新世代防火牆。

STEP 3 | 將政策規則建議匯入防火牆或 Panorama 中的安全性政策規則庫。

1. 開啟或重新整理 **Policy Recommendation**（政策建議）> **IoT** 頁面。

   當您選取 **Policy Recommendation**（政策建議）> **IoT**後，防火牆或 Panorama 會與 IoT Security 進行通訊，以獲取最新政策規則建議。原則規則建議不會在防火牆或 Panorama

©2024 Palo Alto Networks, Inc.

上進行快取。如果在 IoT Security 中啟用或修改新的政策規則集時您已經在此頁面上，則重新整理頁面將從 IoT Security 中擷取新的或更新的建議。

（防火牆）選擇 **Device**（裝置） > **Policy Recommendation**（政策建議） > **IoT**。

(Panorama) 選擇 **Panorama** > **Policy Recommendation**（政策建議） > **IoT**。

2. 選擇要匯入到安全性政策規則庫中的政策規則建議。

   驗證您要匯入的每個規則中的目的地和允許的應用程式是否正確。然後選擇最多十個政策規則建議以匯入規則庫。對於 Panorama，您可以將政策規則建議匯入到多個裝置群組的多個防火牆規則庫中。

3. 選擇 **Import Policy Rule(s)**（匯入政策規則），輸入以下內容，然後按一下 **OK**（確定）：

   （防火牆）

   在規則庫中，選擇您希望 PAN-OS 在其後放置所匯入規則的規則名稱。如果您選擇 **No Rule Selection**（未選取規則），防火牆會將所選規則匯入到頂部。

   (Panorama)

   Location（位置）：選擇一個或多個要匯入政策規則的裝置群組。

   Suggested Location（建議位置）：IoT Security 從新世代防火牆接收的日誌中瞭解區域和裝置群組，並相應地為各種政策規則建議裝置群組。您可以在 **Location**（位置）清單或偏好的任何其他裝置群組中的可用裝置群組中選擇這些建議的裝置群組。

   Destination Type（目的地類型）：選擇 **Pre-Rulebase**（規則庫之前）以在防火牆上本機定義的規則之前新增建議的政策規則，或選擇 **Post-Rulebase**（規則庫之後）以在本機定義的規則之後新增它們。

   After Rule（規則之後）：選擇要在其後新增所匯入規則的規則。如果您選擇 **No Rule Selection**（未選取規則），防火牆會將所選規則匯入到頂部。這是一個選用設定。如果您不選擇規則，匯入的規則將新增到規則庫的頂部。

   Device-ID 規則必須優先於套用至規則庫中相同裝置的任何現有規則。*IoT Security* 使用裝置的受信任行為建立政策規則建議，因此每個規則的預設動作為「允許」。

4. 重複此過程以匯入更多規則，以允許裝置透過指定的應用程式與指定的目的地進行通訊。
5. 按一下 **OK**（確定）並 **Commit**（交付）變更。

©2024 Palo Alto Networks, Inc.

STEP 4 | 在您想要使用 Device-ID 偵測裝置和執行安全性政策規則的每個區域啟用 Device-ID。

依預設，Device-ID 會對應您啟用了 Device-ID 的區域中的所有子網路。您可以在 **Include List**（包含清單）和 **Exclude List**（排除清單）中修改 Device-ID 對應哪些子網路。

最佳做法是，在來源區域中啟用 *Device-ID* 以偵測裝置和執行 *Device-ID* 安全性政策規則。僅為內部區域啟用 *Device-ID*。

1. 選取 **Network**（網路）> **Zones**（區域）。
2. 選取您想要啟用 Device-ID 的區域。
3. **Enable Device Identification**（啟用裝置識別），然後按一下 **OK**（確定）。
4. 根據需要對您要對其執行 Device-ID 安全性政策規則的其他區域重複此操作。

STEP 5 | **Commit**（提交）您的變更。

STEP 6 | 驗證您的安全性政策規則是否正確。

1. 選取 **Policies**（政策），然後選取您根據政策規則建議建立的一條規則。

   IoT Security 會指派說明，包含來源裝置物件和標籤，這些標籤用於標識來源裝置物件以及該規則是來自 IoT Security 的建議。
2. 選取 **Source**（來源）頁簽，然後驗證來源裝置設定檔。
3. 選擇 **Destination**（目的地）頁簽並驗證目的地。
4. 選取 **Application**（應用程式）頁簽，並驗證應用程式。
5. 選取 **Actions**（動作）頁簽，並驗證動作（預設值為 **Allow**（允許））。
6. 使用探索驗證日誌記錄服務是否收到您的日誌並檢閱它獲取了哪些日誌。

STEP 7 | 為沒有 IoT Security 原則規則建議的任何裝置建立自訂裝置物件。

例如，您不能使用政策規則建議保護筆記型電腦和智慧型手機等傳統 IT 裝置，因此，您必須為這些類型的裝置手動建立裝置物件，以在您的安全性政策規則中使用。如需自訂裝置物件的詳細資訊，請參閱 管理 Device-ID。

STEP 8 | 使用裝置物件執行政策規則以及監控並識別潛在問題。

以下清單包含裝置物件的一些範例用例。

- 在安全性、驗證、QoS 和解密政策中使用來源裝置物件和目的地裝置物件。
- 使用解密日誌識別故障以及哪些資產最需要解密。
- 檢視 ACC 中的裝置物件活動以追蹤新裝置和裝置行為。
- 使用裝置物件建立自訂報告（例如，事件報告或稽核）。

©2024 Palo Alto Networks, Inc.

管理 Device-ID

根據需要執行以下工作，以確保您的原則規則建議和裝置物件為最新，或還原原則規則建議對應。

STEP 1 | 根據需要更新政策規則建議。

隨著 IoT 裝置獲得新功能，IoT Security 將更新其政策規則建議，以建議防火牆應允許哪些其他流量或通訊協定。每天查看 IoT Security 以獲取變更，並儘快更新您的政策規則建議。更新過程因您是否使用 Panorama 來管理防火牆而有所不同。

當使用 Panorama 管理防火牆時：

1. (IoT Security) **Edit**（編輯）已啟用政策規則中的政策規則，然後按一下 **Next**（下一步）。
2. 選擇任何新建議，按一下 **Next**（下一步），然後 **Save**（儲存）變更。
3. (Panorama) 選擇 **Policy Recommendation**（政策建議） > **IoT**，然後 **Import Policy Rules**（匯入政策規則）。
4. 選擇一個或多個裝置群組，然後按一下 **Yes**（是）以確認要覆寫規則庫中的當前規則建議和以前匯入的規則。
5. **Commit**（提交）您的變更。

當不使用 Panorama 管理防火牆時：

1. (IoT Security) **Edit**（編輯）已啟用政策規則中的政策規則，然後按一下 **Next**（下一步）。
2. 選擇任何新建議，按一下 **Next**（下一步），然後 **Save**（儲存）變更。
3. (PAN-OS UI) 選擇 **Policy Recommendation**（政策建議） > **IoT**，記下「新更新可用」欄中顯示 `Yes`（是）的任何政策規則建議的詳細資料，然後在 **Policies**（政策）頁面上編輯並儲存相應的已匯入政策規則。
4. 選擇 **Policy Recommendation**（政策建議） > **IoT**，然後 **Sync Policy Rules**（同步政策規則）以重新整理編輯的規則和規則建議之間的對應。

   當 **Policies**（政策）頁面和 **Policy Recommendation**（政策建議） > **IoT** 頁面上的相應規則匹配時，「新更新可用」欄會從 `Yes`（是）變成 `No`（否）。
5. **Commit**（提交）您的變更。

©2024 Palo Alto Networks, Inc.

STEP 2 | 在裝置字典中檢閱、更新和維護裝置物件。

您必須為沒有 *IoT Security* 原則規則建議的任何裝置建立裝置物件。例如，您不能使用 *IoT Security* 政策規則建議保護筆記型電腦和智慧型手機等傳統 *IT* 裝置，因此，您必須為這些類型的裝置建立裝置物件並在您的安全性政策中使用以保護這些裝置。

1. 選取 **Objects**（物件） > **Devices**（裝置）。
2. **Add**（新增）一個裝置物件。
3. **Browse**（瀏覽）清單或使用關鍵字 **Search**（搜尋）。

   搜尋結果可能包含多個類型的裝置物件屬性（例如，同時包含 **Category**（類別）和 **Profile**（設定檔））。
4. 要新增自訂裝置物件，請為裝置物件輸入一個 **Name**（名稱），還可以選擇輸入 **Description**（說明）。

   始終為每個裝置物件使用唯一名稱。不要根據原則規則建議變更裝置物件的說明中的標籤。
5. （僅限 Panorama）選取 **Shared**（共用）選項以使此裝置物件對其他裝置群組可用。
6. 為裝置物件選取屬性（**Category**（類別）、**OS**（作業系統）、**Profile**（設定檔）、**Osfamily**（作業系統系列）、**Model**（型號）和 **Vendor**（廠商））。
7. 按一下 **OK**（確定）確認您的變更。

STEP 3 | 刪除不再需要的任何原則規則建議。

如果政策規則建議不再適用，則可以移除建議和對應到建議的規則。

1. 在 IoT Security 中，從政策規則集中刪除一個或多個政策規則建議。

   Edit（編輯）政策集，清除要移除的政策規則，然後 **Save**（儲存）政策集。
2. 移除規則建議與規則庫中相關規則之間的對應。

   （防火牆）選擇 **Device**（裝置） > **Policy Recommendation**（政策建議） > **IoT**，最多選擇十個要移除的政策規則建議，然後 **Remove Policy Mapping**（移除政策對應）。

   (Panorama) 選擇 **Device**（裝置） > **Policy Recommendation**（政策建議） > **IoT**，最多選擇十個要移除的政策規則建議，**Remove Policy Mapping**（移除政策對應），然後選擇要從中移除對應的 **Location**（位置）。
3. 按一下 **Yes**（是）以確認移除對應。
4. 選取 **Policies**（原則） > **Security**（安全性）。對於 Panorama，選取 **Policies**（原則） > **Security**（安全性） > **Pre-Rules/Post-Rules**（預先規則/後續規則）。
5. 選擇要從規則庫中移除的規則，然後 **Delete**（刪除）它們。
6. **Commit**（提交）您的變更。

STEP 4 | 使用 CLI 命令對防火牆和 IoT Security 之間的問題進行疑難排解。

©2024 Palo Alto Networks, Inc.

Device-ID 的 CLI 命令

使用以下 CLI 命令檢視對防火牆和 IoT Security 之間的任何問題進行疑難排解的資訊。一般來說，包含 **eal** 的 CLI 命令顯示傳出資料的計數器，包含 **icd** 的 CLI 命令顯示傳入資料的計數器。

範例	命令
檢視增強型應用程式記錄 (EAL) 計數器，例如防火牆和 Cortex 資料湖之間的連線數和日誌量。	**show iot eal all**
檢視有關防火牆與 Cortex 資料湖之間連線的更多詳細資料。	**show iot eal conn**
按平面（資料平面或管理平面）檢視 EAL 計數器的摘要，例如 PAN-OS 版本和序號。	**show iot eal dpi-eal**
按平面（資料平面或管理平面）以及按通訊協定檢視 EAL 計數器。	**show iot eal dpi-stats all**
按通訊協定檢視 EAL 計數器。	**show iot eal dpi-stats subtype dhcp|http**
檢視主機資訊設定檔 (HIP) 符合報告計數器的摘要。	**show iot eal hipreport-eal**
檢視 EAL 日誌回應時間計數器。	**show iot eal response-time**
檢視防火牆和 IoT Security 應用程式之間邊際服務連線之健康狀況的詳細資料，以及 IP 位址到裝置的對應和原則規則建議的計數器。	**show iot icd statistics all**
檢視到邊際服務的連線的計數器。	**show iot icd statistics conn**
檢視 IP 位址到裝置的對應的計數器。	**show iot icd statistics verdict**
檢視防火牆上的所有 IP 位址到裝置對應。	**show iot ip-device-mapping-mp all**
檢視特定 IP 位址的 IP 位址到裝置對應。	**show iot ip-device-mapping-mp ip *IP-address***
檢視資料平面上 IP 位址到裝置對應的清單。	**show iot ip-device-mapping all**

©2024 Palo Alto Networks, Inc.

範例	命令
清除管理平面上的 IP 位址到裝置對應。	**debug iot clear-all type device**
清除資料平面上的 IP 位址到裝置對應。	**clear user-cache all**

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

解密

Palo Alto Networks 防火牆可以解密和檢查流量，讓威脅無所遁形，並控制通訊協定、憑證驗證和故障處理。解密可以對加密流量強制執行各種原則，以便防火牆根據您設定的安全性設定處理加密流量。解密流量可防止惡意加密內容進入您的網路，並防止敏感內容隱藏為加密流量而離開您的網路。啟用解密包括備妥解密所需的金鑰與憑證、建立解密設定檔與原則及設定解密連接埠鏡像。

解密概要介紹

Secure Sockets Layer（安全通訊端層，SSL）與 Secure Shell（安全殼層，SSH）加密通訊協定用於保護兩個實體（例如 Web 伺服器與用戶端）之間的流量。SSL 與 SSH 會將流量封裝並加密資料，讓資料只對擁有憑證與金鑰的用戶端與伺服器有意義，憑證用於確認裝置之間值得信任，金鑰則用於將資料解碼。解密 SSL 和 SSH 流量可：

- 防止隱藏為加密流量的惡意軟體滲入您的網路。例如，攻擊者會入侵使用 SSL 解密的網站。員工造訪該網站並在不知情的情況下下載漏洞或惡意軟體。惡意軟體隨後使用受感染的員工端點在網路中橫向傳播，並危及其他系統。
- 防止敏感資訊移到網路之外。
- 確保適當的應用程式在安全的網路上執行。
- 選擇性地解密流量；例如，建立解密原則和設定檔以使金融或健康照護網站的流量免於解密。

Palo Alto Networks 防火牆解密以原則為基礎，可解密、檢查及控制輸入與輸出的 SSL 和 SSH 連線。解密原則可讓您按目的地、來源、服務或 URL 類別指定要解密的流量，並根據相關聯之解密設定檔中的安全性設定封鎖、限制或轉送指定流量。解密設定檔控制 SSL 通訊協定、憑證驗證以及失敗檢查，以防使用弱演算法或不受支援之模式的流量存取該網路。防火牆使用憑證與金鑰將流量解密為純文字，然後在純文字流量上執行 App-ID 與安全性設定，包括「解密」、「防毒」、「漏洞」、「反間諜軟體」、「URL 篩選」、WildFire 及「檔案封鎖」等設定檔。防火牆在解密與檢查流量後，會在流量離開它時重新加密純文字流量，確保流量的隱私性與安全性。

防火牆提供三種類型的解密原則規則：SSL 正向 Proxy以控制輸出的 SSL 流量，SSL 輸入檢查以控制輸入的 SSL 流量，以及 SSH Proxy以控制通道式 SSH 流量。您可將解密設定檔附加到原則規則以將精確存取設定套用於流量，比如檢查伺服器憑證、不受支援的模式以及失敗。

SSL 解密（正向 Proxy 和輸入檢查）需要憑證將防火牆建立為受信任的協力廠商，並在用戶端與伺服器之間建立信任以保護 SSL/TLS 連線安全。您還可以在因技術原因將伺服器排除在 SSL 解密之外（網站因憑證釘選、不受支援的密碼或相互驗證等原因中斷解密）時使用憑證。SSH 加密不需要憑證。

使用解密最佳做法檢查清單，規劃、實作和保持解密部署。

您可以將硬體安全性模組 (HSM) 與防火牆整合，以增強 SSL 正向 Proxy 與 SSL 輸入檢查解密中所使用的私密金鑰安全性。若要進一步瞭解使用 HSM 存放與產生金鑰及將 HSM 與您防火牆整合的詳細資訊，請參閱使用硬體安全性模組保護金鑰。

您還可以使用解密鏡像，將解密流量作為純文字轉送給協力廠商解決方案，以進行其他分析與存檔。

若啟用解密鏡像，請務必留意有關可鏡像的流量與流量的儲存位置與方式的當地法律與法規，因為所有鏡像流量（包括敏感資訊）都以純文字形式轉送。

©2024 Palo Alto Networks, Inc.

解密概念

檢閱以下主題以詳細瞭解解密功能與支援：

- 用於解密原則的金鑰與憑證
- SSL 正向 Proxy
- SSL 正向 Proxy 解密設定檔
- SSL 輸入檢查
- SSL 輸入檢查解密設定檔
- SSL 通訊協定設定解密設定檔
- SSH Proxy
- SSH Proxy 解密設定檔
- 無解密的 SSL 設定檔
- 橢圓曲線加密 (ECC) 憑證的 SSL 解密
- SSL 解密的完美轉送密碼 (PFS) 支援
- SSL 解密與主旨替代名稱 (SAN)
- TLSv1.3 解密
- 解密工作階段高可用性支援
- 解密鏡像

用於解密原則的金鑰與憑證

金鑰是數字字串，一般是透過數學運算亂數與大質數所產生的。金鑰將密碼和共用密碼等字串在未加密純文字與加密密文之間進行轉換。金鑰可以是對稱性 (使用同一個金鑰加密與解密) 或是非對稱性 (使用某個金鑰加密，然後使用在數學上有關係的金鑰解密)。任何系統都能產生金鑰。

X.509 憑證用於建立用戶端與伺服器之間的信任，以建立 SSL 連線。嘗試驗證伺服器的用戶端（或驗證用戶端的伺服器）知道 X.509 憑證的結構，因此知道如何在憑證的欄位內擷取伺服器識別資訊，例如 FQDN 或 IP 位址（在憑證內稱作通用名稱 (common name) 或是 *CN*），或擷取簽發憑證的組織、部門或使用者名稱。憑證授權單位 (CA) 必須簽發所有憑證。CA 驗證用戶端或伺服器後，CA 會簽發憑證並使用私密金鑰簽署憑證。

如果您有兩個具有相同主題和金鑰的 *CA*（***Device***（裝置） > ***Certificate Management***（憑證管理） > ***Device Certificates***（裝置憑證）），且其中一個 *CA* 過期，則刪除（自訂）或停用（預先定義）過期的 *CA*。如果您不刪除或停用過期的 *CA*，如果在受信任鏈中啟用，則防火牆可能構建一個到過期 *CA* 的鏈，從而導致出現封鎖頁面。

如將解密原則套用至流量，則只有在防火牆信任簽署伺服器憑證的 CA 時，才會建立用戶端與伺服器之間的工作階段。為了建立信任，防火牆在其憑證信任清單 (CTL) 中必須有伺服器的根 CA 憑

©2024 Palo Alto Networks, Inc.

證，並使用包含在根 CA 憑證內包含的公開金鑰來驗證特徵碼。接著防火牆會出示由「轉送信任」憑證簽署的伺服器憑證複本，讓用戶端進行驗證。您也可以設定防火牆使用企業 CA 作為 SSL 轉送代理程式的 Forward Trust（轉送信任）憑證。如果防火牆的 CTL 中沒有伺服器的根 CA 憑證，則防火牆會對用戶端出示由「轉送不信任」憑證簽署的伺服器憑證複本。Forward Untrust（轉送不信任）憑證可確認當用戶端嘗試使用不信任的憑證存取伺服器裝載的站點時，系統會以憑證警告提示用戶端。

如需關於憑證的詳細資訊，請參閱憑證管理。

若要控制防火牆信任的受信任 *CA*，可使用防火牆 *Web* 介面上的 ***Device***（裝置）> ***Certificate Management***（憑證管理）> ***Certificates***（憑證）> ***Default Trusted Certificate Authorities***（預設受信任憑證授權單位）頁籤。

下表介紹了 Palo Alto Networks 防火牆用於解密的不同憑證。

用於解密的憑證	說明
轉送信任（用於 SSL 正向 Proxy 解密）	用戶端嘗試連線的網站擁有由防火牆所信任 CA 簽署的憑證時，防火牆在解密期間向用戶端出示的憑證。在伺服器憑證由受信任的 CA 簽署時，若要設定防火牆上向用戶端出示的轉送信任憑證，請參閱設定 SSL 正向 Proxy。 依預設，防火牆會根據目的地伺服器的金鑰大小來決定用於用戶端憑證的金鑰大小。然而，可為 SSL 正向 Proxy 伺服器憑證設定金鑰大小。為了增強安全性，請考量將與轉送信任憑證關聯的私密金鑰儲存在硬體安全性模組上（參見將私密金鑰儲存在 HSM 上）。 將與防火牆的轉送信任 *CA* 憑證相關聯的私密金鑰（而不是防火牆的主要金鑰）備份在安全的儲存庫中，以便在防火牆出現問題時，仍可以存取轉送信任 *CA* 憑證。為了增強安全性，請考量將與轉送信任憑證關聯的私密金鑰儲存在硬體安全性模組上（參見將私密金鑰儲存在 HSM 上）。
轉送不可信（用於 SSL 正向 Proxy 解密）	用戶端嘗試連線的站點擁有由防火牆不信任 CA 簽署的憑證時，防火牆在解密期間向用戶端出示的憑證。若要在防火牆上設定轉送不可信憑證，請參閱設定 SSL 正向 Proxy。
SSL 輸入檢查	網路上伺服器的憑證，要為這些伺服器執行預期送達這些伺服器之流量的 SSL 輸入檢查。將伺服器的憑證匯入到防火牆上。

©2024 Palo Alto Networks, Inc.

用於解密的憑證	說明
	從 *PAN-OS 8.0* 開始，防火牆將使用橢圓曲線 *Diffie-Hellman* 暫時 *(ECDHE)* 算法執行嚴格的憑證檢查。這意味著，若防火牆使用中繼憑證，則必須在升級至 *PAN-OS 8.0* 或更新版本後，將憑證從 *Web* 伺服器重新匯入至防火牆，並將伺服器憑證與中繼憑證合併（安裝鏈結憑證）。否則，憑證鏈中包含中繼憑證的 *SSL* 輸入檢查工作階段發生故障。若要安裝鏈結憑證： 1. 在純文字編輯器（例如記事本）中開啟每個憑證 *(.cer)* 檔案。 2. 將每個憑證端對端貼至頂部的伺服器憑證，且包含下列簽署者。 3. 將檔案儲存為文字 *(.txt)* 或憑證 *(.cer)* 檔案（檔案名稱不能包含空格）。 4. 將合併（鏈結）後的憑證匯入到防火牆。

SSL 正向 Proxy

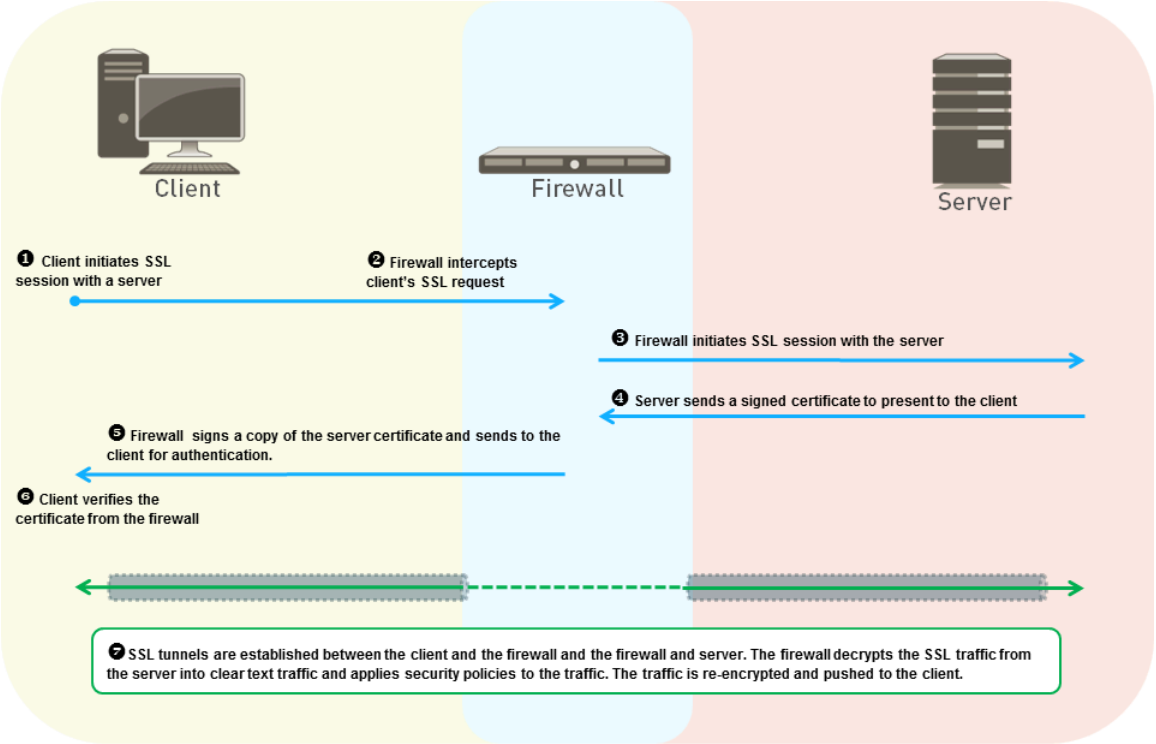
當您設定防火牆解密通往外部網站的 SSL 流量時，防火牆會用作 SSL 正向 Proxy。使用 Ssl 正向 Proxy 解密原則將從內部使用者流到 Web 的 SSL/TLS 流量進行解密與檢查。SSL 正向 Proxy 解密可防止隱藏為 SSL 加密流量的惡意軟體透過解密流量滲入公司網路，以便防火牆可以將解密設定檔和安全性原則及設定檔套用於流量。

在 SSL 正向 Proxy 解密中，防火牆為內部用戶端與外部伺服器之間的媒介。防火牆使用憑證以透明方式向伺服器表明為用戶端，並以透明方式向用戶端表明為伺服器，以便用戶端認為它正與伺服器直接通訊（即使用戶端工作階段的對象是防火牆），並且伺服器認為它正在與用戶端直接通訊（即使伺服器工作階段的對象也是防火牆）。防火牆使用憑證，讓自己成為對用戶端與伺服器之間的工作階段而言值得信任的協力廠商（媒介）（如需憑證的詳細資訊，請參閱用於解密原則的金鑰與憑證）。

由於防火牆是 *Proxy* 裝置，*SSL* 正向 *Proxy* 解密無法解密某些工作階段，例如具有用戶端驗證或固定憑證的工作階段。成為 *Proxy* 還意味著防火牆不支援解密 *SSL* 工作階段的高可用性 *(HA)* 同步。

下圖詳細展示了此流程。關於設定 Ssl 正向 Proxy 的詳細資訊，請參閱設定 Ssl 正向 Proxy。

©2024 Palo Alto Networks, Inc.



1. 網路上的內部用戶端試圖啟動與外部伺服器的 TLS 工作階段。
2. 防火牆攔截用戶端的 SSL 憑證要求。對於用戶端，防火牆充當外部伺服器，即使正在建立的安全工作階段的對象是防火牆，而不是實際伺服器。
3. 防火牆隨後將用戶端 SSL 憑證要求轉送到伺服器，以啟用與伺服器的單獨工作階段。對於伺服器而言，防火牆看起來像用戶端，伺服器不知道有一個媒介，且伺服器驗證了憑證。
4. 伺服器會向防火牆傳送面向用戶端的已簽署憑證。
5. 防火牆分析伺服器憑證。如果伺服器憑證由防火牆信任的 CA 簽署且符合設定的原則及設定檔，則防火牆會產生伺服器憑證的 SSL 轉送信任副本並將其傳送到用戶端。如果伺服器憑證由防火牆不可信的 CA 簽署，則防火牆會產生伺服器憑證的 SSL 轉送不可信副本並將其傳送到用戶端。防火牆產生並傳送到用戶端的憑證副本，包含了原始伺服器憑證中的延伸，並被稱為模擬 (impersonation) 憑證，因為它不是伺服器的真實憑證。若防火牆不可信伺服器，用戶端會看到封鎖頁面警告訊息，表示其嘗試連線的網站不受信任，若您允許使用者選擇退出 SSL 解密，用戶端可以選擇繼續或終止工作階段。
6. 用戶端驗證防火牆的模擬憑證。用戶端隨後啟動與伺服器的工作階段金鑰交換，防火牆會以對憑證執行 Proxy 作業相同的方式對此執行 Proxy 作業。防火牆將用戶端金鑰轉送到伺服器，並為用戶端建立伺服器金鑰的模擬副本，因此防火牆仍然是「隱形」Proxy，用戶端和伺服器相信彼此之間進行了直接工作階段，但仍有兩個單獨的工作階段，一個在用戶端和防火牆之間，另一個在防火牆和伺服器之間。現在各方均有所需的憑證和金鑰，防火牆便可解密流量。
7. 用戶端和伺服器之間的所有 SSL 工作階段流量均以透明方式通過防火牆。防火牆可解密 SSL 流量，將安全性原則和設定檔以及解密設定檔套用於流量，重新加密流量，然後將其轉送。

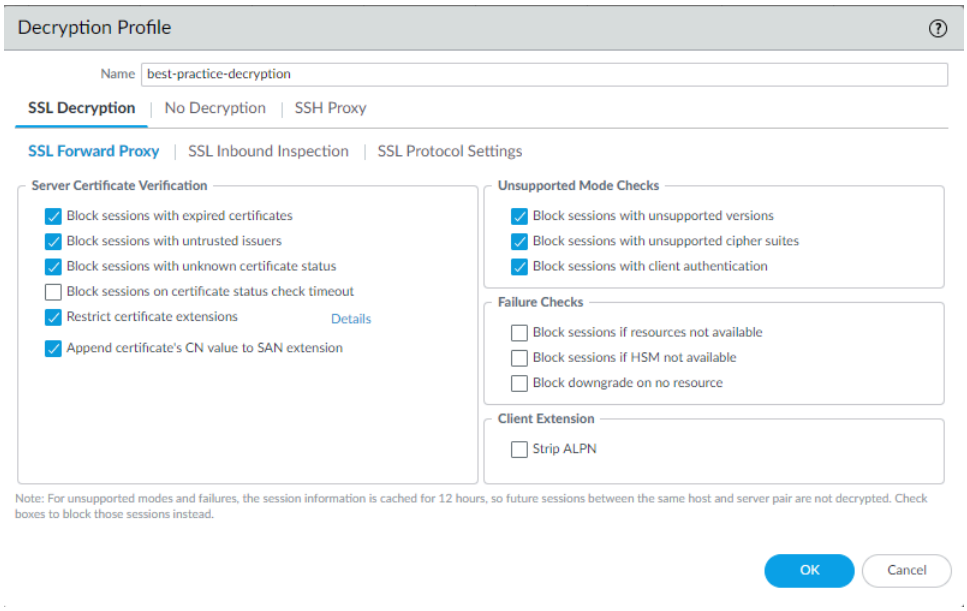
當您設定 *SSL* 正向 *Proxy* 時，通過 *Proxy* 的流量不支援 *DSCP* 代碼點或 *QoS*。

©2024 Palo Alto Networks, Inc.

SSL 正向 Proxy 解密設定檔

針對您附加有設定檔之正向 Proxy 解密原則內定義的輸出 SSL/TLS 流量，SSL 正向 Proxy 解密設定檔（**Objects**（物件） > **Decryption Profile**（解密設定檔） > **SSH Decryption**（**SSH** 解密） > **SSL Forward Proxy**（**SSL** 正向 **Proxy**））會控制伺服器驗證、工作階段模式檢查與失敗檢查。下圖顯示了正向 Proxy 解密設定檔設定的一般最佳做法建議，但您使用的設定還取決於貴公司的安全性符合性規則和當地法律與法規。還對周邊網際網路閘道解密設定檔和資料中心解密設定檔提供了具體的最佳做法。

由於防火牆是 *Proxy* 裝置，*SSL* 正向 *Proxy* 解密無法解密某些工作階段，例如具有用戶端驗證或固定憑證的工作階段。成為 *Proxy* 還意味著防火牆不支援解密 *SSL* 工作階段的高可用性 *(HA)* 同步。

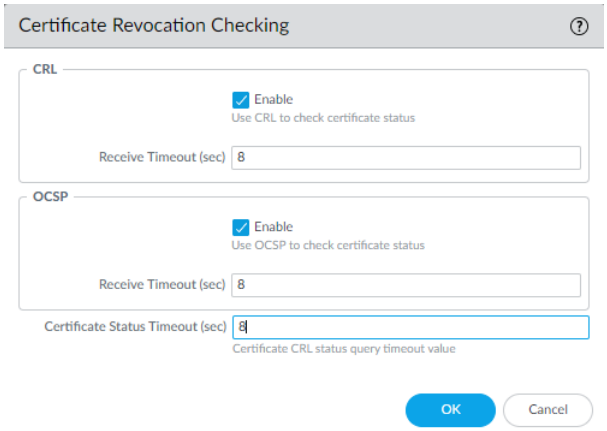


伺服器憑證驗證：

- 封鎖具有過期憑證的工作階段—一律核取此方塊以封鎖與具有過期憑證之伺服器的工作階段，並防止存取可能不安全的網站。若不核取此方塊，則使用者可以與潛在的惡意網站建立連線並進行交易，並在試圖連線時查看警告訊息，但不會阻止連線。
- 封鎖具有不受信任之簽發者的工作階段—一律核取此方塊以封鎖與具有不受信任憑證簽發者之伺服器的工作階段。不受信任的簽發者可能會指出媒介攻擊、重播攻擊或其他攻擊。
- 封鎖憑證狀態未知的工作階段—當伺服器的憑證撤銷狀態傳回狀態「未知」時封鎖 SSL/TLS 工作階段。由於憑證狀態可能因多種原因而未知，對於一般的解密安全性，核取此方塊通常會過多地加強安全性。然而，在網路安全性較高的區域（如資料中心）中，核取此方塊才有意義。
- 憑證狀態檢查逾時時封鎖工作階段—是否在狀態檢查逾時時封鎖工作階段取決於貴公司的安全性符合性立場，因為這是在更嚴格的安全性與更佳的使用者體驗之間的權衡。憑證狀態驗證檢查撤銷伺服器上的憑證撤銷清單 (CRL)，或使用線上憑證狀態通訊協定 (OCSP) 以確定簽發的 CA 是否已撤銷憑證，並且該憑證不應受信任。然而，撤銷伺服器可能回應速度緩慢，導致工作階段逾時，以及防火牆即使在憑證可能有效的情況下也會封鎖工作階段。若在 **Block sessions**

©2024 Palo Alto Networks, Inc.

on certificate status check timeout（憑證狀態檢查逾時時封鎖工作階段）並且撤銷伺服器回應速度緩慢，則可使用 **Device**（裝置） > **Setup**（設定） > **Session**（工作階段） > **Decryption Settings**（解密設定），然後按一下 **Certificate Revocation Checking**（憑證撤銷檢查） 以將預設逾時值 5 秒變更為其他值。例如，您可以將逾時值增加到 8 秒，如下圖所示。由於伺服器憑證可能包含 CRL 分佈點 (CDP) 延伸內的 CRL URL 或授權資訊存取 (AIA) 憑證延伸內的 OCSP URL，同時啟用 CRL 和 OCSP 憑證撤銷檢查。



- 限制憑證延伸—核取此方塊，可將伺服器憑證中的憑證延伸限制為金鑰使用和延伸金鑰使用，並封鎖其他延伸的憑證。然而，在某些部署中，可能需要一些其他憑證延伸，因此，僅在部署不需要其他憑證延伸時核取此方塊。
- 將憑證的 **CN** 值附加至 **SAN** 延伸—核取此方塊，可確保在瀏覽器需要伺服器憑證使用主體替代名稱 (SAN) 並且不支援基於通用名稱 (CN) 的憑證相符項時，若該憑證沒有 SAN 延伸，則使用者仍可以存取所要求的 Web 資源，因為防火牆將 SAN 延伸（基於 CN）新增到模擬憑證。

不受支援的模式檢查。如果未封鎖採用不受支援模式的工作階段，則使用者會在其與可能不安全的伺服器連線時收到警告訊息，並且他們可以按一下該訊息並造訪存在潛在危險的網站。封鎖這些工作階段可以保護您免受伺服器（使用了存在風險的弱通訊協定版本和演算法）的攻擊：

- 封鎖具有不受支援版本的工作階段—當您設定 SSL 通訊協定設定解密設定檔時，您可以指定網路上允許的最低 SSL 通訊協定版本，以透過封鎖弱通訊協定來減少受攻擊面。一律核取此方塊，封鎖已選擇不支援之弱 SSL/TLS 通訊協定版本的工作階段。
- 封鎖具有不受支援密碼套件的工作階段—一律核取此方塊，可在防火牆不支援交握中指定的密碼套件時封鎖工作階段。您可以在解密設定檔的 **SSL Protocol Settings**（**SSL** 通訊協定設定）頁籤上設定防火牆支援的演算法。
- 封鎖用戶端驗證的工作階段—如果沒有需要用戶端驗證的重要應用程式，請將其封鎖，因為防火牆無法解密需要用戶端驗證的工作階段。防火牆需要用戶端和伺服器憑證才能執行雙向解密，但使用用戶端驗證，防火牆只知道伺服器憑證。防火牆會中斷用戶端驗證工作階段的解密。核取此方塊後，防火牆會封鎖所有用戶端驗證的工作階段，但 SSL 解密排除清

©2024 Palo Alto Networks, Inc.

單（**Device**（裝置） > **Certificate Management**（憑證管理） > **SSL Decryption Exclusion**（**SSL** 解密排除項））上網站中的工作階段除外。

若沒有封鎖具有用戶端驗證的工作階段，則在防火牆試圖解密使用用戶端驗證的工作階段時，防火牆會允許該工作階段，並新增一個項目（包含伺服器 URL/IP 位址、應用程式以及解密設定檔）至其本機解密排除快取。

您可能需要允許來自使用用戶端驗證以及不在 *SSL* 解密排除項清單中預先定義網站中的網站的網路流量。建立的解密設定檔容許用戶端驗證的工作階段。將其新增到僅適用於託管該應用程式之伺服器的解密原則規則。為了進一步增強安全性，您可以要求多因素驗證來完成使用者登入過程。

失敗檢查：

- 當資源不可用時封鎖工作階段—如果當沒有防火牆處理資源可用時封鎖工作階段，則防火牆會在其沒有資源來解密流量時丟棄該流量。如果當防火牆由於缺少資源而不能處理解密時不封鎖工作階段，那麼您想要解密的流量進入網路時將仍然為加密狀態，因此不會被檢查。但是，若在資源不可用時封鎖工作階段，則會讓使用者無法存取通常可臨時存取的網站，從而影響使用者體驗。是否實作此失敗檢查取決於貴公司的安全性符合性立場，以及使用者體驗的重要性（與更嚴格的安全性權衡利弊）。或者，考慮使用具有更強處理能力的防火牆型號，以便您可以解密更多流量。
- **HSM** 不可用時封鎖工作階段—如果使用硬體安全性模組 (HSM) 儲存私密金鑰，則是否使用私密金鑰取決於有關私密金鑰來源的合規性規則以及 HSM 不可用時如何處理加密流量。例如，如果貴公司強制使用 HSM 進行私密金鑰簽署，則會在 HSM 不可用時封鎖工作階段。然而，如果貴公司對此並不嚴格，則在 HSM 不可用時可以考慮不封鎖工作階段。（如果 HSM 關閉，則防火牆可以針對其已快取來自 HSM 之回應的網站處理解密，但不會處理其他網站的解密。）這種情況下的最佳做法取決於貴公司的原則。如果 HSM 對您的業務至關重要，請在高可用性 (HA) 配對中執行 HSM（PAN-OS 8.1 支援 HSM HA 配對中的兩個成員）。
- 無資源時封鎖降級—防止防火牆在沒有可用的 TLSv1.3 處理資源時從 TLSv1.3 降級到 TLSv1.2。如果封鎖降級，那麼當防火牆用盡 TLSv1.3 資源時，它會丟棄使用 TLSv1.3 的流量，而不是將其降級至 TLSv1.2。如果不封鎖降級，那麼當防火牆用盡 TLSv1.3 資源時，它會降級至 TLSv1.2。但是，若在防火牆處理資源不可用時封鎖降級，則會讓使用者無法存取通常可臨時存取的網站，從而影響使用者體驗。是否實作此失敗檢查取決於貴公司的安全性符合性立場，以及使用者體驗的重要性（與更嚴格的安全性權衡利弊）。對於不想要降級 TLS 版本的敏感流量，您可能想要建立單獨的解密原則和設定檔來控管其解密。

SSL 輸入檢查

使用 SSL 輸入檢查可對從用戶端流向目標網路伺服器（任何您有其憑證並能將憑證匯入到防火牆上的伺服器）的輸入 SSL/TLS 流量進行解密與檢查，並封鎖可疑工作階段。例如，假設惡意行為者想要利用 Web 伺服器中的已知漏洞。輸入 SSL/TLS 解密提供對流量的可見度，從而允許防火牆主動回應威脅。

SSL 輸入檢查的工作方式與 SSL 正向 Proxy 類似，不同之處在於防火牆解密流入內部伺服器的輸入流量，而不是解密來自內部用戶端的輸出流量。防火牆作為外部用戶端與內部伺服器之間的中間

©2024 Palo Alto Networks, Inc.

人 Proxy，并為每個安全的工作階段產生新的工作階段金鑰。防火牆在用戶端與防火牆之間建立一個安全的工作階段，在防火牆與伺服器之間建立另一個安全的工作階段，以解密和檢查流量。

由於防火牆是 *Proxy* 裝置，*SSL* 輸入檢查無法解密某些工作階段，例如具有用戶端驗證或固定憑證的工作階段。成為 *Proxy* 還意味著防火牆不支援解密 *SSL* 工作階段的高可用性 *(HA)* 同步。

在防火牆上，您必須為要執行 SSL 輸入檢查的每個伺服器安裝憑證與私密金鑰。防火牆驗證目標伺服器在 SSL/TLS 交握期間傳送的憑證與解密政策規則中的憑證是否相符。如果存在相符項，防火牆會將伺服器的憑證轉送給發出要求的伺服器存取的用戶端，並建立安全的連線。

Web 伺服器支援的 TLS 版本決定在防火牆上安裝伺服器憑證和金鑰的方式。如果您的 Web 伺服器支援 TLS 1.2 和 Rivest、Shamir、Adleman (RSA) 或完整轉寄密碼 (PFS) 金鑰交換演算法並且您的終端實體（分葉）憑證由中繼憑證簽署，我們建議上傳憑證鏈（單一檔案）到防火牆。上傳憑證鏈可避免用戶端伺服器憑證驗證問題。

TLS 1.3 移除了對 *RSA* 金鑰交換演算法的支援。

防火牆處理 TLS 1.3 連線的方式與處理 TLS 1.2 連線的方式不同。在 TLS 1.3 交握期間，防火牆向用戶端傳送與從伺服器接收的憑證或憑證鏈相同的憑證或憑證鏈。因此，如果正確設定 Web 伺服器，將伺服器憑證和私密金鑰上傳到防火牆就足夠了。例如，如果伺服器的分葉憑證由中繼憑證簽署，就需要在伺服器上安裝憑證鏈，以避免出現用戶端伺服器驗證問題。

©2024 Palo Alto Networks, Inc.

多憑證支援

SSL 輸入檢查政策規則最多支援 *12* 個憑證，使您能夠更新受保護內部伺服器的憑證，而不會造成停機。有效的憑證必須始終存在於政策規則和伺服器上，才能進行連續解密。在伺服器憑證過期或以其他方式失效之前，應續訂憑證或獲取新憑證。然後，將憑證和私密金鑰匯入防火牆，並將其新增至 *SSL* 輸入檢查政策規則，然後再將相同的憑證安裝到 *Web* 伺服器上。使用新憑證更新您的政策規則，而另一個憑證在 *Web* 伺服器上處於作用中狀態時，會讓防火牆準備好解密流向伺服器的流量，而不論使用中的憑證為何。

當您準備好部署新憑證時，請將其載入您的 *Web* 伺服器，並檢查是否已正確安裝。安裝新憑證不會影響現有的連線。防火牆會驗證 *Server Hello* 訊息中的憑證與解密政策規則中的新憑證是否相符。如果不符，工作階段就會結束。對應的解密日誌項目會將工作階段結束原因報告為防火牆與伺服器憑證不相符。記錄成功交握，以檢視在所有輸入檢查工作階段中使用的伺服器憑證。

您還可以建立政策規則來檢查流向託管各種網域且每個網域都有各自憑證之伺服器的流量。

(Panorama™) 在 *PAN-OS 10.2* 之前的 *PAN-OS®* 版本中，不支援 *SSL* 輸入檢查政策規則中具有多個憑證。如果您將具有多個憑證的 *SSL* 輸入檢查政策規則從執行 *PAN-OS 11.0* 的 *Panorama* 管理伺服器推送到執行較早版本的防火牆，則受管理防火牆上的政策規則只會繼承依照字母順序排序的憑證清單中的第一個憑證。

在從 *Panorama* 推送解密政策規則之前，建議您為執行 *PAN-OS 10.1* 及較早版本的防火牆設定不同的範本或裝置群組，以確保推送正確的政策規則和憑證到適當的防火牆。

為 *SSL* 輸入檢查流量設定 SSL 通訊協定設定解密設定檔時，需為具有不同安全性功能的伺服器建立單獨的設定檔。例如，若一組伺服器僅支援 *RSA*，則 *SSL* 通訊協定設定僅需要支援 *RSA*。但是，支援 *PFS* 的伺服器的 *SSL* 通訊協定設定應支援 *PFS*。設定 *SSL* 通訊協定設定可獲取伺服器支援的最高安全性等級，但檢查效能可確保防火牆資源可以處理更高安全性通訊協定和演算法要求的更高處理負載。

SSL 輸入檢查不支援工作階段恢復。

當您設定 *SSL* 輸入檢查時，通過 *Proxy* 的流量不支援 *DSCP* 代碼點或 *QoS*。

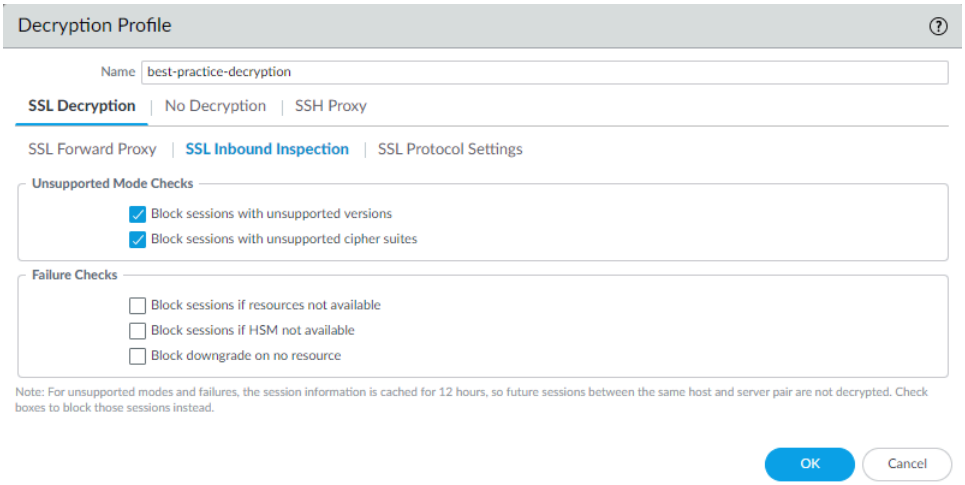
為了保護內部伺服器，請按照步驟操作，設定 SSL 輸入檢查政策規則。

©2024 Palo Alto Networks, Inc.

SSL 輸入檢查解密設定檔

針對您附加有設定檔之輸入檢查解密原則內定義的輸入 SSL/TLS 流量，SSL 輸入檢查解密設定檔（**Objects**（物件） > **Decryption Profile**（解密設定檔） > **SSH Decryption**（**SSH** 解密） > **SSL Inbound Inspection**（**SSL** 輸入檢查））會控制工作階段模式檢查與失敗檢查。下圖顯示了輸入檢查解密設定檔設定的一般最佳做法建議，但您使用的設定還取決於貴公司的安全性符合性規則和當地法律與法規。

由於防火牆是 *Proxy* 裝置，*SSL* 輸入檢查無法解密某些工作階段，例如具有用戶端驗證或固定憑證的工作階段。成為 *Proxy* 還意味著防火牆不支援解密 *SSL* 工作階段的高可用性 *(HA)* 同步。



不受支援的模式檢查。如果未封鎖採用不受支援模式的工作階段，則使用者會在其與可能不安全的伺服器連線時收到警告訊息，並且他們可以按一下該訊息並造訪存在潛在危險的網站。封鎖這些工作階段可以保護您免受伺服器（使用了存在風險的弱通訊協定版本和演算法）的攻擊：

1. 封鎖具有不受支援版本的工作階段—當您設定 SSL 通訊協定設定解密設定檔時，您可以指定網路上允許的最低 TLS 通訊協定版本，以透過封鎖弱通訊協定來減少受攻擊面。一律核取此方塊，封鎖已選擇不支援之弱 SSL 和 TLS 通訊協定版本的工作階段。
2. 封鎖具有不受支援密碼套件的工作階段—一律核取此方塊，可在防火牆不支援交握中指定的密碼套件時封鎖工作階段。您可以在解密設定檔的 **SSL Protocol Settings**（**SSL** 通訊協定設定）頁籤上設定防火牆支援的演算法。

失敗檢查：

- 當資源不可用時封鎖工作階段—如果當沒有防火牆處理資源可用時封鎖工作階段，則防火牆會在其沒有資源來解密流量時丟棄該流量。如果當防火牆由於缺少資源而不能處理解密時不封鎖工作階段，那麼您想要解密的流量進入網路時將仍然為加密狀態，因此不會被檢查。但是，若在資源不可用時封鎖工作階段，則會讓使用者無法存取通常可臨時存取的網站，從而影響使用者體驗。是否實作此失敗檢查取決於貴公司的安全性符合性立場，以及使用者體驗的重要性（與更嚴格的安全性權衡利弊）。或者，考慮使用具有更強處理能力的防火牆型號，以便您可以解密更多流量。

©2024 Palo Alto Networks, Inc.

- **HSM** 不可用時封鎖工作階段—如果使用硬體安全性模組 (HSM) 儲存私密金鑰，則是否使用私密金鑰取決於有關私密金鑰來源的合規性規則以及 HSM 不可用時如何處理加密流量。例如，如果貴公司強制使用 HSM 進行私密金鑰簽署，則會在 HSM 不可用時封鎖工作階段。然而，如果貴公司對此並不嚴格，則在 HSM 不可用時可以考慮不封鎖工作階段。（如果 HSM 關閉，則防火牆可以針對其已快取來自 HSM 之回應的網站處理解密，但不會處理其他網站的解密。）這種情況下的最佳做法取決於貴公司的原則。如果 HSM 對您的業務至關重要，請在高可用性 (HA) 配對中執行 HSM（PAN-OS 8.1 支援 HSM HA 配對中的兩個成員）。
- 無資源時封鎖降級—防止防火牆在沒有可用的 TLSv1.3 處理資源時從 TLSv1.3 降級到 TLSv1.2。如果封鎖降級，那麼當防火牆用盡 TLSv1.3 資源時，它會丟棄使用 TLSv1.3 的流量，而不是將其降級至 TLSv1.2。如果不封鎖降級，那麼當防火牆用盡 TLSv1.3 資源時，它會降級至 TLSv1.2。但是，若在防火牆處理資源不可用時封鎖降級，則會讓使用者無法存取通常可臨時存取的網站，從而影響使用者體驗。是否實作此失敗檢查取決於貴公司的安全性符合性立場，以及使用者體驗的重要性（與更嚴格的安全性權衡利弊）。對於不想要降級 TLS 版本的敏感流量，您可能想要建立單獨的解密原則和設定檔來控管其解密。

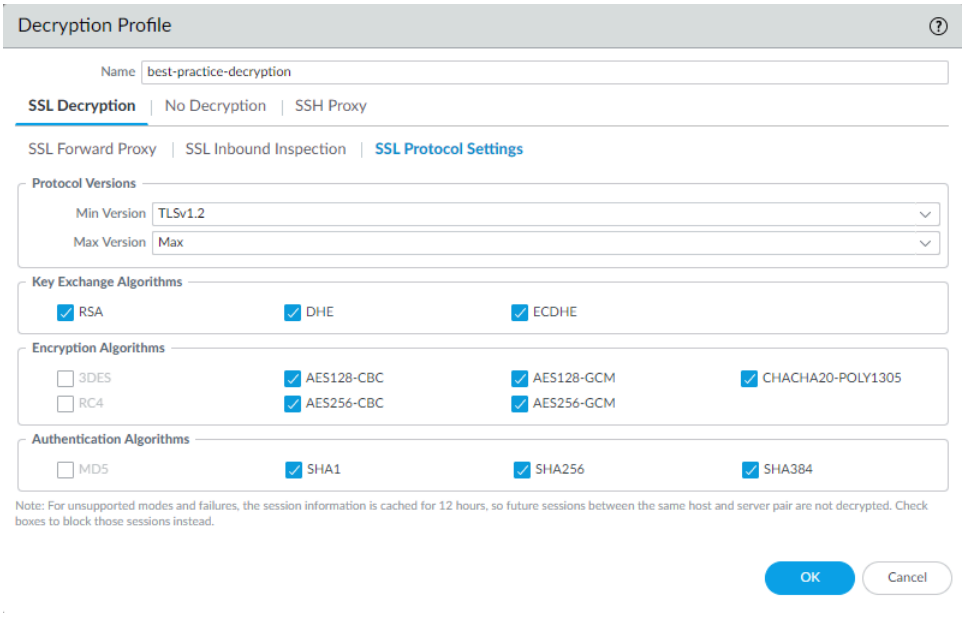
SSL 通訊協定設定解密設定檔

SSL 通訊協定設定（**Objects**（物件） > **Decryption Profile**（解密設定檔） > **SSL Decryption**（**SSL** 解密） > **SSL Protocol Settings**（**SSL** 通訊協定設定））控制您是否允許有漏洞的 SSL/TLS 通訊協定版本、弱加密演算法以及弱驗證演算法。SSL 通訊協定設定套用於輸出 SSL 正向 Proxy 和輸入 SSL 輸入檢查流量。這些設定不會套用於 SSH Proxy 流量或您不解密的流量。

下圖顯示了 SSL 通訊協定設定的一般最佳做法建議。還對周邊網際網路閘道解密設定檔和資料中心解密設定檔提供了具體的最佳做法。

為 *SSL* 輸入檢查流量設定 *SSL* 通訊協定設定時，需為具有不同安全性功能的伺服器建立單獨的設定檔。例如，若一組伺服器僅支援 *RSA*，則 *SSL* 通訊協定設定僅需要支援 *RSA*。但是，支援 *PFS* 的伺服器的 *SSL* 通訊協定設定應支援 *PFS*。設定 *SSL* 通訊協定設定可獲取要保護之目標伺服器支援的最高安全性等級，但檢查效能可確保防火牆資源可以處理更高安全性通訊協定和演算法要求的更高處理負載。

©2024 Palo Alto Networks, Inc.



通訊協定版本：

- 將 **Min Version**（最低版本）設定為 **TLSv1.2** 即可提供最強的安全性—重視安全性的業務網站支援 TLSv1.2。如果網站（或某類網站）僅支援加密強度較弱的密碼，請檢閱該網站並確定其是否託管合法的業務應用程式。若有包含，則僅對該網站進行例外處理，方式是：設定與網站支援的最強密碼相符之 **Min Version**（最低版本）的解密設定檔，然後將該設定檔套用於解密原則規則，從而僅對一個或多個有問題的網站限制使用弱密碼。若網站沒有託管合法的業務應用程式，請勿降低安全性等級來支援網站—弱通訊協定（和密碼）包含攻擊者可以利用的已知漏洞。

  如果網站屬於出於業務目的而不需要的某類網站，請使用 URL 篩選來封鎖對整個類別的存取權限。請勿支援弱加密或驗證演算法，除非必須這樣做才能支援重要的舊式網站，並且當您建立例外時，請建立單獨的解密設定檔，以僅對這些網站使用較弱的通訊協定。不要只是為了容納一些例外而將大多數網站使用的主要解密設定檔降級為 TLSv1.1。

  Qualys SSL Labs SSL Pulse 網頁提供了有關世界上 *150,000* 個最受歡迎的網站中使用不同密碼與通訊協定的百分比的最新統計資料，方便您瞭解趨勢以及全球範圍內對更安全密碼與通訊協定的支援程度。

- 將 **Max Version**（最高版本）設定為 **Max**（最高）而不是特定版本，以便通訊協定可以改進，防火牆自動支援最新與最佳的通訊協定。無論您打算將解密設定檔附加到管理輸入（SSL 輸入檢查）還是輸出（SSL 轉送 Proxy）流量的解密原則規則，都要避免允許採用弱演算法。

  如果您的解密原則支援行動應用程式（其中許多使用釘選的憑證），請將 ***Max Version***（最大版本）設定為 ***TLSv1.2***。由於 *TLSv1.3* 會加密在之前的 *TLS* 版本中未加密的憑證資訊，防火牆無法基於憑證資訊自動新增解密排除項，這會影響一些行動應用程式。因此，如果您啟用 *TLSv1.3*，防火牆可能會丟棄一些行動應用程式流量，除非您為該流量建立「不解密」原則。

  如果您瞭解出於業務目的而使用的行動應用程式，請考慮為這些應用程式建立單獨的解密原則和設定檔，以便您可以為所有其他應用程式流量啟用 *TLSv1.3*。

©2024 Palo Alto Networks, Inc.

金鑰交換演算法：核取全部三個方塊（預設）以同時支援 RSA 和 PFS（DHE 和 ECDHE）金鑰交換，除非最低版本設定為 TLSv1.3，導致僅支援 ECDHE。

若要支援 *HTTP/2* 流量，您必須核取 *ECDHE* 方塊。

加密演算法：在將最低通訊協定版本設定為 TLSv1.2 時，將會自動取消核取（封鎖）較舊、較弱的 3DES 和 RC4 演算法。在將最低通訊協定版本設定為 TLSv1.3 時，將會自動封鎖 3DES、RC4、AES128-CBC 和 AES256-CBC 演算法。對於必須允許加密強度較弱的 TLS 通訊協定的任何流量，請建立單獨的解密設定檔並僅將其套用於該網站，並取消選中適當的方塊以允許該演算法。允許使用 3DES 或 RC4 演算法的流量會使您的網路面臨大量風險。如果封鎖 3DES 或 RC4 會妨礙您存取業務中必須使用的網站，請為該網站建立單獨的解密設定檔和原則。請勿弱化任何其他網站的解密。

驗證演算法：防火牆會自動封鎖較舊、較弱的 MD5 演算法。當 TLSv1.3 為最低版本時，防火牆還會封鎖 SHA1。請勿在網路中允許 MD5 驗證的流量；SHA1 是您應該允許的最弱驗證演算法。如果沒有必要的網站使用 SHA1，請封鎖 SHA1 流量以進一步減少受攻擊面。

SSH Proxy

在 SSH Proxy 組態中，防火牆位於用戶端與伺服器之間。SSH Proxy 使防火牆能夠對輸入和輸出 SSH 連線進行解密，並確保攻擊者不會使用 SSH 來挖掘不需要的應用程式和內容。SSH 解密不需要憑證，防火牆會在其啟動時自動產生用於 SSH 解密的金鑰。在啟動程序期間，防火牆會檢查是否有現有的金鑰。若沒有，防火牆則產生一個金鑰。防火牆使用金鑰來對已在防火牆設定之所有虛擬系統的 SSH 工作階段以及所有 SSH v2 工作階段進行解密。

SSH 允許通道作業，可隱藏惡意流量以免解密。防火牆無法解密 SSH 通道內的流量。透過為應用程式 **ssh-tunnel** 設定安全性原則規則，並將 **Action**（動作）設定為 **Deny**（拒絕），可以封鎖所有 SSH 通道流量（以及允許來自 **ssh** 應用程式之流量的安全性原則規則）。

SSH 通道作業工作階段可發掘 X11 Windows 封包和 TCP 封包。一個 SSH 連線可能包含多個通道。當您將 SSH 解密設定檔套用至流量時，對於連線中的每個通道，防火牆都會檢查流量的 App-ID 並識別通道類型。通道類型可以是：

- 工作階段
- X11
- forwarded-tcpip
- direct-tcpip

當通道類型是工作階段時，防火牆會將流量識別為允許的 SSH 流量，如 SFTP 或 SCP。當通道類型是 X11、forwarded-tcpip 或 direct-tcpip 時，防火牆會將流量識別為 SSH 通道流量並將其封鎖。

僅限管理員使用 *SSH* 管理網路裝置，記錄所有 *SSH* 流量以及考量設定多因素驗證，有助於確保只有合法使用者可以使用 *SSH* 存取裝置，從而減少受攻擊面。

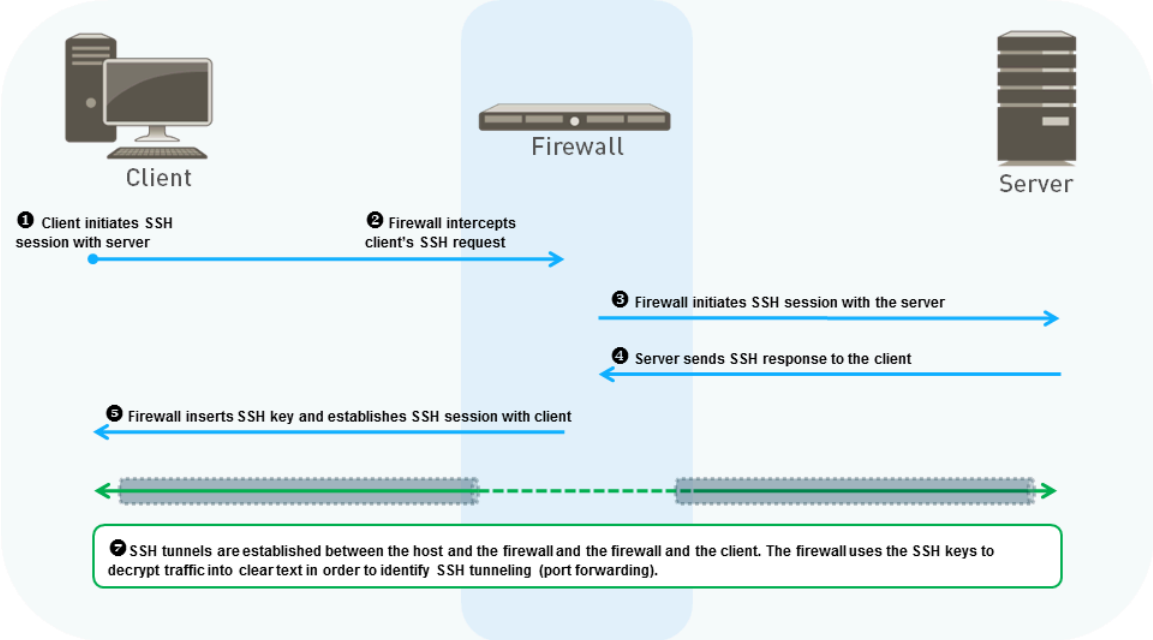
©2024 Palo Alto Networks, Inc.

在防火牆上啟用 *SSH* 解密後，由於 *SSH* 用戶端不再使用公開金鑰型驗證，向具有憑證的主機驗證失敗，因此伺服器無法使用用戶端可以使用其私密金鑰解密來完成交握的公開金鑰。用使用者名稱和密碼驗證來啟動 *SSH* 工作階段。

對於必須使用金鑰型驗證的系統，請將 *SSH* 解密政策規則設定為排除需要公開金鑰驗證的系統。若要編輯 *SSH* 解密政策規則：

1. 前往 ***Policies***（政策） > ***Decryption***（解密），然後選取控制 *SSH* 解密的政策規則。
2. 選取 ***Destination***（目的地）頁籤。
3. 新增要從規則中排除的系統 *IP* 位址。
4. 選取 ***Negate***（否定）。
5. 按一下 ***OK***（確定）。
6. ***Commit***（提交）變更。

下圖顯示了 SSH Proxy 解密的運作原理。關於如何啟用 SSH Proxy 解密的詳細資訊，請參閱設定 SSH Proxy。



1. 用戶端向伺服器傳送 SSH 要求以啟動工作階段。
2. 防火牆攔截用戶端的 SSH 要求。
3. 防火牆將要求轉送至伺服器，並啟動與伺服器的 SSH 工作階段。這會建立防火牆建立之兩個單獨的工作階段中的第一個工作階段。每個工作階段都會建立單獨的 SSH 通道。

©2024 Palo Alto Networks, Inc.

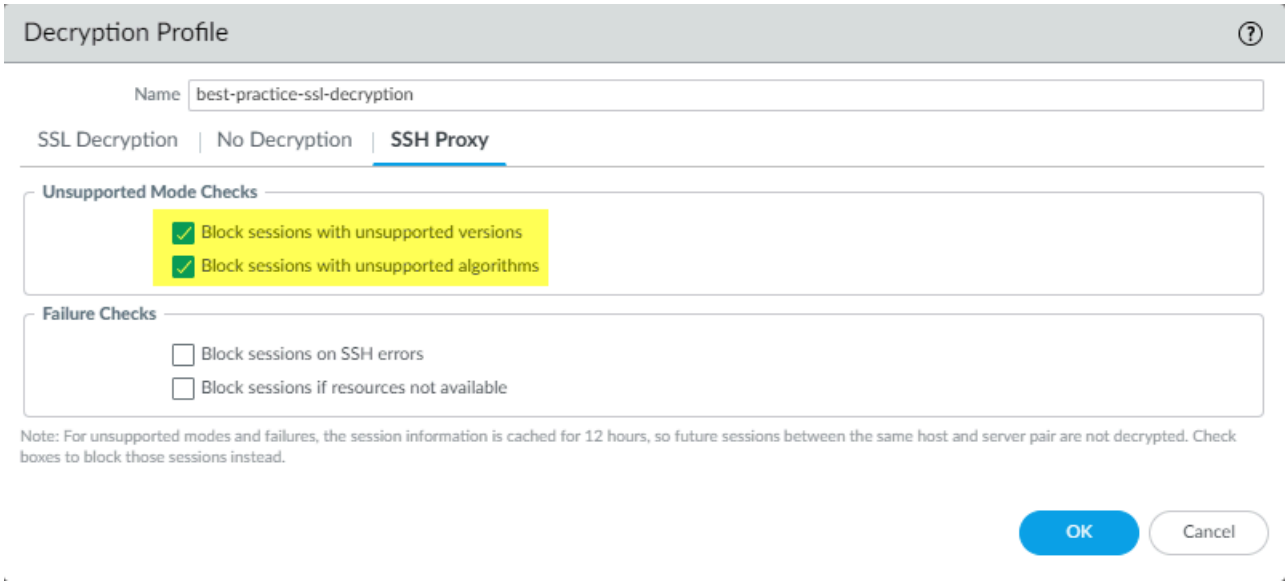
4. 伺服器回應防火牆攔截的要求。
5. 防火牆將 SSH 金鑰插入到伺服器的回應中，並將其轉送至用戶端。這會建立防火牆建立之第二個單獨的工作階段（以及單獨的 SSH 通道）。
6. （圖中「7」的第一部分）防火牆與伺服器和用戶端建立單獨的工作階段後，防火牆充當它們之間的 Proxy。
7. 防火牆會檢查用戶端與伺服器之間的流量，以查看其是否正常路由，或是否使用 SSH 連接埠轉送（SSH 通道）。如果防火牆識別出 SSH 連接埠轉送，則防火牆會封鎖通道流量，並根據設定的安全性政策加以限制。防火牆只會尋找 SSH 連接埠轉送，不會在 SSH 通道上執行內容和威脅檢查。

當您設定 *SSH Proxy* 時，通過 *Proxy* 的流量不支援 *DSCP* 代碼點或 *QoS*。

SSH Proxy 解密設定檔

針對您附加有設定檔之 SSH Proxy 解密原則內定義的 SSH 流量，SSH Proxy 解密設定檔（**Objects**（物件） > **Decryption Profile**（解密設定檔） > **SSH Proxy**）會控制工作階段模式檢查與失敗檢查。下圖顯示了 SSH Proxy 解密設定檔設定的一般最佳做法建議，但您使用的設定還取決於貴公司的安全性符合性規則和當地法律與法規。

防火牆不對 *SSH* 通道（連接埠轉送）執行內容和威脅檢查。然而，防火牆會區分 *SSH* 應用程式和 *SSH* 通道應用程式。如果防火牆識別了 *SSH* 通道，它便會封鎖 *SSH* 通道式流量並根據已設定的安全性原則限制流量。



不受支援的模式檢查。防火牆支援 SSHv2。如果未封鎖採用不受支援模式的工作階段，則使用者會在其與可能不安全的伺服器連線時收到警告訊息，並且他們可以按一下該訊息並造訪存在潛在危險的網站。封鎖這些工作階段可以保護您免受伺服器（使用了存在風險的弱通訊協定版本和演算法）的攻擊：

©2024 Palo Alto Networks, Inc.

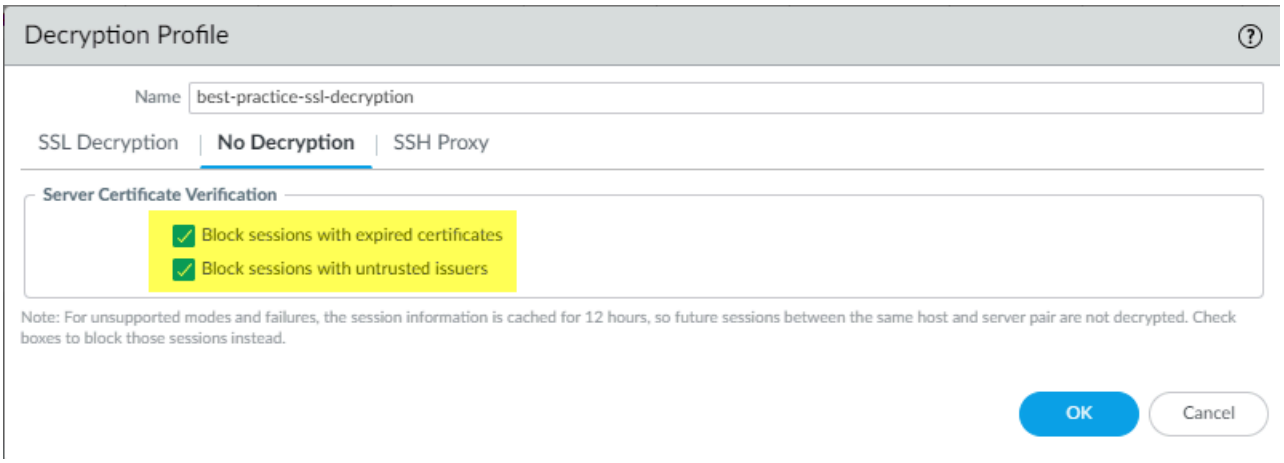
1. 封鎖具有不受支援版本的工作階段—防火牆具有一組預先定義的受支援版本。核取此方塊會封鎖較弱版本的流量。一律核取此方塊，封鎖弱通訊協定版本的工作階段以減少受攻擊面。
2. 封鎖具有不受支援演算法的工作階段—防火牆具有一組預先定義的受支援演算法。核取此方塊會封鎖弱演算法的流量。一律核取此方塊，封鎖具有不受支援演算法的工作階段以減少受攻擊面。

失敗檢查：

- **SSH** 發生錯誤時封鎖工作階段—核取此方塊將會在發生 SSH 錯誤時終止工作階段。
- 資源不可用時封鎖工作階段—若在防火牆處理資源不可用時沒有封鎖工作階段，則要解密的加密流量仍會以加密形式進入網路，從而導致具有潛在危險連線的風險。但是，若在防火牆處理資源不可用時封鎖工作階段，則會讓使用者無法存取通常可臨時存取的網站，從而影響使用者體驗。是否實作失敗檢查取決於貴公司的安全性符合性立場，以及使用者體驗對您的業務的重要性（與更嚴格的安全性權衡利弊）。或者，考慮使用具有更強處理能力的防火牆型號，以便您可以解密更多流量。

「不解密」的設定檔

「不解密」設定檔（**Objects**（物件） > **Decryption Profile**（解密設定檔） > **No Decryption**（不解密））為您選擇不解密的流量執行伺服器驗證檢查。將「不解密」設定檔附加到「不解密」解密原則，定義要從解密中排除的流量。（請勿使用原則排除無法解密的流量，因為網站會因釘選憑證或相互驗證之類的技術原因而中斷解密。而是將主機名稱新增到解密排除項清單。） 下圖顯示了「不解密」設定檔設定的一般最佳做法建議，但您使用的設定還取決於貴公司的安全性符合性規則和當地法律與法規。



- 封鎖具有過期憑證的工作階段—核取此方塊以封鎖與具有過期憑證之伺服器的工作階段，並防止存取可能不安全的網站。若不核取此方塊，則使用者可以與潛在的惡意網站建立連線並進行交易，並在試圖連線時查看警告訊息，但不會阻止連線。
- 封鎖具有不受信任之簽發者的工作階段—核取此方塊以封鎖與具有不受信任憑證簽發者之伺服器的工作階段。不受信任的簽發者可能會指出媒介攻擊、重播攻擊或其他攻擊。

©2024 Palo Alto Networks, Inc.

對於不解密的 *TLSv1.3* 流量，不要將不解密設定檔附加至解密原則。與以前的版本不同，*TLSv1.3* 會加密憑證資訊，防火牆無法查看憑證資料，因此無法封鎖具有過期憑證或不受信任簽發者的工作階段，這樣，設定檔便沒有效果。（防火牆可以使用 *TLSv1.2* 及早前版本執行憑證檢查，因為這些通訊協定不會加密憑證資訊，您應將「不解密」設定檔套用至其流量。）但是，您應為不解密的 *TLSv1.3* 流量建立解密原則，因為除非解密原則控制未解密的流量，否則防火牆不會記錄該流量。

（適用於 *TLSv1.2* 和更早版本）如果您選擇允許具有不受信任簽發者的工作階段（不建議），且僅允許封鎖憑證過期的工作階段，則可能會有具有受信任但已過期的簽發者的工作階段無意中被封鎖。如果防火牆的憑證存儲區包含有效的、自我簽署的受信任 *CA*，且伺服器在憑證鏈中傳送了過期的 *CA*，則防火牆不會檢查其憑證存儲區。相反，當防火牆應找到受信任的有效替代信任錨並允許基於該受信任的自我簽署憑證的工作階段時，其會根據到期的 *CA* 封鎖工作階段。

要避免這種狀況，除了封鎖憑證過期的工作階段外，還需啟用封鎖具有不受信任簽發者的工作階段的封鎖工作階段。這將強制防火牆檢查其憑證存儲區，並找到自我簽署的受信任 *CA*，並允許該工作階段。

橢圓曲線加密 (ECC) 憑證的 SSL 解密

防火牆將自動解密使用 ECC 憑證之網站和應用程式的 SSL 流量，包括橢圓曲線數字特徵碼演算法 (ECDSA) 憑證。隨著組織轉向使用 ECC 憑證以受益於強金鑰和較小的憑證大小，您可以繼續保持監控並安全啟用受 ECC 保護之應用程式和網站的流量。

對於鏡像至防火牆的流量，不支援對使用 *ECC* 憑證之網站和應用程式進行解密；使用 *ECC* 憑證的加密流量必須直接通過防火牆，以便防火牆進行解密。

您可以使用硬體安全性模組 (HSM) 來儲存與 *ECDSA* 憑證關聯的私密金鑰。對於 *TLSv1.3* 流量，*PAN-OS* 僅對於 *SSL* 正向 *Proxy* 支援 *HSM*。它對於 *SSL* 輸入檢查不支援 *HSM*。

SSL 解密的完美轉送密碼 (PFS) 支援

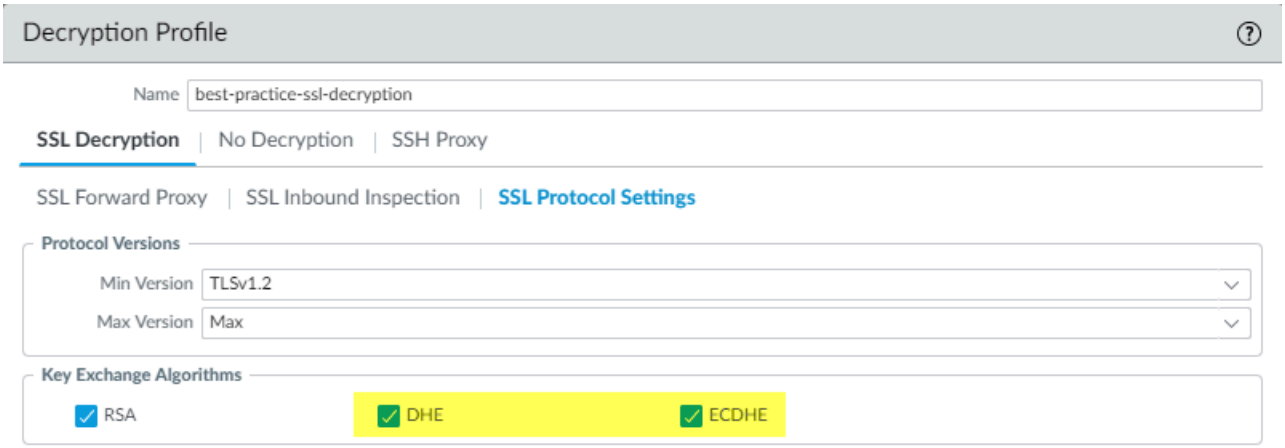
PFS 是一種安全的通訊協定，用於防止一個加密工作階段洩露造成多個加密工作階段洩露。透過 PFS，伺服器將為其在用戶端上建立的每個安全工作階段建立唯一私密金鑰。如果伺服器私密金鑰洩露，僅有使用該金鑰建立的單一工作階段才易受攻擊的 — 攻擊者無法從過去及未來的工作階段擷取資料，因為伺服器將使用所產生的唯一金鑰建立了連線的工作階段。防火牆將解密使用 PFS 金鑰交換演算法建立的 SSL 工作階段，並為過去和未來的工作階段保留 PFS 保護。

預設會啟用對基於 Diffie-Hellman (DHE) 之 PFS 和基於橢圓曲線 Diffie-Hellman (ECDHE) 之 PFS 的支援（**Objects**（物件）> **Decryption Profile**（解密設定檔）> **SSL Decryption**（**SSL** 解密）> **SSL Protocol Settings**（**SSL** 通訊協定設定））。

如果您使用 *DHE* 或 *ECDHE* 金鑰交換演算法啟用 *SSL* 解密的 *PFS* 支援，則可使用硬體安全性模組 (HSM) 來儲存用於 *SSL* 輸入檢查的私密金鑰。

©2024 Palo Alto Networks, Inc.

當您設定 *SSL* 輸入檢查並使用 *PFS* 加密時，不支援工作階段繼續執行。

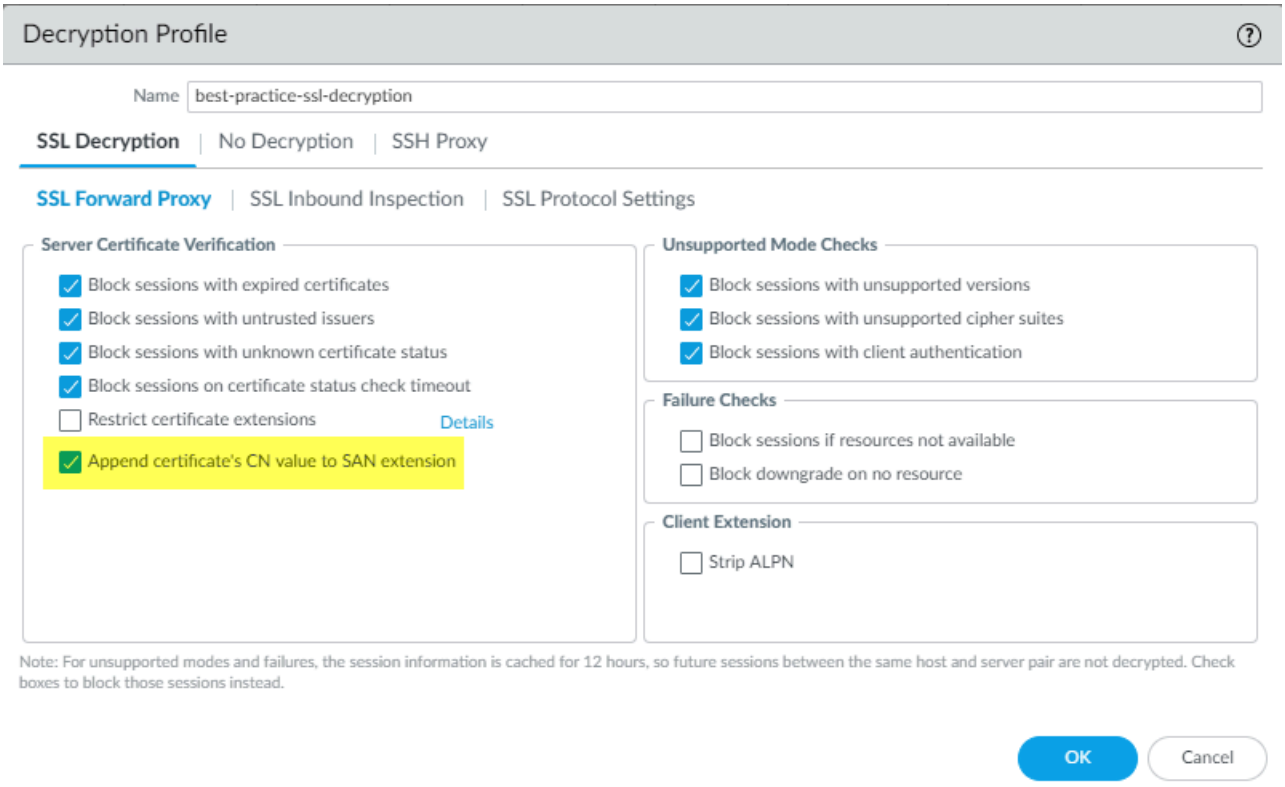


SSL 解密與主旨替代名稱 (SAN)

部分瀏覽器要求伺服器憑証使用主旨替代名稱 (SAN) 來指定憑證所保護的網域，不再支援依據伺服器憑證通用名稱 (CN) 執行憑證比對。透過 SAN，單個伺服器憑證可保護多個名稱；CN 的定義完善度不如 SAN，而且僅可保護單個網域或者網域上的所有一級子網域。但是，如果伺服器憑證僅包含 CN，需要 SAN 的瀏覽器將不會允許一般使用者連線至所要求的 Web 資源。防火牆可將 SAN 新增至其所產生的模擬憑證，以使其在 SSL 解密中充當受信任的協力廠商。伺服器憑證僅包含 CN 時，執行 SSL 解密的防火牆會將伺服器憑證 CN 複製到模擬憑證 SAN 中。防火牆向用戶端出示包含 SAN 的模擬憑證，瀏覽器能夠支援連線。一般使用者可繼續存取所需資源，防火牆可解密工作階段。

若要為解密 SSL 流量啟用 SAN 支援，請更新附加至相關解密原則的解密設定檔：選取 **Objects**（物件） > **Decryption Profile**（解密設定檔） > **SSL Decryption**（**SSL** 解密） > **SSL Forward Proxy**（**SSL** 正向 **Proxy**） > **Append Certificate's CN Value to SAN Extension**（將憑證的 **CN** 值附加至 **SAN** 副檔名）。

©2024 Palo Alto Networks, Inc.



TLSv1.3 解密

您可以解密 TLSv1.3 流量，全面瞭解 TLSv1.3 流量中的已知和未知威脅，並進行防禦。TLSv1.3 是 TLS 通訊協定的最新版本，可提供改進的應用程式安全性和效能。若要支援 TLSv1.3 解密，您必須將解密設定檔套用於現有和新的解密政策規則，並將 TLSv1.3 設定為最低通訊協定版本或將 Max（最高）或 TLSv1.3 設定為最高通訊協定版本。您可以編輯現有設定檔以支援 TLSv1.3。如果您未在解密設定檔中指定 TLSv1.3 支援，依預設，PAN-OS 支援 TLSv1.2 作為最高通訊協定版本。防火牆支援正向 Proxy、輸入檢查、解密網路封包代理程式流量和解密連接埠鏡像的 TLSv1.3 解密。

要使用 TLSv1.3，用戶端和伺服器必須能夠交涉 TLSv1.3 密碼。對於不支援 TLSv1.3 的網站，防火牆會選取伺服器支援的舊版 TLS 通訊協定。

防火牆支援 TLSv1.3 的以下解密演算法：

- TLS13-AES-128-GCM-SHA256
- TLS13-AES-256-GCM-SHA384
- TLS13-CHACHA20-POLY1305-SHA256

如果您套用至解密流量的解密設定檔指定通訊協定的 **Max Version**（最高版本）為 **Max**（最高），那麼設定檔將支援 TLSv1.3，且會對支援 TLSv1.3 的網站自動使用 TLSv1.3。（您可以將 **Max Version**（最高版本）設定為 **TLSv1.3** 以支援 TLSv1.3，但是當下一個版本的 TLS 發佈時，您將需要更新設定檔。將 **Max Version**（最高版本）設定為 **Max**（最高）可適應設定檔，以在新 TLS 版本發佈時進行自動支援。） 當您升級到 PAN-OS 10.0 時，**Max Version**（最高版本）設定為

©2024 Palo Alto Networks, Inc.

Max（最高）的所有解密設定檔都會重設為 **TLSv1.2**，以自動支援使用釘選憑證的行動應用程式，並防止丟棄該流量。

並非所有應用程式都支援 TLSv1.3 通訊協定。按照解密最佳做法，將 TLS 通訊協定的 **Min Version**（最低版本）設定為 **TLSv1.2**，並將 **Max Version**（最高版本）設定保留為 **Max**（最高）。如果因業務需求需要允許使用較弱的 TLS 通訊協定，請建立一個 **Min Version**（最低版本）且允許使用較弱通訊協定的單獨 SSL 解密設定檔，並將其附加到定義需要透過較弱 TLS 通訊協定允許的流量的解密原則中。

如果您的解密原則支援行動應用程式（其中許多使用釘選的憑證），請將 **Max Version**（最大版本）設定為 **TLSv1.2**。由於 TLSv1.3 會加密在之前的 TLS 版本中未加密的憑證資訊，防火牆無法基於憑證資訊自動新增解密排除項，這會影響一些行動應用程式。因此，如果您啟用 TLSv1.3，防火牆可能會丟棄一些行動應用程式流量，除非您為該流量建立「不解密」原則。如果您瞭解出於業務目的而使用的行動應用程式，請考慮為這些應用程式建立單獨的解密原則和設定檔，以便您可以為所有其他流量啟用 TLSv1.3。

如果您知道某個特定原則僅控制 *TLSv1.3* 流量，對於不解密的 *TLSv1.3* 流量，不要將不解密設定檔附加至解密原則。與之前 *TLS* 版本相比的一個變更是，*TLSv1.3* 會加密憑證資訊，因此防火牆無法再瞭解該資料，因此無法封鎖具有過期憑證或不受信任簽發者的工作階段，這樣，設定檔便沒有效果。（防火牆可以使用 *TLSv1.2* 及早前版本執行憑證檢查，因為這些通訊協定不會加密憑證資訊，您應將「不解密」設定檔套用至其流量。）但是，您可以透過在解密原則中啟用記錄成功和不成功的 *TLS* 交握來記錄所有類型的未解密流量（預設啟用記錄不成功的 *TLS* 交握）。

當您在 SSL 通訊協定設定解密設定檔中允許不受支援的模式時，防火牆會自動將流量新增到本機解密排除快取。防火牆仍會解密並檢查從 TLSv1.3 降級到 TLSv1.2 的流量，且快取中顯示的將伺服器新增到快取的 **Reason**（原因） 是 TLS13_UNSUPPORTED。

如果您從 PAN-OS 11.0 降級到之前的版本，將 TLSv1.3 指定為 **Min Version**（最低版本）或 **Max Version**（最高版本）的任何解密設定檔都會變更為受支援的最高版本。例如，從 PAN-OS 11.0 降級到 PAN-OS 9.1 會將 TLSv1.3 取代為 TLSv1.2。如果執行 PAN-OS 11.0 的 Panorama 裝置將設定推送到執行舊版 PAN-OS 的裝置，則將 TLSv1.3 指定為 **Min Version**（最低版本）或 **Max Version**（最高版本）的任何解密設定檔也都會變更為受支援的最高版本。

對於使用硬體安全性模組 *(HSM)* 的客戶，*PAN-OS* 僅對 *SSL* 正向 *Proxy* 支援 *TLSv1.3*。它對於 *SSL* 輸入檢查不支援 *HSM*。

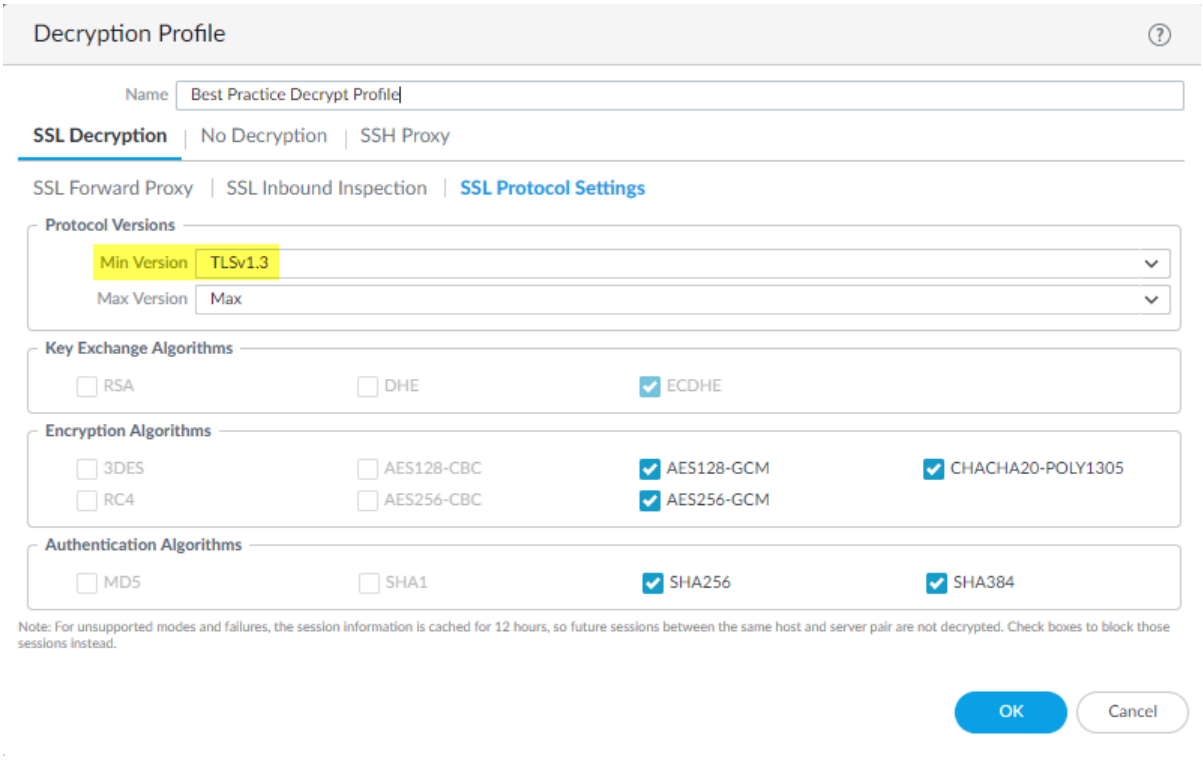
您可以設定 SSL 解密設定檔，將 TLSv1.3 設定為允許的最低通訊協定版本，以實現最牢固的安全性。但是，某些應用程式不支援 TLSv1.3，如果 TLSv1.3 是允許的最低通訊協定，這些應用程式可能無法運作。僅將把 TLSv1.3 設定為最低版本的設定檔套用至僅支援 TLSv1.3 的應用程式流量。

1. 建立新的 SSL 解密設定檔或編輯現有設定檔（**Objects**（物件） > **Decryption**（解密） > **Decryption Profile**（解密設定檔））。

   如果是新設定檔，請指定設定檔 **Name**（名稱）。
2. 選取 **SSL Protocol Settings**（**SSL** 通訊協定設定）。

©2024 Palo Alto Networks, Inc.

3. 將 **Min Version**（最低版本）變更為 **TLSv1.3**。



   Max Version（最高版本）使用 **Max**（最高）可確保該設定檔控制的流量使用可用的最強通訊協定版本。**Min Version**（最低版本）設定流量可使用的最弱通訊協定版本。將最低版本設定為 **TLSv1.3** 意味著流量必須使用 TLSv1.3（或更高版本），更弱的通訊協定版本將被封鎖。（解密原則規則定義設定檔控制的流量。）

   當您將 TLSv1.3 設定為 **Min Version**（最低版本）時，必須使用完美轉送密碼 (PFS)，更弱的金鑰交換、加密和驗證演算法將不可用。

4. 設定您需要設定或變更的任何其他解密設定檔設定。
5. 按一下 **OK**（確定）來儲存設定檔。
6. 將設定檔附加到適當的解密原則規則以將其套用至適當的流量。

解密的工作階段不支援高可用性

容錯移轉之後，對於解密的 SSL 工作階段，防火牆不支援高可用性 (HA) 同步。防火牆不會繼續解密的 SSL 正向 Proxy、SSL 輸入檢查或 SSH Proxy 工作階段。防火牆根據解密原則解密在容錯移轉之後開始的新工作階段。

解密鏡像

解密鏡像可讓您從防火牆建立解密的流量複本，再將複本傳送到可接收原始封包擷取的流量集合工具（例如 NetWitness 或 Solera）以執行封存和分析。對於因論證和歷史用途或資料洩露保護 (DLP) 功能而需要廣泛擷取資料的組織而言，可安裝免費授權，以啟用此功能。

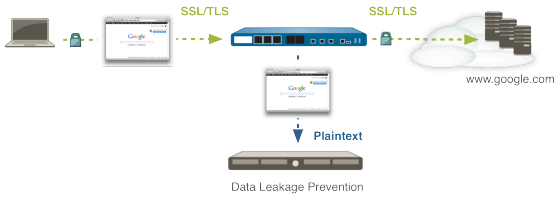
©2024 Palo Alto Networks, Inc.

在您安裝完授權後，請將流量收集工具直接連線至防火牆上的乙太網路介面，並將**Interface Type**（介面類型）設定為 **Decrypt Mirror**（解密鏡像）。防火牆使用收集工具模擬 TCP 交握，然後透過該介面傳送解密的每個資料封包（以純文字形式）。

解密連接埠鏡像在公共雲端平台（*AWS*、*Azure*、*Google* 雲端平台）不可用於 *VM* 系列以及 *VMware NSX*。

請記住，SSL 流量的解密、存放、檢查和/或使用在某些國家是受到管制的，必須經過使用者同意才能使用解密連接埠鏡像功能。此外，使用此功能會讓具有管理權限的惡意使用者存取防火牆，以收集使用者名稱、密碼、身分證字號、信用卡號或其他使用加密通道提交的機密資料。Palo Alto Networks 建議您在生產環境中啟動與使用此功能前，先向公司顧問諮詢。

下列圖片顯示了鏡像解密流量和連接埠的過程，設定解密連接埠鏡像一節中介紹了如何授權和啟用此功能。



©2024 Palo Alto Networks, Inc.

準備部署解密

部署解密最耗時的部分不是設定解密原則及設定檔，而是部署的準備工作：與利益關係人合作決定要解密和不解密的流量，為使用者群體提供有關網站存取權限變更的訓練，開發私密金鑰基礎結構 (PKI) 策略，並規劃設定有優先順序的分階段部署。

設定解密目標並檢閱解密規劃最佳做法檢查清單，以確保您瞭解建議的最佳做法。最佳做法目標是解密防火牆資源允許的盡可能多的流量，並先解密最重要的流量。

在建立和部署解密原則規則之前，從以連接埠為基礎的安全性原則規則移轉至以應用程式為基礎的安全性原則規則。如果您根據以連接埠為基礎的安全性原則建立解密規則，然後移轉至以應用程式為基礎的安全性原則，則變更可能會導致解密規則封鎖您打算允許的流量，因為安全性原則規則可能使用應用程式預設連接埠來防止應用程式流量使用非標準連接埠。例如，識別為 *Web* 瀏覽應用程式流量（預設連接埠為 *80*）的流量可能具有擁有不同預設連接埠的基礎應用程式，如 *HTTPS* 流量（預設連接埠為 *443*）。應用程式預設規則封鎖 *HTTPS* 流量，因為它使用「非標準」連接埠（*443* 而不是 *80*）查看解密流量。在部署解密之前移轉到以 *App-ID* 為基礎的規則意味著，當您在 *POC* 中測試解密部署時，您將發現安全性原則設定錯誤並在將其推廣到一般使用者群體之前進行修正。

若要準備部署解密：

- 與利益關係人合作制定解密部署策略
- 制定 PKI 部署計劃
- 調整解密防火牆部署的大小
- 規劃設定有優先順序的分階段部署

與利益關係人合作制定解密部署策略

與法律、財務、人力資源、高階主管、安全性部門和 IT /支援部門等利益關係人合作，共同制定解密部署策略。首先獲得解密流量所需核准，以保障公司安全。解密流量需瞭解法律法規和業務需求對您可以解密和不能解密的內容有何影響。

識別要解密的流量並對其設定優先順序。最佳做法是解密盡可能多的流量，以便發現加密流量中的潛在威脅並防止這些威脅。如果防火牆規模不當，阻止您解密要解密的所有流量，則對最關鍵的伺服器、最高風險的流量類別以及不太可信的區段和 IP 子網路設定優先順序。為幫助設定優先順序，可以問自己這樣的問題：「如果此伺服器遭到入侵該怎麼辦？」和「對於我想達到的效能層級，我願意承擔多大的風險？」

接下來，識別無法解密的流量，因為流量會因釘選憑證、不完整的憑證鏈、不受支援的密碼或相互驗證之類的技術原因而中斷解密。解密技術性破壞解密站點會封鎖該流量。對技術上中斷解密的網站進行評估，並自問是否出於業務原因需要存取這些網站。若不需要存取這些網站，則允許解密對其進行封鎖。如果出於業務目的需要存取任何這些網站，請將其新增到 SSL 解密排除項清單，以將其排除在解密之外。SSL 解密排除項清單僅適用於技術上中斷解密的網站。

©2024 Palo Alto Networks, Inc.

識別敏感流量，出於法律、法規、個人或其他原因（例如財務、健康或政府流量或某些高階主管流量），選擇不解密這些流量。這並不是技術上中斷解密的流量，因此請勿使用 SSL 解密排除項清單以將此流量排除在解密之外。而是建立基於原則的解密排除項，識別並控制選擇不解密的流量，並將「無解密」解密設定檔套用於該原則，以防具有憑證問題的伺服器存取網路。基於原則的解密排除項僅用於您選擇不解密的流量。

當您規劃解密原則時，請考慮貴公司的安全性符合性規則、電腦使用原則以及業務目標。透過防止使用者存取過去存取的非業務網站，極為嚴格的控制可能會影響使用者體驗，但政府或金融機構可能需要這些控制。在可用性、管理負荷以及安全性之間一律存在權衡。解密原則越嚴格，網站無法存取的可能性就越大，可能會導致使用者投訴並可能修改規則庫。

儘管嚴格的解密原則最初可能會引起一些使用者投訴，但這些投訴可能會讓您注意到那些非認可或不適當的網站，這些網站因使用弱演算法或存在憑證問題而被封鎖。將投訴用作一種工具，可以更好地瞭解網路上的流量。

不同群組的使用者以及甚至個別使用者可能需要不同的解密原則，或者您可能想要對所有使用者套用相同的解密原則。例如，高階主管可能會排除在適用於其他員工的解密原則之外。您可能想要對員工群組、承包商、合作夥伴以及來賓套用不同的解密原則。備妥更新的法律和人力資源電腦使用原則，散佈給所有員工、承包商、合作夥伴、來賓和任何其他網路使用者，以便在部署解密時，使用者便已瞭解可以對其資料進行解密並掃描以發現威脅。

如何處理來賓使用者具體取決於其所需的存取權限。透過將來賓置於單獨的 *VLAN* 以及單獨的 *SSID* 上進行無線存取，將這些來賓與其餘網路隔離。若來賓不需要存取貴公司的網路，請勿讓其存取，也沒有必要解密其流量。若來賓需要存取貴公司的網路，請對其流量進行解密：

- 企業不會控制來賓的裝置。解密來賓流量並使其符合來賓安全性原則，以便防火牆可以檢查流量並防止威脅。為此，請透過驗證入口網站重新導向來賓使用者，指導他們如何下載和安裝 *CA* 憑證，並明確通知來賓將會對其流量進行解密。包含您公司隱私和電腦使用原則的流程。
- 建立單獨的解密原則規則和安全性原則規則，嚴格地控制來賓存取權限，使其只能存取他們需要存取的網路區域。

與不同的使用者群組類似，確定要解密的裝置和要解密的應用程式。如今的網路不僅支援企業裝置，還支援 BYOD、行動裝置、遠端使用者裝置和其他裝置，包括承包商、合作夥伴和來賓裝置。如今的使用者嘗試存取許多認可和未認可的網站，您應該決定要解密的流量。

企業不會控制 *BYOD* 裝置。若您允許網路上的 *BYOD* 裝置，請解密其流量並使其符合套用於其他網路流量的相同安全性原則，以便防火牆可以檢查流量並防止威脅。為此，請透過驗證入口網站重新導向 *BYOD* 使用者，指導他們如何下載和安裝 *CA* 憑證，並明確通知使用者將會對其流量進行解密。向 *BYOD* 使用者提供有關此過程的訓練，並將其納入貴公司的隱私權和電腦使用原則中。

確定要記錄的流量並調查可以記錄的流量。對於可以記錄和儲存的資料類型以及資料的記錄和儲存位置，敬請留意當地相關法律。例如，當地法律可能阻止記錄和儲存健康與財務資料等個人資訊。

©2024 Palo Alto Networks, Inc.

確定如何處理錯誤憑證。例如，將要封鎖或允許其憑證狀態為未知的工作階段嗎？瞭解想要如何處理錯誤憑證可確定如何設定附加到解密原則的解密設定檔，從而根據伺服器憑證驗證狀態控制允許的工作階段。

制定 PKI 部署計劃

規劃如何部署公開金鑰基礎結構 (PKI)。網路裝置在受信任網站上需要 SSL 轉送信任 CA 憑證，在不受信任網站上則需要 SSL 轉送不可信 CA 憑證。產生單獨的轉送信任和轉送不可信憑證（不要用企業根 CA 簽署轉送不可信憑證，因為想要用不可信憑證來警告使用者他們試圖存取可能不安全的網站）。Palo Alto Networks 新世代防火牆為 SSL 解密產生 CA 憑證的方法有兩種：

- 從企業根 **CA** 產生作為次級憑證的 **SSL CA** 憑證—若您有現有企業 PKI，這便為最佳做法。由於網路裝置已信任企業根 CA，從企業根 CA 產生次級憑證可使部署更容易更順暢，進而在開始部署階段時便可避免所有的憑證問題。若您沒有 Enterprise Root CA，請考慮取得一個。
- 在防火牆上產生自簽根 **CA** 憑證，並在該防火牆上建立次級 **CA** 憑證—若沒有企業根 CA，則可使用此方法獲取自簽根 CA 憑證以及次級轉送信任和不可信 CA 憑證。藉助此方法，您必須在所有網路裝置上安裝自簽憑證，以便這些裝置識別防火牆的自簽憑證。由於憑證必須部署到所有裝置，相較於大型部署，小型部署和概念驗證 (POC) 試驗更適合使用此方法。

請勿將轉送不可信憑證匯出到網路裝置上的憑證信任清單#這一點至關重要，因為安裝信任清單中的不可信憑證會導致裝置信任防火牆不可信的網站。此外，使用者不會看到不可信網站的憑證警告，因此他們不會知道這些網站不受信任，甚至可能會存取這些網站，進而使網路面臨威脅。

無論是從企業根 *CA* 產生轉送信任憑證，還是使用在防火牆上產生的自簽憑證，均會為每個防火牆產生獨立的次級轉送信任 *CA* 憑證。靈活使用單獨的次級 *CA* 可讓您在解除裝置（或裝置組）時撤銷一個憑證，而不影響部署的其餘部分，並降低了在需要撤銷憑證之任何情況下的影響。每個防火牆上的單獨轉送信任 *CA* 也有助於排解問題，因為使用者看到的 *CA* 錯誤訊息包含流量正在遍訪之防火牆的相關資訊。如果在每個防火牆上使用相同的轉送信任 *CA*，則會丟失該資訊的精度。

在不同防火牆上使用不同的轉送不可信憑證毫無益處，因此您可以在所有防火牆上使用相同的轉送不可信憑證。若您的私密金鑰需要額外的安全性，請考慮將它們儲存於 HSM 上。

您可能需要為來賓使用者進行特殊的調節。若來賓使用者不需要存取貴公司網路，則不允許其存取，然後也不必解密其流量或建立基礎結構來支援來賓存取。若您需要支援來賓使用者，請與法務部門討論是否可以解密來賓流量。

若您可以解密來賓流量，則將來賓作為 BYOD 裝置進行處理。解密來賓流量，並使其遵守您應用在其他網路流量上相同的安全性原則。為此，請透過驗證入口網站重新導向訪客使用者，指示他們如何下載和安裝 CA 證書，並明確通知使用者該流量將被解密。包含您公司隱私和電腦使用原則的流程。此外，將來賓流量限制到來賓需要存取的區域。

如果您因法務原因而無法解密來賓流量，則須隔離來賓流量，以防止其在網路內橫向移動：

- 為來賓建立單獨的區域，並限制賓客對該區域的存取。若要防止橫向移動，請勿允許賓客存取其他區域。

©2024 Palo Alto Networks, Inc.

- 僅允許認可的應用程式，使用 URL 篩選防止存取存在風險的 URL 類別，並套用最佳做法安全性設定檔。
- 套用不解密解密原則與設定檔，以防止賓客存取使用未知或過期 CA 的網站。

所有員工、契約商、合作夥伴及其他使用者都應使用您的常規公司基礎設施，且您應解密和檢查其流量。

調整解密防火牆部署的大小

解密加密流量會耗用防火牆 CPU 資源，並可能影響傳輸量。一般而言，安全性越嚴格（解密的 SSL 流量越多，通訊協定設定就越嚴格），解密所耗用的防火牆資源就越多。與您的 Palo Alto Networks SE/CE 合作，調整防火牆部署大小，避免大小錯誤。影響解密資源耗用情況的因素，以及防火牆可以解密的流量包括：

- 要解密的 SSL 流量。這因網路而異。例如，某些應用程式必須進行解密才能防止惡意軟體或漏洞攻擊滲入網路或未經授權的資料傳輸，而某些應用程式因當地法律與法規或業務原因無法進行解密，其他應用程式則是純文字（未加密），不需要進行解密。要解密的流量越多，所需資源就越多。
- TLS 通訊協定版本。版本更高會更安全，但亦會耗用更多資源。使用最高的 TLS 通訊協定版本可以最大限度地提高安全性。
- 金鑰大小。金鑰大小越大，安全性越好，但金鑰處理所耗用的資源也就越多。
- 金鑰交換演算法。完美轉送密碼 (PFS) 暫時金鑰交換演算法（例如 Diffie-Hellman 暫時 (DHE)、橢圓曲線 Diffie-Hellman 交換 (ECDHE)）耗用的處理資源比 Rivest-Shamir-Adleman (RSA) 演算法要多。PFS 金鑰交換演算法提供比 RSA 金鑰交換演算法更高的安全性，因為防火牆必須為每個工作階段產生新的金鑰（但這會耗用更多的防火牆資源）。然而，如果攻擊者破壞了工作階段金鑰，PFS 會阻止攻擊者使用該金鑰對同一用戶端和伺服器之間的任何其他工作階段進行解密，而 RSA 則不會。
- 加密演算法。金鑰交換演算法確定加密演算法是 PFS 還是 RSA。
- 憑證驗證方法。RSA（不是 RSA 金鑰交換演算法）耗用的資源比橢圓曲線數位特徵碼演算法 (ECDSA) 要少，但 ECDSA 更安全。

  結合使用金鑰交換演算法和憑證驗證方法會影響輸送量效能，如 *RSA* 和 *ECDSA* 基準測試中所示。*PFS* 的效能成本與其實現的更高安全性進行了權衡，但所有類型的流量可能不需要 *PFS*。透過將 *RSA* 用於要解密及檢查威脅的不敏感流量，可以節省防火牆 *CPU* 週期。
- 平均交易大小。例如，平均交易大小較小會耗用更多的處理能力來解密。測量所有流量的平均交易大小，然後測量連接埠 443（HTTPS 加密流量的預設連接埠）上流量的平均交易大小，以瞭解進入防火牆的加密流量與總流量和平均交易大小的比例。消除異常大的交易等異常值，以更真實地測量平均交易大小。
- 防火牆型號和資源。較新的防火牆型號比舊型號具有更強的處理能力。

綜合這些因素可確定解密如何耗用防火牆處理資源。若要最佳利用防火牆的資源，請瞭解您要保護之資料的風險。如果防火牆資源存在問題，請對較高優先順序的流量使用較強解密，並使用需要較

 ©2024 Palo Alto Networks, Inc.

少處理器的解密來解密和檢查較低優先順序的流量，直到您可以增加可用資源為止。例如，您可以將 RSA 而不是 ECDHE 和 ECDSA 用於不敏感或高優先順序的流量，以保護防火牆資源，從而對較高優先順序的敏感流量使用基於 PFS 的解密。（您仍然在解密和檢查較低優先順序的流量，但使用不如 PFS 安全的演算法可耗用更少的計算資源。） 關鍵是要瞭解不同流量類型的風險並相應地對其進行處理。

測量防火牆效能，以便瞭解目前可用的資源，有助於您瞭解是否需要更多防火牆資源來解密要解密的流量。測量防火牆效能還為部署解密後的效能比較設定了基準線。

在調整防火牆部署大小時，不僅要根據現行需求，還要根據未來需求進行操作。Gartner 預測，到 2019 年，超過 80# 的企業網路流量將被加密，超過 50# 的新惡意軟體活動將使用各種形式的加密，因此為解密流量增長提供了頂部空間。與您的 Palo Alto Networks 代表合作，充分利用他們在調整防火牆大小方面的經驗，協助您調整防火牆解密部署的大小。

規劃設定有優先順序的分階段部署

計劃以受控方式逐個推出解密。請勿一次推出整個解密部署。測試並確保解密按計劃進行，並讓使用者瞭解您所執行的工作以及理由。若工作無法按預期進行，以這種方式推出解密可更容易地進行疑難排解，並幫助使用者適應變化。

為利益關係人、員工以及承包商和合作夥伴等其他使用者提供相關訓練至關重要，因為解密設定可能會變更他們存取某些網站的權限。使用者應該瞭解如何應對之前可存取的網站變得無法存取的情況，以及哪些資訊可提供技術支援。支援人員應瞭解將要推出哪些內容、推出時間以及如何為遇到問題的使用者提供協助。在向一般群體推出解密之前：

- 確定可幫助支援解密的早期採用者，他們將能夠幫助在全面部署期間有疑問的其他員工。向部門經理尋求幫助，協助他們瞭解解密流量的益處。
- 在早期採用者和其他瞭解解密流量重要性的員工所在的每個部門中，設定概念驗證 (POC) 試驗。向 POC 參與者提供相關訓練，讓其瞭解這些變更以及在遇到問題時如何聯絡技術支援人員。透過這種方式，解密 POC 讓您有機會與技術支援人員合作，對如何支援解密進行 POC，並共同開發為一般部署提供支援的最為輕鬆的方法。POC 使用者和技術支援人員之間的交互還允許您細部調整原則以及與使用者的通訊方式。

  透過 POC，您可以搶先體驗設定解密內容的優先順序，這樣當您在一般群體中分階段解密時，您的 POC 體驗可幫助您瞭解如何分階段解密不同的 URL 類別。測量解密影響防火牆 CPU 和記憶體利用率的方式，以幫助瞭解防火牆大小是否適當或是否需要升級。POC 還可以顯示技術上中斷解密（解密會封鎖其流量）且需要新增至 Decryption Exclusion（解密排除項）清單的應用程式。

  設定 POC 後，還要設定一個使用者群組，可在一般部署之前驗證操作備妥情況和程序。
- 在一般部署之前為使用者群體提供相關訓練，並計劃在新使用者加入公司時對其進行訓練。這是部署解密的關鍵階段，由於部署可能會影響使用者之前造訪過但不安全的網站，因此這些網站不再可存取。POC 體驗有助於確定通訊要點。
- 解密階段。您可以透過幾種方式完成此作業。您可以先解密最高優先順序的流量（例如，最有可能包含惡意流量的 URL 類別，比如賭博），然後隨著經驗積累解密更多流量。或者，您還可以採取更保守的方法，先解密不會影響業務的 URL 類別（因此，出現問題時，也不會發生影響

 ©2024 Palo Alto Networks, Inc.

業務的問題），例如新聞資訊來源。在所有情況下，分階段解密的最佳方法是，解密一些 URL 類別，考慮使用者回饋，執行報告以確保解密按預期進行，然後逐步解密更多 URL 類別並進行驗證等等。若因技術原因而無法解密網站，或者您選擇不對其進行解密，請根據解密排除項將這些網站排除在解密之外。

若您允許使用者選擇退出 SSL 解密（使用者會看到一個回應頁面，允許他們選擇退出解密並結束該工作階段而無需造訪該網站，或繼續造訪該網站並同意將流量解密），請向其說明相關內容、他們看到該內容的原因，以及他們的選擇有哪些。

- 建立實際部署排程，以便有時間評估部署的每個階段。

將防火牆放置在其可以看到所有網路流量的位置，以防沒有加密的流量繞過防火牆意外地存取網路。

©2024 Palo Alto Networks, Inc.

定義解密流量

解密原則規則可讓您定義想要防火牆解密的流量，以及因個人流量或當地法規而選擇免於解密的流量。

將解密設定檔附加到每個解密原則規則，可啟用憑證檢查、工作階段模式檢查、失敗檢查以及通訊協定與演算法檢查，具體視設定檔而定。執行以上檢查可防止有風險的連線，比如具有不受信任之憑證簽發者的工作階段、使用弱通訊協定、密碼以及演算法的工作階段以及存在憑證問題的伺服器。

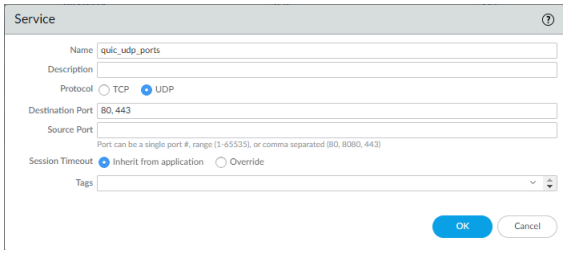
檢閱解密部署最佳做法檢查清單，以確保您瞭解建議的最佳做法。

封鎖已知危險的 URL 篩選類別，比如惡意軟體、網路釣魚、動態 DNS、未知、命令和控制、Proxy 規避與匿名者網站、侵犯著作權、 極端主義、新註冊網域、灰色軟體和寄放。如果出於業務原因必須允許任何這些類別，則對其進行解密並對流量套用嚴格的安全性設定檔。

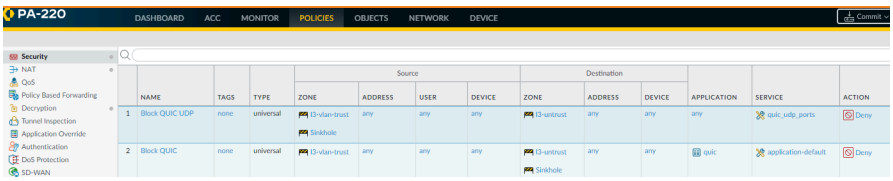
若允許，則應一律解密 URL 類別，其中包含：線上儲存與備份、基於 Web 的電子郵件、Web 裝載、個人網站與部落格以及內容傳送網路。

在安全性原則中，除非出於業務原因，您希望允許加密的瀏覽器流量，否則封鎖快速 *UDP* 網際網路連線 *(QUIC)* 通訊協定。*Chrome* 以及其他一些瀏覽器會使用 *QUIC* 而非 *TLS* 建立工作階段，但 *QUIC* 使用防火牆無法解密的專用加密手法，因此潛在危險的流量可能會如加密流量般進入網路。封鎖 *QUIC* 會強制瀏覽器回退到 *TLS*，並讓防火牆可以解密流量。

建立建立安全性原則規則以在其 *UDP* 服務連接埠（*80* 和 *443*）封鎖 *QUIC*，並建立單獨的規則以封鎖 *QUIC* 應用程式。對於封鎖 *UDP* 連接埠 *80* 和 *443* 的規則，建立一個包括 *UDP* 連接埠 *80* 和 *443* 的服務（***Objects***（物件） > ***Services***（服務））：



使用該服務指定 *UDP* 連接埠以封鎖 *QUIC*。在第二條規則中，封鎖 *QUIC* 應用程式：



 ©2024 Palo Alto Networks, Inc.

- 建立解密設定檔
- 建立解密原則規則

建立解密設定檔

解密設定檔可讓您對解密流量及您選擇要排除在解密之外的 SSL 流量執行檢查。（如果伺服器因憑證釘選或其他原因而在技術上中斷了 SSL 解密，則將該伺服器新增至解密排除項清單。） 根據需要，建立解密設定檔以執行以下動作：

- 根據憑證狀態封鎖工作階段，包括封鎖具有以下內容的工作階段：過期憑證、不受信任的簽發者、未知憑證狀態、憑證狀態檢查逾時和憑證延伸。
- 若工作階段具有不受支援的版本和密碼套件且需要使用用戶端驗證，則將其封鎖。
- 執行解密的資源不可用，或者硬體安全性模組無法用於簽署憑證時封鎖工作階段。
- 在 SSL 通訊協定設定中，定義 SSL 正向 Proxy 和 SSL 輸入檢查流量容許的通訊協定版本和金鑰交換、加密和驗證演算法。

為了容納防禦性較弱的網站，請勿弱化大多數網站使用的主要解密設定檔作用。而是為需要支援但其不支援強密碼和演算法的網站建立一個或多個單獨的解密設定檔。您還可以為不同的 URL 類別建立不同的解密設定檔，以細微調整不包含敏感材料之流量的安全性與效能；然而，您應一律解密並檢查所有流量。

建立解密設定檔後，可以將其附加於解密原則規則；防火牆隨後對符合解密原則規則的流量強制執行解密設定檔組態。

Palo Alto Networks 防火牆包含您可用於強制執行建議的基本通訊協定版本的預設解密設定檔，以及用於解密流量的加密套件。但是，最佳做法是啟用更嚴格的解密控制，如SSL 正向 Proxy 解密設定檔、SSL 輸入檢查解密設定檔和 SSL 通訊協定設定解密設定檔中所描述。

避免使用弱通訊協定或演算法，因為它們包含攻擊者可利用的已知漏洞。如果您必須使用加密強度較弱的通訊協定或演算法，為使用弱通訊協定的舊式系統使用者（重要合作夥伴或承包商）提供支援，請為該例外建立單獨的解密設定檔，並將其附加到僅將該設定檔套用於相關流量（例如，合作夥伴的來源 *IP* 位址）的解密原則規則。請勿對所有流量使用弱通訊協定。

STEP 1 | 建立新的解密設定檔。

選取 **Objects**（物件） > **Decryption Profile**（解密設定檔）, **Add**（新增）或修改解密設定檔規則，然後為規則輸入描述性 **Name**（名稱）。

STEP 2 | （選用）允許設定檔規則在防火牆或每一個 Panorama 裝置群組的每一個虛擬系統上 **Shared**（共用）。

STEP 3 | （僅限解密鏡像）啟用防火牆用於複製及轉送解密流量的乙太網路介面。

對於此工作，請按照設定解密連接埠鏡像的步驟操作。由於當地隱私權法規可能會禁止鏡像或控制您可以鏡像的流量類型，敬請留意這些法規。解密連接埠鏡像需要解密連接埠鏡像授權。

©2024 Palo Alto Networks, Inc.

STEP 4 | （選用）封鎖並控制 SSL 通道及/或輸入流量：

儘管將解密設定檔套用於解密流量是選用作業，但最佳做法是一律將解密設定檔套用於原則規則，保護網路免受加密威脅。無法保護自己免受看不見的威脅。

選取 **SSL Decryption**（SSL 解密）：

- 選取 **SSL Forward Proxy**（**SSL** 正向 **Proxy**），以設定驗證憑證，強制執行通訊協定版本及密碼套件，以及對 SSL 解密流量執行失敗檢查。這些設定僅當此設定檔附加至解密原則規則（設定用於執行 SSL 正向 Proxy 解密）時才有效。
- 選取 **SSL Inbound Inspection**（**SSL** 輸入檢查），以設定強制執行通訊協定版本及密碼套件，以及對輸入 SSL 流量執行失敗檢查。這些設定僅當此設定檔附加至用於執行 SSL 輸入檢查的解密原則規則時才有效。
- 選取 **SSL Protocol Settings**（**SSL** 通訊協定設定）以設定用於控制對解密 SSL 流量強制執行的最低及最高通訊協定版本以及金鑰交換、加密及驗證演算法。這些設定在設定檔附加至解密原則規則（設定用於執行 SSL 轉送代理程式解密或 SSL 輸入檢查）時才有效。

如果防火牆處於 *FIPS-CC* 模式，且由標準模式的 *Panorama*™ 管理伺服器進行管理，則必須在防火牆本機上建立解密設定檔。在標準模式的 *Panorama* 上建立的解密設定檔包含對 ***3DES*** 和 ***RC4*** 加密演算法和 ***MD5*** 驗證演算法的引用，這些演算法並不受支援，且會導致無法推送至受管理防火牆。

STEP 5 | （選用）封鎖並控制您已選擇用來建立基於原則的解密排除項的流量（例如，URL 類別）。

儘管將解密設定檔套用於選擇不解密的流量是選用作業，但最佳做法是一律將解密設定檔套用於原則規則，保護網路免受具有過期憑證或不受信任之簽發者的工作階段影響。

選取 **No Decryption**（無解密）以設定「不解密」的設定檔，並核取 **Block sessions with expired certificates**（封鎖具有過期憑證的工作階段）以及 **Block sessions with untrusted issuers**（封鎖具有不受信任之簽發者的工作階段）方塊，以驗證從解密中排除之流量的憑證。僅為您選擇不解密的流量建立基於原則的排除項。若伺服器因技術原因而中斷解密，請勿建立基於原則的排除項，而是將伺服器新增至 SSL 解密排除項清單（**Device**（裝置） > **Certificate Management**（憑證管理） > **SSL Decryption Exclusion**（**SSL** 解密排除項））。

這些設定僅當解密設定檔附加至解密原則規則（對某些流量停用解密）時才有效。

STEP 6 | （選用）封鎖並控制已解密的 SSH 流量。

選取 **SSH Proxy** 設定 SSH Proxy 解密設定檔，然後進行設定，以強制執行受支援的通訊協定版本，並在沒有可用系統資源執行解密時封鎖工作階段。

這些設定僅當解密設定檔附加至解密原則規則（解密 SSH 流量）時才有效。

STEP 7 | 建立解密原則規則時新增解密設定檔。

防火牆套用解密設定檔並對符合解密原則規則的流量強制執行設定檔的設定。

©2024 Palo Alto Networks, Inc.

STEP 8 | **Commit**（提交）組態。

建立解密原則規則

建立解密政策規則來定義防火牆要解密的流量，以及您希望防火牆執行解密的類型：Ssl 正向 Proxy、SSL 輸入檢查 或 SSH Proxy 解密。您還可以使用解密政策規則來定義解密鏡像。

在設定解密政策規則之前，確保您瞭解 IPv4 位址集會被視為 IPv6 位址集的子集，原則中對此進行了詳細說明。

STEP 1 | 新增解密政策規則。

選取 **Policies**（政策）> **Decryption**（解密），**Add**（新增）解密政策規則，然後為政策規則輸入描述性 **Name**（名稱）。

STEP 2 | 設定解密規則，根據網路及原則物件比對流量：

- 防火牆安全性區域 — 選取 **Source**（來源）及/或 **Destination**（目的地），然後根據 **Source Zone**（安全性區域）及/或 **Destination Zone**（目的地區域）比對流量。
- **IP** 位址、位址物件及/或位址群組 — 選取 **Source**（來源）及/或 **Destination**（目的地），根據 **Source Address**（來源位址）及/或 **Destination Address**（目的地）位址比對流量。或者，選取 **Negate**（否定），將來源位址清單排除在解密之外。
- 使用者 — 選取 **Source**（來源）並設定要對其解密流量的 **Source User**（來源使用者）。您可以解密特定使用者或群組流量，或解密特定類型的使用者流量，例如未知使用者或預登入的使用者（連線至 GlobalProtect 但尚未登入的使用者）。
- 連接埠和通訊協定 — 選取 **Service/URL Category**（服務/**URL** 類別）可設定規則，以根據服務比對流量。依預設，原則規則設定為解密 **Any**（任何）TCP 及 UDP 連接埠上的流量。您可以 **Add**（新增）服務或服務群組，然後選擇性地設定 **application-default**（應用程式預設）的規則，只比對應用程式預設連接埠上的應用程式。

  在您建立基於政策的解密排除項時，應用程式預設設定可能會非常有用。您可以將在其預設連接埠上執行的應用程式排除在解密之外，同時在非標準連接埠上偵測到相同應用程式時，繼續對其解密。

- **URL** 及 **URL** 類別 — 選取服務/URL 類別並根據下列各項解密流量：
  - 防火牆為強制執行原則所擷取的 URL 外部托管清單（請參閱 **Objects**（物件）> **External Dynamic Lists**（外部動態清單））。
  - Palo Alto Networks 預先定義了 URL 類別，讓您能輕鬆解密整個允許流量的類別。建立基於原則的解密排除項時，此選項也很有用，因為您可以按類別而非單個地排除敏感網站。例如，雖然您可以建立自訂 URL 類別，對您不希望解密的網站分組，但您還可以根據預先定義的 Palo Alto Networks URL 類別將金融或健康照護相關的網站排除在解密之外。此

 ©2024 Palo Alto Networks, Inc.

外，您還可以封鎖有風險的 URL 類別並建立舒適頁面，以傳達網站被封鎖的原因或允許使用者選擇退出 SSL 解密。

您可以使用預先定義的高風險和中等風險 URL 類別建立解密原則規則，以解密所有高風險和中等風險 URL 流量。將規則置於規則庫底部（所有解密例外項必須位於此規則之上，確保您不會解密敏感資訊），作為安全網，以確保解密和檢查所有存在風險的流量。但是，如果您允許存取的高風險或中等風險網站包含個人身份資訊 (PII) 或您不想解密的其他敏感資訊，您可封鎖這些網站以避免允許加密的危險流量，或建立「不解密」規則以處理敏感流量。

- 自訂 URL 類別（請參閱 **Objects**（物件） > **Custom Objects**（自訂物件） > **URL Category**（**URL** 類別））。例如，您可以建立自訂 URL 類別以指定出於業務目的而需要存取的一組網站，但不支援最安全的通訊協定和演算法，然後套用自訂的解密設定檔以只對那些網站使用更寬鬆的通訊協定和演算法（因此，降級大部分網站使用的解密設定檔亦不會降低安全性）。

©2024 Palo Alto Networks, Inc.

STEP 3 | 設定規則，以解密相符流量或在解密操作中排除相符流量。

選取 **Options**（選項）並設定原則規則 **Action**（動作）：

若要解密相符流量：

1. 將 **Action**（動作）設定為 **Decrypt**（解密）。
2. 設定解密 **Type**（類型），以便防火牆對相符流量執行解密：
   - SSL 正向 Proxy。
   - SSL 輸入檢查。然後，為輸入 SSL 流量的目的地內部伺服器 **Add**（新增）一或多個 **Certificates**（憑證）。SSL 輸入檢查政策規則最多支援 12 個憑證。

     您可以設定解密政策規則，以解密管理多個網域（每個網域都有自己的憑證）的內部伺服器的 *SSL/TLS* 流量繫結。防火牆使用政策規則中的憑證（符合伺服器針對要求之 *URL* 提供的憑證）來交涉 *SSL/TLS* 連線。

     若要更新受保護內部伺服器的憑證而不會造成停機，請在新的伺服器憑證到期之前更新或取得該伺服器憑證，否則憑證將會無效。然後，將憑證和私密金鑰匯入防火牆，並將其新增至 *SSL* 輸入檢查政策規則，然後再將相同的憑證安裝到 *Web* 伺服器上。使用新憑證更新您的政策規則，而其他憑證在 *Web* 伺服器上處於作用中狀態時，會準備防火牆以解密流向伺服器的流量，而不論使用中的憑證為何。設定 SSL 輸入檢查進一步介紹了此程序。

     (Panorama™) 在 *PAN-OS 10.2* 之前的 *PAN-OS®* 版本中，不支援 *SSL* 輸入檢查政策規則中具有多個憑證。如果您將具有多個憑證的 *SSL* 輸入檢查政策規則從執行 *PAN-OS 10.2* 的 *Panorama* 管理伺服器推送到執行較早版本的防火牆，則受管理防火牆上的政策規則只會繼承依照字母順序排序的憑證清單中的第一個憑證。

     在從 *Panorama* 推送解密政策規則之前，建議您為執行 *PAN-OS 10.1* 及較早版本的防火牆設定不同的範本或裝置群組，以確保推送正確的政策規則和憑證到適當的防火牆。
   - SSH Proxy。

若要將相符流量排除在解密之外：

將 **Action**（動作）設定為 **No Decrypt**（不解密）。

©2024 Palo Alto Networks, Inc.

STEP 4 | （選用）選取 **Decryption Profile**（解密設定檔），以對符合原則規則的流量執行額外的檢查。

儘管將解密設定檔套用於解密流量是選用作業，但最佳做法是一律將解密設定檔套用於原則規則，保護網路免受加密威脅。無法保護自己免受看不見的威脅。

例如，將解密設定檔附加於政策規則，以確保伺服器憑證有效，並封鎖使用不受支援通訊協定或密碼的工作階段。若要建立解密設定檔，可選取 **Objects**（物件） > **Decryption Profile**（解密設定檔）。

1. 建立解密政策規則或開啟現有規則加以修改。
2. 選取 **Options**（選項），然後選取 **Decryption Profile**（解密設定檔），以封鎖並控制符合規則之流量的各個方面。

   防火牆套用於相符流量的設定檔規則設定視原則規則 **Action**（動作）（解密或不解密）及原則規則 **Type**（類型）（SSL 正向 Proxy、SSL 輸入檢查或 SSH Proxy）而定。這允許您搭配使用不同解密設定檔與套用於不同類型流量和使用者的不同類型解密政策規則。
3. 按一下 **OK**（確定）。

STEP 5 | 設定解密記錄（設定是否同時記錄成功和不成功的 TLS 交握，並設定解密日誌轉送）。

STEP 6 | 按一下 **OK**（確定）儲存原則。

STEP 7 | 選擇接下來的步驟，使防火牆解密流量……

- 設定 SSL 正向 Proxy。
- 設定 SSL 輸入檢查。
- 設定 SSH Proxy。
- 為您選擇不解密的流量建立基於政策的解密排除項，並將因技術原因（例如釘選憑證或相互驗證）而中斷解密的網站新增到 SSL 解密排除項清單中。

©2024 Palo Alto Networks, Inc.

設定 SSL 轉送代理程式

若要啟用防火牆執行 SSL 正向 Proxy 解密，您必須設定所需憑證以作為受信任的協力廠商 (proxy) 對用戶端與伺服器之間的工作階段建立防火牆。防火牆可以將企業憑證授權單位 (CA) 簽署的憑證或防火牆上產生的自簽憑證用作轉送信任憑證 (Forward Trust certificates) 來驗證與用戶端的 SSL 工作階段。

- （最佳做法）企業 **CA** 簽署憑證—企業 CA 會簽發簽署憑證，防火牆之後會使用此憑證為需要 SSL 解密的網站簽署憑證。防火牆在信任簽署目的地伺服器憑證的 CA 後，會傳送目的地伺服器憑證副本至企業 CA 簽署的用戶端。此為最佳做法。通常所有網路裝置均已信任企業 CA（其通常已安裝在裝置的 CA 信任儲存體中），因此您無需在端點上部署憑證，部署過程也就更順暢。
- 自簽憑證—防火牆可以充當 CA 並產生自簽憑證，防火牆之後可以使用該憑證為需要 SSL 解密的網站簽署憑證。防火牆可以簽署要對用戶端顯示的伺服器憑證副本並建立 SSL 工作階段。此方法要求您必須在所有網路裝置上安裝自簽憑證，以便這些裝置識別防火牆的自簽憑證。由於憑證必須部署到所有裝置，相較於大型部署，小型部署和概念驗證 (POC) 試驗更適合使用此方法。

此外，當伺服器憑證由防火牆不可信的 CA 簽署時，為防火牆設定轉送不可信憑證 (forward untrust certificate) 以對用戶端顯示。這可確認當用戶端嘗試使用不信任的憑證存取站台時，系統會以憑證警告提示用戶端。

無論是從企業根 *CA* 產生轉送信任憑證，還是使用在防火牆上產生的自簽憑證，均會為每個防火牆產生獨立的次級轉送信任 *CA* 憑證。靈活使用單獨的次級 *CA* 可讓您在解除裝置（或裝置組）時撤銷一個憑證，而不影響部署的其餘部分，並降低了在需要撤銷憑證之任何情況下的影響。每個防火牆上的單獨轉送信任 *CA* 也有助於排解問題，因為使用者看到的 *CA* 錯誤訊息包含流量正在遍訪之防火牆的相關資訊。如果在每個防火牆上使用相同的轉送信任 *CA*，則會丟失該資訊的精度。

設定 SSL 正向 Proxy 解密所需的轉送信任及轉送不可信憑證之後，建立一個解密原則規則以定義您想要防火牆解密的流量，以及建立一個解密設定檔以將 SSL 控制和檢查套用至流量。解密原則會將符合規則的 SSL 通道式流量解密為純文字流量。防火牆會根據附加到解密原則的解密設定檔和防火牆安全性原則封鎖和限制流量。防火牆會在流量離開時重新對其加密。

當您設定 *SSL* 正向 *Proxy* 時，通過 *Proxy* 的流量不支援 *DSCP* 代碼點或 *QoS*。

STEP 1 | 確定將適當的介面設定為虛擬介接、Layer 2 或 Layer 3 介面。

在 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路）頁籤上檢視已設定的介面。如果介面設定為 **Virtual Wire** 或是 **Layer 2** 或 **Layer 3** 介面，則會顯示 **Interface Type**（介面類型）。您可以選取某個介面來修改其設定，包括為何種介面類型。

©2024 Palo Alto Networks, Inc.

STEP 2 | 若受信任的 CA 簽署了伺服器憑證，則設定防火牆轉送信任憑證以對用戶端顯示。您可以使用企業 CA 簽署的憑證或自我簽署的憑證作為轉送信任憑證。

（建議的最佳做法）使用企業 CA 簽署的憑證作為轉送信任憑證。在每個防火牆上建立名稱唯一的轉送信任憑證：

1. 產生憑證簽署要求 (CSR)，供企業 CA 進行簽署與驗證：
   1. 選取 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證）並按一下 **Generate**（產生）。
   2. 輸入 **Certificate Name**（憑證名稱）。為每個防火牆使用唯一的名稱。
   3. 在 **Signed By**（簽署者）下拉式清單中，選取 **External Authority (CSR)**（外部授權單位 **(CSR)**）。
   4. （選用）如果您的企業 CA 要求憑證，請新增 **Certificate Attributes**（憑證屬性）來進一步識別防火牆詳細資訊，如國家/地區或部門。
   5. 按一下 **Generate**（產生）以儲存 CSR。擱置中憑證現在會顯示在 **Device Certificates**（裝置憑證）頁籤中。
2. 匯出 CSR：
   1. 選取 **Device Certificates**（裝置憑證）頁籤上顯示的擱置中憑證。
   2. 按一下 **Export**（匯出）以下載並儲存憑證檔案。

      讓 ***Export private key***（匯出私密金鑰）保持不選取，以確保私密金鑰安全地保留在防火牆上。
   3. 按一下 **OK**（確定）。
3. 將憑證檔案提供給您的企業 CA。若您從企業 CA 接收企業 CA 簽署憑證，請儲存企業 CA 簽署憑證以匯入到防火牆上。
4. 將企業 CA 簽署憑證匯入到防火牆上：
   1. 選取 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證），再按一下 **Import**（匯入）。
   2. 準確地輸入擱置中的 **Certificate Name**（憑證名稱）。您輸入的 **Certificate Name**（憑證名稱）必須與擱置中的憑證名稱完全相同，才能驗證擱置中的憑證。
   3. 選取您要從企業 CA　收到的已簽署憑證檔案。
   4. 按一下 **OK**（確定）。憑證會顯示為有效，(金鑰) 與 (CA) 核取方塊皆已勾選。
5. 選取已驗證的憑證，讓此憑證成為用於 SSL 正向 Proxy 解密的 **Forward Trust Certificate**（轉送信任憑證）。
6. 按一下 **OK**（確定），儲存企業 CA 簽署轉送信任憑證。

使用自簽憑證作為轉送信任憑證：

1. 建立自我簽署根 CA 憑證。

©2024 Palo Alto Networks, Inc.

2. 按一下自簽根 CA 憑證（**Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證） > **Device Certificates**（裝置憑證））即可開啟 **Certificate information**（憑證資訊），然後按一下 **Trusted Root CA**（受信任的根 **CA**） 核取方塊。
3. 按一下 **OK**（確定）。
4. 為每個防火牆產生新的次級 CA 憑證：
   1. 選取 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證）。
   2. 按一下視窗下方的產生。
   3. 輸入 **Certificate Name**（憑證名稱）。
   4. 輸入通用名稱，如 192.168.2.1。這應該是出現在憑證中的 IP 或 FQDN。在此情況下，我們會使用信任介面的 IP。避免在此欄位中使用空格。
   5. 在 **Signed By**（簽署者）欄位中，選取已建立的自簽根 CA 憑證。
   6. 按一下憑證授權單位核取方塊，以確保防火牆會簽發憑證。選取此核取方塊後，即可在防火牆上建立憑證授權單位 (CA)，然後匯入用戶端瀏覽器，讓用戶端可如同信任 CA 般地信任防火牆。
   7. 產生憑證。
5. 按一下新的憑證加以修改，然後按一下 **Forward Trust Certificate**（轉送信任憑證）核取方塊以將該憑證設定為轉送信任憑證。
6. 按一下 **OK**（確定），儲存自我簽署的轉送信任憑證。
7. 若要在每個防火牆上產生唯一的次級 CA 憑證，請重複此過程。

©2024 Palo Alto Networks, Inc.

STEP 3 | 將轉送信任憑證散佈給用戶端系統憑證存放區。

如果使用企業 CA 簽署憑證用作轉送信任憑證進行 SSL 正向 Proxy 解密，且用戶端系統已安裝本機信任根 CA 清單內的企業 CA，則可略過此步驟。（用戶端系統信任在防火牆上產生的次級 CA 憑證，因為企業信任根 CA 已簽署了這些憑證。）

如果用戶端系統上未安裝轉送信任憑證，使用者會看到每個其所造訪 *SSL* 網站的憑證警告。

防火牆設定為 GlobalProtect 入口網站：

Windows 及 *Mac* 用戶端作業系統版本均支援此選項，且需要在用戶端系統上安裝 *GlobalProtect* 代理程式 *3.0.0* 或更新版本。

1. 選取 **Network**（網路） > **GlobalProtect** > **Portals**（入口網站），然後選取現有的入口網站組態或 **Add**（新增） 新的入口網站。
2. 選取 **Agent**（代理程式），然後選取現有的代理程式組態或 **Add**（新增）新的代理程式組態。
3. **Add**（新增）自簽防火牆信任根 CA 憑證至信任根 CA 區段。在 GlobalProtect 將防火牆的信任根 CA 憑證散佈到用戶端系統後，用戶端系統會信任防火牆的次級 CA 憑證，因為用戶端信任防火牆的根 CA 憑證。
4. **Install in Local Root Certificate Store**（在本機根憑證存放區上安裝）以便 GlobalProtect 入口網站自動散佈憑證並將其安裝在 GlobalProtect 用戶端系統上的憑證存放區。
5. 按兩下 **OK**（確定）。

無 GlobalProtect：

匯出防火牆信任根 CA 憑證，以便可將其匯入用戶端系統。強調顯示該憑證，然後按一下視窗底部的 **Export**（匯出）。選擇 PEM 格式。

切勿選中 ***Export private key***（匯出私密金鑰）核取方塊！私密金鑰應保留在防火牆上，不應匯出到用戶端系統。

將防火牆的信任根 CA 憑證匯入到用戶端系統上瀏覽器的信任根 CA 清單中，用戶端才會信任該憑證。匯入至用戶端瀏覽器時，請確保您將憑證新增至信任根憑證授權單位憑證存放區。在 Windows 系統上，預設的匯入位置是個人憑證存放區。您也可以使用集中部署選項，如 Active Directory 群組原則物件 (GPO) 來簡化此程序。

©2024 Palo Alto Networks, Inc.

STEP 4 | 設定轉送不可信憑證（對所有防火牆使用相同的轉送不可信憑證）。

1. 按一下憑證頁面下方的產生。
2. 輸入 **Certificate Name**（憑證名稱），例如 my-ssl-fwd-untrust。
3. 設定 **Common Name**（通用名稱），例如 192.168.2.1。**Signed By**（簽署者）請保留空白。
4. 按一下憑證授權單位核取方塊，以確保防火牆會簽發憑證。
5. 按一下產生，產生憑證。
6. 按一下 **OK**（確定）儲存。
7. 按一下新的 my-ssl-fw-untrust 憑證加以修改，並啟用 **Forward Untrust Certificate**（轉送不可信憑證）選項。

   請勿將轉送不可信憑證匯出到網路裝置上的憑證信任清單#請勿在用戶端系統上安裝轉送不可信憑證。這一點至關重要，因為安裝信任清單中的不可信憑證會導致裝置信任防火牆不可信的網站。此外，使用者不會看到不可信網站的憑證警告，因此他們不會知道這些網站不受信任，甚至可能會存取這些網站，進而使網路面臨威脅。
8. 按一下 **OK**（確定）儲存。

STEP 5 | （選用）設定 Ssl 正向 Proxy 伺服器憑證的金鑰大小，防火牆會向用戶端呈現這些憑證。依預設，防火牆會根據目的地伺服器的金鑰大小來決定使用的金鑰大小。

STEP 6 | 建立解密原則規則以定義防火牆要解密的流量，以及建立解密設定檔以將 SSL 控制套用至流量。

儘管解密設定檔為選用內容，但最佳做法是在每個解密原則規則中包含解密設定檔，以防加密強度不夠且存在漏洞的通訊協定和演算法允許網路中的可疑流量。

1. 選取 **Policies**（原則） > **Decryption**（解密），Add（新增）或修改現有的規則，然後定義要解密的流量。
2. 選取 **Options**（選項），然後：
   - 設定規則 **Action**（動作）以 **Decrypt**（解密）符合的流量。
   - 將規則 **Type**（類型）設定為 **SSL Forward Proxy**（**SSL** 轉送代理程式）。
   - （選用，但為最佳做法）設定或選取現有 **Decryption Profile**（解密設定檔）以封鎖及控制解密流量的各個方面（例如，建立解密設定檔來執行憑證檢查，並強制執行強密碼套件與通訊協定版本）。
3. 按一下 **OK**（確定）儲存。

STEP 7 | 啟用防火牆以轉送解密 SSL 流量進行 WildFire 分析。

此選項需要啟用 *WildFire* 授權，這是 WildFire 的最佳做法。

©2024 Palo Alto Networks, Inc.

STEP 8 | **Commit**（提交）組態。

STEP 9 | 選擇下一步：

- 允許使用者選擇退出 SSL 解密。
- 繼續設定解密排除項，以對特定類型的流量停用解密。

 ©2024 Palo Alto Networks, Inc.

設定 SSL 輸入檢查

使用 SSL 輸入檢查解密並檢查預定要送達網路伺服器之輸入 SSL 流量（如果將伺服器憑證載入至防火牆，您可以對任何伺服器執行 SSL 輸入檢查）。啟用 SSL 輸入檢查解密原則後，防火牆會將該原則識別的所有 SSL 流量解密為純文字流量並對其檢查。防火牆會根據附加到原則的解密設定檔和套用於流量的安全性原則（包括任何已設定的防毒、漏洞保護、反間諜軟體、URL 篩選和檔案封鎖設定檔）封鎖、限制或允許流量。最佳做法是，啟用防火牆來轉送解密 SSL 流量進行 WildFire 分析及產生特徵碼。

設定 SSL 輸入檢查包括：

- 在防火牆上安裝目標伺服器憑證。
- 建立 SSL 輸入檢查解密政策規則。
- 將解密設定檔套用至政策規則。

當您設定 *SSL* 輸入檢查時，通過 *Proxy* 的流量不支援 *DSCP* 代碼點或 *QoS*。

SSL 輸入檢查不支援驗證入口網站重新導向。要使用驗證入口網站重新導向和解密，您必須使用 SSL 正向 Proxy。

STEP 1 | 確保將適當的介面設定為 Virtual Wire（虛擬介接）、Layer 2（第二層）或 Layer 3（第三層）介面。

不能將旁接模式介面用於 *SSL* 輸入檢查。

在 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路） 頁籤上檢視已設定的介面。如果介面設定為 **Virtual Wire**（虛擬介接）、**Layer 2**（第二層）或 **Layer 3**（第三層）介面，則會顯示 **Interface Type**（介面類型）欄。您可以選取某個介面來修改其組態，包括介面類型。

©2024 Palo Alto Networks, Inc.

STEP 2 | 確定目標伺服器憑證已安裝在防火牆上。

在 Web 介面上，選擇 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證） > **Device Certificates**（裝置憑證），以檢視安裝在防火牆上的憑證。

Web 伺服器支援的 *TLS* 版本決定在防火牆上安裝伺服器憑證和金鑰的方式。

如果您的終端實體（分葉）憑證由一或多個中繼憑證簽署並且您的 *Web* 伺服器支援 *TLS 1.2* 和 *Rivest*、*Shamir*、*Adleman (RSA)* 或完整轉送密碼 *(*PFS*)* 金鑰交換演算法，我們建議上傳憑證鏈（單一檔案）到防火牆。上傳憑證鏈可避免用戶端伺服器憑證驗證問題。您應該按照以下方式排列該檔案中的憑證：

1. 終端實體（分葉）憑證
2. 中繼憑證（按簽發順序排列）
3. （選用）根憑證

如果您的 *Web* 伺服器支援 *TLS 1.3* 連線，且伺服器上已安裝憑證鏈，您可以在分葉憑證由中繼憑證簽署時，單獨將伺服器憑證和私密金鑰上傳到防火牆。SSL 輸入檢查更詳細地討論每種情況。

若要將目標伺服器的憑證匯入到防火牆上：

1. 在**Device Certificates**（裝置憑證）頁籤上，選取**Import**（匯入）。
2. 輸入描述性的憑證名稱。
3. 瀏覽並選取目標伺服器的 **Certificate File**（憑證檔案）。
4. 按一下 **OK**（確定）。

©2024 Palo Alto Networks, Inc.

