paloalto
TECHDOCS

Administración de Advanced WildFire

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

© 2021-2023 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

June 29, 2023

Table of Contents

 ©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

Descripción general de Advanced WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

Advanced WildFire™ proporciona detección y prevención de malware de día cero mediante una combinación de análisis dinámico/estático y análisis inteligente de memoria en tiempo de ejecución para detectar amenazas altamente evasivas y crear protecciones para bloquear el malware.

El entorno de análisis de Advanced WildFire identifica el malware desconocido previamente y genera firmas que los NGFW de Palo Alto Networks pueden utilizar para detectar y bloquear el malware. Cuando un cortafuegos de Palo Alto Networks detecta una muestra desconocida, el cortafuegos reenvía automáticamente todos los tipos de archivos compatibles desde cualquier aplicación al servicio de nube pública de WildFire para el análisis de Advanced WildFire. En función de las propiedades, los comportamientos y las actividades que muestre la muestra cuando se analice y ejecute en el espacio aislado, Advanced WildFire determinará si la muestra es benigna, grayware, phishing o maliciosa y, a continuación, generará firmas para reconocer el malware recién descubierto y hacer que las firmas más recientes estén disponibles en todo el mundo para su obtención en tiempo real. Todos los cortafuegos de Palo Alto Networks pueden comparar las muestras entrantes con estas firmas para bloquear automáticamente el malware detectado inicialmente por un solo cortafuegos.

Para obtener más información sobre Advanced WildFire o para comenzar, consulte los siguientes temas:

- Revise Conceptos de Advanced WildFire para obtener más información sobre los tipos de muestras que puede enviar para el análisis de WildFire, los veredictos de WildFire y las firmas de WildFire.
- Obtenga más información sobre las Implementaciones de Advanced WildFire que puede configurar con el cortafuegos. Puede enviar las muestras que desea que se analicen a una nube de WildFire alojada en Palo Alto Networks o una nube privada de WildFire alojada localmente, o puede utilizar una nube híbrida, en cuyo caso, el cortafuegos envía determinadas muestras a la nube pública y determinadas muestras a una nube privada.
- Comience con Advanced WildFire para definir las muestras que desea enviar para el análisis y para comenzar a enviar muestras a una nube de WildFire.
- Si va a implementar un dispositivo WildFire, consulte la Administración de dispositivos WildFire.

Opciones de suscripción

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

El servicio WildFire básico se incluye como parte del cortafuegos de próxima generación de Palo Alto Networks y no requiere una suscripción a Advanced WildFire o WildFire. Con el servicio básico de WildFire, el cortafuegos puede enviar archivos portables ejecutables (PE) para el análisis, y puede recuperar las firmas en Advanced WildFire solamente con el antivirus y/o las actualización de prevención de amenazas que están disponibles cada 24-48 horas.

Palo Alto Networks ofrece varias opciones de suscripción:

- **WildFire**: la suscripción a WildFire proporciona protección frente a malware al enviar muestras a la nube de Advanced WildFire, donde se utilizan una serie de entornos de análisis para detectar y prevenir amenazas de malware desconocidas generando protecciones que bloquean más instancias de la amenaza. Como parte de su suscripción, obtendrá acceso a actualizaciones periódicas de firmas de Advanced WildFire, reenvío avanzado de tipos de archivos y la posibilidad de cargar archivos utilizando la API de WildFire. Si está operando un entorno que requiere una solución local, la suscripción de WildFire se puede utilizar para reenviar archivos a un dispositivo WildFire local.
- **Advanced WildFire**:(PAN-OS 10.0 y posterior) La suscripción a Advanced WildFire incluye todas las funciones que se encuentran en la suscripción estándar de WildFire y las mejora al proporcionar análisis de muestras a través de un detector avanzado basado en la nube. El sistema de detección avanzado analiza muestras utilizando análisis inteligente de memoria en tiempo de ejecución en tiempo real, emulación de DLL en tiempo de ejecución, desempaquetado automatizado, clasificación familiar, observación sigilosa y otras técnicas para atacar malware altamente evasivo.
- **API independiente de WildFire**: los clientes de Palo Alto Networks que operan herramientas SOAR, aplicaciones de seguridad personalizadas y otro software de evaluación de amenazas pueden acceder a las capacidades avanzadas de análisis de archivos de la nube de WildFire con una suscripción independiente que proporciona acceso solo a la API. Esto le permite aprovechar los análisis basados en WildFire sin depender del cortafuegos de Palo Alto Networks como mecanismo de reenvío. La suscripción a la API independiente de WildFire le permite realizar consultas directas a la base de datos de amenazas en la nube de WildFire para obtener información sobre contenido potencialmente malicioso y enviar archivos para su análisis utilizando las capacidades avanzadas de análisis de amenazas de WildFire, en base a los requisitos específicos de su organización. Los límites de acceso mejorados de la suscripción permiten a organizaciones de varios tamaños personalizar sus límites de acceso según su uso; esto incluye licencias adaptables que permiten un número específico de consultas de archivos/informes, envíos de muestras (para análisis de Advanced WildFire) o una combinación de los dos. Consulte la Referencia de API de WildFire para obtener más información.

 ©2025 Palo Alto Networks, Inc.

La suscripción estándar a WildFire proporciona las siguientes funciones:

- **Actualizaciones en tiempo real)**: [PAN-OS 10.0 y posterior]: el cortafuegos puede recuperar firmas de Advanced WildFire para malware recién detectado tan pronto como la nube pública de Advanced WildFire pueda generarlas. Las firmas que se descargan durante una verificación de muestra se guardan en la caché del cortafuegos y están disponibles para búsquedas rápidas (locales). Además, para maximizar la cobertura, el cortafuegos también descarga automáticamente un paquete de firmas de forma regular cuando las firmas en tiempo real están habilitadas. Estas firmas complementarias se añaden a la caché del cortafuegos y permanecen disponibles hasta que se vuelven obsoletas y se actualizan, o se sobrescriben con nuevas firmas. El uso de actualizaciones de Advanced WildFire en tiempo real es una opción recomendable.

  Seleccione **Device (Dispositivo)** > **Dynamic Updates (Actualizaciones dinámicas)** y habilite el cortafuegos para obtener las firmas de Advanced WildFire más recientes en tiempo real.

- **Actualizaciones cada cinco minutos)** (todas las versiones de PAN-OS): la nube pública de Advanced WildFire puede generar y distribuir firmas de Advanced WildFire cada cinco minutos para cada nuevo malware descubierto, y usted puede configurar el cortafuegos para recuperar e instalar estas firmas cada minuto (esto permite al cortafuegos recibir las firmas más recientes en un plazo de disponibilidad de un minuto).

  Si utiliza PAN-OS 10.0 o una versión posterior, se recomienda usar actualizaciones de Advanced WildFire en tiempo real en lugar de programar actualizaciones periódicas.

  Seleccione **Device (Dispositivo)** > **Dynamic Updates (Actualizaciones dinámicas)** para habilitar el cortafuegos y obtener las firmas de Advanced WildFire más recientes. Dependiendo de su implementación de Advanced WildFire, puede configurar una o ambas de las siguientes actualizaciones del paquete de firmas:

  - **WildFire**: obtiene las firmas más recientes de la nube pública de WildFire.
  - **WF-Private**: obtiene las firmas más recientes de un dispositivo WildFire configurado para generar firmas y categorías de URL localmente.

- **Aprendizaje automático en línea de Advanced WildFire** (PAN-OS 10.0 y versiones posteriores): evite que las variantes maliciosas de portables ejecutables, los archivos de formato vinculados (ELF) y ejecutables, y los scripts de PowerShell entren a su red en tiempo real mediante el aprendizaje automático (ML) en el plano de datos del cortafuegos. Mediante el uso de la tecnología de análisis de la nube de Advanced WildFire en el cortafuegos, Aprendizaje automático en línea de Advanced WildFiredetecta dinámicamente archivos maliciosos de un tipo específico, mediante la evaluación de varios detalles del archivo, incluidos los campos y patrones del descodificador, para formular una clasificación de alta probabilidad de un archivo. Esta protección se extiende a variantes de amenazas actualmente desconocidas y futuras que coinciden con características que Palo Alto Networks ha identificado como maliciosas. Aprendizaje automático en línea de Advanced WildFire complementa la configuración de protección de su perfil de antivirus existente. Además, puede especificar excepciones de hash de archivos para excluir cualquier falso positivo que encuentre, lo que le permite crear reglas más detalladas en sus perfiles para satisfacer sus necesidades de seguridad específicas.

- **Compatibilidad con tipos de archivos**: además de PE, envía tipos de archivos avanzados para el análisis de Advanced WildFire, incluidos APK, archivos Flash, PDF, archivos de Microsoft Office, applets Java, archivos Java (.jar y .class) y enlaces de correo electrónico HTTP/HTTPS contenidos en mensajes de correo electrónico SMTP y POP3. (El análisis de nube privada de WildFire no admite archivos APK, Mac OS X, Linux (ELF), archivos de almacenamiento (RAR/7-Zip) y archivos de script (JS, BAT, VBS, script de shell, PS1 y HTA)).

 ©2025 Palo Alto Networks, Inc.

- **API de Advanced WildFire**: acceda a la API de WildFire, que permite el acceso programático directo a la nube pública de Advanced WildFire o a una nube privada de WildFire. Use la API para enviar archivos para el análisis y para recuperar los posteriores informes de análisis de Advanced WildFire. Como parte de la suscripción a Advanced WildFire o WildFire, puede enviar hasta 150 envíos de muestra y hasta 1050 consultas de muestra por día. Estos límites de envío de muestras diarias se pueden ampliar, en función de las necesidades específicas de su organización. Póngase en contacto con su representante de ventas de Palo Alto Networks para obtener más información.
- **Compatibilidad con la nube híbrida y privada de WildFire**:Reenviar archivos para Advanced WildFire Analysis. Las implementaciones de nube privada de WildFire y nube híbrida de WildFire requieren que el cortafuegos pueda enviar muestras a un dispositivo WildFire. La habilitación de un dispositivo WildFire necesita solamente una licencia de asistencia.

Si adquirió una suscripción a Advanced WildFire, debe activar la licencia para poder aprovechar las funciones que solo están en la suscripción a WildFire.

La suscripción a Advanced WildFire desbloquea la siguiente función:

- **Análisis inteligente de memoria en tiempo de ejecución**: el análisis inteligente de memoria en tiempo de ejecución es un motor de análisis avanzado basado en la nube que complementa los motores de análisis estáticos y dinámicos para detectar y prevenir amenazas de malware evasivas. Estas técnicas evasivas utilizadas por las amenazas avanzadas incluyen, entre otras, malware que utiliza estrategias de encubrimiento, muestra signos de diseño personalizado/comportamientos efímeros, se crea con herramientas sofisticadas y exhibe cualidades de rápida propagación. Al aprovechar una infraestructura de detección basada en la nube, los detectores de análisis introspectivo operan una amplia gama de mecanismos de detección que se actualizan e implementan automáticamente, sin necesidad de que el usuario descargue paquetes de actualización de contenido o ejecute analizadores basados en dispositivos que consumen muchos recursos. Los motores de detección basados en la nube se supervisan y actualizan continuamente, utilizando conjuntos de datos basados en aprendizaje automático que se utilizan para analizar muestras de Advanced WildFire, con el apoyo adicional de los investigadores de amenazas de Palo Alto Networks, que brindan intervención humana para mejoras de detección altamente precisas.

  El análisis inteligente de memoria en tiempo de ejecución se basa en la configuración del perfil de análisis de WildFire existente y no requiere ninguna configuración adicional; sin embargo, deberá tener una licencia de Advanced WildFire activa. Las muestras que se muestran o indican de algún modo cualidades de malware evasivas y/o avanzadas se reenvían automáticamente a los entornos de análisis adecuados.

 ©2025 Palo Alto Networks, Inc.

Conceptos de Advanced WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

- Muestras
- Envío desde el cortafuegos
- Uso compartido de la información de la sesión
- Entorno de análisis
- Análisis en línea en la nube para Advanced WildFire
- Aprendizaje automático en línea de Advanced WildFire
- Veredictos
- Análisis de archivos
- Análisis de enlaces de correo electrónico
- Análisis de URL
- Análisis de archivos comprimidos y codificados
- Firmas avanzadas de WildFire
- Ejemplo avanzado de WildFire

Muestras

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

©2025 Palo Alto Networks, Inc.

Las muestras son todos los tipos de archivos y enlaces de correo electrónico enviados para el análisis de Advanced WildFire desde el cortafuegos y la API pública. Consulte en Análisis de archivos y Análisis de enlaces de correo electrónico más información sobre los tipos de archivos y enlaces que un cortafuegos puede enviar para el análisis de Advanced WildFire.

Envío desde el cortafuegos

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

El cortafuegos reenvía muestras desconocidas, además de los archivos bloqueados que coinciden con las firmas de antivirus, para el análisis de Advanced WildFire según los ajustes de perfil de análisis de WildFire configurados (**Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **WildFire Analysis (Análisis de WildFire)**). Además de detectar los enlaces incluidos en correos electrónicos, los archivos que se adjuntan a los correos electrónicos y las descargas de archivos basadas en navegadores, el cortafuegos aprovecha App-ID para detectar las transferencias de archivos dentro de las aplicaciones. En el caso de las muestras que detecta el cortafuegos, el cortafuegos analiza la estructura y el contenido de la muestra y la compara con las firmas existentes. Si la muestra coincide con una firma, el cortafuegos aplica la acción predeterminada definida para la firma (permitir, enviar alerta o bloquear). Si la muestra coincide con una firma de antivirus o sigue siendo desconocida tras compararla con las firmas de Advanced WildFire, el cortafuegos la envía para el análisis de Advanced WildFire.

De manera predeterminada, el cortafuegos también reenvía información sobre la sesión en la que se detectó la muestra desconocida. Para gestionar la información de la sesión que reenvía el cortafuegos, seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **WildFire** y edite la configuración de información de sesión.

Uso compartido de la información de la sesión

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

©2025 Palo Alto Networks, Inc.

¿Dónde puedo usar esto?	¿Qué necesito?
• CN-Series	

Además de reenviar muestras desconocidas y bloqueadas para el análisis, el cortafuegos reenvía información sobre la sesión de la red para una muestra. Palo Alto Networks utiliza la información de la sesión para obtener más información sobre el contexto del evento de red sospechoso, los indicadores de compromiso relacionados con el malware, los hosts y los clientes afectados, y las aplicaciones utilizadas para entregar el malware.

El reenvío de la información de sesión está habilitado de forma predeterminada; sin embargo, puede ajustar la configuración predeterminada y elegir qué tipo de información de sesión se reenvía a una de las opciones de nube de WildFire.

- Strata Cloud Manager
- PAN-OS y Panorama

Uso compartido de la información de la sesión (Cloud Management)

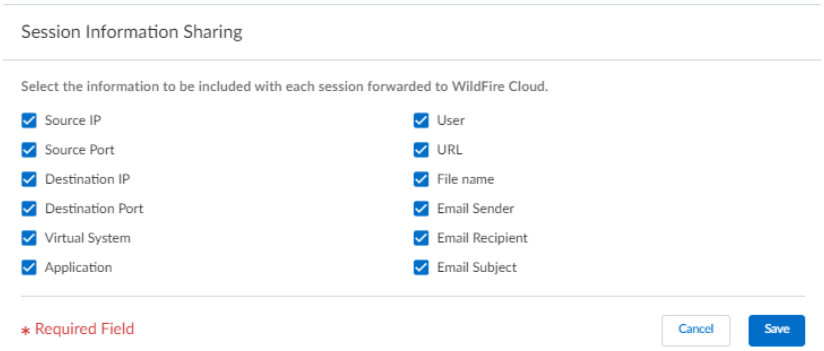
Si está utilizando Panorama para gestionar Prisma Access:

*Desplácese a la pestaña **PAN-OS** y siga las instrucciones que se indican allí.*

Si está utilizando Prisma Access Cloud Management, continúe aquí.

STEP 1 | Utilice las credenciales asociadas con su cuenta de asistencia técnica de Palo Alto Networks e inicie sesión en la aplicación de Strata Cloud Manager en el hub.

STEP 2 | Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and (NGFW y)Prisma Access** > **Security Services (Servicios de seguridad)** > **WildFire and Antivirus (WildFire y antivirus)** y configure las opciones de **Session Information Settings (Configuración de información de sesión)**.



- **Source IP (IP de origen)**: se reenvía la dirección IP de origen que envió el archivo desconocido.
- **Source Port (puerto de origen)**: se reenvía el puerto de origen que envió el archivo desconocido.
- **Destination IP (IP de destino)**: se reenvía la dirección IP de destino del archivo desconocido.
- **Destination Port (puerto de destino)**: se reenvía el puerto de destino del archivo desconocido.
- **Virtual System (Sistema virtual)**: se reenvía el sistema virtual que detectó el archivo desconocido.

 ©2025 Palo Alto Networks, Inc.

- **Application (Aplicación)**: se reenvía la aplicación de usuario que transmitió el archivo desconocido.
- **User (Usuario)**: se reenvía el usuario de destino.
- **URL**: se reenvía la URL asociada al archivo desconocido.
- **Filename (Nombre del archivo)**: se reenvía el nombre del archivo desconocido.
- **Email sender (Remitente del correo electrónico)**: se reenvía el remitente de un enlace de correo electrónico desconocido (el nombre del remitente del correo electrónico también aparece en los logs e informes de WildFire).
- **Email recipient (Destinatario del correo electrónico)**: se reenvía el destinatario de un enlace de correo electrónico desconocido (el nombre del destinatario del correo electrónico también aparece en los logs e informes de WildFire).
- **Email subject (Asunto del correo electrónico)**: se reenvía el asunto de un enlace de correo electrónico desconocido (el asunto del correo electrónico también aparece en los logs e informes de WildFire).

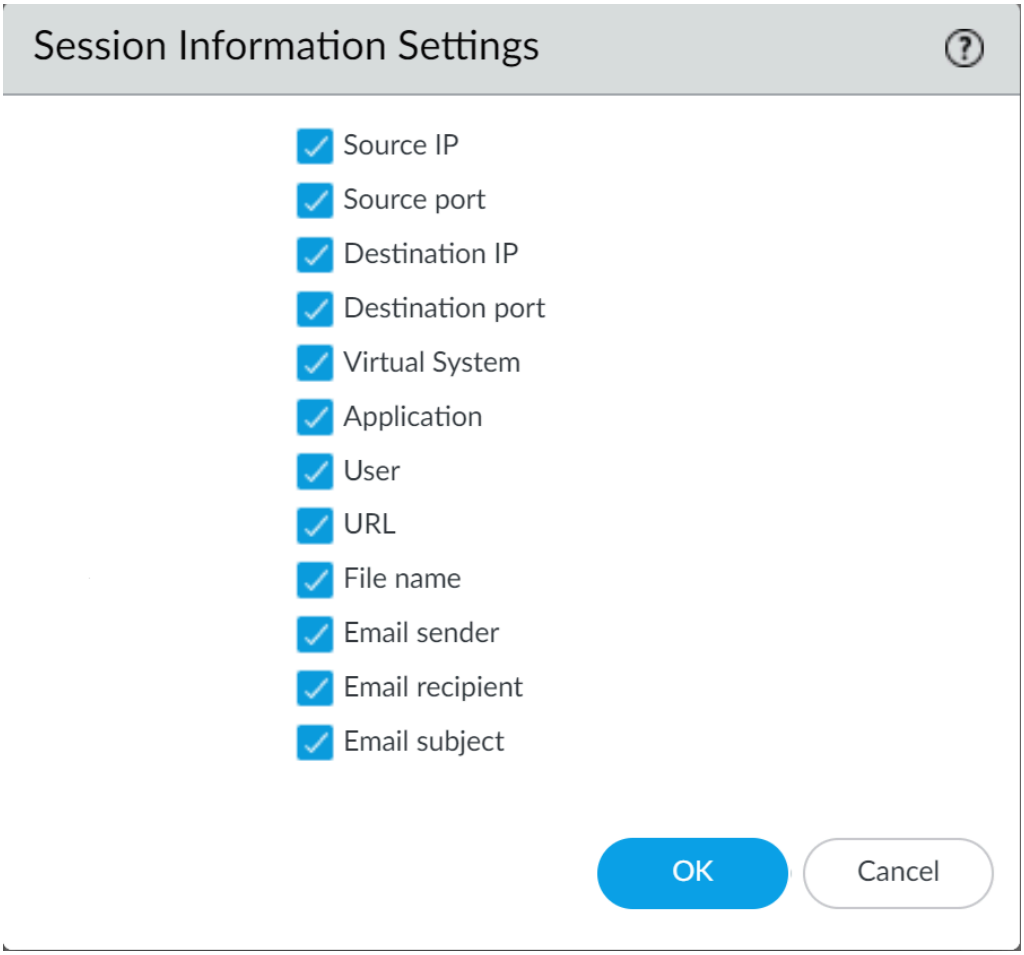
STEP 3 | Haga clic en **Save (Guardar)** para guardar sus cambios.

Uso compartido de sesión (PAN-OS y Panorama)

STEP 1 | Inicie sesión en la interfaz web de PAN-OS.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **WildFire** y seleccione o elimine las siguientes opciones de **Session Information Settings (Configuración de información de sesión)**.



- **Source IP (IP de origen)**: se reenvía la dirección IP de origen que envió el archivo desconocido.
- **Source Port (puerto de origen)**: se reenvía el puerto de origen que envió el archivo desconocido.
- **Destination IP (IP de destino)**: se reenvía la dirección IP de destino del archivo desconocido.
- **Destination Port (puerto de destino)**: se reenvía el puerto de destino del archivo desconocido.
- **Virtual System (Sistema virtual)**: se reenvía el sistema virtual que detectó el archivo desconocido.
- **Application (Aplicación)**: se reenvía la aplicación de usuario que transmitió el archivo desconocido.
- **User (Usuario)**: se reenvía el usuario de destino.
- **URL**: se reenvía la URL asociada al archivo desconocido.
- **Filename (Nombre del archivo)**: se reenvía el nombre del archivo desconocido.
- **Email sender (Remitente del correo electrónico)**: se reenvía el remitente de un enlace de correo electrónico desconocido (el nombre del remitente del correo electrónico también aparece en los logs e informes de WildFire).
- **Email recipient (Destinatario del correo electrónico)**: se reenvía el destinatario de un enlace de correo electrónico desconocido (el nombre del destinatario del correo electrónico también aparece en los logs e informes de WildFire).

 ©2025 Palo Alto Networks, Inc.

- **Email subject (Asunto del correo electrónico)**: se reenvía el asunto de un enlace de correo electrónico desconocido (el asunto del correo electrónico también aparece en los logs e informes de WildFire).

STEP 3 | Haga clic en **OK (Aceptar)** para guardar los cambios.

Entorno de análisis

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

Advanced WildFire reproduce diversos entornos de análisis, entre el que se incluye el sistema operativo, para identificar los comportamientos malintencionados en las muestras. Según las características y las funciones de la muestra, es posible que se utilicen múltiples entornos de análisis para determinar la naturaleza del archivo. Advanced WildFire utiliza análisis estáticos con aprendizaje automático para determinar inicialmente si las muestras conocidas y sus variantes son malintencionadas. Según el veredicto inicial del envío, Advanced WildFire envía las muestras desconocidas a entornos de análisis para inspeccionar el archivo con mayor detalle extrayendo información adicional e indicadores de análisis dinámicos. Si el archivo se cifra con métodos personalizados o de código abierto, la nube de Advanced WildFire descomprime y descifra el archivo en la memoria dentro del entorno de análisis dinámico antes de realizar el análisis estático. Durante los análisis dinámicos, Advanced WildFire observa el comportamiento del archivo cuando se ejecuta en los sistemas cliente y busca varios signos de actividades malintencionadas, como cambios en la configuración de seguridad del explorador, introducción de código en otros procesos, modificación de archivos de las carpetas del sistema operativo o dominios malintencionados a los que la muestra ha intentado acceder. Además, las PCAP que se generan durante el análisis dinámico en la nube de Advanced WildFire se analizan detalladamente y se usan para crear perfiles de actividad en la red. Los perfiles de tráfico de red pueden detectar malware conocido y malware previamente desconocido con una coincidencia múltiple de perfil.

Advanced WildFire puede analizar archivos utilizando los siguientes métodos, en base a las características de la muestra:

- **Static Analysis (Análisis estático)**: detecta amenazas conocidas analizando las características de las muestras antes de la ejecución.
- **Machine Learning (Aprendizaje automático)**: identifica variantes de amenazas conocidas comparando conjuntos de malware con un sistema de clasificación de actualización dinámica.
- **Dynamic Unpacking (Advanced WildFire global cloud only) [Descompresión dinámica (nube global de Advanced WildFire únicamente)]**: identifica y descomprime los archivos que se cifraron con métodos personalizados/de código abierto y los prepara para el análisis estático.

 ©2025 Palo Alto Networks, Inc.

- **Dynamic Analysis (Análisis dinámico)**: un entorno virtual personalizado resistente a las evasiones en el que se detonan envíos desconocidos previamente para determinar los efectos y el comportamiento en el mundo real.
- **Análisis inteligente de memoria en tiempo de ejecución (Licencia de Advanced WildFire | Solo nube global de Advanced WildFire; requiere PAN-OS 10.0 y versiones posteriores en NGFW)**: un entorno de análisis basado en la nube que opera detectores avanzados utilizados para analizar amenazas modernas utilizando una multitud de técnicas de evasión.

Advanced WildFire opera entornos de análisis que replican los siguientes sistemas operativos:

- **Microsoft Windows XP de 32 bits (compatible como opción únicamente para la nube privada de WildFire)**
- **Microsoft Windows 7 de 64 bits**
- **Microsoft Windows 7 de 32 bits (compatible como opción para la nube privada de WildFire únicamente)**
- **Microsoft Windows 10 de 64 bits (compatible como opción para la nube pública de Advanced WildFire y la nube privada de WildFire que ejecutan PAN-OS 10.0 o posterior)**
- **Mac OS X (nube pública de Advanced WildFire únicamente)**
- **Android (nube pública de Advanced WildFire únicamente)**
- **Linux (nube pública de Advanced WildFire únicamente)**

La nube pública de Advanced WildFire también analiza los archivos utilizando múltiples versiones de software para identificar con precisión el malware que apunta a las versiones específicas de las aplicaciones de cliente. La nube privada de WildFire no admite análisis en varias versiones y no analiza archivos específicos de una aplicación en varias versiones.

Análisis en línea en la nube para Advanced WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire

La nube de Advanced WildFire opera una serie de motores de detección basados en aprendizaje automático en línea en la nube para analizar muestras de PE (ejecutables portátiles) que atraviesan su red para detectar y prevenir malware desconocido en tiempo real. Esto permite que el servicio en la nube de Advanced WildFire detecte malware nunca antes visto (que no tiene una firma WildFire existente o que es detectable a través de los detectores de aprendizaje automático en línea en la nube de Advanced WildFirelocales) y evite que infecte al cliente. Esto incluye escenarios en los que ciertos tipos de malware que no se habían visto anteriormente y que no son interceptados por el ML en línea de Advanced WildFire pueden avanzar sin obstáculos porque el archivo no se vio bien recientemente como para que su firma esté presente en el cortafuegos debido a la caducidad de la firma o a los límites de capacidad de la base de datos de firmas. Los archivos maliciosos recientemente definidos se bloquearán en encuentros posteriores del cortafuegos ya que la firma habrá pasado a formar parte del conjunto actual; sin embargo, eso ocurre después de que la nube de WildFire analiza el archivo malicioso.

 ©2025 Palo Alto Networks, Inc.

La nube en línea de Advanced WildFire puede evitar que los archivos se descarguen (y potencialmente se propaguen dentro de su red) mientras analiza estos archivos sospechosos en busca de malware en la nube, en un intercambio en tiempo real. Al igual que con otro contenido malicioso analizado por WildFire, cualquier amenaza detectada por la nube en línea de Advanced WildFire genera una firma de amenaza que Palo Alto Networks difunde a los clientes a través de un paquete de actualización de firmas para brindar una defensa futura a todos los clientes de Palo Alto Networks.

