User-ID 最佳实践

10.0 (EoL)

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS

Contact Information

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

About the Documentation

- To ensure you are viewing the most current version of this document, or to access 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

Last Revised

November 16, 2020

Table of Contents

User-ID 最佳实践

User-ID 最佳实践入门

利用来自广泛存储库（如目录服务器、无线 LAN 控制器、VPN、NACs、代理等）的用户上下文，User-ID™ 支持：

- 识别用户，根据用户的信任级别和行为应用最小权限原则，无需考虑以下因素：
  - 用户位置（如在办公室或在家）
  - 他们使用的设备（如 iOS、Android 移动设备、macOS、Windows、Linux台式机、笔记本电脑、Citrix、Microsoft VDI 或终端服务器）
  - 用户访问的应用程序
- 无需对应用程序进行任何更改，通过在网络层为任何应用程序启用多因素身份验证 (MFA) 来防止在第三方网站上使用企业凭据，同时防止凭据遭到窃取或重用。

无论位置如何，始终可以识别网络上用户的能力为用户活动提供了更好的可见性，支持基于用户和组的安全策略，并帮助您获得更深刻的分析见解（日志、报告和取证）。利用以下最佳实践指南学习如何在网络中计划、部署和维护 User-ID。

User-ID 支持多个功能；本指南介绍了以下几个功能：

- GlobalProtect
- Syslog 监视
- 重新分发
- 组映射
- 动态用户组

其他未包含在本指南中的功能包括：

- Panorama 托管的 Prisma Access
- 凭据网络钓鱼防护
- 以下对象的 IP 地址到用户名映射：
  - 网络访问控制 (NAC) 设备
  - 身份验证门户
  - Active Directory

User-ID 用于 GlobalProtect 的最佳实践

Palo Alto Networks 推荐将 GlobalProtect 作为 User-ID 的最佳实践解决方案。它提供到远程用户的连接，并使用内部网关为内部网络上的用户收集映射。由于 GlobalProtect 要求用户在网络连接、设备状态或用户身份验证状态发生变化时使用他们的凭据进行身份验证，因此可以确保为基于用户的策略实施准确映射用户。

User-ID 用于 GlobalProtect 部署的最佳实践

- 按照 GlobalProtect 快速配置指南确定如何最好地部署 GlobalProtect。对于 User-ID，请使用使用在 VPN 配置中启用和混合内外网关配置。
- 在想要识别用户的所有端点上安装 GlobalProtect 应用程序。
- 确定用于 GlobalProtect 身份验证的用户名的目录属性（如 UserPrincipalName、sAMAccountName 或 common-name）。将这些属性指定为组映射配置文件中的主用户名或备选用户名。
- 如果使用客户端证书身份验证，则证书主题名称字段必须标识用户名。User-ID 不支持机器证书。
- 如果只有一个内部网关，但有其他防火墙需要从该网关学习映射，则计划如何部署重新分发来将映射发送到其他防火墙。
- 确定是否从多个来源接收映射。如果是，请使用 Web 界面或 CLI 评估源，以确定对于从 GlobalProtect 收集到的“IP 地址到用户名”映射，是否可以使用提供其他映射（可能不如 GlobalProtect 提供的映射准确或及时）的来源将其覆盖。