STEP 3 | 建立解密政策規則以定義防火牆要解密的流量，以及建立解密設定檔以將 SSL 控制套用至流量。

儘管解密設定檔為選用內容，但最好是在每個解密政策規則中包含解密設定檔，以防加密強度不夠且存在漏洞的通訊協定和演算法允許網路中的可疑流量。

1. 選取 **Policies**（原則） > **Decryption**（解密），**Add**（新增） 或修改現有的規則，然後定義要解密的流量。
2. 選取 **Options**（選項），然後：
   - 設定 **Action**（動作）以 **Decrypt**（解密）符合的流量。
   - 將 **Type**（類型）設定為 **SSL Inbound Inspection**（**SSL** 輸入檢查）。
   - 針對作為輸入 SSL 流量目的地的內部伺服器 **Add**（新增）**Certificates**（憑證）。SSL 輸入檢查政策規則最多支援 12 個憑證。

     您可以設定解密政策規則，以解密管理多個網域（每個網域都有自己的憑證）的內部伺服器的 *SSL/TLS* 流量繫結。防火牆使用政策規則中的憑證（符合伺服器針對要求之 *URL* 提供的憑證）來交涉 *SSL/TLS* 連線。

     若要更新受保護內部伺服器的憑證而不會造成停機，請在新的伺服器憑證到期之前更新或取得該伺服器憑證，否則憑證將會無效。然後，將憑證和私密金鑰匯入防火牆，並將其新增至 *SSL* 輸入檢查政策規則，然後再將新憑證安裝到 *Web* 伺服器上。使用新憑證更新您的政策規則，而其他憑證在 *Web* 伺服器上處於作用中狀態時，會準備防火牆以解密流向伺服器的流量，而不論使用中的憑證為何。

     當您準備好部署新憑證時，請將其載入您的 *Web* 伺服器，並檢查是否已正確安裝。安裝新憑證不會影響現有的連線。防火牆會驗證 *Server Hello* 訊息中的憑證與解密政策規則中的新憑證是否相符。如果不符，工作階段就會結束。對應的解密日誌項目會將工作階段結束原因報告為防火牆與伺服器憑證不相符。將成功交握記入日誌，以檢視在所有輸入檢查工作階段中使用的伺服器憑證。

     (Panorama™) 在 *PAN-OS 10.2* 之前的 *PAN-OS®* 版本中，不支援 *SSL* 輸入檢查政策規則中具有多個憑證。如果您將具有多個憑證的 *SSL* 輸入檢查政策規則從執行 *PAN-OS 11.0* 的 *Panorama* 管理伺服器推送到執行較早版本的防火牆，則受管理防火牆上的政策規則只會繼承依照字母順序排序的憑證清單中的第一個憑證。

     在從 *Panorama* 推送解密政策規則之前，建議您為執行 *PAN-OS 10.1* 及較早版本的防火牆設定不同的範本或裝置群組，以確保推送正確的政策規則和憑證到適當的防火牆。

©2024 Palo Alto Networks, Inc.

- （選用，但為最佳做法）設定或選取現有 **Decryption Profile**（解密設定檔）以封鎖及控制解密流量的各個方面（例如，建立解密設定檔來終止具有不受支援演算法及密碼套件的工作階段）。

  為 *SSL* 輸入檢查流量設定 SSL 通訊協定設定解密設定檔時，需為具有不同安全性功能的伺服器建立單獨的設定檔。例如，若一組伺服器僅支援 *RSA*，則 *SSL* 通訊協定設定僅需要支援 *RSA*。但是，支援 *PFS* 的伺服器的 *SSL* 通訊協定設定應支援 *PFS*。設定 *SSL* 通訊協定設定可獲取伺服器支援的最高安全性等級，但檢查效能可確保防火牆資源可以處理更高安全性通訊協定和演算法要求的更高處理負載。

3. 按一下 **OK**（確定）儲存。

STEP 4 | 啟用防火牆以轉送解密 SSL 流量進行 WildFire 分析。

此選項需要啟用 *WildFire* 授權，這是 WildFire 的最佳做法。

STEP 5 | **Commit**（提交）組態。

STEP 6 | 選擇下一步。

- 允許使用者選擇退出 SSL 解密。
- 設定解密排除項，以對特定類型的流量停用解密。

©2024 Palo Alto Networks, Inc.

設定 SSH Proxy

設定 SSH Proxy 不需要憑證，啟動期間會自動在防火牆上產生用於將 SSH 工作階段解密的金鑰。啟用 SSH 解密後，防火牆將解密 SSH 流量，並根據解密原則和解密設定檔的設定封鎖及/或限制 SSH 流量。流量離開防火牆時會重新加密。

當您設定 *SSH Proxy* 時，通過 *Proxy* 的流量不支援 *DSCP* 代碼點或 *QoS*。

STEP 1 | 確定將適當的介面設定為虛擬介接、Layer 2 或 Layer 3 介面。解密只會在虛擬介接、Layer 2 或 Layer 3 介面上執行。

在 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路）頁籤上檢視已設定的介面。如果介面設定為 **Virtual Wire** 或是 **Layer 2** 或 **Layer 3** 介面，則會顯示 **Interface Type**（介面類型）。您可以選取某個介面來修改其設定，包括為何種介面類型。

STEP 2 | 建立解密原則規則以定義防火牆要解密的流量，以及建立解密設定檔以將檢查套用至 SSH 流量。

儘管解密設定檔為選用內容，但最佳做法是在每個解密原則規則中包含解密設定檔，以防加密強度不夠且存在漏洞的通訊協定和演算法允許網路中的可疑流量。

1. 選取 **Policies**（原則） > **Decryption**（解密），Add（新增）或修改現有的規則，然後定義要解密的流量。
2. 選取 **Options**（選項），然後：
   - 設定規則 **Action**（動作）以 **Decrypt**（解密）符合的流量。
   - 將規則 **Type**（類型）設定為 **SSH Proxy**（**SSL** 代理程式）。
   - （選用，但為最佳做法）設定或選取現有 **Decryption Profile**（解密設定檔）以封鎖及控制解密流量的各個方面（例如，建立解密設定檔來終止具有不受支援版本及演算法的工作階段）。
3. 按一下 **OK**（確定）儲存。

STEP 3 | **Commit**（提交）組態。

STEP 4 | （選用）繼續設定解密排除項，以對特定類型的流量停用解密。

©2024 Palo Alto Networks, Inc.

為未解密的流量設定伺服器憑證驗證

對於個人流量、敏感流量或受當地法律法規約束的流量，您選擇不進行解密，且為其建立無解密原則。例如，您可以選擇不解密某些高階主管的流量，或財務使用者與包含個人資訊的財務伺服器之間的流量。（請勿排除無法解密的流量，因為網站會因釘選憑證或原則的相互驗證之類的技術原因而中斷解密。而是將主機名稱新增到解密排除項清單。）

但是，只是因為您沒有解密流量，並不意味著應讓網路中的任何和所有流量均保持未解密。最佳做法是將「不解密」設定檔套用至未解密的流量，以封鎖使用過期憑證和不受信任之簽發者的工作階段。

STEP 1 | 建立解密原則規則以識別未解密的流量，建立解密設定檔以封鎖不良工作階段。

1. 選取 **Policies**（原則） > **Decryption**（解密），然後 Add（新增）或修改現有規則以識別未解密的流量。
2. 選取 **Options**（選項），然後：
   - 將規則 **Action**（動作）設定為 **No Decrypt**（無解密），以便防火牆不會解密與規則相符的流量。
   - 由於流量未解密，忽略規則 **Type**（類型）。
   - （選用，但為最佳做法）設定或選取現有未解密流量的解密設定檔以封鎖使用過期憑證和不受信任之憑證簽發者的工作階段。

   不要為您未解密的 *TLSv1.3* 流量的解密原則附加「不解密」設定檔，因為防火牆無法讀取加密的憑證資訊，從而無法執行憑證檢查。但是，您仍應為未解密的 *TLSv1.3* 流量建立解密原則，因為除非解密原則控制未解密的流量，否則不會記錄該流量。

STEP 2 | **Commit**（提交）組態。

STEP 3 | 選擇下一步：

- 允許使用者選擇退出 SSL 解密。
- 繼續設定解密排除項，以對特定類型的流量停用解密。

©2024 Palo Alto Networks, Inc.

解密排除項

您可以從解密中排除兩種類型的流量：

- 因技術原因而中斷解密的流量，比如使用釘選憑證、不完整的憑證鏈、不受支援的密碼或相互驗證（嘗試解密流量導致封鎖流量）。Palo Alto Networks 提供了預先定義的 SSL 解密排除項清單（**Device**（裝置）> **Certificate management**（憑證管理）> **SSL Decryption Exclusion**（**SSL** 解密排除項）），用於排除具有應用程式和服務（依預設，從 SSL 解密技術上中斷解密）的主機。如果您遇到在技術上中斷解密且不在 SSL 解密排除項清單的網站，則可以按伺服器主機名稱手動將其新增到清單中。防火牆會封鎖包含技術上中斷解密的應用程式和服務的網站，除非您將其新增到 SSL 解密排除項清單。

  如果解密設定檔允許 **Unsupported Modes**（不受支援的模式）（具有用戶端驗證、不受支援版本或不受支援加密套件的工作階段），防火牆會自動將使用允許的不受支援模式的伺服器和應用程式新增到其本機 SSL 解密排除項快取（**Device**（裝置）> **Certificate Management**（憑證管理）> **SSL Decryption Exclusion**（**SSL** 解密排除項）> **Show Local Exclusion Cache**（顯示本機排除項快取））。封鎖不受支援的模式後，可增加安全性，但同時也封鎖了與使用那些模式的應用程式進行通訊。
- 出於業務、法規、個人或其他原因（例如金融服務、醫療保健或政府流量），選擇不解密這些流量。您可以選擇根據來源、目的地、URL 類別和服務排除流量。

您可用星號 (*) 作為萬用字元，為與網域關聯的多個主機名稱名建立解密排除項。星號的表現與 URL 類別排除項的脫字符 (^) 的表現相同—每個星號控制主機名稱中的一個子網域（標籤）。這使您可以建立非常具體和非常一般的排除項。例如：

- mail.*.com 匹配 mail.company.com，但不匹配 mail.company.sso.com。
- *.company.com 匹配 tools.company.com，但不匹配 eng.tools.company.com.
- *.*.company.com 匹配 eng.tools.company.com，但不匹配 eng.company.com.
- *.*.*.company.com 匹配 corp.exec.mail.company.com，但不匹配 corp.mail.company.com.
- mail.google.* 匹配 mail.google.com，但不匹配 mail.google.uk.com.
- mail.google.*.* 匹配 mail.google.co.uk，但不匹配 mail.google.com.

例如，要使用萬用字元將 video-stats.video.google.com 從解密中排除，而不將 video.google.com 從解密中排除，請排除 *.*.google.com。

不管主機名稱前面有多少個星號萬用字元（主機名稱之前沒有非萬用字元標籤），主機名稱都與項目匹配。例如，**.google.com*、**.*.google.com* 和 **.*.*.google.com* 都與 *google.com* 匹配。然而，**.dev.*.google.com* 不匹配 *google.com*，因為標籤 *(dev)* 不是萬用字元。

為了提高流量的可見性並盡可能減少受攻擊面，除非必須，否則不要建立解密例外項。

- Palo Alto Networks 預先定義解密排除項
- 出於技術原因將伺服器排除在解密之外

©2024 Palo Alto Networks, Inc.

- 本機解密排除快取
- 建立基於原則的解密排除項

Palo Alto Networks 預先定義解密排除項

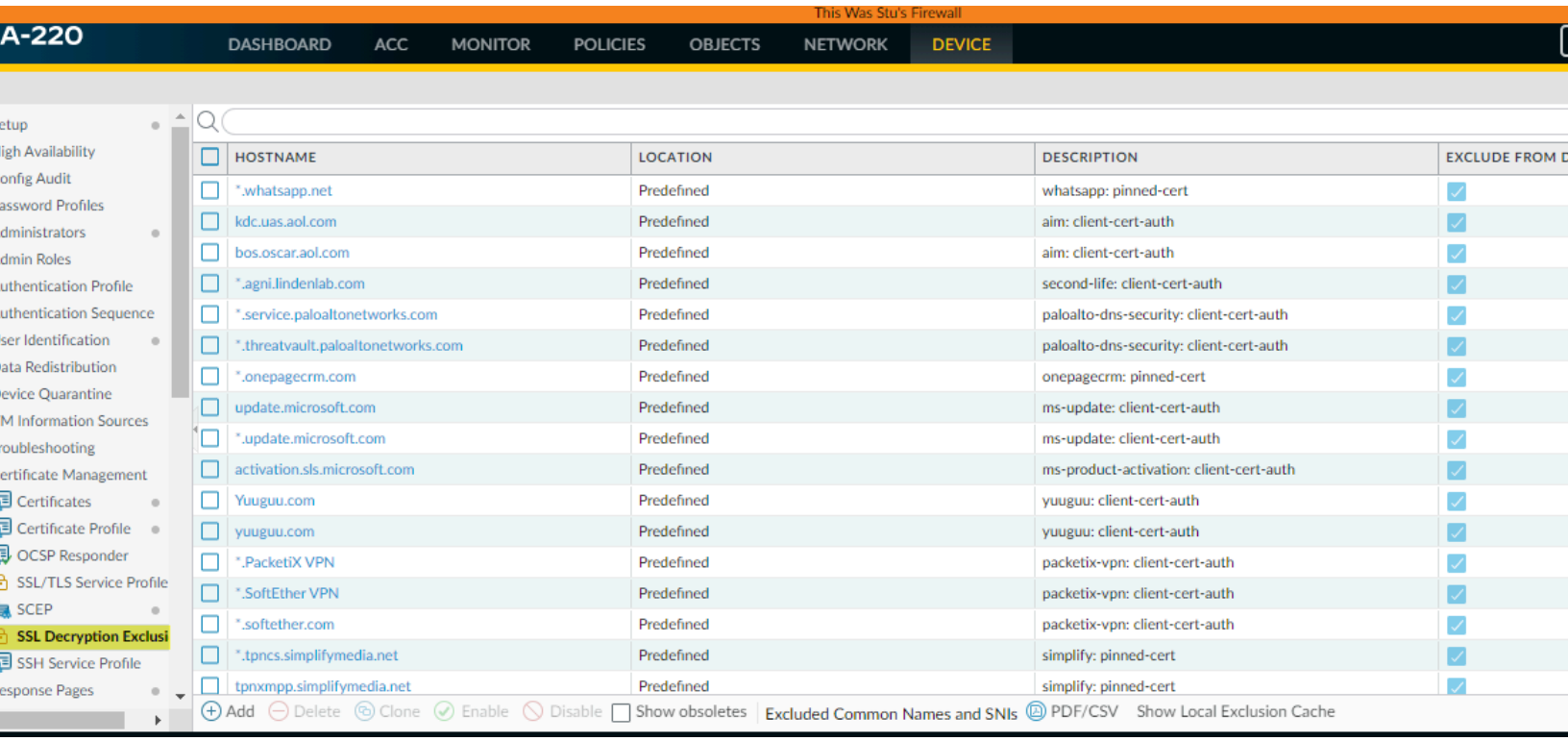
防火牆提供預先定義的 SSL 解密排除項清單，以便將因釘選憑證和相互驗證之類的技術原因而中斷解密的常用網站排除在解密之外。依預設，啟用預先定義的解密排除項，Palo Alto Networks 將向防火牆傳送新的和更新的預先定義解密排除項，作為應用程式和威脅內容更新或應用程式內容更新（如果您沒有 Threat Prevention（威脅防禦）授權）的一部分。防火牆不會解密符合預先定義排除項的流量，並根據管理該流量的安全性原則允許加密流量。然而，防火牆無法檢查加密流量或對其執行安全性原則。

出於法律、法規、業務、隱私權或其他意志原因而選擇不解密的網站不適合使用 *SSL* 解密排除項清單，該清單僅適用於技術上中斷解密的網站（解密這些網站會封鎖網站流量）。對於您選擇不解密的流量，例如 *IP* 位址、使用者、*URL* 類別、服務，甚至是整個區域，請建立基於原則的解密排除項。

由於 SSL 解密排除項清單上的網站流量仍為加密狀態，防火牆不會檢查流量或為其提供進一步的安全性執行。您可以停用預先定義的排除項。例如，您可以選擇停用預先定義的排除項，強制執行嚴格的安全性原則，以僅允許防火牆可以檢查以及對其強制執行安全性原則的應用程式和服務。但是，如果未在 SSL 解密排除項清單中啟用技術上中斷解密的應用程式和服務，則防火牆會封鎖包含這些應用程式和服務的網站。

您可以直接在防火牆上檢視和管理 Palo Alto Networks 預先定義的所有 SSL 解密排除項（**Device**（裝置） > **Certificate Management**（憑證管理） > **SSL Decryption Exclusions**（**SSL** 解密排除項））。

©2024 Palo Alto Networks, Inc.



Hostname（主機名稱）顯示包含技術上中斷解密之應用程式或服務的主機名稱。若伺服器不在預先定義的清單上，您還可以 **Add**（新增）主機，以出於技術原因將伺服器排除在解密之外。

Description（說明）顯示防火牆無法解密網站流量的原因，例如 **pinned-cert**（釘選憑證）或 **client-cert-auth**（用戶端驗證）。

如果已啟用的預先定義 SSL 解密排除項過時，防火牆會自動將其從清單中移除（若之前進行解密而造成中斷的應用程式現在已支援解密，防火牆會移除該應用程式）。**Show Obsoletes**（顯示過時）檢查是否有任何已停用的預先定義排除項保留在清單上且不再需要。防火牆不會自動將已停用的預先定義解密排除項從清單中移除，但您可以選取並 **Delete**（刪除）過時項目。

您可以選取主機名稱的核取方塊，然後按一下 **Disable**（停用）以從清單中移除預先定義的網站。僅對因技術原因而中斷解密的網站使用 SSL 解密排除項清單，請勿對選擇不解密的網站使用該清單。

出於技術原因將伺服器排除在解密之外

如果解密在技術上中斷了重要的應用程式或服務（解密流量會將其封鎖），則可以將管理到應用程式或服務之網站的主機名稱新增至 Palo Alto Networks 預先定義的 SSL 解密排除項清單，以建立自訂解密例外項。由於流量仍為加密狀態，防火牆不會對 SSL 解密排除項清單允許的流量進行解密、檢查和強制執行安全性原則，務必確保新增到清單中的網站確實包含業務所需的應用程式或服務。例如，某些關鍵業務內部自訂應用程式可能會中斷解密，您可以將其新增到清單中，以便防火牆允許加密的自訂應用程式流量。

©2024 Palo Alto Networks, Inc.

出於法律、法規、業務、隱私權或其他意志原因而選擇不解密的網站不適合使用 *SSL* 解密排除項清單，該清單僅適用於技術上中斷解密的網站。對於您選擇不解密的流量（*IP* 位址、使用者、*URL* 類別、服務，甚至是整個區域），請建立基於原則的解密排除項。

網站技術上中斷解密的原因包括釘選憑證、用戶端驗證、不完整的憑證鏈和不受支援的密碼。對於 HTTP 公開金鑰固定 (HPKP)，只要在用戶端安裝了企業 CA 憑證（或憑證鏈），大部分使用 HPKP 的瀏覽器都會允許正向 Proxy 解密。

如果將網站排除在解密之外的技術原因是憑證鏈不完整，則新世代防火牆不會像瀏覽器那樣自動修正該鏈。如果需要將網站新增到 *SSL* 解密排除項清單，請手動檢閱網站以確保它是合法的業務網站，然後下載遺失的子 *CA* 憑證並將其載入及部署到防火牆上。

將伺服器新增到 SSL 解密排除清單後，防火牆會將用於定義解密排除項之伺服器主機名稱，與 Client Hello 訊息中的伺服器名稱指示 (SNI) 和伺服器憑證中的通用名稱 (CN) 進行比較。如果 SNI 或 CN 與 SSL 解密排除清單中的項目相符，則防火牆會從解密中排除流量。

STEP 1 | 選取 **Device**（裝置） > **Certificate Management**（憑證管理） > **SSL Decryption Exclusions**（**SSL** 解密排除）。

STEP 2 | **Add**（新增）新的解密排除項，或選取現有自訂項目進行修改。

STEP 3 | 輸入您要從解密工作中排除的網站或應用程式的 **hostname**（主機名稱）。

主機名稱區分大小寫。

您可以使用萬用字元排除與網域關聯的多個主機名稱。防火牆排除伺服器顯示匹配解密工作網域的 CN 的所有工作階段。

確保每個自訂項目的主機名稱欄位都是唯一的。如果預先定義的排除項與自訂項目相符，則優先選擇自訂項目。

STEP 4 | （選用）選取 **Shared**（共用），可在多個虛擬系統防火牆中的所有虛擬系統間共用排除項。

STEP 5 | 將應用程式排除在解密外。或者，如果您要修改現有解密排除項，可以清除此核取方塊，以開始解密之前已從解密工作中排除項目。

STEP 6 | 按一下 **OK**（確定）以儲存新的解密項目。

本機解密排除快取

防火牆可以將伺服器新增到本機解密排除快取（**Device**（裝置） > **Certificate Management**（憑證管理） > **SSL Decryption Exclusion**（**SSL** 解密排除項） > **Show Local Exclusion Cache**（顯示本機排除快取）），且如果該流量由於技術原因（如釘選憑證或不受支援的憑證）而中斷解密，則會在 12 個小時內自動將其流量從解密中排除。當解密設定檔允許使用不受支援的模式（具有用戶端驗證、不受支援的版本或不受支援的加密套件的工作階段），以及允許的流量使用不受支援的模式

©2024 Palo Alto Networks, Inc.

時，裝置會自動將伺服器新增到本機排除快取中並繞過解密。防火牆不會對本機解密排除快取允許的流量進行解密、檢查和強制執行安全性原則，因為流量仍處於加密狀態。確保您從解密中排除的網站（透過套用允許不受支援模式的解密設定檔）是具有業務所需的應用程式或服務的網站。

封鎖不受支援的模式將封鎖與使用那些模式的應用程式進行通訊，以提高安全性。用戶端驗證是將應用程式從解密中排除的常見原因，這也是為什麼最佳做法是封鎖不受支援的版本和不受支援的密碼，並在解密設定檔中允許用戶端驗證。如果解密設定檔允許用戶端驗證，則當用戶端啟動伺服器要求用戶端進行驗證的工作階段時，防火牆會將應用程式和伺服器新增到本機排除快取並允許該流量，而不是由於防火牆無法解密流量而將其封鎖。

如果您允許來自使用用戶端驗證的網站的流量，且這些網站不在 SSL 解密排除清單上的預先定義網站中，請建立一個允許進行用戶端驗證之工作階段的解密設定檔。將該設定檔新增到僅適用於託管該應用程式之伺服器的解密原則規則。為了進一步增強安全性，您可以要求多因素驗證來完成使用者登入過程。或者，您可以將網站新增到 *SSL* 解密排除清單中，以在不使用明確解密原則的情況下跳過解密。

防火牆根據控制應用程式流量的解密原則和設定檔新增本機 SSL 解密排除快取項目。如果您沒有在解密設定檔中封鎖不受支援模式檢查，則在以下情況下，防火牆會將項目新增到本機 SSL 解密排除快取中：

- 用戶端僅支援 TLSv1.2 且伺服器僅支援 TLSv1.3。在本機快取中，針對此排除項顯示的原因為 SSL_UNSUPPORTED。
- 用戶端支援 TLSv1.3 和 TLSv1.2，而伺服器僅支援 TLSv1.2。在此情況下，**Reason**（原因）欄顯示 TLS13_UNSUPPORTED。

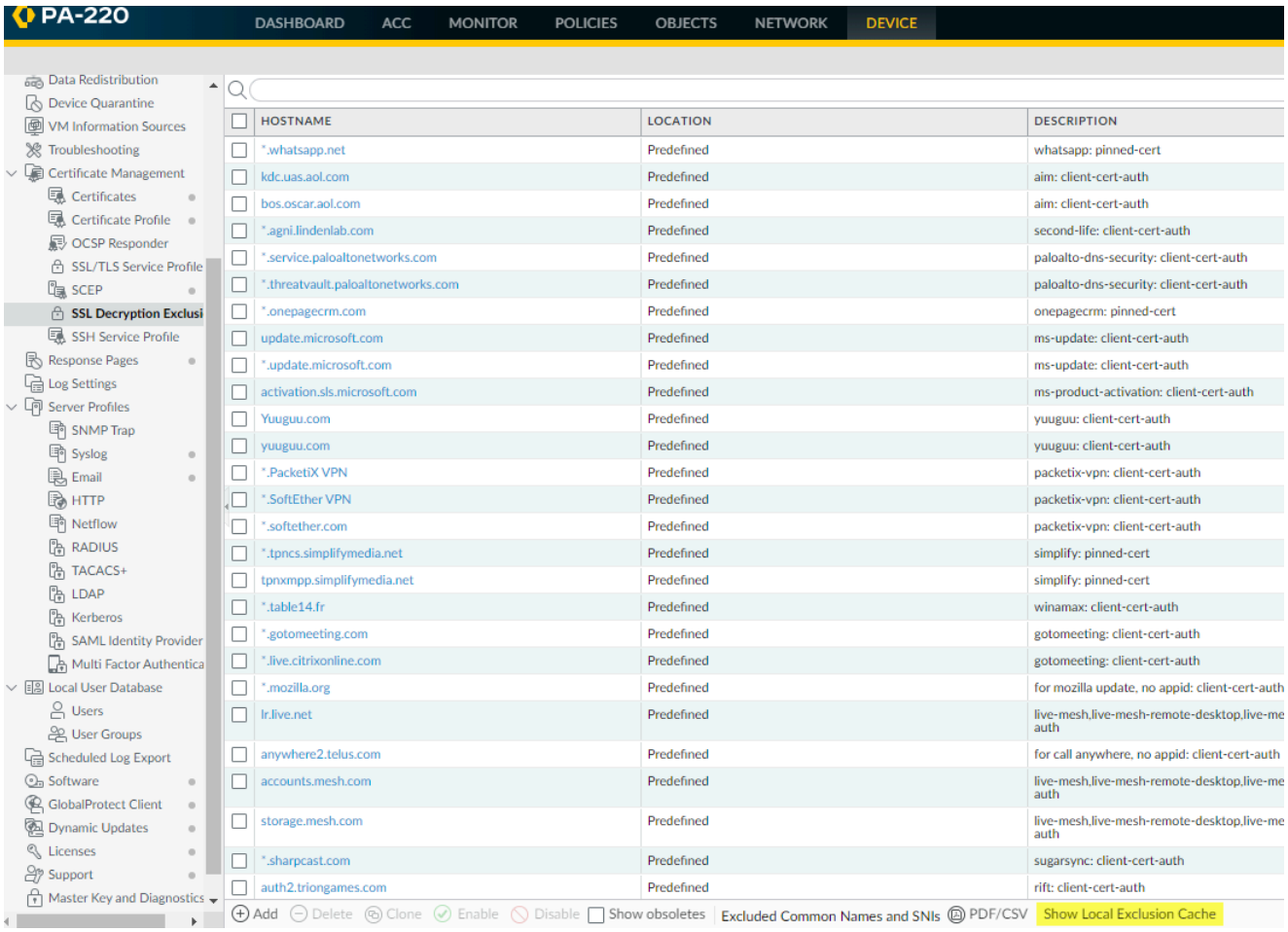
  

  當將伺服器新增到本機 *SSL* 解密排除快取的 ***Reason***（原因）為 *TLS13_UNSUPPORTED* 時，防火牆會將通訊協定降級到 *TLSv1.2*，且防火牆會解密並檢查流量。
- 用戶端宣告伺服器不支援的特定密碼。
- 用戶端宣告伺服器不支援的特定曲線。

本機快取包含最多 1,024 個項目。您不能手動將本機排除項新增到本機 SSL 解密排除快取中（但您可以手動將解密排除項新增到 SSL 解密排除清單中）。

您必須具有超級使用者或憑證管理存取權限，才能檢視本機 SSL 解密排除快取。要檢視該快取，請導覽至 **Device**（裝置）> **Certificate Management**（憑證管理）> **SSL Decryption Exclusion**（**SSL** 解密排除），然後按一下靠近螢幕底部的 **Show Local Exclusion Cache**（顯示本機排除快取）。本機排除快取顯示每個項目的應用程式、伺服器、包含在快取中的原因、控制流量的解密設定檔以及更多資訊。您可以手動從本機快取中選取並刪除項目。

©2024 Palo Alto Networks, Inc.



您還可以使用 CLI 刪除快取的項目：

```
clear ssl-decrypt exclude-cache [server <value>] [application
 <value>]
```

如果有人在本機快取項目逾時（12 個小時）之前嘗試存取同一伺服器，則防火牆會將工作階段與快取項目進行比對，繞過解密並允許流量。若變更解密原則或設定檔，則防火牆會清除本機排除快取，因為這些變更可能會變更工作階段的分類。若快取已滿，則防火牆會在新項目抵達時清除最舊的項目。

建立基於原則的解密排除項

基於原則的解密排除項用於排除您選擇不解密的流量。您可以根據流量的來源、目的地、服務或 URL 類別的任意組合建立基於原則的解密排除項。您可能選擇不解密的流量範例包括：

- 由於包含個人可識別資訊 (PII) 或其他敏感資訊而不得解密的流量，例如金融服務、醫療保健或政府流量等 URL 篩選類別。
- 源自或預期送達高階主管或其他不應解密流量之使用者的流量。
- 某些裝置（如財務伺服器）可能需要排除在解密之外。

©2024 Palo Alto Networks, Inc.

- 根據業務的不同，一些公司可能看重隱私權和使用者體驗，而不僅僅是某些應用程式的安全性。
- 禁止解密某些流量的法律或當地法規。

  歐盟 (EU) 一般資料保護法規 (GDPR) 便是一個為遵循法規和法律符合性而不解密流量的範例。EU GDPR 將要求對所有個人的所有個人資料進行強有力的保護。GDPR 影響了所有收集或處理歐盟居民個人資料的公司（包括外國公司）。

  不同的法規和符合性規則可能意味著，您在不同的國家或地區對相同資料的處理方式會有所不同。由於企業擁有其公司資料中心中的個人資訊，企業通常可解密該資訊。最佳做法是盡可能多地解密流量，以便您可以瞭解流量並對其套用安全性保護。

您可以使用預先定義的 URL 類別來使整個網站類別免於解密，可以建立自訂 URL 類別來定義您不想解密之自訂 URL 的清單，或者您可以建立外部動態清單 (EDL) 來定義您不想解密之自訂 URL 的清單。

在具有動態變化 IP 位址的環境（如 Office 365）中，或者在您要對免於解密的 URL 清單進行頻繁更改的環境中，通常最好使用 EDL 而不是 URL 類別來指定排除的 URL。在動態環境中使用 EDL 所造成的干擾較少，因為編輯 EDL 會導致 URL 類別動態變化，無需 **Commit**（提交），而編輯自訂 URL 類別需要 **Commit**（提交）才能生效。

建立 *EDL* 或自訂 *URL* 類別，其中包含您選擇不解密的所有類別，以便一個解密原則規則管理您選擇允許的加密流量。套用不解密設定檔至規則。新增類別至 *EDL* 或自訂 *URL* 類別的功能，讓您可輕鬆將流量排除在解密之外，並有助於保持規則庫整潔。

與安全性原則規則類似，防火牆將傳入流量與原則規則庫順序中的解密原則規則進行比較。將解密排除項規則置於規則庫頂端以防止意外解密法律或法規阻止您解密的流量。

如果您建立基於原則的解密排除項，則最佳做法是將以下排除項規則置於解密規則庫的頂端，順序如下：

1. 適用於敏感目的地伺服器之基於 IP 位址的例外。
2. 適用於高階主管和其他使用者或群組之基於來源使用者的例外。
3. 適用於目的地 URL 之基於自訂 URL 或 EDL 的例外。
4. 基於預先定義之敏感 URL 類別的例外，用於整個類別（如金融服務、醫療保健和政府）的目的地 URL。

將這些規則之後的流量解密規則放在解密規則庫中。

©2024 Palo Alto Networks, Inc.

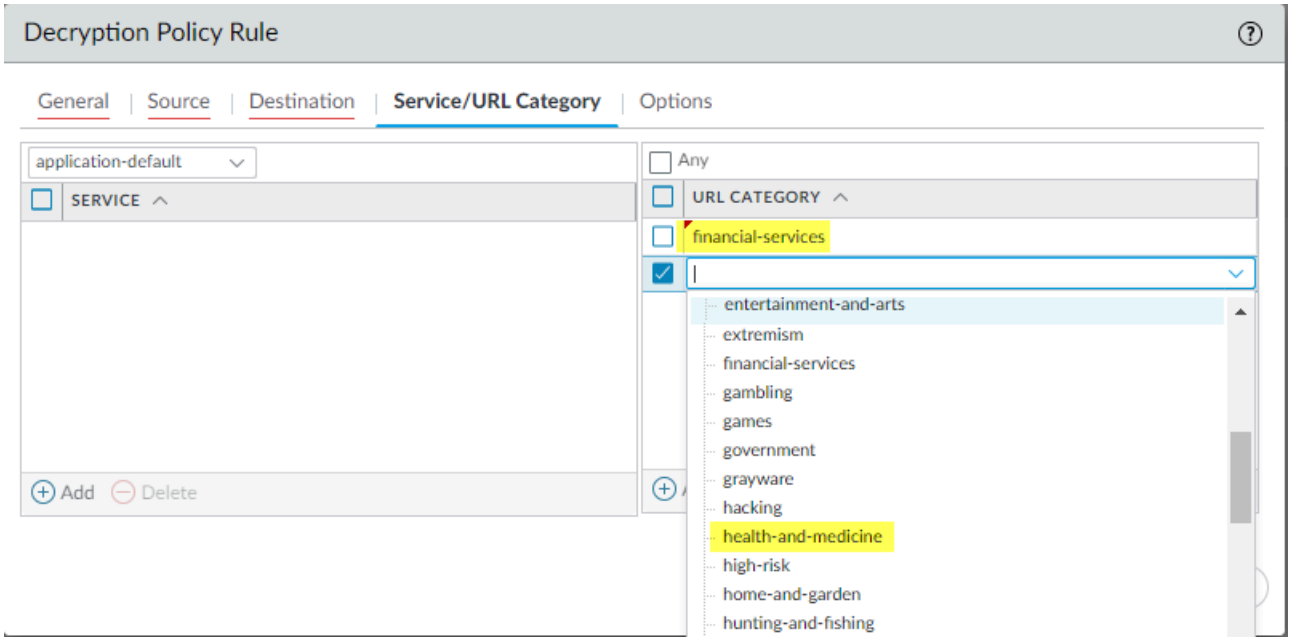
STEP 1 | 根據比對準則將流量排除在解密之外。

此範例顯示如何將歸類為金融或健康相關的流量排除 SSL 正向 Proxy 解密。

1. 選取 **Policies**（原則） > **Decryption**（解密），然後 **Add**（新增） 或修改安全性原則規則。
2. 定義您要排除在解密之外的流量。

   在本範例中：

   1. 為規則指定具描述性的 **Name**（名稱），例如 No-Decrypt-Finance-Health。
   2. 將 **Source**（來源）與 **Destination**（目的地）設定為 **Any**（任何），以將 No-Decrypt-Finance-Health 規則套用至目的地為外部伺服器的所有 SSL 流量。
   3. 選取 **URL Category**（**URL** 類別）並 **Add**（新增）URL 類別（金融服務及醫療保健）。



3. 選取 **Options**（選項），將規則設定為 **No Decrypt**（無解密）。
4. （選用，但為最佳做法）建立一個無解密設定檔，並將其附加到該規則，以驗證防火牆未解密的工作階段的憑證。將設定檔設定為 **Block sessions with expired certificates**（封鎖具有到期憑證的工作階段）與 **Block sessions with untrusted issuers**（封鎖具有不受信任之簽發者的工作階段）。

   例外狀況：不要為您未解密的 *TLSv1.3* 流量的解密原則附加「不解密」設定檔，因為防火牆無法讀取加密的憑證資訊，從而無法執行憑證檢查。但是，您仍應為未解密的 *TLSv1.3* 流量建立解密原則，因為除非解密原則控制未解密的流量，否則不會記錄該流量。
5. 按一下 **OK**（確定）來儲存 No-Decrypt-Finance-Health 解密規則。

©2024 Palo Alto Networks, Inc.

STEP 2 | 將解密排除項規則放置在解密原則規則庫頂端。

防火牆對規則庫順序中的傳入流量強制執行解密規則，並強制執行與流量相符的第一個規則。

選取 **No-Decrypt-Finance-Health** 原則（**Decryption**（解密） > **Policies**（原則）），然後按一下 **Move Up**（上移），直至其出現在清單頂端，或者拖放規則。

STEP 3 | 儲存組態。

按一下 **Commit**（交付）。

 ©2024 Palo Alto Networks, Inc.

封鎖私密金鑰匯出

當您在 PAN-OS 或 Panorama 中產生憑證私密金鑰或將憑證私密金鑰匯入其中時，可以永久封鎖匯出憑證的私密金鑰。封鎖從您的 PAN-OS 裝置匯出私密金鑰可加強安全性，因為這會阻止惡意管理員或其他危險分子誤用金鑰。具有憑證管理權限的管理員可以封鎖匯出私密金鑰。您不能封鎖裝置上已經存在的金鑰；您只能在 PAN-OS 中產生金鑰或向其匯入金鑰時封鎖金鑰。

當一名管理員封鎖匯出私密金鑰後，任何管理員都不能匯出該金鑰，即使超級使用者管理員也不可以。如果您需要從 PAN-OS 設備匯出私密金鑰，請重新產生憑證和金鑰，同時不要選取封鎖私密金鑰匯出的選項。

要降級到之前的 PAN-OS 版本，您必須先刪除封鎖了私密金鑰的憑證。如果您在嘗試降級前沒有刪除封鎖了私密金鑰的憑證，會出現一條錯誤訊息，要求您刪除這些憑證。在刪除前，您將無法降級。降級後，如果您有需要，可以重新匯入或重新產生刪除的憑證。

如果您使用企業公開金鑰基礎結構 *(PKI)* 來產生憑證和私密金鑰，請封鎖匯出私密金鑰。因為您可以從您的企業憑證授權單位 *(CA)* 將其安裝在新的防火牆和 *Panoramas* 上，所以沒有理由再從 *PAN-OS* 匯出它們。

如果您在防火牆或 *Panorama* 產生自我簽署憑證並套用封鎖私密金鑰匯出選項，則不能將憑證和金鑰匯出至其他 *PAN-OS* 設備。

即使您封鎖匯出私密金鑰，仍可以匯出和匯入裝置狀態（**Device**（裝置） > **Setup**（設定） > **Operations**（操作））。我們在裝置狀態匯入和匯出中包含了私密金鑰，但是管理員無法讀取或解碼它們。

如果兩個防火牆上的主要金鑰相同，您可以在一個防火牆上匯入或載入另一個防火牆的設定。如果防火牆上的主要金鑰不相同，那麼匯入或載入設定不起作用，且在讀取憑證時會提交失敗。

- 產生私密金鑰並將其封鎖
- 匯入私密金鑰並將其封鎖
- 匯入 IKE 閘道的私密金鑰並將其封鎖
- 驗證私密金鑰封鎖

產生私密金鑰並將其封鎖

在產生憑證後封鎖匯出私密金鑰以防止其誤用。

STEP 1 | 選取 **Device**（設備） > **Certificate Management**（憑證管理） > **Certificates**（憑證） > **Device Certificates**（裝置憑證）。

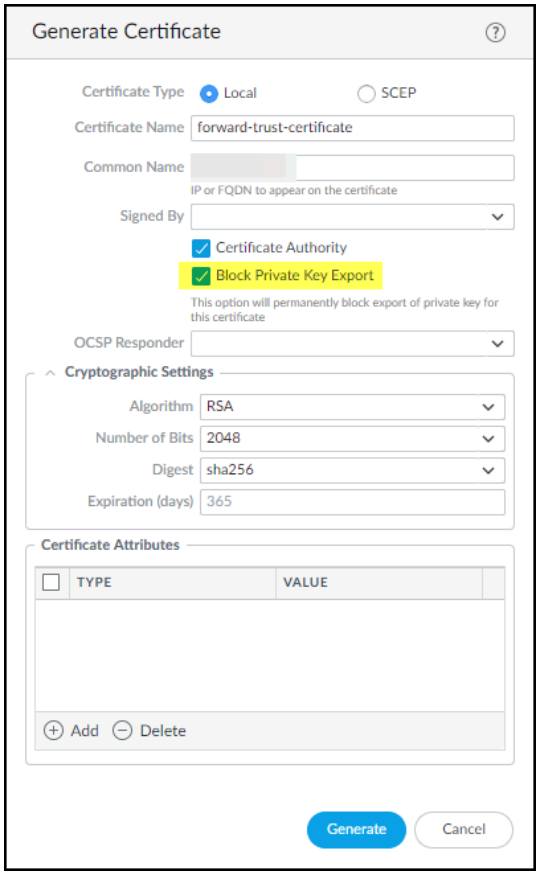
若存在多個虛擬系統，為憑證選取一個 **Location**（位置）或 **Shared**（共用）。

STEP 2 | 產生憑證。

STEP 3 | 選取 **Block Private Key Export**（封鎖私密金鑰匯出）以防止任何人匯出憑證。

©2024 Palo Alto Networks, Inc.

參閱產生憑證獲取有關其他憑證欄位的資訊。



STEP 4 | 按一下 **Generate**（產生），產生新憑證。

您還可以使用操作 *CLI* 命令產生憑證並封鎖其私密金鑰匯出：

```
admin@pa-220> request certificate generate block-private-keys yes
```

之前的 *CLI* 命令還可以包含憑證和未顯示的其他參數。

匯入私密金鑰並將其封鎖

在匯入憑證後封鎖匯出私密金鑰以防止其誤用。

STEP 1 | 選取 **Device**（設備） > **Certificate Management**（憑證管理） > **Certificates**（憑證） > **Device Certificates**（裝置憑證）。

若存在多個虛擬系統，為憑證選取一個 **Location**（位置）或 **Shared**（共用）。

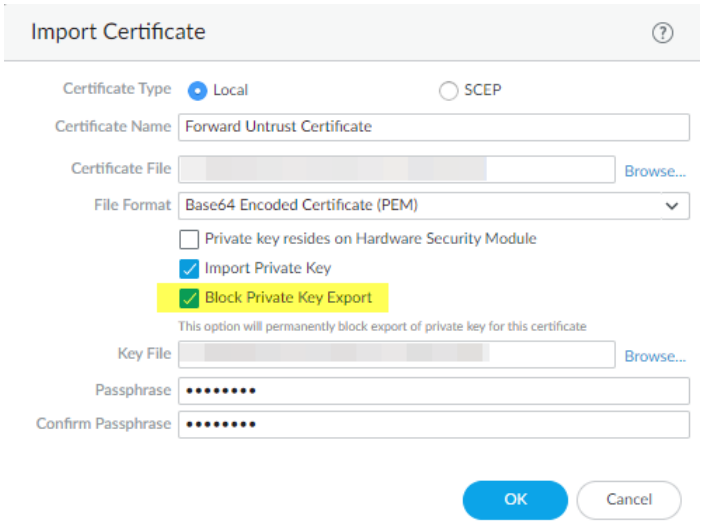
STEP 2 | **Import**（匯入）憑證。

©2024 Palo Alto Networks, Inc.

STEP 3 | 選取 **Import Private Key**（匯入私密金鑰）以啟動封鎖私密金鑰匯出的選項。

STEP 4 | 選取 **Block Private Key Export**（封鎖私密金鑰匯出）以防止任何人匯出憑證。

請參閱匯入憑證和私密金鑰，獲取有關其他憑證匯入欄位的資訊。



STEP 5 | 按一下確定匯入憑證。

如果您使用 *SCP* 操作性 *CLI* 命令匯入憑證或為憑證匯入私密金鑰，您仍然可以封鎖匯出私密金鑰：

- ***admin@pa-220> scp import private-key block-private-key ...***

每個之前的 *CLI* 命令還可以包含關鍵字以指定來源、憑證名稱和未顯示的其他參數。

如果您使用 *SCP* 操作 *CLI* 命令來匯出憑證並包含其私密金鑰 ***(scp export certificate passphrase <phrase> remote-port <1-65536> to <destination> certificate-name <name> include-key <yes | no> format <der | pem | pkcs10 | pkcs12>)***，且如果憑證的私密金鑰被封鎖，則命令會失敗，並返回一條錯誤訊息，因為您無法匯出被封鎖的私密金鑰。

匯入 IKE 閘道的私密金鑰並將其封鎖

在為 IKE 閘道驗證產生憑證後封鎖匯出私密金鑰以防止其誤用。

STEP 1 | 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **IKE Gateways**（**IKE** 閘道）。

©2024 Palo Alto Networks, Inc.

STEP 2 | **Add**（新增）一個新 IKE 閘道。

STEP 3 | 在 **General**（一般）頁簽上，針對 **Authentication**（驗證），選取 **Certificate**（憑證）。

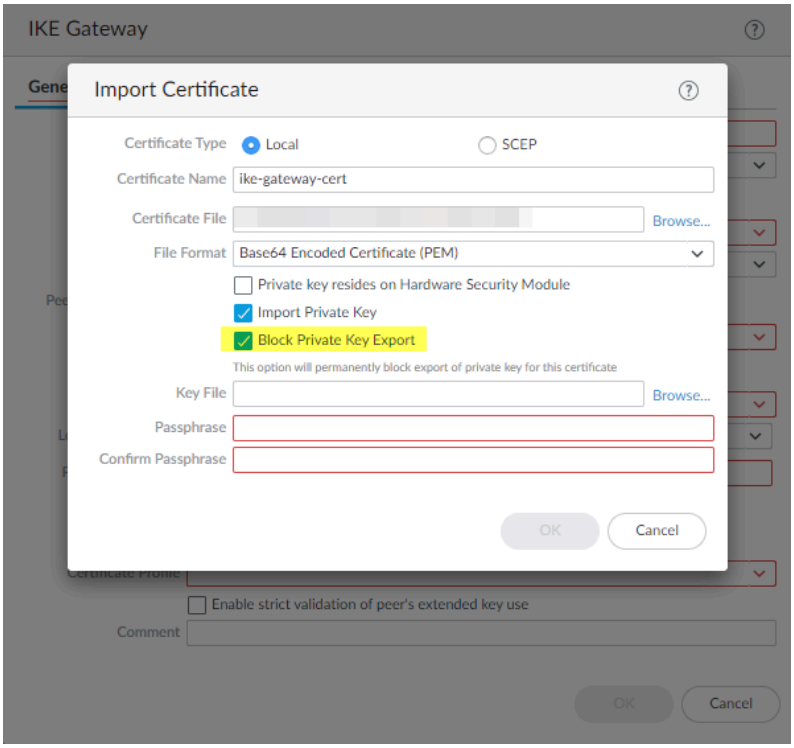
STEP 4 | 對於 **Local Certificate**（本機憑證），選取 **Import**（匯入）或 **Generate**（產生），具體取決於您想要匯入現有憑證還是建立憑證。

STEP 5 | 輸入憑證資訊。如果匯入憑證，則選取 **Import Private Key**（匯入私密金鑰）以啟動 **Block Private Key Export**（封鎖私密金鑰匯出）核取方塊。

©2024 Palo Alto Networks, Inc.

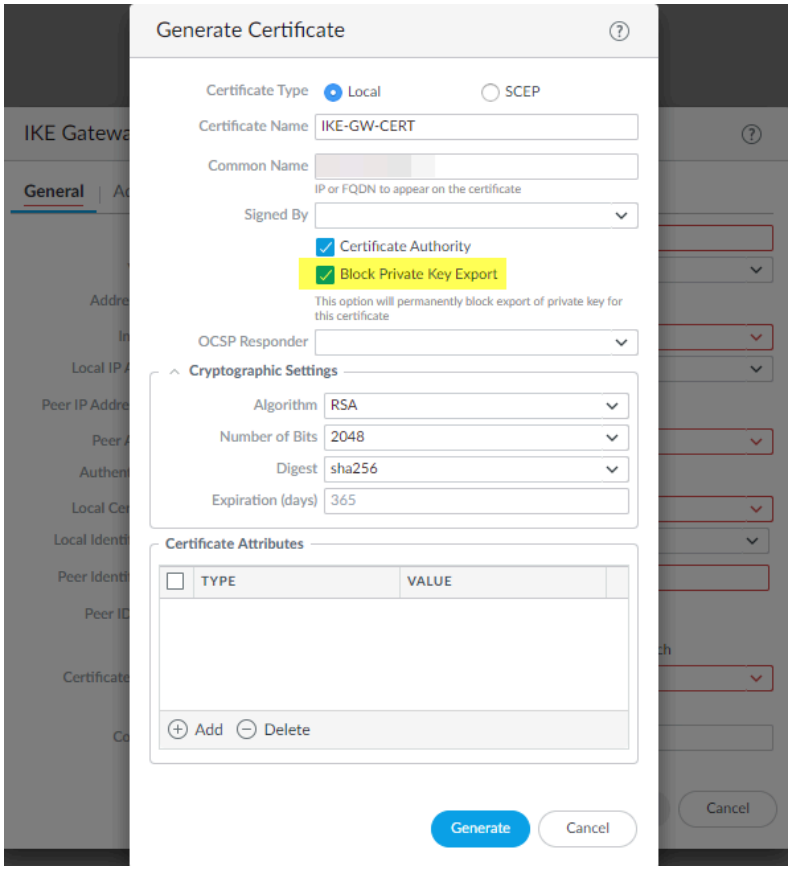
STEP 6 | 選取 **Block Private Key Export**（封鎖私密金鑰匯出）以防止任何人匯出金鑰。

若要匯入憑證，輸入並確認 **Passphrase**（複雜密碼），然後按一下 **OK**（確定）



若要產生憑證，按一下 **Generate**（產生）。

 ©2024 Palo Alto Networks, Inc.



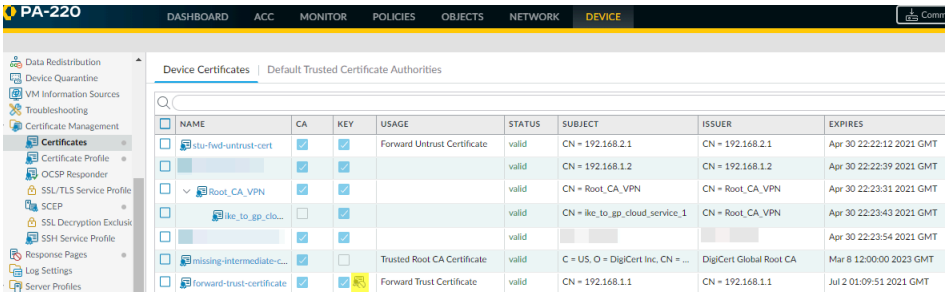
STEP 7 | 輸入 **Passphrase**（複雜密碼），確認，然後按一下 **OK**（確定）。

驗證私密金鑰封鎖

您可以使用幾種方法驗證是否已封鎖匯出私密金鑰。

查看 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證） > **Device Certificates**（裝置憑證）中的 **Key**（金鑰）欄。

在本範例中，forward-trust-certificate 被封鎖：



當您嘗試匯出其私密金鑰被封鎖匯出的憑證時，**Export Private Key**（匯出私密金鑰）核取方塊將不可用，且您無法匯出金鑰，只能匯出憑證。

 ©2024 Palo Alto Networks, Inc.

使用以下操作性 CLI 命令列出裝置上或特定 Vsys 上私密金鑰被封鎖匯出的所有憑證：

```
admin@pa-220> request certificate show-blocked <shared | vsys>
```

使用以下操作性 CLI 命令檢查特定憑證的私密金鑰是否封鎖匯出：

```
admin@pa-220> request certificate is-blocked certificate-name
 <name>
```

If the certificate is blocked from export, the command returns **yes** and if the certificate is not blocked the command returns **no**.

©2024 Palo Alto Networks, Inc.

允許使用者選擇退出 SSL 解密

在涉及敏感隱私的情況下，您可能需要提醒使用者防火牆正在解密某些網路流量，並允許他們在瞭解其流量會被解密的情況下繼續造訪該網站，或終止工作階段並阻止其移至網站。（無法選擇造訪網站以及避免解密。）

使用者第一次嘗試瀏覽符合解密原則的 HTTPS 網站或應用程式時，防火牆會顯示回應頁面來通知使用者將解密該工作階段。使用者可以按一下 **Yes**（是）允許解密並接續瀏覽該網站，或按一下 **No**（否）選擇退出解密並終止工作階段。該選項可允許解密套用至使用者在接下來 24 小時內嘗試存取的所有 HTTPS 網站，此後，防火牆將重新顯示回應頁面。在下一分鐘選擇退出 SSL 解密的使用者無法存取請求的 Web 頁面，或任何其他 HTTPS 網站。此後，防火牆將在使用者下次嘗試存取 HTTPS 網站時，重新顯示回應頁面。

防火牆包括您可以啟用的預先定義 (SSL 解密選擇退出頁面)。您可以選擇性地使用自己的文字和/或影像自訂頁面。然而，最佳做法是不允許使用者選擇退出解密。

大於支援大小上限的自訂回應頁面不會被解密或顯示給使用者。在 *PAN-OS 8.1.2* 與較早版本 *PAN-OS 8.1* 中，解密網站上的自訂回應頁面不能超過 *8,191* 個位元組；在 *PAN-OS 8.1.3* 及更高版本中，最大大小增加到 *17,999* 個位元組。

STEP 1 | （選用）自訂 SSL 解密選擇退出頁面。

1. 選取 **Device**（裝置） > **Response Pages**（回應頁面）。
2. 選取 **SSL Decryption Opt-out Page**（**SSL** 解密選擇退出頁面）連結。
3. 選取**Predefined**（預先定義）頁面，然後按一下**Export**（匯出）。
4. 使用您所選擇的 HTML 文字編輯器來編輯頁面。
5. 如果您要新增影像，請在可從一般使用者系統存取的 Web 伺服器上代管該影像。
6. 在 HTML 中新增一行以指向該影像。例如：

```
<img src="http://cdn.slidesharecdn.com/ Acme-logo-96x96.jpg?
1382722588"/>
```

7. 以新檔案名稱儲存編輯的頁面。請確保該頁面保留其 UTF-8 編碼。
8. 回到防火牆，選取 **Device**（裝置） > **Response Pages**（回應頁面）。
9. 選取 **SSL Decryption Opt-out Page**（**SSL** 解密選擇退出頁面）連結。
10. 按一下 **Import**（匯入），然後在 **Import File**（匯入檔案）欄位中輸入路徑與檔案名稱，或 **Browse**（瀏覽）以尋找檔案。
11. （選用）從 **Destination**（目的地）下拉式清單中選取將要使用此登入頁面的虛擬系統，或選取 shared（共用）以使其可用於所有虛擬系統。
12. 按一下 **OK**（確定）匯入檔案。
13. 選取您剛才匯入的回應頁面，再按一下 **Close**（關閉）。

©2024 Palo Alto Networks, Inc.

STEP 2 | 啟用 SSL 解密選擇退出。

1. 在 **Device**（裝置） > **Response Pages**（回應頁面） 頁面上，按一下 **Disabled**（已停用）連結。
2. 選取 **Enable SSL Opt-out Page**（啟用 **SSL** 選擇退出頁面），然後按一下 **OK**（確定）。
3. **Commit**（提交）變更。

STEP 3 | 確認當您嘗試瀏覽網站時，選擇退出頁面會顯示。

在瀏覽器中移至符合您解密原則的加密網站。

確認顯示 SSL 解密選擇退出回應頁面。

 ©2024 Palo Alto Networks, Inc.

暫時停用 SSL 解密

在某些狀況下，您會想要暫時停用 SSL 解密。例如，若您過於倉促地部署 SSL 解密致使某些工作無法正常進行，但您又不確定具體問題並且需要檢查許多規則，則可以使用 CLI 暫時關閉解密，並給自己時間來分析和解決問題。解決問題之後，您可以使用 CLI 再次開啟 SSL 解密。由於使用 CLI 暫時停用然後再次啟用解密並不需要執行 Commit（提交）作業，無需中斷網路流量便可完成此作業。

使用下列 CLI 命令暫時停用 SSL 解密，然後將其重新啟用，而無需執行 Commit（提交）作業。

重新啟動後，停用 *SSL* 解密的命令不會保留在組態中。若您暫時關閉解密然後重新啟動防火牆，則無論問題是否已修正，皆會再次開啟解密。

停用 SSL 解密

```
set system setting ssl-decrypt skip-ssl-decrypt yes
```

重新啟用 SSL 解密

```
set system setting ssl-decrypt skip-ssl-decrypt no
```


©2024 Palo Alto Networks, Inc.

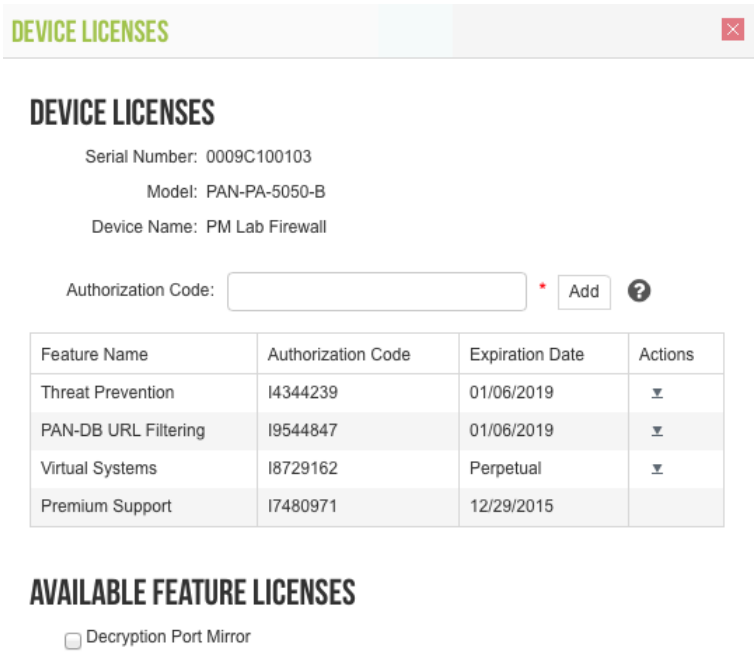
設定解密連接埠鏡像

您必須先取得並安裝解密連接埠鏡像授權，才能啟用解密鏡像。此授權免費，並可依照下列程序所述透過支援入口網站啟動。安裝解密連接埠鏡像授權並重新啟動防火牆後，您便可以啟用解密連接埠鏡像。

請記住，對 SSL 流量的解密、儲存、檢查和/或使用在某些國家/地區受到管制，必須經過使用者同意才能使用解密連接埠鏡像功能。此外，使用此功能會讓具有管理權限的惡意使用者存取防火牆，以收集使用者名稱、密碼、身分證字號、信用卡號或其他使用加密通道提交的機密資料。Palo Alto Networks 建議您在生產環境中啟動與使用此功能前，先向公司顧問諮詢。

STEP 1 | 為每個您想要啟用解密連接埠鏡像的防火牆要求授權。

1. 登入 Palo Alto Networks 客戶支援網站，導覽至 **Assets**（資產）頁籤。
2. 選取代表您想要授權的防火牆項目，然後選取 **Actions**（動作）。
3. 選取 **Decryption Port Mirror**（設定解密連接埠鏡像）。隨即顯示法律聲明。
4. 如果您已經明瞭可能的法律後果與需求，並仍想要設定解密連接埠鏡像，請按一下 **I understand and wish to proceed**（我瞭解並願意繼續）。
5. 按一下 **Activate**（啟動）。



 ©2024 Palo Alto Networks, Inc.

STEP 2 | 在防火牆上安裝解密連接埠鏡像授權。

1. 從防火牆 Web 介面中，選取 **Device**（裝置） > **Licenses**（授權）。
2. 按一下 **Retrieve license keys from license server**（從授權伺服器擷取授權金鑰）。
3. 確認授權已在防火牆上啟動。

4. 重新啟動防火牆（**Device**（裝置） > **Setup**（設定） > **Operations**（操作））。重新載入 PAN-OS 前，無法將此功能用於組態。

STEP 3 | 為轉送的解密流量啟用防火牆。必須有超級使用者權限才能執行此步驟。

在含單一虛擬系統的防火牆上：

1. 選取 **Device**（裝置） > **Setup**（設定） > **Content - ID**（內容-ID）。
2. 選取 **Allow forwarding of decrypted content**（允許轉送解密的內容核取方塊）。
3. 按一下 **OK**（確定）儲存。

在含多個虛擬系統的防火牆上：

1. 選取 **Device**（裝置） > **Virtual System**（虛擬系統）。
2. 選取要編輯的虛擬系統，或選取 **Add**（新增）建立新的虛擬系統。
3. 選取 **Allow forwarding of decrypted content**（允許轉送解密的內容核取方塊）。
4. 按一下 **OK**（確定）儲存。

STEP 4 | 啟用要用於解密鏡像的乙太網路介面。

1. 選取 **Network**（網路） > **Interfaces**（界面） > **Ethernet**（乙太網路）。（網路 > 介面 > 乙太網路）
2. 選取您要設定解密連接埠鏡像的乙太網路介面。
3. 選取 **Decrypt Mirror**（解密鏡像）作為 **Interface Type**（介面類型）。

   此介面只有在已安裝解密連接埠鏡像授權時才會出現。
4. 按一下 **OK**（確定）儲存。

©2024 Palo Alto Networks, Inc.

STEP 5 | 啟用解密流量的鏡像。

1. 選取 **Objects**（物件） > **Decryption Profile**（解密設定檔）。
2. 啟用要用於 **Decryption Mirroring**（解密鏡像）的 **Interface**（介面）。

   Interface（介面）下拉式清單中包含所有已定義為以下類型的 Ethernet 介面：**Decrypt Mirror**（解密鏡像）。
3. 指定要在原則執行前或後將加密的流量鏡像。

   依預設，防火牆會在查閱安全性原則前將所有解密的流量鏡像到介面，讓您能夠重播事件並分析會產生威脅或觸發丟棄動作的流量。如果您只想要鏡像安全性原則執行後的解密流量，請選取 **Forwarded Only**（僅限轉送）核取方塊。透過此選項，便能僅鏡像透過防火牆轉送的流量。如果您正將解密的流量轉送至其他威脅偵測裝置，例如 DLP 裝置或其他入侵防禦系統 (IPS)，此選項十分有幫助。
4. 按一下 **OK**（確定）來儲存解密設定檔。

STEP 6 | 附加解密設定檔規則 (包含啟用解密連接埠鏡像) 到解密原則規則。根據鏡像的原則規則解密所有流量。

1. 請參閱 **Policies**（原則） > **Decryption**（解密）。（原則 > 解密）
2. 按一下 **Add**（新增）設定解密原則，或選取現有的解密原則進行編輯。
3. 在 **Options**（選項）頁籤中，選取 **Decrypt**（解密），再選取在步驟 4 中建立的 **Decryption Profile**（解密設定檔）。
4. 按一下 **OK**（確定）儲存原則。

STEP 7 | 儲存組態。

按一下 **Commit**（交付）。

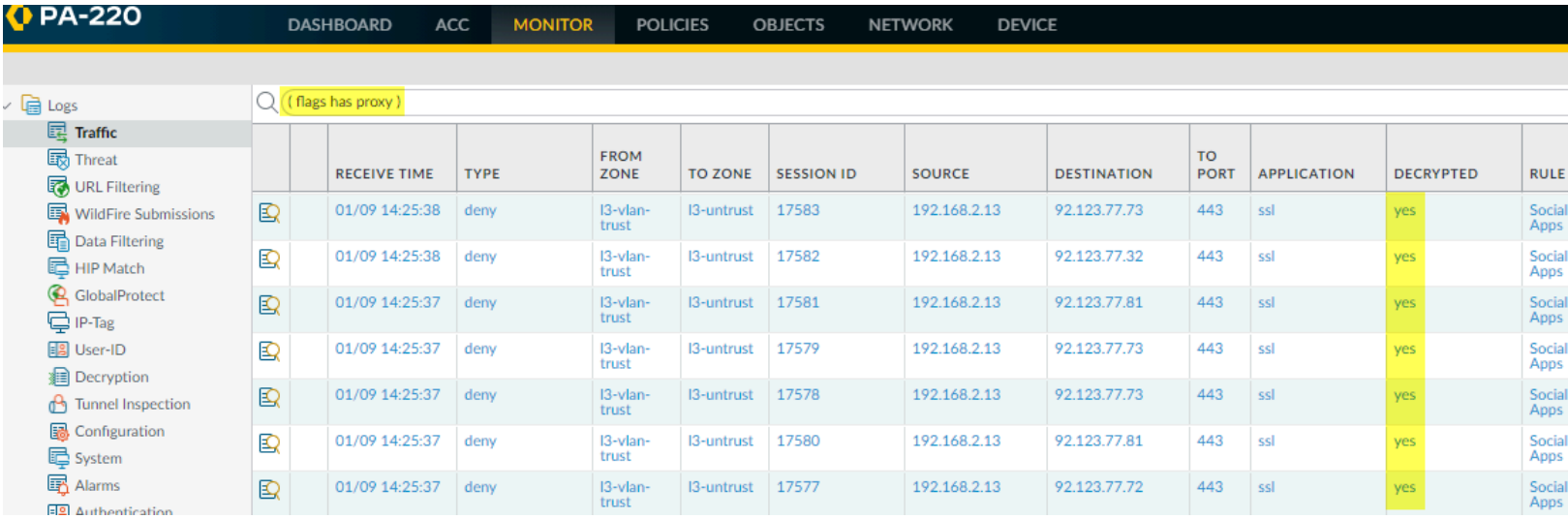
©2024 Palo Alto Networks, Inc.

確認解密

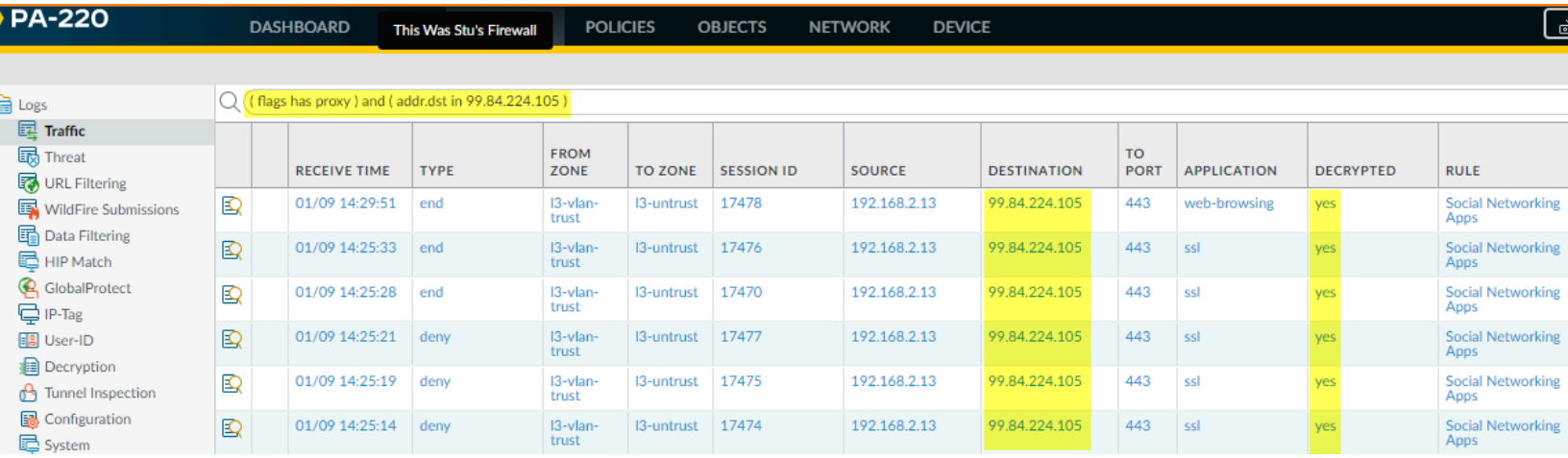
設定最佳做法解密設定檔並將其套用於流量後，您可以檢查解密日誌（PAN-OS 10.0 中引入）和流量日誌，以確認防火牆會解密您意圖解密的流量，以及防火牆不會解密您不想解密的流量。此主題顯示如何使用流量日誌檢查解密。此外，遵循後置部署解密最佳做法來維護部署。

檢視解密流量工作階段—使用篩選器 **(flags has proxy)** 篩選流量日誌（**Monitor**（監控） > **Logs**（日誌） > **Traffic**（流量））。

此篩選器僅顯示 SSL Proxy 旗標開啟的日誌，意味著只有解密流量 - 每個日誌項目在 **Decrypted**（解密）欄中的值為 yes（是）。



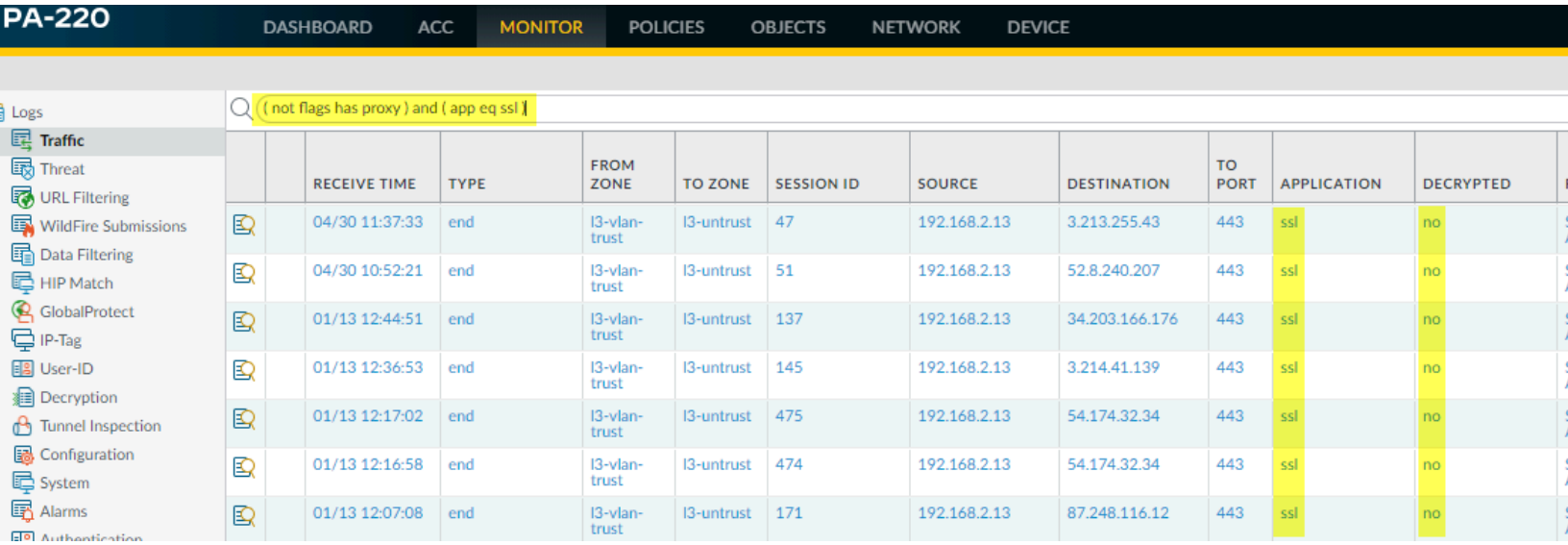
若要更細微地篩選流量，您可新增更多術語至篩選器。例如，您可透過新增篩選器 **(addr.dst in 99.84.224.105)** 來篩選僅流向目的地 IP 位址 99.84.224.105 的解密流量：



©2024 Palo Alto Networks, Inc.

檢視未解密的 **SSL** 流量工作階段—使用篩選器 **(not flags has proxy)** 與 **(app eq ssl)** 來篩選流量日誌（**Monitor**（監控） > **Logs**（日誌） > **Traffic**（流量））。

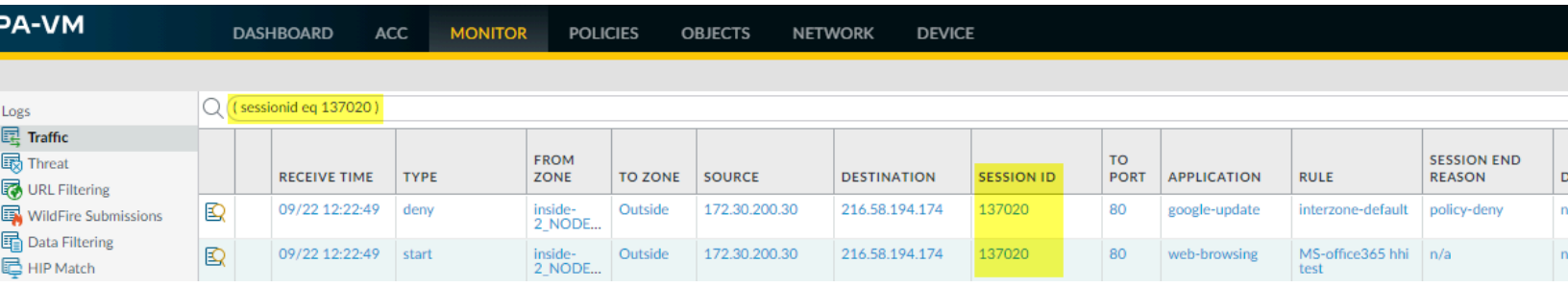
此篩選器僅顯示 SSL Proxy 旗標關閉的日誌（意味著只有加密流量），並且流量為 SSL 流量；每個日誌項目在 **Decrypted**（解密）欄中的值為 **no**（否），在 **Application**（應用程式）欄中的值為 **ssl**。



與檢視解密流量日誌的範例類似，您可新增術語來篩選未以更細微的方式進行解密的流量。

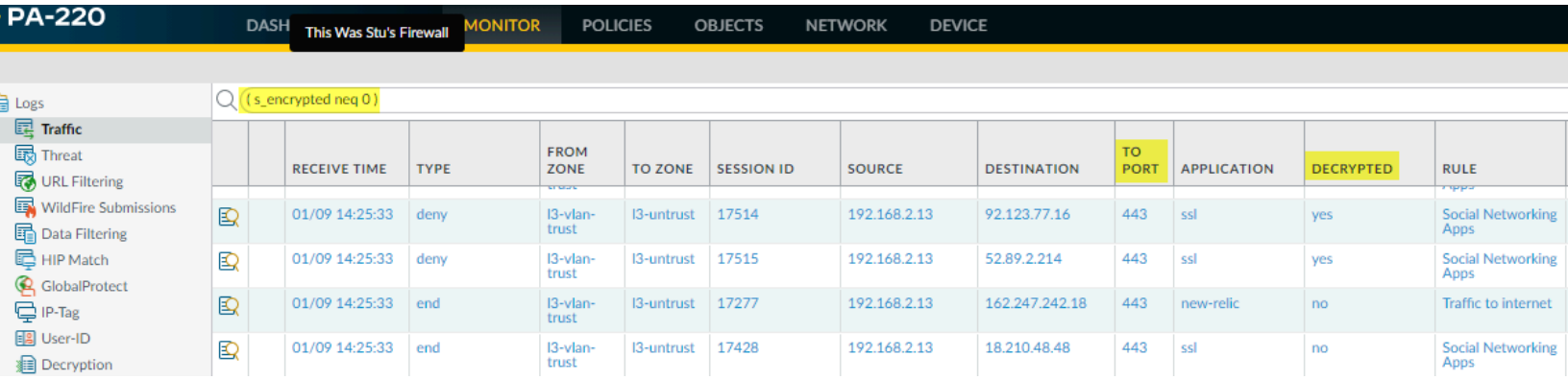
檢視特定工作階段的日誌—若要檢視特定工作階段的流量日誌，請依據 Session ID（工作階段 ID）來篩選。

例如，若要查看 ID 為 137020 之工作階段的日誌，請使用術語 **(sessionid eq 137020)** 進行篩選。您可以在日誌輸出的 Session ID（工作階段 ID）欄中找到 ID 號碼，如上一畫面所示。若未顯示 Session ID（工作階段 ID）欄，則新增該欄至輸出。



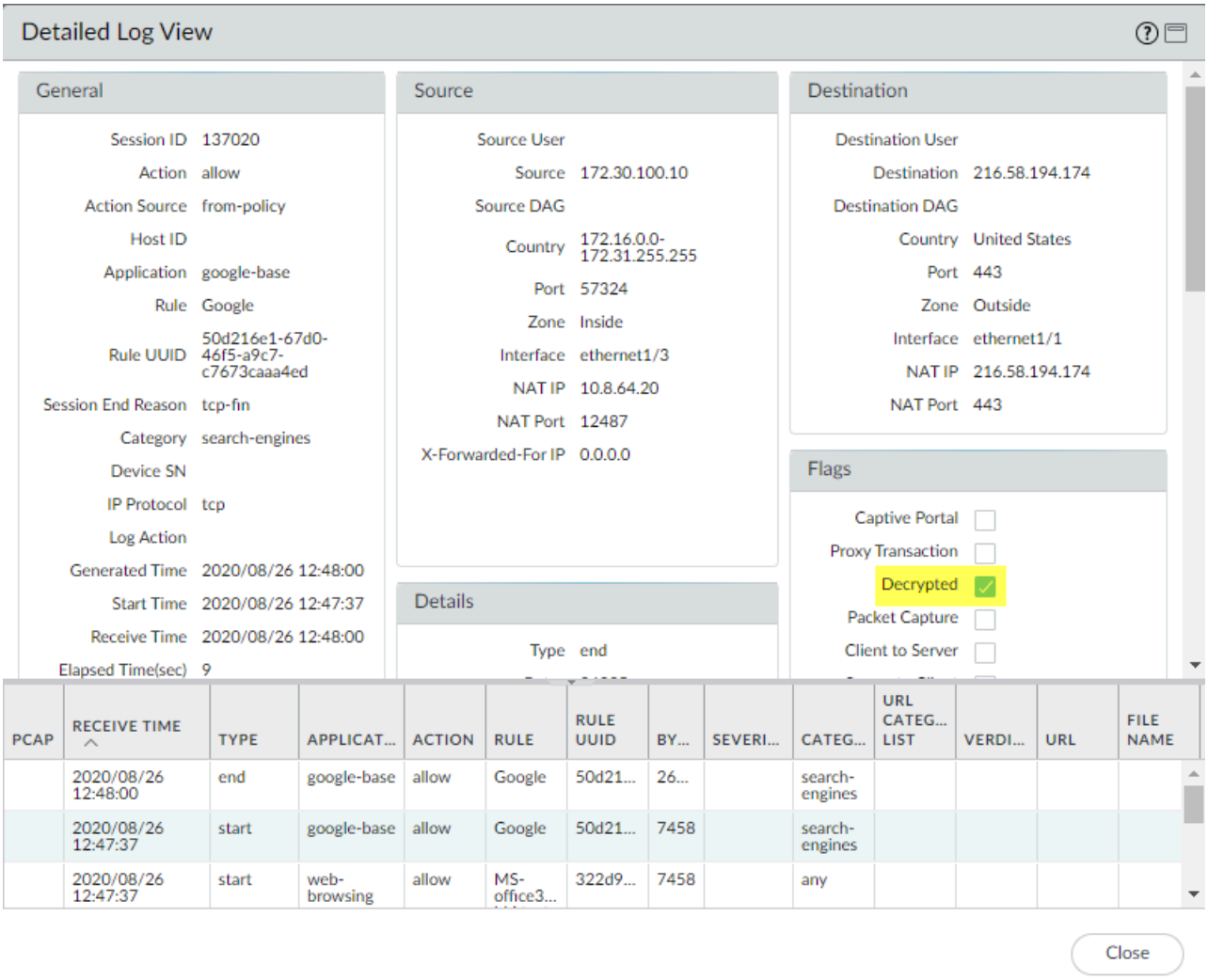
 ©2024 Palo Alto Networks, Inc.

檢視所有 **TLS** 和 **SSH** 流量—使用篩選器 **(s_encrypted neq 0)** 篩選流量日誌（**Monitor**（監控） > **Logs**（日誌） > **Traffic**（流量））以檢視已解密和未解密的 TLS 和 SSH 流量：



 ©2024 Palo Alto Networks, Inc.

深入查看詳細資料—若要檢視有關特定日誌項目的更多資訊，請按一下放大鏡查看詳細的日誌視圖。例如，對於 Session ID（工作階段 ID）137020（顯示在上一個項目符號中），詳細日誌如下所示：



還可以使用 **Decrypted**（解密）旗標的方塊來確認流量是否已解密。

您還可以擷取解密流量的上游與下游封包畫面，以檢視防火牆如何處理 SSL 流量以及對封包執行動作，或執行深層封包檢查。

©2024 Palo Alto Networks, Inc.

疑難排解和監控解密

疑難排解工具提供了增強的 TLS 流量可視性，以便您可以監控解密部署。使用這些工具，您可以快速且輕鬆地診斷和解決解密問題，強化解密部署中的薄弱環節，並修復解密問題以改善安全狀態。例如，您可以：

- 透過服務名稱標識 (SNI)和應用程式識別導致解密失敗的流量。
- 識別使用弱通訊協定和演算法的流量。
- 檢查網路中的成功和不成功解密活動。
- 檢視有關單個工作階段的詳細資訊。
- 設定檔解密使用方式和模式。
- 監控詳細的解密統計資料以及有關採用、失敗、版本、演算法等的資訊。

以下工具讓您能夠全面洞悉 TLS 交握，並幫助您疑難排解和監控解密部署：

- **ACC** > **SSL Activity**（**ACC SSL** 活動）—此頁簽上的五個 ACC Widget（在 PAN-OS 10.0 中引入）提供了有關網路中成功和不成功解密活動的詳細資料，包括解密失敗、TLS 版本、金鑰交換以及解密和未解密流量的數量與類型。
- **Monitor**（監控） > **Logs**（日誌） > **Decryption**（解密）—解密日誌（在 PAN OS 10.0 中引入）提供了有關與解密政策相符的個別工作階段（對不解密的流量使用「不解密」政策）和當您在 GlobalProtect 入口網站或 GlobalProtect 閘道設定中啟用解密記錄時有關 GlobalProtect 工作階段的全方位資訊。選取要顯示的欄，以檢視以下資訊：應用程式、SNI、解密原則名稱、錯誤索引、TLS 版本、金鑰交換版本、加密演算法、憑證金鑰類型以及許多其他特性。篩選欄中的資訊以識別使用特定 TLS 版本和演算法、具有特定錯誤或您要調查的任何其他特性的流量。依預設，解密原則僅記錄不成功的 TLS 交握。如果您有可用的日誌儲存空間，請設定解密政策以記錄成功的 TLS 交握，以及取得對這些解密工作階段的可見度。
- 本機解密排除快取—有兩種網站構造會由於技術原因（如用戶端驗證或釘選憑證）而中斷解密，因此需要從解密中排除：SSL 解密排除清單和本機解密排除快取。SSL 解密排除清單包含 Palo Alto Networks 識別為技術性中斷解密的伺服器。內容更新使清單保持最新，您可以手動將伺服器新增到該清單中。在套用至流量的解密設定檔允許不受支援模式的情況下，本機解密排除快取會自動新增本機使用者遇到的由於技術原因而中斷解密的伺服器，並將其從解密中排除（如果封鎖不受支援的模式，則會封鎖流量而不是將其新增至本機快取中）。
- 解密的自訂報告範本—您可以使用四個總結解密活動的預先定義範本建立自訂報告（**Monitor**（監控） > **Manage Custom Reports**（管理自訂報告））（PAN-OS 10.0 中引入）。

一般的疑難排解方法是從 ACC 小工具開始，以識別造成解密問題的流量。接下來，使用解密日誌和自訂報告範本深入查看詳細資訊並獲得有關該流量的上下文。這讓您能夠準確且比以往更輕鬆地診斷問題。瞭解解密問題及其原因讓您能夠選取適當的方法來修復每個問題，例如：

- 修改解密政策規則（政策規則定義該規則影響的流量、對該流量執行的動作、日誌設定以及套用至該流量的解密設定檔）。

©2024 Palo Alto Networks, Inc.

- 修改解密設定檔（解密政策規則所控制流量的可接受通訊協定和演算法，以及失敗檢查、項目的不受支援模式檢查（如不受支援的密碼和版本）、憑證檢查等）
- 將由於技術原因中斷解密的網站新增至 SSL 解密排除清單。
- 評估有關您的員工、客戶和合作夥伴真正需要存取哪些網站以及當網站使用弱解密通訊協定或演算法時可以封鎖哪些網站的安全性決策。

目標是解密所有可以解密的流量（解密最佳做法）以便您可以對其進行檢查，同時正確處理未解密的流量。

在 PAN-OS 10.0 或更高版本中，裝置將佔用 1# 的日誌空間並將其指派給解密日誌。設定解密記錄中的第 3 步向您顯示如何修改日誌空間配置，為解密日誌提供更多空間。

如果從 PAN-OS 10.0 或更高版本降級到 PAN-OS 9.1 或更低版本，PAN-OS 10.0 中引入的功能（解密日誌、ACC 中的「SSL 活動」Widget、自訂報告解密範本）將從 UI 中移除。解密日誌的參考也將從日誌轉送設定檔中移除。此外，只能在 PAN-OS 9.1 和更低版本中使用 CLI 來檢視「本機解密排除快取」（PAN-OS 10.0 將本機快取新增到 UI 中）。

如果將設定從執行 PAN-OS 10.0 或更高版本的 Panorama 推送到執行 PAN-OS 9.1 或更低版本的裝置，則 Panorama 會移除 PAN-OS 10.0 中引入的功能。

- 解密應用程式控管中心 (ACC) Widget
- 解密日誌
- 解密的自訂報告範本
- 解密疑難排解工作流程範例

解密應用程式控管中心 (ACC) Widget

PAN-OS 11.0 中引入了用於解密的應用程式控管中心 (ACC) 小工具（**ACC** > **SSL Activity**（**SSL** 活動）），搭配 解密日誌，可幫助您快速輕鬆地診斷和解決解密問題。使用 **SSL** 活動 Widget 檢視和分析網路解密活動，如已解密和未解密的工作階段數、有多少流量使用不同的 TLS 通訊協定版本、最常見的解密失敗原因，以及哪些應用程式和伺服器名稱識別 (SNI) 使用弱密碼和演算法。接下來，使用解密日誌向下鑽研工作階段並診斷確切問題，以便您能夠採取適當的動作。

PAN-OS 11.0 引入了五個新解密小工具。使用 Widget 提供的資訊來識別設定錯誤的解密原則和設定檔，並對要允許和封鎖哪些流量做出明智的決定：

- 流量活動—按工作階段總數或流量位元組數顯示 SSL/TLS 活動與非 SSL/TLS 活動之比。
- **SSL/TLS** 流量—按工作階段數或流量位元組數顯示已解密和未解密的流量數量。不解密流量的原因包括：
  - 對流量套用了不解密原則。
  - 解密原則有意免除解密流量（如，不解密原則）。
  - 解密原則設定錯誤，本打算解密的流量實際沒有解密。
  - 網站在 SSL Decryption Exclusion List（SSL 解密排除清單）（**Device**（裝置）> **Certificate Management**（憑證管理）> **SSL Decryption Exclusion**（**SSL** 解密排除））中，該清單包含

 ©2024 Palo Alto Networks, Inc.

Palo Alto Networks 已確認由於釘選憑證或用戶端驗證等技術原因而中斷解密的網站。對於這些網站，防火牆會繞過解密。

- 網站在 Local Decryption Exclusion Cache（本機解密排除快取）中，其中包含本機使用者遇到的因技術原因阻止解密的網站。

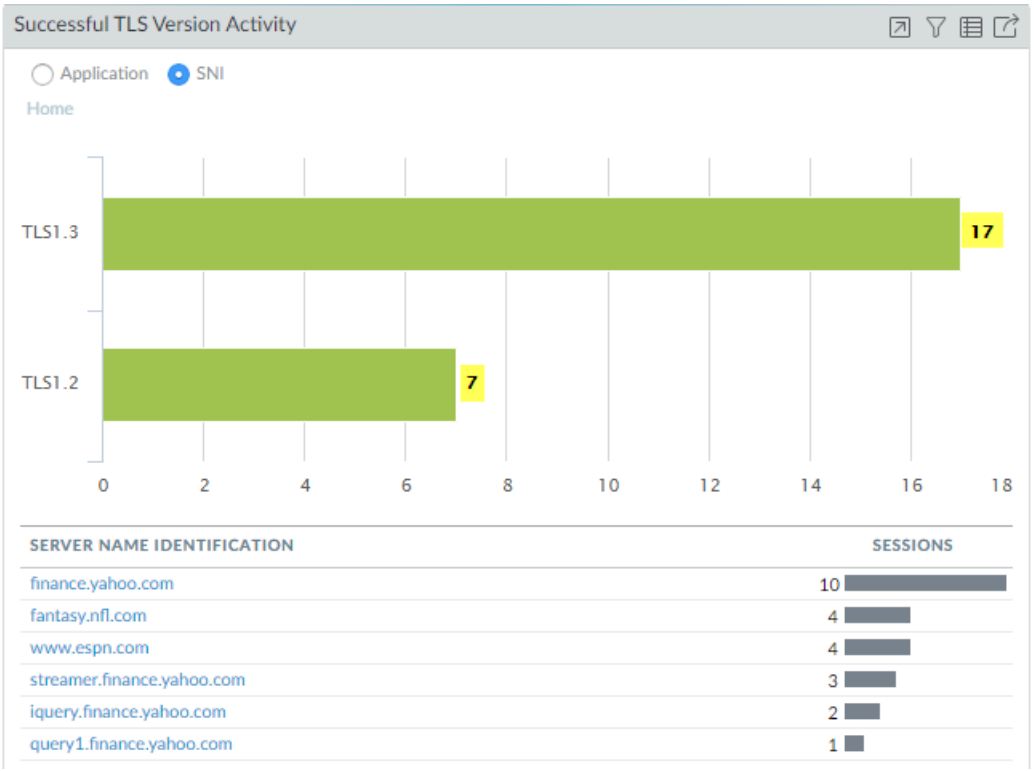
ACC 僅使用來自解密原則所控制流量的資料填入後面三個 Widget。如果您沒有套用解密原則到流量，該流量不會填入這些 Widget。

- 解密失敗原因—顯示解密失敗的原因：SNI 提出的通訊協定、憑證、版本、密碼、HSM、資源、繼續或功能問題。使用此資訊來偵測由解密原則或設定檔設定錯誤或者使用不受支援的弱通訊協定或演算法的流量引起的問題。按一下失敗原因以向下鑽研並隔離遇到失敗的每個 SNI 的工作階段數，或者按一下 SNI 以檢視該 SNI 的所有解密失敗。
- 成功 **TLS** 版本活動—按應用程式或 SNI 的 TLS 版本顯示成功的 TLS 連線（SNI 僅可用於正向 Proxy），這樣您可以透過允許使用較弱的 TLS 通訊協定版本來評估承受的風險。識別使用弱通訊協定的應用程式和 SNI 讓您能夠評估每個應用程式和 SNI，並確定是否需要出於業務原因允許對其進行存取。如果您不需要出於業務目的使用該應用程式，則可以封鎖流量（而不是允許），以便降低風險。按一下 TLS 版本以向下鑽研並檢視使用該 TLS 版本的 SNI 或應用程式。按一下一個應用程式或 SNI 以向下鑽研，並查看有多少個此類應用程式或 SNI 工作階段使用了每個 TLS 版本。
- 成功金鑰交換活動—顯示應用程式或 SNI 的每個演算法的成功金鑰交換活動（SNI 僅可用於正向 Proxy）。按一下金鑰交換演算法以僅查看該演算法的活動，或者按一下應用程式或 SNI 以檢視該應用程式或 SNI 的金鑰交換演算法活動。

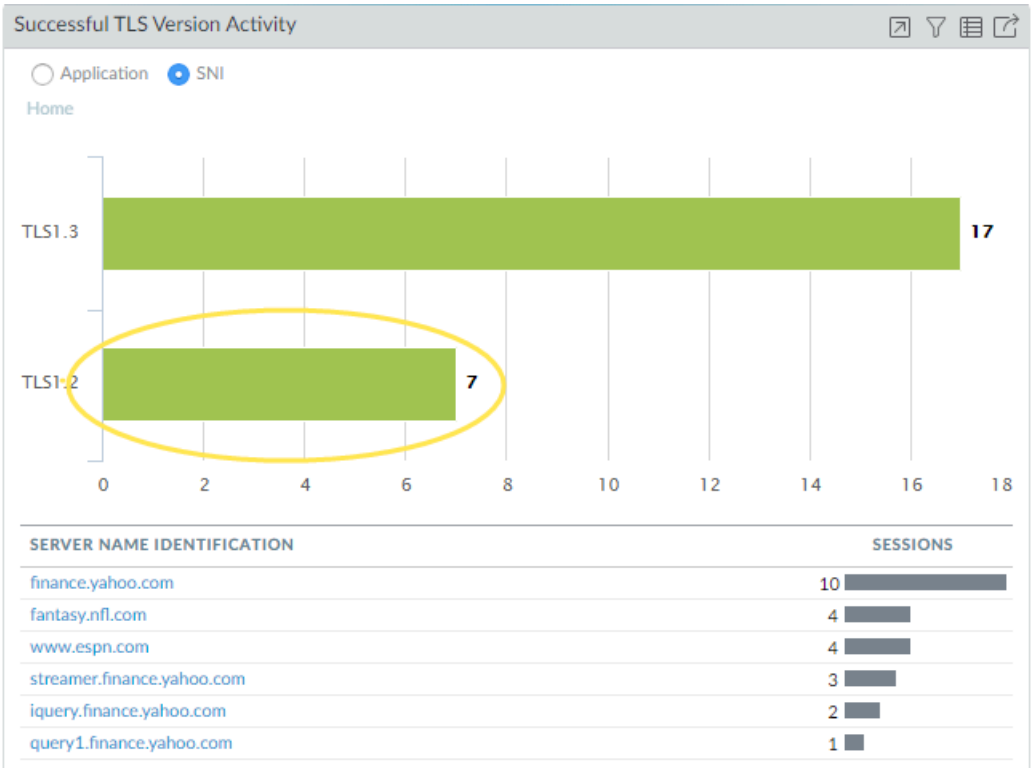
以下向下鑽研 ACC 資料的範例顯示了如何檢查成功的 TLS 版本活動：

©2024 Palo Alto Networks, Inc.

1. 成功 **TLS** 版本活動 Widget 顯示，十七個工作階段使用了 TLSv1.3，七個工作階段使用了 TLSv1.2。SNI 清單顯示目的地 SNI 和每個 SNI 的工作階段數。

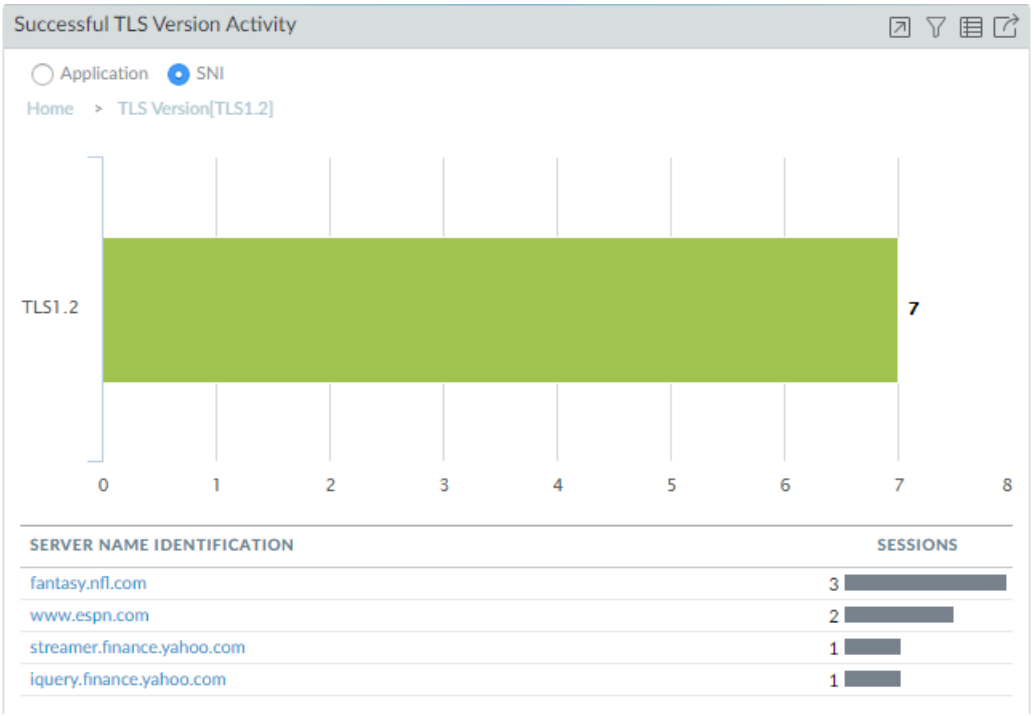


2. 要查看哪些 SNI 使用了 TLSv1.2，按一下標有 TLS1.2 的綠色列。

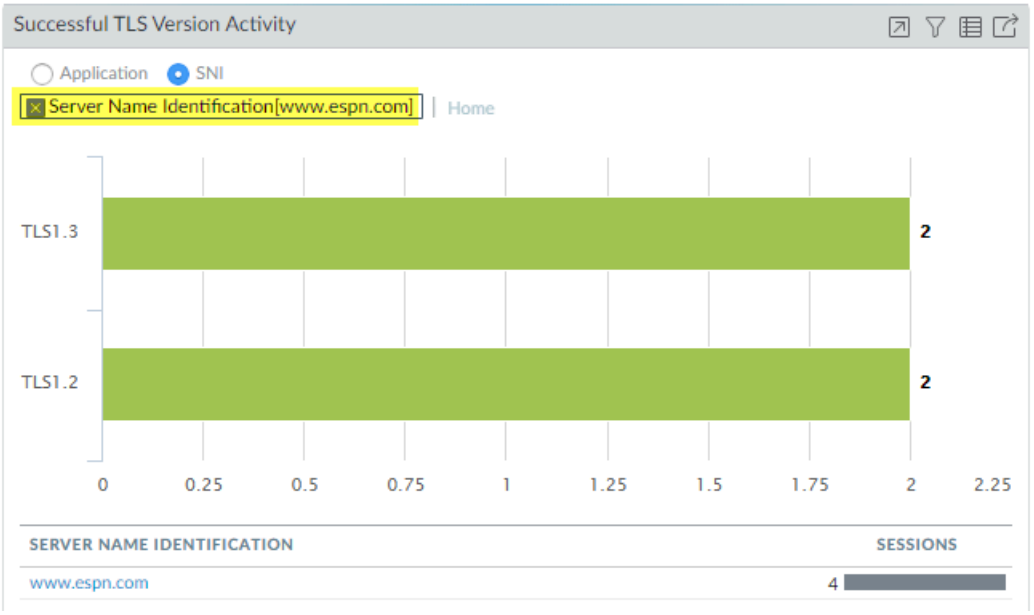


 ©2024 Palo Alto Networks, Inc.

3. 現在您可以看到七個 TLSv1.2 工作階段分佈在四個伺服器中。



4. 按一下 **Home**（首頁）返回主畫面。現在，按一下 www.espn.com，SNI 顯示其使用了哪些 TLS 版本。我們可以看到，在四個工作階段中，有兩個使用 TLSv1.3，另外兩個使用 TLSv1.2。



對於任何解密 Widget，按一下「跳至日誌」圖示，直接跳到對應於 ACC 中資料的解密日誌：

在前面的範例中，在調查過程的任何時候，您都可以跳至資料的解密日誌，以向下鑽研更多資訊。例如，您可以檢查使用 TLSv1.2 的各個工作階段的日誌，找出它們不使用 TLSv1.3 的原因。

©2024 Palo Alto Networks, Inc.

解密 ACC Widget 基於 Palo Alto Networks App-ID 顯示已解密應用程式的名稱。要填入 ACC，防火牆只能識別具有 Palo Alto Networks App-ID 的應用程式；防火牆無法使用自訂應用程式或沒有 App-ID 的應用程式填入 ACC。內容更新定期更新 App-ID。應用程式可能顯示為不完整或未知的其他原因包括：

- 防火牆在識別應用程式前丟棄了工作階段。
- 解密日誌依賴流量日誌來填入解密日誌應用程式欄位。但是，如果流量日誌未在 60 秒或更短時間內完成，則流量日誌不會在解密日誌中填入應用程式，且該應用程式顯示為不完整或未知。

解密日誌

解密日誌（**Monitor**（監控） > **Logs**（日誌） > **Decryption**（解密））提供了符合解密政策的工作階段的全方位資訊，幫助您獲取有關該流量的背景，以便您可以準確、輕鬆地診斷和解決解密問題。如果流量不符合解密原則，則防火牆不會記錄該流量。如果要記錄沒有解密的流量，需建立基於原則的解密排除，對於控管 TLSv1.2 和更早版本流量的原則，套用無解密設定檔至流量。

PAN-OS 對以下類型的流量支援解密日誌：

- 正向 Proxy—幾個欄位僅顯示有關正向 Proxy 流量的資訊，包括根 CA（僅適用於受信任的憑證）和伺服器名稱識別 (SNI)。
- 輸入檢查。
- 不解密（解密原則排除解密的流量）。

  由於工作階段保持加密，防火牆顯示較少的資訊。*TLSv1.3* 會加密憑證資訊，因此未解密的 *TLSv1.3* 流量沒有憑證資訊。
- GlobalProtect—覆蓋 GlobalProtect 閘道、GlobalProtect 入口網站和 GlobalProtect 無用戶端 VPN（僅用戶端到防火牆）。

  GlobalProtect 不支援 *TLSv1.3*。
- 解密鏡像

並非所有類型的流量都支援每個參數。Proxy 類型和 TLS 版本不支援的參數 提供了每種解密流量類型不支援的參數的完整清單。

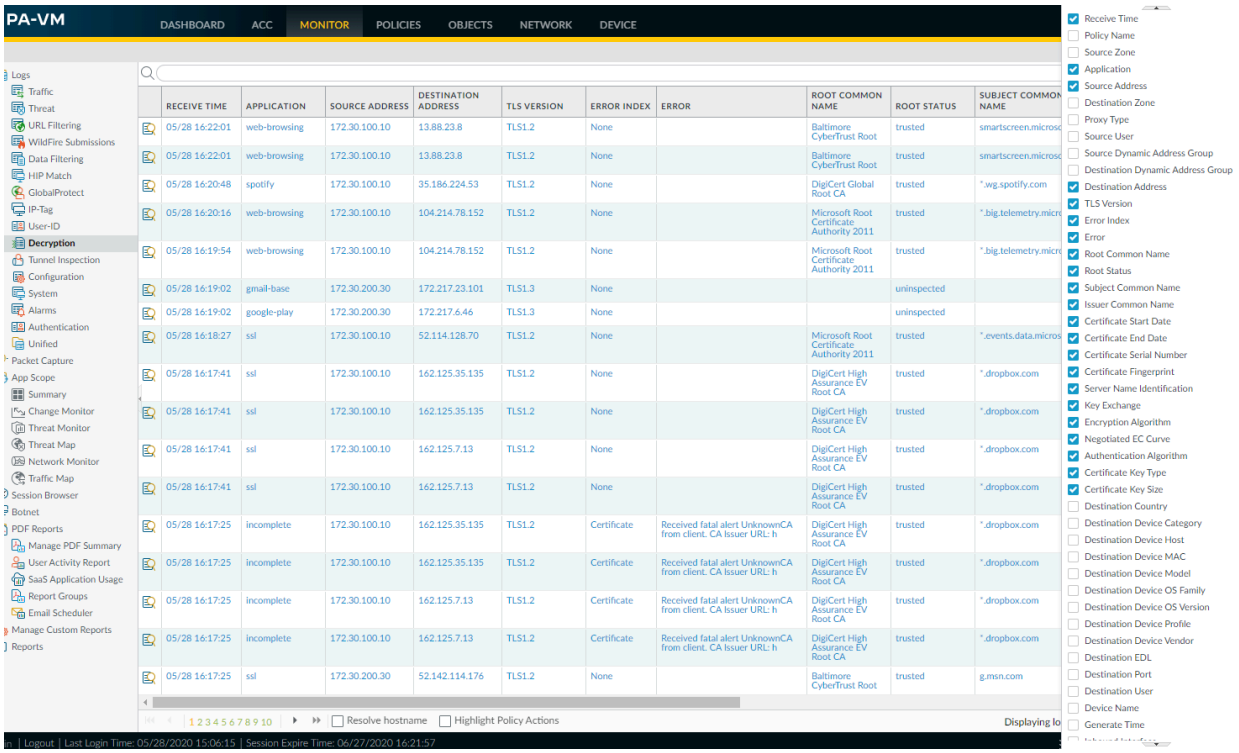
正向 Proxy 流量的資料基於 TLS 交握是成功還是不成功。對於不成功的 TLS 交握，防火牆會傳送導致錯誤的交易支柱的錯誤資料，可以是從用戶端到防火牆，也可以是從防火牆到伺服器。對於成功的 TLS 交握，資料來自首先成功完成的支柱，通常是用戶端到防火牆。

防火牆不會針對 SSL/TLS 交握期間封鎖的 *Web* 流量產生解密日誌項目。這些工作階段不會出現在解密日誌中，因為防火牆會在重設 *SSL/TLS* 連線時阻止解密，結束交握。您可以在 *URL* 篩選日誌中檢視被封鎖工作階段的詳細資料。

SSH Proxy 流量不支援解密日誌。此外，憑證資訊不可用於工作階段繼續日誌。

©2024 Palo Alto Networks, Inc.

依預設，防火牆記錄所有不成功的 TLS 交握流量。您也可以選擇記錄成功的 TLS 交握流量。您可檢視最多 62 欄日誌資訊，例如，應用程式、SNI、解密原則名稱、錯誤索引、TLS 版本、金鑰交換版本、加密演算法、憑證金鑰類型以及許多其他特性：



按一下放大鏡圖示 ( ) 以查看工作階段的詳細日誌檢視。

解密日誌會從流量日誌中瞭解到每個工作階段的 *App-ID*，因此必須啟用流量日誌才能在解密日誌中查看 *App-ID*。如果流量日誌停用，*App-ID* 會顯示為 ***incomplete***（不完整）。例如，許多 *GlobalProtect* 流量是內部網路區流量（從不受信任的區域到不受信任的區域），但是預設的內部網路區原則不會啟用流量日誌。要查看 *GlobalProtect* 內部網路區流量的 *App-ID*，您需要為內部網路區流量啟用流量日誌。

App-ID 可能顯示為 ***incomplete***（不完整）的另一個原因是，對於長工作階段，防火牆可能會在流量日誌完成之前產生解密日誌（流量日誌通常在工作階段結束時產生）。在這種情況下，*App-ID* 對解密日誌不可用。此外，當 *TLS* 交握失敗並產生錯誤日誌時，*App-ID* 不可用，因為失敗會在防火牆確定 *App-ID* 之前終止工作階段。在這種情況下，應用程式可能顯示為 ***ssl*** 或 ***incomplete***（不完整）。

要解決問題，請使用解密 ACC 小工具（**ACC** > **SSL Activity**（**SSL** 活動））來識別引起解密問題的流量，然後使用解密日誌和 解密的自訂報告範本 向下鑽研詳細資料。

在轉送解密日誌以供儲存時，請確保適當保護日誌傳輸和儲存，因為解密日誌包含敏感資訊。

啟用解密日誌後，防火牆會將 *HTTP/2* 日誌作為通道檢查日誌傳送（停用解密日誌後，*HTTP/2* 日誌將作為流量日誌傳送），因此您需要查看通道檢查日誌而不是流量日誌來瞭解 *HTTP/2* 事件。此外，您必須啟用通道內容檢查來獲取 *HTTP/2* 流量的 *App-ID*。

©2024 Palo Alto Networks, Inc.

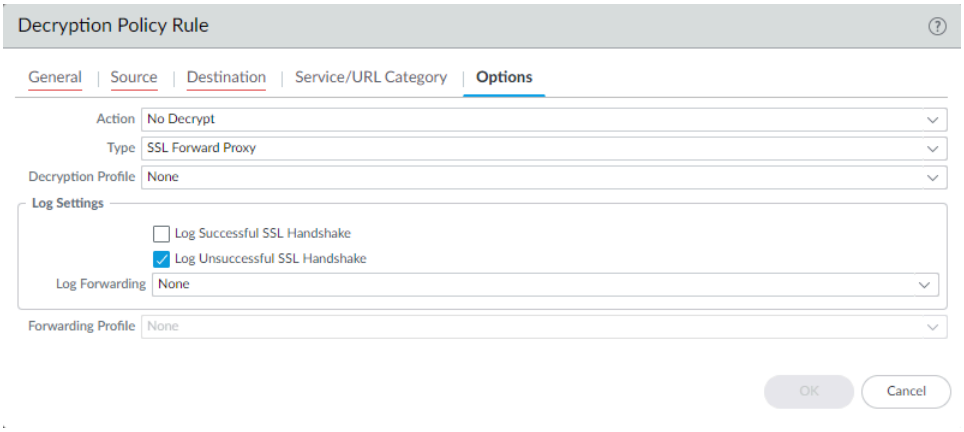
- 設定解密記錄
- 修復不完整的憑證鏈結
- 加密日誌錯誤、錯誤索引和位元遮罩

設定解密記錄

防火牆為解密原則控管的工作階段產生解密日誌，包括具有「不解密」原則的工作階段。在控制您想要記錄的流量的解密原則中設定解密記錄。

STEP 1 | 在解密原則中設定您想要記錄的解密流量（**Policies**（原則） > **Decryption**（解密））。

依預設，防火牆僅記錄不成功的 TLS 交握：

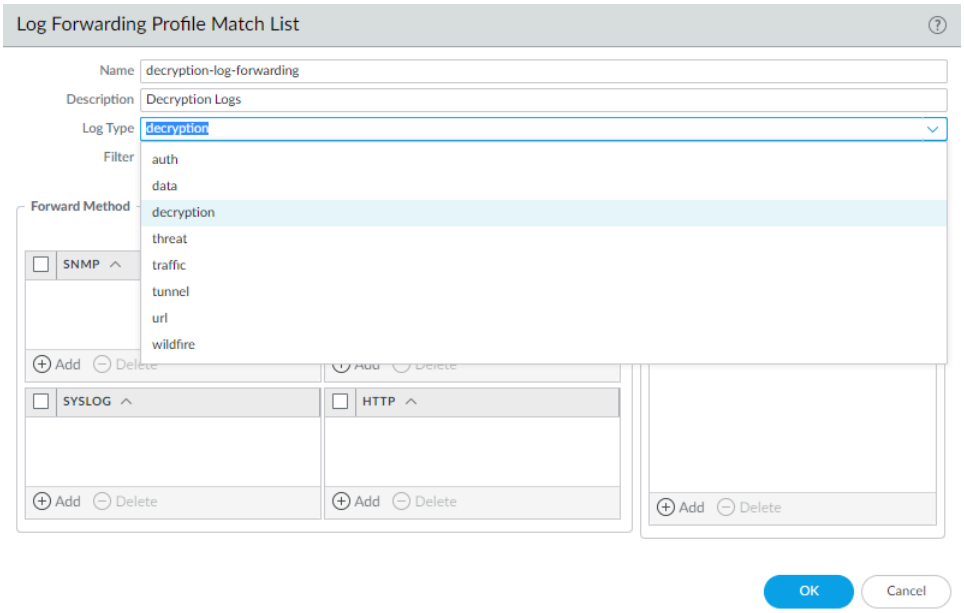


記錄成功的交握和不成功的交握，以在裝置可用資源允許的範圍內，洞悉盡可能多的解密流量（不解密私人或敏感流量；遵循解密最佳做法並解密盡可能多的流量）。

©2024 Palo Alto Networks, Inc.

STEP 2 | 建立日誌轉送設定檔以將解密日誌轉送到日誌收集器、其他儲存裝置或指定管理員，然後在解密原則選項頁簽的 **Log Forwarding**（日誌轉送）欄位中指定該設定檔。

要轉送解密日誌，您必須設定日誌轉送設定檔（**Objects**（物件） > **Log Forwarding**（日誌轉送））以指定解密日誌類型和轉送日誌的方法。

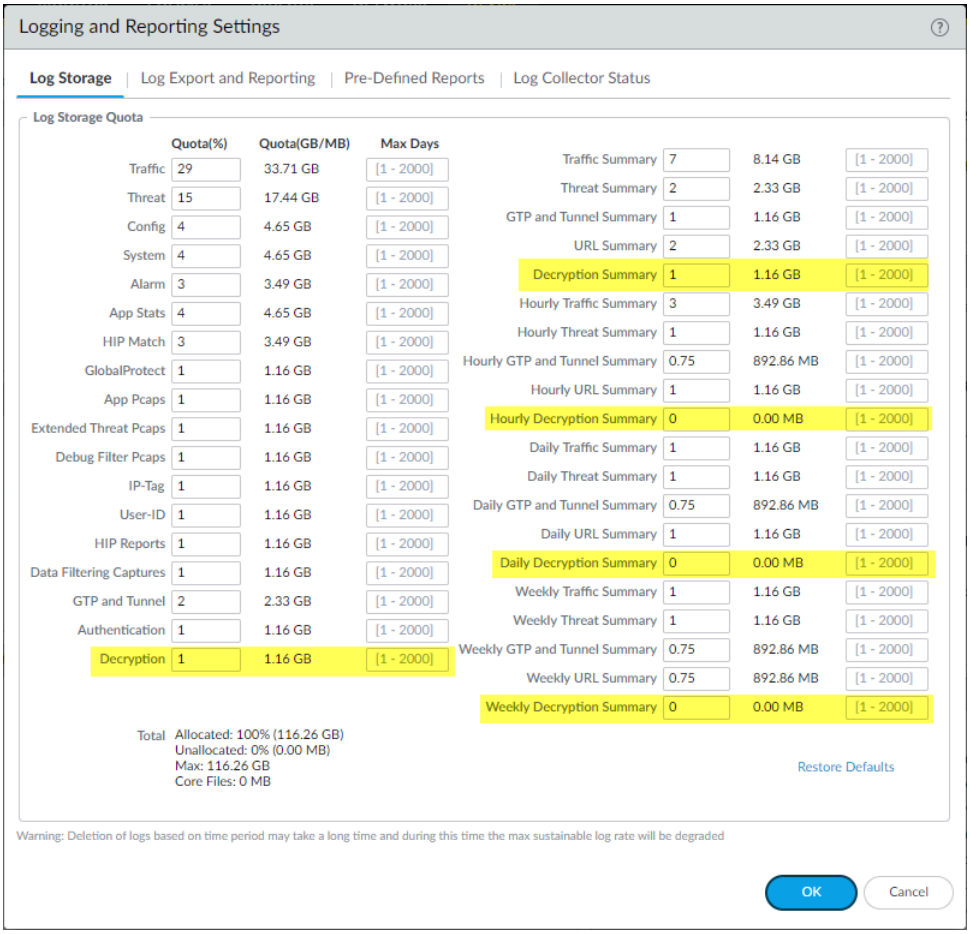


如果您轉送解密日誌，確保安全儲存日誌，因為它們包含敏感資訊。

©2024 Palo Alto Networks, Inc.

STEP 3 | 如果您在記錄不成功的 TLS 交握之外，還記錄成功的 TLS 交握，請為防火牆上的解密日誌設定較大的日誌儲存空間配額（**Device**（裝置）> **Setup**（設定）> **Management**（管理）> **Logging and Reporting Settings**（記錄和報告設定）> **Log Storage**（日誌儲存））。

預設配額（配置）是裝置日誌存儲容量的百分之一用於解密日誌，百分之一用於一般解密摘要。沒有預設配置用於每小時、每天或每週解密摘要。



確定解密日誌所需儲存空間的因素有很多，具體取決於您的部署。例如，考慮以下因素：

- 通過防火牆的 TLS 流量數量。
- 您解密的 TLS 流量數量。
- 您對其他日誌的使用情況（評估應從哪些日誌中分配容量以配置給解密日誌）。
- 如果您同時記錄成功和不成功 TLS 交握，那麼與僅記錄不成功 TLS 交握相比，所需的容量要多很多。根據解密的流量數量，解密日誌可能會消耗與流量日誌或威脅日誌相同的容量，且如果裝置的容量已被完全訂閱，則可能需要在它們之間進行權衡。

日誌配額的總組合配置不能超過可用防火牆日誌資源的 *100#*。

您可能需要進行試驗，來為特定部署中的每個日誌類別找到正確的配額。如果僅記錄不成功的交握，則可以從預設值開始，或者將配置增加到百分之二或百分之三。如果同時記錄成功和不

©2024 Palo Alto Networks, Inc.

成功的交握，則可以先將配置給流量日誌的一半空間配置給解密日誌。要從哪些日誌分配空間來配置給解密日誌取決於您的流量、業務和監控要求。

加密日誌錯誤、錯誤索引和位元遮罩

解密日誌中的 **Error Index**（錯誤索引）和 **Error**（錯誤）欄分別提供有關解密錯誤類別和詳細資料的資訊。您還可以在詳細日誌檢視的「交握詳細資料」區段中查看錯誤和錯誤索引資訊（按一下 獲取任何日誌項目）。解密日誌 **Error Index**（錯誤索引）指示八個錯誤類別之一：

錯誤索引	錯誤（錯誤索引顯示可能的錯誤）
憑證	無效的憑證、過期的憑證、不受支援的用戶端憑證、OCSP/CRL 檢查撤銷和失敗、不受信任的簽發者 CA（由不受信任的根簽署的工作階段，其中包括不完整的憑證鏈結）以及其他憑證錯誤。 當防火牆由於網站未傳送完整的憑證鏈而沒有中繼憑證時，您可以找到缺失的憑證並將其安裝到 修復不完整的憑證鏈結。
密碼	不受支援的密碼錯誤，其中： • 用戶端嘗試交涉防火牆支援但套用至流量的解密設定檔不支援的密碼。 • 用戶端嘗試交涉防火牆不支援的密碼。 • （罕見）啟用了輸入檢查，且伺服器的功能與解密設定檔設定不符。 錯誤消息包括支援的用戶端密碼位元遮罩值和支援的解密設定檔密碼位元遮罩值。使用位元遮罩值來標識用戶端嘗試使用的密碼，並列出解密設定檔支援的密碼值，如本主題後面所述。
功能	過大 TLS 交握或未知交握、過大憑證鏈結（超過五個憑證）以及其他不受支援的功能等錯誤。
HSM	硬體儲存模組 (HSM) 錯誤，例如未知要求、設定中未找到的項目、要求逾時以及其他 HSM 錯誤和故障。
通訊協定	TLS 交握失敗、私有和公用金鑰不符、Heartbleed 錯誤、TLS 金鑰交換失敗以及其他 TLS 通訊協定錯誤之類的錯誤。當伺服器不支援用戶端支援的通訊協定、伺服器使用防火牆不支援的憑證類型以及出現一般 TLS 通訊協定錯誤時，會顯示通訊協定錯誤。
資源	記憶體不足之類的錯誤。
繼續	與繼續工作階段 ID 和票證、繼續防火牆快取中的工作階段項目以及其他工作階段繼續錯誤相關的工作階段繼續錯誤。
版本	有關用戶端和解密設定檔版本不符以及用戶端和伺服器版本不符的錯誤。

©2024 Palo Alto Networks, Inc.

錯誤索引	錯誤（錯誤索引顯示可能的錯誤）
	該錯誤訊息包括標識受支援用戶端和解密設定檔版本的位元遮罩值。使用位元遮罩值來標識用戶端嘗試使用的密碼，並列出解密設定檔支援的密碼值，如本主題後面所述。

如果一個錯誤沒有適當的錯誤描述類別，則預設訊息為 一般 ***TLS*** 通訊協定錯誤。

版本和密碼日誌錯誤資訊包括位元遮罩值，您可以使用操作性 CLI 命令將其轉換為實際值：

- 版本錯誤位元遮罩值標識用戶端和伺服器使用的 TLS 通訊協定版本之間的不符，還標識用戶端和套用至流量的解密設定檔之間的 TLS 通訊協定不符。用於轉換版本錯誤位元遮罩的 CLI 命令為：

  ```
  admin@vm1>debug dataplane show ssl-decrypt bitmask-version
   <bitmask-value>
  ```

  該命令返回與位元遮罩相符的 TLS 版本。
- 密碼錯誤位元遮罩值標識用戶端和套用至流量的解密設定檔之間的加密和其他不符。

  ```
  admin@vm1>debug dataplane show ssl-decrypt bitmask-cipher <bitmask-
  value>
  ```

  該命令返回與位元遮罩相符的密碼。

篩選解密日誌以查找版本和密碼錯誤，將具有錯誤的工作階段的位元遮罩值插入相應的 CLI 命令中，獲取導致錯誤的通訊協定版本或密碼的值。如果您想要允許存取相關網站，則使用該資訊更新解密原則或設定檔。

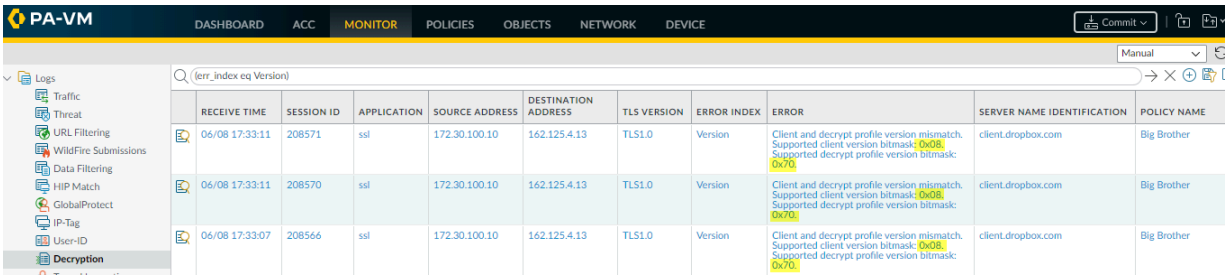
- 版本錯誤
- 密碼錯誤
- 根狀態「未受檢查」

版本錯誤

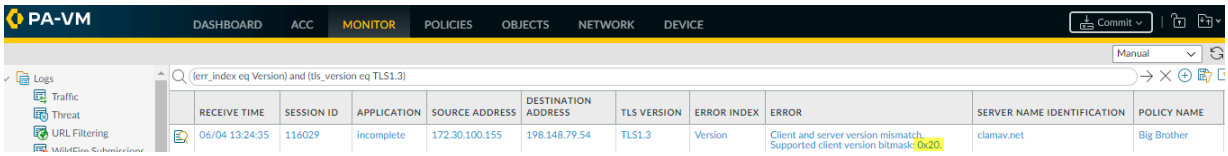
要識別和修正版本不符錯誤：

©2024 Palo Alto Networks, Inc.

1. 使用篩選器 **(err_index eq Version)** 篩選解密日誌以識別版本錯誤。反白顯示的值是位元遮罩值：



您可使用多種方法篩選解密日誌。例如，要僅查看 TLSv1.3 版本錯誤，請使用篩選器 **(err_index eq Version)** 和 **(tls_version eq TLS1.3)**：



2. 登入至 CLI 並查找位元遮罩值。第一個螢幕擷取畫面中的版本錯誤（所有三個工作階段都存在的相同錯誤）顯示了用戶端和解密設定檔不符的問題—支援的用戶端版本位元遮罩為 0x08，支援的解密設定檔版本位元遮罩為 0x70：

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-version 0x08
```

```
TLSv1.0
```

此輸出顯示用戶端僅支援 TLSv1.0。

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-version 0x70
```

```
TLSv1.1
```

```
TSLv1.2
```

```
TLSv1.3
```

此輸出顯示解密設定檔支援 TLSv1.1、TLSv1.2 和 TLSv1.3，但不支援 TLSv1.0。現在您知道了問題所在，即用戶端僅支援舊版本的 TLS 通訊協定，而附加到控制流量的解密原則規則的解密設定檔不允許 TLSv1.0 流量。

接下來要做的就是決定要採取的動作。您可以更新用戶端，使其接受更安全的 TLS 版本。如果用戶端出於某種原因需要 TLSv1.0，則可以讓防火牆繼續封鎖流量，或者可以更新解密設定檔以允許所有 TLSv1.0 流量（不推薦），或者建立允許 TLSv1.0 的解密原則和設定檔，並將其

©2024 Palo Alto Networks, Inc.

僅套用至必須使用 TLSv1.0 且不能支援更安全通訊協定（允許流量的最安全選項）的用戶端裝置。

第二個螢幕擷取畫面中的版本錯誤顯示了另一個問題：用戶端和伺服器版本不符。該錯誤表示，受支援的用戶端位元遮罩為 0x20：

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-version 0x20
```

```
TLSv1.2
```

輸出顯示用戶端僅支援 TLSv1.2。由於伺服器不支援 TLSv1.2，因此它可能僅支援 TLSv1.3 或僅支援 TLSv1.1 或更低版本（安全性較低的通訊協定）。您可以使用 Wireshark 或其他封包分析工具來找出伺服器支援的 TLS 版本。根據伺服器支援的版本，您可以：

- 如果伺服器僅支援 TLSv1.3，您可以編輯解密設定檔以使其支援 TLSv1.3。
- 如果伺服器僅支援 TLSv1.1 或更低版本，則評估您是否需要出於業務原因存取該伺服器。如果不用，則考慮封鎖流量以增加安全性。如果您出於業務目的需要存取該伺服器，則建立伺服器或將其新增到解密原則中，該原則僅套用至您出於業務原因需要存取的伺服器和網站；不允許存取使用安全性較低的 TLS 版本的所有伺服器。

3. 要查找控制工作階段流量的解密原則，請查看日誌中的 **Policy Name**（原則名稱）欄（或按一下解密日誌旁邊的放大鏡圖示 ，以查看詳細日誌檢視的「一般」區段中的資訊）。在上述範例中，解密原則名稱為 Big Brother。要查找解密原則和設定檔，請轉至 **Policies**（原則） > **Decryption**（解密），選取名為 Big Brother 的原則，然後選取 **Options**（選項）頁簽。**Decryption profile**（解密設定檔）顯示解密設定檔的名稱。

   轉至 **Objects**（物件） > **Decryption**（解密） > **Decryption Profile**（解密設定檔），選取適當的解密設定檔，對其進行編輯以解決版本問題。

密碼錯誤

使用解密日誌查找密碼錯誤與查找版本錯誤相似，您可以篩選日誌以查找錯誤並獲取錯誤位元遮罩。然後轉到 CLI，將位元遮罩轉換為錯誤值，然後採取適當的動作解決問題。例如：

1. 使用篩選器 **(err_index eq Cipher)** 篩選解密日誌以識別密碼錯誤。例如，讓我們檢查一個 **Error**（錯誤）訊息為「不受支援的密碼」的密碼錯誤。受支援的用戶端密碼位元遮罩：`0x80000000`。支援解密設定檔密碼位元遮罩 `0x60f79980`。

©2024 Palo Alto Networks, Inc.

2. 登入至 CLI 並查找位元遮罩值：

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-cipher
 0x80000000
```

```
CHACHA_PLY1305_SHA256
```

此輸出顯示，用戶端嘗試交涉防火牆支援的密碼（如果位元遮罩全為零 (0x0000000)，則用戶端嘗試交涉防火牆不支援的密碼）：

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-cipher
 0x80000000
```

```
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS13_WITH_AES_256_GCM_SHA384
TLS13_WITH_AES_128_GCM_SHA256
```

此輸出顯示，控制流量的解密設定檔支援許多密碼，但不支援用戶端嘗試使用的密碼。

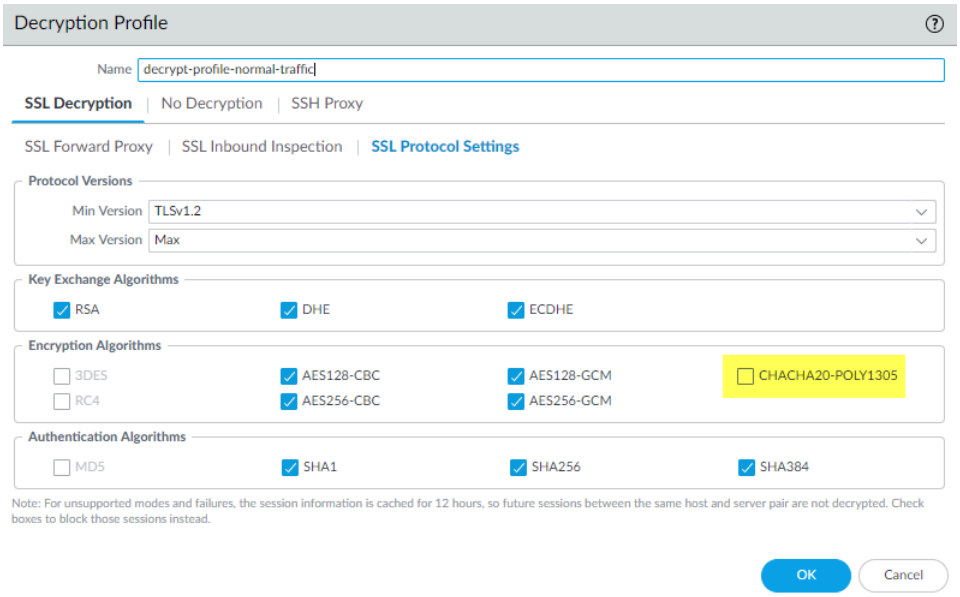
要解決此問題以便防火牆允許並解密流量，您需要在解密設定檔中新增對所缺失密碼的支援。

3. 查看解密日誌或詳細日誌檢視 **Policy Name**（原則名稱）以獲取控制流量的解密原則的名稱。轉至 **Policies**（原則） > **Decryption**（解密），然後選取原則。在 **Options**（選項）頁簽上，

©2024 Palo Alto Networks, Inc.

查找解密設定檔的名稱。接下來，轉至 **Objects**（物件） > **Decryption**（解密） > **Decryption Profile**（解密設定檔），選取適當的解密設定檔，對其進行編輯以解決版本問題。

在本範例中，解密設定檔不支援 TLS13_WITH_CHACHA_POLY1305_SHA256 密碼，因此用戶端不能連線：



要解決此問題，請選取 **CHACHA20-POLY1305** 加密演算法選項（**Max**（最大值）的 **Max Version**（最高版本）設定意味著設定檔已支援 TLSv1.3，且驗證演算法設定已經包含 SHA256，因此僅缺少加密演算法支援），然後 **Commit**（提交）設定。提交設定後，解密設定檔將支援缺失的密碼，流量的解密工作階段成功。

如果防火牆不支援加密套件，且您出於業務目的需要允許流量，則建立一個僅套用至該流量的解密政策和設定檔。在解密設定檔中，停用 ***Block sessions with unsupported cipher suites***（封鎖具有不受支援加密套件的工作階段）選項

。

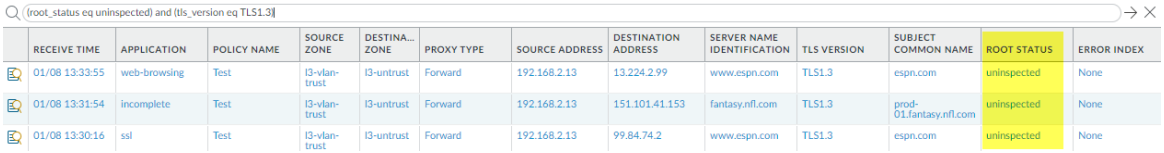
根狀態「未受檢查」

在某些情況下，**Root Status**（根狀態）欄顯示值 **uninspected**（未受檢查）。防火牆無法檢查根狀態的原因有很多，包括：

- 工作階段繼續。
- 流量未解密，由於「不解密」原則控制了流量，因此防火牆未解密流量。
- 在防火牆能夠檢查伺服器憑證之前發生了解密失敗。

篩選解密日誌 **(root_status eq uninspected)** 和 **(tls_version eq TLS1.3)** 以查看根狀態未受檢查的解密工作階段：

©2024 Palo Alto Networks, Inc.



修復不完整的憑證鏈結

儘管 RFC 5246 TLSv1.2 標準要求經過驗證的伺服器提供有效的憑證鏈結，從而成為可接受的憑證授權單位，但並非所有網站都會傳送其完整的憑證鏈結。當您啟用解密並套用在解密政策中啟用了 **Block sessions with untrusted issuers**（封鎖具有不受信任簽發者的工作階段）的正向 Proxy 解密設定檔時，如果網站伺服器提供給防火牆的憑證清單中缺少中繼憑證，則防火牆無法構建憑證鏈到頂部（根）憑證。在這些情況下，防火牆會向用戶端提供其轉送不受信任憑證，因為防火牆無法建構鏈結到根憑證，且沒有缺失的中繼憑證，就無法建立信任。

防火牆僅在其預設受信任憑證授權單位商店才有根憑證。

如果您出於業務目的需要與之通訊的網站缺少一個或多個中繼憑證，且解密設定檔封鎖了具有不受信任簽發者的工作階段，那麼您可以找到並下載缺失的中繼憑證，並將其作為受信任的根 CA 安裝在防火牆上，使防火牆信任該網站的伺服器。（替代方法是聯絡網站擁有者，並要求他們設定其伺服器，以便在交握期間傳送中繼憑證。）

如果您在解密設定檔中允許具有不受信任簽發者的工作階段，則即使簽發者不受信任，防火牆也會建立工作階段；但是，最佳做法是封鎖具有不受信任簽發者的工作階段，以獲得更好的安全性。

STEP 1 | 找到引起不完整憑證鏈結錯誤的網站。

1. 篩選解密日誌以識別由於憑證鏈結不完整而失敗的解密工作階段。

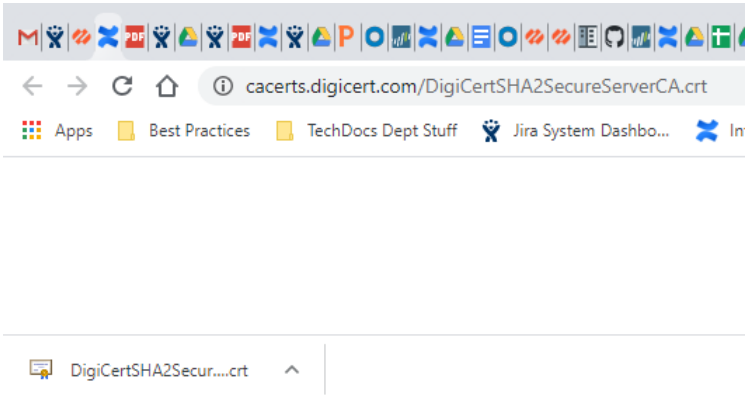
   在篩選器欄位中，鍵入查詢 **(err_index eq Certificate)** 和 **(error contains 'http')**。該查詢會篩選包含字串「http」之憑證錯誤的日誌，以找出包含 CA 簽發者 URL（通常稱為 URI）的所有錯誤項目。CA 簽發者 URL 是 CA 簽發者的授權單位資訊存取 (AIA) 資訊。

2. 按一下以「Received fatal alert UnknownCA from client. CA Issuer URL:」開頭，後跟 URI 的 **Error**（錯誤）欄項目。

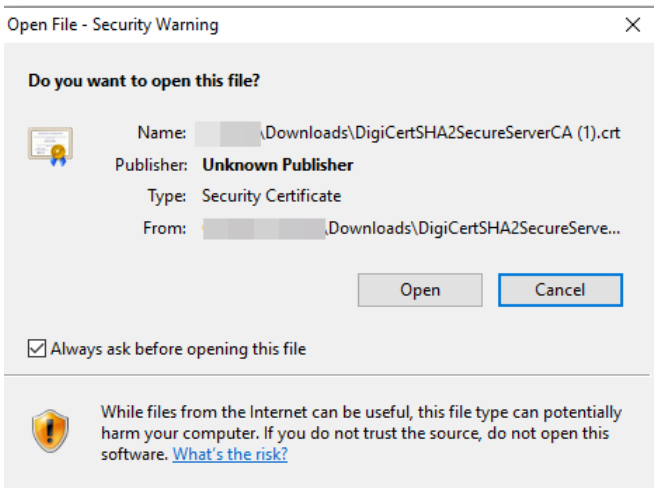
   防火牆會將所選錯誤自動新增到查詢，並顯示完整 URI 路徑（完整 URI 路徑可能在 **Error**（錯誤）欄中被截斷）。

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 將 URI 複製並貼入瀏覽器中，然後按 Enter 以下載缺失的中繼憑證。

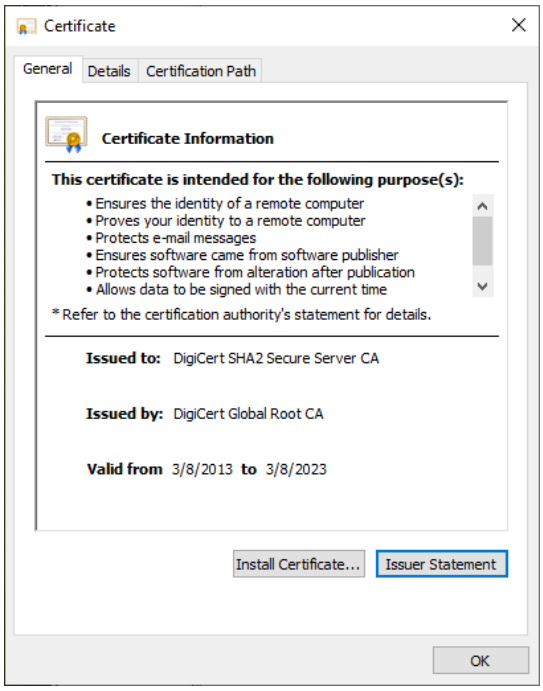


STEP 3 | 按一下憑證以開啟對話方塊。

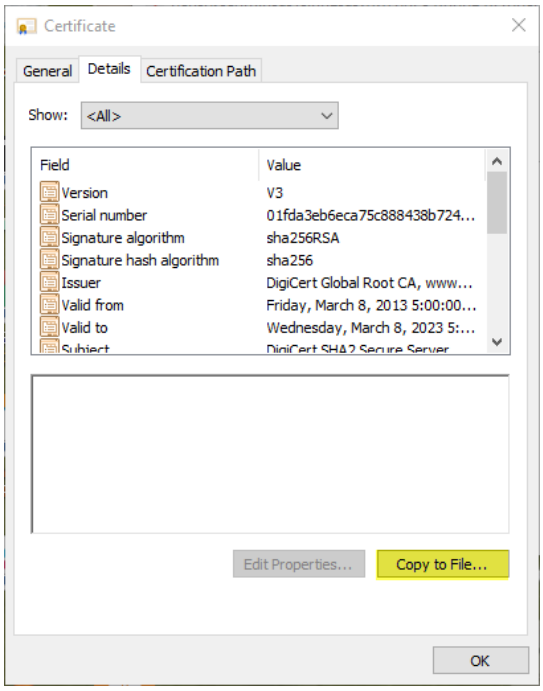


 ©2024 Palo Alto Networks, Inc.

STEP 4 | 按一下 **Open**（開啟）以開啟憑證檔案。



STEP 5 | 選取 **Details**（詳細資料）頁簽，然後按一下 **Copy to File...**（複製到檔案...）。

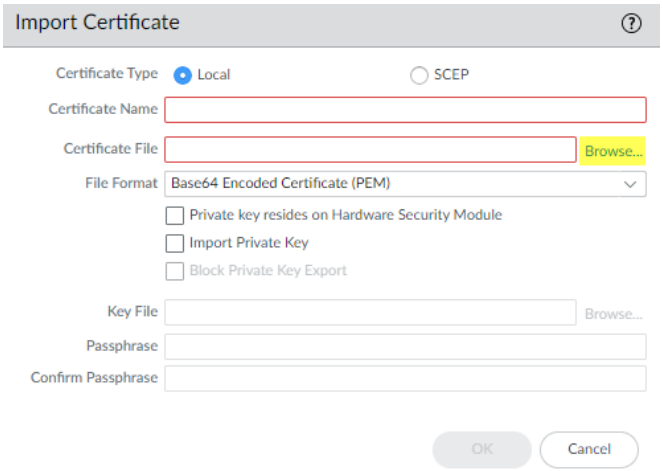


遵循匯出指令。憑證會複製到您指定為預設下載資料夾的資料夾。

©2024 Palo Alto Networks, Inc.

STEP 6 | 將憑證匯入到防火牆。

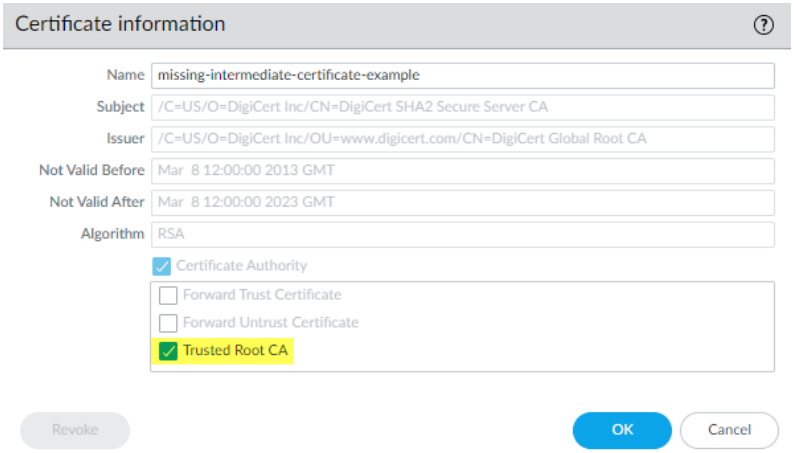
1. 導覽到 **Device**（裝置）> **Certificate Management**（憑證管理）> **Certificates**（憑證），然後選取 **Import**（匯入）。
2. **Browse**（瀏覽）到您儲存缺失中繼憑證的資料夾，然後選取它。將 **File Format**（檔案格式）保留為 **Base64 Encoded Certificate (PEM)**（**Base64** 編碼憑證 **(PEM)**）。



3. 命名憑證並指定您想要使用的任何其他選項，然後按一下 **OK**（確定）。

STEP 7 | 匯入憑證後，在 **Device Certificates**（裝置憑證）清單中選取憑證，以開啟「憑證資訊」對話方塊。

STEP 8 | 選取 **Trusted Root CA**（受信任的根 **CA**）以將憑證標記為防火牆上「受信任的根 CA」，然後按一下 **OK**（確定）。



在 **Device**（裝置）> **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Device Certificates**（裝置憑證）中，匯入的憑證現在會出現在憑證清單中。選取 **Usage**（使用方式）欄確認狀態為 **Trusted Root CA Certificate**（受信任的根 **CA** 憑證），以確認防火牆將該憑證視為受信任的根 CA。

STEP 9 | **Commit**（提交）組態。

©2024 Palo Alto Networks, Inc.

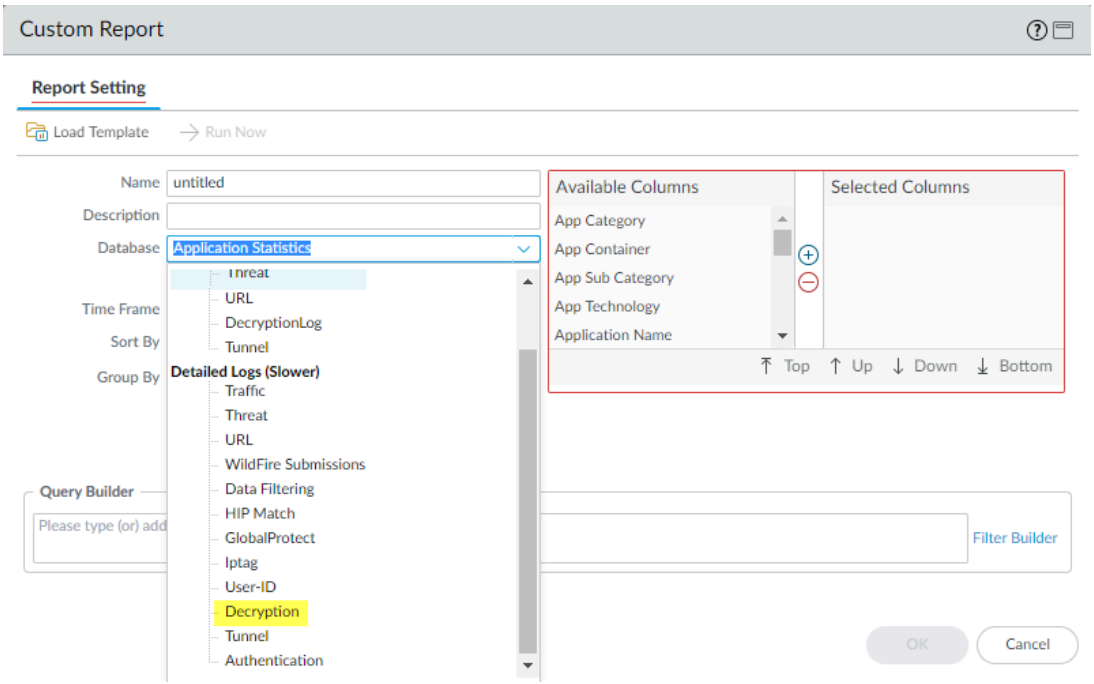
STEP 10 | 您現在已修復中斷的憑證鏈結。

防火牆不會再因 CS 簽發者不受信任而封鎖流量。對所有缺失的中繼憑證重複此程序，以修復其憑證鏈結。

解密的自訂報告範本

您可以基於解密日誌欄位和自訂範本為解密事件建立自訂報告，並產生它們。選取日誌欄位以包含在自訂報告中，選取範本以調整日誌查詢：

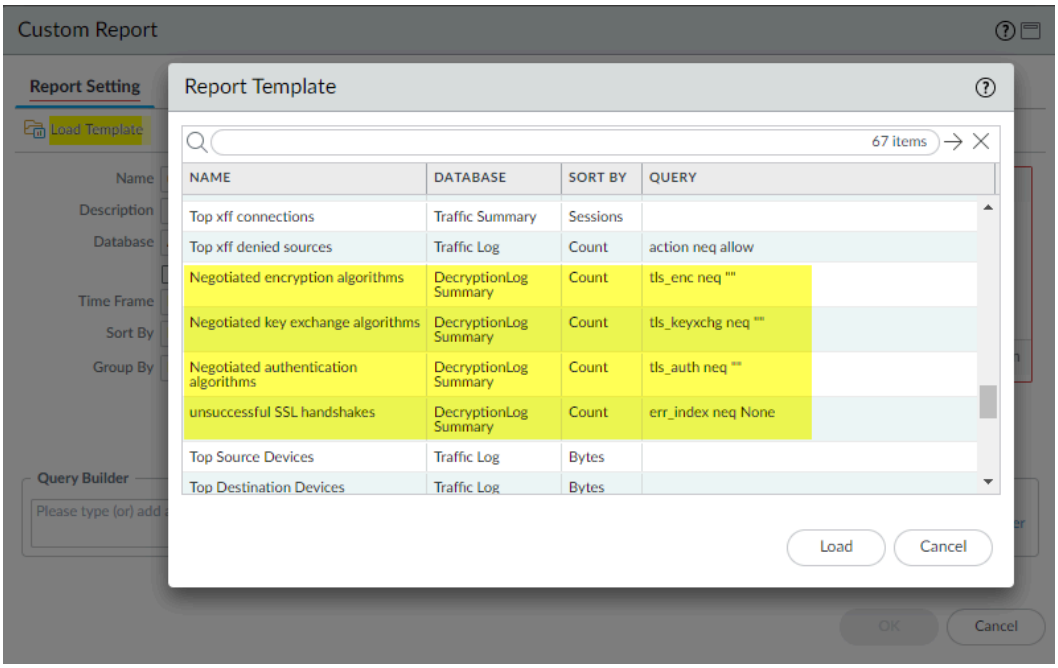
1. **Monitor**（監控） > **Manage Custom Reports**（管理自訂報告）。
2. **Add**（新增）自訂報告。
3. 要設定解密日誌欄位在自訂報告中使用，請選取 **Decryption**（解密）作為 **Database**（資料庫）。



Available Columns（可用欄）清單會變更以符合解密日誌中可用的欄。選取並新增您想要包含在自訂報告中的欄（資訊）。如果您不想進一步調整自訂報告，按一下 **OK**（確定）以產生報告。

©2024 Palo Alto Networks, Inc.

4. 如果需要，使用 PAN-OS 10.0 中引入的查詢建立器和四個範本調整自訂解密報告的輸出。要選取範本以篩選報告輸出，請按一下 **Load Template**（載入範本）並從四個解密範本中進行選取：



Query（查詢）欄顯示每個範本代表的篩選器查詢。**Load**（載入）所需查詢，然後按一下 **OK**（確定）以產生自訂報告。

Proxy 類型和 TLS 版本不支援的參數

解密日誌欄位顯示每種解密 Proxy 類型的解密工作階段參數。但是，由於版本支援、TLS 交握的加密部分、資訊可用性等原因，某些參數不適用於每種 Proxy 類型或 TLS 版本。以下表格按 Proxy 類型和 TLS 版本顯示了不受支援的解密日誌參數。

Proxy 類型	不受支援的參數	**TLS** 版本
正向 Proxy	交涉的 EC 曲線	TLSv1.3
輸入檢查	伺服器名稱識別 根通用名稱	全部
	交涉的 EC 曲線	TLSv1.3
不解密（解密原則規則中的不解密動作）	交涉的 EC 曲線 伺服器名稱識別	TLSv1.2
	交涉的 EC 曲線	TLSv1.3

©2024 Palo Alto Networks, Inc.

Proxy 類型	不受支援的參數	TLS 版本
	伺服器名稱識別 憑證資訊（所有憑證資訊欄位，例如，憑證開始日期、憑證結束日期、憑證金鑰類型等）	
網路封包代理程式	交涉的 EC 曲線	TLSv1.3
GlobalProtect 入口網站	伺服器名稱識別 根通用名稱 解密原則名稱 App-ID	全部
GlobalProtect 閘道	伺服器名稱識別 解密原則名稱 App-ID	全部
無用戶端 SSLVPN	伺服器名稱識別	全部
SSH	解密日誌不受支援	
純文字	解密日誌不受支援	

解密疑難排解工作流程範例

應用程式控管中心 (ACC) 的 解密日誌 和 SSL 活動 Widget 提供功能強大的解密疑難排解工具，這些工具可以獨立工作，也可以一起工作。當您瞭解了如何使用這些工具後，就可以調查並解決各種各樣的解密問題。

以下範例顯示如何使用疑難排解工具來識別、調查和解決解密問題。套用這些方法來解決在解密部署中遇到的任何問題。

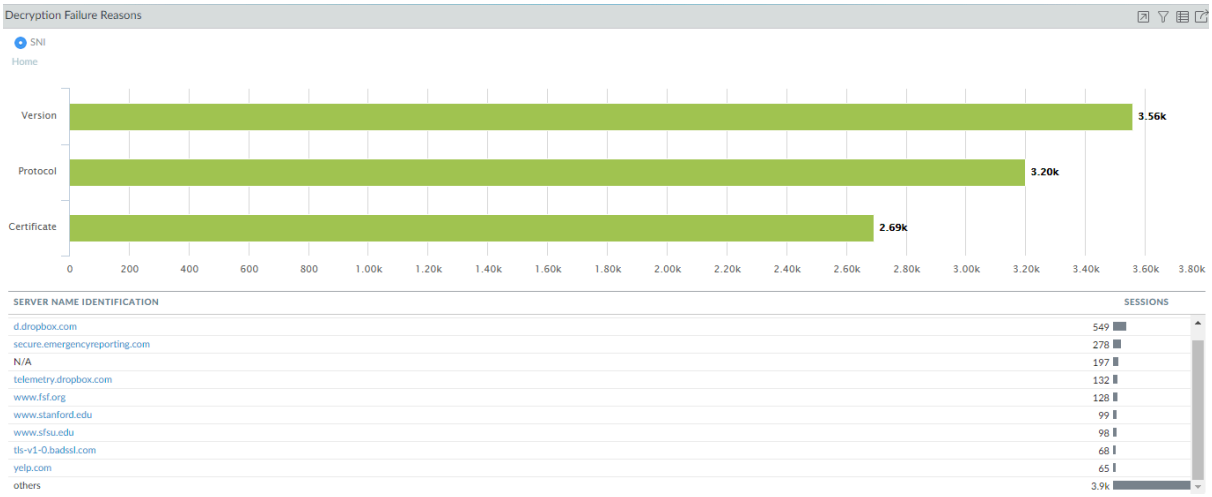
- 調查解密失敗原因
- 疑難排解不受支援的加密套件
- 識別弱通訊協定和加密套件
- 識別不受信任的 CA 憑證
- 疑難排解過期的憑證
- 疑難排解撤銷的憑證
- 疑難排解釘選的憑證

©2024 Palo Alto Networks, Inc.

調查解密失敗原因

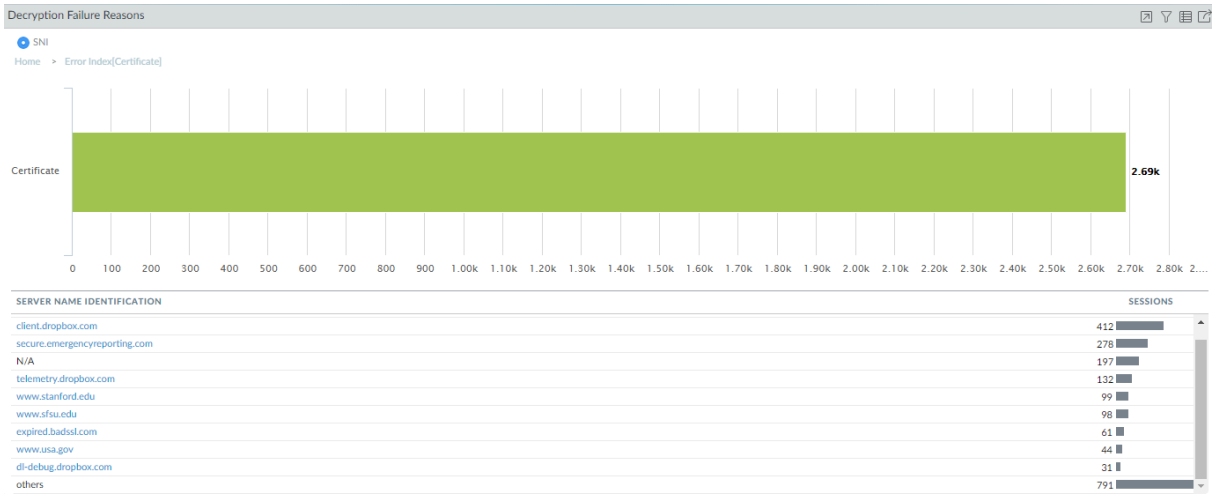
解密失敗的最常見原因是 TLS 通訊協定錯誤、密碼版本錯誤（用戶端和伺服器版本不相符以及用戶端和解密設定檔版本不相符）以及憑證錯誤。要調查解密錯誤，請先透過應用程式控管中心 (ACC) 識別失敗，然後轉到解密日誌以向下鑽研詳細資料。

STEP 1 | 先調查 **ACC** > **SSL Activity**（**SSL** 活動），然後查看「解密失敗原因」Widget。



在此範例中，我們會調查憑證錯誤。您可以使用相同程序來調查版本和通訊協定錯誤。

STEP 2 | 按一下 **Certificate**（憑證）旁邊的綠色列，以查看哪些主機 (SNI) 遇到憑證錯誤，並查看遇到最多憑證錯誤的主機清單。



 ©2024 Palo Alto Networks, Inc.

STEP 3 | 轉到 **Monitor**（監控） > **Logs**（日誌） > **Decryption**（解密）以向下鑽研日誌。

使用查詢 **(err_index eq Certificate)** 篩選解密日誌以檢視遇到憑證錯誤的所有解密工作階段。

(err_index eq Certificate)

RECEIVE TIME	SESSION ID	APPLICATION	SOURCE ADDRESS	DESTINATION ADDRESS	TLS VERSION	SERVER NAME IDENTIFICATION	POLICY NAME	ERROR INDEX	ERROR
06/08 13:22:11	205207	incomplete	172.30.100.10	52.203.88.8	TLS1.3	www.stanford.edu	Big Brother	Certificate	Received fatal alert CertificateUnknown from client
06/08 11:17:14	203671	ssl	172.30.100.10	52.9.173.94	TLS1.2	expired-isrgrootx1.letsencrypt.	Big Brother	Certificate	Expired server certificate. CA Issuer URL: http://cert.int-x3.letsencrypt.org/
06/08 11:17:14	203669	incomplete	172.30.100.10	52.9.173.94	TLS1.2	expired-isrgrootx1.letsencrypt.	Big Brother	Certificate	Received fatal alert CertificateUnknown from client. CA Issuer URL: http://cert.int-x3.letsencrypt.org/
06/08 11:17:11	203666	incomplete	172.30.100.10	52.9.173.94	TLS1.2	expired-isrgrootx1.letsencrypt.	Big Brother	Certificate	Received fatal alert CertificateUnknown from client. CA Issuer URL: http://cert.int-x3.letsencrypt.org/
06/08 11:17:11	203663	incomplete	172.30.100.10	52.9.173.94	TLS1.2	expired-isrgrootx1.letsencrypt.	Big Brother	Certificate	Received fatal alert CertificateUnknown from client. CA Issuer URL: http://cert.int-x3.letsencrypt.org/
06/08 11:16:18	203598	ssl	172.30.100.10	52.9.173.94	TLS1.2	revoked-isrgrootx1.letsencrypt.	Big Brother	Certificate	OCSP/CRL check: certificate revoked. CA Issuer URL: http://cert.int-x3.letsencrypt.org/
06/08 11:16:18	203576	ssl	172.30.100.10	52.9.173.94	TLS1.2	revoked-isrgrootx1.letsencrypt.	Big Brother	Certificate	OCSP/CRL check: certificate revoked
06/08 11:16:18	203575	ssl	172.30.100.10	52.9.173.94	TLS1.2	revoked-isrgrootx1.letsencrypt.	Big Brother	Certificate	OCSP/CRL check: certificate revoked
06/04 18:26:34	123731	incomplete	172.30.100.10	99.84.224.10	TLS1.2	www.usa.gov	Big Brother	Certificate	Received fatal alert CertificateUnknown from client

Error（錯誤）欄顯示憑證錯誤的原因。要篩選發生相同錯誤的所有解密工作階段，請按一下錯誤訊息以將其新增到查詢中，然後執行查詢。例如，要基於從用戶端收到的嚴重警示發現所有錯誤，按一下錯誤以產生查詢 **(err_index eq Certificate)** 和 **(error eq 'Received fatal alert CertificateUnknown from client')**：

(err_index eq Certificate) and (error eq 'Received fatal alert CertificateUnknown from client')

RECEIVE TIME	SESSION ID	APPLICATION	SOURCE ADDRESS	DESTINATION ADDRESS	TLS VERSION	SERVER NAME IDENTIFICATION	POLICY NAME	ERROR INDEX	ERROR
06/08 13:22:11	205206	incomplete	172.30.100.10	52.203.88.8	TLS1.3	www.stanford.edu	Big Brother	Certificate	Received fatal alert CertificateUnknown from client
06/08 13:22:11	205207	incomplete	172.30.100.10	52.203.88.8	TLS1.3	www.stanford.edu	Big Brother	Certificate	Received fatal alert CertificateUnknown from client
06/04 18:26:34	123731	incomplete	172.30.100.10	99.84.224.10	TLS1.2	www.usa.gov	Big Brother	Certificate	Received fatal alert CertificateUnknown from client
06/04 18:26:34	123732	incomplete	172.30.100.10	99.84.224.10	TLS1.2	www.usa.gov	Big Brother	Certificate	Received fatal alert CertificateUnknown from client

要篩選特定主機收到的憑證錯誤，請將該 SNI 新增到查詢中，而不是新增錯誤訊息文字。例如，要找出 expired.badssl.comm 的所有憑證錯誤，請使用查詢 **(err_index eq Certificate)** 和 **(sni eq 'expired.badssl.com')**：

(err_index eq Certificate) and (sni eq 'expired.badssl.com')

RECEIVE TIME	SESSION ID	APPLICATION	SOURCE ADDRESS	DESTINATION ADDRESS	TLS VERSION	SERVER NAME IDENTIFICATION	POLICY NAME	ERROR INDEX	ERROR
06/02 17:17:20	12959	ssl	172.30.100.10	104.154.89.105	TLS1.2	expired.badssl.com	Big Brother	Certificate	Expired server certificate. CA Issuer URL: htt
06/02 17:17:19	12957	ssl	172.30.100.10	104.154.89.105	TLS1.2	expired.badssl.com	Big Brother	Certificate	Expired server certificate. CA Issuer URL: htt
06/02 17:17:19	12955	ssl	172.30.100.10	104.154.89.105	TLS1.2	expired.badssl.com	Big Brother	Certificate	Expired server certificate. CA Issuer URL: htt
06/02 17:17:19	12958	incomplete	172.30.100.10	104.154.89.105	TLS1.2	expired.badssl.com	Big Brother	Certificate	Received fatal alert CertificateUnknown from client. CA Issuer URL: htt
06/02 17:17:18	12956	incomplete	172.30.100.10	104.154.89.105	TLS1.2	expired.badssl.com	Big Brother	Certificate	Received fatal alert CertificateUnknown from client. CA Issuer URL: htt
06/02 17:17:18	12951	incomplete	172.30.100.10	104.154.89.105	TLS1.2	expired.badssl.com	Big Brother	Certificate	Received fatal alert CertificateUnknown from client. CA Issuer URL: htt
06/02 17:11:48	12802	ssl	172.30.100.10	104.154.89.105	TLS1.2	expired.badssl.com	Big Brother	Certificate	Expired server certificate. CA Issuer URL: htt

Error（錯誤）欄顯示與 expired.badssl.com 關聯的每個憑證錯誤的具體原因。

在知道導致解密失敗的憑證問題的原因後，就可以解決它。例如，如果憑證鏈結不完整，您可以修復不完整的憑證鏈結。如果憑證已過期，您可以通知網站管理員，如果您需要存取該網站，則可以建立基於原則的例外。

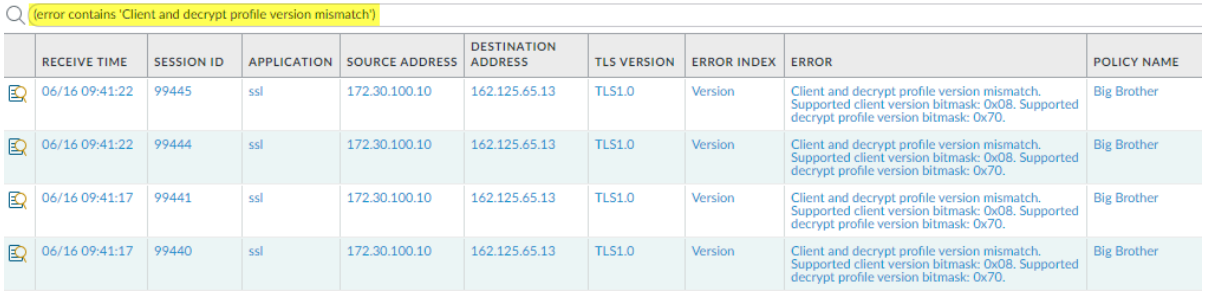
©2024 Palo Alto Networks, Inc.

疑難排解不受支援的加密套件

識別解密日誌中不受支援的加密套件并進行疑難排解是版本錯誤調查的一個方面，值得單獨研究。

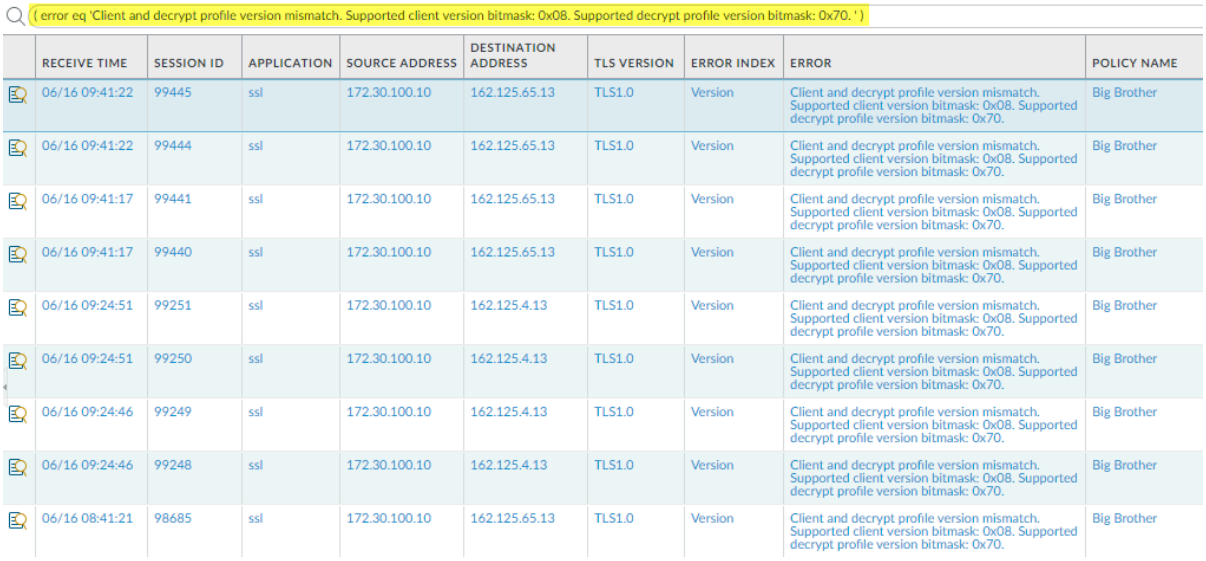
STEP 1 | 在解密日誌中（**Monitor**（監控） > **Logs**（日誌） > **Decryption**（解密）），使用查詢 **(error contains 'Client and decrypt profile mismatch')** 識別所有加密套件版本不符的情況。

篩選日誌找出此類不符情況，可識別出用戶端和解密設定檔加密套件支援不符的所有執行個體。


(error contains 'Client and decrypt profile version mismatch')

	RECEIVE TIME	SESSION ID	APPLICATION	SOURCE ADDRESS	DESTINATION ADDRESS	TLS VERSION	ERROR INDEX	ERROR	POLICY NAME
	06/16 09:41:22	99445	ssl	172.30.100.10	162.125.65.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
	06/16 09:41:22	99444	ssl	172.30.100.10	162.125.65.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
	06/16 09:41:17	99441	ssl	172.30.100.10	162.125.65.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
	06/16 09:41:17	99440	ssl	172.30.100.10	162.125.65.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother

要找出發生相同錯誤的所有解密工作階段，請按一下錯誤訊息以將其新增到查詢中並移除原始查詢，例如：


(error eq 'Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. ')

	RECEIVE TIME	SESSION ID	APPLICATION	SOURCE ADDRESS	DESTINATION ADDRESS	TLS VERSION	ERROR INDEX	ERROR	POLICY NAME
	06/16 09:41:22	99445	ssl	172.30.100.10	162.125.65.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
	06/16 09:41:22	99444	ssl	172.30.100.10	162.125.65.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
	06/16 09:41:17	99441	ssl	172.30.100.10	162.125.65.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
	06/16 09:41:17	99440	ssl	172.30.100.10	162.125.65.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
	06/16 09:24:51	99251	ssl	172.30.100.10	162.125.4.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
	06/16 09:24:51	99250	ssl	172.30.100.10	162.125.4.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
	06/16 09:24:46	99249	ssl	172.30.100.10	162.125.4.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
	06/16 09:24:46	99248	ssl	172.30.100.10	162.125.4.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
	06/16 08:41:21	98685	ssl	172.30.100.10	162.125.65.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother

十六進位代碼標識用戶端支援的確切版本以及解密設定檔支援的確切版本。

©2024 Palo Alto Networks, Inc.

STEP 2 | 登入至 CLI 並查找位元遮罩值。

錯誤顯示用戶端和解密設定檔不符。受支援的用戶端位元遮罩為 0x08，而受支援的解密設定檔位元遮罩為 0x70：

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-version 0x08
```

```
TLSv1.0
```