La nube en línea de Advanced WildFire funciona utilizando un mecanismo de reenvío ligero en el cortafuegos para minimizar cualquier impacto en el rendimiento local; y para mantenerse al día con los últimos cambios en el panorama de amenazas, los modelos de detección de ML en línea en la nube se agregan y actualizan sin problemas en la nube, sin requerir actualizaciones de contenido o soporte de lanzamiento de funciones.

El análisis en línea en la nube de Advanced WildFire se habilita y configura a través del perfil de análisis de WildFire y requiere PAN-OS 11.1 o posterior con una licencia avanzada de WildFire activa.

Aprendizaje automático en línea de Advanced WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

La opción de Aprendizaje automático en línea de Advanced WildFire presente en el perfil de antivirus permite que el plano de datos del cortafuegos aplique el aprendizaje automático en archivos ejecutables portátiles (PE), archivos ELF (formato ejecutable y vinculado), archivos MS Office, OOXML, Mach-O y scripts PowerShell y shell en tiempo real. Esta capa de protección antivirus complementa las firmas basadas en Advanced WildFire para proporcionar una cobertura ampliada para archivos cuyas firmas aún no existen. Cada modelo de aprendizaje automático en línea detecta dinámicamente archivos maliciosos de un tipo específico mediante la evaluación de los detalles del archivo, incluidos los campos y patrones del descodificador, para formular una clasificación de alta probabilidad de un archivo. Esta protección se extiende a variantes de amenazas actualmente desconocidas y futuras que coinciden con características que Palo Alto Networks ha identificado como maliciosas. Para mantenerse al día con los últimos cambios en el panorama de las amenazas, se añaden o actualizan modelos de aprendizaje automático en línea a través de lanzamientos de contenido. Para poder habilitar el aprendizaje automático en línea de Advanced WildFire, debe poseer una suscripción activa a Advanced WildFire o a una suscripción estándar a WildFire.

La protección basada en aprendizaje automático en línea también se puede habilitar para detectar URL maliciosas en tiempo real como parte de su configuración de filtrado de URL.

El aprendizaje automático en línea de Advanced WildFire no es compatible en el dispositivo virtual VM-50 o VM50L.

 ©2025 Palo Alto Networks, Inc.

Veredictos

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

Cuando Advanced WildFire analiza una muestra desconocida previamente en una de las nubes públicas de Advanced WildFire alojada en Palo Alto Networks o en una nube privada de WildFire alojada a nivel local, se produce un veredicto para identificar las muestras como malintencionadas, indeseadas (el grayware se considera intrusivo, pero no malintencionado), phishing o benignas:

- **Benigno**: la muestra es segura y no da signos de comportamiento malicioso.
- **Grayware**: La muestra clasificada como grayware no supone una amenaza de seguridad directa, pero puede mostrar un comportamiento agresivo de algún tipo. Grayware normalmente incluye adware, spyware y objetos de ayuda del explorador (BHO).
- **Phishing:** el enlace dirige a los usuarios a un sitio de phishing y representa una amenaza de seguridad. Los sitios de phishing son sitios que los atacantes disfrazan de sitios web legítimos con el objetivo de robar información del usuario, especialmente, las contraseñas corporativas que proporcionan acceso a su red. El dispositivo WildFire no admite el veredicto de phishing y continúa clasificando este tipo de enlaces como malintencionados.
- **Malintencionado:** la muestra es malware y plantea una amenaza de seguridad. El malware puede incluir virus, gusanos, troyanos, herramientas de acceso remoto (RAT), rootkits y botnets. Para los archivos que se identifican como malware, se generan y distribuyen firmas para evitar una futura exposición a la amenaza.

Cada nube de Advanced WildFire —global (EE. UU.) y regional, y la nube privada WildFire— analiza muestras y genera veredictos de WildFire independientemente de las otras opciones de nube de WildFire. A excepción de los veredictos de la nube privada de WildFire, los veredictos se comparten de manera global, lo que le permite a los usuarios de Advanced WildFire acceder a una base de datos mundial de datos de amenazas.

Los veredictos que sospecha que son falsos positivos o falsos negativos pueden enviarse al equipo de amenazas de Palo Alto Networks para un análisis adicional. Además, puede cambiar manualmente los veredictos de las muestras enviadas a los dispositivos WildFire.

©2025 Palo Alto Networks, Inc.

Análisis de archivos

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

Un cortafuegos de Palo Alto Networks configurado con un perfil de análisis de WildFire reenvía muestras para el análisis de Advanced WildFire según el tipo de archivo (incluso enlaces de correo electrónico). Además, el cortafuegos descodifica archivos que se han codificado o comprimido hasta cuatro veces (por ejemplo, en formato ZIP); si el archivo descodificado coincide con los criterios del perfil de Advanced WildFire Analysis, el cortafuegos envía el archivo descodificado para su análisis.

Las capacidades de análisis de Advanced WildFire también se pueden habilitar en el cortafuegos para proporcionar protección antivirus en línea. La opción de Advanced WildFire Inline ML (Aprendizaje automático en línea de Advanced WildFire) presente en los perfiles de antivirus permite que el plano de datos del cortafuegos aplique análisis de aprendizaje automático en tiempo real en archivos PE y ELF, además de scripts de PowerShell. Cada modelo de aprendizaje automático en línea detecta dinámicamente archivos maliciosos de un tipo específico mediante la evaluación de los detalles del archivo, incluidos los campos y patrones del descodificador, para formular una clasificación de alta probabilidad de un archivo. Esta protección se extiende a variantes de amenazas actualmente desconocidas y futuras que coinciden con características que Palo Alto Networks ha identificado como maliciosas. Para mantenerse al día con los últimos cambios en el panorama de las amenazas, se añaden o actualizan modelos de aprendizaje automático en línea a través de lanzamientos de contenido. Consulte Aprendizaje automático en línea de Advanced WildFire para obtener más información.

La nube de Advanced WildFire también permite analizar ciertos tipos de archivos que se utilizan como cargas secundarias como parte de los paquetes de malware de varias etapas PE, APK y ELF. El análisis de cargas secundarias puede proporcionar cobertura adicional para interrumpir ataques sofisticados perpetrados por amenazas avanzadas. Estas amenazas avanzadas operan mediante la ejecución de código que activa cargas útiles maliciosas adicionales, incluidas las diseñadas para ayudar a eludir las medidas de seguridad y facilitar la proliferación de la carga útil principal. Advanced WildFire analiza las amenazas de varias etapas mediante su procesamiento en entornos de análisis estáticos y dinámicos. Los archivos a los que hace referencia el malware de varias etapas se tratan de forma independiente durante el análisis. Como resultado, los veredictos y protecciones se proporcionan en cuanto finalizan para cada archivo. El veredicto general para el archivo de varias etapas se determina en base a una evaluación de amenazas de contenido malicioso que se encuentra en todas las etapas analizadas del ataque. El contenido malicioso detectado durante el análisis del archivo de varias etapas marca inmediatamente el archivo como malicioso.

Las organizaciones con procedimientos de gestión segura de contenido malicioso pueden enviar manualmente muestras protegidas con contraseña mediante formato RAR a través de la API o el portal de WildFire. Cuando la nube de Advanced WildFire reciba una muestra cifrada con la contraseña *infectada* o

 ©2025 Palo Alto Networks, Inc.

con un *virus*, la nube de Advanced WildFire descifrará y analizará el archivo. Podrá ver el veredicto y los resultados del análisis del archivo en el formato en el que se recibió, en este caso, un archivo.

Mientras que el cortafuegos puede reenviar todos los tipos de archivos que se muestran a continuación, la compatibilidad del análisis de Advanced WildFire varía según la nube de Advanced WildFire a la que envíe las muestras. Revise la Compatibilidad con tipos de archivos de Advanced WildFire para obtener más información.

Tipos de archivos compatibles para el reenvío de WildFire	Description (Descripción)
`apk`	Archivos de paquete de aplicaciones Android (APK) *Los archivos DEX dentro de los archivos APK se analizan como parte del análisis de los archivos APK.*
`flash`	Los applets de Adobe Flash y el contenido de Flash insertado en páginas web.
`jar`	Applets de Java (Tipos de archivo JAR/Class).
`ms-office`	Archivos de Microsoft Office, que incluye documentos (DOC, DOCX, RTF), libros (XLS, XLSX) y presentaciones de PowerPoint (PPT, PPTX), además de documentos Office Open XML (OOXML) 2007+. Los archivos de consulta de Internet (IQY) y enlace simbólico (SLK) son compatibles con la versión de contenido 8462.
`pe`	Archivos ejecutables portables (Portable executable, PE). Los PE incluyen archivos ejecutables, código de objeto, DLL, FON (fuentes) y archivos LNK. Los archivos MSI son compatibles con la versión de contenido 8462. No se requiere una suscripción para el reenvío de los tipos de archivos PE a WildFire para su análisis, pero sí se requiere para todos los demás tipos de archivos admitidos.
`pdf`	Archivos con formato de documento portable (Portable document format, PDF).
`MacOSX`	Varios tipos de archivos utilizados por la plataforma macOS. El análisis estático de archivos DMG, PKG y ZBundle solo está disponible en las regiones de nube global (EE. UU.) y europea de Advanced WildFire; sin embargo, el análisis estático de otros archivos de Mac OS X (fat y macho) es compatible en todas las nubes regionales. El análisis dinámico de todos los archivos de MacOSX solo se admite en las regiones de nube

 ©2025 Palo Alto Networks, Inc.

Tipos de archivos compatibles para el reenvío de WildFire	Description (Descripción)
	global (EE. UU.) y europea de Advanced WildFire. Para obtener más información, consulte Soporte de tipo de archivo
`email-link`	En HTTP/HTTPS incluidos en mensajes de correo electrónico SMTP y POP3. Consulte Análisis de enlaces de correo electrónico.
`archive`	Archivos de almacenamiento Roshal Archive (RAR) and 7-Zip (7z). Los archivos multivolumen que se dividen en varios archivos más pequeños no se pueden enviar para el análisis. La nube de Advanced WildFire solo descifra y analiza los archivos RAR cifrados con la contraseña *infectada* o con un *virus*. *Si bien el cortafuegos es capaz de reenviar archivos compatibles que se encuentran en archivos ZIP después de decodificarse, no puede reenviar archivos ZIP completos en su estado codificado. Si desea enviar archivos ZIP completos, puede cargar de forma manual un archivo ZIP mediante el portal de WildFire o la API de WildFire.*
`Linux`	Archivos de formato ejecutable (Executable and Linkable Format, ELF).
`script`	Varios archivos de script. • Los archivos Jscript (JS), VBScript (VBS) y PowerShell Script (PS1) son compatibles con la versión de contenido 8101. • Los lotes (BAT) son compatibles con la versión de contenido 8168. • La aplicación HTML (HTA) es compatible con la versión de contenido 8229.

Análisis de enlaces de correo electrónico

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

©2025 Palo Alto Networks, Inc.

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	

Un cortafuegos de Palo Alto Networks puede extraer enlaces HTTP/HTTPS incluidos en mensajes de correo electrónico SMTP y POP3, y enviar los enlaces para su análisis en WildFire. El cortafuegos solo extrae enlaces e información de sesión asociada (remitente, destinatario y asunto) de los mensajes de correo electrónico; no recibe, almacena, reenvía ni ve el mensaje de correo electrónico.

WildFire visita los enlaces enviados para determinar si la página web correspondiente contiene exploits o muestra actividad de phishing. Un enlace que WildFire considera malintencionado o de phishing es:

- Registrado en el cortafuegos como entrada de log de WildFire Submissions. El informe de análisis de WildFire que detalla el comportamiento y la actividad observada para el enlace está disponible para entrada de log de WildFire Submissions. La entrada de log incluye la información del encabezado de correo electrónico (remitente, destinatario y asunto de correo electrónico) de manera que pueda identificar el mensaje y eliminarlo del servidor de correo, o mitigar la amenaza si el correo electrónico ya se envió o abrió.
- Se añade a PAN-DB la URL que se considera malware.

El cortafuegos envía los enlaces de correo electrónico a WildFire en lotes de 100 enlaces de correo electrónico o cada dos minutos (según qué límite se alcance primero). Cada carga por lotes a WildFire cuenta como una carga para la capacidad de carga por minuto del cortafuegos específico. Capacidad de reenvío de archivos del cortafuegos según el modelo. Si un enlace incluido en un correo electrónico corresponde a una descarga de archivo en lugar de una URL, el cortafuegos reenvía el archivo únicamente si el tipo de archivo correspondiente está habilitado para el análisis de WildFire.

Para permitir que el cortafuegos reenvíe enlaces incluidos en correos electrónicos para el análisis de WildFire, consulte Reenviar archivos para Advanced WildFire Analysis. Con la licencia de filtrado avanzado de URL, también puede bloquear el acceso de los usuarios a los sitios malintencionados y de phishing.

Análisis de URL

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

 ©2025 Palo Alto Networks, Inc.

La nube global de Advanced WildFire (EE. UU.) y las nubes regionales pueden analizar URL y, por extensión, enlaces de correo electrónico para proporcionar veredictos e informes estandarizados a través de la API de WildFire. Advanced WildFire puede generar un veredicto más preciso y proporcionar datos de análisis de URL coherentes gracias a la adición de detalles del análisis de amenazas de todos los servicios de Palo Alto Networks, incluido PAN-DB.

Los analizadores de URL que operan en la nube global de Advanced WildFire procesan feeds de URL, fuentes de URL correlacionadas (como enlaces de correo electrónico), listas de NRD (dominio recién registrado), contenido de PAN-DB y URL cargadas de forma manual para proporcionar a todas las nubes de Advanced WildFire las capacidades mejoradas sin afectar el cumplimiento normativo de GDPR. Una vez que se haya procesado una URL, puede recuperar el informe de análisis de URL, que incluye el veredicto, los motivos de detección con pruebas, capturas de pantalla y datos de análisis generados para la solicitud web. También puede recuperar artefactos de páginas web (capturas de pantalla y archivos descargados) visualizados durante el análisis de URL para investigar más a fondo la actividad anómala.

No es necesaria ninguna configuración adicional para aprovechar esta función; sin embargo, si desea enviar automáticamente enlaces de correo electrónico para su análisis (que ahora se analizan a través de este servicio), debe Reenviar archivos para Advanced WildFire Analysis.

Los veredictos que sospecha que son falsos positivos o falsos negativos pueden enviarse al equipo de amenazas de Palo Alto Networks para un análisis adicional.

Análisis de archivos comprimidos y codificados

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

Por defecto, el cortafuego descodifica los archivos codificados o comprimidos hasta cuatro veces, incluidos los archivos que se han comprimido en formato ZIP. A continuación, el cortafuegos inspecciona y aplica la política en el archivo descodificado; si el archivo es desconocido, el cortafuegos envía el archivo descodificado para el análisis de WildFire. Si bien el cortafuegos no puede reenviar archivos ZIP completos para el análisis de Advanced WildFire, usted puede enviar archivos directamente a la nube pública de Advanced WildFire mediante el portal de WildFire o la API de WildFire.

El cortafuegos no decodifica los archivos de almacenamiento RAR y 7-Zip. Todo el procesamiento de estos archivos se produce en la nube pública de Advanced WildFire.

 ©2025 Palo Alto Networks, Inc.

Firmas avanzadas de WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

Advanced WildFire permite detectar malware de día cero en el tráfico web (HTTP/HTTPS), los protocolos de correo electrónico (SMTP, IMAP y POP) y el tráfico FTP, y permite generar firmas rápidamente como método de protección frente a futuras infecciones por el malware detectado. Advanced WildFire genera automáticamente una firma basada en la carga útil de malware de la muestra y comprueba su precisión y seguridad.

Cada nube de Advanced WildFire analiza muestras y genera firmas de malware independientemente de las otras nubes de Advanced WildFire. A excepción de las firmas de la nube privada de WildFire, las firmas de Advanced WildFire se comparten globalmente, lo que le permite a los usuarios en todo el mundo beneficiarse de la cobertura de malware independientemente de la ubicación donde se detectó por primera vez el malware. Dado que el malware evoluciona rápidamente, las firmas que genera Advanced WildFire cubren diversas variantes de dicho malware.

Los cortafuegos con una licencia de Advanced WildFire activa pueden recuperar las últimas firmas de Advanced WildFire en tiempo real en cuanto estén disponibles. Si no tiene una suscripción a Advanced WildFire, las firmas estarán disponibles en un plazo de 24-48 horas como parte de la actualización de antivirus de los cortafuegos con una licencia de Threat Prevention activa.

En cuanto el cortafuegos descarga e instala la nueva firma, bloquea todos los archivos que contienen el malware (o una variante de este). Las firmas de malware no detectan enlaces malintencionados y de phishing; para forzar estos enlaces, debe tener una licencia de filtrado de URL PAN-DB. De este modo, podrá bloquear el acceso de los usuarios a sitios malintencionados y de phishing.

©2025 Palo Alto Networks, Inc.

Implementaciones avanzadas de WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

Puede configurar un cortafuegos de Palo Alto Networks para enviar muestras desconocidas a una de las nubes públicas de Advanced WildFire alojadas en Palo Alto Networks, la nube gubernamental estadounidense, una nube privada de WildFire alojada a nivel local, o puede habilitar el cortafuegos para que reenvíe ciertas muestras a una de las opciones de nube pública de Advanced WildFire y determinadas muestras a una nube privada de WildFire:

- Nube pública de Advanced WildFire
- Nube privada de WildFire
- Nube híbrida de WildFire
- WildFire: EE. UU. WildFire en EE. UU.

Nube pública de Advanced WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

Un cortafuegos de Palo Alto Networks puede reenviar archivos y enlaces de correo electrónico desconocidos a la nube global de Advanced WildFire (EE. UU.) o a una de las nubes regionales de Advanced WildFire que Palo Alto Networks posee y mantiene. Seleccione la nube pública de Advanced WildFire que desea que envíe muestras para el análisis según su ubicación y las necesidades de su organización:

©2025 Palo Alto Networks, Inc.

- **Nube global de Advanced WildFire (EE. UU.)**

  La nube global de Advanced WildFire (EE. UU.) es un entorno de nube pública alojado en Estados Unidos.

  Utilice la siguiente URL para enviar archivos a la nube global de Advanced WildFire (EE. UU) para su análisis y acceder al portal global de Advanced WildFire (EE. UU): wildfire.paloaltonetworks.com.

- **Nube de Advanced WildFire de Europa**

  La nube de Europa de WildFire es un entorno de nube pública regional alojado en Holanda. Se diseña para respetar las regulaciones de privacidad de datos de la Unión europea (EU) y las muestras que se envían a la nube de Europa de WildFire permanecen dentro de los límites de la EU.

  Utilice la siguiente URL para enviar archivos a la nube de WildFire de Europa para el análisis y para acceder al portal de Advanced WildFire de Europa: eu.wildfire.paloaltonetworks.com.

- **Nube de Advanced WildFire de Japón**

  La nube de Japón de Advanced WildFire es un entorno de nube pública regional alojado en Japón.

  Utilice la siguiente URL para enviar archivos a la nube de Advanced WildFire de Japón para su análisis y acceder al portal de Advanced WildFire Japón: jp.wildfire.paloaltonetworks.com.

- **Nube de Advanced WildFire de Singapur**

  La nube de Singapur de Advanced WildFire es un entorno de nube pública regional alojado en Singapur.

  Utilice la siguiente URL para enviar archivos a la nube de Advanced WildFire de Singapur para su análisis y para acceder al portal de la nube de Advanced WildFire Singapur: sg.wildfire.paloaltonetworks.com.

- **Nube de Advanced WildFire de Reino Unido**

  La nube de Reino Unido de Advanced WildFire es un entorno de nube pública regional alojado en el Reino Unido.

  Utilice la siguiente URL para enviar archivos a la nube de Advanced WildFire de Reino Unido para su análisis y para acceder al portal de Advanced WildFire Reino Unido: uk.wildfire.paloaltonetworks.com.

- **Nube de Advanced WildFire de Canadá**

  La nube de WildFire de Canadá es un entorno de nube pública regional alojado en Canadá.

  Utilice la siguiente URL para enviar archivos a la nube de Advanced WildFire de Canadá para su análisis y para acceder al portal de Advanced WildFire Canadá: ca.wildfire.paloaltonetworks.com.

- **Nube de Advanced WildFire de Australia**

  La nube de Australia de WildFire es un entorno de nube pública regional alojado en Australia.

  Utilice la siguiente URL para enviar archivos a la nube de Advanced WildFire de Australia para su análisis y para acceder al portal de Advanced WildFire Australia: au.wildfire.paloaltonetworks.com.

- **Nube de Advanced WildFire de Alemania**

  La nube de Alemania de Advanced WildFire es un entorno de nube pública regional alojado en Alemania.

  Utilice la siguiente URL para enviar archivos a la nube de Advanced WildFire de Alemania para su análisis y para acceder al portal de Advanced WildFire Alemania: de.wildfire.paloaltonetworks.com.

 ©2025 Palo Alto Networks, Inc.

- **Nube de Advanced WildFire de India**

  La nube de India de Advanced WildFire es un entorno de nube pública regional alojado en la India.

  Utilice la siguiente URL para enviar archivos a la nube de Advanced WildFire de India para su análisis y para acceder al portal de Advanced WildFire India: in.wildfire.paloaltonetworks.com.
- **Nube de Advanced WildFire de Suiza**

  La nube de Advanced WildFire de Suiza es un entorno de nube pública regional alojado en Suiza.

  Utilice la siguiente URL para enviar archivos a la nube de Advanced WildFire de Suiza para su análisis y para acceder al portal en la nube de Advanced WildFire Suiza: ch.wildfire.paloaltonetworks.com.
- **Nube de Advanced WildFire de Polonia**

  La nube de Advanced WildFire de Polonia es un entorno de nube pública regional alojado en Polonia.

  Utilice la siguiente URL para enviar archivos a la nube de Advanced WildFire de Polonia para su análisis y para acceder al portal de la nube de Advanced WildFire Polonia: pl.wildfire.paloaltonetworks.com.
- **Nube de Advanced WildFire de Indonesia**

  La nube de Advanced WildFire de Indonesia es un entorno de nube pública regional alojado en Indonesia.

  Utilice la siguiente URL para enviar archivos a la nube de Advanced WildFire de Indonesia para su análisis y para acceder al portal de Advanced WildFire Indonesia: id.wildfire.paloaltonetworks.com.
- **Nube de Advanced WildFire de Taiwán**

  La nube de Advanced WildFire de Taiwán es un entorno de nube pública regional alojado en Taiwán.

  Utilice la siguiente URL para enviar archivos a la nube de Advanced WildFire de Taiwán para su análisis y para acceder al portal de Advanced WildFire Taiwán: tw.wildfire.paloaltonetworks.com.
- **Nube de Advanced WildFire de Francia**

  La nube de Advanced WildFire de Francia es un entorno de nube pública regional alojado en Francia.

  Utilice la siguiente URL para enviar archivos a la nube de Advanced WildFire de Francia para su análisis y para acceder al portal de Advanced WildFire Francia: fr.wildfire.paloaltonetworks.com.
- **Nube de Advanced WildFire de Catar**

  La nube de Advanced WildFire de Catar es un entorno de nube pública regional alojado en Catar.

  Utilice la siguiente URL para enviar archivos a la nube de Advanced WildFire de Catar para su análisis y para acceder al portal en la nube de Advanced WildFire Catar: qatar.wildfire.paloaltonetworks.com.
- **Nube de Advanced WildFire de Corea del Sur**

  La nube de Advanced WildFire de Corea del Sur es un entorno de nube pública regional alojado en Corea del Sur.

  Utilice la siguiente URL para enviar archivos a la nube de Advanced WildFire de Corea del Sur para su análisis y para acceder al portal de Advanced WildFire Corea del Sur: kr.wildfire.paloaltonetworks.com.

 ©2025 Palo Alto Networks, Inc.

- **Nube de Advanced WildFire de Israel**

  La nube de Advanced WildFire de Israel es un entorno de nube pública regional alojado en Israel.

  Utilice la siguiente URL para enviar archivos a la nube de Advanced WildFire de Israel para su análisis y para acceder al portal de Advanced WildFire Israel: il.wildfire.paloaltonetworks.com.
- **Nube de Advanced WildFire de Arabia Saudita**

  La nube de Advanced WildFire de Arabia Saudita es un entorno de nube pública regional alojado en Arabia Saudita.

  Utilice la siguiente URL para enviar archivos a la nube de Advanced WildFire de Arabia Saudita para su análisis y para acceder al portal de Advanced WildFire Arabia Saudita: sa.wildfire.paloaltonetworks.com.
- **Nube de Advanced WildFire España**

  La nube de Advanced WildFire de España es un entorno de nube pública regional alojado en España.

  Utilice la siguiente URL para enviar archivos a la nube de Advanced WildFire de España para su análisis y acceder al portal de Advanced WildFire España: es.wildfire.paloaltonetworks.com.

Cada nube de Advanced WildFire global (EE. UU) y regional analiza las muestras y genera firmas de malware y veredictos independientemente de las otras nubes de WildFire. Las firmas y los veredictos de Advanced WildFire se comparten globalmente, lo que le permite a los usuarios de WildFire en todo el mundo beneficiarse de la cobertura de malware independientemente de la ubicación donde se detectó por primera vez el malware. Revise Compatibilidad de los tipos de archivos de Advanced WildFire para obtener más información sobre los tipos de archivos que analiza cada nube.

Si tiene un dispositivo WildFire, puede habilitar una implementación de nube híbrida de WildFire donde el cortafuegos puede reenviar determinados archivos a una nube pública de WildFire y otros archivos a una nube privada de WildFire para el análisis local. El dispositivo WildFire también puede configurarse a fin de que recoja veredictos con rapidez para muestras conocidas al consultar a la nube pública antes de realizar el análisis. Esto le permite al dispositivo WildFire dedicar recursos de análisis a las muestras que son desconocidas para su red privada y para la comunidad global de WildFire.

Nube privada de WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	☐ Licencia de Advanced WildFire o WildFire

En una implementación de nube privada de Palo Alto Networks, los cortafuegos de Palo Alto Networks reenvían archivos a un dispositivo WildFire de su red corporativa que se utiliza para alojar una ubicación de análisis de nube privada.

Para obtener más información sobre el reenvío de nube híbrida, consulte la Guía del administrador del dispositivo WildFire.

©2025 Palo Alto Networks, Inc.

Nube híbrida de WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia de Advanced WildFire o WildFire

Un cortafuegos en una implementación de nube híbrida de WildFire puede reenviar ciertas muestras a las nubes públicas de WildFire alojadas en Palo Alto Networks y otras muestras a una nube privada de WildFire alojada en un dispositivo WildFire.

Para obtener más información sobre el reenvío de nube híbrida, consulte la Guía del administrador del dispositivo WildFire.

Plataformas en la nube autorizadas por FedRAMP de WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.* ❑ Complemento de FedRAMP para Advanced WildFire

Además de las opciones de implementación de nube global de WildFire, nube privada y nube híbrida de WildFire, Palo Alto Networks también brinda acceso a varios entornos de nube de alta seguridad autorizados por FedRAMP para organizaciones que necesitan cumplir con estándares operativos de nube segura. Las nubes autorizadas por FedRAMP están disponibles en dos niveles de impacto: Alto y moderado, estando el nivel moderado disponible en dos configuraciones de nube. La nube gubernamental de Advanced WildFire cumple con el alto estándar de certificación FedRAMP, mientras que la nube gubernamental de Advanced WildFire y nube gubernamental de Advanced WildFire EE. UU. cumple con el estándar de certificación moderada FedRAMP.

La nube gubernamental de WildFire EE. UU. (que cumple con los estándares de certificación moderada de FedRAMP) está prevista para su desactivación. Para todos los clientes nuevos, Palo Alto Networks recomienda utilizar la nube para el sector público de Advanced WildFire, que tiene un conjunto de funciones mejorado y soporte para la nube de Advanced WildFire.