使用 User-ID 最佳实践部署 GlobalProtect

- 部署 GlobalProtect 门户和网关。部署内部和外部网关以一致标识用户，而不考虑其位置。
- 使用内部和外部网关时，使用预登录（始终启用）或用户登录（始终启用）连接方法来启用对网络的访问。
- 如果为身份验证使用证书，请使用简单证书注册协议 (SCEP) 部署为身份验证使用用户特定客户端证书。
- 如果使用内部网关，请使用内部主机检测，以便让 GlobalProtect 应用知道何时将用户发送到内部网关。
- 仅在源区域启用用户标识。例如，如果使用 GlobalProtect 外部网关，则在与隧道接口相关联的区域（**Network**（网络）> **Zones**（区域）> *tunnel-zone*（隧道区域））中启用 User-ID。
- 如果从多个来源接收用户映射，请排除 User-ID 代理上外部 GlobalProtect 网关的 GlobalProtect 子网，从而让 GlobalProtect 提供的用户映射不被其他来源（提供的映射不如 GlobalProtect 提供的映射准确或及时）覆盖。
- 配置重新分发以共享 GlobalProtect 网关使用其他防火墙收集的映射。
- 指定所有允许用户在组映射配置文件中将 GlobalProtect 作为主用户名或备用用户名属性进行身份验证的用户名格式。如果用户在 GlobalProtect 认证期间没有提供域名，则启用 **Allow matching usernames without domains**（允许匹配不包含域的用户名）（**Device**（设备）> **User Identification**（用户标识）> **User Mapping**（用户映射）> **Palo Alto Networks User-ID Agent Setup**（**Palo Alto Networks User-ID** 代理设置））。
- 创建安全策略规则，并测试这些规则是否与预期用户流量流匹配。

为 User-ID 使用 GlobalProtect 的部署后最佳实践

- 在端点上维护并更新 GlobalProtect 应用。如果要更新大量端点，则在 Web 服务器上更新主机应用，从而在用户连接和下载应用时，减少防火墙上的负载，或者使用软件分发工具将更新推送到托管端点。
- 在 GlobalProtect 应用中，确认用户可以成功连接到外部网关。
- 验证防火墙从 GlobalProtect 接收到“IP 地址到用户名”映射。
  - 在 Web 界面上，选择 **Monitor**（监视）> **User-ID**，并确认 **User**（用户）列中显示的用户名。
  - 使用 CLI 命令确认防火墙可以正确收到映射。

User-ID 用于 Syslog 监视的最佳实践

Palo Alto Networks 防火墙可以解析 Syslog 消息，从而获得“IP 地址到用户名”映射。您可以使用现有网络服务和设备（如第三方 VPN 解决方案、网络访问控制 (NAC) 解决方案或使用 Syslog 消息的安全信息和事件管理 (SIEM) 系统）中的身份验证事件。为了保持用户映射处于最新状态，还可以配置防火墙解析注销事件的Syslog 消息，从而自动删除过时的映射。

计划 Syslog 监视部署的 User-ID 最佳实践

- 查看 Syslog 发送方使用的格式，以确定它们使用的语法，即是否包含域名，是否满足条件。
- 确定是否监视登录事件、注销事件，或同时监视两者。如果要监视注销事件，请确认 Syslog 发送方在消息中包含 IP 地址和用户名。
- 根据 Syslog 消息，确定是需要使用正则表达式还是字段标识符。如果 Syslog 消息一致且可预测，则使用字段标识符。如果消息较复杂，且难以预测，则使用正则表达式。
- 建议在防火墙上使用 PAN-OS 集成的 User-ID 代理部署 Syslog 监控，而不要使用 Windows 的 User-ID 代理。

使用 User-ID 最佳实践部署 Syslog 监控

- 如果 Syslog 发送方使用不同的格式，则需要为每种格式配置 Syslog 解析配置文件。
- 如果要同时监视登录和注销事件，请为每种事件类型配置一个 Syslog 解析配置文件。
- 如果 Syslog 消息中不包含域名，且所有域的用户名都是唯一的，请启用 **Allow matching usernames without domains**（允许匹配不包含域的用户名）。
- 在 PAN-OS 集成的 User-ID 代理上，请始终使用 SSL 侦听 Syslog 消息，因为流量是加密的。由于 UDP 以明文发送流量，因此，如果您必须使用 UDP，请确保 Syslog 发送方和客户端均在专用的安全网络上，以防止不可信主机向防火墙发送 UDP 流量。
- 验证要监视的所有 Syslog 发送方是否作为条目包含在服务器监视列表中，因为防火墙会忽略来自该列表之外的发送方的任何 Syslog 消息。
- 按照最可能匹配的顺序对筛选器列表中的条目进行排序。例如，如果您认为 80% 的 Syslog 消息将匹配 filter1，20% 将匹配 filter2，则确保 filter1 在列表中位于 filter2 之前。