此輸出顯示用戶端僅支援 TLSv1.0。

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-version 0x70
```

```
TLSv1.1
```

```
TSLv1.2
```

```
TLSv1.3
```

此輸出顯示解密設定檔支援 TLSv1.1、TLSv1.2 和 TLSv1.3，但不支援 TLSv1.0。現在您知道，用戶端僅支援舊版本的 TLS 通訊協定，而附加到控制流量的解密原則規則的解密設定檔不允許該版本。

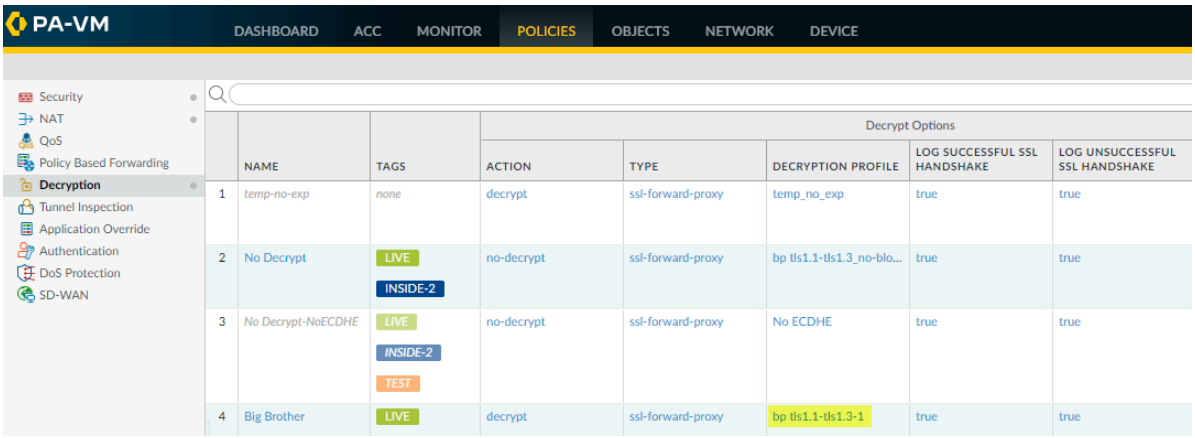
STEP 3 | 確定要採取什麼動作。

您可以更新用戶端，使其接受更安全的 TLS 版本。如果用戶端出於某種原因需要 TLSv1.0，則可以讓防火牆繼續封鎖流量，或者可以更新解密設定檔以允許所有 TLSv1.0 流量（不推薦），或者建立允許 TLSv1.0 的解密原則和設定檔，並將其僅套用至必須使用 TLSv1.0 且不能支援更安全通訊協定（允許流量的最安全選項）的用戶端裝置。

©2024 Palo Alto Networks, Inc.

STEP 4 | 如果您選擇編輯解密設定檔，要找出控制工作階段流量的解密原則，請查看日誌中的 **Policy Name**（原則名稱）欄（或按一下解密日誌旁邊的放大鏡圖示 ，以查看詳細日誌檢視的「一般」區段中的資訊）。

1. 在本範例中，解密原則名稱為 Big Brother；要找出解密設定檔，請轉至 **Policies**（原則）> **Decryption**（解密），並檢查 **Decryption Profile**（解密設定檔）欄。

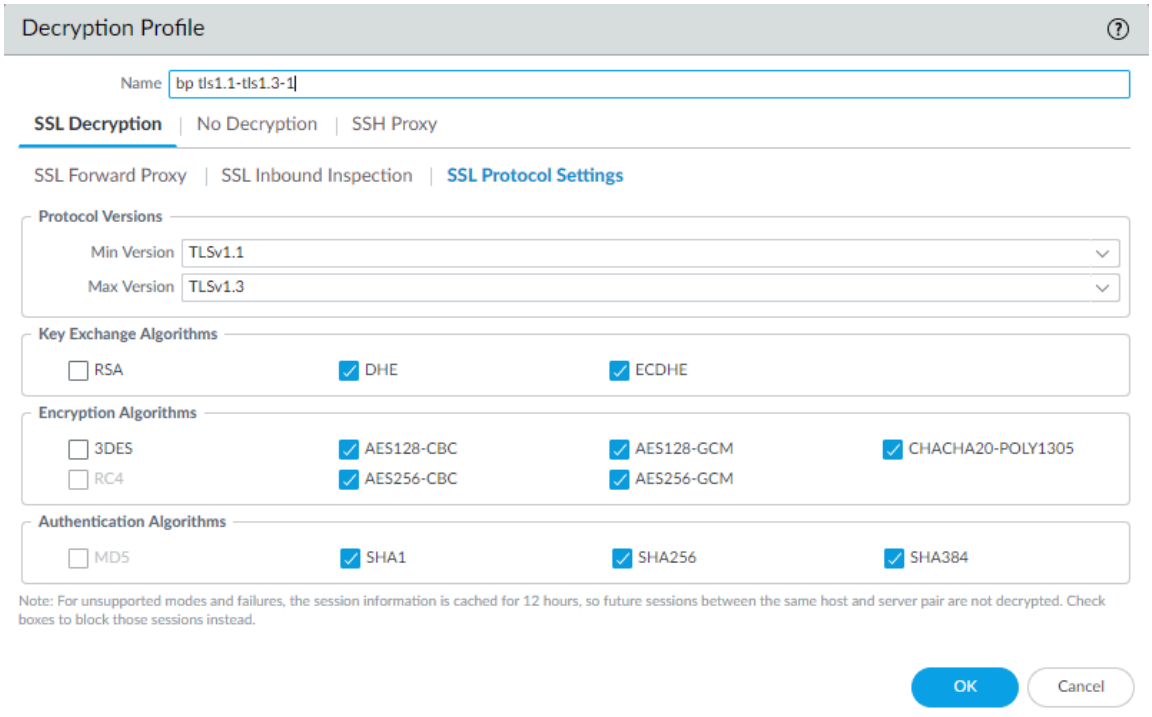


解密設定檔的名稱為 **bp tls1.1-tls1.3-1**。您還可以選取 Big Brother 原則，然後選取 **Options**（選項）頁簽以查看解密設定檔的名稱。

轉至 **Objects**（物件）> **Decryption**（解密）> **Decryption Profile**（解密設定檔），選取適當的解密設定檔，對其進行編輯以解決版本問題。

2. 轉至 **Objects**（物件）> **Decryption**（解密）> **Decryption Profile**（解密設定檔）。

選取 **bp tls1.1-tls1.3-1** 解密設定檔，然後按一下 **SSL Protocol Settings**（**SSL** 通訊協定設定）頁簽。



 ©2024 Palo Alto Networks, Inc.

設定檔支援的最低 TLS 通訊協定版本（**Min Version**（最低版本））為 TLSv1.1。要允許版本不符封鎖的流量，您可以將 **Min Version**（最低版本）變更為 TLSv1.0。但是，更安全的選項是更新用戶端以使用最新的 TLS 通訊協定版本。如果無法更新用戶端，則可以建立僅適用於該使用者、裝置或來源位址（以及任何類似使用者、裝置或來源位址，以便一個原則和設定檔控制所有此類流量）的解密原則和設定檔，而不是套用允許 TLSv1.0 流量的一般解密原則。

識別弱通訊協定和加密套件

弱 TLS 通訊協定和弱加密套件（加密演算法、驗證演算法、金鑰交換演算法和交涉的 EC 曲線）會削弱您的安全狀態，且與強 TLS 通訊協定和強加密套件相比，更容易被危險分子利用。

解密日誌項目中的五個欄位顯示了解密工作階段的通訊協定和加密套件：

TLS VERSION	ENCRYPTION ALGORITHM	KEY EXCHANGE	AUTHENTICATI... ALGORITHM	NEGOTIATED EC CURVE
TLS1.2	AES_128_GCM	ECDHE	SHA256	secp256r1
TLS1.2	AES_256_GCM	ECDHE	SHA384	secp256r1

追蹤易受攻擊的舊 TLS 版本和加密套件，以便您可以就是否允許與可能危害安全狀態的伺服器和應用程式連線做出明智的決定。

本主題中的範例顯示如何：

- 識別使用安全性較低的 TLS 通訊協定版本的流量。
- 識別使用特定金鑰交換演算法的流量。
- 識別使用特定驗證演算法的流量。
- 識別使用特定加密演算法的流量。

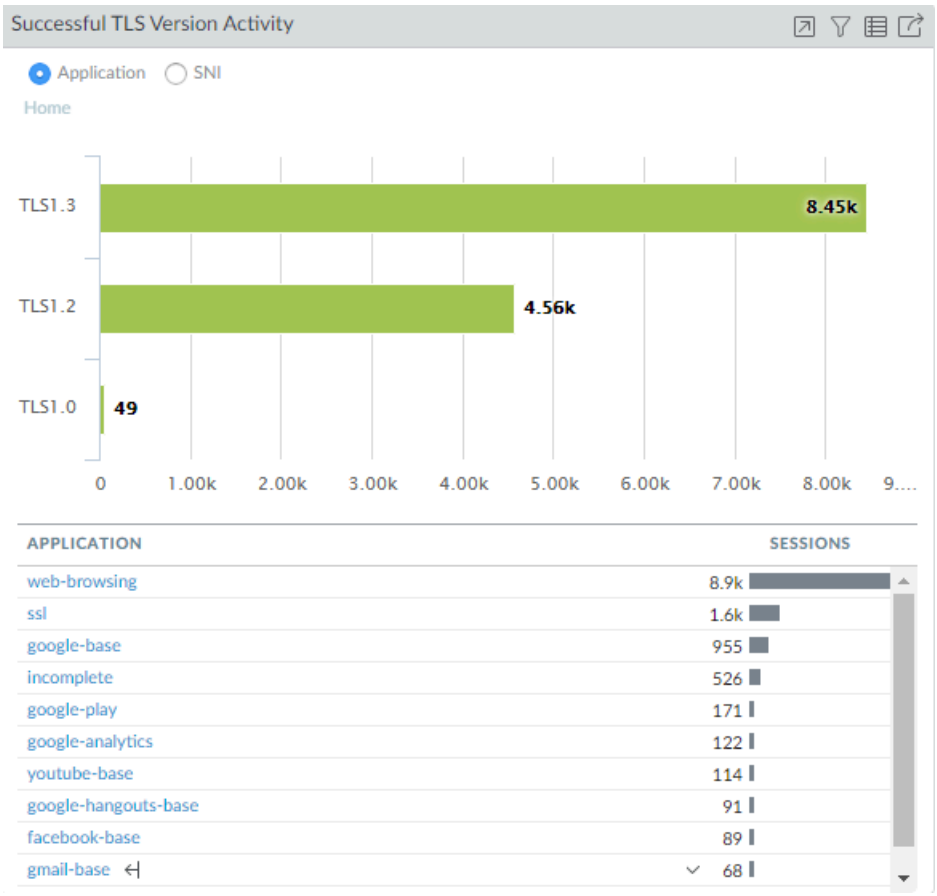
這些範例向您展示瞭如何以各種方式使用解密疑難排解工具，以便您可以學習使用它們來對可能遇到的任何解密問題進行疑難排解。

您可以使用 *Wireshark* 或其他封包分析器來仔細檢查是用戶端還是伺服器引發了問題、*TLS* 用戶端和伺服器版本以及其他加密套件資訊。這有助於分析版本不符和其他問題。

©2024 Palo Alto Networks, Inc.

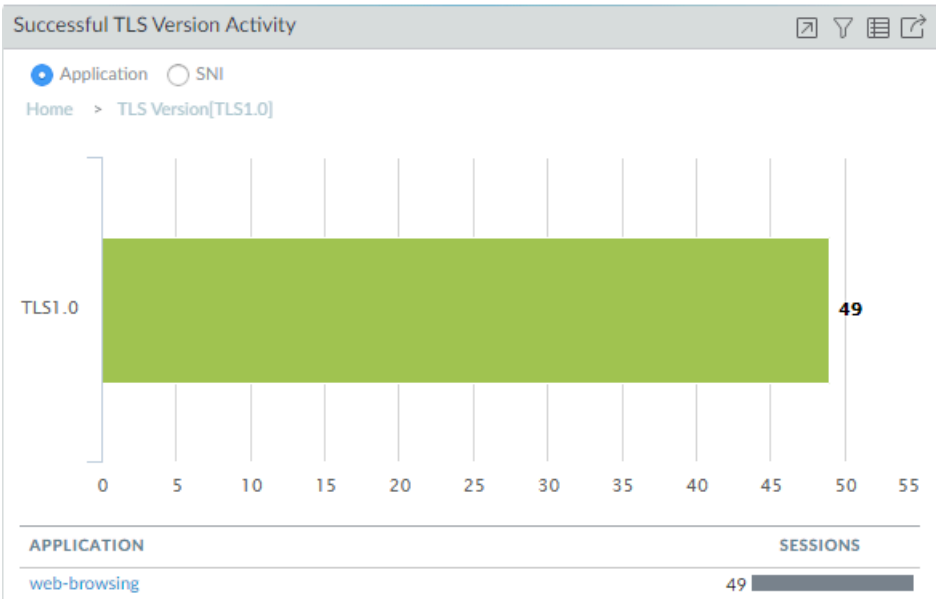
TLS 通訊協定—識別使用較舊且安全性較低的 TLS 通訊協定版本的流量，以便您可以評估是否允許存取使用弱通訊協定的伺服器和應用程式。

1. 首先檢查應用程式控管中心 (ACC)，以查看防火牆是否允許弱通訊協定（**ACC** > **SSL Activity**（**SSL** 活動） > **Successful TLS Version Activity**（成功 **TLS** 版本活動））並獲取活動的整體檢視。



在此範例中，大多數成功的 TLS 活動是 TLSv1.2 和 TLSv1.3 活動。但是，有少數允許的 TLSv1.0 流量的執行個體。我們按一下數字 **49** 來向下鑽研 TLSv1.0 活動，並查看哪些應用程式建立了成功的 TLSv1.0 連線：

©2024 Palo Alto Networks, Inc.

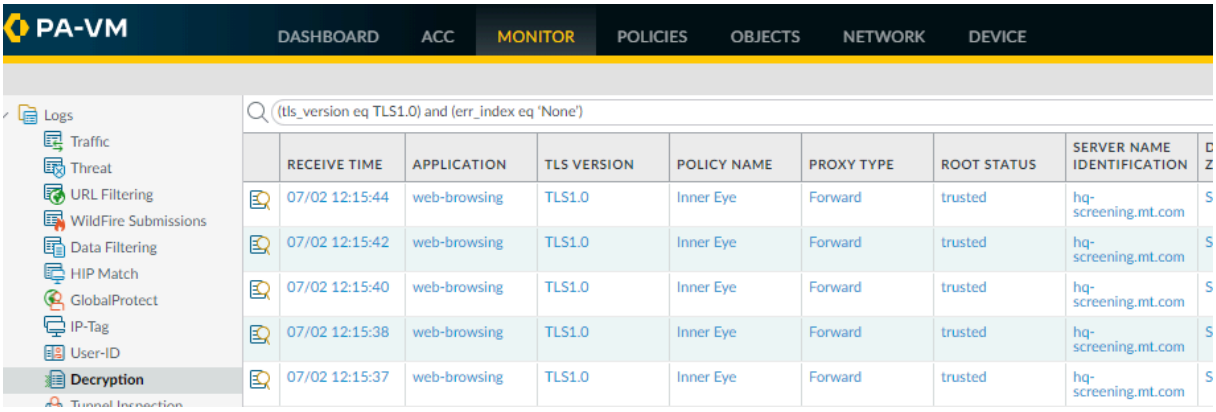


我們看到防火牆允許標識為 Web 瀏覽流量的流量。為了深入瞭解 TLSv1.0 Web 瀏覽流量是什麼以及為什麼允許它，我們看一下旁邊的解密日誌。

2. 篩選解密日誌以查看 TLSv1.0 活動詳細資料。

   使用查詢 **(tls_version eq TLS1.0)** 和 **(err_index eq 'None')** 顯示成功的 TLSv1.0 解密工作階段。

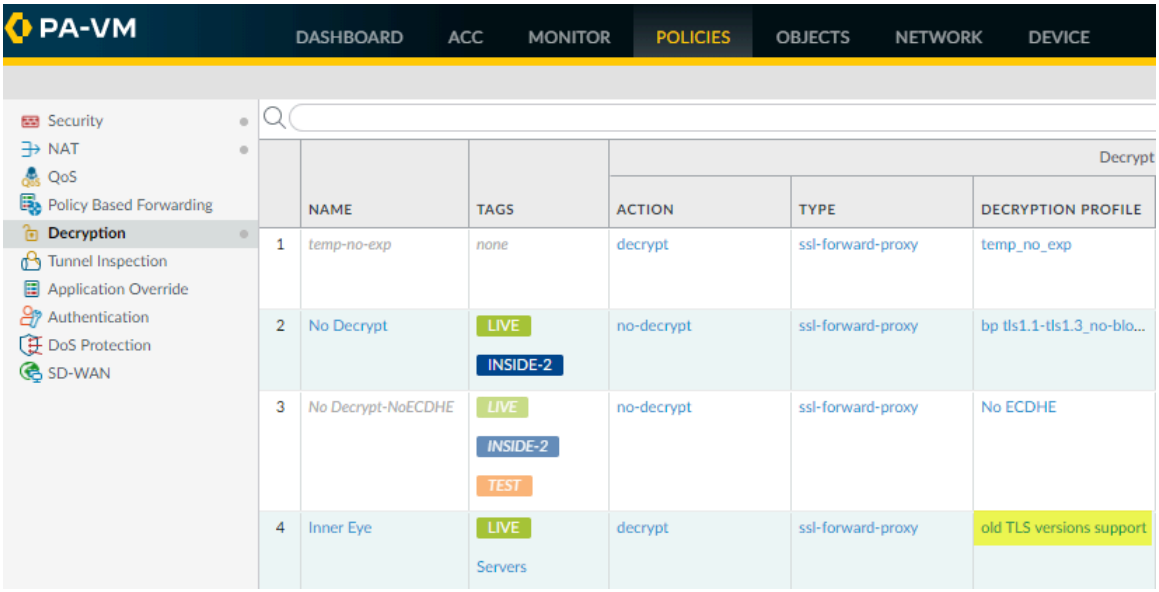
   在您設定解密記錄後，僅當您在解密政策中啟用記錄成功的 *TLS* 交握時，解密日誌才顯示成功的 *TLS* 活動。如果記錄成功 *TLS* 交握被停用，則您無法查看此資訊。



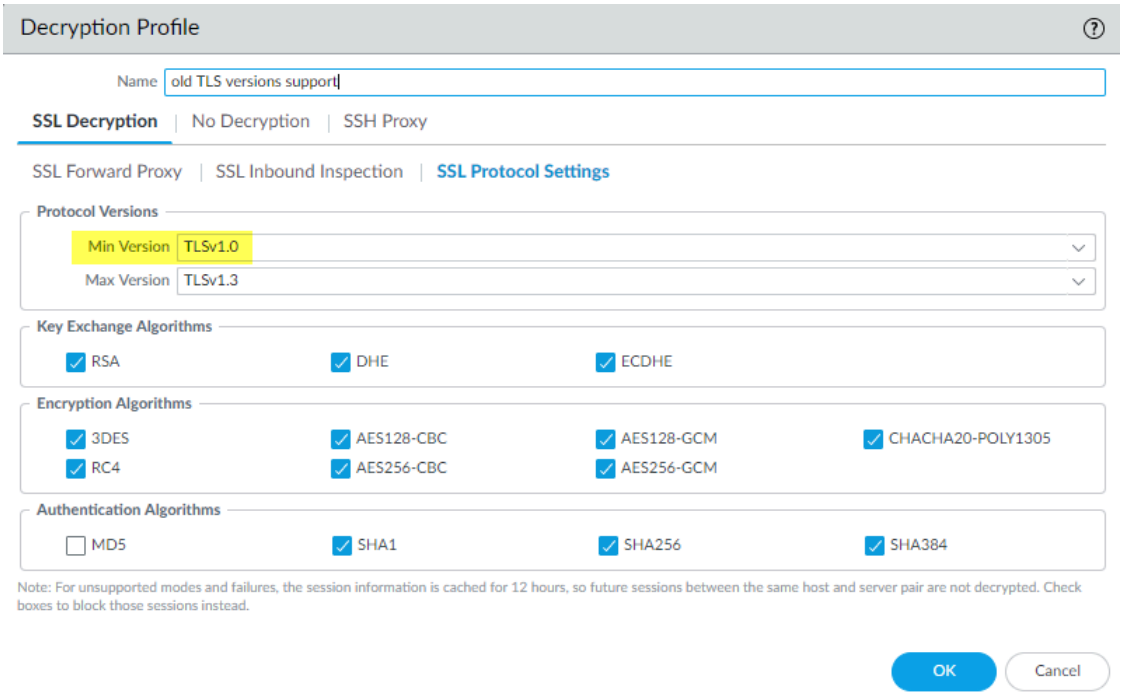
解密日誌顯示，控制流量的解密原則的名稱為 **Inner Eye**，主機的名稱為 **hq-screening.mt.com**。現在我們知道了使用 TLSv1.0 的網站，而且可以查看解密原則

 ©2024 Palo Alto Networks, Inc.

（**Policies**（原則） > **Decryption**（解密））來查找控制流量的解密設定檔，並瞭解為什麼允許該流量：



我們看到，與該原則關聯的解密設定檔支援舊 **TLS** 版本。查看設定檔（**Objects**（物件） > **Decryption**（解密） > **Decryption Profile**（解密設定檔））並查看 SSL 通訊協定設定來確切瞭解設定檔允許的流量：



設定檔允許 TLSv1.0 流量。接下來要做的是，確定是想要允許存取該網站（是否出於業務目的需要存取？）還是想要封鎖它。

©2024 Palo Alto Networks, Inc.

導致防火牆允許使用安全性較低之通訊協定的流量的另一種常見情況是未解密該流量。當您篩選 TLSv1.0 流量的解密日誌時，如果 **Proxy Type**（**Proxy** 類型）欄包含值 **No Decrypt**（不解密），則由不解密原則控制流量，因此防火牆不會解密或檢查流量。如果您不想允許使用弱通訊協定，請修改解密設定檔，以封鎖 TLSv1.0 流量。

您可以使用多種方式來篩選解密日誌，以查找使用弱通訊協定的應用程式和網站，例如：

- 使用查詢 **(tls_version eq TLS1.0)** 篩選成功和不成功的 TLSv1.0 交握，而不是僅篩選成功的 TLSv1.0 交握。
- 使用查詢 **(tls_version eq TLS1.0)** 和 **(err_index neq 'None')** 僅篩選不成功的 TLSv1.0 交握。
- 使用查詢 **(tls_version leq tls1.1)** 篩選所有安全性較低的通訊協定（TLSv1.1 和之前版本）。

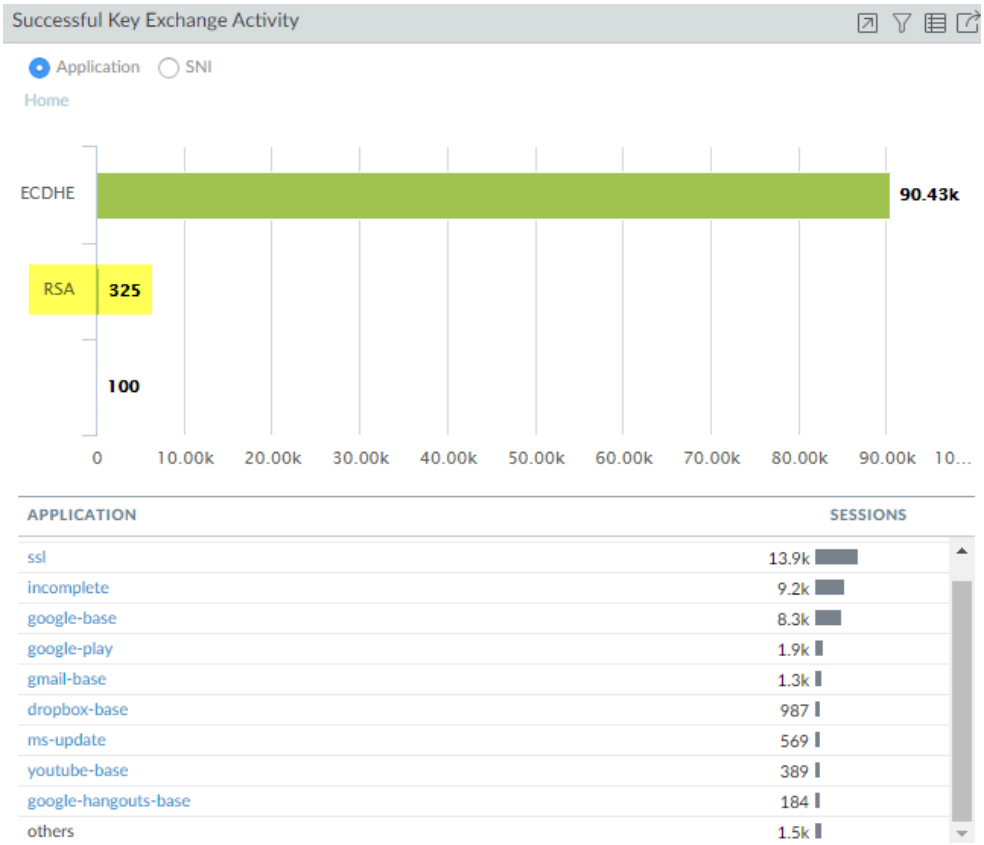
如果您想要篩選其他 TLS 版本的日誌，僅需使用另一 TLS 版本替換 **TLS1.0** 或 **TLS1.1**。

3. 確定對使用弱 TLS 通訊協定的網站採取什麼動作。
   - 如果您不需要出於業務目的存取該網站，最安全的動作是編輯控制流量的解密原則和解密設定檔，封鎖對該網站的存取。解密日誌 **Policy Name**（原則名稱）欄提供了原則名稱，解密原則顯示了附加的解密設定檔（**Options**（選項）頁簽）。
   - 如果需要出於業務目的存取該網站，則考慮建立僅套用至該網站（或該網站和其他相似網站）的解密原則和解密設定檔，並封鎖使用安全性較低之通訊協定的所有其他流量。

©2024 Palo Alto Networks, Inc.

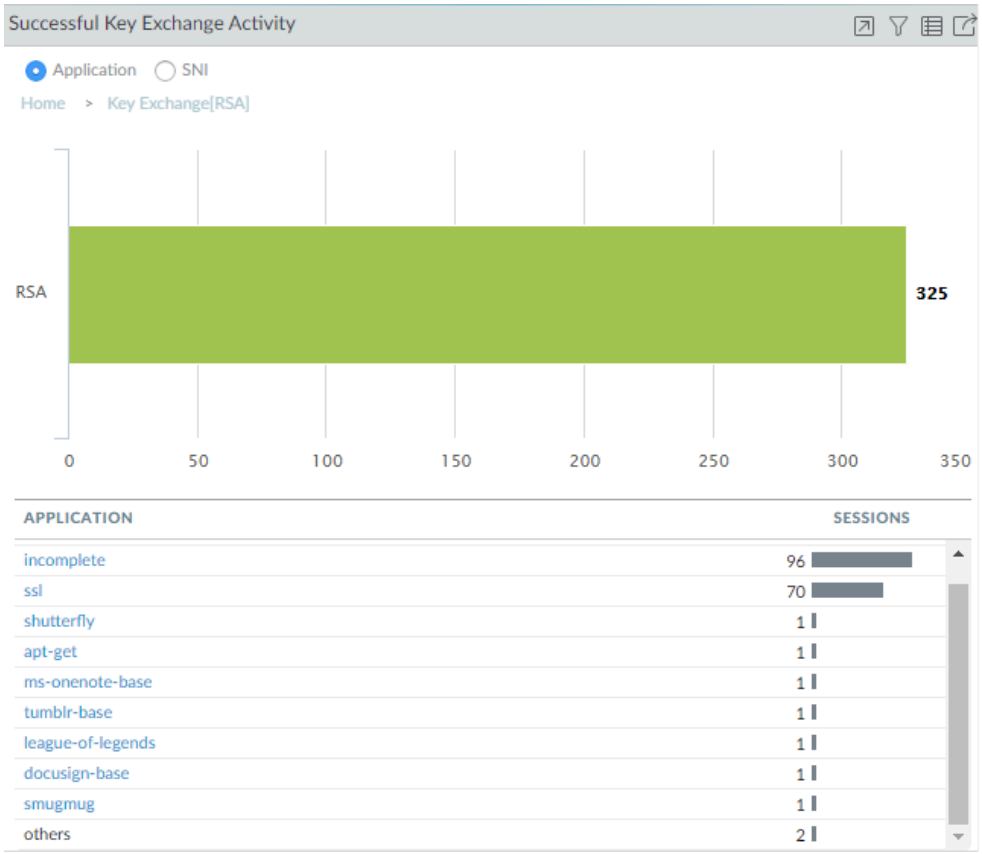
金鑰交換—標識使用安全性較低的金鑰交換演算法的流量。

1. 首先檢查應用程式控管中心 (ACC)，以查看防火牆允許的金鑰交換演算法（**ACC** > **SSL Activity**（**SSL** 活動） > **Successful Key Exchange Activity**（成功金鑰交換活動））並獲取活動的整體檢視。



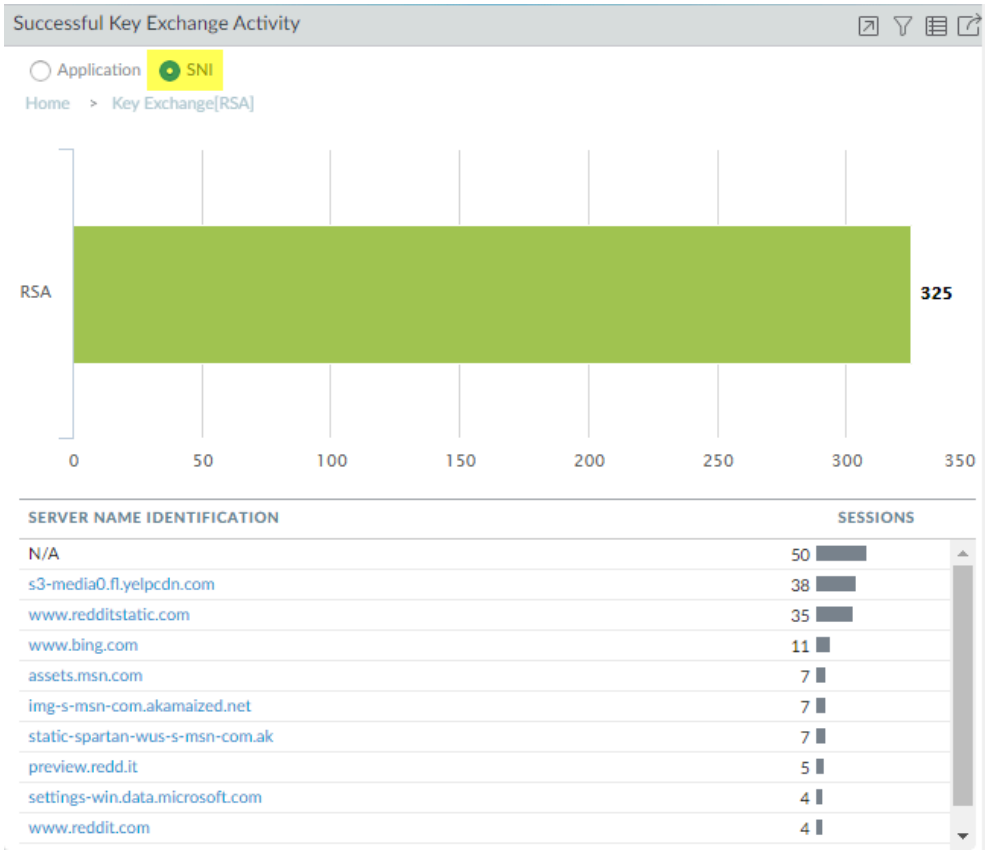
大多數金鑰交換使用安全的 ECDHE 金鑰交換演算法。但是，某些金鑰交換工作階段使用安全性較低的 RSA 演算法，而另一些則使用另一種金鑰演算法。要開始調查使用 RSA 金鑰交換的流量，例如，按一下數字 **325** 以向下鑽研資料。

©2024 Palo Alto Networks, Inc.



此向下鑽研顯示使用 RSA 金鑰交換的應用程式。我們還可以按一下 **SNI** 選項按鈕以根據 SNI 檢視 RSA 金鑰交換：

©2024 Palo Alto Networks, Inc.



有了這些資訊，我們可以轉到日誌以獲取有關 RSA 金鑰交換使用情況的更多背景資訊。

2. 轉到解密日誌（**Monitor**（監控） > **Logs**（日誌） > **Decryption**（解密）），並使用查詢 **(tls_keyxchg eq RSA)** 篩選出使用 RSA 金鑰交換的解密工作階段：

(tls_keyxchg eq RSA)

RECEIVE TIME	SESSION ID	APPLICATION	SOURCE ADDRESS	DESTINATION ADDRESS	TLS VERSION	ERROR INDEX	ERROR	POLICY NAME
06/04 09:29:50	92884	ssl	172.30.200.30	185.31.128.129	TLS1.2	None		No Decrypt
06/04 09:29:50	92887	ssl	172.30.200.30	185.31.128.129	TLS1.2	None		No Decrypt
06/04 09:29:44	92998	ssl	172.30.200.30	74.120.19.22	TLS1.2	None		No Decrypt
06/04 09:29:24	92882	ssl	172.30.200.30	192.132.33.46	TLS1.2	Certificate	Expired server certificate	No Decrypt
06/04 09:29:24	92880	ssl	172.30.200.30	192.132.33.46	TLS1.2	Certificate	Expired server certificate	No Decrypt
06/04 09:29:23	92874	ssl	172.30.200.30	192.132.33.46	TLS1.2	Certificate	Expired server certificate	No Decrypt
06/04 09:29:23	92873	ssl	172.30.200.30	192.132.33.46	TLS1.2	Certificate	Expired server certificate	No Decrypt
06/03 22:30:11	36522	vudu	172.30.100.155	208.79.221.210	TLS1.2	None		Big Brother
06/03 20:08:57	16896	ssl	172.30.200.30	66.117.28.86	TLS1.2	None		No Decrypt
06/03 20:08:22	16947	ssl	172.30.200.30	185.31.128.129	TLS1.2	None		No Decrypt

從日誌的 **Policy Name**（原則名稱）欄中，我們看到 **No Decrypt**（不解密）解密原則控制著大多數使用 RSA 金鑰交換的流量，且可以推斷出防火牆不解密該流量且在未經檢查的情況下允許該流量。因為流量沒有解密，防火牆不能識別應用程式並將其列為 **ssl**。如果

©2024 Palo Alto Networks, Inc.

您不想允許使用 RSA 金鑰交換的流量，請修改附加到控制該流量的解密原則的解密設定檔。

您可以新增到查詢中，以進一步篩選在 ACC 或第一個解密日誌查詢中看到的特定 SNI 或應用程式的結果。

3. 確定對使用安全性較低的金鑰交換演算法的流量採取什麼動作。

   封鎖存取使用安全性較低的金鑰交換通訊協定的網站，除非您出於業務目的需要存取它們。對於此類網站，考慮建立僅套用至該網站（或該網站和其他相似網站）的解密原則和解密設定檔，並封鎖使用安全性較低的金鑰交換演算法的所有其他流量。

使用解密日誌來識別使用安全性較低的舊版驗證演算法的工作階段。

篩選解密日誌以識別安全性較低的舊版驗證演算法。

例如，要識別使用 SHA1 演算法的所有工作階段，請使用查詢 **(tls_auth eq SHA)**：

(tls_auth eq SHA)

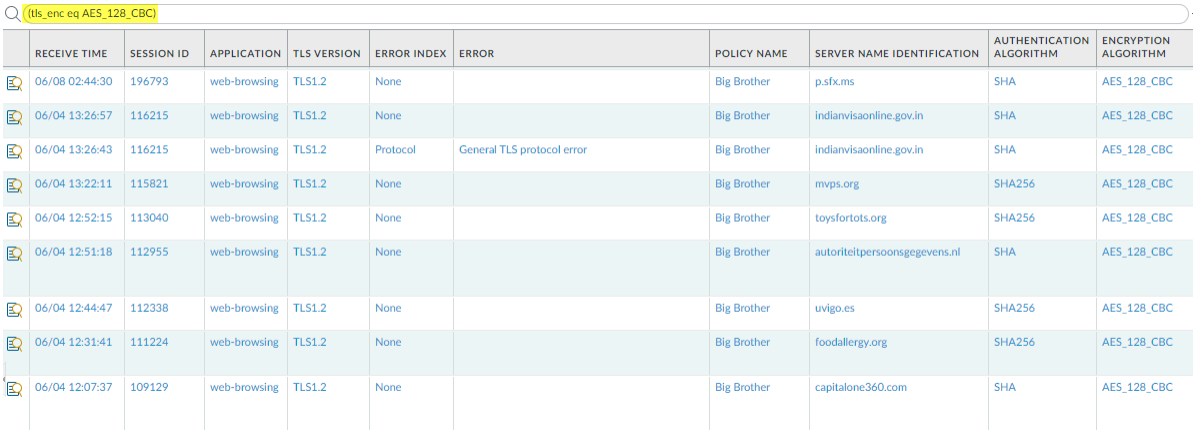
	RECEIVE TIME	SESSION ID	APPLICATION	TLS VERSION	ERROR INDEX	ERROR	POLICY NAME	SERVER NAME IDENTIFICATION	AUTHENTICATION ALGORITHM
	06/08 23:12:02	213635	ssl	TLS1.2	None		No Decrypt		SHA
	06/08 11:16:02	203438	incomplete	TLS1.2	None		Big Brother	p.sfx.ms	SHA
	06/08 11:16:02	203439	web-browsing	TLS1.2	None		Big Brother	p.sfx.ms	SHA
	06/08 11:15:01	203437	web-browsing	TLS1.2	None		Big Brother	p.sfx.ms	SHA
	06/08 02:45:32	196795	incomplete	TLS1.2	None		Big Brother	p.sfx.ms	SHA
	06/08 02:44:30	196794	web-browsing	TLS1.2	None		Big Brother	p.sfx.ms	SHA
	06/08 02:44:30	196793	web-browsing	TLS1.2	None		Big Brother	p.sfx.ms	SHA
	06/04 13:38:36	117329	web-browsing	TLS1.2	None		Big Brother	inegi.org.mx	SHA
	06/04 13:35:01	116980	web-browsing	TLS1.2	None		Big Brother	rupress.org	SHA

您可以新增到查詢以進一步向下鑽研結果。例如，您可以新增特定的 SNI、金鑰交換版本（例如篩選還使用 RSA 金鑰交換的 SHA1 工作階段）、TLS 版本或在解密日誌欄中找到的任何其他指標。

©2024 Palo Alto Networks, Inc.

使用解密日誌來識別使用特定加密演算法的工作階段。

例如，要識別使用 AES-128-CBC 加密演算法的所有工作階段，請使用查詢 **(tls_enc eq AES_128_CBC)**：



RECEIVE TIME	SESSION ID	APPLICATION	TLS VERSION	ERROR INDEX	ERROR	POLICY NAME	SERVER NAME IDENTIFICATION	AUTHENTICATION ALGORITHM	ENCRYPTION ALGORITHM
06/08 02:44:30	196793	web-browsing	TLS1.2	None		Big Brother	p.sfx.ms	SHA	AES_128_CBC
06/04 13:26:57	116215	web-browsing	TLS1.2	None		Big Brother	indianvisaonline.gov.in	SHA	AES_128_CBC
06/04 13:26:43	116215	web-browsing	TLS1.2	Protocol	General TLS protocol error	Big Brother	indianvisaonline.gov.in	SHA	AES_128_CBC
06/04 13:22:11	115821	web-browsing	TLS1.2	None		Big Brother	mvps.org	SHA256	AES_128_CBC
06/04 12:52:15	113040	web-browsing	TLS1.2	None		Big Brother	toysfortots.org	SHA256	AES_128_CBC
06/04 12:51:18	112955	web-browsing	TLS1.2	None		Big Brother	autoriteitpersoonsgegevens.nl	SHA	AES_128_CBC
06/04 12:44:47	112338	web-browsing	TLS1.2	None		Big Brother	uvigo.es	SHA256	AES_128_CBC
06/04 12:31:41	111224	web-browsing	TLS1.2	None		Big Brother	foodallergy.org	SHA256	AES_128_CBC
06/04 12:07:37	109129	web-browsing	TLS1.2	None		Big Brother	capitalone360.com	SHA	AES_128_CBC

您可以新增到查詢以進一步向下鑽研結果。

用於查找其他舊版加密演算法的查詢範例包括：**(tls_enc eq DES_CBC)**、**(tls_enc eq 3DES_EDE_CBC)** 和 **(tls_enc eq DES40_CBC)**。

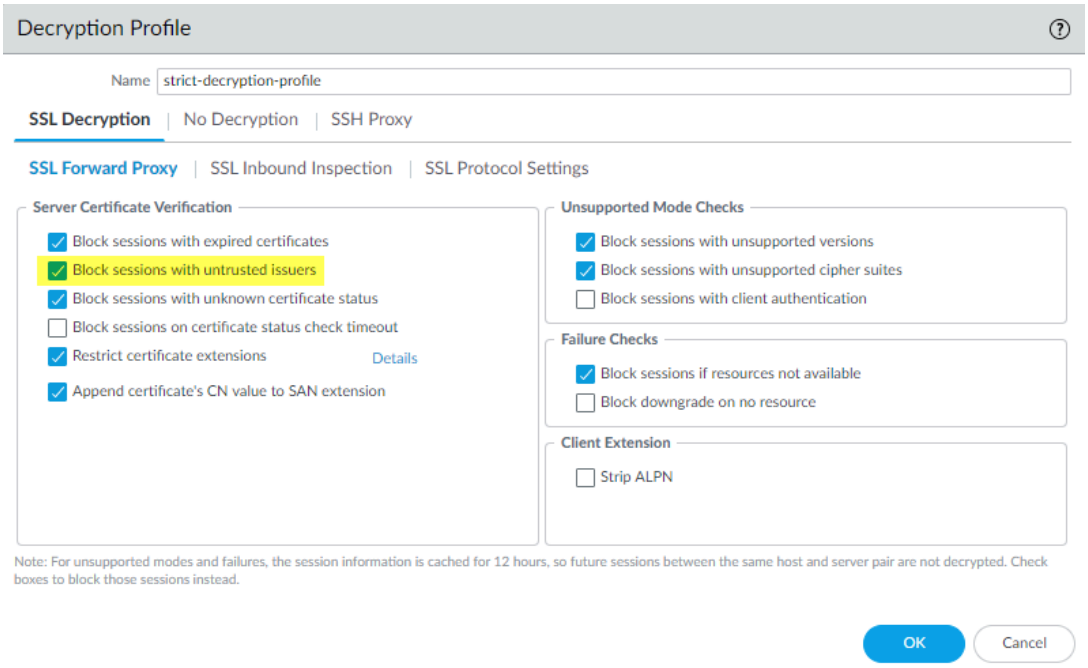
使用此方法和日誌篩選建立器來建立查詢，以調查交涉的 ECC 曲線以及在解密日誌中找到的任何其他資訊。

識別不受信任的 CA 憑證

封鎖存取具有不受信任 CA 憑證和由不受信任根 CA 自我簽署之憑證的網站是最佳做法，因為具有不受信任 CA 的網站可能帶來中間人攻擊、重播攻擊或其他惡意活動。

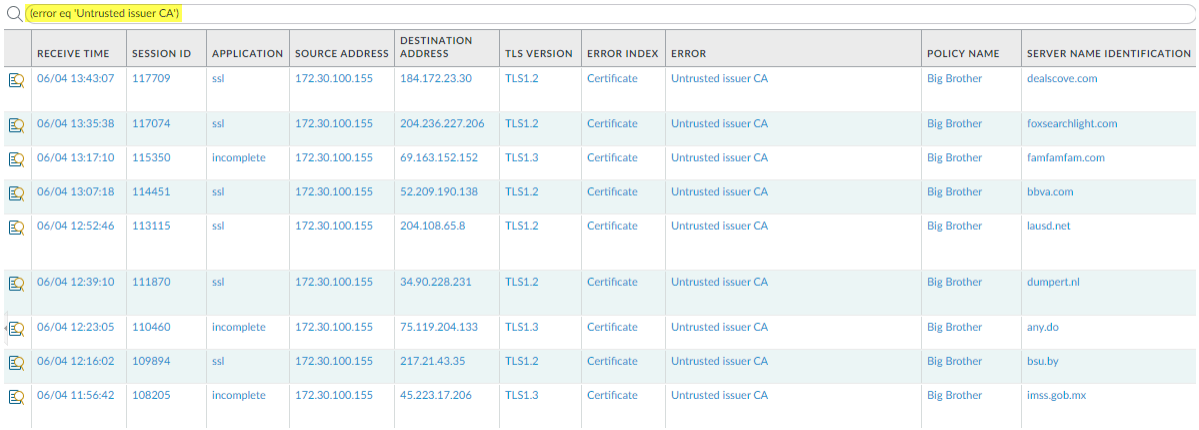
©2024 Palo Alto Networks, Inc.

STEP 1 | 確保在正向 Proxy 解密設定檔中封鎖具有不受信任簽發者的工作階段（**Objects**（物件） > **Decryption**（解密） > **Decryption Profiles**（解密設定檔））以封鎖具有不受信任 CA 的網站。



當在解密設定檔中封鎖具有不受信任簽發者的工作階段時，解密日誌（**Monitor**（監控） > **Logs**（日誌） > **Decryption**（解密））會記錄錯誤。

STEP 2 | 使用查詢 **(error eq 'Untrusted issuer CA')** 篩選日誌以識別因撤銷憑證而失敗的工作階段。



RECEIVE TIME	SESSION ID	APPLICATION	SOURCE ADDRESS	DESTINATION ADDRESS	TLS VERSION	ERROR INDEX	ERROR	POLICY NAME	SERVER NAME IDENTIFICATION
06/04 13:43:07	117709	ssl	172.30.100.155	184.172.23.30	TLS1.2	Certificate	Untrusted issuer CA	Big Brother	dealscove.com
06/04 13:35:38	117074	ssl	172.30.100.155	204.236.227.206	TLS1.2	Certificate	Untrusted issuer CA	Big Brother	foxsearchlight.com
06/04 13:17:10	115350	incomplete	172.30.100.155	69.163.152.152	TLS1.3	Certificate	Untrusted issuer CA	Big Brother	famfamfam.com
06/04 13:07:18	114451	ssl	172.30.100.155	52.209.190.138	TLS1.2	Certificate	Untrusted issuer CA	Big Brother	bbva.com
06/04 12:52:46	113115	ssl	172.30.100.155	204.108.65.8	TLS1.2	Certificate	Untrusted issuer CA	Big Brother	lausd.net
06/04 12:39:10	111870	ssl	172.30.100.155	34.90.228.231	TLS1.2	Certificate	Untrusted issuer CA	Big Brother	dumpert.nl
06/04 12:23:05	110460	incomplete	172.30.100.155	75.119.204.133	TLS1.3	Certificate	Untrusted issuer CA	Big Brother	any.do
06/04 12:16:02	109894	ssl	172.30.100.155	217.21.43.35	TLS1.2	Certificate	Untrusted issuer CA	Big Brother	bsu.by
06/04 11:56:42	108205	incomplete	172.30.100.155	45.223.17.206	TLS1.3	Certificate	Untrusted issuer CA	Big Brother	imss.gob.mx

STEP 3 | （選用）在 Qualys SSL Labs 網站仔細檢查憑證到期日期。

在 **Hostname**（主機名稱）欄位中輸入伺服器的主機名稱（解密日誌的 **Server Name Identification**（伺服器名稱識別）欄），然後 **Submit**（提交）以檢視主機的憑證資訊。

©2024 Palo Alto Networks, Inc.

疑難排解過期的憑證

如果您遵循解密最佳做法，在正向 Proxy 解密設定檔或不解密設定檔中封鎖憑證過期的工作階段，當伺服器提供過期的憑證時，防火牆就會封鎖該工作階段。但是，如果您出於業務原因需要存取的網站允許其憑證過期，指向該網站的連線可能會被封鎖，且您可能並不知道原因。

您可以使用解密日誌來檢查過期憑證以及檢查即將到期的憑證，這樣您就可以瞭解情況，並採取適當動作。

STEP 1 | 使用查詢 **(error eq 'Expired server certificate')** 篩選解密日誌找出過期的憑證。


(error eq 'Expired server certificate')

RECEIVE TIME	SESSION ID	APPLICATION	SOURCE ADDRESS	DESTINATION ADDRESS	TLS VERSION	ERROR INDEX	ERROR	SERVER NAME IDENTIFICATION	POLICY NAME
06/04 16:19:49	121352	incomplete	172.30.100.10	34.225.62.221	TLS1.3	Certificate	Expired server certificate	www.stanford.edu	Big Brother
06/04 13:43:26	117747	incomplete	172.30.100.155	104.197.149.89	TLS1.3	Certificate	Expired server certificate	phone.com	Big Brother
06/04 13:41:03	117572	incomplete	172.30.100.155	208.117.9.16	TLS1.3	Certificate	Expired server certificate	netcarshow.com	Big Brother
06/04 13:38:51	117379	ssl	172.30.100.155	69.172.200.184	TLS1.2	Certificate	Expired server certificate	royal.gov.uk	Big Brother
06/04 13:36:27	117150	ssl	172.30.100.155	107.21.104.61	TLS1.2	Certificate	Expired server certificate	www.uthscsa.edu	Big Brother
06/04 13:34:53	117004	incomplete	172.30.100.155	66.115.56.251	TLS1.3	Certificate	Expired server certificate	gunsamerica.com	Big Brother
06/04 13:33:17	116853	incomplete	172.30.100.155	34.107.140.234	TLS1.3	Certificate	Expired server certificate	skiplagged.com	Big Brother
06/04 13:32:45	116798	ssl	172.30.100.155	104.236.4.58	TLS1.2	Certificate	Expired server certificate	uploading.com	Big Brother
06/04 13:31:28	116655	incomplete	172.30.100.155	35.186.201.59	TLS1.3	Certificate	Expired server certificate	shared.com	Big Brother
06/04 13:29:32	116507	ssl	172.30.100.155	147.139.136.53	TLS1.2	Certificate	Expired server certificate	beautynesia.id	Big Brother
06/04 13:28:56	116426	incomplete	172.30.100.155	45.55.105.190	TLS1.3	Certificate	Expired server certificate	designbundles.net	Big Brother

此查詢會識別產生過期伺服器憑證錯誤的伺服器。防火牆會因為憑證過期而封鎖對這些伺服器的存取。

STEP 2 | （選用）在 Qualys SSL Labs 網站仔細檢查憑證到期日期。

在 **Hostname**（主機名稱）欄位中輸入伺服器的主機名稱（解密日誌的 **Server Name Identification**（伺服器名稱識別）欄），然後 **Submit**（提交）以檢視主機的憑證資訊。

©2024 Palo Alto Networks, Inc.

STEP 3 | 使用可以識別即將到來的憑證結束日期的查詢來篩選解密日誌（**Monitor**（監控） > **Logs**（日誌） > **Decryption**（解密））以找出即將到期的憑證。

例如，如果今天的日期為 2020 年 2 月 1 日，您想給自己兩個月的時間來評估和準備，以防網站不更新其憑證，請查詢解密日誌以找出在 2020 年 4 月 1 日或之前到期的憑證 (**`notafter leq '2020/4/01' )`**)：

(notafter leq '2020/4/01')

RECEIVE TIME	APPLICATION	POLICY NAME	PROXY TYPE	SERVER NAME IDENTIFICATION	ROOT STATUS	TLS VERSION	CERTIFICATE START DATE	CERTIFICATE END DATE
01/09 14:25:38	incomplete	Test 2	Forward	a4.espncdn.com	uninspected	TLS1.2	2019/11/14 04:44:43	2020/02/13 04:44:43
01/09 14:25:38	incomplete	Test 2	Forward	a2.espncdn.com	uninspected	TLS1.2	2019/11/14 04:44:43	2020/02/13 04:44:43
01/09 14:25:38	incomplete	Test 2	Forward	a3.espncdn.com	uninspected	TLS1.2	2019/11/14 04:44:43	2020/02/13 04:44:43
01/09 14:25:38	incomplete	Test 2	Forward	a.espncdn.com	uninspected	TLS1.2	2019/11/14 04:44:43	2020/02/13 04:44:43

Certificate End Date（憑證結束日期）欄顯示憑證到期的確切日期。

STEP 4 | 確定對憑證過期的網站採取的動作。

- 如果您無需出於業務目的存取該網站，最安全的動作是繼續封鎖對該網站的存取。
- 如果您出於業務目的需要存取該網站，請採取以下動作之一：
  - 聯絡憑證過期之網站的管理員，並通知其更新或續訂憑證。
  - 建立僅適於于憑證過期且您出於業務目的需要存取之網站的解密原則，以及允許憑證過期之網站的解密設定檔。不要將該原則套用至您不需要出於業務目的存取的任何網站。當網站更新其憑證後，將其從原則中移除。

疑難排解撤銷的憑證

撤銷的憑證不再有效。它可能表明網站存在安全問題，以及憑證不可信，但也有可能出於良性原因而撤銷憑證。

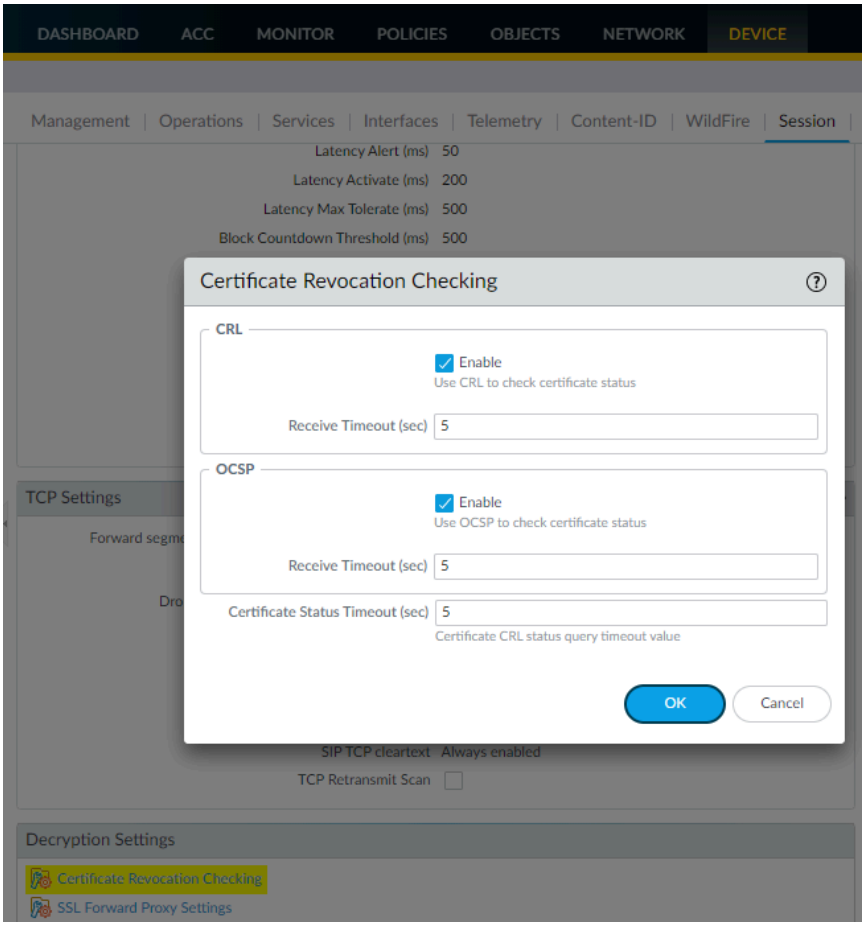
不要相信撤銷的憑證；啟用憑證撤銷檢查以拒絕對存取具有已撤銷憑證的網站。

要丟棄具有已撤銷憑證的工作階段並對已撤銷憑證進行疑難排解，您需要啟用憑證撤銷檢查。如果不啟用憑證撤銷檢查，則防火牆不會檢查撤銷的憑證，您就不會知道網站是否具有已撤銷憑證。

©2024 Palo Alto Networks, Inc.

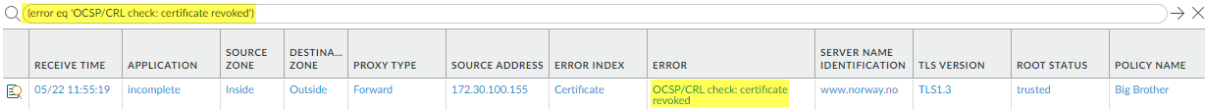
STEP 1 | 如果尚未啟用憑證撤銷檢查，請啟用。

1. 轉至 **Device**（裝置） > **Setup**（設定） > **Session**（工作階段） > **Decryption Settings**（解密設定）。
2. 啟用 OCSP 和 CRL 憑證檢查。



如果您在正向 Proxy 解密設定檔中在憑證狀態檢查逾時時封鎖工作階段，並擔心 5 秒鐘的時間不夠，可能導致太多工作階段因逾時而被封鎖，請將 **Receive Timeout (sec)**（接收逾時（秒））設定為更長的時間。

STEP 2 | 使用查詢 **(error eq 'OCSP/CRL check: certificate revoked')** 篩選解密日誌（**Monitor**（監控） > **Logs**（日誌） > **Decryption**（解密））以找出憑證撤銷錯誤。



STEP 3 | （選用）在 Qualys SSL Labs 網站仔細檢查憑證到期日期。

在 **Hostname**（主機名稱）欄位中輸入伺服器的主機名稱（解密日誌的 **Server Name Identification**（伺服器名稱識別）欄），然後 **Submit**（提交）以檢視主機的憑證資訊。

©2024 Palo Alto Networks, Inc.

疑難排解釘選的憑證

憑證釘選會強制用戶端應用程式根據已知複本驗證伺服器的憑證，以確保憑證確實來自該伺服器。釘選憑證的意圖是防止中間人 (MITM) 攻擊，在該攻擊中，用戶端和伺服器之間的裝置會使用其他憑證替換伺服器憑證。

儘管這會防止惡意行為者攔截和操縱連線，這也會阻止正向 proxy 解密，因為防火牆會建立一個模擬憑證而不是將伺服器憑證提供給用戶端。正向 proxy 不會建立一個直接連線用戶端和伺服器的工作階段，而是建立兩個工作階段，一個在用戶端和防火牆之間，另一個在防火牆和伺服器之間。這樣可以與用戶端建立信任關係，以便防火牆可以解密和檢查流量。

但是，當憑證被釘選時，防火牆將無法解密流量，因為用戶端不接受防火牆的模擬憑證—用戶端僅接受釘選到應用程式的憑證。

STEP 1 | 使用查詢 **(error contains 'UnknownCA')** 篩選解密日誌（**Monitor**（監控） > **Logs**（日誌） > **Decryption**（解密））以找出釘選的憑證。

(error contains 'UnknownCA')

RECEIVE TIME	APPLICATION	PROXY TYPE	SOURCE ADDRESS	ERROR INDEX	ERROR	SERVER NAME IDENTIFICATION	TLS VERSION	POLICY NAME
06/02 11:25:30	incomplete	Forward	172.30.115.10	Certificate	Received fatal alert UnknownCA from client. CA Issuer URL: h	d.dropbox.com	TLS1.2	Big Brother
06/02 11:16:53	incomplete	Forward	172.30.115.10	Certificate	Received fatal alert UnknownCA from client. CA Issuer URL: h	telemetry.dropb...	TLS1.2	Big Brother
06/02 11:15:52	incomplete	Forward	172.30.115.10	Certificate	Received fatal alert UnknownCA from client. CA Issuer URL: h	dl-debug.dropbox.c...	TLS1.2	Big Brother
06/02 11:15:52	incomplete	Forward	172.30.115.10	Certificate	Received fatal alert UnknownCA from client. CA Issuer URL: h	dl-debug.dropbox.c...	TLS1.2	Big Brother
06/02 11:09:03	incomplete	Forward	172.30.115.10	Certificate	Received fatal alert UnknownCA from client. CA Issuer URL: h	d.dropbox.com	TLS1.2	Big Brother
06/02 11:09:03	incomplete	Forward	172.30.115.10	Certificate	Received fatal alert UnknownCA from client. CA Issuer URL: h	d.dropbox.com	TLS1.2	Big Brother
06/02 10:51:34	incomplete	Forward	172.30.115.10	Certificate	Received fatal alert UnknownCA from client. CA Issuer URL: h	d.dropbox.com	TLS1.2	Big Brother

當應用程式無法驗證伺服器憑證時，會產生 TLS 錯誤代碼（警示）。不同的應用程式可能使用不同的錯誤代碼來表明釘選憑證。釘選憑證的最常見錯誤指標是 UnknownCA 和 BadCertificate。在執行 **(error contains 'UnknownCA')** 查詢後，執行查詢 **(error contains 'BadCertificate')** 以擷取更多釘選憑證錯誤。

您可以使用 *Wireshark* 或其他封包分析器來仔細檢查錯誤。在 *TLS* 交握後，立即查找中斷連線的用戶端，以確認這是釘選憑證問題。

STEP 2 | 確定就釘選憑證採取什麼動作。

如果您無需出於業務目的存取，可以讓防火牆繼續封鎖存取。如果您需要存取，則可以透過將其新增至 SSL 解密排除清單（**Device**（裝置） > **Certificate Management**（憑證管理） > **SSL Decryption Exclusion**（SSL 解密排除））來出於技術原因將伺服器排除在解密之外。

防火牆會對 SSL 解密排除清單上的網站繞過解密。防火牆不會檢查該流量，但該流量將得到允許。

©2024 Palo Alto Networks, Inc.

啟動解密功能的免費授權

解密 SSH 流量以及 SSL 流量（SSL 網際網路流量或至內部伺服器的 SSL 流量）無需使用授權。但是，您必須啟動免費授權才可啟用 Decryption Mirroring（解密鏡像）。啟動免費授權這一要求，可確保只有在經核准人員特意啟動相關授權後才能使用此功能。

在 *PAN-OS 10.1* 中，解密代理程式功能和免費授權已被網路封包代理程式取代（請參閱網路管理員指南），除了解密的 *TLS* 流量之外，還將代理程式的功能擴展到非解密 *TLS* 流量和非 *TLS* 流量。網路封包代理程式授權也可從客戶支援入口網站免費下載並安裝。

請依照 Palo Alto Networks 客戶支援入口網站上的相關步驟啟動解密鏡像功能授權。

STEP 1 | 登入客戶支援入口網站。

STEP 2 | 在左側導覽窗格上，選取 **Assets**（資產） > **Devices**（裝置）。

STEP 3 | 找到要在其中啟用解密連接埠鏡像的裝置，然後選取 **Actions**（動作）（鉛筆圖示）。

STEP 4 | 在 Activate Licenses（啟動授權）下方，選取 **Activate Feature License**（啟動功能授權）。

STEP 5 | 選取您要啟動免費授權的功能：**Decryption Port Mirror**（解密連接埠鏡像）。

STEP 6 | **Agree and Submit**（同意並提交）。

STEP 7 | 在防火牆上安裝解密鏡像授權。

1. 選取 **Device**（裝置） > **Licenses**（授權）。
2. 按一下 **Retrieve license keys from the license server**（從授權伺服器擷取授權金鑰）。
3. 確認 **Decryption Port Mirror**（解密連接埠鏡像）授權此時已作用於防火牆。
4. 重新啟動防火牆（**Device**（裝置） > **Setup**（設定） > **Operations**（操作））。在防火牆重新載入之前，解密連接埠鏡像不可用於設定。

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

服務品質

Quality of Service (服務品質) (QoS) 是一組在網路上運作的技術，保證在有限的網路功能下仍能夠可靠地執行高優先權的應用程式與流量。QoS 技術透過對網路流量中特定的流向進行差異性處理與容量分配來達成。這讓網路管理員能指派處理流量的順序，及指派可負擔流量的頻寬量。

Palo Alto Networks Application Quality of Service (服務品質) (QoS) 提供適合網路的基本 QoS，並擴大將 QoS 提供給應用程式與使用者。

下列主題可協助您瞭解與設定 Palo Alto Networks 以應用程式為基礎的 QoS：

- QoS 概要介紹
- QoS 概念
- 設定 QoS
- 設定虛擬系統的 QoS
- 根據 DSCP 分類強制執行 QoS
- QoS 使用案例

使用 Palo Alto Networks 產品比較工具檢視防火牆型號上支援的 QoS 功能。選取兩個以上的產品型號，然後按一下 **Compare Now**（立即比較）以檢視每個型號的 QoS 功能（例如，您可以檢查防火牆型號是否支援子介面上的 QoS，如果支援，則為其 QoS 可啟用的子介面數上限）。

執行 PAN-OS 7.0 或更新發行版本的 PA-7000 Series、PA-5400 Series、PA-5200 Series、PA-3400 Series、PA-3200 Series 以及 PA-400 Series 防火牆支援彙總乙太網路 (AE) 介面上的 QoS。

QoS 概要介紹

使用 QoS 為網路流量的品質安排優先順序並加以調整。您可以指派處理封包的順序並配置頻寬，確保能夠為所選的流量、應用程式與使用者採用可負擔得起的偏好處理方式，並得到最佳的效能層級。

受 QoS 實作影響的服務品質量值有頻寬 (最大傳輸率)、輸送量 (真正的傳輸率)、延遲與抖動 (延遲的變化)。能夠形成與控制這些服務品質量值的能力，讓 QoS 對於高頻寬、即時流量而言特別重要，例如 voice over IP (VoIP)、視訊會議，以及對於延遲與抖動高度敏感的隨選視訊。此外，使用 QoS 可達成如下的成果：

- 安排網路與應用程式流量的優先順序、保證重要流量的高優先權，或限制非必要的流量。
- 達成不同子網路、類別或網路中的使用者之間有等同的頻寬份額。
- 在外部和/或內部配置頻寬能讓 QoS 套用到上傳與下載流量，或僅套用到上傳或下載流量。
- 確保客戶及企業環境中能產生收益的流量其延遲性低。
- 設定應用程式的流量設定檔，確保能有效運用頻寬。

想要在 Palo Alto Networks 防火牆上實作 QoS，要從支援完整 QoS 解決方案的三個主要設定元件開始：QoS 設定檔、QoS 原則及設定 QoS 輸出介面。QoS 設定工作中的每個元件都能促使處理層面擴大，將流量流向最佳化及安排優先順序，並根據可設定的參數配置與確保頻寬。

QoS 流量流向圖中顯示的流量自來源流出、然後由具備 QoS 功能的防火牆形成，最後被設定優先順序其傳遞到其目的地。

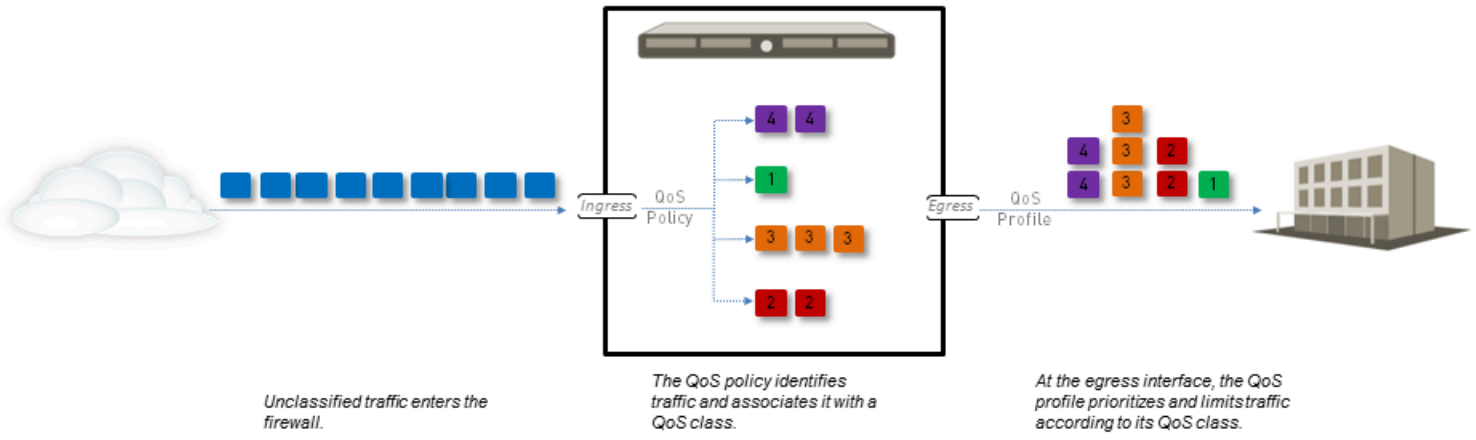


圖 **6: QoS** 流量流向

QoS 設定選項可讓您控制流量流向，並在流向的不同點定義流量。QoS 流量流向圖中顯示了可設定選項在何處定義流量流向。QoS 原則規則可用於定義要接受 QoS 處理的流量並向該流量指派一個 QoS 類別。符合流量然後在退出實體介面時根據 QoS 設定檔類別設定形成。

每個 QoS 組態元件可影響彼此，QoS 組態選項可用於建立完整且精確的 QoS 實作，或用於減少管理員的工作。

©2024 Palo Alto Networks, Inc.

當佇列填充速度快於清空速度時，裝置有兩種選擇來丟棄流量。它可以等到佇列已滿並在封包到達時簡單地丟棄它們（尾部丟棄），或者它可以偵測到初期擁塞並根據與佇列平均深度相關的概率函數主動開始丟棄封包。這種技術稱為隨機早期丟棄 (RED)。PAN-OS 使用加權 RED (WRED) 演算法。

每一個防火牆型號都支援可為 QoS 設定的最大連接埠數目。請參閱規格表以得知您的防火牆型號，或使用產品比較工具在單一頁面上檢視兩個以上防火牆的 QoS 功能支援。

©2024 Palo Alto Networks, Inc.

QoS 概念

下列主題可幫助您瞭解 Palo Alto Networks 防火牆上 QoS 設定的不同元件與機制：

- 應用程式與使用者適用的 QoS
- QoS 原則
- QoS 設定檔
- QoS 類別
- QoS 優先順序佇列
- QoS 頻寬管理
- QoS 輸出介面
- 純文字與通道流量適用的 QoS

應用程式與使用者適用的 QoS

Palo Alto Networks 防火牆提供基本的 QoS，可根據網路或子網路控制離開防火牆的流量，並擴展 QoS 的能力使其也會根據應用程式與使用者分類及形成流量。Palo Alto Networks 防火牆將 App-ID 和 使用者-ID 功能與 QoS 設定整合，以此來提供此功能。QoS 組態中提供 App-ID 與 User-ID 項目，用於識別您網路中特定的應用程式與使用者，讓您能夠輕鬆地指定要為其管理及/或保證頻寬的應用程式與使用者。

QoS 原則

使用 QoS 原則規則定義接收 QoS 處理的流量（無論是優先處理或頻寬限制），並指派該流量服務的 QoS 等級。

根據下列條件，定義比對流量的 QoS 原則規則：

- 應用程式與應用程式群組。
- 來源區域、來源位置與來源使用者。
- 目的地區域與目的地位址。
- 限制在特定 TCP 和/或 UDP 連接埠號碼的服務與服務群組。
- URL 類別，包括自訂 URL 類別。
- Differentiated Services Code Point（差異服務字碼指標，DSCP）與 Type of Service（服務類型，ToS）值，用於指出流量要求的服務層級，例如高優先順序或盡力傳遞。

您無法將 *DSCP* 代碼點或 *QoS* 套用至 *SSL* 正向 *Proxy*、*SSL* 輸入檢查和 *SSH Proxy* 流量。

設定多個 QoS 政策規則（**Policies**（政策） > **QoS**）將不同類型的流量與不同的服務 QoS 類別建立關聯。

©2024 Palo Alto Networks, Inc.

由於 QoS 在流量輸出防火牆時被強制執行，因此，在防火牆強制執行所有其他安全性原則規則（包括網路位址轉譯 (NAT) 規則）之後，QoS 原則規則會套用於流量。如果要對基於源的流量應用 QoS 處理方法，請確保在 QoS 原則規則中指定 NAT 後的來源位址（不得使用 NAT 前的來源位址）。

QoS 設定檔

使用 QoS 設定檔定義單個設定檔內包含的多達八個 QoS 類別的值。

使用 QoS 設定檔，您可以為 QoS 類別定義 QoS 優先順序佇列和 QoS 頻寬管理。每個 QoS 設定檔可用於為多達八個 QoS 類別設定個別頻寬及優先順序設定，並為八個類別一起配置總頻寬。將 QoS 設定檔（或多個 QoS 設定檔）附加到實體介面，以將所定義的優先順序及頻寬設定套用至退出該介面的流量。

防火牆提供預設的 QoS 設定檔。設定檔中定義的預設定檔與類別沒有預先定義的最大或保證頻寬限制。

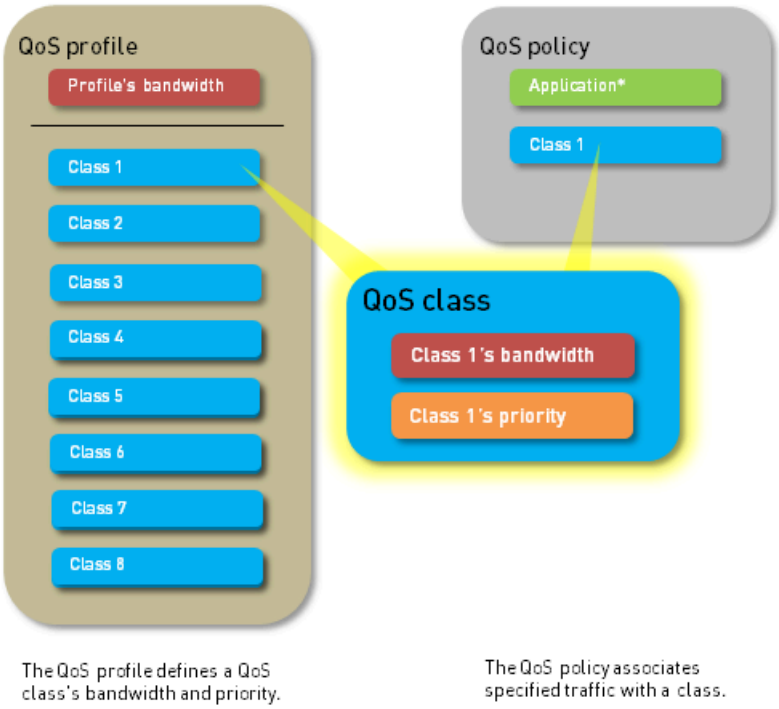
若要為 QoS 類別定義優先順序和頻寬設定，請參閱步驟新增 QoS 設定檔。

QoS 類別

QoS 類別可決定符合 QoS 原則規則的流量的優先順序及頻寬。您可使用 QoS 設定檔定義 QoS 類別。單一 QoS 設定檔中最多有 8 個可定義的 QoS 類別。除非另有設定，不符合 QoS 類別的流量會被指派至類別 4。

QoS 優先順序佇列及 QoS 頻寬管理為 QoS 設定的基本機制，需在 QoS 類別定義內設定（請參閱步驟 4）。對於每個 QoS 類別，您可為符合流量設定優先順序（即時、高、中和低）以及最大和保證頻寬。QoS 優先順序佇列與頻寬管理可決定流量的順序，以及流量進出網路時如何處理流量。

©2024 Palo Alto Networks, Inc.



QoS 優先順序佇列

可針對 QoS 類別強制執行四個優先順序之一：即時、高、中與低。系統會為符合 QoS 原則規則的流量指派與該規則關聯的 QoS 類別，防火牆還會根據 QoS 類別優先順序處理符合流量。傳出流量中的封包會根據其優先順序排入佇列中，直到網路準備好處理封包為止。此優先順序佇列可用於確保重要的流量、應用程式或使用者具有優先權。即時優先順序通常用於對於延遲特別敏感的應用程式，例如音訊與視訊應用程式。

QoS 頻寬管理

使用 QoS 頻寬管理，可以控制網路上的流量流向，讓流量不超過網路流量（而造成網路擁塞），還可以為某些類型的流量以及應用程式與使用者配置頻寬。利用 QoS，您可以在狹窄或廣泛的範圍內為流量強制執行頻寬。您可使用 QoS 設定檔為個別 QoS 類別設定頻寬限制，並為全部八個 QoS 類別設定總綜合頻寬。在設定 QoS 的步驟中，您可將 QoS 設定檔附加至實體介面，以針對退出介面的流量強制執行頻寬設定——針對符合該 QoS 類別（QoS 類別指派給符合 QoS 政策規則的流量）的流量強制執行個別 QoS 類別設定，設定檔的總頻寬限制可套用至所有純文字流量、源自來源介面及來源子網路、所有通道流量以及個別通道介面的特定純文字流量。您可以將多個設定檔規則新增至單個 QoS 介面，以向退出該介面的流量套用不同的頻寬設定。

以下欄位支援 QoS 頻寬設定：

©2024 Palo Alto Networks, Inc.

- **Egress Guaranteed**（輸出保證）—針對符合流量而保証的頻寬量。超過輸出保證頻寬時，防火牆將盡力傳送流量。保證但未使用的頻寬繼續對所有流量保持可用。根據 QoS 組態，您可針對單個 QoS 類別、所有或部分純文字流量以及所有或部分通道流量提供頻寬保證。

  範例：

  Class 1 流量具有 5 Gbps 的輸出保證頻寬，這意味著 5 Gbps 可用但不為 Class 1 流量保留。若 Class 1 流量不使用或僅使用部分保證頻寬，則剩餘頻寬可由其他類別的流量使用。但是，在高流量期，5 Gbps 的頻寬絕對可用於 Class 1 流量。在擁塞期內，任何 Class 1 流量會盡力超過 5 Gbps。

- 輸出最大—針對符合流量配置的總頻寬。防火牆會丟棄超出所設最大值的流量。根據 QoS 組態，可以針對所有或部分純文字流量、所有或部分通道流量以及退出 QoS 介面的所有流量設定 QoS 類別的頻寬上限。

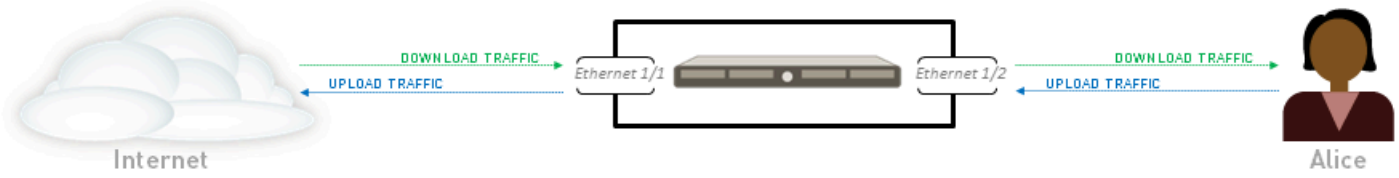
  附加至介面的 *QoS* 設定檔的累計保證頻寬不得超過為介面配置的總頻寬。

若要為 QoS 類別定義頻寬設定，請參閱步驟新增 QoS 設定檔。若要隨後將這些頻寬設定套用於純文字及通道流量並為 QoS 介面設定整體頻寬限制，請參閱步驟在實體介面上啟用 QoS。

QoS 輸出介面

針對已識別為需進行 QoS 處理的流量，在其輸出介面上啟用 QoS 設定檔能使 QoS 組態更為完備。QoS 流量的輸入介面是流量進入防火牆的介面。QoS 流量的輸出介面是流量離開防火牆的介面。QoS 在流量的輸出介面上一律啟用且強制執行。QoS 設定中的輸出介面是防火牆的對外或對內介面，這視接收 QoS 處理的流量其流向而定。

例如在公司網路中，如果您限制員工從特定網站下載的流量，則 QoS 設定中的輸出介面便是防火牆的內部介面，因為流量流向是從網際網路通過防火牆，最後流到您的公司網路。相反的，當限制員工上傳到同一個網站的流量時，QoS 設定中的輸出介面便是防火牆的外部介面，因為您限制的流量流向是從公司網路通過防火牆，最後流向網際網路。



- The egress interface for Alice's download traffic is Ethernet 1/2. To prioritize or limit her download traffic, Alice enables QoS on Ethernet 1/2.
- The egress interface for Alice's upload traffic is Ethernet 1/1. To prioritize or limit her upload traffic, Alice enables QoS on Ethernet 1/1.

由於 QoS 在流量輸出防火牆時被強制執行，因此，在防火牆強制執行所有其他安全性原則規則（包括網路位址轉譯 (NAT) 規則）之後，QoS 原則規則會套用於流量。如果要基於來源對流量進行 QoS 處理，則必須在 QoS 政策規則中指定 NAT 前來源位址（如 NAT 前來源 IP、NAT 前來

©2024 Palo Alto Networks, Inc.

源區域、NAT 前目的地 IP、NAT 後目的地區域）。如果要對來源流量進行 QoS 處理，請勿使用 NAT 後來源位址設定 QoS 政策。

瞭解更多有關如何為要接受 QoS 處理的應用程式確定輸出介面的資訊。

純文字與通道流量適用的 QoS

至少，啟用 QoS 介面需要您選取預設 QoS 設定檔，用於定義從介面輸出之純文字流量的頻寬與優先順序設定。但是，在設定或修改 QoS 介面時，您可以將精確的 QoS 設定套用至傳出的純文字流量和通道流量。可針對通道流量、個別通道介面和/或源自不同來源介面和來源子網路的純文字流量，強制執行 QoS 優先處理和頻寬限制。在 Palo Alto Networks 防火牆上，通道流量是指通道介面流量，尤其是通道模式中的 IPSec 流量。

©2024 Palo Alto Networks, Inc.

設定 QoS

請依照以下步驟設定 Quality of Service (服務品質，QoS)，包括建立 QoS 設定檔、建立 QoS 原則及啟用介面上的 QoS。

在設定 QoS 政策規則之前，確保您瞭解 IPv4 位址集會被視為 IPv6 位址集的子集，原則中對此進行了詳細說明。

STEP 1 | 確定要使用 QoS 來管理的流量。

此範例顯示如何使用 QoS 限制網頁瀏覽。

選取 **ACC** 以檢視 **Application Command Center**（應用程式監測中心）頁面。使用 **ACC** 頁面上的設定與圖表可檢視 [應用程式]、[URL 篩選]、[資安威脅]、[資料篩選] 及 [HIP 比對] 的相關趨勢與流量。

按一下任何應用程式名稱即可顯示詳細的應用程式資訊。

©2024 Palo Alto Networks, Inc.

STEP 2 | 為要接受 QoS 處理的應用程式確定輸出介面。

流量的輸出介面取決於流量流向。如果您正在形成傳入流量，則輸出介面是對內的介面。如果您正在形成傳出流量，則輸出介面是對外的介面。

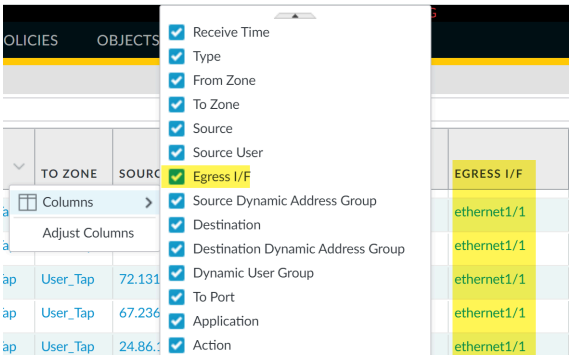
選取 **Monitor**（監控） > **Logs**（日誌） > **Traffic**（流量） 可檢視流量日誌。

若要篩選且僅顯示特定應用程式的日誌：

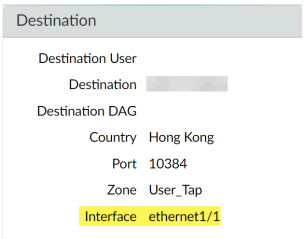
- 如果有顯示應用程式的項目，請按一下應用程式欄中加上底線的連結，然後按一下提交圖示。
- 如果未顯示應用程式的項目，請按一下新增日誌圖示，然後搜尋該應用程式。

流量日誌中的 Egress 介面會顯示每個應用程式的 **Egress I/F**（**Egress** 介面）。如果依預設未顯示 **Egress I/F**（**Egress** 介面）欄，請依照下列步驟顯示此欄：

- 按一下任何欄標題將該欄新增至此日誌：



- 按一下任何項目左側的望遠鏡圖示可顯示詳細的日誌，包括目的地區段中會列出應用程式的輸出介面：



 ©2024 Palo Alto Networks, Inc.

STEP 3 | 新增 QoS 原則規則。

QoS 原則規則可定義接受 QoS 處理的流量。防火牆會向符合原則規則的流量指派 QoS 服務類別。

由於 *QoS* 在流量輸出防火牆時被強制執行，因此，在防火牆強制執行所有其他安全性原則規則（包括網路位址轉譯 *(NAT)* 規則）之後，*QoS* 原則規則會套用於流量。如果要基於來源對流量進行 *QoS* 處理，則必須在 *QoS* 政策規則中指定 *NAT* 前來源位址（如 *NAT* 前來源 *IP*、*NAT* 前來源區域、*NAT* 前目的地 *IP*、*NAT* 後目的地區域）。如果要對來源流量進行 *QoS* 處理，請勿使用 *NAT* 後來源位址設定 *QoS* 政策。

1. 選取 **Policies**（原則） > **QoS**，然後 **Add**（新增） 新的原則規則。
2. 在一般頁籤上，為 QoS 原則規則指定一個描述性名稱.。
3. 根據 **Source**（來源）、**Destination**（目的地）、**Application**（應用程式）、**Service/URL Category**（服務/URL 類別）以及 **DSCP/ToS** 值（**DSCP/ToS** 設定可允許您 根據 DSCP 分類執行 QoS），指定接受 QoS 處理的流量。

   例如，選取 **Application**（應用程式）頁籤，按一下 **Add**（新增），並選取 **web-browsing**（網頁瀏覽）以將 QoS 套用到網頁瀏覽流量。
4. （選用）繼續定義其他參數。例如，選取 **Source**（來源）並 **Add**（新增）**Source User**（來源使用者），來為特定使用者的 Web 流量提供 QoS。
5. 選取 **Other Settings**（其他設定）並將 **QoS Class**（**QoS** 類別）指派給符合該原則規則的流量。例如，將 Class 2 指派給 user1 的網頁流量。
6. 按一下 **OK**（確定）。

©2024 Palo Alto Networks, Inc.

STEP 4 | 新增 QoS 設定檔。

使用 QoS 設定檔，可以定義流量可接受的八類服務，包括優先順序，然後啟用 QoS 頻寬管理。

按一下 QoS 設定檔名稱便可編輯任何現有的 QoS 設定檔，包括預設值。

1. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **QoS Profile**（**QoS** 設定檔），然後 **Add**（新增） 新的設定檔。
2. 輸入描述性的 **Profile Name**（設定檔名稱）。
3. 為 QoS 設定檔設定總頻寬限制：
   - 輸入 **Egress Max**（輸出最大值）以設定 QoS 設定檔的整體頻寬配置。
   - 輸入 **Egress Guaranteed**（輸出保證）值以設定 QoS 設定檔的保證頻寬。

   任何超過 *Egress Guaranteed*（輸出保證）值的流量為盡力超過，但不保證一定超過。保證但未使用的頻寬繼續對所有流量保持可用。

   您可以設定 **Egress Guaranteed**（輸出保證值）和 **Egress Max**（輸出最大值），以 Mbps 為單位或以百分比的形式。以百分比設定這些值時，應考慮下列注意事項：

   - 每個類別的 **Egress Guaranteed**（輸出保證值）(%) 是使用 **Egress Max**（輸出最大值）而非 **Egress Guaranteed**（輸出保證值）計算得出。
   - 設定檔 **Egress Guaranteed**（輸出保證值）等於每個類別的 **Egress Guaranteed**（輸出保證值）(%) 的總和乘以 **Egress Max**（輸出最大值）。

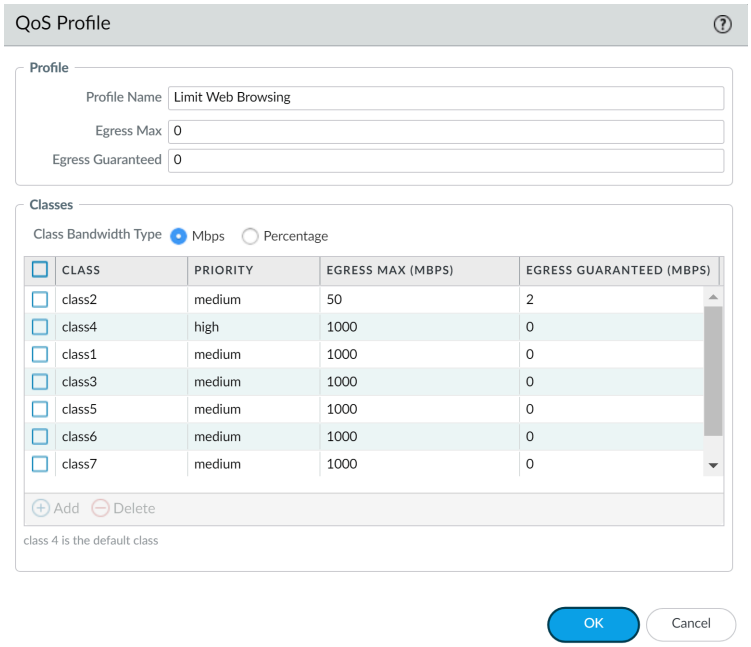
   例如：**Egress Max**（輸出最大值）設定為 100Mbps。為類別 1 設定的保證百分比為 30#，類別 2 為 20%，類別 3為 5#，類別 4 為 1#。此設定產生的總百分比保證值為 56#。在此情況下，設定檔 為 56Mbps（56% x **Egress Max**（輸出最大值））。這也意味著類別 1

©2024 Palo Alto Networks, Inc.

Egress Guaranteed（輸出保證值） 為 30Mbps，類別 2 **Egress Guaranteed**（輸出保證值） 為 20Mbps，以此類推。

4. 在類別區段中，指定如何處理最多 8 個 QoS 類別：
   1. **Add**（新增）一個類別至 QoS 設定檔。
   2. 為類別選取 **Priority**（優先順序）：即時、高、中或低。
   3. 為指派給每個 QoS 類別的流量輸入 **Egress Max**（輸出最大）和 **Egress Guaranteed**（輸出保證）頻寬。
5. 按一下 **OK**（確定）。

在下列範例中，QoS 設定檔 Limit Web Browsing 會限制 Class 2 流量，讓其最大頻寬為 50 Mbps，保證頻寬為 2 Mbps。



 ©2024 Palo Alto Networks, Inc.

STEP 5 | 啟用實體介面上的 QoS。

這一步中包括為獨特 QoS 處理選擇純文字及通道流量的選項。

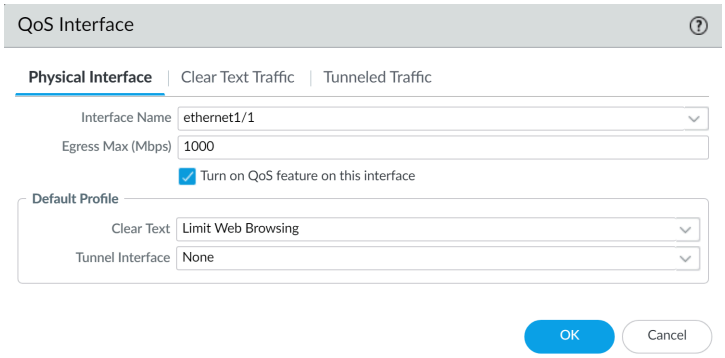
檢閱產品規格摘要，以檢查確認您正在使用的防火牆型號是否支援啟用子介面上的 *QoS*。

1. 選取 **Network**（網路） > **QoS**，然後 **Add**（新增） QoS 介面。
2. 選取 **Physical Interface**（實體介面）並選擇要在其上啟用 QoS 的介面的 **Interface Name**（介面名稱）。

   在此範例中，乙太網路 1/1 是網頁瀏覽流量的輸出介面（請參閱步驟 2）。
3. 為退出此介面的所有流量設定 **Egress Max**（輸出最大）頻寬。

   最佳做法是一律為 *QoS* 介面定義 *Egress Max*（輸出最大）值。確保附加至介面的 *QoS* 設定檔的累計保證頻寬不超過為介面配置的總頻寬。
4. 選取 **Turn on QoS feature on this interface**（開啟此介面上的 **QoS** 功能）。
5. 在預設設定檔區段中，選取要套用至退出實體介面的所有 **Clear Text**（純文字）流量的 QoS 設定檔。
6. （選用）選取要套用至退出介面的所有通道流量的預設 QoS 設定檔。

例如，在 ethernet 1/1 上啟用 QoS，並套用您為 QoS 設定檔 Limit Web Browsing（步驟 4）定義的頻寬及優先順序設定，以用作純文字輸出流量的預設設定。



1. （選用）繼續定義更多細微設定，以提供純文字與通道流量適用的 QoS。**Clear Text Traffic**（純文字流量）頁籤和 **Tunneled Traffic**（通道流量）頁籤上完成的設定會自動覆寫實體介面頁籤上的純文字及通道流量的預設設定檔設定。
   - 選取 **Clear Text Traffic**（純文字流量）並：
     - 為純文字流量設定 **Egress Guaranteed**（輸出保證）與 **Egress Max**（輸出最大）頻寬。
     - 按一下 **Add**（新增）並套用 QoS 設定檔，以根據來源介面和子網路強制執行純文字流量。

©2024 Palo Alto Networks, Inc.

（僅限 *PA-3200* 系列、*PA-5200* 系列、*PA-5450* 防火牆和 *PA-7000* 系列）在設定 *QoS* 政策規則時，如果該規則會套用至特定子介面，則還必須選取目的地介面。

- 選取 **Tunneled Traffic**（通道流量）並：
  - 為通道流量設定 **Egress Guaranteed**（輸出保證）與 **Egress Max**（輸出最大）頻寬。
  - 按一下 **Add**（新增）並將 QoS 設定檔附加至單一通道介面。

2. 按一下 **OK**（確定）。

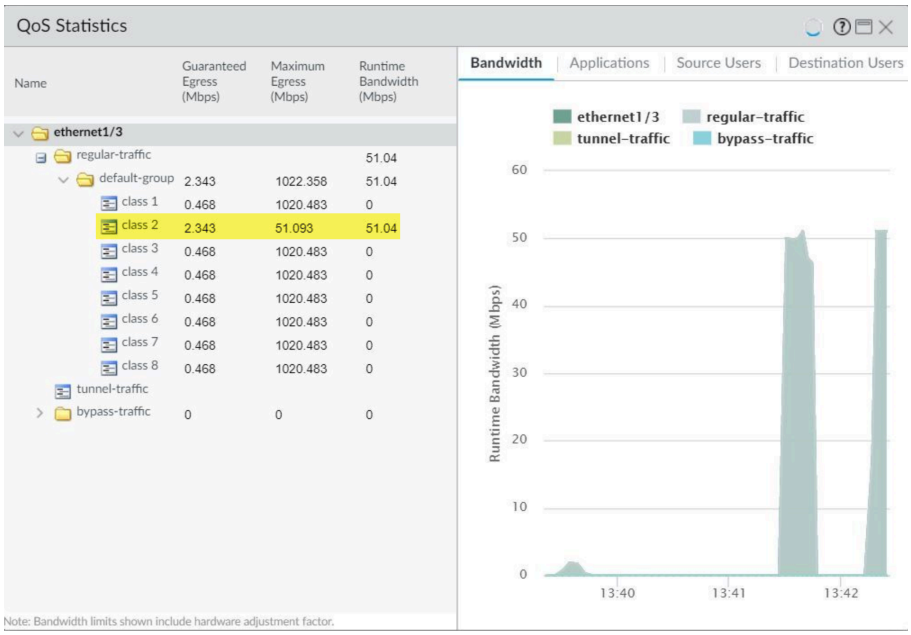
STEP 6 | Commit（提交）您的變更。

按一下 **Commit**（交付）。

STEP 7 | 驗證 QoS 組態。

選取 **Network**（網路）> **QoS**，然後選取 **Statistics**（統計資料）以檢視 QoS 頻寬、所選 QoS 類別的使用中工作階段，以及所選 QoS 類別的使用中應用程式。

例如，檢視 QoS 已啟用的乙太網路 1/3 統計資料：



Class 2 流量限制為 2.343 Mbps 的保證頻寬，以及 51.093 Mbps 的最大頻寬。

繼續按一下頁籤可顯示應用程式、來源使用者、目的地使用者、安全性規則及 QoS 規則的進一步資訊。

在 ***QoS Statistics***（***QoS*** 統計資料）視窗上顯示的頻寬限制包括硬體調整係數。

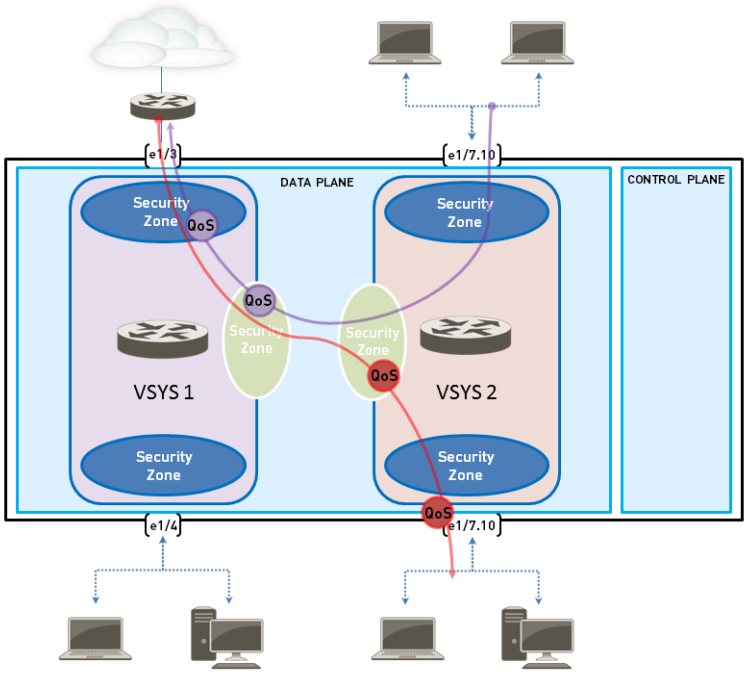
©2024 Palo Alto Networks, Inc.

設定虛擬系統的 QoS

在 Palo Alto Networks 防火牆內所設定的單一或數個虛擬系統可設定 QoS。由於虛擬系統是獨立的防火牆，因此必須為單一虛擬系統單獨設定 QoS。

為虛擬系統設定 QoS 與在實體防火牆上設定 QoS 類似，不同處在於為虛擬系統設定 QoS 需要指定流量的來源與目的地。由於虛擬系統可無須設定實體邊界而存在，且在虛擬環境中流量可以橫跨多個虛擬系統，因此對於為單一虛擬系統控制與形成流量而言，指定流量的來源與目的地區域和介面是必要的。

下列範例的防火牆上設有兩個虛擬系統。VSYS 1 (紫色) 與 VSYS 2 (紅色) 皆有設定 QoS，以針對其對應的紫線 (VSYS 1) 與紅線 (VSYS 2) 所指示的兩個不同的流量向設定優先順序或加以限制。QoS 節點指示流量中的點比對至 QoS 原則並具有服務的 QoS 等級指派，並在稍後指示當流量輸出防火牆時形成流量的點。



有關虛擬系統的資訊及其設定方法，請參閱虛擬系統 。

STEP 1 | 確認每個虛擬系統皆與適當的介面、虛擬路由器與安全性區域建立關聯。

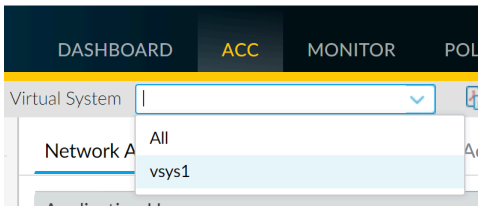
- 若要檢視已設定的介面，請選取 **Network**（網路） > **Interface**（介面）。
- 若要檢視設定好的區域，可選取 **Network**（網路） > **Zones**（區域）。
- 若要檢視所定義虛擬路由器的資訊，可選取 **Network**（網路） > **Virtual Routers**（虛擬路由器）。

©2024 Palo Alto Networks, Inc.

STEP 2 | 識別要套用 QoS 的流量。

選取 **ACC** 以檢視 **Application Command Center**（應用程式監測中心）頁面。使用 **ACC** 頁面上的設定與圖表可檢視 [應用程式]、[URL 篩選]、[資安威脅]、[資料篩選] 及 [HIP 比對] 的相關趨勢與流量。

若要檢視特定虛擬系統的資訊，請從 **Virtual System**（虛擬系統）下拉式清單中選取該虛擬系統：



按一下任何應用程式名稱即可顯示詳細的應用程式資訊。

©2024 Palo Alto Networks, Inc.

STEP 3 | 針對您識別為需要 QoS 處理的應用程式找出其輸出介面。

在虛擬系統環境中，QoS 會套用到虛擬系統上流量 輸出點的流量。QoS 流量的輸出點可以與實體介面或是區域建立關聯，這視虛擬系統的設定與 QoS 原則而定。

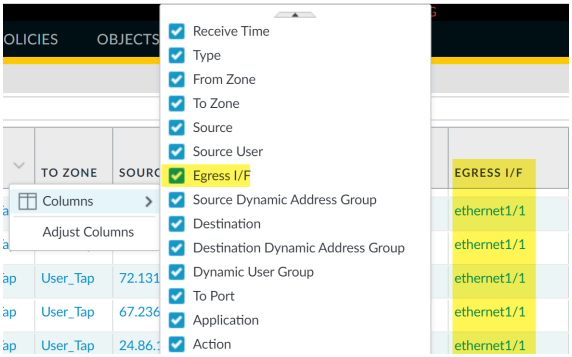
此範例顯示如何限制 vsys 1 上的網頁瀏覽流量。

選取 **Monitor**（監控） > **Logs**（日誌） > **Traffic**（流量） 可檢視流量日誌。每個項目都有選項可顯示直欄，以提供在虛擬系統環境中設定 QoS 的必要資訊：

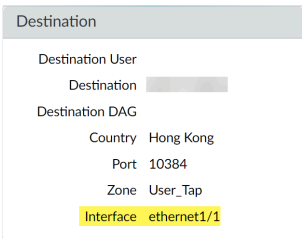
- 虛擬系統
- 輸出介面
- 輸入介面
- 來源區域
- 目的地區域

如果依預設未顯示直欄，請依照下列步驟顯示：

- 按一下任何欄標題將該欄新增至此日誌：



- 在來源與目的地區段中，按一下任何項目左側的望遠鏡圖示可顯示詳細的日誌，日誌中會包含應用程式的 Egress 介面及 **Source**（來源）與 **Destination**（目的地區域）：



例如，來自 VSYS 1 的網頁瀏覽流量其輸入介面是乙太網路 1/2，輸出介面是乙太網路 1/1，來源區域信任，目的地區域不信任。

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 建立 QoS 設定檔。

按一下 QoS 設定檔名稱便可編輯任何現有的 QoS 設定檔，包括預設值。

1. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **QoS Profile**（**QoS** 設定檔），然後按一下 **Add**（新增） 以開啟 QoS Profile（QoS 設定檔）對話方塊。
2. 輸入描述性的 **Profile Name**（設定檔名稱）。
3. 輸入 **Egress Max**（輸出最大）以設定 QoS 設定檔的整體頻寬配置。
4. 輸入 **Egress Guaranteed**（**Egress** 保證）以設定 QoS 設定檔的保證頻寬。

   任何超過 *QoS* 設定檔其輸出保證限制的流量為盡力超過，但不保證一定超過。
5. 在 **QoS Profile**（**QoS** 設定檔）的 [類別] 區段中指定如何處理最多 8 個 QoS 類別：
   1. 按一下 **Add**（新增）在 QoS 設定檔中新增類別。
   2. 選取類別的 **Priority**（優先順序）。
   3. 輸入類別的 **Egress Max**（**Egress** 最大），以設定該類別的整體頻寬限制。
   4. 輸入類別的 **Egress Guaranteed**（輸出保證），以設定該類別的保證頻寬。
6. 按一下 **OK**（確定）來儲存 QoS 設定檔。

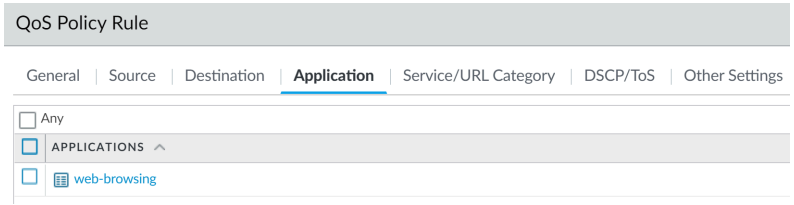
©2024 Palo Alto Networks, Inc.

STEP 5 | 建立 QoS 原則。

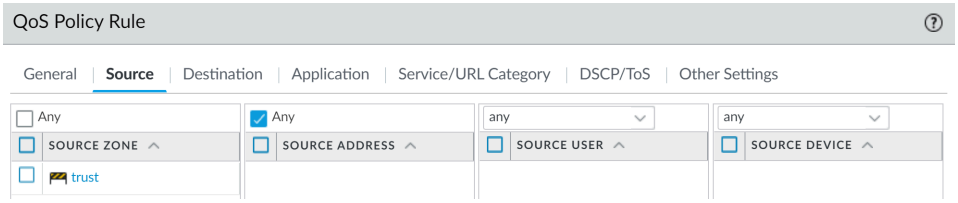
在具有多個虛擬系統的環境中，流量會橫跨多個虛擬系統。有鑑於此，當您為虛擬系統啟用 QoS 時，必須根據來源與目的地區域定義要接收 QoS 處理的流量。如此才可確保會優先處理流量並僅為該虛擬系統形成流量（而非流量可能通過的其他虛擬系統）。

1. 選取 **Policies**（原則）> **QoS**，然後 **Add**（新增） QoS 原則規則。
2. 選取 **General**（一般）並為 QoS 原則規則指定一個描述性 **Name**（名稱）。
3. 指定將套用 QoS 原則規則的流量。使用 **Source**（來源）、**Destination**（目的地）、**Application**（應用程式）與 **Service/URL Category**（服務/**URL**）類別頁籤定義用來識別流量的比對參數。

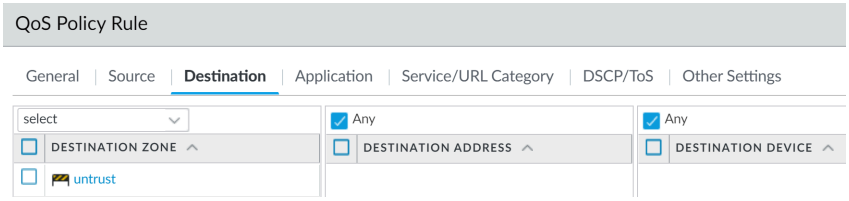
   例如，選取 **Application**（應用程式），然後 **Add**（新增）網頁瀏覽，以將 QoS 原則規則套用到該應用程式：



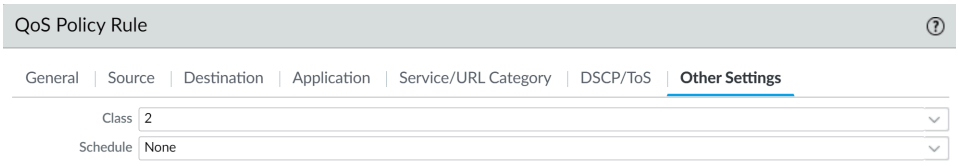
4. 選取 **Source**（來源）並 **Add**（新增）vsys 1 網頁瀏覽流量的來源區域。



5. 選取 **Destination**（目的地）並 **Add**（新增）vsys 1 網頁瀏覽流量的目的地區域。



6. 選取 **Other Settings**（其他設定）並選取要指派給 QoS 原則規則的 **QoS Class**（**QoS** 類別）。例如，將 Class 2 指派給 vsys 1 上的網頁瀏覽流量：



7. 按一下 **OK**（確定）來儲存 QoS 原則規則。

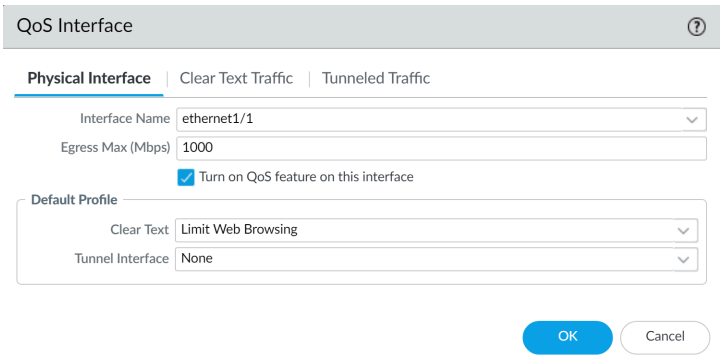
©2024 Palo Alto Networks, Inc.

STEP 6 | 啟用實體介面上的 QoS 設定檔。

最佳做法是一律為 *QoS* 介面定義 ***Egress Max***（輸出最大）值。

1. 選取 **Network**（網路） > **QoS**，然後按一下 **Add**（新增） 以開啟 QoS Interface（QoS 介面）對話方塊。
2. 啟用實體介面上的 QoS：
   1. 在 **Physical Interface**（實體介面）頁籤上，選取要套用 QoS 設定檔至的介面的 **Interface Name**（介面名稱）。

      在此範例中，乙太網路 1/1 是 vsys 1 上網頁瀏覽流量的輸出介面（請參閱步驟 2）。

   2. 選取 **Turn on QoS feature on this interface**（開啟此介面上的 **QoS** 功能）。
3. 在 **Physical Interface**（實體介面）頁籤上，選取預設的 QoS 設定檔以套用到所有的 **Clear Text**（純文字）流量。

   （選用）使用 **Tunnel Interface**（通道介面）欄位將預設的 QoS 設定檔套用至所有的通道流量。
4. （選用）在 **Clear Text Traffic**（純文字流量）頁籤上，為純文字流量設定其他的 QoS 設定：
   - 為純文字流量設定 **Egress Guaranteed**（輸出保證）與 **Egress Max**（輸出最大）頻寬。
   - 按一下 **Add**（新增）將 QoS 設定檔套用到所選的純文字流量，並根據來源介面與來源子網路進一步選取須 QoS 處理的流量（建立 QoS 節點）。
5. （選用）在 **Tunneled Traffic**（通道流量）頁籤上，為通道介面設定其他的 QoS 設定：
   - 為通道流量設定 **Egress Guaranteed**（輸出保證）與 **Egress Max**（輸出最大）頻寬。
   - 按一下 **Add**（新增）將所選的通道介面與 QoS 設定檔建立關聯。
6. 按一下 **OK**（確定）以儲存變更。
7. **Commit**（提交）變更。

©2024 Palo Alto Networks, Inc.

STEP 7 | 驗證 QoS 組態。

- 選取 **Network**（網路） > **QoS**，以檢視 QoS Policies（QoS 原則）頁面。**QoS Policies**（**QoS** 原則）頁面可用來確認 QoS 已啟用並包含 **Statistics**（統計資料）連結。按一下統計資料連結可檢視 QoS 頻寬、所選 QoS 節點或類別的使用中工作階段，以及所選 QoS 節點或類別的使用中應用程式。
- 在多 VSYS 環境中，工作階段無法橫跨多個系統。如果流量通過多個虛擬系統，則會為一個流量流向建立多個工作階段。若要瀏覽在防火牆上執行的工作階段，及檢視套用的 QoS 規則與 QoS 類別，請選取 **Monitor**（監控） > **Session Browser**（工作階段瀏覽器）。

©2024 Palo Alto Networks, Inc.

根據 DSCP 分類強制執行 QoS

Differentiated Services Code Point（差異服務字碼指標，DSCP）是一個封包標頭值，可用於要求流量的高優先順序或盡力傳遞等。在工作階段流量退出防火牆時，以工作階段為基礎的 DSCP 分類可以接受傳入流量的 DSCP 值並使用 DSCP 值標記工作階段。這使工作階段的所有輸入與輸出流量在通過您的網路時可接收連續的 QoS 處理。例如，從外部伺服器返回的輸入流量，現在可以依與防火牆據工作階段開始時偵測到的 DSCP 值最初為輸出流量強制執行的相同 QoS 優先順序來處理。在防火牆與一般使用者之間的網路設備也將會為返回流量（以及工作階段的任何其他輸出或輸入流量）強制執行相同的優先順序。

您無法將 *DSCP* 代碼點或 *QoS* 套用至 *SSL* 正向 *Proxy*、*SSL* 輸入檢查和 *SSH Proxy* 流量。

不同類型的 DSCP 標記表示不同層級的服務：

完成此步驟可讓防火牆以在工作階段一開始偵測到的相同 DSCP 值標記流量（在此範例中，防火牆會以 DSCP AF11 值標記返回流量）。設定 QoS 可讓您在流量輸出防火牆時形成流量，而在安全性規則中啟用此選項可讓其他網路設備干預防火牆和用戶端，以強制執行具 DSCP 標記流量的優先順序。

- **Expedited Forwarding (EF)**（快速式轉送，**EF**）：可用來要求流量的低損失、低延遲和保證頻寬。具有 EF 字碼指標值的封包通常保證以最高優先順序傳遞。
- **Assured Forwarding (AF)**（保證式轉送，**AF**）：可用來提供可靠的應用程式傳遞。具有 AF 字碼指標的封包表示要求流量接收比盡力服務所提供更高優先順序的處理（不過具有 EF 字碼指標封包的優先順序會持續高於具有 AF 字碼指標的封包）。
- **Class Selector (CS)**（類別選取器，**CS**）：可用來提供回溯相容使用 IP 優先順序欄位以標記優先順序流量的網路設備。
- **IP Precedence (ToS)**（**IP** 優先順序，**ToS**）：可讓傳統網路設備用來標記優先順序流量（IP 優先順序標頭欄位是用來指示引入 DSCP 分類前封包的優先順序）。
- **Custom Codepoint**（自訂字碼指標）：輸入 **Codepoint Name**（字碼指標名稱）和 **Binary Value**（二進位值）建立比對至流量的自訂字碼指標。

例如，選取 **Assured Forwarding (AF)**（保證式轉送，**AF**）可確保標記為 AF 字碼指標值的流量，比起標記為接收較低優先順序的應用程式具有較高的優先順序，可獲得可靠的傳遞。請執行以下步驟來啟用以工作階段為基礎的 DSCP 分類。首先根據工作階段一開始偵測到的 DSCP 標記設定 QoS。接著您便能使用與為初始輸出流量強制執行 QoS 相同的 DSCP 值，繼續啟用防火牆標記工作階段的返回流量。

STEP 1 | 執行預備步驟來設定 QoS。

©2024 Palo Alto Networks, Inc.

STEP 2 | 定義流量以根據 DSCP 值接受 QoS 處理。

1. 選取 **Policies**（原則） > **QoS**，然後 **Add**（新增） 或修改現有的 QoS 規則並填入必要欄位。
2. 選取 **DSCP/ToS**，然後選取字碼指標。
3. **Add**（新增）您要為其強制執行 QoS 的 DSCP/ToS 字碼指標。
4. 選取 DSCP/ToS 標記的 **Type**（類型）以讓 QoS 規則比對至流量：

   最佳做法是使用單一 *DSCP* 類型管理並設定網路流量的優先順序。

5. 指定 **Codepoint**（字碼指標）值，以細微地比對 QoS 原則和流量。例如，選取保證式轉送 (AF) 作為 DSCP 值的 **Type**（類型）以供原則比對時，需進一步指定 AF **Codepoint**（字碼指標）值（例如 AF11）。

   當選取快速式轉送 *(EF*）作為 *DSCP* 標記的 ***Type***（類型）時，便無法指定更精準的 ***Codepoint***（字碼指標）值。*QoS* 原則規則會比對至使用任何 *EF* 字碼指標值標記的流量。

6. 選取 **Other Settings**（其他設定）並將 **QoS Class**（**QoS** 類別）指派給比對至 QoS 規則的流量。在此範例中，將 Class 1 指派給工作階段，而在該工作階段中的第一個封包偵測到 AF11 的 DSCP 標記。
7. 按一下 **OK**（確定）來儲存 QoS 規則。

STEP 3 | 當流量根據在工作階段一開始偵測到的 DSCP 標記比對至 QoS 規則時，為流量定義要接收的 QoS 優先順序。

1. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **QoS Profile**（**QoS** 設定檔），然後 **Add**（新增） 或修改現有的 QoS 設定檔。如需設定流量優先順序與頻寬的設定檔選項詳細資訊，請參閱 QoS 概念和設定 QoS。
2. **Add**（新增）或修改設定檔類別。例如，由於步驟 2 已顯示將 AF11 流量分類為 class 1 流量的步驟，因此您可以新增或修改 **class1** 項目。
3. 選取流量類別的 **Priority**（優先順序），例如 **high**（高）。
4. 按一下 **OK**（確定）來儲存 QoS 設定檔。

STEP 4 | 啟用介面上的 QoS。

選取 **Network**（網路） > **QoS**，然後 **Add**（新增）或修改現有的介面並 **Turn on QoS feature on this interface**（開啟此介面上的 **QoS** 功能）。

在此範例中，具有 AF11 DSCP 標記的流量比對至 QoS 規則和指派的 Class 1。在介面上啟用的 QoS 設定檔會為 Class 1 流量強制執行高優先順序處理，因為其輸出防火牆（工作階段輸出流量）。

©2024 Palo Alto Networks, Inc.

STEP 5 | 啟用 DSCP 標記。

以 DSCP 值標記返回流量可使工作階段的輸入流量被標記為輸出流量所偵測到相同的 DSCP 值。

1. 選取 **Policies**（原則） > **Security**（安全性），然後 **Add**（新增） 或修改安全性原則。
2. 選取 **Actions**（動作）並在 **QoS Marking**（**QoS** 標記）下拉式清單中選擇 **Follow-Client-to-Server Flow**（依照用戶端至伺服器流向）。
3. 按一下 **OK**（確定）儲存您的變更。

完成此步驟可讓防火牆以在工作階段一開始偵測到的相同 DSCP 值標記流量（在此範例中，防火牆會以 DSCP AF11 值標記返回流量）。設定 QoS 可讓您在流量輸出防火牆時形成流量，而在安全性規則中啟用此選項可讓其他網路設備干預防火牆和用戶端，以強制執行具 DSCP 標記流量的優先順序。

STEP 6 | 提交組態。

Commit（提交）您的變更。

 ©2024 Palo Alto Networks, Inc.

QoS 使用案例

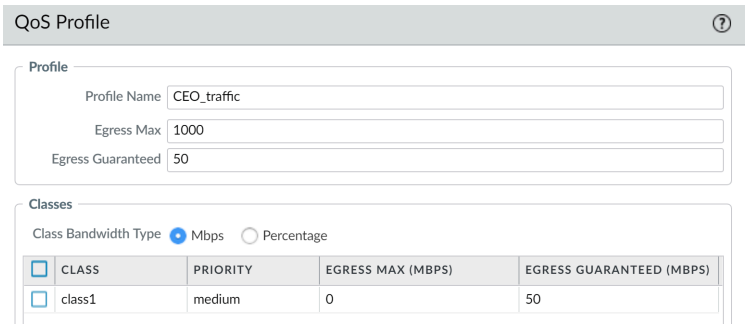
以下使用案例示範如何在一般的狀況下使用 QoS：

- 使用案例：單一使用者適用的 QoS
- 使用案例：音訊與視訊應用程式適用的 QoS

使用案例：單一使用者適用的 QoS

一位 CEO 發現在網路使用量高的時候無法存取公司的應用程式，因此無法有效率地回覆重要的業務通訊。IT 管理員想要確保這位 CEO 出入的流量會比其他員工的流量優先處理，因此向她保證不但能夠存取資源，還保證重要的網路資源會有高效能。

STEP 1 | 管理員建立了一個名為 *CEO_traffic* 的設定檔，以定義要如何處理來自 CEO 的流量，以及當流量流出公司網路時要如何形成：



管理員指派 50 Mbps 的保證頻寬（**Egress** 保證），確保無論網路是否擁塞，CEO 隨時都有保護的頻寬量（超過其所需）。

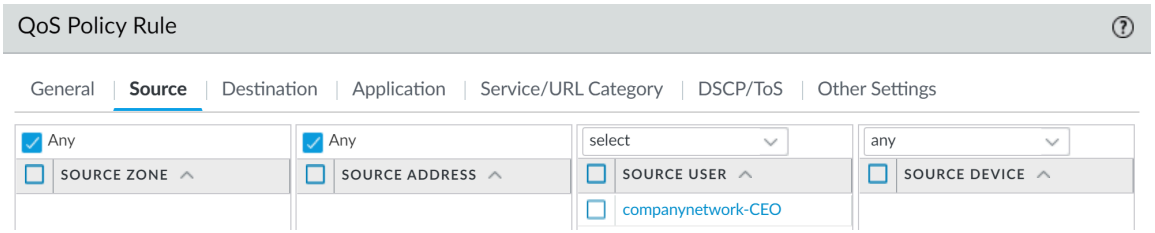
管理員繼續指派 Class 1 流量為高優先權，並設定好設定檔的最大頻寬使用量（**Egress Max**（輸出最大））為 1000 Mbps，此頻寬與管理員將啟用 QoS 之介面的最大頻寬相同。管理員選擇無論如何都不限制 CEO 的頻寬使用量。

最佳作法是填入 *QoS* 設定檔的 ***Egress Max***（***Egress*** 最大）欄位，即使設定的最大頻寬符合介面的最大頻寬。*QoS* 設定檔的最大頻寬絕不能超過您打算啟用 *QoS* 之介面的最大頻寬。

STEP 2 | 管理員建立一個用於識別 CEO 流量的 QoS 原則（**Policies**（原則） > **QoS**），並將在 QoS 設定檔中定義的類別指派給該流量（請參閱上一步驟）。由於已設定 User-ID，因此管理員使用 QoS 原則中的 **Source**（來源）頁籤依 CEO 的公司網路使用者名稱來單一識別 CEO 的流量。

©2024 Palo Alto Networks, Inc.

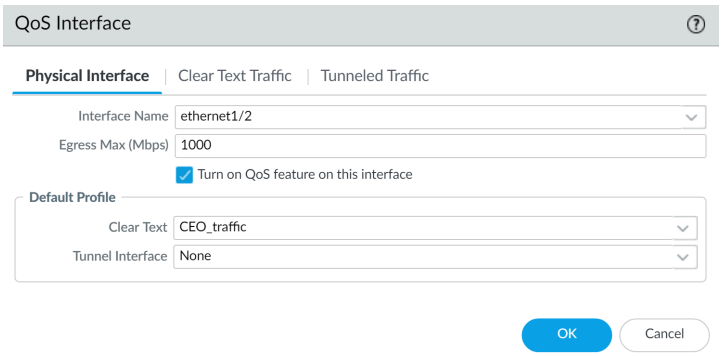
（如果未設定 User-ID，則管理員可在 **Source Address**（來源位址）中 **Add**（新增）CEO 的 IP 位址。請參閱 User-ID。）：



管理員將 CEO 的流量與 Class 1 建立關聯（**Other Settings**（其他設定）頁籤），然後繼續填入其餘的必要原則填位；管理員為原則設定具描述性 **Name**（名稱）（**General**（一般）頁籤），並將 **Source Zone**（來源區域）（**Source**（來源）頁籤）與 **Destination Zone**（目的地區域）（**Destination**（目的地）頁籤）設為 **Any**（任何）：

	NAME	TAGS	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	DSCP/TOS	CLASS
1	HTTPS	none	trust	any	any	any	untrust	any	any	web-browsing	any	any	2
2	Voice-Video	none	any	any	any	any	any	any	any	voip-video-l...	any	any	1
3	Guarantee CEO bandwidth	none	any	any	companynet...	any	any	any	any	any	any	any	1

STEP 3 | Class 1 已與 CEO 的流量建立關聯，管理員現在可以核取 **Turn on QoS feature on interface**（開啟此介面上的 **QoS** 功能）並選取流量流向的 Egress 介面，來啟用 QoS。CEO 流量流向的輸出介面是對外介面，在本案例中為 乙太網路 1/2：



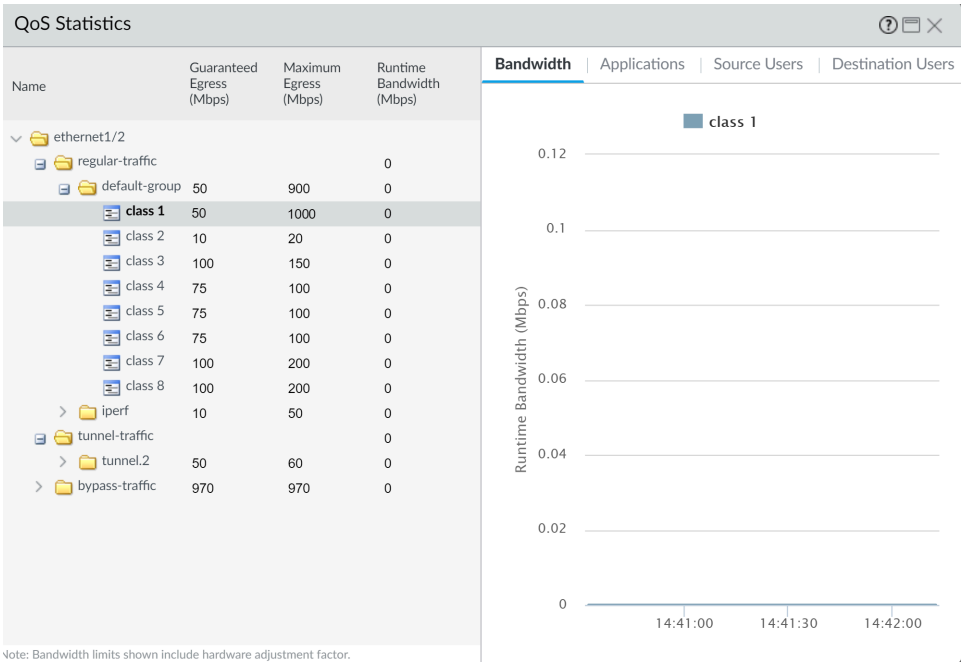
由於管理員想要確保源自 CEO 的所有流量都能受到管理員所建立 QoS 設定檔與相關 QoS 原則的保證，因此選擇 *CEO_traffic* 以套用到來自 ethernet 1/2 的 **Clear Text**（純文字）流量上。

STEP 4 | 提交 QoS 組態之後，管理員導覽至 **Network**（網路） > **QoS** 頁面以確認設定檔 CEO_traffic 是否已於對外介面 ethernet 1/2 上啟用:

NAME	GUARANTEED EGRESS (MBPS)	MAXIMUM EGRESS (MBPS)	PROFILE	ENABLED	
ethernet1/2		1,000.000		✓	Statistics
Tunneled Traffic					
Clear Text Traffic	50.000		CEO_traffic		

©2024 Palo Alto Networks, Inc.

STEP 5 | 管理員按一下 **Statistics**（統計資料）以檢視源自 CEO (Class 1) 的流量從 ethernet 1/2 流來時要如何形成流量：



此案例示範如何將 *QoS* 套用到源自單一來源使用者的流量。然而，如果您也要對目的地使用者保證或形成流量，您可以設定類似的 *QoS* 設定。除了此工作流程外（或者您不想要使用此工作流程），您還可以在 ***Policies***（原則） > ***QoS*** 頁面上建立 *QoS* 原則，將使用者的 *IP* 位址指定為 ***Destination Address***（目的地位址）（而非指定使用者的來源資訊），然後在 ***Network***（網路） > ***QoS*** 頁面上啟用網路對內介面上的 *QoS*（而非對外介面）。

使用案例：音訊與視訊應用程式適用的 QoS

音訊與視訊流量對於 QoS 功能形成與控制的量值特別敏感，尤其是延遲與抖動。為了讓傳輸的音訊與視訊能聽得見且畫質清晰，因此音訊與視訊封包不能丟棄、延遲或傳遞不一致。對於音訊與視訊應用程式而言的最佳做法是除了保證頻寬外，也要保證音訊與視訊流量的優先權。

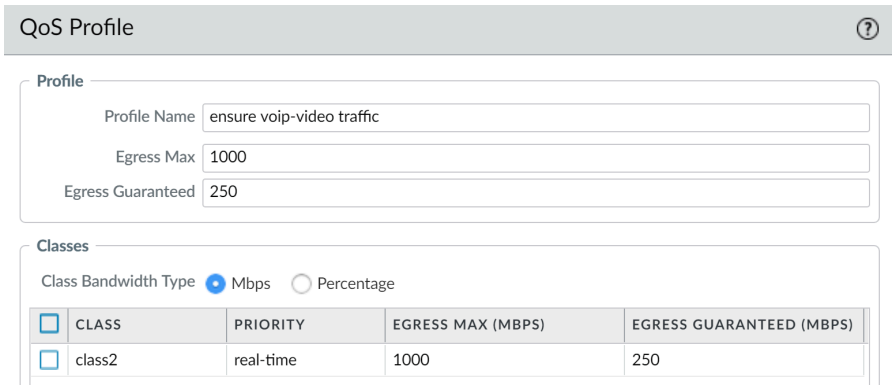
在此範例中，分公司辦公室員工在使用視訊會議與 Voice over IP（VoIP；IP 語音）技術與其他分公司辦公室、合作夥伴及客戶進行業務通訊時，碰到困難且發現不穩定。IT 管理員打算實作 QoS 來處理這些問題，確保為分公司員工提供有效率且穩定的業務通訊環境。由於管理員想要保證傳入與傳出網路流量的 QoS，因此啟用了防火牆對內與對外介面的 QoS。

©2024 Palo Alto Networks, Inc.

STEP 1 | 管理員建立 QoS 設定檔並定義 Class 2，讓 Class 2 流量得到即時優先權，並在最大頻寬為 1000 Mbps 的介面得到隨時有 250 Mbps 的保證頻寬，即使在網路使用尖峰期也獲得保證。

即時優先權一般建議用於會受到延遲影響的應用程式，且對於保證音訊與視訊應用程式的效能及品質特別有用。

在防火牆網頁介面上，管理員選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **Qos Profile**（**QoS** 設定檔） 頁面，按一下 **Add**（新增），然後輸入 **Profile Name**（設定檔名稱）ensure voip-video traffic，並定義 Class 2 流量。

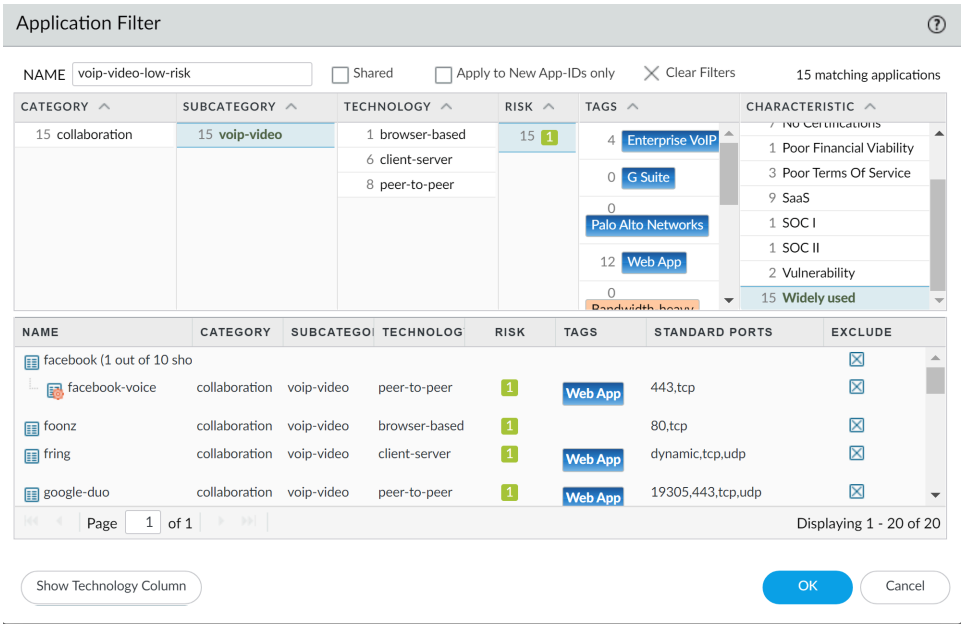


STEP 2 | 管理員建立 QoS 原則以識別音訊與視訊流量。由於公司沒有一個標準的音訊與視訊應用程式，因此管理員想要確定 QoS 會套用到員工間廣泛且固定用來與其他辦公室、合作夥伴及客戶通訊的應用程式。在 **Policies**（原則） > **QoS** > **QoS Policy Rule**（**QoS** 原則規則） > **Applications**（應用程式）頁籤上，管理員按一下 **Add**（新增），開啟 **Application Filter**（應

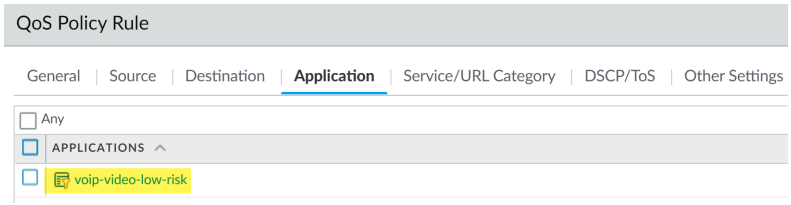
 ©2024 Palo Alto Networks, Inc.

用程式篩選器）視窗。管理員繼續選取準則以篩選出想要套用 QoS 的應用程式，選擇子類別 voip-video，並藉由僅指定低風險且廣為使用的 voip-video 應用程式來縮小篩選範圍。

應用程式篩選器是一種動態工具，當用於在 QoS 原則中篩選應用程式時，可讓 QoS 在任何指定的時間套用到所有符合 voip-video、low risk與widely used準則的應用程式。



管理員將此 **Application Filter**（應用程式篩選器）命名為 voip-video-low-risk，並將它包含在 QoS 原則中：



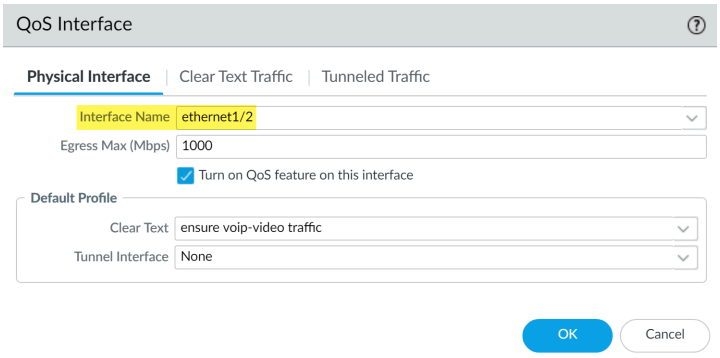
管理員將 QoS 原則命名為 Voice-Video 並選取其他設定來指派符合原則類別 2 的所有流量。管理員要為傳入與傳出 QoS 流量使用 Voice-Video QoS 原則，因此將 **Source**（來源）與 **Destination**（目的地）資訊設為 **Any**（任何）：

	NAME	TAGS	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	DSCP/TOS	CLASS
1	HTTPS	none	trust	any	any	any	untrust	any	any	web-browsing	any	any	2
2	Voice-Video	none	any	any	any	any	any	any	any	voip-video-l...	any	any	1

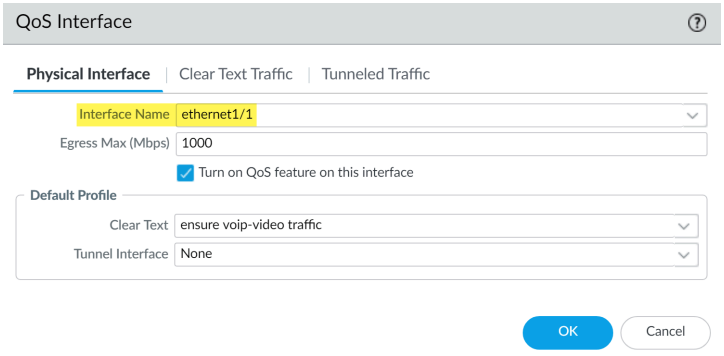
©2024 Palo Alto Networks, Inc.

STEP 3 | 管理員想要確定 QoS 會用於傳入與傳出的音訊與視訊通訊，因此他在網路的對外介面上啟用 QoS (藉此將 QoS 套用到傳出通訊)，也在對內介面上啟用 QoS (藉此將 QoS 套用到傳入通訊)。

管理員一開始先在對外介面（在本案例中為 ethernet 1/2）啟用他所建立的 QoS 設定檔 ensure voice-video traffic（此設定檔中的 Class 2 與原則 Voice-Video 相關聯）。



接著他在對內介面的第二個介面上（在本案例中為 ethernet 1/1）啟用同一個 QoS 設定檔 ensure voip-video traffic。



STEP 4 | 管理員選取 **Network**（網路） > **QoS** 以確認傳入與傳出的音訊與視訊流量上皆已啟用 QoS：

NAME	GUARANTEED EGRESS (MBPS)	MAXIMUM EGRESS (MBPS)	PROFILE	ENABLED	
ethernet1/1		1,000.000		☑	Statistics
Tunneled Traffic					
Clear Text Traffic	250.000		ensure voip-video traffic		
ethernet1/2		1,000.000		☑	Statistics
Tunneled Traffic					
Clear Text Traffic	250.000		ensure voip-video traffic		

管理員已在網路的對內與對外介面上成功啟用 QoS。現在確定音訊與視訊應用程式流入與流出網路時會取得即時優先權，以確保這些對於延遲與抖動特別敏感的通訊能夠可靠且有效地用於執行內部與外部的業務通訊上。

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

VPN

虛擬私人網路 (VPN) 可讓使用者/系統透過公共網路安全連線來建立通道，就像它們是透過區域網路 (LAN) 連線一樣。若要設定 VPN 通道，您必須有一對能夠互相驗證的裝置，並會加密彼此之間的資訊流量。這對裝置可以是一對 Palo Alto Networks 防火牆，或是 Palo Alto Networks 防火牆搭配其他廠商具備 VPN 功能的裝置。

- VPN 部署
- 站台對站台 VPN 概覽
- 站台對站台 VPN 概念
- 設定站台對站台 VPN
- 站台對站台 VPN 快速設定

VPN 部署

Palo Alto Networks 防火牆支援下列 VPN 部署：

- 站台對站台 **VPN**—一種簡單的 VPN，可連接中央站台與遠端站台，或可連接中心點與軸輻式 VPN，讓中央站台與多個遠端站台連接。防火牆會使用 IP 安全性 (IPSec) 通訊協定集為兩個站台間的流量設定安全通道。請參閱站點對站點 VPN 概覽。
- 遠端使用者對站台 **VPN**—此解決方案使用 GlobalProtect 代理程式，讓遠端使用者能夠透過防火牆建立安全連線。此解決方案使用 SSL 與 IPSec 在使用者與站台之間建立安全連線。請參閱《GlobalProtect 管理者指南》。
- 大規模 **VPN**— Palo Alto Networks GlobalProtect 大規模 VPN (LSVPN) 提供經過簡化的機制，能夠提供可調式中心點與軸輻式 VPN，最多可含 1,024 個衛星辦公室。此解決方案需要在中心點與每一個軸輻點上部署 Palo Alto Networks 防火牆。它使用憑證進行裝置驗證，使用 SSL 讓所有元件之間有安全的通訊，並使用 IPSec 保護資料。請參閱大規模 VPN (LSVPN)。

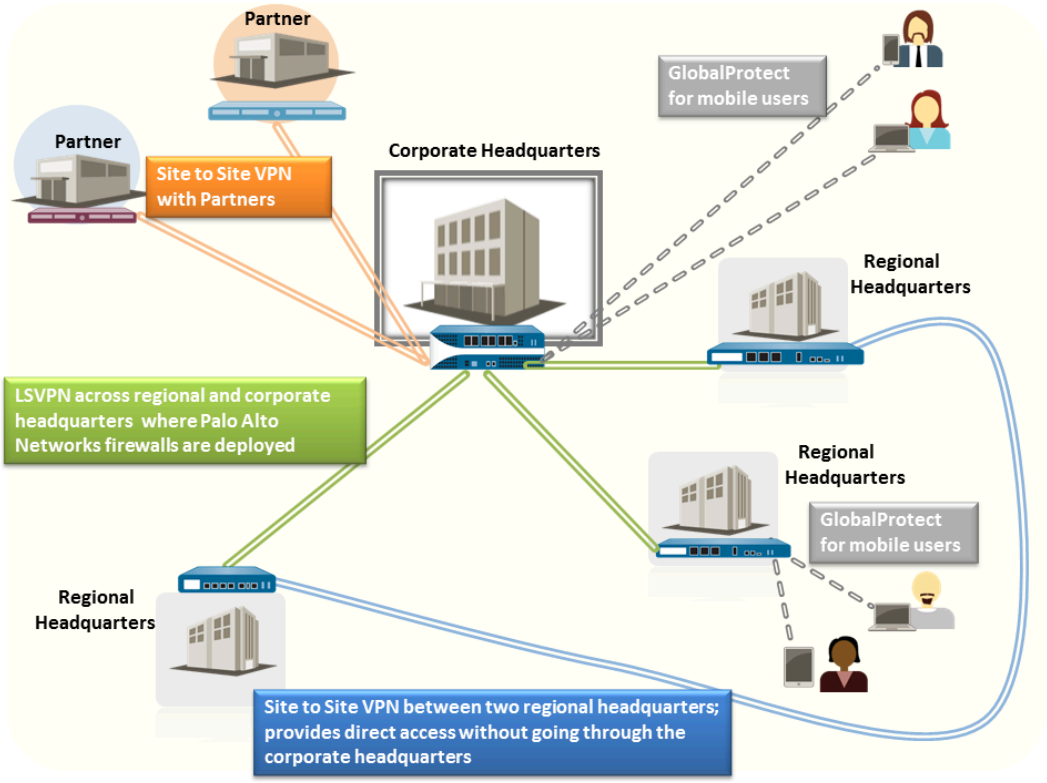


圖 **7: VPN** 部署

©2024 Palo Alto Networks, Inc.

站台對站台 VPN 概覽

允許您將兩個區域網路 (LAN) 連接的 VPN 連線稱做站台對站台 VPN。您可以設定以路由為基礎的 VPN，以連接兩個站台的 Palo Alto Networks 防火牆，或將 Palo Alto Networks 防火牆與其他位置的協力廠商安全性裝置連接。防火牆也可以與以協力廠商原則為基礎的 VPN 裝置交互操作；Palo Alto Networks 防火牆支援以路由為基礎的 VPN。

Palo Alto Networks 防火牆會設定以路由為基礎的 VPN，在此防火牆會根據目的地 IP 位址來決定路由。如果流量透過 VPN 通道路由到特定目的地，會將其作為 VPN 流量處理。

IP 安全性 (IPSec) 通訊協定集可用於為 VPN 流量設定安全通道，並保護 TCP/IP 封包中的資訊 (如果通道類型為 ESP 則加密)。IP 封包 (標頭與承載) 會內嵌於另一個 IP 承載中，會套用新的標頭並隨後透過 IPSec 通道傳送此標頭。新標頭中的來源 IP 位址是本地 VPN 對等的 IP 位址，目的地 IP 位址是通道遠端處 VPN 對等的 IP 位址。當封包到達遠端 VPN 對等 (通道遠端的防火牆)，會移除外部標頭，原始封包會傳送至其目的地。

為了設定 VPN 通道，首先必須驗證對等。成功驗證後，對等會交涉加密機制與演算法，來保護通訊安全。網際網路金鑰交換 (IKE) 程序用於驗證 VPN 對等，IPSec 安全性關聯 (SA) 則會在通道的每一端定義，以保護 VPN 通訊安全。IKE 使用數位憑證或預先共用的金鑰及 Diffie Hellman 金鑰為 IPSec 通道設定 SA。SA 會指定安全傳輸所需的所有參數—包括安全性參數索引 (SPI)、安全性通訊協定、加密金鑰及目的地 IP 位址—加密、資料驗證、資料完整性及端點驗證。

下圖顯示兩個站台之間的 VPN 通道。當 VPN 對等 A 保護的用戶端需要位於另一個站台的伺服器內容時，VPN 對等 A 會對 VPN 對等 B 的連線啟動要求。如果安全性原則允許連線，VPN 對等 A 會使用 IKE 密碼設定檔參數（IKE 階段 1）建立安全連線並驗證 VPN 對等 B。接著，VPN 對等 A 會使用 IPSec 密碼設定檔來定義 IKE 階段 2 參數，以允許在兩個站台之間安全傳輸資料。

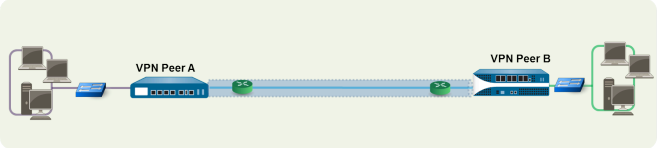


圖 **8:** 站台對站台 **VPN**

©2024 Palo Alto Networks, Inc.

站台對站台 VPN 概念

VPN 連線能讓您在兩個以上站台之間安全地存取資訊。為了能夠安全存取資源並提供可靠的連線，VPN 連線需要下列元件：

- IKE 閘道
- 隧道接口
- 通道監控器
- VPN 的網際網路金鑰交換 (IKE)
- IKEv2

IKE 閘道

Palo Alto Networks 防火牆或啟動並終止兩個網路間 VPN 連線的防火牆與安全性裝置，可稱為 IKE 閘道。若要設定 VPN 通道並在 IKE 閘道之間傳送流量，則每個對等必須有 IP 位址—靜態或動態—或 FQDN。VPN 對等使用預先共用的金鑰或憑證彼此互相驗證。

對等也必須交涉模式—主要或積極—以設定 IKE 階段 1 中的 VPN 通道與 SA 存留時間。主要模式可保護對等的識別，而且更安全，因為設定通道時會交換更多的封包。如果兩個對等皆支援，則主要模式則為 IKE 交涉的建議模式。加強模式會使用較少的封包設定 VPN 通道，因此速度較快，但設定 VPN 通道的安全選項較少。

如需設定詳細資料，請參閱 設定 IKE 閘道。

隧道接口

若要設定 VPN 通道，各端的 Layer 3 介面均必須具有邏輯通道介面，防火牆才能連線並建立 VPN 通道。通道介面是邏輯 (虛擬) 介面，用於在兩個端點之間傳遞流量。若您設定了任何 Proxy ID，則該 Proxy ID 將計入任何 IPSec 通道容量。

通道介面必須屬於安全性區域才能套用原則，且必須指派給虛擬路由器才能使用現有的路由基礎結構。確定通道介面與實體介面指派給同一個虛擬路由器，讓防火牆可執行路由查閱，並決定要使用的適當通道。

一般而言，附加通道介面的 Layer 3 介面屬於外部區域，例如不信任區域。雖然通道介面可以與實體介面位在同一個安全性區域中，但為了增加安全性與更好的可見度，您可以為通道介面另外建立一個區域。如果您為通道介面另外建立的區域為 VPN 區域，則必須建立安全性原則才能讓流量在 VPN 區域與信任區域之間流動。

若要在站台之間路由流量，通道介面不需要 IP 位址。如果您想要啟用通道監控，或者使用動態路由通訊協定在整個通道間路由流量，則只需要 IP 位址。有了動態路由，通道 IP 位址會作為將流量路由至 VPN 通道的下一個躍點 IP 位址。

如果您正在設定 Palo Alto Networks 防火牆，且其中的 VPN 對等執行以原則為基礎的 VPN，當設定 IPSec 通道時，您必須設定本機與遠端 Proxy ID。各對等均會與設定於對等上的 Proxy-ID 進行

©2024 Palo Alto Networks, Inc.

比較，在封包中必須收到 Proxy-ID，IKE 階段 2 交涉才能成功。如果需要多個通道，請為每個通道介面設定唯一的 Proxy ID；通道介面最多可以有 250 個 Proxy ID。每個 Proxy ID 會計入防火牆的 IPSec VPN 通道容量中，通道容量會隨著防火牆型號而異。

如需設定詳細資料，請參閱設定 IPSec 通道（通道模式）。

通道監控器

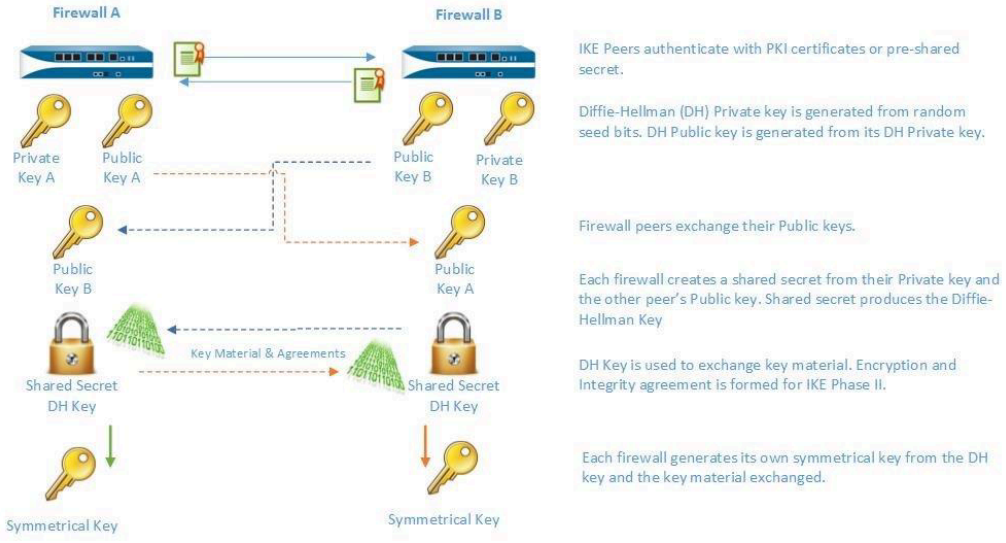
對於 VPN 通道而言，您可以在整個通道中檢查目的地 IP 位址的連線。防火牆的網路監控設定檔可讓您以指定的輪詢間隔驗證對目的地 IP 位址或下一個躍點的連線 (使用 ICMP)，並指定失敗時存取所監控 IP 位址的動作。

如果目的地 IP 無法連線，您可以設定防火牆等待通道復原，或設定自動容錯移轉至另一個通道。無論是哪種方式，防火牆都會產生系統日誌來提醒您通道失敗，並重新交涉 IPSec 金鑰以加速復原。

如需設定詳細資料，請參閱設定通道監控。

VPN 的網際網路金鑰交換 (IKE)

IKE 程序允許通道兩端的 VPN 對等使用互相同意的金鑰或憑證與加密方法將封包加密與解密。IKE 程序分成兩個階段：IKE 階段 1 和 IKE 階段 2。每個階段皆使用以密碼設定檔—IKE 密碼設定檔與 IPSec 密碼設定檔—定義的金鑰與演算法，IKE 交涉的結果是安全性關聯 (SA)。SA 是一組互相同意的金鑰與演算法，VPN 對等雙方用於允許整個 VPN 通道的資料流量。下圖說明用於設定 VPN 通道的金鑰交換程序：



IKE 階段 1

在此階段中，防火牆使用在 IKE 閘道組態和 IKE 密碼設定檔中定義的參數互相驗證，並設定安全控制通道。IKE 階段支援使用預先共用金鑰或數位憑證 (使用公開金鑰基礎結構，PKI) 互相驗證 VPN 對等。預先共用金鑰是保護小型網路的簡單解決方案，因為小型網路不需要支援 PKI 基礎結構。對於需要更強驗證安全性的大型網路或實作而言，數位憑證更為方便。

©2024 Palo Alto Networks, Inc.

使用憑證時，請確定兩個閘道對等皆信任簽發憑證的 CA，憑證鏈結中憑證的最大長度為 5 以下。在 IKE 區段啟用的狀況下，防火牆最多可使用憑證鏈中最多 5 個憑證重新組合 IKE 訊息，並成功建立 VPN 通道。

IKE 密碼設定檔會定義下列在 IKE SA 交涉中使用的選項：

- 用於產生 IKE 對稱金鑰的 Diffie-Hellman (DH) 群組。

  Diffie-Hellman 演算法使用一方的私密金鑰及另一方的公開金鑰來建立共用金鑰，亦即由 VPN 通道對等雙方共用的加密金鑰。防火牆上支援的 DH 群組有：

群組編號	位元組數
群組 1	768 位元
群組 2	1024 位元（預設值）
群組 5	1536 位元
群組 14	2048 位元
群組 15	3072 位元模指數群組
群組 16	4096 位元模指數群組
群組 19	256 位元橢圓曲線群組
群組 20	384 位元橢圓曲線群組
群組 21	512 位元隨機橢圓曲線群組

- 驗證演算法—sha1、sha 256、sha 384、sha 512 或 md5
- 加密演算法—aes-256-gcm、aes-128-gcm、3des、aes-128-cbc、aes-192-cbc 或 aes-256-cbc

IKE 階段 2

保護與驗證通道後，會進一步保護階段 2 中的通道，以在網路之間傳輸資料。IKE 階段 2 會使用在程序的階段 1 及 IPSec 密碼設定檔中建立的金鑰，這些金鑰會定義在 IKE 階段 2 中用於 SA 的 IPSec 密碼設定檔與金鑰。

IPSEC 會使用下列通訊協定啟用安全通訊：

- 封裝安全有效負載 (ESP)—允許您加密整個 IP 封包，並驗證來源與資料完整性。ESP 要求您加密與驗證封包時，您可以透過將加密選項設為 (空值)，來選擇僅加密或僅驗證；不鼓勵使用加密但不進行驗證。
- 驗證標頭 (AH)—驗證封包來源與資料完整性。AH 不會加密資料承載，且不適用於資料隱私很重要的部署。AH 常用於主要考量為驗證對等合法性且資料隱私為非必要時。

©2024 Palo Alto Networks, Inc.

表 **2:** 支援的 **IPSEC** 驗證與加密演算法

ESP	AH
支援的 Diffie Hellman (DH) 交換選項	
• 群組 1—768 位元 • 群組 2—1024 位元（預設值） • 群組 5—1536 位元 • 群組 14—2048 位元 • 群組 15—3072 位元模指數群組 • 群組 16—4096 位元模指數群組 • 群組 19—256 位元橢圓曲線群組 • 群組 20—384 位元橢圓曲線群組 • 群組 21—512 位元隨機橢圓曲線群組 • 無 pfs—依預設會啟用完整轉寄密碼 (PFS)，這表示會在 IKE 階段 2 中使用前述其中一個群組產生新的 DH 金鑰。此金鑰獨立於在 IKE 階段 1 中交換的金鑰以外，並且可提供更好的資料傳輸安全性。如果您選取「無 pfs」，在階段 1 中建立的 DH 金鑰將不會更新，且 IPSec SA 交涉會使用單一金鑰。VPN 對等雙方必須同時為 PFS 啟用或停用。	
支援加密演算法	
• 3des	安全性長度為 112 位元的三重資料加密標準 (3DES)
• aes-128-cbc	使用安全性長度為 128 位元之加密區塊鏈結 (CBC) 的進階加密標準 (AES)
• aes-192-cbc	使用安全性長度為 192 位元之 CBC 的 AES
• aes-256-cbc	使用安全性長度為 256 位元之 CBC 的 AES
• aes-128-ccm	使用安全性長度為 128 位元之 CBC-MAC (CCM) 計數器的 AES
• aes-128-gcm	使用安全性長度為 128 位元之伽羅瓦計數器模式 (GCM) 的 AES
• aes-256-gcm	使用安全性長度為 256 位元之 GCM 的 AES
支援驗證演算法	
• md5	• md5

©2024 Palo Alto Networks, Inc.

ESP	AH
• sha 1	• sha 1
• sha 256	• sha 256
• sha 384	• sha 384
• sha512	• sha 512

保護 IPSec VPN 通道的方法（IKE 階段 2）

IPSec VPN 通道可使用手動金鑰或自動金鑰予以保護。此外，IPSec 組態選項包括金鑰協議的 Diffie-Hellman 群組，和/或加密演算法與訊息驗證的雜湊。

- 手動金鑰—手動金鑰通常用於 Palo Alto Networks 防火牆使用舊有裝置建立 VPN 通道時，或者您想要減少產生工作階段金鑰的負荷。如果使用手動金鑰，則必須在雙方對等建立相同的金鑰。

  不建議使用手動金鑰建立 VPN 通道，因為在對等之間轉送金鑰資訊時可能會洩漏工作階段金鑰；如果金鑰遭到洩漏，便再也無法安全地傳輸資料。
- 自動金鑰—自動金鑰允許您自動產生金鑰，以根據在 IPSec 密碼設定檔中定義的演算法設定與維護 IPSec 通道。

IKEv2

IPSec VPN 閘道會使用 IKEv1 或 IKEv2 來交涉 IKE 安全性關聯 (SA) 和 IPSec 通道。IKEv2 可於 RFC 5996 中定義。

不同於使用階段 1 SA 和階段 2 SA 的 IKEv1，IKEv2 使用的是封裝安全有效負載 (ESP) 或驗證標頭 (AH) 的子 SA，這是以 IKE SA 設定的。

如果您在位於兩個閘道之間的設備上執行 NAT，則必須在兩個閘道上都啟用 NAT 周遊 (NAT-T)。閘道只能看見 NAT 裝置的公用（可全域路由傳送）IP 位址。

IKEv2 提供下列優於 IKEv1 的好處：

- 通道端點只需交換較少的訊息即可建立通道。IKEv2 使用四個訊息；IKEv1 使用九個訊息（在主要模式中）或六個訊息（在加強模式中）。
- 內建的 NAT-T 功能可改善廠商之間的相容性。
- 內建的健康度檢查可在通道失效時自動加以重新建立。活性檢查取代了 IKEv1 中使用的「無效對等偵測」。
- 支援流量選取器（每個交換一個）。流量選取器可在 IKE 交涉中用來控制哪個流量可存取通道。
- 支援雜湊與 URL 憑證交換，以減少分散的狀況。

©2024 Palo Alto Networks, Inc.

- 透過改良的對等驗證，能夠在 DoS 攻擊之後復原。額外的半開啟 SA 可觸發 Cookie 驗證。

在設定 IKEv2 之前，您應熟悉下列概念：

- 活性檢查
- Cookie 啟用臨界值和嚴格 Cookie 驗證
- 流量選取器
- 雜湊與 URL 憑證交換
- SA 金鑰的存留時間和重新驗證間隔

在設定 IKE 閘道之後，如果您選擇 IKEv2，請根據您的環境需求，執行下列與 IKEv2 有關的選用工作：

- 匯出憑證讓對等使用雜湊與 URL 加以存取
- 匯出憑證供 IKEv2 閘道驗證使用
- 變更 IKEv2 的金鑰存留時間或驗證層級
- 變更 IKEv2 的 Cookie 啟用臨界值
- 設定 IKEv2 流量選取器

活性檢查

IKEv2 的活性檢查類似於無效對等偵測 (DPD)，後者是 IKEv1 用來判斷對等是否仍可用的方法。

在 IKEv2 中，活性檢查可使用由閘道依據可設定的間隔 (預設為五秒) 傳送至對等的任何 IKEv2 封包傳輸或空資訊訊息來執行。如有需要，寄件者最多可嘗試重新傳輸十次。如果沒有回應，寄件者會關閉並刪除 IKE_SA 與對應的 CHILD_SA。寄件者會重新開始寄出另一個 IKE_SA_INIT 訊息。

Cookie 啟用臨界值和嚴格 **Cookie** 驗證

對於 IKEv2 一律會啟用 Cookie 驗證；這有助於防止半 SA DoS 攻擊。您可以設定會觸發 Cookie 驗證之半開放 SA 的全域臨界值數。您也可以設定個別的 IKE 閘道，使其為每個新的 IKEv2 SA 強制執行 Cookie 驗證。

- **Cookie Activation Threshold**（**Cookie** 啟用臨界值）是一項全域 VPN 工作階段設定，可限制同時的半開啟 IKE SA 數目（預設值為 500）。當半開啟的 IKE SA 數目超過 **Cookie Activation Threshold**（**Cookie** 啟用臨界值）時，回應程式會要求一個 Cookie，且啟動者必須回應一個包含 Cookie 的 IKE_SA_INIT 以驗證連線。若 Cookie 驗證成功，則可以啟動另一個 SA。若值為 0，表示 Cookie 驗證一律開啟。

  在啟動者傳回 Cookie 前，回應者將不會維護啟動者的狀態，也不會執行 Diffie-Hellman 金鑰交換。IKEv2 Cookie 驗證可緩解會嘗試致使許多連線半開啟的 DoS 攻擊。

  Cookie Activation Threshold（**Cookie** 啟用臨界值）必須低於 **Maximum Half Opened SA**（半開啟 **SA** 上限）設定。如果您 變更 IKEv2 的 Cookie 啟用臨界值 非常高的數值（例如 65534），且 **Maximum Half Opened SA**（半開啟 **SA** 上限）設定仍維持在預設值 65535，Cookie 驗證實質上會停用。

©2024 Palo Alto Networks, Inc.

- 如果您想要為閘道所接收的每個新的 IKEv2 SA 執行 Cookie 驗證，無論全域臨界值為何，您可以啟用 **Strict Cookie Validation**（嚴格 **Cookie** 驗證）。**Strict Cookie Validation**（嚴格 **Cookie** 驗證）只會影響正在設定的 IKE 閘道，且預設為停用。如果 **Strict Cookie Validation**（嚴格 **Cookie** 驗證）停用，系統會使用 **Cookie Activation Threshold**（**Cookie** 啟用臨界值）來判定是否需要某個 Cookie。

流量選取器

在 IKEv1 中，具有路由型 VPN 的防火牆必須使用本機和遠端 Proxy ID，以設定 IPSec 通道。每個對等都會比較其 Proxy ID 與它在封包中接收到的 ID，以成功交涉 IKE 階段 2。IKE 階段 2 與交涉 SA 以設定 IPSec 通道的程序有關。（如需 Proxy ID 的詳細資訊，請參閱隧道接口。）

在 IKEv2 中，您可以 設定 IKEv2 流量選取器，這是在 IKE 交涉期間所使用的網路流量元件。流量選取器可在 CHILD_SA（通道建立）階段 2 期間用來設定通道，以及決定哪些流量可通過通道。兩個 IKE 閘道對等必須互相交涉，並一致同意其流量選取器；否則，其中一方會縮小其位址範圍以達成協議。一個 IKE 連線可以有多個通道；例如，您可以將不同的通道指派給每個部門，以隔離其流量。流量的區隔可讓 QoS 之類的功能得以實作。

IPv4 和 IPv6 的流量選取器包括：

- 來源 **IP** 位址—網路首碼、位址範圍、特定主機或萬用字元。
- 目的地 **IP** 位址—網路首碼、位址範圍、特定主機或萬用字元。
- 通訊協定—一個傳輸通訊協定，例如 TCP 或 UDP。
- 來源連接埠—送出封包的連接埠。
- 目的地連接埠—封包預定要送達的連接埠。

在 IKE 交涉期間，可能會有用於不同網路和通訊協定的多個流量選取器。例如，啟動者可能會指出它要將 TCP 封包從 172.168.0.0/16 透過通道傳送至其對等，並以 198.5.0.0/16 作為目標。它也要將 UDP 封包從 172.17.0.0/16 透過相同的通道傳送至相同的閘道，並以 0.0.0.0（任何網路）作為目標。對等閘道必須同意這些流量選取器，以得知應有的預期。

一個閘道開始交涉時所使用的流量選取器，是比另一個閘道的 IP 位址更為特定的 IP 位址，是有可能發生的情況。

- 例如，閘道 A 提供的來源 IP 位址為 172.16.0.0/16，目的地 IP 位址為 192.16.0.0/16。但閘道 B 設定了 0.0.0.0（任何來源）作為來源 IP 位址，並以 0.0.0.0（任何目的地）作為目的地 IP 位址。因此，閘道 # 將其來源 IP 位址縮小為 192.16.0.0/16，並將目的地位址縮小為 172.16.0.0/16。據此，縮小範圍以接納閘道 A 的位址，兩個閘道的流量選取器得以達成協議。
- 如果閘道 B（設定的來源 IP 位址為 0.0.0.0）是啟動者而非回應者，則閘道 A 將會以其較特定的 IP 位址回應，而閘道 B 將會縮小其位址以達成協議。

雜湊與 URL 憑證交換

IKEv2 支援「雜湊與 URL 憑證交換」，這是在 IKEv2 交涉 SA 期間所使用的功能。您會將憑證儲存在 URL 所指定的 HTTP 伺服器上。對等會根據接收到的伺服器 URL，從伺服器提取憑證。雜湊可用來檢查憑證的內容是否有效。因此，兩個對等將會與 HTTP CA 交換憑證，而不是互相交換。

©2024 Palo Alto Networks, Inc.

「雜湊與 URL」的雜湊部分可減少訊息大小，因此「雜湊與 URL」可說是能夠在 IKE 交涉期間降低封包分散可能性的方式之一。對等會接收它所預期的憑證和雜湊，因此 IKE 階段 1 驗證了對等。減少分散的狀況有助於防止 DoS 攻擊。

在設定 IKE 閘道時，您可以選取 **HTTP Certificate Exchange**（**HTTP** 憑證交換）並輸入 **Certificate URL**（憑證 **URL**），以啟用「雜湊與 URL」憑證交換。此外，對等也必須使用「雜湊與 URL」憑證交換，交換才能成功。如果對等無法使用「雜湊與 URL」，則 X.509 憑證的交換方式將會類似於在 IKEv1 中的交換。

如果您啟用「雜湊與 URL」憑證交換，您必須將憑證匯出至憑證伺服器（如果已不在那裡）。匯出憑證時，檔案格式應為 **Binary Encoded Certificate (DER)**（二進位編碼憑證 **(DER)**）。請參閱 匯出憑證讓對等使用雜湊與 URL 加以存取。

SA 金鑰的存留時間和重新驗證間隔

IKEv2 中有兩個 IKE Crypto 設定檔值 **Key Lifetime**（金鑰存留時間）和 **IKEv2 Authentication Multiple**（**IKEv2** 驗證倍數），可控制 IKEv2 IKE SA 的建立。金鑰存留時間是交涉的 IKE SA 金鑰有效的時間長度。在金鑰存留時間到期之前，必須重設 SA 金鑰，否則在到期時，SA 必須開始新的 IKEv2 IKE SA 金鑰重設。預設值是 8 小時。

重新驗證間隔衍生自 **Key Lifetime**（金鑰存留時間）與 **IKEv2 Authentication Multiple**（**IKEv2** 驗證倍數）的乘積。驗證倍數預設為 0，這會停用重新驗證功能。

驗證倍數的範圍為 0-50。因此，舉例來說，如何您將驗證倍數設定為 20，系統將會在每次經過 20 次金鑰重設時（也就是每 160 小時）執行重新驗證。這表示，在閘道必須向 IKE 重新驗證以從頭重新建立 IKE SA 之前，閘道有 160 小時可以執行子 SA 建立。

在 IKEv2 中，啟動者和回應者閘道各有其本身的金鑰存留期間值，而金鑰存留期間較短的閘道，將會是要求為 SA 重設金鑰的閘道。

©2024 Palo Alto Networks, Inc.

設定站台對站台 VPN

若要設定站台對站台 VPN：

- 確定已正確設定乙太網路介面、虛擬路由器與區域。如需詳細資訊，請參閱設定介面及區域。
- 建立您的通道介面。理想狀況是將通道介面放置在不同的區域中，以便進入通道的流量可使用不同的原則。
- 設定靜態路由或指派路由通訊協定，以將流量重新導向至 VPN 通道。若要支援動態路由 (支援 OSPF、BGP、RIP)，您必須將 IP 位址指派給通道介面。
- 定義 IKE 閘道，藉以在 VPN 通道兩端的對等之間建立通訊；此外也定義密碼設定檔，此設定檔會為用於在 IKEv1 階段 1 中設定 VPN 通道的識別、驗證與加密等功能指定通訊協定與演算法。請參閱設定 IKE 閘道以及定義 IKE 加密設定檔。
- 設定建立在 VPN 通道之間傳輸資料所用 IPSec 連線所需的參數；請參閱設定 IPSec 通道。對於 IKEv1 階段 2，請參閱定義 IPSec 加密設定檔。
- （選用）指定防火牆監控 IPSec 通道的方式。請參閱設定通道監控。
- 定義安全性原則以篩選及檢查流量。

如果安全性規則庫的結束處有拒絕規則，除非有另外允許，否則會封鎖區域內流量。允許 *IKE* 和 *IPsec* 應用程式的規則必須包含在拒絕規則之前。

如果您的 *VPN* 流量要通過（而非來源於或終止於）*PA-7000* 系列或 *PA-5200* 系列防火牆，則設定雙向安全性原則，以允許兩個方向上的 *ESP* 或 *AH* 流量。

完成這些工作之後，通道便已準備好可供使用了。系統會根據路由表中的目的地路由，正確自動路由目的地為原則中所定義區域/位址的流量，並將此類流量作為 VPN 流量處理。關於站台對站台 VPN 的範例，請參閱站台對站台 VPN 快速組態。

為了便於進行疑難排解，您可以啟用/停用、重新整理或重新啟動 IKE 閘道或 IPSec 通道。

設定 IKE 閘道

若要設定 VPN 通道，VPN 對等或閘道必須使用預先共用金鑰或數位憑證互相驗證，並建立安全通道，以交涉用於保護每一端主機之間流量的 IPSec 安全性關聯 (SA)。

STEP 1 | 選取 IKE 閘道。

1. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **IKE Gateways**（**IKE** 閘道），**Add**（新增）閘道，並輸入閘道 **Name**（名稱）（**General**（一般）頁籤）。
2. 將 **Version**（版本）設定為 **IKEv1 only mode**（僅 **IKEv1** 模式）、**IKEv2 only mode**（僅 **IKEv2** 模式）或 **IKEv2 preferred mode**（偏好 **IKEv2** 模式）。IKE 閘道會在此處指定的模式下開始與其對等交涉。如果您選取 **IKEv2 preferred mode**（偏好 **IKEv2** 模式），在遠端對等支援 IKEv2 的情況下，兩個對等會使用 IKEv2，否則將會使用 IKEv1。

   您所選取的 **Version**（版本）也會決定您可在 **Advanced Options**（進階選項）頁籤上設定的選項。

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 建立通道（閘道）的本機端點。

1. 選取 **Address Type**（位址類型）：**IPv4** 或 **IPv6**。
2. 在本機閘道所在的防火牆上，選取實體傳出 **Interface**（介面）。
3. 從 **Local IP Address**（本機 **IP** 位址）清單中，選取 VPN 連線將用作端點的 IP 位址；這是面向防火牆上可公開路由的 IP 位址的對外介面。

STEP 3 | 在通道（閘道）的遠端建立對等。

對於 **Peer IP Address Type**（對等 **IP** 位址類型），選取下列一項並輸入對等對應的資訊：

- **IP**—輸入 **Peer Address**（對等位址）（IPv4 或 IPv6 位址），或輸入作為 IPv4 或 IPv6 位址的位址物件。
- **FQDN**—輸入 **Peer Address**（對等位址）（FQDN 字串或使用 FQDN 字串的位址物件）。如果 FQDN 或 FQDN 位址物件解析超過一個 IP 位址，則防火牆會選取下列來自符合 IKE 閘道的位址類型（IPv4 或 IPv6）位址集中的偏好位址：
  - 如果沒有任何交涉的 IKE 安全性關聯 (SA)，則偏好的位址為帶有最小值的 IP 位址。
  - 如果 IKE 閘道使用傳回位址組中的位址，則防火牆會選取該位址（無論它是否為集合中的最小位址）。
  - 如果 IKE 閘道使用傳回位址集以外的位址，則防火牆會選取新位址，該位址是集合中的最小位址。
- **Dynamic**（動態）—如果對等 IP 位址或 FQDN 值未知，請選取 **Dynamic**（動態），以便對等啟動交涉。

使用 *FQDN* 或 *FQDN* 位址物件減少在環境中的問題，在該環境中對等會受制於動態 *IP* 位址變更（並因此需要您重新設定此 *IKE* 閘道對等位址）。

STEP 4 | 指定如何驗證對等。

選取 **Authentication**（驗證）方法：**Pre-Shared Key**（預先共用金鑰）或 **Certificate**（憑證）。如果您選擇預先共用金鑰，則繼續執行下一步。如果選取憑證，則跳至步驟 6，設定基於憑證的驗證。

STEP 5 | 設定預先共用金鑰。

1. 輸入 **Pre-shared Key**（預先共用金鑰），這是用於通道驗證的安全性金鑰。將值重新輸入 **Confirm Pre-shared Key**（確認預先共用金鑰）中。最多使用 255 個 ASCII 或非 ASCII 字元。

   產生字典攻擊難以破解的金鑰；可視需要使用預先共用金鑰。

2. 針對 **Local Identification**（本機識別），從下列類型中選擇，然後輸入您所決定的值：**FQDN (hostname)**（**FQDN**（主機名稱））、**IP address**（**IP** 位址）、**KEYID (binary format ID string in HEX)**（**KEYID**（十六進位的二進位格式 **ID** 字串））以及

©2024 Palo Alto Networks, Inc.

User FQDN (email address)（使用者 **FQDN**（電子郵件地址））。本機識別會定義本機閘道的格式和識別。如果您未指定值，將使用本機 IP 位址作為本機識別值。

3. 針對 **Peer Identification**（對等識別），從下列類型中選擇，然後輸入您所決定的值：**FQDN (hostname)**（**FQDN**（主機名稱））、**IP address**（**IP** 位址）、**KEYID (binary format ID string in HEX)**（**KEYID**（十六進位的二進位格式 **ID** 字串））以及 **User FQDN (email address)**（使用者 **FQDN**（電子郵件地址））。對等識別會定義對等閘道的格式和識別。如果您未指定值，將使用對等 IP 位址作為對等識別值。
4. 繼續執行步驟 7（設定閘道的進階選項）。

STEP 6 | 設定憑證式驗證。

如果您選取了 **Certificate**（憑證），作為對通道另一端的對等閘道進行驗證的方法，請執行此程序中的其餘步驟。

1. 選取已在防火牆上的 **Local Certificate**（本機憑證）、**Import**（匯入）憑證，或 **Generate**（產生）新憑證。
   - 若需 **Import**（匯入）憑證，先匯入憑證供 IKEv2 閘道驗證使用，然後回到此工作。
   - 如果您想要 **Generate**（產生）新憑證，請先在防火牆上產生憑證，然後回到這項工作。
2. （選用）啟用（選取）**HTTP Certificate Exchange**（**HTTP** 憑證交換）以設定雜湊與 URL（僅限 IKEv2）。針對 HTTP 憑證交換，輸入 **Certificate URL**（憑證 **URL**）。如需詳細資訊，請參閱雜湊與 URL 憑證交換。
3. 選取 **Local Identification**（本機識別）類型—**Distinguished Name (Subject), FQDN (hostname)**（辨別名稱（主旨）、**FQDN**（主機名稱））、**IP address**（**IP** 位址）或 **User FQDN (email address)**（使用者 **FQDN**（電子郵件地址）），然後輸入值。本機識別會定義本機閘道的格式和識別。
4. 選取 **Peer Identification**（對等識別）類型—**Distinguished Name (Subject), FQDN (hostname)**（辨別名稱（主旨）、**FQDN**（主機名稱））、**IP address**（**IP** 位址）或 **User FQDN (email address)**（使用者 **FQDN**（電子郵件地址）），然後輸入值。對等識別會定義對等閘道的格式和識別。
5. 指定 **Peer ID Check**（對等 **ID** 檢查）的類型：
   - **Exact**（完全符合）—確保本機設定和對等 IKE ID 承載完全相符。
   - **Wildcard**（萬用字元）—讓對等識別比對出萬用字元 (*) 之前的每個相符字元。萬用字元之後的字元不需要符合。
6. （選用）如果即使對等識別不符合憑證中的對等識別，也仍然想要允許成功的 IKE SA，請 **Permit peer identification and certificate payload identification mismatch**（容許對等識別與憑證承載識別不相符）。
7. 選擇 **Certificate Profile**（憑證設定檔）。憑證設定檔包含關於如何驗證對等閘道的資訊。
8. （選用）若要嚴格控制金鑰的使用方式，請 **Enable strict validation of peer's extended key use**（對對等的擴充金鑰使用方法啟用嚴格驗證）。

©2024 Palo Alto Networks, Inc.

STEP 7 | 設定閘道的進階選項。

1. （選用）若要指定防火牆僅回應 IKE 連線請求而絕不會啟動連線，請在「通用選項」（**Advanced Options**（進階選項））中選取 **Enable Passive Mode**（啟用被動模式）。
2. 如果您有裝置在閘道之間執行 NAT，請 **Enable NAT Traversal**（啟用 **NAT** 周遊），在 IKE 與 UDP 通訊協定上使用 UDP 封裝，使這些通訊協定能通過中繼 NAT 裝置。
3. 若您之前已在步驟 1 中設定 **IKEv1 only mode**（僅 **IKEv1** 模式），則在 IKEv1 頁籤上：
   - 選取 **Exchange Mode**（交換模式）：**auto**（自動）、**aggressive**（加強） 或**main**（主要）。當將防火牆設定為使用 **auto**（自動）交換模式時，它可以接受 **main**（主要）模式與 **aggressive**（加強）模式交涉要求；但若可能，它會在 **main**（主要）模式下啟動交換。

     如果您未將交換模式設為 ***auto***（自動），則必須將對等雙方設為相同的交換模式，才能讓每個對等接受交涉要求。
   - 從 **IKE Crypto Profile**（**IKE** 加密設定檔）清單中選取現有的設定檔或保留預設設定檔。若有必要，您可定義 IKE 加密設定檔。
   - （僅適用於使用憑證式驗證，以及交換模式未設為加強模式的情況）按一下 **Enable Fragmentation**（啟用分散），讓防火牆能操作 IKE 分散功能。
   - 按一下 **Dead Peer Detection**（無效對等偵測），然後輸入 **Interval**（間隔）（範圍為 2 至 100 秒）。對於 **Retry**（重試），請指定在斷開與 IKE 對等的連線之前的重試次數（範圍為 2 到 100）。無效對等偵測功能會識別非使用中或無法使用的 IKE 對等，做法是將 IKE 階段 1通知承載傳送至對等，並等待通知。
4. 如果您在步驟 1 中設定了 **IKEv2 only mode**（僅 **IKEv2** 模式）或 **IKEv2 preferred mode**（偏好 **IKEv2** 模式），則在 IKEv2 頁籤上：
   - 選取 **IKE Crypto Profile**（**IKE** 加密設定檔），這會設定 IKE 階段 1 選項，例如 DH 群組、雜湊演算法和 ESP 驗證。關於 IKE 密碼設定檔的相關資訊，請參閱 IKE 階段 1。
   - （選用）啟用 **Strict Cookie Validation**（嚴格 **Cookie** 驗證）Cookie 啟用臨界值和嚴格 Cookie 驗證。
   - （選用）若要讓閘道將訊息要求傳送至其閘道對等以要求回應，請 **Enable Liveness Check**（啟用活性檢查），然後輸入 **Interval (sec)**（間隔（秒））（預設值為 5）。如有需要，啟動者可嘗試活性檢查至多 10 次。如果沒有回應，啟動者會關閉並刪除 IKE_SA 與 CHILD_SA。啟動者會重新開始寄出另一個 IKE_SA_INIT。

STEP 8 | 按一下 **OK**（確定）並 **Commit**（交付）變更。

匯出憑證讓對等使用雜湊與 URL 加以存取

IKEv2 支援以 雜湊與 URL 憑證交換 作為方法，讓位於通道遠端的對等可從您匯出憑證所在的伺服器擷取憑證。執行這項工作，將您的憑證匯出至該伺服器。您必須已使用 **Device**（裝置） > **Certificate Management**（憑證管理）建立憑證。

 ©2024 Palo Alto Networks, Inc.

STEP 1 | 選取 **Device**（裝置） > **Certificates**（憑證），如果您的平台支援多個虛擬系統，您可以選取適當的虛擬系統作為 **Location**（位置）。

STEP 2 | 在 **Device Certificates**（裝置憑證）頁籤上，選取要 **Export**（匯出）至伺服器的憑證。

憑證的狀態應為有效，而不是已過期。防火牆並不會阻止您匯出無效憑證。

STEP 3 | 針對 **File Format**（檔案格式），選取 **Binary Encoded Certificate (DER)**（二進位編碼憑證 **(DER)**）。

STEP 4 | 將 **Export private key**（匯出私密金鑰）保留為清除。使用「雜湊與 URL」時不一定需要匯出私密金鑰。

STEP 5 | 按一下 **OK**（確定）。

匯出憑證供 IKEv2 閘道驗證使用

如果您要驗證 IKEv2 閘道的對等，但您未在防火牆上使用本機憑證，而想要從他處匯入憑證，請執行此工作。

這項工作假設您已選取 **Network**（網路） > **IKE Gateways**（**IKE** 閘道）、新增閘道，並已針對 **Local Certificate**（本機憑證）按一下 **Import**（匯入）。

STEP 1 | 匯入憑證。

1. 選取 **Network**（網路） > **IKE Gateways**（**IKE** 閘道），**Add**（新增）閘道，然後，在 **General**（一般）頁籤上，針對 **Authentication**（驗證）選取 **Certificate**（憑證）。針對 **Local Certificate**（本機憑證），按一下 **Import**（匯入）。
2. 在匯入憑證視窗中，輸入您所匯入之憑證的 **Certificate Name**（憑證名稱）。
3. 如果要在多個虛擬系統之間共用此憑證，請選取 **Shared**（共用）。
4. 針對 **Certificate File**（憑證檔案），**Browse**（瀏覽）至憑證檔案。按一下檔案名稱，然後按 **Open**（開啟），以填入 **Certificate File**（憑證檔案）欄位。
5. 對於 **File Format**（檔案格式），請選取下列其中一項：
   - **Base64 Encoded Certificate (PEM)**（**Base64** 編碼憑證 **(PEM)**）—包含憑證，但不包含金鑰。這是純文字。
   - **Encrypted Private Key and Certificate (PKCS12)**（加密的私密金鑰與憑證 **(PKCS12)**）—包含憑證與金鑰。
6. 如果私密金鑰位於與憑證檔案不同的檔案中，請選取 **Import private key**（匯入私密金鑰）。金鑰是選用的，但有下列例外：
   - 如果您將 **File Format**（檔案格式）設為 **PEM** (PEM)，則必須匯入金鑰。按一下 **Browse**（瀏覽）並導覽至要匯入的金鑰檔案，以輸入 **Key file**（金鑰檔案）。
   - 輸入 **Passphrase**（複雜密碼）和 **Confirm Passphrase**（確認複雜密碼）。
7. 按一下 **OK**（確定）。

©2024 Palo Alto Networks, Inc.

STEP 2 | 繼續下一項工作。

步驟設定憑證式驗證。

變更 IKEv2 的金鑰存留時間或驗證層級

此工作是選用的；IKEv2 IKE SA 金鑰重設存留時間的預設值為 8 小時。IKEv2 驗證倍數的預設值為 0，表示重新驗證功能停用。詳細資訊，請參閱 SA 金鑰的存留時間和重新驗證間隔。

若要變更預設值，請執行下列工作。先決條件是 IKE 密碼設定檔已存在。

STEP 1 | 變更 IKE 密碼設定檔的金鑰存留時間或驗證層級。

1. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **IKE Crypto**，然後套用至本機閘道的 IKE Crypto 設定檔。
2. 針對 **Key Lifetime**（金鑰存留時間），選取單位（**Seconds**（秒）、**Minutes**（分鐘）、**Hours**（小時）或 **Days**（天）），然後輸入一個值。最小值為三分鐘。
3. 針對 **IKE Authentication Multiple**（**IKE** 驗證倍數）輸入一個值，此值會與存留時間相乘，以決定重新驗證間隔。

STEP 2 | Commit（提交）您的變更。

按一下 **OK**（確定）與 **Commit**（提交）。

變更 IKEv2 的 Cookie 啟用臨界值

如果您想要讓防火牆使用不同於預設值（達到 500 個半開啟的 SA 工作階段之後需要 Cookie 驗證）的臨界值，請執行下列工作。關於 Cookie 驗證的詳細資訊，請參閱 Cookie 啟用臨界值和嚴格 Cookie 驗證。

STEP 1 | 變更 Cookie 啟用臨界值。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Session**（工作階段），然後編輯 VPN Session Settings（VPN 工作階段設定）。針對 **Cookie Activation Threshold**（**Cookie** 啟用臨界值），輸入回應者向啟動者要求 Cookie 之前所允許的半開啟 SA 數目上限（範圍為 0-65535；預設值為 500）。
2. 按一下 **OK**（確定）。

STEP 2 | Commit（提交）您的變更。

按一下 **OK**（確定）與 **Commit**（提交）。

設定 IKEv2 流量選取器

在 IKEv2 中，您可以設定流量選取器，這是在 IKE 交涉期間所使用的網路流量元件。流量選取器可在 CHILD_SA（通道建立）階段 2 期間用來設定通道，以及決定哪些流量可通過通道。兩個 IKE 閘道對等必須互相交涉，並一致同意其流量選取器；否則，其中一方會縮小其位址範圍以達成協議。一個 IKE 連線可以有多個通道；例如，您可以將不同的通道指派給每個部門，以隔離其流量。流量的區隔可讓 QoS 之類的功能得以實作。使用下列工作流程，設定流量選取器。

 ©2024 Palo Alto Networks, Inc.

STEP 1 | 選取 **Network**（網路） > **IPSec Tunnels**（**IPSec** 通道） > **Proxy IDs**（**Proxy ID**）。

STEP 2 | 選取 **IPv4** 或 **IPv6** 頁籤。

STEP 3 | 按一下 **Add**（新增），然後在 **Proxy ID** 欄位中輸入 **Name**（名稱）。

STEP 4 | 在 **Local**（本機）欄位中，輸入 **Source IP Address**（來源 **IP** 位址）。

STEP 5 | 在 **Remote**（遠端）欄位中，輸入 **Destination IP Address**（目的地 **IP** 位址）。

STEP 6 | 在 **Protocol**（通訊協定）欄位中，選取傳輸通訊協定（**TCP** 或 **UDP**）。

STEP 7 | 按一下 **OK**（確定）。

定義密碼設定檔

密碼設定檔會指定用於在兩個 IKE 對等之間進行驗證和/或加密的密碼，以及金鑰的存留時間。每個重新交涉之間的時段稱做存留時間；當指定時間過期時，防火牆將重新交涉一組新的金鑰。

為了保護整個 VPN 通道的通訊，防火牆需要 IKE 與 IPSec 密碼設定檔分別完成 IKE 階段 1 與階段 2 交涉。防火牆包括已可供使用的預設 IKE Crypto 設定檔與預設 IPSec 加密設定檔。

- 定義 IKE 密碼設定檔
- 定義 IPSec 密碼設定檔

定義 IKE 密碼設定檔

IKE 密碼設定檔用於設定在 IKE 階段 1 中交換金鑰程序所使用的加密與驗證演算法，並用於設定金鑰存留時間，亦即金鑰的有效時間。若要呼叫該設定檔，您必須將它附加到 IKE 閘道組態。

當將 *IKE* 閘道的 ***Peer IP Address Type***（對等 ***IP*** 位址類型）設定為 ***Dynamic***（動態）且套用了 *IKEv1* 主要模式或 *IKEv2* 時，在同一介面或本機 *IP* 位址上設定的所有 *IKE* 閘道必須使用相同的密碼設定檔。

STEP 1 | 建立新 IKE 設定檔。

1. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **IKE Crypto**（**IKE** 加密），然後選取 **Add**（新增）。
2. 輸入新設定檔的 **Name**（名稱）。

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 指定金鑰交換的 DH (Diffie‑Hellman) 群組，以及驗證和加密演算法。

在對應的區段（DH 群組、驗證和加密）中按一下 **Add**（新增），然後從功能表中選取。

如果您不確定 VPN 對等所支援的項目，請從最安全到最不安全的順序新增多個群組或演算法；對等會交涉最強的支援群組或演算法來建立通道。

- DH 群組 —
  - **group21**（在僅 IKEv2 模式中）
  - **group20**
  - **group16**（在僅 IKEv2 模式中）
  - **group15**（在僅 IKEv2 模式中）
  - **group19**
  - **group14**
  - **group5**
  - **group2**
  - **group1**
- 驗證—
  - **sha512**
  - **sha384**
  - **sha256**
  - **sha1**
  - **md5**
  - **none**（無）

  如果您選取 *AES-GCM* 演算法用於加密，則必須選取驗證設定 ***none***（無），否則提交將失敗。會基於所選的 *DH* 群組自動選取雜湊。*DH* 群組 *19* 及以下版本使用 ***sha256***；*DH* 群組 *20* 使用 ***sha384***。
- 加密—
  - **aes-256-gcm**（需要 IKEv2；DH 群組應設定為 **group20**）
  - **aes-128-gcm**（需要 IKEv2，並且 DH 群組設定為 **group19**）
  - **aes-256-cbc**
  - **aes-192-cbc**
  - **aes-128-cbc**
  - **3des**

 ©2024 Palo Alto Networks, Inc.

選取對等能夠支援的最強驗證和加密演算法。對於驗證演算法，使用 *SHA-256* 或更高版本（存留時間較長的交易偏好 *SHA-384* 或更高版本）。請勿使用 *SHA-1* 或 *MD5*。對於加密演算法，使用 *AES*；*DES* 以及 *3DES* 強度不夠且存在漏洞。帶有 *Galois/*計數器模式的 *AES (AES-GCM)* 提供最強的安全性並具有內建驗證，因此，如果您選取 ***aes-256-gcm*** 或 ***aes-128-gcm***加密，則必須將驗證設定為 ***none***（無）。

STEP 3 | 指定金鑰的有效期間和重新驗證間隔。

如需詳細資訊，請參閱 SA 金鑰的存留時間和重新驗證間隔。

1. 在 **Key Lifetime**（金鑰存留時間）欄位中，指定金鑰的有效期間（範圍為 3 分鐘到 365 天；預設值為 8 小時）。金鑰過期時，防火牆會重新交涉新的金鑰。存留時間是每次重新交涉之間的期間。
2. 為 **IKEv2 Authentication Multiple**（**IKEv2** 驗證倍數）指定一個值（範圍為 0-50；預設值為 0），此值會與 **Key Lifetime**（金鑰存留時間）相乘，以決定驗證計數。預設值為 0，會停用重新驗證功能。

STEP 4 | 提交 IKE 密碼設定檔。

按一下確定，再按一下提交。

STEP 5 | 將 IKE 密碼設定檔附加至 IKE 閘道組態。

請參閱設定閘道的進階選項。

定義 IPSec 密碼設定檔

IPSec 密碼設定檔會在 IKE 階段 2 中叫用。它會指定當使用自動金鑰 IKE 自動為 IKE SA 產生金鑰時，如何保護通道內資料的安全。

©2024 Palo Alto Networks, Inc.

STEP 1 | 建立新 IPSec 設定檔。

1. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **IPSec Crypto**（**IPSec** 加密），然後選取 **Add**（新增）。
2. 輸入新設定檔的 **Name**（名稱）。
3. 選取您要套用的 **IPSec** 通訊協定—ESP 或 AH—用於當資料在通道之間周遊時保護資料安全。

   作為最佳做法，相比 *AH*（驗證標頭），優先選取 *ESP*（封裝安全有效負載），因為 *ESP* 可同時提供連線機密性與驗證，而 *AH* 只能提供驗證。
4. 按一下 **Add**（新增），然後為 ESP 選取 **Authentication**（驗證）與 **Encryption**（加密）演算法，為 AH 選取 **Authentication**（驗證）演算法，讓 IKE 對等能夠交涉金鑰以安全地在整個通道間傳輸資料。

   如果您不確定 IKE 對等所支援的項目，請依照下列方式，從最安全到最不安全的順序新增多個演算法；對等會交涉最強的支援演算法來建立通道：

   - 加密—**aes-256-gcm**、**aes-256-cbc**、**aes-192-cbc**、**aes-128-gcm**、**aes-128-ccm**（VM-Series 防火牆不支援此選項）、**aes-128-cbc**、**3des**。

     作為最佳做法，選取對等能夠支援的最強驗證和加密演算法。對於驗證演算法，使用 *SHA-256* 或更高版本（存留時間較長的交易偏好 *SHA-384* 或更高版本）。請勿使用 *SHA-1*、*MD5* 或無。對於加密演算法，使用 *AES*；*3DES* 很弱且易受攻擊。
   - 驗證—**sha512**、**sha384**、**sha256**、**sha1**、**md5**。

STEP 2 | 選取在 IKE 階段 2 中用於 IPSec SA 交涉的 DH 群組。

從 **DH Group**（**DH** 群組）中，選取您想要使用的金鑰強度：**group1**、**group2**、 **group5**、**group14**、**group15**、**group16**、**group19**、**group20** 或 **group21**。若要獲得最高的安全性，請選取數字最高的群組。

如果您不想要更新防火牆在 IKE 階段 1 期間建立的金鑰，請選取 **no-pfs**（無 **pfs**）（無 perfect forward secrecy）：防火牆會重複使用目前的金鑰來進行 IPSec 安全性關聯 (SA) 交涉。

STEP 3 | 指定金鑰有效期間— 時間與流量數量。

將時間與流量結合使用，可讓您確保資料安全。

選取 **Lifetime**（存留時間）或金鑰有效的時段，單位為秒、分鐘、小時或天（範圍為 3 分鐘到 365 天）。當過了指定時間後，防火牆會重新交涉一組新的金鑰。

選取生命週期或資料數量，過了此值後必須重新交涉金鑰。

STEP 4 | 提交您的 IPSec 設定檔。

按一下確定，再按一下提交。

 ©2024 Palo Alto Networks, Inc.

STEP 5 | 將 IPSec 設定檔附加至 IPSec 通道組態。

請參閱設定金鑰交換。

設定 IPSec 通道

IPSec 是一套用於保護對等之間通訊的通訊協定。在 IPSec 中，您可以配置各種設定，例如加密和驗證演算法以及安全性關聯逾時。IPSec 模式（通道模式或傳輸模式）就是這樣一種設定。

- 設定 IPSec 通道（通道模式）
- 設定 IPSec 通道（傳輸模式）

設定 **IPSec** 通道（通道模式）

IPSec 通道設定允許您在資料於通道中周遊時驗證和/或加密資料 (IP 封包)。

如果您正在設定防火牆搭配使用支援以原則為基礎 VPN 的對等，您必須定義 Proxy ID。支援以原則為基礎 VPN 的裝置，使用特定的安全性規則/原則或存取清單（來源位址、目的地位址與連接埠）來允許您所要的流量通過 IPSec 通道。在快速模式/IKE 階段 2 交涉期間會參照這些規則，並會在程序的第一或第二個訊息中作為 Proxy-ID 交換這些規則。因此，如果您正在設定防火牆搭配以原則為基礎的 VPN 對等使用，為了讓階段 2 交涉能夠成功，您必須定義 Proxy-ID，讓對等雙方的設定相同。如果未設定 Proxy-ID，由於防火牆支援以路由為基礎的 VPN，因此作為 Proxy-ID 的預設值為 source ip:0.0.0.0/0，destination ip:0.0.0.0/0 且 application: any；當與對等交換這些值時，會造成無法設定 VPN 連線。

STEP 1 | 選取 **Network**（網路） > **IPSec Tunnels**（**IPSec** 通道），然後**Add**（新增）通道組態。

STEP 2 | 在 **General**（一般）頁籤上，輸入通道的 **Name**（名稱）。

©2024 Palo Alto Networks, Inc.

STEP 3 | 選取要在其上設定 IPSec 通道的**Tunnel interface**（通道介面）。

若要建立新通道介面：

1. 選取現有通道介面，或按一下 **Tunnel Interface**（通道介面） > **New Tunnel Interface**（新通道介面）。（您也可以選取 **Network**（網路） > **Interfaces**（介面） > **Tunnel**（通道），然後按一下 **Add**（新增）。）
2. 在 **Interface Name**（介面名稱）欄位中，指定數值尾碼，例如 **.2**。
3. 在 **Config**（組態）頁籤中，選取 **Security Zone**（安全性區域），並以下列方式定義區域：

若要使用您的信任區域作為通道的終止點—請選取該區域。將通道介面與和封包進入防火牆時所在對外介面相同的區域（和虛擬路由器）建立關聯，可減少建立區域間路由的需求。

或者：

為 **VPN** 通道終止建立一個單獨區域（建議）—選取 **New Zone**（新區域），為新區域定義 **Name**（名稱）（例如 vpn-corp)，然後按一下 **OK**（確定）。

1. 針對 **Virtual Router**（虛擬路由器），選取 **default**（預設）。
2. （選用）若要將 IPv4 位址指派給通道介面，則選取 **IPv4** 頁籤，**Add**（新增） IP 位址及網路遮罩，例如 10.31.32.1/32。
3. 按一下 **OK**（確定）。

STEP 4 | （選用）在通道介面上啟用 IPv6。

1. 在 **Network**（網路） > **Interfaces**（介面） > **Tunnel**（通道） > **IPv6** 上選取 IPv6 頁籤。
2. 選取 **Enable IPv6 on the interface**（在介面上啟用 **IPv6**）。

   此選項可讓您透過 IPv4 IPSec 通道路由 IPv6 流量，並且將提供 IPv6 網路之間的機密性。IPv6 流量先由 IPv4 封裝，再由 ESP 封裝。若要將 IPv6 流量路由至通道，您可以使用對通道的靜態路由，或使用 OSPFv3，或使用基於原則的轉送 (PBF) 規則。
3. 以十六進位格式輸入 64 位元延伸唯一 **Interface ID**（介面 **ID**），例如，00:26:08:FF:FE:DE:4E:29。依預設，防火牆將使用從實體介面的 MAC 位址所產生的 EUI-64。
4. 若要指派 IPv6 **Address**（位址），則 **Add**（新增） IPv6 位址及首碼長度，例如 2001:400:f00::1/64。如果未選取首碼，會將指定給介面的 IPv6 位址全部指定在位址文字方塊中。
   1. 選取 **Use interface ID as host portion**（使用介面 **ID** 作為主機部分），將 IPv6 位址指定給將使用介面 ID 作為位址主機部分的介面。
   2. 選取 **Anycast**（任播）來包括最近節點中的路由。

 ©2024 Palo Alto Networks, Inc.

STEP 5 | 設定金鑰交換。

在 **General**（一般）頁籤上，設定下列其中一種金鑰交換類型：

設定自動金鑰交換

1. 選取 IKE 閘道。若要設定 IKE 閘道，請參閱設定 IKE 閘道。
2. （選用）選取預設的 IPSec Crypto 設定檔。若要建立新 IPSec 設定檔，請參閱 定義 IPSec 密碼設定檔。

設定手動金鑰交換

1. 指定 **Local SPI**（本機 **SPI**） 作為本地防火牆。SPI 是 32 位元的十六進位索引，加入 IPSec 通道的標頭中以協助區分 IPSec 流量；SPI 用於建立在建立 VPN 通道時所需的 SA。
2. 選取要做為通道端點的 **Interface**（介面），並選擇性選取通道端點的本地介面　IP 位址。
3. 選取要使用的通訊協定—**AH** 或 **ESP**。
4. 若為 AH，請選取 **Authentication**（驗證）方法，然後依序輸入 **Key**（金鑰）與 **Confirm Key**（確認金鑰）。
5. 若為 ESP，請選取 **Authentication**（驗證）方法，然後依序輸入 **Key**（金鑰）與 **Confirm Key**（確認金鑰）。接著選取 **Encryption**（加密）方法，然後視需要依序輸入 **Key**（金鑰）與 **Confirm Key**（確認金鑰）。
6. 指定 **Remote SPI**（遠端 **SPI**） 作為遠端對等。
7. 輸入 **Remote Address**（遠端位址），亦即遠端對等的 IP 位址。

STEP 6 | 防禦重播攻擊。

防重播是 IPsec 的子通訊協定，是網際網路工程任務推動小組 (IETF) 要求註解 (RFC) 6479 的一部分。防重播通訊協定用於防止駭客注入或變更從來源傳送到目的地的封包，並使用單向安全性關聯，以便在網路中的兩個節點之間建立安全連線。

建立安全連線之後，防重播通訊協定會使用封包序號來擊敗重播攻擊。當來源傳送訊息時，會將一個序號新增到其封包；序號從 0 開始，每個後續封包遞增 1。目的地會以滑動視窗格式保留數字序列及保留已驗證之接收封包的序號記錄，並拒絕序號低於滑動視窗中最低序號的所有封包（太舊的封包）或已經顯示在滑動視窗中的封包（重複或重播的封包）。接受的封包在經過驗證之後，會更新滑動視窗，如果視窗已滿，則將取代視窗中的最低序號。

1. 在一般頁籤上，選取 **Show Advanced Options**（顯示進階選項），然後選取 **Enable Replay Protection**（啟用重播防護）偵測與撤銷重播攻擊。
2. 選取要使用的 **Anti Replay Window**（反重播視窗）。您可以選取大小為 64、128、256、512、1024、2048 或 4096 的反重播視窗。預設值為 1024。

 ©2024 Palo Alto Networks, Inc.

STEP 7 | （選用）保留 [服務類型] 標頭以安排處理 IP 封包的優先順序。

在顯示進階選項區段中，選取 **Copy TOS Header**（複製 **TOS** 標頭）。這會複製服務類型 (TOS) 標頭從封裝封包的內部 IP 標頭複製到外部 IP 標頭，以保留原始 TOS 資訊。

如果通道內存在多個工作階段（每個通道具有不同的 *TOS* 值），複製 *TOS* 標頭可能導致 *IPSec* 封包無序到達。

STEP 8 | 預設情況下，如果未設定 IPSec 模式，IPSec 通道將以 **Tunnel**（通道）模式啟動。您還可以在 **Show Advanced Options**（顯示進階選項）區段中針對 **IPSec Mode**（**IPSec** 模式）選擇 **Tunnel**（通道），以在通道模式下建立 IPSec。

STEP 9 | （選用）選取 **Add GRE Encapsulation**（新增 **GRE** 封裝）以在 IPSec 上啟用 GRE。

如果遠端端點要求在 IPSec 加密流量前將流量封裝到 GRE 通道，則新增 GRE 封裝。例如，某些實作要求在 IPSec 加密多點傳送流量前對其進行封裝。當封裝於 IPSec 的 GRE 封包之來源 IP 位址和目的地 IP 位址與封裝 IPSec 通道相同時，新增 GRE 封裝。

STEP 10 | 啟用通道監控。

您必須將 *IP* 位址指派給通道介面，才能進行監控。

若向裝置管理員警示通道失敗，並提供自動容錯移轉到其他通道介面的功能：

1. 選取 **Tunnel Monitor**（通道監控）。
2. 指定通道另一端的 **Destination IP**（目的地 **IP**位址），以監控通道是否正常運作。
3. 選取 **Profile**（設定檔）以決定通道失敗時的動作。若要建立新設定檔，請參閱 定義 通道監控設定檔。

 ©2024 Palo Alto Networks, Inc.

STEP 11 | 建立 Proxy ID 以識別 VPN 對等。

只有 VPN 對等使用基於原則的 VPN 時，才需要執行此步驟。

1. 選取 **Network**（網路） > **IPSec Tunnels**（**IPSec** 通道），然後按一下 **Add**（新增）。
2. 選取 **Proxy ID** 頁籤。
3. 選取 **IPv4** 或 **IPv6** 頁籤。
4. 按一下 **Add**（新增），然後輸入 **Proxy ID** 名稱。
5. 輸入 VPN 閘道的 **Local**（本機）IP 位址或子網路。
6. 輸入 VPN 閘道的 **Remote**（遠端）位址。
7. 選取 **Protocol**（通訊協定）：
   - 號碼—指定通訊協定號碼（用於與第三方裝置交互操作）。
   - 任何—允許 TCP 與/或 UDP 流量。
   - **TCP**—指定本機連接埠和遠端連接埠號碼。
   - **UDP**—指定本機連接埠和遠端連接埠號碼。
8. 按一下 **OK**（確定）。

STEP 12 | Commit（提交）您的變更。

按一下 **OK**（確定）與 **Commit**（提交）。

設定 IPSec 通道（傳輸模式）

在設定 IPSec 通道時，您現在可以選擇 IPSec 模式作為通道，或選擇傳輸模式以建立安全連線。即您可以選擇在傳輸模式或通道模式中對封包進行加密或驗證。PAN-OS® 預設支援通道模式，而傳輸模式是從 PAN-OS 11.0 版本開始引入的新選項。

傳輸模式支援：

- 僅 IPv4 位址。
- 僅裝安全有效負載 (ESP) 通訊協定。
- 僅限 IKEv2。
- DH-group 20 用於 Diffie-Hellman (DH) 群組和完整轉寄密碼 (PFS)。
- 在 GCM 模式下僅支援具有 256 位元金鑰的 AES。

您可以根據您的網路需求選擇 IPSec 模式：

- 如果要對新世代防火牆之間切換的管理平面通訊協定（如 OSPF）進行加密，則必須設定 IPSec 傳輸模式。傳輸模式使您能夠使用最穩健的通訊協定加密控制流量（例如路由通訊協定和訊號訊息）。使用傳輸模式，您可以加密屬於防火牆 IP 位址的點對點流量。
- 如果要加密在新世代防火牆之間傳輸的資料平面流量，則必須設定 IPSec 通道模式。

通道和傳輸模式之間的差異

 ©2024 Palo Alto Networks, Inc.

通道模式	傳輸方式
加密整個封包，包括 IP 標頭。加密後的封包中會新增一個新的 IP 標頭。	僅加密有效負載，同時保留原始 IP 標頭。
通道監控使用通道介面 IP 位址。	通道監控自動使用實體介面的 IP 位址（閘道介面 IP 位址），忽略通道介面 IP 位址。
支援雙重封裝。	不支援雙重封裝。
此模式通常用於站點到站點通訊。	此模式通常用於主機到主機通訊。

啟用傳輸模式之前要記住的要點：

- 啟用 NAT-T 時無法選擇傳輸模式。
- 啟用傳輸模式後，您無法將回送介面設定為 IPSec 通道。
- 您只能將傳輸模式與 **auto-key** 金鑰交換一起使用。
- 您應該在 **Transport**（傳輸）模式下啟用 **Add GRE Encapsulation**（新增 **GRE** 封裝）以封裝多點傳送封包。
- 如果您設定沒有 IPSec 通道的 IKE 閘道，預設情況下 IKE 會交涉通道模式子安全性關聯 (SA)。
- 在 IPSec 傳輸模式下，如果在通道介面中設定 BGP 路由，則流量不會流動。當為 BGP 路由使用 IPSec 傳輸模式時，在實體介面（例如，ethernet 1/1）而不是通道介面上設定 BGP 路由。BGP 路由的 IPSec 通道模式適用於通道介面，而 BGP 路由的 IPSec 傳輸模式僅適用於實體介面。
- 預設情況下，IPSec 通道以 **Tunnel**（通道）模式運作。

由於 PAN-OS 11.0 及更早版本不支援傳輸模式，因此如果降級至之前的任何版本都會導致相容性問題。在降級之前，您必須手動移除任何傳輸模式通道或切換到通道模式。否則，降級將導致故障。

STEP 1 | 選取 **Network**（網路） > **IPSec Tunnels**（**IPSec** 通道），然後**Add**（新增）通道組態。

STEP 2 | 在 **General**（一般）頁籤上，輸入通道的 **Name**（名稱）。

©2024 Palo Alto Networks, Inc.

STEP 3 | 選取要在其上設定 IPSec 通道的**Tunnel interface**（通道介面）。

若要建立新通道介面：

1. 選取現有通道介面，或按一下 **Tunnel Interface**（通道介面） > **New Tunnel Interface**（新通道介面）。（您也可以選取 **Network**（網路） > **Interfaces**（介面） > **Tunnel**（通道），然後按一下 **Add**（新增）。）
2. 在 **Interface Name**（介面名稱）欄位中，指定數值尾碼，例如 **.2**。
3. 在 **Config**（組態）頁籤中，選取 **Security Zone**（安全性區域），並以下列方式定義區域：

若要使用您的信任區域作為通道的終止點—請選取該區域。將通道介面與和封包進入防火牆時所在對外介面相同的區域（和虛擬路由器）建立關聯，可減少建立區域間路由的需求。

或者：

為 **VPN** 通道終止建立一個單獨區域（建議）—選取 **New Zone**（新區域），為新區域定義 **Name**（名稱）（例如 vpn-corp)，然後按一下 **OK**（確定）。

1. 針對 **Virtual Router**（虛擬路由器），選取 **default**（預設）。
2. （選用）若要將 IPv4 位址指派給通道介面，則選取 **IPv4** 頁籤，**Add**（新增） IP 位址及網路遮罩，例如 10.31.32.1/32。

   在傳輸模式下，您不需要為通道介面設定位址（即使您啟用了通道監控選項）。PAN-OS 會忽略在通道模式下設定的任何通道介面 IP 位址。
3. 按一下 **OK**（確定）。

STEP 4 | 設定金鑰交換。

在 **General**（一般）頁簽上，設定自動金鑰交換：

設定自動金鑰交換

1. 選取 IKE 閘道。若要設定 IKE 閘道，請參閱設定 IKE 閘道。
2. （選用）選取預設的 IPSec Crypto 設定檔。若要建立新 IPSec 設定檔，請參閱 定義 IPSec 密碼設定檔。

您只能將傳輸模式與 auto-key 交換一起使用。

STEP 5 | 防禦重播攻擊。

防重播是 IPsec 的子通訊協定，是網際網路工程任務推動小組 (IETF) 要求註解 (RFC) 6479 的一部分。防重播通訊協定用於防止駭客注入或變更從來源傳送到目的地的封包，並使用單向安全性關聯，以便在網路中的兩個節點之間建立安全連線。

建立安全連線之後，防重播通訊協定會使用封包序號來擊敗重播攻擊。當來源傳送訊息時，會將一個序號新增到其封包；序號從 0 開始，每個後續封包遞增 1。目的地會以滑動視窗格式保留數字序列及保留已驗證之接收封包的序號記錄，並拒絕序號低於滑動視窗中最低序號的所有

 ©2024 Palo Alto Networks, Inc.

封包（太舊的封包）或已經顯示在滑動視窗中的封包（重複或重播的封包）。接受的封包在經過驗證之後，會更新滑動視窗，如果視窗已滿，則將取代視窗中的最低序號。

1. 在一般頁籤上，選取 **Show Advanced Options**（顯示進階選項），然後選取 **Enable Replay Protection**（啟用重播防護）偵測與撤銷重播攻擊。
2. 選取要使用的 **Anti Replay Window**（反重播視窗）。您可以選取大小為 64、128、256、512、1024、2048 或 4096 的反重播視窗。預設值為 1024。

STEP 6 | （選用）保留 [服務類型] 標頭以安排處理 IP 封包的優先順序。

在顯示進階選項區段中，選取 **Copy TOS Header**（複製 **TOS** 標頭）。這會複製服務類型 (TOS) 標頭從封裝封包的內部 IP 標頭複製到外部 IP 標頭，以保留原始 TOS 資訊。

如果通道內存在多個工作階段（每個通道具有不同的 *TOS* 值），複製 *TOS* 標頭可能導致 *IPSec* 封包無序到達。

STEP 7 | 在 **Show Advanced Options**（顯示進階選項）區段中，針對 **IPSec Mode**（**IPSec** 模式）選擇 **Transport**（傳輸）以在傳輸模式下建立 IPSec 通道。

STEP 8 | （選用）選取 **Add GRE Encapsulation**（新增 **GRE** 封裝）以在 IPSec 上啟用 GRE。

如果遠端端點要求在 IPSec 加密流量前將流量封裝到 GRE 通道，則新增 GRE 封裝。例如，某些實作要求在 IPSec 加密多點傳送流量前對其進行封裝。當封裝於 IPSec 的 GRE 封包之來源 IP 位址和目的地 IP 位址與封裝 IPSec 通道相同時，新增 GRE 封裝。

由於 IPSec 傳輸模式會重複使用封包的 IP 標頭，因此它不能像 OSPF 那樣封裝多點傳送封包。要封裝多點傳送封包，啟用 IPSec 通道的 **GRE Encapsulation**（**GRE** 封裝）選項，以先將封包轉換為單點傳送 GRE 封包（將使用通道介面的 IP 位址）。請注意，不能先使用單獨的 GRE 通道封裝封包，再將其轉送到傳輸模式通道。由於 IPSec 傳輸模式不支援雙重封裝，所以無法使用雙重封裝。上述 **GRE Encapsulation**（**GRE** 封裝）選項之所以有效，是因為 PAN-OS 將其視為單個封裝。

STEP 9 | 啟用通道監控。

傳輸模式下的通道監控自動使用實體介面的 IP 位址（閘道介面 IP），忽略通道介面 IP 位址。因此，沒有必要為通道介面指派 IP 位址。

若向裝置管理員警示通道失敗，並提供自動容錯移轉到其他通道介面的功能：

1. 選取 **Tunnel Monitor**（通道監控）。
2. 指定通道另一端的 **Destination IP**（目的地 **IP**位址），以監控通道是否正常運作。
3. 選取 **Profile**（設定檔）以決定通道失敗時的動作。若要建立新設定檔，請參閱 定義 通道監控設定檔。

STEP 10 | Commit（提交）您的變更。

按一下 **OK**（確定）與 **Commit**（提交）。

©2024 Palo Alto Networks, Inc.

設定通道監控

若要提供不中斷 VPN 服務，您可以使用防火牆上的無效對等偵測功能及通道監控功能。您也可以監控通道狀態。以下幾節將監控工作進行說明：

- 定義通道監控設定檔
- 檢視通道狀態

定義通道監控設定檔

通道監控設定檔可讓您驗證 VPN 對等之間的連線；您可以設定通道介面每隔指定間隔即偵測目的地 IP 位址，並指定如果整個通道通訊中斷時應採取的動作。

STEP 1 | 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **Monitor**（監控）。預設通道監控設定檔可供使用。

STEP 2 | 按一下 **Add**（新增），然後輸入設定檔的 **Name**（名稱）。

STEP 3 | 選取無法連線目的地 IP 位址時要執行的 **Action**（動作）。

- 等待復原—防火牆等待通道復原。防火牆會繼續使用路由決策中的通道介面，如同通道仍然運作中。
- 容錯移轉—如果有可用路徑，強制流量進入備用路徑。防火牆會停用通道介面，並因此停用路由表中任何使用該介面的路由器。

無論是哪一種狀況，防火牆都會嘗試交涉新的 IPSec 金鑰來加速復原。

STEP 4 | 指定觸發指定的動作 **Interval (sec)**（間隔（秒））與 **Threshold**（臨界值）。

- **Threshold**（臨界值）指定了在採取指定動作之前，要等待的活動訊號數（範圍為 2-100；預設值為 5）。
- **Interval (sec)**（間隔（秒））指定活動訊號之間的時間（單位為秒；範圍為 2-10；預設值為 3）。

STEP 5 | 將監控設定檔附加至 IPsec 通道組態。請參閱 啟用通道監控。

檢視通道狀態

通道狀態會告知您是否已建立有效的 IKE 階段 1 與階段 2 SA，以及通道介面是否有運作且可供傳遞流量。

由於通道介面是邏輯介面，所以無法指示實體連結狀態。因此，您必須啟用通道監控，讓通道介面能夠驗證對 IP 位址的連線，並判定路徑是否仍能使用。如果 IP 位址無法連線，防火牆會等待通道復原或容錯移轉。發生容錯移轉時，現有的通道會被卸除，然後觸發路由變更以設定新的通道並將流量重新導向。

STEP 1 | 選取 **Network**（網路） > **IPSec Tunnels**（ **IPSec** 通道）。（網路 > IPSec 通道）

©2024 Palo Alto Networks, Inc.

STEP 2 | 檢視**Tunnel Status**（通道狀態）。

- 綠色表示有效的 IPSec SA 通道。
- 紅色表示 IPSec SA 無法使用或已過期。

STEP 3 | 檢視 **IKE Gateway Status**（**IKE** 閘道狀態）。

- 綠色表示有效的 IKE 階段 1 SA。
- 紅色表示 IKE 階段 1 SA 無法使用或已過期。

STEP 4 | 檢視 **Tunnel Interface Status**（通道介面狀態）。

- 綠色表示通道介面有運作。
- 紅色表示由於已啟用通道監控，且狀態為關閉，因此通道介面已關閉。

若要疑難排解尚未運作的 VPN 通道，請參閱判讀 VPN 錯誤訊息。

啟用/停用、重新整理或重新啟動 IKE 閘道或 IPSec 通道

您可以啟用、停用、重新整理或重新啟動 IKE 閘道或 IPSec 通道，以便進行疑難排解。

- 啟用或停用 IKE 閘道或 IPSec 通道
- 重新整理及重新啟動行為
- 重新整理或重新啟動 IKE 閘道或 IPSec 通道

啟用或停用 **IKE** 閘道或 **IPSec** 通道

您可以啟用或停用 IKE 閘道或 IPSec 通道，以便進行疑難排解。

啟用或停用 IKE 閘道。

1. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **IKE Gateways**（**IKE** 閘道），然後選取您要啟用或停用的閘道。
2. 在畫面底部按一下 **Enable**（啟用）或 **Disable**（停用）。

啟用或停用 IPSec 通道。

1. 選取 **Network**（網路） > **IPSec Tunnels**（**IPSec** 通道），然後選取您要啟用或停用的通道。
2. 在畫面底部按一下 **Enable**（啟用）或 **Disable**（停用）。

重新整理及重新啟動行為

您可以啟用/停用、重新整理或重新啟動 IKE 閘道或 IPSec 通道。IKE 閘道和 IPSec 通道的重新整理與重新啟動行為如下：

©2024 Palo Alto Networks, Inc.

階段	重新整理	重新啟動
IKE 閘道（IKE 階段 1）	更新所選 IKE 閘道的螢幕統計資料。 相當於在 CLI 中發出第二個 `show` 命令 (在初始 `show` 命令之後)。	重新啟動選取的 IKE 閘道。 **IKEv2**:也會重新啟動任何相關聯的子 IPSec 安全性關聯 (SA)。 **IKEv1**:不會重新啟動相關聯的 IPSec SA。 重新啟動會中斷所有現有的工作階段。 相當於在 CLI 中發出 **`clear`**、**`test`**、**`show`** 命令序列。
IPSec 通道（IKE 階段 2）	更新所選 IPSec 通道的螢幕統計資料。 相當於在 CLI 中發出第二個 `show` 命令 (在初始 `show` 命令之後)。	重新啟動 IPSec 通道。 重新啟動會中斷所有現有的工作階段。 相當於在 CLI 中發出 **`clear`**、**`test`**、**`show`** 命令序列。

重新整理或重新啟動 IKE 閘道或 IPSec 通道

請注意，重新啟動 IKE 閘道的結果視乎於是 IKEv1 還是 IKEv2。請參閱重新整理及重新啟動行為，以瞭解 IKE 閘道（IKEv1 和 IKEv2）以及 IPSec 通道。

重新整理或重新啟動 IKE 閘道。

1. 選取 **Network**（網路） > **IPSec Tunnels**（**IPSec** 通道），然後為您要重新整理或重新啟動的閘道選取通道。
2. 在該通道的列中，按一下狀態欄下方的 **IKE Info**（**IKE** 資訊）。
3. 在 IKE 資訊畫面底部，按一下您要的動作：
   - 重新整理—更新畫面上的統計資料。
   - 重新啟動—清除 SA，在 IKE 交涉重新開始且通道重新建立之前捨棄流量。

©2024 Palo Alto Networks, Inc.

重新整理或重新啟動 IPSec 通道。

由於您使用通道監控器來監控通道狀態，或使用外部網路監控器來監控透過 IPSec 通道的網路連線狀態，因此您可能會判斷通道需要重新整理或重新啟動。

1. 選取 **Network**（網路） > **IPSec Tunnels**（**IPSec** 通道），然後選取您要重新整理或重新啟動的通道。
2. 在該通道的列中，按一下狀態欄下方的 **Tunnel Info**（通道資訊）。
3. 在通道資訊畫面底部，按一下您要的動作：
   - 重新整理—更新螢幕統計資料。
   - 重新啟動—清除 SA，在 IKE 交涉重新開始且通道重新建立之前捨棄流量。

測試 VPN 連線

執行此工作以測試 VPN 連線。

STEP 1 | ping 通道另一端的主機或使用下列 CLI 命令啟動 IKE 階段 1：