Las nubes moderadas de FedRAMP (Advanced WildFire para la nube gubernamental y la nube gubernamental de WildFire EE. UU.) están generalmente disponibles para los clientes de Palo Alto Networks; sin embargo, la nube gubernamental de Advanced WildFire, que cumple con los altos

 ©2025 Palo Alto Networks, Inc.

estándares de certificación de FedRAMP, solo está disponible para clientes federales, del Departamento de Defensa o de la Base Industrial de Defensa Aprobada (DIB).

Debido a la naturaleza sensible de estos servicios, las nubes de FedRAMP tienen un proceso de incorporación específico que difiere del de otros servicios. Para obtener más información, consulte el tipo de nube FedRAMP específico:

- Nube gubernamental de Advanced WildFire
- Nube para el sector público de Advanced WildFire
- WildFire: EE. UU. WildFire en EE. UU.

Las nubes FedRAMP mencionadas anteriormente no se pueden combinar en el mismo dispositivo, ni se pueden usar simultáneamente con las nubes globales o regionales de Advanced WildFire. Sin embargo, cualquier nube de FedRAMP se puede utilizar en cooperación con otros servicios de seguridad basados en la nube (por ejemplo, Advanced Threat Prevention, DLP, etc.). Si necesita incorporar múltiples niveles de seguridad de FedRAMP en un solo dispositivo, debe utilizar identificaciones de cuenta separadas. Una vez completada la incorporación, puede hacer referencia a la URL de la nube FedRAMP en su perfil de seguridad antivirus y API de la misma manera que en cualquier otra nube Advanced WildFire.

Nube gubernamental de Advanced WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.* ❑ Complemento de GovCloud de Advanced WildFire

Palo Alto Networks ofrece a los clientes del gobierno federal, del Departamento de Defensa o de la Base Industrial de Defensa Aprobada (DIB), Advanced WildFire Government Cloud; una plataforma de análisis de malware de alta seguridad que cumple con los altos estándares de certificación FedRAMP (Federal Risk and Authorization Management Program).

La nube del sector público de Advanced WildFire funciona como una entidad independiente y distinta de las regiones comerciales o de la nube gubernamental: cualquier información de privacidad que pueda estar presente en muestras enviadas para su análisis, como direcciones de correo electrónico, direcciones IP y DNS pasivo, no se compartirá con ninguna otra instancia de la nube de WildFire. Sin embargo, puede seguir aprovechando los datos de amenazas generados por las nubes públicas de Advanced WildFire para maximizar la capacidad de cobertura, así como las protecciones y firmas antivirus producidas a través del análisis de archivos.

Para obtener información más detallada sobre las autorizaciones FedRAMP de Advanced WildFire de Palo Alto Network, visite: FedRAMP.gov

 ©2025 Palo Alto Networks, Inc.

Para obtener información más detallada sobre la autorización FedRAMP de WildFire de Palo Alto Network, visite: Palo Alto Networks Government Cloud Services (Servicios en la nube gubernamental de Palo Alto Networks) - WildFire.

La nube gubernamental de Advanced WildFire tiene varias diferencias funcionales con respecto a las nubes públicas de Advanced WildFire comerciales estándar. La siguiente funcionalidad no está disponible para los clientes que se conectan a las nubes gubernamentales de Advanced WildFire:

- El análisis de hardware no es compatible con Advanced WildFire U.S. Regiones de nubes gubernamentales
- No se puede acceder a la nube gubernamental de Advanced WildFire a través del portal WildFire.
- El derecho a eliminar funcionalidades no está disponible sin una solicitud de servicio.

Introducción a la nube gubernamental de Advanced WildFire

Siga las medidas de procedimiento interno para determinar la idoneidad del uso de Advanced WildFire EE. UU. Nube gubernamental dentro de su red, como, entre otras, la realización de un análisis de riesgos, una evaluación del paquete de presentación de CSP y las aprobaciones de autorización. Póngase en contacto con su representante de ventas de Palo Alto Networks / Advanced WildFire: EE. UU. para analizar cualquier detalle sobre funcionamiento adicional.

El acceso a las regiones de la nube gubernamental de Advanced WildFire EE. UU. comienza cuando cumple con los requisitos de organización adecuados para utilizar un servicio con autorización FedRAMP.

Póngase en contacto con el equipo de cuentas de Palo Alto Networks para iniciar el proceso de incorporación. Después de completar la activación de Advanced WildFire, reconfigure el cortafuegos para reenviar archivos desconocidos y enlaces de correo electrónico para su análisis utilizando la siguiente URL: gov-cloud.wildfire.paloaltonetworks.com. Para obtener más información, consulte Reenvío de archivos para el análisis de WildFire. Si necesita asistencia adicional, póngase en contacto con el servicio de atención al cliente de Palo Alto Networks.

Nube para el sector público de Advanced WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.* ❑ Complemento PubSec para Advanced WildFire

Palo Alto Networks ofrece a los clientes la Nube para el sector público de Advanced WildFire, una plataforma de análisis de malware de alta seguridad que cumple con los estándares de certificación moderados de FedRAMP (Programa Federal de Gestión de Riesgos y Autorizaciones). La nube para el sector público de Advanced WildFire reemplaza a la Nube de WildFire EE. UU. Nube gubernamental.

 ©2025 Palo Alto Networks, Inc.

La nube del sector público de Advanced WildFire funciona como una entidad independiente y distinta de las regiones comerciales o de la nube gubernamental: cualquier información de privacidad que pueda estar presente en muestras enviadas para su análisis, como direcciones de correo electrónico, direcciones IP y DNS pasivo, no se compartirá con ninguna otra instancia de la nube de WildFire. Sin embargo, puede seguir aprovechando los datos de amenazas generados por las nubes públicas de Advanced WildFire para maximizar la capacidad de cobertura, así como las protecciones y firmas antivirus producidas a través del análisis de archivos.

Para obtener información más detallada sobre las autorizaciones FedRAMP de Advanced WildFire de Palo Alto Network, visite: FedRAMP.gov

La nube para el sector público de Advanced WildFire tiene varias diferencias funcionales con respecto a las nubes públicas comerciales estándar de Advanced WildFire. La siguiente funcionalidad no está disponible para los clientes que se conectan a las nubes para el sector público de Advanced WildFire:

- El análisis de hardware no es compatible con Advanced WildFire U.S. Regiones de la nube gubernamental.
- No se puede acceder a la región de nube para el sector público de Advanced WildFire EE. UU. a través del portal de WildFire.
- El derecho a eliminar funcionalidades no está disponible sin una solicitud de servicio.

Comience a utilizar la nube para el sector público de Advanced WildFire

Siga las medidas de procedimiento internas para determinar la idoneidad de usar la nube para el sector público de Advanced WildFire dentro de su red, como, entre otros, la realización de un análisis de riesgos, la evaluación del paquete de presentación de CSP y las aprobaciones de autorización. Póngase en contacto con su representante de ventas de Palo Alto Networks / Advanced WildFire: EE. UU. punto de contacto de la nube para el sector público para hablar cualquier detalle operativo adicional.

El acceso a las regiones de la nube para el sector público de Advanced WildFire comienza cuando cumple con los requisitos de organización adecuados para utilizar un servicio con autorización FedRAMP.

Póngase en contacto con el equipo de cuentas de Palo Alto Networks para iniciar el proceso de incorporación. Después de completar la activación de Advanced WildFire, reconfigure el cortafuegos para reenviar archivos desconocidos y enlaces de correo electrónico para su análisis utilizando la siguiente URL: pubsec-cloud.wildfire.paloaltonetworks.com.

Para obtener más información, consulte Reenvío de archivos para el análisis de WildFire. Si necesita asistencia adicional, póngase en contacto con el servicio de atención al cliente de Palo Alto Networks.

WildFire: EE. UU. WildFire en EE. UU.

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.* ❑ Nube gubernamental en EE. UU. Incorporación del gobierno

©2025 Palo Alto Networks, Inc.

¿Dónde puedo usar esto?	¿Qué necesito?
• CN-Series	

A partir del 15 de julio de 2024 la nube gubernamental de EE. UU. de WildFire de Palo Alto Networks ha sido reemplazada por el Nube gubernamental de Advanced WildFire *y* Nube para el sector público de Advanced WildFire*, que proporciona acceso a entornos avanzados de alta seguridad de WildFire Cloud que operan una base de código más reciente con un conjunto de funciones mejoradas. Como resultado, Palo Alto Networks ya no incorpora nuevos clientes a WildFire EE. UU. Nube gubernamental. Los clientes existentes pueden seguir accediendo a la página web de WildFire EE. UU. Nube gubernamental, Government Cloud, hasta la fecha de desmantelamiento del 30 de noviembre de 2024, momento en el que el URI existente se redirigirá a la nube del sector público, Public Sector Cloud, de Advanced WildFire.*

Para obtener más información sobre las nuevas ofertas en la nube, póngase en contacto con su representante de ventas de Palo Alto Networks para analizar cualquier detalle operativo adicional.

La nube gubernamental de EE. UU. de WildFire de Palo Alto Networks es una plataforma de análisis de malware de alta seguridad con autorización FedRAMP (Federal Risk and Authorization Management Program, programa federal de gestión de autorizaciones y riesgos). Este entorno en la nube de WildFire está diseñado para que se utilice únicamente para las agencias federales de EE. UU. que requieren un enfoque estandarizado para la evaluación de seguridad, la autorización y la supervisión continua de productos y servicios en la nube. Wildfire: EE. UU. La nube gubernamental funciona como una entidad independiente y distinta: cualquier información de privacidad que pueda estar presente en muestras enviadas para su análisis, como direcciones de correo electrónico, direcciones IP y DNS pasivo, no se compartirá con ninguna otra instancia de la nube de WildFire. Sin embargo, puede seguir aprovechando los datos de amenazas generados por la nube pública de WildFire para maximizar la capacidad de cobertura, así como las protecciones y firmas antivirus producidas a través del análisis de archivos.

Para obtener información más detallada sobre la autorización FedRAMP de WildFire de Palo Alto Network, visite: Palo Alto Networks Government Cloud Services (Servicios en la nube gubernamental de Palo Alto Networks) - WildFire.

La nube pública de WildFire (las nubes globales y regionales) y la nube gubernamental de EE. UU. de WildFire presentan varias diferencias funcionales con respecto a la nube pública. La siguiente funcionalidad no está disponible para los clientes que se conectan a WildFire: EE. UU. Nube gubernamental:

- El análisis de hardware no es compatible con la nube gubernamental Nube gubernamental.
- El análisis de archivos de script (Bat, JS, BVS, PS1, script de shell y HTA) no es actualmente compatible.
- Wildfire: EE. UU. No es posible acceder a la nube gubernamental a través del portal de WildFire.
- Wildfire: EE. UU. de WildFire con otros servicios basados en la nube.
- La funcionalidad de eliminación directa no está disponible.
- Wildfire: Actualmente, la nube gubernamental de EE. UU. no admite el análisis de Advanced WildFire.

 ©2025 Palo Alto Networks, Inc.

Comenzar con WildFire: EE. UU. WildFire en EE. UU.

Para conectarse a la WildFire: nube gubernamental de EE. UU. , debe solicitar acceso. Siga las medidas de procedimiento interno para determinar la idoneidad del uso de WildFire: nube gubernamental de EE. UU. dentro de su red, como, entre otras, la realización de un análisis de riesgos, una evaluación del paquete de presentación de CSP y las aprobaciones de autorización. Póngase en contacto con su representante de ventas de Palo Alto Networks o con su punto de conectado de WildFire: nube gubernamental de EE. UU. para analizar cualquier detalle sobre funcionamiento adicional.

Las solicitudes para acceder a la nube gubernamental de EE. UU. de WildFire comienzan cuando cumple los requisitos de organización adecuados para utilizar un servicio con autorización FedRAMP. Hay dos categorías de entidades que pueden acceder a WildFire EE. UU. Nube gubernamental: EE. UU. Los contratistas del gobierno y agencias federales de EE. UU. (y otros departamentos gubernamentales aprobados). Ambas entidades tienen requisitos específicos para acceder a WildFire EE. UU. Nube gubernamental:

1. **EE. UU. Agencias Federales**

   EE. UU. La Autoridad de aprobación designada (DAA) otorga a las agencias, departamentos y oficinas federales la operación de la nube gubernamental de WildFire EE. UU. dentro de las operaciones de una agencia, antes de que se otorgue el acceso.

   1. Informe al punto de contacto de Palo Alto Networks (fedramp@paloaltonetworks.com) sobre la intención de utilizar la nube gubernamental de WildFire EE. UU. Nube gubernamental.
   2. Envíe una solicitud a info@fedramp.gov.
   3. Complete el formulario de solicitud de acceso al paquete de FedRAMP y envíelo a info@fedramp.gov.

      La oficina de gestión del programa (Program Management Office, PMO) de FedRAMP revisa el formulario y generalmente emite un acceso temporal de 30 días al paquete de FedRAMP de WildFire.
   4. Revise el paquete de seguridad de FedRAMP para la nube gubernamental Nube gubernamental. Complete todos los procesos internos necesarios para implementar la nube gubernamental de EE. UU. en su organización.
   5. Emita la ATO.
   6. Envíe una solicitud a la PMO de FedRAMP para obtener acceso permanente a WildFire EE. UU. Nube gubernamental.
2. **EE. UU. Contratistas del gobierno de**

   EE. UU. Los contratistas del gobierno que usan o acceden a WildFire EE. UU. La nube gubernamental debe cumplir los siguientes requisitos.

   1. Deben ser ciudadanos de Estados Unidos.
   2. Tener un contrato activo (o subcontrato) con una empresa gubernamental federal de EE. UU. con un requisito ocupacional para el intercambio de información a través de Internet, como la correspondencia por correo electrónico, el intercambio de documentos y otras formas de comunicación por Internet.
   3. Al finalizar el empleo de un contratista, el usuario debe dejar de usar o acceder a WildFire EE. UU. Nube gubernamental.
   4. Deben cumplir las disposiciones de confidencialidad que aparecen en el contrato de licencia de usuario final de Palo Alto Networks.

 ©2025 Palo Alto Networks, Inc.

Después de que su organización emita una Autorización para operar (ATO) o cuando los contratistas del gobierno de EE. UU. cumplen con todos los requisitos de uso, solo entonces se puede hacer una solicitud para acceder a WildFire EE. UU. Para ello, debe ponerse en contacto con su equipo de cuentas de Palo Alto Networks.

1. Póngase en contacto con su oficina de gestión del programa (Program Management Office, PMO) de FedRAMP para determinar la viabilidad de la nube gubernamental de EE. UU. para sus necesidades de seguridad.
2. Póngase en contacto con el punto de contacto de Palo Alto Networks especificado en FedRAMP Marketplace (Mercado de FedRAMP). El punto de contacto proporciona información adicional sobre el servicio, así como cualquier otro detalle operativo relativo a su implementación particular de WildFire.
3. Póngase en contacto con el equipo de cuentas de Palo Alto Networks para iniciar el proceso de incorporación. El equipo de cuentas solicitará la siguiente información con respecto a los detalles del cliente y los detalles de implementación.
   - Información de contacto.
   - Una breve descripción para migrar a la nube gubernamental Nube gubernamental.
   - Una declaración de cumplimiento organizacional con las disposiciones de confidencialidad descritas en el contrato de licencia de usuario final de Palo Alto Networks.
   - Direcciones IP de salida todas las puertas de enlace de puerta de enlace (incluidos los planos de gestión), así como todas las instancias de Panorama.
4. Una vez que la gestión del programa de WildFire conceda la aprobación para usar la nube gubernamental de EE. UU. de WildFire. (generalmente en uno o tres días laborables), las operaciones de desarrollo de redes de Palo Alto aplicarán los controles apropiados.
5. Después de que se garantice el acceso a la nube gubernamental de EE. UU. de WildFire, La nube gubernamental se otorga, vuelva a configurar el cortafuegos para reenviar archivos desconocidos y enlaces de correo electrónico para su análisis mediante la siguiente URL: wildfire.gov.paloaltonetworks.com. Para obtener más información, consulte Reenvío de archivos para el análisis de WildFire. Si necesita asistencia adicional, póngase en contacto con el servicio de atención al cliente de Palo Alto Networks.

 ©2025 Palo Alto Networks, Inc.

Soporte de tipo de archivo

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

En la siguiente tabla, se enumeran los tipos de archivo compatibles para el análisis en los entornos de nube de WildFire.

Para obtener una lista completa de tipos de archivos específicos compatibles con WildFire, consulte Tipos de archivos compatibles (lista completa).

Tipos de archivos compatibles para el análisis	Nube pública avanzada de WildFire (todas las regiones)	Nube gubernamental en EE. UU. WildFire en EE. UU.	Portal de Advanced Wildfire | API (carga directa; todas las regiones)
Los enlaces se encuentran en los correos electrónicos	✓	✓	✓
Archivos de paquete de aplicaciones Android (Android application package, APK)	✓	✓	✓
Archivos de Adobe Flash	✓	✓	✓
Archivos de almacenamiento Java (Java Archive, JAR)	✓	✓	✓
Archivos de Microsoft Office	✓	✓	✓

©2025 Palo Alto Networks, Inc.

Tipos de archivos compatibles para el análisis	Nube pública avanzada de WildFire (todas las regiones)	Nube gubernamental en EE. UU. WildFire en EE. UU.	Portal de Advanced Wildfire | API (carga directa; todas las regiones)
(incluye archivos SLK e IQY)			
Archivos ejecutables portátiles (incluye archivos MSI)	✓	✓	✓
Archivos con formato de documento portable (Portable document format, PDF)	✓	✓	✓
Archivos Mac OS X*	✓	✓	✓
Archivos de Linux (archivos ELF y scripts de Shell)	✓	✓	✓
Archivar archivos (RAR, 7-Zip, ZIP**)	✓	✓	✓
Archivos de script (BAT, JS, VBS, PS1 y HTA)	✓	✗	✓
Scripts de Python	✓	✓	✓
Scripts de Perl	✗	✗	✓
Archivos (ZIP [carga directa] e ISO)	✗	✗	✓
Archivos de imagen (JPG y PNG)	✗	✗	✓

©2025 Palo Alto Networks, Inc.

* El análisis estático de archivos DMG, PKG y ZBundle solo está disponible en las regiones de nube global (EE. UU.) y europea de Advanced WildFire; sin embargo, el análisis estático de otros archivos de Mac OS X (fat y macho) es compatible en todas las nubes regionales. El análisis dinámico de todos los archivos de Mac OS X solo se admite en las regiones de nube global (EE. UU.) y europea de Advanced WildFire.

** Los archivos ZIP no se reenvían directamente a la nube de Advanced Wildfire para su análisis. En su lugar, primero son decodificados por el cortafuegos y los archivos que coinciden con los criterios del perfil de WildFire Analysis se envían por separado para su análisis.

¿Busca más información?

- *Para obtener detalles sobre cada implementación en la nube de Advanced WildFire, consulte* Implementaciones avanzadas de WildFire.
- *Para obtener información detallada sobre cada tipo de archivo compatible con el análisis de WildFire, consulte* Análisis de archivos.

Tipos de archivos compatibles (lista completa)

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

La siguiente tabla enumera los tipos de archivos admitidos por el análisis de WildFire. Para los archivos marcados como Sí en la columna Soporte de reenvío, esto incluye archivos codificados en MIME en tráfico web (HTTP/HTTPS) y protocolos de correo electrónico (SMTP, IMAP, POP).

Tipo de contenido admitido	Ejemplo de extensión	Soporte de reenvío
Archivo 7zip	7z	Sí
Archivo Adobe Flash	swf	Sí
APK de Android	apk	Sí
Android DEX	dex	Sí
lote	bat	Sí
Archivo bzip2	bz	Sí

 ©2025 Palo Alto Networks, Inc.

Tipo de contenido admitido	Ejemplo de extensión	Soporte de reenvío
Valores separados por comas	csv	No
DLL, DLL64	dll	Sí
ELF	elf	Sí
Archivo Gzip	gz	No
Aplicación HTML	hta	Sí
ISO	iso	No
Clase JAVA	clase	Sí
JAVA JAR	jar	Sí
Javascript/JScript	js, jse, wsf	Sí (solo JS)
Joint Photographic Experts Group	jpg	No
Enlace	elink	Sí
Mach-O	macho	Sí
Instalador de aplicaciones macOS	pkg	Sí
Paquete de aplicaciones macOS en archivo ZIP	paquete z	No
Archivo binario universal de macOS	fat	No
imagen de disco de macOS	dmg	Sí
Documento de Microsoft Excel 97 - 2003	xls	Sí
Documento de Microsoft Excel	xlsx	Sí
Documento de Microsoft One Note	one	Sí
Documento de Microsoft PowerPoint 97 - 2003	ppt	Sí

©2025 Palo Alto Networks, Inc.

Tipo de contenido admitido	Ejemplo de extensión	Soporte de reenvío
Documento de Microsoft PowerPoint	pptx	Sí
Archivo de enlace simbólico de Microsoft	slk	Sí
Archivo de consulta web de Microsoft	iqy	Sí
Documento de Microsoft Word 97 - 2003	doc	Sí
Documento de Microsoft Word	docx	Sí
Documento de hoja de cálculo de OpenDocument	ods	No
Documento de texto de OpenDocument	odt	No
PDF	pdf	Sí
PE, PE64	exe	Sí
Secuencia de comandos perl	pl	No
Archivo de gráficos de red portátiles	png	No
PowerShell	ps1	Sí
Secuencia de comandos de Python	py	Sí
Archivo RAR	rar	Sí
RTF	rtf	Sí
Script de shell	sh	Sí
Archivo tar	tar	No
VBScript	vbs, vbe	Sí (solo VBS)
Paquete de instalación de Windows	msi	Sí

©2025 Palo Alto Networks, Inc.

Tipo de contenido admitido	Ejemplo de extensión	Soporte de reenvío
Archivo de enlace de Windows	lnk	Sí
Script de Windows	wsf	No
Archivo Zip	zip	No
Páginas activas del servidor	asp	No
Páginas de servidor activas extendidas	aspx	No
Lenguaje de marcado extensible	xml	No
Lenguaje de marcado de hipertexto	html	No

©2025 Palo Alto Networks, Inc.

Ejemplo avanzado de WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

El siguiente escenario de ejemplo resume el ciclo de vida completo de Advanced WildFire™. En este ejemplo, un representante de ventas de Palo Alto Networks descarga una nueva herramienta de ventas de software que un socio de ventas ha cargado en Dropbox. El socio de ventas cargó sin querer una versión infectada del archivo de instalación de la herramienta de ventas y el representante de ventas descargó después el archivo infectado.

Este ejemplo mostrará cómo un cortafuegos de Palo Alto Networks junto con Advanced WildFire puede detectar malware de día cero descargado por un usuario final incluso cuando el tráfico ya cifrado con SSL. Una vez que Advanced WildFire identifica el malware, se envía un log al cortafuegos y este alerta al administrador, que a continuación se pone en contacto con el usuario para eliminar el malware. Luego, Advanced WildFire genera una nueva firma para el malware, después de lo cual los cortafuegos descargan automáticamente la firma para proteger frente a exposiciones futuras. Aunque algunos sitios web de uso compartido de archivos tienen una función antivirus que comprueba los archivos cuando se cargan, solo pueden proteger contra malware “conocido”.

Este ejemplo utiliza un sitio web que emplea el cifrado SSL En este caso, el cortafuegos cuenta con un descifrado habilitado, que incluye la opción de reenviar contenido descifrado para su análisis.

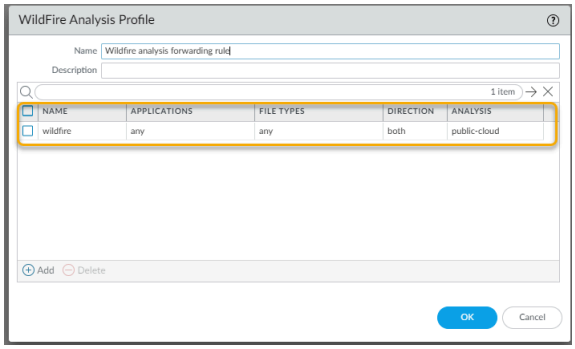
STEP 1 | El representante de ventas de la empresa asociada sube el archivo de una herramienta de ventas denominado sales-tool.exe en su cuenta de Dropbox y, a continuación, envía un mensaje de correo electrónico a la representante de ventas de Palo Alto Networks con un enlace al archivo.

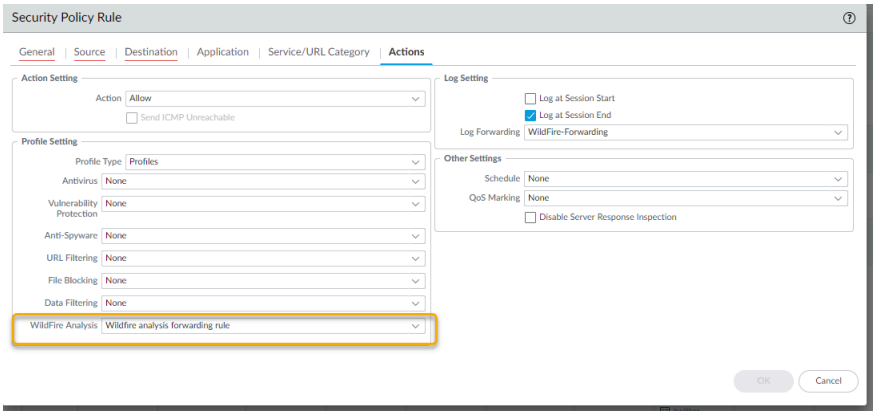
STEP 2 | La representante de ventas de Palo Alto recibe el correo electrónico del socio de ventas y hace clic en el enlace de descarga, que la lleva al sitio de Dropbox. A continuación, hace clic en **Download (Descargar)** para guardar el archivo en su escritorio.

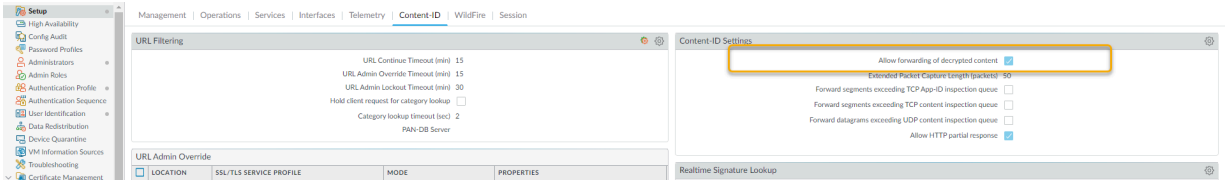
STEP 3 | El cortafuegos que protege a la representante de ventas de Palo Alto tiene una regla de perfil de WildFire Analysis adjunta a una regla de política de seguridad que busca archivos en cualquier aplicación utilizada para descargar o cargar cualquier tipo de archivo compatible. El cortafuegos también puede estar configurado para el reenvío del tipo de archivo de enlace de correo electrónico, que permite al cortafuegos extraer enlaces HTTP/HTTPS contenidos en mensajes de correo electrónico SMTP y POP3. En cuanto la representante de ventas hace clic en Descargar, la política del cortafuegos reenvía el archivo sales-tool.exe a Advanced WildFire, donde el archivo se analiza

 ©2025 Palo Alto Networks, Inc.

para comprobar si hay malware de día cero. Aún cuando la representante de ventas use Dropbox, que tiene cifrado SSL, el cortafuegos está configurado para descifrar tráfico, por lo que todo el tráfico se puede inspeccionar. Las siguientes capturas de pantalla muestran la regla del perfil de WildFire Analysis, la regla de política de seguridad configurada con el perfil de análisis de WildFire y la opción para permitir el reenvío de contenido descifrado.

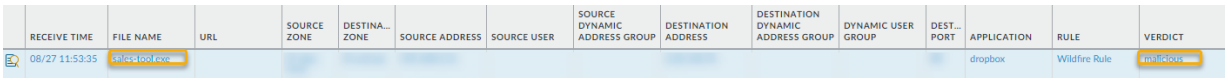






STEP 4 | En este momento, Advanced WildFire ha recibido el archivo y está analizándolo en busca de más de 200 comportamientos malintencionados distintos.