为 User-ID 使用 Syslog 监控的部署后最佳实践

- 验证 Syslog 消息是否与 Syslog 解析配置文件匹配，防火墙是否从 Syslog 消息接收“IP 地址到用户名”映射。
- 使用 `show user server-monitor statistics` CLI 命令验证防火墙是否接收来自 Syslog 发送方的消息并正确映射用户。

User-ID 用于重新分发的最佳实践

在大型网络中，您可以配置防火墙通过重新分发来收集已经在其他防火墙上的映射信息，而不是配置所有防火墙来直接查询映射信息源，从而简化资源使用情况。

计划重新分发部署的 User-ID 最佳实践

- 计划重新分发架构。要考虑的一些因素是：
  - 哪些防火墙将对所有数据类型（如“IP 地址到用户名”映射或设备隔离信息）实施策略，哪些防火墙会接收数据的子集？
  - 哪些IP范围需要“IP地址到用户名”映射？
  - 如果您有一个提供用户映射的内部网关，其他哪些设备需要这些数据？它们有哪些功能和角色？
  - 如何最小化聚合所有数据所需的跃点数量？“IP 地址到用户名”映射的最大允许跃点数为 10，“用户名到标记”映射和“IP 地址到标记”映射的最大允许跃点数均为 1。
  - 如何最大程度减少用于查询用户映射信息源的防火墙的数量？查询防火墙的数量越少，防火墙和信息源上的处理负载就越少。
- 确定重新分发中心的最佳选择：
  - 专用 VM 系列防火墙最适合大规模 User-ID 部署。如果仅重新分发用户映射，则 VM-50 已足够。如果您还计划重新分发“IP 地址到标记”映射，建议使用 VM-300 或更高规格的系列。
  - 如果不使用 Syslog 或服务器监控来收集用户映射，Panorama 最适合中小规模的环境。
- 根据网络需求，请确定要使用哪一种类型的拓扑结构：
  - 适用于单个区域的中心辐射型结构
  - 适用于多个区域的中心辐射型结构
  - 层级结构

使用 User-ID 最佳实践部署重新分发

- 配置要重新分发的信息源：
  - User-ID“IP 地址到用户名”映射（包含 Windows User-ID 代理）
  - 动态地址组的“IP 地址到标记”映射
  - 动态用户组的“用户名到标记”映射
  - 基于 HIP 的策略实施的数据
  - 设备隔离信息
- 配置您希望代理在数据重新分发中包含的网络，以及您希望从重新分发“IP 地址到标记”映射或“IP 地址到用户名”映射中排除的网络。
- 使用包含/排除网络列表定义重新分发在重新分发映射时包含或排除的子网。
- 配置通过重新分发接收特定数据类型的网络或资源。
- 启用为重新分发使用自定义证书进行身份验证，从而为重新分发代理与客户端之间的交互认证使用自定义证书。
- 使用 VM 系列防火墙或 Panorama 重新分发数据。由于 Panorama 可以使用代理或客户端，因此，请使用 **Panorama** > **Data Redistribution**（重新分发数据）在 Panorama 上配置数据重新分发。
- 如果执行策略的防火墙同时需要来自远程和本地用户的映射（因为它也是 GlobalProtect 网关和数据中心），则启用双向重新分发。
- 为了确保最佳弹性，您只能在一个区域内启用双向重新分发，而不能在区域之间启用。

为 User-ID 使用重新分发的部署后最佳实践

- 按照配置数据重新分发中的最后两个步骤验证代理已正确将数据重新分发给客户端。

User-ID 用于组映射的最佳实践

根据用户组成员资格（而不是个人用户）来定义策略规则将简化管理，因为这样避免了只要组成员资格发生更改，您就必须更新规则的情况。对于轻型目录访问协议 (LDAP) 部署的组映射配置，建议使用以下最佳实践。