```
test vpn ike-sa gateway <gateway_name>
```

STEP 2 | 輸入下列命令，測試是否已設定 IKE 階段 1：

```
show vpn ike-sa gateway <gateway_name>
```

檢查輸出中是否顯示安全性關聯。如果沒有，則檢閱系統日誌訊息以判讀失敗原因。

STEP 3 | ping 通道另一端的主機或使用下列 CLI 命令啟動 IKE 階段 2：

```
test vpn ipsec-sa tunnel <tunnel_name>
```

STEP 4 | 輸入下列命令，測試是否已設定 IKE 階段 2：

```
show vpn ipsec-sa tunnel <tunnel_name>
```

檢查輸出中是否顯示安全性關聯。如果沒有，則檢閱系統日誌訊息以判讀失敗原因。

STEP 5 | 若要檢視 VPN 流量資訊，請使用下列命令：

```
show vpn flow total tunnels configured:            1 filter - type
 IPSec, state any total IPSec tunnel configured:       1 total
 IPSec tunnel shown:                1 name                    id
      state      local-ip       peer-ip       tunnel-i/f
 ------------------------------------------------------------------------
 vpn-to-siteB       5       active
    100.1.1.1     200.1.1.1     tunnel.41
```


©2024 Palo Alto Networks, Inc.

判讀 VPN 錯誤訊息

下表列出系統日誌中記錄的常見 VPN 錯誤訊息。

表 **3: VPN** 問題的系統日誌錯誤訊息

如果錯誤是：	請嘗試：

`IKE phase-1 negotiation is failed as initiator, main mode.Failed SA: x.x.x.x[500]-y.y.y.y[500] cookie:84222f276c2fa2e9:0000000000000000 due to timeout.`
或
`IKE phase 1 negotiation is failed.Couldn’ t find configuration for IKE phase-1 request for peer IP x.x.x.x[1929]`
	• 確認 IKE 閘道組態中每個 VPN 對等的公開 IP 位址皆正確。
	• 確認可 ping 到 IP 位址，且路由問題不會造成連線失敗。

`Received unencrypted notify payload (no proposal chosen) from IP x.x.x.x(500) to y.y.y.y(500), ignored...`
或
`IKE phase-1 negotiation is failed.Unable to process peer’ s SA payload.`
	檢查 IKE 密碼設定檔組態，確認雙方的提案有共同的加密、驗證及 DH 群組提案。

`pfs group mismatched:my:2peer:0`
或
`IKE phase-2 negotiation failed when processing SA payload.No suitable proposal found in peer’ s SA payload.`
	檢查 IPSec Crypto 設定檔組態以確認：
	• VPN 對等雙方的 pfs 為啟用或停用
	• 每個對等提案的 DH 群組至少有一個共用的 DH 群組

`IKE phase-2 negotiation failed when processing Proxy ID.Received local id x.x.x.x/x type IPv4 address protocol 0 port 0, received remote id y.y.y.y/y type IPv4 address protocol 0 port 0.`	某一端的 VPN 對等使用的是基於原則的 VPN。您必須在 Palo Alto Networks 防火牆上設定 Proxy ID。請參閱建立 Proxy ID 以識別 VPN 對等體。

©2024 Palo Alto Networks, Inc.

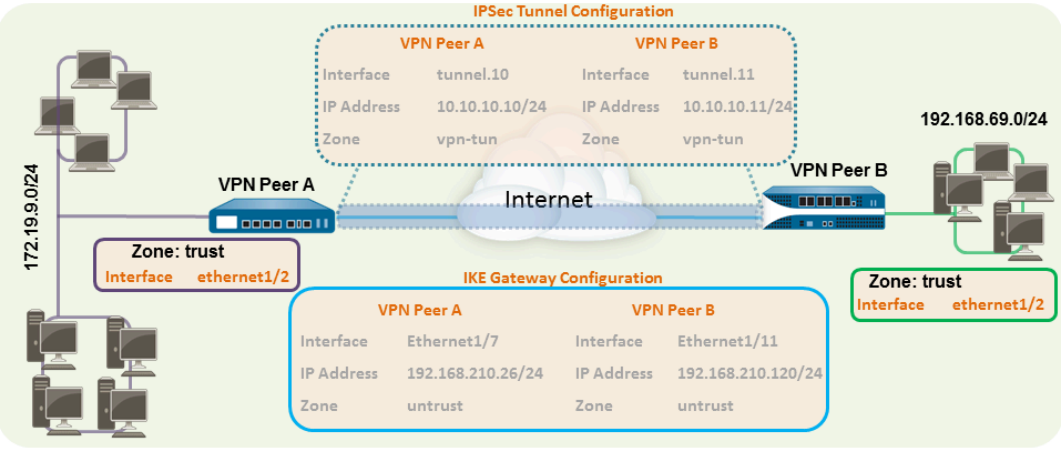
站台對站台 VPN 快速設定

以下幾節提供設定某些常用 VPN 部署的說明：

- 含靜態路由的站台對站台 VPN
- 含 OSPF 的站台對站台 VPN
- 含靜態與動態路由的站台對站台 VPN

含靜態路由的站台對站台 VPN

以下範例顯示使用靜態路由的兩個站台之間的 VPN 連線。在沒有動態路由的狀況下，VPN 對等 A 與 VPN 對等 B 上的通道介面不需要 IP 位址，因為防火牆會自動使用通道介面作為在站台之間路由流量的下一個躍點。但是為了啟用通道監控，已將靜態 IP 位址指派給每個通道介面。



 ©2024 Palo Alto Networks, Inc.

STEP 1 | 設定 Layer 3 介面。

此介面用於 IKE 階段 1 通道。

1. 選取**Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），然後選取您要為 VPN 設定的介面。
2. 從 **Interface Type**（介面類型）中選取 **Layer3**。
3. 在 **Config**（組態）頁籤上，選取介面所屬的 **Security Zone**（安全性區域）：
   - 介面必須可從您信任網路之外的區域存取。請考慮建立專用的 VPN 區域以取得可見度，並控制您的 VPN 流量。
   - 如果您尚未建立區域，請從 **Security Zone**（安全性區域）中選取 **New Zone**（新區域），為新區域定義 **Name**（名稱），然後按一下 **OK**（確定）。
4. 選取要使用的 **Virtual Router**（虛擬路由器）。
5. 若要將 IP 位址指定至介面，請選取 **IPv4** 頁籤，在 [IP] 區段中按一下 **Add**（新增），然後輸入 IP 位址及網路遮罩以指定至介面，例如 192.168.210.26/24。
6. 若要儲存介面設定，請按一下 **OK**（確定）。

   在此範例中，VPN 對等 A 的組態為：
   - 介面—ethernet1/7
   - 安全性區域—不信任
   - 虛擬路由器—預設值
   - **IPv4**—192.168.210.26/24

   VPN 對等 B 的組態為：
   - 介面—ethernet1/11
   - 安全性區域—不信任
   - 虛擬路由器—預設值
   - **IPv4**—192.168.210.120/24

©2024 Palo Alto Networks, Inc.

STEP 2 | 建立通道介面，並附加至虛擬路由器與安全性區域。

1. 選取 **Network**（網路） > **Interfaces**（介面） > **Tunnel**（通道），然後按一下 **Add**（新增）。
2. 在 **Interface Name**（介面名稱）欄位中，指定數值尾碼，例如 **.1**。
3. 在 **Config**（組態）頁籤中，展開 **Security Zone**（安全性區域），並以下列方式定義區域：
   - 若要使用您的信任區域作為通道的終止點，請選取該區域。
   - （建議）若要為另外建立一個區域終止 VPN，請按一下 **New Zone**（新區域）。在 Zone（區域）對話方塊中，定義新區域的 **Name**（名稱）（例如 *vpn-tun*），然後按一下 **OK**（確定）。
4. 選取 **Virtual Router**（虛擬路由器）。
5. （選用）若要將 IP 位址指定至通道介面，請選取 **IPv4** 或 **IPv6** 頁籤，按一下 [IP] 區段中按一下**Add**（新增），然後輸入要指派給介面的 IP 位址及網路遮罩。

   在使用靜態路由的狀況下，通道介面不需要 IP 位址。對於目的地為指定子網路/IP 位址的流量，通道介面不會自動變成下一個躍點。如果您想要啟用通道監控，請考慮新增 IP 位址。
6. 若要儲存介面設定，請按一下 **OK**（確定）。

   在此範例中，VPN 對等 A 的組態為：
   - **Interface**（介面）—tunnel.10
   - 安全性區域—vpn_tun
   - 虛擬路由器—預設值
   - **IPv4**—172.19.9.2/24

   VPN 對等 B 的組態為：
   - 介面—tunnel.11
   - 安全性區域—vpn_tun
   - 虛擬路由器—預設值
   - **IPv4**—192.168.69.2/24

©2024 Palo Alto Networks, Inc.

STEP 3 | 設定虛擬路由器上對目的地子網路的靜態路由。

1. 選取 **Network**（網路） > **Virtual Router**（虛擬路由器），然後按一下您在前一步中定義的路由器。
2. 選取靜態路由，按一下新增，然後輸入新路由以存取通道另一端的子網路。

   在此範例中，VPN 對等 A 的組態為：

   - 目的地—192.168.69.0/24
   - **Interface**（介面）—tunnel.10

   VPN 對等 B 的組態為：

   - **Destination**（目的地）—172.19.9.0/24
   - 介面—tunnel.11

STEP 4 | 設定 Crypto 設定檔（IKE 加密設定檔適用於階段 1，IPSec Crypto 設定檔適用於階段 2）。

在對等雙方完成此工作，並確定設定相同的值。

1. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **IKE Crypto**（**IKE** 加密）。在此範例中，我們使用預設設定檔。
2. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **IPSec Crypto**（**IPSec** 加密）。在此範例中，我們使用預設設定檔。

STEP 5 | 設定 IKE 閘道。

1. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **IKE Gateway**（**IKE** 閘道）。
2. 按一下 **Add**（新增），然後在設定 **General**（一般）頁籤中選項。

   在此範例中，VPN 對等 A 的組態為：

   - 介面—ethernet1/7
   - 本機 **IP** 位址—192.168.210.26/24
   - 對等 **IP** 類型/位址—靜態/192.168.210.120
   - 預先共用金鑰—輸入值
   - 本機識別—請注意，這表示將使用本機 IP 位址作為本機識別值。
   - VPN 對等 B 的組態為：
   - 介面—ethernet1/11
   - 本機 **IP** 位址—192.168.210.120/24
   - 對等 **IP** 類型/位址—靜態/192.168.210.26
   - 先共用金鑰—輸入與對等 A 相同的值
   - 本機識別—無
3. 選取進階階段 **1** 選項，然後選取您先前建立用於 IKE 階段 1 的 IKE 加密設定檔。

©2024 Palo Alto Networks, Inc.

STEP 6 | 設定 IPSec 通道。

1. 選取 **Network**（網路） > **IPSec Tunnels**（ **IPSec** 通道）。
2. 按一下 **Add**（新增），然後在設定 **General**（一般）頁籤中選項。

   在此範例中，VPN 對等 A 的組態為：

   - **Tunnel Interface**（通道介面）—tunnel.10
   - 類型—自動金鑰
   - **IKE** 閘道—選取下述定義的 IKE 閘道。
   - **IPSec Crypto Profile**（**IPSec** 加密設定檔）—選取在步驟 4 中定義的 IPSec 加密設定檔。

   VPN 對等 B 的組態為：

   - **Tunnel Interface**（通道介面）—tunnel.11
   - 類型—自動金鑰
   - **IKE** 閘道—選取下述定義的 IKE 閘道。
   - **IPSec Crypto Profile**（**IPSec** 加密設定檔）—選取在步驟 4 中定義的 IPSec 加密設定檔。
3. （選用）選取 **Show Advanced Options**（顯示進階選項），然後選取 **Tunnel Monitor**（通道監控器），並指定要偵測的目的地 IP 位址以驗證連線。一般而言，會為 VPN 對等使用通道介面 IP 位址。
4. （選用）若要定義無法建立連線時的動作，請參閱定義通道監控設定檔。

STEP 7 | 建立要允許站台（子網路）之間流量的原則。

1. 選取 **Policies**（原則） > **Security**（安全性）。
2. 建立規則以針對源自於指定來源與目的地 IP 位址的流量，允許不信任區域與 vpn-tun 區域之間的流量。

STEP 8 | 提交任何擱置中的組態變更。

按一下 **Commit**（交付）。

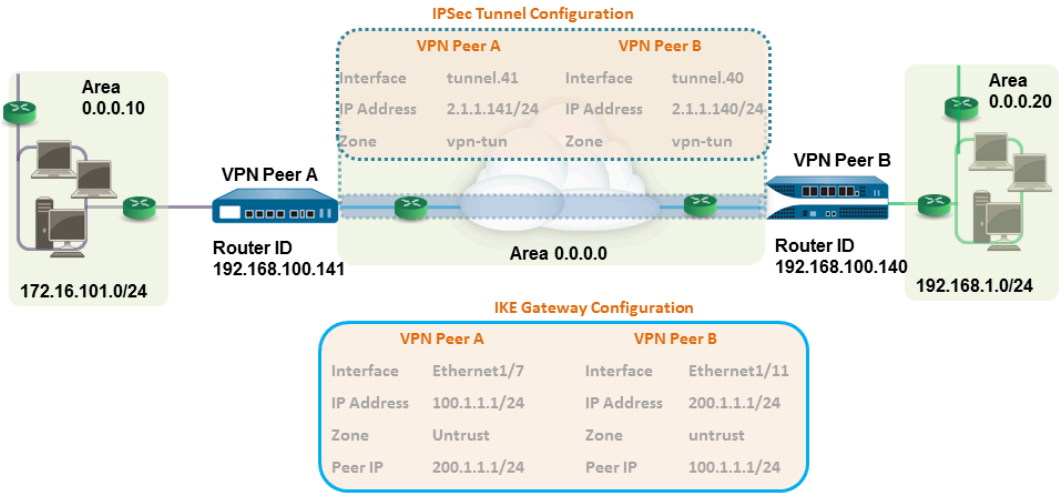
STEP 9 | 測試 VPN 連線。

另請參閱檢視通道狀態。

含 OSPF 的站台對站台 VPN

在此範例中，每個站台會使用 OSPF 進行動態路由流量。系統會靜態指派每個 VPN 對等上的通道 IP 位址，並作為兩個站台之間路由流量時的下一個躍點。

©2024 Palo Alto Networks, Inc.



STEP 1 | 在每個防火牆上設定 Layer 3 介面。

1. 選取**Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），然後選取您要為 VPN 設定的介面。
2. 從 **Interface Type**（介面類型）清單中選取 **Layer3**。
3. 在 **Config**（組態）頁籤上，選取介面所屬的 **Security Zone**（安全性區域）：
   - 介面必須可從您信任網路之外的區域存取。請考慮建立專用的 VPN 區域以取得可見度，並控制您的 VPN 流量。
   - 如果您尚未建立區域，請從 **Security Zone**（安全性區域）清單中選取 **New Zone**（新區域），為新區域定義 **Name**（名稱），然後按一下 **OK**（確定）。
4. 選取要使用的 **Virtual Router**（虛擬路由器）。
5. 若要將 IP 位址指定至介面，請選取 **IPv4** 頁籤，在 [IP] 區段中按一下 **Add**（新增），然後輸入 IP 位址及網路遮罩以指定至介面，例如 192.168.210.26/24。
6. 若要儲存介面設定，請按一下 **OK**（確定）。

   在此範例中，VPN 對等 A 的組態為：
   - 介面—ethernet1/7
   - 安全性區域—不信任
   - 虛擬路由器—預設值
   - **IPv4**—100.1.1.1/24

   VPN 對等 B 的組態為：
   - 介面—ethernet1/11
   - 安全性區域—不信任
   - 虛擬路由器—預設值
   - **IPv4**—200.1.1.1/24

©2024 Palo Alto Networks, Inc.

STEP 2 | 建立通道介面，並附加至虛擬路由器與安全性區域。

1. 選取 **Network**（網路） > **Interfaces**（介面） > **Tunnel**（通道），然後按一下 **Add**（新增）。
2. 在 **Interface Name**（介面名稱）欄位中，指定數值尾碼，例如 **.11**。
3. 在 **Config**（組態）頁籤中，展開 **Security Zone**（安全性區域），並以下列方式定義區域：
   - 若要使用您的信任區域作為通道的終止點，請選取該區域。
   - （建議）若要為另外建立一個區域終止 VPN，請按一下 **New Zone**（新區域）。在區域對話方塊中，定義新區域的 **Name**（名稱）（例如 vpn-tun），然後按一下 **OK**（確定）。
4. 選取 **Virtual Router**（虛擬路由器）。
5. 將 IP 位址指派給通道介面，選取 **IPv4** 或 **IPv6** 頁籤，按一下 IP 區段的 **Add**（新增），然後輸入要指派給介面的 IP 位址及網路遮罩/首碼，例如 172.19.9.2/24。

   此 IP 位址將作為將流量路由至通道的下一個躍點 IP 位址，也可用於監控通道狀態。
6. 若要儲存介面設定，請按一下 **OK**（確定）。

   在此範例中，VPN 對等 A 的組態為：
   - **Interface**（介面）—tunnel.41
   - 安全性區域—vpn_tun
   - 虛擬路由器—預設值
   - **IPv4**—2.1.1.141/24

   VPN 對等 B 的組態為：
   - **Interface**（介面）—tunnel.40
   - 安全性區域—vpn_tun
   - 虛擬路由器—預設值
   - **IPv4**—2.1.1.140/24

STEP 3 | 設定 Crypto 設定檔（IKE 加密設定檔適用於階段 1，IPSec Crypto 設定檔適用於階段 2）。

在對等雙方完成此工作，並確定設定相同的值。

1. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **IKE Crypto**（**IKE** 加密）。在此範例中，我們使用預設設定檔。
2. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **IPSec Crypto**（**IPSec** 加密）。在此範例中，我們使用預設設定檔。

©2024 Palo Alto Networks, Inc.

STEP 4 | 在虛擬路由器上設定 OSPF 設定，並在防火牆上附加含適當介面的 OSPF 區域。

如需防火牆上可用 OSPF 選項的詳細資訊，請參閱設定 OSPF。

當有兩個以上的 OSPF 路由器需要交換路由資訊時，請使用 (廣播) 作為連結類型。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後選取預設路由器或新增路由器。
2. 選取 **OSPF**（適用於 IPv4）或 **OSPFv3**（適用於 Ipv6），然後選取 **Enable**（啟用）。
3. 在此範例中，VPN 對等 A 的 OSPF 組態為：
   - **Router ID**（路由器 **ID**）：192.168.100.141
   - **Area ID**（區域 **ID**）：0.0.0.0，指派給 tunnel.1 介面，連結類型為：p2p
   - **Area ID**（區域 **ID**）：0.0.0.10，指派給 Ethernet1/1 介面，連結類型為：廣播

   VPN 對等 B 的 OSPF 組態為：
   - **Router ID**（路由器 **ID**）：192.168.100.140
   - **Area ID**（區域 **ID**）：0.0.0.0，指派給 tunnel.1 介面，連結類型為：p2p
   - **Area ID**（區域 **ID**）：0.0.0.20，指派給 Ethernet1/15 介面，連結類型為：廣播

STEP 5 | 設定 IKE 閘道。

此範例在 VPN 對等雙方使用靜態 IP 位址。一般而言，總公司會使用靜態設定的 IP 位址，分公司則使用動態設定的 IP 位址；動態 IP 位址並不適用於設定穩定服務，例如 VPN。

1. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **IKE Gateway**（**IKE** 閘道）。
2. 按一下 **Add**（新增），然後在設定 **General**（一般）頁籤中選項。

   在此範例中，VPN 對等 A 的組態為：
   - 介面—ethernet1/7
   - 本地 **IP** 位址—100.1.1.1/24
   - 對等 **IP** 位址—200.1.1.1/24
   - 預先共用金鑰—輸入值

   VPN 對等 B 的組態為：
   - 介面—ethernet1/11
   - **Local IP address**（本機 **IP** 位址）—200.1.1.1/24
   - **Peer IP address**（對等 **IP** 位址）—100.1.1.1/24
   - 先共用金鑰—輸入與對等 A 相同的值
3. 選取您先前建立用於 IKE 階段 1 的 IKE 密碼設定檔。

©2024 Palo Alto Networks, Inc.

STEP 6 | 設定 IPSec 通道。

1. 選取 **Network**（網路） > **IPSec Tunnels**（ **IPSec** 通道）。
2. 按一下 **Add**（新增），然後在設定 **General**（一般）頁籤中選項。

   在此範例中，VPN 對等 A 的組態為：

   - **Tunnel Interface**（通道介面）—tunnel.41
   - 類型—自動金鑰
   - **IKE** 閘道—選取下述定義的 IKE 閘道。
   - **IPSec Crypto** 設定檔—選取上述定義的 IKE 閘道。

   VPN 對等 B 的組態為：

   - 通道介面—tunnel.40
   - 類型—自動金鑰
   - **IKE** 閘道—選取下述定義的 IKE 閘道。
   - **IPSec Crypto** 設定檔—選取上述定義的 IKE 閘道。
3. 選取 **Show Advanced Options**（顯示進階選項），然後選取 **Tunnel Monitor**（通道監控器），並指定要 ping 的目的地 IP 位址以驗證連線。
4. 若要定義無法建立連線時的動作，請參閱定義通道監控設定檔。

STEP 7 | 建立要允許站台（子網路）之間流量的原則。

1. 選取 **Policies**（原則） > **Security**（安全性）。
2. 建立規則以針對源自於指定來源與目的地 IP 位址的流量，允許不信任區域與 vpn-tun 區域之間的流量。

©2024 Palo Alto Networks, Inc.

STEP 8 | 使用 CLI 確認 OSPF 相鄰項與路由。

確認兩個防火牆都能看見彼此為完整狀態的網路芳鄰。亦確認 VPN 對等通道介面的 IP 位址與 OSPF 路由器 ID。在每個 VPN 對等上使用下列 CLI 命令。

- **show routing protocol ospf neighbor**

```
admin@FW-A> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.140
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.140
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no

admin@FW-B> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.141
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.141
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no
```

- **show routing route type ospf**

```
admin@FW-A> show routing route type ospf

flags: A:active, ?:loose, C:connect, H:host, S:static, ~:internal, R:rip, O:ospf, B:bgp,
       Oi:ospf intra-area, Oo:ospf inter-area, O1:ospf ext-type-1, O2:ospf ext-type-2


VIRTUAL ROUTER: vr1 (id 1)
  ==========
destination             nexthop             metric flags      age   interface          next-AS
2.1.1.0/24              0.0.0.0                 10   Oi       6760  tunnel.41
172.16.101.0/24         0.0.0.0                 10   Oi       6854  ethernet1/1
192.168.1.0/24          2.1.1.140               20 A Oo       6754  tunnel.40
total routes shown: 3
    admin@FW-B> show routing route type ospf

    flags: A:active, C:connect, H:host, S:static, R:rip, O:ospf,
           Oi:ospf intra-area, Oo:ospf inter-area, O1:ospf ext-type-1, O2:ospf ext-type-2


    VIRTUAL ROUTER: vr1 (id 1)
      ==========
    destination             nexthop             metric flags      age   interface
    2.1.1.0/24              0.0.0.0                 10      Oi       20033 tunnel.40
    172.16.101.0/24         2.1.1.141               20     AOo       6896  tunnel.40
    192.168.1.0/24          0.0.0.0                 10      Oi       8058  ethernet1/15
    total routes shown: 3
```


©2024 Palo Alto Networks, Inc.

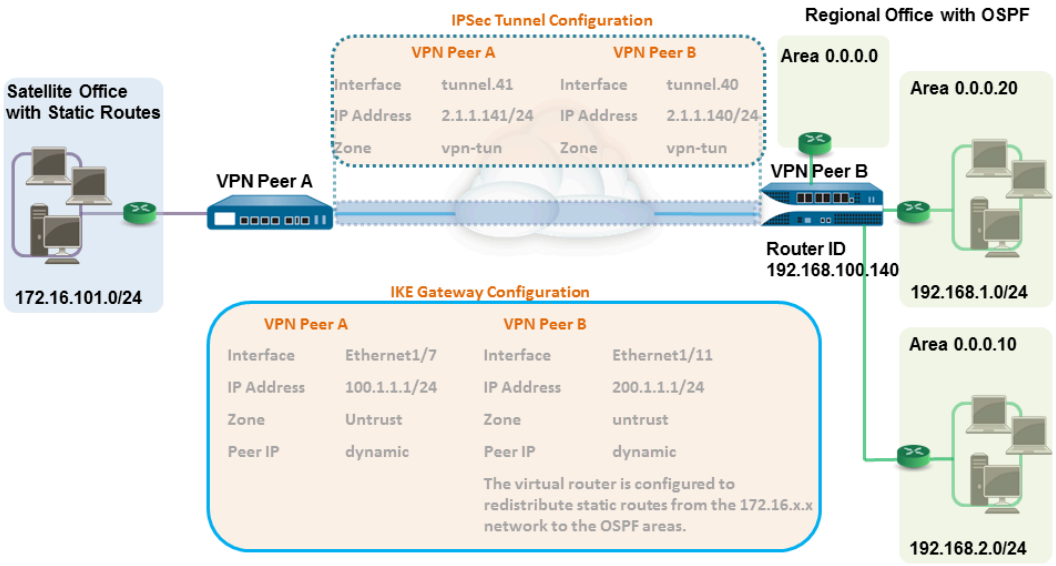
STEP 9 | 測試 VPN 連線。

請參閱設定通道連線以及檢視通道狀態。

含靜態與動態路由的站台對站台 VPN

在此範例中，一個站台使用靜態路由，另一個站台使用 OSPF。當兩個位置之間的路由通訊協定不相同時，則必須以靜態 IP 位置設定每個防火牆上的通道介面。因此，為了能交換路由資訊，必須以重新散佈設定檔設定靜態與動態路由程序皆參與的防火牆。設定重新散佈設定檔時，請讓虛擬路由器重新散佈及篩選通訊協定之間的路由—靜態路由、連線的路由及主機—從靜態自發系統到 OSPF 自發系統。若無此重新散佈設定檔，則每個通訊協定會獨自運作，不會與在相同虛擬路由器上執行的其他通訊協定交換任何路由資訊。

在此範例中，衛星辦公室有靜態路由，且所有目的地為 192.168.x.x 網路的流量會路由至 tunnel.41。VPN 對等 B 的虛擬路由器會同時參與靜態和動態路由程序，並用重新散佈設定檔設定，以便將靜態路由傳播 (匯出) 至 OSPF 自發系統。



 ©2024 Palo Alto Networks, Inc.

STEP 1 | 在每個防火牆上設定 Layer 3 介面。

1. 選取**Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），然後選取您要為 VPN 設定的介面。
2. 從 **Interface Type**（介面類型）中選取 **Layer3**。
3. 在 **Config**（組態）頁籤上，選取介面所屬的 **Security Zone**（安全性區域）：
   - 介面必須可從您信任網路之外的區域存取。請考慮建立專用的 VPN 區域以取得可見度，並控制您的 VPN 流量。
   - 如果您尚未建立區域，請從 **Security Zone**（安全性區域）中選取 **New Zone**（新區域），為新區域定義 **Name**（名稱），然後按一下 **OK**（確定）。
4. 選取要使用的 **Virtual Router**（虛擬路由器）。
5. 若要將 IP 位址指定至介面，請選取 **IPv4** 頁籤，在 [IP] 區段中按一下 **Add**（新增），然後輸入 IP 位址及網路遮罩以指定至介面，例如 192.168.210.26/24。
6. 若要儲存介面設定，請按一下 **OK**（確定）。

   在此範例中，VPN 對等 A 的組態為：
   - 介面—ethernet1/7
   - 安全性區域—不信任
   - 虛擬路由器—預設值
   - **IPv4**—100.1.1.1/24

   VPN 對等 B 的組態為：
   - 介面—ethernet1/11
   - 安全性區域—不信任
   - 虛擬路由器—預設值
   - **IPv4**—200.1.1.1/24

STEP 2 | 設定 Crypto 設定檔（IKE 加密設定檔適用於階段 1，IPSec Crypto 設定檔適用於階段 2）。

在對等雙方完成此工作，並確定設定相同的值。

1. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **IKE Crypto**（**IKE** 加密）。在此範例中，我們使用預設設定檔。
2. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **IPSec Crypto**（**IPSec** 加密）。在此範例中，我們使用預設設定檔。

©2024 Palo Alto Networks, Inc.

STEP 3 | 設定 IKE 閘道。

使用預先共用金鑰時，在設定 IKE 階段 1 通道時若要新增驗證監督，您可以設定（本地識別）與（對等識別）屬性，以及在 IKE 交涉程序中比對的對應值。

1. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **IKE Gateway**（**IKE** 閘道）。
2. 按一下 **Add**（新增），然後在設定 **General**（一般）頁籤中選項。

   在此範例中，VPN 對等 A 的組態為：

   - 介面—ethernet1/7
   - 本地 **IP** 位址—100.1.1.1/24
   - 對等 **IP** 類型—動態
   - 預先共用金鑰—輸入值
   - 本機識別—選取 **FQDN(hostname)**（**FQDN**（主機名稱)），然後輸入 VPN 對等 A 的值。
   - 對等識別—選取 **FQDN(hostname)**（**FQDN**（主機名稱)），然後輸入 VPN 對等 B 的值

   VPN 對等 B 的組態為：

   - 介面—ethernet1/11
   - **Local IP address**（本機 **IP** 位址）—200.1.1.1/24
   - 對等 **IP** 位址—動態
   - 先共用金鑰—輸入與對等 A 相同的值
   - 本機識別—選取 **FQDN(hostname)**（**FQDN**（主機名稱）），然後輸入 VPN 對等 B 的值
   - 對等識別—選取 **FQDN(hostname)**（**FQDN**（主機名稱）），然後輸入 VPN 對等 A 的值
3. 選取您先前建立用於 IKE 階段 1 的 IKE 密碼設定檔。

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 建立通道介面，並附加至虛擬路由器與安全性區域。

1. 選取 **Network**（網路） > **Interfaces**（介面） > **Tunnel**（通道），然後按一下 **Add**（新增）。
2. 在 **Interface Name**（介面名稱）欄位中，指定數值尾碼，例如 **.41**。
3. 在 **Config**（組態）頁籤中，展開 **Security Zone**（安全性區域），並以下列方式定義區域：
   - 若要使用您的信任區域作為通道的終止點，請選取該區域。
   - （建議）若要為另外建立一個區域終止 VPN，請按一下 **New Zone**（新區域）。在 Zone（區域）對話方塊中，定義新區域的 **Name**（名稱）（例如 *vpn-tun*），然後按一下 **OK**（確定）。
4. 選取 **Virtual Router**（虛擬路由器）。
5. 將 IP 位址指派給通道介面，選取 **IPv4** 或 **IPv6** 頁籤，按一下 IP 區段的 **Add**（新增），然後輸入要指派給介面的 IP 位址及網路遮罩/首碼，例如 172.19.9.2/24。

   此 IP 位址將用於將流量路由至通道及監控通道狀態。
6. 若要儲存介面設定，請按一下 **OK**（確定）。

   在此範例中，VPN 對等 A 的組態為：
   - **Interface**（介面）—tunnel.41
   - 安全性區域—vpn_tun
   - 虛擬路由器—預設值
   - **IPv4**—2.1.1.141/24

   VPN 對等 B 的組態為：
   - **Interface**（介面）—tunnel.42
   - 安全性區域—vpn_tun
   - 虛擬路由器—預設值
   - **IPv4**—2.1.1.140/24

STEP 5 | 指定將流量路由至 192.168.x.x 網路上目的地的介面。

1. 在 VPN 對等 A 上，選取虛擬路由器。
2. 選取 **Static Routes**（靜態路由），再按一下 **Add**（新增），將 tunnel.41 新增為用於路由流量的 **Interface**（介面），並以 192.168.x.x 網路為 **Destination**（目的地）。

©2024 Palo Alto Networks, Inc.

STEP 6 | 在虛擬路由器上設定靜態路由與 OSPF 設定，並在防火牆上附加含適當介面的 OSPF 區域。

1. 在 VPN 對等體 B 上，選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後選取預設路由器或新增路由器。
2. 選取 **Static Routes**（靜態路由），然後按一下 **Add**（新增）將通道 IP 位址新增為 172.168.x.x. 網路中流量的下一個躍點。

   指派所需的路由公制；使用的值愈小，在轉送表格中路由選擇的優先順序愈高。
3. 選取 **OSPF**（適用於 IPv4）或 **OSPFv3**（適用於 Ipv6），然後選取 **Enable**（啟用）。
4. 在此範例中，VPN 對等 # 的 OSPF 組態為：
   - 路由器 ID：192.168.100.140
   - 區域 ID：0.0.0.0，指派給 Ethernet1/12 介面，連結類型為：廣播
   - 區域 ID：0.0.0.10，指派給 Ethernet1/1 介面，連結類型為：廣播
   - 區域 ID：0.0.0.20，指派給 Ethernet1/15 介面，連結類型為：廣播

STEP 7 | 建立重新散佈設定檔，用於將靜態路由插入到 OSPF 自發系統。

1. 在 VPN 對等 B 建立重新散佈設定檔。
   1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後選取上述使用的路由器。
   2. 選取 **Redistribution Profiles**（重新散佈設定檔），然後按一下 **Add**（新增）。
   3. 輸入設定檔名稱，選取 **Redist**（重新散佈），然後指派 **Priority**（優先順序）值。如果您設定了多個設定檔，第一個會比對優先順序值最小的設定檔。
   4. 將 **Source Type**（來源類型）設為 **static**（靜態），然後按一下 **OK**（確定）。將使用步驟 6 中所定義的靜態路由進行重新散佈。
2. 將靜態路由插入到 OSPF 系統中。
   1. 選取 **OSPF** > **Export Rules**（匯出規則）（適用於 IPv4）或 **OSPFv3** > **Export Rules**（匯出規則）（適用於 IPv6）。
   2. 按一下 **Add**（新增），然後選取您剛剛建立的重新散佈設定檔。
   3. 選取將外部路由帶入 OSPF 系統中的方式。預設選項為 **Ext2**，僅使用外部公制計算路由總成本。若內部與外部 OSPF 公制都要使用，請使用 **Ext1**。
   4. 為插入到 OSPF 系統中的路由指派 **Metric**（公制）（成本值）。此選項可讓您在插入的路由進入 OSPF 系統時變更其公制。
   5. 按一下 **OK**（確定）。

©2024 Palo Alto Networks, Inc.

STEP 8 | 設定 IPSec 通道。

1. 選取 **Network**（網路） > **IPSec Tunnels**（ **IPSec** 通道）。
2. 按一下 **Add**（新增），然後在設定 **General**（一般）頁籤中選項。

   在此範例中，VPN 對等 A 的組態為：

   - **Tunnel Interface**（通道介面）—tunnel.41
   - 類型—自動金鑰
   - **IKE** 閘道—選取下述定義的 IKE 閘道。
   - **IPSec Crypto** 設定檔—選取上述定義的 IKE 閘道。

   VPN 對等 B 的組態為：

   - 通道介面—tunnel.40
   - 類型—自動金鑰
   - **IKE** 閘道—選取下述定義的 IKE 閘道。
   - **IPSec Crypto** 設定檔—選取上述定義的 IKE 閘道。
3. 選取 **Show Advanced Options**（顯示進階選項），然後選取 **Tunnel Monitor**（通道監控器），並指定要 ping 的目的地 IP 位址以驗證連線。
4. 若要定義無法建立連線時的動作，請參閱定義通道監控設定檔。

STEP 9 | 建立要允許站台（子網路）之間流量的原則。

1. 選取 **Policies**（原則） > **Security**（安全性）。
2. 建立規則以針對源自於指定來源與目的地 IP 位址的流量，允許不信任區域與 vpn-tun 區域之間的流量。

©2024 Palo Alto Networks, Inc.

STEP 10 | 使用 CLI 確認 OSPF 相鄰項與路由。

確認兩個防火牆都能看見彼此為完整狀態的網路芳鄰。亦確認 VPN 對等通道介面的 IP 位址與 OSPF 路由器 ID。在每個 VPN 對等上使用下列 CLI 命令。

- **show routing protocol ospf neighbor**

```
admin@FW-A> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.140
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.140
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no

admin@FW-B> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.141
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.141
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no
```

- **show routing route**

以下為每個 VPN 對等的輸出範例。

```
VPN PeerA

destination             next hop        metric  flags   age     interface       next-AS
192.168.1.0/24          2.1.1.141       20      A S             tunnel.41
192.168.2.0/24          2.1.1.141       20      A S             tunnel.41
172.16.101.0/24         0.0.0.0         1       A H             ethernet1/1
2.1.1.140/24            2.1.1.141       20      A S             tunnel.41