STEP 5 | Una vez que Advanced WildFire ha completado el análisis del archivo, envía un log de Advanced WildFire al cortafuegos con los resultados del análisis. En este ejemplo, el registro muestra que el archivo es malicioso.



 ©2025 Palo Alto Networks, Inc.

STEP 6 | El cortafuegos se configura con un perfil de reenvío de logs que enviará alertas al administrador de seguridad cuando se detecte malware.

NAME	LOCATION	DESCRIPTION	LOG TYPE	FILTER	PANORAMA	SNMP	EMAIL	SYSLOG	HTTP	QUARANTINE	BUILT-IN ACTIONS
WildFire-Forwarding			threat	(severity eq critical)			WildFire-Forwarding				
			wildfire	(category eq benign)	☐						
			wildfire	(category neq benign) and (category neq malicious)			WildFire-Forwarding				
			wildfire	(category eq malicious)	☐		WildFire-Forwarding				

STEP 7 | El administrador de seguridad identificará al usuario por el nombre (si está configurada la ID de usuario) o, en caso contrario, por dirección IP. En este punto, el administrador puede desconectar la red o la conexión de VPN que está usando la representante de ventas y, a continuación, ponerse en contacto con el grupo de asistencia técnica para que ayude al usuario a comprobar y limpiar el sistema.

Al usar el informe de análisis detallado de Advanced WildFire, el técnico del grupo de asistencia técnica puede determinar si el sistema del usuario está infectado con malware examinando los archivos, los procesos y la información de registro detallados en el informe del análisis de Advanced WildFire. Si el usuario ejecuta el malware, el técnico puede intentar limpiar el sistema manualmente o volver a crear una imagen de este.

FILE INFORMATION

File Type	PE
File Signer	
SHA-256	721b79505757ec7831844795afc4e88c23ce57cd4590118895cbfb86bcd34a77
SHA-1	2e8a6dd285f8fa829918aae60cb1b6172d918437
MD5	c67fdb7887368e41469a1a2556ac30df
File Size	55296 bytes
First Seen Timestamp	2016-12-13 18:39:45 UTC
Sample File	Download File
Verdict	Malware

SESSION INFORMATION

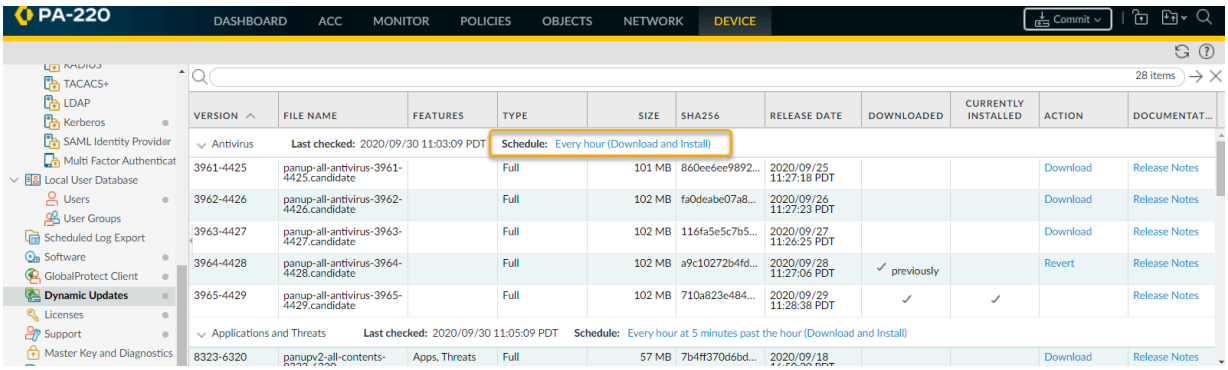
File Source	
File Destination	
User-ID	
Timestamp	2016-12-13 18:39:45 UTC
Serial Number	Manual
Firewall Hostname/IP	
Virtual System	
Application	
URL	
File Name	wildfire-test-pe-file (3).exe
Status	

COVERAGE STATUS

For endpoint antivirus coverage information for this sample, visit VirusTotal

 ©2025 Palo Alto Networks, Inc.

STEP 8 | Una vez que el administrador ha identificado el malware y está comprobando el sistema del usuario, ¿cómo puede protegerse frente a futuras exposiciones? La respuesta: En este ejemplo, el administrador ha definido una programación en el cortafuegos para descargar e instalar firmas de Advanced WildFire cada 15 minutos y para descargar e instalar actualizaciones del antivirus a diario. En menos de una hora y media, la representante de ventas ha descargado el archivo infectado, Advanced WildFire ha identificado el malware de día cero, ha generado una firma, la ha añadido a la base de datos de firmas de actualización de Advanced WildFire proporcionada por Palo Alto Networks y el cortafuegos ha descargado e instalado la nueva firma. Este cortafuegos y cualquier otro cortafuegos de Palo Alto Networks configurado para descargar firmas de Advanced WildFire y de antivirus ahora están protegidos frente a este malware detectado recientemente. La siguiente captura de pantalla muestra el programa de actualización de Advanced WildFire:



Todo esto tiene lugar mucho antes de que la mayoría de los proveedores de antivirus perciban incluso la existencia de software malintencionado de día cero. En este ejemplo, en un plazo muy breve, el malware ya no se considera de día cero porque Palo Alto Networks ya lo ha detectado y ha proporcionado protección a los clientes para evitar exposiciones futuras.

 ©2025 Palo Alto Networks, Inc.

Comience con Advanced WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

Los siguientes pasos proporcionan un flujo de trabajo rápido para comenzar con Advanced WildFire™ en el cortafuegos. Si desea obtener más información sobre Advanced WildFire antes de comenzar, eche un vistazo a la Descripción general de Advanced WildFirey consulte las Prácticas recomendadas de Advanced WildFire.

Para obtener información sobre el uso de la nube privada o la nube híbrida de WildFire, consulte la administración de dispositivo WildFire.

Si está utilizando Advanced WildFire en Prisma Access, familiarícese con el producto antes de configurar su Perfil de seguridad de WildFire Analysis a Reenviar archivos para Advanced WildFire Analysis.

STEP 1 | Obtenga su Suscripción de WildFire o Advanced WildFire. Si no tiene una suscripción, aún podrá reenviar ficheros PE para análisis en WildFire.

STEP 2 | Decida qué Implementaciones avanzadas de WildFire se adapta mejor a sus necesidades:

- Nube pública de Advanced WildFire: se reenvían muestras a una nube pública de Advanced WildFire alojada en Palo Alto Networks.
- Nube gubernamental en EE. UU. WildFire en EE. UU. : se reenvían muestras a una nube gubernamental de WildFire de EE. UU. Nube gubernamental.

Si está implementando una nube privada o híbrida de WildFire, consulte la administración de dispositivos WildFire.

STEP 3 | Confirme que su licencia esté activa en el cortafuegos.

1. Inicie sesión en el cortafuegos.
2. Seleccione **Device (Dispositivo)** > **Licenses (Licencias)** y compruebe que la licencia de WildFire esté activa.

   Si no se muestra la licencia de WildFire, seleccione una de las opciones de Gestión de licencias para activar esta licencia.

©2025 Palo Alto Networks, Inc.

STEP 4 | Conecte el cortafuegos a WildFire y configure el dispositivo.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **WildFire** y modifique la configuración general.
2. Utilice el campo **WildFire Public Cloud (Nube pública de WildFire)** para reenviar muestras a la nube pública de Advanced WildFire.
3. Defina los límites de tamaño para los archivos que el cortafuegos reenvía y realice la configuración de registro e informes de WildFire.

   *Es una Prácticas recomendadas de Advanced WildFire establecer el **File Size (Tamaño de archivo)** para PE al límite máximo de tamaño de 10 MB y dejar el **File Size (Tamaño de archivo)** del resto de los tipos de archivo en el valor predeterminado.*
4. Haga clic en **OK (Aceptar)** para guardar la configuración general de WildFire.

STEP 5 | Habilite el cortafuegos para que envíe tráfico descifrado SSL para el análisis de Advanced WildFire.

Esta es una práctica recomendada de Advanced WildFire recomendada.

STEP 6 | Comience a enviar muestras para su análisis.

1. Defina el tráfico que debe reenviarse para el análisis de WildFire. (Seleccione **Objects [Objetos]** > **Security Profiles [Perfiles de seguridad]** > **WildFire Analysis [Análisis de WildFire]** y, luego, realice las modificaciones o haga clic en **Add [Añadir]** para añadir un perfil de análisis de WildFire).

   *Como práctica recomendada, utilice el perfil predeterminado de análisis para garantizar una cobertura completa del tráfico que permite el cortafuegos. Si aún decide crear un perfil de análisis de WildFire personalizado, configure el perfil para que reenvíe **Any (todos)** los tipos de archivo; esto le permite al cortafuegos comenzar a reenviar automáticamente los tipos de archivos compatibles recientemente para el análisis.*
2. Para cada regla de perfil, establezca **public-cloud** como **Destination (Destino)** para reenviar muestras a la nube de Advanced WildFire para su análisis.
3. Adjunte el perfil de análisis de WildFire a una regla de la política de seguridad. El tráfico que coincide con la regla de la política se reenvía para el análisis de WildFire (**Policies [Políticas]** > **Security [Seguridad]** y haga clic en **Add [Añadir]** o modifique una regla de la política de seguridad).

©2025 Palo Alto Networks, Inc.

STEP 7 | Habilite el cortafuegos para obtener las firmas de Advanced WildFire más recientes.

Las nuevas firmas de Advanced WildFire se recuperan en tiempo real para detectar e identificar malware. Si utiliza PAN-OS 9.1 o una versión anterior, puede recibir nuevas firmas cada cinco minutos.

- PAN-OS 9.1 y versiones anteriores
  1. Seleccione **Device (Dispositivo)** > **Dynamic Updates (Actualizaciones dinámicas)**:
     - Compruebe que se muestren las actualizaciones de **WildFire**.
     - Seleccione **Check Now (Comprobar ahora)** para recuperar los paquetes de actualización de firmas más recientes.
  2. Configure la **Schedule (Programación)** de descarga e instalación de las firmas de Advanced WildFire más recientes.
  3. Utilice el **campo Periodicidad** para establecer la frecuencia con la que el cortafuegos comprueba si hay nuevas actualizaciones de **Cada minuto**.

     Como las nuevas firmas de WildFire están disponibles cada cinco minutos, esta configuración garantiza que el cortafuegos recupere estas firmas dentro de un minuto de disponibilidad.
  4. Habilite el cortafuegos para **Download and Install (Descargar e instalar)** estas actualizaciones según el cortafuegos las recupera.
  5. Haga clic en **OK (Aceptar)**.
- PAN-OS 10.0.x y posterior
  1. Seleccione **Device (Dispositivo)** > **Dynamic Updates (Actualizaciones dinámicas)**:
  2. Compruebe que se muestren las actualizaciones de **WildFire**.
  3. Seleccione Schedule (Programación) para configurar la frecuencia de actualización y, a continuación, use el campo **Recurrence (Recurrencia)** para configurar el cortafuegos para que recupere firmas de WildFire en **tiempo real**.
  4. Haga clic en **OK (Aceptar)**.

STEP 8 | Comience a examinar el tráfico en busca de amenazas, que incluye el malware que identifica Advanced WildFire.

Añada el perfil de antivirus **default (predeterminado)** a una regla de la política de seguridad para examinar el tráfico que permite la regla en función de las firmas de antivirus de WildFire (seleccione **Policies (Políticas)** > **Security (Seguridad)**, y añada o modifique las **Actions (Acciones)** definidas para una regla).

 ©2025 Palo Alto Networks, Inc.

STEP 9 | Controle el acceso a los sitios web donde Advanced WildFire identificó el enlace asociado como malintencionado o phishing.

Esta opción requiere una licencia de filtrado de URL PAN-DB. Obtenga más información sobre el Filtrado de URL y cómo le permite controlar el acceso a los sitios web y los envíos de credenciales corporativas (para evitar los intentos de phishing) según la categoría de URL.

Para configurar el filtrado de URL:

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **URL Filtering (Filtrado de URL)** y **Add (Añadir)** para añadir o modificar un perfil de filtrado de URL.
2. Seleccione **Categories (Categorías)** y defina **Site Access (Acceso a sitios)** para las categorías de URL malintencionadas y de phishing.
3. Haga clic en **Block (Bloquear)** para evitar que los usuarios accedan a sitios en estas categorías o, en cambio, permita el acceso, pero genere una alerta haciendo clic en **Alert (Generar alerta)** cuando los usuarios accedan a sitios en esas categorías para garantizar que tenga visibilidad sobre esos eventos.
4. Habilite la prevención de phishing de credenciales para evitar que los usuarios envíen credenciales a sitios no fiables, sin bloquear su acceso a esos sitios.
5. Aplique el perfil de filtrado de URL nuevo o actualizado, y añádalo a la regla de la política de seguridad para aplicar la configuración del perfil al tráfico permitido:
   1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y **Add (Añadir)** o modifique una regla de política de seguridad.
   2. Seleccione **Actions (Acciones)** y en la sección Profile Settings (Configuración de perfil), configure el **Profile Type (Tipo de perfil)** en Profiles (Perfiles).
   3. Añada el perfil de **URL Filtering (Filtrado de URL)** nuevo o actualizado a la regla de política de seguridad.
   4. Haga clic en **OK (Aceptar)** para guardar la regla de la política de seguridad.

STEP 10 | Confirme que el cortafuegos reenvía muestras con éxito.

- Si ha habilitado el log de archivos benignos, seleccione **Monitor (Supervisar)** > **WildFire Submissions (Envíos de WildFire)** y compruebe que se están registrando las entradas para los archivos benignos enviados para su análisis. (Si desea deshabilitar el registro de archivos benignos tras confirmar que el cortafuegos está conectado a WildFire, seleccione **Device [Dispositivo]** > **Setup [Configuración]** > **WildFire** y borre **Report Benign Files [Informar de archivos benignos]**).
- Otras opciones para permitirle confirmar que el cortafuegos reenvió una muestra específica, ver muestras que el cortafuegos envía según el tipo de archivo y ver el número total de muestras que envía el cortafuegos.
- Test con un archivo de malware de prueba para probar su configuración completa de WildFire.

 ©2025 Palo Alto Networks, Inc.

STEP 11 | Investigar los resultados del análisis.

- Encuentre resultados de análisis:
  - utilice el cortafuegos para supervisar el malware y vea los informes de análisis de WildFire para una muestra.
  - Lleve a cabo la Visualización de informes en el portal de Advanced WildFire para todas las muestras enviadas a la nube pública de Advanced WildFire, incluso las muestras enviadas manualmente a la nube pública de WildFire.
  - Utilice la API de Advanced WildFire para recuperar los veredictos de las muestras y los informes de un dispositivo WildFire.

STEP 12 | Siguiente paso:

Lea e implemente las Prácticas recomendadas de Advanced WildFire.

 ©2025 Palo Alto Networks, Inc.

©2025 Palo Alto Networks, Inc.

Prácticas recomendadas de la implementación de Advanced WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

Los siguientes temas describen implementaciones y configuraciones que Palo Alto Networks recomienda cuando utiliza hardware o servicios de WildFire® como parte de su solución de detección y prevención de amenazas de red.

Prácticas recomendadas de Advanced WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

Usuarios Prisma Access: consulte la documentación de Prisma Access para obtener información específica del producto sobre la interfaz de usuario.

- ❑ Respete las prácticas recomendadas para proteger su red de las evasiones de capa 4 y capa 7, y garantizar una identificación y un análisis fiables del contenido. En especial, asegúrese de implementar las prácticas recomendadas de configuración de TCP (**Device [Dispositivo]** > **Setup [Configuración]** > **Session [Sesión]** > **TCP Settings [Configuración de TCP]**) y los ajustes de Content-ID™ (**Device [Dispositivo]** > **Setup [Configuración]** > **Content-ID** > **Content-ID Settings [Configuración de Content-ID]**).
- ❑ Asegúrese también de tener una suscripción a Threat Prevention activa. En conjunto, Advanced WildFire® y Threat Prevention permiten la detección y prevención de amenazas integral.
- ❑ Descargue e instale las actualizaciones de contenido a diario para recibir las novedades de productos y las protecciones contra amenazas más recientes generadas por Palo Alto Networks. Revise las instrucciones para instalar contenido y actualizaciones de software para obtener más información sobre lo que se incluye en los paquetes de actualización.
- ❑ Si utiliza PAN-OS 10.0 o una versión posterior, configure el cortafuegos para recuperar firmas de Advanced WildFire en tiempo real. Esto proporciona acceso a firmas de malware recién detectadas en cuanto la nube pública de Advanced WildFire pueda generarlas. De esa forma, se evita que los ataques sean fructíferos, ya que se minimiza el tiempo de exposición a actividades maliciosas.
- ❑ Si ha configurado el cortafuegos para descifrar tráfico de SSL, permita que el cortafuegos realice el reenvío de tráfico SSL descifrado para el análisis de WildFire. Solo un superusuario puede habilitar esta opción.
- ❑ Utilice el perfil de WildFire Analysis predeterminado para definir el tráfico que el cortafuegos debe reenviar para su análisis (**Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **WildFire Analysis (Análisis de WildFire)**). El perfil de WildFire Analysis predeterminado garantiza una cobertura completa para todo el tráfico que admite su política de seguridad; especifica que todos

 ©2025 Palo Alto Networks, Inc.

los tipos de archivo compatibles en todas las aplicaciones se reenvíen para el análisis de Advanced WildFire, independientemente de si los archivos se cargaron o descargaron.

Si decide crear un perfil de WildFire Analysis predeterminado, se recomienda establecer el perfil para que reenvíe **any (todos)** los tipos de archivos. Esto le permite al cortafuegos comenzar a reenviar tipos de archivos automáticamente a medida que son compatibles con el análisis.

Para obtener información detallada sobre cómo aplicar un perfil de WildFire Analysis al tráfico del cortafuegos, vea cómo Reenviar archivos para Advanced WildFire Analysis.

La configuración de una acción de WildFire en el perfil de antivirus puede influir en el tráfico si este genera una firma de Advanced WildFire que tenga como resultado una acción de restablecimiento o borrado. Puede excluir el tráfico interno, como aquellas aplicaciones de distribución de software a través de las cuales implementa programas de creación personalizada para realizar una transición segura *a una práctica recomendada, ya que Advanced WildFire puede identificar programas de creación personalizada como maliciosos y generar una firma para ellos. Compruebe* ***Monitor (Supervisar)*** *>* ***Logs*** *>* ***WildFire Submissions (Envíos de WildFire)*** *para ver si algún programa de creación personalizada activa las firmas de Advanced WildFire.*

- Mientras configura el cortafuegos para Reenviar archivos para Advanced WildFire Analysis, revise el **Size Limit (Límite de tamaño)** de archivo para todos los tipos de archivos admitidos. Establezca el **límite de tamaño** para todos los tipos de archivos en el límite predeterminado. (Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **WildFire** y edite la configuración general para ajustar el límite de tamaño según el tipo de archivo. Puede ver la información de ayuda. para encontrar el límite de tamaño predeterminado para cada tipo de archivo).

  Acerca de los límites predeterminados de tamaño de archivos para el reenvío de WildFire

  Los límites de tamaño de archivos predeterminados en el cortafuegos se diseñan para incluir la mayoría del malware en estado salvaje (cuya cantidad es menor a los límites de tamaño predeterminados) y excluir a los archivos grandes que es poco probable que sean malintencionados y que pueden afectar la capacidad de reenvío de archivos de WildFire. Debido a que el cortafuegos tiene una capacidad específica reservada para reenviar archivos para el análisis de Advanced WildFire, reenviar grandes cantidades de archivos grandes podría provocar que el cortafuegos omita el reenvío de algunos archivos. Es posible que esta condición se produzca cuando los límites máximos de tamaño de los archivos se configuran para un tipo de archivo que atraviesa el cortafuegos a una alto velocidad. En este caso, un archivo potencialmente malintencionado podría no reenviarse para el análisis de Advanced WildFire. Considere esta posible condición si desea incrementar el límite de tamaño de archivos diferentes a los PE más allá del límite de tamaño predeterminado.

  El siguiente gráfico es un ejemplo ilustrativo de la distribución de los tamaños de archivos para malware, como lo observa el equipo de investigación de amenazas de Palo Alto Networks. Puede aumentar la configuración de tamaño de archivos predeterminada del cortafuegos al tamaño máximo de

 ©2025 Palo Alto Networks, Inc.

archivos para obtener un incremento relativamente pequeño en la tasa de captura de malware para cada tipo de archivo.

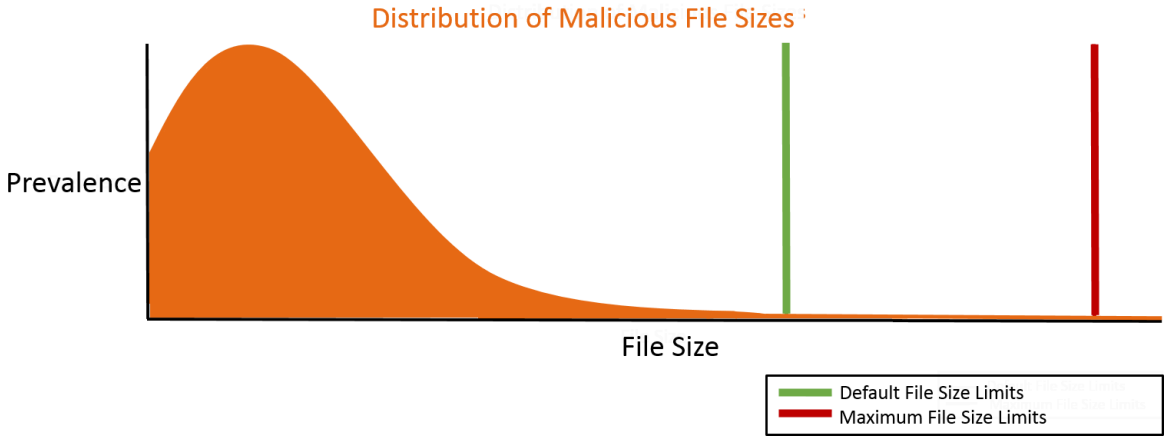


Figure 1: Límites de tamaño de archivos recomendados para capturar archivos malintencionados inusualmente grandes

Si está preocupado específicamente por los archivos malintencionados inusualmente grandes, puede incrementar los límites de tamaño de los archivos más allá de la configuración predeterminada. En estos casos, las siguientes configuraciones se recomiendan para capturar archivos malintencionados raros y muy grandes.

Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **WildFire** y edite la configuración general para ajustar el **límite de tamaño** para cada tipo de archivo:

File Type	Recomendaciones sobre el tamaño máximo de reenvío de archivos para PAN-OS 9.0 y posteriores	Recomendaciones sobre el tamaño máximo de reenvío de archivos para PAN-OS 8.1
pe	16MB	10MB
apk	10MB	10MB
pdf	3,072KB	1000 KB
ms-office	16,384KB	2000 KB
jar	5MB	5MB
flash	5MB	5MB
MacOSX	10MB	1MB
archive	50MB	10MB
Linux	50MB	10MB
script	20KB	20KB

©2025 Palo Alto Networks, Inc.

Configurar Advanced WildFire Analysis

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

Los siguientes temas describen cómo habilitar el análisis de Advanced WildFire™ en su implementación de red. Puede configurar los cortafuegos de Palo Alto Networks para que envíen automáticamente los archivos desconocidos a la nube pública de Advanced WildFire o a una nube privada de WildFire, y también puede enviar manualmente los archivos para el análisis usando el portal de Advanced WildFire. Las muestras enviadas para el análisis reciben un veredicto de benigna, grayware, malware o phishing, y se genera un informe detallado para cada muestra.

- Reenviar archivos para Advanced WildFire Analysis
- Reenviar tráfico SSL descifrado para Advanced WildFire Analysis
- Habilitación del aprendizaje automático en línea de Advanced WildFire
- Habilitar Análisis en línea en la nube para Advanced WildFire
- Habilite el modo de espera para la búsqueda de firma en tiempo real
- Verificación de los envíos de WildFire
- Carga manual de archivos en el portal de WildFire
- Capacidad de reenvío de archivos del cortafuegos según el modelo

Reenviar archivos para Advanced WildFire Analysis

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

Configure el cortafuegos de Palo Alto Networks para reenviar archivos desconocidos o enlaces de correo electrónico y archivos bloqueados que coincidan con las firmas de antivirus existentes para el análisis. Use el perfil de **WildFire Analysis (Análisis de WildFire)** para definir archivos para enviar a una de las opciones de nube pública de Advanced WildFire y luego adjunte el perfil a una regla de seguridad para activar la inspección de malware de día cero.

Especifique el tráfico que debe enviarse para el análisis en función de la aplicación en uso, el tipo de archivo detectado, los enlaces incluidos en los mensajes de correo electrónico o la dirección de la transmisión de la muestra (carga, descarga o ambas). Por ejemplo, puede configurar el cortafuegos para que envíe archivos portables ejecutables (PE) o cualquier archivo que los usuarios intenten descargar durante una sesión de exploración web. Además de las muestras desconocidas, el cortafuegos reenvía los archivos bloqueados que coinciden con las firmas de antivirus existentes. Esto le proporciona a Palo Alto Networks una fuente valiosa de inteligencia de amenazas basada en las variantes de malware que las firmas evitaron correctamente pero que no se habían observado anteriormente.

Si utiliza un dispositivo WildFire para albergar una nube privada de WildFire, puede extender los recursos de análisis de WildFire a una nube híbrida de WildFire configurando el cortafuegos para que continúe reenviando archivos confidenciales a su nube privada de WildFire para el análisis local y reenvíe los tipos de archivo menos confidenciales o no compatibles a la nube pública de WildFire. Para obtener más información sobre el uso y la configuración del dispositivo WildFire, consulte la Administración de dispositivos WildFire.

Antes de comenzar:

- La compatibilidad con el análisis de archivos puede tener pequeñas diferencias entre las regiones de nubes de Advanced WildFire. Para obtener más información, consulte Soporte de tipo de archivo
- Si un cortafuegos reside entre el cortafuegos que está configurando para reenviar los archivos y la nube de Advanced WildFire, asegúrese de que el cortafuegos en medio permita los siguientes puertos:

Puerto	Uso
443	Registro, descargas PCAP, descargas de muestras, recuperación de informes, envío de archivos, descargas de informes en formato PDF

©2025 Palo Alto Networks, Inc.

Puerto	Uso
10443	Actualizaciones dinámicas

- Strata Cloud Manager
- PAN-OS y Panorama

Reenviar archivos para Advanced WildFire Analysis (Cloud Management)

Si está utilizando Panorama para gestionar Prisma Access:

*Desplácese a la pestaña **PAN-OS** y siga las instrucciones que se indican allí.*

Si está utilizando Prisma Access Cloud Management, continúe aquí.

STEP 1 | Especifique la nube de Advanced WildFire a la que desea reenviar muestras.

Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW y (NGFW y Prisma Access** > **Security Services (Servicios de seguridad)** > **WildFire and Antivirus (WildFire y antivirus)** > **General Settings (Configuración general)** y edite la configuración general en función de su implementación en la nube de WildFire (pública, gubernamental, privada o híbrida).

Wildfire en EE. UU. EE. UU. de WildFire solo está disponible para EE. UU. Las agencias federales funcionan como un entorno de análisis opcional.

Añada la URL de **WildFire Cloud (Nube de WildFire)** para que el entorno de nube reenvíe muestras para su análisis.

Opciones avanzadas de la nube pública de WildFire:

1. Introduzca la URL de la **WildFire Public Cloud (nube pública de WildFire)**:
   - Estados Unidos: **`wildfire.paloaltonetworks.com`**
   - Europa: **`eu.wildfire.paloaltonetworks.com`**
   - Japón: **`jp.wildfire.paloaltonetworks.com`**
   - Singapur: **`sg.wildfire.paloaltonetworks.com`**
   - Reino Unido: **`uk.wildfire.paloaltonetworks.com`**
   - Canadá: **`ca.wildfire.paloaltonetworks.com`**
   - Australia: **`au.wildfire.paloaltonetworks.com`**
   - Alemania: **`de.wildfire.paloaltonetworks.com`**
   - India: **`in.wildfire.paloaltonetworks.com`**
   - Suiza: **`ch.wildfire.paloaltonetworks.com`**
   - Polonia: **`pl.wildfire.paloaltonetworks.com`**
   - Indonesia: **`id.wildfire.paloaltonetworks.com`**
   - Taiwán: **`tw.wildfire.paloaltonetworks.com`**

 ©2025 Palo Alto Networks, Inc.