以下部分介绍了为本地目录服务部署组映射的最佳实践。

计划组映射部署的 User-ID 最佳实践

- 确定目录服务（如 Active Directory 或基于 LDAP 的服务，如 OpenLDAP），并确定目录服务器的拓扑结构。需要考虑的一些问题包括：
  - 目录服务器、数据中心和域控制器分别有多少？
  - 组信息的主要来源是什么？
  - 域控制器位于相对于目录服务器的何处？
  - 目录服务器和域控制器是否在不同的区域？
  - 哪些资源是本地的，哪些是区域化的？
- 在部署时，组映射的主要来源是 Active Directory 服务器：
  - 如果您具有单个域，则仅需要一个带 LDAP 服务器配置文件的组映射配置，此配置文件将防火墙连接到连接性最佳的域控制器。最多可以将四个域控制器添加到 LDAP 服务器配置文件以实现冗余。
  - 如果您具有通用组，则创建一个 LDAP 服务器配置文件以与 SSL 端口 3268 或 3269 上的全局目录服务器的根域连接，然后创建另一个 LDAP 服务器配置文件以使用端口 636 上的 LDAPS 与根域控制器连接。如果不使用 TLS，请使用端口 389。这有助于所有域和子域都能使用用户和组信息。
  - 如果没有通用组，但有多个域或多个林，则必须创建一个带 LDAP 服务器配置文件的组映射配置，以将防火墙连接至每个域/林中的域服务器。执行相应步骤以确保单个林中用户名的唯一性。
  - 在使用组映射之前，请为基于用户的安全策略规则配置主用户名，因为此属性将标识策略配置、日志和报告中的用户。
- 要创建 LDAP 目录中没有的自定义组，请使用用户属性创建自定义组。
- 如果创建多个使用相同基本重新分发名称 (DN) 或 LDAP 服务器的组映射配置，请确保组映射配置不包含重叠组。例如，一个组映射配置的包含列表不能包含另一个组映射配置中的组。
- 确保用户名和组属性对于每个域中的所有用户和组都是唯一的。
- 通过使用组包括列表或应用自定义搜索筛选器，仅检索将在基于组的安全策略和配置中使用的组。
- 请评估目录中的组更改频率，以确定组映射配置文件的最佳 **Update Interval**（更新间隔）值。例如，如果经常更改组，则配置一个较小的值，但如果它们通常是静态的，则输入一个较大的值。
- 确定要在日志、报告和策略配置中表示用户的用户名属性。如果 User-ID 源以不同的格式发送用户名，请指定这些用户名作为替代属性。

确保主用户名、备用用户名和电子邮件属性对每个用户都是唯一的。

使用 User-ID 最佳实践部署组映射

- 如果仅使用目录中的自定义组，请将未使用的组添加到包含列表中，以防止 User-ID 从目录中检索所有组。
- 使用 **Group Include List**（组包含列表）将策略规则限制到特定的组。或者，通过输入 **Search Filter**（搜索筛选器）（LDAP 查询）和 **Object Class**（对象类）（组定义）来筛选防火墙跟踪的组映射。如果 LDAP 目录中没有现有组，可以使用用户属性在防火墙上创建自定义组。确保用于构建自定义组的属性是目录上的索引属性。

- 指定用于识别报告和日志中用户的主用户名。

为 User-ID 使用组映射的部署后最佳实践

- 要确认与 LDAP 服务器的连接，请使用 CLI 命令 `show user group mapping state all`。
- 要查看组成员资格，请运行 `show user group name <group name>` 命令。
- 在安全策略中使用组之前，确认用户位于组中。要验证策略规则中当前可以使用哪些组，请使用 CLI 命令 `show user group`。
- 如果已更改组映射，请手动刷新缓存。要手动刷新缓存，请运行 `debug user-id refresh group-mapping all` 命令。