VPN PeerB

destination             next hop        metric  flags   age     interface       next-AS
192.168.1.0/24          0.0.0.0         10      A Oo            ethernet1/1
192.168.2.0/24          0.0.0.0         10      A Oo            ethernet1/15
172.16.101.0/24         2.1.1.140       20      A H             tunnel.40
2.1.1.141/24            2.1.1.140       10      A C             tunnel.40
```

STEP 11 | 測試 VPN 連線。

請參閱設定通道連線以及檢視通道狀態。

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

大規模 VPN (LSVPN)

Palo Alto Networks 新一代防火牆上的 GlobalProtect 大規模 VPN (LSVPN) 功能簡化了傳統的中心點與軸輻式 VPN 架構，讓您能夠快速部署含有數個分公司的企業網路，只需在遠端衛星上進行少許組態即能達成。此解決方案使用憑證驗證防火牆，使用 IPSec 保護資料安全。

LSVPN 允許在兩個 Palo Alto Networks 防火牆之間建立站點對站點 VPN。若要在 Palo Alto Networks 防火牆與另一個裝置之間建立站點對站點 VPN，請參閱 VPN。LSVPN 不需要 GlobalProtect 訂閱。

下列主題說明 LSVPN 元件與如何設定元件，藉以在 Palo Alto Networks 防火牆之間建立站點對站點 VPN 服務：

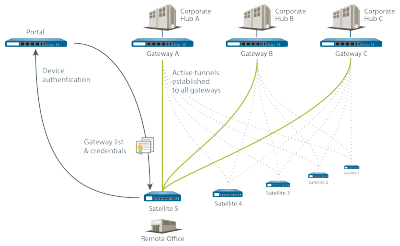
- LSVPN 概要介紹
- 建立 LSVPN 的介面與區域
- 啟用 GlobalProtect LSVPN 元件之間的 SSL
- 設定入口網站以驗證衛星
- 為 LSVPN 設定 GlobalProtect 閘道
- 為 LSVPN 設定 GlobalProtect 入口網站
- 備妥衛星以加入 LSVPN
- 驗證 LSVPN 組態
- LSVPN 快速設定

LSVPN 概要介紹

GlobalProtect 有完整的基礎結構，可管理從遠端站台對公司資源的安全存取。此基礎結構包含下列元件：

- **GlobalProtect** 入口網站—提供多種功能管理您的 GlobalProtect LSVPN 基礎結構。參與 GlobalProtect LSVPN 的每個衛星都能從入口網站接收組態資訊，包括能夠讓衛星 (軸輻) 連線到閘道 (中心點) 的組態資訊。您可在任何 Palo Alto Networks 新一代防火牆上的介面上設定入口網站。
- **GlobalProtect** 閘道—Palo Alto Networks 防火牆，可為衛星連線提供通道對等。衛星存取的資源受到閘道上安全性原則的保護。不需要另外的入口網站與閘道；一個防火牆可同時作為入口網站與閘道。
- **GlobalProtect** 衛星—位於遠端站台的 Palo Alto Networks 防火牆，能與位於您公司辦公室的閘道建立 IPSec 通道，以保護存取中央資源的安全性。衛星防火牆上的組態規模很小，讓您能夠快速、輕鬆地隨著新增站台來調整您的 VPN。

下圖說明 GlobalProtect LSVPN 元件如何運作。



©2024 Palo Alto Networks, Inc.

建立 LSVPN 的介面與區域

您必須為 LSVPN 基礎結構設定下列介面與區域：

- **GlobalProtect** 入口網站—需要讓 GlobalProtect 衛星連線的 Layer 3 介面。如果入口網站與閘道位於同一個防火牆上，它們便可以使用相同介面。入口網站必須位於可從您分公司存取的區域中。
- **GlobalProtect** 閘道—需要三個介面：位於遠端衛星可連線區域中的 Layer 3 介面、位於連線至受保護資源之信任區域中的內部介面，以及用於從衛星終止 VPN 通道的邏輯通道介面。不同於其他站台對站台 VPN 解決方案，GlobalProtect 閘道只需要單一通道介面，閘道將為您所有遠端衛星的通道連線使用此介面（單點對多點）。如果您打算使用動態路由，您必須將 IP 位址指派給通道介面。對於通道介面，GlobalProtect 支援 IPv6 和 IPv4 定址。
- **GlobalProtect** 衛星—需要單一通道介面與遠端閘道建立 VPN (最多可以有 25 個閘道)。如果您打算使用動態路由，您必須將 IP 位址指派給通道介面。對於通道介面，GlobalProtect 支援 IPv6 和 IPv4 定址。

關於入口網站、閘道與衛生的詳細資訊，請參閱 LSVPN 概要介紹。

STEP 1 | 設定 Layer 3 介面。

入口網站與每個閘道及衛星都需要 Layer 3 介面，才能讓流量在站台之間路由。

如果閘道與入口網站位於同一個防火牆上，您可以為這兩個元件使用單一介面。

1. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），然後選取您要為 GlobalProtect LSVPN 設定的介面。
2. 從 **Interface Type**（介面類型）下拉式清單中選取 **Layer3**。
3. 在 **Config**（組態）頁籤上，選取介面所屬的 **Security Zone**（安全性區域）：
   - 介面必須可從您信任網路之外的區域存取。請考慮建立專用的 VPN 區域以取得可見度，並控制您的 VPN 流量。
   - 如果您尚未建立區域，請從 **Security Zone**（安全性區域）下拉式清單中選取 **New Zone**（新區域），為新區域定義 **Name**（名稱），然後按一下 **OK**（確定）。
4. 選取要使用的 **Virtual Router**（虛擬路由器）。
5. 為介面指派 IP 位址：
   - 對於 IPv4 位址，選取 **IPv4**，然後 **Add**（新增）要指派給介面的 IP 位址和網路遮罩，例如 203.0.11.100/24。
   - 對於 IPv6 位址，選取 **IPv6**，**Enable IPv6 on the interface**（在介面上啟用 **IPv6**），然後 **Add**（新增）要指派給介面的 IP 位址和網路遮罩，例如 2001:1890:12f2:11::10.1.8.160/80。
6. 若要儲存介面設定，請按一下 **OK**（確定）。

©2024 Palo Alto Networks, Inc.

STEP 2 | 在裝載 GlobalProtect 閘道的防火牆上設定邏輯通道介面，用於終止由 GlobalProtect 衛星建立的 VPN 通道。

通道介面上不需要 *IP* 位址，除非您打算使用動態路由。但是，將 *IP* 位址指派給通道介面對於疑難排解連線問題很有用。

確定在 *VPN* 通道終止的區域中啟用 *User-ID*。

1. 選取 **Network**（網路） > **Interfaces**（介面） > **Tunnel**（通道），然後按一下 **Add**（新增）。
2. 在 **Interface Name**（介面名稱）欄位中，指定數值尾碼，例如 **.2**。
3. 在 **Config**（組態）頁籤中，展開 **Security Zone**（安全性區域）下拉式清單，並以下列方式定義區域：
   - 若要使用您的信任區域作為通道的終止點，請從下拉式清單中選取該區域。
   - （建議）若要為另外建立一個區域終止 VPN，請按一下 **New Zone**（新區域）。在 [區域] 對話方塊中，定義新區域的 **Name**（名稱）（例如 *lsvpn-tun*），選取 **Enable User Identification**（啟用使用者識別）核取方塊，然後按一下 **OK**（確定）。
4. 選取 **Virtual Router**（虛擬路由器）。
5. （選用）為通道介面指派 IP 位址：
   - 對於 IPv4 位址，選取 **IPv4**，然後 **Add**（新增）要指派給介面的 IP 位址和網路遮罩，例如 203.0.11.100/24。
   - 對於 IPv6 位址，選取 **IPv6**，**Enable IPv6 on the interface**（在介面上啟用 **IPv6**），然後 **Add**（新增）要指派給介面的 IP 位址和網路遮罩，例如 2001:1890:12f2:11::10.1.8.160/80。
6. 若要儲存介面設定，請按一下 **OK**（確定）。

STEP 3 | 如果您已經建立另外的區域讓通道終止 VPN 連線，請建立安全性原則讓流量在 VPN 區域與您的信任區域之間流動。

例如，原則規則允許 *lsvpn-tun* 區域與 *L3-Trust* 區域之間的流量。

STEP 4 | Commit（提交）您的變更。

按一下 **Commit**（交付）。

©2024 Palo Alto Networks, Inc.

啟用 GlobalProtect LSVPN 元件之間的 SSL

GlobalProtect 元件之間所有的互動都是透過 SSL/TLS 連線發生的。因此，您必須先產生和/或安裝必要的憑證，再設定每個元件，讓您可以為每個元件參照設定中適當的憑證和/或憑證設定檔。下列各節說明各種 GlobalProtect 憑證的支援憑證部署方法、說明及最佳做法指南，並提供產生與部署必要憑證的指示：

- 關於憑證部署
- 將伺服器憑證部署至 GlobalProtect LSVPN 元件
- 使用 SCEP 將用戶端憑證部署至 GlobalProtect 衛星

關於憑證部署

為 GlobalProtect LSVPN 部署憑證的基本方法有兩種：

- 企業憑證授權單位 — 如果您已經有自己的企業憑證授權單位，您可以使用此內部 CA 為 GlobalProtect 入口網站簽發中繼 CA 憑證，讓該入口網站能夠簽發憑證給 GlobalProtect 閘道與衛星裝置。您還可以設定 GlobalProtect 入口網站，將其用作簡易憑證註冊通訊協定 (SCEP) 用戶端，以對 GlobalProtect 衛星裝置簽發用戶端憑證。
- 自我簽署憑證 — 您可以在防火牆上產生自我簽署的根 CA 憑證，並用來為入口網站、閘道與衛星裝置簽發伺服器憑證。使用自我簽署根 CA 憑證時，最佳做法是在入口網站上建立自我簽署的根 CA 憑證，並用它來為閘道與衛星裝置簽發伺服器憑證。如此一來，用於簽署憑證的私密金鑰會留在入口網站上。

將伺服器憑證部署至 GlobalProtect LSVPN 元件

GlobalProtect LSVPN 元件使用 SSL/TLS 互相驗證。部署 LSVPN 前，您必須將 SSL/TLS 服務設定檔指派給入口網站與閘道。設定檔會指定伺服器憑證與允許的衛星通訊 TLS 版本。您不必為衛星建立 SSL/TLS 服務設定檔，因為入口網站在第一次連線期間，會在衛星註冊程序中為每顆衛星簽發伺服器憑證。

此外，您必須匯入根憑證授權單位 (CA) 憑證，用於將伺服器憑證簽發到每個您打算裝載以作為閘道或衛星的防火牆上。最後，在每個參與 LSVPN 的閘道與衛星上，您必須設定憑證設定檔，讓它們能夠使用互相驗證來建立 SSL/TLS 連線。

下列工作流程顯示將 SSL 憑證部署至 GlobalProtect LSVPN 元件的最佳做法步驟：

©2024 Palo Alto Networks, Inc.

STEP 1 | 在裝載 GlobalProtect 入口網站的防火牆上建立根 CA 憑證，來為 GlobalProtect 元件簽署憑證。

建立自我簽署根 CA 憑證：

1. 選取 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證） > **Device Certificates**（裝置憑證），然後按一下 **Generate**（產生）。
2. 輸入 **Certificate Name**（憑證名稱），例如 **`LSVPN_CA`**。
3. 請勿在 **Signed By**（簽署者）欄位中選取數值（表示此為自我簽署）。
4. 選取 **Certificate Authority**（憑證授權單位）核取方塊，然後按一下 **OK**（確定）以產生憑證。

STEP 2 | 為 GlobalProtect 入口網站與閘道建立 SSL/TLS 服務設定檔。

針對入口網站與每個閘道，您必須指派參考唯一自我簽署伺服器憑證的 SSL/TLS 服務設定檔。

最佳做法是在入口網站上簽發所有必要的憑證，因此不必匯出簽署憑證（與私密金鑰）。

如果 *GlobalProtect* 入口網站與閘道位於同一個防火牆介面上，您可以為這兩個元件使用相同的伺服器憑證。

1. 在入口網站上使用根 CA，為每個您將部署的閘道產生憑證：
   1. 選取 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證） > **Device Certificates**（裝置憑證），然後按一下 **Generate**（產生）。
   2. 輸入 **Certificate Name**（憑證名稱）。
   3. 在 **Common Name**（通用名稱）欄位中輸入您要設定閘道的 FQDN（建議）或 IP 位址。
   4. 在 **Signed By**（簽署者）欄位中，選取您剛剛建立的 **`LSVPN_CA`** 憑證。
   5. 在 [憑證屬性] 區段中，按一下**Add**（新增）並定義屬性，以唯一識別閘道。如果您新增 **Host Name**（主機名稱）屬性（會填入憑證的 SAN 欄位），則必須與您為 **Common Name**（通用名稱）定義的值完全符合。
   6. 產生憑證。
2. 為入口網站和每個閘道組態 SSL/TLS 服務設定檔：
   1. 選取 **Device**（裝置） > **Certificate Management**（憑證管理） > **SSL/TLS Service Profile**（**SSL/TLS** 服務設定檔），再按一下 **Add**（新增）。
   2. 輸入 **Name**（名稱）以識別設定檔，並選取您剛剛為入口網站或閘道建立的 **Certificate**（憑證）。
   3. 定義與衛星通訊的允許 TLS 服務範圍（**Min Version**（最低版本）到 **Max Version**（最高版本）），然後按一下 **OK**（確定）。

©2024 Palo Alto Networks, Inc.

STEP 3 | 將自我簽署的伺服器憑證部署至閘道。

最佳做法：

- 從入口網站匯出由根 CA 簽發的自我簽署伺服器憑證，並匯入至閘道上。
- 請務必為每個閘道簽發唯一的伺服器憑證。
- 憑證的 Common Name（通用名稱）(CN) 及 Subject Alternative Name（主旨替代名稱）(SAN) 欄位（如果適用的話），必須符合您設定閘道所在介面的 IP 位址或完全合格的網域名稱 (FQDN)。

1. 在入口網站上，選取 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證） > **Device Certificates**（裝置憑證），選取您要部署的閘道憑證，然後按一下 **Export**（匯出）。
2. 從 **File Format**（檔案格式）下拉式清單選取 **Encrypted Private Key and Certificate (PKCS12)**（加密的私密金鑰與憑證 **(PKCS12)**）。
3. 輸入（然後重新輸入）複雜密碼以加密與憑證相關聯的私密金鑰，然後按一下確定將 PKCS12 檔案下載到您的電腦上。
4. 在閘道上，選取 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證） > **Device Certificates**（裝置憑證），然後按一下 **Import**（匯入）。
5. 輸入 **Certificate Name**（憑證名稱）。
6. 輸入您剛剛從入口網站下載之 **Certificate File**（憑證檔案）的路徑與名稱，或 **Browse**（瀏覽）以尋找檔案。
7. 選取 **Encrypted Private Key and Certificate (PKCS12)**（加密的私密金鑰與憑證 **(PKCS12)**）作為 **File Format**（檔案格式）。
8. 在 **Key File**（金鑰檔案）欄位中輸入 PKCS12 檔案的路徑與名稱，或 **Browse**（瀏覽）以尋找該檔案。
9. 輸入並重新輸入您將私密金鑰從入口網站匯出時用來將它加密的 **Passphrase**（複雜密碼），然後按一下 **OK**（確定）匯入憑證與金鑰。

©2024 Palo Alto Networks, Inc.

STEP 4 | 匯入用來為 LSVPN 元件簽發伺服器憑證的根 CA 憑證。

您必須將根 CA 憑證匯入到所有閘道與衛星上。基於安全因素，請確定僅匯出憑證，未匯出關聯的私密金鑰。

1. 從入口網站下載根 CA 憑證。
    1. 選取 **Device**（設備）> **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Device Certificates**（裝置憑證）。
    2. 選取用來為 LSVPN 元件簽發憑證的根 CA 憑證，並按一下匯出。
    3. 從 **File Format**（檔案格式）下拉式清單中選取 **Base64 Encoded Certificate (PEM)**（**Base64** 編碼憑證 **(PEM)**），然後按一下 **OK**（確定）來下載憑證。(請勿匯出私密金鑰。)
2. 在裝載閘道與衛星的防火牆上匯入根 CA 憑證。
    1. 選取 **Device**（裝置）> **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Device Certificates**（裝置憑證），然後按一下 **Import**（匯入）。
    2. 輸入作為用戶端 CA 憑證識別的 **Certificate Name**（憑證名稱）。
    3. **Browse**（瀏覽）至從 CA 下載的 **Certificate File**（憑證檔案）。
    4. 選取 **Base64 Encoded Certificate (PEM)**（**Base64** 編碼憑證 **(PEM)**）作為 **File Format**（檔案格式），然後按一下 **OK**（確定）。
    5. 選取剛匯入至 **Device Certificates**（裝置憑證）頁籤上的憑證，然後開啟。
    6. 選取 **Trusted Root CA**（信任根 **CA**），然後按一下 **OK**（確定）。
    7. **Commit**（提交）變更。

STEP 5 | 建立憑證設定檔。

GlobalProtect LSVPN 入口網站與每個閘道皆需要憑證設定檔，以指定要使用哪一個憑證驗證衛星。

1. 選取 **Device**（裝置）> **Certificate Management**（憑證管理）> **Certificate Profile**（憑證設定檔），然後按一下 **Add**（新增）並輸入設定檔 **Name**（名稱）。
2. 確保將 **Username Field**（使用者名稱欄位）設為 **None**（無）。
3. 在 **CA Certificates**（**CA** 憑證）欄位中，按一下 **Add**（新增），選取您在上一步中匯入的受信任根 CA 憑證。
4. （建議）允許使用 CRL 和/或 OCSP 以啟用憑證狀態驗證。
5. 按一下 **OK**（確定）來儲存設定檔。

STEP 6 | Commit（提交）您的變更。

按一下 **Commit**（交付）。

 ©2024 Palo Alto Networks, Inc.

使用 SCEP 將用戶端憑證部署至 GlobalProtect 衛星

作為部署用戶端憑證至衛星的替換方法，您可以設定 GlobalProtect 入口網站，將其用作企業 PKI 中 SCEP 伺服器的簡易憑證註冊通訊協定 (SCEP) 用戶端。SCEP 在該企業 PKI 中動態運作，以便在入口網站請求時產生憑證，並將憑證傳送至入口網站。

當衛星裝置請求連線至入口網站或閘道時，連線請求中還包含其序號。入口網站使用 SCEP 設定檔中的設定提交 CSR 至 SCEP 伺服器，並且在用戶端憑證主旨中自動包含裝置序號。從企業 PKI 收到用戶端憑證後，入口網站以透明方式將用戶端憑證部署至衛星裝置。衛星裝置隨後向入口網站或閘道呈現用戶端憑證以進行驗證。

STEP 1 | 建立 SCEP 設定檔。

1. 選取 **Device**（裝置） > **Certificate Management**（憑證管理） > **SCEP**，然後 **Add**（新增） 新的設定檔。
2. 輸入用來識別 SCEP 設定檔的 **Name**（名稱）。
3. 如果此設定檔適用於具有多重虛擬系統功能的防火牆，請選取一個虛擬系統或 **Shared**（共用）作為設定檔可用的 **Location**（位置）。

STEP 2 | （選用）為使基於 SCEP 的憑證產生更安全，在 PKI 與各憑證要求的入口網站之間設定 SCEP 質詢回應機制。

在您設定此機制後，其操作不可見，您不必進行進一步輸入。

為了符合美國聯邦資訊處理標準 (FIPS)，請使用 **Dynamic**（動態）SCEP 挑戰，並指定一個使用 HTTPS 的 **Server URL**（伺服器 **URL**）（請參閱步驟 7）。

選取下列其中一個選項：

- **None**（無） — （預設）SCEP 伺服器在簽發憑證之前，不會質詢入口網站。
- 固定 — 在 PKI 基礎結構中，從 SCEP 伺服器取得註冊質詢密碼（例如 **`http://10.200.101.1/CertSrv/mscep_admin/`**），然後複製密碼或在 Password（密碼）欄位輸入密碼。
- 動態 — 輸入 SCEP **Server URL**（伺服器 URL），入口網站-用戶端在此提交憑證（例如 **`http://10.200.101.1/CertSrv/mscep_admin/`**），以及您選擇的使用者名稱與 OTP。使用者名稱與密碼可以是 PKI 管理員的憑證。

©2024 Palo Alto Networks, Inc.

STEP 3 | 指定 SCEP 伺服器與入口網站之間的連線設定，以啟用入口網站來請求和接收用戶端憑證。

為了識別衛星，入口網站在向 SCEP 伺服器提交的 CSR 請求中自動包含裝置序號。由於 SCEP 設定檔需要 **Subject**（主旨）欄位中的值，即使該值沒有在 LSVPN 的用戶端憑證中使用，您仍可保留預設值 **`$USERNAME`**。

1. 設定入口網站用於連線 PKI 中 SCEP 伺服器的 **Server URL**（伺服器 **URL**）（例如 **`http://10.200.101.1/certsrv/mscep/`**）。
2. 在 **CA-IDENT Name**（**CA-IDENT** 名稱）欄位中輸入字串（長度最大為 255 個字元），用以識別 SCEP 伺服器。
3. 選取 **Subject Alternative Name Type**（主旨替代名稱類型）：
   - **RFC 822 Name**（**RFC 822** 名稱）—在憑證的主旨或主旨替代副檔名輸入電子郵件名稱。
   - **DNS Name**（**DNS** 名稱）—輸入用於評估憑證的 DNS 名稱。
   - **Uniform Resource Identifier**（統一資源識別項）—輸入用戶端從中取得憑證的資源名稱。
   - **None**（無）—請勿指定憑證的屬性。

STEP 4 | （選用）進行憑證密碼設定。

- 選取憑證的金鑰長度（**Number of Bits**（位元數））。如果防火牆處於 FIPS-CC 模式，則金鑰產生演算法為 RSA。RSA 金鑰必須為 2048 位元或更大。
- 選取 **Digest for CSR**（**CSR** 摘要），這是指憑證簽署請求 (CSR) 的摘要演算法：SHA1、SHA256、SHA384 或 SHA512。

STEP 5 | （選用）設定允許使用的憑證（簽署或加密）。

- 若要使用此憑證進行簽署，請選取 **Use as digital signature**（用作數位簽章）核取方塊。此選項可讓端點使用憑證中的私密金鑰來驗證數位特徵碼。
- 若要使用此憑證進行加密，請選取 **Use for key encipherment**（用作金鑰加密）核取方塊。此選項可讓用戶端使用憑證中的私密金鑰來加密透過 HTTPS 連線（使用 SCEP 伺服器核發的憑證建立連線）交換的資料。

STEP 6 | （選用）若要確保入口網站連線至正確的 SCEP 伺服器，請輸入 **CA Certificate Fingerprint**（**CA** 憑證指紋）。從 Thumbprint（指紋）欄位的 SCEP 伺服器介面取得該指紋。

1. 為 SCEP 伺服器管理員 UI 輸入 URL（例如 **`http://<hostname or IP>/CertSrv/mscep_admin/`**）。
2. 複製指紋並在 **CA Certificate Fingerprint**（**CA** 憑證指紋）欄位中輸入。

©2024 Palo Alto Networks, Inc.

STEP 7 | 啟用 SCEP 伺服器與 GlobalProtect 入口網站之間的手動 SSL 驗證。這需要符合美國美國聯邦資訊處理標準 (FIPS)。

FIPS-CC 操作顯示於防火牆登入頁面及其狀態列。

選取 SCEP 伺服器的根 **CA Certificate**（**CA** 憑證指紋）。選取 **Client Certificate**（用戶端憑證）來選取性地在 SCEP 伺服器與 GlobalProtect 入口網站之間啟用相互 SSL 驗證。

STEP 8 | 儲存並提交組態。

1. 按一下 **OK**（確定）以儲存設定並關閉 SCEP 組態。
2. **Commit**（提交）組態。

入口網站嘗試使用 SCEP 設定檔中的設定請求 CA 憑證，並將其儲存至托管入口網站的防火牆。如果成功，CA 憑證將顯示在 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證）中。

STEP 9 | （選用）如果在儲存 SCEP 設定檔之後，入口網站無法取得憑證，您可以手動透過入口網站產生憑證簽署請求 (CSR)。

1. 選取 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證） > **Device Certificates**（裝置憑證），然後按一下 **Generate**（產生）。
2. 輸入 **Certificate Name**（憑證名稱）。此名稱不能包含空格。
3. 選取 **SCEP Profile**（**SCEP** 設定檔），用以提交 CSR 至企業 PKI。
4. 按一下 **OK**（確定），以提交請求並產生憑證。

©2024 Palo Alto Networks, Inc.

設定入口網站以驗證衛星

若要使用 LSVPN 註冊，每個衛星必須與入口網站間建立 SSL/TLS 連線。建立連線後，入口網站會驗證衛星，以確保授權該衛星加入 LSVPN。成功驗證衛星後，入口網站會為衛星簽發伺服器憑證，並推送 LSVPN 組態以指定衛星可連線至哪些閘道，並指定與閘道建立 SSL 連線時所需的根 CA 憑證。

要讓衛星在其初始連線期間向入口網站進行驗證，您必須為入口網站 LSVPN 設定建立驗證設定檔。衛星管理員必須手動向入口網站驗證衛星以建立第一個連線。成功驗證後，入口網站會返回一個衛星 Cookie，以在後續連線中驗證衛星。入口網站發出的衛星 Cookie 的有效期預設為 6 個月。當 Cookie 過期時，衛星管理員必須再次手動驗證，此時入口網站將發出一個新的 Cookie。

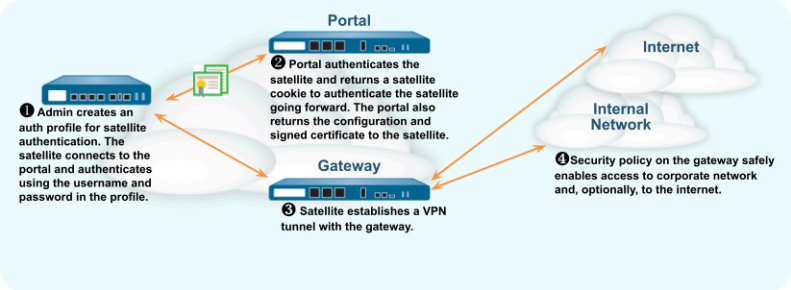
（PAN-OS 11.0.1 及更高版本）您可以將 cookie 有效期設定為 1 到 5 年，而預設值保持為 6 個月。

在入口網站上：

- 使用 **`request global-protect-portal set-satellite-cookie-expiration value <1-5>`** CLI 命令來變更當前的衛星 cookie 到期時間。
- 使用 **`show global-protect-portal satellite-cookie-expiration`** CLI 命令來檢視當前的衛星 cookie 到期時間。

在衛星上：

- 使用 **`show global-protect-satellite satellite`** CLI 命令來檢視（在「`Satellite Cookie Generation Time`」（衛星 Cookie 產生時間）欄位中）當前衛星驗證 cookie 的產生時間。



下列工作流程說明如何設定入口網站對現有的驗證服務驗證衛星。為了向入口網站驗證衛星，GlobalProtect LSVPN 僅支援本機資料庫驗證。

STEP 1 | 設定本機資料庫驗證，以便衛星管理員可以向入口網站驗證衛星。

1. 選取 **Device**（裝置） > **Local User Database**（本機使用者資料庫） > **Users**（使用者）並將使用者帳戶 **Add**（新增）到本機資料庫。
2. **Add**（新增）使用者帳戶到本機資料庫。

©2024 Palo Alto Networks, Inc.

STEP 2 | 設定驗證設定檔。

1. 選取 **Device**（裝置） > **Authentication Profile**（驗證設定檔） > **Add**（新增）。
2. 輸入設定檔的 **Name**（名稱），然後將 **Type**（類型）設定為 **Local Database**（本機資料庫）。
3. 按一下 **OK**（確定）並 **Commit**（提交）變更。

STEP 3 | 驗證衛星。

為了向入口網站驗證衛星，衛星管理員必須提供在本機資料庫中設定的使用者名稱和密碼。

1. 選取 **Network**（網路） > **IPSec Tunnels**（**IPSec** 通道），然後在您為 LSVPN 建立的通道組態 Status（狀態）欄中按一下 **Gateway Info**（閘道資訊） 連結。
2. 按一下 **Portal Status**（**Portal** 狀態）欄位中的 **enter credentials**（輸入認證）連結，必須有使用者名稱與密碼才能對入口網站驗證衛星。

   入口網站首次成功向入口網站驗證後，入口網站會產生一個衛星 Cookie，用於在後續工作階段中驗證衛星。

©2024 Palo Alto Networks, Inc.

為 LSVPN 設定 GlobalProtect 閘道

由於入口網站傳遞給衛星的 GlobalProtect 設定包括衛星可連線的閘道清單，因此最好先設定閘道，再設定入口網站。

您必須先完成下列工作，才能設定 GlobalProtect 閘道：

- 建立 LSVPN 的介面與區域 在您將用來設定各閘道的介面上。實體介面與虛擬通道介面皆須設定。
- 啟用 GlobalProtect LSVPN 元件之間的 SSL 藉由設定建立 GlobalProtect 衛星與閘道互相 SSL/TLS 連線時所需的閘道伺服器憑證、SSL/TLS 服務設定檔以及憑證設定檔。

將各 GlobalProtect 閘道組態為參與 LSVPN，如下所示：

STEP 1 | 新增閘道。

1. 選取 **Network**（網路） > **GlobalProtect** > **Gateways**（閘道），然後按一下 **Add**（新增）。
2. 在 **General**（一般）螢幕中，輸入閘道的 **Name**（名稱）。閘道名稱不應包含任何空格，且命名的最佳做法是將可協助使用者與管理者識別閘道的位置或其他描述性資訊包含其中。
3. （選用）從 **Location**（位置）欄位中選取此閘道所屬的虛擬系統。

STEP 2 | 指定允許衛星裝置連線至閘道的網路資訊。

如果您沒有為閘道建立網路介面，請參閱 建立 LSVPN 的介面與區域 以取得指示。

1. 選取衛星用來輸入存取閘道的 **Interface**（介面）。
2. 指定用於存取閘道的 **IP Address Type**（**IP** 位址類型）和 **IP address**（**IP** 位址）。
   - IP 位址類型可以是 **IPv4**（僅限）、**IPv6**（僅限）或 **IPv4 and IPv6**（**IPv4** 和 **IPv6**）。如果您的網路支援雙堆疊組態（也就是會同時執行 IPv4 和 IPv6），請使用 **IPv4 and IPv6**（**IPv4** 和 **IPv6**）。
   - IP 位址必須與 IP 位址類型相容。例如，**`172.16.1/0`**（適用於 IPv4）或 **`21DA:D3:0:2F3B`**（適用於 IPv6）。對於雙堆疊組態，輸入 IPv4 和 IPv6 位址。
3. 按一下 **OK**（確定）以儲存變更。

©2024 Palo Alto Networks, Inc.

STEP 3 | 指定閘道如何驗證嘗試建立通道的衛星。如果您尚未為閘道建立 SSL/TLS 服務設定檔，請參閱 將伺服器憑證部署至 GlobalProtect LSVPN 元件。

如果您未設定驗證設定檔或憑證設定檔，請參閱 設定入口網站以驗證衛星 以取得指示。

如果您尚未設定憑證設定檔，請參閱 啟用 GlobalProtect LSVPN 元件之間的 SSL 以取得指示。

在 GlobalProtect 閘道組態對話方塊上，選取 Authentication（驗證），然後設定下列任意項：

- 若要保障閘道與衛星間的通訊安全，為閘道選取 **SSL/TLS Service Profile**（**SSL/TLS** 服務設定檔）。
- 若要指定用於驗證衛星的驗證設定檔，可 **Add**（新增）Client Authentication（用戶端驗證）。然後輸入用來識別組態的 **Name**（名稱），並選取 **OS**（作業系統）：選取 **Satellite**（衛星）以套用組態至所有衛星，然後指定 **Authentication Profile**（驗證設定檔），用以驗證衛星。您還可以為閘道選取 **Certificate Profile**（憑證設定檔），用以驗證嘗試建立通道的衛星裝置。

STEP 4 | 設定通道參數並啟用通道。

1. 在 GlobalProtect 閘道組態對話方塊中，選取 **Satellite**（衛星裝置） > **Tunnel Settings**（通道組態）。
2. 選取**Tunnel Configuration**（通道組態）核取方塊啟用通道。
3. 選取所定義的 **Tunnel Interface**（通道介面），以終止 GlobalProtect 衛星裝置在您執行 建立 LSVPN 的介面與區域 工作時間裡的 VPN 通道。
4. （選用）如果您想要保留封裝封包中的 Type of Service（服務類型，ToS）資訊，請選取 **Copy TOS**（複製 **TOS**）。

   如果通道內存在多個工作階段（每個通道具有不同的 *TOS* 值），複製 *TOS* 標頭可能導致 *IPSec* 封包無序到達。

STEP 5 | （選用）啟用通道監控。

通道監控允許衛星監控其閘道通道連線，讓衛星在連線中斷時能容錯移轉至備份閘道。容錯移轉至另一個閘道是唯一一種通道可監控 LSVPN 所支援的設定檔。

1. 選取 **Tunnel Monitoring**（通道監控器）核取方塊。
2. 指定衛星用來判斷閘道是否在使用中的 **Destination IP Address**（目的地 **IP** 位址）。您可以指定 **IPv4** 位址、**IPv6** 位址或二者。或者，如果您為通道介面設定 IP 位址，您可以將此欄位保留空白，通道監控器會改用通道介面來判斷連線是否作用中。
3. 從通道監控器設定檔下拉式清單中選取容錯移轉（這是唯一支援 LSVPN 適用的通道監控設定檔）。

STEP 6 | 選取建立通道連線時使用的 IPSec 加密設定檔。

設定檔可指定 IPSec 加密類型和驗證方法，用於保護周遊在通道中的資料。由於 LSVPN 中的通道端點雙方是您組織內的信任防火牆，因此您通常可以使用預設（預先定義）設定檔，該設定

 ©2024 Palo Alto Networks, Inc.

檔會將 ESP 用作 IPSec 通訊協定、group2 用為 DH 群組、AES 128 CVC 用為加密，以及 SHA-1 用為驗證。

從 **IPSec Crypto Profile**（**IPSec** 加密設定檔）下拉式清單中選取 **default**（預設值）以使用預先定義的設定檔，或選取 **New IPSec Crypto Profile**（新 **IPSec** 加密設定檔）來定義新的設定檔。如需驗證和加密選項的詳細資料，請參閱 定義 IPSec 密碼設定檔。

STEP 7 | 設定建立 IPSec 通道期間用於指派衛星的網路設定。

您也可以透過在裝載衛星的防火牆上設定 *DHCP* 伺服器，來設定衛星將 *DNS* 設定推送至其本地用戶端。在此設定中，衛星會將其自閘道中取得的 *DNS* 設定推送至 *DHCP* 用戶端。

1. 在 GlobalProtect 閘道組態對話方塊中，選取 **Satellite**（衛星裝置） > **Network Settings**（網路設定）。
2. （選用）如果衛星的本地用戶端需要解析公司網路上的 FQDN，請以下列其中一個方法設定閘道將 DNS 設定推送至衛星：
   - 如果閘道的介面設定成 DHCP 用戶端，您可以將 **Inheritance Source**（繼承來源）設為該介面，並將 DHCP 用戶端收到的相同設定指派給 GlobalProtect 衛星。您還可以從相同來源繼承 DNS 尾碼。
   - 手動定義主要 **DNS**、次要 **DNS** 與 **DNS** 尾碼設定以推送至衛星。
3. 若要指定位址的 **IP Pool**（**IP** 配發範圍），用於在建立 VPN 時於衛星上指派通道介面，請按一下 **Add**（新增），然後指定要使用的 IP 位址範圍。
4. 若要定義要將哪些目的地子網路路由穿越通道，請按一下 **Access Route**（存取路由）區域中的 **Add**（新增），然後輸入路由，如下所述：
   - 如果您想要將衛星的所有流量路由穿越通道，請將此欄保留空白。

     在此情況下，除了目的地為本地子網路的流量外，所有的流量都會經由通道前往閘道。

   - 若要僅路由部分的流量穿越閘道 (稱做分割通道)，請指定必須穿越通道的目的地子網路。在此狀況下，衛星將使用自己的路由表來路由目的地不是指定存取路由流量。例如，您可以選擇只將目的地為您公司網路的流量穿越通道，並使用本地衛星來安全地啟用網際網路存取。
   - 如果您想要啟用衛星之間的路由，請為各個衛星所保護的網路輸入摘要路由。

©2024 Palo Alto Networks, Inc.

STEP 8 | （選用）定義閘道將從衛星接受哪些路由（若有的話）。

依預設，閘道不會將任何路由衛星宣告新增其至路由表。如果您不要閘道接受來自衛星的路由，則不必完成此步驟。

1. 若要讓閘道接受衛星宣告的路由，則選取 **Satellite**（衛星裝置） > **Route Filter**（路由過濾器）。
2. 選取 **Accept published routes**（接受發行的路由）核取方塊。
3. 若要過濾衛星宣告的路由以新增至閘道路由表，請按一下 **Add**（新增），再定義要包含的子網路。例如，如果所有的衛星皆設定成子網路為 LAN 端的 192.168.x.0/24，請設定許可的 192.168.0.0/16 路由，讓衛星如果在 192.168.0.0/16 子網路中，則閘道只接受來自該子網路的路由。

STEP 9 | 儲存閘道組態。

1. 按一下 **OK**（確定）儲存設定並關閉 GlobalProtect Gateway Configuration（GlobalProtect 閘道組態）對話方塊。
2. **Commit**（提交）組態。

 ©2024 Palo Alto Networks, Inc.

為 LSVPN 設定 GlobalProtect 入口網站

GlobalProtect 入口網站為 GlobalProtect LSVPN 提供管理功能。參與 LSVPN 的每個衛星系統都會收到入口網站的設定資訊，包括可用閘道的相關資訊，以及連線到閘道所需的憑證。

以下幾節提供設定入口網站的程序：

- LSVPN 先決工作的 GlobalProtect 入口網站
- 設定入口網站
- 定義衛星組態

LSVPN 先決工作的 GlobalProtect 入口網站

您必須先完成下列工作，才能設定 GlobalProtect 入口網站：

- 建立 LSVPN 的介面與區域 在您將用來設定入口網站的介面上。
- 透過為入口網站伺服器憑證建立 SSL/TLS 服務設定檔、發出閘道伺服器憑證以及設定要為 GlobalProtect 衛星發出伺服器憑證的入口網站，啟用 GlobalProtect LSVPN 元件之間的 SSL。
- 透過設定本機資料庫驗證並定義入口網站將用於驗證衛星的驗證設定檔，設定入口網站以驗證衛星。
- 為 LSVPN 設定 GlobalProtect 閘道。

設定入口網站

在完成為 LSVPN 設定 GlobalProtect 入口網站的先決工作之後，按下列步驟設定 GlobalProtect 入口網站：

STEP 1 | 新增入口網站。

1. 選取 **Network**（網路） > **GlobalProtect** > **Portals**（入口網站），然後按一下 **Add**（新增）。
2. 在 **General**（一般）頁籤上，輸入入口網站的 **Name**（名稱）。入口網站名稱不能包含空格。
3. （選用）從 **Location**（位置）欄位中選取此入口網站所屬的虛擬系統。

©2024 Palo Alto Networks, Inc.

STEP 2 | 指定允許衛星連線至入口網站的網路資訊。

如果您還沒有為閘道建立網路介面，請參閱為 LSVPN 建立介面與區域，獲取相關說明。

1. 選取衛星用來輸入存取入口網站的 **Interface**（介面）。
2. 指定衛星裝置用於存取該入口網站的 **IP Address Type**（**IP** 位址類型）和 **IP address**（**IP** 位址）：
   - IP 位址類型可以是 **IPv4**（僅限 IPv4 流量）、**IPv6**（僅限 IPv6 流量）或 **IPv4 and IPv6**（**IPv4** 和 **IPv6**）。如果您的網路支援雙堆疊組態（也就是會同時執行 IPv4 和 IPv6），請使用 **IPv4 and IPv6**（**IPv4** 和 **IPv6**）。
   - IP 位址必須與 IP 位址類型相容。例如，**`172.16.1/0`**（適用於 IPv4）或 **`21DA:D3:0:2F3B`**（適用於 IPv6）。對於雙堆疊組態，輸入 IPv4 和 IPv6 位址。
3. 按一下 **OK**（確定）以儲存變更。

STEP 3 | 指定 SSL/TLS Service Profile（SSL/TLS 服務設定檔）使衛星能建立對入口網站的 SSL/TLS 連線。

如果您還沒有為此入口網站建立 SSL/TLS 服務設定檔並簽發閘道憑證，請參閱為 GlobalProtect LSVPN 元件部署伺服器憑證。

1. 在 GlobalProtect Portal Configuration（GlobalProtect 入口網站組態）對話方塊上，選取 **Authentication**（驗證）。
2. 選取 **SSL/TLS Service Profile**（**SSL/TLS** 服務設定檔）。

STEP 4 | 指定用於驗證衛星的驗證設定檔和選用憑證設定檔。

衛星首次連線到入口網站時，必須使用本機資料庫驗證進行驗證（在後續工作階段中，它使用入口網站發出的衛星 *Cookie*）。因此，儲存入口網站設定（透過按一下***OK***（確定））之前，您必須設定驗證設定檔。

Add（新增）用戶端驗證，然後輸入 **Name**（名稱）以識別組態，選取 **OS**（作業系統）：選取 **Satellite**（衛星）以套用組態至所有衛星，然後指定 **Authentication Profile**（驗證設定檔），用以驗證衛星裝置。您還可以為入口網站指定 **Certificate Profile**（憑證設定檔），用以驗證衛星裝置。

STEP 5 | 繼續定義要推送至衛星的組態，或者如果您已經建立衛星組態，則請儲存入口網站組態。

按一下 **OK**（確定）以儲存入口網站組態，或繼續定義衛星裝置組態。

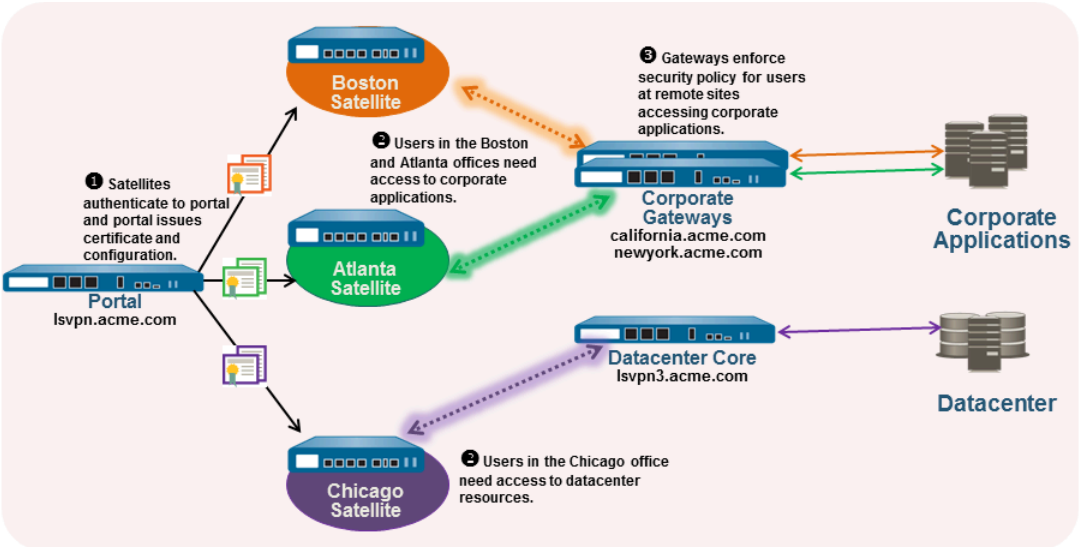
定義衛星組態

GlobalProtect 衛星連線至 GlobalProtect 入口網站並成功驗證該入口網站後，入口網站會傳遞衛星組態，此組態會指定衛星可連線至哪些閘道。如果您所有的衛星皆使用相同的閘道與憑證設定，則您可以建立單一設定，讓成功驗證時將此設定傳遞給所有的衛星。然而，如果您需要不同的衛星組態—例如，如果您想要將一組衛星連線至一個閘道，另一組衛星連線至不同的閘道，您可以為每個閘道建立不同的衛星組態。入口網站接著會使用註冊使用者名稱/群組名稱或衛星的序號，來決定要

 ©2024 Palo Alto Networks, Inc.

部署的衛星組態。藉助安全性規則評估，入口網站會從清單頂端開始尋找符合項。找到符合項目時，會將對應的設定傳遞給衛星。

例如，下圖所顯示網路中的分公司需要 VPN 存取由您周邊防火牆保護的公司應用程式，且有另一個站台需要 VPN 存取資料中心。



請使用下列程序建立一或多個衛星組態。

STEP 1 | 新增衛星組態。

衛星組態會指定要部署至連線衛星的 GlobalProtect LSVPN 組態設定。您必須定義至少一個衛星組態。

1. 選取 **Network**（網路） > **GlobalProtect** > **Portals**（入口網站），選取您要為其新增衛星組態的入口網站組態，然後選取 **Satellite**（衛星裝置）頁籤。
2. 在 Satellite（衛星裝置）區段中，按一下 **Add**（新增）。
3. 輸入設定的 **Name**（名稱）。

   如果您打算建立多個設定，請確定您為每個設定定義的名稱具有描述性，足以讓您識別這些設定。
4. 若要變更衛星應檢查入口網站進行組態更新的頻率，請在 **Configuration Refresh Interval (hours)**（設定重新整理間隔（小時））欄位中指定一個值（範圍是 1-48；預設為 24）。

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 指定部署此組態的衛星。

入口網站會使用登記使用者/使用者群組設定和/或裝置序號比對衛星與組態。因此，如果您有多個設定，請確定以適當的順序排序設定。入口網站只要找到符合項目便會傳遞設定。因此，較具體的設定必須位於較一般性設定的前方。關於衛星設定清單排序的說明，請參閱步驟 5。

指定衛星組態的比對準則，如下所述：

- 若要將組態限制在具有特定序號的衛星裝置，請選取 **Devices**（裝置）頁籤，按一下 **Add**（新增），然後輸入序號（您不必輸入衛星主機名稱，當衛星連線時會自動新增該主機名稱）。針對每個要接收此設定的衛星重複此步驟。
- 選取登記使用者/使用者群組頁籤，按一下新增，然後選取您要接收此組態的使用者或群組。若衛星不符合序號，則必須將衛星驗證為在此指定的使用者 (個別使用者或群組成員)。

您必須先依照所述將使用者對應至群組，才能將組態限制於特定的群組。

STEP 3 | 指定具備此設定的衛星可建立 VPN 通道的閘道。

系統會將閘道發行的路由安裝在衛星上，作為靜態路由。靜態路由的公制為公制優先順序的 *10* 倍。如果您有多個閘道，請確定也設定路由器優先順序，以確保備份閘道所宣告路由的公制，會比主要閘道所宣告相同路由的公制還高。例如，如果您為主要閘道與備份閘道分別設定 *1* 與 *10* 的路由器優先順序，則衛星將使用 *10* 作為主要閘道的度量，使用 *100* 作為備份閘道的度量。

1. 在 **Gateways**（閘道）頁籤上按一下 **Add**（新增）。
2. 輸入閘道的描述性 **Name**（名稱）。您在此輸入的名稱應符合您在設定閘道時定義的名稱，且應具有描述性，足以讓您識別閘道的位置。
3. 在 **Gateways**（閘道）欄位中輸入用來設定閘道的介面其 FQDN 或 IP 位址。您指定的位址必須與閘道伺服器憑證中的通用名稱 (CN) 完全符合。
4. （選用）如果您正將兩個以上的閘道新增至組態，**Routing Priority**（路由器優先順序）會幫助衛星挑選優先使用的閘道。輸入範圍 1-25 的值，數字愈小，優先順序愈高 (亦即當所有閘道皆可使用時衛星會連線的閘道)。衛星會將路由器優先順序乘以 10，以決定路由公制。

STEP 4 | 儲存衛星組態。

1. 按一下確定儲存衛星組態。
2. 如果您想要建立其他衛星組態，則重複前面的步驟。

STEP 5 | 排列衛星組態，讓每一個衛星上都能部署適當的設定。

- 若要將組態清單中的衛星組態向上移，請選取該組態並按一下 **Move Up**（上移）。
- 若要將組態清單中的衛星組態向下移，請選取該組態並按一下 **Move Down**（下移）。

©2024 Palo Alto Networks, Inc.

STEP 6 | 指定讓衛星能夠參與 LSVPN 所需的憑證。

1. 在 **Trusted Root CA**（受信任的根 **CA**）欄位中按一下 **Add**（新增），然後選取用於簽發閘道伺服器憑證的 CA 憑證。入口網站會將您在此新增的根 CA 憑證，部署至設定中所有的衛星，讓衛星能與閘道建立 SSL 連線。最佳做法是所有的閘道應使用相同的簽發者。
2. 選取 **Client Certificate**（用戶端憑證）的散佈方法：
   - 在入口網站上儲存用戶端憑證 — 選取 **Local**（本機），並從 **Issuing Certificate**（正在簽發憑證）下拉式清單中選取根 CA 憑證，可讓入口網站在成功驗證衛星後使用該憑證並將用戶端憑證簽發給衛星。

     如果用於簽發閘道伺服器憑證的根 *CA* 憑證不在入口網站上，您可以立即 ***Import***（匯入）。關於如何匯入根 *CA* 憑證的詳細資訊，請參閱 啟用 GlobalProtect LSVPN 元件之間的 SSL。

   - 使入口網站用作 **SCEP** 用戶端，以動態方式請求並簽發用戶端憑證 — 選取 **SCEP**，然後選取 **SCEP** 設定檔以產生對 SCEP 伺服器的 CSR。

     如果您尚未設定入口網站用作 *SCEP* 用戶端，可以立即新增 ***New***（新）*SCEP* 設定檔。如需詳細資訊，請參閱使用 SCEP 將用戶端憑證部署至 GlobalProtect 衛星。

STEP 7 | 儲存入口網站組態。

1. 按一下 **OK**（確定）儲存設定並關閉 GlobalProtect Portal Configuration（GlobalProtect 入口網站組態）對話方塊。
2. **Commit**（提交）您的變更。

 ©2024 Palo Alto Networks, Inc.

備妥衛星以加入 LSVPN

衛星必須至少具備最少數量的組態，才能參與 LSVPN。由於所需的組態很少，因此將組態出貨到分公司進行安裝前，您都能夠重新設定衛星。

STEP 1 | 設定第三層介面。

這是衛星用來連線至入口網站與閘道的實體介面。此介面必須位於允許在本地信任網路外部存取的區域中。最佳做法是為 VPN 連線建立專用的區域，並控制目的地為公司閘道的流量。

STEP 2 | 為通道建立邏輯通道介面，以用於與 GlobalProtect 閘道建立 VPN 通道。

通道介面上不需要 *IP* 位址，除非您打算使用動態路由。但是，將 *IP* 位址指派給通道介面對於疑難排解連線問題很有用。

1. 選取 **Network**（網路）> **Interfaces**（介面）> **Tunnel**（通道），然後按一下 **Add**（新增）。
2. 在 **Interface Name**（介面名稱）欄位中，指定數值尾碼，例如 **.2**。
3. 在 **Config**（組態）頁籤上展開 **Security Zone**（安全性地區）下拉式清單，然後選取現有的區域，或是按一下 **New Zone** 並為新區域定義 **Name**（名稱）（例如 *lsvpnsat*），另外為 VPN 通道流量建立一個區域。
4. 在 **Virtual Router**（虛擬路由器）下拉式清單中，選取 **default**（預設值）。
5. （選用）為通道介面指派 IP 位址：
   - 對於 IPv4 位址，選取 **IPv4**，然後 **Add**（新增）要指派給介面的 IP 位址和網路遮罩，例如 203.0.11.100/24。
   - 對於 IPv6 位址，選取 **IPv6**，**Enable IPv6 on the interface**（在介面上啟用 **IPv6**），然後 **Add**（新增）要指派給介面的 IP 位址和網路遮罩，例如 2001:1890:12f2:11::10.1.8.160/80。
6. 若要儲存介面設定，請按一下 **OK**（確定）。

©2024 Palo Alto Networks, Inc.

STEP 3 | 如果您使用衛星不信任的根 CA 產生入口網站伺服器憑證（例如您使用自我簽署的憑證），請匯入用於簽發入口網站伺服器憑證的根 CA 憑證。

必須有根 CA 憑證才能讓衛星與入口網站間建立初始連線，以取得 LSVPN 組態。

1. 下載用於產生入口網站伺服器憑證的 CA 憑證。如果您使用的是自我簽署憑證，請從入口網站匯出根 CA 憑證，如下所述：
    1. 選取 **Device**（設備）> **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Device Certificates**（裝置憑證）。
    2. 選取 CA 憑證，然後按一下匯出。
    3. 從 **File Format**（檔案格式）下拉式清單中選取 **Base64 Encoded Certificate (PEM)**（**Base64** 編碼憑證 **(PEM)**），然後按一下 **OK**（確定）來下載憑證。(您不需要匯出私密金鑰。)
2. 匯入您剛剛匯出到每個衛星上的根 CA 憑證，如下所述。
    1. 選取 **Device**（裝置）> **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Device Certificates**（裝置憑證），然後按一下 **Import**（匯入）。
    2. 輸入作為用戶端 CA 憑證識別的 **Certificate Name**（憑證名稱）。
    3. **Browse**（瀏覽）至從 CA 下載的 **Certificate File**（憑證檔案）。
    4. 選取 **Base64 Encoded Certificate (PEM)**（**Base64** 編碼憑證 **(PEM)**）作為 **File Format**（檔案格式），然後按一下 **OK**（確定）。
    5. 選取剛匯入至 **Device Certificates**（裝置憑證）頁籤上的憑證，然後開啟。
    6. 選取 **Trusted Root CA**（信任根 **CA**），然後按一下 **OK**（確定）。

STEP 4 | 設定 IPSec 通道組態。

1. 選取 **Network**（網路）> **IPSec Tunnels**（**IPSec** 通道），然後按一下 **Add**（新增）。
2. 在 **General**（一般）頁籤上，為 IPSec 組態輸入描述性的 **Name**（名稱）。
3. 選取您為衛星建立的 **Tunnel Interface**（通道介面）。
4. 選取 **GlobalProtect Satellite**（**GlobalProtect** 衛星）作為 **Type**（類型）。
5. 輸入入口網站的 IP 位址或 FQDN 作為 **Portal Address**（入口網站位址）。
6. 選取您為衛星設定的 Layer 3 介面。
7. 選取在所選介面上使用的 **IP Address**（**IP** 位址）。您可以選取 **IPv4** 位址、**IPv6** 位址或二者。指定您是否希望 **IPv6 preferred for portal registration**（將 **IPv6** 作為入口網站註冊的首選）。

©2024 Palo Alto Networks, Inc.

STEP 5 | （選用）設定衛星將本地路由發行至閘道。

將路由發行至閘道能夠讓流量透過閘道流到於衛星本地的子網路。然而，您也必須設定閘道以接受路由，如為 LSVPN 設定 GlobalProtect 閘道中的詳細說明。

1. 若要讓衛星將路由推送至閘道，請在 **Advanced**（進階）頁籤上選取 **Publish all static and connected routes to Gateway**（將所有靜態與連接的路由發佈至閘道）。

   如果您選取此核取方塊，防火牆將會轉送衛星的所有靜態與連結路由至閘道。然而，若要避免建立路由迴圈，防火牆將會套用一些路由篩選器，例如下列範例：

   - 預設路由
   - 虛擬路由器內，而非與通道介面相關虛擬路由器的路由
   - 使用通道介面的路由
   - 使用與通道介面相關之實體介面的路由

2. （選用）如果您只想要推送特定子網路的路由，而非所有的路由，請在 [子網路] 區段中按一下 **Add**（新增），然後指定要推送哪一個子網路的路由。

STEP 6 | 儲存衛星組態。

1. 按一下 **OK**（確定）以儲存 IPSec 通道設定。
2. 按一下 **Commit**（交付）。

STEP 7 | 若有需要，請提供讓衛星對入口網站驗證的認證。

為了首次向入口網站進行驗證，衛星管理員必須在本機資料庫中提供與衛星管理員帳戶關聯的使用者名稱和密碼。

1. 選取 **Network**（網路）> **IPSec Tunnels**（**IPSec** 通道），然後在您為 LSVPN 建立的通道組態 Status（狀態）欄中按一下 **Gateway Info**（閘道資訊） 連結。
2. 按一下 **Portal Status**（**Portal** 狀態）欄位中的 **enter credentials**（輸入認證）連結，必須有使用者名稱與密碼才能對入口網站驗證衛星。

   當入口網站成功對入口網站驗證後，會收到其已簽署的憑證與設定，可供入口網站用於連線至閘道。您應該會看到建立一個通道，且 **Status**（狀態）變更為 **Active**（主動）。

©2024 Palo Alto Networks, Inc.

驗證 LSVPN 組態

設定入口網站、閘道與衛星後，請確認衛星能夠連線至入口網站與閘道，並能與閘道間建立 VPN 通道。

STEP 1 | 驗證衛星與入口網站的連線。

從裝載入口網站的防火牆中選取 **Network**（網路） > **GlobalProtect** > **Portal**（入口網站），然後按一下入口網站組態項目 Info（資訊）欄中的 **Satellite Info**（衛星裝置資訊），以確認衛星裝置已成功連線。

STEP 2 | 確認衛星與閘道間的連線。

在裝載閘道的防火牆中選取 **Network**（網路） > **GlobalProtect** > **Gateways**（閘道），然後按一下閘道組態項目 Info（資訊）欄中的 **Satellite Info**（衛星裝置資訊），以確認衛星裝置也建立了 VPN 通道。成功與閘道間建立通道的衛星將會顯示在主動式衛星頁籤上。

STEP 3 | 確認衛星上的 LSVPN 通道狀態。

在每個裝載衛星的防火牆上選取 **Network** > **IPSec Tunnels**（**IPSec** 通道） 以確認通道狀態，並確認其狀態為綠色圖示所表示的主動。

©2024 Palo Alto Networks, Inc.

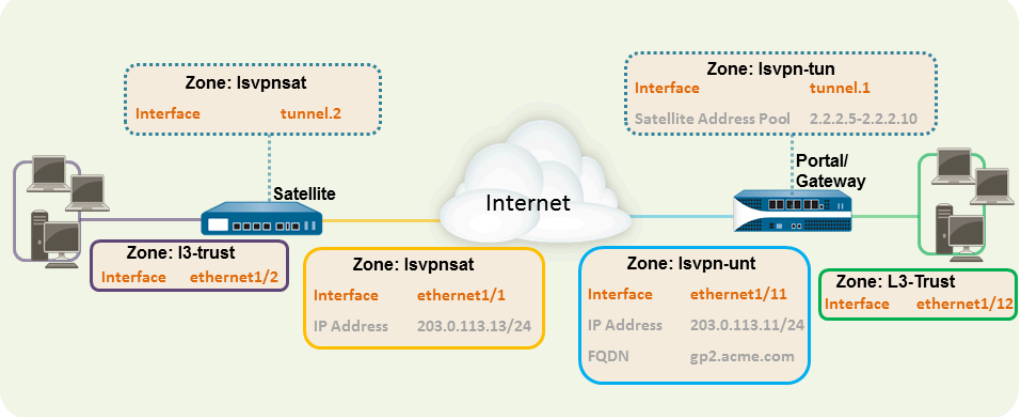
LSVPN 快速設定

以下幾節提供設定某些常用 GlobalProtect LSVPN 部署的分解步驟說明：

- 含靜態路由的基本 LSVPN 組態
- 含動態路由的進階 LSVPN 組態
- 含 iBGP 的進階 LSVPN 組態

含靜態路由的基本 LSVPN 組態

此快速設定顯示透過 LSVPN 啟動與運作的最快方法。在此範例中，會將總公司站台處的一個防火牆同時設定成入口網站與閘道。您能夠快速、輕鬆地以最小組態部署衛星，讓延展性最佳化。



下列工作流程顯示設定此基本設定的步驟：

STEP 1 | 設定 Layer 3 介面。

在此範例中，入口網站/閘道上的 Layer 3 介面需要下列設定：

- 介面—ethernet1/11
- 安全性區域—lsvpn-tun
- **IPv4**—203.0.113.11/24

STEP 2 | 在裝載 GlobalProtect 閘道的防火牆上設定邏輯通道介面，用於終止由 GlobalProtect 衛星建立的 VPN 通道。

為了能夠檢視透過 *VPN* 連線的使用者與群組，請在 *VPN* 通道終止的區域中啟用 *User-ID*。

在此範例中，入口網站/閘道上的通道介面需要下列設定：

- **Interface**（介面）—tunnel.1
- 安全性區域—lsvpn-tun

©2024 Palo Alto Networks, Inc.

STEP 3 | 建立安全性原則規則，讓流量能夠在通道終止的 VPN 區域 (lsvpn-tun) 與公司應用程式所在的信任區域 (L3-Trust) 之間流動。

請參閱建立安全性原則規則。

STEP 4 | 將 SSL/TLS 服務設定檔指派給入口網站/閘道。設定檔必須參考自我簽署的伺服器憑證。

憑證主旨名稱必須符合您為入口網站/閘道所建立 Layer 3 介面的 FQDN 或 IP 位址。

1. 在裝載 GlobalProtect 入口網站的防火牆上建立根 CA 憑證，來為 GlobalProtect 元件簽署憑證。在此範例中，根 CA 憑證 **lsvpn-CA** 將用於為入口網站/閘道簽發伺服器憑證。此外，入口網站將使用此根 CA 憑證簽署來自衛星的 CSR。
2. 為 GlobalProtect 入口網站與閘道建立 SSL/TLS 服務設定檔。

   由於在此範例中入口網站與閘道位於同一個介面上，因此可以共用使用相同伺服器憑證的 SSL/TLS 服務設定檔。在此範例中，設定檔名稱為 **lsvpnserver**。

STEP 5 | 建立憑證設定檔。

在此範例中，憑證設定檔 **lsvpn-profile** 會參照根 CA 憑證 **lsvpn-CA**。閘道將使用此憑證設定檔驗證嘗試建立 VPN 通道的衛星。

STEP 6 | 設定入口網站以使用本機資料庫驗證來驗證衛星。

STEP 7 | 為 LSVPN 設定 GlobalProtect 閘道。

選取 **Network**（網路） > **GlobalProtect** > **Gateways**（閘道），然後 **Add**（新增） 組態。此範例需要下列閘道組態：

- 介面—ethernet1/11
- **IP** 位址—203.0.113.11/24
- **SSL/TLS** 伺服器設定檔—lsvpnserver
- 憑證設定檔 — lsvpn-profile
- 通道介面— tunnel.1
- 主要 **DNS**/次要 **DNS**—4.2.2.1/4.2.2.2
- **IP** 集區—2.2.2.111-2.2.2.120
- 存取路由—10.2.10.0/24

©2024 Palo Alto Networks, Inc.

STEP 8 | 設定入口網站。

選取 **Network**（網路） > **GlobalProtect** > **Portal**（入口網站），然後 **Add**（新增）組態。此範例需要下列入口網站設定：

- 介面—ethernet1/11
- **IP** 位址—203.0.113.11/24
- **SSL/TLS** 伺服器設定檔—lsvpnserver
- 驗證設定檔—lsvpn-sat

STEP 9 | 定義衛星裝置組態。

在入口網站組態的 **Satellite**（衛星裝置）頁籤中，**Add**（新增）衛星裝置組態與受信任的根 CA，並指定入口網站將用來為衛星裝置簽發憑證的 CA。以下為此範例的必要設定：

- 閘道—203.0.113.11
- 簽發憑證—lsvpn-CA
- 受信任的根 **CA** — lsvpn-CA

STEP 10 | 備妥衛星裝置以加入 LSVPN。

此範例中的衛星組態需要下列設定：

介面組態

- Layer 3 介面—ethernet1/1, 203.0.113.13/24
- 通道介面—tunnel.2
- 區域—lsvpnsat

入口網站的根 CA 憑證

- lsvpn-CA

IPSec 通道組態

- **Tunnel Interface**（通道介面）—tunnel.2
- 入口網站位址—203.0.113.11
- 介面 —ethernet1/1
- 本機 **IP** 位址—203.0.113.13/24
- 將所有靜態與連接的路由發佈至閘道—已啟用

含動態路由的進階 LSVPN 組態

在有許多閘道與衛星的大型 LSVPN 部署中，若投入多一點時間在初始組態中設定動態路由，將能簡化閘道的維護作業，因為存取路由將會動態更新。下列範例設定顯示如何延伸基本 LSVPN 組態，以將 OSPF 設定為動態路由通訊協定。

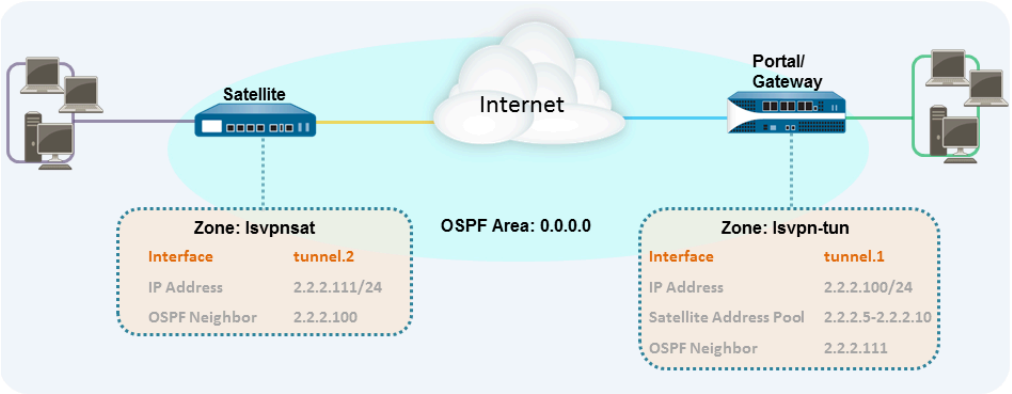
©2024 Palo Alto Networks, Inc.

若要設定 LSVPN 使用 OSPF 以便能動態路由，則需要在閘道與衛星上進行下列額外步驟：

- 手動將 IP 位址指派給所有閘道與衛星上的通道介面。
- 在所有閘道與衛星的虛擬路由器上設定 OSPF 單點對多點 (P2MP)。此外在每個閘道的 OSPF 設定中，您必須手動將每個衛星的通道 IP 位址定義成 OSPF 芳鄰。同樣的在每個衛星上，您必須手動將每個閘道的通道 IP 位址定義成 OSPF 芳鄰。

雖然在 LSVPN 的初始組態期間，動態路由需要額外的設定，但它可減少一些維護工作，如讓路由隨著網路上拓撲的變更而保持在最新的狀態。

下圖顯示 LSVPN 動態路由設定。此範例顯示如何為 VPN 將 OSPF 設定成動態路由通訊協定。



對於 LSVPN 的基本設定，請執行含靜態路由的基本 LSVPN 組態中的步驟。接著您可以完成後續工作流程中的步驟，來延展設定以使用動態路由，而非靜態路由。

STEP 1 | 將 IP 位址新增至每個閘道與衛星的通道介面組態。

在每個閘道與衛星上完成下列步驟：

1. 選取 **Network**（網路） > **Interfaces**（介面） > **Tunnel**（通道），然後選取您為 LSVPN 建立的通道組態，以開啟 Tunnel Interface（通道介面）對話方塊。

   如果您尚未建立通道介面，請參閱為 LSVPN 建立介面與區域中的步驟 2。
2. 在 **IPv4** 頁籤上按一下 **Add**（新增），然後輸入 IP 位址與子網路遮罩。例如，您輸入2.2.2.100/24 為閘道通道介面新增 IP 位址。
3. 按一下 **OK**（確定）來儲存組態。

©2024 Palo Alto Networks, Inc.

STEP 2 | 在閘道上設定動態路由通訊協定。

若要在閘道上設定 OSPF：

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後選取與 VPN 介面相關聯的虛擬路由器。
2. 在 **Areas**（地區）頁籤上按一下 **Add**（新增）以建立骨幹地區；如果已經設定，請按一下地區 ID 進行編輯。
3. 如果您正在建立新的地區，請在 **Type**（類型）頁籤上輸入 **Area ID**（地區 **ID**）。
4. 在 **Interface**（介面）頁籤上按一下 **Add**（新增），然後選取您為 LSVPN 建立的通道 **Interface**（介面）。
5. 選取 **p2mp** 作為 **Link Type**（連結類型）。
6. 按一下芳鄰區段中的 **Add**（新增），然後輸入每個衛星通道介面的 IP 位址，例如 2.2.2.111。
7. 按 **Ok**（確定）兩次以儲存虛擬路由器組態，然後兩次以儲存虛擬路由器組態，然後 **Commit**（提交）閘道的變更。
8. 每次您將新衛星新增至 LSVPN 後即重複此步驟。

STEP 3 | 在衛星上設定動態路由通訊協定。

若要在衛星上設定 OSPF：

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後選取與 VPN 介面相關聯的虛擬路由器。
2. 在 **Areas**（地區）頁籤上按一下 **Add**（新增）以建立骨幹地區；如果已經設定，請按一下地區 ID 進行編輯。
3. 如果您正在建立新的地區，請在 **Type**（類型）頁籤上輸入 **Area ID**（地區 **ID**）。
4. 在 **Interface**（介面）頁籤上按一下 **Add**（新增），然後選取您為 LSVPN 建立的通道 **Interface**（介面）。
5. 選取 **p2mp** 作為 **Link Type**（連結類型）。
6. 按一下 [芳鄰] 區段中的 **Add**（新增），然後輸入每個 GlobalProtect 閘道通道介面的 IP 位址，例如 2.2.2.100。
7. 按 **Ok**（確定）兩次以儲存虛擬路由器組態，然後兩次以儲存虛擬路由器組態，然後 **Commit**（提交）閘道的變更。
8. 每次您新增新閘道後即重複此步驟。

STEP 4 | 確認閘道與衛星能夠形成路由器相鄰項。

- 在每個衛星與每個閘道上，確認對等相鄰項已形成，且已經為對等建立路由表項目 (亦即衛星有到閘道的路由，且閘道有到衛星的路由)。選取 **Network**（網路） > **Virtual Router**（虛擬路由器），然後按一下您為 LSVPN 所使用之虛擬路由器的 **More Runtime Stats**（更多執行階段統計資料）連結。在路由頁籤上確認 LSVPN 對等有路由。
- 在 **OSPF** > **Interface**（介面） 頁籤中，確認 **Type**（類型）是否為 **p2mp**。

 ©2024 Palo Alto Networks, Inc.

- 在 **OSPF** > **Neighbor**（芳鄰） 頁籤上，確認裝載閘道的防火牆已與裝置衛星的防火牆間建立了路由器相鄰項，反之亦然。亦請確認 **Status**（狀態）為 **Full**（完整），表示已建立完整的相鄰項。

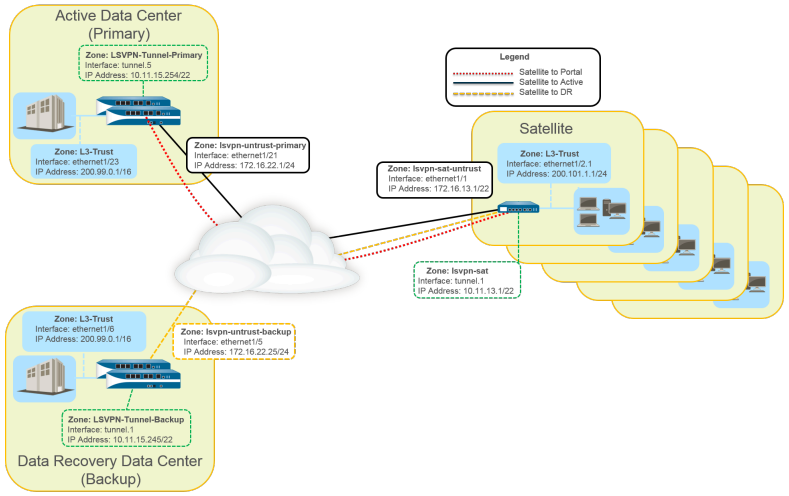
含 iBGP 的進階 LSVPN 組態

此使用案例描述了 GlobalProtect LSVPN 如何可靠地連接分散式辦公室與裝有供使用者使用的重要應用程式的主資料中心和嚴重損壞修復資料中心，以及內部邊界閘道通訊協定 (iBGP) 如何簡化部署和維護。透過此方法，您可以擴充至 500 個連接單一閘道的衛星辦公室。

BGP 是一種具有高延展性的動態路由通訊協定，特別適用於中樞和支點部署，例如 LSVPN。作為一種動態路由通訊協定，它能透過相對簡化額外衛星防火牆的部署，消除很多與存取路由（靜態路由）相關的額外負荷。由於具有路由篩選功能，例如多個可調計時器、路由抑制以及路由重新整理，BGP 可以擴充至具有更多路由首碼，而且穩定性要高於 RIP 和 OSPF 等其他路由通訊協定。對於 iBGP，對等群組（在 LSVPN 部署中包含所有衛星裝置和閘道）將在通道端點上方建立相鄰項。然後，該通訊協定將暗中控制路由宣告、更新及聚合。

在此範例設定中，PA-5200 防火牆的主動/被動 HA 配對部署在主要（主動）資料中心內，將用作入口網站和主要閘道。嚴重損壞修復資料中心也有兩個採用主動/被動 HA 配對的 PA-5200，用作 LSVPN 閘道。入口網站和閘道將為在分公司內作為 LSVPN 衛星裝置部署的 500 PA-220 提供服務。

這兩個資料中心站點都將宣告路由，但使用不同的指標。因此，衛星裝置將優先安裝主動資料中心的路由。但是，在本機路由資訊庫 (RIB) 內也存在備用路由。如果主動資料中心出現故障，該資料中心宣告的路由將被移除，並被嚴重損壞修復資料中心的路由取代。容錯移轉時間視乎於所選的 iBGP 時間以及與 iBGP 關聯的路由聚合。



下列工作流程顯示設定此部署的步驟：

©2024 Palo Alto Networks, Inc.

STEP 1 | 為 LSVPN 建立介面與區域。

入口網站和主要閘道：

- 區域：LSVPN-Untrust-Primary
- 介面：Ethernet1/21
- IPv4：172.16.22.1/24
- 區域：L3-信任
- **Interface**（介面）：Ethernet1/23
- **IPv4**：200.99.0.1/16

備用閘道：

- 區域：LSVPN-Untrust-Primary
- 介面 ：Ethernet1/5
- **IPv4**：172.16.22.25/24
- 區域：L3-信任
- 介面 ：Ethernet1/6
- **IPv4**：200.99.0.1/16

衛星裝置：

- 區域：LSVPN-Sat-Untrust
- 介面：Ethernet1/1
- **IPv4**：172.16.13.1/22
- 區域：L3-信任
- 介面：Ethernet1/2.1
- **IPv4**：200.101.1.1/24

在每個衛星裝置上設定區域、介面和 *IP* 位址。每個衛星裝置的介面和本機 *IP* 位址均不相同。此介面將用於與入口網站和閘道之間的 *VPN* 連線。

©2024 Palo Alto Networks, Inc.

STEP 2 | 在裝載 GlobalProtect 閘道的防火牆上設定邏輯通道介面，用於終止由 GlobalProtect 衛星建立的 VPN 通道。

主要閘道：

- 介面：tunnel.5
- **IPv4**：10.11.15.254/22
- 區域：LSVPN-Tunnel-Primary

備用閘道：

- 介面：tunnel.1
- **IPv4**：10.11.15.245/22
- 區域：LSVPN-Tunnel-Backup

STEP 3 | 啟用 GlobalProtect LSVPN 元件之間的 SSL。

閘道將使用自我簽署的根憑證授權 (CA) 來向 GlobalProtect LSVPN 中的衛星裝置簽發憑證。由於一個防火牆內裝載有入口網站和主要閘道，因此將使用單一憑證來驗證衛星裝置。同一個 CA 將用於為備用閘道產生憑證。CA 產生的憑證將從入口網站推送至為衛星裝置，然後由衛星裝置用於驗證閘道。

您還必須從同一個 CA 為備用閘道產生憑證，允許其用於驗證衛星裝置。

1. 在裝載 GlobalProtect 入口網站的防火牆上建立根 CA 憑證，來為 GlobalProtect 元件簽署憑證。在此範例中，根 CA 憑證被稱為 CA-cert。
2. 為 GlobalProtect 入口網站與閘道建立 SSL/TLS 服務設定檔。由於 GlobalProtect 入口網站與主要閘道位屬於同一個防火牆介面，您可以為這兩個元件使用相同的伺服器憑證。
   - 根 **CA** 憑證：CA-Cert
   - 憑證名稱：LSVPN-Scale
3. 將自我簽署的伺服器憑證部署至閘道。
4. 匯入用來為 LSVPN 元件簽發伺服器憑證的根 CA 憑證。
5. 建立憑證設定檔。
6. 使用以下設定，對備用閘道重複步驟 2 到 5：
   - 根 **CA** 憑證：CA-cert
   - 憑證名稱：LSVPN-back-GW-cert

©2024 Palo Alto Networks, Inc.

STEP 4 | 為 LSVPN 設定 GlobalProtect 閘道。

1. 選取 **Network**（網路） > **GlobalProtect** > **Gateways**（閘道），然後按一下 **Add**（新增）。
2. 在 **General**（一般）頁籤中，將主要閘道命名為 **`LSVPN-Scale`**。
3. 在 **Network Settings**（網路設定）下，選取 **`ethernet1/21`** 作為主要閘道介面，然後輸入 **`172.16.22.1/24`** 作為 IP 位址。
4. 在 **Authentication**（驗證）頁籤中，選取在 3 中建立的 LSVPN-Scale 憑證。
5. 選取 **Satellite (**衛星裝置**)** > **Tunnel Settings**（通道組態），然後選取 **Tunnel Configuration**（通道組態）。將 **Tunnel Interface**（通道介面）設定為 tunnel.5。此使用案例中的所有衛星裝置都將連線至單一閘道，因此需要單一的衛星裝置設定。將根據序號比對衛星裝置，因此衛星裝置無需作為使用者進行驗證。
6. 建立 VPN 連線後，在 **Satellite**（衛星裝置） > **Network Settings**（網路設定）上定義 IP 位址集區，以指派給衛星裝置上的通道介面。由於此使用案例採用了動態路由，因此 Access Routes（存取路由）設定將保持空白。
7. 使用以下設定，對備用閘道重複步驟 1 到 5：
   - 名稱：LSVPN-backup
   - 閘道介面：ethernet1/5
   - 閘道 **IP**：172.16.22.25/24
   - 伺服器憑證：LSVPN-backup-GW-cert
   - 通道介面：tunnel.1

 ©2024 Palo Alto Networks, Inc.

STEP 5 | 在主要和備用閘道上設定 iBGP，然後新增重新散佈設定檔，以允許衛星裝置將本機路由插入閘道。

每個衛星辦公室將管理自己的網路和防火牆，因此將設定名稱為 ToAllSat 的重新散佈設定檔，以將本機路由重新散佈回 GlobalProtect 閘道。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後 **Add**（新增） 虛擬路由器。
2. 在 **Router Settings**（路由器設定）中，為虛擬路由器新增 **Name**（名稱）和 **Interface**（介面）。
3. 在 **Redistribution Profile**（重新散佈設定檔）中，選取 **Add**（新增）。
   1. 將重新散佈設定檔命名為 **`ToAllSat`**，然後將 **Priority**（優先順序）設定為 1。
   2. 將 Redistribute（重新散佈）設定為 **Redist**（可轉散發）。
   3. 從 Interface（介面）下拉式清單 **Add**（新增） **`ethernet1/23`**。
   4. 按一下 **OK**（確定）。
4. 在虛擬路由器上選取 **BGP** 以設定 BGP。
   1. 在 **BGP** > **General**（一般） 中，選取 **Enable**（啟用）。
   2. 輸入閘道 IP 位址作為 **Router Id**（路由器 **ID**）(**`172.16.22.1`**)，輸入 **`1000`** 作為 **AS Number**（**AS** 號碼）。
   3. 在 Options（選項）區段中，選取 **Install Route**（安裝路由）。
   4. 在 **BGP** > **Peer Group**（對等群組）中，按一下 **Add**（新增）以新增對等群組，其中包含所有將要連線至閘道的衛星裝置。
   5. 在 **BGP** > **Redist Rules**（可轉散發規則）中，**Add**（新增）您之前建立的 **`ToAllSat`** 重新散佈設定檔。
5. 按一下 **OK**（確定）。
6. 將 **`ethernet1/6`** 用於重新散佈設定檔，對備用閘道重複步驟 1 到 5。

©2024 Palo Alto Networks, Inc.

STEP 6 | 備妥衛星裝置以加入 LSVPN。

所示的設定為單一衛星裝置的範例。

每次您將新衛星裝置新增至 LSVPN 部署後，需重複此設定。

1. 將通道介面設定為通道端點，以使 VPN 連線至閘道。
2. 將 IPSec 通道類型設定為 GlobalProtect 衛星，並輸入 GlobalProtect 入口網站的 IP 位址。
3. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後 **Add**（新增） 虛擬路由器。
4. 在 **Router Settings**（路由器設定）中，為虛擬路由器新增 **Name**（名稱）和 **Interface**（介面）。
5. 選取 **Virtual Router**（虛擬路由器） > **Redistribution Profile**（重新散佈設定檔），然後進行以下設定，以 **Add**（新增） 設定檔。
   1. 將重新散佈設定檔命名為 **`ToLSVPNGW`**，然後將 **Priority**（優先順序）設定為 1。
   2. **Add**（新增） **Interface**（介面）**`ethernet1/2.1`**。
   3. 按一下 **OK**（確定）。
6. 選取 **BGP** > **General**（一般），**Enable**（啟用）BGP，並按照下列步驟設定通訊協定：
   1. 輸入閘道 IP 位址作為 **Router Id**（路由器 **ID**）(**`172.16.22.1`**)，輸入 **`1000`** 作為 **AS Number**（**AS** 號碼）。
   2. 在 Options（選項）區段中，選取 **Install Route**（安裝路由）。
   3. 在 **BGP** > **Peer Group**（對等群組）中，**Add**（新增）對等群組，其中包含所有將要連線至閘道的衛星裝置。
   4. 在 **BGP** > **Redist Rules**（可轉散發規則）中，**Add**（新增）您之前建立的 **`ToLSVPNGW`** 重新散佈設定檔。
7. 按一下 **OK**（確定）。

©2024 Palo Alto Networks, Inc.

STEP 7 | 為 LSVPN 設定 GlobalProtect 入口網站。

兩個資料中心都將宣告各自的路由，但會使用不同的路由優先順序，以確保主動資料中心是優先閘道。

1. 選取 **Network**（網路） > **GlobalProtect** > **Portals**（入口網站），然後按一下 **Add**（新增）。
2. 在 **General**（一般）中，輸入 **`LSVPN-Portal`** 作為入口網站名稱。
3. 在 **Network Settings**（網路設定）中，選取 **`ethernet1/21`** 作為主要 **Interface**（介面），然後選取 **`172.16.22.1/24`** 作為 **IP Address**（IP 位址）。
4. 在 **Authentication**（驗證）頁籤中，從 **SSL/TLS Service Profile**（SSL/TLS 服務設定檔）下拉式選單中選取之前建立的主要閘道 SSL/TLS 設定檔 **`LSVPN-Scale`**。
5. 在 **Satellite**（衛星裝置）頁籤中，**Add**（新增）衛星裝置，然後 **Name**（命名）為 **`sat-config-1`**。
6. 將 **Configuration Refresh Interval**（設定重新整理間隔）設定為 **`12`**。
7. 在 **GlobalProtect Satellite**（**GlobalProtect** 衛星裝置） > **Devices**（裝置）中，新增 LSVPN 中每個衛星裝置的序號和主機名稱。
8. 在 **GlobalProtect Satellite**（**GlobalProtect** 衛星裝置） > **Gateways**（閘道） 中，新增每個閘道的名稱和 IP 位址。將主要閘道的路由優先順序設為 1，將備用閘道的優先順序設為 10，以確保主動資料中心是優先閘道。

STEP 8 | 驗證 LSVPN 組態。

STEP 9 | （選用）新增站點到 LSVPN 部署。

1. 選取 **Network**（網路） > **GlobalProtect** > **Portals**（入口網站） > **GlobalProtect Portal**（**GlobalProtect** 入口網站） > **Satellite Configuration**（衛星裝置設定） > **GlobalProtect Satellite**（**GlobalProtect** 衛星裝置） > **Devices**（裝置），以將新衛星裝置的序號新增至 GlobalProtect 入口網站。
2. 使用 GlobalProtect 入口網站 IP 位址設定衛星裝置上的 IPSec 通道。
3. 選取 **Network**（網路） > **Virtual Router**（虛擬路由器） > **BGP** > **Peer Group**（對等群組），以將衛星裝置新增至每個閘道上的 BGP 對等群組設定。
4. 選取 **Network**（網路） > **Virtual Router**（虛擬路由器） > **BGP** > **Peer Group**（對等群組），以將閘道新增至新衛星裝置上的 BGP 對等群組設定。

©2024 Palo Alto Networks, Inc.

原則

可讓您強制規定及採取動作的原則。您可在防火牆上建立的不同類型原則規則如下：安全性、NAT、服務品質 (QoS)、基於原則的轉送原則 (PBF)、解密、應用程式覆寫、驗證、拒絕服務 (DoS) 和區域保護原則。所有這些不同的原則共同合作後，即可視需要允許、拒絕、設定優先權、轉送、加密、解密、建立例外、驗證存取及重設連線以協助保護您的網路。

請務必瞭解，在防火牆政策規則中，IPv4 位址集會被視為 IPv6 位址集的子集。然而，IPv6 位址集並非 IPv4 位址集的子集。IPv4 位址可以匹配一個 IPv6 位址集或位址範圍；但 IPv6 位址不能匹配一個 IPv4 位址集或位址範圍。

在所有政策類型中，來源或目的地位址的關鍵字 **any**（任何）表示任何 IPv4 或 IPv6 位址。關鍵字 **any**（任何）等同於 ::/0。如果要表示「任何 IPv4 位址」，請指定 0.0.0.0/0。

在政策比對期間，防火牆會將 IPv4 位址轉換為 IPv6 首碼，其中前 96 個位元為 0。位址 ::/8 意味著，如果前 8 個位元為 0，則匹配規則。所有的 IPv4 位址都將匹配 ::/8、::/9、::/10、::/11、... ::/16、... ::/32，...直至 ::/96。

如果您想要表示「任何 IPv6 位址，但沒有 IPv4 位址」，您必須設定兩個規則。第一個規則拒絕 0.0.0.0/0，以拒絕任何 IPv4 位址（作為來源或目的地位址），第二個規則具有 ::/0，表示任何 IPv6 位址（作為來源或目的地位址），以滿足您的需求。

下列主題說明如何使用原則：

- 識別透過 Proxy 伺服器連線的使用者
- 基於原則的轉送
- 應用程式覆寫政策
- 測試原則規則

©2024 Palo Alto Networks, Inc.

原則類型

Palo Alto Networks 新一代的防火牆支援各種原則，這些原則會一起運作，讓網路上的應用程式能安全地啟用。

確保您瞭解在政策規則中，IPv4 位址集被視為 IPv6 位址集的子集，如 原則 中所述。

對於所有政策類型，當您執行原則規則說明、標籤和稽核註解時，可以使用稽核註解封存檔檢視政策規則如何隨時間變化。該封存檔包括稽核註解歷程記錄和組態日誌，讓您能夠比較組態版本並檢視規則的建立者和修改者及其原因。

原則類型	說明
security	根據流量屬性，例如來源及目的地安全性區域、來源與目的地 IP 位址、應用程式、使用者及服務，決定封鎖或允許工作階段。如需詳細資料，請參閱安全性原則。
NAT	指示防火牆有需要轉譯的封包及轉譯的方式。防火牆支援來源位址及/或連接埠轉譯和目的地位址及/或連接埠轉譯。如需詳細資訊，請參閱 NAT。
QoS	使用已定義的參數或多個參數識別出需要 QoS 處理的流量 (無論是優先處理或頻寬限制)，並將它指派給某個類別。如需詳細資料，請參閱服務品質。
基於原則的轉送	根據路由表識別不應使用一般介面，而應改用其他輸出介面的流量。如需詳細資料，請參閱基於原則的轉送。
解密	識別需要您檢查可見度、控制與精確安全性的加密流量。如需詳細資料，請參閱解密。
應用程式覆寫	確定要繞過 App-ID 第七層處理和威脅檢查的工作階段。當流量匹配應用程式覆寫政策時，將會導致防火牆將工作階段作為第四層具狀態檢查防火牆處理。僅在必須且您可以嚴格套用最低權限原則的最受信任環境中使用應用程式覆寫。如需更多詳細資訊，請參閱應用程式覆寫。
驗證	識別需要使用者進行驗證的流量。如需詳細資料，請參閱驗證原則。
DoS 保護	識別潛在的拒絕服務 (DoS) 攻擊，並在回應規則相符情況時採取保護動作。如需詳細資料，請參閱 DoS 保護設定檔。

©2024 Palo Alto Networks, Inc.

安全性原則

安全性原則用途為保護網路資產免受威脅及發生故障，並協助以最佳方式配置網路資源，以強化業務程序中的產能和效率。在 Palo Alto Networks 防火牆上，個別的安全性原則規則可根據流量屬性決定是否封鎖或允許工作階段，例如來源及目的地安全性區域、來源與目的地 IP 位址、應用程式、使用者及服務。

為確保當一般使用者嘗試存取您的網路資源時會驗證，防火牆在評估安全性原則前會評估驗證原則。

所有通過防火牆的流量均將與工作階段進行比對，而各工作階段也將與安全性原則規則進行比對。當有相符的工作階段時，防火牆會將相符的安全性原則規則套用到該工作階段內的雙向流量（用戶端到伺服器及伺服器到用戶端）。當流量不符合任何已定義的規則時，則會套用預設規則。會預先定義預設規則（顯示於安全性規則庫底部）來允許所有區域內流量和拒絕所有區域間流量。雖然這些規則是預先定義設定的一部分，且預設為唯讀，但您可以覆寫它們並變更有限數量的設定，包括標籤、動作 (允許或封鎖)、日誌設定和安全性設定檔。

安全性原則規則的評估順序為由左至右、從上到下。依據符合定義準則的第一條規則比對封包；在觸發配對後，將不會評估後續的規則。因此，具體的規則順序必須比廣泛的規則優先，如此一來才能強制獲得最符合的條件。如果針對該規則啟用日誌記錄，則符合規則的流量會在工作階段結束時於流量日誌中產生日誌項目。各規則皆可設定日誌記錄選項，例如可設定為在工作階段開始時記錄，或者在工作階段結束時記錄（或者同時設定兩者）。

在管理員設定規則後，您可檢視原則規則使用情況，以確定流量與安全性原則規則相符的時間與次數，從而判斷規則的有效性。隨著規則庫的發展，除非您在建立和修改規則時封存此資訊，否則變更和稽核資訊會逐漸遺失。您可執行原則規則說明、標籤和稽核註解以確保所有管理員都輸入稽核註解，以便您檢視稽核註解封存檔和檢閱註解及設定日誌歷程記錄，並比較所選規則的設定版本。現在，您可以更深入地洞察和控制整個規則庫。

- 安全性原則規則的元件
- 安全性原則動作
- 建立安全性原則規則

安全性原則規則的元件

安全性政策規則結構允許組合必要及選用的欄位，如下表細述。如需在來源或目的地位址中使用萬用字元位址物件的詳細資料，請參閱下表。

必要/選用	欄位	說明
必要	名稱	用來識別規則的標籤（最多 63 個字元）。

©2024 Palo Alto Networks, Inc.

必要/選用	欄位	說明
	UUID	通用唯一識別碼 (UUID) 是一個獨特的 32 字元字串，可永久標識規則，因此無論規則如何變更（例如變更名稱），您都可以對其進行追蹤。
	規則類型	指定將規則套用至區域中和#或區域之間的流量： • 通用（預設值）—將規則套用至指定的來源和目的地區域中所有符合的區域間和區域內流量。例如，如果您以來源區域 A 和 B 以及目的地區域 A 和 B 建立通用規則，則會將規則套用至區域 A 中的所有流量、區域 B 中的所有流量，以及區域 A 到區域 B 的所有流量，和區域 B 到區域 A 的所有流量。 • 區域內—將規則套用至指定的來源區域（無法為區域內規則指定目的地區域）中的所有符合流量。例如，如果將來源區域設定為 A 和 B，則會將規則套用至區域 A 中的所有流量和區域 B 中的所有流量，但不會套用至區域 A 與區域 B 之間的流量。 • 區域間 — 將規則套用至指定的來源與目的地區域之間的所有符合流量。例如，如果將來源區域設為 A、B 和 C，並將目的地區域設為 A 和 B，則會將規則套用至區域 A 到區域 B 的流量、區域 B 到區域 A 的流量、區域 C 到區域 A 的流量，及區域 C 到區域 B 的流量，但不會套用至區域 A、B 或 C 中的流量。
	來源區域	流量起始的區域。
	目的地區域	流量終止的區域。如果您使用 NAT，請確定永遠參考後置 NAT 區域。
	應用程式	您要控制的應用程式。防火牆會使用一種稱之為流量分類技術的 App-ID 來識別您網路上的流量。App-ID 在建立封鎖未知應用程式的安全性原則方面提供應用程式控制及可見度，並同時啟用、檢查和塑形允許的應用程式。
	動作	根據在規則中定義的條件，指定 *Allow*（允許）或 *Deny*（拒絕）流量的動作。當您將防火牆設定為拒絕流量時，它會重設連線或無訊息丟棄封包。為了提供更佳的使用者體驗，您可以將精確選項設定為拒絕流量，而非無訊息丟棄封包，這可能會導致某些應用程式中斷並讓使用者感覺無回應。詳細資訊，請參閱安全性原則工作。
選用	頁籤	可讓您篩選安全性規則的關鍵字或字詞。當您已定義多項規則並希望在之後檢閱標記關鍵字（例如 *IT* 認可的應用程式或高風險應用程式）的規則，此功能十分方便。

©2024 Palo Alto Networks, Inc.

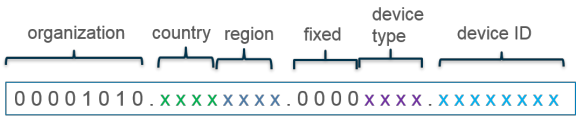
必要/選用	欄位	說明
	說明	可用於說明規則的文字欄位，最多 1024 個字元。
	來源位址	定義主機 IP 位址、子網路、位址物件（類型包括 IP 網路遮罩、IP 範圍、FQDN 或 IP 萬用字元遮罩）、位址群組或國家的強制動作。如果您使用 NAT，請確定參考封包中的原始 IP 位址 (即預先 NAT IP 位址)。如需 IP 萬用字元遮罩的詳細資料，請參閱下表。
	目的地位址	封包的位置或目的地。定義 IP 位址、子網路、位址物件（類型包括 IP 網路遮罩、IP 範圍、FQDN 或 IP 萬用字元遮罩）、位址群組或國家的強制動作。如果您使用 NAT，請確定參考封包中的原始 IP 位址 (即預先 NAT IP 位址)。如需 IP 萬用字元遮罩的詳細資料，請參閱下表。
	使用者	原則套用的使用者或群組使用者。您必須在該區域啟用 User-ID。若要啟用 User-ID，請參閱 User-ID 概要介紹。
	URL 類別	將 URL 類別作為比對準則可讓您以各個 URL 類別為基礎，自訂安全性設定檔（防毒、反間諜軟體、漏洞、檔案封鎖、資料篩選和 DoS）。例如，您可防止有更高風險的 URL 類別進行下載/上傳 .exe 檔案，但允許其他類別下載/上傳。此功能也能讓您將排程附加至特定的 URL 類別 (在午餐時及下班後允許社交網站)、使用 QoS 標記特定的 URL 類別 (金融、醫藥和商業)，並依每個 URL 類別為基礎選取不同的日誌轉送設定檔。 雖然您可在防火牆上手動設定 URL 類別，但若要使用 Palo Alto Networks 防火牆上的可用動態 URL 類別更新，您必須購買 URL 篩選授權。 若要根據 *URL* 類別封鎖或允許流量，您必須將 *URL* 篩選設定檔套用到安全性原則規則。將 *URL* 類別定義為任何項目，並將 *URL* 篩選設定檔附加至安全性原則。如需使用安全性原則中的預設設定檔資訊，請參閱設定基本安全性原則。
	服務	可讓您為應用程式選取 Layer 4 (TCP 或 UDP) 連接埠。您可選擇任何項目、指定連接埠或使用應用程式預設值，以允許使用該應用程式的標準連接埠。例如，對於包含已知埠號的應用程式，例如 DNS，應用程式預設值選項只會比對 TCP 連接埠 53 上的 DNS 流量。您也可以新增自訂應用程式，及定義應用程式可使用的連接埠。

©2024 Palo Alto Networks, Inc.

必要/選用	欄位	說明
		若為內送允許規則 (例如，從不信任到信任)，請使用 (應用程式預設值)，防止在不常見的連接埠和通訊協定上執行應用程式。[應用程式預設值] 是預設選項，防火牆仍將檢查所有連接埠上的所有應用程式，但使用此設定時，應用程式只允許在其標準的連接埠/通訊協定上執行。
	安全性設定檔	提供額外的威脅、弱點及資料洩漏保護。安全性設定檔只能用來評估具有允許動作的規則。
	HIP 設定檔（適用於 GlobalProtect）	可讓您識別有主機資訊設定檔 (HIP) 的用戶端，然後強制限定存取權限。
	選項	可讓您定義工作階段的日誌記錄、日誌轉送設定、變更符合規則的封包服務品質 (QoS) 標記，以及排程安全性規則應生效的時刻 (日期與時間)。

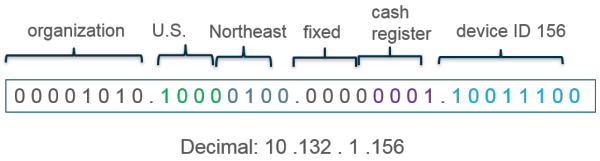
本節說明如何在安全性政策規則的 Source Address（來源位址）或 Destination Address（目的地位址）中使用萬用字元位址物件。將私人 IPv4 位址指派給內部裝置時，您可以使用 IP 定址結構，將含義指派給位址中的某些位元。例如，IP 位址的第三個八位元中的前三個位元表示裝置類型。此結構可協助您根據裝置的 IP 位址輕鬆識別裝置的詳細資料，例如裝置類型或位置。您可以在安全性政策規則中使用相同的 IP 定址結構，以便於部署。您建立使用萬用字元位址（IP 位址和萬用字元遮罩，以斜線分隔，例如 10.1.2.3/0.127.248.0）的位址物件。萬用字元位址可以在單一安全性政策規則中識別許多來源或目的地位址，這對於為許多裝置提供服務的資料中心防火牆特別有用。由於 IP 位址容量限制，您不需要管理不必要的大量位址物件來涵蓋所有相符的 IP 位址，也不需要使用比所需限制少的安全性政策規則。

例如，假設您使用下圖中顯示的 IPv4 定址結構，其中第一個八位元代表您的組織（位元 00001010 是固定的）。在第二個八位元中，前四個位元指定網路裝置所在的國家/地區（1000 表示美國），最後四個位元表示區域（0100 表示東北部）。在第三個八位元中，前四個位元為零，最後四個位元表示裝置類型（0001 表示收銀機，0011 表示印表機）。最後一個八位元表示網路裝置的識別碼。



根據該結構，美國東北部收銀機號碼 156 的 IP 位址為 10.132.1.156：

 ©2024 Palo Alto Networks, Inc.



您可以使用 **IP Wildcard Mask**（**IP** 萬用字元遮罩）類型的位址物件，在安全性政策規則中支援此類定址結構。您可以將萬用字元遮罩套用至 IPv4 來源或目的地位址，以指定哪些位址受規則約束。在 Palo Alto Networks 萬用字元遮罩中，零位元表示被比較的位元必須符合零涵蓋之 IP 位址中的位元。遮罩中的一位元是萬用字元或「忽略」位元，這意味著被比較的位元不需要符合 IP 位址中的位元。例如，以下 IP 位址和萬用字元遮罩片段說明了其如何產生四個相符項：

```
0011    binary snippet
1010    wildcard mask
--------
0001    yields four matches
0011
1001
1011
```

並非所有廠商都使用一作為萬用字元位元，使用零作為比對位元。

在此範例中，收銀機的 IPv4 位址的第三個八位元為 00000001，而印表機的 IPv4 位址的第三個八位元 00000011。假設您要將安全性政策規則套用至識別碼為 0 到 255 的所有收銀機和印表機。為了取得這樣的結果，您需要一個萬用字元遮罩；該萬用字元遮罩的第三個八位元必須是 2，並且裝置 ID（第四個八位元）必須是 255。指定美國東北部所有收銀機和印表機的位址物件會使用萬用字元位址 10.132.1.2/0.0.2.255：

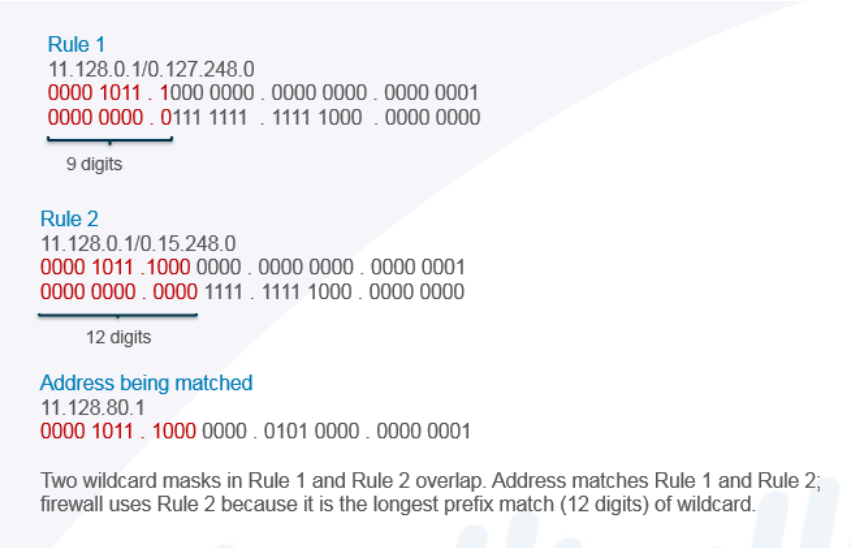
```
0000 1010.1000 0100.0000 0001.0000 0010 (IP address 10.132.1.2)
0000 0000.0000 0000.0000 0010.1111 1111 (wildcard mask 0.0.2.255)
--------------------------------------------------------------------------------
yields these matches:
0000 1010.1000 0100.0000 0001.0000 0000
0000 1010.1000 0100.0000 0001.0000 0001
0000 1010.1000 0100.0000 0001.0000 0010
0000 1010.1000 0100.0000 0001.0000 0011
   ... and so on (fourth octet yields every number from 0 to 255)
and
0000 1010.1000 0100.0000 0011.0000 0000
0000 1010.1000 0100.0000 0011.0000 0001
0000 1010.1000 0100.0000 0011.0000 0010
0000 1010.1000 0100.0000 0011.0000 0011
   ... and so on (fourth octet yields every number from 0 to 255)
```

因此，使用萬用字元位址 10.132.1.2/0.0.2.255 作為目的地位址的位址物件的單一安全性政策規則與 512 個裝置（256 個收銀機 + 256 個印表機）的位址相符，這是將規則套用至許多裝置的有效方法。萬用字元遮罩必須以至少一個零 (0) 開頭，例如 0.0.2.255。

在安全性政策規則中使用 **IP Wildcard Mask**（**IP** 萬用字元遮罩）類型的位址物件時，請考量下列事項：

 ©2024 Palo Alto Networks, Inc.

- 使用 **IP Wildcard Mask**（**IP** 萬用字元遮罩）類型之位址物件的來源或目的地位址不支援 **Negate**（否定）選項。
- 進行陰影比對時，防火牆不會考慮萬用字元位址，也就是說，如果使用類型為 **IP Wildcard Mask**（**IP** 萬用字元遮罩）之位址物件的安全性政策規則與後續規則重疊或被清單上較高的規則重疊，您將不會收到警告。
- 如果位址符合具有重疊萬用字元遮罩的規則，防火牆會選擇與萬用字元遮罩中最長首碼相符的規則，如下圖所示：



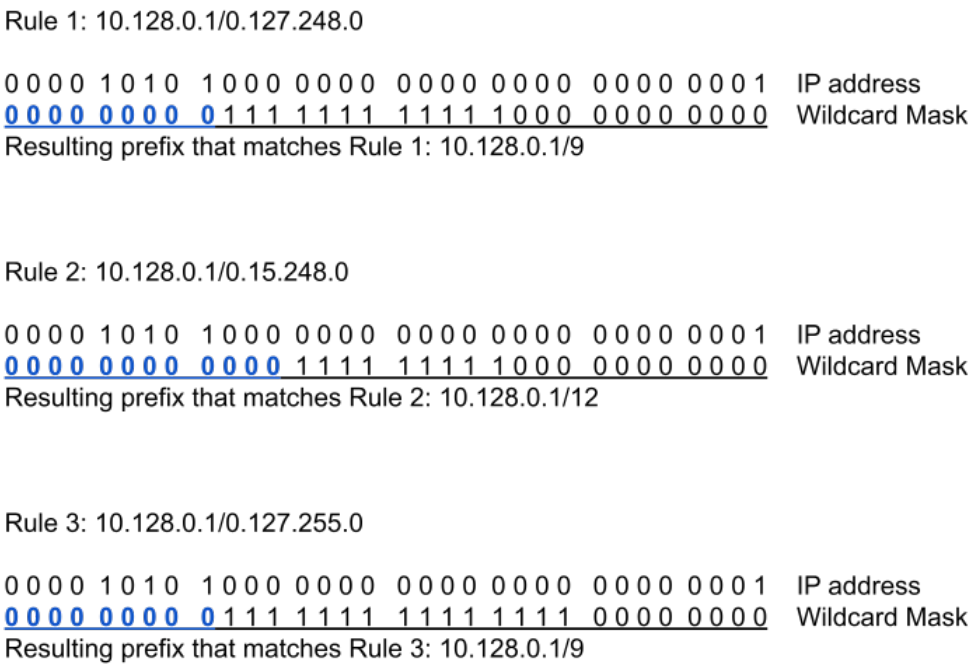
前面的項目符號介紹了預設行為。但是，在某些使用案例中，您希望具有廣泛的規則，允許某些來源存取一般應用程式（例如 Ping、Traceroute 和 Web 瀏覽），但具有較窄的規則，允許這些來源的子集除了可以存取一般應用程式之外，還可以存取其他應用程式（例如 SSH、SCP）。在較早的版本中，此類部署無法正常工作，因為只會處理與萬用字元遮罩中最長首碼相符的規則，而且不會考慮其他規則。

從 PAN-OS 10.2.1 開始，您可以啟用 **Wildcard Top Down Match Mode**（萬用字元自上而下比對模式）；因此，如果具有 IP 位址的封包符合具有重疊萬用字元遮罩的安全性政策規則中的首碼，防火牆會以自上而下的順序選擇第一個完全符合的規則（而不是選擇與萬用字元遮罩中最長首碼相符的規則）。在使用重疊萬用字元遮罩的規則中找到符合首碼的封包；然後防火牆會根據遮罩選擇完全符合所有位址位元的規則，同時記住遮罩中的規則指示萬用字元或「忽略」位元。然後檢查其他規則準則，例如應用程式和區域。在其他規則準則檢查期間，防火牆會選擇符合準則的規則中的第一個規則（依自上而下的順序）。不會評估其他規則。

Wildcard Top Down Match Mode（萬用字元自上而下比對模式）表示可能會在不同的封包上強制執行多個規則（而不僅僅是與最長首碼相符的規則）。將更具體的規則放在清單頂部。例如，您可以允許較小範圍的相符位址（較長的萬用字元遮罩）存取特定應用程式，并在後續規則中允許較大範圍的 IP 位址（較短的萬用字元遮罩）存取不同（較一般）的應用程式集。您可以透過選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理），然後編輯政策規則庫設定，來啟用 **Wildcard Top Down Match Mode**（萬用字元自上而下比對模式）。

 ©2024 Palo Alto Networks, Inc.

下面的範例已啟用 **Wildcard Top Down Match Mode**（萬用字元自上而下比對模式），並且三個安全性政策規則（每個規則都指定具有萬用字元遮罩位址物件的來源 IP 位址）和萬用字元遮罩重疊：



在此範例中，來源 IP 位址為 10.143.8.1 (0000 1010 1000 1111 0000 1000 0000 0001) 的用戶端 A 完全符合規則 1、規則 2 和規則 3；第一個相符項是規則 1（自上而下的順序）。假設其他規則準則相符，則來自用戶端 A 的封包會受到規則 1 動作的約束。

來源 IP 位址為 10.160 2.1 (0000 1010 1010 0000 0000 0010 0000 0001) 的用戶端 B 不完全符合規則 1 中的位址，而且不符合規則 2 中的首碼。用戶端 B 的位址完全符合規則 3，這是依自上而下的順序排列的第一個相符規則。假設其他規則準則相符，則來自用戶端 B 的封包會受到規則 3 動作的約束。因此，我們看到了 **Wildcard Top Down Match Mode**（萬用字元自上而下比對模式）的好處，即規則 1 和規則 3 可以同時在不同的封包上生效。

安全性原則動作

針對安全性原則中定義符合屬性的流量，您可以套用下列動作：

動作	說明
Allow（允許）（預設）	允許流量。
拒絕	封鎖流量並強制執行針對要拒絕之應用程式定義的預設 *Deny Action*（拒絕動作）。若要檢視應用程式預設定義的拒絕動作，請

 ©2024 Palo Alto Networks, Inc.

動作	說明
	在 **Objects**（物件） > **Applications**（應用程式）中檢視應用程式詳細資料，或在 Applipedia 中檢查應用程式詳細資料。
丟棄	無訊息丟棄流量；對於應用程式，將覆寫預設拒絕動作。TCP 重設不會傳送至主機/應用程式。 針對 Layer 3 介面，若要將 ICMP 無法連線回應選擇性地傳送至用戶端，請設定 (動作)：**Drop**（丟棄）並啟用 **Send ICMP Unreachable**（傳送 **ICMP** 無法連線）核取方塊。啟用後，防火牆會針對與目的地通訊已遭系統管理禁止的情況傳送 ICMP 指令碼—ICMPv4：類型 3、代碼 13；ICMPv6：類型 1、代碼 1。
Reset client（重設用戶端）	傳送 TCP 重設至用戶端設備。
Reset server（重設伺服器）	傳送 TCP 重設至伺服器設備。
Reset both（重設兩者）	傳送 TCP 重設至用戶端及伺服器設備。

只有在形成工作階段之後才會傳送重設。若在 *3* 方交握完成之前工作階段就遭封鎖，則防火牆將不會傳送重設。

針對具有重設動作的 TCP 工作階段，防火牆不會傳送 ICMP 無法連線回應。

針對具有丟棄或重設動作的 TCP 工作階段，若選取 **ICMP Unreachable**（**ICMP** 無法連線）核取方塊，則防火牆會傳送 ICMP 訊息至用戶端。

建立安全性原則規則

在設定安全性政策規則之前，確保您瞭解 IPv4 位址集會被視為 IPv6 位址集的子集，原則中對此進行了詳細說明。

STEP 1 | （選用）刪除預設安全性原則規則。

依預設，本防火牆包括名為 *rule1* 的安全性規則，並允許信任區域到不信任區域的所有流量。您可刪除或修改規則，以反映您的區域命名慣例。

STEP 2 | 新增規則。

1. 選取 **Policies**（原則） > **Security**（安全性），並 **Add**（新增） 新的規則。
2. 在 **General**（一般）頁籤中，輸入規則的描述性 **Name**（名稱）。
3. 選取 **Rule Type**（規則類型）。

©2024 Palo Alto Networks, Inc.

STEP 3 | 為封包中的來源欄位定義比對準則。

1. 在 **Source**（來源）頁籤中，選取 **Source Zone**（來源區域）。
2. 指定 **Source IP Address**（來源 **IP** 位址）或將此值設為 **any**（任何）。

   如果您決定 ***Negate***（否定）一個區域作為 ***Source Address***（來源位址），請確保將包含私人 *IP* 位址的所有區域都新增到 ***Source Address***（來源位址），以避免這些私人 *IP* 位址之間的連線丟失。
3. 指定來源 **User**（使用者）或將此值設為 **any**（任何）。

STEP 4 | 為封包中的目的地欄位定義比對準則。

1. 在 **Destination**（目的地）頁籤上，設定 **Destination Zone**（目的地區域）。
2. 指定 **Destination IP Address**（目的地 **IP** 位址）或將此值設為 **any**（任何）。

   如果您決定 ***Negate***（否定）一個區域作為 ***Destination Address***（目的地位址），請確保將包含私人 *IP* 位址的所有區域都新增到 ***Destination Address***（目的地位址），以避免這些私人 *IP* 位址之間的連線丟失。

   作為最佳做法，使用位址物件作為 ***Destination Address***（目的地位址），來啟用僅對特定伺服器或特定伺服器群組的存取權限，特別是針對容易被入侵的 *DNS* 和 *SMTP* 等服務。憑藉限制使用者僅使用特定的目的地伺服器位址，可以防止資料外洩以及命令與控制流量透過 *DNS* 通道等技術來建立通訊。

STEP 5 | 指定規則將允許或封鎖的應用程式。

最佳做法是，一律使用以應用程式為基礎的安全性原則規則，而不是以連接埠為基礎的規則，並一律將服務設為應用程式預設值，除非您使用的連接埠清單具有比應用程式的標準連接埠更嚴格的限制。

1. 在 **Applications**（應用程式）頁籤上，**Add**（新增）您要安全啟用的 **Application**（應用程式）。您可以選取多個應用程式，或者可使用應用程式群組或應用程式篩選器。
2. 在 **Service/URL Category**（服務/**URL** 類別）頁籤上，將服務設為 **application-default**（應用程式預設值），確保規則允許的任何應用程式僅在其標準連接埠上被允許。

STEP 6 | （選用）將 URL 類別指定為規則的比對準則。

在 **Service/URL Category**（服務/**URL** 類別）頁籤上，選取 **URL Category**（**URL** 類別）。

如果您選取 URL 類別，僅網頁流量與規則相符且流量僅限於以指定類別為目標。

STEP 7 | 定義需要防火牆對與規則相符的流量採取的動作。

在 **Actions**（動作）頁籤上選取 **Action**（動作）。關於每個動作的說明，請參閱安全性原則動作。

 ©2024 Palo Alto Networks, Inc.

STEP 8 | 進行日誌設定。

- 依預設，規則將設為 **Log at Session End**（工作階段結束時記錄）。如果您不想在流量與此規則相符時產生任何日誌，可以停用此設定，或者可選取 **Log at Session Start**（工作階段開始時記錄）進行更詳細的記錄。

  Log At Session Start（工作階段開始時記錄）比僅在工作階段結束時記錄會耗用更多的資源。在大多數情況下，您只能 **Log At Session End**（工作階段結束時記錄）。啟用 **Log At Session Start**（工作階段開始時記錄）和 **Log At Session End**（工作階段結束時記錄）僅用於疑難排解、長期通道工作階段（例如 GRE 通道）（除非您在工作階段開始時記錄，否則您無法在 ACC 中看到這些工作階段），並獲得對營運技術/工業控制系統 (OT/ICS) 工作階段的可見性（這些工作階段也是長期工作階段）。

- 選取 **Log Forwarding**（日誌轉送）設定檔。

作為最佳做法，請勿選取 ***Disable Server Response Inspection***（停用伺服器回應檢查）*(DSRI)* 的核取方塊。選取此選項，會阻止防火牆檢查從伺服器通向用戶端的封包。為確保最佳安全性，防火牆必須同時檢查用戶端至伺服器的流量以及伺服器至用戶端的流量，以偵測並防禦威脅。

STEP 9 | 附加安全性設定檔，讓防火牆可以掃描所有允許的流量存在的威脅。

務必建立最佳做法安全性設定檔，幫助保護網路免遭已知和未知威脅的攻擊。

在 **Actions**（動作）頁籤上，從 **Profile Type**（設定檔類型）下拉式清單中選取 **Profiles**（設定檔），然後選取個別安全性設定檔以附加到規則。

或者，從 **Profile Type**（設定檔類型）下拉式清單中選取 **Group**（群組），然後選取要附加的安全性 **Group Profile**（群組設定檔）。

STEP 10 | 按一下 **Commit**（提交），將您的原則規則儲存至防火牆上正在執行的組態。

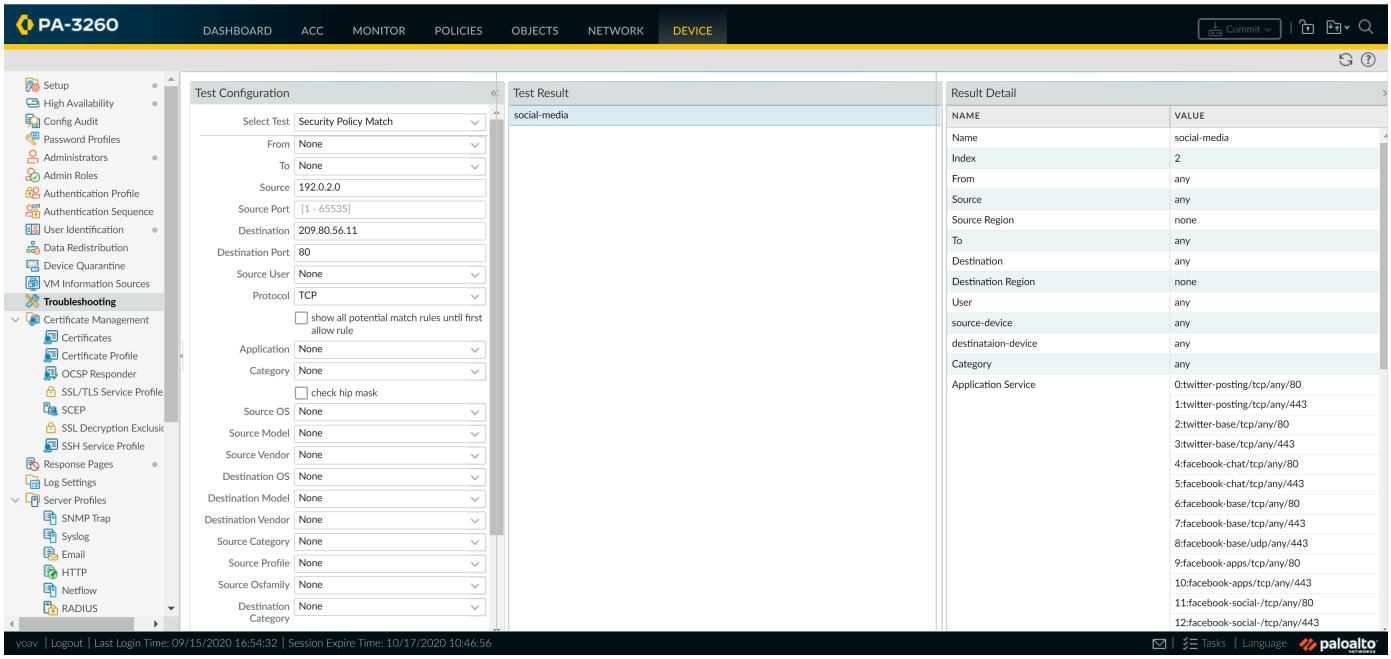
©2024 Palo Alto Networks, Inc.

STEP 11 | 若要確認已有效設定基本的安全性原則，請測試安全性原則規則是否經過評估，再決定要套用流量的安全性原則規則。

輸出顯示最佳規則符合在 CLI 命令中指定的來源與目的地 IP 位址。

例如，若要確認原則規則將在 IP 位址 208.90.56.11 的資料中心伺服器存取 Microsoft 更新伺服器時套用：

1. 選取 **Device**（裝置） > **Troubleshooting**（疑難排解），然後從 Select Test（選取測試）下拉式清單中選取 **Security Policy Match**（安全性原則比對）。
2. 輸入來源與目的地 IP 位址。
3. 輸入通訊協定。
4. **Execute**（執行）安全性原則比對測試。



STEP 12 | 等待足夠長時間以允許流量通過防火牆後，檢視原則規則使用情況，以監控原則規則的使用狀態並確定原則規則的有效性。

©2024 Palo Alto Networks, Inc.

原則物件

原則物件為聚集離散識別碼 (例如 IP 位址、URL、應用程式或使用者) 的單一物件或收集單元。如具備屬於收集單元的原則物件，您可參考安全性原則中的物件，不必一次手動選取多個物件。一般而言，在建立原則物件時，您可聚集需要類似原則權限的物件。例如，如果您的組織使用一組伺服器 IP 位址進行使用者驗證，則您可將多組伺服器 IP 位址編組作為位址群組原則物件，並參考安全性原則中的位址群組。將物件編組後，您即可大幅減少建立原則的管理負荷。

如果您需匯出組態的特定部分以進行內部檢閱或稽核，可透過 *PDF* 或 *CSV* 檔案的格式匯出組態表格資料。

您可在防火牆上建立下列原則物件：

原則物件	說明
位址/位址群組，地區	可讓您將需要強制執行相同原則的特定來源或目的地位址編組。位址物件可能包括一組 IPv4 或 IPv6 的位址（單一 Ip、範圍、子網路）、一個 IP 萬用字元位址（IPv4 位址/萬用字元遮罩）或 FQDN。此外，可透過經度與緯度座標來定義區域，或者可選取國家並定義 IP 位址或 IP 範圍。之後您即可將收集的位址物件編組，以建立位址群組物件。 您也可使用動態位址群組，以動態方式更新主機 IP 位址頻繁變更環境中的 IP 位址。 防火牆上預先定義的外部動態清單 *(EDL)* 計入某防火牆型號支援的位址物件數目上限。
使用者/使用者群組	可讓您從本機資料庫、外部資料庫或匹配條件中建立使用者清單並加以編組。
應用程式群組及應用程式篩選	您可使用應用程式篩選動態篩選應用程式。可讓您使用防火牆應用程式資料庫中定義的屬性來篩選及儲存應用程式群組。例如，您可依據一項或多項屬性（類別、子類別、技術、風險、特性）來建立應用程式篩選器。進行內容更新時，所有符合篩選條件的新篩選應用程式都可以使用應用程式篩選自動新增至您儲存的應用程式篩選。 您可使用應用程式群組建立想要一併編組群組使用者或進行特定服務的特定應用程式靜態群組，或達成特定原則目標。請參閱建立應用程式群組。
服務/服務群組	可讓您指定來源及目的地連接埠與服務可用的通訊協定。防火牆包括兩項預先定義服務 (http 及 https 服務) 其中 HTTP 使用 TCP 埠號 80 及 8080，而 HTTPS 則使用 TCP 埠號 443。但是您可在選擇的任何 TCP/

©2024 Palo Alto Networks, Inc.

原則物件	說明
	UDP 連接埠上建立任何自訂服務，以限制您網路上特定連接埠的應用程式用途 (換句話說，您可為應用程式定義預設連接埠)。 若要檢視應用程式使用的標準連接埠，在 ***Objects***（物件） > ***Applications***（應用程式） 中搜尋應用程式，然後按一下連結。此時會顯示簡短的說明。

©2024 Palo Alto Networks, Inc.

安全性設定檔

雖然安全性原則規則可讓您允許或封鎖網路上的流量，但安全性設定檔卻可協助您定義允許但掃描規則，也就是掃描允許的應用程式是否潛藏威脅，例如病毒、惡意軟體、間諜軟體與 DDOS 攻擊。當流量符合安全性原則中定義的允許規則後，會套用連結規則的安全性設定檔，以供未來內容檢查規則使用，例如防毒檢查及資料篩選。

在流量符合標準中不使用安全性設定檔。安全性原則允許應用程式或類別後，會套用安全性設定檔以掃描流量。

防火牆提供預設安全性設定檔，讓您跳脫出既有的框架，以開始保護網路免受威脅侵擾。如需使用安全性原則中的預設設定檔資訊，請參閱設定基本安全性原則。在您更進一步瞭解您網路的安全性需求後，請參閱建立最佳做法網際網路閘道安全性設定檔，以瞭解如何能夠建立自訂設定檔。

如需安全性設定檔的最佳做法設定相關建議，請參閱建立最佳做法網際網路閘道安全性設定檔。

您可以新增一般會一起套用的安全性設定檔，以建立安全性設定檔群組；這組設定檔可被視為一個單元，並可以單一步驟新增到安全性原則（如果您選擇設定預設安全性設定檔群組，則會預設包含在安全性原則內）。

設定檔類型	說明
防毒設定檔	防毒設定檔可防禦病毒、蠕蟲與木馬程式及間諜軟體下載。Palo Alto Networks 防毒解決方案在收到第一個封包時使用串流惡意軟體保護引擎檢查流量，可在未明顯影響防火牆效能的情況下提供用戶端保護。此設定檔會掃描廣大的惡意軟體執行檔、PDF 檔案、HTML 與 JavaScript 病毒，其中包括支援掃描內部壓縮檔及資料編碼結構描述。如果您已在防火牆上啟用解密，則設定檔也會啟用解密內容掃描功能。 預設設定檔會檢查所有列出的通訊協定解碼器是否有病毒，並產生 SMTP、IMAP 和 POP3 通訊協定的警示，同時封鎖 FTP、HTTP 及 SMB 通訊協定。您可以為解碼器或防毒特徵碼設定動作，並指定防火牆回應威脅事件的方式： • 預設—針對 Palo Alto Networks 定義的每個威脅特徵碼與防毒特徵碼，會內部指定預設動作。一般而言，預設動作為警示或重設兩者。在威脅或防毒特徵碼中，預設動作會顯示在括號中，例如，預設 (警示)。 • **Allow**—允許應用程式流量。 ***Allow*** 動作不會產生與特徵碼或設定檔相關的日誌。

©2024 Palo Alto Networks, Inc.

設定檔類型	說明
	• **Alert**—針對每個應用程式流量產生警示。警示會儲存在威脅日誌中。 • **Drop**—丟棄應用程式流量。 • 重設用戶端—針對 TCP，會重設用戶端連線。針對 UDP，會丟棄連線。 • 重設伺服器—針對 TCP，會重設伺服器端連線。針對 UDP，會丟棄連線。 • 重設用戶端與伺服器—針對 TCP，會重設用戶端及伺服器的連線。針對 UDP，會丟棄連線。 自訂設定檔可以用來最小化受信任安全性區域之間流量的防毒檢驗，及最大化從不受信任區域（例如網際網路）中收到的流量以及傳送至高機密目的地（例如伺服器群）的流量的檢驗。 Palo Alto Networks WildFire 系統也提供更會規避且其他防毒解決方案尚未發現的持續性威脅特徵碼。WildFire 發現威脅後，會迅速建立特徵碼，然後整合至威脅防範用戶可每日下載（WildFire 用戶每小時內可取得）的標準防毒特徵碼。
反間諜軟體設定檔	反間諜軟體設定檔會阻止受危害主機上的間諜軟體嘗試回報 (phone-home) 或發出訊號至外部的命令與控制 (C2) 伺服器，讓您能夠偵測從受感染的用戶端離開網路的惡意流量。您可在區域之間套用各種層級的保護。例如，您可自訂反間諜軟體設定檔，將信任區域間的檢查次數降至最低，同時將從不信任區域接收的流量檢查次數升至最高，例如網際網路取向的區域。當防火牆由 Panorama 管理伺服器管理時，ThreatID 會對應到防火牆上相應的自訂威脅，以使防火牆能夠產生填充了已設定自訂 ThreatID 的威脅日誌。 將反間諜軟體套用到安全性原則規則時，您可在定義自己的反間諜軟體設定檔，或選擇下列其中一個預先定義的設定檔： • 預設—建立特徵碼時針對各特徵碼採用 Palo Alto Networks 指定的預設動作。 • 嚴格—不論特徵碼檔案中定義的動作為何，一律將重要、高度與中度嚴重性威脅的預設動作覆寫為封鎖動作。此設定檔仍會對嚴重性為低及資訊的特徵碼採用預設動作。 當防火牆偵測到威脅事件時，您可以在反間諜軟體設定檔中設定下列動作： • 預設—針對 Palo Alto Networks 定義的每個威脅特徵碼與反間諜軟體特徵碼，會內部指定預設動作。一般而言，預設動作為警示或重設

©2024 Palo Alto Networks, Inc.

設定檔類型	說明
	兩者。在威脅或防毒特徵碼中，預設動作會顯示在括號中，例如，預設 (警示)。 • 允許—允許應用程式流量 ***Allow*** 動作不會產生與特徵碼或設定檔相關的日誌。 • **Alert**—針對每個應用程式流量產生警示。警示會儲存在威脅日誌中。 • **Drop**—丟棄應用程式流量。 • 重設用戶端—針對 TCP，會重設用戶端連線。針對 UDP，會丟棄連線。 • 重設伺服器—針對 TCP，會重設伺服器端連線。針對 UDP，會丟棄連線。 • 重設用戶端與伺服器—針對 TCP，會重設用戶端及伺服器的連線。針對 UDP，會丟棄連線。 在某些情況下，當設定檔動作設定為 ***reset-both***（重設兩者）時，相關聯的威脅日誌可能會將動作顯示為 ***reset-server***（重設伺服器）。若防火牆在工作階段開始時偵測到威脅並向用戶端顯示 *503* 封鎖頁面，則會發生這種情況。由於封鎖頁面不允許連線，不需要重設用戶端，只重設伺服器端連線。 • 封鎖 **IP**—此動作可封鎖來自來源或來源-目的地對的流量。可針對指定時段設定。 此外，您可以在反間諜軟體設定檔中啟用 DNS Sinkholing 動作，讓防火牆偽造對 DNS 查詢已知惡意網域的回應，使其將惡意網域名稱解析為您所定義的 IP 位址。此功能有助於使用 DNS 流量識別受保護網路上被感染的主機。接著可在流量與威脅日誌中輕易識別受感染的主機，因為嘗試連線至 sinkhole IP 位址的任何主機最可能感染到惡意軟體。 反間諜軟體及漏洞保護設定檔的設定方式相似。
漏洞保護設定檔	漏洞保護設定檔會阻止嘗試利用系統瑕疵或取得對系統未經授權之存取。反間諜軟體設定檔可在流量離開網路時幫助識別受感染的主機，而漏洞防護設定檔則是防範威脅進入網路。例如，漏洞保護設定檔可幫助防範緩衝區溢位、非法指令碼執行及其他嘗試利用系統弱點的行為。預設漏洞保護設定檔可保護用戶端與伺服器免受所有已知重要、高與中度嚴重性威脅。您也可以建立例外狀況，變更對特定特徵碼的回應。當防火牆由 Panorama 管理伺服器管理時，ThreatID 會對應到防火牆上相應的自訂威脅，以使防火牆能夠產生填充了已設定自訂 ThreatID 的威脅日誌。

©2024 Palo Alto Networks, Inc.

設定檔類型	說明
	當防火牆偵測到威脅事件時，您可以在反間諜軟體設定檔中設定下列動作： • 預設—針對 Palo Alto Networks 定義的每個威脅特徵碼與反間諜軟體特徵碼，會內部指定預設動作。一般而言，預設動作為警示或重設兩者。在威脅或防毒特徵碼中，預設動作會顯示在括號中，例如，預設 (警示)。 • 允許—允許應用程式流量 ***Allow*** 動作不會產生與特徵碼或設定檔相關的日誌。 • **Alert**—針對每個應用程式流量產生警示。警示會儲存在威脅日誌中。 • **Drop**—丟棄應用程式流量。 • 重設用戶端—針對 TCP，會重設用戶端連線。針對 UDP，會丟棄連線。 • 重設伺服器—針對 TCP，會重設伺服器端連線。針對 UDP，會丟棄連線。 • 重設用戶端與伺服器—針對 TCP，會重設用戶端及伺服器的連線。針對 UDP，會丟棄連線。 在某些情況下，當設定檔動作設定為 ***reset-both***（重設兩者）時，相關聯的威脅日誌可能會將動作顯示為 ***reset-server***（重設伺服器）。若防火牆在工作階段開始時偵測到威脅並向用戶端顯示 *503* 封鎖頁面，則會發生這種情況。由於封鎖頁面不允許連線，不需要重設用戶端，只重設伺服器端連線。 • 封鎖 **IP**—此動作可封鎖來自來源或來源-目的地對的流量。可針對指定時段設定。
URL 篩選原則	URL 篩選設定檔可讓您監控及控制使用者如何透過 HTTP 與 HTTPS 存取 Web。防火牆其預設設定檔已設定為封鎖如已知惡意軟體、網路釣魚及成人內容等網站。您可以在安全性原則中使用預設的原則、複製原則作為新 URL 篩選原則的起點，或新增 URL 設定檔，讓新設定檔中所有的類別設為允許看見您網路上的流量。接著您可以自訂新增的 URL 設定檔，並新增要永遠封鎖或允許的特定網站清單，如此能更精確控制 URL 類別。
資料篩選設定檔	資料篩選設定檔可防止機密資訊 (例如信用卡或社會安全號碼) 從受保護的網路外洩。資料篩選設定檔也可讓您篩選關鍵字，例如機密專案名稱或機密文字。讓設定檔鎖定所需的檔案類型以減少誤判非常重要。例

©2024 Palo Alto Networks, Inc.

設定檔類型	說明
	如，您可能只想搜尋 Word 文件或 Excel 試算表。但也可能只想掃描網頁瀏覽流量或 FTP。 您可以建立自訂資料模式物件並將其附加至資料篩選設定檔，以定義您要篩選的資訊類型。根據下列項建立資料模式物件： • 預先定義模式—使用預先定義的模式篩選信用卡號碼和社會安全號碼（有或沒有短破折號）。 • 規則運算式—篩選字元字串。 • 檔案屬性—根據檔案類型篩選檔案屬性和值。 如果您使用協力廠商端點資料外洩防護 *(DLP)* 解決方案來填入檔案屬性以指示敏感內容，此選項可讓防火牆強制執行 *DLP* 原則。 如要開始，請參閱 資料篩選
檔案封鎖設定檔	防火牆使用檔案封鎖設定檔，透過指定的應用程式並以指定的工作階段流動方向 (輸入/輸出/兩者) 來封鎖指定的檔案類型。您可設定好設定檔，以便警示或封鎖上傳及/或下載，並可指定受檔案封鎖設定檔管理的應用程式。也可進行相關設定，在使用者嘗試下載指定檔案類型時，顯示自訂封鎖頁面。這可讓使用者有時間考慮是否要下載檔案。 將檔案封鎖套用到安全性原則規則時，您可在定義自訂檔案封鎖設定檔，或選擇下列其中一個預先定義的設定檔。這些預先定義的設定檔（653 及更新內容版本中會提供）將允許您快速啟用最佳做法檔案封鎖設定： • 基本檔案封鎖—將此設定檔附加至允許流量進出不敏感應用程式的安全性原則規則，以封鎖惡意軟體攻擊活動中一般包含的檔案或沒有真實使用案例要上傳/下載的檔案。此設定檔將封鎖 PE 檔案（.scr、.cpl、.dll、.ocx、.pif、.exe）、Java 檔案（.class、.jar）、Help 檔案 (.chm、.hlp) 以及其他可能有惡意的檔案類型，包括 .vbe、.hta、.wsf、.torrent、.7z、.rar、.bat。此外，它還將在嘗試下載加密 rar 或加密 zip 檔案時提示使用者進行認可。此規則將針對所有其他檔案類型發出警示，讓您可以完全看到進出網路的所有檔案類型。 • 嚴格檔案封鎖—對安全性原則規則使用此更嚴格的設定檔，以允許存取最敏感之應用程式。此設定檔用於封鎖與其他設定檔相同的檔案類型，此外還可以封鎖 Flash、.tar、多層級編碼、.cab、.msi、加密 rar 以及加密 zip 檔案。 設定採取下列動作的檔案封鎖設定檔： • 警示—偵測到指定的檔案類型時，在資料篩選日誌中產生日誌。

©2024 Palo Alto Networks, Inc.

設定檔類型	說明
	• 封鎖—偵測到指定的檔案類型時，封鎖檔案，並向使用者顯示可自訂的封鎖頁面。同時在資料篩選日誌中產生日誌。 • 繼續—偵測到指定的檔案類型時，向使用者顯示可自訂的回應頁面。使用者可點選頁面以下載檔案。同時在資料篩選日誌中產生日誌。由於這一類的轉送動作需要使用者互動，所以僅適用於 Web 流量。 如要開始，設定檔案封鎖
WildFire 分析設定檔	使用 WildFire 分析設定檔可讓防火牆轉送未知檔案或電子郵件連結，以進行 WildFire 分析。根據應用程式、檔案類型與傳輸方向 (上傳或下載) 指定要轉送以進行分析的檔案。與設定檔規則相符的檔案或電子郵件連結會根據為規則定義的分析位置，轉送 WildFire 公共雲端或 WildFire 私人雲端 (使用 WF-500 裝置主控)。如果設定檔規則設定用於向 WildFire 公用雲端轉送檔案，則防火牆除了轉送未知檔案以外，還會轉送與現有防毒特徵碼相符的檔案。 您也可以使用 WildFire 分析設定檔來設定 WildFire 混合雲端部署。如果您使用 WildFire 裝置本機分析敏感檔案 (例如 PDF)，您可以指定，以讓不太敏感的檔案類型 (例如 PE 檔案) 或 WildFire 裝置分析不支援的檔案類型 (例如 APK) 能夠由 WildFire 公共雲端進行分析。同時使用 WildFire 裝置與 WildFire 雲端進行分析可讓您從雲端已處理檔案及裝置分析不支援之檔案的提示裁定中獲益，並可釋放裝置容量來處理敏感內容。
DoS 保護設定檔	DoS 保護設定檔提供拒絕服務 (DoS) 保護原則的詳細控制。DoS 保護原則可讓您根據彙總工作階段或來源及/或目的地 IP 位址，控制介面、區域、位址與國家之間的工作階段數量。Palo Alto Networks 防火牆支援兩種 DoS 保護機制。 • 爆流保護—偵測並預防使用大量封包攻擊網路導致半開啟的工作階段及/或服務過多，因而無法回應每一個要求。在此情況下，發起攻擊的來源位址通常是偽造的。請參閱設定對新工作階段流量的 DoS 保護。 • 資源消耗保護—偵測並預防工作階段資源消耗攻擊。此類攻擊會使用大量主機 (Bot) 盡可能建立最多完整建立的工作階段來消耗所有系統資源。 您可以在單一 DoS 保護設定檔中定義這兩種保護機制。 DoS 設定檔可用於指定採取的動作類型及 DoS 原則的比對標準詳細資訊。DoS 設定檔可定義 SYN、UDP 與 ICMP Flood 攻擊的設定、啟用資源消耗保護，以及定義工作階段的上限。設定 DoS 保護設定檔後，即可將其連結至 DoS 原則。

©2024 Palo Alto Networks, Inc.

設定檔類型	說明
	設定 DoS 保護時，分析環境以設定正確臨界值非常重要，由於定義 DoS 保護原則有些複雜，因此本指南不列出詳細的範例。
區域保護設定檔	區域保護設定檔提供特定網路區域之間額外的保護，保護區域免受攻擊。設定檔必須套用至整個區域，因此仔細測試設定檔以防止正常流量周遊區域時發生問題便相當重要。定義地區保護設定檔的每秒封包數 (pps) 臨界值時，臨界值將依據與先前建立的工作階段不相符的每秒封包數。
安全性設定檔群組	安全性設定檔群組是一組安全性設定檔，您可以將這一組設定檔視為一個單元，輕鬆地將此單元新增至安全性原則。您可以將經常一起指派的服務新增到設定檔群組，以簡化安全性原則的建立。您也可以設定預設的安全性設定檔群組—新的安全性設定檔將使用在預設設定檔群組中定義的設定，來檢查與控制符合安全性原則的流量。將安全性設定檔群組命名為 default，可讓該群組中的設定檔會預設新增至新的安全性原則。這可讓您一致地將組織偏好的設定檔設定自動包含在新的原則中，而無須在每次建立新規則時手動新增安全性設定檔。 請參閱建立安全性設定檔群組以及設定或覆寫預設安全性設定檔群組。 如需安全性設定檔的最佳做法設定相關建議，請參閱建立最佳做法網際網路閘道安全性設定檔。

建立安全性設定檔群組

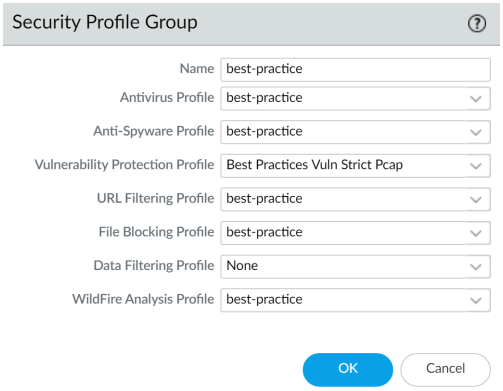
使用下列步驟可建立安全性設定檔群組，並將它新增至安全性原則中。

©2024 Palo Alto Networks, Inc.

STEP 1 | 建立安全性設定檔群組。

若您將群組指定為 `default`（預設值），防火牆會自動將其附加到您建立的新規則。如果您有一組偏好的安全性設定檔並想要確保已將它們附加到每個新規則，這是一個節省時間的好方法。

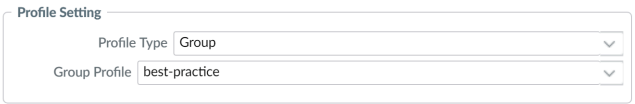
1. 選取 **Objects**（物件） > **Security Profile Groups**（安全性設定檔群組），然後 新增 一個新的安全性設定檔群組。
2. 為設定檔群組設定具描述性的 **Name**（名稱），例如「威脅」。
3. 如果防火牆在多個虛擬系統模式下，請啟用設定檔讓所有的虛擬系統 **Shared**（共用）。
4. 將現有設定檔新增至群組。



5. 按一下 **OK**（確定）儲存設定檔群組。

STEP 2 | 將安全性設定檔群組新增至安全性原則。

1. 選取 **Policies**（原則） > **Security**（安全性），然後 **Add**（新增） 或修改安全性原則規則。
2. 選取 **Actions**（動作）頁籤。
3. 在 Profile Setting（設定檔組態）區段中，為 **Profile Type**（設定檔類型）選取 **Group**（群組）。
4. 在 **Group Profile**（群組設定檔）下拉式清單中，選取您建立的群組（例如，選取最佳做法群組）：



5. 按一下 **OK**（確定）儲存原則，然後 **Commit**（提交）變更。

STEP 3 | 儲存變更。

按一下 **Commit**（交付）。

©2024 Palo Alto Networks, Inc.

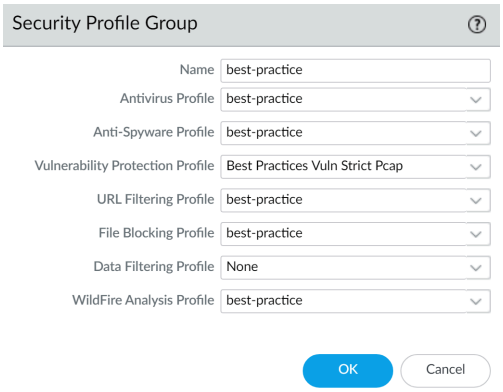
設定或覆寫預設安全性設定檔群組

使用下列選項可設定在新安全性原則中使用的預設安全性設定檔群組，或取代現有的預設群組。當管理員建立新的安全性原則時，系統會自動選取預設設定檔群組作為原則的設定檔設定，並根據在設定檔群組中定義的設定來檢查符合原則的流量 (管理員可以視需要選擇手動選取其他的設定檔設定)。使用下列選項可設定預設安全性設定檔群組，或覆寫預設設定。

如果沒有預設安全性設定檔存在，則新安全性原則的設定檔設定會預設為 ***None***（無）。

建立安全性設定檔群組。

1. 選取 **Objects**（物件） > **Security Profile Groups**（安全性設定檔群組），然後新增一個新的安全性設定檔群組。
2. 為設定檔群組設定具描述性的 **Name**（名稱），例如「威脅」。
3. 如果防火牆在多個虛擬系統模式下，請啟用設定檔讓所有的虛擬系統 **Shared**（共用）。
4. 將現有設定檔新增至群組。關於建立設定檔的詳細資料，請參閱安全性設定檔。



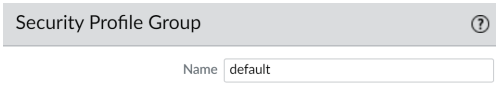
5. 按一下 **OK**（確定）儲存設定檔群組。
6. 將安全性設定檔群組新增至安全性原則。
7. **Add**（新增）或修改安全性原則規則，然後選取 **Actions**（動作）頁籤。
8. 為 **Profile Type**（設定檔類型）選取 **Group**（群組）。
9. 在 **Group Profile**（群組設定檔）下拉式清單中，選取您建立的群組（例如，選取「威脅」群組）：

10. 按一下 **OK**（確定）儲存原則，然後 **Commit**（提交）變更。

©2024 Palo Alto Networks, Inc.

設定預設安全性設定檔群組。

1. 選取 **Objects**（物件） > **Security Profile Groups**（安全性設定檔群組），然後新增新的安全性設定檔群組，或修改現有的安全性設定檔群組。
2. 將安全性設定檔群組 **Name**（名稱）設為 **`default`**：



3. 按一下 **OK**（確定）與 **Commit**（提交）。
4. 確認預設安全性設定檔群組已依預設包含在新的安全性原則中：
   1. 選取 **Policies**（原則） > **Security**（安全性），然後**Add**（新增）一個新的安全性原則。
   2. 選取 **Actions**（動作）頁籤，然後檢視 **Profile Setting**（設定檔設定）欄位：

依預設，新的安全性原則會正確顯示 **Profile Type**（設定檔類型）已設為 Group（群組），並已選取名為 default 的 **Group Profile**（群組設定檔）。

覆寫預設安全性設定檔群組。

如果您有現有的預設安全性設定檔群組，且您不想要該組設定檔附加到新的安全性原則，則您可以根據您的偏好繼續修改 Profile Setting（設定檔設定）欄位。首先為您的原則選取不同的設定檔類型（**Policies**（原則） > **Security**（安全性） > **Security Policy Rule**（安全性原則規則） > **Actions**（動作））。

資料篩選

使用資料篩選設定檔來防止敏感、機密和專有資訊離開您的網路。預先定義的模式、內建設定與自訂選項能方便您保護包含某些檔案屬性（如文件標題或作者）、信用卡號碼、不同國家的監管資訊（如社會安全號碼）及協力廠商資料外洩防護 (DLP) 標籤的檔案。

- 預先定義的資料模式—輕鬆篩選常見模式，包括信用卡號碼。預先定義的資料篩選模式還可以識別全球不同國家的特定（監管）資訊，例如社會安全號碼（美國）、INSEE 識別碼（法國）和紐西蘭稅務局識別碼。許多預先定義的資料篩選模式都符合 HIPAA、GDPR、格雷姆-里奇-比利雷法案等標準。
- 對 **Azure** 資訊保護和 **Titus** 資料分類的內建支援—預先定義的檔案屬性方便您根據 Azure 資料保護和 Titus 標籤篩選內容。Azure 資訊保護標籤儲存在中繼資料中，因此請確保您知道希望防火牆篩選的 Azure 資訊保護標籤 GUID。
- 用於資料遺失防護 **(DLP)** 解決方案的自訂資料模式—如果您使用協力廠商端點 DLP 解決方案來填入檔案屬性以指示敏感內容，則可建立自訂資料模式，以識別 DLP 解決方案標記的檔案屬性和值，然後記錄或封鎖資料篩選設定檔根據該模式偵測到的檔案。

©2024 Palo Alto Networks, Inc.

建立資料篩選設定檔

資料篩選設定檔可以防止敏感資訊離開網路。

若要開始使用，首先需要建立一個資料模式，以指定您希望防火牆篩選的資訊類型和欄位。然後，將該模式附加到資料篩選設定檔，以指定防火牆所篩選內容的執行方式。新增資料篩選設定檔至安全性政策規則以開始篩選與規則相符的流量。

如果您正在利用企業資料丟失防護 *(DLP)*，請參閱企業 DLP 管理員指南。

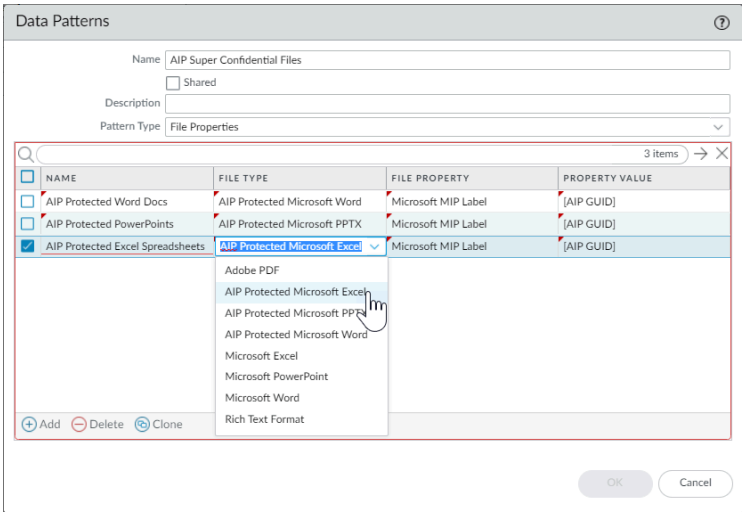
©2024 Palo Alto Networks, Inc.

STEP 1 | 定義新資料模式物件，以偵測您要篩選的資訊。

1. 選取 **Objects**（物件） > **Custom Objects**（自訂物件） > **Data Patterns**（資料模式），然後 **Add**（新增） 物件。
2. 提供新物件的描述性 **Name**（名稱）。
3. （選用）若要讓以下對象使用資料模式，則選取 **Shared**（共用）：
   - 多虛擬系統防火牆上的每個虛擬系統 **(vsys)**—如果清除（停用），資料模式將僅供 **Objects**（物件）頁籤上選定的虛擬系統使用。
   - **Panorama** 上的每個裝置群組—如果清除（停用），資料模式將僅供 **Objects**（物件）頁籤上選定的裝置群組使用。
4. （選用—僅限 Panorama）選取 **Disable override**（停用覆寫），可防止管理員在繼承此資料模式物件的裝置群組中覆寫該物件的設定。預設會清除此選取項目，這表示管理員可以覆寫繼承此物件之任何設備群組的設定。
5. （選用—僅限 Panorama）選取 **Data Capture**（資料擷取）可自動收集由篩選器所封鎖的資料。

   在 *Settings*（設定）頁面上指定 *Manage Data Protection*（管理資料保護）的密碼，以檢視您擷取的資料（***Device***（裝置） > ***Setup***（設定） > ***Content-ID***（內容 ***ID***） > ***Manage Data Protection***（管理資料保護））。
6. 將 **Pattern Type**（模式類型）設為下列其中一項：
   - **Predefined Pattern**（預先定義的模式）—篩選信用卡、社會安全號碼和個人可識別資訊，以符合 HIPAA、GDPR、格雷姆-里奇-比利雷法案等合規標準。
   - 規則運算式—篩選自訂資料模式。
   - 檔案屬性—根據檔案屬性和相關值進行篩選。
7. 新增規則到資料模式物件。
8. 根據您為此物件選取的 **Pattern Type**（模式類型）指定資料模式：
   - 預先定義—選取 **Name**（名稱）並選擇要據此進行篩選的預先定義資料模式。
   - 規則運算式—指定描述性 **Name**（名稱），選取您要掃描的 **File Type**（檔案類型）（或多個類型），然後輸入您希望防火牆偵測的特定 **Data Pattern**（資料模式）。
   - 檔案屬性—指定描述性 **Name**（名稱），選取您要掃描的 **File Type**（檔案類型）和 **File Property**（檔案屬性），然後輸入您希望防火牆偵測的特定 **Property Value**（屬性值）。
     - 若要篩選 **Titus** 分類文件：選取一個不受 AIP 保護的檔案類型，並將 **File Property**（檔案類型）設為 TITUS GUID。輸入 Titus 標籤 GUID 作為 **Property Value**（屬性值）。
     - 對於帶有 **Azure** 資訊保護標籤的文件：選取除富文字格式以外的任何 **File Type**（檔案類型）。對於所選檔案類型，將 **File Property**（檔案屬性）設為 Microsoft MIP 標籤，然後輸入 Azure 資訊保護標籤 GUID 作為 **Property Value**（屬性值）。

 ©2024 Palo Alto Networks, Inc.



9. 按一下 **OK**（確定）以儲存資料模式。

STEP 2 | 新增資料模式物件到資料篩選設定檔。

1. 選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **Data Filtering**（資料篩選），然後 **Add**（新增） 或修改資料篩選設定檔。
2. 提供新設定檔的描述性 **Name**（名稱）。
3. **Add**（新增）設定檔規則，然後選取您在步驟中建立的資料模式。
4. 指定 **Applications**（應用程式）、**File Types**（檔案類型） 以及您要根據資料模式篩選的流量 **Direction**（方向）（上傳或下載）。

   您選取的檔案類型必須與您之前為資料模式定義的檔案類型相同，或者其必須包含資料模式檔案類型。例如，您可以定義資料模式物件和資料篩選設定檔，以掃描所有 *Microsoft Office* 文件。或者，您也可以設定資料模式物件，以僅比對 *Microsoft PowerPoint* 簡報，同時讓資料篩選設定檔掃描所有 *Microsoft Office* 文件。

   如果資料模式物件已附加至資料篩選設定檔，但所設定的檔案類型並不一致，則設定檔將無法正確篩選與資料模式物件相符的文件。
5. 設定 **Alert Threshold**（警示臨界值），指定為了觸發警示而必須在檔案中偵測到資料模式的次數。
6. 設定 **Block Threshold**（封鎖臨界值），以封鎖包含至少這麼多資料模式實例的檔案。
7. 設定為與此規則相符的檔案記錄的 **Log Severity**（日誌嚴重性）。
8. 按一下 **OK**（確定）來儲存資料篩選設定檔。

 ©2024 Palo Alto Networks, Inc.

STEP 3 | 對流量套用資料篩選設定。

1. 選取 **Policies**（原則） > **Security**（安全性），然後 **Add**（新增） 或修改安全性原則規則。
2. 選取 **Actions**（動作），然後將 Profile Type（設定檔類型）設定為 **Profiles**（設定檔）。
3. 將您在步驟 2 中建立的資料篩選設定檔附加至安全性原則規則。
4. 按一下 **OK**（確定）。

STEP 4 | （建議）阻止 Web 瀏覽器繼續防火牆已終止的工作階段。

此選項可確保在防火牆偵測到敏感檔案並隨後丟棄時，*Web* 瀏覽器無法繼續嘗試擷取該檔案的工作階段。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Content-ID**（內容-**ID**），然後編輯 Content-ID Settings（內容-ID 設定）。
2. 清除 **Allow HTTP partial response**（允許 **HTTP** 部分回應）。
3. 按一下 **OK**（確定）。

STEP 5 | 監控防火牆篩選的檔案。

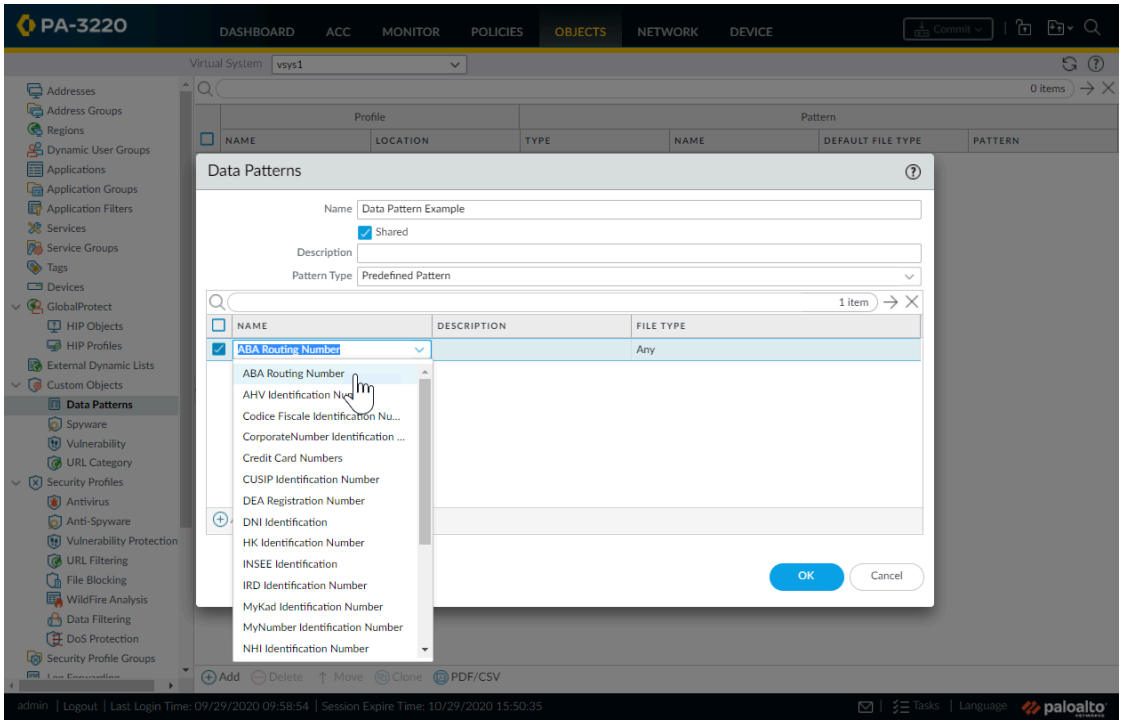
選取 **Monitor**（監控） > **Data Filtering**（資料篩選），以檢視防火牆根據資料篩選設定偵測並封鎖的檔案。

預先定義的資料篩選模式

為符合 HIPAA、GDPR 及格雷姆-里奇-比利雷法案等標準， 防火牆提供了預先定義的資料模式。您可使用這些模式來防止諸如信用卡號和社會安全號碼等常見類型的敏感資訊從網路外洩。

您可透過選取物件 > 自訂物件 > 資料模式並按一下新增新物件以找到預先定義的資料模式。然後，將模式類型設為預先定義的模式並新增新規則至資料模式物件。從顯示於名稱下方的清單中選取資料模式。

©2024 Palo Alto Networks, Inc.



如果要保護的資料類型不在預先定義模式的清單中，您可使用規則運算式建立自訂模式。

以下是可用資料模式清單：

模式	說明
信用卡號	16 位信用卡號
社會安全號碼	9 位社會安全號碼（帶短破折號）
社會安全號碼（不帶短破折號分隔符）	9 位社會安全號碼（不帶短破折號）
ABA 路由號碼	美國銀行協會路由號碼
AHV 識別號碼	瑞士 Alters und Hinterlassenenversicherungsnummer
稅務識別號碼	意大利財務稅號卡識別號碼
CorporateNumber 識別號碼	日本國家稅務機關公司號碼
CUSIP 識別號碼	統一安全識別程序委員會識別號碼
DEA 註冊號碼	美國美國藥品監督管理局註冊號碼

©2024 Palo Alto Networks, Inc.

模式	說明
DNI 識別號碼	西班牙 Documento nacional de identidad 識別號碼
香港身份證號碼	香港居民身份證號碼
INSEE 識別號碼	法國國家統計及經濟研究局識別號碼
IRD 識別號碼	紐西蘭國稅局識別號碼
MyKad 識別號碼	馬來西亞 MyKad 身份證識別號碼
MyNumber 識別號碼	日本社會安全與稅號系統識別號碼
NHI 識別號碼	紐西蘭國民健康指數
NIF 識別號碼	西班牙稅務識別號碼
NIN 識別號碼	台灣身份證號碼
NRIC 識別號碼	新加坡國民身份證識別號碼
永久帳戶識別號碼	印度國民永久帳戶號碼
PRC 識別號碼	中華人民共和國居民身份證號碼
PRN 識別號碼	韓國居民註冊號碼
韓國居民註冊	韓國居民註冊號碼

設定檔案封鎖

檔案封鎖設定檔可讓您識別要封鎖或監控的特定檔案類型。對於大多數流量（包括內部網路上的流量），需要封鎖已知存在威脅的檔案，或者並非實際用於上傳/下載的檔案。目前，這些包括批次檔、DLL、Java 類別檔案、說明檔案、Windows 捷徑 (.lnk) 及 BitTorrent 檔案。此外，可提供偷渡式下載防護，允許可執行及封存檔案（.zip 和 .rar）下載/上傳，但強制使用者確認其正在傳送檔案，以便讓使用者注意到瀏覽器正在嘗試下載其不知情的內容。對於允許一般 Web 瀏覽的原則規則，務必更嚴格地執行檔案封鎖，因為使用者在不知情的情況下下載惡意檔案的風險更高。對於這類流量，需要附加更嚴格的檔案封鎖設定檔，該設定檔同時也會封鎖可攜式可執行 (PE) 檔。

將檔案封鎖套用到安全性原則規則時，您可在定義自訂檔案封鎖設定檔，或選擇下列其中一個預先定義的設定檔。轉換到最佳做法檔案封鎖設定時，您可以複製和編輯預先定義的設定檔（653 及更新內容版本中會提供），然後按照檔案封鎖設定檔安全轉換步驟保留應用程式可用性：

©2024 Palo Alto Networks, Inc.

- 基本檔案封鎖—將此設定檔附加至允許流量進出不敏感應用程式的安全性原則規則，以封鎖惡意軟體攻擊活動中一般包含的檔案或沒有真實使用案例要上傳/下載的檔案。此設定檔將封鎖 PE 檔案（.scr、.cpl、.dll、.ocx、.pif、.exe）、Java 檔案（.class、.jar）、Help 檔案 (.chm、.hlp) 以及其他可能有惡意的檔案類型，包括 .vbe、.hta、.wsf、.torrent、.7z、.rar、.bat。此外，它還將在嘗試下載加密 rar 或加密 zip 檔案時提示使用者進行認可。此規則將針對所有其他檔案類型發出警示，讓您可以完全看到進出網路的所有檔案類型。
- 嚴格檔案封鎖—對安全性原則規則使用此更嚴格的設定檔，以允許存取最敏感之應用程式。此設定檔用於封鎖與其他設定檔相同的檔案類型，此外還可以封鎖 Flash、.tar、多層級編碼、.cab、.msi、加密 rar 以及加密 zip 檔案。

這些預先定義的設定檔用於提供最安全的網路環境。但是，如果您有業務關鍵性應用程式依賴於預設設定檔中指定要封鎖的某些應用程式，則您可以複製設定檔，然後根據需要進行修改。確保您僅為需要上傳及/或下載有風險之檔案類型的使用者使用修改過的設定檔。此外，為了減小受攻擊面，務必使用了其他安全性措施來確保使用者上傳和下載的檔案不會對組織造成威脅。例如，如果您必須允許下載 PE 檔案，則務必要傳送所有未知 PE 檔案到 WildFire 進行分析。此外，還需維持嚴格的 URl 篩選原則，以確保使用者無法從已知裝載有惡意內容的網站下載內容。

STEP 1 | 建立檔案封鎖設定檔。

1. 選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **File Blocking**（檔案封鎖），然後 **Add**（新增）設定檔。
2. 輸入檔案封鎖設定檔的 **Name**（名稱），例如 **`Block_EXE`**。
3. （選用）輸入 **Description**（說明），例如 **`Block users from downloading exe files from websites`**。
4. （選用）指定與下列項 **Shared**（共用）設定檔：
   - 多虛擬系統防火牆上的每個虛擬系統 **(vsys)**—如果清除（停用），設定檔將僅供 **Objects**（物件）頁籤上選定的虛擬系統使用。
   - **Panorama** 上的每個裝置群組—如果清除（停用），設定檔將僅供 **Objects**（物件）頁籤上選定的裝置群組使用。
5. （選用—僅限 Panorama）選取 **Disable override**（停用覆寫），可防止管理員在繼承此檔案封鎖設定檔的裝置群組中覆寫該設定檔的設定。預設會清除此選取項目，這表示管理員可以覆寫繼承此設定檔之任何設備群組的設定。

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 設定檔案封鎖選項。

1. 為設定檔 **Add**（新增）並定義規則。
2. 為該規則輸入 **Name**（名稱），例如 **`BlockEXE`**。
3. 選取 **Any**（任何）或指定一個或多個要篩選的特定 **Applications**（應用程式），例如 **web-browsing**（**Web** 瀏覽）。

   僅 *Web* 瀏覽器才能顯示回應頁面（提示繼續），讓使用者確認選取任何其他導致這些應用程式流量被封鎖的應用程式，因為不會顯示讓使用者繼續的提示。
4. 選取 **Any**（任何）或指定一個或多個要篩選的特定 **File Types**（檔案類型），例如 **exe**。
5. 指定 **Direction**（方向），例如 **download**（下載）。
6. 指定 **Action**（行動）（**alert**（警示）、**block**（封鎖） 或 **continue**（繼續））。

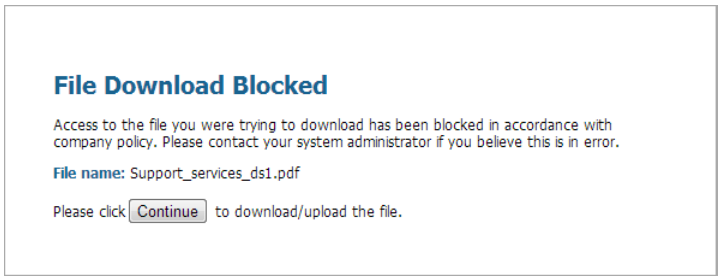
   例如，選取 **continue**（繼續），以提示使用者在需要先確認，然後才能下載可執行檔 (.exe)。或者，您也可以 **block**（封鎖）指定檔案，或設定防火牆在使用者下載可執行檔時僅觸發 **alert**（警示）。

   如果伺服器在不同的封包中傳送 *HTTP* 回應標頭和檔案內容，即使對該檔案類型的動作是 *`continue`*（繼續），防火牆也會封鎖該檔案。
7. 按一下 **OK**（確定）來儲存設定檔。

STEP 3 | 將檔案封鎖設定檔套用至安全性原則規則。

1. 選取 **Policies**（原則） > **Security**（安全性），再選取現有的原則規則或 **Add**（新增）規則，如設定基本安全性原則中所述。
2. 在 **Actions**（動作）頁籤中，選取您在上一步中設定的檔案封鎖設定檔。在此範例中，設定檔名稱為 **`Block_EXE`**。
3. **Commit**（提交）組態。

STEP 4 | 若要測試檔案封鎖組態，可存取防火牆信任區域中的端點 PC，並嘗試從不信任區域的網站下載可執行檔；應該要顯示回應頁面。按一下 **Continue**（繼續）以確認下載檔案。您也可以設定其他動作，例如 **alert**（警示）或 **block**（封鎖），不向使用者提供繼續下載的選項。下列顯示檔案封鎖的預設回應頁面：



 ©2024 Palo Alto Networks, Inc.

STEP 5 | （選用）定義自訂檔案封鎖回應頁面（**Device**（裝置） > **Response Pages**（回應頁面））。您可藉此在使用者看見回應頁面時，提供更多的資訊。您可以包含公司原則及服務台聯絡方式等資訊。

在建立使用 ***continue***（繼續）動作的檔案封鎖設定檔時，您可以僅選取 ***web-browsing***（***Web*** 瀏覽）應用程式。如果您選擇其他任何應用程式，與安全性原則相符的流量將不通過防火牆，因為將不會為使用者提供繼續選項。此外，您還需要為 *HTTPS* 網站設定並啟用解密原則。

檢查日誌，以確定測試此功能時使用的應用程式。例如，如果您正在使用 *Microsoft Sharepoint* 下載檔案，即使您使用網頁瀏覽器存取網站，但應用程式實際上是 `sharepoint-base` 或 `sharepoint-document`。（該命令可幫助您將應用程式類型設定為 ***Any***（任何），以便進行測試。）

©2024 Palo Alto Networks, Inc.

追蹤規則庫中的規則

若要追蹤規則庫中的規則，您可參考規則編號，其根據規則庫中規則的順序進行變更。規則編號決定防火牆套用規則的順序。

即使修改規則（例如變更規則名稱），規則的通用唯一識別碼 *(UUID)*也不會變更。UUID 讓您即使在刪除規則後，也可以追蹤規則庫中的規則。

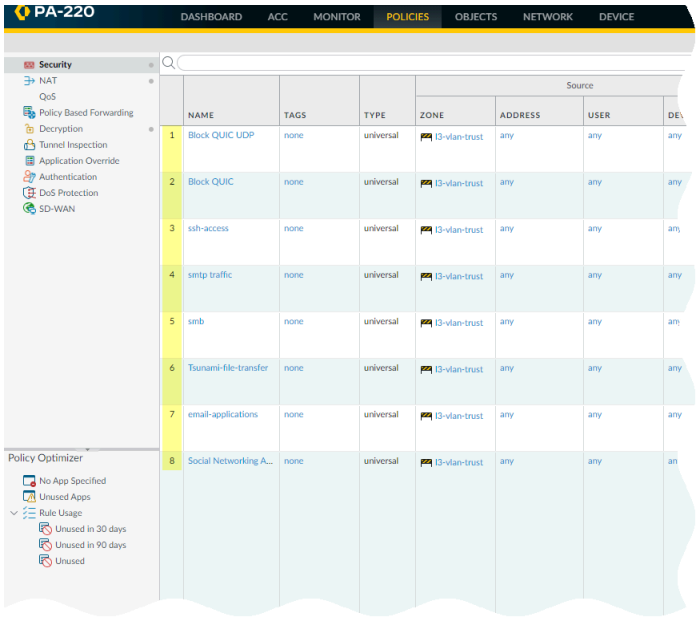
規則編號

防火牆會自動對規則庫中的每個規則進行編號；當您移動或重新排序規則時，編號將根據新的順序進行變更。當您篩選規則清單以尋找符合特定篩選器的規則時，防火牆會在規則庫中完整規則集的內容中列出每個規則及其編號，以及其在評估順序中的位置。

Panorama 獨立地為預先規則、後續規則以及預設規則編號。Panorama 將規則推送至防火牆時，規則編號會反映共用規則、裝置群組預先規則、防火牆規則、裝置群組後續規則以及預設規則的階層與評估順序。您可在 Panorama 中 **Preview Rules**（預覽規則），顯示防火牆上規則總數的編號清單。

檢視防火牆上編號的規則清單。

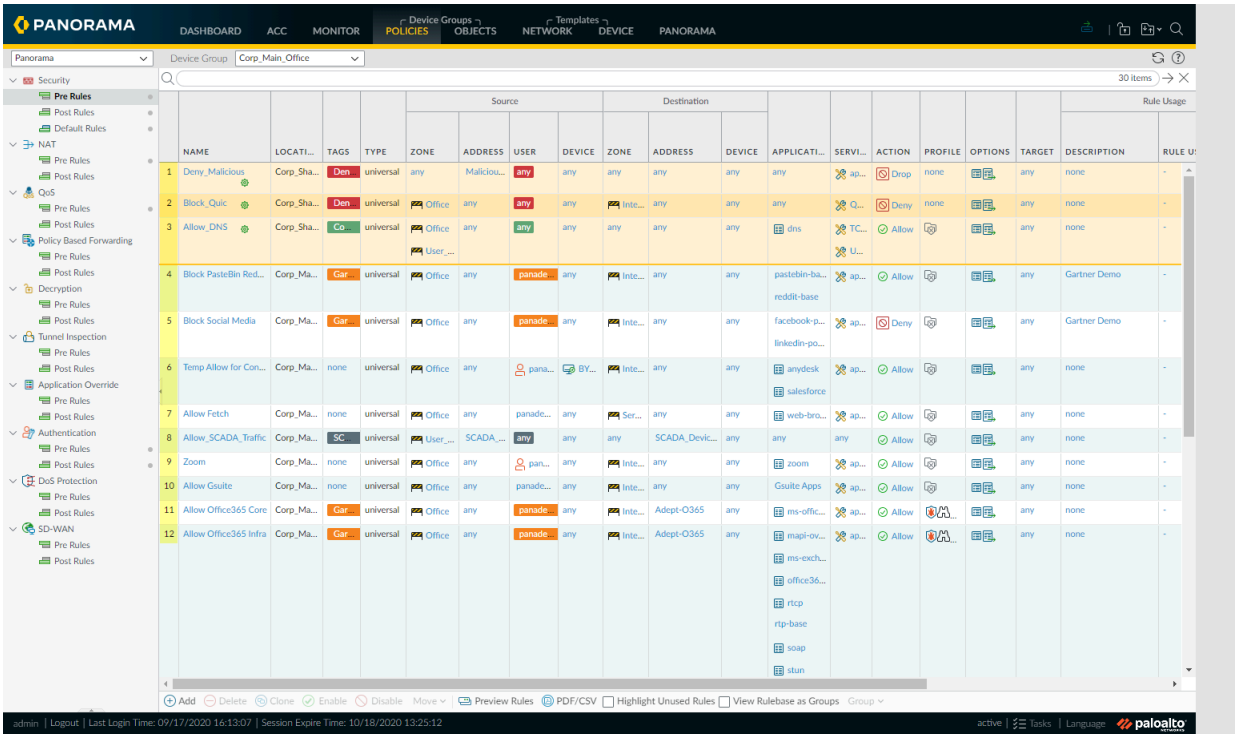
選取 **Policies**（原則），然後選取其下方的任何一個規則庫。例如，**Policies**（原則） > **Security**（安全性）。表格最左側的欄會顯示規則編號。



 ©2024 Palo Alto Networks, Inc.

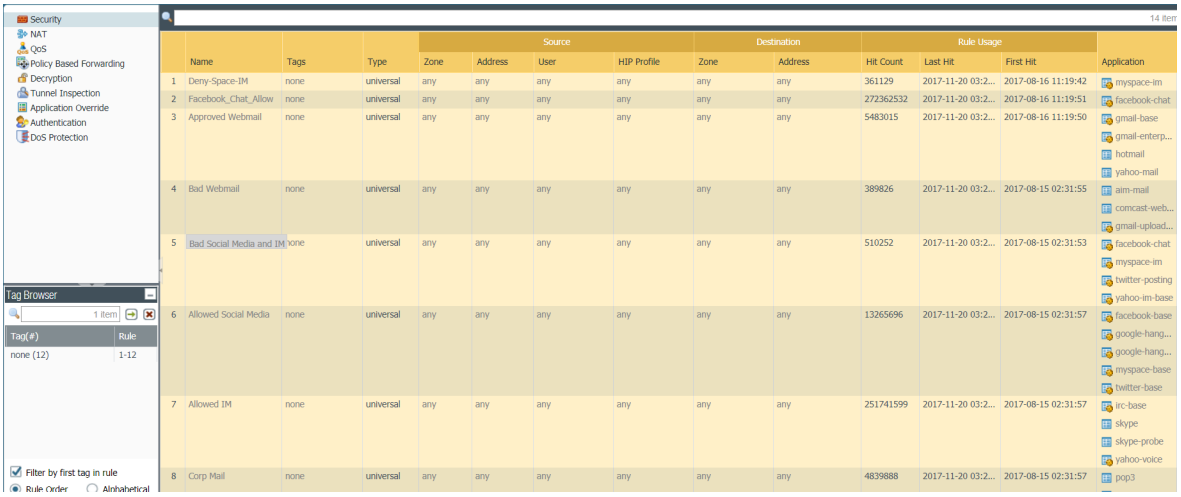
檢視 Panorama 上編號的規則清單。

選取 **Policies**（原則），然後選取其下方的任何一個規則庫。例如，**Policies**（原則） > **Security**（安全性） > **Pre-rules**（預先規則）。



在您從 Panorama 推送規則後，請檢視防火牆上完整的規則清單及編號。

從防火牆的網頁介面上，選取 **Policies**（原則），然後挑選其下的任何規則庫。例如，選取 **Policies**（原則） > **Security**（安全性），然後檢視防火牆將評估的已編號完整規則集。



 ©2024 Palo Alto Networks, Inc.

規則 UUID

規則的通用唯一識別碼 (UUID) 是防火牆或 Panorama 指派給規則的 32 字元字串（基於網路位址和建立時間戳記等資料）。UUID 採用 8-4-4-4-12 格式（其中 8、4 和 12 表示由連字號分隔的唯一字元數）。UUID 識別所有原則規則庫的規則。您還可使用 UUID 識別以下日誌類別中的適用規則：流量、威脅、URL 篩選、WildFire 提交、篩選資料、GTP、SCTP、通道檢查、組態與統一。

使用 UUID 搜尋規則讓您可以在數千個可能具有類似或相同名稱的規則中，找到所需的特定規則。UUID 還簡化了不支援名稱的協力廠商系統（例如票務或協調運作系統）中規則的自動化與整合。

在某些情況下，您可能需要為現有規則庫產生新的 UUID。例如，若要將組態匯出至另一個防火牆，則需要在匯入組態時為規則重新產生 *UUID*，以確保沒有重複的 UUID。如果重新產生了 UUID，則無法再使用這些規則先前的 UUID 對其進行追蹤，且這些規則的命中資料與應用程式使用資料將重設。

在執行下列操作時，防火牆或 Panorama 會指定 UUID：

- 建立新規則
- 複製現有規則
- 覆寫預設安全性規則
- 載入具名組態和重新產生 UUID
- 載入包含未在執行中組態內之新規則的具名組態
- 將防火牆或 Panorama 升級至 PAN-OS 9.0 版本

當您載入包含帶 UUID 之規則的組態時，如果規則名稱、規則庫和虛擬系統全部相符，則防火牆認為規則相同。如果規則名稱、規則庫和裝置群組全部相符，則 Panorama 認為規則相同。

請記住 UUID 的以下重要注意事項：

- 如果從 Panorama 管理防火牆原則，UUID 將在 Panorama 上產生，因此必須從 Panorama 推送。如果在將防火牆升級至 PAN-OS 9.0 之前沒有從 Panorama 推送組態，由於沒有 UUID，防火牆升級將失敗。
- 此外，如果升級的是 HA 配對，在升級至 PAN-OS 9.0 時，各對等體會單獨為各原則規則指定 UUID。因此，在同步組態之前，對等體將顯示為不同不（**Dashboard**（儀表板） > **Widgets**（**Widget**） > **System**（系統） > **High Availability**（高可用性） > **Sync to peer**（同步到對等體））。
- 如果您在升級至 PAN-OS 9.0 之後移除現有高可用性 (HA) 組態，則必須在其中一個對等體上重新產生 UUID（**Device**（裝置） > **Setup**（設定） > **Operations**（操作） > **Load named configuration snapshot**（載入具名組態快照） > **Regenerate UUIDs for the selected named configuration**（為選定的具名組態重新產生 **UUID**））並提交變更以防止 UUID 重複。
- 所有從 Panorama 產生的規則將共用同一 UUID；所有防火牆本機規則都具有不同的 UUID。如果您在從 Panorama 推送規則至防火牆後，在防火牆上建立本機規則，則建立的本機規則有自己的 UUID。

©2024 Palo Alto Networks, Inc.

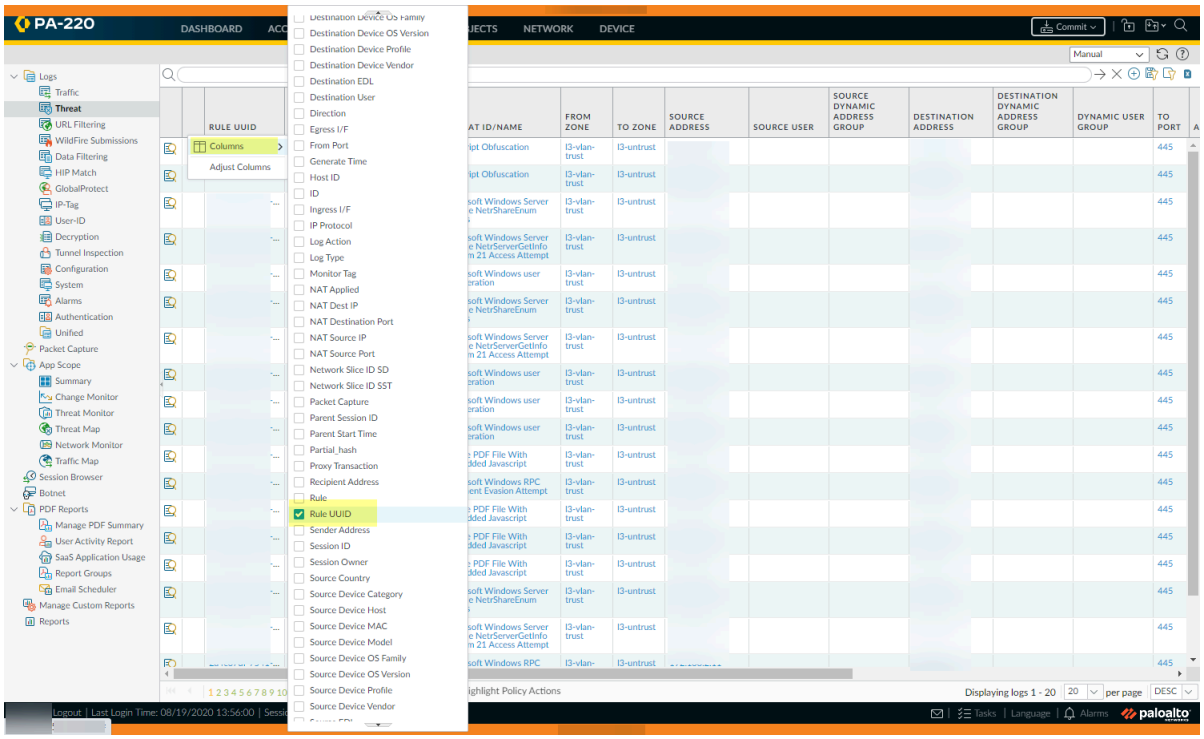
- 若要取代 RMA Panorama，請確保在載入具名 Panorama 組態快照時 **Retain Rule UUIDs**（保留規則 **UUID**）。如果沒有選取此選項，Panorama 將從組態快照中移除所有先前的規則 UUID，並在 Panorama 上為規則指定新的 UUID，這表示其不會保留與先前 UUID 相關的資訊，例如原則規則命中數。

©2024 Palo Alto Networks, Inc.

顯示日誌的規則 UUID 欄和原則規則的 UUID 欄。

若要檢視 UUID，您必須顯示這些欄（依預設不顯示）。

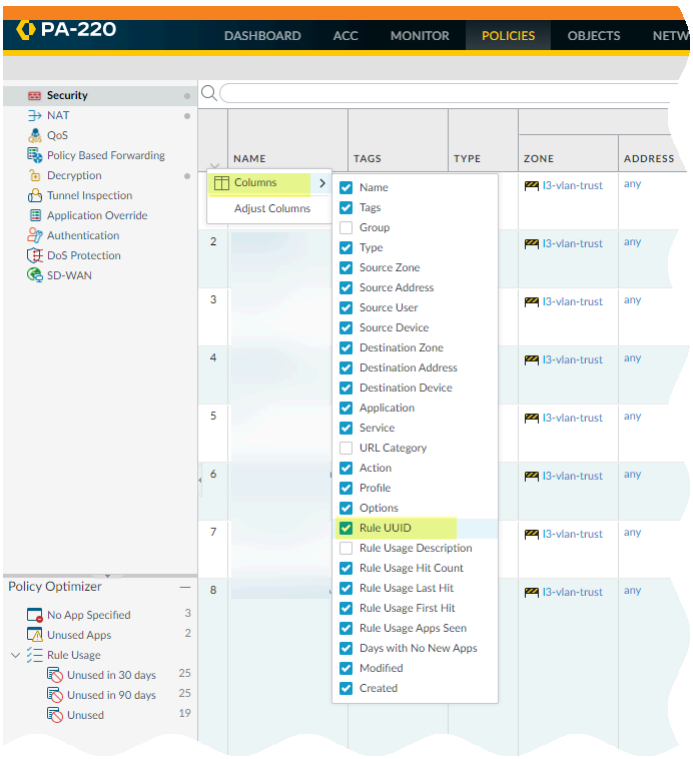
- 若要在日誌中顯示 UUID：
  1. 選取 **Monitor**（監控），然後展開欄標頭 ( )。
  2. 選取 **Columns**（欄）。
  3. 啟用 **Rule UUID**（規則 **UUID**）。



- 若要在原則規則庫上顯示 UUID：
  1. 選取 **Policies**（政策），然後展開欄標頭 ( )。
  2. 選取 **Columns**（欄）。
  3. 啟用 **Rule UUID**（規則 **UUID**）。

     UUID 適用於所有政策規則庫。

 ©2024 Palo Alto Networks, Inc.

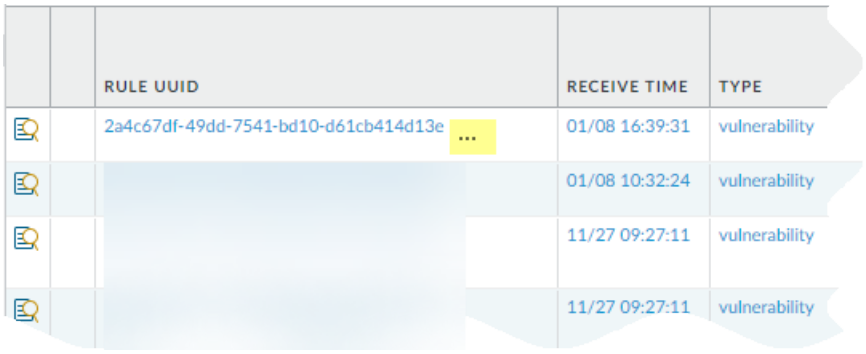


©2024 Palo Alto Networks, Inc.

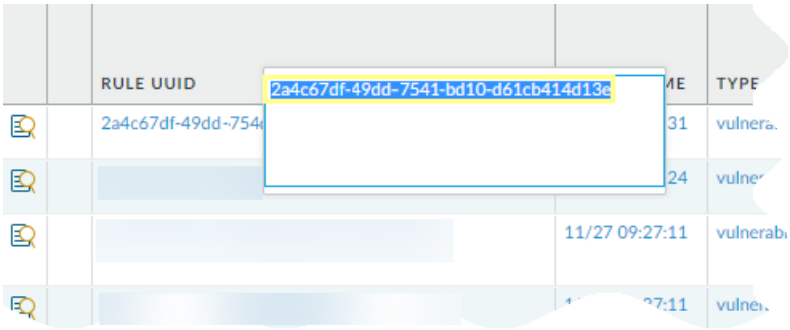
複製日誌或原則規則的 UUID。

複製 UUID 後，您可將其貼入搜尋列、ACC、自訂報告、篩選器及任何必要位置以尋找由該 UUID 標識的規則。

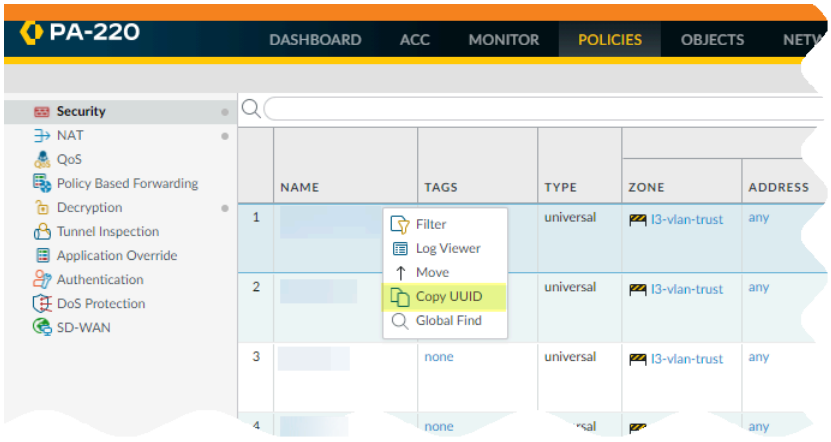
1. 選取將游標移至規則 UUID 欄中項目上時顯示的橢圓形。



2. 從快顯視窗中複製 UUID。



您還可移至 **Policies**（原則）頁籤，按一下規則名稱右側的箭頭，然後選取 **Copy UUID**（複製 **UUID**）。



選中 Configuration Logs（組態日誌）以檢視已刪除規則的 UUID。

若要視已刪除規則的 UUID，請選取 **Monitor**（監控） > **Logs**（日誌） > **Configuration**（組態）。

 ©2024 Palo Alto Networks, Inc.

執行原則規則說明、標籤和稽核註解

建立或修改規則時，可以要求提供規則說明、標籤和稽核註解，以確保原則規則庫正確組織和分組，並保留重要的規則歷程記錄以用於稽核目的。透過要求提供規則說明、標籤和稽核註解，可以簡化原則規則庫檢閱，方法是確保對規則進行適當分組，並在建立或修改規則時追蹤規則的變更歷程記錄。為確保一致性，可以為稽核註解能夠包含的內容設定特定要求。

依預設，說明、標籤和稽核註解的執行未啟用。您可以指定要成功新增或修改規則，是否需要提供說明、標籤、稽核註解，或這三者的任意組合。透過稽核註解封存檔，您可以檢視為所選規則輸入的稽核註解、檢閱組態日誌歷程記錄並比較各規則組態版本。

STEP 1 | 啟動 Web 介面。

STEP 2 | 選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理），然後編輯 Policy Rulebase Settings（原則規則庫設定）。

STEP 3 | 設定要執行的設定。在此範例中，所有原則都需要標籤和稽核註解。

對原則規則執行稽核註解，以擷取管理員建立或修改規則的原因。要求對原則規則執行稽核註解，有助於保留準確的規則歷程記錄以用於稽核目的。

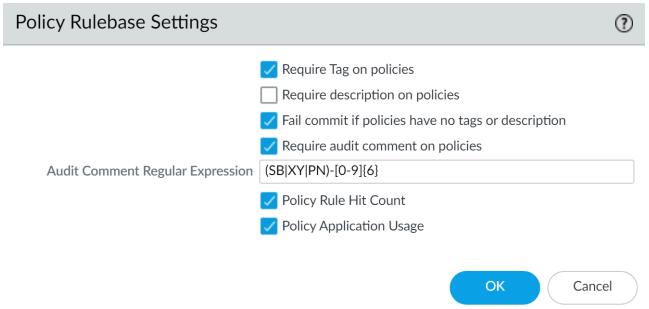
STEP 4 | 設定 Audit Comment Regular Expression（稽核註解規則運算式）以指定稽核註解格式。

當管理員建立或修改規則時，可要求其輸入一個註解，並透過指定字母和數字運算式，讓這些稽核註解遵循適合業務和稽核需求的特定格式。例如，您可使用以下設定來指定與票證號碼格式相符的規則運算式：

- **[0-9]{<Number of digits>}**—要求稽核註解包含數值介於 0 到 9 之間的最少數字數。例如，**[0-9]{6}** 要求數字運算式包含最少六位數值介於 0 到 9 之間的數字。
- <**Letter Expression**>—要求稽核註解包含字母運算式。例如，**Reason for Change-** 要求管理員設定以此字母運算式開頭的稽核註解。
- <**Letter Expression**>-**[0-9]{<Number of digits>}**—要求稽核註解包含預先確定的字元，後接數值介於 0 到 9 之間的最少數字數。例如，**SB-[0-9]{6}** 要求稽核註解格式以 **SB-** 開頭，後接包含最少六位數（數值介於 0 到 9 之間）的數字運算式。例如 **SB-012345**。
- **(**<**Letter Expression**>**)|(**<**Letter Expression**>**)|(**<**Letter Expression**>**)|-[0-9]{<Number of digits>}**—要求稽核註解包含一個首碼，該首碼使用任意一個預先確定的字母運算式，並包含數值介於 0 到 9 之間的最少數字數。例如，**(SB|XY|PN)-[0-9]{6}** 要求稽核註解格式以**SB-**、**XY-** 或 **PN-** 開頭，後接包含最少六位數（數值介於 0 到 9 之間）的數字運算式。例如，**SB-012345**、**XY-654321** 或 **PN-012543**。

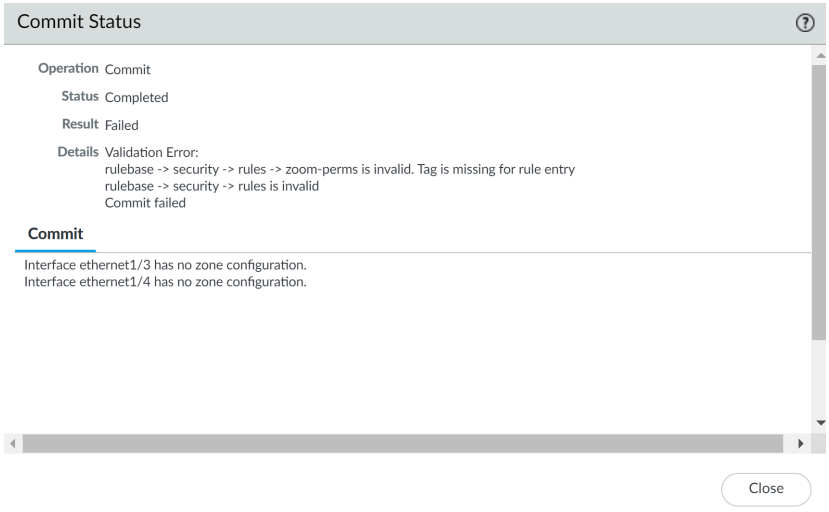
©2024 Palo Alto Networks, Inc.

STEP 5 | 按一下 **OK**（確定）以套用新的原則規則庫設定。



STEP 6 | **Commit**（提交）變更。

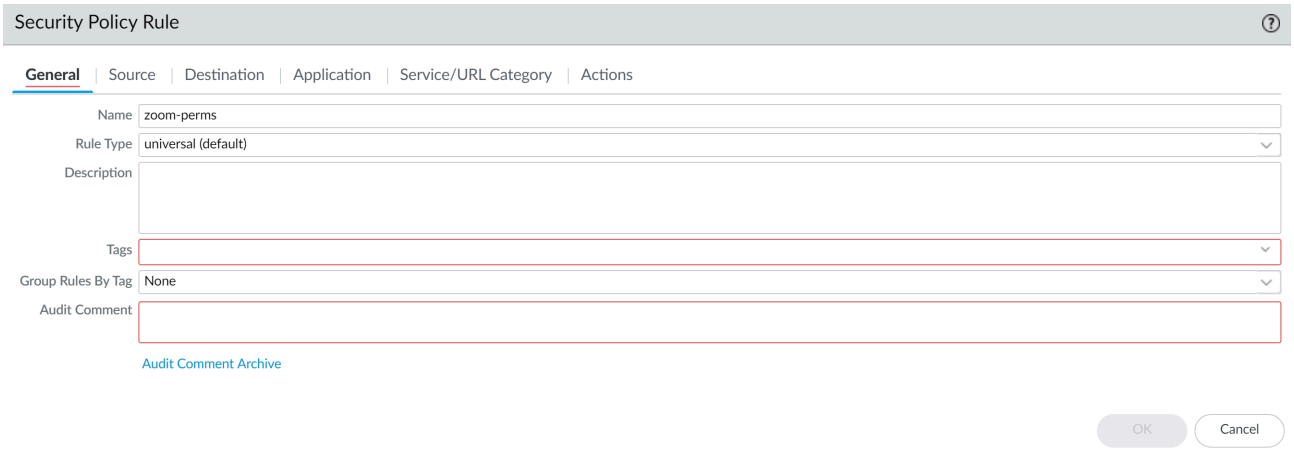
提交原則規則庫組態變更後，根據決定要執行的規則庫設定來修改現有原則規則。



 ©2024 Palo Alto Networks, Inc.

STEP 7 | 確認防火牆正在執行新的原則規則庫設定。

1. 選取 **Policies**（原則）並 **Add**（新增）新的規則。
2. 確認您必須新增標籤並輸入稽核註解，然後按一下 **OK**（確定）。



 ©2024 Palo Alto Networks, Inc.

將原則規則或物件移動或複製到其他虛擬系統

在具有一個以上虛擬系統 (VSYS) 的防火牆中，您可以將原則規則與物件移動或複製到其他 vsys 或共用位置。移動及複製可讓您在刪除、重新建立或重新命名規則與物件方面節省精力。如果您將從 vsys 移動或複製的原則規則或物件擁有該 vsys 中物件的參考，請同時移動或複製參考的物件。如果參考是共用物件的參考，移動或複製時，您無須包含這些參考。您可以使用全域尋找搜尋防火牆或 Panorama 管理伺服器，以尋找參考。

在複製多個原則規則時，您選取規則時的順序將決定規則複製到裝置群組的順序。例如，如果您有規則 *1-4*，您的選擇順序為 *2-1-4-3*，將複製這些規則的裝置群組會以相同的順序顯示規則。但是，複製成功後，您可以按照您任何合適的順序重新整理這些規則。

STEP 1 | 選取原則類型（例如，**Policy**（原則） > **Security**（安全性））或物件類型（例如，**Objects**（物件） > **Addresses**（位址））。

STEP 2 | 選取 **Virtual System**（虛擬系統），然後選取一或多個原則規則或物件。

STEP 3 | 執行下列其中一個步驟：

- 選取 **Move**（移動） > **Move to other vsys**（移至其他虛擬系統）（適用於原則規則）。
- 按一下 **Move**（移動） (適用於物件)。
- 按一下 **Clone**（複製）（適用於原則規則或物件）。

STEP 4 | 在 **Destination**（目的地）下拉式清單中，選取新的虛擬系統或 **Shared**（共用）。

STEP 5 | （僅限原則規則）選取 **Rule order**（規則順序）：

- **Move top**（移至頂部）（預設）—規則將位於所有其他規則之前。
- **Move bottom**（移至底部）—規則將位於所有其他規則之後。
- **Before rule**（規則之前）—在相鄰下拉式清單中，選取所選規則後的規則。
- **After rule**（規則之後）—在相鄰下拉式清單中，選取所選規則前的規則。

STEP 6 | 依預設，會選取 **Error out on first detected error in validation**（驗證中第一次偵測到錯誤時離開）核取方塊。當防火牆發現第一個錯誤時，它會停止執行對移動或複製動作的檢查，並且只會顯示此錯誤。例如，如果在 **Destination**（目的地）vsys 沒有您移動之原則規則所參考的物件時發生錯誤，防火牆將顯示錯誤，並會停止任何進一步驗證。當您一次移動或複製多個項目時，選取此核取方塊將可讓您一次找到一個錯誤，並進行疑難排解。若您清除核取方塊，防火牆會收集並顯示錯誤清單。如果驗證中有任何錯誤，將不會移動或複製物件，直到您解決所有錯誤為止。

STEP 7 | 按一下 **OK**（確定）以啟動錯誤驗證。如果防火牆顯示錯誤，請加以解決，然後重試移動或複製操作。如果防火牆找不到錯誤，則會成功移動或複製物件。操作完成後，按一下 **Commit**（交付）。

©2024 Palo Alto Networks, Inc.

使用位址物件表示 IP 位址

在防火牆上建立位址物件以分組 IP 位址或指定 FQDN，然後在防火牆原則規則、篩選器或其他功能中參照此位址物件，以避免在規則、篩選器或其他功能中個別指定多個 IP 位址。

此外，您還可以在多個原則規則、篩選器或其他功能中參照同一位址物件，無需在每次使用時指定相同的個別位址。例如，您可以建立指定 IPv4 位址範圍的位址物件，然後在安全性原則規則、NAT 原則規則和自訂報告日誌篩選器中參照該位址物件。

- 位址物件
- 建立位址物件

位址物件

位址物件是一組 IP 位址，可以在同一位址進行管理，並在多個防火牆原則規則、篩選器及其他功能中使用。位址物件有四種類型：**IP Netmask**（**IP** 網路遮罩）、**IP Range**（**IP** 範圍）、**IP Wildcard Mask**（**IP** 萬用字元遮罩）及 **FQDN**。

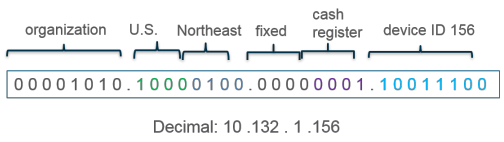
類型為 **IP Netmask**（**IP** 網路遮罩）、**IP Range**（**IP** 範圍）或 **FQDN** 的位址物件可以指定 IPv4 或 IPv6 位址。類型為 **IP Wildcard Mask**（**IP** 萬用字元遮罩）的位址物件僅可指定 IPv4 位址。

類型為 **IP Netmask**（**IP** 網路遮罩）的位址物件要求輸入使用斜線標記的 IP 位址或網路以表示 IPv4 網路或 IPv6 首碼長度。例如，192.168.18.0/24 或 2001:db8:123:1::/64。

類型為 **IP Range**（**IP** 範圍）的位址物件要求輸入由連字號分隔的 IPv4 或 IPv6 位址範圍。

類型為 **FQDN**的位址物件（例如，paloaltonetworks.com）更加易於使用，因為 DNS 提供了對 IP 位址的 FQDN 解析，因此 FQDN 每次解析為新的 IP 位址時， 您無需知道 IP 位址並手動更新。

當您為內部裝置定義私人 IPv4 位址及定址結構為位址中的某些位元指派含義時，類型為 **IP Wildcard Mask**（**IP** 萬用字元遮罩）的位址物件非常有用。例如，根據這些位元指派，美國東北部收銀機 156 的 IP 位址為 10.132.1.156：



類型為 **IP Wildcard Mask**（**IP** 萬用字元遮罩）的位址物件可以指定哪些來源或目的地位址須符合安全性原則規則。例如，10.132.1.1/0.0.2.255。遮罩中的零 (0) 位元表示被比較的位元必須符合零涵蓋之 IP 位址中的位元。遮罩中的一 (1) 位元（萬用字元位元）表示被比較的位元不需要符合 IP 位址中的位元。以下 IP 位址和萬用字元遮罩片段說明了其如何產生四個相符項：

©2024 Palo Alto Networks, Inc.

建立位址物件後：

- 您可在安全性、驗證、NAT、NAT64、解密、DoS 保護、基於原則的轉送 (PBF)、QoS、應用程式覆寫或通道檢查的規則規則中，或 NAT 位址集區、VPN 通道、路徑監控、外部動態清單、偵察保護、ACC 全域篩選器、日誌篩選器或自訂報告日誌篩選器中，參照類型為 **IP Netmask**（**IP** 網路遮罩）, **IP Range**（**IP** 範圍）或 **FQDN**的位址物件。
- 您只能在安全性原則規則中引用類型為 **IP Wildcard Mask**（**IP** 萬用字元遮罩）的位址物件。

建立位址物件

建立 位址物件 以代表一個或多個 IP 位址，然後在一個或多個政策規則、篩選器或其他防火牆功能中引用此位址物件。若要變更位址組，只需變更位址物件一次，無需變更多個原則規則或篩選器，從而減少您的操作負荷。

STEP 1 | 建立位址物件。

1. 選取 **Objects**（物件） > **Addresses**（位址），然後依 **Name**（名稱）**Add**（新增） 位址物件。名稱區分大小寫且必須是唯一的，最多可使用 63 個字元（字母、數字、空格、連字號和底線）。
2. 選取位址物件的 **Type**（類型）：
   - **IP Netmask**（**IP** 網路遮罩）—指定單一 IPv4 或 IPv6 位址、帶斜線標記的 IPv4 網路或 IPv6 位址與首碼。例如，192.168.80.0/24 或 2001:db8:123:1::/64。（選用）按一下 **Resolve**（解析）以查看關聯的 FQDN（基於防火牆或 Panorama 的 DNS 組態）。若要將位址物件類型從 **IP Netmask**（**IP** 網路遮罩）變更為 **FQDN**，請選取 FQDN 並按一下 **Use this FQDN**（使用此 **FQDN**）。**Type**（類型）變更為 **FQDN** 且您選取的 FQDN 顯示於文字欄位中。
   - **IP Range**（**IP** 範圍）—指定由連字號分隔的 IPv4 位址或 IPv6 位址範圍。例如，192.168.40.1-192.168.40.255 或 2001:db8:123:1::1-2001:db8:123:1::22。
   - **IP Wildcard Mask**（**IP** 萬用字元遮罩）—指定 IP 萬用字元位址（IPv4 位址後接斜線與遮罩，遮罩必須以 0 開頭）。例如，10.5.1.1/0.127.248.2。遮罩中的零 (0) 表示被比較的位元必須符合零涵蓋之 IP 位址中的位元。遮罩中的一 (1)（萬用字元位元）表示被比較的位元不需要符合一所涵蓋之 IP 位址中的位元。
   - **FQDN**—指定網域名稱。FQDN 最初會在提交時間解析。只要 TTL 大於或等於您設定的 **Minimum FQDN Refresh Time**（**FQDN** 重新整理時間下限）（或預設值 30 秒），防火牆隨後會根據 DNS 中 FQDN 的存留時間 (TTL) 重新整理 FQDN。若設定了代理程式，則 FQDN 會由系統 DNS 伺服器或 DNS 代理程式物件解析。按一下 **Resolve**（解析）以查看關聯的 IP 位址（基於防火牆或 Panorama 的 DNS 組態）。

 ©2024 Palo Alto Networks, Inc.

若要將位址物件類型從 FQDN 變更為 IP 網路遮罩，請選取 IP 位址並按一下 **Use this address**（使用此位址）。**Type**（類型）變更為 **IP Netmask**（**IP** 網路遮罩） 且您選取的 IP 位址顯示於文字欄位中。

3. （選用）輸入一個或多個使用標籤分組及在視覺上區分物件以套用至位址物件。
4. 按一下 **OK**（確定）。

STEP 2 | **Commit**（提交）您的變更。

STEP 3 | 檢視依位址物件、位址群組或萬用字元位址篩選的日誌。

1. 例如，選取 **Monitor**（監控） > **Logs**（日誌） > **Traffic**（流量）以檢視流量日誌。
2. 選取 ＋ 以新增日誌篩選器。
3. 選取 **Address**（位址）屬性，及 **in** 運算子，然後輸入要檢視其日誌的位址物件名稱。或者，輸入位址群組名稱或萬用字元位址，例如 10.155.3.4/0.0.240.255。
4. 按一下 **Apply**（套用）。

STEP 4 | 檢視以位址物件為基礎的自訂報告。

1. 選取 **Monitor**（監控） > **Manage Custom Reports**（管理自訂報告），然後選取使用流量日誌等資料庫的報告。
2. 選取 **Filter Builder**（篩選器建立器）。
3. 選取一個屬性，例如 **Address**（位址）、**Destination Address**（目的地位址）或 **Source Address**（來源位址），選取運算子，然後輸入要檢視其報告的位址物件名稱。

STEP 5 | 使用 ACC 中的篩選器根據使用位址物件的來源 IP 位址或目的地 IP 位址檢視網路活動。

1. 選取 **ACC** > **Network Activity**（網路活動）。
2. 檢視來源 **IP** 活動—針對全域篩選器，按一下 ＋ 以新增篩選器並選取下列選項之一：**Address**（位址）或 **Source**（來源） > **Source Address**（來源位址）或**Destination**（目的地） > **Destination Address**（目的地位址），然後選取位址物件。
3. 檢視 **Destination IP Activity**—**For Global Filters**（目的地 **IP** 活動—針對全域篩選器），按一下 ＋ 以新增篩選器並選取下列選項之一：**Address**（位址）或 **Source**（來源） > **Source Address**（來源位址）或**Destination**（目的地） > **Destination Address**（目的地位址），然後選取位址物件。

©2024 Palo Alto Networks, Inc.

使用標籤分組及在視覺上區分物件

您可以為物件加上標籤來編組相關項目，並為標籤設定顏色，藉此在視覺上區分它們以便於掃描。您可為下列物件建立標籤：位址物件、位址群組、使用者群組、區域、服務群組和原則規則。

防火牆和 Panorama 支援靜態標籤和動態標籤。動態標籤是從各種來源註冊的標籤，不會與靜態標籤一起顯示，因為動態標籤不是防火牆或 Panorama 設定的一部分。如需動態註冊標籤的相關資訊，請參閱動態註冊 IP 位址與標籤。本節中討論的標籤會靜態地新增至組態中，且為該組態的一部分。

您可將一或多個標籤套用在物件與原則規則上；每個物件最多可套用 64 個標籤。Panorama 最多可支援 10,000 個標籤，您可在 Panorama（共用群組與裝置群組）及受管理防火牆（包括含多個虛擬系統的防火牆）之間分配這些標籤。

- 建立及套用標籤
- 修改標籤
- 按標籤群組檢視規則

建立及套用標籤

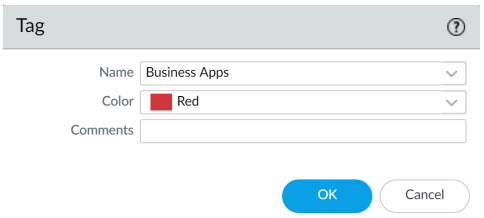
使用標籤來識別規則或組態物件的目的，並幫助您更好地組織規則庫。若要確保政策規則已正確標記，請參閱如何 執行原則規則說明、標籤和稽核註解。此外，您還可以透過建立標籤並將其設為群組標籤來 按標籤群組檢視規則。

©2024 Palo Alto Networks, Inc.

STEP 1 | 建立標籤。

若要將區域加上標籤，您必須建立與區域同名的標籤。將區域附加至原則規則後，標籤顏色會自動顯示成區域名稱的背景顏色。

1. 選取 **Objects**（物件） > **Tags**（ 頁籤）。
2. 在 Panorama 或多虛擬系統的防火牆上，選取 **Device Group**（裝置群組）或 **Virtual System**（虛擬系統）以使此標籤可用。
3. **Add**（新增）標籤並輸入 **Name**（名稱）以識別標籤或區域 **Name**（名稱），以便為區域建立標籤。最大長度為 127 個字元。
4. （選用）選取**Shared**（共用）在共用的位置中建立物件，藉此在 Panorama 中作為共用物件存取，或在多虛擬系統防火牆中的所有虛擬系統之間使用。
5. 選用從 17 個預先定義顏色中分配 **Color**（顏色） 。依預設，**Color**（顏色）為 **None**（無）。



6. 按一下 **OK**（確定）和 **Commit**（提交），以儲存變更。

STEP 2 | 將頁籤套用至原則。

1. 選取 **Policies**（原則），然後選取其下方的任何一個規則庫。
2. **Add**（新增）原則規則，然後使用您在步驟 1 中建立的已加上標籤的物件。
3. 確認標籤正在使用中。

	NAME	TAGS	TYPE	Source				Destination	
				ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
1	General Business Apps	Business Apps	universal	any	any	known-user	any	any	any

STEP 3 | 將標籤套用至位址物件、位址群組、服務或服務群組。

1. 建立物件。

   例如，若要建立服務群組，請選取 **Objects**（物件） > **Service Groups**（服務群組） > **Add**（新增）。

2. 選取標籤（**Tag**（標籤））或在欄位中輸入名稱以建立新的標籤。

   若要編輯標籤或為標籤新增顏色，請參閱修改標籤。

修改標籤

 ©2024 Palo Alto Networks, Inc.

選取 **Objects**（物件） > **Tags**（標籤） 執行下列任何一項標籤作業：

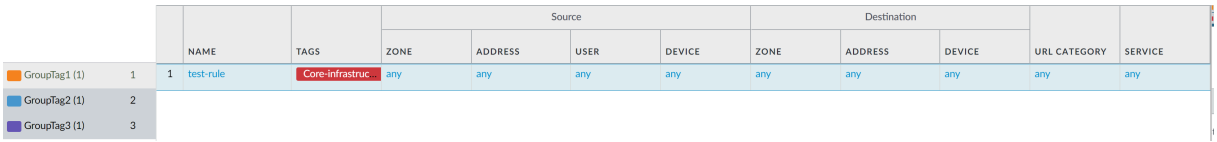
- 按一下 **Name**（名稱），以編輯標籤的屬性。
- 選取表格中的標籤，然後 **Delete**（刪除）防火牆中的標籤。
- **Clone** （複製）標籤，以復制具有相同屬性的標籤。標籤名稱後會加上數字尾碼（例如，FTP-1）。

如需建立標籤的詳細資料，請參閱建立及套用標籤。如需使用標籤的相關資訊，請參閱按標籤群組檢視規則。

按標籤群組檢視規則

以標籤群組形式檢視原則規則庫以根據您建立的標記結構以視覺方式對規則分組。在此檢視中，您可執行各種操作程序，例如在所選標籤群組中更輕鬆地新增、刪除和移動規則。按標籤群組檢視規則庫可以維持規則的評估順序，且單一標籤可以在整個資料庫中多次出現，從而以視覺方式保留規則階層。

您必須先建立標籤，然後才能將其指派給規則上的群組標籤。在升級至 PAN-OS 9.0 時已標記的原則規則會將第一個標籤自動指派為群組標籤。在您升級至 PAN-OS 9.0 之前，請檢閱規則庫中已標記的規則，以確保規則被正確分組。如果在升級至 PAN-OS 9.0 後規則未被正確分組，則必須手動編輯各標籤規則並設定正確的群組標籤。



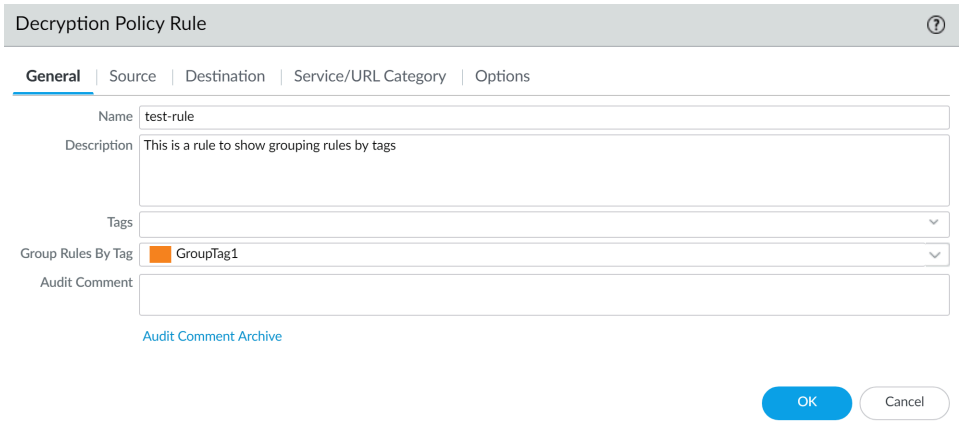
STEP 1 | 啟動 Web 介面.

STEP 2 | 建立及套用標籤要用於分組規則。

©2024 Palo Alto Networks, Inc.

STEP 3 | 為標籤群組指派原則規則。

1. 建立原則規則。如需建立政策規則的更多資訊，請參閱原則。
2. 在 **Group Rules by Tag**（依標籤對規則分組）欄位中，從下拉式清單中選取標籤，然後按一下 **OK**（確定）。

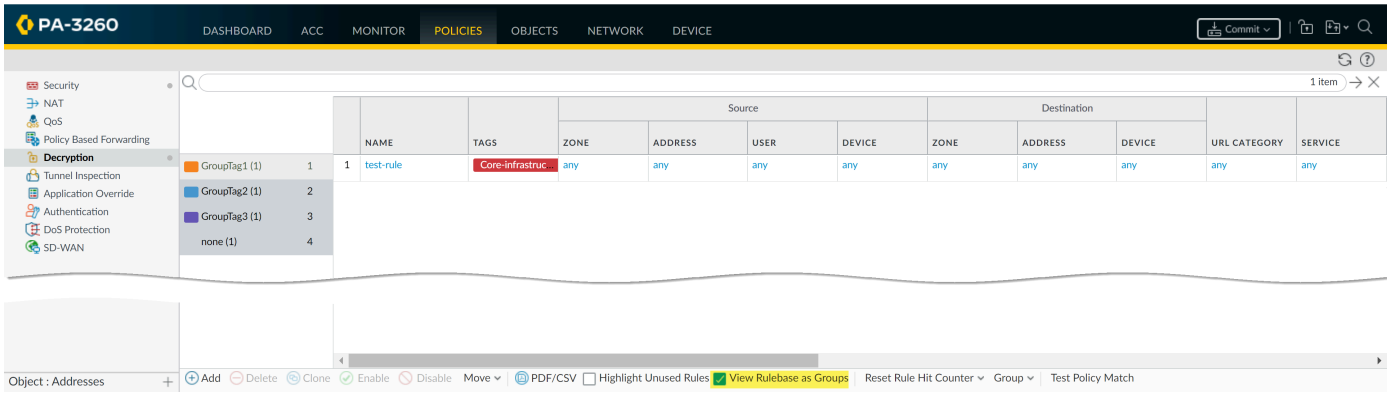


3. **Commit**（提交）您的變更。

STEP 4 | 以群組形式檢視原則規則庫。

1. （僅限 Panorama）從 **Device Group**（裝置群組）中，選取要檢視的裝置群組規則庫，或檢視所有共用規則。
2. 按一下 **Policies**（原則）並選取您在步驟 2 中建立規則的規則庫。
3. 選取 **View Rulebase as Groups**（以群組形式檢視規則庫）選項（底部）。

未指派為標籤群組的規則將顯示為 ***None***（無）。

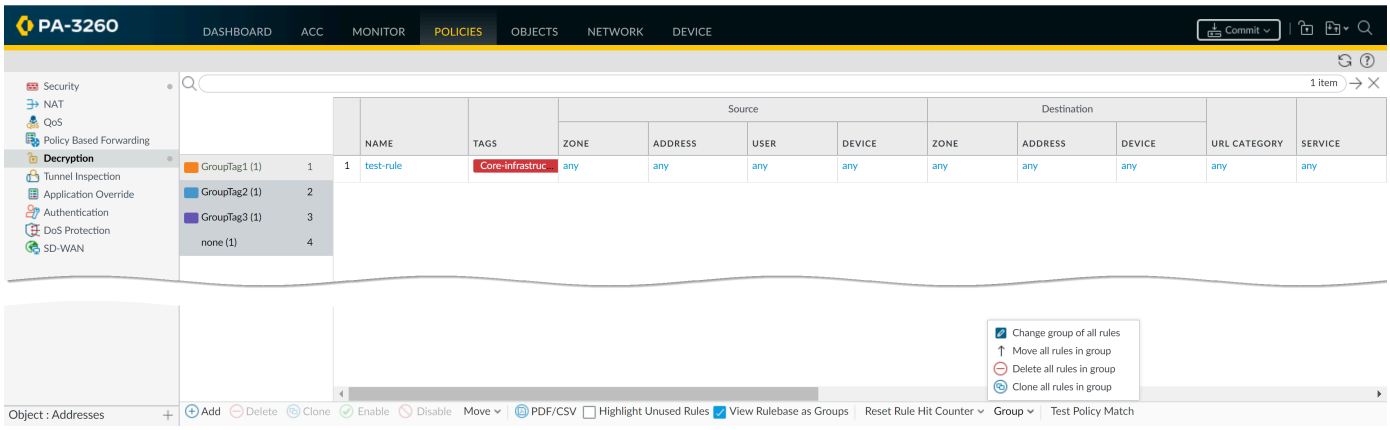


 ©2024 Palo Alto Networks, Inc.

STEP 5 | 視需執行群組操作。

1. 按一下 **Group**（群組）以對所選標籤群組中的規則執行群組操作。

   - （僅限 Panorama）將群組中的規則移至其他規則庫或裝置群組—將所選標籤群組中的所有原則規則移至前置規則庫或後置規則庫，或將其移動至其他裝置群組。
   - **Change group of all rules**（變更所有規則的群組）—將選定頁籤群組中的所有規則移動到其他頁籤群組。
   - **Move all rules in group**（移動群組中的所有規則）—移動選定頁籤群組中的所有規則以變更規則的優先順序。
   - **Delete all rules in group**（刪除群組中的所有規則）—刪除選定頁籤群組中的所有規則。
   - **Clone all rules in group**（複製群組中的所有規則）—複製選定頁籤群組中的所有規則。



2. **Commit**（提交）您的變更。

 ©2024 Palo Alto Networks, Inc.

在原則中使用外部動態清單

外部動態清單（以前稱為動態封鎖清單）是您或其他來源在外部 Web 伺服器上裝載的文字檔，使防火牆可以匯入物件（IP 位址、URL、網域），以針對清單中的項目強制執行原則。在更新清單時，防火牆會依設定的間隔動態地匯入清單，並強制執行原則，而不需執行組態變更或在防火牆上提交。

- 外部動態清單
- 外部動態清單的格式設定方針
- 內建外部動態清單
- 設定防火牆存取外部動態清單
- 設定防火牆從 EDL 主機服務存取外部動態清單
- 從網頁伺服器擷取外部動態清單
- 檢視外部動態清單項目
- 從外部動態清單中排除項目
- 對外部動態清單強制執行原則
- 尋找驗證失敗的外部動態清單
- 為外部動態清單停用驗證

外部動態清單

外部動態清單是一個在外部網頁伺服器上代管的文字檔，使防火牆可以匯入清單中包括的物件（IP 位址、URL、網域、國際行動裝置識別 (IMEI) 、國際行動用戶識別 (IMSI) ）並強制執行原則。若要針對外部動態清單中包括的項目強制執行安全性原則，您必須參考受支援的原則規則或設定檔中的清單。參考多個清單時，您可設定評估順序的優先順序，以確保在達到容量限制之前提交最重要的 EDL。在修改清單時，防火牆會依設定的間隔動態地匯入清單，並強制執行原則，而不需執行組態變更或在防火牆上提交。如果無法連線到網頁伺服器，防火牆會使用上一次成功擷取的清單來強制執行原則，一直到與網頁伺服器恢復連線為止。如果對 EDL 的驗證失敗，安全性原則會停止執行 EDL。為了擷取外部動態清單，防火牆將使用設定了 **Palo Alto Networks Services** 服務路由的介面。

如果出現以下情況，防火牆會保留最後一次成功擷取到的 EDL，並繼續使用最新的 EDL 資訊進行操作，直到還原與託管 EDL 的伺服器的連線：

- 您升級或降級防火牆
- 您重新啟動防火牆、管理平面或資料平面
- 託管 EDL 的伺服器變得無法連線

當防火牆無法連線或以其他方式從伺服器擷取最新的 EDL 資訊時，將顯示以下警告。

無法擷取外部清單。使用舊副本進行重新整理。

©2024 Palo Alto Networks, Inc.

防火牆支援以下類型的外部動態清單：

- 預先定義的 **IP** 位址—預先定義的 IP 位址清單是指參考了擁有固定內用或「預先定義」內容之內建、動態 IP 清單的一種 IP 位址清單。如果您有有效的威脅防禦授權，這些 Built-In External Dynamic Lists（內建外部動態清單）（用於防彈主機提供的已知惡意、高風險 IP 位址）將自動新增至防火牆。預先定義的 IP 位址清單還可參考將這些內建清單用作來源的 EDL。由於您無法修改預先定義之清單的內容，因此如果要新增或排除清單項目，可以使用預先定義的清單作為不同 EDL 的來源。
- 預先定義的 **URL** 清單—這種類型的外部動態清單包含應用程式用於背景服務（例如更新或憑證撤銷清單 (CRL) 檢查）的預先填入 URL，防火牆可以將這些 URL 安全地從驗證原則中排除。Palo Alto Networks 會透過內容更新來修訂和維持這種類型的外部動態清單，也稱為驗證入口網站排除清單。
- **IP** 位址—當某一來源或目的地 IP 位址在防火牆上被定義為靜態物件時，防火牆通常會強制為其執行原則（請參閱 Enforce Policy on an External Dynamic List（強制執行外部動態清單的原則））。如果您需要靈活地為非常設的臨時來源/目的地 IP 位址清單強制執行原則，則可以將 IP 位址類型的外部動態清單用作原則規則中的來源或目的地位址物件，並將防火牆設定為拒絕或允許清單中包含的 IP 位址（IPv4 和 IPv6 位址、IP 範圍和 IP 子網路）。您還可以在 SD-WAN 原則規則的來源或目的地中使用 IP 位址 EDL。防火牆會將 IP 位址類型的外部動態清單視為一個位址物件；清單中包含的所有 IP 位址將被作為一個位址物件進行處理。
- 網域—這種類型的外部動態清單允許您將自訂網域名稱匯入防火牆，以強制執行使用反間諜軟體設定檔的原則或 SD-WAN 原則規則。如果您訂閱第三方威脅情報摘要並想要在瞭解惡意網域後立即保護網路免遭新型威脅或惡意軟體攻擊，反間諜軟體設定檔中的 EDL 會非常有用。對於外部動態清單中包括的每個網域，防火牆會建立一個自訂 DNS 式間諜軟體特徵碼，以便您可以啟用 DNS Sinkholing。DNS 式間諜軟體特徵碼屬於中等嚴重性的間諜軟體類型，每個特徵碼名稱為 **Custom Malicious DNS Query *<domain name>***。您還可指定防火牆以包含指定網域的子網域。例如，如果您的網域清單包含 paloaltonetworks.com，網域名稱所有較低等級的配件（例如，*.paloaltonetworks.com）也將作為清單的一部分包含在內。當此設定啟用時，指定清單中的每個網域都需要一個附加項目，從而有效地將清單所佔用的項目數量加倍。如需有關設定網域清單的詳細資訊，請參閱為自訂網域清單設定 DNS Sinkholing。
- **URL**—這種類型的外部動態清單可讓您靈活地保護網路免遭新型威脅或惡意軟體攻擊。防火牆會像自訂 URL 類別那樣處理 URL 類型的外部動態清單，您可依以下兩種方式使用此清單：
  - 作為安全性原則規則、解密原則規則及 QoS 原則規則中的比對準則，用於為自訂類別中的 URL 允許、拒絕、解密、不解密或配置頻寬。
  - 在 URL 篩選設定檔中，您可以定義更細化的動作，例如繼續、警示或覆寫，然後將設定檔附加至安全性原則規則（請參閱在 URL 篩選設定檔中使用外部動態清單）。
- 裝置識別—您可以在安全性原則規則中引用由國際行動裝置識別 (IMEI) 定義的 IoT 裝置的外部動態清單，以控制連線到 5G 或 4G 網路的裝置的流量。有關在支援的防火牆型號上設定裝置 ID 安全性的資訊，請參閱《行動網路基礎結構入門》。
- 用戶識別—您可以在安全性原則規則中引用國際行動用戶識別 (IMSI) 的外部動態清單，以控制連線到 5G 或 4G 網路的用戶的流量。有關在支援的防火牆型號上設定用戶 ID 安全性的資訊，請參閱《行動網路基礎結構入門》。

 ©2024 Palo Alto Networks, Inc.

對於每種防火牆型號，您最多可新增 30 個具有唯一來源（可用於執行政策）的自訂 EDL。外部動態清單數量限制不適用於 Panorama。當使用 Panorama 來管理針對多個虛擬系統啟用的防火牆時，若超出防火牆的限制，Panorama 上會顯示提交錯誤。來源是包括 IP 位址或主機名稱、路徑及外部動態清單檔案名稱的 URL。防火牆比對 URL（完整字串）來確定來源是否唯一。

雖然防火牆不針對特定類型的清單數量設限，但會強制執行下列限制：

- IP 位址 — PA-3200 系列、PA-5200 系列及 PA-7000 系列防火牆最多可支援 150,000 個 IP 位址；所有其他型號最多可支援 50,000 個 IP 位址。不會對每份清單的 IP 位址數量強制執行限制。當防火牆上達到支援 IP 位址的上限時，防火牆會產生一則 Syslog 訊息。預先定義的 IP 位址清單中的 IP 位址並不會計入此限值。
- URL 及網域—支援的最大 URL 和網域數目依型號而有所不同。不會對每份清單的 URL 或網域項目數量強制執行限制。各型號的具體數目參見下表：

Model	URL 清單項目限制	網域清單項目限制
PA-5200 Series、PA-5400 Series、PA-7000 Series（升級為 PA-7000 20GXM NPC、PA-7000 20GQXM NPC 或 PA-7000 100G NPC）。 具有混合 *NPC* 的 *PA-7000* 設備僅支援標準容量。	250,000	4,000,000
VM-500, VM-700	100,000	2,000,000
PA-400 Series（PA-410 除外）、PA-850、PA-820、PA-3200 Series、PA-3400 Series	100,000	1,000,000
PA-7000 系列（升級至 PA-7000 20GQ NPC 或 PA-7000 20G NPC 的設備）、VM-300	100,000	500,000
PA-220、PA-410、VM-50、VM-50 (Lite)、VM-100、VM-1000-HV	50,000	50,000

只有在清單項目屬於原則中參考之外部動態清單時，它們才會計入防火牆的限制。

©2024 Palo Alto Networks, Inc.

- 當剖析清單時，防火牆會跳過與清單類型不相符的項目，並忽略超出型號支援之最大數目的項目。為了確保項目數量不會超出限制，需檢查原則中目前使用的項目數。選取 ***Objects***（物件） > ***External Dynamic Lists***（外部動態清單），然後按一下 ***List Capacities***（清單容量）。
- 外部動態清單必須包含項目。如果您要停止使用清單，請從原則規則或設定檔中移除引用，而非將清單留空。如果清單不包含任何項目，防火牆重新整理清單會失敗，並會繼續使用它上次擷取的資訊。
- *Palo Alto Networks* 建議的最佳做法是，在使用多個虛擬系統時，使用共享 *EDL*。為每個虛擬系統使用具有重複項目的個別 *EDL*，將使用更多記憶體，從而導致過度使用防火牆資源。
- 執行多個虛擬系統之防火牆上的 *EDL* 項目計數須考慮其他因素（如 *DAG*、虛擬系統數目、規則庫），以產生更準確的容量消耗清單。這可能會導致從 *PAN-OS 8.x* 版本升級後出現容量使用差異。
- 根據防火牆上啟用的功能，由於記憶體配置更新，在達到 *EDL* 容量限制之前，可能會超過記憶體使用量限制。*Palo Alto Networks* 建議的最佳做法是，經常檢閱 *EDL* 容量，並在必要時將 *EDL* 移除或合併到共用清單中，以減少記憶體使用量。

外部動態清單的格式設定方針

一個類型（IP 位址、網域或 URL）的外部動態清單必須僅包括該類項目。預先定義的 IP 位址清單中的項目需符合 IP 位址清單的格式指引。

- IP 位址清單
- 網域清單
- URL 清單

IP 位址清單

外部動態清單包含個別的 IP 位址、子網路位址 (位址/遮罩) 或 IP 位址範圍。此外，區塊清單可包含註解與特殊字元，例如 **`*`**、**`:`**、**`;`**、**`#`** 或 **`/`**。清單中每一行的語法為 **`(IP`** 位址、**`IP/`**遮罩或 **`IP`** 開始範圍**`-IP`** 結束範圍**`)`** **`(`**空格**`)`** **`(`**註解**`)`**。

在新的一行輸入每個 IP 位址/範圍/子網路；此清單中不支援 URL 或網域。子網路或 IP 位址範圍（例如 92.168.20.0/24 或 192.168.20.40-192.168.20.50）可算為一個 IP 位址項目，而不算是多個 IP 位址。如果您新增註解，註解必須與 IP 位址/範圍/子網路在同一行。IP 位址結尾的空格是將註解與 IP 位址分隔的分隔符號。

IP 位址清單範例：

 ©2024 Palo Alto Networks, Inc.