- Francia: **fr.wildfire.paloaltonetworks.com**
- Qatar: **qatar.wildfire.paloaltonetworks.com**
- Corea del Sur: **kr.wildfire.paloaltonetworks.com**
- Israel: **il.wildfire.paloaltonetworks.com**
- Arabia Saudita: **sa.wildfire.paloaltonetworks.com**
- España: **es.wildfire.paloaltonetworks.com**

2. Asegúrese de que el campo de la **WildFire Private Cloud (nube privada de WildFire)** esté vacío.

Opciones de nube de WildFire FedRAMP:

1. Introduzca la URL de **WildFire FedRAMP Cloud (Nube de WildFire FedRAMP)**:
   - EE. UU. Nube gubernamental: **wildfire.gov.paloaltonetworks.com**
   - Nube gubernamental de Advanced WildFire: gov-cloud.wildfire.paloaltonetworks.com
   - Nube para el sector público de Advanced WildFire: pubsec-cloud.wildfire.paloaltonetworks.com
2. Asegúrese de que el campo de la **WildFire Private Cloud (nube privada de WildFire)** esté vacío.

STEP 2 | Habilitar Prisma Access para reenviar el tráfico SSL descifrado para el análisis de Advanced WildFire seleccionando **Allow Forwarding of Decrypted Content (Permitir reenvío de contenido descifrado)**. El tráfico descifrado se evalúa según las reglas de la directiva de seguridad; si coincide con el perfil de análisis de WildFire adjunto a la regla de seguridad, el tráfico descifrado se reenvía para su análisis antes de volver a cifrarse.

El reenvío de tráfico SSL descifrado para el análisis es una práctica recomendada de Advanced WildFire.

STEP 3 | Defina los límites de tamaño para las muestras que Prisma Access reenvía para su análisis.

Es una práctica recomendada de Advanced WildFire establecer los valores de reenvío de archivos en la configuración predeterminada.

STEP 4 | Configurar los ajustes del log de envíos.

1. Seleccione **Report Benign Files (Informar archivos benignos)** para permitir el registro de archivos para los archivos que reciben un veredicto benigno.
2. Seleccione **Report Grayware Files (informar archivos de grayware)** para permitir el registro de archivos para los archivos que reciben un veredicto de grayware.

STEP 5 | Cuando haya terminado, deberá **Save (Guardar)** los cambios.

STEP 6 | Defina el tráfico que se va a reenviar para su análisis.

1. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and (NGFW y) Prisma Access** > **Security Services (Servicios de seguridad)** > **WildFire and Antivirus (WildFire y antivirus)** y luego **Add Profile (Añadir perfil)**. Proporcione un **Name (Nombre)** y una **Description (Descripción)** para el perfil.

 ©2025 Palo Alto Networks, Inc.

2. **Add (Añadir)** regla para definir el tráfico que debe enviarse para el análisis y asigne a la regla un **Name (Nombre)** descriptivo, tal como local-PDF-análisis.
3. Defina la regla de perfil para que coincida con el tráfico desconocido y para que reenvíe muestras para el análisis en función de lo siguiente:
   - **Direction of Traffic (Dirección del tráfico)**: reenvíe archivos para su análisis en función de la dirección de transmisión del archivo [**Upload (Cargar)**, **Download (Descargar)** o **Upload and Download (Cargar y descargar)**]. Por ejemplo, seleccione **Upload and Download (Cargar y descargar)** para enviar todos los PDF desconocidos para el análisis, independientemente de la dirección de transmisión.
   - **Applications (Aplicaciones)**: envíe archivos para el análisis según la aplicación en uso.
   - **File Types (Tipos de archivos)**: envíe archivos para el análisis según el tipo de archivo, incluidos los enlaces de mensajes de correo electrónico. Por ejemplo, seleccione **PDF** para reenviar PDF desconocidos detectados por el cortafuegos para el análisis.
   - Seleccione el destino del tráfico que se reenviará para su análisis:
     - Seleccione **Nube pública** para que todo el tráfico que coincida con la regla se reenvíe a la nube pública de Advanced WildFire para su análisis.
     - Seleccione **Private Cloud (Nube privada)** para que todo el tráfico que coincida con la regla se reenvíe al dispositivo de WildFire para su análisis.
     - Elija **Save (Guardar)** la regla de reenvío de análisis de WildFire cuando haya terminado.
4. Elija **Save (Guardar)** el perfil de seguridad de WildFire y antivirus.

STEP 7 | Habilite el perfil de seguridad de WildFire y antivirus.

El tráfico permitido por la regla de política de seguridad se evalúa con respecto al perfil de análisis WildFire adjunto; Prisma Access reenvía el tráfico que coincide con el perfil para el análisis de WildFire.

STEP 8 | Insertar cambios en la configuración.

STEP 9 | (Opcional) Habilitación del aprendizaje automático en línea de Advanced WildFire

STEP 10 | Seleccione que hacer a continuación...

- Verifique los envíos de WildFire para confirmar que el cortafuegos reenvía archivos correctamente para su análisis.
- Supervisión de actividad de WildFire para evaluar las alertas y los detalles informados para el malware.

Archivos de avance para el análisis de Advanced Wildfire (PAN-OS y Panorama)

STEP 1 | (Solo para cortafuegos PA-7000 Series) Para habilitar un cortafuegos PA-7000 Series a fin de que reenvíe muestras para su análisis, primero debe configurar un puerto de datos en una NPC como una interfaz de tarjeta de logs. Si tiene un dispositivo PA-7000 Series que cuenta con una LFC (tarjeta de reenvío de logs),debe configurar un puerto que utilice la LFC. Cuando se configura, el puerto de la tarjeta de log o la interfaz LFC tiene prioridad sobre el puerto de gestión al reenviar muestras.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Especifique la Implementaciones avanzadas de WildFire al que desea reenviar las muestras.

Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **WildFire** y edite la configuración general en función de su implementación de nube WildFire (pública, gubernamental, privada o híbrida).

Wildfire en EE. UU. EE. UU. de WildFire solo está disponible para EE. UU. Las agencias federales funcionan como un entorno de análisis opcional.

Nube pública de Advanced WildFire:

1. Introduzca la URL de la **WildFire Public Cloud (nube pública de WildFire)**:
   - Estados Unidos: **`wildfire.paloaltonetworks.com`**
   - Europa: **`eu.wildfire.paloaltonetworks.com`**
   - Japón: **`jp.wildfire.paloaltonetworks.com`**
   - Singapur: **`sg.wildfire.paloaltonetworks.com`**
   - Reino Unido: **`uk.wildfire.paloaltonetworks.com`**
   - Canadá: **`ca.wildfire.paloaltonetworks.com`**
   - Australia: **`au.wildfire.paloaltonetworks.com`**
   - Alemania: **`de.wildfire.paloaltonetworks.com`**
   - India: **`in.wildfire.paloaltonetworks.com`**
   - Suiza: **`ch.wildfire.paloaltonetworks.com`**
   - Polonia: **`pl.wildfire.paloaltonetworks.com`**
   - Indonesia: **`id.wildfire.paloaltonetworks.com`**
   - Taiwán: **`tw.wildfire.paloaltonetworks.com`**
   - Francia: **`fr.wildfire.paloaltonetworks.com`**
   - Qatar: **`qatar.wildfire.paloaltonetworks.com`**
   - Corea del Sur: **`kr.wildfire.paloaltonetworks.com`**
   - Israel: **`il.wildfire.paloaltonetworks.com`**
   - Arabia Saudita: **`sa.wildfire.paloaltonetworks.com`**
   - España: **`es.wildfire.paloaltonetworks.com`**
2. Asegúrese de que el campo de la **WildFire Private Cloud (nube privada de WildFire)** esté vacío.

Opciones de nube de WildFire FedRAMP:

1. Introduzca la URL de **WildFire FedRAMP Cloud (Nube de WildFire FedRAMP)**:
   - EE. UU. Nube gubernamental: **`wildfire.gov.paloaltonetworks.com`**
   - Nube gubernamental de Advanced WildFire: gov-cloud.wildfire.paloaltonetworks.com
   - Nube para el sector público de Advanced WildFire: pubsec-cloud.wildfire.paloaltonetworks.com

 ©2025 Palo Alto Networks, Inc.

2. Asegúrese de que el campo de la **WildFire Private Cloud (nube privada de WildFire)** esté vacío.

STEP 3 | Defina los límites de tamaño para los archivos que el cortafuegos reenvía y realice la configuración de registro e informes.

Continúe editando la Configuración general [**Device (Dispositivo)** > **Setup (Configuración)** > **WildFire**].

- Revise los **File Size Limits (Límites de tamaño de archivo)** para los archivos reenviados desde el cortafuegos.

  *Es una Prácticas recomendadas de Advanced WildFire establecer el **File Size (Tamaño de archivo)** para PE en el límite de tamaño máximo de 10 MB y dejar el **File size (Tamaño de archivo)** para todos los demás tipos de archivo establecido en el valor predeterminado.*

- Seleccione **Report Benign Files (Informar archivos benignos)** para permitir el registro de archivos para los archivos que reciben un veredicto benigno.
- Seleccione **Report Grayware Files (informar archivos de grayware)** para permitir el registro de archivos para los archivos que reciben un veredicto de grayware.
- Defina la información de sesión que se registra en los informes de análisis de WildFire editando la configuración de información de sesión. De manera predeterminada, toda la información de sesión se muestra en los informes de análisis de WildFire. Desmarque las casillas de verificación para quitar los campos correspondientes de los informes de análisis de WildFire y haga clic en **OK (Aceptar)** para guardar la configuración.

STEP 4 | Defina el tráfico que se va a reenviar para su análisis.

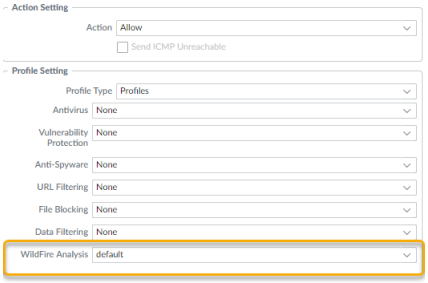
1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **WildFire Analysis (Análisis de WildFire)**, haga clic en**Add (Añadir)** para añadir un nuevo perfil de análisis de WildFire y asigne al perfil un **Name (Nombre)** descriptivo.
2. **Add (Añada)** una regla de perfil para definir el tráfico que debe enviarse para el análisis y asigne a la regla un **Name (Nombre)** descriptivo, tal como local-PDF-análisis.
3. Defina la regla de perfil para que coincida con el tráfico desconocido y para que reenvíe muestras para el análisis en función de lo siguiente:
   - **Applications (Aplicaciones)**: envíe archivos para el análisis según la aplicación en uso.
   - **File Types (Tipos de archivos)**: envíe archivos para el análisis según el tipo de archivo, incluidos los enlaces de mensajes de correo electrónico. Por ejemplo, seleccione **PDF** para reenviar PDF desconocidos detectados por el cortafuegos para el análisis.
   - **Direction (Dirección)**: envíe archivos para el análisis según la dirección de transmisión del archivo (carga, descarga o ambas). Por ejemplo, seleccione **both (ambas)** para enviar todos los PDF desconocidos para el análisis, independientemente de la dirección de transmisión.
4. Haga clic en **OK (Aceptar)** para guardar el perfil de análisis de WildFire.

 ©2025 Palo Alto Networks, Inc.

STEP 5 | Adjunte el perfil de WildFire Analysis a una regla de la política de seguridad.

El tráfico permitido por la regla de política de seguridad se evalúa en función del perfil de análisis de WildFire adjunto; los cortafuegos envían el tráfico que coincide con el perfil para el análisis de WildFire.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y **Add (Añadir)** o modifique una regla de política.
2. Haga clic en la pestaña **Actions (Acciones)** en la regla de la política.
3. En la sección de Profile Settings (Configuración de perfil), seleccione **Profiles (Perfiles)** como el **Profile Type (Tipo de perfil)** y seleccione un perfil de **WildFire Analysis (Análisis de WildFire)** para adjuntar la regla de la política



STEP 6 | Asegúrese de habilitar el cortafuegos para garantizar el Reenvío de tráfico descifrado SSL para Advanced WildFire Analysis.

Esta es una práctica recomendada.

STEP 7 | (Opcional) Habilitación del aprendizaje automático en línea de Advanced WildFire

STEP 8 | (Opcional) Habilite el modo de espera para la búsqueda de firma en tiempo real

STEP 9 | Lea e implemente las Prácticas recomendadas de Advanced WildFire.

STEP 10 | Haga clic en **Commit (Confirmar)** para aplicar la configuración actualizada.

STEP 11 | (Opcional) Instale un Certificado de dispositivo para actualizar a la versión más reciente del certificado utilizado por el cortafuegos para comunicarse con los servicios en la nube de Palo Alto Networks.

STEP 12 | (Opcional) Configurar los ajustes de FQDN de nube de contenido.

STEP 13 | Seleccione que hacer a continuación...

- Verifique los envíos de WildFire para confirmar que el cortafuegos reenvía archivos correctamente para su análisis.
- Supervisión de actividad de WildFire para evaluar las alertas y los detalles informados para el malware.

 ©2025 Palo Alto Networks, Inc.

Carga manual de archivos en el portal de WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

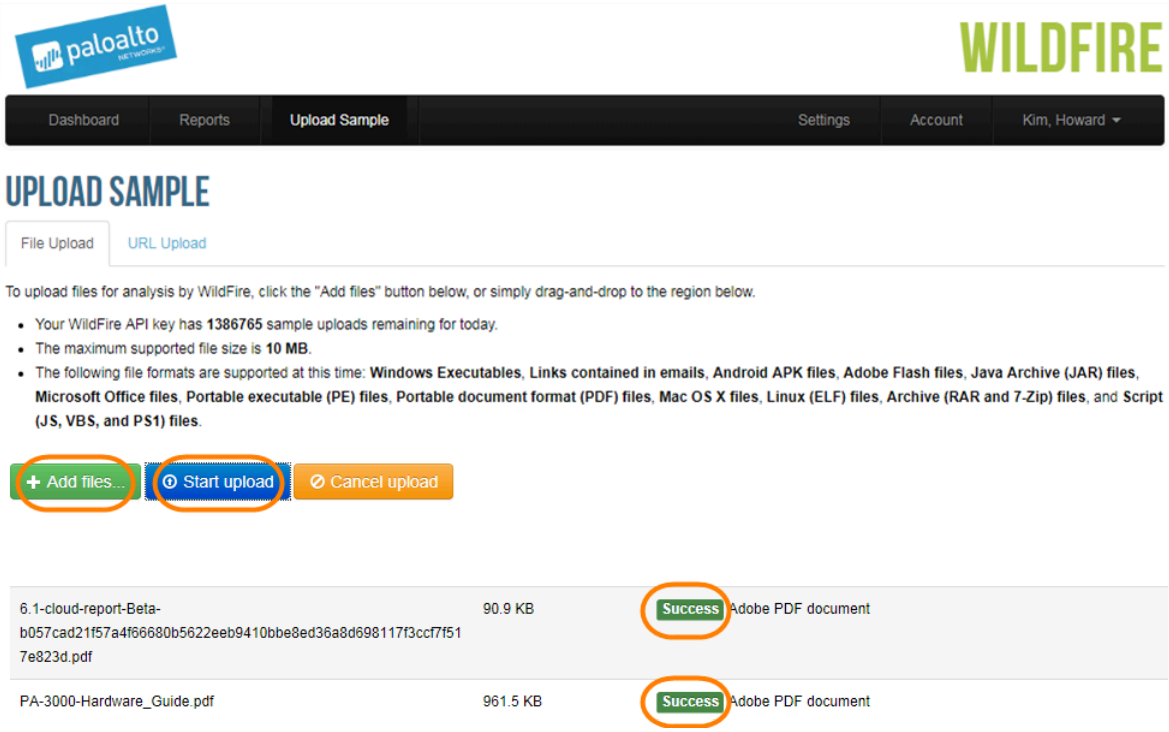
Todos los clientes de Palo Alto Networks con una cuenta de asistencia técnica pueden usar el portal de WildFire de Palo Alto Networks para enviar manualmente hasta cinco muestras al día para su análisis. Si tiene una suscripción de Advanced WildFire o WildFire, puede enviar manualmente muestras al portal como parte de su límite diario de envío de 1000 muestras; sin embargo, tenga en cuenta que el límite diario de 1000 muestras también incluye los envíos desde la API de WildFire.

STEP 1 | Cargue manualmente archivos o URL en el portal de WildFire para su análisis.

1. Inicie sesión en el portal de WildFire.
2. Haga clic en **Upload Sample (cargar muestra)** en la barra de menú.
   - Para enviar archivos para analizar, seleccione **File Upload (Carga de archivos)** y **Open (Abrir)** para abrir los archivos que desea enviar para su análisis. Haga clic en **Start (Iniciar)** para comenzar con el análisis de un archivo o haga clic en **Start Upload (Iniciar carga)** para enviar todos los archivos que añadió para su análisis.

©2025 Palo Alto Networks, Inc.

- Para enviar una URL para el análisis, haga clic en **URL Upload (Carga de URL)**, introduzca una URL, y haga clic en **Submit (Enviar)** para enviarla para su análisis.



3. Cierre el cuadro de diálogo emergente **Uploaded File Information (Información sobre archivo cargado)**.

STEP 2 | Visualice el veredicto y los resultados del análisis del archivo.

Espere al menos cinco minutos para que Advanced WildFire analice la muestra.

Como no se asocia la carga manual con un cortafuegos específico, las cargas manuales no muestran información de la sesión en los informes.

1. Vuelva al panel del Portal de WildFire.
2. En la sección 1 hora anterior, seleccione **Manual** en la columna de fuente para ver información del análisis para las muestras más recientes enviadas manualmente.
3. Encuentre los archivos o URL que ha cargado y haga clic en el icono de detalles a la izquierda de la Hora de recepción.

 ©2025 Palo Alto Networks, Inc.

Reenviar tráfico SSL descifrado para Advanced WildFire Analysis

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

Habilite el cortafuegos para que envíe tráfico descifrado SSL para el análisis de Advanced WildFire. El tráfico que descifra el cortafuegos se evalúa con las reglas de la política de seguridad; si coincide con el perfil de análisis de WildFire adjunto a la regla de seguridad, el tráfico descifrado se reenvía para el análisis antes de que el cortafuegos vuelva a cifrarlo. Solo un superusuario puede habilitar esta opción.

Reenviar tráfico SSL descifrado para su análisis es una Prácticas recomendadas de Advanced WildFire.

- En un cortafuegos que no tiene múltiples sistemas virtuales habilitados:
  1. Si aún no lo ha hecho, habilite el cortafuegos para realizar el descifrado y el Reenviar archivos para Advanced WildFire Analysis.
  2. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Content ID (ID de contenido)**.
  3. Edite los ajustes de ID de contenido y seleccione la casilla de verificación **Allow Forwarding of Decrypted Content (Permitir reenvío de contenido descifrado)**.
  4. Haga clic en **OK (Aceptar)** para guardar los cambios.

- En un cortafuegos con sistemas virtuales habilitados:
  1. Si aún no lo ha hecho, habilite el descifrado y el Reenviar archivos para Advanced WildFire Analysis.
  2. Seleccione **Device (Dispositivo)** > **Virtual Systems (Sistemas virtuales)**, haga clic en el sistema virtual que desea modificar y seleccione la casilla de verificación **Allow Forwarding of Decrypted Content (Permitir reenvío de contenido descifrado)**.

- Por Prisma Access, esto se configura como parte de la configuración de perfil de seguridad de **WildFire and Antivirus (WildFire y antivirus)**. Para obtener más información, consulte Reenviar archivos para Advanced WildFire Analysis para Prisma Access.

©2025 Palo Alto Networks, Inc.

Habilitar Análisis en línea en la nube para Advanced WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire

Advanced WildFire de Palo Alto Networks opera una serie de motores de detección de aprendizaje automático (ML) basados en la nube que proporcionan análisis en línea de archivos PE (ejecutables portátiles) que atraviesan su red para detectar y prevenir malware avanzado en tiempo real. Al igual que con el resto de contenido malicioso que WildFire detecta, las amenazas detectadas por el Análisis en línea en la nube para Advanced WildFire generan una firma que luego se difunde a los clientes a través de un paquete de actualización, proporcionando una defensa futura para todos los clientes de Palo Alto Networks.

Los motores basados en la nube permiten la detección de malware nunca antes visto (por ejemplo, un malware de día cero de Palo Alto Networks o malware nunca visto por Palo Alto Networks) y su bloqueo para impedir su entrada en su entorno. El Análisis en línea en la nube de Advanced WildFire utiliza un mecanismo de reenvío ligero en el cortafuegos para minimizar el impacto en el rendimiento. Los modelos de ML basados en la nube se actualizan sin problemas para abordar el panorama de amenazas en constante cambio sin requerir actualizaciones de contenido o soporte de versiones de funciones.

El análisis en línea en la nube de Advanced WildFire se habilita y configura a través del perfil de análisis de WildFire y requiere PAN-OS 11.1 o posterior con una licencia avanzada de WildFire activa.

STEP 1 | Instale un certificado de dispositivo de cortafuegos actualizado que se usa para autenticarse en el servicio de análisis en la nube de Advanced WildFire. Repita el procedimiento para todos los cortafuegos habilitados para el análisis en línea de la nube.

Este paso no es necesario si ya ha instalado la versión actual del certificado del dispositivo en su cortafuegos.

STEP 2 | Inicie sesión en la interfaz web de PAN-OS.

©2025 Palo Alto Networks, Inc.

STEP 3 | Para habilitar el análisis en línea en la nube de Advanced WildFire, debe tener una suscripción activa a Advanced WildFire. Para obtener más información, consulte: Licencia, registro y activación.

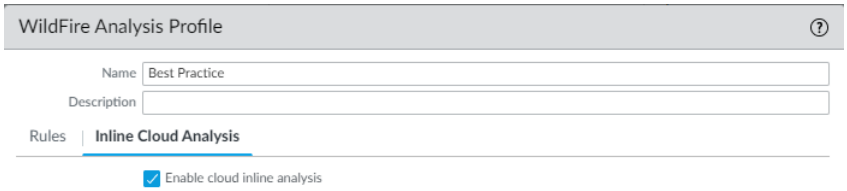
Para verificar las suscripciones para las que tiene licencias actualmente activas, seleccione **Device (Dispositivo)** > **Licenses (Licencias)** y verifique que las licencias correspondientes estén disponibles y no estén vencidas.

Si su licencia actual de WildFire ha caducado y está instalando una licencia de Advanced WildFire, primero debe eliminar la licencia de WildFire del NGFW antes de instalar la licencia de Advanced WildFire.

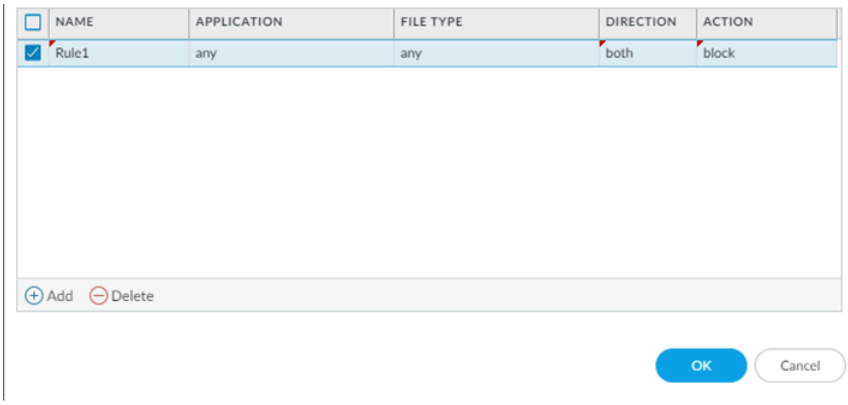
 ©2025 Palo Alto Networks, Inc.

STEP 4 | Actualice o cree un nuevo perfil de seguridad de análisis de WildFire para habilitar el análisis en línea en la nube de Advanced WildFire.

1. Seleccione un **WildFire Analysis Profile (Perfil de análisis de WildFire)** existente o seleccione **Add (Añadir)** uno nuevo [**Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **WildFire Analysis (Análisis de WildFire)**].
2. Seleccione su perfil de análisis de WildFire y, a continuación, vaya a **Inline Cloud Analysis (Análisis en línea en la nube)** y **Enable cloud inline analysis (Habilitar el análisis en línea en la nube)**.



3. Especifique una regla que defina una acción a tomar cuando el análisis en línea en la nube de Advanced WildFire detecte malware avanzado.



- Nombre: introduzca un Nombre descriptivo para cada regla que añada al perfil (hasta 31 caracteres).
- Aplicación: añada tráfico de aplicaciones para que coincida con las reglas que definen las acciones de Inline Cloud ML.
- Tipo de archivo: seleccione un tipo de archivo que se analizará en el destino de análisis definido para la regla.

  Solo se admiten archivos PE (ejecutable portátil) en este momento.

- Dirección: aplique la regla al tráfico dependiendo de la Dirección de la transmisión. Puede aplicar la regla para **descargar** tráfico.
- Acción: configure la acción que debe realizar cuando se detecte una amenaza mediante el análisis en línea a la nube de Advanced WildFire. Puede **allow (permitir)** que el tráfico de la aplicación continúe hacia el destino o **block (bloquear)** el tráfico desde una fuente o un origen-destino.

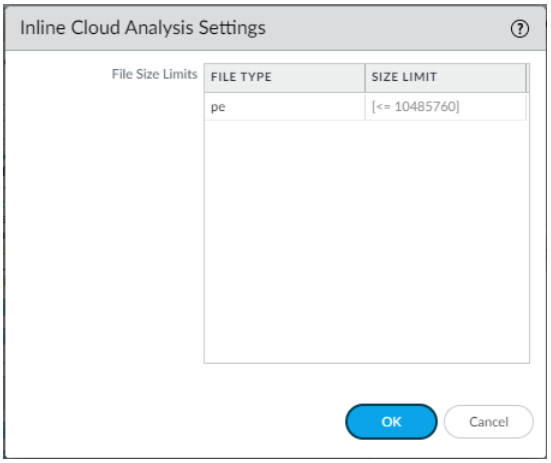
  Palo Alto Networks recomienda configurar la acción en bloquear para una seguridad óptima.

 ©2025 Palo Alto Networks, Inc.

4. Haga clic en **OK (Aceptar)** para salir del cuadro de diálogo de configuración del perfil de análisis de WildFire.

STEP 5 | Revise el tamaño máximo de archivo que se puede reenviar para su análisis con el análisis en línea en la nube de Advanced WildFire

El análisis en línea en la nube de Advanced WildFire proporciona un veredicto rápido de WildFire. Sin embargo, un informe completo para una muestra maliciosa solo está disponible después de que la muestra se someta a un análisis dinámico completo, que puede tardar hasta 30 minutos.

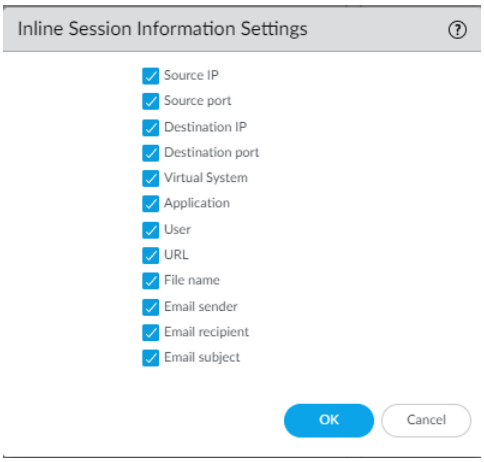


1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **WildFire** > **Inline Cloud Analysis Settings (Configuración de análisis en línea en la nube)** y revise los límites de tamaño de archivo.
2. Haga clic en **OK (Aceptar)** para confirmar los cambios.