User-ID 用于动态用户组的最佳实践

利用动态用户组，您可以响应用户行为、业务需求或潜在威胁的更改，无需手动更改策略或创建和更新组。动态用户组可以帮助您创建具有以下特点的安全策略：

- 用户访问资源有时间限制
- 自动修复异常用户行为和恶意活动，同时保持用户可见性

使用标记定义组的条件并提交更改之后，动态用户组的成员关系将根据用户标记自动更新。

计划动态用户组部署的 User-ID 最佳实践

- 根据业务需求或用户行为的变化等因素，确定您希望防火墙如何控制用户访问权限：
  - 是否希望通过安全策略来允许或限制访问权限？
  - 是否希望要求用户使用 MFA？
  - 是否需要解密用户流量以获得对用户活动的更多了解？
- 确定用户在特定动态用户组中的成员资格持续时间。
  - 防火墙是否应根据时间（例如，承包商临时资源访问需要的小时数）自动将用户从组中删除？
  - 防火墙是否需要特定的事件来关联或解除用户与组的关联（例如，恶意活动）？
- 评估通过防火墙生成的哪些事件可以识别用户行为或业务需求的变化。您可以通过 API、自动标记来分配标记，也可以使用 Web 界面手动分配。
  - 根据用例，确定将使用哪些标记对用户进行分组，以及如何生成标记。
  - 例如，根据用户行为评估用户的风险级别（如“高风险”、“中等风险”和“低风险”），并根据这些事件自动为用户分配标记。
- 识别标记的用户信息来源：
  - 防火墙日志
    - 对于身份验证、数据、威胁、流量、隧道检测、URL 和 WildFire 日志，请创建日志转发配置文件并使用内置操作。
    - 对于 User-ID、HIP 匹配、GlobalProtect 和 IP 标记日志，请配置日志设置。
  - Cortex XSOAR
  - 安全信息和事件管理系统，如 Splunk
  - 自定义 API 脚本
- 将多个来源的标记组合在一起，从而定义动态用户组的标准。例如，仅当您收到来自多个安全应用程序（而不是单个应用程序）的用户凭据发生泄露的警报时，您可能才会希望基于信任级别拒绝用户访问。

使用 User-ID 部署动态用户组的最佳实践

- 如果需要将大量用户添加到动态用户组，或者需要根据其他安全应用程序的事件添加用户，请使用 API（而不是 Web 界面）添加用户。
- 从该组中移除用户时，请使用 API 或手动定义 **Timeout**（超时）（例如，在合同到期时）。
- 创建使用动态用户组作为源用户的安全策略规则来控制用户访问权限，启用 MFA 或为动态用户组的用户解密流量。
- 配置来源，为用户标记提供信息：
  - 如果使用防火墙日志，则通过配置自动标记来标记用户。
  - 如果使用 Splunk，则可以使用用于 Splunk 的 Palo Alto Networks 应用将标记分配给用户。
  - 在 Cortex XSOAR 或其他安全编排、自动化和响应 (SOAR) 平台中使用剧本，根据特定的事件将标记应用到用户。
  - 如果您使用自定义脚本，请修改脚本以使用 API 填充标记。

- 使用防火墙的 Web 界面手动将用户添加到组中。

为 User-ID 使用动态用户组的部署后最佳实践

- 检查组成员资格，确保仅希望包括的用户是该组的成员。如果该组包括不属于其中的用户（例如，“contractor-access”组中的永久员工），则 **Unregister Users**（取消注册用户），以移除其“用户名到标记”映射，并将其从组中 **Delete**（删除）。
- 检查 User-ID 日志，以验证防火墙是否为用户正确生成了标记。
- 使用 CLI 命令了解关于动态用户组的更多详细信息（例如，查看与组相关联的用户）。
- 使用“流量和威胁日志”上的动态用户组列确保防火墙将组匹配到预期安全策略。
- 将用户标记重新分发到其他防火墙，以确保所有防火墙一致地应用安全策略。请记住，您只能为一个跃点重新分发用户标记。