```
192.168.20.10/32 2001:db8:123:1::1 #test IPv6 address
 192.168.20.0/24 ; test internal subnet 2001:db8:123:1::/64 test
 internal IPv6 range 192.168.20.40-192.168.20.50
```

對於封鎖的 *IP* 位址，只有在通訊協定為 *HTTP* 時，您才能顯示通知頁面。

網域清單

您可使用網域清單中的預留位置字元來設定單一項目，以與多個網站子網域、網頁（包括整個頂層網域）以及特定網頁進行比對。

建立網域清單項目時請遵循這些方針：

- 在新的一行輸入每個網域名稱；此清單中不支援 URL 或 IP 位址。
- 請勿在網域名稱前加通訊協定首碼 http:// 或 https://。
- 您可使用星號 (*) 表示萬用字元值。
- 您可使用插入符號 (*) 表示完全符合值。
- 以下字元視為語彙基元分隔符號：: . / ? & = ; +

  每一個由此類字元中的一個或兩個字元分隔的字串為一個語彙基元。使用萬用字元作為語彙基元預留位置，表明特定語彙基元可包含任何值。
- 萬用字元必須為語彙基元中的唯一字元；但是項目可包含多個萬用字元。
- 每個網域項目長度可最多為 255 個字元。

何時使用該星號 **(*)** 萬用字元：

使用星號 (*) 萬用字元以表明一個或多個可變子網域。例如，若要指定 Palo Alto Network 網站的執行方式（不受所使用的網域延伸的影響，視乎位置而定，可能為一個或兩個子網域），您會新增項目：**`*.paloaltonetworks.com`**。此項目會同時與 docs.paloaltonetworks.com 和 support.paloaltonetworks.com 相符。

您還可使用此萬用字元表示整個頂層網域。例如，若要指定名為 .work 的 TLD 之執行方式，您可新增以下項目**`*.work`**。此項目與所有以 .work 結尾的網站匹配。

(*) 萬用字元僅可置於網域項目前面。

星號 **(*)** 範例

EDL 網域清單項目	相符網站
`*.company.com`	eng.tools.company.com support.tools.company.com tools.company.com

©2024 Palo Alto Networks, Inc.

EDL 網域清單項目	相符網站
	docs.company.com
***.click**	所有以 .click 頂層網域結尾的網站。

何時使用插入符號 **(^)** 字元：

使用插入符號 (^) 表示子網域的完全符合值。例如，**^paloaltonetworks.com** 僅與 paloaltonetworks.com 匹配。此項目與其他任何網站都不相符。

插入符號 **(^)** 舉例

EDL 網域清單項目	匹配網站
^company.com	company.com
^eng.company.com	eng.company.com

URL 清單

請參閱 URL 類別例外指南。

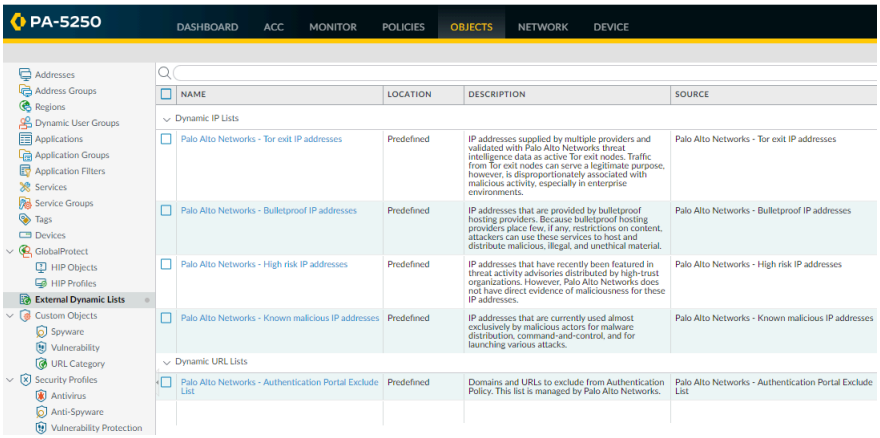
內建外部動態清單

如果具有有效的威脅防禦授權，Palo Alto Networks 提供了內建的 IP 位址 EDL，您可以用其封鎖惡意主機攻擊。

- **Palo Alto Networks** 防彈 **IP** 位址—包含防彈主機供應商提供的 IP 位址。由於防彈主機供應商對內容的限制很少（如果有），攻擊者經常使用這些服務來託管和散佈惡意、非法及不道德的材料。
- **Palo Alto Networks** 高風險 **IP** 位址—包含了來自受信任協力廠商所發行之威脅諮詢報告的惡意 IP 位址。Palo Alto Networks 將編譯威脅諮詢報告清單，但沒有 IP 位址具有惡意的直接證據。
- **Palo Alto Networks** 已知惡意 **IP** 位址—包含根據 WildFire 分析、Unit 42 研究和遙測資料認定為惡意的 IP 位址（與 Palo Alto Networks 分享威脅情報）。攻擊者幾乎專門利用這些 IP 位址來散發惡意軟體、啟動命令控制活動以及發動攻擊。
- **Palo Alto Networks Tor** 結束 **IP** 位址—包含由多個提供者提供並由 Palo Alto Networks 威脅情報資料驗證為作用中 Tor 結束節點的 IP 位址。儘管來自 Tor 結束節點的流量可以用於合法目的，但其更多地與惡意活動相關聯，在企業環境中尤為如此。

防火牆將透過內容更新接收這些摘要更新，這可讓防火牆根據 Palo Alto Networks 提供的最新威脅情報，自動執行原則。您無法修改內建清單的內容。依原樣使用清單（請參閱對外部動態清單強制執行原則），或者按需建立將清單用作來源的自訂外部動態清單（請參閱設定防火牆存取外部動態清單）以及從清單中排除項目。

©2024 Palo Alto Networks, Inc.



設定防火牆存取外部動態清單

您必須先在防火牆與裝載外部動態清單的來源之間建立連線，然後才能對外部動態清單中的項目強制執行原則。

STEP 1 | （選用）自訂防火牆將用於擷取外部動態清單的服務路由。

選取 **Device**（裝置） > **Setup**（設定） > **Services**（服務） > **Service Route Configuration**（服務路由組態） > **Customize**（自訂），然後修改 外部動態清單 服務路由。

防火牆不使用外部動態清單服務路由擷取 內建外部動態清單；內容更新修改或更新這些清單的內容（需要作用中的 *Threat Prevention* 授權）。

STEP 2 | 找到要與防火牆一起使用的外部動態清單。

- 建立一個外部動態請單並在 Web 伺服器上裝載。在空白文字檔案中輸入 IP 位址、網域或 URL。每個清單項目必須各自為一行。例如：

  ```
  financialtimes.co.in
  www.wallaby.au/joey
  www.exyang.com/auto-tutorials/How-to-enter-Data-for-Success.aspx
  ```

  請參閱外部動態清單的格式設定方針，確保防火牆不會略過清單項目。為了防止出現提交錯誤和無效項目，請勿對任何項目加首碼 http:// 或 https://。
- 使用其他來源裝載的外部動態清單，以確認其是否遵循外部動態清單的格式設定方針。

STEP 3 | 選取**Objects**（物件） > **External Dynamic Lists**（外部動態清單）。

STEP 4 | 按一下 **Add**（新增），並為清單輸入描述性 **Name**（名稱）。

 ©2024 Palo Alto Networks, Inc.

STEP 5 | （選用）選取 **Shared**（共用），讓已啟用多虛擬系統之裝置上所有的虛擬系統共用清單。依預設，系統會在**Virtual Systems**（虛擬系統）下拉式清單中目前所選的虛擬系統上建立物件。

Palo Alto Networks 建議的最佳做法是，在使用多個虛擬系統時，使用共享 *EDL*。為每個 *vsys* 使用具有重複項目的個別 *EDL*，將使用更多記憶體，從而導致過度使用防火牆資源。

STEP 6 | （僅限 Panorama）選取 **Disable override**（停用覆寫），確保防火牆管理員無法在本機覆寫防火牆上之透過裝置群組提交從 Panorama 繼承此組態的設定。

STEP 7 | 選取清單 **Type**（類型）（例如 **URL List**（**URL** 清單）。

確保該清單僅包括此清單類型的項目。請參閱確認是否忽略或跳過外部動態清單中的項目。

如果您使用的是網址清單，也可啟用 **Automatically expand to include subdomains**（自動展開以包含子網域），以同時包含指定網域的子網域。例如，如果您的網域清單包含 paloaltonetworks.com，網域名稱所有較低等級的配件（例如，*.paloaltonetworks.com）也將作為清單的一部分包含在內。請記住，當此設定啟用時，指定清單中的每個網域都需要一個附加項目，從而有效地將所佔用的項目數量加倍。

STEP 8 | 為您剛剛在網頁伺服器上建立的清單輸入 **Source**（來源）。來源必須包括存取清單的完整路徑。例如，**`https://1.2.3.4/EDL_IP_2015`**。

- 如果您建立預先定義的 IP 外部動態清單，則將 Palo Alto Networks 惡意 IP 位址摘要用作來源。
- 如果您建立預先定義的 URL 外部動態清單，請選取 **panw-auth-portal-exclude-list** 作為來源。

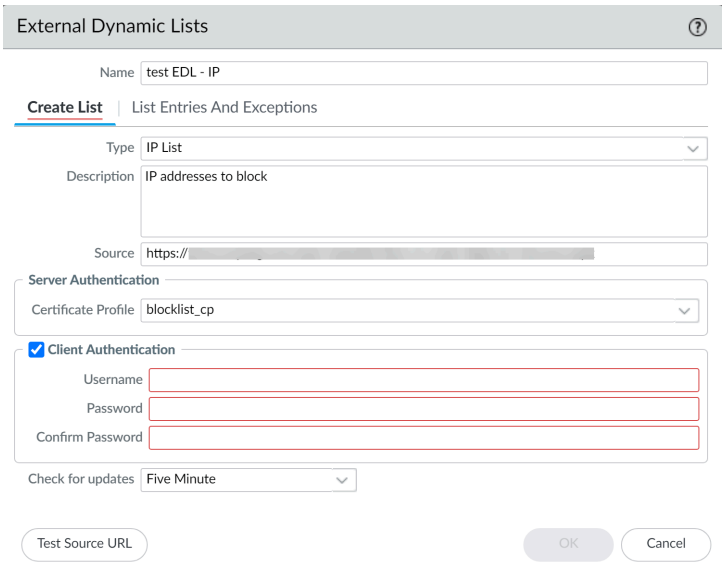
STEP 9 | 如果清單來源受 SSL 保護（即清單帶有 HTTPS URL），則啟用伺服器驗證。選取 **Certificate Profile**（憑證設定檔）或建立 **New Certificate Profile**（新憑證設定檔），以驗證裝載清單的伺服器。您選取的憑證設定檔必須的根憑證授權單位 (CA) 和中繼 CA 憑證必須與您所驗證的伺服器上安裝的憑證相符。

增加了您可用於強制執行原則的外部動態清單數量。使用相同的憑證設定檔驗證來自相同來源 *URL*的外部動態清單。如果您將不同憑證設定檔指派給來自相同來源 *URL* 的外部動態清單，防火牆會將每個清單計為唯一的外部動態清單。

©2024 Palo Alto Networks, Inc.

STEP 10 | 如果清單來源有 HTTPS URL 並且需要基本的 HTTP 驗證以存取清單，則啟用用戶端驗證。

1. 選取 **Client Authentication**（用戶端驗證）。
2. 輸入有效的 **Username**（使用者名稱）來存取清單。
3. 輸入 **Password**（密碼）與 **Confirm Password**（確認密碼）。



STEP 11 | （不適用於 Panorama 或預先定義的 URL EDL）按一下 **Test Source URL**（測試來源 **URL**）以確認防火牆可連線至網頁伺服器。

當驗證用於 *EDL* 存取時，測試來源 ***URL*** 功能不可用。

STEP 12 | （選用）指定防火牆檢查清單更新的頻率。依預設，防火牆會每小時擷取一次清單並提交變更。

該間隔是相對於上次提交。因此，對於五分鐘間隔，如果上次提交是在一個小時前，則該提交會在 5 分鐘後進行。若要立即擷取清單，請參閱從 Web 伺服器擷取外部動態清單。

STEP 13 | 按一下 **OK**（確定）並 **Commit**（交付）變更。

STEP 14 | （選用）EDL 按評估順序從上到下顯示。使用頁面底部的方向控制變更清單順序。這允許您對清單進行排序，以確保在達到容量限制之前提交最重要的 EDL。

您只能在取消選取 ***Group By Type***（按類型分組）後才能變更 *EDL* 順序。

STEP 15 | 對外部動態清單強制執行原則。

如果伺服器或用戶端驗證失敗，防火牆將根據上次成功擷取的外部動態清單，停止強制執行原則。尋找驗證失敗的外部動態清單，並檢視驗證失敗的原因。

©2024 Palo Alto Networks, Inc.

設定防火牆從 EDL 主機服務存取外部動態清單

設定防火牆，從軟體即服務 (SaaS) 應用程式的 EDL 主機服務存取外部動態清單 (EDL)

- 使用 EDL 主機服務建立外部動態清單
- 將 GlobalSign Root R1 憑證轉換為 PEM 格式

使用 **EDL** 主機服務建立外部動態清單

一些軟體即服務 (SaaS) 供應商發佈 IP 位址和 URL 清單作為其 SaaS 應用程式的目的地端點。隨著支援的增長和服務的擴展，SaaS 供應商會經常更新 SaaS 應用程式目的地端點清單。這要求您手動監控 SaaS 應用程式端點以瞭解變更，並手動更新原則設定，以確保與這些關鍵 SaaS 應用程式的連線能力，或設定外部工具來監控和更新您的 EDL。

設定由 Palo Alto Networks 維護、使用 EDL主機服務的 EDL，以減輕為 SaaS 應用程式維護 EDL 的運營負擔。EDL 主機服務為 SaaS 應用程式供應商發布的 SaaS 應用程式端點提供公開可用的摘要 URL。利用摘要 URL 作為 EDL 中的來源，可以動態執行 SaaS 應用程式流量，而無需託管和維護自己的 EDL 來源。

Palo Alto Networks 每天檢查 SaaS 提供者發布的應用程式摘要 URL，並最佳化從 SaaS 應用程式提供者處收到的 IP 位址資訊，以減少在每個 EDL 中發布的 IP 位址數量。這種最佳化包括識別和移除重複的 IP 位址，然後將剩餘的 IP 位址彙總到數量較少的連續位址範圍中。

Microsoft 在每個日曆月末更新所有 Microsoft 365 摘要 URL，並在更新前 30 天提供通知。有關更多資訊，請參閱官方 Microsoft 365 Web 服務頁面。此外，Microsoft 365 Common 和 Office Online SaaS 應用程式的端點始終新增到 EDL 主機服務中的每個摘要 URL。

EDL 主機服務可用性狀態和更新將發佈到 Palo Alto Networks 雲端服務狀態頁面。

STEP 1 | 造訪 EDL 主機服務，並確定 SaaS 應用程式的摘要 URL。

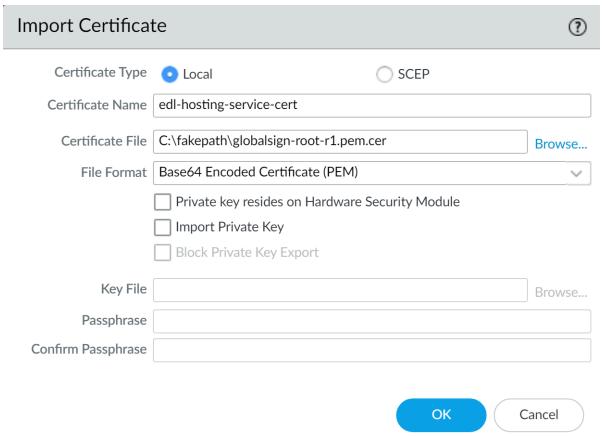
檢閱 Microsoft 365 文件以獲取更多資訊，瞭解哪些摘要 URL 最適合您的使用案例。此外，在確定摘要 URL 時，請考慮 SaaS 應用程式和存取 SaaS 應用程式之使用者的位置。例如，如果您在德國有一個僅需要存取 Exchange Online 的分支機構，請從以下服務區域選取一個摘要 **URL**：適用於德國的 **Exchange Online**。

對於基於原則的轉送原則規則，請使用基於 *IP* 的摘要 *URL*。

©2024 Palo Alto Networks, Inc.

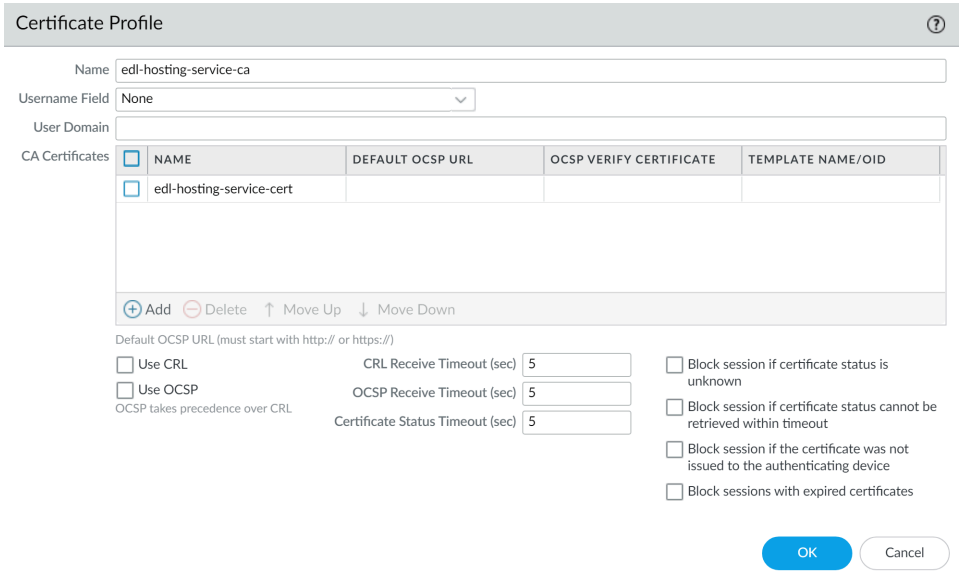
STEP 2 | （最佳做法）建立憑證設定檔來驗證 EDL 主機服務。

1. 下載 GlobalSign Root R1 憑證。
2. 將 GlobalSign Root R1 憑證轉換為 PEM 格式。
3. 啟動防火牆 Web 介面。
4. 匯入 GlobalSign Root R1 憑證。
   1. 選取 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證），然後 **Import**（匯入）新的憑證。
   2. 對於 **Certificate Type**（憑證類型），選取 **Local**（本機）。
   3. 輸入描述性的憑證名稱。
   4. 對於 **Certificate File**（憑證檔案），選取 **Browse**（瀏覽），然後選取您在上一步中轉換的憑證。
   5. 對於 **File Format**（檔案格式），選取 **Base64 Encoded Certificate (PEM)**（**Base64 編碼憑證 (PEM)**）。
   6. 按一下 **OK**（確定）。



5. 建立憑證授權單位 (CA) 憑證設定檔。
   1. 選取 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificate Profile**（憑證設定檔），並 **Add**（新增）新的憑證設定檔。
   2. 輸入描述性的 **Name**（名稱）。
   3. 對於 **CA Certificates**（**CA** 憑證），請 **Add**（新增）您在上一步中匯入的憑證。
   4. 按一下 **OK**（確定）。

©2024 Palo Alto Networks, Inc.



6. **Commit**（認可）。

 ©2024 Palo Alto Networks, Inc.

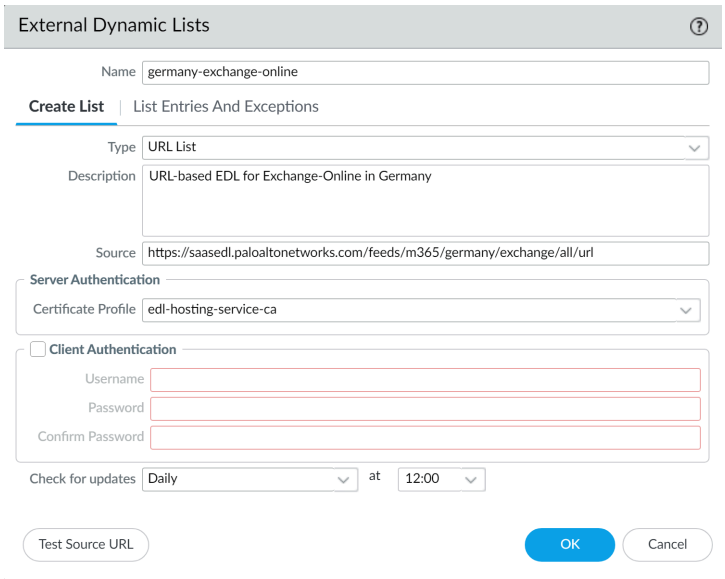
STEP 3 | 使用來自 EDL 主機服務的摘要 URL 建立 EDL。

1. 選取 **Objects**（物件） > **External Dynamic Lists**（外部動態清單），然後 **Add**（新增）新 EDL。
2. 為 EDL 輸入描述性 **Name**（名稱）。
3. 選取 EDL **Type**（類型）。
   - 對於基於 IP 的 EDL，請選取 **IP List**（**IP** 清單）。
   - 對於基於 URL 的 EDL，請選取 **URL List**（**URL** 清單）。
4. （選用）輸入 **Description for the EDL**（**EDL** 的說明）
5. 輸入摘要 URL 作為 EDL **Source**（來源）。

   在特定的摘要 *URL* 中強制執行所有端點。從摘要 *URL*中新增或排除特定端點可能會導致 *SaaS* 應用程式的連線問題。
6. （最佳做法）選取您在上一步中建立的 **Certificate Profile**（憑證設定檔）。
7. 指定防火牆應檢查更新的頻率，以比對摘要 URL 的更新頻率。

   例如，如果摘要 URL 由 Palo Alto Networks 每天更新，則將 EDL 檢查更新的頻率設定為 **Daily**（每日）。

   Palo Alto Networks 會顯示 EDL 主機服務中每個摘要 URL 的更新頻率。摘要 URL 會在任何新的端點自動更新。
8. 按一下 **Test Source URL**（測試來源 **URL**）以確認防火牆能夠從 EDL 主機服務存取摘要 URL。
9. 按一下 **OK**（確定）。



 ©2024 Palo Alto Networks, Inc.

STEP 4 | 對外部動態清單強制執行原則.

當您在來自 EDL 主機服務的 EDL（其中 EDI 是來源）上執行原則時，在設定哪些使用者有權存取 SaaS 應用程式時請務必具體，以避免過度佈建對應用程式的存取權限。

在原則規則中將 App-ID 與 *EDL* 搭配使用，以進一步嚴格執行 *SaaS* 應用程式流量。

將 GlobalSign Root R1 憑證轉換為 PEM 格式

您必須將 GlobalSign Root R1 憑證轉換為 PEM 格式，才能建立用於驗證 EDL 主機服務的憑證設定檔。在使用 EDL 主機服務的情況下，當您將防火牆設定為從 EDL 主機服務存取外部動態清單時，建立憑證設定檔來驗證 EDL 主機服務是最佳做法。

根據您下載 GlobalSign Root R1 憑證之裝置的作業系統，參閱適當的程序。

STEP 1 | 如果您尚未下載 GlobalSign Root R1 憑證，請下載該憑證。

©2024 Palo Alto Networks, Inc.

STEP 2 | 轉換憑證。

- **Mac** 與 **Linux** 作業系統

1. 開啟終端機並轉換您下載的 GlobalSign Root R1 憑證。

```
admin: openssl x509 -in <certificate-path>.crt -inform DER -out
 <target-export-path>.pem -outform PEM
```

```
admin-1@admin-1:~$ openssl x509 -in /home/admin-1/Downloads/Root-R1.crt -inform
DER -out /home/admin-1/Downloads/globalsign-root-r1.pem -outform PEM
```

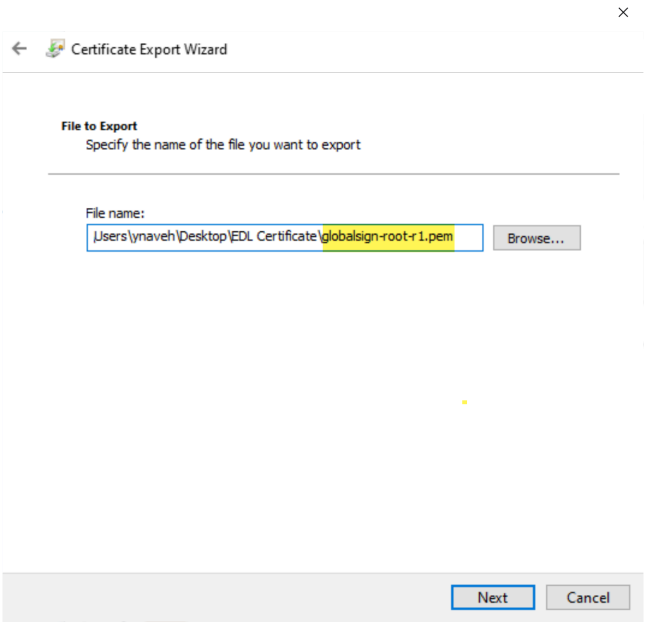
如果未指定目標匯出路徑，則會在裝置桌面上建立轉換的憑證。

- **Windows** 作業系統

1. 導覽至您下載 GlobalSign Root1 憑證的位置。
2. 按兩下並 **Open**（開啟）憑證。
3. 按一下 **Details**（詳細資料）和 **Copy to File**（複製到檔案）。

   出現提示時，按一下 **Next**（下一步）以繼續。
4. 選取**Base-64 encoded x.509 (.CER)**，然後按一下 **Next**（下一步）
5. 按一下 **Browse**（瀏覽）以導覽至您要複製憑證的位置，輸入憑證的名稱（包括附加到檔案名稱末尾的 **.pem**）。例如，**globalsign-root-r1.pem**

   Save（儲存）憑證。顯示的 **File Name**（檔案名稱）會顯示目標匯出路徑，以及您輸入的已附加 .cer 的憑證名稱。刪除附加的 .cer。



6. 按一下 **Next**（下一步），並 **Finish**（完成）匯出憑證。

©2024 Palo Alto Networks, Inc.

從網頁伺服器擷取外部動態清單

在設定防火牆存取外部動態清單時，您可以設定防火牆每小時（預設）、每五分鐘、每天、每週或每月從 Web 伺服器擷取一次清單。如果您已在清單上新增或刪除 IP 位址，且需要觸發即時重新整理，可使用以下程序擷取更新後的清單。

STEP 1 | 若要隨選擷取清單，可選取 **Objects**（物件） > **External Dynamic Lists**（外部動態清單）。

STEP 2 | 選取要重新整理的清單，然後按一下 **Import Now**（立即匯入）。匯入清單的工作將排入佇列。

STEP 3 | 若要檢視工作管理員中工作的狀態，請參閱管理並監控管理工作。

STEP 4 | （選用）在防火牆擷取清單後，檢視外部動態清單項目。

檢視外部動態清單項目

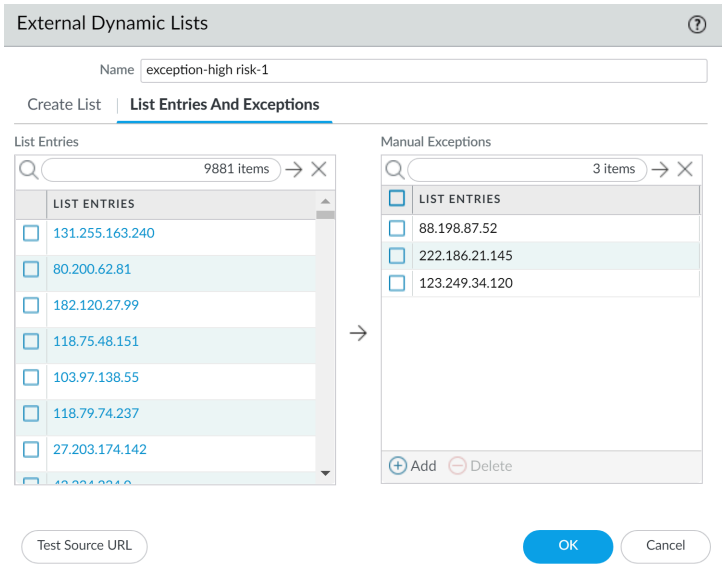
在您對外部動態清單強制執行原則時，可以直接在防火牆上檢視外部動態清單的內容，以檢查其是否包含特定 IP 位址、網域或 URL。所顯示的項目視乎於防火牆最近擷取的外部動態清單版本。

STEP 1 | 選取**Objects**（物件） > **External Dynamic Lists**（外部動態清單）。

STEP 2 | 按一下您要檢視的外部動態清單。

 ©2024 Palo Alto Networks, Inc.

STEP 3 | 按一下 **List Entries and Exceptions**（清單項目和例外），檢視防火牆從該清單中擷取的物件。



對於下列情況，清單可能為空白：

- EDL 尚未套用至安全性原則規則。若要將 EDL 套用至安全性政策規則並填入 EDL，請參閱對外部動態清單強制執行原則。
- 防火牆尚未擷取外部動態清單。若要強制防火牆立即擷取外部動態清單，可從 Web 伺服器擷取外部動態清單。
- 防火牆服務存取裝載外部動態清單的伺服器。按一下 **Test Source URL**（測試來源 **URL**）以確認防火牆是否可連線至伺服器。

STEP 4 | 在篩選條件欄位中輸入 IP 位址、網域或 URL（視乎清單類型），然後套用篩選條件 (→)，以檢查其是否在清單中。根據您需要封鎖或允許的 IP 位址、網域和 URL，從外部動態清單中排除項目。

從外部動態清單中排除項目

在您檢視外部動態清單中的項目時，可以從清單中排除最多 100 個項目。從外部動態清單中排除項目的功能讓您可以對清單中的部分（而非全部）項目強制執行原則。當外部動態清單（如 Palo Alto Networks 高風險 IP 位址摘要）來自於協力廠商來源而無法編輯其內容時，這會非常有用。

STEP 1 | 檢視外部動態清單項目。

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 選取最多 100 個要從清單中排除的項目，然後按一下 Submit（提交）(→) 或手動 **Add**（新增） 清單例外項。

- 如果手動例外狀況清單中有重複的項目，您就無法將變更儲存至外部動態清單中。若要識別重複項目，可尋找帶紅色底線的項目。
- 手動新增的例外項必須與清單項目完全相符。此外，您無法從 IP 位址範圍內排除特定的 IP 位址。若要從 IP 位址範圍中排除特定 IP 位址，您必須將範圍中的每個 IP 位址新增為清單項目，然後排除所需的 IP 位址。

  防火牆不支援從 IP 位址範圍中排除個別 IP 位址。

STEP 3 | 按一下 **OK**（確定）和 **Commit**（提交），以儲存變更。

STEP 4 | （選用）對外部動態清單強制執行原則。

對外部動態清單強制執行原則

根據外部動態清單中的 IP 位址或 URL封鎖或允許流量，或使用動態網域清單，利用 DNS sinkhole 阻止對惡意網域的存取。

關於針對帶有外部動態清單的防火牆強制執行原則的提示：

- 在檢視防火牆上的外部動態清單時（***Objects***（物件） > ***External Dynamic Lists***（外部動態清單）），按一下 ***List Capacities***（清單容量），以比較原則中目前使用的 *IP* 位址、網域及 *URL* 數目和防火牆對每種清單類型支援的項目總數。
- 使用全域尋找搜尋防火牆或 Panorama 管理伺服器，以尋找屬於原則中使用的一個或多個外部動態清單的網域、*IP* 位址或 *URL*。這對於確定是（安全性原則規則中所引用的）哪個外部動態清單造成防火牆封鎖或允許特定網域、*IP* 位址或 *URL*。
- 使用頁面底部的方向控制變更 *EDL* 的評估順序。這允許您對清單進行排序，以確保在達到容量限制之前提交 *EDL* 中最重要的條目。

  您只能在取消選取 ***Group By Type***（按類型分組）後才能變更 *EDL* 順序。

為自訂網域清單設定 DNS Sinkholing。

在 URL 篩選設定檔中使用外部動態清單。

©2024 Palo Alto Networks, Inc.

將 **URL** 類型的外部動態清單用作安全性原則規則中的比對準則。

1. 選取 **Policies**（政策） > **Security**（安全性）。
2. 按一下 **Add**（新增），並為規則輸入描述性 **Name**（名稱）。
3. 在 **Source**（來源）頁籤上選取 **Source Zone**（來源區域）。
4. 在 **Destination**（目的地）頁籤上選取 **Destination Zone**（目的地區域）。
5. 在 **Service/URL Category**（服務/**URL** 類別）頁籤上，按一下 **Add**（新增）以從 URL 類別清單中選取適當的外部動態清單。
6. 在 **Actions**（動作）頁籤上，將 **Action Setting**（動作設定）設為 **Allow**（允許）或 **Deny**（拒絕）。
7. 按一下 **OK**（確定）與 **Commit**（提交）。
8. 確認是否忽略或跳過外部動態清單中的項目。

   在防火牆上使用以下 CLI 命令以檢閱清單詳情。

   ```
   request system external-list show type <domain | ip | url>
    name_of_list
   ```

   例如：

   ```
   request system external-list show type url EBL_ISAC_Alert_List
   ```

9. 測試已強制執行該原則動作。
   1. 檢視外部動態清單項目以獲取 URL 清單，並嘗試存取該清單中的 URL。
   2. 確認是否能強制執所您定義的動作。
   3. 若要監控防火牆上的活動：
      - 選取 **ACC** 並新增 URL 網域作為全域篩選器，以檢視您存取的 URL 的網路活動和封鎖活動。
      - 選取 **Monitor**（監控） > **Logs**（日誌） > **URL Filtering**（**URL** 篩選）以存取詳細日誌檢視。

©2024 Palo Alto Networks, Inc.

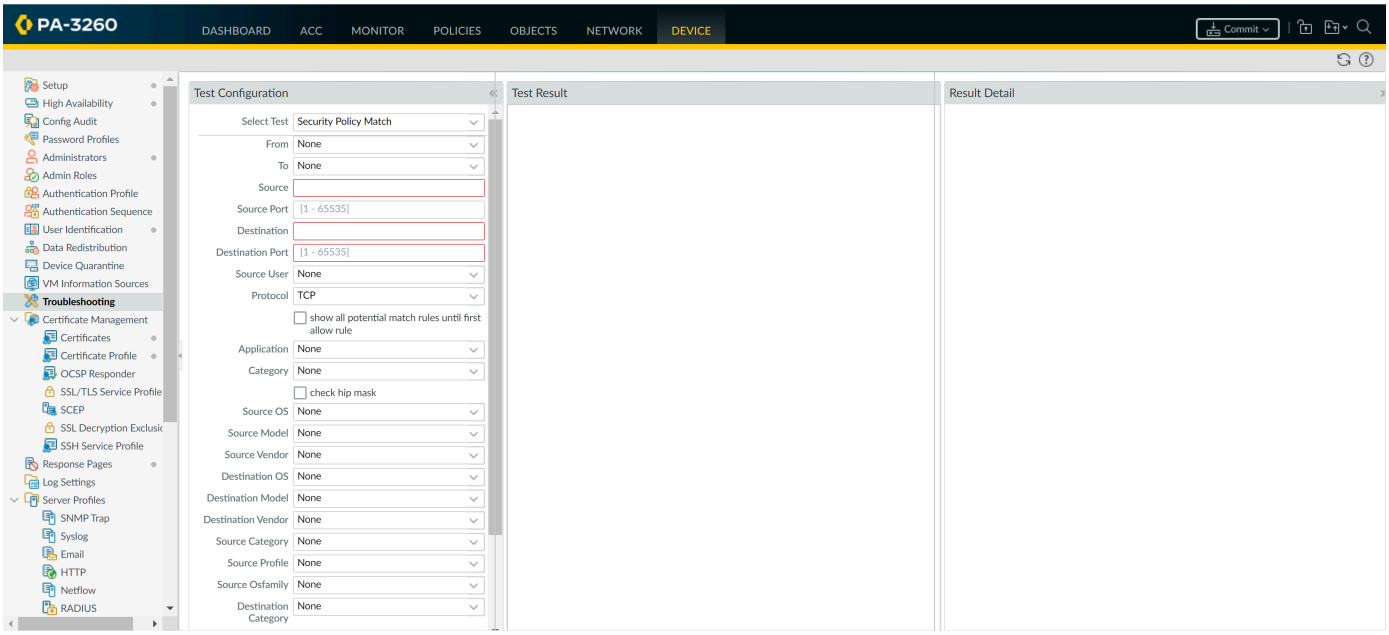
將 **IP** 外部動態清單或預先定義的 **IP** 外部動態清單用作安全性原則規則中的來源或目的地位址物件。

如果您部署新伺服器並想要允許存取新部署的伺服器而不需防火牆提交，這個功能會很有用。

1. 選取 **Policies**（原則） > **Security**（安全性）。
2. 按一下 **Add**（新增），並為規則指定一個描述性 **Name**（名稱）。
3. 在 **Source/Destination**（來源/目的地）頁籤上，設定外部動態清單以用作 **Source/Destination Address**（來源/目的地位址）。
4. 在 Service/URL Category（服務/URL 類別）頁籤上，確保將 **Service**（服務）設為 **application-default**（應用程式預設值）。
5. 在 Actions（動作）頁籤上，將 Action Setting（動作設定）設為 **Allow**（允許）或 **Deny**（拒絕）。

   如果您想要為特定的 *IP* 位址指定允許與拒絕動作，請建立單獨的外部動態清單。
6. 所有其他選項保持預設值不變。
7. 按一下 **OK**（確認）以儲存變更。
8. **Commit**（提交）變更。
9. 測試已強制執行該原則動作。
   1. 檢視外部動態清單項目以獲取外部動態清單，並嘗試存取該清單中的 IP 位址。
   2. 確認是否能強制執所您定義的動作。
   3. 選取 **Monitor**（監控） > **Logs**（日誌） > **Traffic**（流量），然後檢視該工作階段的日誌項目。
   4. 若要驗證與流量相符的原則規則，請選取 **Device**（裝置） > **Troubleshooting**（疑難排解），並執行安全性原則比對測試：

©2024 Palo Alto Networks, Inc.



使用預先定義的 **URL** 外部動態清單將應用程序用於背景流量的良性網域從驗證政策中排除。

當您選取 **panw-auth-portal-exclude-list** EDL 類型時，可以輕鬆地從驗證原則執行中排除許多應用程式用於背景流量（例如更新和其他受信任的服務）的網域。這樣可以確保防火牆不會封鎖這些服務的必要流量，且不會中斷應用程式維護。

1. 選取 **Policies**（原則）> **Authentication**（驗證）。
2. 在 **Service/URL Category**（服務/**URL** 類別）頁籤上，選取預先定義的 URL EDL 作為 **URL Category**（**URL** 類別）。
3. 在 **Actions**（動作）頁簽上，選取 **`default-no-captive-portal`** 作為 **Authentication Enforcement**（驗證執行）。
4. 按一下 **OK**（確定）。
5. 將規則 **Move**（移動）至頂部以使其成為原則中的第一條規則。
6. **Commit**（提交）您的變更。

尋找驗證失敗的外部動態清單

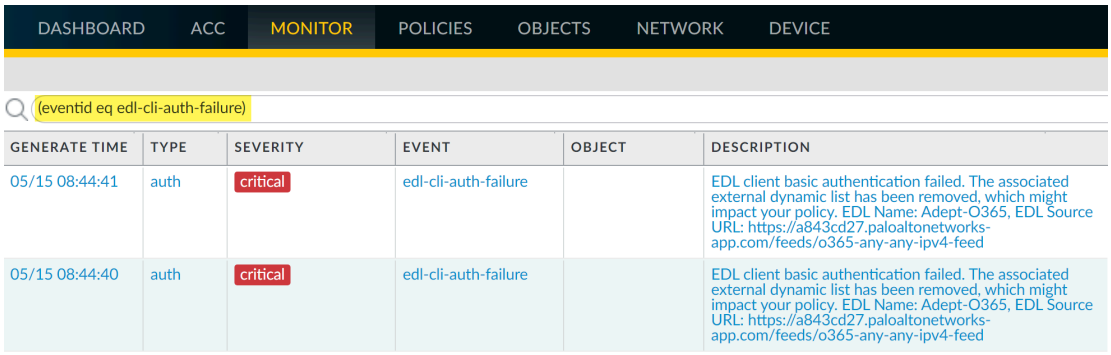
當需要 SSL 的外部動態清單的用戶端或伺服器驗證失敗時，防火牆會產生關鍵嚴重性的系統日誌。日誌非常重要，因為防火牆會在驗證失敗後，根據上次成功的外部動態清單繼續執行政策，而不是使用最新版本。使用下列程序檢視告知您與外部動態清單相關之驗證失敗的關鍵系統日誌訊息。

STEP 1 | 選取 **Monitor**（監控）> **Logs**（日誌）> **System**（系統）。

©2024 Palo Alto Networks, Inc.

STEP 2 | 構建下列篩選器，以檢視所有與驗證失敗相關的訊息，然後套用篩選器。如需更多資訊，請檢閱篩選日誌的完整工作流程。

- 伺服器驗證失敗—**(eventid eq tls-edl-auth-failure)**
- 用戶端驗證失敗—**(eventid eq edl-cli-auth-failure)**



STEP 3 | 檢閱系統日誌訊息。該訊息的描述中包含外部動態清單的名稱、清單的來源 URL 以及驗證失敗的原因。

如果憑證過期，裝載外部動態清單的伺服器將驗證失敗。如果您已設定憑證設定檔來透過憑證撤銷清單 (CRL) 或線上憑證狀態通訊協定 (OCSP) 來檢查憑證撤銷狀態，出現下列情況時，伺服器也可能驗證失敗：

- 憑證已被撤銷。
- 憑證撤銷狀態未知。
- 在防火牆嘗試連線至 CRL/OCSP 服務時逾時。

關於憑證設定檔組態的詳細資訊，請參閱設定憑證設定檔的步驟。

確認是否已將伺服器的根 *CA* 和中間 *CA* 新增至設定了外部動態清單的憑證設定檔。否則，防火牆將無法正確驗證該清單。

如果您為外部動態清單輸入了錯誤的使用者名稱和密碼組合，用戶端將驗證失敗。

STEP 4 | （可選）為驗證失敗的外部動態清單停用驗證，作為權宜之計，直至清單擁有者更新了裝載該清單的伺服器憑證。

為外部動態清單停用驗證

Palo Alto Networks 建議對裝載防火牆上設定之外部動態清單的伺服器啟用驗證。但是，如果發現外部動態清單驗證失敗並更希望對這些清單停用伺服器遇難者，可以透過 CLI 操作。下列程序僅適用於使用 SSL 保護的外部動態清單（即具有 HTTPS URL 的清單）；防火牆不會對具有 HTTP URL 的清單強制執行伺服器驗證。

對外部動態清單停用伺服器驗證還會停用用戶端驗證。停用用戶端驗證後，防火牆將無法連線至需要使用者和密碼才能存取的外部動態清單。

©2024 Palo Alto Networks, Inc.

STEP 1 | 啟動 CLI，並按下方所示切換至設定模式：

```
username@hostname> configure Entering configuration mode [edit]
 username@hostname#
```

從 > 變更為 # 符號表示現已處於設定模式。

STEP 2 | 針對清單類型輸入相應的 CLI 命令：

- IP 位址

```
set external-list <external dynamic list name> type ip
 certificate-profile None
```

- 網域

```
set external-list <external dynamic list name> type domain
 certificate-profile None
```

- URL