STEP 6 | Especifique la información de sesión de red que el cortafuegos reenvía sobre una muestra determinada. Palo Alto Networks utiliza la información de la sesión para obtener más información sobre el contexto del evento de red sospechoso, los indicadores de compromiso relacionados con el

 ©2025 Palo Alto Networks, Inc.

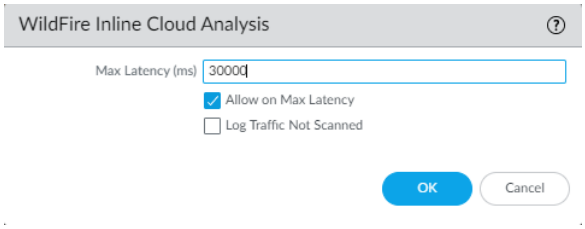
malware, los hosts y los clientes afectados, y las aplicaciones utilizadas para entregar el malware. Estas opciones están activadas de forma predeterminada.



1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **WildFire** > **Inline Session Information Settings (configuración de información de sesión en línea)** y seleccione o desactive las opciones según sea necesario.
   - **Source IP (IP de origen)**: se reenvía la dirección IP de origen que envió el archivo desconocido.
   - **Source Port (puerto de origen)**: se reenvía el puerto de origen que envió el archivo desconocido.
   - **Destination IP (IP de destino)**: se reenvía la dirección IP de destino del archivo desconocido.
   - **Destination Port (puerto de destino)**: se reenvía el puerto de destino del archivo desconocido.
   - **Virtual System (Sistema virtual)**: se reenvía el sistema virtual que detectó el archivo desconocido.
   - **Application (Aplicación)**: se reenvía la aplicación de usuario que transmitió el archivo desconocido.
   - **User (Usuario)**: se reenvía el usuario de destino.
   - **URL**: se reenvía la URL asociada al archivo desconocido.
   - **Filename (Nombre del archivo)**: se reenvía el nombre del archivo desconocido.
   - **Email sender (Remitente del correo electrónico)**: se reenvía el remitente de un enlace de correo electrónico desconocido (el nombre del remitente del correo electrónico también aparece en los logs e informes de WildFire).
   - **Email recipient (Destinatario del correo electrónico)**: se reenvía el destinatario de un enlace de correo electrónico desconocido (el nombre del destinatario del correo electrónico también aparece en los logs e informes de WildFire).
   - **Email subject (Asunto del correo electrónico)**: se reenvía el asunto de un enlace de correo electrónico desconocido (el asunto del correo electrónico también aparece en los logs e informes de WildFire).
2. Haga clic en **OK (Aceptar)** para confirmar los cambios.

 ©2025 Palo Alto Networks, Inc.

STEP 7 | Configure la latencia de tiempo de espera y la acción que se debe realizar cuando la solicitud supere la latencia máxima.



1. Especifique las medidas que debe tomar cuando se alcancen los límites de latencia para las solicitudes de análisis en línea en la nube de Advanced WildFire:
   - Máxima latencia (ms): especifique el tiempo máximo de procesamiento aceptable, en segundos, para que el análisis en línea en la nube de Advanced WildFire devuelva un resultado.
   - Permitir en latencia máxima: permite que el cortafuegos realice la acción de permitir, cuando se alcanza la latencia máxima. Al anular la selección de esta opción, se establece que la acción del cortafuegos se bloquee.
   - Registrar tráfico no analizado: permite que el cortafuegos registre solicitudes de Análisis en línea en la nube para Advanced WildFire que muestren la presencia de malware avanzado, pero que no hayan sido procesadas por la nube de Advanced WildFire.
2. Haga clic en **OK (Aceptar)** para confirmar los cambios.

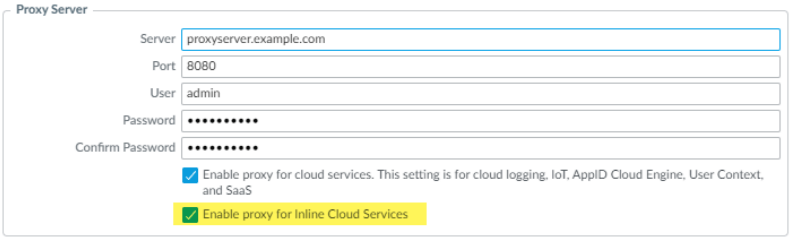
STEP 8 | (Necesario cuando el cortafuegos se implementa con un servidor proxy explícito) Configure el servidor proxy utilizado para acceder a los servidores que facilitan las solicitudes generadas por todas las características de análisis en la nube configuradas. Se puede especificar un único servidor

 ©2025 Palo Alto Networks, Inc.

proxy que se aplica a todos los servicios de actualización de Palo Alto Networks, incluidos todos los servicios de registro de logs y nube en línea configurados.

1. (PAN-OS 11.2.3 y posterior) Configure el servidor proxy a través de PAN-OS.
   1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)** y edite la sección detalles de **Services (Servicios)**.
   2. Especifique la configuración del **Proxy Server (Servidor proxy)** y **Enable proxy for Inline Cloud Services (Habilitar el proxy para servicios en la nube en línea)**. Puede proporcionar una dirección IP o FQDN en el campo **Server (Servidor)**.

      La contraseña del servidor proxy debe contener un mínimo de seis caracteres.

   3. Haga clic en **OK (Aceptar)**.
2. (PAN-OS 11.1.5 y posterior) Configure el servidor proxy a través de la CLI del cortafuegos.
   1. Acceda a la CLI del cortafuegos.
   2. Configure los ajustes del servidor proxy base mediante los siguientes comandos de la CLI:

      ```
      set deviceconfig system secure-proxy-server <FQDN_or_IP>
       set deviceconfig system secure-proxy-port <1-65535>
       set deviceconfig system secure-proxy-user <value> set
       deviceconfig system secure-proxy-password <value>
      ```

      La contraseña del servidor proxy debe contener un mínimo de seis caracteres.

   3. Habilite el servidor proxy para enviar solicitudes a los servidores de servicios en la nube en línea mediante el siguiente comando de la CLI:

      ```
      debug dataplane mica set inline-cloud-proxy enable
      ```

   4. Vea el estado operativo actual del soporte de proxy para los servicios en la nube en línea mediante el siguiente comando de la CLI:

      ```
      debug dataplane mica show inline-cloud-proxy
      ```

      Por ejemplo:

      ```
      debug dataplane mica show inline-cloud-proxy Proxy for
       Advanced Services is Disabled
      ```

 ©2025 Palo Alto Networks, Inc.

STEP 9 | (Recomendado) Configure el cortafuegos para impedir que el cliente busque parte de un archivo y posteriormente iniciar una nueva sesión para buscar el resto de un archivo después de que el cortafuegos termine la sesión original debido a la actividad maliciosa detectada. Esto ocurre cuando un navegador web implementa la opción de rango HTTP. Si bien habilitar la **Allow HTTP partial response (Permitir respuesta parcial de HTTP)** proporciona la máxima disponibilidad, también puede aumentar el riesgo de un ciberataque correcto. Palo Alto Networks recomienda deshabilitar **Allow HTTP partial response (Permitir respuesta parcial HTTP)** para obtener la máxima seguridad.

> ***Allow HTTP partial response (Permitir respuesta parcial de HTTP)*** *es una configuración global y afecta a las transferencias de datos basadas en HTTP que usan el encabezado RANGE, lo que puede causar anomalías en el servicio para determinadas aplicaciones. Después de deshabilitar* ***Allow HTTP partial response (Permitir respuesta parcial de HTTP)****, debe validar el funcionamiento de sus aplicaciones críticas para el negocio.*

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Content-ID** > **Content-ID Settings (Configuración de Content-ID)**.
2. Anule la selección **Allow HTTP partial response (Permitir respuesta parcial de HTTP)** y haga clic en **OK (Aceptar)**.

STEP 10 | Haga clic en **Commit (Confirmar)** para compilar los cambios.

STEP 11 | (Opcional) Configurar los ajustes de FQDN de nube de contenido.

 ©2025 Palo Alto Networks, Inc.

Habilitación del aprendizaje automático en línea de Advanced WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

Puede evitar que las variantes maliciosas de ejecutables portátiles y scripts de PowerShell entren en su red en tiempo real mediante el aprendizaje automático (ML) basado en análisis en el plano de datos del cortafuegos. El aprendizaje automático en línea de Advanced Wildfire, mediante el uso de tecnología de análisis de la nube de WildFire® en su plataforma de seguridad, detecta dinámicamente archivos maliciosos de un tipo específico mediante la evaluación de varios detalles del archivo, incluidos los campos y patrones del descodificador, para formular una clasificación de alta probabilidad de un archivo. Esta protección se extiende a variantes de amenazas actualmente desconocidas y futuras que coinciden con características que Palo Alto Networks ha identificado como maliciosas. Aprendizaje automático en línea de Advanced WildFire complementa la configuración de protección de su perfil de antivirus existente. Además, puede especificar excepciones de hash de archivos para excluir cualquier falso positivo que encuentre, lo que le permite crear reglas más detalladas en sus perfiles para satisfacer sus necesidades de seguridad específicas.

Para habilitar el aprendizaje automático en línea de Advanced WildFire, debe tener una suscripción activa a Advanced WildFire o WildFire, crear (o modificar) un perfil de seguridad de Antivirus (o WildFire y Antivirus para Prisma Access) para configurar y habilitar el servicio y luego adjuntar el perfil de Antivirus a una regla de política de seguridad.

El Aprendizaje automático en línea de Advanced WildFire no es compatible actualmente en el dispositivo virtual VM-50 o VM50L.

- Strata Cloud Manager
- PAN-OS y Panorama

Habilite el aprendizaje automático en línea de Advanced WildFire (Pan-OS y Panorama)

Para habilitar su configuración de aprendizaje automático en línea de WildFire, adjunte el perfil de antivirus configurado con la configuración de aprendizaje automático en línea a una regla de política de seguridad.

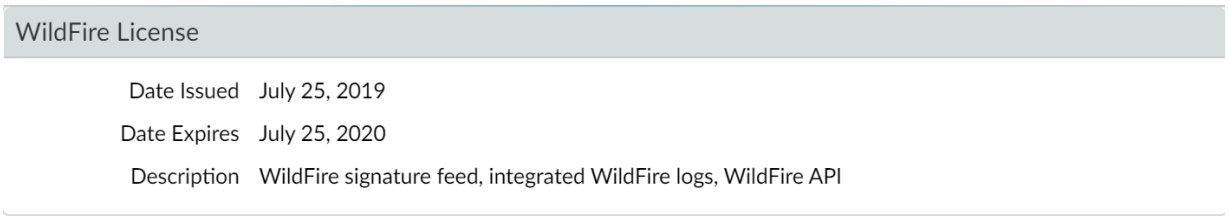
©2025 Palo Alto Networks, Inc.

Para omitir el ML en línea de Advanced WildFire, debe establecer el parámetro **Action Setting (Configuración de acción)** para **disable (for all protocols) [deshabilitar (para todos los protocolos)]** por modelo o cree una excepción de archivo de aprendizaje automático en línea de WildFire mediante el hash parcial. No configure su perfil de antivirus con excepciones de firma basadas en los ID de amenazas de ML en línea de WildFire. Esto hará que el cortafuegos bloquee todo el tráfico de su red a la dirección IP.

WildFire Inline ML (Aprendizaje automático en línea de WildFire) no es compatible actualmente en el dispositivo virtual VM-50 o VM50L.

STEP 1 | Para aprovechar WildFire Inline ML (Aprendizaje automático en línea de WildFire), debe tener una suscripción activa a WildFire para analizar los archivos ejecutables de Windows.

Verifique que tenga una suscripción a WildFire. Para verificar las suscripciones para las que tiene licencias actualmente, seleccione **Device (Dispositivo)** > **Licenses (Licencias)** y verifique que las licencias correspondientes se muestren y no estén vencidas.

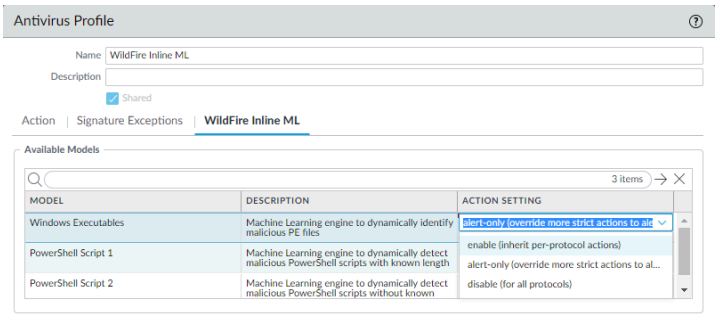


STEP 2 | Cree un nuevo perfil o actualice sus perfiles de seguridad de antivirus existentes para utilizar los modelos de WildFire Inline ML (Aprendizaje automático en línea de WildFire) en tiempo real.

1. Seleccione un **perfil de antivirus** existente o cree uno nuevo (seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Antivirus** y **añada** un nuevo perfil.
2. Configure su perfil de antivirus.
3. Seleccione la pestaña **WildFire Inline ML (Aprendizaje automático en línea de WildFire)** y aplique una **configuración de acción** para cada modelo de WildFire Inline ML (Aprendizaje automático en línea de WildFire). Esto aplica la configuración de las acciones de WildFire Inline ML (Aprendizaje automático en línea de WildFire) configuradas para cada protocolo en función del modelo. Los siguientes motores de clasificación están disponibles:
   - Ejecutables de Windows
   - Scripts de PowerShell 1
   - Scripts de PowerShell 2
   - Formato vinculado ejecutable (disponible con la instalación de la versión de contenido de PAN-OS 8367 y posterior)
   - MSOffice (disponibles con la instalación de la versión 8434 de contenido de PAN-OS y posteriores):
   - Scripts de shell (disponibles con la instalación de la versión 8543 de contenido de PAN-OS y posteriores):
   - OOXML (disponible con la instalación de PAN-OS 11.1.3 y versiones posteriores y la versión de contenido 8825 y posteriores de PAN-OS)

 ©2025 Palo Alto Networks, Inc.

- Mach-O (disponible con la instalación de PAN-OS 11.1.3 y versiones posteriores y la versión de contenido 8885-8930 y posteriores de PAN-OS)



La siguiente configuración de acción está disponible:

- **enable (inherit per-protocol actions) [habilitar (heredar acciones según el protocolo)]**: WildFire inspecciona el tráfico de acuerdo con sus selecciones en la columna WildFire Inline ML Action (Acción de aprendizaje automático en línea de WildFire) en la sección de decodificadores de la pestaña **Action (Acción)**.
- **alert-only (override more strict actions to alert) [solo alerta (sobrescribir acciones más estrictas para la alerta)]**: WildFire inspecciona el tráfico según sus selecciones en la columna WildFire Inline ML Action (Acción de aprendizaje automático en línea de WildFire) en la sección de descodificadores de la pestaña **Action (Acción)** y cancela cualquier acción con un nivel de gravedad superior a `alert (alerta)` (`drop (descartar)`, `reset-client (restablecer cliente)`, `reset-server (restablecer servidor)`, `reset-both (restablecer ambos)`) `alert (alerta)`, que permite que el tráfico pase mientras sigue generando y guardando una alerta en los logs de amenazas.
- **disable (for all protocols) [deshabilitar (para todos los protocolos)]**: WildFire permite que el tráfico pase sin ninguna acción de la política.

4. Haga clic en **OK (Aceptar)** para salir de la ventana de configuración del perfil de antivirus y **confirmar** su nueva configuración.

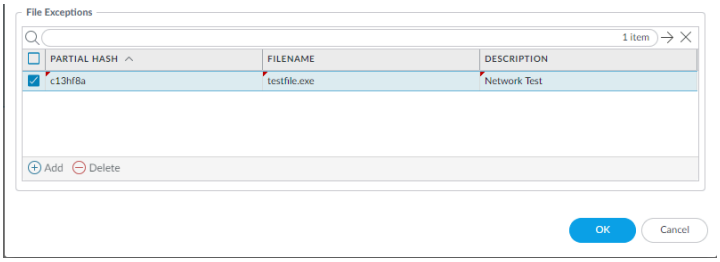
STEP 3 | (Opcional) Añada excepciones de archivo a su perfil de seguridad de antivirus si encuentra falsos positivos. Por lo general, esto se hace para los usuarios que no están reenviando archivos a WildFire

 ©2025 Palo Alto Networks, Inc.

para su análisis. Puede añadir los detalles de la excepción del archivo directamente a la lista de excepciones o especificar un archivo de los logs de amenazas.

Si su perfil de seguridad de WildFire Analysis está configurado para reenviar los tipos de archivo analizados mediante el AA en línea de WildFire, los falsos positivos se corrigen automáticamente a medida que se reciben. Si continúa viendo alertas de ml-virus para archivos que han sido clasificados como benignos por WildFire Analysis, comuníquese con el soporte de Palo Alto Networks.

- Añada excepciones de archivos directamente a la lista de excepciones.
  1. Seleccione **Objects (Objetos) > Security Profiles (Perfiles de seguridad) > Antivirus**.
  2. Seleccione un perfil de antivirus para el que desee excluir archivos específicos y, a continuación, seleccione **WildFire Inline ML (Aprendizaje automático en línea de WildFire)**.
  3. Añada el hash, el nombre de archivo y la descripción del archivo que desee excluir de la aplicación.



  4. Haga clic en **OK (Aceptar)** para guardar el perfil de antivirus y, a continuación, **confirme** las actualizaciones.
- Añada excepciones de archivos a partir de las entradas de los logs de amenazas.
  1. Seleccione **Monitor (Supervisar) > Logs > Threat (Amenaza)** y filtre los logs por el tipo de amenaza **ml-virus (virus de aprendizaje automático)**. Seleccione un log de amenazas para un archivo para el que desee crear una excepción de archivo.
  2. Vaya a la **Detailed Log View (Vista de log detallada)** y desplácese hacia abajo hasta el panel **Details (Detalles)** y, a continuación, seleccione **Create Exception (Crear excepción)**.

  3. Añada una **descripción** y haga clic en **OK (Aceptar)** para añadir la excepción del archivo.
  4. La nueva excepción de archivo se puede encontrar en la lista **File Exceptions (Excepciones de archivo)** en **Objects (Objetos) > Security Profiles (Perfiles de seguridad) > Antivirus > WildFire Inline ML (Aprendizaje automático en línea de WildFire)**.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | (Opcional) Verifique el estado de la conectividad del cortafuegos con el servicio en la nube de aprendizaje automático en línea.

Utilice el siguiente comando de la CLI en el cortafuegos para ver el estado de la conexión.

```
show mlav cloud-status
```

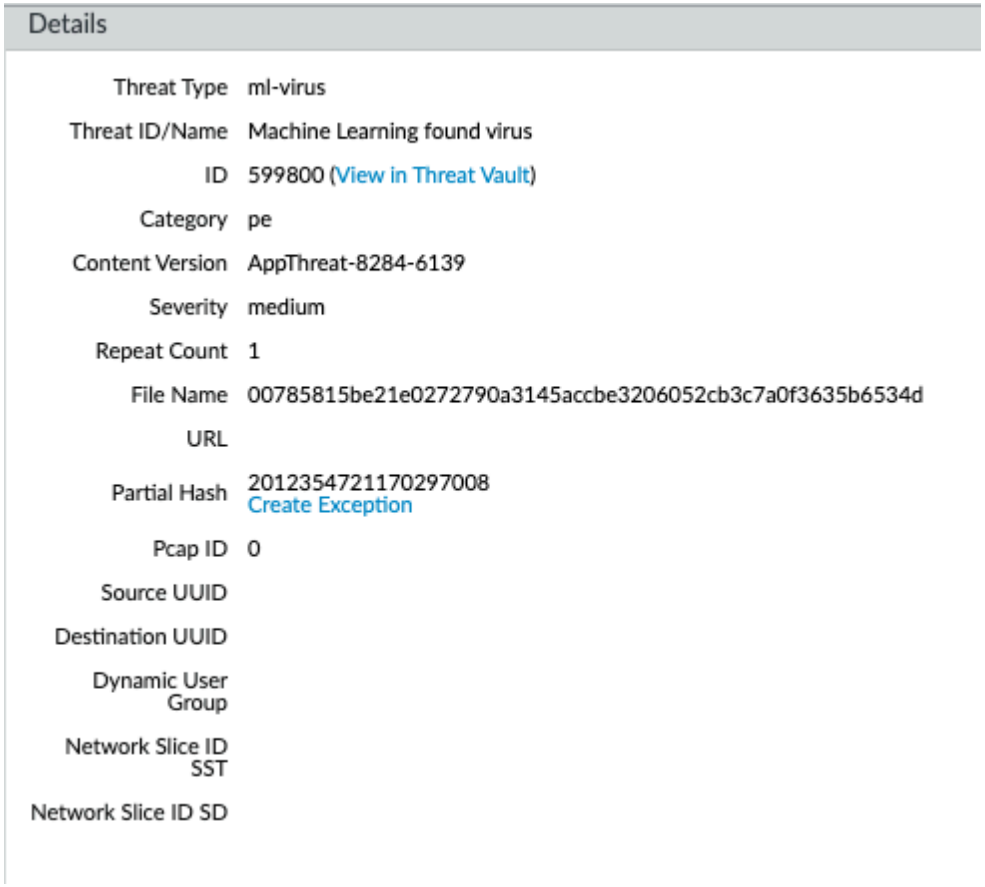
Por ejemplo:

```
show mlav cloud-status MLAV cloud Current cloud server:
 ml.service.paloaltonetworks.com Cloud connection: connected
```

Si no puede conectarse al servicio en la nube de aprendizaje automático en línea, verifique que el siguiente dominio no esté bloqueado: ml.service.paloaltonetworks.com.

STEP 5 | (Opcional) Configurar los ajustes de FQDN de nube de contenido.

Para ver información sobre los archivos que se han detectado con WildFire Inline ML (Aprendizaje automático en línea de WildFire), examine los logs de amenazas (**Monitor (Supervisar) > Logs > Threat (Amenaza)** y, a continuación, seleccione el tipo de log de la lista). Los archivos que se han analizado con WildFire inline ML (Aprendizaje automático en línea de WildFire) están etiquetados con el tipo de amenaza **ml-virus**:



 ©2025 Palo Alto Networks, Inc.

Habilitación del aprendizaje automático en línea de Advanced WildFire (Cloud Management)

Si está utilizando Panorama para gestionar Prisma Access:

*Desplácese a la pestaña **PAN-OS** y siga las instrucciones que se indican allí.*

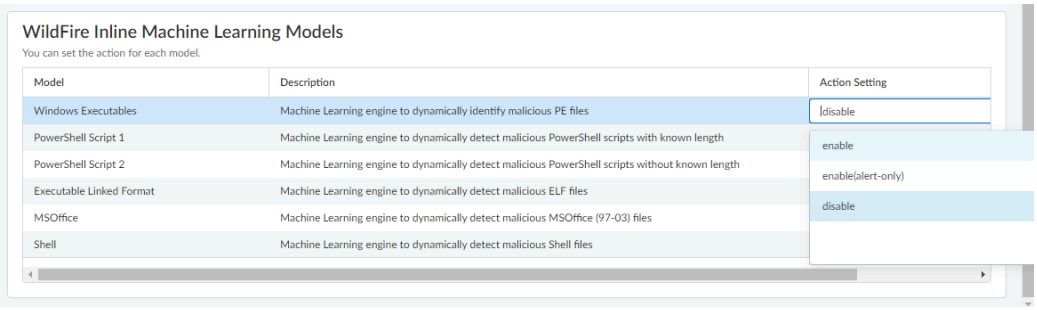
Si está utilizando Prisma Access Cloud Management, continúe aquí.

STEP 1 | Para aprovechar el aprendizaje automático en línea de WildFire, debe tener una suscripción activa a WildFire como parte de su suscripción a Prisma Access.

Compruebe que tiene una suscripción a WildFire válida y que no haya caducado.

STEP 2 | Cree un nuevo perfil o actualice su perfil de seguridad de **WildFire y antivirus** existente para utilizar los modelos de aprendizaje automático en línea de WildFire en tiempo real.

1. Seleccione un perfil de seguridad existente de **WildFire and Antivirus (WildFire y antivirus)** o cree uno nuevo [seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and (NGFW y)Prisma Access** > **Security Services (Servicios de seguridad)** > **WildFire and Antivirus (WildFire y antivirus)** y **Add Profile (Añadir perfil)**].
2. Configure su perfil de WildFire y antivirus para reenviar muestras para su análisis.
3. Seleccione **WildFire Inline Machine Learning Models (Modelos de aprendizaje automático en línea de WildFire)** y aplique una **Action Setting (Configuración de acción)** para cada modelo de WildFire Inline ML. Esto aplica la configuración de las acciones de WildFire Inline ML (Aprendizaje automático en línea de WildFire) configuradas para cada protocolo en función del modelo.



Los siguientes motores de clasificación están disponibles:

- Ejecutables de Windows
- Scripts de PowerShell 1
- Scripts de PowerShell 2
- Formato vinculado ejecutable
- MSOffice
- Scripts de Shell
- **habilitar**: WildFire inspecciona el tráfico de acuerdo con sus selecciones en la columna WildFire Inline ML Action (Acción de aprendizaje automático en línea de WildFire) en la sección de decodificadores de la pestaña **Action (Acción)**.

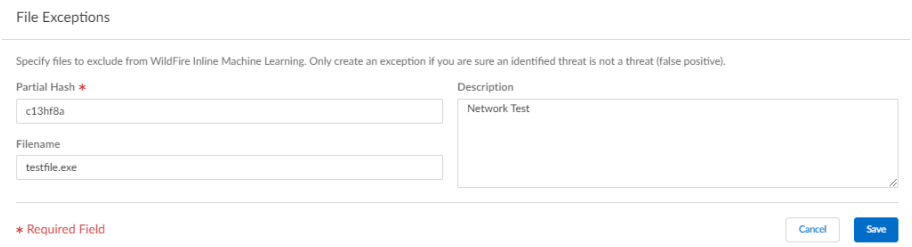
 ©2025 Palo Alto Networks, Inc.

- **habilitar (solo alerta)**: WildFire inspecciona el tráfico según sus selecciones en la columna WildFire Inline ML Action (Acción de aprendizaje automático en línea de WildFire) en la sección de descodificadores de la pestaña **Action (Acción)** y cancela cualquier acción con un nivel de gravedad superior a `alert (alerta)` (`drop (descartar)`, `reset-client (restablecer cliente)`, `reset-server (restablecer servidor)`, `reset-both (restablecer ambos)`) `alert (alerta)`, que permite que el tráfico pase mientras sigue generando y guardando una alerta en los logs de amenazas.
- **deshabilitar**: WildFire permite que el tráfico pase sin ninguna acción de la política.

STEP 3 | (Opcional) Añada excepciones de archivo a su WildFire y perfil de seguridad de antivirus si encuentra falsos positivos. Por lo general, esto se hace para los usuarios que no están reenviando archivos a WildFire para su análisis. Puede añadir los detalles de la excepción del archivo directamente a la lista de excepciones o especificar un archivo de los logs de amenazas.

Si su perfil de seguridad de WildFire Analysis está configurado para reenviar los tipos de archivo analizados mediante el AA en línea de WildFire, los falsos positivos se corrigen automáticamente a medida que se reciben. Si continúa viendo alertas de ml-virus para archivos que han sido clasificados como benignos por WildFire Analysis, comuníquese con el soporte de Palo Alto Networks.

- Añada excepciones de archivos directamente a la lista de excepciones.
  1. Seleccione **Advanced Settings (Configuración avanzada)** y **Add Exception (Añadir excepción)** en el panel **File Exceptions (Excepciones de archivo)**
  2. Añada el hash, el nombre de archivo y la descripción del archivo que desee excluir de la aplicación.



  3. Cuando haya terminado, seleccione **Save (Guardar)** sus excepciones de archivo.

STEP 4 | Debe **Save (Guardar)** la configuración de su perfil de WildFire y Antivirus y envíe los cambios de configuración.