```
set external-list <external dynamic list name> type url
 certificate-profile None
```

STEP 3 | 確認是否已為外部動態清單停用驗證。

針對清單觸發重新整理（請參閱從 Web 伺服器擷取外部動態清單）。如果防火牆成功擷取清單，則表示伺服器驗證已停用。

 ©2024 Palo Alto Networks, Inc.

動態註冊 IP 位址與標籤

為了減輕擴充、缺乏彈性與效能等挑戰，現今的網路架構允許依需求佈建、變更和刪除虛擬機器 (VMs) 與應用程式。這種靈活性卻為安全性管理員帶來挑戰，因為他們對動態佈建的 VM 以及可在這些虛擬資源上啟用的大量應用程式之 IP 位址的檢視能力受到限制。

防火牆（硬體式與 VM-Series 型號）支援動態註冊 IP 位址、IP 組（IP 範圍和子網路）與標籤的功能。可直接在防火牆上或從 Panorama 註冊 IP 位址和標籤。您可以自動移除防火牆日誌中所包含的來源和目的地 IP 位址上的標籤。

PAN-OS 僅支援動態位址群組中的 *IPv4 IP* 子網路和範圍。

您可使用下列任一選項啟用動態註冊流程：

- **Windows** 適用的 **User-ID** 代理程式—在您已部署 User-ID 代理程式的環境中，您可以啟用 User-ID 代理程式以監控最多 100 個 VMware ESXi 伺服器 vCenter Server，或兩者的組合。當您在這些 VMware 伺服器上佈建或修改虛擬電腦時，代理程式可以擷取 IP 位址變更，並與防火牆共用這些變更。
- **VM** 資訊來源—當您在這些來源上佈建或修改虛擬機器時，可在防火牆上用原生方式監控 VMware ESXi、vCenter Server、AWS-VPC 和 Google 計算引擎，並擷取 IP 位址變更。VM 資訊來源選項會輪詢預先定義的屬性集，且不需要外部的指令碼即可透過 XML API 註冊 IP 位址。請參閱 監控虛擬環境中的變更。
- **Panorama** 外掛程式—可讓您啟用 Panorama™ M-Series 或虛擬設備，以連線到 Azure 或 AWS 公共雲端環境，並擷取有關訂閱或 VPC 中部署之虛擬機器的資訊。然後，Panorama 將 VM 資訊註冊到您已設定通知的受管理 Palo Alto Networks 防火牆，然後您可以使用這些屬性定義動態位址群組並將其附加到安全性原則規則，以允許和拒絕來往這些 VM 的流量。
- **VMware Service Manager**（僅在註冊的 NSX 解決方案）—整合的 NSX 解決方案在設計上可自動佈建與散佈 Palo Alto Networks 新世代 Security Operating Platform®，並使用 Panorama 傳遞動態內容式安全性原則。NSX 管理員會更新 Panorama 中與在此整合解決方案中部署的虛擬電腦相關聯的 IP 位址、IP 組和標籤資訊。如需此解決方案的相關資訊，請參閱設定 VM 系列 NSX 版防火牆。
- **XML API**—防火牆與 Panorama 支援使用標準 HTTP 要求傳送與接收資料的 XML API。您可以使用此 API 向防火牆或 Panorama 註冊 IP 位址與標籤。您直接從 cURL 之類的命令列公用程式進行 API 叫用，或透過使用支援 REST 式服務的任何指令碼或應用程式架構進行 API 叫用。如需詳細資料，請參閱《PAN-OS XML REST API 用法指南》。
- 自動標記 —當防火牆上產生日誌時，自動標記來源和目的地 IP 位址，並向防火牆或 Panorama 上的 User-ID 代理程式註冊 IP 位址和標記對應，或使用 HTTP 伺服器設定檔想原則 User-ID 代

©2024 Palo Alto Networks, Inc.

理程式註冊。例如，當防火牆產生威脅日誌時，您可以設定防火牆使用特定標籤名稱標記威脅日誌中的來源 IP 位址。如需詳細資訊，請參閱使用自動標記自動執行安全性動作。

此外，您還可以使用逾時設定防火牆，以在設定的時間後動態取消註冊標籤。例如，您可以將逾時設定為與 IP 位址的 DHCP 租約逾時相同的持續時間。這使得 IP 位址至標籤對應與 DHCP 租用同時到期，這樣您便不會在重新指派 IP 位址時無意套用原則。

請參閱將日誌轉送至 HTTP(S) 目的地。

如需建立與使用動態位址群組的相關資訊，請參閱 在原則中使用動態位址群組。

如需用於動態註冊標籤之 CLI 命令的相關資訊，請參閱 動態 IP 位址與標籤的 CLI 命令。

©2024 Palo Alto Networks, Inc.

在原則中使用動態使用者群組

動態使用者群組可幫助您建立原則，可為異常使用者行為和惡意活動提供自動修復，同時保持使用者的洞察性。建立群組並提交變更後，防火牆將註冊使用者和關聯的標籤，然後自動更新動態使用者群組的成員資格。因為動態使用者群組的成員資格的更新為自動，所以使用動態使用者群組而不是靜態群組物件將允許您能夠回應使用者行為的變更或潛在威脅，而無需手動變更原則。

未確定包含哪些使用者作為成員，動態使用者群組會將標籤用作篩選準則。一旦使用者符合篩選準則，該使用者便會成為動態使用者群組的成員。基於標籤的篩選器使用邏輯的 *and* 與 *or* 運算子。每個標籤都為您在來源上靜態或動態註冊的中繼資料元素或屬性-值對。靜態標籤是防火牆設定的一部分，而動態標籤是執行階段設定的一部分。因此，如果動態標籤已與您在防火牆上提交的原則相關聯，則無需提交對動態標籤更新

若要動態註冊標籤，您可以使用：

- XML API
- User-ID 代理程式
- Panorama
- 防火牆上的網頁介面

防火牆將動態使用者群組的標籤重新散佈給接聽重新散佈代理程式，該代理程式包括其他防火牆、Panorama 或專用日誌收集器以及 Cortex 應用程式。

為了支援動態使用者群組標籤的重新散佈，所有防火牆必須使用 *PAN-OS 9.1* 以從註冊來源接收標籤。

防火牆將動態使用者群組的標籤重新散佈到下一個躍點，您可以設定日誌轉送以將日誌傳送到特定伺服器。日誌轉送還允許您使用 auto-tagging（自動標記） 以根據日誌中的事件自動新增或移除動態使用者群組的成員。

STEP 1 | 選取 **Objects**（物件） > **Dynamic User Groups**（動態使用者群組），然後 **Add**（新增）一個新的動態使用者群組。

©2024 Palo Alto Networks, Inc.

STEP 2 | 定義動態使用者群組的成員資格。

1. 輸入群組的 **Name**（名稱）。
2. （選用）輸入群組的 **Description**（說明）。
3. 使用動態標記新增比對規則，以定義動態使用者群組中的成員。
4. （選用）將 **And** 或 **Or** 運算子與要用於篩選或匹配的標籤一起使用。不支援否定。
5. 按一下 **OK**（確定）。
6. （選用）選取要指派給群組自身的 **Tags**（標籤）。

   該標籤顯示在 ***Dynamic User Group***（動態使用者群組）清單的 ***Tags***（標籤）欄中，並定義動態群組物件，而不是群組中的成員。
7. 按一下 **OK**（確定）並 **Commit**（交付）變更。

   如果更新使用者群組物件篩選器，則必須提交變更以更新設定。

STEP 3 | 根據要用作比對規則的日誌資訊，透過建立日誌轉送設定檔或設定日誌設定來設定 auto-tagging（自動標記）。

- 對於驗證、資料、威脅、流量、通道檢查、URL 和 WildFire 日誌，請建立日誌轉送設定檔。
- 對於 User-ID、GlobalProtect、IP-Tag 日誌，請設定日誌設定。

STEP 4 | （選用）要在特定時間段後將動態使用者群組成員傳回到其原始群組，請輸入 **Timeout**（逾時）值（以分鐘為單位，預值設為 0，範圍為 0 至 43200）。

STEP 5 | 在原則中使用動態使用者群組來管制該群組成員的流量。

您將至少需要建立兩個規則：一個規則允許初始流量填入動態使用者群組，另一個規則拒絕要阻止的活動的流量。為標籤使用者，允許流量的規則在您的規則庫中必須具有比拒絕流量的規則更高的規則數。

1. 從步驟 1 中選取動態使用者群組作為 **Source User**（來源使用者）。
2. 建立 **Action**（動作）拒絕對動態使用者群組成員發送流量的規則。
3. 建立允許流量填入動態使用者群組成員的規則。
4. 如果在步驟 3 中設定 **Log Forwarding**（日誌轉送）設定檔，請選取該設定檔並將其新增到原則中。
5. **Commit**（提交）您的變更。

©2024 Palo Alto Networks, Inc.

STEP 6 | （選用）調整群組的成員資格，並定義使用者-標籤的對應更新的註冊來源。

如果初始使用者-標籤的對應擷取到不應該成為成員的使用者，或者如果其不包括應該成為成員的使用者，請修改群組的成員以包括要對其強制執行原則的使用者，並指定對應的來源。

1. 在 **Users**（使用者）欄中，選取更多。
2. **Register Users**（註冊使用者）將其新增至群組中，然後為標籤和使用者到標籤的對應選取 **Registration Source**（註冊來源）。
   - **Local**（本機）（預設值）—在防火牆上本機註冊動態使用者群組成員的標籤和對應。
   - **Panorama User-ID Agent**（**Panorama User-ID** 代理程式）—在連線到 Panorama 的 User-ID 代理程式上註冊動態使用者群組成員的標籤和對應。如果動態使用者群組來自 Panorama，則該行顯示為黃色，且群組名稱、說明、比對規則和標籤為唯讀。但是，您仍然可以在群組中註冊或取消註冊使用者。
   - **Remote device User-ID Agent**（遠端裝置 **User-ID** 代理程式）—在遠端 User-ID 代理程式上註冊動態使用者群組成員的標籤和對應。要選取此選項，則必須設定 HTTP server profile（HTTP 伺服器設定檔）。
3. 選取您想要在使用用來設定群組的標籤的來源上註冊的 **Tags**（標籤）。
4. （選用）要在特定時間段後將動態使用者群組成員傳回到其原始群組，請輸入 **Timeout**（逾時）值（以分鐘為單位，預值設為 0，範圍為 0 至 43200）。
5. 根據需要 **Add**（新增）或 **Delete** （刪除）使用者。
6. （選用）**Unregister Users**（取消註冊使用者）以移除其標籤和使用者-標籤的對應。

STEP 7 | 確認防火牆正確填入動態使用者群組中的使用者。

1. 確認流量、威脅、 URL 篩選、WildFire 提交、資料篩選和通道檢查日誌中的**Dynamic User Group**（動態使用者群組）欄正確顯示動態使用者群組。
2. 使用 **`show user group list dynamic`** 命令顯示所有動態使用者群組的清單以及動態使用者群組的總數。
3. 使用 **`show object registration-user all`** 命令顯示動態使用者群組的註冊成員的使用者清單。
4. 使用 **`show user group name`** ***`group-name`*** 命令顯示有關動態使用者群組的資訊，例如來源類型。

©2024 Palo Alto Networks, Inc.

使用自動標記自動執行安全性動作

自動標記允許防火牆或 Panorama 在接收到符合特定準則的日誌時標記原則物件對象，並建立 IP 位址-標籤或使用者-標籤的對應。例如，當防火牆產生威脅日誌時，您可以設定防火牆使用特定標籤名稱標記威脅日誌中的來源 IP 位址或來源使用者。然後，您可以使用這些標籤自動填入原則物件，例如動態使用者群組或動態地址群組，然後可以使用這些物件自動執行安全性、驗證或解密原則中的安全性動作。例如，當您在 **Credential Detected**（認證已偵測） 欄中為是建立 URL標籤篩選器時，可以將標籤套用於使用者，強制執行要求使用者使用多因素驗證 (MFA) 進行驗證的驗證原則。

動態使用者群組不支援從 *HIP* 比對日誌自動標記。

透過將 IP 位址-標籤和使用者-標籤的對應註冊到防火牆或 Panorama 上的 PAN-OS 整合式 User-ID 代理程式，或使用 HTTP 伺服器設定檔註冊到遠端 User-ID 代理程式，在您的網路上重新散佈對應。當您將逾時設定為日誌轉送設定檔的內建動作的一部分或日誌轉送設定的一部分時，防火牆可以自動移除（取消註冊）與 IP 位址或使用者關聯的標籤。例如，如果防火牆偵測到使用者的認證可能受到威脅，則可以將防火牆設定為在指定的時間段內要求對該使用者進行 MFA 驗證，然後設定逾時以將該使用者從 MFA 要求組中移除。

STEP 1 | 依據要用於標籤的日誌類型，請建立日誌轉送設定檔或設定日誌設定以定義希望防火牆或 Panorama 處理日誌的方式。

- 對於驗證、資料、威脅、流量、通道檢查，URL 和 WildFire 日誌，請建立日誌轉送設定檔。
- 對於 User-ID、GlobalProtect、IP-Tag 日誌，請設定日誌設定。

STEP 2 | 定義匹配清單準則，該準則確定防火牆或 Panorama 將標籤新增到原則物件的時間。

例如，您可以使用篩選器設定臨界值或定義一個值（例如 `user eq “unknown”` 用於識別防火牆尚未對應的使用者）；當防火牆達到該臨界值或找到該值時，防火牆將新增該標籤。

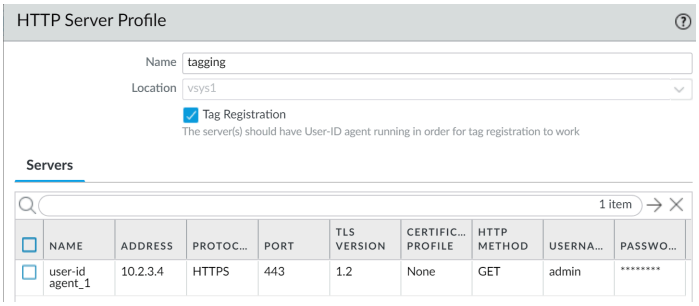
- 要建立日誌轉送設定檔，請 **Add**（新增）設定檔，然後選取要針對匹配清單準則監控的 **Log Type**（日誌類型）（ **Objects**（物件） > **Log Forwarding**（日誌轉送） ）。
- 要設定日誌設定，請 **Add**（新增）要針對匹配清單準則監控的日誌類型的日誌設定（**Device**（裝置） > **Log Settings**（日誌設定））。

STEP 3 | 複製並粘貼 **Filter**（篩選器） 值，或使用 **Filter Builder**（篩選建立器） 以定義標籤的匹配準則。

©2024 Palo Alto Networks, Inc.

STEP 4 | （僅遠端 User-ID ）設定 HTTP 伺服器設定檔以將日誌轉送到遠端 User-ID 代理程式。

1. 選取 **Device**（裝置） > **Server Profiles**（伺服器設定檔） > **HTTP**。
2. 為伺服器 **Add**（新增）設定檔並指定 **Name**（名稱）。
3. （僅限虛擬系統）選取 **Location**（位置）。該設定檔可由所有虛擬系統 **Shared**（共用），也可以屬於特定虛擬系統。
4. 選取 **Tag Registration**（標籤註冊），以允許防火牆使用遠端防火牆上的 User-ID 代理程式註冊 IP 位址與標籤對應。啟用標籤註冊後，您無法再指定裝載格式。
5. **Add**（新增）伺服器連線詳細資料，以存取遠端 User-ID 代理程式，然後按一下 **OK**（確定）。



6. 選取您建立的日誌轉送設定檔，然後選取此伺服器設定檔作為您 **Remote User-ID**（遠端 **User-ID**）標籤 **Registration**（註冊）的 HTTP 伺服器設定檔。

STEP 5 | 定義您想要向其套用標籤的原則物件。

1. 建立或選取以下政策物件之一：動態位址群組、在原則中使用動態使用者群組、位址、位址群組、區域、政策規則、服務或服務群組。
2. 輸入要套用於物件的標籤作為 **Match**（匹配）準則。

   確認標籤與步驟 4 中的標籤相同。

STEP 6 | 將帶標籤的原則物件新增至您的原則。

此工作流程使用安全性原則作為範例，但您也可以在驗證原則中使用帶標籤的原則物件。

1. 選取 **Policies**（原則） > **Security**（安全性）。
2. 按一下 **Add**（新增），然後輸入原則的 **Name**（名稱）和（選用） **Description**（說明）。
3. 新增流量來源的 **Source Zone**（來源區域）。
4. 新增流量終止的 **Destination Zone**（目的地區域）。
5. 選取您在第 5.1 步驟中建立的 **Source**（來源）物件。
6. 選取規則 **Allow**（允許）還是 **Deny**（拒絕）該流量。

STEP 7 | 如果設定日誌轉送設定檔，請將其指派至您的安全性原則。

您可以為每個原則分配一個日誌轉送設定檔，但可以為每個設定檔分配多個方法和動作。如需範例，請參閱在原則中使用動態位址群組。

©2024 Palo Alto Networks, Inc.

STEP 8 | **Commit**（提交）您的變更。

STEP 9 | （選用）設定逾時，以在經過指定時間後從原則物件中刪除標籤。

指定防火牆從原則物件中刪除標籤之前通過的時間（以分鐘為單位）。範圍為 0 至 43,200。如果將逾時設定為零，則 IP 位址到標籤的對應不會逾時，且必須使用明確動作將其移除。如果將逾時設定為最大值 43,200 分鐘，則防火牆將在 30 天後移除該標籤。

您無法使用 ***Remove Tag***（移除標籤）動作設定逾時。

1. 選取日誌轉送設定檔。
2. **Add**（新增）或編輯其中一項 **Built-in Actions**（內建動作）。
3. 指定 **Timeout**（逾時）（以分為單位）。經過指定的時間後，防火牆或 Panorama 會將該標籤刪除。

   將 *IP-tag IP* 逾時時間設為與該 *IP* 位址的 *DHCP* 租用逾時時間相同。這使得 *IP* 至標籤對應與 *DHCP* 租用同時到期，這樣您便不會在重新指派 *IP* 位址時無意套用原則。
4. 按一下 **OK**（確定）並 **Commit**（交付）變更。

©2024 Palo Alto Networks, Inc.

監控虛擬環境中的變更

若要在不斷出現新使用者與伺服器的環境中保護應用程式及防禦威脅，您的安全性原則必須相當靈活。若要靈活，防火牆必須能夠瞭解新的或已修改的 IP 位址，並一致地套用原則，無須變更防火牆上的組態。

為達成此目的，系統會協調防火牆上的 **VM** 資訊來源與動態位址群組功能。防火牆與 Panorama 會自動收集每一個所監控來源的虛擬機器 (或來賓) 詳細目錄，並建立與網路動態變更同步的原則物件。

- 啟用 VM 監控以追蹤虛擬網路變更
- 所監控的有關雲端平台中虛擬機器的屬性
- 在原則中使用動態位址群組

啟用 VM 監控以追蹤虛擬網路變更

VM 資訊來源會自動收集每一個所監控來源（主機）的虛擬機器 (VM) 詳細目錄相關資訊；防火牆會監控 VMware ESXi、vCenter Server、AWS-VPC、Microsoft Azure VNet 及 Google Cloud。部署或移動虛擬機器（來賓）時，防火牆會收集預先定義的屬性值（或中繼資料元素）作為標籤，這些標籤之後可用來定義動態位址群組（請參閱在原則中使用動態位址群組）並對照原則進行比對。

您可以直接設定防火牆或使用 Panorama 範本監控最多10個 VM 資訊來源。**VM Information Sources**（**VM** 資訊來源）可讓您輕鬆進行設定，並監控一組 16 個預先定義的中繼資料元素或屬性。請參閱所監控的有關雲端平台中虛擬機器的屬性，獲取清單。依預設，防火牆與所監控來源之間的流量會使用防火牆上的管理 (MGT) 連接埠。

- 當監控 *ESXi* 主機為 VM 系列 NSX 版本解決方案的一部分時，使用動態位址群組而非 *VM* 資訊來源來記住虛擬環境中的變更。對於 *VM* 系列 *NSX* 版本解決方案，*NSX Manager* 將為 *Panorama* 提供 *IP* 位址所屬 *NSX* 安全性群組的相關資訊。*NSX Manager* 提供的資訊為在動態位址群組中定義比對準則提供了完整內容，因為它將服務設定檔 *ID* 用作辨別屬性，並在不同的 *NSX* 安全性群組間擁有重疊 *IP* 位址時，允許您適當強制執行原則。最多 *32* 個標籤（來自 *vCenter* 伺服器與 *NSX* 管理員）可註冊至 *IP* 位址。
- 對於在 *Azure* 部署中監控虛擬機器而言，您需部署在 *Azure* 公共雲端中虛擬機器上執行的 VM 監控指令碼而非 *VM* 監控來源。此指令碼會收集 *Azure* 資產的 *IP* 位址至標籤對應資訊，並將其發佈至防火牆以及您在指令碼中指定的對應虛擬系統。
- 對於 *Panorama 8.1.3* 版及更高版本，您還可以使用 *AWS* 或 *Azure* 的 *Panorama* 外掛程式來擷取 *VM* 資訊並將其註冊到受管理的防火牆。如需詳細資料，請參閱所監控的有關雲端平台中虛擬機器的屬性。

STEP 1 | 啟用 VM 監控。

©2024 Palo Alto Networks, Inc.

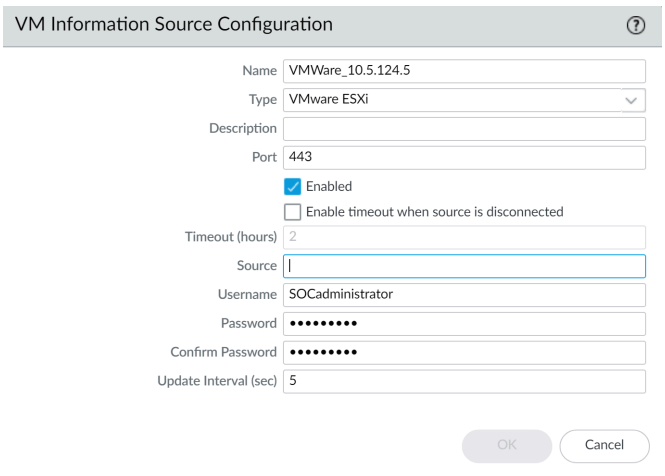
您可為每個防火牆或為具多虛擬系統功能的防火牆上的每個虛擬系統設定多達 *10* 個 *VM* 資訊來源。

若是在高可用性設定中設定防火牆：

- 在主動/被動設定中，只有主動防火牆會監控 VM 來源。
- 在主動/被動設定中，只有包含主要之優先順序值的防火牆會監控 VM 來源。

1. 選取 **Device**（裝置） > **VM Information Sources**（**VM** 資訊來源）。此範例向您展示如何新增 VMware ESX(i) 或 vCenter Server。
2. 按一下 **Add**（新增）並輸入下列資訊：
   - **Name**（名稱）用來識別您要監控的來源。
   - 選取 **Type**（類型）以表明來源是 **AWS VPC**、**Google Compute Engine**（**Goggle** 計算引擎）實例、**VMware ESX(i)** 伺服器還是 **VMware vCenter** 伺服器。

     所選類型確定所顯示的欄位。
   - 輸入來源正在接聽的 **Port**（連接埠）。
   - 若要變更預設值，請選取 **Enable timeout when the source is disconnected**（當來源中斷連線時啟用逾時）核取方塊並指定值。達到指定的限制、無法存取主機或主機未回應時，防火牆將關閉至來源的連線。
   - 將要驗證的認證 (**Username**（使用者名稱）與 **Password**（密碼）新增至上述指定的伺服器。
   - 定義 **Source**（來源）—主機名稱或 IP 位址。
   - （選用）將 **Update interval**（更新間隔）修改成在 5-600 秒之間的值。依預設，防火牆每 5 秒會輪詢一次。系會將 API 呼叫排入佇列中並每隔 60 秒擷取這些呼叫，因此更新花費的時間為 60 秒加上所設定的輪詢間隔。



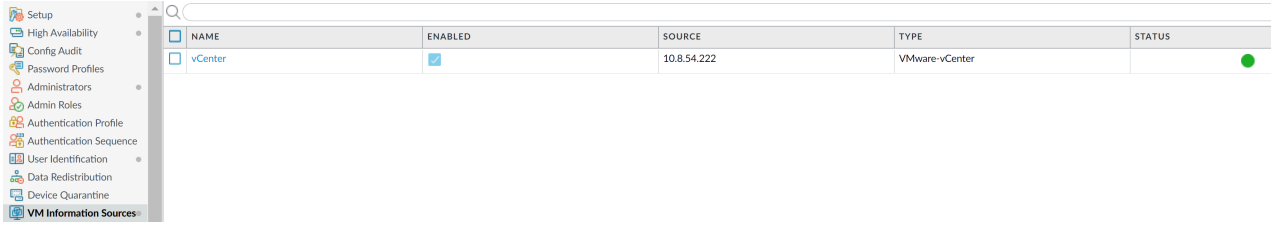
   - 按一下 **OK**（確定）並並 **Commit**（交付）變更。

 ©2024 Palo Alto Networks, Inc.

- 確認連線 **Status**（狀態）顯示為已連線。

STEP 2 | 確認連線狀態。

確認連線 **Status**（狀態）顯示為已連線。



如果連線狀態為擱置中或已中斷，請確認來源正在運作中，且防火牆也能存取來源。如果您使用非 MGT 連接埠的連接埠與監控的來源通訊，您必須變更服務路由（選取 **Device**（裝置） > **Setup**（設定） > **Services**（服務），按一下 **Service Route Configuration**（服務路由組態）連結，然後修改 **VM Monitor**（**VM** 監控）服務的 **Source Interface**（來源介面））。

所監控的有關雲端平台中虛擬機器的屬性

在私人雲端或公共雲端中佈建或移除虛擬機器時，您可以在新世代防火牆上使用 Panorama 外掛程式、VM 監控指令碼或 VM 資訊來源來監控虛擬環境中所部署之虛擬機器 (VM) 的相關變更。

VM 資訊來源—在硬體或 VM 系列防火牆上，您可以在佈建或修改受監控來源（AWS、ESXi 或 vCenter Server 或 AWS）上設定的來賓虛擬機器時，監控虛擬機器實例並擷取變更。對於每個防火牆及#或虛擬系統（若防火牆具有多個虛擬系統功能），您可最多設定 10 個來源。如需 VM 資訊來源與動態位址群組如何同步工作，以及讓您能夠監控虛擬環境中的變更的相關資訊，請參閱 VM-Series 部署指南。若是在高可用性設定中設定防火牆：

- 在主動/被動設定中，只有主動防火牆會監控 VM 資訊來源。
- 在主動/主動設定中，只有主要防火牆會監控 VM 資訊來源。

Panorama 外掛程式—在執行 8.1.3 版 Panorama 的硬體設備或虛擬設備上，您可以安裝適用於 Microsoft Azure 與 AWS 的外掛程式。該外掛程式允許您將 Panorama 連線到 Azure 公共雲端訂閱或 AWS VPC，並擷取虛擬機器之 IP 位址到標籤的對應。然後，Panorama 向已設定通知的受管理 Palo Alto Networks® 防火牆註冊 VM 資訊。

參閱以下章節，檢閱各雲端廠商所支援的選項，以及用以建立動態位址群組的可監控虛擬機器屬性：

- VMware ESXi
- Amazon Web Services (AWS)
- Microsoft Azure
- Google

 ©2024 Palo Alto Networks, Inc.

VMware ESXi

受監控的 ESXi 或 vCenter 伺服器上的每個 VM 必須已安裝並正在執行 VMware 工具。VMware 工具提供收集指派給每個 VM 之 IP 位址和其他值的能力。

當監控的 *ESXi* 主機為 *VM* 系列 *NSX* 版本解決方案的一部分時，使用動態位址群組（而非 *VM* 資訊來源）來記住虛擬環境中的變更。對於 *VM* 系列 *NSX* 版本解決方案，*NSX Manager* 將為 *Panorama* 提供 *IP* 位址所屬 *NSX* 安全性群組的相關資訊。*NSX Manager* 提供的資訊為在動態位址群組中定義比對準則提供了完整內容，因為它將服務設定檔 *ID* 用作辨別屬性，並在不同的 *NSX* 安全性群組間擁有重疊 *IP* 位址時，允許您適當強制執行原則。

最多 *32* 個標籤（來自 *vCenter* 伺服器與 *NSX* 管理員）可註冊至 *IP* 位址。

為了收集指派給受監控 VM 的值，請使用防火牆上的 VM 資訊來源來監控以下預先定義的 ESXi 屬性集：

VMware 來源上監控的屬性
UUID
名稱
來賓 OS
VM 狀態—電力狀態可為 poweredOff、poweredOn、standBy 和 unknown。
註釋
版本
網路—虛擬交換器名稱、連接埠群組名稱和 VLAN ID
容器名稱—vCenter 名稱、資料中心物件名稱、資源集區名稱、叢集名稱、主機、主機 IP 位址。

Amazon Web Services (AWS)

在 AWS VPC 中佈建或修改虛擬機器時，您有兩種方法可以監控這些實例並擷取標籤，用作動態位址群組中的比對準則。

- **VM** 資訊來源—在新世代防火牆上，您總共可監控多達 32 個標籤—14 個預先定義的標籤和 18 個使用者定義的鍵值組（標籤）。下列屬性（或標籤名稱）可作為動態位址群組的比對準則。
- **Panorama** 上的 **AWS** 外掛程式—AWS 專用 Panorama 外掛程式可讓您將 Panorama 連線至您的 AWS VPC，並擷取 AWS 虛擬機器的 IP 位址-標籤對應。然後，Panorama 向已設定通知的受管理 Palo Alto Networks® 防火牆註冊 VM 資訊。透過該外掛程式，Panorama 可為每個虛擬機器共擷取 32 個標籤，11 個預先定義標籤和多達 21 個使用者定義標籤。

©2024 Palo Alto Networks, Inc.

AWS-VPC 上監控的屬性	防火牆上的 VM 資訊來源	Panorama 上的 AWS 外掛程式
架構	是	否
來賓 OS	是	否。
AMI ID	是	是
IAM 實例設定檔	否。	是
實例 ID	是	否。
實例狀態	是	否。
實例類型	是	否。
金鑰名稱	是	是
擁有者 ID	否。	是
放置—租戶	是	是
放置—群組名稱	是	是
放置—可用性區域	是	是
私人 DNS 名稱	是	否。
公開 DNS 名稱	是	是
子網路 ID	是	是
安全性群組 ID	否。	是
安全性群組名稱	否	是
VPC ID	是	是
Tag (金鑰，值)	是； 支援多達 18 個使用者定義標籤。使用者定義的標籤按字母順序排序，前 18 個標籤可用於防火牆。	是； 支援多達 21 個使用者定義標籤。使用者定義的標籤按字母順序排序，前 21 個標籤可用於 Panorama 及防火牆。

©2024 Palo Alto Networks, Inc.

Microsoft Azure

對於 Azure 上的 VM 監控，您需要擷取 Azure VM 的 IP 位址-標籤對應，並使其用作動態位址群組中的比對規則。Microsoft Azure 專用 Panorama 外掛程式可讓您將 Panorama 連線至 Azure 公共雲端訂閱並擷取 Azure 虛擬機器的 IP 位址-標籤對應。Panorama 可擷取每台虛擬機器的總共 26 個標籤、11 預先定義標籤和最多 15 個使用者定義標籤，並可將 VM 資訊註冊到您已為通知設定的受管理 Palo Alto Networks® 防火牆。

使用 Azure 專用 Panorama 外掛程式，您可監控 Microsoft Azure 部署中的下列虛擬機器屬性組。

Microsoft Azure 上監控的屬性	**Panorama** 上的 **Azure** 外掛程式
VM 名稱	是
VM 大小	否
網路安全性群組名稱	是
作業系統類型	是
作業系統發行商	是
作業系統優惠	是
作業系統 SKU	是
子網路	是
VNet	是
Azure 區域	是
資源群組名稱	是
訂閱 ID	是
使用者定義的標籤	是 支援多達 15 個使用者定義標籤。使用者定義的標籤按字母順序排序，前 15 個標籤可用於 Panorama 及防火牆。

Google

透過使用新世代防火牆上的 VM 資訊來源，您可以監控以下預先定義的 Google 計算引擎 (GCE) 屬性集。

©2024 Palo Alto Networks, Inc.

高可用性在防火牆上不受支援。

Google 計算引擎上監控的屬性
VM 的主機名稱
機器類型
專案 ID
來源（作業系統類型）
STATUS （狀態）
子網路
VPC 網路

在原則中使用動態位址群組

動態位址群組在政策中使用。可讓您建立能因應變更—新增、移動或刪除伺服器—自動調整的原則。此外它也非常的彈性靈活，會根據標籤將不同的規則套用到同一個伺服器上；標籤會定義動態位址群組在網路、作業系統、及該群組所處理不同種類流量上的角色。

動態位址群組使用標籤作為篩選準則來決定其成員。篩選器使用邏輯的 *and* 與 *or* 運算子。所有符合篩選準則的 IP 位址或位址群組皆會成為動態位址群組的成員。您可以在防火牆上以靜態方式定義標籤，或以動態的方式向防火牆註冊標籤。靜態與動態標籤之間的差異是，靜態標籤是防火牆設定的一部分，動態標籤是執行階段設定的一部分。這意味著不需要提交即可更新動態標籤；但是標籤必須由在政策中參照的動態位址群組所使用，且政策必須在防火牆上提交。

若要動態註冊標籤，您可以使用防火牆上或 User-ID 代理程式上的 XML API 或 VM 監控代理程式。每個標籤都是在防火牆或 Panorama 上註冊的中繼資料元素或屬性值配對。例如，IP1 {tag1, tag2,.....tag32}，其中 IP 位址與相關聯的標籤皆以清單方式維護；每個已註冊的 IP 位址都會有多達 32 個標籤，例如其所屬的作業系統、資料中心或虛擬交換器。收到 API 呼叫後，防火牆會註冊 IP 位址與相關聯的標籤，並自動更新動態位址群組的成員資訊。

可為每個型號註冊的 IP 位址數目上限並不相同。下表列出了各型號的具體數目：

Model	動態註冊 IP 位址的數目上限
M-Series 與 Panorama 虛擬設備	500,000

©2024 Palo Alto Networks, Inc.

Model	動態註冊 IP 位址的數目上限
PA-5400 Series（PA-5450 除外）、PA-5200 Series、VM-7000 SMC-B Series	500,000
VM-500, VM-700	300,000
PA-3430、PA-3440、PA-3200 Series、VM-300	200,000
PA-3410、PA-3420	150,000
PA-7000 Series、PA-5450、PA-450、PA-460	100,000
PA-440	50,000
PA-850, VM-100	2,500
PA-820、PA-410、PA-220、VM-50	1,000

如果將 *IP* 組（如 *IP* 範圍或子網路）計入每個防火牆型號支援的最大註冊 *IP* 位址數，則將其視為單個註冊 *IP* 位址。

下列範例顯示動態位址群組如何簡化網路安全性的執行。範例工作流程顯示如何：

- 在防火牆上啟用 VM 監控代理程式，藉以監控 VMware ESX(i) 主機或 vCenter Server，及註冊 VM IP 位址與相關聯的標籤。
- 建立動態位址群組及定義要篩選的標籤。在此範例中會建立兩個位址群組。一個只會篩選動態標籤，另一個會篩選靜態與動態標籤以填入群組成員。
- 確認在防火牆上已填入動態位址群組的成員。
- 在政策中使用動態位址群組。此範例使用兩個不同的安全性政策：
  - 一是所有部署為 FTP 伺服器的 Linux 伺服器其安全性政策，此規則會在動態註冊的標籤上比對。
  - 另一是所有部署為網頁伺服器的 Linux 伺服器其安全性政策，此規則會在使用靜態與動態標籤的動態位址群組上比對。
- 確認當部署新的 FTP 或網頁伺服器時會更新動態位址群組的成員。這可確保也會在這些新的虛擬機器上強制執行安全性規則。

STEP 1 | 啟用 VM 來源監控。

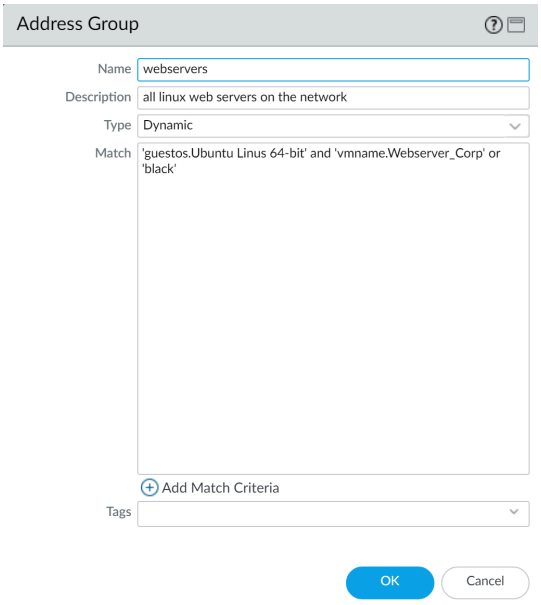
請參閱啟用 VM 監控以追蹤虛擬網路變更。

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 在防火牆上建立動態位址群組。

如需該功能的概況檢視，請參閱教學課程。

1. 登入防火牆的網頁介面。
2. 選取 **Object**（物件）> **Address Groups**（位址群組）。
3. 按一下 **Add**（新增），再輸入位址群組的 **Name**（名稱）和 **Description**（說明）。
4. 在 **Type**（類型）中選取 **Dynamic**（動態）。
5. 定義比對準則。您可以選取動態與靜態標籤作為比對準則，以填入群組的成員。按一下 **Add Match Criteria**（新增比對準則），選取 **And** 或 **Or** 運算式，選取您在篩選或比對時要對照的屬性，然後按一下 **OK**（確定）。不支援否定。

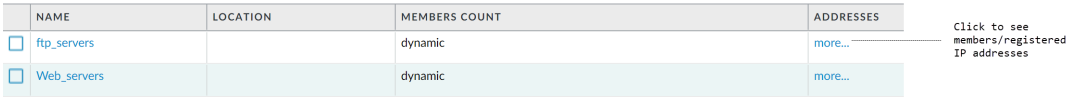


6. 按一下 **Commit**（交付）。

STEP 3 | 此範例中每個動態位址群組的比對準則如下所示：

ftp_server：在來賓作業系統「Linux 64-bit」上比對，並加上「ftp」註解 ('guestos.Ubuntu Linux 64-bit' and 'annotation.ftp')。

web-servers：對照兩個準則比對—黑色標籤，或如果來賓作業系統為 64 位元的 Linux，且伺服器使用的名稱為 Web_server_Corp。('guestos.Ubuntu Linux 64-bit' and 'vmname.WebServer_Corp' or 'black')



 ©2024 Palo Alto Networks, Inc.

STEP 4 | 在政策中使用動態位址群組。

檢視教學課程。

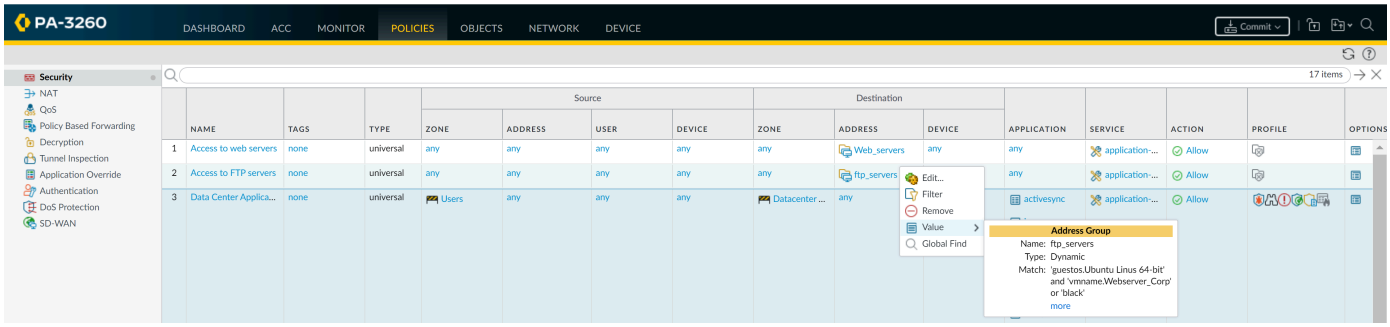
1. 選取 **Policies**（政策） > **Security**（安全性）。
2. 按一下 **Add**（新增），然後輸入原則的 **Name**（名稱）和 **Description**（說明）。
3. 新增 **Source Zone**（來源區域）以指定流量來源於哪個區域。
4. 新增流量將終止於哪個 **Destination Zone**（目的地區域）。
5. 對於 **Destination Address**（目的地位址），請選取您剛才建立的動態位址群組。
6. 針對流量指定動作—**Allow**（允許）或 **Deny**（拒絕），並選擇性地將預設安全性設定檔附加至規則。
7. 重複步驟 1 到 6，建立另一個政策規則。
8. 按一下 **Commit**（交付）。

STEP 5 | 此範例顯示如何建立兩個原則：一個用來存取所有的 FTP 伺服器，另一個用來存取 Web 伺服器。

	NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTI
1	Access to web servers	none	universal	any	any	any	any	any	Web_servers	any	any	application-...	Allow		
2	Access to FTP servers	none	universal	any	any	any	any	any	ftp_servers	any	any	application-...	Allow		

STEP 6 | 確認在防火牆上已填入動態位址群組的成員。

1. 選取 **Policies**（政策） > **Security**（安全性），然後選取規則。
2. 選取位址群組連結旁的下拉箭頭，再選取 **Value**（值）。您也可以驗證比對準則是否正確。



3. 按一下 **more**（更多）連結，並確認出現已註冊的 IP 位址清單。

   將為此位址群組的所有 IP 位址強制執行原則，並在此處顯示。

如果要刪除所有註冊的 *IP* 位址，請使用*CLI*命令 ***debug object registered-ip clear all***，然後在清除標籤後重新啟動防火牆。

©2024 Palo Alto Networks, Inc.

動態 IP 位址與標籤的 CLI 命令

防火牆與 Panorama 上的命令列介面可讓您詳細檢視動態註冊的標籤與 IP 位址所來自不同的來源。它也可以讓您稽核已註冊與未註冊的標籤。下列範例說明 CLI 的功能。

範例	CLI 命令
檢視符合 `state.poweredOn` 標籤或未加上 `vSwitch0` 標籤的所有已註冊 IP 位址。	**show log iptag tag_name equal state.poweredOn** **show log iptag tag_name not-equal switch.vSwitch0**
檢視其來源是名稱為 `vmware1` 的 VM 資訊來源且已加上 `poweredOn` 標籤的所有動態註冊的 IP 位址。	**show vm-monitor source source-name vmware1 tag state.poweredOn registered-ip all** registered IP Tags ---------- ---------- ---------- fe80::20c:29ff:fe69:2f76 "state.poweredOn" 10.1.22.100 "state.poweredOn" 2001:1890:12f2:11:20c:29ff:fe69:2f76"state.poweredOn" fe80::20c:29ff:fe69:2f80 "state.poweredOn" 192.168.1.102 "state.poweredOn" 10.1.22.105 "state.poweredOn" 2001:1890:12f2:11:2cf8:77a9:5435:c0d"state.poweredOn" fe80::2cf8:77a9:5435:c0d "state.poweredOn"
清除從特定 VM 監控來源得知的所有 IP 位址與標籤，但不中斷來源連線。	**debug vm-monitor clear source-name *<name>***
顯示自所有來源註冊的 IP 位址。	**show object registered-ip all**
顯示自所有來源註冊的 IP 位址計數。	**show object registered-ip all option count**
清除自所有來源註冊的 IP 位址	**debug object registered-ip clear all**

©2024 Palo Alto Networks, Inc.

範例	CLI 命令
新增或刪除使用 XML API 註冊的指定 IP 位址其標籤。	**debug object registered-ip test [<register/unregister>] <ip/netmask><tag>**
檢視自特定資訊來源註冊的所有標籤。	**show vm-monitor source source-name vmware1 tag all** vlanId.4095 vswitch.vSwitch1 host-ip.10.1.5.22 portgroup.TOBEUSED hostname.panserver22 portgroup.VM Network 2 datacenter.ha-datacenter vlanId.0 state.poweredOn vswitch.vSwitch0 vmname.Ubuntu22-100 vmname.win2k8-22-105 resource-pool.Resources vswitch.vSwitch2 guestos.Ubuntu Linux 32-bit guestos.Microsoft Windows Server 2008 32-bit annotation. version.vmx-08 portgroup.VM Network vm-info-source.vmware1 uuid.564d362c-11cd-b27f-271f-c361604dfad7 uuid.564dd337-677a-eb8d-47db-293bd6692f76 Total:22
檢視自特定資料來源註冊的所有標籤，例如自防火牆上的 VM 監控代理程式、XML API、Windows User-ID 代理程式或 CLI。	• 若要檢視自 CLI 註冊的標籤： **show log iptag datasource_type equal unknown** • 若要檢視自 XML API 註冊的標籤： **show log iptag datasource_type equal xml-api** • 若要檢視自 VM 資訊來源註冊的標籤： **show log iptag datasource_type equal vm-monitor** • 若要檢視自 Windows User-ID 代理程式註冊的標籤： **show log iptag datasource_type equal xml-api datasource_subtype equal user-id-agent**

©2024 Palo Alto Networks, Inc.

範例	CLI 命令
檢視為特定 IP 位址 (在所有來源之間) 註冊的所有標籤。	`debug object registered-ip show tag-source ip ip_address tag all`

©2024 Palo Alto Networks, Inc.

對上游裝置後的端點和使用者強制執行原則

如果您在網路上的使用者與防火牆之間部署了上游裝置（例如明確 Proxy 伺服器或負載平衡），防火牆會將上游裝置 IP 位址視為 Proxy 所轉送 HTTP/HTTPS 流量中的來源 IP 位址，而非要求內容之用戶端的 IP 位址。在許多情況下，上游裝置會將 X-Forwarded-For (XFF) 標頭新增到包含用戶端（已請求內容或發起請求）實際 IPv4 或 Ipv6 位址的 HTTP 請求。

在這種情況下，您可以將防火牆設定為從 XFF 欄位中擷取 IP 位址，並將其對應到具有 User-ID 的使用者，或基於 IP 位址套用安全性原則。

- 在 **User-ID** 中使用 **X-Forwarded-For** 標頭—透過這一點，您可執行以使用者為基礎的原則，為 Proxy 伺服器後的使用者安全啟用 Web 應用程式的存取。此外，如果 User-ID 可將 XFF IP 位址對應至使用者名稱，防火牆會在流量、威脅、WildFire 提交以及 URL 篩選日誌中將此使用者名稱顯示為來源使用者，以針對 Proxy 後的使用者的 Web 活動提供可見度。
- 在安全性原則中使用 **X-Forwarded-For** 標頭—這讓您能夠使用 HTTP 標頭的 XFF 欄位中的 IP 位址基於來源 IP 位址來強制執行安全性原則。此外，將原則套用至包含 XFF 欄位中 IP 位址的流量時，您可以設定流量、威脅、資料篩選和 Wildfire 提交日誌，以幫助進行疑難排解和修復。

為了確保攻擊者無法讀取及利用 Web 要求封包 (這些封包會離開防火牆以從外部伺服器擷取內容) 中的 XFF 值，您也可以設定防火牆來從傳出封包除去 XFF 值。對 User-ID 或在原則中使用使用 XFF IP 位址和去除 XFF 值並非互相排斥：如果您設定這兩個選項，防火牆僅在將其用於原則執行與日誌記錄之後才會將 XFF 值調整為零。

您不能將防火牆設定為在 *User-ID* 的 *XFF* 欄位和安全性原則中同時使用 *IP* 位址。

- 將 XFF 值用於原則與日誌來源使用者
- 在安全性原則和記錄中使用 XFF IP 位址值
- 使用 XFF 標頭中的 IP 位址疑難排解事件

基於來源使用者將 XFF 值用於原則

您可將防火牆設定為使用 User-ID 將 XFF 標頭中的 IP 位址對應至使用者名稱，以便您可瞭解 Proxy 伺服器之後無法識別之使用者的 Web 流量，並可採用以使用者為基礎的原則來控制這些流量。若要將 XFF 標頭中的 IP 位址對應至使用者名稱，首先必須啟用 User-ID。

啟用此選項後，防火牆僅會將 XFF 標頭中的 IP 位址用於使用者對應。防火牆所記錄的來源 IP 位址仍然為 Proxy 伺服器的 IP 位址，並非來源使用者的 IP 位址。如果您看到歸因於使用者的日誌事件（防火牆已使用從 XFF 標頭中擷取的 IP 位址對這位使用者進行對應處理），可能會難以追蹤與事件相關的特定裝置。若要針對歸因於 Proxy 伺服器後之使用者的事件簡化偵錯與疑難排解，您還必須設定防火牆，以使用 XFF 標頭中的 IP 位址填入 URL 篩選日誌中的 X-Forwarded-For 欄，以便您可追蹤與日誌事件（與 URL 篩選日誌項目關聯）相關的特定使用者與裝置。

©2024 Palo Alto Networks, Inc.

Proxy 伺服器新增的 XFF 標頭，必須包含發起請求之一般使用者的來源 IP 位址。若標頭包含多個 IP 位址，則防火牆僅會使用第一個 IP 位址。如果標頭包含的資訊並非 IP 位址，防火牆將無法執行使用者對應。

啟用防火牆以使用 *X-Forwarded-For* 標頭來執行使用者對應，不會將防火牆設定為使用 *XFF* 標頭中的用戶端 *IP* 位址作為日誌中的來源位址；日誌中仍然會將 *Proxy* 伺服器的 *IP* 位址顯示為來源位址。但是，為簡化偵錯與疑難排解流程，您可將防火牆設定為將 XFF 值新增至 URL 篩選日誌，在 *URL* 篩選日誌中顯示 *XFF* 標頭中的用戶端 *IP* 位址。

STEP 1 | 啟用防火牆來在原則與日誌的來源使用者欄位中使用 XFF 值。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Content-ID**，然後編輯 X-Forwarded-For 標頭設定。
2. 選擇 **Enabled for User-ID**（為 **User-ID** 啟用）以便為 User-ID **Use X-Forwarded-For Header**（使用 **X-Forwarded-For** 標頭）。

STEP 2 | 從傳出 Web 要求移除 XFF 值。

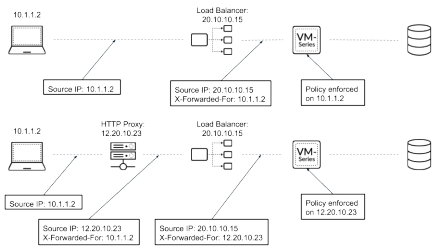
1. 選取 **Strip X-Forwarded-For Header**（除去 **X-Forwarded-For** 標頭）。
2. 按一下 **OK**（確定）與 **Commit**（提交）。

STEP 3 | 確認防火牆正在填入日誌的來源使用者欄位。

1. 選取擁有來源使用者欄位的日誌類型（例如，**Monitor**（監控） > **Logs**（日誌） > **Traffic**（流量））。
2. 確認 Source User（來源使用者）欄顯示存取 Web 應用程式之使用者的使用者名稱。

在安全性原則和記錄中使用 XFF IP 位址值

您可以將防火牆設定為使用 X-Forwarded-For (XFF) HTTP 標頭欄位中的來源 IP 位址來強制執行安全性政策。如果封包在到達防火牆之前通過單個 Proxy 伺服器，XFF 欄位將包含原始端點的 IP 位址。但是，如果封包通過多個上游裝置，則防火牆將使用最近新增的 IP 位址來強制執行政策或使用其他依賴 IP 資訊的功能。



- 在原則中使用 XFF 值
- 在日誌中顯示 XFF 值
- 在報告中顯示 XFF 值

©2024 Palo Alto Networks, Inc.

在原則中使用 XFF 值

請完成以下程序以使用 XFF 標頭中的用戶端 IP 位址強制執行安全性政策。

在 *Microsoft Azure* 中，依預設，應用程式閘道會將原始來源 *IP* 位址和連接埠插入 *XFF* 標頭中。要在防火牆上的原則中使用 *XFF* 標頭，必須將應用程式閘道設定為忽略 *XFF* 標頭中的連接埠。如需詳細資訊，請參閱 Azure文件。

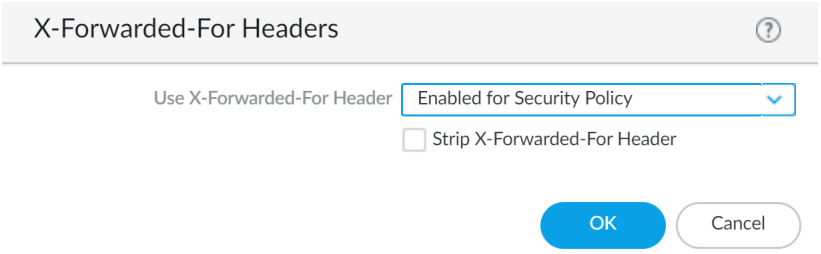
STEP 1 | 登入防火牆。

STEP 2 | 選取 **Device**（裝置） > **Setup**（設定） > **Content-ID** > **X-Forwarded-For Headers**（**X-Forwarded-For** 標頭）。

STEP 3 | 按一下編輯圖示。

STEP 4 | 從 **Use X-Forwarded-For Header**（使用 **X-Forwarded-For** 標頭）下拉式功能表中選取 **Enabled for Security Policy**（為安全性原則啟用）。

您不能同時啟用「為安全性政策使用 *X-Forwarded-For* 標頭」和 *User-ID*。



STEP 5 | （選用）選取 **Strip X-Forwarded-For Header**（除去 **X-Forwarded-For** 標頭）以從傳出的 HTTP 要求中移除 XFF 欄位。

選取此選項不會停用 XFF 標頭。防火牆在使用 XFF 欄位來強制執行政策并記錄 IP 位址後，會從用戶端要求中除去 XFF 欄位。

STEP 6 | 按一下 **OK**（確定）。

STEP 7 | **Commit**（提交）您的變更。

在日誌中顯示 XFF 值

除了在安全性政策中使用 XFF 標頭外，您還可以在各種日誌、報告和應用程式控管中 (ACC) 中檢視 XFF IP 位址，以幫助進行監控和疑難排解。您可以將 X-Forwarded-For 欄新增到流量、威脅、資料篩選和 WildFire 提交日誌。

對於非 *URL* 篩選日誌，僅當未啟用封包擷取時才支援 *XFF IP* 日誌記錄。

©2024 Palo Alto Networks, Inc.

如果防火牆偵測到需要重設動作 (***reset-client, reset-server, or reset-both***) 的威脅並且最後檢查的封包不包含 *XFF* 標頭，則 *X-Forwarded-For IP* 欄不顯示值。

要在您的日誌中檢視 XFF IP 位址，請完成以下步驟。

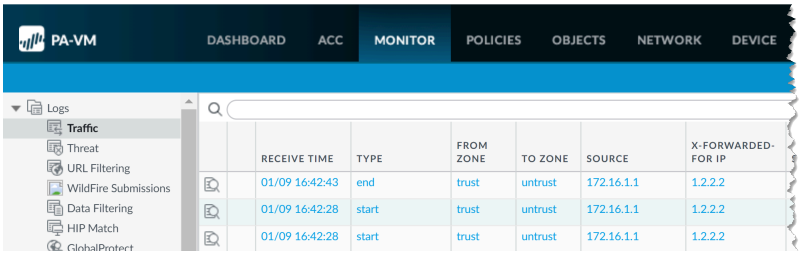
STEP 1 | 登入防火牆。

STEP 2 | 選取 **Monitoring**（監控） > **Logs**（日誌）。

STEP 3 | 選取 **Traffic**（流量）、**Threat**（威脅）、**Data Filtering**（資料篩選）或 **Wildfire Submissions**（**Wildfire** 提交）。

STEP 4 | 按一下任何欄標頭右側的箭頭，然後選取 **Columns**（欄）。

STEP 5 | 選取 **X-Forwarded-For IP** 以在您的日誌中顯示 XFF IP。



在報告中顯示 XFF 值

防火牆產生的預先定義報告不包含 XFF 值。但是，防火牆具有包含 XFF 資訊的內建報告範本。若要檢視報告中的 XFF IP 位址，請按照步驟使用內建範本產生報告。

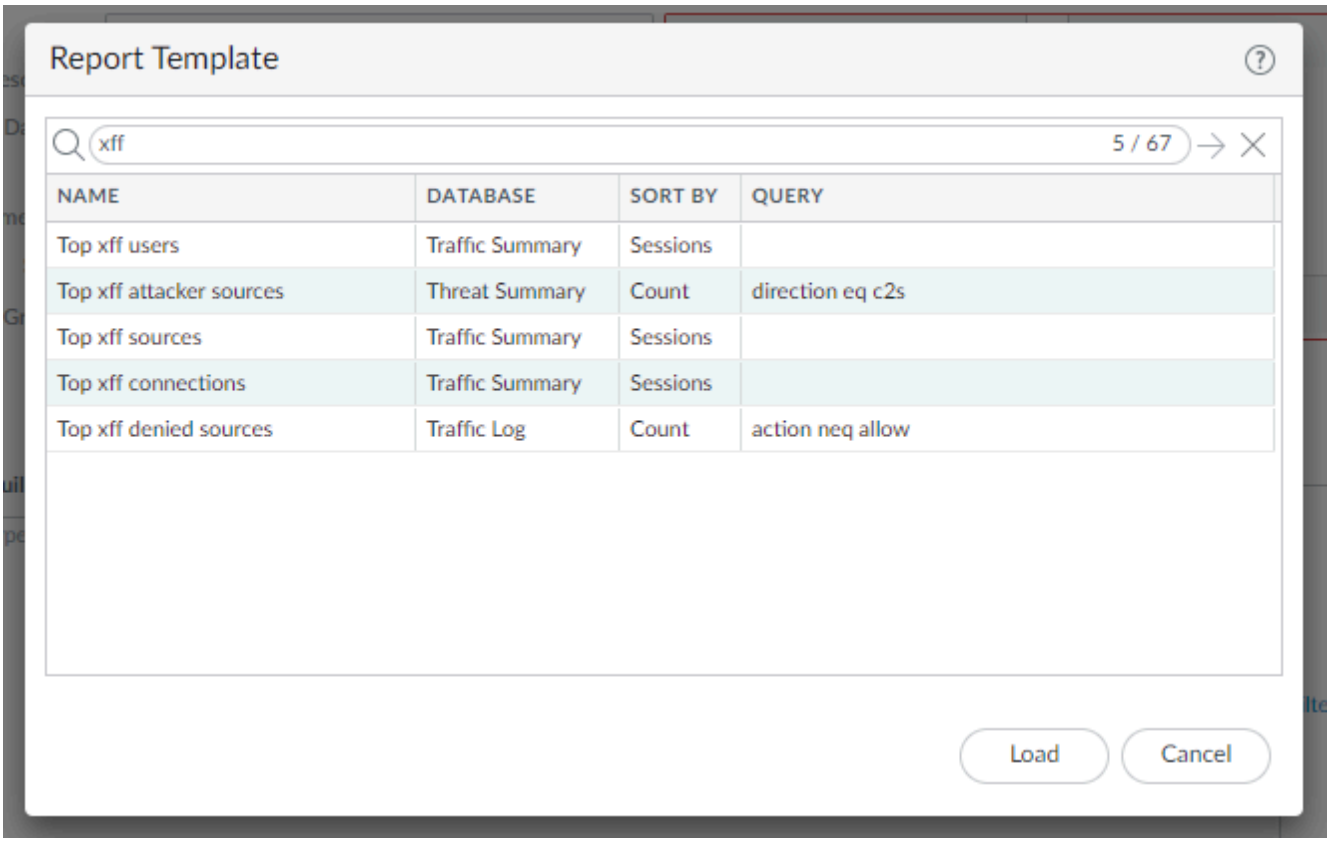
STEP 1 | 登入防火牆。

STEP 2 | 選取 **Monitor**（監控） > **Manage Custom Reports**（管理自訂報告） > **Add**（新增）。

STEP 3 | 按一下 **Load Template**（載入範本）。

©2024 Palo Alto Networks, Inc.

STEP 4 | 將 XFF 輸入搜尋列中，按一下搜尋按鈕以找到內建 XFF 報告範本。



STEP 5 | 按一下 **Load**（載入）。

STEP 6 | 設定您的自訂報告。按一下 **Time Frame**（時間範圍）、**Sort By**（排序方式）和 **Group By**（分組方式），以最符合您需求的方式顯示 XFF 資訊。

STEP 7 | （選用）除根據 **Scheduled Time**（排程時間）外，還可以視需要按一下 **Run Now**（立即執行）以產生報告。

使用 XFF 標頭中的 IP 位址疑難排解事件

依預設，防火牆不會記錄 Proxy 伺服器後用戶端的來源位址，即便您使用這一來自 X-Forwarded-For (XFF) 標頭的位址進行使用者對應。因此，雖然您可識別與日誌事件相關的特定使用者，但是您無法輕易識別產生日誌事件的來源裝置。為簡化 Proxy 伺服器後之使用者事件的偵錯與疑難排解，請在 URL 篩選設定檔（您將此設定檔附加至允許存取 Web 式應用程式的安全性政策規則中）中啟用 X-Forwarded-For 選項。啟用此選項後，防火牆將來自 XFF 標頭的 IP 位址記錄為所有與規則相符之流量的來源位址。

URL 篩選日誌不會顯示 *X-Forwarded For IP*（*X* 轉送針對 - *IP*）欄位。若要檢視 *X-Forwarded-For IP* 日誌事件，您必須將日誌匯出為 *CSV* 格式。

©2024 Palo Alto Networks, Inc.

啟用防火牆以使用 *XFF* 標頭作為 *URL* 篩選日誌中的來源位址，不會啟用來源位址的使用者對應。若要填入來源使用者欄位，請參閱將 XFF 值用於原則和記錄來源使用者。

STEP 1 | 在 URL 篩選設定檔中啟用 X-Forwarded-For 選項。

1. 選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **URL Filtering**（**URL** 篩選），並選取您要設定的 URL 篩選設定檔，或者新增新的篩選設定檔。

   您無法在預設 *URL* 篩選設定檔中啟用 *XFF* 日誌記錄。

2. 選取 **URL Filtering Settings**（**URL** 篩選設定）頁籤，然後啟用 **X-Forwarded-For**。
3. 按一下 **OK**（確定）來儲存設定檔。

STEP 2 | 將 URL 篩選設定檔附加至允許存取 Web 應用程式的安全性政策規則。

1. 選取 **Policies**（原則） > **Security**（安全性），然後按一下規則。
2. 選取 **Actions**（動作）頁籤，將 **Profile Type**（設定檔類型）設定為 **Profiles**（設定檔），然後選取您剛剛為 X-Forwarded-For HTTP 標頭記錄設定的 **URL Filtering**（**URL** 篩選）設定檔。
3. 按一下 **OK**（確定）與 **Commit**（提交）。

STEP 3 | 確認防火牆正在記錄 XFF 值。

XFF 欄在防火牆的 *URL* 篩選日誌中看不到。

1. 選取 **Monitor**（監控） > **Logs**（日誌） > **URL Filtering**（**URL** 篩選）。
2. 以下列其中一種方式檢視 XFF 值：
   - 按一下 Export to CSV（匯出至 CSV）()，以將 URL 篩選日誌匯出為逗號分隔值檔案。下載完成後，按一下 **Download file**（下載檔案）以將檔案複本儲存至本機裝置。
   - 使用 **`show log url csv-output equal yes`** CLI 命令。

©2024 Palo Alto Networks, Inc.

STEP 4 | 使用 URL 篩選日誌中的 XFF 欄位，來對另一種日誌類型中的日誌事件進行疑難排解。

如果您注意到與 HTTP/HTTPS 流量關聯的事件，但因為它是 Proxy 伺服器的來源 IP 位址而無法識別，則可以在關聯的 URL 篩選日誌中使用 X-Forwarded-For 值，以協助您識別與日誌事件關聯的來源位址。為此：

1. 在 Traffic（流量）、Threat（威脅）或 WildFire 提交日誌中找到您要調查的將 Proxy 伺服器的 IP 位址顯示為來源位址的事件。
2. 按一下日誌的望遠鏡圖示，以顯示其詳細資訊，並在 Detailed Log Viewer（詳細日誌檢視器）視窗的底部尋找相關的 URL 篩選日誌。
3. 將相關聯的 URL 篩選日誌匯出至 CSV 檔案，並尋找 X-Forwarded For IP（X 轉送針對 - IP）欄。此欄中的 IP 位址代表 Proxy 伺服器後來源使用者的 IP 位址。使用此 IP 位址來追蹤觸發您調查之事件的裝置。

©2024 Palo Alto Networks, Inc.

基於原則的轉送

一般而言，防火牆會使用封包中的目的地 IP 位址來決定傳出介面。防火牆會使用與介面所連線之虛擬路由器相關聯的路由表來執行路由查閱。基於原則的轉送 (PBF) 可讓您覆寫路由表，並根據如來源或目的地 IP 位址或流量類型等特定參數，來指定傳出或輸出介面。

- PBF
- 建立基於原則的轉送規則
- 使用案例：有雙 ISP 之輸出存取的 PBF

PBF

PBF 規則允許流量從路由表中指定的下一躍點取得替代路徑，基於安全或效能考量，PBF 規則一般用於指定輸出介面。讓我們假設您的公司在總公司與分公司之間有兩個連結：一是較便宜的網際網路連結，另一是較昂貴的租用線路。租用線路是高頻寬、低延遲的連結。若要增強安全性，您可以使用 PBF 透過私人租用線路傳送非加密流量（例如 FTP 流量）的應用程式，所有其他流量則透過網際網路連結傳送。或者若要增強效能，您可以選擇透過租用線路路由關鍵業務應用程式，並透過較便宜的連結傳送所有其他的流量，如瀏覽網頁。

- 輸出路徑與對稱傳回
- PBF 的路徑監控
- PBF 中服務與應用程式的比較

輸出路徑與對稱傳回

您可以使用 PBF 將流量導向至防火牆上特定的介面、丟棄流量，或將流量導向至另一個虛擬系統 (已啟用多虛擬系統的系統上)。

在路由不對稱的網路中，例如雙 ISP 環境，當流量到達防火牆上的某個介面，卻從另一個介面離開時，會發生連線問題。如果路由不對稱，也就是轉送 (SYN 封包) 與傳回 (SYN/ACK) 路徑不同，則防火牆會無法追蹤整個工作階段的狀態，並造成連線失敗。若要確保流量使用對稱路徑，亦即流量會到達建立工作階段所在的介面，並從同一個介面離開，您可以啟用 *Symmetric Return*（對稱傳回）選項。

透過對稱傳回，虛擬路由器會取代傳回流量的路由查閱，改為將流量導向回其擷取 SYN 封包 (或第一個封包) 的 MAC 位址。但如果目的地 IP 位址與輸入/輸出介面的 IP 位址位在同一個子網路上，則會執行路由查閱，且不會強制執行對稱傳回。此行為會防止無訊息丟棄流量。

為決定對稱傳回的下一躍點，防火牆會使用位址解析通訊協定 *(ARP)* 表。此 *ARP* 表格支援的項目數目上限受到防火牆型號限制，且使用者無法設定此值。若要判斷您型號的限制，請使用 *CLI* 命令：***show pbf return-mac all***。

©2024 Palo Alto Networks, Inc.

PBF 的路徑監控

路徑監控可讓您驗證 IP 位址連線，讓防火牆可以視需要透過替代路由來導向流量。防火牆會使用 ICMP 偵測作為活動訊號，以確認可以連線至指定的 IP 位址。

監控設定檔可讓您指定活動訊號數目的臨界值，來判斷是否可連線至該 IP 位址。當無法連線至所監控的 IP 位址時，您可以停用 PBF 規則，或指定容錯移轉或等待復原動作。停用 PBF 規則可允許虛擬路由器接管路由決策。採取容錯移轉或等待復原動作時，監控設定檔會繼續監控是否可達到目標 IP 位址，當它恢復時，防火牆會還原為使用原始路由。

下表列出新工作階段與已建立工作階段之間路徑監控失敗時的行為差異。

監控失敗時工作階段的行為	當無法連線至所監控的 **IP** 位址時，如果規則保持為啟用	當無法連線至所監控的 **IP** 位址時，如果規則為停用
對於已建立的工作階段	等待復原—繼續使用在 PBF 規則中指定的輸出介面。	等待復原—繼續使用在 PBF 規則中指定的輸出介面。
	容錯移轉—使用由路由表（非 PBF）決定的路徑。	容錯移轉—使用由路由表（非 PBF）決定的路徑。
對於新的工作階段	等待復原—使用由路由表（非 PBF）決定的路徑。	等待復原—檢查剩餘的 PBF 規則。如果沒有符合的項目，則使用路由表
	容錯移轉—使用由路由表（非 PBF）決定的路徑。	容錯移轉—檢查剩餘的 PBF 規則。如果沒有符合的項目，則使用路由表

PBF 中服務與應用程式的比較

PBF 規則會套用到第一個封包 (SYN) 或對第一個封包的第一個回應 (SYN/ACK)。這表示在防火牆有足夠的資訊可判斷應用程式前即會套用 PBF 規則。因此不建議將應用程式特定的規則與 PBF 搭配使用。只要有可能，請使用服務物件，亦即通訊協定或應用程式所使用的 Layer 4 連接埠 (TCP 或 UDP)。

但如果您在 PBF 規則中指定某個應用程式，防火牆會執行 *App-ID* 快取。當應用程式第一次通過防火牆時，防火牆沒有足夠的資訊可識別應用程式，因此無法執行 PBF 規則。隨著到達的封包愈多，防火牆便能判斷應用程式、在 App-ID 快取中建立項目，並為工作階段保持此 App-ID。當以相同的目的地 IP 位址、目的地連接埠與通訊協定 ID 建立新的工作階段時，防火牆便能識別出該應用程式來自相同的初始工作階段 (根據 App-ID 快取) 並套用 PBF 規則。因此，系統會根據 PBF 規則轉送未完全相同且不是同一個應用程式的工作階段。

此外，隨著防火牆收到愈多的封包，應用程式便有相依性，應用程式的識別會變更。由於 PBF 會在工作階段開始時進行路由決策，因此防火牆無法強制執行應用程式識別變更。例如，YouTube 一開始為網頁瀏覽，但隨後會根據網頁中包含的各種連結或視訊而變更為 Flash、RTSP 或

 ©2024 Palo Alto Networks, Inc.

YouTube。但使用 PBF 時，由於防火牆會在工作階段開始時將應用程式視為網頁瀏覽，因此之後無法辨識應用程式中的變更。

您不能在 *PBF* 規則中設定自訂應用程式、應用程式篩選器或應用程式群組。

建立基於原則的轉送規則

使用 PBF 規則可將流量導向至防火牆上特定的輸出介面，並取代流量的預設路徑。

在設定 PBF 規則之前，確保您瞭解 IPv4 位址集會被視為 IPv6 位址集的子集，原則中對此進行了詳細說明。

©2024 Palo Alto Networks, Inc.

STEP 1 | 建立基於原則的轉送(PBF)規則。

建立 PBF 規則時，您必須指定規則的名稱、來源區域或介面，以及輸出介面。所有其他的元件為選用或具有預設值。

您可以使用 *IP* 位址、位址物件或 *FQDN* 指定來源和目的地位址。

1. 選取 **Policies**（原則） > **Policy Based Forwarding**（基於原則的轉送），然後 **Add** （新增）PBF 原則規則。
2. 為規則設定描述性名稱（**General**（一般））。
3. 選取 **Source**（來源）並設定以下選項：
   1. 選取您將套用轉送原則的 **Type**（類型）（**Zone**（區域）或 **Interface**（介面）），並指定相關的區域或介面。如果您要強制執行對稱傳回，則必須選取來源介面。

      僅 *Layer 3* 介面支援 *PBF*；回送介面不支援 *PBF*。
   2. （選用）指定將套用 PBF 規則的 **Source Address**（來源位址）。例如，您想要將特定 IP 位址或子網路 IP 位址 (即為來源位址) 的流量轉送至此規則中指定的介面或區域。

      按一下 ***Negate***（否定）以執行 *PBF* 規則中的一個或多個 ***Source Address***（來源位址）。例如，如果 *PBF* 規則會將指定區域的所有流量導向至網際網路，***Negate***（否定）可讓您將內部 *IP* 位址自 *PBF* 規則中排除。

      評估順序為由上到下。依據符合定義準則的第一條規則比對封包；在觸發配對後，將不會評估後續的規則。
   3. （選用）**Add**（新增）並選取要套用原則的 **Source User**（來源使用者）或使用者群組。
4. 選取 **Destination/Application/Service**（目的地/應用程式/服務），並設定下列選項：
   1. **Destination Address**（目的地位址）—依預設，規則會套用到 **Any**（任意） IP 位址。按一下 **Negate**（否定）以執行 PBF 規則中的一個或多個目的地 IP 位址。
   2. **Add**（新增）您要使用 PBF 控制的任何**Application**（應用程式）和 **Service**（服務）。

      我們不建議將特定於應用程式的規則與 *PBF* 搭配使用，因為 *PBF* 規則可能會在防火牆有足夠的資訊判斷應用程式前套用。只要有可能，請使用服務物件，亦即通訊協定或應用程式所使用的 *Layer 4* 連接埠 *(TCP* 或 *UDP)*。如需詳細資訊，請參閱 PBF 中服務與應用程式的比較。

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 指定與規則相符的封包轉送方式。

如果在多 VSYS 的環境中設定 PBF，您必須為每個虛擬系統建立單獨的 *PBF* 規則（並建立相應的安全性原則規則，以啟用流量）。

1. 選取 **Forwarding**（轉送）。
2. 設定比對封包時要執行的 **Action**（動作）：
   - **Forward**（轉送）—將封包導向至指定的 **Egress Interface**（輸出介面）。
   - **Forward to VSYS**（轉送至 **VSYS**）（在已啟用多虛擬系統的防火牆上）—選取要將封包轉送到哪一個虛擬系統。
   - **Discard**（丟棄） — 丟棄封包。
   - **No PBF**（非 **PBF**） — 排除符合在規則中所定義來源、目的地、應用程式或服務準則的封包。比對封包時會使用路由表，而非 PBF；防火牆會使用路由表將符合的流量從重新導向的連接埠中排除。
3. 若要每日、每週或以非週期性頻率來觸發指定的 **Action**（動作），請建立並附加 **Schedule**（排程）。
4. 對於 **Next Hop**（下一個躍點），選取以下任何項：
   - **IP Address**（**IP** 位址） — 輸入 IP 位址或選取類型為 IP 網路遮罩的位址物件，而防火牆會將相符封包轉送到該物件。IPv4 位址物件須具有 /32 網路遮罩，而 IPv6 位址物件須具有 /128 網路遮罩。
   - **FQDN**—輸入 FQDN（或選取或建立類型為 FQDN 的位址物件），防火牆會將相符封包轉送到該物件。FQDN 可以解析為 IPv4 位址、IPv6 位址或二者。如果 FQDN 解析為 IPv4 和 IPv6 位址，PBF 規則的下一個躍點將有兩個：一個 IPv4 位址和一個 IPv6 位

 ©2024 Palo Alto Networks, Inc.

址。您可以為 IPv4 和 IPv6 流量設定相同的 PBF 規則。IPv4 流量被轉送到 IPv4 下一個躍點；IPv6 流量被轉送到 IPv6 下一個躍點。

此 *FQDN* 必須解析為與您為 *PBF* 設定的介面屬於同一子網路的 *IP* 位址；否則，防火牆拒絕解析，*FQDN* 保持未解析狀態。

防火牆僅使用 *FQDN* 的 *DNS* 解析中的一個 *IP* 位址（來自每個 *IPv4* 或 *IPv6* 家族類型）。如果 *DNS* 解析返回多個位址，防火牆會使用與為下一個躍點設定的 *IP* 系列類型（*IPv4* 或 *IPv6*）相符的偏好 *IP* 位址。偏好 *IP* 位址是 *DNS* 伺服器在初始回應中返回的第一個位址。只要此位址出現在後續回應中，無論順序如何，防火牆都會保留此位址作為偏好位址。

- **None**（無）—無下一個躍點意味著封包的目的地 IP 位址用作下一個躍點。如果目的地 IP 位址與輸出介面未在同一個子網路上，轉送將失敗。

5. （選用）如果未指定 IP 位址，則啟用監控功能以確認對目標 IP 位址或 **Next Hop**（下一躍點）IP 位址的連線。選取 **Monitor**（監控），然後附加監控 **Profile**（設定檔）（預設或自訂）；該設定檔會指定當無法連線至所監控位址時的動作。

   - 您可以 **Disable this rule if nexthop/monitor ip is unreachable**（在無法連線下一個躍點/監控 **ip** 時停用此規則）。
   - 輸入要監控的目標 **IP Address**（**IP** 位址）。

   Egress Interface（輸出介面）可以具有 IPv4 和 IPv6 位址，且 **Next Hop**（下一個躍點）FQDN 可以解析為 IPv4 和 IPv6 位址。在本案例中：

   1. 如果輸出介面具有 IPv4 和 IPv6 位址，且下一個躍點 FQDN 僅解析為一個位址系列類型，防火牆將監控已解析的 IP 位址。如果 FQDN 解析為 IPv4 和 IPv6 位址但輸出介面只有一個位址系列類型位址，防火牆將監控與輸出介面的位址系列相符的已解析下一個躍點位址。
   2. 如果輸出介面和下一個躍點 FQDN 均具有 IPv4 和 IPv6 位址，防火牆將監控 IPv4 下一個躍點位址。
   3. 如果輸出介面有一個位址系列位址，且下一個躍點 FQDN 解析為不同的位址系列位址，則防火牆不會監控任何位址。

6. （若為非對稱的路由環境則為必要，否則為選用）**Enforce Symmetric Return**（強制執行對稱傳回），並在 **Next Hop Address List**（下一個躍點位址清單）中 **Add**（新增）一或多個 IP 位址。您最多可新增 8 個下一個躍點 IP 位址；通道和 PPoE 介面不能用作下一個躍點 IP 位址。

   若啟用對稱傳回，則可確保會透過流量從網際網路進入時所經過的相同介面轉送出傳回流量（例如從 LAN 上的信任區域傳回至網際網路）。

STEP 3 | **Commit**（提交）您的變更。PBF 規則隨即生效。

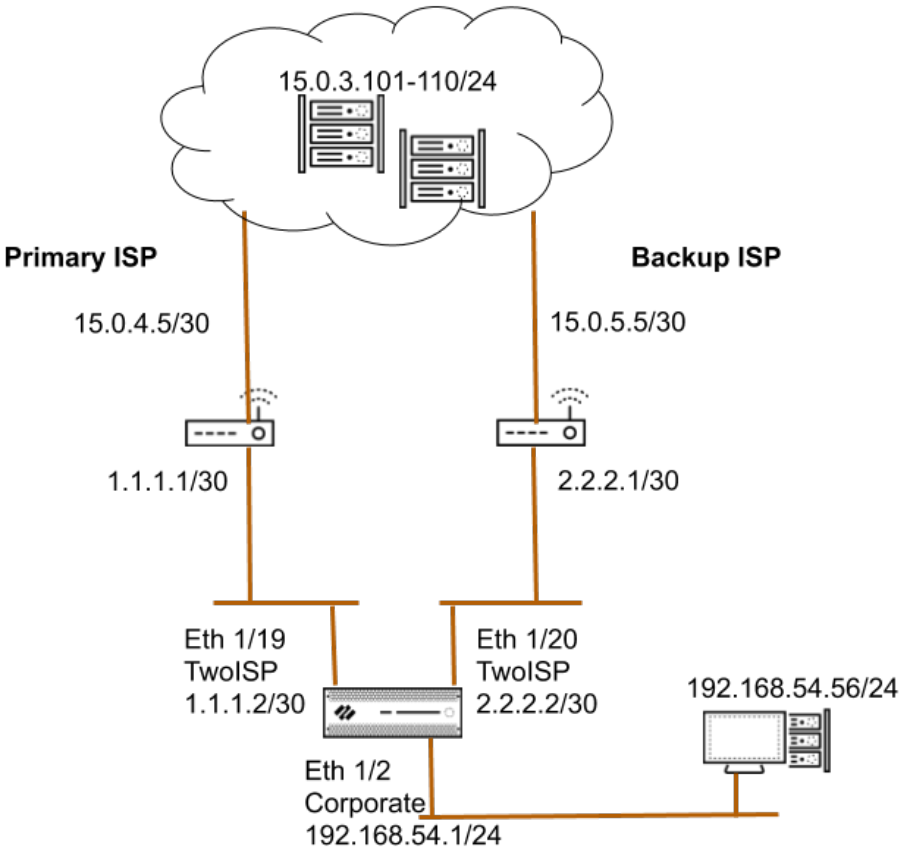
	Source			Destination			Forwarding			Monitoring	
NAME	ZONE/INTERFACE	ADDRESS	USER	ADDRESS	SERVICE	ACTION	EGRESS I/F	NEXT HOP	ENFORCE SYMMETRIC RETURN	PROFILE	DISABLE IF UNREACHABL
pdf2	ethernet1/3	any	any	HQ-subnet	service-http	forward	ethernet1/1.100	192.168.100.2	false	none	false

©2024 Palo Alto Networks, Inc.

使用案例：有雙 ISP 之輸出存取的 PBF

在此使用案例中，分公司有雙 ISP 設定，並實作 PBF 作為備援網際網路存取。備用 ISP 是從用戶端到網頁伺服器之流量的預設路由。為了啟用備援網際網路存取，但不使用如 BGP 等網際網路工作通訊協定，我們將 PBF 與以目的地介面為基礎的來源 NAT 和靜態路由搭配使用，並如下所述設定防火牆：

- 啟用 PBF 規則以透過主要 ISP 路由流量，並將監控設定檔附加至該規則。當主要 ISP 無法使用時，監控設定檔會觸發防火牆透過備用 ISP 使用預設路由。
- 為主要與備用 ISP 定義來源 NAT 規則，該規則會指示防火牆使用與相對應 ISP 其輸出介面相關聯的來源 IP 位址。這可確保輸出流量有正確的來源 IP 位址。
- 將靜態路由新增至備用 ISP，如此一來當主要 ISP 無法使用時，預設路由便會生效，且系統會透過備用 ISP 導向流量。



 ©2024 Palo Alto Networks, Inc.

STEP 1 | 在防火牆上設定輸入與輸出介面。

輸出介面可以在同一個區域中。

1. 選取 **Network**（網路） > **Interfaces**（介面），然後選取要設定的介面。

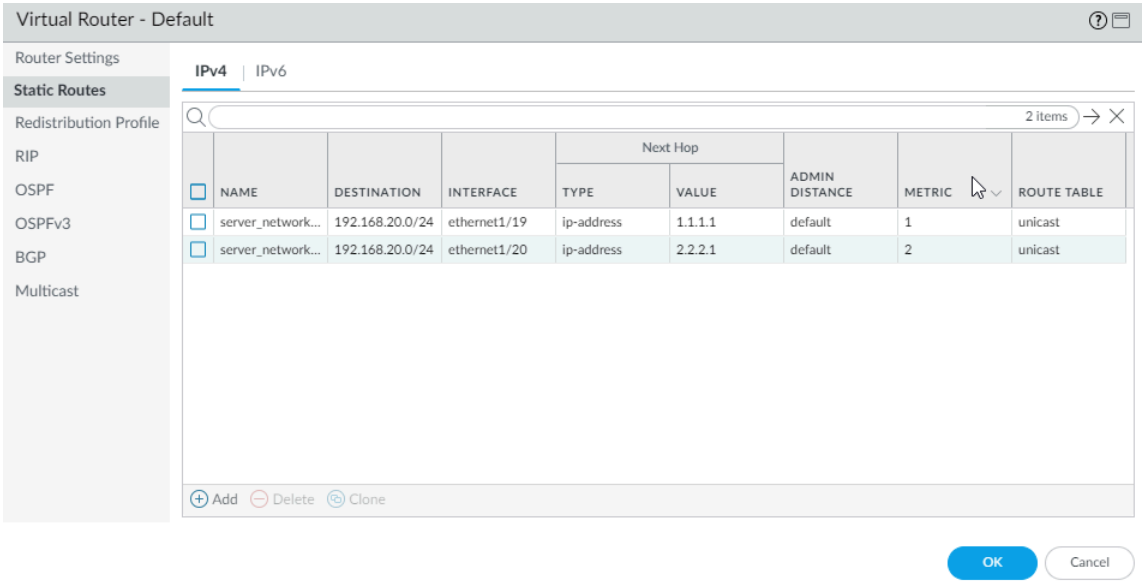
   此範例中使用的防火牆介面組態如下所示：

   - 連線至主要 ISP 的乙太網路 1/19：
     - 區域：TwoISP
     - IP 位址：1.1.1.2/30
     - 虛擬路由器：預設值
   - 連線至備用 ISP 的乙太網路 1/20：
     - 區域：TwoISP
     - IP 位址：2.2.2.2/30
     - 虛擬路由器：預設值
   - Ethernet 1/2 是輸入介面，由網路用戶端用來連線至網際網路：
     - 區域：企業
     - IP 位址：192.168. 54.1/24
     - 虛擬路由器：預設值
2. 若要儲存介面設定，請按一下 **OK**（確定）。

©2024 Palo Alto Networks, Inc.

STEP 2 | 在虛擬路由器上，將靜態路由新增至備用 ISP。

1. 選取 **Network**（網路）> **Virtual Router**（虛擬路由器），然後選取 **default**（預設）連結以開啟 Virtual Router（虛擬路由器）對話方塊。
2. 選取 **Static Routes**（靜態路由），然後按一下 **Add**（新增）。輸入路由的 **Name**（名稱），並指定您正在定義其靜態路由的 **Destination**（目的地）IP 位址。在此範例中，我們為所有的流量使用 0.0.0.0/0。
3. 選取 **IP Address**（**IP** 位址）選項按鈕，並為連線至備用網際網路閘道的路由器設定 **Next Hop**（下一個躍點）IP 位址（您不能將網域名稱用作下一個躍點）。在此範例中為 2.2.2.1。
4. 為路由指定成本公制。



5. 按兩下 **OK**（確定）以儲存虛擬路由器組態。

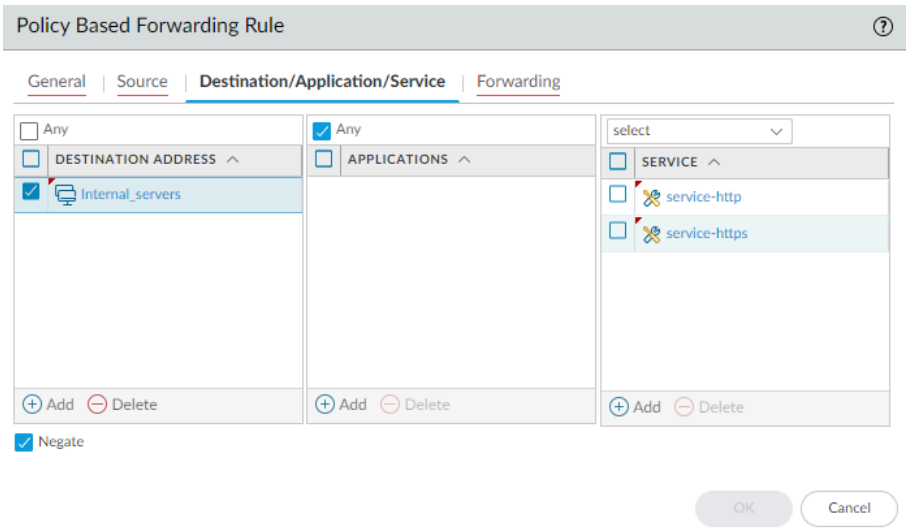
©2024 Palo Alto Networks, Inc.

STEP 3 | 建立 PBF 規則將流量導向至與主要 ISP 連線的介面。

確定將目的地為內部伺服器/IP 位址的流量從 PBF 排除。定義否定規則，讓系統不會透過 PBF 規則中定義的輸出介面路由目的地為內部 IP 位址的流量。

1. 選取 **Policies**（原則） > **Policy Based Forwarding**（基於原則的轉送），然後按一下 **Add**（新增）。
2. 在 **General**（一般）頁籤上為規則設定描述性 **Name**（名稱）。
3. 在 **Source**（來源）頁簽中，設定 **Source Zone**（來源區域）；在本範例中，該區域為「企業」。
4. 在 **Destination/Application/Service**（目的地/應用程式/服務）頁籤上，設定下列選項：
   1. 在 Destination Address（目的地位址）區段中，為內部網路上的伺服器 **Add**（新增）IP 位址或位址範圍，或為您的內部伺服器建立位址物件。選取 **Negate**（否定）將以上所列的 IP 位址或位址物件排除使用此規則。
   2. 在 Service（服務）區段中，**Add**（新增） **service-http** 與 **service-https** 服務，讓 HTTP 與 HTTPS 流量使用預設的連接埠。對於安全性原則允許的所有其他流量，將會使用預設路由。

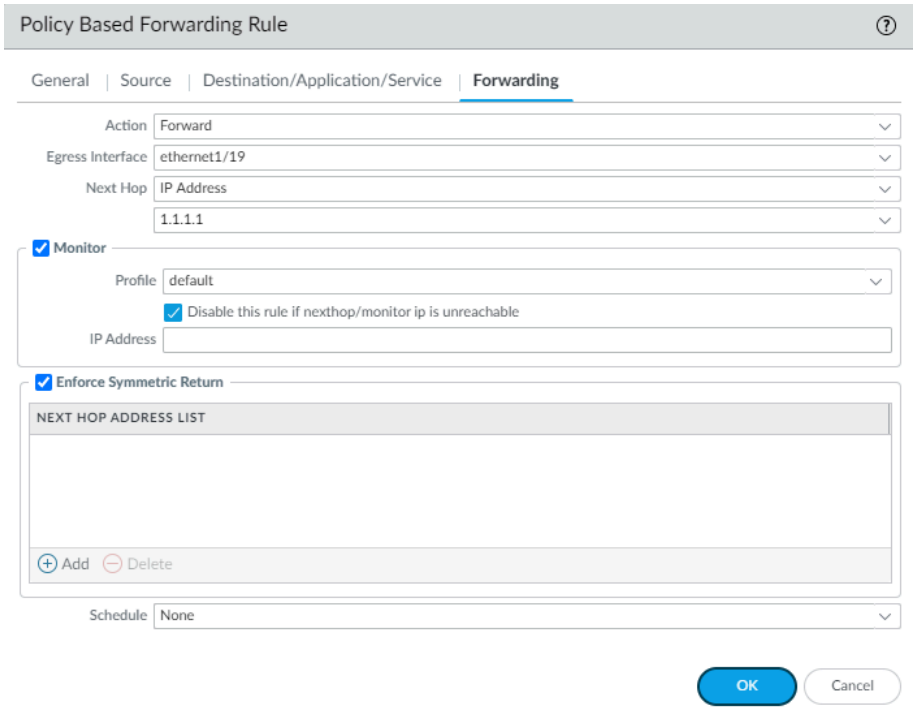
若要使用 *PBF* 轉送所有流量，請將 *Service*（服務）設為 ***Any***（任何）。



 ©2024 Palo Alto Networks, Inc.

STEP 4 | 指定將流量轉送到哪裡。

1. 在 **Forwarding**（轉送）頁籤上，指定您要將流量轉送到哪一個介面，並啟用路徑監控。
2. 若要轉送流量，可將 **Action**（動作）設為 **Forward**（轉送），然後選取 **Egress Interface**（輸出介面）並指定 **Next Hop**（下一躍點）。在此範例中，輸出介面為 ethernet1/19，下一個躍點 IP 位址為 1.1.1.1（您不能應將 FQDN 作為下一個躍點）。



3. 啟用 **Monitor**（監控），並附加預設的監控設定檔，以觸發容錯移轉至備用 ISP。在此範例中，我們不指定要監控的目標 IP 位址。防火牆將監控下一躍點 IP 位址；如果無法連線至此 IP 位址，則防火牆會將流量導向至在虛擬路由器中指定的預設路由。
4. （若採用非對稱路由，需執行此步驟） 選取 **Enforce Symmetric Return**（強制對稱傳回），以確保從企業區域流至網際網路的傳回流量會透過從網際網路輸入流量的相同介面上轉送。
5. NAT 可確保來自網際網路的流量會傳回到防火牆上正確的介面/IP 位址。
6. 按一下 **OK**（確認）以儲存變更。

		Source			Destination				Forwarding			Monitoring		
	NAME	ZONE/INTERFACE	ADDRESS	USER	ADDRESS	APPLICATION	SERVICE	ACTION	EGRESS I/F	NEXT HOP	ENFORCE SYMMETRIC RETURN	PROFILE	TARGET	DISABLE IF UNR
1	pbf_rule_source_zone	Corporate	192.168.10.2	any	any	any	service-http service-https	forward	ethernet1/19	1.1.1.1	true	default	none	true

 ©2024 Palo Alto Networks, Inc.

STEP 5 | 根據輸出介面與 ISP 建立 NAT 規則。這些規則可確保會為輸出連線使用正確的來源 IP 位址。

1. 選取 **Policies**（原則）> **NAT**，然後按一下 **Add**（新增）。
2. 在此範例中，我們為每個 ISP 建立的 NAT 規則如下所示：

   主要 **ISP** 的 **NAT**

   在 **Original Packet**（原始的封包）頁籤上，

   Source Zone (來源區域)：企業

   Destination Zone（目的地區域）：TwoISP

   在 **Translated Packet**（轉譯的封包）頁籤上的 Source Address Translation（來源位址轉譯）下方

   Translation Type（轉譯類型）：Dynamic IP and Port （動態 IP 及連接埠）

   Address Type（位址類型）：介面位址

   介面：ethernet1/19

   IP Address（**IP** 位址）：1.1.1.2/30

   備用 **ISP** 的 **NAT**

   在 **Original Packet**（原始的封包）頁籤上，

   Source Zone (來源區域)：企業

   Destination Zone（目的地區域）：TwoISP

   在 **Translated Packet**（轉譯的封包）頁籤上的 Source Address Translation（來源位址轉譯）下方

   Translation Type（轉譯類型）：Dynamic IP and Port （動態 IP 及連接埠）

   Address Type（位址類型）：介面位址

   介面：ethernet1/20

   IP Address（**IP** 位址）：2.2.2.2/30

			Original Packet						Translated Packet	
	NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSL
1	NAT for Primary ISP	none	Corporate	TwoISP	any	any	any	any	dynamic-ip-and-port ethernet1/19 1.1.1.2/30	none
2	NAT for Backup ISP	none	Corporate	TwoISP	any	any	any	any	dynamic-ip-and-port ethernet1/20 2.2.2.2/30	none

©2024 Palo Alto Networks, Inc.

STEP 6 | 建立安全性原則以允許輸出存取網際網路。

若要安全地啟用應用程式，可建立允許存取網際網路的簡易規則，並附加防火牆上可用的安全性設定檔。

1. 選取 **Policies**（原則）> **Security**（安全性），然後按一下 **Add**（新增）。
2. 在 **General**（一般）頁籤上為規則設定描述性 **Name**（名稱）。
3. 在 **Source**（來源）頁籤中，將 **Source Zone**（來源區域）設定為 Corporate（企業）。
4. 在 **Destination**（目的地）頁籤中，設定 **Destination Zone**（目的地區域）為 TwoISP。
5. 在 **Service/ URL Category**（服務/**URL** 類別）頁籤上，保留預設值 **application-default**。
6. 在 **Actions**（動作）頁籤中，完成這些工作：
   1. 將 **Action Setting**（動作設定）設定為 **Allow**（允許）。
   2. 在 **Profile Setting**（設定檔設定）下連接防毒、反間諜軟體、漏洞保護及 URL 篩選的預設設定檔。
7. 在 **Options**（選項）下，確認會在工作階段結束時啟用日誌記錄。只有符合安全性規則的流量才會記錄。

	NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION
				ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE			
1	Copr2ISP	none	universal	Corporate	any	any	any	TwoISP	any	any	any	any	Allow

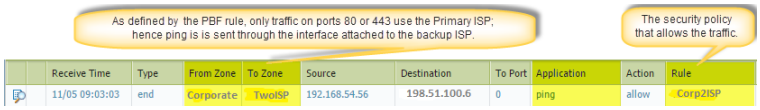
STEP 7 | 將您的原則儲存到防火牆上的執行中組態。

按一下 **Commit**（交付）。

STEP 8 | 確認 PBF 規則為使用中，且為網際網路存取使用主要 ISP。

1. 啟動網頁瀏覽器，並存取網頁伺服器。在防火牆上查看流量日誌中的網頁瀏覽活動。
2. 從網路上的用戶端使用 ping 公用程式，以確認可連線至網際網路上的網頁伺服器，並查看防火牆上的流量日誌。

```
C:\Users\pm-user1>ping 198.51.100.6 Pinging 198.51.100.6 with
 32 bytes of data:Reply from 198.51.100.6: bytes=32 time=34ms
 TTL=117 Reply from 198.51.100.6: bytes=32 time=13ms TTL=117
 Reply from 198.51.100.6: bytes=32 time=25ms TTL=117 Reply
 from 198.51.100.6: bytes=32 time=3ms TTL=117 Ping statistics
 for 198.51.100.6:Packets:Sent = 4, Received = 4, Lost = 0 (0%
 loss), Approximate round trip times in milliseconds:Minimum =
 3ms, Maximum = 34ms, Average = 18ms
```



 ©2024 Palo Alto Networks, Inc.

3. 若要確認 PBF 正在使用中，可使用下列 CLI 命令：

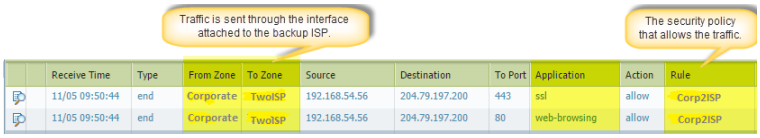
```
admin@PA-NGFW> show pbf rule all Rule ID Rule State Action Egress
 IF/VSYS NextHop ========== === ========== ====== ==============
 Use ISP-Pr 1 Active Forward ethernet1/1 1.1.1.1
```

STEP 9 | 確認會容錯移轉至備用 ISP，並正確套用來源 NAT。

1. 拔除主要 ISP 的接線。
2. 若要確認 PBF 已停用，可使用下列 CLI 命令：

```
admin@PA-NGFW> show pbf rule all Rule ID Rule State Action
 Egress IF/VSYS NextHop ========== === ========== ======
 ============== === Use ISP-Pr 1 Disabled Forward ethernet1/19
 1.1.1.1
```

3. 存取網頁伺服器並檢查流量日誌，以確認正透過備用 ISP 轉送流量。



4. 檢視工作階段詳細資料來確認 NAT 規則會正常運作。

```
admin@PA-NGFW> show session all
 ---------------------------------------------------------- ID
 Application State Type Flag Src[Sport]/Zone/Proto (translated
 IP[Port]) Vsys Dst[Dport]/Zone (translated IP[Port])
 ----------------------------------------------------------------
 87212 ssl ACTIVE FLOW NS 192.168.54.56[53236]/Corporate/6
 (2.2.2.2[12896]) vsys1 204.79.197.200[443]/TwoISP
 (204.79.197.200[443])
```

5. 從輸出取得工作階段識別號碼，並檢視工作階段詳細資料。

PBF 規則並未使用，因此未列在輸出中。

```
admin@PA-NGFW> show session id 87212 Session 87212 c2s flow:
 source:192.168.54.56 [Corporate] dst:204.79.197.200 proto:6
 sport:53236 dport:443 state:ACTIVE type:FLOW src user:
 unknown dst user: unknown s2c flow: source:204.79.197.200
 [TwoISP] dst:2.2.2.2 proto:6 sport:443 dport:12896
 state:ACTIVE type:FLOW src user: unknown dst user: unknown
 start time :Wed Nov5 11:16:10 2014 timeout :1800 sec time
 to live :1757 sec total byte count(c2s) :1918 total byte
 count(s2c) :4333 layer7 packet count(c2s) :10 layer7 packet
 count(s2c) :7 vsys : vsys1 application : ssl rule :Corp2ISP
 session to be logged at end :True session in session
 ager :True session synced from HA peer :False address/
port translation : source  nat-rule :NAT-Backup ISP(vsys1)
```


©2024 Palo Alto Networks, Inc.

```
layer7 processing : enabled URL filtering enabled :True URL
category : search-engines session via syn-cookies :False
session terminated on host :False session traverses
tunnel :False authentication portal session :False ingress
interface : ethernet1/2  egress interface : ethernet1/20
session QoS rule :N/A (class 4)
```


©2024 Palo Alto Networks, Inc.

應用程式覆寫政策

應用程式覆寫政策會繞過第七層處理和威脅檢查，而是使用不太安全的具狀態第四層檢查。應用程式覆寫政策阻止防火牆執行第七層應用程式識別以及第七層威脅檢查和預防；除非必須，否則不要使用應用程式覆寫。而是可以建立自訂應用程式或建立自訂服務逾時，以便您在常規第七層安全性政策規則中保持對應用程式的可見性、控制和檢查。

僅在您可以嚴格套用最低權限原則的最受信任環境中使用應用程式覆寫。在端點上安裝端點保護，在伺服器上安裝補償保護，並制定最具限制性的應用程式覆寫規則（僅必要的來源、目的地、使用者、應用程式和服務），因為您對流量的可見性有限。如果您必須使用應用程式覆寫並且流量周遊多個檢查點（例如資料中心防火牆，然後是周邊防火牆），請沿路徑一致地套用應用程式覆寫。

應用程式覆寫有兩個主要使用案例：

- 在 Prisma Access 中，您無法在雲端進行應用程式層級閘道 (ALG) 變更，也無法透過 Panorama 推送它們，因此如果您需要 SIP ALG，您可能需要建立應用程式覆寫規則。
- 在 SMB 流量效能極低且停用伺服器回應檢查 (DRSI) 無法充分提高效能的環境中，您可能需要建立一個應用程式覆寫規則（防火牆會更快地處理應用程式覆寫規則，但會以安全為代價，因為它們繞過了第七層檢查）。

檢閱您現有的政策規則庫。如果您對 SMB 或 SIP 以外的流量有任何應用程式覆寫規則，請將規則轉換為基於 App-ID 的規則，以便您可以在第七層解密和檢查流量並防止威脅。

©2024 Palo Alto Networks, Inc.

測試原則規則

測試執行中組態的原則規則，以確保原則適當地允許和拒絕流量，並根據您的業務需要和要求存取應用程式及網站。您可直接從 Web 介面對防火牆執行原則比對測試，以測試和驗證原則規則是否能允許和拒絕正確的流量。

STEP 1 | 啟動 Web 介面。

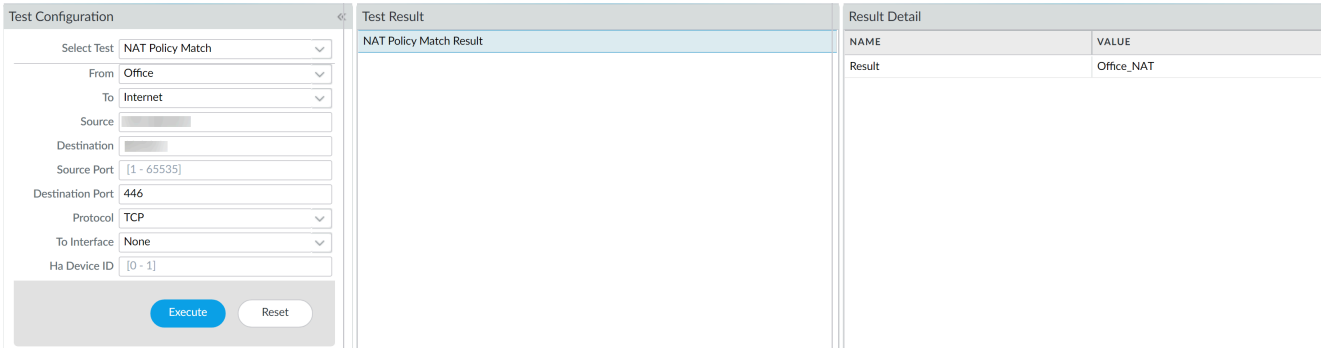
STEP 2 | 選取 **Device**（裝置） > **Troubleshooting**（疑難排解）以執行原則比對或連線測試。

STEP 3 | 輸入必要資訊以執行原則比對測試。在此範例中，我們將執行 NAT 原則比對測試。

1. **Select Test**（選取測試）—選取 **NAT Policy Match**（**NAT** 原則比對）。
2. **From**（自）—選取流量的來源區域。
3. **To**（至）—選取流量的目標區域。
4. **Source**（來源）—輸入流量的來源 IP 位址。
5. **Destination**（目的地）—輸入流量的目標裝置之 IP 位址。
6. **Destination Port**（目的地連接埠）—輸入用於流量的連接埠。此連接埠視乎以下步驟所使用的 IP 通訊協定而有所不同。
7. **Protocol**（通訊協定）—輸入用於流量的 IP 通訊協定。
8. 如有必要，請輸入任何與 NAT 原則規則測試相關的其他資訊。

STEP 4 | **Execute**（執行）NAT 原則比對測試。

STEP 5 | 檢視 **NAT Policy Match Result**（**NAT** 原則比對結果），以查看符合測試準則的原則規則。



 ©2024 Palo Alto Networks, Inc.

虛擬系統

本主題說明虛擬系統、其優點、一般使用案例及設定方式。此外也提供其他主題的連結，說明虛擬系統其他功能的相關章節。

- 虛擬系統概要介紹
- 虛擬系統之間通訊
- 共用閘道
- 設定虛擬系統
- 設定防火牆內的虛擬系統間通訊
- 設定共用閘道
- 自訂虛擬系統的服務路由
- 虛擬系統的其他功能

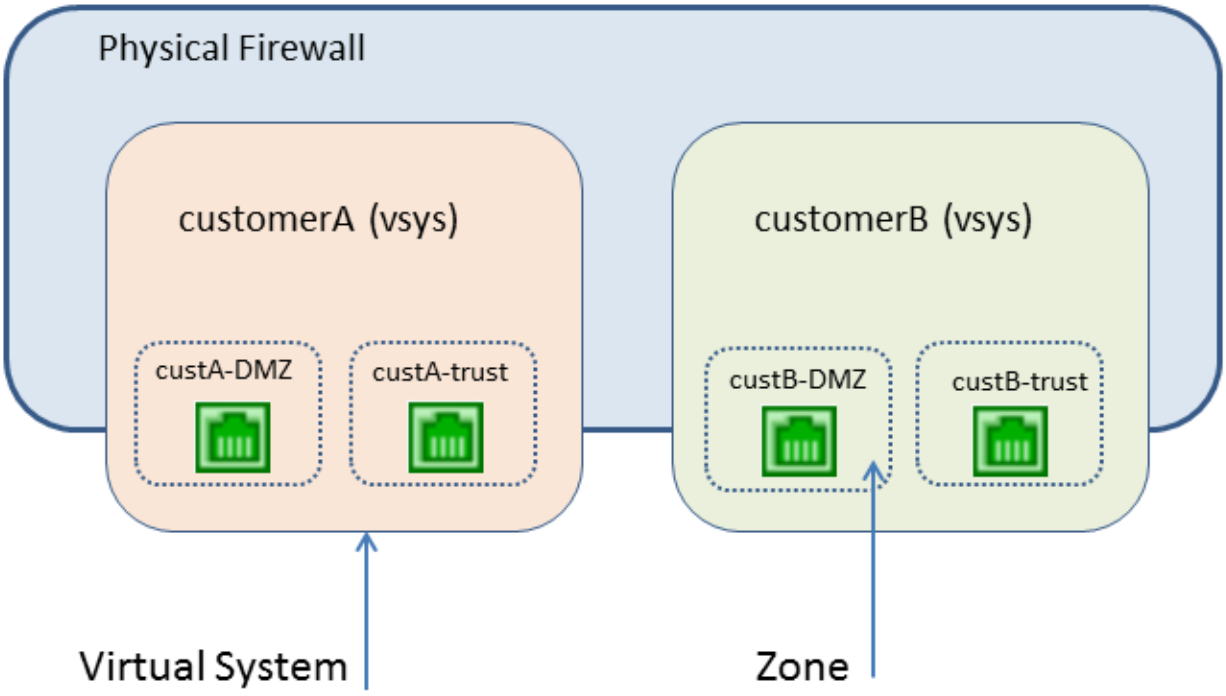
虛擬系統概要介紹

虛擬系統是在單一實體 Palo Alto Networks 防火牆內獨立的邏輯防火牆實例。受管理服務供應商與企業並非使用多個防火牆，而是使用一對防火牆（以得到高可用性），並啟用這對防火牆上的虛擬系統。每一個虛擬系統 (簡稱 vsys) 是獨立、分開管理的防火牆，其流量與其他虛擬系統的流量分開。

- 虛擬系統元件與區段
- 虛擬系統優點
- 虛擬系統的使用案例
- 虛擬系統的平台支援與授權
- 虛擬系統的管理角色
- 虛擬系統的共用物件

虛擬系統元件與區段

虛擬系統是一種可建立管理界限的物件，如下圖所示。



虛擬系統包含一組實體與邏輯介面和子介面 (包括 VLAN 與虛擬介接)、虛擬路由器及安全性區域。您會選擇每個虛擬系統的部署模式 (虛擬介接、Layer 2 或 Layer 3 的任何組合)。透過使用虛擬系統，您可以將下列項目分段：

- 管理存取權

©2024 Palo Alto Networks, Inc.

- 所有原則（安全性、NAT、QoS、基於原則的轉送、解密、應用程式覆寫、通道檢查、驗證及 DoS 保護）的管理
- 所有的物件（例如位址物件、應用程式群組與篩選器、外部動態清單、安全性原則、解密設定檔，以及自訂物件等）
- 使用者-ID
- 憑證管理
- 伺服器設定檔
- 記錄、報告與可見性功能

整組虛擬系統雖足以影響防火牆的安全性功能，但如靜態與動態路由等單一虛擬系統則不會影響網路功能。您可以透過為每個虛擬系統建立一或多個虛擬路由器，將每個虛擬系統的路由分段，如下列使用案例所示：

- 如果您具備一個組織其部門的虛擬系統，且所有部門的網路流量都在一個共同網路內，則您可以為多個虛擬系統建立單一虛擬路由器。
- 如果您想要有路由區段，且必須將每個虛擬系統的流量與其他虛擬系統的流量隔離，您可以為每個虛擬系統建立一或多個虛擬路由器。
- 若您想要將使用者對應分段，以便只在虛擬系統之間共享部分對應，則可以在不是 User-ID 中心點的虛擬系統上設定 User-ID 來源。請參閱 在虛擬系統之間共享 User-ID 對應。

虛擬系統優點

虛擬系統提供的基本功能與實體防火牆相同，但有其他的優點：

- 分段管理—不同的組織（或是客戶或事業單位）可控制（與監控）分開的防火牆實例，讓它們可控制各自的流量，不會干擾相同實體防火牆上其他防火牆實例的流量或原則。
- 延展性—設定實體防火牆後，便可有效率地新增或移除客戶或事業單位。ISP (亦即受管理的安全性服務供應商) 或企業可為每個客戶提供不同的安全性服務。
- 減少資金與營運費用—虛擬系統不需要在一個位置上有多個實體防火牆，因為虛擬系統可共存於一個防火牆上。組織不需要購買多個防火牆，因此能省下硬體費用、電費及機架空間，並減少維護與管理費用。
- 能夠共享 **IP** 位址到使用者對應—透過指定虛擬系統作為 User-ID 中心點，您可在虛擬系統之間共享 IP 位址到使用者對應，以充分利用防火牆的 User-ID 容量，並降低操作複雜度。

虛擬系統的使用案例

在防火牆上使用虛擬系統的方法有許多種。一個常見的使用案例就是讓 ISP 或受管理安全性服務供應商 (MSSP) 將服務透過單一防火牆提供給多個客戶。客戶可選擇各式各樣可輕鬆啟用或停用的服務。以防火牆角色為基礎的管理方式可讓 ISP 或 MSSP 控制每個客戶對功能 (例如記錄與報告) 的存取權，同時隱藏或提供其他功能的唯讀功能。

©2024 Palo Alto Networks, Inc.

另一個常見使用案例就是在大型企業內需要不同的防火牆實例，因為多個部門之間需要不同的技術與機密性。如上例所述，不同的群組會有不同的存取層級，同時 IT 會自行管理防火牆。由於可查出部門使用服務的量並/或向部門收費，因此組織內可能會有分開的財務責任。

虛擬系統的平台支援與授權

PA-400 系列、PA-3200 系列、PA-3400 系列、PA-5200 系列、PA-5400 系列 及 PA-7000 系列防火牆均支援虛擬系統。每一個防火牆型號皆支援基本數量的虛擬系統，此數量因平台的不同而異。需要虛擬系統授權才能支援在 PA-400 系列、PA-3200 系列和 PA-3400 系列防火牆上部署多個虛擬系統，並建立比平台所支援基本數目更多的虛擬系統。

如需授權資訊，請參閱訂閱。如需所支援虛擬系統的基本與上限數目，請參閱比較防火牆工具。

PA-220、PA-800 或 VM 系列防火牆不支援多虛擬系統。

預設值為 ***vsys1***。由於 *vsys1* 與防火牆上的內部層次結構相關，因此您無法刪除；*vsys1* 甚至會出現在不支援多個虛擬系統的防火牆模型上。

您可以限制為虛擬系統允許的工作階段、規則與 VPN 通道的資源配置，從而控制防火牆的資源。每個資源設定將顯示有效值範圍，該範圍視防火牆型號而異。預設設定為 0，這表示虛擬系統的限制即為防火牆型號的限制。但是，特定設定的限制不會複寫到每個系統。例如，如果防火牆有四個虛擬系統，每個虛擬系統的解密規則數不得為每個防火牆允許的解密規則總數。所有虛擬系統的解密規則總數達到防火牆限制時，將無法新增更多。

虛擬系統的管理角色

Superuser（超級使用者）管理員能夠建立虛擬系統及新增**Device Administrator**（裝置管理員）、**vsysadmin** 或 **vsysreader**。**Device administrator**（裝置管理員）可存取所有的虛擬系統，但無法新增管理員。當您建立管理員角色設定檔並選取要成為 **Virtual System**（虛擬系統）的角色時，角色將套用至防火牆上的特定虛擬系統。在 **Command Line**（命令行）頁籤中，虛擬系統管理角色有兩種：

- **vsysadmin**—可存取防火牆上的特定虛擬系統以建立和管理虛擬系統的特定方面。vsysadmin 無法存取網路介面、VLAN、Virtual Wire、虛擬路由器、IPSec 通道、GRE 通道、DHCP、DNS Proxy、QoS、LLDP 或網路設定檔。具備 vsysadmin 權限的人只能提交指派給他們之虛擬系統的組態。
- **vsysreader**—對防火牆上的特定虛擬系統和虛擬系統的特定方面具有唯讀存取權限 。vsysreader 無法存取網路介面、VLAN、Virtual Wire、虛擬路由器、IPSec 通道、GRE 通道、DHCP、DNS Proxy、QoS、LLDP 或網路設定檔。

虛擬系統管理員只能檢視指派給該管理員之虛擬系統的日誌。**Superuser**（超級使用者）或 **Device administrator**（裝置管理員）可檢視所有日誌，選取要檢視的虛擬系統，或設定虛擬系統作為 User-ID 中心點。

©2024 Palo Alto Networks, Inc.

虛擬系統的共用物件

如果您的管理員帳戶橫跨多個虛擬系統，您可以選擇為特定的虛擬系統設定物件（例如位址物件）與原則，或將物件與原則設為共用物件，以套用到防火牆上所有的虛擬系統上。如果您嘗試建立一個名稱與類型和虛擬系統中現有物件相同的共用物件，則可使用虛擬系統物件。

©2024 Palo Alto Networks, Inc.

虛擬系統之間通訊

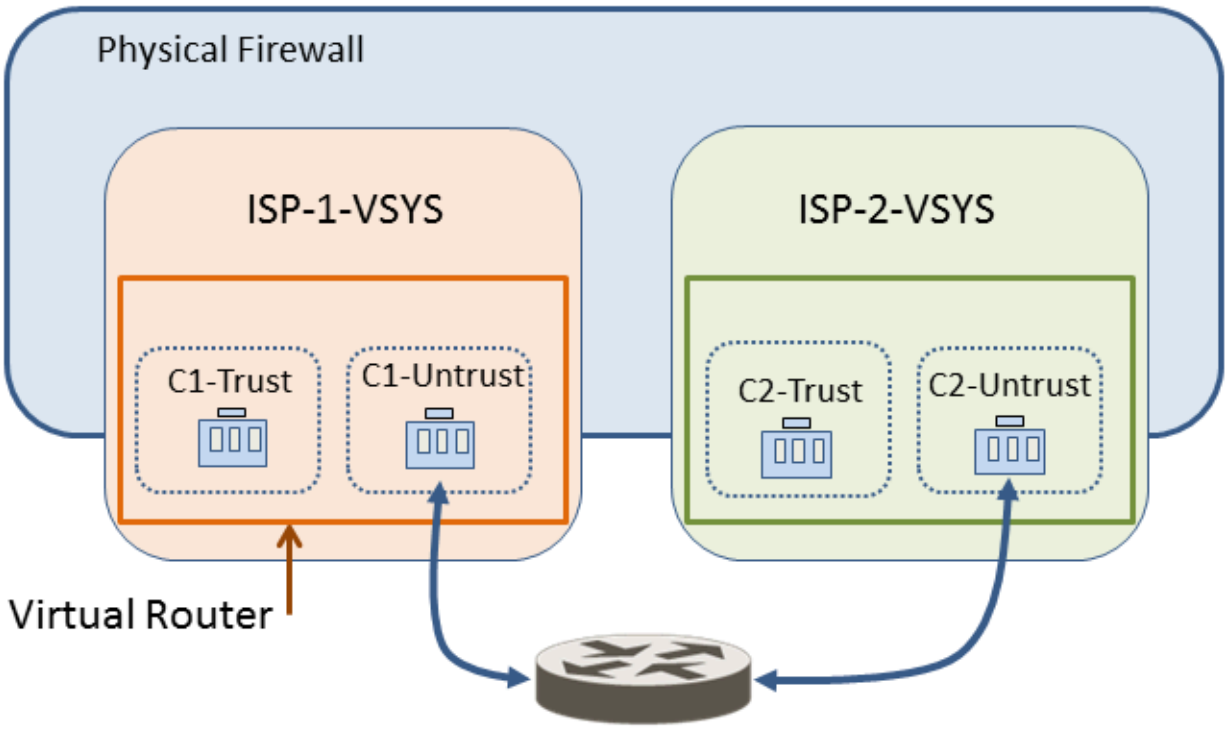
以下說明兩個虛擬系統 (vsys 間流量) 之間通訊的一般狀況。在多租戶的環境中，讓流量離開防火牆、經過網際網路，然後再重新進入防火牆，虛擬系統之間即發生通訊。在單一組織環境中，虛擬系統之間的通訊協定會保持在防火牆內進行。本節會討論這兩種案例。

- 必須離開防火牆的 VSYS 間流量
- VSYS 間的流量保留在防火牆內
- VSYS 間通訊使用兩個工作階段

必須離開防火牆的 VSYS 間流量

在防火牆上有多個客戶（所謂的多租戶）的 ISP 可為每個客戶使用虛擬系統，因此讓每個客戶能控制其虛擬系統組態。ISP 會將 **vsysadmin** 權限授予客戶。每個客戶的流量與管理工作皆彼此隔離。每個虛擬系統必須設有自己的 IP 位址與一或多個虛擬路由器，才能管理流量及其自己在網際網路上的連線。

如果虛擬系統必須彼此通訊，則流量會離開防火牆到另一個 Layer 3 路由裝置，再返回防火牆，即使是虛擬系統存在於同一個實體防火牆上亦是如此，如下圖所示。



VSYS 間的流量保留在防火牆內

不同於先前的多租戶案例，防火牆上的虛擬系統可在單一組織的控制之下。組織想要隔離虛擬系統之間的流量，並允許虛擬系統之間通訊。這是當組織想要將部門分開，但讓部門仍能夠彼此通訊或

©2024 Palo Alto Networks, Inc.

連線至同一個網路時常使用的案例。在此案例中，vsys 間流量會保持在防火牆內，如以下主題所述：

- 外部區域
- 防火牆內流量適用的外部區域與安全性原則

外部區域

如需達成如上例所述的通訊方式，可設定安全性原則指向外部區域或從外部區域指出。外部區域是安全性物件，與它可連接的特定虛擬系統相關聯；該區域在虛擬系統的外部。無論虛擬系統內有多少個安全性區域，虛擬系統只能有一個外部區域。必須要有外部區域，不同虛擬系統中的區域之間才能有流量，流量無須離開防火牆。

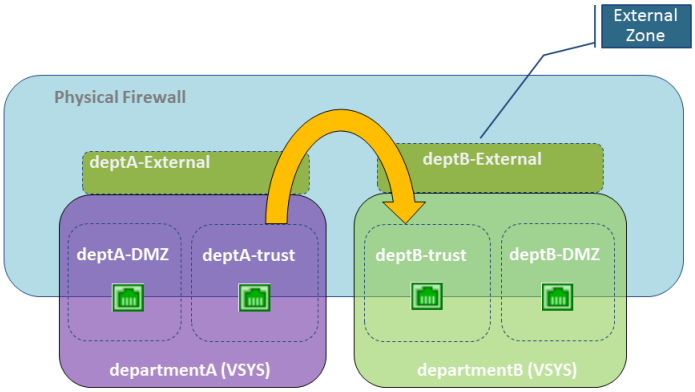
虛擬系統管理員可設定允許兩個虛擬系統之間流量所需的安全性原則。不同於安全性區域，外部區域與介面之間沒有關聯，而是與虛擬系統之間有關聯。安全性原則允許或拒絕安全性（內部）區域與外部區域之間的流量。

由於外部區域沒有與其關聯的介面或 IP 位址，因此外部區域上不支援某些區域保護設定檔。

請記住，每個虛擬系統都是個別的防火牆實例，這表示系統會檢查在虛擬系統之間移動的每個封包，以進行安全性原則與 App-ID 評估。

防火牆內流量適用的外部區域與安全性原則

在下列範例中，企業會有兩個分開的管理群組：departmentA 與 departmentB 虛擬系統。下圖顯示與每個虛擬系統相關聯的外部區域，以及從一個信任區域流出、離開外部區域、進入另一個虛擬系統的外部區域，然後進入其信任區域的流量。



為了建立外部區域，防火牆管理員會設定虛擬系統，讓它們能夠彼此看見。外部區域之間沒有安全性原則，因為其虛擬系統可看見彼此。

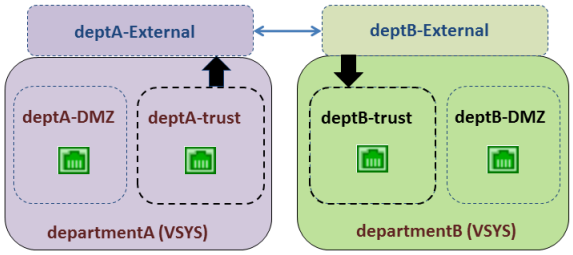
為了讓虛擬系統之間進行通訊，系統會將防火牆上的輸入與輸出介面指派給單一虛擬路由器，或是使用虛擬路由器間靜態路由來連接這些介面。這兩者之中較簡單的方法是，將必須彼此通訊的所有虛擬系統指派給單一虛擬路由器。

這麼做的原因是虛擬系統必須有自己的虛擬路由器，例如當虛擬系統使用重疊的 IP 位址範圍時。系統會在虛擬系統之間路由流量，但每個虛擬路由器必須有一個靜態路由會指向其他虛擬路由器作為下一躍點。

©2024 Palo Alto Networks, Inc.

請參閱上圖的案例，某企業有兩個管理群組：departmentA 與 departmentB。departmentA 群組會管理區域網路與 DMZ 資源。departmentB 群組會管理進出網路中銷售區段的流量。所有的流量都在區域網路上，因此會使用單一虛擬路由器。為了在兩個虛擬系統之間進行通訊，因此設定了兩個外部區域。departmentA 虛擬系統有三個區域用於安全性原則，分別是：deptA-DMZ、deptA-trust 及 deptA-External。departmentB 虛擬系統也有三個區域：deptB-DMZ、deptB-trust 及 deptB-External。這兩個群組都會控制通過其虛擬系統的流量。

為了允許流量從 deptA-trust 流到 deptB-trust，需要兩個安全性原則。在下圖中，兩個垂直箭頭表示安全性原則（如下圖所述）正在控制流量。



- 安全性原則 1：在上圖中，流量的目前地是 deptB-trust 區域。流量會離開 deptA-trust 區域，然後移至 deptA-External 區域。安全性原則必須允許流量從來源區域 (deptA-trust) 到目的地區域 (deptA-External)。虛擬系統允許任何原則類型用於此流量，包括 NAT。

  外部區域之間不需要原則，因為傳送到外部區域的流量會出現在原始外部區域看得到的其他外部區域中，而且具備該外部區域的自動存取權。
- 安全性原則 2：在上圖中，來自 deptB-External 的流量目的地仍為 deptB-trust 區域，且必須設定安全性原則以允許該流量。原則必須允許流量從來源區域 (deptB-External) 到目的地區域 (deptB-trust)。

可將 departmentB 虛擬系統設為封鎖來自 departmentA 虛擬系統的流量，反之亦然。如同來自任何其他區域的流量，原則必須明確允許來自外部區域的流量可連接到虛擬系統的其他區域。

除了未離開防火牆的虛擬系統間流量所需要的外部區域外，如果您設定共用閘道，則還需要外部區域，在此狀況下流量會離開防火牆。

VSYS 間通訊使用兩個工作階段

不同於單一虛擬系統會使用一個工作階段，兩個虛擬系統之間的通訊會使用到兩個工作階段，瞭解這一點是很有幫助的。讓我們比較一下這兩種狀況。

案例 1—Vsys1 有兩個區域：trust1 與 untrust1。trust1 區域中的主機需要與 untrust1 區域中的裝置通訊時，會啟動流量。主機會將流量傳送至防火牆，防火牆會為來源區域 trust1 建立一個到目的地區域 untrust 1 的新工作階段。此流量只需要一個工作階段。

案例 2—vsys1 中的主機需要 vsys2 上伺服器的存取權。trust1 區域中的主機會啟動流到防火牆的流量，且防火牆會建立第一個工作階段：來源區域 trust1 到目的地區域 untrust1。流量會路由到 vsys2，無論是內部或外部。接著防火牆必須建立第二個工作階段：來源區域 untrust2 到目的地區域 trust2。此 vsys 間流量需要兩個工作階段。

©2024 Palo Alto Networks, Inc.

共用閘道

此主題包括下列有關共用閘道的資訊：

- 外部區域與共用閘道
- 共用閘道的網路考量

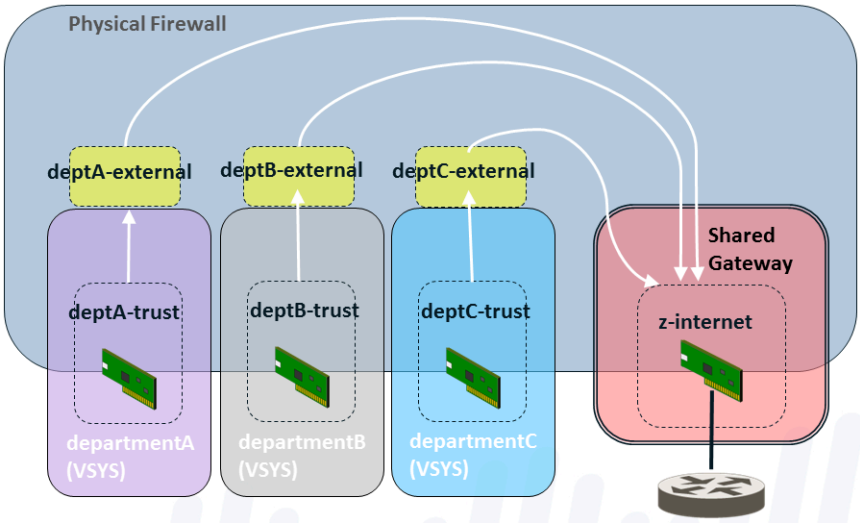
外部區域與共用閘道

共用閘道是多個虛擬系統為了透過網際網路通訊而共用的介面。每個虛擬系統都需要一個 外部區域 作為中繼者來設定安全性政策，以允許或拒絕虛擬系統的內部區域到共用閘道的流量。

共用閘道使用單一虛擬路由來路由所有虛擬系統的流量。共用閘道用於當介面不需要完整的管理界限時，或當多個虛擬系統必須共用單一網際網路連線時。如果 ISP 提供的組織只有一個 IP 位址（介面），但多個虛擬系統需要外部通訊時，便會發生第二種狀況。

不同於虛擬系統之間的行為，虛擬系統與共用閘道之間不會執行安全性原則與 App-ID 評估。這也是為何使用共用閘道存取網際網路所需的管理負荷少於建立另一個虛擬系統所需的負荷。

在下圖中有三個客戶共用防火牆，但網際網路只可存取一個介面。建立另一個虛擬系統會增加 App-ID 的管理負荷，且需要對透過新增的虛擬系統傳送到介面的流量進行安全性原則評估。若要避免新增另一個虛擬系統，解決方法是設定共用閘道，如下圖所示。



共用閘道有一個可全域路由的 IP 位址，用於與外部世界通訊。虛擬系統中的介面也有 IP 位址，但為不可路由的私人 IP 位址。

您將會想起，管理員必須指定虛擬系統是否可讓其他虛擬系統看見。不同於虛擬系統，共用閘道一律可讓防火牆上所有的虛擬系統看到。

共用閘道 ID 號碼在網頁介面上會顯示成 **sg<ID>**。建議您為共用閘道組態的名稱應包含其 ID 號碼。

©2024 Palo Alto Networks, Inc.

當您將如區域或介面等物件新增至共用閘道時，共用閘道會在 vsys 功能表中顯示為可用的虛擬系統。

共用閘道是功能有限制的虛擬系統版本，支援 NAT 和基於原則的轉送 (PBF)，但不支援安全性、DoS 原則、QoS、解密、應用程式覆寫或驗證原則。

共用閘道的網路考量

設定共用閘道時，請記住下列幾點。

- 共用閘道案例中的虛擬系統會透過使用單一 IP 位址透過共用閘道的實體介面存取網際網路。如果虛擬系統的 IP 位址不是可全域路由，則設定來源 NAT 將這些位址轉譯至可全域路由的 IP 位址。
- 虛擬路由器會透過共用閘道路由所有虛擬系統的流量。
- 虛擬系統的預設路由應指向共用閘道。
- 您必須為每個系統設定安全性原則，來允許內部區域與外部區域之間的流量 (共用閘道可看見此流量)。
- 防火牆管理員應控制虛擬路由器，讓虛擬系統中不會有任何成員影響到其他虛擬系統的流量。
- 在 Palo Alto Networks 防火牆內，封包會從某個虛擬系統跳躍至另一個虛擬系統或共用的閘道。封包不會在兩個以上的虛擬系統或共用閘道之間周遊。例如，封包不能從 vsys1 傳輸到 vsys2 再到 vsys3，或從 vsys1 到 vsys2 再到共用閘道1。這兩個範例均涉及兩個以上的虛擬系統，是不允許的。

若要省下設定的時間與工作，請考慮使用共用閘道，其優點如下：

- 您可以為共用閘道設定 NAT，而不用為與共用閘道相關聯的多個虛擬系統設定 NAT。
- 您可以為共用閘道設定基於原則的轉送 (PBR)，而非為與共用閘道相關聯的多個虛擬系統設定 PBR。

©2024 Palo Alto Networks, Inc.

設定虛擬系統

若要建立虛擬系統，您必須具備下列項目：

- 超級使用者管理角色。
- 設定好的介面。
- 如果您建立的虛擬系統超過平台上所支援的基本數目，則需有虛擬系統授權。請參閱虛擬系統的平台支援與授權。

（*Panorama* 管理的防火牆）對於由 *Panorama* 管理伺服器管理的防火牆，*Palo Alto Networks* 建議在變更虛擬系統設定狀態之前，記下 *Panorama* 上您新增了受管理防火牆的所有政策規則目標清單，以確保維持安全態勢。

變更受管理防火牆多重 *vsys* 狀態會影響在其中將受管理防火牆新增到政策目標清單的所有政策規則。以任何方式變更多重 *vsys* 狀態都會從 *Panorama* 管理的政策規則的目標清單中移除防火牆，從而影響 *Panorama* 將政策規則推送到的防火牆。如果移除的防火牆是唯一的目標，則規則現在將推送到與受影響的裝置群組關聯的所有防火牆。

- 在 `deny`（拒絕）政策規則的情況下，這可能會導致某些防火牆拒絕它們之前允許的工作階段。
- 在 `allow`（允許）政策規則的情況下，這可能會導致某些防火牆允許它們之前拒絕的工作階段。

STEP 1 | 啟用虛擬系統。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理），然後編輯 **General Settings**（一般設定）。
2. 選取 **Multi Virtual System Capability**（多重虛擬系統功能）核取方塊，然後按一下 **OK**（確定）。如果您核准此動作，這會觸發提交。

   只有在啟用虛擬系統後，**Device**（裝置）頁籤才會顯示**Virtual Systems**（虛擬系統）與 **Shared Gateways**（共用閘道）選項。

STEP 2 | 建立虛擬系統。

1. 選取 **Device**（裝置） > **Virtual Systems**（虛擬系統），按一下 **Add**（新增），然後輸入虛擬系統 **ID**，此 ID 會附加到「vsys」（範圍為 1-255）。

   預設值為 ***vsys1***。由於 *vsys1* 與防火牆上的內部層次結構相關，因此您無法刪除；*vsys1* 甚至會出現在不支援多個虛擬系統的防火牆模型上。
2. 如果您要允許防火牆將解密內容轉送至外部服務，則選取 **Allow forwarding of decrypted content**（允許轉送解密內容）。例如，您必須啟用此選項，防火牆才能將解密的內容轉送至 WildFire 進行分析。

©2024 Palo Alto Networks, Inc.

3. 為虛擬系統輸入具描述性的 **Name**（名稱）。最多允許 31 個英數字、空格與底線字元。

STEP 3 | 指派介面給虛擬系統。

虛擬路由器、Virtual Wire 或 VLAN 可以已經設定好，或者可於日後當您在指定其相關聯的虛擬系統時加以設定。

1. 如果您要將 DNS Proxy 規則套用至介面，則在 **General**（一般）頁籤上選取 **DNS Proxy** 物件。
2. 在 **Interfaces**（介面）欄位中按一下 **Add**（新增），以輸入要指派給虛擬系統的介面或子介面。介面只可以屬於一個虛擬系統。
3. 請根據您在虛擬系統中需要的部署類型執行下列任何一項：
   - **Add**（新增）要指派給 vsys 的 **VLAN** 。
   - **Add**（新增）要指派給 vsys 的 **Virtual Wires**（虛擬介接）。
   - **Add**（新增）要指派給 vsys 的 **Virtual Routers**（虛擬路由器）。
   - 如果防火牆啟用了 **Advanced Routing**（進階路由），請 **Add**（新增）要指派給 vsys 的 **Logical Routers**（邏輯路由器）。
4. 在 **Visible Virtual System**（可見虛擬系統）欄位中，勾選所有應該讓正在設定的虛擬系統看見的虛擬系統。對於需要互相通訊的虛擬系統，這是必要的。

   在需要嚴格管理界限的多租戶案例中，不會勾選虛擬系統。
5. 按一下 **OK**（確定）。

STEP 4 | （Panorama 管理的防火牆需要）登入到 Panorama 網頁介面並選取 **Commit**（提交） > **Push to Devices**（推送到裝置），然後將整個 Panorama 管理的設定推送到多重 vsys 防火牆的每個 vsys。

這是將共用設定物件用於由 Panorama 管理的多重 vsys 防火牆所必需的。

STEP 5 | （選用） 限制為虛擬系統允許的工作階段、規則與 VPN 通道的資源配置。能夠配置各虛擬系統限制的彈性，可讓您有效地控制防火牆資源。

1. 在 **Resource**（資源）頁籤上，選擇性地設定虛擬系統的限制。每個欄位將顯示有效值範圍，該範圍視防火牆型號而異。預設設定為 0，這表示虛擬系統的限制即為防火牆型號的限制。但是，特定設定的限制不會複寫到每個系統。例如，如果防火牆有四個虛擬系統，

©2024 Palo Alto Networks, Inc.

每個虛擬系統的解密規則數不得為每個防火牆允許的解密規則總數。所有虛擬系統的解密規則總數達到防火牆限制時，將無法新增更多。

- 工作階段數量限制

  如果您使用 *CLI* 命令 *show session meter*，將顯示每個資料平面允許的工作階段數量上限、虛擬系統目前使用的工作階段數量以及每個虛擬系統的節流工作階段數量。在 *PA-5200* 或 *PA-7000* 系列防火牆上，目前是喲個的工作階段數量可能大於所設定的工作階段數量上限，因為每個虛擬系統有多個資料平面。您在 *PA-5200* 或 *PA-7000* 系列防火牆上設定的工作階段數量限制是針對每個資料平面，而每個虛擬系統的工作階段數數量上限會更高。
- 安全性規則
- **NAT** 規則
- 解密規則
- **QoS** 規則
- 應用程式取代規則
- 原則路由規則
- 驗證規則
- **DoS** 防護規則
- 站台對站台 **VPN** 通道
- 同時 **SSL VPN** 通道

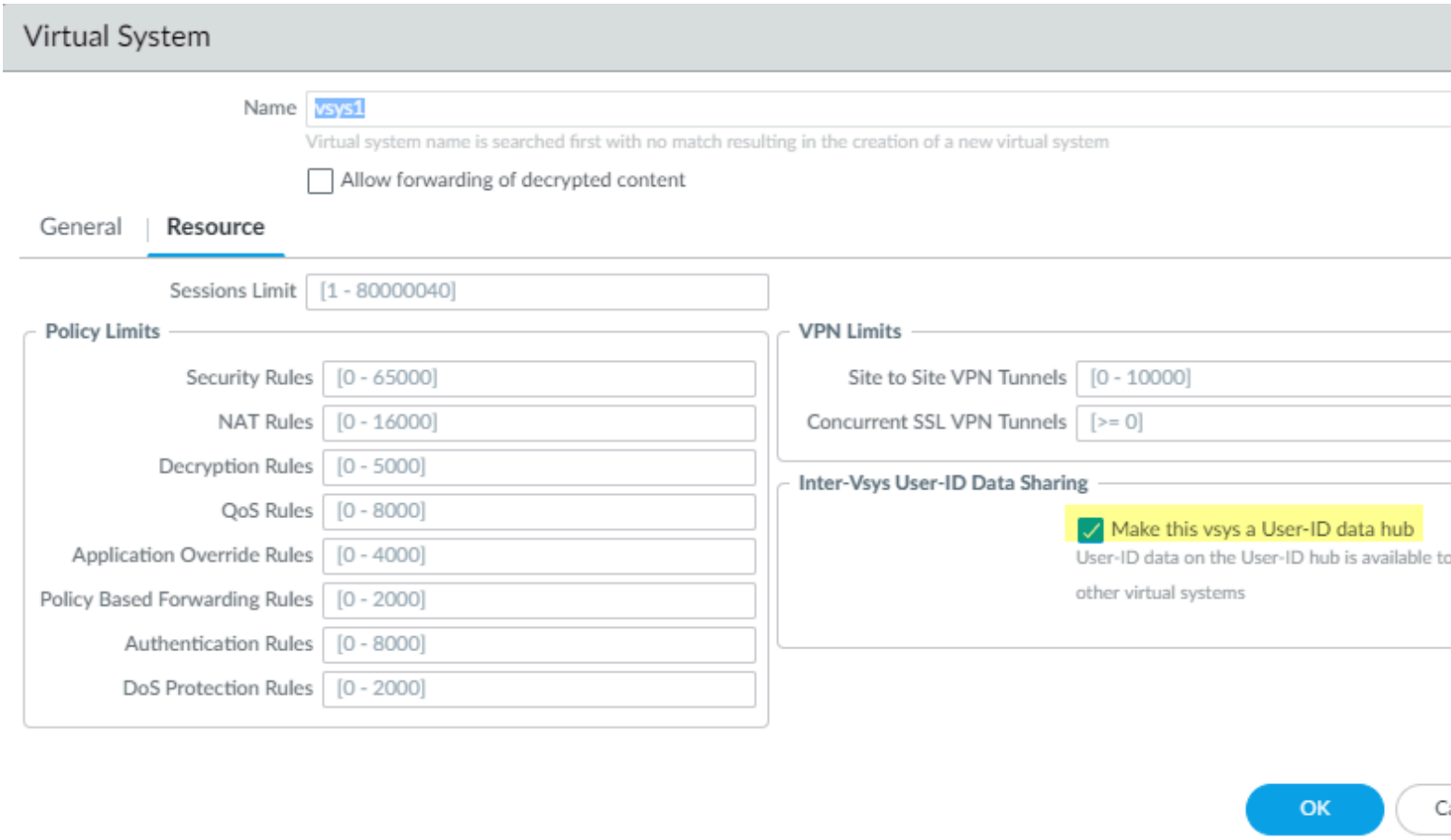
2. 按一下 **OK**（確定）。

©2024 Palo Alto Networks, Inc.

STEP 6 | （選用）將虛擬系統設為 User-ID 中心點以在虛擬系統之間共享 User-ID 對應。

終端機伺服器代理程式的 *IP* 位址與連接埠到使用者名稱對應資訊和群組對應資料不會在虛擬系統中心點與連線的虛擬系統之間共享。

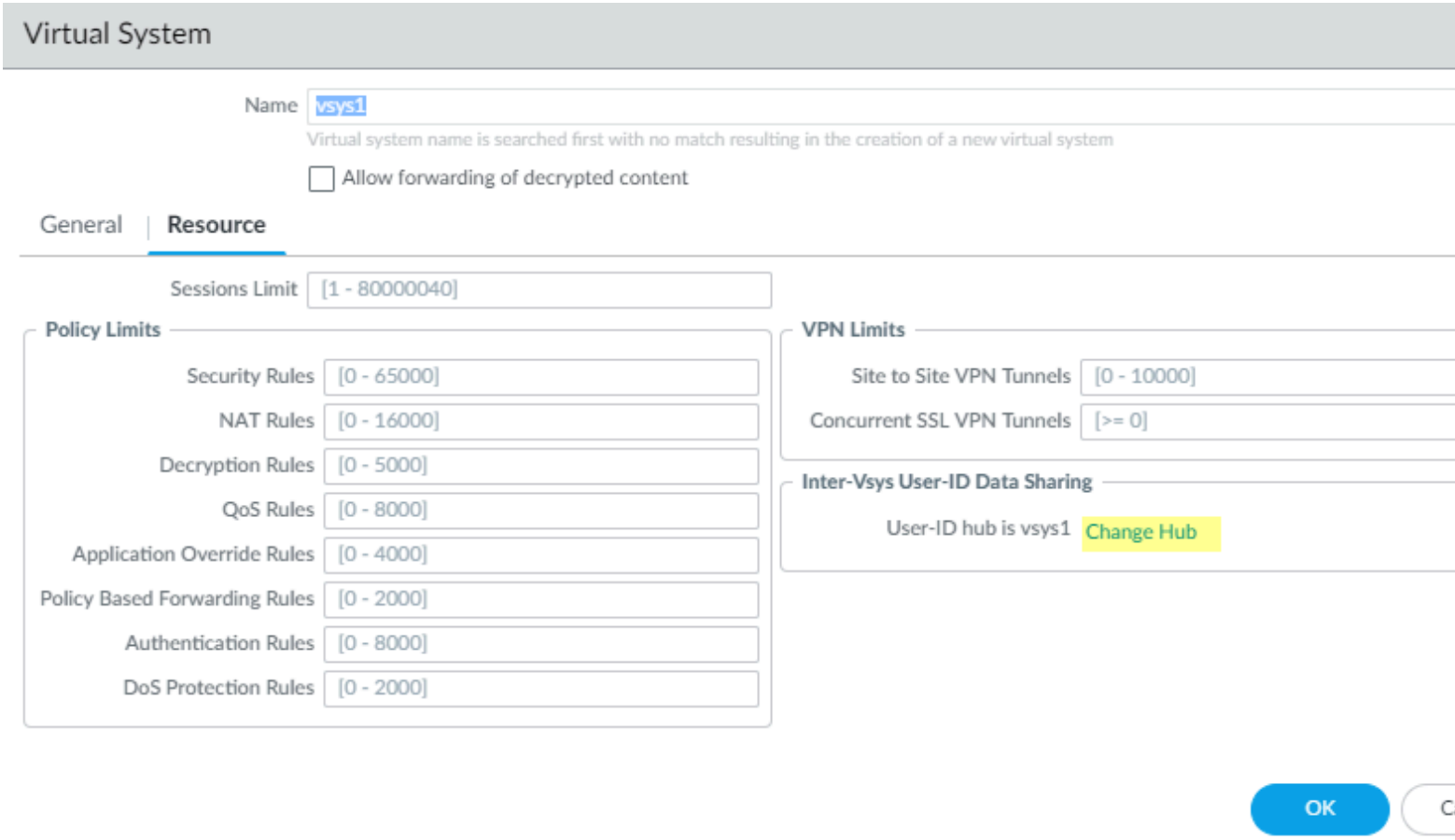
1. 對於現有虛擬系統，將您想要共享的 User-ID 來源（如受監控伺服器和 User-ID 代理程式）的組態傳輸到將用作中心點的虛擬系統。
2. 在 **Resource**（資源）頁籤上，選取 **Make this vsys a User-ID data hub**（將此 **vsys** 設為 **User-ID** 資料中心）。



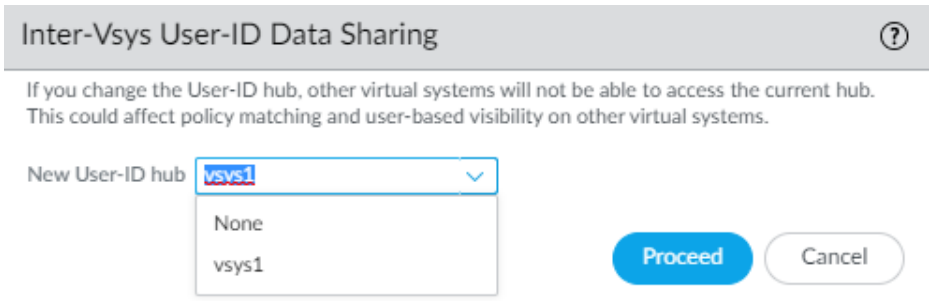
3. 按一下 **Yes**（是）以確認，然後按一下 **OK**（確定）。

   如果您想要將 User-ID 中心點變更為不同虛擬系統或將其停用，請選取目前設定為 User-ID 中心點的虛擬系統，然後選取 **Resource**（資源） > **Change Hub**（變更中心點）。

 ©2024 Palo Alto Networks, Inc.



從清單選取 **New User-ID hub**（新 **User-ID** 中心點），或選取 **none**（無）以停用 User-ID 中心點並停止在虛擬系統之間共用對應。



按一下 **Proceed**（繼續）以確認，然後提交變更。

STEP 7 | 提交組態。

按一下 **Commit**（交付）。虛擬系統現在是可從 **Objects**（物件）頁籤存取的物件。

 ©2024 Palo Alto Networks, Inc.

STEP 8 | 為虛擬系統建立至少一個虛擬路由器，讓虛擬系統能夠有網路功能，例如靜態與動態路由。

或者，您的虛擬系統可使用 VLAN 或虛擬介接，視您的部署而定。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後依 **Name**（名稱） **Add**（新增） 虛擬路由器。
2. 對於 **Interfaces**（介面），按一下 **Add**（新增），然後選取屬於虛擬路由器的介面。
3. 按一下 **OK**（確定）。

STEP 9 | 為虛擬系統中的每個介面設定安全性區域。

為至少一個介面建立 Layer 3 安全性區域。請參閱設定介面及區域。

STEP 10 | 設定安全性原則，以允許或拒絕流量進出虛擬系統中的區域。

請參閱建立安全性原則規則。

STEP 11 | 提交組態。

按一下 **Commit**（交付）。

在建立虛擬系統後，您可使用 *CLI* 僅為特定的虛擬系統提交組態：

```
commit partial vsys <vsys-id>
```

STEP 12 | （選用）檢視為虛擬系統設定的安全性原則。

開啟 SSH 工作階段以使用 CLI。若要檢視虛擬系統的安全性原則，請在操作模式中使用下列命令：

```
set system setting target-vsys <vsys-id>
show running security-policy
```

 ©2024 Palo Alto Networks, Inc.

設定防火牆內的虛擬系統間通訊

如果您有使用案例，或許您要在單一企業內讓虛擬系統能夠在防火牆內互相通訊，請執行此工作。VSYS 間的流量保留在防火牆內小節中描述了此情境。此工作假設：

- 您已完成設定虛擬系統。
- 設定虛擬系統時，在 **Visible Virtual System**（可見虛擬系統）欄位中，您可以核取所有必須互相通訊才能看到彼此之虛擬系統的方塊。

STEP 1 | 為每個虛擬系統設定外部區域。

1. 選取 **Network**（網路） > **Zones**（區域），然後依 **Name**（名稱）**Add**（新增） 新的區域。
2. 對於 **Location**（位置），選取您要建立外部區域的虛擬系統。
3. 對於 **Type**（類型），選取 **External**（外部）。
4. 針對 **Virtual Systems**（外部）按一下 **Add**（新增），輸入外部區域可以連接的虛擬系統。
5. （選用）選取 **Zone Protection Profile**（區域保護設定檔）或稍後設定一個，以防禦洪水、偵察或封包式攻擊。
6. （選用）在 **Log Setting**（日誌設定）中，選取用來將區域保護日誌轉送至外部系統的日誌轉送設定檔。
7. （選用）選取 **Enable User Identification**（啟用使用者識別），為外部區域啟用 User-ID。
8. 按一下 **OK**（確定）。

STEP 2 | 設定安全性原則規則，以允許或拒絕流量從內部區域流到虛擬系統的外部區域，反之亦然。

- 請參閱建立安全性原則規則。
- 請參閱VSYS 間的流量保留在防火牆內。

STEP 3 | Commit（提交）您的變更。

按一下 **Commit**（交付）。

©2024 Palo Alto Networks, Inc.

設定共用閘道

如果您需要多個虛擬系統才能共用網際網路的介面（共用閘道），請執行此工作。此工作假設：

- 您設定了一個具備可全域路由 IP 位址的介面，此介面將會是共用閘道。
- 您已完成前一個工作：設定虛擬系統。針對此介面，您選擇具備可全域路由 IP 位址的對外介面。
- 設定虛擬系統時，在 **Visible Virtual System**（可見虛擬系統）欄位中，您可以核取所有必須通訊才能看到彼此之虛擬系統的方塊。

STEP 1 | 設定共用閘道。

1. 選取 **Device**（裝置） > **Shared Gateway**（共用閘道）、按一下 **Add**（新增），然後輸入 **ID**。
2. 輸入有幫助的 **Name**（名稱），最好包括閘道的 **ID**。
3. 如果您想要將 DNS Proxy 規則套用到介面上，則在 **DNS Proxy** 欄位中選取 DNS Proxy 物件。
4. **Add**（新增）連接到外部環境的 **Interface**（介面）。
5. 按一下 **OK**（確定）。

STEP 2 | 設定共用閘道的區域。

將如區域或介面等物件新增至共用閘道時，共用閘道本身將列示為 ***VSYS*** 功能表中的可用 *vsys*。

1. 選取 **Network**（網路） > **Zones**（區域），然後依 **Name**（名稱）**Add**（新增） 新的區域。
2. 對於**Location**（位置），選取您要建立區域的共用閘道。
3. 對於 **Type**（類型），選取 **Layer3**。
4. （選用）選取 **Zone Protection Profile**（區域保護設定檔）或稍後設定一個，以防禦洪水、偵察或封包式攻擊。
5. （選用）在 **Log Setting**（日誌設定）中，選取用來將區域保護日誌轉送至外部系統的日誌轉送設定檔。
6. （選用）選取 **Enable User Identification**（啟用使用者識別），為共用閘道啟用 User-ID。
7. 按一下 **OK**（確定）。

STEP 3 | Commit（提交）您的變更。

按一下 **Commit**（交付）。

©2024 Palo Alto Networks, Inc.

自訂虛擬系統的服務路由

為多個虛擬系統啟用防火牆時，虛擬系統將繼承全域服務和服務路由設定。例如，防火牆可使用共用電子郵件伺服器，將電子郵件警示傳送至所有虛擬系統。在某些情況下，您可能希望為每個虛擬系統建立不同的服務路由。

當您是 ISP，需在單一 Palo Alto Networks 防火牆上支援多個個別租用戶時，就需要在虛擬系統層級設定服務路由。每個租戶都需要自訂服務路由來存取服務，例如 DNS、Kerberos、LDAP、NetFlow、RADIUS、TACACS+、多因素驗證、電子郵件、SNMP 設陷、syslog、HTTP、User-ID 代理程式、VM 監控器以及 Panorama（部署內容和軟體更新）。其他使用案例還包括想要為設定服務伺服器的群組提供完整自主性的 IT 組織。每個群組都可以有一個虛擬系統，並將定義其本身的服務路由。

您可以位虛擬系統中的服務路由選取虛擬路由器，但無法選取輸出介面。在您選取虛擬路由器，且防火牆從虛擬路由器傳送封包後，防火牆會根據目的地 *IP* 位址選取輸出介面。因此，如果虛擬系統有多個虛擬路由器，傳至所有服務伺服器的封包即必須只能從一個虛擬路由器輸出。具有介面來源位址的封包可以輸出不同的介面，但傳回流量將位於具有來源 *IP* 位址的介面上，因而產生不對稱的流量。

- 自訂虛擬系統服務的服務路由
- 為 PA-7000 系列防火牆設定依據虛擬系統的記錄
- 設定依據虛擬系統或防火牆的管理存取權

自訂虛擬系統服務的服務路由

如果啟用 Multi Virtual System Capability（多虛擬系統功能），任何未設定特定服務路由的虛擬系統，都將繼承防火牆的全域服務和服務路由設定。您也可以按照下列工作流程所述，設定虛擬系統使用不同服務路由。

具有多個虛擬系統的防火牆必須具有 IP 位址不重疊的介面和子介面。SNMP 設陷或 Kerberos 依個別虛擬系統的服務路由，僅適用於 IPv4。

服務的服務路由嚴格遵循您為服務設定伺服器設定檔的方式：

- 如果您為共用位置定義伺服器設定檔（**Device**（裝置） > **Server Profiles**（伺服器設定檔）），防火牆會為此服務使用全域服務路由。
- 如果您為特定虛擬系統定義伺服器設定檔，防火牆會為此服務使用虛擬系統特定的服務路由。
- 如果您為特定虛擬系統定義伺服器設定檔，但未為此服務設定虛擬系統特定的服務路由，防火牆會為此服務使用全域服務路由。

防火牆支援以虛擬系統為基準的 *syslog* 轉送。當防火牆上的多個虛擬系統使用 *SSL* 傳輸連接到 *syslog* 伺服器時，防火牆只能為安全通訊產生一個憑證。防火牆不支援讓每個虛擬系統有其本身的憑證。

©2024 Palo Alto Networks, Inc.

STEP 1 | 自訂虛擬系統的服務路由。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Services**（服務） > **Virtual Systems**（虛擬系統），然後選取您要設定的虛擬系統。
2. 按一下 **Service Route Configuration**（服務路由組態）連結。
3. 選取一個：
   - 繼承全域服務路由組態—使虛擬系統繼承與虛擬系統有關的全域服務路由設定。如果您選擇此選項，則跳過自訂步驟。
   - 自訂—可讓您指定每個服務的來源位址。
4. 如果您選擇 **Customize**（自訂），請根據服務的伺服器產品所使用的定址類型，選取 **IPv4** 或 **IPv6** 頁籤。您可以為服務同時指定 IPv4 和 IPv6 位址。按一下服務。（只有與虛擬系統相關的服務才可使用。）

   為了便於對多個服務使用相同來源位址，可選中服務的核取方塊，然後按一下 ***Set Selected Routes***（設定選定的路由），然後再繼續。

   - 若要限制來源位址的清單，可選取 **Source Interface**（來源介面），然後（從該介面）選取來源位址，作為服務路由。選取 **Any**（任何）來源介面會使虛擬系統所有介面的所有 IP 位址出現在來源位址清單中，供您選取。您可以選取 **Inherit Global Setting**（繼承全域設定）。
   - 如果您針對 **Source Interface**（來源介面）選取了 **Inherit Global Setting**（繼承全域設定），**Source Address**（來源位址）將會指出 **Inherited**（已繼承），否則，它會指出您選取的來源位址。如果您針對 **Source Interface**（來源介面）選取了 **Any**（任何），請選取 IP 位址，或輸入 IP 位址（使用與您選擇的頁籤相符的 IPv4 或 IPv6 格式），以指定傳送至外部服務的封包中所將使用的來源位址。
   - 如果您修改位址物件，且 IP 系列類型 (IPv4/IPv6) 有所變更，您必須進行 **Commit**（提交），才能更新所要使用的服務路由系列。
5. 按一下 **OK**（確定）。
6. 重複前面的步驟，以設定其他外部服務的來源位址。
7. 按一下 **OK**（確定）。

STEP 2 | Commit（提交）您的變更。

按一下 **Commit**（提交）與 **OK**（確定）。

如果您要設定依據虛擬系統的服務路由，以用於 PA-7000 系列防火牆的記錄服務，請繼續執行工作設定 PA-7000 系列防火牆針對每個虛擬系統進行記錄。

為 PA-7000 系列防火牆設定依據虛擬系統的記錄

針對流量、HIP 比對、威脅和 WildFire 日誌類型，PA-7000 系列防火牆不會將服務路由用於 SNMP 設陷、Syslog 和電子郵件服務。PA-7000 系列防火牆支援使用記錄日誌卡。

根據防火牆組態，您可能擁有下列卡類型其中之一：

 ©2024 Palo Alto Networks, Inc.

- 日誌處理卡 **(LPC)**—支援虛擬系統特定路徑；從 LPC 子介面到內部部署交換器，再到伺服器上的個別服務。針對系統和組態日誌，PA-7000 系列防火牆會使用全域服務路由，而不是 LPC。如果防火牆已安裝 LPC，您需要組態日誌卡連接埠。
- 日誌轉送卡 **(LFC)**—支援將所有資料層日誌高速轉送至外部日誌收集器（例如，Panorama 和 syslog 伺服器）。如果防火牆已安裝 LPC，您無需組態日誌卡連接埠。

> 從執行 *PAN-OS 10.1* 或更新版本的 *PA-7000 Series* 防火牆轉送系統日誌的唯一方法是設定 *LFC*。

> *LFC* 子介面尚不支援將日誌轉送至外部伺服器。

在其他 Palo Alto Networks 型號中，資料平面會將記錄服務路由流量傳送至管理平面，平面再將流量傳送至記錄伺服器。在 PA-7000 系列防火牆中，LPC 或 LFC 只有一個介面，而多個虛擬系統的資料平面會將記錄伺服器流量（前述類型）傳送至 PA-7000 系列防火牆記錄日誌卡。記錄日誌卡設定有多個子介面，可讓平台用來將記錄服務流量傳送至客戶的交換器，而交換器可連接到多個記錄伺服器。

每個子介面可分別以一個子介面名稱和一個點線子介面號碼來設定。子介面會指派給為記錄服務設定的虛擬系統。PA-7000 系列防火牆上的其他服務路由，運作方式與其他 Palo Alto Networks 平台上的服務路由相似。如需 LPC 或 LFC 的相關資訊，請參閱 PA-7000 系列硬體參考指南。

- 為 PA-7000 系列 LPC 設定依據虛擬系統的記錄
- 為 PA-7000 系列 LFC 設定依據虛擬系統的記錄

為 PA-7000 系列 LPC 設定依據虛擬系統的記錄

如果您在已安裝日誌處理卡 (LPC) 的 PA-7000 系列防火牆上啟用了多重虛擬系統功能，則可以按照下列工作流程所述，為不同的虛擬系統設定日誌記錄。

STEP 1 | 建立日誌卡子介面。

1. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），然後選取將作為日誌卡介面的介面。
2. 輸入 **Interface Name**（介面名稱）。
3. 對於 **Interface Type**（介面類型），選取 **Log Card**（日誌卡）。
4. 按一下 **OK**（確定）。

©2024 Palo Alto Networks, Inc.

STEP 2 | 在 LPC 實體介面上，為每個租用戶新增一個子介面。

1. 強調顯示屬於日誌卡介面類型的乙太網路介面，然後按一下 **Add Subinterface**（新增子介面）。
2. 針對 **Interface Name**（介面名稱），在句點之後輸入指派給租用戶之虛擬系統的子介面。
3. 針對 **Tag**（標籤），輸入 VLAN 標籤值。

   使用標籤的號碼與子介面號碼相同，以方便使用；但也可以用不同的號碼。

4. （選用）輸入 **Comment**（註解）。
5. 在 **Config**（組態）頁籤的 **Assign Interface to Virtual System**（將介面指派給虛擬系統）欄位中，選取 LPC 子介面所指派到的虛擬系統。或者，您可以按一下 **Virtual Systems**（虛擬系統），以新增虛擬系統。
6. 按一下 **OK**（確定）。

STEP 3 | 輸入指派給子介面的位址，然後設定預設閘道。

1. 選取 **Log Card Forwarding**（日誌卡轉送）頁籤，然後執行下列一或兩項：
   - 對於 IPv4 區段，輸入指派給子介面的 **IP Address**（**IP** 位址）和 **Netmask**（網路遮罩）。輸入 **Default Gateway**（預設閘道）（在路由資訊庫 (RIB) 中沒有已知的下一個躍點位址的封包將進行傳送的下一個躍點）。
   - 針對 IPv6 區段，輸入指派給子介面的 **IPv6 Address**（**IPv6** 位址）。輸入 **IPv6 Default Gateway**（**IPv6** 預設閘道）。
2. 按一下 **OK**（確定）。

STEP 4 | Commit（提交）您的變更。

按一下 **OK**（確定）與 **Commit**（提交）。

STEP 5 | 如果您尚未設定虛擬系統的其餘服務路由，請在此時設定。

自訂虛擬系統的服務路由。

為 PA-7000 系列 LFC 設定依據虛擬系統的記錄

如果您在已安裝日誌轉送卡 (LFC) 的 PA-7000 系列防火牆上啟用了多重虛擬系統 (multi-vsys) 功能，則可以為不同的虛擬系統設定日誌記錄。LFC 隨後可以將日誌轉送到 Panorama 日誌收集器或 syslog 伺服器。

您可以選擇只設定實體介面。由於 *LFC* 尚不支援透過子介面進行 *syslog* 轉送，每個虛擬系統都使用單一未標記的實體介面。

如果您將 *LFC* 子介面設定為從外部轉送日誌，介面將不再按預期工作。

©2024 Palo Alto Networks, Inc.

要為每個虛擬系統設定單獨的子介面，請新增子介面到實體介面，並指派必要的標籤來分割子介面流量。

對於由 *Panorama* 管理伺服器管理的 *PA-7000* 系列防火牆，如果 *LFC* 設定推送自 *Panorama*，則無法在防火牆上本機覆寫或還原 *LFC* 設定。要覆寫從 *Panorama* 推送的 *LFC* 設定，您必須登入防火牆 CLI 並刪除 *Panorama* 推送的設定。

```
admin> configure
```

```
admin# delete deviceconfig log-fwd-card
```

```
admin# 提交
```

設定依據虛擬系統或防火牆的管理存取權

如果您具有超級使用者管理帳戶，則您可以為 vsysadmin 或裝置管理員角色建立及設定細微權限。

STEP 1 | 建立管理員角色設定檔，以授予或停用管理員設定或唯讀網頁介面各個區域的權限。

1. 選取 **Device**（裝置） > **Admin Roles**（管理員角色），然後 **Add**（新增）**Admin Role Profile**（管理員角色設定檔）。
2. 輸入 **Name**（名稱），然後選擇性地輸入設定檔的 **Description**（說明）。
3. 針對 **Role**（角色），指定設定檔所影響到的控制層級：
   - 裝置—設定檔允許對全域設定和任何虛擬系統進行管理。
   - 虛擬系統—設定檔僅允許對指派給具有此設定檔之管理員的虛擬系統進行管理。（管理員將可存取**Device**（裝置） > **Setup**（設定） > **Services**（服務） > **Virtual Systems**（虛擬系統），但無法存取 **Global**（全域） 頁籤。）
4. 在管理員角色設定檔的 **Web UI**（網頁 **UI**）頁籤上，向下捲動至 **Device**（裝置），並保留綠色核取標記（啟用）。
   - 在 **Device**（裝置）下，啟用 **Setup**（設定）。在 **Setup**（設定）下，啟用此設定檔會其設定權限授予給管理員的區域，如下所示。（如果一項設定允許唯讀，唯讀鎖定圖示就會出現在啟用/停用輪換中。）
     - 管理—可讓具有此設定檔的管理員設定 **Management**（管理）頁籤上的設定。
     - 作業—可讓具有此設定檔的管理員設定 **Operations**（作業）頁籤上的設定。
     - 服務—可讓具有此設定檔的管理員設定 **Services**（服務）頁籤上的設定。管理員必須啟用 **Services**（服務），才能存取 **Device**（裝置） > **Setup Services**（設定服務） > **Virtual Systems**（虛擬系統）頁籤。如果 **Role**（角色） 在先前的步驟中指定為 **Virtual System**（虛擬系統），**Services**（服務）就會是唯一可在 r **Device**（裝置） > **Setup**（設定） 下啟用的設定。

©2024 Palo Alto Networks, Inc.

- 內容 **ID**—可讓具有此設定檔的管理員設定 **Content-ID**（內容 **ID**）頁籤上的設定。
- **WildFire**—可讓具有此設定檔的管理員設定 **WildFire** 頁籤上的設定。
- 工作階段—可讓具有此設定檔的管理員設定 **Session**（工作階段）頁籤上的設定。
- **HSM**—可讓具有此設定檔的管理員設定 **HSM** 頁籤上的設定。

5. 按一下 **OK**（確定）。
6. （選用）視需要重複整個步驟，以建立具有不同權限的另一個管理員角色設定檔。

STEP 2 | 將管理員角色設定檔套用至管理員。

1. 選取 **Device**（裝置）> **Administrators**（管理員），按一下 **Add**（新增），然後輸入管理員的 **Name**（名稱）。
2. （選用）選取驗證設定檔。
3. （選用）選取 **Use only client certificate authentication (Web)**（僅使用用戶端憑證驗證 **(Web)**）以啟用雙向驗證；使伺服器驗證用戶端。
4. 輸入 **Password**（密碼）和 **Confirm Password**（確認密碼）。
5. （選用）如果您想要使用採用 SSH 公開金鑰（而不只是密碼）、而更為嚴密的金鑰型驗證方法，請選取 **Use Public Key Authentication (SSH)**（使用公開金鑰驗證 **(SSH)**）。
6. 針對 **Administrator Type**（管理員類型），選取 **Role Based**（角色型）。
7. 針對 **Profile**（設定檔），選取您剛剛建立的設定檔。
8. （選用）選取密碼設定檔。
9. 按一下 **OK**（確定）。

STEP 3 | 提交組態。

按一下 **Commit**（交付）。

©2024 Palo Alto Networks, Inc.

虛擬系統的其他功能

每個虛擬系統的很多防火牆功能皆可加以設定、檢視、記錄或製成報告。因此在此不再贅述本文中其他相關位置所提及的虛擬系統。某些特定的章節如下所述：

- 如果您設定主動/被動 HA，則兩個防火牆必須有相同的虛擬系統功能 (單一或多個系統功能) 。請參閱 High availability（高可用性）。
- 若要為虛擬系統設定 QoS，請參閱設定虛擬系統的 QoS。
- 如需在使用子介面（與 VLAN 標籤）的虛擬介接部署中設定防火牆與虛擬系統的相關資訊，請參閱虛擬介接介面。
- 如果您已設定 User-ID 和多個虛擬系統，可在虛擬系統之間共享使用者對應。請參閱 在虛擬系統之間共享 User-ID 對應。

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

區域保護和 DoS 保護

將網路分割成多個功能區域和組織區域，可減小網路的受攻擊面—可能被攻擊者利用的網路部分。區域保護保護網路區域免遭爆流攻擊、偵察嘗試、基於封包的攻擊以及使用非 IP 通訊協定的攻擊。自訂區域保護設定檔以保護每個區域（您可以將相同的設定檔套用於類似區域）。拒絕服務 (DoS) 保護為特定重要系統防禦爆流攻擊，特別是使用者從網際網路存取的裝置（如 Web 伺服器和資料庫伺服器），並保護資源免受工作階段爆流攻擊。自訂 DoS 保護設定檔和原則規則，以保護每組重要裝置。造訪最佳做法說明文件入口網站，獲取區域保護和 DoS 保護最佳做法的檢查清單。

檢查並監控防火牆資料平面 *CPU* 耗用情況，確保每個防火牆大小適當，為 *DoS* 和區域保護以及任何其他耗用 *CPU* 週期的功能（如解密）提供支援。若您使用 *Panorama* 管理防火牆，請使用「裝置監控」（***Panorama*** > ***Managed Devices***（受管理的裝置）> ***Health***（健康））一次檢查和監控所有受管理防火牆的 *CPU* 耗用情況。

- 使用區域分割網路
- 區域如何保護網路？
- 區域防禦
- 設定區域保護以提升網路安全性
- 針對新工作階段流量湧入的 DoS 保護

使用區域分割網路

網路越大，越難保護。未分割的大型網路很難以進行管理和保護，因此受攻擊面很大。由於流量和應用程式能夠存取整個網路，一旦攻擊者取得網路存取權，將能夠在整個網路中存取關鍵資料。此外，大型網路也更難監控和控制。分割網路有助於透過阻止區域間橫向活動來限制攻擊者通過整個網路。

安全性區域是由一個或多個實體或虛擬防火牆介面以及與這些介面連線的網路區段構成的群組。您可以單獨控制對每個區域的保護，以便每個區域都能獲得所需的特定保護。例如，財務部門的網路區域可能不需要允許 IT 部門網路區域所允許的全部應用程式。

為了充分保護網路，所有流量必須要經過防火牆。設定介面和區域，為不同職能區域（如網際網路、閘道、敏感資料儲存區以及商業應用程式）和不同的組織群組（如財務、IT、行銷和工程部門）建立單獨的區域。如果功能、應用程式使用或使用者存取權限有邏輯分區，則您可以建立單獨的區域來隔離和保護相應區域，並套用適當的安全性原則規則，以防止不必要地存取僅某個或某些群組需要存取的資料和應用程式。區域越細微，您對網路流量的可見性和控制程度就越大。將網路分割成多個區域，有助於建立 零信任架構，從而執行不可信任何使用者、裝置、應用程式或封包並驗證一切的安全性理念。最終的目標是建立一個僅允許存取具有合法業務需求的使用者、裝置和應用程式，並拒絕所有其他流量。

正確限制和允許區域存取的方式視乎於網路環境。例如，在半導體製造車間或機器人裝配工廠等環境中，工作站控制著敏感的製作裝置或高度限制存取的區域，因此可能需要實施物理分割區域，禁止透過外部裝置存取（不允許透過行動裝置存取）。

在使用者可透過行動裝置存取網路的環境中，啟用 User-ID 和 App-ID 並將網路分割成多個區域，以確保無論在哪裡存取網路，使用者都能取得相應存取權限，因為存取權限與使用者或使用者群組繫結，而非與特定區域內的裝置繫結。

不同職能區域和群組的保護需求也可能不同。例如，處理較多流量的區域需要的流量保護臨界值可能與處理較少流量的區域不相同。分割網路的另一個原因是可以為每個區域定義相應的保護措施。具體的保護措施視乎於網路架構、要保護的對象以及要允許和拒絕的流量。

©2024 Palo Alto Networks, Inc.

區域如何保護網路？

區域不僅能透過將網路分割成更小、更易受管理的區域來保護網路，而且還能讓您可以控制對各區域的存取以及區域間的流量，從而進一步保護網路。

區域能夠防止非受控流量通過防火牆介面進入網路，因為在您將防火牆介面指派給區域之前，這些介面將無法處理流量。防火牆將對輸入介面（流量從這裡進入防火牆，流量方向為用戶端到相應伺服器 (c2s)）套用區域保護，以在流量進入區域之前進行篩選。

防火牆介面類型及區域類型（旁接、Virtual Wire、L2、L3、通道或外部）必須相符，這樣有助於保護網路，防止不屬於該區域的流量進入。例如，您可以將 L2 介面指派給 L2 區域或將 L3 介面指派給 L3 區域，但您不能將 L2 介面指派給 L3 區域。

此外，一個防火牆介面只能屬於一個區域。目的地區域不同的流量不能使用相同的介面，這有助於防止錯誤流量進入區域，讓您可以為每個區域設定相應的保護。您可以將多個防火牆介面連線至一個區域，以增大頻寬，但每個介面只能連線至一個區域。

防火牆允許流量進入某個區域後，流量將在該區域內自由流動，不會被記錄。區域越細小，您對存取該區域的流量的控制就越強，惡意軟體就越難在區域間的網路中橫向傳播。除非安全性原則規則允許並且區域類型（旁接、Virtual Wire、L2、L3、通道或外部）相同，否則流量不能在兩個區域之間流動。例如，安全性原則規則可能允許流量在兩個 L3 區域間流動，但不允許在 L3 區域和 L2 區域之間流動。當安全性原則規則允許區域間流量時，防火牆將記錄在區域之間流動的流量。

依預設，安全性原則規則會阻止流量在區域間橫向流動，因此惡意軟體無法取得區域的存取權，然後透過網路自由移動到另一個目標。

通道區域適用於非加密通道。您可以對通道內容和外部通道的區域套用不同的安全性原則規則，如通道內容檢查概述中所述。

©2024 Palo Alto Networks, Inc.

區域防禦

區域保護設定檔保護區域免遭爆流、偵察、基於封包的攻擊和基於非 IP 通訊協定的攻擊。DoS 保護原則規則中使用的 DoS 保護設定檔可以保護特定的重要裝置免遭目標爆流和基於資源的攻擊。DoS 攻擊將利用大量垃圾流量使網路或目標重要系統過載，從而使網路服務中斷。

規劃保護網路免受不同類型的 Dos 攻擊：

- 基於應用程式的攻擊—針對特定應用程式中的漏洞並嘗試耗盡其資源，以便合法使用者無法使用。其中一個範例為 Slowloris 攻擊。
- 基於通訊協定的攻擊—亦稱為狀態耗盡攻擊，這些攻擊針對的是通訊協定漏洞。一般範例為 SYN 爆流攻擊。
- 體積型攻擊—大容量的攻擊試圖佔用可用的網路資源，特別是頻寬，並癱瘓目標以防合法使用者存取這些資源。其中一個範例為 UDP 爆流攻擊。

沒有預設的區域保護設定檔或 DoS 保護設定檔和 DoS 保護原則規則。根據每個區域的流量特性設定並套用區域保護，以及根據意圖在每個區域保護的個別重要系統設定 DoS 保護。

- 區域防禦工具
- 區域防禦工具如何運作？
- 用於 DoS 保護的防火牆位置
- 區域保護設定檔
- 封包緩衝區保護
- DoS 保護設定檔和原則規則

區域防禦工具

需要使用分層方法才能有效防禦 Dos 攻擊。第一層防禦應該是面向網際網路之網路周邊的專用大容量 DDoS 保護裝置，以及周邊路由器、交換器或其他具有適當存取控制清單 (ACL) 之基於硬體的封包丟棄裝置，以抵禦基於工作階段的防火牆不能處理的體積型攻擊。防火牆會新增更精確的 DoS 攻擊防禦層，還提升對專用 DDoS 裝置未提供之應用程式流量的檢視能力。

Palo Alto Networks 防火牆提供四種互補工具，可為您的網路區域和重要裝置提供分層保護：

- 區域保護設定檔用於保護輸入區域邊緣免遭 IP 爆流攻擊、偵察連接埠掃描與主機掃描、基於 IP 封包的攻擊以及非 IP 通訊協定攻擊。輸入區域是流量從用戶端到伺服器 (c2s) 方向進入防火牆的區域，其中用戶端是流程的發起者，伺服器是回應者。透過將新的每秒連線數 (CPS) 限制為區域，區域保護設定檔根據進入區域的彙總流量提供針對 DoS 攻擊的第二層廣泛防禦。由於設定檔套用於進入區域的彙總流量，區域保護設定檔並未考慮個別裝置（IP 位址）。

  區域保護設定檔可在工作階段形成時，防火牆執行 DoS 保護原則和安全性原則規則查閱之前為網路提供保護，消耗的 CPU 週期數比 DoS 保護原則或安全性保護原則規則查閱少。如果區域保護設定檔拒絕了流量，防火牆不會在原則規則查閱上消耗 CPU 週期。

  將區域保護設定檔套用於每個區域（面向網際網路和內部）。

©2024 Palo Alto Networks, Inc.

- **DoS** 保護設定檔和原則規則用於保護特定個別端點和資源免遭爆流攻擊，尤其是使用者從網際網路中存取的高價值目標。雖然區域保護設定檔可以保護區域免受爆流攻擊，但具有適當 DoS 保護設定檔的 DoS 保護原則規則可以保護區域中的重要個別系統免受目標爆流攻擊，從而針對 DoS 攻擊提供精確的第三層防禦。

  由於 *DoS* 保護的目的是為重要裝置提供保護，且其消耗資源，*DoS* 保護僅保護您在 *DoS* 保護原則規則中指定的裝置。不保護其他裝置。

  DoS 保護設定檔設定了個別裝置或裝置群組的爆流保護臨界值（新 CPS 限制）、資源保護臨界值（針對指定端點和資源的工作階段限制）以及是對彙總流量還是分類流量套用設定檔。DoS 保護原則規則指定相符準則（來源、目的地、服務連接埠），流量與規則相符時要採取的動作，以及與每個規則相關聯的彙總和分類 DoS 保護設定檔。

  彙總 DoS 保護原則規則將彙總 DoS 保護設定檔中定義的 CPS 臨界值套用於符合 DoS 保護原則規則相符準則的所有裝置的組合流量。例如，如果將彙總 DoS 保護設定檔設定為將 CPS 速率限制為 20,000，則 20,000 的 CPS 限制會套用於整個群組的總連線數。在這種情況下，一個裝置可以接收大多數允許的連線。

  分類 DoS 保護原則規則將分類 DoS 保護設定檔中定義的 CPS 臨界值套用於符合原則規則的每個個別裝置。例如，如果將分類 DoS 保護設定檔設定為將 CPS 速率限制為 4,000，則群組中沒有任何裝置可以接受超過 4,000 的 CPS。DoS 保護原則可以有一個彙總設定檔和一個分類設定檔。

  分類設定檔可以按來源 *IP*、目的地 *IP* 或兩者對連線進行分類。對於面向網際網路的區域，由於無法擴充防火牆以保存網際網路路由表，按僅限目的地 *IP* 進行分類。

  僅將 DoS 保護套用於重要裝置，尤其是使用者從網際網路存取的常用攻擊目標，例如 Web 伺服器和資料庫伺服器。

- 對於現有工作階段，封包緩衝區保護使用臨界值和計時器來緩解濫用的工作階段，從而保護防火牆（以及區域）免遭試圖使防火牆封包緩衝區爆滿的單一工作階段 DoS 攻擊。您可以全域設定封包緩衝區保護，然後將其套用至每個區域。
- 安全性原則規則將影響工作階段的輸入和輸出流程。若要建立工作階段，傳入流量必須與現有安全性原則規則相符。如果不相符，防火牆將捨棄封包。安全性原則使用區域、IP 位址、使用

©2024 Palo Alto Networks, Inc.

者、應用程式、服務和 URL 類別等準則允許或拒絕區域之間（區域間）和區域內部（區域內）流量。

將最佳做法漏洞保護設定檔套用於每個安全性原則規則，以幫助抵禦 *DoS* 攻擊。

預設安全性原則規則將不允許流量在區域之間傳輸，因此如果您要允許區域間流量，需要再設定一個安全性原則規則。預設會允許所有區域內流量。您可以設定安全性原則規則來比對和控制區域內、區域間或通用（區域內和區域間）流量。

區域保護設定檔、*DoS* 保護設定檔和原則規則以及安全性原則規則僅影響防火牆上的資料平面流量。源於防火牆管理界面的流量不會通過資料平面，因此防火牆不會對照這些設定檔或原則規則比對管理流量。

- 您還可以按雜湊、CVE、特徵碼 ID、網域名稱、URL 或 IP 位址搜尋 Palo Alto Networks Threat Vault（需要有效的支援帳戶和登入）以發現威脅。

區域防禦工具如何運作？

當封包抵達防火牆時，防火牆會嘗試根據封包標頭中的輸入區域、輸出區域、來源 IP 位址、目的地 IP 位址、通訊協定以及應用程式，將封包與現有工作階段進行比對。如果防火牆發現二者相符，該封包將使用已控制工作階段的安全性原則規則。如果封包與現有工作階段不相符，防火牆將使用區域保護設定檔、DoS 保護設定檔與原則規則以及安全性原則規則，確定是建立工作階段還是捨棄封包，並確保封包接收的存取權層級。

在流量流經面向網際網路之網路邊緣的專用 DDoS 裝置後，防火牆套用的第一重保護是區域保護設定檔的廣泛防禦（若有附加到區域）。防火牆將確定封包將到達的介面區域（每個介面僅指派給一個區域，所有攜帶流量的介面必須屬於某一個區域）。若區域保護設定檔拒絕封包，則防火牆會捨棄封包並儲存資源，而不需查閱 DoS 保護原則或安全性原則。防火牆僅對新工作階段（與現有工作階段不相符的封包）套用區域保護設定檔。防火牆在建立工作階段後，將繞過區域保護設定檔查閱，以繼承該工作階段中的封包。

若區域保護設定檔沒有捨棄封包，則防火牆套用的第二重保護為 DoS 保護原則規則。若區域保護設定檔根據進入區域的彙總流量允許封包，則 DoS 保護原則規則可能會在以下情況下拒絕封包：封包將進入特定目的地或來自於特定來源，該目的地或特定來源超出了規則的 DoS 保護設定檔中的爆流保護或資源保護設定。如果封包與 DoS 保護原則規則相符，防火牆會對封包套用該規則。如果規則拒絕存取，防火牆將捨棄該封包，不會執行安全性原則查閱。如果規則允許存取，防火牆將執行安全性原則查閱。與區域保護設定檔一樣，防火牆只會對新工作階段強制執行 DoS 保護原則。

防火牆套用的第三重保護是安全性原則查閱，只有當區域保護設定檔和 DoS 保護原則規則允許封包時才會執行。如果防火牆發現封包與安全性原則規則不相符，則防火牆會捨棄封包。如果防火牆發現相符的安全性原則規則，則防火牆會對封包套用該規則。防火牆將在整個工作階段期間，同時對兩個方向（用戶端到伺服器和伺服器到用戶端）的流量強制執行安全性原則規則。將最佳做法漏洞保護設定檔 套用於所有安全性原則規則，以幫助抵禦 DoS 攻擊。

防火牆套用的第四重保護是封包緩衝區保護，可全域套用該保護以保護裝置，也可個別套用於區域，以防試圖使防火牆封包緩衝區爆滿的單一工作階段 DoS 攻擊。對於全域保護，當流量層次超

©2024 Palo Alto Networks, Inc.

過保護臨界值時，防火牆使用了隨機早期丟棄 (RED) 丟棄封包（不是工作階段）。對於每個區域的保護，若來源 IP 位址違反封包緩衝區臨界值，防火牆則會將其封鎖。與區域和 DoS 保護不同之處在於，封包緩衝區保護套用至現有工作階段。

用於 DoS 保護的防火牆位置

防火牆是一種基於工作階段的裝置，其設計不能擴充到數百萬的每秒連線數 (CPS) 來抵禦體積型 DoS 攻擊。防火牆將每個唯一流量（根據輸入和輸出區域、來源和目的地 IP、通訊協定及應用程式）視為工作階段，在連接埠和 IP 層次處消耗 CPU 週期進行封包檢查以顯示應用程式流量，並且必須計算爆流臨界值計數器的每個工作階段，因此防火牆位置對於避免防火牆發生爆流至關重要。

為了獲得最佳 DoS 保護，請將防火牆盡可能靠近您要保護的資源。這樣便可減少防火牆需要處理的工作階段數，進而減少提供 DoS 保護所需的防火牆資源量。

在面向網際網路的周邊處，請勿將用於 DoS 保護或區域保護的防火牆放在專用 DDoS 裝置和周邊路由器和交換器前面。使這些大容量裝置作為 DoS 防禦的第一道防線，可有效緩解體積型爆流攻擊。對於周邊處區域和 DoS 保護，請使用高容量防火牆並將其置於高容量裝置後面。一般來說，防火牆離周邊越近，處理流量所需的容量就越大。

將網路分割為區域的方式有助於緩解內部 DoS 攻擊。較小的區域可以更好地查看流量並防止惡意軟體橫向傳播，因為較多流量必須跨越區域，並且允許流量跨區域要求您建立特定的安全性原則規則（預設允許所有區域內流量）。如果您的網路相對未分割，請再次考慮您的分割方法。

用於設定爆流臨界值的基準線 CPS 測量

爆流保護臨界值確定以下項目允許的新每秒連線數 (CPS)：區域（區域保護設定檔）、區域內裝置的群組（彙總 DoS 保護原則）或區域內的個別裝置（分類 DoS 保護原則），還確定何時控制節流新連線以開始緩解潛在的爆流攻擊，以及何時捨棄所有新連線。預設的區域保護設定檔和 DoS 保護設定檔爆流保護臨界值不適用於大多數網路，因為每個網路都是唯一的。您必須瞭解每個區域以及意圖保護之個別關鍵系統的彙總正常 CPS 和尖峰 CPS，以便分別進行以下動作：設定有效的區域保護設定檔臨界值，以及設定有效的 DoS 保護設定檔臨界值，這不會意外地將臨界值設定過高而容許爆流攻擊，或者將臨界值設定過低而對流量進行控制節流。

- 要進行的 CPS 測量
- 如何測量 CPS

要進行的 **CPS** 測量

在至少五個工作日內或在您確信測量結果反映了網路的一般流量模式之後，測量平均 CPS 流量與尖峰 CPS 流量；測量週期越長，測量結果就越準確。考慮可能會突增您需要支援之 CPS 數量的特殊事件、季度事件和年度事件。如果防火牆有能力處理額外流量，您可能需要調整區域保護設定檔，並排程調整過後的 DoS 保護原則規則以適應這些類型的事件。進行以下基準線測量：

- 對於區域保護設定檔，請測量進入每個區域的平均 CPS 和尖峰 CPS。
- 對於彙總 DoS 保護設定檔，請測量要保護的每組裝置的綜合平均 CPS 和尖峰 CPS。
- 對於分類 DoS 保護設定檔，請測量要保護的個別裝置的平均 CPS 和尖峰 CPS。

©2024 Palo Alto Networks, Inc.

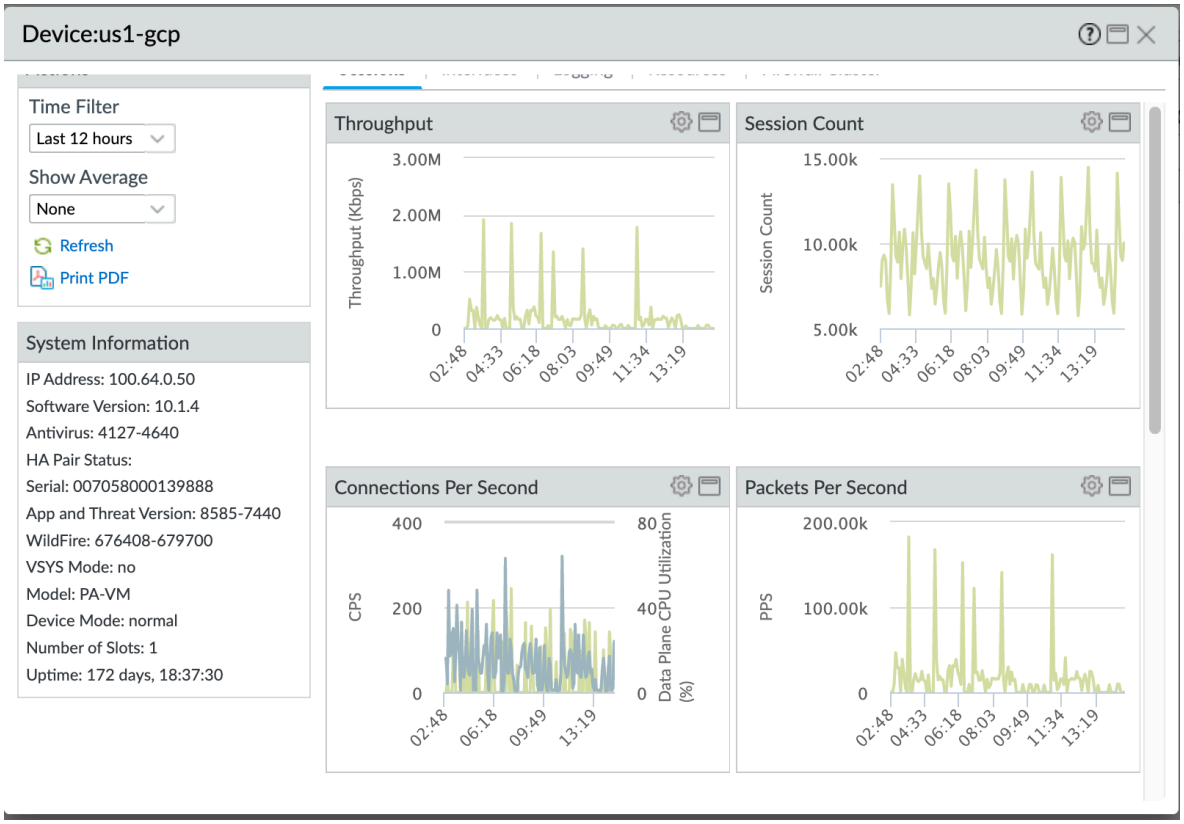
還要瞭解防火牆的容量以及其他消耗資源的功能（如解密）如何影響每個防火牆可以控制的連線數。一般來說，防火牆越接近外圍，其容量需求就越大，因為它需處理更多流量。每個防火牆型號的資料表包括防火牆支援的每秒新工作階段總數 (CPS)，防火牆比較工具可讓您比較其他防火牆型號的 CPS（和其他指標）。

如何測量 CPS

有許多方法可以測量 CPS，以幫助您設定區域保護設定檔和 DoS 防護設定檔洪水閾值設定：

- 針對區域保護設定檔閾值，如果您執行 PAN-OS 10.0 或更新版本，則測量 CPS 的最佳方法是使用來自 AIOps 雲端服務的區域保護設定檔閾值建議警示，此服務使用系統遙測來提供平均和平均尖峰 CPS 值的精確估計值。您可以為服務註冊防火牆和 Panorama。使用 PAN-OS 10.2.1 或更新版本，您可以先安裝用於 Panorama 的 AIOps 外掛程式，以在設定上主動強制執行安全性檢查，再將設定推送至受管理的防火牆。
- 如果您使用 Panorama 管理您的防火牆，請使用裝置監控測量傳入防火牆的 CPS。選擇一個裝置以查看測量值，該測量值可幫助您瞭解該裝置在可設定時間範圍內的 CPS，從而幫助您瞭解防火牆的容量。裝置監控還可以顯示 90 天的 CPU 平均趨勢線和尖峰使用情況，以助您瞭解每個防火牆的一般可用容量。要查看 CPS 如何影響防火牆資源，您可以將 CPS 與 CPU 使用率、封包緩衝區或封包描述元等指標疊加在同一時間線上：

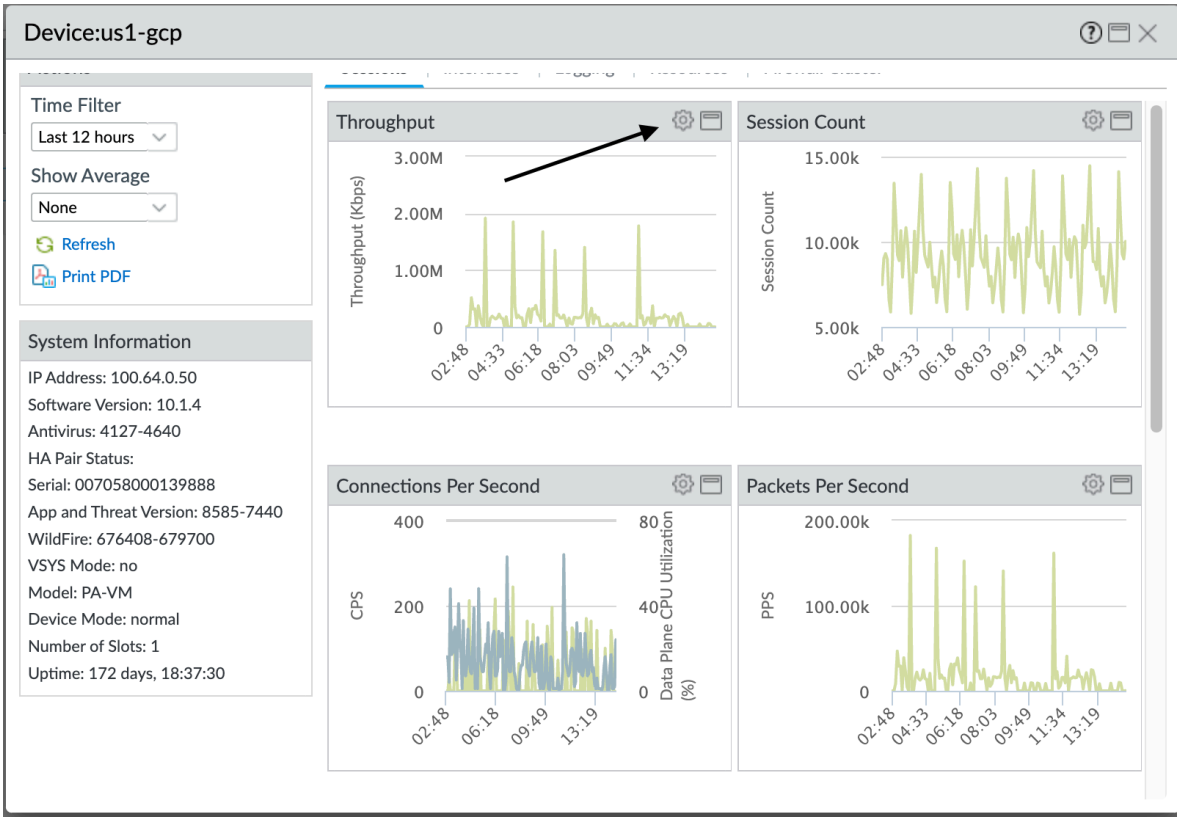
  1. **Panorama** > **Managed Devices**（受管理裝置） > **Health**（健康情況） > **All Devices**（所有裝置）。
  2. 按一下 **Device Name**（裝置名稱）以選擇裝置並檢視和篩選裝置資訊。



 ©2024 Palo Alto Networks, Inc.

3. 選擇齒輪圖示 ( ) 以存取裝置監控器註釋、覆疊和比較動作。

   您可以選擇對話方塊頂部的頁簽（未顯示）以查看更多指標。下圖顯示了 ***Sessions***（工作階段）頁籤。其他頁簽包括 ***Interfaces***（介面）、***Logging***（日誌記錄）、***Resources***（資源）和 ***Firewall Cluster***（防火牆叢集）。每個頁簽顯示不同的預設指標，對於每個預設指標，您可以覆疊其他指標，將所選裝置與其他裝置（包括裝置插槽和資料平面）進行比較，並對指標進行註釋。

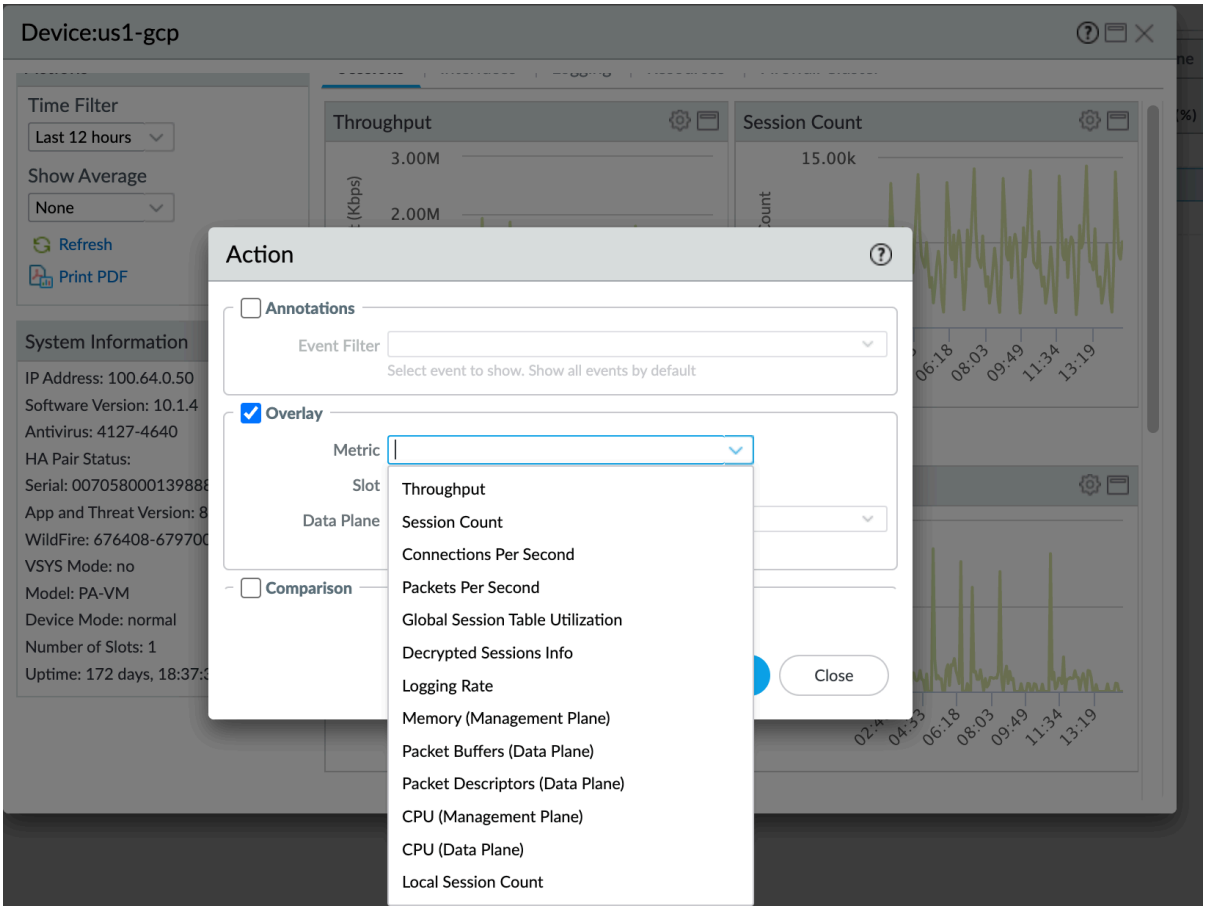


   前面的螢幕顯示過去 *12* 小時（***Time Filter***（時間篩選器））的 *CPS* 資料，上面覆疊了資料平面 *CPU* 使用率。下一步將向您展示如何在每個頁簽中的預設指標上覆疊指標。

4. 按一下齒輪圖示以查看您可以採取哪些動作來將其他指標覆疊在預設指標上。您可以在特定時間範圍內一次在每個預設指標上覆疊一個指標：

   1. 選擇 **Overlay**（覆疊）以查看覆疊選項，然後選擇 **Metric**（指標）下拉式清單。

©2024 Palo Alto Networks, Inc.



2. 您可以將這些指標中的任何一個覆疊在同一時間段內的預設指標上，以查看一個指標的狀態如何影響另一個指標。

   例如，在 **Sessions**（工作階段）頁簽上，您可以覆疊「資料平面封包緩衝區」或「資料平面封包描述元」，以查看高 CPS、輸送量、工作階段計數或每秒封包數 (PPS) 條件對封包緩衝區或封包描述元的影響。

   Sessions（工作階段）頁簽上的另一個範例是，將 CPS 輸送量或 PPS 與資料平面 CPU 和封包緩衝區指標覆疊，以查看流量峰值如何影響 CPU 和緩衝區。

   另一個範例是選擇 **Resources**（資源）頁簽，然後將資料平面 CPU 覆疊在封包緩衝區上，以查看封包緩衝區使用率如何影響 CPU。

   覆疊可幫助您查看趨勢和相關性，例如高緩衝區使用率是否與高 CPS 或 PPS 速率相關，並讓您瞭解 CPS 和 PPS 在影響 CPU、封包緩衝區或封包描述元之前可以達到多高。

5. 按一下 **OK**（確定）以查看資料覆疊並使用該資訊瞭解不同 CPS 負載和條件下的裝置資源行為。

- 要隨時間收集 CPS 資料以幫助設定區域保護設定檔閾值，如果您使用 SNMP 伺服器，則可以使用您自己的管理工具來輪詢 SNMP MIB。但是，重要的是要瞭解 MIB 中的 CPS 測量結果會顯示實際 CPS 值的兩倍（例如，如果真實 CPS 測量值為 10,000，則 MIB 會將值顯示為 20,000；發生這種情況是因為 MIB 分別計算 C2S 和 S2C 工作階段區段而不是單個工作階段）。您仍然可以從 MIB 中看到趨勢，且可以將 CPS 值除以二來得出真實值。SNMP MIB OID

©2024 Palo Alto Networks, Inc.

為：PanZoneActiveTcpCps、PanZoneActiveUdpCps 和 PanZoneOtherIpCps。由於防火牆僅每 10 秒進行一次測量和 SNMP 伺服器更新，因此每 10 秒鐘輪詢一次。

- 執行操作性 CLI 命令 **`show session info`**。

  您還可以使用操作 *CLI* 命令 ***`show counter interface`*** 查看 *CPS* 值，但此命令顯示實際 *CPS* 值的兩倍，因為它分別計算 *C2S* 和 *S2C* 工作階段區段而不是單個工作階段，因此需要將 *CPS* 值除以二才能得出真實的 *CPS* 值。

- **DoS** 防護設定檔可以保護伺服器免受 DoS 攻擊，還可以防止設定錯誤或遭入侵的伺服器攻擊您的網路。當 DoS 防護政策規則將伺服器指定為目的地時，表明您正在保護它免受 DoS 攻擊。當規則將伺服器指定為來源時，表明您正在保護您的網路免受來自該伺服器的無意或惡意攻擊。

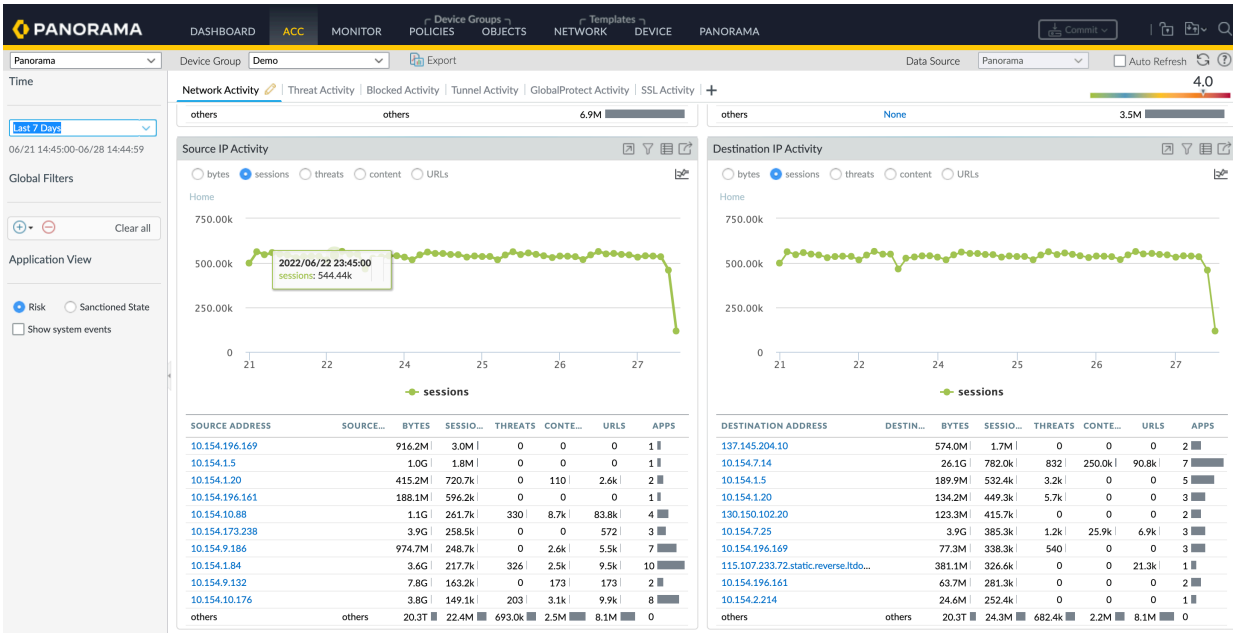
  要測量單個裝置的 CPS 或查看哪些裝置具有最高的 CPS 速率，以便您可以設定 DoS 防護設定檔閾值，請使用應用程式控管中心 (ACC)。ACC 顯示伺服器工作階段速率，讓您能夠計算單個裝置（針對分類的 DoS 防護政策規則）和裝置群組（彙總 DoS 防護政策規則）的平均 CPS。進行至少一周的測量；更長的時間週期提供更大的樣本量，因此可以獲得更具代表性的測量值。使用測量值瞭解您希望伺服器接收的正常連線數和峰值連線數，並根據這些測量值設定閾值。要查找在特定時間段內具有最高 CPS 速率的裝置：

  1. 選擇 **ACC**。
  2. 設定要查看其工作階段流量的 **Time**（時間）段。
  3. 在 **Network Activity**（網路活動）上，前往 **Source IP Activity**（來源 **IP** 活動）小工具和/或 **Destination IP Activity**（目的地 **IP** 活動）小工具，然後選擇 **sessions**（工作階段）（預設為 **bytes**（位元組））。您可以同時查看來源 IP 活動和目的地 IP 活動，以查看裝置產生的工作階段數（來源 IP）和裝置接收的工作階段數（目的地 IP）。
  4. 在小工具的來源位址表格中，按一下 **SESSIONS**（工作階段）以顯示在選定 **Time**（時間）內具有最高工作階段計數的來源 IP 位址。
  5. 要確定伺服器在選定 **Time**（時間）內的 CPS 值，請將工作階段數除以 **Time**（時間）中的秒數。例如，如果 **Time**（時間）設定為 **Last Hour**（最後一小時），則將工作階段數除以 3,600 秒即可得出 CPS 值。

  ACC 讓您瞭解一段時間內的平均 CPS 值。您可以查看過去一周、一個月或任何對您的環境有意義的時間段內的工作階段數，以瞭解裝置的工作階段負載。例如，要查看上週的工作階段活

©2024 Palo Alto Networks, Inc.

動，請將 **Time**（時間）設定為 **Last 7 Days**（過去 **7** 天），並將來源和目的地 IP 小工具設定為 **sessions**（工作階段）：



例如，要使用圖中的 ACC 資訊測量 CPS 以保護伺服器免受 DoS 攻擊，讓我們計算一下接收最多工作階段的伺服器在七天內的平均 CPS 值（**Destination IP Activity**（目的地 **IP** 活動）小工具中的 IP 位址 137.145.204.10）。我們將 170 萬個工作階段除以七天內的秒數（7 天 x 24 小時 x 60 分鐘 x 60 秒 = 604,800 秒）。該伺服器的平均值略低於每秒三個工作階段。測量一段時間內的 CPS，代表您要保護的伺服器的正常平均流量和峰值流量，並根據這些值設定初始閾值。觀察伺服器並根據需要調整閾值以調整 DoS 防護，以便既能夠保護伺服器，又不會不必要地限制合法連線。

- 測量分類 **DoS** 防護設定檔的 CPS — 分類 DoS 防護設定檔保護單個裝置。目標是在分類 DoS 防護設定檔中設定 CPS 閾值，並將該設定檔附加到 DoS 防護政策規則，該政策規則會套用

 ©2024 Palo Alto Networks, Inc.

至具有類似 DoS 攻擊閾值的特定伺服器。例如，您可以將分類 DoS 防護設定檔套用至 Web 伺服器或關鍵檔案伺服器，以防止 DoS 攻擊破壞它們的可用性。

您在設定檔中設定的閾值適用於政策規則中指定的每個單獨裝置。例如，如果您在分類 DoS 防護設定檔中設定最大速率 5,000 CPS，則關聯的 DoS 防護政策規則中的每個裝置最多只能接受 5,000 CPS，超過此數值就會丟棄新連線。

要計算平均和峰值 CPS 值，請在 **Global Filters**（全域篩選器）中指定要對其套用分類 DoS 防護的每台裝置的 IP 位址（您可以指定多個 IP 位址）。

1. 選擇要查看工作階段活動的 **Time**（時間）範圍。
2. 在 **Destination IP Activity**（目的地 **IP** 活動）小工具中選擇 **sessions**（工作階段）。
3. 在 **Global Filters**（全域篩選器）中指定要對其套用分類 DoS 防護的每台裝置的目的地 IP 位址（您可以指定多個 IP 位址）。

   您可以針對要保護之重要裝置的目的地 *IP* 位址，篩選防火牆流量日誌和威脅日誌，以獲取正常和峰值工作階段活動資訊。
4. 將工作階段值加在一起，然後將總數除以時間段內的秒數，得出 CPS 值。例如，在 30 天（2,592,000 秒）的時間段內，如果工作階段總數為 155,300,000，則該時間段內的平均 CPS 約為 60 CPS。
5. 檢查該時間段內的工作階段數是否足夠接近，以至於初始閾值可以保護每台裝置免受 DoS 攻擊，同時又不會導致裝置未得到充分利用。
6. 微調閾值以確保沒有任何受保護的伺服器成為 DoS 攻擊的受害者，同時為合法連線獲得最高的安全效能。

要計算平均峰值 CPS，請使用小工具中的圖形顯示來識別峰值工作階段時段，並從中計算平均峰值 CPS。

- 測量彙總 **DoS** 防護設定檔的 CPS — 彙總 DoS 防護設定檔保護裝置群組。目標是在彙總 DoS 防護設定檔中設定 CPS 閾值，並將該設定檔附加到 DoS 防護政策規則，該政策規則會套用至整個伺服器群組。彙總 DoS 防護在專用的大容量周邊 DDoS 裝置和防火牆的區域保護之後增加了另一層廣泛的保護。

  彙總設定檔不會像分類設定檔那樣，將設定的閾值套用至每個單獨的裝置。相反，該閾值適用於整個受保護群組。例如，如果您對包含五台伺服器的伺服器群組設定最大 CPS 閾值 20,000 個工作階段，則該群組可以支援的組合總工作階段數為 20,000 個工作階段。群組中單個伺服器的唯一限制是 20,000 個工作階段中有多少可用。一台裝置可以接收 15,000 CPS，則其他四台裝置總共只能接收最多 5,000 CPS。

  根據需要調整閾值。查找彙總設定檔的平均正常和峰值 CPS 的過程，與在 ACC 中查找分類設定檔的正常和峰值 CPS 的過程相同。請記住，對於彙總設定檔，您需要將閾值基於群組的總 CPS，而不是基於單個伺服器的 CPS。
- 為防止一台或多台伺服器無意或惡意攻擊您的網路，請將 CPS 測量值基於 **Source IP Activity**（來源 **IP** 活動）小工具，該小工具顯示伺服器產生的工作階段活動。按工作階段篩選以查看最活躍的伺服器，或使用 **Global Settings**（全域設定）按特定伺服器的來源 IP 位址進行篩選。在伺服器的 DoS 防護政策規則中，套用具有低閾值的 DoS 防護設定檔，以便伺

 ©2024 Palo Alto Networks, Inc.

服器無法中斷網路。例如，將 Alarm Rate 的閾值設為 10 CPS，將 Activate Rate 的閾值設為 20 CPS，以及將 Max Rate 的閾值設為 30 CPS，可確保防火牆將來源位址新增到硬體區塊表格中，而不是使用其他系統資源。

- 要設定彙總 **DoS** 防護設定檔閾值，您可以使用區域保護設定檔閾值測量值作為起點，如果您打算使用彙總 DoS 防護覆蓋區域中的大多數伺服器則尤為如此。如果區域僅包含您要對其套用彙總 DoS 防護設定檔的裝置，則 CPS 數量與區域保護設定檔數量完全相同。如果該區域包含您想要使用彙總 DoS 防護設定檔保護的裝置和您不想使用彙總 DoS 防護設定檔保護的裝置，您可以使用區域保護 CPS 測量值作為起點，並對閾值進行試驗以適當調整。
- 使用 Wireshark 或 NetFlow 等協力廠商工具收集和分析網路流量。
- 使用指令碼自動執行 CPS 資訊收集和連續監控作業，以及從日誌中發掘資訊。
- 將防火牆上的每個安全性原則規則設定為 **Log at Session End**（工作階段結束時記錄）。如果您沒有 NetFlow 或 Wireshark 之類的監控工具，且無法獲取或開發自動執行指令碼，則 **Log at Session End**（工作階段結束時記錄）會擷取工作階段結束時的連線數。儘管這不提供 CPS 資訊，但會顯示在所選持續時間內結束的工作階段數，您可以根據該資訊估算每秒的工作階段數。
- 與應用程式團隊合作理解到他們的伺服器的正常與峰值 CPS，以及這些伺服器可以支援的最大 CPS。

為了節省資源，防火牆以 *10* 秒的間隔測量彙總 *CPS*。由於這個原因，您在防火牆上看到的測量結果可能無法擷取十秒鐘間隔內的激增情況。儘管平均 *CPS* 測量結果不受影響，但尖峰 *CPS* 測量結果可能不准確。例如，如果防火牆日誌在 *10* 秒間隔內報告平均 *CPS* 為 *5,000*，則可能有 *4,000 CPS* 在一秒鐘內激增，而其他 *1,000 CPS* 在剩餘 *9* 秒內分散。

為爆流事件建立單獨的日誌轉送設定檔，以便相應的管理員接收僅包含爆流（潛在的 DoS 攻擊）事件的電子郵件。為區域保護和 DoS 保護臨界值事件組態日誌轉送。

實作區域和 *DoS* 保護後，使用這些方法監控部署，以便在網路發展和流量模式發生變化時，您可以調整爆流保護臨界值。

區域保護設定檔

對每個區域套用區域保護設定檔，以根據進入輸入區域的彙總流量保護整個區域。

除了設定區域保護和 *DoS* 保護之外，還應將最佳做法漏洞保護設定檔 套用於每個安全性原則規則，以幫助抵禦 *DoS* 攻擊。

- Flood 攻擊保護
- 偵察保護
- 封包式攻擊保護
- 通訊協定保護
- 乙太網路 SGT 保護

©2024 Palo Alto Networks, Inc.

Flood 攻擊保護

設定了爆流保護的區域保護設定檔保護整個輸入區域免遭 SYN、ICMP、ICMPv6、UDP 和其他 IP 爆流攻擊。防火牆將以新的每秒連線數 (CPS) 測量進入區域的每種爆流攻擊類型的彙總量，並將此總量與區域保護設定檔中設定的臨界值進行比較。（您可以使用 DoS 保護設定檔和原則規則保護區域內的重要個別裝置。）

測量並監控防火牆資料平面 *CPU* 耗用情況，確保每個防火牆大小適當，為 *DoS* 和區域保護以及任何其他耗用 *CPU* 週期的功能（如解密）提供支援。若您使用 *Panorama* 管理防火牆，則 裝置監控（***Panorama*** > ***Managed Devices***（受管理的裝置） > ***Health***（健康） > ***All Devices***（所有裝置））向您顯示了每個受管理防火牆的 *CPU* 與記憶體耗用情況。還可以顯示 *90* 天的 *CPU* 平均趨勢線和尖峰使用情況，以助您瞭解每個防火牆的一般可用容量。

對於每種爆流類型，為進入區域的新 CPS 設定三個臨界值，並可為 SYN 爆流設定捨棄 **Action**（動作）。若知道區域的基準線 CPS 速率，請使用這些準則設定初始臨界值，然後根據需要監控和調整臨界值。

- 警報速率—用於觸發警報的新 CPS 臨界值。目標是將 **Alarm Rate**（警報速率）設定為高於該區域平均 CPS 速率的 15-20#，這樣正常波動就不會產生警示。
- 啟動—新 CPS 臨界值，用於啟動爆流保護機制，並開始捨棄新連線。對於 ICMP、ICMPv6、UDP 和其他 IP 爆流，保護機制則為隨機早期丟棄 (RED)（也稱為隨機早期偵測）。僅對於 SYN 爆流，您可以將捨棄 **Action**（動作）設定為 SYN Cookie 或 RED。目標是將 **Activate**（啟動）速率設定為剛高於該區域的尖峰 CPS 速率以開始緩解潛在的爆流。
- 上限—當採用 RED 作為保護機制時，每秒連線數達到此臨界值後，將丟棄傳入的封包。目標是將 **Maximum**（最大）速率設定為防火牆容量的 80-90% 左右，並考量耗用防火牆資源的其他功能。

若您不知道區域的基準線 CPS 速率，請首先將 **Maximum**（最大）CPS 速率設定為防火牆容量的 80-90% 左右，並將其用於產生合理爆流緩解警報以及啟動速率。根據 Maximum（最大）速率，設定 **Alarm Rate**（警報速率）和 **Activate Rate**（啟動速率）。例如，您可以將 **Alarm Rate**（警報速率）設定為 **Maximum**（最大）速率的一半，並根據您收到的警報數量和消耗的防火牆資源進行調整。**Activate Rate**（啟動速率）開始丟棄連線，因此對其進行設定時要小心。由於正常流量負載會經歷一些波動，最好不要太武斷地丟棄連線。如果防火牆資源受到影響，則執行較高速率時出錯並調整速率。

©2024 Palo Alto Networks, Inc.

SYN 爆流保護是設定有捨棄 ***Action***（動作）的唯一類型。首先將 ***Action***（動作）設定為 ***SYN Cookie***。*SYN Cookie* 會公平地處理合法流量，只丟棄未通過 *SYN* 交握的流量，而使用隨機早期丟棄會隨機丟棄流量，因此 *RED* 可能會影響合法流量。但是，*SYN Cookie* 更佔用資源，因為防火牆充當目標伺服器的 *Proxy*，並處理伺服器的三方交握。權衡不丟棄合法流量 *(SYN Cookie)* 與保留防火牆資源 *(RED)*。監控防火牆，若 *SYN Cookie* 耗用過多資源，則切換到 *RED*。若在防火牆前面沒有專用的 *DDoS* 防禦裝置，請一律使用 *RED* 作為丟棄機制。

啟動 ***SYN Cookie*** 時，防火牆不會遵守伺服器傳送的 *TCP* 選項，因為在它代理 *SYN/ACK* 時並不知道這些值。因此，在 *TCP* 交握期間，無法交涉 *TCP* 伺服器的視窗大小和 *MSS* 值之類的值，防火牆會使用自己的預設值。在伺服器路徑的 *MSS* 小於防火牆的預設 *MSS* 值的場景中，封包將需要進行分段。

預設臨界值一般較大，以便區域保護設定檔不會意外地丟棄合法流量。將臨界值調整為適合網路流量的值。瞭解如何設定合理爆流臨界值的最佳方法是，對每種爆流類型進行平均 CPS 和尖峰 CPS 的基準線測量，以確定每個區域的正常流量情況，並瞭解防火牆的容量，包括其他消耗資源的功能（如解密）的影響。隨著網路發展，根據需要監控並調整爆流臨界值。

有多個資料層處理器 *(DP)* 的防火牆跨 *DP* 分配連線。一般而言，防火牆會平均跨 *DP* 分配 *CPS* 臨界值設定。例如，若防火牆有五個 *DP*，您可將 ***Alarm Rate***（警報速率）設定為 *20,000 CPS*，每個 *DP* 的 ***Alarm Rate***（警報速率）為 *4,000 CPS (20,000 / 5 = 4,000)*，因此若 *DP* 上的新工作階段超過 *4,000*，則會觸發該 *DP* 的 ***Alarm Rate***（警報速率）臨界值。

偵察保護

與軍事上的偵察定義相似，網路安全性方面的偵察定義為：攻擊者試圖透過秘密探查網路尋找弱點的方式，取得網路漏洞的資訊。偵察活動通常是網路攻擊的前奏。對所有區域啟用偵察保護可針對連接埠掃描和主機掃描進行防禦：

- 連接埠掃描用於探索網路上已開啟的連接埠。連接埠掃描工具將對主機上的多個連接埠號傳送用戶端要求，以尋找能夠在攻擊時利用的使用中連接埠。區域保護設定檔能針對 TCP 和 UDP 連接埠掃描進行防禦。
- 主機掃描用於檢查多個主機，以確定特定連接埠是否已開啟並存在漏洞。

您可以將偵察工具用於合法用途，例如對網路安全性或防火牆強度進行滲透測試。您可以指定最多 20 個要從偵察保護中排除的 IP 位址或網路遮罩位址物件，以便內部 IT 部門能夠進行滲透測試，尋找並修正網路漏洞。

您可以設定當偵察流量（不包括滲透測試流量）超出您設定偵察保護期間所設定閾值時要執行的動作。封鎖偵察作業之前，保留預設 **Interval**（間隔）和 **Threshold**（臨界值）以記錄幾個封包進行分析。

封包式攻擊保護

封包式攻擊有多種形式。區域保護設定檔將檢查 IP、TCP、ICMP、IPv6 和 ICMPv6 封包標頭，並透過下列方式保護區域：

©2024 Palo Alto Networks, Inc.

- 丟棄具有不適當特性的封包。
- 剝除封包中的不適當選項，然後再允許其進入區域。

若您設定基於封包的攻擊保護，請為每個封包類型選取丟棄特性。適用於每個 IP 通訊協定的最佳做法是：

- **IP Drop**（**IP** 丟棄）—丟棄 **Unknown**（未知）和 **Malformed**（錯誤）封包。允許這些選項則表示允許攻擊者繞過將目的地 IP 位址用作相符準則的安全性原則規則，因此還會丟棄 **Strict Source Routing**（嚴格來源路由）和 **Loose Source Routing**（鬆散來源路由）。僅對內部區域核取 **Spoofed IP Address**（偽造 **IP** 位址），因此僅具有符合防火牆路由表之來源位址的流量可以存取該區域。
- **TCP Drop**（**TCP** 丟棄）—保留預設 **TCP SYN with Data**（帶資料的 **TCP SYN**）和 **TCP SYNACK with Data**（帶資料的 **TCP SYNACK**）丟棄，丟棄 **Mismatched overlapping TCP segment**（不相符的重疊 **TCP** 區段）和 **Split Handshake**（分割交握）封包，然後從封包中剝離 **TCP Timestamp**（**TCP** 時間戳記）。

  將已提交的最新設定或編輯的安全性原則規則套用於現有工作階段的最佳做法是，啟用 ***Rematch Sessions***（重新比對工作階段）（***Device***（裝置） > ***Setup***（設定） > ***Session***（工作階段） > ***Session Settings***（工作階段設定））。然而，如果在區域上設定通道內容檢查且已啟用 ***Rematch Sessions***（重新比對工作階段），則還必須停用 ***Reject Non-SYN TCP***（拒絕非 ***SYN TCP***）（將選項從 ***Global***（全域）變更為 ***No***（否）），否則在啟用或編輯通道內容檢查原則時， 防火牆會丟棄所有現有通道工作階段。建立單獨的區域保護設定檔，可僅在具有通道內容檢查原則的區域上，且僅在啟用 ***Rematch Sessions***（重新比對工作階段）時停用 ***Reject Non-SYN TCP***（拒絕非 ***SYN TCP***）。
- **ICMP Drop**（**ICMP** 丟棄）—由於丟棄 ICMP 封包取決於如何使用 ICMP（或是否使用 ICMP），沒有提供最佳做法的標準設定。例如，若要封鎖 ping 活動，則可封鎖 **ICMP Ping ID 0**。
- **IPv6 Drop**（**IPv6** 丟棄）—如需遵從符合性，請確保防火牆丟棄包含不符合標準的路由標頭、延伸等的封包。
- **ICMPv6 Drop**（**ICMPv6** 丟棄）—如需遵從符合性，請確保防火牆在封包不符合安全性原則規則時丟棄某些封包。

通訊協定保護

在區域保護設定檔中，通訊協定保護可防禦基於非 IP 通訊協定的攻擊。啟用通訊協定保護，即可封鎖或允許Layer 2 VLAN 或 Virtual Wire（虛擬介接）上的安全性區域之間或 Layer 2 上單一區域內介面之間的非 IP 通訊協定（Layer 3 介面和區域會捨棄非 IP 通訊協定，因此不套用非 IP 通訊協定保護）。設定通訊協定保護 阻止安全性較低的通訊協定進入區域或區域內介面，以降低安全性風險並提高法規符合性。

如果未設定區域保護設定檔，致使同一區域內的非 *IP* 通訊協定從一個 *Layer 2* 介面轉到另一個介面，則根據預設區域內允許的安全性原則規則，防火牆會允許該流量。您可以建立區域保護設定檔，用於封鎖區域內的 LLDP 等通訊協定，以防透過其他區域介面發現可存取的網路。

©2024 Palo Alto Networks, Inc.

如果需要發現執行於網路上的非 IP 通訊協定，請使用 NetFlow、Wireshark 等監控工具或其他協力廠商工具發現網路上的非 IP 通訊協定。您可以封鎖或允許的非 IP 通訊協定範例包含 LLDP、NetBEUI、Spanning Tree 以及通用物件導向變電所事件 (GOOSE) 等監管控制及資料擷取 (SCADA) 系統等等。

建立 **Exclude List**（排除清單）或 **Include List**（包含清單）來為區域設定通訊協定保護。**Exclude List**（排除清單）為封鎖清單—防火牆會封鎖置於 **Exclude List**（排除清單）內的所有通訊協定，並允許所有其他通訊協定。**Include List**（包含清單）為允許清單—防火牆僅允許清單中指定的通訊協定，並允許所有其他通訊協定。

對通訊協定保護使用包含清單而非排除清單。包含清單僅專門認可您要允許的通訊協定，並封鎖網路上不需要或不知道的通訊協定，從而減少受攻擊面並封鎖未知流量。

清單最多支援 64 個 Ethertype 項目，每個項目均透過其 IEEE 十六位元組 Ethertype 代碼識別。Ethertype 代碼的其他來源包括 standards.ieee.org/develop/regauth/ethertype/eth.txt 和 http://www.cavebear.com/archive/cavebear/Ethernet/type.html。對具有彙總乙太網路 (AE) 介面的區域設定非 IP 通訊協定區域保護後，將無法僅在一個 AE 介面成員上封鎖或允許非 IP 通訊協定，因為 AE 介面成員被視為一個群組。

通訊協定保護並不允許封鎖 *IPv4 (Ethertype 0x0800)*、*IPv6 (0x86DD)*、*ARP (0x0806)* 或 *VLAN* 標記的框架 *(0x8100)*。即使您沒有明確列出 ***Include List***（包含清單） 中的這四種 *Ethertype*，防火牆也一律隱含地允許這些 *Ethertype*，但不允許您將其新增至 ***Exclude List***（排除清單）。

乙太網路 SGT 保護

在 Cisco TrustSec 網路中，Cisco Identity Services Engine (ISE) 會指派一個 16 位元的 Layer 2 安全性群組標籤 (SGT) 到使用者或端點的工作階段。當您的防火牆屬於 Cisco TrustSec 網路時，您可以建立具有乙太網路 SGT 保護的區域保護設定檔。防火牆可以檢查具有 802.1Q (Ethertype 0x8909) 的標頭中的特定 Layer 2 安全性群組標籤 (SGT) 值，如果 SGT 與您為附加到介面的區域保護設定檔設定的清單相符，則會丟棄封包。確定您想要拒絕哪些 SGT 值存取區域。

封包緩衝區保護

封包緩衝區保護可保護防火牆和網路免遭可能使防火牆封包緩衝區爆滿、造成合法流量被丟棄的單一工作階段 DoS 攻擊。雖然您未在區域保護設定檔或 DoS 保護設定檔或原則規則中設定封包緩衝區保護，但封包緩衝區保護仍會為輸入區域提供保護。雖然區域和 DoS 保護適用於新工作階段（連線）且非常精確，但封包緩衝區保護適用於現有工作階段且具有全域性。

您可以全域設定封包緩衝區保護 來保護整個防火牆，還可對每個區域啟用封包緩衝區保護以保護區域：

- 全域封包緩衝區保護—防火牆監控來自所有區域的工作階段（無論區域中是否啟用了封包緩衝區保護）以及這些工作階段如何利用封包緩衝區。您必須全域設定封包緩衝區保護（**Device**（裝置） > **Setup**（設定） > **Session Settings**（工作階段設定））以保護防火牆並對個別區域啟用封包緩衝區保護。當封包緩衝區消耗達到設定的 **Activate**（啟動）百分比時，防火

©2024 Palo Alto Networks, Inc.

牆使用隨機早期丟棄 (RED) 來丟棄來自入侵工作階段的封包（防火牆不會丟棄全域層次的完整工作階段）。

- 每個區域的封包緩衝區保護—對每個區域啟用封包緩衝區保護（**Network**（網路） > **Zones**（區域））以在第二層次保護中進行分層。當封包緩衝區消耗超過 **Activate**（啟動）臨界值並且全域保護開始將 RED 套用於工作階段流量時，將會啟動 **Block Hold Time**（封鎖保持時間）計時器。**Block Hold Time**（封鎖保持時間）是指入侵工作階段在防火牆封鎖整個工作階段之前可以繼續的時間量（以秒為單位）。入侵工作階段會保持為封鎖，直至 **Block Duration**（封鎖持續時間）到期為止。

您必須在全域啟用封包緩衝區保護以便其在區域中作用。

有兩種類型的封包緩衝區保護：

- 基於緩衝區使用率的封包緩衝區保護
- 基於延遲的封包緩衝區保護

基於緩衝區使用率的封包緩衝區保護

依預設啟用基於緩衝區使用率的封包緩衝區保護。依預設啟用基於緩衝區使用率的封包緩衝區保護。對一段時間內的防火牆封包緩衝區使用率進行基準線測量，直到您瞭解平常的使用情況。進行至少一個工作週的測量；但是，較長的測量週期可提供更好的基準線。要查看指定時間段的封包緩衝區使用率，請使用操作 CLI 命令：

```
admin1138@thxvm1>show running resource-monitor [day | hour | ingress-backlogs | minute | second | week]
```

CLI 命令提供指定時間段內緩衝區使用率的快照，但是既不是自動的也不是連續的。要自動連續進行封包緩衝區使用率測量，以便您可以監控行為變更和異常事件，請使用指令碼。您的 Palo Alto Networks 帳戶團隊可以提供一個範例指令碼，您可以對其進行修改以制定自己的指令碼；但是，該指令碼不受官方支援，且沒有針對指令碼使用或修改的技術支援。

如果基準線測量結果始終顯示異常高的封包緩衝區利用率，那對於一般流量負載，防火牆的容量可能不足。在這種情況下，請考慮調整防火牆部署的大小。否則，您需要仔細調整封包緩衝區保護臨界值，以防受影響的緩衝區溢出（並防止丟棄合法流量）。當防火牆大小適合部署時，只有攻擊才會導致緩衝區使用量大幅增加。

超限執行防火牆封包緩衝區會對防火牆的封包轉送功能產生負面影響。當緩衝區已滿時，任何介面上均沒有封包可以進入防火牆，而不僅僅是遭到攻擊的介面。

設定臨界值的最佳做法是：

- **Alert**（警示）和 **Activate**（啟動）—以預設臨界值開始，監控封包緩衝區使用率，並根據需要調整臨界值。**Alert**（警示）臨界值預設為 50%；當封包緩衝區使用率超過臨界值 10 秒時，防火牆會每分鐘在系統日誌中建立一個警示項目。**Activate**（啟動）臨界值預設為 80%；達到臨界值時，防火牆會開始將濫用最嚴重的工作階段減速。如果防火牆大小適當，緩衝區利用率應遠低於 50#。

©2024 Palo Alto Networks, Inc.

- **Block Hold Time**（封鎖保持時間）—當封包緩衝區利用率觸發 **Activate**（啟動）臨界值時，**Block Hold Time**（封鎖保持時間）會設定入侵工作階段在防火牆封鎖該工作階段之前可以繼續的時間量。**Block Hold Time**（封鎖保持時間）期間，防火牆繼續將 RED 套用於入侵工作階段的封包。以預設 **Block Hold Time**（封鎖保持時間）臨界值（60 秒）開始，監控封包緩衝區利用率，並根據需要調整臨界值。如果封包緩衝區利用率百分比在 **Block Hold Time**（封鎖保持時間）到期之前低於 **Activate**（啟動）臨界值，則計時器會進行重設並直到再次超過 **Activate**（啟動）臨界值時才會啟動 。增加 **Block Hold Time**（封鎖保持時間） 會對入侵工作階段施加更大的懲罰，減少則會對入侵工作階段施加較小的懲罰。
- **Block Duration**（封鎖持續時間）—當 **Block Hold Time**（封鎖保持時間）到期時，防火牆會在 **Block Duration**（封鎖持續時間）定義的時間段內封鎖入侵工作階段。以預設臨界值（3600 秒）開始，監控封包緩衝區利用率，並根據需要調整臨界值。當您對區域啟用封包緩衝區保護時，即使只有一個來自 IP 位址的工作階段過度使用封包緩衝區，**Block Duration**（封鎖持續時間）也會影響 IP 位址中的每個工作階段。如果您認為封鎖 IP 位址一小時（3600秒）的懲罰太大，請將 **Block Duration**（封鎖持續時間）減少到可接受的值。

除了監控個別工作階段使用緩衝區的情況，如果符合特定準則，封包緩衝區保護還可以封鎖 IP 位址。在防火牆監控封包緩衝區時，如果偵測到來源 IP 位址正在快速建立不會被單獨視為攻擊的工作階段，防火牆會在已設定的 **Block Duration**（封鎖持續時間）內封鎖該 IP 位址。

網路位址轉譯 (NAT)（一種使用來源 *NAT* 轉譯其網際網路連結流量的外部來源）可因 *IP* 位址轉譯活動而產生更大的封包緩衝區利用率。如果發生這種情況，請以懲罰個別工作階段的方式調整臨界值，但不會懲罰基礎 *IP* 位址（因此來自同一 *IP* 位址的其他工作階段不會受影響）。為此，請減少 ***Block Hold Time***（封鎖保持時間），以便防火牆封鎖更快地過度使用緩衝區的個別工作階段，並減少 ***Block Duration***（封鎖持續時間），以便不會對基礎 *IP* 位址進行不當懲罰。

基於延遲的封包緩衝區保護

作為基於使用率的封包緩衝區保護的替代方法，您可以觸發基於封包延遲的封包緩衝區保護，該延遲由資料平面封包緩衝引起，表明防火牆上出現擁塞。此類封包緩衝區保護透過向您發出擁塞警示並對封包執行隨機早期丟棄 (RED) 來減輕列首封鎖。基於延遲的封包緩衝區保護可以在對延遲敏感的通訊協定或應用程式受到影響之前觸發保護。

如果您的流量包含對延遲敏感的通訊協定或應用程式，那麼基於延遲的封包緩衝區保護將比基於緩衝區使用率的封包緩衝區保護更有幫助。

基於延遲的封包緩衝區保護包括設定 **Latency Alert**（延遲警示）臨界值（以毫秒為單位），超出該臨界值，防火牆將開始產生警示日誌事件。**Latency Activate**（延遲啟動）臨界值表示防火牆在傳入封包上啟動 RED 和開始產生啟動日誌的時間。**Latency Max Tolerate**（延遲最大容忍）臨界值表示防火牆使用具有幾乎 100% 丟棄率的 RED 的時間。

Block Hold Time（封鎖保持時間）和 **Block Duration**（封鎖持續時間）設定對基於延遲的封包緩衝區保護的作用與對基於使用率的封包緩衝區保護的作用相同。

©2024 Palo Alto Networks, Inc.

DoS 保護設定檔和原則規則

DoS 保護設定檔和 DoS 保護原則規則可共同保護重要資源特定群組以及個別重要資源免遭工作階段爆流攻擊。與保護整個區域免受爆流攻擊的區域保護設定檔相比，DoS 保護為特定系統提供了精確防禦，特別是使用者從網際網路存取的重要系統，通常是攻擊目標，如 Web 伺服器和資料庫伺服器。套用這兩種類型的保護，因為如果您只套用區域保護設定檔，則在每秒連線總數 (CPS) 未超過該區域的 **Activate**（啟動）和 **Maximum**（最大）速率時，便可順利發起以該區域內特定系統為目標的 DoS 攻擊。

DoS 保護佔用資源，因此僅將其用於重要系統。與區域保護設定檔類似，DoS 保護設定檔指定爆流臨界值。DoS 保護原則規則確定套用有 DoS 設定檔的裝置、使用者、區域和服務。

除了設定 *DoS* 保護和區域保護之外，還應將最佳做法漏洞保護設定檔套用於每個安全性原則規則，以幫助抵禦 *DoS* 攻擊。

- 分類 DoS 保護與彙總 DoS 保護
- DoS 保護設定檔
- DoS 保護原則規則

分類 DoS 保護與彙總 DoS 保護

您可以設定彙總與分類 DoS 保護設定檔，然後在設定 DoS 保護時將一個或每種類型的其中一種設定檔套用至DoS 保護原則規則。

- **Aggregate**（彙總）—設定套用至 DoS 保護原則規則中指定之整個裝置群組（而非每個個別裝置）的臨界值，因此一個裝置可以接收大部分容許的連線流量。例如，**Max Rate**（最大速率）為 20,000 CPS 表示該群組的總 CPS 為 20,000，若其他裝置沒有任何連線，則個別裝置最多可接收 20,000 CPS。在您要對特定子網路、使用者或服務套用額外限制時，彙總 DoS 保護原則為特定重要裝置群組提供另一層廣泛保護（在網際網路周邊與區域保護設定檔處的專用 DDoS 裝置之後）。
- **Classified**（分類）—設定套用至 DoS 保護原則規則中指定之每個個別裝置的爆流臨界值。例如，若將 **Max Rate**（最大速率）設為 5,000 CPS，則規則中指定的每個裝置在捨棄新連線之前最多可接受 5,000 CPS。如果將分類 DoS 保護原則規則套用於多個裝置，則受規則約束的裝置在容量以及您想要控制其 CPS 速率的方式上應該類似，因為分類臨界值套用於每個個別裝置。分類設定檔保護個別重要資源。

  若設定具有分類 DoS 保護設定檔的 DoS 保護原則規則（**Option/Protection**（選項/保護） > **Classified**（分類） > **Address**（位址）），請使用 **Address**（位址） 欄位，指定傳入連線是否根據與 **source-ip-only**（僅限來源 **IP**）、**destination-ip-only**（僅限目的地 **IP**） 或 **scr-dest-ip-both** 相符計入設定檔臨界值（防火牆會同時將來源 IP 與目的地 IP 位址相符項計入臨界值）。計數器耗用資源，因此位址相符項的計數方式會影響防火牆資源耗用情況。透過使用分類 DoS 保護，您可以：

  - 保護重要個別裝置，尤其是使用者透過網際網路存取並通常是攻擊目標的伺服器，例如 Web 伺服器、資料庫伺服器和 DNS 伺服器。在分類 DoS 保護設定檔中設定適當的爆流和資源保護臨界值。建立 DoS 保護原則規則，可透過新增 IP 位址作為規則的目的地準則，將設定檔

©2024 Palo Alto Networks, Inc.

套用至每個伺服器的 IP 位址，然後設定 **Address**（位址）為 **destination-ip-only**（僅限目的地 **IP**）。

請勿對分類 *DoS* 保護原則規則中面向網際網路的區域使用 ***source-IP-only***（僅限來源 ***IP***）或 ***src-dest-ip-both*** 分類，因為防火牆無法為網際網路上每個可能的 *IP* 位址儲存計數器。僅為內部區域或同一區域規則增加來源 *IP* 的臨界值計數器。在周邊區域，請使用 ***destination-ip-only***（僅限目的地 ***IP***）。

- 監控可疑主機或主機群組的 CPS 速率（包含主機的區域不能面向網際網路）。在分類 DoS 保護設定檔中設定適當的警報臨界值，以便在主機啟動異常大量的連線時通知您。建立 DoS 保護原則規則，可將設定檔套用至個別來源或來源位址群組，然後設定 **Address**（位址）為 **source-ip-only**（僅限來源 **IP**）。調查啟動的新連線觸發了警報的主機。

如何為分類設定檔組態 **Address**（位址）（**source-ip-only**（僅限來源 **IP**）、**destination-ip-only**（僅限目的地 **IP**）或 **src-dest-ip-both**）取決於您的 DoS 保護目標、要保護的內容以及受保護裝置是否位於面向網際網路的區域內。

由於計數器同時消耗來源 *IP* 位址和目的地 *IP* 位址（而非只是其中一個）的資源，防火牆會使用更多資源來追蹤作為 ***Address***（位址）的 ***src-dest-ip-both***，而不是追蹤 ***source-IP-only***（僅限來源 ***IP***）或 ***destination-ip-only***（僅限目的地 ***IP***）。

如果將彙總 DoS 保護設定檔和分類 DoS 保護設定檔同時套用於同一個 DoS 保護原則規則，則防火牆會先套用彙總設定檔，然後根據需要套用分類設定檔。例如，我們使用 DoS 保護原則規則中的兩種設定檔保護一組五個 Web 伺服器。若群組總計達到 25,000 CPS 的 **Max Rate**（最大速率），彙總設定檔組態會捨棄新連線。分類設定檔組態會在群組達到 6,000 CPS 的 **Max Rate**（最大速率）時捨棄該群組內任何個別 Web 伺服器的新連線。在三種情況下，新連線流量會超過 **Max Rate**（最大速率）臨界值：

- 新的 CPS 速率超出了彙總 **Max Rate**（最大速率），但未超出分類 **Max Rate**（最大速率）。在此種情況下，防火牆會套用彙總設定檔並在已設定的 Block Duration（封鎖持續時間）內封鎖所有新連線。
- 新的 CPS 速率未超出彙總 **Max Rate**（最大速率），但某個 Web 伺服器的 CPS 超出了分類 **Max Rate**（最大速率）。在此種情況下，防火牆會檢查彙總設定檔，並發現該群組的速率小於 25,000 CPS，因此防火牆不會藉此封鎖新連線。隨後，防火牆會檢查分類設定檔，並發現特定伺服器的速率超出了 6,000 CPS。防火牆會套用分類設定檔並在已設定的 Block Duration（封鎖持續時間）內封鎖該特定伺服器的新連線。由於群組內的其他伺服器位於分類設定檔的 **Max Rate**（最大速率）範圍內，其流量不受影響。
- 新的 CPS 速率超出了彙總 **Max Rate**（最大速率），還超出了其中一個 Web 伺服器的分類 **Max Rate**（最大速率）。在此種情況下，防火牆會檢查彙總設定檔，並發現該群組的速率超出了 25,000 CPS，因此防火牆會封鎖新連線以限制該群組的總 CPS。然後，防火牆會檢查分類設定檔，並發現特定伺服器的速率超出了 6,000 CPS（因此彙總設定檔強制執行了群組的組合限制，但這不足以保護此特定伺服器）。防火牆會套用分類設定檔並在已設定的 Block Duration（封鎖持續時間）內封鎖該特定伺服器的新連線。由於群組內的其他伺服器位於分類設定檔的 **Max Rate**（最大速率）範圍內，其流量不受影響。

©2024 Palo Alto Networks, Inc.

如果您希望彙總 *DoS* 保護設定檔和分類 *DoS* 保護設定檔均套用至相同流量，則必須將兩個設定檔套用於同一個 *DoS* 保護原則規則。若將彙總設定檔套用於一個規則並將分類設定檔套用於其他規則，即使它們指定的流量完全相同，防火牆也只能套用一個設定檔，因為防火牆會在流量與第一個 *DoS* 保護原則規則相符時執行該規則中指定的 ***Action***（動作），並且不與任何後續規則的流量進行比較，因此流量永遠不會與第二個規則相符，防火牆亦無法套用其動作。（這與安全性原則規則的工作方式相同。）

DoS 保護設定檔

DoS 保護設定檔組態臨界值，可防禦新工作階段 IP 爆流攻擊，並提供資源保護（限制指定端點與資源的最大並行工作階段數）。DoS 保護設定檔保護特定裝置（分類設定檔）與裝置群組（彙總設定檔）免遭 SYN、UDP、ICMP、ICMPv6 和其他 IP 爆流攻擊。設定 DoS 保護設定檔中的洪水保護閾值與設定區域保護設定檔中的 Flood 攻擊保護類似，但區域保護設定檔可保護整個進入區域，而 DoS 保護設定檔和政策規則更為細微且更具有針對性，甚至可以分類為單一裝置（IP 位址）。防火牆測量一組裝置的每秒連線總數 (CPS)（彙總設定檔），也可測量個別裝置的 CPS（分類設定檔）。

測量並監控防火牆資料平面 *CPU* 耗用情況，確保每個防火牆大小適當，為 *DoS* 和區域保護以及任何其他耗用 *CPU* 週期的功能（如解密）提供支援。若您使用 *Panorama* 管理防火牆，則 裝置監控（***Panorama*** > ***Managed Devices***（受管理的裝置） > ***Health***（健康） > ***All Devices***（所有裝置））向您顯示了每個受管理防火牆的 *CPU* 與記憶體耗用情況。還可以顯示 *90* 天的 *CPU* 平均趨勢線和尖峰使用情況，以助您瞭解每個防火牆的一般可用容量。

對於每個爆流類型，您可以將新 CPS 的三個臨界值設定給一組裝置（彙總）或個別裝置（分類）以及設定 **Block Duration**（封鎖持續時間），然後您可為 SYN 爆流設定捨棄 **Action**（動作）：

- **Alarm Rate**（警報速率）—當新 CPS 超出此臨界值時，防火牆會產生一個 DoS 警報。對於分類設定檔，請將速率設定為高於裝置的平均 CPS 速率的 15-20%，以便正常波動不會產生警示。對於彙總設定檔，請將速率設定為高於群組的平均 CPS 速率的 15-20%。
- **Activate Rate**（啟動速率）—當新 CPS 超出此臨界值時，防火牆將開始捨棄一些新連線，以緩解爆流攻擊，直至 CPS 速率降至此臨界值以下為止。對於分類設定檔，**Max Rate**（最大速率）應該是需要保護的裝置可接受的 CPS 速率（**Max Rate**（最大速率）將不會對關鍵裝置進行爆流攻擊）。您可以將 **Activate Rate**（啟動速率）的臨界值設定得與 **Max Rate**（最大速率）的臨界值一樣，以便防火牆不會在其達到 **Max Rate**（最大速率）之前使用 RED 或 SYN Cookie 開始捨棄流量。僅當您希望在達到 **Max Rate**（最大速率）之前捨棄流量時，將 **Activate Rate**（啟動速率）設定為低於 **Max Rate**（最大速率）。對於彙總設定檔，將臨界值設定為剛好高於該群組的平均尖峰 CPS 速率，以便使用 RED（或用於 SYN 爆流的 SYN Cookie）開始緩解爆流攻擊。
- **Max Rate**（最大速率）—當新 CPS 超出此臨界值時，防火牆會在指定的 **Block Duration**（封鎖持續時間）內封鎖（捨棄）來自入侵 IP 位址的所有新連線。對於分類設定檔，根據要保護之裝置的容量設定 **Max Rate**（最大速率）臨界值，以便 CPS 速率不會對這些裝置進行爆流攻擊。關於彙總設定檔，設定為群組容量的 80-90%。
- **Block Duration**（封鎖持續時間）—當新 CPS 超出 **Max Rate**（最大速率）時，防火牆會封鎖來自入侵 IP 位址的新連線。**Block Duration**（封鎖持續時間）指定防火牆繼續封鎖 IP 位址新連線

©2024 Palo Alto Networks, Inc.

的時間量。防火牆在封鎖新連線時，並不會對傳入連線進行計數，也不會增加臨界值計數器。對於分類和彙總設定檔，使用預設值（300 秒）來封鎖攻擊工作階段，而不會長時間處罰來源中的合法工作階段。

SYN 爆流保護是設定有捨棄 ***Action***（動作）的唯一類型。首先將 ***Action***（動作）設定為 ***SYN Cookie***。*SYN Cookie* 會公平地處理合法流量，只丟棄未通過 *SYN* 交握的流量，而使用隨機早期丟棄會隨機丟棄流量，因此 *RED* 可能會影響合法流量。但是，*SYN Cookie* 更佔用資源，因為防火牆充當目標伺服器的 *Proxy*，並處理伺服器的三方交握。權衡不丟棄合法流量 *(SYN Cookie)* 與保留防火牆資源 *(RED)*。監控防火牆，若 *SYN Cookie* 耗用過多資源，則切換到 *RED*。若在防火牆前面沒有專用的 *DDoS* 防禦裝置，請一律使用 *RED* 作為丟棄機制。

預設臨界值一般較大，以便 DoS 區域保護設定檔不會意外地丟棄合法流量。監控連線流量，並將臨界值調整為適合於網路的值。首先對每種爆流類型進行平均 CPS 和尖峰 CPS 的基準線測量，以確定要保護之重要裝置的正常流量情況。由於正常流量負載會經歷一些波動，最好不要太武斷地丟棄連線。隨著網路發展，根據需要監控並調整爆流臨界值。

設定爆流臨界值的另一種方法是，使用基準線測量來設定您想要允許的最大 CPS，並從該處返回以產生合理的爆流緩解警報和啟動速率。

有多個資料層處理器 *(DP)* 的防火牆跨 *DP* 分配連線。一般而言，防火牆會平均跨 *DP* 分配 *CPS* 臨界值設定。例如，若防火牆有五個 *DP*，您可將 ***Alarm Rate***（警報速率）設定為 *20,000 CPS*，每個 *DP* 的 ***Alarm Rate***（警報速率）為 *4,000 CPS (20,000 / 5 = 4,000)*，因此若 *DP* 上的新工作階段超過 *4,000*，則會觸發該 *DP* 的 ***Alarm Rate***（警報速率）臨界值。

除了設定 IP 爆流臨界值，您還可以使用 DoS 保護設定檔偵測並防禦工作階段資源消耗攻擊，此類攻擊會使用大量主機 (Bot) 盡可能建立最多工作階段來消耗目標資源。在設定檔的 **Resources Protection**（資源保護）頁籤上，您可以設定裝置（定義於套用了設定檔的 DoS 保護原則規則）可以接收的最大並行工作階段數目。當同時工作階段數目達到此最大限值時，將丟棄新工作階段。

要設定的並行工作階段最大數目具體取決於網路內容。瞭解要保護之資源（定義於附加有設定檔的 DoS 保護原則規則）可以處理的並行工作階段數目。將臨界值設定為資源容量的 80# 左右，然後根據需要監控和調整臨界值。

對於彙總設定檔，**Resources Protection**（資源保護）臨界值適用於原則規則中定義之裝置的所有流量（來源和目的地）。對於分類設定檔，**Resources Protection**（資源保護）臨界值適用於流量，具體取決於分類原則規則是套用於僅限來源 IP、僅限目的地 IP，還是同時套用於來源和目的地 IP。

DoS 保護原則規則

DoS 保護原則規則控制防火牆套用 DoS 保護的系統（您附加到 DoS 保護原則規則之 DoS 保護設定檔內設定的爆流臨界值），流量符合規則中定義的準則時要採取的動作，以及如何記錄 DoS 流量。由於 DoS 保護會消耗防火牆資源，僅將其用來保護特定的重要資源免遭工作階段爆流攻擊，尤其是使用者透過網際網路存取的一般目標（例如 Web 伺服器及資料庫伺服器）。使用區域保護設定檔可以保護整個區域免受爆流和其他攻擊。DoS 保護原則規則提供了細微的比對準則，以便您能靈活地定義要保護的項目：

 ©2024 Palo Alto Networks, Inc.

- 來源區域、介面、IP 位址（包括整個區域）和使用者。
- 目的地區域、介面和 IP 位址（包括整個區域）。
- 服務（依連接埠和通訊協定）。DoS 保護僅套用於您指定的服務。然而，指定服務並不會允許服務，並隱含地封鎖所有其他服務。指定服務會限制對這些服務的 DoS 保護，但不會封鎖其他服務。

除了保護關鍵伺服器上使用中的服務連接埠之外，您還可以保護關鍵伺服器上未使用的服務連接埠免遭 *DoS* 攻擊。對於關鍵系統，若要完成此動作，您可以建立一個 *DoS* 保護原則規則和設定檔來保護正在執行服務的連接埠，以及另一個 *DoS* 保護原則規則和設定檔來保護沒有執行服務的連接埠。例如，您可以使用一個原則/設定檔保護 *Web* 伺服器的一般服務連接埠（例如 *80* 和 *443*），並使用其他原則/設定檔保護所有其他服務連接埠。請留意防火牆的容量，以便為 *DoS* 計數器提供服務而不影響效能。

當流量與 DoS 保護原則規則相符時，防火牆將執行下列三種動作之一：

- 拒絕—防火牆將拒絕存取，不會套用 DoS 保護設定檔。與規則相符的流量會被封鎖。
- 允許—防火牆將允許存取，不會套用 DoS 保護設定檔。與規則相符的流量會被允許。
- 保護—防火牆保護 DoS 保護原則規則中定義的裝置，方法是將指定的 DoS 保護設定檔或設定檔臨界值套用於與規則相符的流量。規則可以具有一個彙總 DoS 保護設定檔和一個分類 DoS 保護設定檔，而對於分類設定檔，您可以使用來源 IP、目的地 IP 或兩者來增加爆流臨界值計數器，如分類 DoS 保護與彙總 DoS 保護中所述。如果符合規則，將對照這兩個 DoS 保護設定檔臨界值對傳入封包計數。

只有在 **Action**（動作）設為 **Protect**（保護）時，防火牆才會套用 DoS 保護設定檔。如果 DoS 保護原則規則的 **Action**（動作）設定為 **Protect**（保護），則在規則中指定相應的彙總及/或分類 DoS 保護設定檔，以便防火牆對符合規則的流量套用 DoS 保護設定檔的臨界值。大多數規則為 **Protect**（保護）規則。

Allow（允許）和 **Deny**（拒絕）動作使您可在較大群組中建立例外項，但不對流量套用 DoS 保護。例如，您可以拒絕來自大多數群組的流量，但允許該流量的子集。相反，您可以允許來自大多數群組的流量，但拒絕該流量的子集。

您可以 **Schedule**（排程） DoS 保護原則規則處於使用中狀態的時間（開始和結束時間、重複週期）。在一天或一星期的不同時間內套用不同的爆流臨界值便是排程的一個使用案例。例如，如果您的業務在夜間的流量明顯少於白天，則您可能希望在白天套用比夜晚更高的爆流臨界值。另一個使用案例是為特殊事件排程特殊臨界值，前提條件是防火牆支援 CPS 速率。

為了更方便地管理和提供精確的報告，請將 **Log Forwarding**（日誌轉送）設定為將 DoS 保護日誌與其他威脅日誌分開。除了將日誌轉送到伺服器（如 SNMP 或 syslog 伺服器）之外，還可以透過電子郵件將 DoS 臨界值違規事件直接轉送給管理員。如果防火牆大小適當，則不應頻繁地發生臨界值違規事件，並且這些違規事件將成為嘗試攻擊的強有力指標。

©2024 Palo Alto Networks, Inc.

設定區域保護以提升網路安全性

下列主題介紹了設定區域保護的範例：

- 設定偵察保護
- 設定基於封包的攻擊保護
- 設定通訊協定保護
- 設定封包緩衝區保護
- 基於延遲設定封包緩衝區保護
- 設定乙太網路 SGT 保護

設定偵察保護

為防火牆設定下列 偵察保護 動作，以回應相應的偵察：

- 允許—防火牆將允許連接埠掃描或主機掃描偵察繼續進行。
- 警示—在指定的時間間隔內，防火牆將針對每個符合所設定臨界值的連接埠掃描或主機掃描產生警示。警示為預設動作。
- 封鎖—防火牆將針對指定時間間隔的剩餘時間，丟棄來源與目的地之間所有後續封包。
- 封鎖 **IP**—防火牆針對指定 **Duration**（持續時間），丟棄所有後續封包（以秒為單位，範圍為 1-3600）。**Track By**（追蹤方式）決定了是封鎖來源流量還是來源及目的地流量。

STEP 1 | 設定偵察保護。

1. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **Zone Protection**（區域保護）。
2. 選取區域保護設定檔或 **Add**（新增）新的設定檔，並輸入 **Name**（名稱）。
3. 在 Reconnaissance Protection（偵察保護）頁籤上，選取要針對其實施保護的掃描類型。
4. 選取針對每種掃描的 **Action**（動作）。如果您選取 Block IP（封鎖 IP），則還必須設定**Track By**（追蹤方式）（來源或來源及目的地）以及 **Duration**（持續時間）。
5. 設定 **Interval**（間隔），單位為秒。此選項定義了連接埠掃描與主機掃描偵測的時間間隔。
6. 設定 **Threshold**（臨界值）。此臨界值定義了在所設定的間隔內發生的連接埠掃描和主機掃描次數，超過此次數後，將觸發相應動作。

©2024 Palo Alto Networks, Inc.

STEP 2 | （選用）設定來源位址排除。

1. 在 Reconnaissance Protection（偵察保護）頁籤上，**Add**（新增）來源位址排除。
   1. 為要排除的位址輸入描述性 **Name**（名稱）。
   2. 將 Address Type（位址類型）設定為 **IPv4** 或 **IPv6**，然後選取位址物件或輸入 IP 位址。
   3. 按一下 **OK**（確定）。
2. 按一下 **OK**（確定）來儲存區域防護設定檔。
3. **Commit**（提交）您的變更。

設定基於封包的攻擊保護

為了增強某個地區的安全性，封包式攻擊保護 允許您指定防火牆是丟棄具有某些特性的 IP、IPv6、TCP、ICMP 或 ICMPv6 封包還是將某些選項從封包中剝離。

例如，您可以在 TCP 三向交握期間，丟棄裝載中包含資料 TCP SYN 和 SYN-ACK 封包。依預設，區域保護設定檔將設定為丟棄包含資料的 SYN 和 SYN-ACK 封包（您必須將設定檔套用於相應區域）。

TCP 快速開啟選項 (RFC 7413) 將透過在裝載 SYN 和 SYN-ACK 封包時包含資料的方式保持連線速度。區域保護設定檔會區分使用 TCP 快速開啟選項的交握與其他 SYN 和 SYN-ACK 封包；依預設，該設定檔將設定為允許交握封包，只要這些封包中包含有效快速開啟 Cookie。

如果在升級至 *PAN-OS 8.0* 有正在使用的區域保護設定檔，這三項預設設定將套用於每個設定當，並且防火牆將相應地運作。

從 PAN-OS 8.1.2 及更高版本開始，您可以使用 CLI 命令（此工作中的步驟 4），使防火牆在其接收和丟棄以下類型的封包時產生威脅日誌，以便您可以更容易地分析這些事件並滿足稽核和符合性要求：

- Teardrop 攻擊
- 使用 Ping of Death 的 DoS 攻擊

此外，如果啟用相應的封包式攻擊保護，則使用同一 CLI 命令還可使防火牆產生以下類型封包的威脅日誌：

- 片段式 IP 封包
- IP 位址偽造
- 大於 1024 個位元組的 ICMP 封包
- 包含 ICMP 片段的封包
- 內嵌錯誤訊息的 ICMP 封包
- TCP 工作階段的第一個封包不是 SYN 封包

©2024 Palo Alto Networks, Inc.

STEP 1 | 建立區域保護設定檔並對封包式攻擊保護進行設定。

1. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **Zone Protection**（區域保護），然後 **Add**（新增） 新的設定檔。
2. 輸入設定檔的 **Name**（名稱），選擇性地輸入 **Description**（描述）。
3. 選取 **Packet Based Attack Protection**（基於封包的攻擊保護）。
4. 在每個頁籤（**IP Drop**（**IP** 丟棄）、**TCP Drop**（**TCP** 丟棄）、**ICMP Drop**（**ICMP** 丟棄）、**IPv6 Drop**（**IPv6** 丟棄）和 **ICMPv6 Drop**（**ICMPv6** 丟棄））上，選取您要執行以保護區域的封包式攻擊保護設定。
5. 按一下 **OK**（確定）。

STEP 2 | 將區域保護設定檔套用至將指派給您要保護之介面的安全性區域。

1. 選取 **Network**（網路） > **Zones**（區域），然後選取要指派區域保護設定檔的區域。
2. **Add**（新增）屬於虛擬路由器的 **Interfaces**（介面）。
3. 對於 **Zone Protection Profile**（區域保護設定檔），選取您剛剛建立的設定檔。
4. 按一下 **OK**（確定）。

STEP 3 | **Commit**（提交）您的變更。

STEP 4 | （PAN-OS 8.1.2 及更高版本）使防火牆能夠產生 Teardrop 攻擊與使用 Ping of Death 之 DoS 攻擊的威脅日誌；若啟用相應的封包式攻擊保護，則還會使防火牆產生上面所載之封包類型的威脅日誌（步驟 1）。例如，若對 **Spoofed IP address**（偽造 **IP** 位址）啟用封包式攻擊保護，則使用以下 CLI 會使防火牆在其接收和丟棄具有偽造 IP 位址的封包時產生威脅日誌。

1. 存取 CLI。
2. 使用操作 CLI 命令 **`set system setting additional-threat-log on`**。預設為 **`off`**。

設定通訊協定保護

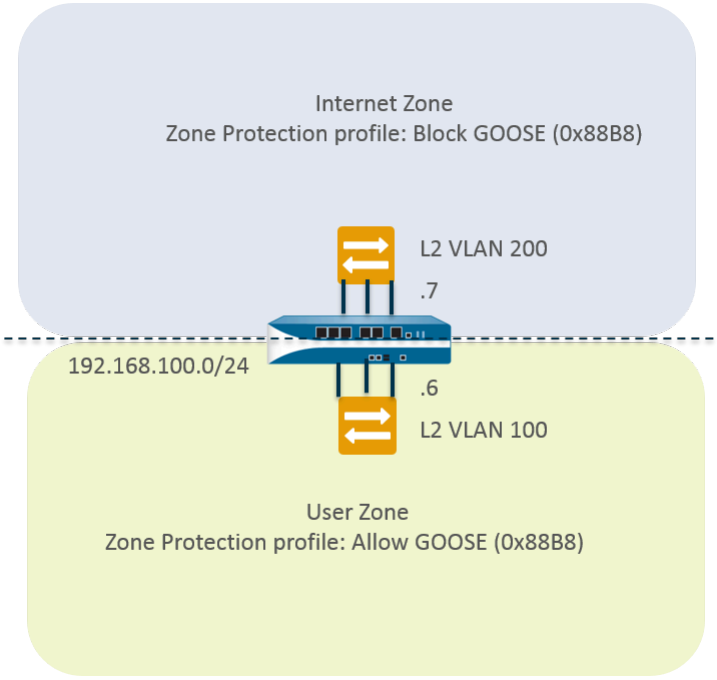
使用 通訊協定保護 保護 Virtual Wire（虛擬介接）或 Layer 2（第二層）安全性地區免遭非 IP 通訊協定封包的影響。

- 使用案例：Layer 2 介面上安全性區域之間的非 IP 通訊協定保護
- 使用案例：Layer 2 介面上安全性區域內的非 IP 通訊協定保護

使用案例：Layer 2 介面上安全性區域之間的非 IP 通訊協定保護

在此使用案例中，防火牆位於分割為兩個子介面的 Layer 2 VLAN 中。VLAN 100 為192.168.100.1/24，子介面 .6。VLAN 200 為192.168.100.1/24，子介面 .7。非 IP 通訊協定保護 適用於輸入區域。在此使用案例中，如果網際網路區域為輸入區域，則防火牆將封鎖通用物件導向變電所事件 (GOOSE) 通訊協定。如果使用者區域為輸入區域，則防火牆將允許 GOOSE 通訊協定。防火牆將在兩個區域中隱含地允許 IPv4、IPv6、ARP 以及 VLAN 標記的框架。

 ©2024 Palo Alto Networks, Inc.



STEP 1 | 設定 VLAN 子介面。

1. 選取 **Network**（網路） > **Interfaces**（介面） > **VLAN**，然後 **Add**（新增）介面。
2. **Interface Name**（介面名稱）預設為 vlan。在句點後，輸入 7。
3. 在 **Config**（組態）頁籤上，**Assign Interface To**（將介面指派給）**VLAN** 200。
4. 按一下 **OK**（確定）。
5. 選取 **Network**（網路） > **Interfaces**（介面） > **VLAN**，然後 **Add**（新增）介面。
6. **Interface Name**（介面名稱）預設為 vlan。在句點後，輸入 6。
7. 在 **Config**（組態）頁籤上，**Assign Interface To**（將介面指派給）**VLAN** 100。
8. 按一下 **OK**（確定）。

©2024 Palo Alto Networks, Inc.

STEP 2 | 在區域保護設定檔中設定通訊協定保護，以封鎖 GOOSE 通訊協定封包。

1. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **Zone Protection**（區域保護），然後 **Add**（新增） 設定檔。
2. 輸入 **Name**（名稱） Block GOOSE。
3. 選取 **Protocol Protection**（通訊協定保護）。
4. 將 **Rule Type**（規則類型）選為 **Exclude List**（排除清單）。
5. 輸入 **Protocol Name**（通訊協定名稱），即 GOOSE，以便在清單上識別 Ethertype。防火牆不會驗證您輸入的名稱是否與 Ethertype 代碼相符；它僅使用 Ethertype 代碼進行篩選。
6. 輸入 **Ethertype** 代碼 0x88B8。Ethertype 代碼前必須有 0x，以指示十六進位值。範圍為 0x0000 到 0xFFFF。
7. 選取 **Enable**（啟用）可強制執行通訊協定保護。您可以停用清單中的通訊協定，例如進行測試。
8. 按一下 **OK**（確定）。

STEP 3 | 對網際網路區域套用區域保護。

1. 選取 **Network**（網路） > **Zones**（區域），然後 **Add**（新增） 區域。
2. 輸入區域的 **Name**（名稱），Internet。
3. 對於 **Location**（位置），選取要套用該區域的虛擬系統。
4. 對於 **Type**（類型），選取 **Layer2**。
5. **Add**（新增）屬於該區域的**Interface**（介面），即 vlan.7。
6. 對於 **Zone Protection Profile**（區域保護設定檔），選取設定檔 Block GOOSE。
7. 按一下 **OK**（確定）。

STEP 4 | 設定通訊協定保護，以允許 GOOSE 通訊協定封包。

建立一個名稱為 Allow GOOSE 的區域保護設定檔，然後將 **Rule Type**（規則類型）選為 **Include List**（包含清單）。

在設定「包含清單」時，需包含所需的全部非 *IP* 通訊協定；不完整的清單可能會導致合法的非 *IP* 流量被封鎖。

STEP 5 | 對使用者區域套用區域保護。

1. 選取 **Network**（網路） > **Zones**（區域），然後 **Add**（新增） 區域。
2. 輸入區域的 **Name**（名稱），User。
3. 對於 **Location**（位置），選取要套用該區域的虛擬系統。
4. 對於 **Type**（類型），選取 **Layer2**。
5. **Add**（新增）屬於該區域的**Interface**（介面），即 vlan.6。
6. 對於 **Zone Protection Profile**（區域保護設定檔），選取設定檔 Allow GOOSE。
7. 按一下 **OK**（確定）。

©2024 Palo Alto Networks, Inc.

STEP 6 | 提交。

按一下 **Commit**（交付）。

STEP 7 | 檢視防火牆根據通訊協定保護丟棄的非 IP 封包數目。

存取 CLI。

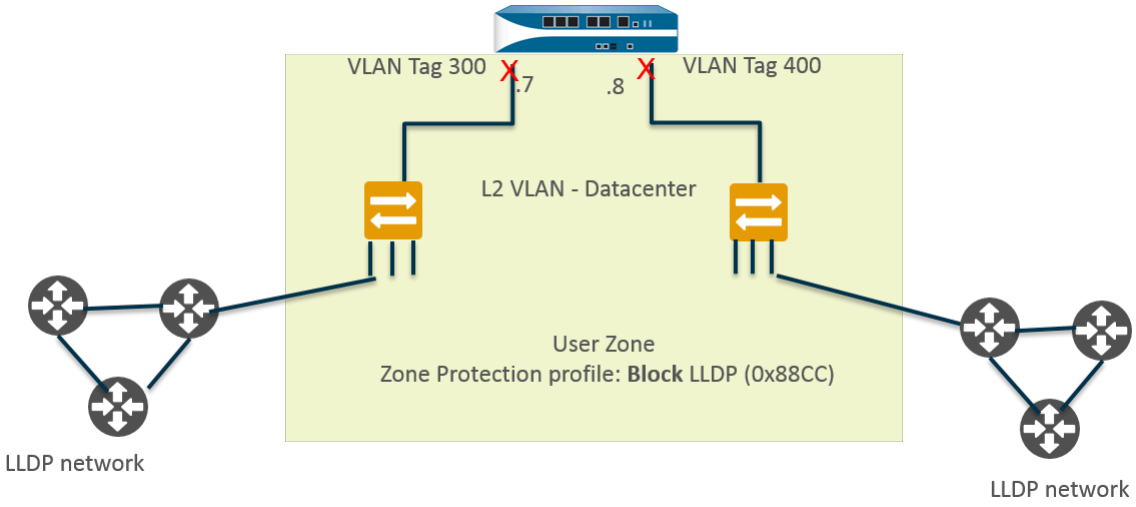
```
> show counter global name pkt_nonip_pkt_drop > show counter global
 name pkt_nonip_pkt_drop delta yes
```

使用案例：Layer 2 介面上安全性區域內的非 IP 通訊協定保護

如果您不實作具有非 IP 通訊協定保護的區域保護設定檔，防火牆將允許某個區域內的非 IP 通訊協定經由 Layer 2 介面到達另一個區域。在此使用案例中，封鎖 LLDP 封包可取保某個網路的 LLDP 不會探索可透過區域中另一個介面連線的網路。

在下圖中，名稱為 Datacenter 的 Layer 2 VLAN 分割為兩個子介面：192.168.1.1/24 子介面 .7 和 192.168.1.2/24 子介面 .8。VLAN 屬於使用者區域。對使用者區域套用將封鎖 LLDP 的區域保護設定檔後：

- 子介面 .7 將封鎖其交換器到防火牆的 LLDP（左側的紅色 X），防止流量進入子介面 .8。
- 子介面 .8 將封鎖其交換器到防火牆的 LLDP（右側的紅色 X），防止流量進入子介面 .7。



 ©2024 Palo Alto Networks, Inc.

STEP 1 | 為乙太網路介面建立一個子介面。

1. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），然後選取一個 Layer 2 介面，在此範例中選取 ethernet1/1。
2. 選取 **Add Subinterfaces**（新增子介面）。
3. **Interface Name**（介面名稱）預設為介面 (ethernet 1/1)。在句點後，輸入 7。
4. 對於 **Tag**（標籤），輸入 300。
5. 對於 **Security Zone**（安全性區域），選取 User（使用者）。
6. 按一下 **OK**（確定）。

STEP 2 | 為乙太網路介面建立第二個子介面。

1. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），然後選取 Layer 2 介面：ethernet1/1。
2. 選取 **Add Subinterfaces**（新增子介面）。
3. **Interface Name**（介面名稱）預設為介面 (ethernet 1/1)。在句點後，輸入 8。
4. 對於 **Tag**（標籤），輸入 400。
5. 對於 **Security Zone**（安全性區域），選取 User（使用者）。
6. 按一下 **OK**（確定）。

STEP 3 | 為 Layer 2 介面和兩個子介面建立 VLAN。

1. 選取 **Network**（網路） > **VLANs**，然後 **Add**（新增）VLAN。
2. 輸入 VLAN 的 **Name**（名稱）；在此範例中，為 Datacenter。
3. 對於 **VLAN Interface**（**VLAN** 介面），選取 **None**（無）。
4. 對於 **Interfaces**（介面），按一下 **Add**（新增），然後選取 Layer 2 介面：ethernet1/1 和兩個子介面：ethernet1/1.7 和 ethernet1/1.8。
5. 按一下 **OK**（確定）。

©2024 Palo Alto Networks, Inc.

STEP 4 | 在區域保護設定檔中封鎖非 IP 通訊協定封包。

1. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **Zone Protection**（區域保護），然後 **Add**（新增） 設定檔。
2. 輸入 **Name**（名稱），在此範例中，為 Block LLDP。
3. 輸入設定檔 **Description**（描述）—封鎖從 LLDP 網路到區域中其他介面的 LLDP 封包（區域內）。
4. 選取 **Protocol Protection**（通訊協定保護）。
5. 將 **Rule Type**（規則類型）選為 **Exclude List**（排除清單）。
6. 輸入 **Protocol Name**（通訊協定名稱）LLDP。
7. 輸入 **Ethertype** 代碼 0x88cc。Ethertype 代碼前必須有 0x，以指示十六進位值。
8. 選取 **Enable**（啟用）。
9. 按一下 **OK**（確定）。

STEP 5 | 對 Layer 2 VLAN 所屬的安全性區域套用區域保護設定檔。

1. 選取 **Network**（網路） > **Zones**（區域）。
2. **Add**（新增）區域。
3. 輸入區域的 **Name**（名稱），User。
4. 對於 **Location**（位置），選取要套用該區域的虛擬系統。
5. 對於 **Type**（類型），選取 **Layer2**。
6. **Add**（新增）屬於該區域的**Interface**（介面），即 ethernet1/1.7
7. **Add**（新增）屬於該區域的**Interface**（介面），即 ethernet1/1.8。
8. 對於 **Zone Protection Profile**（區域保護設定檔），選取設定檔 Block LLDP。
9. 按一下 **OK**（確定）。

STEP 6 | 提交。

按一下 **Commit**（交付）。

STEP 7 | 檢視防火牆根據通訊協定保護丟棄的非 IP 封包數目。

存取 CLI。

```
> show counter global name pkt_nonip_pkt_drop > show counter global
 name pkt_nonip_pkt_drop delta yes
```

設定封包緩衝區保護

您可在兩個層級上設定 Packet Buffer Protection（封包緩衝區保護）：裝置層級（全域），如果是全域啟用的話，則您也可在區域層級啟用。全域封包緩衝區保護（**Device**（裝置） > **Setup**（設定） > **Session**（工作階段））是為了保護防火牆資源並確保惡意流量不會導致防火牆成為無反應狀態。

©2024 Palo Alto Networks, Inc.

每個進入區域（**Network**（網路） > **Zones**（區域））的封包緩衝區保護為第二層保護，如果繼續超出封包緩衝區保護的臨界值，則會開始封鎖違規 IP 位址。防火牆能封鎖所有來自違規來源 IP 位址的流量。請記住，如果來源 IP 位址是轉譯的 NAT IP 位址，則許多使用者可使用相同的 IP 位址。如果一個濫用的使用者觸發了封包緩衝區保護，且輸入區域啟用了封包緩衝區保護，則當防火牆將 IP 位址放入其封鎖清單時，來自該違規來源 IP 地址（甚至來自非濫用使用者）的所有流量都可被封鎖。

封鎖針對防火牆後服務的 DoS 攻擊的最有效方法是在全域和每個輸入區域設定封包緩衝區保護。

您可以為一個區域 **Enable Packet Buffer Protection**（啟用封包緩衝區保護），但是只有您全域啟用封包緩衝區保護並指定設定後，對一個區域的設定才會生效。

STEP 1 | 啟用全域封包緩衝區保護。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Session**（工作階段），然後編輯 Session Settings（工作階段設定）。
2. 選取 **Packet Buffer Protection**（封包緩衝區保護）。
3. 定義封包緩衝區保護行為：
   - 警示 **(%)**—當封包緩衝區使用情況超過臨界值的時間多於 10 秒，則防火牆分鐘都會建立日誌事件。範圍為 0% 至 99%；預設值為 50%。若值為 0%，則防火牆不會建立日誌事件。
   - 啟動 **(%)**—當封包緩衝區使用情況超過此臨界值，則防火牆會開始他透過套用早期隨機丟棄 (RED) 減輕最濫用的工作階段。範圍為 0% 至 99%；預設值為 50%。若值為 0%，則防火牆不會套用 RED。如果濫用者正進入啟用了封包緩衝區保護的區域，則防火牆亦可丟棄濫用的工作階段或封鎖違規來源 IP 位址。從預設臨界值開始並根據需要進行調整。

     防火牆將記錄系統日誌中的警示事件，並記錄威脅日誌中的丟棄流量、捨棄工作階段以及封鎖 *IP* 位址事件。
   - 封鎖保留時間（秒）—在防火牆捨棄工作階段之前，允許 RED 降低的工作階段繼續進行的秒數。範圍為 0 至 65,535；預設值為 60。若值為 0，則防火牆不會根據封包緩衝區保護捨棄工作階段。
   - 封鎖持續時間（秒）—工作階段保持捨棄或 IP 位址保持封鎖狀態的秒數。範圍為 1 至 15,999,999；預設值為 3,600。
4. 按一下 **OK**（確定）。
5. **Commit**（提交）您的變更。

STEP 2 | 對輸入區域啟用其他封包緩衝區保護。

1. 選取 **Network**（網路） > **Zones**（區域）。
2. 選擇輸入區域，然後按一下其名稱。
3. 在「區域保護」區段中 **Enable Packet Buffer Protection**（啟用封包緩衝區保護）。
4. 按一下 **OK**（確定）。
5. **Commit**（提交）您的變更。

©2024 Palo Alto Networks, Inc.

基於延遲設定封包緩衝區保護

設定基於延遲的封包緩衝區保護，並將其套用至具有包含延遲敏感的通訊協定和應用程式之流量的區域。

STEP 1 | 選取 **Device**（裝置） > **Setup**（設定） > **Session**（工作階段）。

STEP 2 | 編輯「工作階段設定」區段，並啟用 **Packet Buffer Protection**（封包緩衝區保護）。

STEP 3 | 啟用 **Buffering Latency Based**（基於緩衝延遲）。

STEP 4 | 輸入 **Latency Alert (milliseconds)**（延遲警示（毫秒））臨界值，如果超過該臨界值，防火牆將開始每分鐘產生一個警示日誌事件；範圍為 1 到 20,000；預設值為 50。

STEP 5 | 輸入 **Latency Activate (milliseconds)**（延遲啟動（毫秒））臨界值，如果超過該臨界值，防火牆將啟動傳入封包的隨機早期丟棄 (RED)，並開始每 10 秒產生一次啟動日誌；範圍為 1 到 20,000 毫秒；預設值為 200 毫秒。

STEP 6 | 輸入 **Latency Max Tolerate (milliseconds)**（延遲最大容忍（毫秒））臨界值，如果超過該臨界值，防火牆將使用接近 100% 丟棄可能性的 RED；範圍為 1 到 20,000 毫秒；預設值為 500 毫秒。

如果當前延遲是介於 **Latency Activate**（延遲啟動）臨界值和 **Latency Max Tolerate**（延遲最大容忍）臨界值之間的值，防火牆會按以下方式計算 RED 丟棄可能性：（當前延遲 - **Latency Activate**（延遲啟動）臨界值）/（**Latency Max Tolerate**（延遲最大容忍）臨界值 - **Latency Activate**（延遲啟動）臨界值）。例如，如果當前延遲為 300，**Latency Activate**（延遲啟動為 200，**Latency Max Tolerate**（延遲最大容忍）為 500，那麼 (300-200)/(500-200) = 1/3，意味著防火牆使用大約 33% 的 RED 丟棄可能性。

STEP 7 | 根據使用率，為 Packet Buffer Protection（封包緩衝區保護）設定 **Block Hold Time**（封鎖保持時間）和 **Block Duration**（封鎖持續時間）。

STEP 8 | 按一下 **OK**（確定）。

STEP 9 | 為您想要基於延遲進行封包緩衝區保護的每個區域啟用第二層保護。

1. 選取 **Network**（網路） > **Zones**（區域），然後選取一個區域。
2. 啟用 **Packet Buffer Protection**（封包緩衝區保護）。

STEP 10 | **Commit**（認可）。

設定乙太網路 SGT 保護

使用以下工作設定 乙太網路 SGT 保護 設定檔。

©2024 Palo Alto Networks, Inc.

STEP 1 | 建立區域保護設定檔以提供乙太網路 SGT 保護。

1. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **Zone Protection**（區域保護）。
2. 按 **Name**（名稱）**Add**（新增）區域保護設定檔。
3. 選取 **Ethernet SGT Protection**（乙太網路 **SGT** 保護）。
4. 按名稱 **Add**（新增）**Layer 2 SGT Exclude List**（第二層 **SGT** 排除清單）。
5. 為清單輸入一個或多個 **Tag**（標籤）值；範圍為 0 到 65,535。您可以輸入標籤值的連續範圍（例如，100-500）作為單個項目。您可以在排除清單中新增最多 100 個（單個或範圍）標籤項目。
6. **Enable**（啟用）Layer 2 SGT 排除清單。您可以隨時停用該清單。
7. 按一下 **OK**（確定）。

STEP 2 | 將區域保護設定檔套用至 Layer 2、虛擬介接或旁接介面所屬的安全性區域。

1. 選取 **Network**（網路） > **Zones**（區域）。（網路 > 區域）
2. **Add**（新增）區域。
3. 輸入區域的 **Name**（名稱）。
4. 對於 **Location**（位置），選取要套用該區域的虛擬系統。
5. 對於 **Type**（類型），選取 **Layer2**（第二層）、**Virtual Wire**（虛擬介接）或 **Tap**（旁接）。
6. **Add**（新增）屬於該區域的 **Interface**（介面）。
7. 對於 **Zone Protection Profile**（區域保護設定檔），選取您建立的設定檔。
8. 按一下 **OK**（確定）。

STEP 3 | **Commit**（認可）。

STEP 4 | 檢視由於採用乙太網路 SGT 保護的所有區域保護設定檔而導致防火牆丟棄的封包的全域計數器。

1. 存取 CLI。
2. **`> show counter global name pan_flow_dos_l2_sec_tag_drop`**

 ©2024 Palo Alto Networks, Inc.

針對新工作階段流量湧入的 DoS 保護

對新工作階段流量的 DoS 保護有益於避免大量單一工作階段與多工作階段攻擊。在單一工作階段攻擊中，攻擊者會使用單一工作階段來將防火牆背後的設備定為目標。如果安全性規則允許流量，則會建立工作階段，且攻擊者會透過以相同的來源 IP 位址與連接埠號碼、目的地 IP 位址與連接埠號碼，以及通訊協定，高速率傳送封包，嘗試癱瘓目標，來發起攻擊。在多工作階段攻擊中，攻擊者會從單一主機中使用多個工作階段 (或每秒連線 [cps]) 來發動 DoS 攻擊。

此功能只能防禦新工作階段的 *DoS* 攻擊，即尚未卸載至硬體的流量。卸載的攻擊不受此功能保護。但是，本主題說明您可以如何建立安全性原則規則來重設用戶端；攻擊者會以許多每秒連線重新啟動攻擊，且會被本主題中所述的防禦封鎖。

DoS 保護設定檔和原則規則 將共同協作，針對大量傳入 SYN、UDP、ICMP 和 ICMPv6 封包以及其他類型 IP 封包提供洪水攻擊防護。確定構成流量攻擊的臨界值。一般而言，DoS 保護設定檔中設定了防火牆產生 DoS 警報、執行隨機早期丟棄等動作以及丟棄額外傳入連線的臨界值。設定用於保護（而不是允許或拒絕封包）的 DoS 保護原則規則決定了封包的比對準則（例如來源位址），以便針對臨界值進行計數。這種靈活性讓您可以封鎖某些流量或允許某些流量，並將其他流量視作 DoS 流量。當傳入速率超過最大臨界值時，防火牆將封鎖來自來源位址的流量。

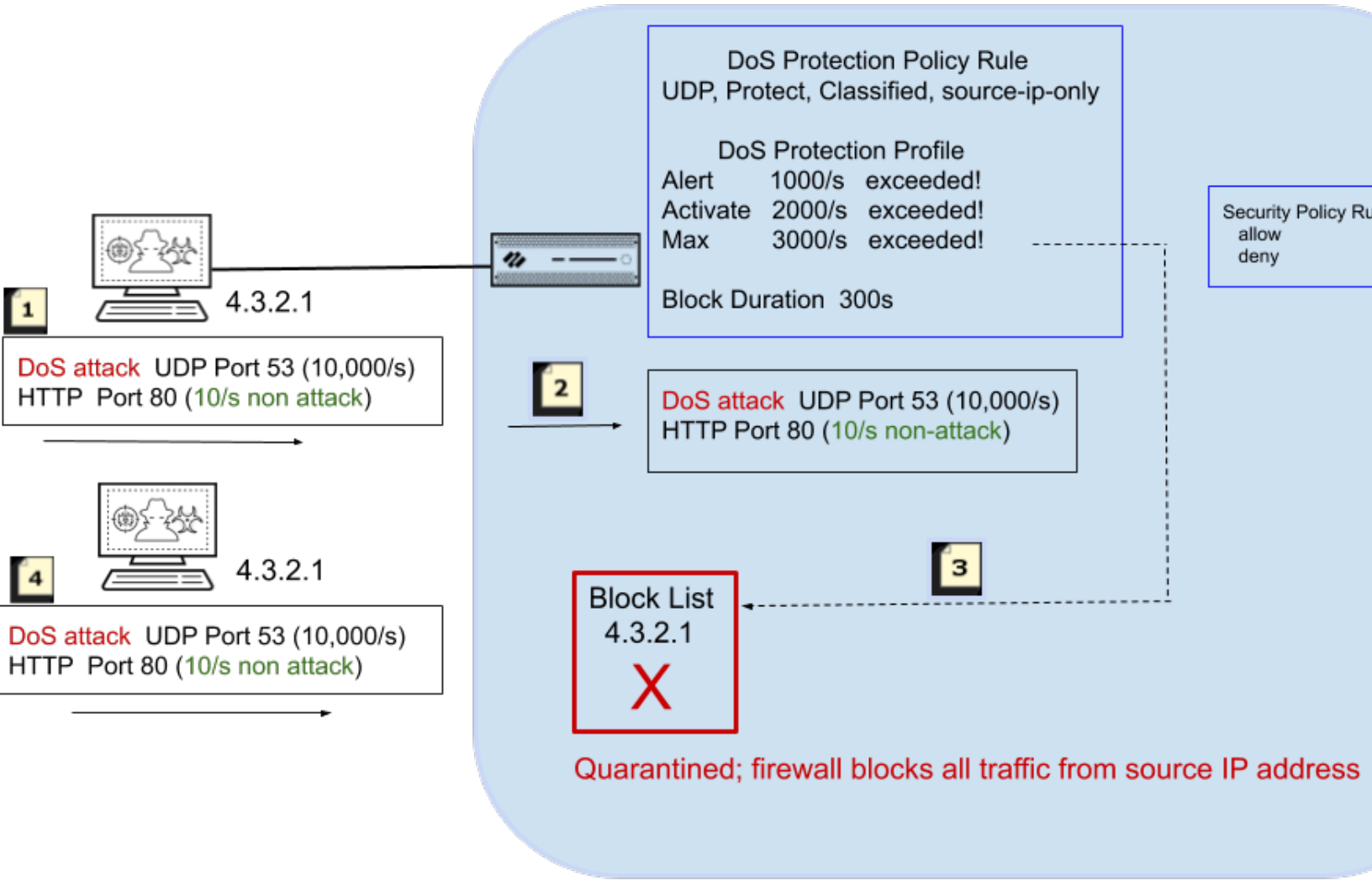
- 多工作階段 DoS 攻擊
- 單一工作階段 DoS 攻擊
- 設定對新工作階段流量的 DoS 保護
- 結束單一工作階段 DoS 攻擊
- 識別使用過多晶片上封包描述元的工作階段
- 丟棄工作階段而不提交

多工作階段 DoS 攻擊

透過設定 DoS 保護原則規則（可確定觸發 **Protect**（保護）動作的準則（當傳入封包與之相符時）），設定對新工作階段流量的 DoS 保護。DoS 保護設定檔會將每次新連線計入 Alarm Rate（警示速率）、Activate Rate（啟動速率）與 Max Rate（最大速率）臨界值。當每秒的傳入新連線超出允許的（啟動速率）時，防火牆會採取 DoS 保護設定檔中指定的動作。

下圖與下表說明安全性原則規則、DoS 保護原則規則與設定檔在範例中協同作業的方式。

©2024 Palo Alto Networks, Inc.



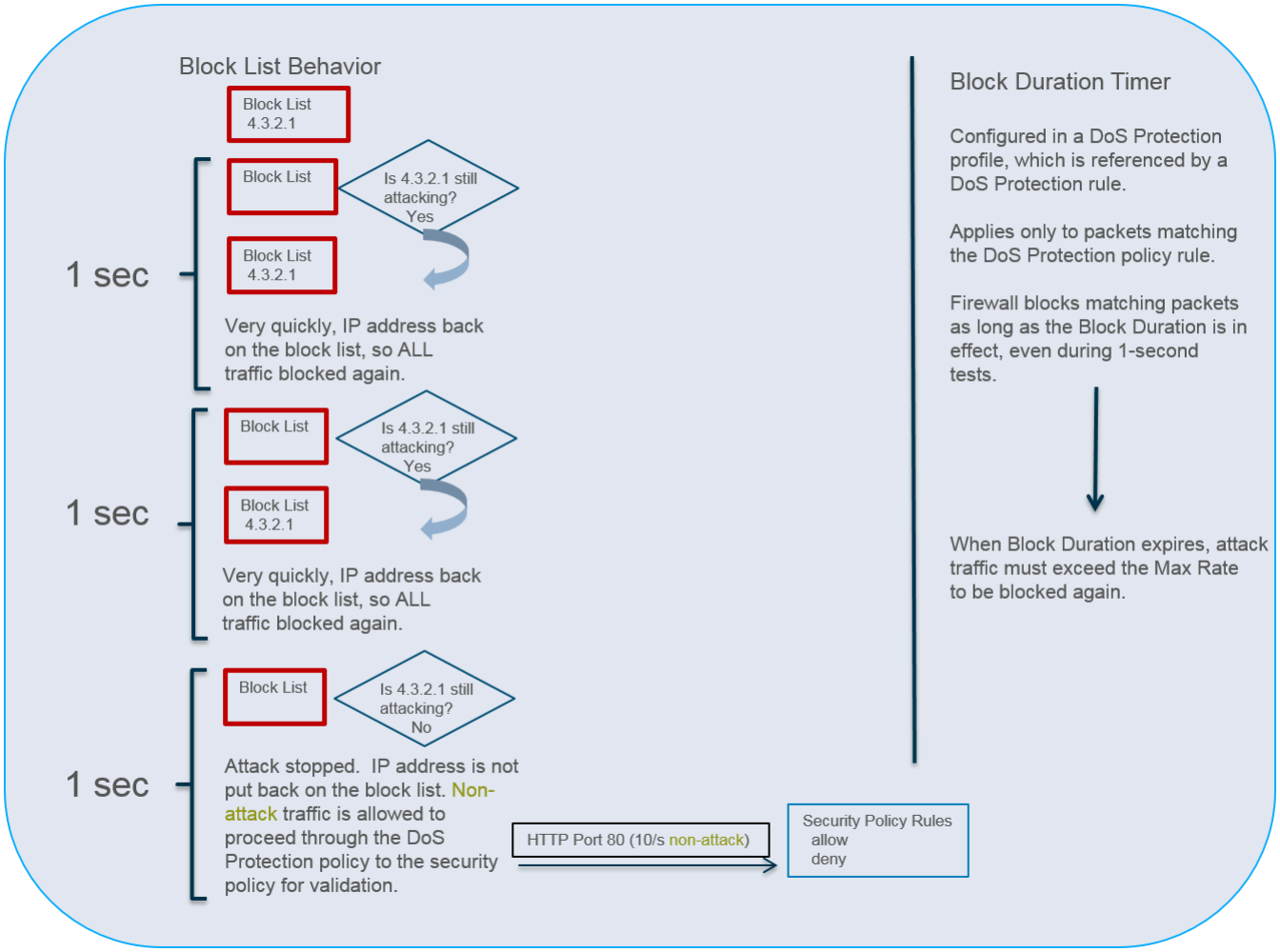
當防火牆隔離 **IP** 位址時的事件順序	
1	在此範例中，攻擊者會以每秒 10,000 次新連線的速率對 UDP 連接埠 53 發動 DoS 攻擊。攻擊者也會將每秒 10 次新連線傳送至 HTTP 連接埠 80。
2	新連線符合 DoS 保護原則規則中的條件，例如來源區域或介面、來源 IP 位址、目的地區域或介面、目的地 IP 位址或服務，以及其他設定。在此範例中，原則規則會指定 UDP。 DoS 保護原則規則也會指定 **Protect**（保護）動作與 **Classified**（分類），這兩個設定可使 DoS 保護設定檔的設定動態生效。DoS 保護設定檔指定允許最大速率為每秒 3000 個封包。當傳入封包符合 DoS 保護原則規則時，會將每秒的新連線計入**Alert**（警示）、**Activate**（啟動）和 **Max Rate**（最大速率）臨界值。

©2024 Palo Alto Networks, Inc.

當防火牆隔離 **IP** 位址時的事件順序	
	如果您認為某來源 *IP* 位址一直都是惡意的，也可以使用安全性原則規則封鎖來自該位址的所有流量。
3	每秒 10,000 個新連線超出 **Max Rate**（最大速率）臨界值。當發生下列所有情況時： • 超出臨界值， • 指定 **Block Duration**（封鎖持續時間），並 • 將 **Classified**（分類）設定為包含來源 IP 位址， 防火牆將入侵來源 IP 位址放在封鎖清單中。
4	封鎖清單中的 IP 位址處於隔離狀態，這表示，會封鎖來自該 IP 位址的所有流量。在其他攻擊封包達到安全性原則之前，防火牆會封鎖入侵來源 IP 位址。

下圖更詳細地說明將符合 DoS 保護原則規則的 IP 位址放入封鎖清單之後會發生的情況。也會說明 (封鎖持續時間) 計時器。

©2024 Palo Alto Networks, Inc.



每一秒鐘，防火牆都會允許 IP 位址脫離封鎖清單，以使防火牆可以測試流量模式並確定攻擊是否正在進行中。防火牆會採取下列動作：

- 在此時間為一秒的測試期間，防火牆將允許不符合 DoS 保護原則條件（此範例中為 HTTP 流量）的封包通過 DoS 保護原則規則進入安全性原則，以進行驗證。很少有封包（如果有）有時間通過，因為 IP 位址脫離封鎖清單之後防火牆收到的第一個攻擊封包將符合 DoS 保護原則條件，並快速導致 IP 位址在下一秒放回到封鎖清單中。防火牆會每秒重複此測試，直到攻擊停止為止。
- 防火牆會封鎖所有攻擊流量，避免其通過 DoS 保護原則規則（位址仍留在封鎖清單內），直到「封鎖持續時間」到期為止。

上圖所示的 *1* 秒檢查發生在具有多個資料平面 *CPU* 和一個硬體網路處理器的防火牆型號中。所有單一資料平面系統或沒有硬體網路處理器的系統在軟件中執行此防護，且時間間隔為 *5* 秒。

攻擊停止時，防火牆不會將 IP 位址放回到封鎖清單。防火牆可讓非攻擊流量通過 DoS 保護原則規則繼續進入安全性原則規則，以進行評估。您必須設定安全性原則規則來允許或拒絕流量，因為如果沒有安全性原則，隱含拒絕規則會拒絕所有流量。

©2024 Palo Alto Networks, Inc.

封鎖清單以來源區域與來源位址組合為基礎。此行為允許存在重複的 IP 位址，只要這些位址處於屬於不同虛擬路由器的不同區域中即可。

DoS 保護設定檔中的「封鎖持續時間」設定指定了防火牆封鎖與 DoS 保護原則規則相符之（攻擊性）封包的時間長度。攻擊流量會保持為封鎖，直到 (封鎖持續時間) 到期為止，在此之後，攻擊流量必須再次超出 (最大速率) 臨界值才能再次遭到封鎖。

如果攻擊者使用多個工作階段，或啟動多個攻擊工作階段的 *Bot*，在未設定好安全性原則拒絕或丟棄規則的情況下，工作階段將計入 *DoS* 保護設定檔中的臨界值。因此，單一工作階段攻擊需要安全性原則拒絕或丟棄規則，才能將每個封包計入臨界值；多工作階段攻擊則不需要。

因此，對新工作階段流量的 DoS 保護可讓防火牆在攻擊流量進行時有效防禦來源 IP 位址，並允許非攻擊流量在攻擊停止時立即通過。將入侵 IP 位址放入封鎖清單可讓 DoS 保護功能利用封鎖清單（設計用於隔離所有來自於該來源 IP 位址的活動，例如帶有不同應用程式的封包）。將 IP 位址隔離於所有活動之外，可防範嘗試輪換應用程式攻擊 (攻擊者僅變更應用程式來啟動新攻擊，或在混合式 DoS 攻擊中使用不同攻擊的組合) 的現代攻擊者。您可以監控封鎖的 IP 位址，以檢視封鎖清單、移除封鎖清單中的項目以及獲取封鎖清單中 IP 位址的其他資訊。

從 *PAN-OS 7.0.2* 開始，防火牆將攻擊來源 *IP* 位址放入封鎖清單的行為已經改變。當攻擊停止後，將允許繼續對非攻擊流量強制執行安全性原則。符合 *DoS* 保護設定檔與 *DoS* 保護原則規則的攻擊流量會保持封鎖，直到「封鎖持續時間」到期為止。

單一工作階段 DoS 攻擊

單一工作階段 DoS 攻擊通常不會觸發 (區域) 或 (DoS 保護) 設定檔，因為它們是建立工作階段之後形成的攻擊。安全性原則允許這些攻擊，因為允許建立工作階段，且建立工作階段之後，攻擊會增加封包量，並會記下目標裝置。

設定對新工作階段流量的 DoS 保護以防禦新工作階段洪水攻擊（單一工作階段與多工作階段洪水攻擊）。若為正在進行的單一工作階段攻擊，請另外 結束單一工作階段 DoS 攻擊。

設定對新工作階段流量的 DoS 保護

在設定 DoS 防護政策規則之前，確保您瞭解 IPv4 位址集會被視為 IPv6 位址集的子集，原則中對此進行了詳細說明。

STEP 1 | 設定安全性原則規則可拒絕來自攻擊者 IP 位址的流量，並根據您的網路需求允許其他流量。您可以在安全性原則規則中指定任何比對準則，例如來源 IP 位址。（減輕單一工作階段攻擊，或未觸發 DoS 保護原則臨界值的攻擊為需要；減輕多工作階段攻擊則為選用）

此步驟是通常執行以停止現有攻擊的其中一步。請參閱 結束單一工作階段 DoS 攻擊。

- 建立安全性原則規則

©2024 Palo Alto Networks, Inc.

STEP 2 | 為流量保護設定 DoS 保護設定檔。

由於流量攻擊可能會跨多個通訊協定發生，因此作為最佳做法，請為 *DoS* 保護設定檔中的所有流量類型啟動保護。

1. 選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **DoS Protection**（**DoS** 保護），然後 **Add**（新增）設定檔 **Name**（名稱）。
2. 將 **Classified**（分類）選為 **Type**（類型）。
3. 對於 **Flood Protection**（流量保護），選取所有類型的流量保護：
   - **SYN** 爆流
   - **UDP** 爆流
   - **ICMP** 爆流
   - **ICMPv6** 爆流
   - 其他 **IP** 爆流
4. 啟用 **SYN Flood**（**SYN** 流量攻擊），選取當每秒連線數 (cps) 超過 **Activate Rate**（啟動速率）臨界值時出現的 **Action**（動作）：
   1. 隨機早期丟棄—防火牆將使用演算法來逐步開始丟棄該類型的封包。如果攻擊繼續，傳入的 cps 速率越高（高於 **Activate Rate**（啟動速率）），防火牆丟棄的封包也越多。防火牆將一直丟棄封包，直至傳入的 cps 速率達到 **Max Rate**（最大速率），此時防火牆將丟棄所有傳入連線。**Random Early Drop**（隨機早期丟棄）(RED) 是 **SYN Flood**（**SYN** 流量攻擊）的預設動作，也是 **UDP Flood**（**UDP** 流量攻擊）、**ICMP Flood**（**ICMP** 流量攻擊）、**ICMPv6 Flood**（**ICMPv6** 流量攻擊）和 **Other IP Flood**（其他 **IP** 流量攻擊）的唯一動作。RED 比 SYN Cookie 更高效，能夠處理更大的攻擊，但不能識別良性流量和不良流量。
   2. **SYN Cookies**—防火牆將代表伺服器產生 Cookie，並在 SYN-ACK 中傳送給用戶端，而不會立即向伺服器傳送 SYN。用戶端將回應 ACK 和 Cookie；完成此驗證後，防火

 ©2024 Palo Alto Networks, Inc.

牆將立即向伺服器傳送 SYN。**SYN Cookies**動作需要的防火牆資源比 **Random Early Drop**（隨機早期丟棄）多；它的識別能力更強，因為它能識別不良流量。

5. （選用）在每個流量頁籤上，變更下列臨界值以符合環境需求：
   - 警示速率（連線/秒）—指定開始產生 DoS 警示的臨界值速率 (cps)。（範圍是 0-2,000,000；預設值是 10,000。）
   - 啟動速率（連線/秒）—指定開始啟動 DoS 回應的臨界值速率 (cps)。達到 **Activate Rate**（啟動速率）臨界值時，會發生 **Random Early Drop**（隨機提前丟棄）。範圍為 0-2,000,000；預設值為 10,000。（對於 SYN 流量攻擊，您可以選取出現的動作。）
   - 最大速率（連線/秒）—指定防火牆允許的臨界值速率（每秒傳入的連線數）。超過此臨界值後，新到達的連線將被丟棄。（範圍為 2-2,000,000；預設值為 40,000。）

   此步驟中的預設臨界值只是起點，且可能不適合您的網路。您必須分析網路的行為，才能正確設定初始臨界值。

6. 在每個流量頁籤上，指定 **Block Duration**（封鎖持續時間）（以秒為單位），此時間為防火牆封鎖符合參考此設定檔之 DoS 保護原則規則的封包的時間長度。指定大於零的值。（範圍為 1-21,600；預設值為 300。）

   如果您擔心將非必要地封鎖未正確識別為攻擊流量的封包，則設定較低的 ***Block Duration***（封鎖持續時間）值。

   如果相對於錯誤封鎖不屬於攻擊一部分的封包，您更擔心封鎖體積攻擊，請設定較高的 **Block Duration**（封鎖持續時間）值。

7. 按一下 **OK**（確定）。

©2024 Palo Alto Networks, Inc.

STEP 3 | 設定指定比對傳入流量之條件的 DoS 保護原則規則。

防火牆資源是有限的，因此您不會希望使用面向網際網路的區域內的來源位址分類，因為可能會有海量的唯一 *IP* 位址與 *DoS* 保護原則規則相符。這將需要更多的計數器，而防火牆將用盡追蹤資源。因此，要定義使用（所保護伺服器的）目的地位址分類的 *DoS* 保護原則規則。

1. 選取 **Policies**（原則）> **DoS Protection**（**DoS** 保護），並在 **General**（一般） 頁籤上 **Add**（新增）**Name**（名稱）。名稱區分大小寫，最多可有 31 個字元，包含字母、數字、空格、連字號和底線。
2. 在 **Source**（來源）頁籤上，選擇要作為 **Zone**（區域）或 **Interface**（介面）的 **Type**（類型），然後 **Add**（新增）區域或介面。根據您的部署和希望保護的項目來選擇區域或介面。例如，如果您只有一個介面傳入防火牆，則選擇 Interface（介面）。
3. （選用）針對 **Source Address**（來源位址），選取 **Any**（任何），使任何傳入 IP 位址都符合規則，或 **Add**（新增）位址物件，例如地理區域。
4. （選用）針對 **Source User**（來源使用者），選取 **any**（任何）或指定使用者。
5. （選用）選取 **Negate**（否定）以比對除您指定之來源以外的任何來源。
6. （選用）在 **Destination**（目的地）頁籤中，選擇要作為 **Zone**（區域）或 **Interface**（介面）的 **Type**（類型），然後 **Add**（新增）目的地區域或介面。例如，輸入您要保護的安全性區域。
7. （選用）針對 **Destination Address**（目的地位址），選取 **Any**（任何），或輸入您要保護之裝置的 IP 位址。
8. （選用）在 **Option/Protection**（選項/保護）頁籤上，**Add**（新增）**Service**（服務）。選取服務或按一下 **Service**（服務），並輸入 **Name**（名稱）。選取 **TCP** 或 **UDP**。輸入 **Destination Port**（目的地連接埠）。不指定特定服務可讓規則比對任何通訊協定類型的流量，而無須考慮應用程式特定連接埠。
9. 在 **Option/Protection**（選項/保護）頁籤上，針對 **Action**（動作），選取 **Protect**（保護）。
10. 選取 **Classified**（分類）。
11. 針對 **Profile**（設定檔），選取建立之 **DoS Protection**（**DoS** 保護）設定檔的名稱。
12. 針對 **Address**（位址），選取 **source-ip-only**（僅限來源 **IP**） 或 **src-dest-ip-both**，其決定套用規則之 IP 位址的類型。根據您希望防火牆以何種方式防禦入侵流量來選擇設定：
    - 如果您想讓防火牆僅在來源 IP 位址中分類，請指定 **source-ip-only**（僅限來源 **IP**）。由於攻擊者通常會針對要攻擊的主機測試整個網路，因此，**source-ip-only**（僅限來源 **IP**）是進行更廣泛檢查的一般設定。
    - 如果您希望僅在擁有特定目的地位址的伺服器上防禦 DoS 攻擊，同時確保每個來源 IP 位址不會超出該伺服器的特定 cps 臨界值，則指定 **src-dest-ip-both**。
13. 按一下 **OK**（確定）。

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 提交。

按一下 **Commit**（交付）。

結束單一工作階段 DoS 攻擊

若要減輕單一工作階段 DoS 攻擊，您仍需提前設定對新工作階段流量的 DoS 保護。有時，在您設定功能之後，工作階段可能會在您發現正在進行的 DoS 攻擊（來自該工作階段的 IP 位址）之前建立。當您發現單一工作階段 DoS 攻擊時，請執行下列工作結束工作階段，以使來自該 IP 位址的後續連線嘗試觸發對新工作階段流量的 DoS 保護。

STEP 1 | 識別導致攻擊的來源 IP 位址。

例如，使用防火牆之具有目的地篩選的封包擷取功能，來收集前往目的地 IP 位址之流量的樣本。或者，您也可以使用 ACC 篩選目的地位址，來檢視受攻擊之目標主機的活動。

STEP 2 | 超出攻擊臨界值之後，建立將封鎖攻擊者 IP 位址的 DoS 保護原則規則。

STEP 3 | 建立安全性原則規則來拒絕來源 IP 位址及其攻擊流量。

STEP 4 | 執行 **clear session all filter source *<ip-address>*** 操作命令，結束來自攻擊來源 IP 位址的現有攻擊。

此外，如果您知道工作階段 ID，您可以執行 **clear session id *<value>*** 命令以僅結束該工作階段。

如果您使用 ***clear session all filter source <ip-address>*** 命令，會丟棄符合來源 *IP* 位址的所有工作階段，其中可能包含良好工作階段與不良工作階段。

在您結束現有攻擊工作階段之後，形成攻擊工作階段的任何後續嘗試都會遭到安全性原則封鎖。DoS 保護原則會將所有連線嘗試計入臨界值。當超出「最大速率」臨界值時，會針對「封鎖持續時間」封鎖來源 IP 位址，如多工作階段 DoS 攻擊中所述。

識別使用過多晶片上封包描述元的工作階段

防火牆如表現出資源耗盡的跡象，則可能是遭受了攻擊，收到過多的封包。此類情況下，防火牆開始緩衝輸入封包。您可快速找出正使用過高百分比晶片上封包描述元的工作階段，並丟棄它們以減輕其影響。

在以硬體為基礎的防火牆型號（而非 VM-Series 防火牆）上執行下列工作，來針對每個插槽與資料平面找出使用的晶片上封包描述元百分比、使用超出百分之二晶片上封包描述元的前五大工作階段以及與這些工作階段相關聯的來源 IP 位址。擁有這些資訊有助於採取正確的行動。

STEP 1 | 檢視防火牆資源使用率、前幾大工作階段以及工作階段詳情。在 CLI 中執行以下操作命令 (來自命令的範例輸出如下)：

```
admin@PA-7050> show running resource-monitor ingress-backlogs
 -- SLOT:s1, DP:dp1 -- USAGE - ATOMIC: 92%  TOTAL:93%
```


©2024 Palo Alto Networks, Inc.

```
 TOP SESSIONS:SESS-ID      PCT   GRP-ID   COUNT
 6            92%   1        156                  7        1732
 SESSION DETAILS SESS-
ID PROTO SZONESRC       SPORT  DST       DPORT  IGR-IF    EGR-
IF       APP
 6    6     trust 192.168.2.35 55653  10.1.8.89 80  ethernet1/21
 ethernet1/22 undecided
```

執行此命令可顯示最多前五大工作階段，其中每個工作階段使用 2% 或以上的晶片上封包描述元。

以上範例輸出表示，工作階段 6 正使用 92% 的晶片上封包描述元，TCP 封包（通訊協定 6）來自來源 IP 位址 192.168.2.35。

- **SESS-ID**—表示所有其他 **show session** 命令中使用的全域工作階段 ID。全域工作階段 ID 在防火牆內是唯一的。
- **GRP-ID**—表示處理封包的一個內部階段。
- **COUNT**—表示有多少個封包位於該工作階段的 GRP-ID 中。
- **APP**—表示從工作階段資訊中擷取的 App-ID，可協助您確定流量是否合法。例如，如果封包使用共同的 TCP 或 UDP 連接埠，但 CLI 輸出表示 undecided APP，則封包可能為攻擊流量。當應用程式 IP 解碼器獲得足夠資訊來確定應用程式時，APP 為 undecided。unknown 應用程式表示應用程式 IP 解碼器無法確定應用程式；使用高百分比晶片上封包描述元的 unknown APP 工作階段也可疑。

若要限制顯示輸出：

您可以將輸出限制為插槽、資料平面或兩者（僅限 PA-7000 系列型號）。例如：

```
admin@PA-7050> show running resource-monitor ingress-backlogs slot
 s1 admin@PA-7050> show running resource-monitor ingress-backlogs
 slot s1 dp dp1
```

您可以將輸出限制為數據平面（僅限 PA-5200 系列和 PA-7000 系列型號）。例如：

```
admin@PA-5260> show running resource-monitor ingress-backlogs dp
 dp1
```


©2024 Palo Alto Networks, Inc.

STEP 2 | 使用命令輸出，來確定位於使用高百分比晶片上封包描述元之來源 IP 位址的來源是在傳送合法流量還是攻擊流量。

在以上範例輸出中，可能發生單一工作階段攻擊。單一工作階段（工作階段 ID 6）為插槽 1 DP 1 使用 92% 的晶片上封包描述元，該點的應用程式為 `undecided`。

- 如果您確定單個使用者正在傳送攻擊並且流量未卸載，您可以結束單一工作階段 DoS 攻擊。您至少可以設定對新工作階段流量的 DoS 保護。
- 在具有現場可程式化閘陣列 (FPGA) 的硬體型號上，防火牆在可能的情況下會將流量卸載到 FPGA 以提升效能。如果流量已卸載到硬體，則清除工作階段沒有助益，因為軟體必須處理無數封包。您應捨棄工作階段而不提交。

若要查看工作階段是否已卸載，請在 CLI 中使用 **show session id *<session-id>*** 操作命令，如以下範例所示。若工作階段已卸載，`layer7processing` 的值顯示為 `completed`，若工作階段未卸載，則顯示為 `enabled`。

```
admin@PA-5060> show session id 68088184

Session        68088184

        c2s flow:
                source:      1.1.42.15 [trust]
                dst:         1.2.27.99
                proto:       6
                sport:       55993           dport:      6881
                state:       ACTIVE          type:       FLOW
                src user:    unknown
                dst user:    unknown
                offload:     Yes

        s2c flow:
                source:      1.2.27.99 [untrust]
                dst:         1.1.42.15
                proto:       6
                sport:       6881            dport:      55993
                state:       ACTIVE          type:       FLOW
                src user:    unknown
                dst user:    unknown
                offload:     Yes

        DP                                   : 2
        index(local):                        : 979320
        start time                           : Tue Oct 27 14:20:09 2015
        timeout                              : 1200 sec
        time to live                         : 1167 sec
        total byte count(c2s)                : 270
        total byte count(s2c)                : 270
        layer7 packet count(c2s)             : 3
        layer7 packet count(s2c)             : 3
        vsys                                 : vsys1
        application                          : bittorrent
        rule                                 : rule1
        session to be logged at end          : True
        session in session ager              : True
        session updated by HA peer           : False
        layer7 processing                    : completed
        URL filtering enabled                : False
        session via syn-cookies              : False
        session terminated on host           : False
        session traverses tunnel             : False
        captive portal session               : False
        ingress interface                    : ethernet1/21
        egress interface                     : ethernet1/22
        session QoS rule                     : N/A (class 4)
        tracker stage l7proc                 : ctd decoder bypass
        end-reason                           : unknown
```


©2024 Palo Alto Networks, Inc.

如果 **show session id <*session-id*>** 命令輸出顯示與以下內容類似的資訊，則輸出意味著工作階段尚未安裝在 PAN-OS 防火牆上。發生這種情況的原因之一是由於設定的安全性原則規則而拒絕流量。

```
> show session id xxxxxxxxxx
Session xxxxxxxxxx
Bad Key: c2s:  'c2s'
Bad Key: s2c:  's2c'
index(local): : yyyyyyy
```

丟棄工作階段而不提交

執行此工作以永久丟棄工作階段，例如使封包緩衝區過載或是晶片上封包描述元的工作階段。不需提交；工作階段將在執行命令後立即丟棄。這些命令適用於卸載和非卸載工作階段。

STEP 1 | 在 CLI 中，在任何硬體型號上執行以下操作命令：

```
admin@PA-7050> request session-discard [timeout <seconds>]
 [reason <reason-string>] id <session-id>
```

預設逾時是 3,600 秒。

STEP 2 | 確認工作階段已丟棄。

```
admin@PA-7050> show session all filter state discard
```


©2024 Palo Alto Networks, Inc.

認證

下列主題說明如何設定 Palo Alto Networks® 防火牆和裝置來支援通用準則和聯邦資訊處理標準 140-2 (FIPS 140-2) 和 140-3 (FIPS 140-3)，它們是安全性憑證，可確保安全性保證和功能的標準集。美國政府機構和政府承包商平民通常需要這些憑證。

關於產品認證和協力廠商憑證的詳細資訊，請參閱憑證頁面。有關擱置中加密模組的詳細資料，請參閱加密模組驗證程式並搜尋 **Palo Alto Networks**。

- 啟用 FIPS 與通用準則支援
- FIPS-CC 安全性功能
- 在以 FIPS-CC 模式執行的防火牆或設備上清除交換記憶體

啟用 FIPS 與通用準則支援

使用下列程序，在支援通用準則和聯邦資訊處理標準 140-2 (Federal Information Processing Standards 140-2，FIPS 140-2) 的軟體版本上啟用 FIPS-CC 模式。當您啟用 FIPS-CC 模式時，會包括所有 FIPS 及 CC 功能。

Palo Alto Networks 的所有新一代防火牆和裝置均支援 FIPS-CC 模式，包括 VM 系列防火牆。若要啟用 FIPS-CC 模式，首先啟動防火牆進入維護復原工具 (MRT)，然後將操作模式從正常模式變更為 FIPS-CC 模式。所有防火牆和設定的操作模式變更程序都相同，但存取 MRT 的程序卻不同。

當您啟用 *FIPS-CC* 模式時，會將防火牆重設回原廠預設設定；將移除所有設定。

- 存取維護復原工具 (MRT)
- 將操作模式變更為 FIPS-CC 模式

存取維護復原工具 (MRT)

維護復原工具 (MRT) 允許您在 Palo Alto Networks 防火牆和裝置上執行多個任務。例如，您可以將防火牆或裝置恢復為原廠預設值、將 PAN-OS 或內容更新恢復為之前的版本、對檔案系統執行診斷、收集系統資訊以及擷取記錄。此外，您還可以使用 MRT 將操作模式變更為 FIPS-CC 模式或從 FIPS-CC 模式變更為正常模式。

下列程序描述了在各種 Palo Alto Networks 產品上如何存取維護復原工具 (MRT)。

©2024 Palo Alto Networks, Inc.

在硬體防火牆和裝置（如 PA-220 防火牆、PA-7000 系列防火牆或 M 系列裝置）上存取 MRT。

1. 建立與防火牆或裝置之間的序列主控台工作階段。
   1. 將序列纜線從電腦上的序列連接埠連接至防火牆或裝置的主控台連接埠。

      如果電腦沒有 *9* 針腳序列連接埠但有 *USB* 連接埠，則使用序列至 *USB* 轉換器來建立連接。如果防火牆有 micro USB 控制台連接埠，則使用 *Type-A USB* 至 *micro USB* 纜線。
   2. 在電腦上開啟終端機模擬軟體，設定為 9600-8-N-1，然後再連接至相應 COM 連接埠。

      在 *Windows* 系統上，可移至「控制台」，檢視「裝置和印表機」的 *COM* 連接埠設定，以確定將哪個 *COM* 連接埠指派給主控台。
   3. 使用管理員帳戶登入。（預設的使用者名稱/和密碼是 admin/admin。）
2. 輸入以下 CLI 命令並按 **y** 確認：

   ```
   debug system maintenance-mode
   ```
3. 在防火牆或裝置啟動到 MRT 歡迎畫面（大約 2 到 3 分鐘）後，選中 **Continue**（繼續）並按 Enter，以存取 MRT 主功能表。

   您也可以透過重新啟動防火牆或裝置並在維護模式提示中輸入 ***maint*** 的方式存取 *MRT*。需要建立直接序列主控台連接。

在防火牆或裝置進入 MRT 後，可以透過與管理 (MGT) 介面 IP 位址建立 SSH 連接的方式從遠端存取 MRT。在登入提示中，輸入 **maint** 作為使用者名稱，輸入防火牆或裝置序號作為密碼。

©2024 Palo Alto Networks, Inc.

存取在私人雲端（例如 VMware ESXi 或 KVM Hypervisor）中部署的 VM 系列防火牆上的 MRT。

1. 與防火牆的管理 IP 位址建立 SSH 工作階段，然後使用管理員帳戶登入。
2. 輸入以下 CLI 命令並按 **y** 確認：

```
debug system maintenance-mode
```

防火牆需要大約 *2* 到 *3* 分鐘才能啟動到 *MRT*。在此期間，*SSH* 工作階段將中斷連線。

3. 當防火牆啟動至 MRT 歡迎畫面之後，根據操作模式登入：
   - 正常模式 — 與防火牆的管理 IP 位址建立 SSH 工作階段，並使用 **maint** 作為使用者名稱，使用防火牆或裝置序號作為密碼。
   - **FIPS-CC** 模式 — 存取虛擬機器管理公用程式（例如 vSphere 用戶端），然後連接至虛擬機器主控台。
4. 在 MRT 歡迎畫面上，選中 **Continue**（繼續）並按 Enter，以存取 MRT 主功能表。

存取在私人雲端（例如 AWS 或 Azure）中部署的 VM 系列防火牆上的 MRT。

1. 與防火牆的管理 IP 位址建立 SSH 工作階段，然後使用管理員帳戶登入。
2. 輸入以下 CLI 命令並按 **y** 確認：

```
debug system maintenance-mode
```

防火牆需要大約 *2* 到 *3* 分鐘才能啟動到 *MRT*。在此期間，*SSH* 工作階段將中斷連線。

3. 當防火牆啟動至 MRT 歡迎畫面之後，根據虛擬機器類登入：
   - **AWS** — 以 **ec2-user** 的身分登入，選取您在部署虛擬機器時與虛擬機器關聯的 SSH 公開金鑰。
   - **Azure** — 輸入您在部署 VM 系列防火牆時建立的認證。
   - **GCP** — 以 **gcp-user** 的身分登入，選取您在部署虛擬機器時與虛擬機器關聯的 SSH 公開金鑰。
4. 在 MRT 歡迎畫面上，選中 **Continue**（繼續）並按 Enter，以存取 MRT 主功能表。

將操作模式變更為 FIPS-CC 模式

下列程序介紹了如何將 Palo Alto Networks 產品的操作模式從正常模式變更為 FIPS-CC 模式。

©2024 Palo Alto Networks, Inc.

當設備處於 *FIPS-CC* 模式時，您將無法透過主控台進行任何設定，包括管理介面設定。在啟用 *FIPS-CC* 模式之前，請確定您的網路已設定為允許透過 *SSH* 或網頁介面存取管理介面。如果使用 *PA-Series* 防火牆，則管理介面預設為 *192.168.1.1* 的靜態位址，如果是 *VM-Series* 防火牆，則預設為透過 *DHCP* 擷取的位址。*WildFire*、虛擬 *Panorama* 和 *M-series Panorama* 設備將預設為 *192.168.1.1* 的靜態位址。

啟用 *FIPS-CC* 模式之後，會清除所有的組態和設定。如果管理員有想在啟用 *FIPS-CC* 模式再次使用的組態或設定，則可以在變更為 *FIPS-CC* 模式之前儲存並匯出組態。操作模式變更完成後，再匯入組態。匯入的設定必須依據 FIPS-CC 安全性功能 進行編輯，否則匯入程序將會失敗。

金鑰、密碼和其他重要的安全性參數無法跨模式共用。

如果您將 *Panorama* 管理伺服器管理的防火牆或專用日誌收集器的操作模式變更為 *FIPS-CC* 模式，您也必須將 *Panorama* 的操作模式變更為 *FIPS-CC* 模式。這是為了保護從 *Panorama* 推送的本機管理員密碼的密碼雜湊。

STEP 1 | （僅適用於現有 HA 設定）停用高可用性 (HA) 設定。

對於已採用 HA 設定的防火牆，成功將操作模式變更為 FIPS-CC 模式需要此動作。

1. 在主要 HA 對等上登入防火牆網頁介面。
2. 選取 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般），然後編輯 HA Pair Settings（HA 配對設定）設定。
3. 取消核取（停用）**Enable HA**（啟用 **HA**），然後按一下 **OK**（確定）。
4. **Commit**（認可）。

STEP 2 | （僅限公共雲端 VM-Series 防火牆或公共雲端 Panorama 虛擬設備）建立 SSH 金鑰並登入防火牆或 Panorama。

在一些公用雲端平台上（如 Microsoft Azure），您必須擁有 SSH 金鑰來防止在變更為 FIPS-CC 模式後驗證失敗。確認您已部署防火牆使用 SSH 金鑰進行驗證。儘管您可以在 Azure 上部署 VM-Series 防火牆或 Panorama 並使用使用者名稱和密碼登入，但將操作模式變更為 FIPS-CC 後，您將無法使用使用者名稱和密碼進行驗證。在重設為 FIPS-CC 模式後，您必須使用 SSH 金鑰來登入，然後可以設定之後可用於登入至防火牆 Web 介面的使用者名稱和密碼。

STEP 3 | 連接至防火牆或設備，並 存取維護復原工具 (MRT)。

STEP 4 | 從功能表選取 **`Set FIPS-CC Mode`**（設定 **`FIPS-CC`** 模式）。

STEP 5 | 選取 **`Enable FIPS-CC Mode`**（啟用 **`FIPS-CC`** 模式）。模式變更操作會啟動完全原廠重設，狀態指示器會顯示進度。模式變更完成後，狀態顯示 `Success`。

所有組態和設定都會被清除，且在模式變更完成後無法擷取。

 ©2024 Palo Alto Networks, Inc.

STEP 6 | 出現提示時，選取 **Reboot**（重新啟動）。

> 如果在部署於公用雲端內的 *VM-Series* 防火牆上變更操作模式，並且在能夠 **Reboot**（重新啟動）之前失去與 *MRT* 的 *SSH* 連線，則您必須等待 *10-15* 分鐘才能完成模式變更，需重新登入 *MRT* 並重新啟動防火牆才能完成操作。重設為 *FIPS-CC* 模式後，在一些虛擬規格（*Panorama* 或 *VM-Series*）上，您只能使用 *SSH* 金鑰登入，如果您沒有設定使用 *SSH* 金鑰驗證，在重新啟動時您將無法登入至防火牆。

切換至 FIPS-CC 模式後，您將看到以下狀態：`FIPS-CC mode enabled successfully`（已成功啟用 `FIPS-CC` 模式）。

此外，下列變更將生效：

- Web 介面底部的狀態列會一直顯示 FIPS-CC。
- 預設的管理員登入認證將變更為 admin/paloalto。

關於 FIPS-CC 模式中執行的安全性功能的詳細資訊，請參閱 FIPS-CC 安全性功能。

STEP 7 | （僅適用於現有 HA）重新啟用 HA。

對於在變更為 FIPS-CC 模式之前採用 HA 設定的防火牆，此步驟是必需的。

如需首次設定 HA 的詳細資訊，請參閱高可用性。

1. 在主要 HA 對等上登入防火牆網頁介面。
2. 選取 **Device**（裝置）> **High Availability**（高可用性）> **General**（一般），然後編輯 HA Pair Settings（HA 配對設定）設定。
3. 核取（啟用）**Enable HA**（啟用 **HA**），然後按一下 **OK**（確定）。
4. **Commit**（認可）。

STEP 8 | 針對 HA1 控制連結啟用加密。

對於 HA 設定中處於 FIPS-CC 模式的所有防火牆，此步驟是必需的。

若要針對 FIPS-CC 模式下的防火牆成功利用 HA，必須設定自動重設金鑰參數，並且必須將資料參數設定為不大於 1000 MB 的值。不能讓金鑰保留預設值，並且必須設定時間間隔（不能讓其保留停用狀態）。

©2024 Palo Alto Networks, Inc.

FIPS-CC 安全性功能

啟用 FIPS-CC 模式後，將對所有防火牆和裝置強制執行下列安全功能：

- 如要登入，瀏覽器必須與 TLS 1.2（或更新版本）相容；在 WF-500 裝置上，您只能透過 CLI 管理裝置，並且必須使用與 SSHv2 相容的用戶端應用程式連線。
- 所有密碼必須至少為八個字元。
- 您必須確保驗證設定中的 **Failed Attempts**（失敗嘗試次數）及 **Lockout Time (min)**（鎖定時間（分鐘））的大於 0。如果管理員達到 **Failed Attempts**（失敗嘗試次數）臨界值，在 **Lockout Time (min)**（鎖定時間（分鐘））欄位中定義的期間，管理員將會被鎖定。

  （Panorama 管理的防火牆）您必須確保，在 FIPS-CC 模式下的受管理防火牆關聯的範本或範本堆疊設定中的驗證設定（**Device**（裝置） > **Setup**（設定） > **Management**（管理））中的 **Failed Attempts**（失敗嘗試）和 **Lockout Time (min)**（鎖定時間（分鐘））大於 0。當您將設定變更從 Panorama 推送到 FIPS-CC 模式下的受管理防火牆時，需要此設定以防止提交失敗。
- 您必須確保驗證設定中的 **Idle Timeout**（閒置逾時）值大於 0。如果登入工作階段閒置時間超過指定時間，管理員將被自動登出。
- 您可以設定 **Absolute Session Length**（絕對工作階段長度）以設定使用者可登入的最大時間長度（以分鐘為單位）。可設定的最小長度為 60 分鐘。在逾時 5 分鐘前，您將收到工作階段終止警告。此功能在 FIPS-CC 模式中不能停用，且預設值為 30 天的工作階段。
- 您可以設定 **Max No. of Sessions**（最大工作階段數）以設定多少使用者可同時登入至同一管理員帳戶。
- 防火牆或裝置會自動判斷自我測試的適當等級，並會強制加密演算法與加密套件的適當強度。
- 未經核准的 FIPS-/CC 演算法不會進行解密，因此在解密期間會遭到忽略。
- 您需要使用設定了利用 TLS 加密的驗證通訊協定的 RADIUS 伺服器設定檔。

  PAP 和 CHAP 驗證通訊協定不是相容的通訊協定，不應在 FIPS-CC 模式下使用。
- 設定 IPSec VPN 時，管理員必須在 IPSec 設定期間選取出現的加密套件選項。
- （僅限 Panorama 和 WildFire）可在管理介面上啟用 IPSec 以保護 NTP、RADIUS、TACACS 和 DNS 等通訊協定。
- 自我產生與匯入的憑證必須包含 RSA 2,048 位元（或更多）或 ECDSA 256 位元（或更多）的公開金鑰；您還必須使用 SHA256 或更高的摘要。
- Telnet、TFTP 與 HTTP 管理連線無法使用。
- （新的 HA 部署）為 FIPS-CC 模式下的防火牆設定高可用性 (HA) 時，您必須針對 HA1 控制連結啟用加密。您必須設定自動金鑰更新參數；您必須設定小於 1000 MB 的資料參數值（不得為預設值）且必須設定時間間隔（不得停用）。

©2024 Palo Alto Networks, Inc.

- （現有 HA 部署）在為採用高可用性 (HA) 設定的防火牆將操作模式變更為 FIPS-CC 模式之前，必須先停用 HA（**Device**（裝置） > **High Availability**（高可用性） > **General**（一般）），然後再將操作模式變更為 FIPS-CC 模式。

  將兩個 HA 對等的操作模式變更為 FIPS-CC 模式後，請如上所述重新啟用 HA 並針對 HA1 控制連結啟用加密。
- FIPS-CC 中的序列主控台連接埠將僅用作限定狀態輸出連接埠；CLI 存取不可用。
- 已啟動進入 MRT 的硬體和私人雲端 VM 系列防火牆上的序列主控台連接埠可提供 MRT 的互動式存取權。
- 以啟動進入 MRT 的 Hypervisor 環境私人雲端 VM 系列防火牆互動式主控台存取；您只能使用 SSH 存取 MRT。
- 您必須在舊主要金鑰到期之前手動設定新主要金鑰；**Auto Renew Master Key**（自動更新主要金鑰）在 FIPS-CC 模式中不受支援。

  如果主要金鑰到期，防火牆或 Panorama 就會自動以維護模式重新啟動。您必須將防火牆重設為原廠預設設定。
- 如果啟用 FIPS-CC 模式，則在 Palo Alto Networks 防火牆上停用零接觸佈建 (ZTP) 模式。
- （Panorama 受管理的裝置）啟用 FIPS-CC 時，檢閱對防火牆和日誌收集器的 Panorama 支援。

Panorama	防火牆		日誌收集器	
啟用 FIPS-CC	啟用 FIPS-CC	停用 FIPS-CC	啟用 FIPS-CC	停用 FIPS-CC
	支援	支援	支援	支援
停用 FIPS-CC	不支援	支援	不支援	支援

- （Panorama 受管理的裝置）如果在執行 PAN-OS 10.2 版本時已將 Panorama 和受管理的裝置新增至 Panorama 管理，則在 FIPS-CC 模式下將 Panorama 和受管理裝置升級到 PAN-OS 11.0 或更新版本時，需要重設 FIPS-CC 模式下裝置的安全連線狀態。

  如需詳細資訊，請參閱升級 FIPS-CC 模式下的 Panorama 和受管理裝置。
- （僅適用於 PA-7000 Series 防火牆）檢閱 Palo Alto Networks 硬體生命週期結束日期和相容性矩陣，以確認您擁有支援的系列卡。已到達生命週期結束或執行不受支援的 PAN-OS 版本的系列卡，可能會導致 PA-7000 Series 防火牆進入維護模式。
- 檢閱在 FIPS-CC 模式中匯入憑證的要求。
  - 要匯入憑證和相應的私密金鑰，私密金鑰必須採用 PKCS8 標準語法（**PEM** 格式），並使用符合 FIPS 的密碼進行加密。
  - 要匯入分葉憑證，您必須先成功匯入整個憑證授權單位 (CA) 鏈。

©2024 Palo Alto Networks, Inc.

在以 FIPS-CC 模式執行的防火牆或設備上清除交換記憶體

在解除防火牆或設備（處於 FIPS-CC 模式）或對其進行修理之前，應確保已從交換記憶體中移除敏感資訊。使用此程序從交換分割區中移除所有加密安全性參數 (CSP) 資訊。

如果您對由 *Panorama* 管理的防火牆進行修理，請參閱開始 RMA 防火牆取代之前的注意事項。

STEP 1 | 開啟防火牆或設備的 SSH 管理工作階段。

STEP 2 | 執行下列操作命令：

```
request [restart | shutdown] system with-swap-scrub [dod | nnsa]
```

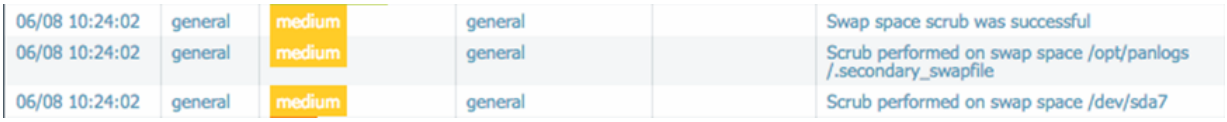
例如，要關閉防火牆或設備並執行防禦部門 (DoD) 清除作業，請執行以下命令：

```
request shutdown system with-swap-scrub dod
```

STEP 3 | 在警告提示處按 **Y** 即可開始清除作業。

STEP 4 | 驗證清除作業是否已順利完成。檢視 **System**（系統）日誌並篩選單字 `swap`。**System**（系統）日誌指示每個交換分割區（一個或兩個分割區，具體取決於型號）的清除狀態，還顯示一個日誌項目，指示清除作業的整體狀態。如果所有交換分割區上的清除作業均已順利完成，則 **System**（系統）日誌會顯示 `Swap space scrub was successful`。

如果一個或多個交換分割區上的清除作業失敗，則 **System**（系統）日誌會顯示 `Swap space scrub was unsuccessful`。以下擷取畫面顯示了具有兩個分割區之防火牆的日誌結果。



06/08 10:24:02	general	medium	general		Swap space scrub was successful
06/08 10:24:02	general	medium	general		Scrub performed on swap space /opt/panlogs /.secondary_swapfile
06/08 10:24:02	general	medium	general		Scrub performed on swap space /dev/sda7

要使用 *CLI* 檢視清除作業日誌，請執行 ***show log system | match swap*** 命令。

如果使用關閉命令啟動清除作業，則防火牆或設備會在清除作業完成后關閉電源。在開啟防火牆或設備電源之前，必須先斷開電源，然後重新連接電源。

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.