 ©2025 Palo Alto Networks, Inc.

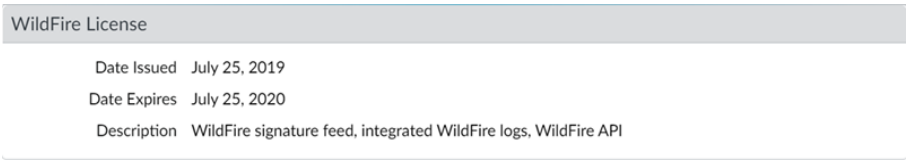
Habilite el modo de espera para la búsqueda de firma en tiempo real

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire

Puede configurar el NGFW para retener la transferencia de una muestra mientras la nube de firmas en tiempo real realiza una búsqueda de firmas. Cuando se completa la búsqueda, el archivo se entrega al cliente que lo solicita (o se bloquea), según la política de seguridad de su organización para veredictos específicos de WildFire, lo que evita la transferencia inicial de malware conocido. Puede configurar el modo de espera por perfil de antivirus y aplicar una configuración global para el tiempo de espera de búsqueda de firmas y la acción asociada.

Esta función está disponible para todos los usuarios con una licencia activa de WildFire o Advanced WildFire que ejecute PAN-OS 11.0.2 o posterior.

STEP 1 | Para habilitar el modo de espera para las búsquedas de firmas en tiempo real de WildFire, debe tener una licencia de servicio de suscripción de WildFire o Advanced WildFire. Asegúrese de activar la licencia en el cortafuegos si aún no lo ha hecho. Para verificar las suscripciones para las que tiene licencias actualmente activas, seleccione **Device (Dispositivo)** > **Licenses (Licencias)** y verifique que las licencias correspondientes se muestren y no estén vencidas. El siguiente ejemplo muestra la descripción de la licencia estándar de WildFire.



STEP 2 | Establezca el programa para que el cortafuegos recupere las firmas de WildFire en tiempo real.

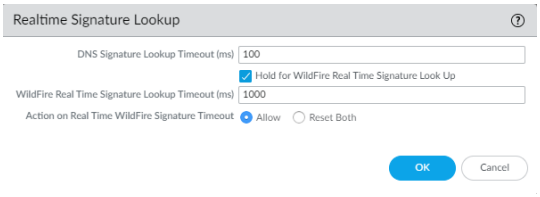
Incluso cuando el cortafuegos está configurado para usar firmas en tiempo real, los paquetes de firmas complementarias se siguen instalando de forma regular. Esto proporciona una fuente de firmas actualizada cuando experimenta problemas de conectividad, así como un beneficio de velocidad, donde las firmas están disponibles localmente.

1. Seleccione **Device (Dispositivo)** > **Dynamic Updates (Actualizaciones dinámicas)**.
2. Seleccione el **Schedule (Programa)** de actualizaciones de WildFire.
3. Establezca la **Recurrence (Recurrencia)** (la frecuencia con la que el cortafuegos comprueba si el servidor de actualizaciones de Palo Alto Networks tiene nuevas firmas) para las actualizaciones en **Real-time (Tiempo real)**.
4. Haga clic en **OK (Aceptar)** para guardar el programa de actualizaciones de WildFire y, a continuación, seleccione **Commit (Enviar)** los cambios.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Configure el ajuste de tiempo de espera y la acción cuando la solicitud supere el tiempo de espera.

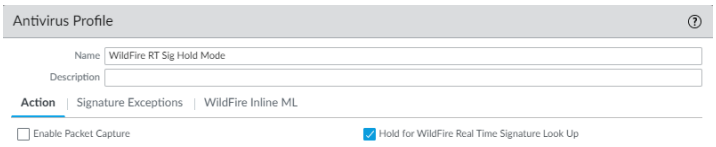
Debe habilitar el modo de espera a nivel global antes de habilitar el modo de espera para las búsquedas de firmas en tiempo real de WildFire por perfil de antivirus.



1. Seleccione **Device Setup (Configuración del dispositivo)** > **ContentID** > **Realtime Signature Lookup (Búsqueda de firma en tiempo real)**
2. Habilite **Hold for WildFire Real Time Signature Look Up (Mantener pulsado para buscar la firma en tiempo real de WildFire)**
3. Especifique el **WildFire Real Time Signature Lookup Timeout (ms) [Tiempo de espera de búsqueda de firmas en tiempo real de WildFire (ms)]** en milisegundos (el valor predeterminado es 1000).

   Palo Alto Networks recomienda utilizar el valor predeterminado de 1000 ms, a menos que experimente tiempos de espera repetidos durante las pruebas.
4. Especifique la **Action On Real Time WildFire Signature Timeout (Acción sobre el tiempo de espera de firma de WildFire en tiempo real)**. El valor predeterminado es **Allow (Permitir)**, sin embargo, Palo Alto Networks recomienda configurarlo en **Reset-Both (Restablecer ambos)** cuando el modo de espera está habilitado. Las opciones incluyen lo siguiente:
   - Permitir: el NGFW permite el paso de paquetes cuando se alcanza el umbral de tiempo de espera.
   - Restablecer ambos: el NGFW restablece la conexión tanto en el cliente como en el servidor cuando se alcanza el umbral de tiempo de espera.
5. Seleccione **OK (Aceptar)** cuando haya terminado.

STEP 4 | Actualice o cree un nuevo perfil de seguridad antivirus para habilitar el modo de espera para las consultas de firmas en tiempo real de WildFire.

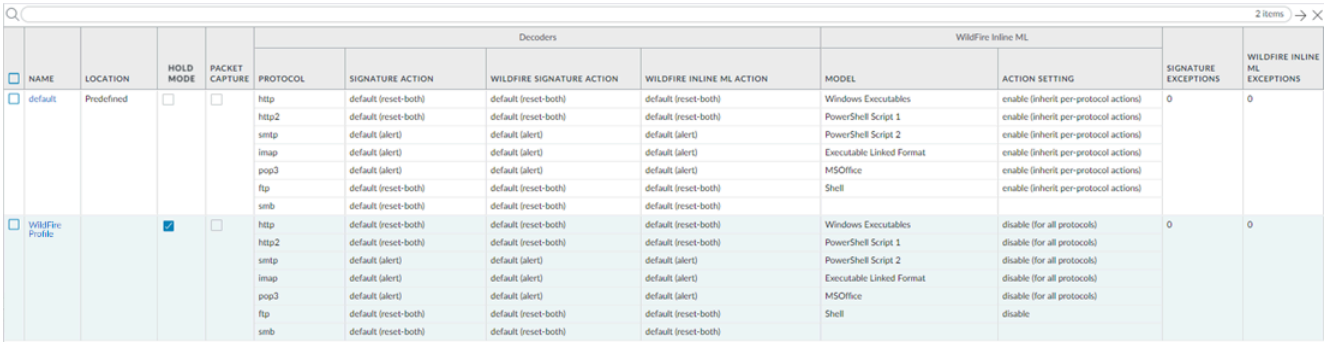


1. Seleccione un perfil de seguridad de antivirus existente o elija **Add (Añadir)** uno nuevo [**Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Antivirus**].
2. Seleccione su perfil de seguridad de antivirus y luego vaya a **Action (Acción)**.
3. Seleccione **Hold for WildFire Real Time Signature Look Up (Mantener pulsado para buscar la firma en tiempo real de WildFire)**
4. Repita los pasos 4.1-4.3 para todos los perfiles de antivirus activos para los que desee habilitar el modo de espera para las búsquedas de firmas en tiempo real de WildFire.

STEP 5 | Haga clic en **Commit (Confirmar)** para compilar los cambios.

 ©2025 Palo Alto Networks, Inc.

STEP 6 | (Opcional) Puede ver un resumen de la configuración del perfil de seguridad de su antivirus, incluida la activación del modo de espera, en la página de vista de resumen del antivirus.



					Decoders				WildFire Inline ML			
NAME	LOCATION	HOLD MODE	PACKET CAPTURE	PROTOCOL	SIGNATURE ACTION	WILDFIRE SIGNATURE ACTION	WILDFIRE INLINE ML ACTION	MODEL	ACTION SETTING	SIGNATURE EXCEPTIONS	WILDFIRE INLINE ML EXCEPTIONS
default	Predefined			http	default (reset-both)	default (reset-both)	default (reset-both)	Windows Executables	enable (inherit per-protocol actions)	0	0
				http2	default (reset-both)	default (reset-both)	default (reset-both)	PowerShell Script 1	enable (inherit per-protocol actions)		
				smtp	default (alert)	default (alert)	default (alert)	PowerShell Script 2	enable (inherit per-protocol actions)		
				imap	default (alert)	default (alert)	default (alert)	Executable Linked Format	enable (inherit per-protocol actions)		
				pop3	default (alert)	default (alert)	default (alert)	MSOffice	enable (inherit per-protocol actions)		
				ftp	default (reset-both)	default (reset-both)	default (reset-both)	Shell	enable (inherit per-protocol actions)		
				smb	default (reset-both)	default (reset-both)	default (reset-both)				
WildFire Profile		☑		http	default (reset-both)	default (reset-both)	default (reset-both)	Windows Executables	disable (for all protocols)	0	0
				http2	default (reset-both)	default (reset-both)	default (reset-both)	PowerShell Script 1	disable (for all protocols)		
				smtp	default (alert)	default (alert)	default (alert)	PowerShell Script 2	disable (for all protocols)		
				imap	default (alert)	default (alert)	default (alert)	Executable Linked Format	disable (for all protocols)		
				pop3	default (alert)	default (alert)	default (alert)	MSOffice	disable (for all protocols)		
				ftp	default (reset-both)	default (reset-both)	default (reset-both)	Shell	disable		
				smb	default (reset-both)	default (reset-both)	default (reset-both)				

 ©2025 Palo Alto Networks, Inc.

Configurar los ajustes de FQDN de nube de contenido

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire

Puede especificar el Nombre de dominio completo (FQDN) del contenido en la nube que utiliza el NGFW para gestionar las solicitudes de servicio de Advanced WildFire. El FQDN predeterminado se conecta a hawkeye.services-edge.paloaltonetworks.com y, a continuación, se resuelve en el servidor de servicios en la nube más cercano. Puede invalidar la selección automática del servidor especificando un servidor de contenido en la nube regional que mejor se adapte a sus requisitos de residencia y rendimiento de datos. tenga en cuenta que el FQDN del contenido en la nube es un recurso utilizado globalmente y afecta a la forma en que otros servicios que dependen de esta conexión envían cargas útiles de tráfico.

En algunos casos, es posible que el FQDN del contenido en la nube no sea totalmente compatible con la funcionalidad de un producto de Palo Alto Networks determinado en determinadas regiones. Compruebe que el producto es totalmente compatible antes de cambiar el FQDN del contenido en la nube.

En función de los servicios que utilice, el FQDN de contenido en la nube facilita las solicitudes de servicio de análisis, incluidas las cargas útiles de tráfico, que envían datos a los servidores en la región seleccionada. Si especifica un FQDN de nube de contenido, Content Cloud, que se encuentra fuera de su región (por ejemplo, si se encuentra en la región de la UE pero especifica el FQDN de la región APAC), puede estar infringiendo las regulaciones legales y de privacidad de su país o su organización. Consulte la documentación específica del producto para obtener información sobre cómo los productos de Palo Alto Networks utilizan el FQDN del contenido en la nube.

Si experimenta problemas de conectividad del servicio, compruebe que nadie está bloqueando el FQDN del contenido en la nube configurado.

STEP 1 | Inicie sesión en la interfaz web de PAN-OS.

©2025 Palo Alto Networks, Inc.

STEP 2 | Seleccione [**Device (Dispositivo)** > **Setup (Configuración)** > **Content-ID** > **Content Cloud Settings (Ajustes de nube de contenido)**] y cambie el FQDN como desee:

- Predeterminado: **hawkeye.services-edge.paloaltonetworks.com**
- Centro de EE. UU. (Iowa, EE. UU.): **us.hawkeye.services-edge.paloaltonetworks.com**
- Europa (Fráncfort, Alemania): **eu.hawkeye.services-edge.paloaltonetworks.com**
- APAC (Singapur): **apac.hawkeye.services-edge.paloaltonetworks.com**
- India (Mumbai): **in.hawkeye.services-edge.paloaltonetworks.com**
- Reino Unido (Londres, Inglaterra): **uk.hawkeye.services-edge.paloaltonetworks.com**
- Francia (París, Francia): **fr.hawkeye.services-edge.paloaltonetworks.com**
- Japón (Tokio, Japón): **jp.hawkeye.services-edge.paloaltonetworks.com**
- Australia (Sídney, Australia): **au.hawkeye.services-edge.paloaltonetworks.com**
- Canadá (Montreal, Canadá): **ca.hawkeye.services-edge.paloaltonetworks.com**
- Suiza: **ch.hawkeye.services-edge.paloaltonetworks.com**
- Países Bajos: **nl.hawkeye.services-edge.paloaltonetworks.com**
- Indonesia: **id.hawkeye.services-edge.paloaltonetworks.com**
- Catar: **qa.hawkeye.services-edge.paloaltonetworks.com**
- Taiwán: **tw.hawkeye.services-edge.paloaltonetworks.com**
- Polonia: **pl.hawkeye.services-edge.paloaltonetworks.com**
- Corea del Sur (Seúl, Corea del Sur): **kr.hawkeye.services-edge.paloaltonetworks.com**
- Arabia Saudita: **sa.hawkeye.services-edge.paloaltonetworks.com**
- Italia. **it.hawkeye.services-edge.paloaltonetworks.com**

STEP 3 | Haga clic en **OK (Aceptar)**.

 ©2025 Palo Alto Networks, Inc.

Verificar envíos de muestra

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire

Compruebe su implementación usando muestras de prueba de malware y también verifique que el cortafuegos esté enviando correctamente los archivos para el análisis de WildFire.

- Test con un archivo de malware de prueba
- Verificación del reenvío de archivos

Test con un archivo de malware de prueba

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia de Advanced WildFire o WildFire

Palo Alto Networks proporciona archivos de malware de muestra que puede utilizar para probar una configuración de Advanced WildFire. Siga los pasos a continuación para descargar la muestra de prueba de malware, verificar que el archivo se esté enviando correctamente para el análisis de Advanced WildFire y visualizar los resultados del análisis.

©2025 Palo Alto Networks, Inc.

STEP 1 | Descargue uno de los archivos de prueba de malware. Puede seleccionar entre PE, APK, MacOSX y ELF.

> *Antes de descargar un archivo de malware de muestra de WildFire cifrado, debe deshabilitar temporalmente la entrada * .wildfire.paloaltonetworks.com de la lista de exclusión de descifrado en la página* ***Device (Dispositivo) > Certificate Management (Gestión de certificados) > SSL Decryption Exclusion (Exclusión del descifrado SSL)****. De lo contrario, la muestra no se descargará correctamente. Después de realizar una prueba de verificación, asegúrese de volver a habilitar la entrada *.wildfire.paloaltonetworks.com en la página de exclusión de descifrado SSL.*

- Si el cifrado SSL está habilitado en el cortafuegos, utilice una de las siguientes URL:
  - PE: https://wildfire.paloaltonetworks.com/publicapi/test/pe
  - APK: https://wildfire.paloaltonetworks.com/publicapi/test/apk
  - MacOSX: https://wildfire.paloaltonetworks.com/publicapi/test/macos
  - ELF: wildfire.paloaltonetworks.com/publicapi/test/elf
- Si el cifrado SSL *no* está habilitado en el cortafuegos, utilice una de las siguientes URL:
  - PE: http://wildfire.paloaltonetworks.com/publicapi/test/pe
  - APK: http://wildfire.paloaltonetworks.com/publicapi/test/apk
  - MacOSX: http://wildfire.paloaltonetworks.com/publicapi/test/macos
  - ELF: wildfire.paloaltonetworks.com/publicapi/test/elf

El archivo de prueba se denomina wildfire-test-*file_type*-file.exe y cada archivo de prueba posee un valor de hash SHA-256 único.

> *También puede utilizar la API de WildFire para recuperar el archivo de prueba de malware. Para más información, consulte la* Referencia de la API de WildFire.

STEP 2 | En la interfaz web del cortafuegos, seleccione **Monitor (Supervisar)** > **WildFire Submissions (Envíos de WildFire)** para confirmar que el archivo se ha reenviado para el análisis.

Espere al menos cinco minutos hasta que los resultados del análisis del archivo se muestren en la página **WildFire Submissions (Envíos de WildFire)**. El veredicto del archivo de prueba siempre se mostrará como malware.

Verificación del reenvío de archivos

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia de Advanced WildFire o WildFire

 ©2025 Palo Alto Networks, Inc.

Después de configurar el cortafuegos para el Reenviar archivos para Advanced WildFire Analysis, utilice las siguientes opciones para verificar la conexión entre el cortafuegos y la nube pública de Advanced WildFire o nube privada de WildFire, y para supervisar el reenvío de archivos.

Varias de las opciones para verificar que un cortafuegos esté enviando muestras para el análisis son comandos de CLI. Para obtener detalles sobre cómo comenzar y usar la CLI, consulte la Guía de inicio rápido de la CLI de PAN-OS.

- Verifique el estado de la conexión del cortafuegos a la nube pública de Advanced WildFire o nube privada de WildFire, incluida la cantidad total de archivos reenviados por el cortafuegos para el análisis.

  Utilice el comando **`show wildfire status`** para lo siguiente:

  - Comprobar el estado de la nube pública de Advanced WildFire a la nube privada de WildFire a la cual el cortafuegos está conectado. El estado de inactividad `Idle` indica que la nube de Advanced WildFire (pública o privada) está lista para recibir los archivos para el análisis.
  - Confirme los límites de tamaño configurados para los archivos reenviados por el cortafuegos (**Device (Dispositivo)** > **Setup (Configuración)** > **WildFire**).
  - Supervise el reenvío de archivos, incluido el recuento total de archivos reenviados por el cortafuegos para el análisis. Si el cortafuegos está en una implementación de nube híbrida de WildFire, la

 ©2025 Palo Alto Networks, Inc.

cantidad de archivos reenviados a la nube pública de WildFire y la nube privada de WildFire también se muestran.

El siguiente ejemplo muestra el resultado de `show wildfire status` para un cortafuegos en una implementación de nube privada de WildFire:

```
admin@VM-FW> show wildfire status

Connection info:
  Signature verification:            enable
  Server selection:                  enable
  File cache:                        enable
WildFire Public Cloud:
  Server address:                    wildfire.paloaltonetworks.com
  Status:                            Disabled due to configuration
  Best server:
  Device registered:                 no
  Through a proxy:                   no
  Valid wildfire license:            yes
  Service route IP address:          X.X.X.X
WildFire Private Cloud:
  Server address:                    X.X.X.X
  Status:                            Idle
  Best server:                       X.X.X.X:XXXXX
  Device registered:                 yes
  Through a proxy:                   no
  Valid wildfire license:            yes
  Service route IP address:          X.X.X.X
File size limit info:
  pe                                 9 MB
  apk                                49 MB
  pdf                                1000 KB
  ms-office                          9500 KB
  jar                                9 MB
  flash                              10 MB
  MacOSX                             1 MB
Forwarding info:
  file idle time out (second):       90
  total concurrent files:            0
  Public Cloud:
    total file forwarded:            0
    file forwarded in last minute:   0
    concurrent files:                0
  Private Cloud:
    total file forwarded:            0
    file forwarded in last minute:   0
    concurrent files:                0
```

Para ver la información de envío para la nube pública de Advanced WildFire o nube privada de WildFire únicamente, use los siguientes comandos:

- **`show wildfire status channel public`**
- **`show wildfire status channel private`**

 ©2025 Palo Alto Networks, Inc.

- Visualice las muestras enviadas por el cortafuegos de acuerdo con el tipo de archivo (incluidos los enlaces de correo electrónico).

  *Utilice esta opción para confirmar que los enlaces de correo electrónico se reenvían para el análisis, ya que solo los enlaces de correo electrónico que reciben un veredicto de malintencionado o phishing se registran como entradas de **WildFire Submissions (Envíos de WildFire)** en el cortafuegos, incluso si está habilitado el registro de muestras benignas y de grayware. Esto se debe a la gran cantidad de entradas de envíos de WildFire que se registrarían para los enlaces de correo electrónicos benignos.*

  Use el comando **`show wildfire statistics`** para confirmar los tipos de archivos que se reenvían a la nube pública de Advanced WildFire o nube privada de Wildfire:

  - El comando muestra el resultado de un cortafuegos en funcionamiento y muestra los contadores para cada tipo de archivo que el cortafuegos reenvía para su análisis. Si el campo de un contador muestra 0, el cortafuegos no está reenviando ese tipo de archivo.
  - Confirme que los enlaces de correo electrónico se estén reenviando para el análisis al comprobar que los siguientes contadores no muestren cero:
  - `FWD_CNT_APPENDED_BATCH`: indica el número de enlaces de correo electrónico agregados a un lote que espera cargarse en una nube pública de Advanced WildFire o nube privada de WildFire.
  - `FWD_CNT_LOCAL_FILE`: indica el número total de enlaces de correo electrónico cargados en una nube pública de Advanced WildFire o privada de WildFire.

- Verifique que una muestra específica haya sido reenviada por el cortafuegos y compruebe el estado de esa muestra.

  Esta opción puede ser útil al resolver problemas para:

  - Confirmar que las muestras que aún no recibieron un veredicto hayan sido reenviadas correctamente por el cortafuegos. Debido a que los **WildFire Submissions (Envíos de WildFire)** se registran en el cortafuegos únicamente cuando el análisis se completa y la muestra ha recibido un veredicto, use esta opción para verificar que el cortafuegos haya enviado una muestra que actualmente está siendo analizada.
  - Realice el seguimiento del estado para un único archivo o para el enlace de correo electrónico permitido de acuerdo con su política de seguridad, cotejado con un perfil de WildFire Analysis y luego reenviado para su análisis.
  - Compruebe que un cortafuegos en una implementación de nube híbrida reenvíe los tipos de archivos correctos y los enlaces de correo electrónico a la nube pública de Advanced WildFire o a una nube privada de WildFire.

  Ejecute los siguientes comandos de CLI en el cortafuegos para ver muestras que el cortafuegos ha enviado para su análisis:

  - Vea todas las muestras reenviadas por el cortafuegos mediante el comando de CLI **`debug wildfire upload-log`**.
  - Vea solo las muestras reenviadas a la nube pública de Advanced WildFire mediante el comando de CLI **`debug wildfire upload-log channel public`**.

 ©2025 Palo Alto Networks, Inc.

- Vea solo las muestras reenviadas a la nube privada de WildFire mediante el comando de CLI **`debug wildfire upload-log channel private`**.

El siguiente ejemplo muestra el resultado para los tres comandos enumerados anteriormente cuando se emiten en un cortafuegos de una implementación de nube pública de Advanced WildFire:

```
user@firewall> debug wildfire upload-log
+ channel   WildFire channel (Public/Private)
  |         Pipe through a command
  <Enter>   Finish input

user@firewall> debug wildfire upload-log channel private

Private Cloud upload logs:


user@firewall> debug wildfire upload-log channel public

Public Cloud upload logs:

    log: 0, filename: support-login.swf
    processed 353590 seconds ago, action: skipped - remote benign dup
    vsys_id:  1, session_id: 169651, transaction_id: 261
    file_len:  91536, flag: 0x81c, file type: flash
    threat id: 52145, user_id: 1238, app_id: 872
    from XX.XX.XX.XX/XXXX to XX.XXX.XXX.XXX/XXX
    SHA256: 6b2f1a23407ab2db9a17ccdf686bacc6dad7d2489c65ba90dbdf02508b3d4efd

    log: 1, filename: G2M_D_because_12.03.2014_300x250.swf
    processed 611505 seconds ago, action: skipped - remote benign dup
    vsys_id:  1, session_id: 259049, transaction_id: 260
    file_len:  39206, flag: 0x81c, file type: flash
    threat id: 52145, user_id: 20583, app_id: 872
    from XX.XX.XX.XX/XXXXX to XXX.XX.XXX.XXX/XX
    SHA256: cd52d1b7a7521a14237c1531edb109627fee084806a300d907b57322b1efd6e7
```

- Supervise las muestras enviadas correctamente para su análisis.

  Utilizando la interfaz web del cortafuegos, seleccione **Monitor (Supervisar)** > **Logs (Logs)** > **WildFire Submissions (Envíos de WildFire)**. Todos los archivos reenviados por un cortafuegos a la nube pública de Advanced WildFire o nube privada de WildFire para el análisis se registran en la página de envíos de WildFire.

  - Compruebe el veredicto para obtener una muestra:

    De forma predeterminada, solo las muestras que reciben veredictos maliciosos o de phishing se muestran como **entradas de envíos** de WildFire. Para habilitar el registro de muestras benignas y/o grayware, seleccione **Device** > **Setup** > **WildFire** > **Report Benign Files/Report Grayware Files**.

    *Habilite el registro de archivos benignos como un paso rápido de solución de problemas para verificar que el cortafuegos está reenviando archivos. Compruebe los logs de **WildFire Submissions (Envíos de WildFire)** para verificar que los archivos se estén reenviando para el análisis y que estén recibiendo veredictos (en este caso, un veredicto benigno).*

  - La columna

    WildFire Cloud (Nube de WildFire) muestra la ubicación a la cual se envió el archivo y en la que se analizó. Esto es útil cuando se implementa una nube híbrida

    .

 ©2025 Palo Alto Networks, Inc.

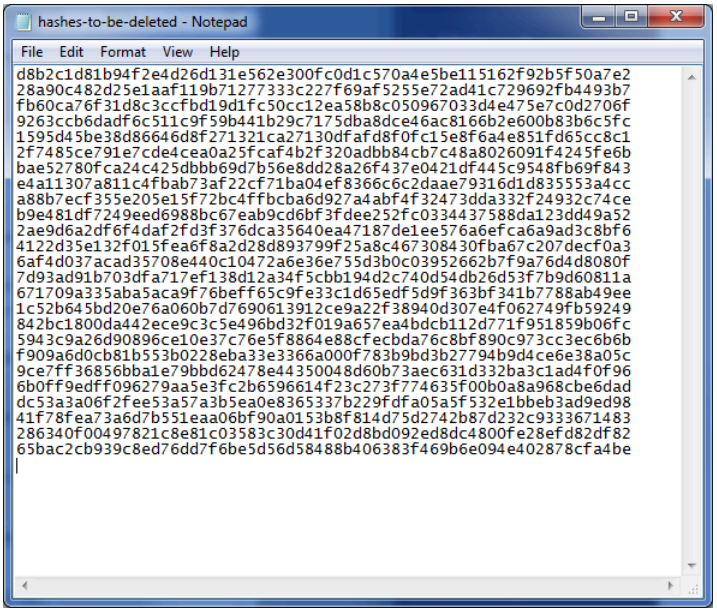
Solicitud de eliminación de muestras

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

Las muestras únicas que se envían a la nube de Advanced WildFire para el análisis pueden eliminarse a discreción del usuario. Esto permite que los usuarios sujetos a las políticas de detección de datos, incluso a aquellos que deben seguir la política GDPR, puedan eliminar permanentemente los datos de las muestras según las políticas de conservación de su organización. Los datos de muestra incluyen datos de la sesión/carga y el archivo de muestra.

STEP 1 | Cree un archivo de texto con una lista de hashes SHA256 o MD5 de las muestras que se eliminarán. Cada hash debe estar en una línea individual en el archivo y puede incluir hasta 100 muestras.

Solo se pueden eliminar los archivos únicos en su entorno. Si los archivos están disponibles en otras fuentes públicas o privadas, solo se eliminan los datos de la sesión y la carga de una cuenta determinada.

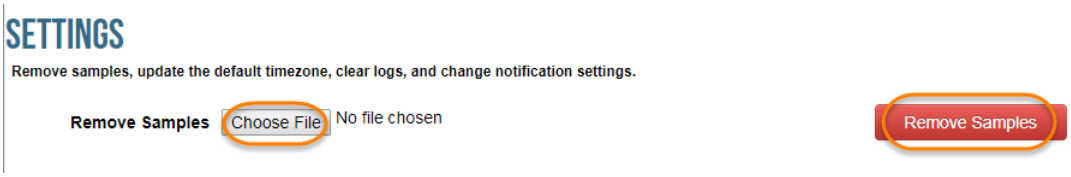


STEP 2 | Inicie sesión en el portal de WildFire con las credenciales de asistencia técnica de Palo Alto Networks o su cuenta de WildFire.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Seleccione **Settings (Configuración)** en la barra del menú.

STEP 4 | Haga clic en **Choose File (Seleccionar archivo)** y seleccione el archivo de texto con la lista de hash que creó en el paso 1 y seleccione **Remove Samples (Eliminar muestras)**. Tras una carga de archivos correcta, recibirá una confirmación.



STEP 5 | Una vez las muestras se eliminen de la nube de WildFire, recibirá un correo electrónico de confirmación con los detalles de la solicitud. Esto incluye una lista de las muestras para las que se solicitó la eliminación y el estado de eliminación de cada muestra. El proceso puede tardar hasta 7 días.

```
Dear WildFire customer,
your request for removal of samples from WildFire cloud has been completed. In total 1 samples were removed from WildFire,
the following table shows removal status for each individual sample hash

+------------------------------------------------------------------+----------+---------------------+
| Hash                                                             |  Status  |      Information    |
+------------------------------------------------------------------+----------+---------------------+
|6d2ef9f79b5b81429cb1ffeebd6b2919a9a84ec0cc0e5023cbf45a68967c6e1c  | Deleted  ||                    |
+------------------------------------------------------------------+----------+---------------------+
```

*Las muestras que no existen o no son únicas en su entorno tendrán el estado **Not found (No encontrado)** y **Rejected (Rechazado)**, respectivamente.*

 ©2025 Palo Alto Networks, Inc.

Capacidad de reenvío de archivos del cortafuegos según el modelo

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES	❑ Licencia avanzada de WildFire

La capacidad de reenvío de archivos es la velocidad máxima por minuto a la que cada modelo de cortafuegos de Palo Alto Networks puede enviar archivos a la nube de Advanced WildFire® para el análisis. Si el cortafuegos alcanza el límite por minuto, coloca en cola las muestras restantes.

En la columna Reserved Drive Space (Espacio de unidad reservado) de la siguiente tabla se indica la cantidad de espacio de la unidad del cortafuegos reservada para poner en cola los archivos. Si el cortafuegos alcanza el límite de espacio en la unidad, cancela el reenvío de nuevos archivos a WildFire hasta que haya más espacio disponible en la cola.

La velocidad a la que el cortafuegos puede reenviar archivos a la nube de Advanced WildFire también depende del ancho de banda de enlace de envío del cortafuegos.

Zero Trust	Número máximo de archivos por minuto	Espacio de unidad reservado
VM-50	5	100MB
VM-100	10	100MB
VM-200	15	200MB
VM-300	25	200MB
VM-500	30	250MB
VM-700	40	250MB
PA-220	20	100MB
PA-400	20	100MB
PA-820	75	300MB
PA-850	75	300MB
PA-1400 Series	20	100MB

©2025 Palo Alto Networks, Inc.

Zero Trust	Número máximo de archivos por minuto	Espacio de unidad reservado
PA-3220	100	200MB
PA-3250/3260	100	500MB
Serie PA-3400	100	500MB
PA-5200 Series	250	1500MB
Serie PA-5400	250	1500MB
PA-7000 Series	300	1GB

©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

Supervisar actividad

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

Según su implementación de WildFire™ (nube pública, privada o híbrida), puede ver muestras enviadas a WildFire y resultados de análisis para cada muestra utilizando el portal de WildFire, accediendo al cortafuegos que envió la muestra (o Panorama, si gestiona centralmente varios cortafuegos) o mediante el uso de la API de WildFire.

Una vez que WildFire ha analizado una muestra y enviado un veredicto de malintencionado, phishing, grayware o benigno, se genera un informe detallado para la muestra. Los informes de análisis de WildFire visualizados en el cortafuegos que envió la muestra también incluyen datos de la sesión durante la cual se detectó la muestra. En el caso de las muestras identificadas como malware, el informe de análisis de WildFire incluye detalles sobre las firmas de WildFire existentes que pueden estar relacionadas con el malware identificado recientemente e información sobre los atributos del archivo, su comportamiento y la actividad que indicaban que la muestra era malintencionada.

También puede ver cómo Advanced WildFire se integra con otras aplicaciones y servicios de seguridad de Palo Alto Networks para proteger a su organización de amenazas, así como obtener una vista de alto nivel del estado operativo general de su implementación, a través del Centro de control de Strata Cloud Manager. El centro de control funciona como su página de inicio de NetSec y proporciona un resumen completo de la salud, la seguridad y la eficacia de su red, en un panel visual interactivo con múltiples facetas de datos para una evaluación fácil y rápida.

Dependiendo de la plataforma del producto, puede acceder a paneles de alto nivel que proporcionan estadísticas avanzadas de detección de malware de Advanced WildFire, así como tendencias de uso, incluido el contexto de la actividad de la red en forma de información de análisis y más.

Palo Alto Networks proporciona varios métodos para supervisar la actividad de Advanced WildFire:

- Centro de control de Strata Cloud Manager
- Panel de Advanced WildFire
- Acerca de los logs e informes de WildFire
- Configuración de los ajustes del log de envíos a WildFire.
- Uso del portal de WildFire para supervisar el malware
- Informes de análisis de WildFire: Detallados
- Configuración de alertas para el malware

Acerca de los logs e informes de WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

Puede Supervisar actividaden el cortafuegos con el portal de WildFire, Strata Cloud Manager o con la API de WildFire.

Para cada muestra que WildFire analiza, WildFire clasifica la muestra como malware, phishing, grayware o benigno, y detalla la información y el comportamiento de la muestra en el informe de análisis de WildFire. Se puede acceder a los informes de análisis de WildFire en el cortafuegos que envió la muestra y la nube de WildFire (pública o privada) que analizó la muestra, o se pueden recuperar usando la API de WildFire:

- En el cortafuegos: todas las muestras enviadas por un cortafuegos para el análisis de WildFire se registran como entradas de envíos de WildFire. La columna Acción en el log de envíos de WildFire indica si el cortafuegos permitió o bloqueó un archivo. Para cada entrada de envío de WildFire, puede abrir una vista de log detallado para visualizar el informe de análisis de WildFire para la muestra o para descargar el informe como PDF.
- En el portal de WildFire: supervise la actividad de WildFire, incluso el informe de análisis de WildFire para cada muestra, que también puede descargarse como PDF. En una implementación de nube privada de WildFire, el portal de WildFire proporciona detalles de las muestras que se cargan manualmente en el portal y las muestras enviadas por un dispositivo WildFire con la inteligencia de nube habilitada.

  La opción para ver informes de análisis de WildFire en el portal solo es compatible para dispositivos WildFire con la función de inteligencia de nube habilitada.
- En Strata Cloud Manager: todas las muestras enviadas por Prisma Access para el análisis de WildFire se registran como logs de WildFire y se pueden examinar a través del Visor de logs de Strata Cloud Manager. Puede ver los detalles del tráfico, el contexto y otros detalles relevantes, incluyendo información sobre cómo progresó la muestra a través de su red.
- Con la API de WildFire: recupere informes de análisis de WildFire desde un dispositivo WildFire o desde la nube pública de WildFire.

©2025 Palo Alto Networks, Inc.

Informes de Advanced WildFire Analysis: Detallados

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire

Acceda a los informes de análisis de Advanced WildFire en el cortafuegos, el portal de WildFire y la API de WildFire.

En los informes del análisis de Advanced WildFire, se muestra información detallada de la muestra, además de información sobre los usuarios de destino, información del encabezado de correo electrónico (si está habilitado), la aplicación que entregó el archivo y todas las URL involucradas en la actividad de comando y control del archivo. Los informes de Advanced WildFire contendrán parte o la totalidad de la información descrita en la siguiente tabla según la información de sesión configurada en el cortafuegos que reenvió el archivo, y también en función del comportamiento observado.

Al visualizar un informe de Advanced WildFire para un archivo que se ha cargado manualmente en el portal de WildFire o mediante la API de WildFire, el informe no mostrará información de sesión, ya que el tráfico no ha atravesado el cortafuegos. Por ejemplo, el informe no mostraría atacante/origen ni víctima/destino.

Encabezado del informe	Description (Descripción)

Información del archivo	• **File Type (Tipo de archivo)**: Flash, PE, PDF, APK, JAR/Class, archivo de almacenamiento, linux, script o MS Office. Este campo se llama URL en el caso de informes de enlaces de correo electrónico HTTP/HTTPS y mostrará la URL analizada.
	• **File Signer (Firmante del archivo)**: entidad que firmó el archivo con el fin de autenticarlo.
	• **Hash Value (Valor hash)**: un archivo hash es muy similar a una huella digital, que identifica exclusivamente un archivo para garantizar que este no se ha modificado de ninguna forma. A continuación, se enumeran las versiones hash que genera WildFire para cada archivo analizado:
	  • **SHA-1**: Muestra la información SHA-1 del archivo.
	  • **SHA-256**: muestra la información SHA-256 del archivo.
	  • **MD5**: muestra la información MD5 del archivo.
	• **File Size (Tamaño del archivo)**: tamaño (en bytes) del archivo que analizó WildFire.
	• **First Seen Timestamp (Marca de tiempo de primera visualización)**: si el sistema WildFire ha analizado el

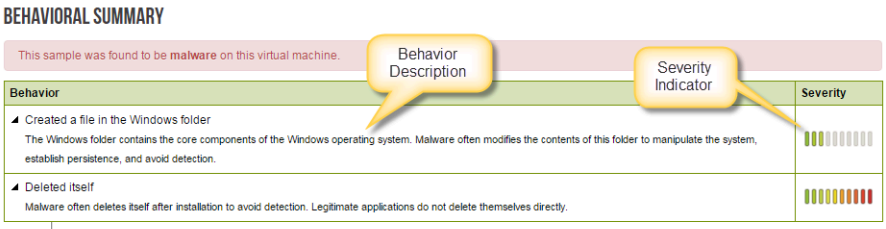
 ©2025 Palo Alto Networks, Inc.

Encabezado del informe	Description (Descripción)
	archivo anteriormente, esta es la fecha/hora en la que se visualizó por primera vez. • **Verdict (Veredicto)**: muestra los veredictos del análisis. • **Sample File (Archivo de muestra)**: haga clic en el enlace **Download File (Descargar archivo)** para descargar el archivo de muestra a su sistema local. Tenga en cuenta que solo puede descargar archivos con el veredicto de malware, no los benignos.
Estado de la cobertura	Haga clic en el enlace **Virus Total** para ver información de cobertura antivirus en el extremo y muestras que ya han sido identificadas por otros proveedores. Si ninguno de los proveedores enumerados ha detectado nunca antes el archivo, se indicará que no se ha encontrado el archivo (file not found). Asimismo, si el informe se presenta en el cortafuegos, la información actualizada acerca de la firma y la cobertura de filtrado de URL que Palo Alto Networks proporciona actualmente para proteger contra amenazas también se muestra en esta sección. Dado que esta información se recupera dinámicamente, no aparecerá en el informe en PDF. La siguiente información de cobertura es proporcionada para firmas activas: • **Coverage Type (Tipo de cobertura)**: el tipo de protección proporcionada por Palo Alto Networks (virus, DNS, WildFire o URL de malware). • **Signature ID (ID de firma)**: se asigna un número de ID único a cada firma que proporciona Palo Alto Networks. • **Detail (Detalle)**: el nombre conocido del virus. • **Date Released (Fecha de publicación)**: la fecha en que Palo Alto Networks publicó la cobertura para protegerse contra el malware. • **Content Version (Versión del contenido)**: el número de versión para la publicación de contenido que ofrece protección contra el malware.
Session information (Información de la sesión)	Contiene información de sesión basada en el tráfico que atraviesa el cortafuegos que reenvió la muestra. Para definir la información de la sesión que WildFire incluirá en los informes, seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **WildFire** > **Session Information Settings (Configuración de información de la sesión)**. Las siguientes opciones están disponibles: • IP de origen

 ©2025 Palo Alto Networks, Inc.

Encabezado del informe	Description (Descripción)
	• Puerto de origen • IP de destino • Puerto de destino • Sistema virtual (si VSYS múltiple está configurado en el cortafuegos) • Application (Aplicación) • Usuario (si ID de usuario está configurado en el cortafuegos) • URL • Filename • Remitente de correo electrónico • Destinatario de correo electrónico • Asunto del mensaje de correo electrónico De manera predeterminada, la información de la sesión incluye el campo Status (Estado), que indica si el cortafuegos permitió o bloqueó la muestra.
Análisis dinámico	Si un archivo tiene un riesgo bajo y WildFire puede determinar fácilmente que es seguro, solo se realiza un análisis estático en lugar de un análisis dinámico. Cuando se realiza un análisis dinámico, esta sección contiene pestañas que muestran los resultados del análisis para cada tipo de entorno en el que se ejecutó la muestra. Por ejemplo, la pestaña Máquina virtual 4 puede mostrar un entorno de análisis que ejecuta Windows 7, Adobe Reader 11, Flash 11 y Office 2010. *En el dispositivo WildFire, solo se utiliza una máquina virtual para el análisis, que se debe seleccionar en función de los atributos de entorno de análisis que más se adapten a su entorno local. Por ejemplo, si la mayoría de los usuarios tiene Windows 7 de 32 bits, se seleccionaría dicha máquina virtual.*
Resumen de comportamientos	Cada pestaña de máquina virtual resume el comportamiento del archivo de muestra en el entorno específico. Algunos ejemplos son si la muestra ha creado o modificado archivos, iniciado un proceso, generado procesos nuevos, modificado el registro o instalado objetos de ayuda del explorador. La columna Severity (Gravedad) indica la gravedad de cada comportamiento. El indicador de gravedad mostrará una barra

 ©2025 Palo Alto Networks, Inc.

Encabezado del informe	Description (Descripción)
	para gravedad baja y varias barras para niveles de gravedad más altos. Esta información también se añade a las secciones de análisis dinámico y estático.  A continuación, se describen los distintos comportamientos que se analizan: • **Network Activity (Actividad de red)**: muestra la actividad de la red realizada por la muestra, como el acceso a otros hosts de la red, consultas DNS y la actividad de llamada a casa. Se proporciona un enlace para descargar la captura de paquete. • **Host Activity (by process) (Actividad del host [por proceso])**: enumera las actividades realizadas en el host, tales como claves de registro que se han establecido, modificado o eliminado. • **Process Activity (Actividad de proceso)**: muestra archivos que han empezado un proceso principal, el nombre del proceso y la acción que ha realizado el proceso. • **File (Archivo)**: muestra archivos que han empezado un proceso secundario, el nombre del proceso y la acción que ha realizado el proceso. • **Mutex (Exclusión mutua)**: si el archivo de muestra genera otros hilos de ejecución de programa, en este campo se registran el nombre del mutex y el proceso principal se registran en este campo. • **Activity Timeline (Línea temporal de actividad)**: proporciona una lista por reproducción de toda la actividad registrada de la muestra. Esto ayudará a comprender la secuencia de eventos que se produjeron durante el análisis. *La información de línea temporal de actividad solamente está disponible en la exportación a PDF de los informes de WildFire.*
Envío de malware	Use esta opción para enviar manualmente la muestra a Palo Alto Networks. La nube de WildFire volverá a analizar la muestra y generará firmas si determina que la muestra es

 ©2025 Palo Alto Networks, Inc.

Encabezado del informe	Description (Descripción)
	malintencionada. Esto es útil en un dispositivo WildFire que no tiene generación de firmas o inteligencia de nube habilitadas y se utiliza para reenviar malware desde el dispositivo a la nube de WildFire.
Informe de veredicto incorrecto	Haga clic en este enlace para enviar la muestra al equipo de amenazas de Palo Alto Networks si cree que el veredicto es un falso positivo o un falso negativo. El equipo de amenazas realizará más análisis en la muestra para determinar si debería volver a clasificarse. Si se determina que una muestra de malware es segura, la firma del archivo se deshabilita en una actualización de firma de antivirus futura o, si se determina que un archivo benigno es malintencionado, se genera una nueva firma. Una vez completada la investigación, recibirá un mensaje de correo electrónico donde se describe la acción que se ha realizado.

©2025 Palo Alto Networks, Inc.

Configuración de los ajustes del log de envíos a WildFire.

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire

Un log de envíos de WildFire es un archivo con marca de tiempo generado automáticamente que proporciona una pista de auditoría para realizar seguimientos de eventos cuando una plataforma de seguridad de red de Palo Alto Networks reenvía muestras (enlaces de archivos y correos electrónicos) a la nube de WildFire para su análisis basado en la configuración del perfil de WildFire Analysis (Objetos > Perfiles de seguridad > WildFire Analysis). Se generan entradas de log de envíos de WildFire para cada muestra enviada a la nube de WildFire que ha completado el análisis estático y/o dinámico de la muestra. Las entradas del registro de envíos de WildFire incluyen la acción tomada en la muestra (permitir o bloquear), el veredicto de WildFire para la muestra enviada, según lo determina el análisis de WildFire, el nivel de gravedad de la muestra y otros detalles.

De forma predeterminada, los logs de envíos de WildFire se crean para muestras benignas y maliciosas, mientras que las muestras de grayware y benignas no generan logs. Puede cambiar la configuración del log de envíos de WildFire para incluir muestras de grayware y benignas, así como información de sesión adicional contenida en los enlaces de correo electrónico.

Habilite las siguientes opciones para los logs de **WildFire Submissions (Envíos de WildFire)**

- Habilitación del registro de muestras benignas y grayware
- Inclusión de información de encabezados de correo electrónico en logs e informes de WildFire

Habilitación del registro de muestras benignas y grayware

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire

El registro de muestras benignas y grayware está deshabilitado de manera predeterminada. Los enlaces de correo electrónico que reciben veredictos benignos o de grayware no se registran.

STEP 1 | Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **WildFire** y modifique **General Settings (Configuración general)**.

STEP 2 | Seleccione **Report Benign Files (Informar archivos benignos)** o **Report Grayware Files (Informar archivos de grayware)**, y haga clic en **OK (Aceptar)** para guardar la configuración.

 ©2025 Palo Alto Networks, Inc.

Inclusión de información de encabezados de correo electrónico en logs e informes de WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire

Siga los pasos a continuación para incluir información de encabezados de correo electrónico (remitente, destinatario y asunto de correo electrónico) en logs e informes de WildFire.

La información de la sesión se reenvía a la nube de WildFire junto con la muestra y se utiliza para generar el informe de análisis de WildFire. Ni el cortafuegos ni la nube de WildFire reciben, almacenan o visualizan el contenido real del correo electrónico.

La información de sesión puede ayudar a rastrear y solucionar rápidamente las amenazas detectadas en documentos adjuntos o enlaces de correo electrónico, incluso a identificar los destinatarios que han descargado o han accedido al contenido malintencionado.

STEP 1 | Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **WildFire**.

STEP 2 | Modifique la sección Ajustes de información de sesión y habilite una o más de las opciones (**Email sender (Remitente del correo electrónico)**, **Email recipient (Destinatario del correo electrónico)** y **Email subject (Asunto del correo electrónico)**).

STEP 3 | Haga clic en **OK (Aceptar)** para guardar.

 ©2025 Palo Alto Networks, Inc.

Configuración de alertas para el malware

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire

Puede configurar un cortafuegos de Palo Alto Networks para enviar una alerta cada vez que WildFire identifica una muestra malintencionada o de phishing. Puede configurar alertas para archivos benignos también, pero no para enlaces de correos electrónicos benignos y grayware. Este ejemplo describe cómo configurar una alerta de correo electrónico; sin embargo, también puede configurar el reenvío de logs para establecer el envío de alertas a través de syslog, traps SNMP o Panorama.

STEP 1 | Configure un perfil del servidor de correo electrónico.

1. Seleccione **Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** > **Email (Correo electrónico)**.
2. Haga clic en **Add** (Añadir) y, a continuación, introduzca un **Name** (Nombre) para el perfil. Por ejemplo, WildFire-Email-Profile.
3. (Opcional) Seleccione el sistema virtual al que se aplica este perfil en el menú desplegable **Location (Ubicación)**.
4. Haga clic en **Add (Añadir)** para añadir un nuevo servidor de correo electrónico e introduzca la información necesaria para conectarse al servidor de protocolo simple de transferencia de correo (SMTP) y enviar mensajes de correo electrónico (puede añadir hasta cuatro servidores de correo electrónico al perfil):
   - **Server (Servidor)**: nombre para identificar el servidor de correo (1-31 caracteres). Este campo es solamente una etiqueta y no tiene que ser el nombre de host de un servidor SMTP existente.
   - **Display Name (Nombre para mostrar)**: el nombre que aparecerá en el campo From (De) del correo electrónico.
   - **From (De)**: la dirección de correo electrónico desde la que se envían las notificaciones de correo electrónico.
   - **To (Para)**: la dirección de correo electrónico a la que se envían las notificaciones de correo electrónico.
   - **Additional Recipient(s) (Destinatarios adicionales)**: introduzca una dirección de correo electrónico para enviar notificaciones a un segundo destinatario.
   - **Gateway (Puerta de enlace)**: la dirección IP o el nombre de host de la puerta de enlace SMTP que se usará para enviar los mensajes de correo electrónico.
5. Haga clic en **OK (Aceptar)** para guardar el perfil de servidor.
6. Haga clic en **Commit (Confirmar)** para guardar los cambios en la configuración en curso.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Configure un perfil de servidor de correo electrónico.

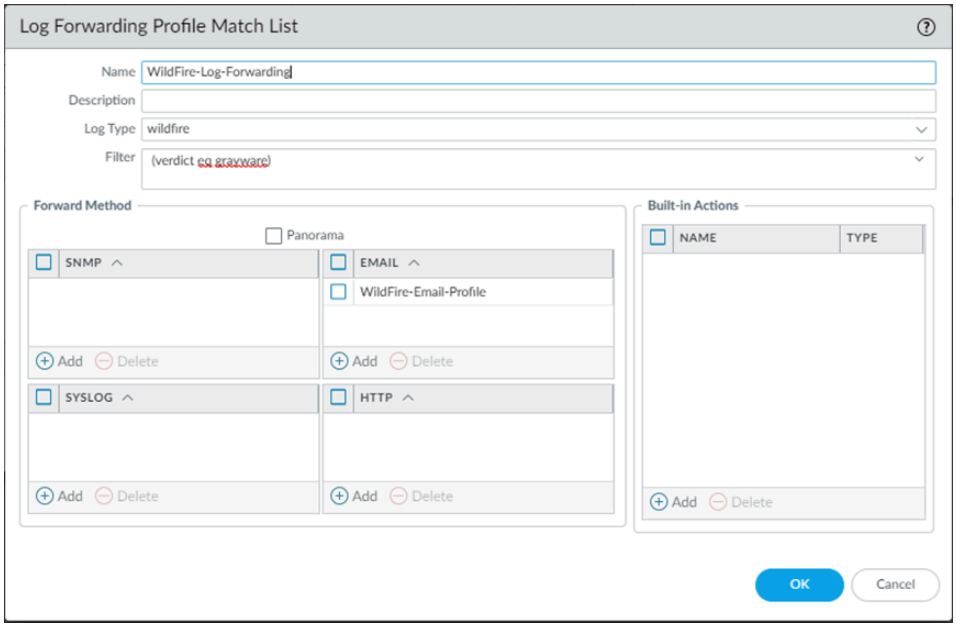
1. Seleccione **Monitor (Supervisar)** > **PDF Reports (Informes PDF)** > **Email Scheduler (Programador de correo electrónico)**.
2. Haga clic en **Add (Añadir)** y seleccione el nuevo perfil de correo electrónico en el menú desplegable **Email Profile (Perfil de correo electrónico)**.
3. Haga clic en el botón **Send test (Enviar prueba)** del correo electrónico y se enviará un correo electrónico de prueba a los destinatarios definidos en el perfil de correo electrónico.

STEP 3 | Configure un perfil de reenvío de logs para reenviar logs de WildFire a Panorama, una cuenta de correo electrónico, SNMP y un servidor Syslog, y como solicitudes HTTP.

En este ejemplo, configurará logs de correo electrónico para cuando se determine que la muestra es malintencionada. También puede habilitar el reenvío de logs Benign (Benignos) y Grayware, lo cual genera más actividad si está realizando pruebas.

El cortafuegos no reenvía logs de WildFire de los archivos bloqueados a una cuenta de correo electrónico.

1. Seleccione **Objects (Objetos)** > **Log Forwarding (Reenvío de logs)**.
2. **Add (Añada)** nombre el perfil, por ejemplo, WildFire-Log-Forwarding. Opcionalmente, puede añadir una **descripción** del perfil de reenvío de logs.
3. **Añada** para configurar métodos de reenvío.

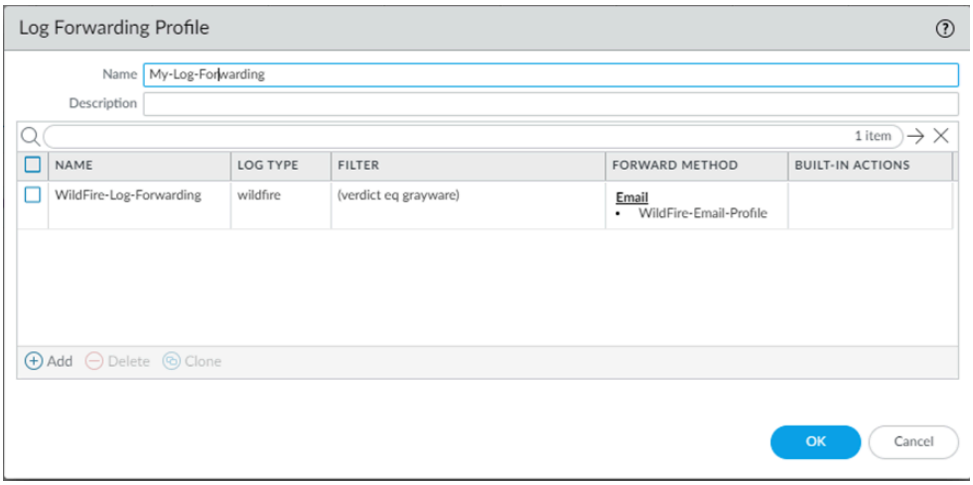


1. Proporcione un nombre para la **lista de coincidencias de perfiles de reenvío de logs**.
2. Seleccione el tipo de log de **WildFire**.
3. **Filtre** los logs mediante la consulta **(verdict eq malicious)**.
4. En las opciones de **Forward Method (Método de reenvío)**, elija el perfil de correo electrónico que se creó en el paso 1 (en este caso, WildFire-Email-Profile [Perfil de correo

 ©2025 Palo Alto Networks, Inc.

electrónico de WildFire]) y haga clic en **OK (Aceptar)** para guardar las actualizaciones de la lista de coincidencias.

4. Haga clic en **OK (Aceptar)** de nuevo para guardar las actualizaciones del perfil de reenvío de logs.



STEP 4 | Añada el perfil de reenvío de logs a una política de seguridad utilizada para el reenvío de WildFire (con un perfil de WildFire Analysis adjunto).

El perfil de WildFire Analysis define el tráfico que el cortafuegos reenvía para el análisis de Advanced WildFire. Para configurar un perfil de análisis de WildFire y adjuntarlo a una regla de política de seguridad, consulte Reenviar archivos para Advanced WildFire Analysis.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y haga clic en la política utilizada para el reenvío de WildFire.
2. En la pestaña **Actions (Acciones)**, dentro de la sección **Log Setting (Configuración de logs)**, seleccione el perfil de **Log Forwarding (Envío de logs)** que configuró.
3. Haga clic en **OK (Aceptar)** para guardar los cambios y, a continuación, haga clic en **Commit (Confirmar)** para guardar la configuración.

 ©2025 Palo Alto Networks, Inc.

Ver logs e informes de análisis de WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

Los logs de WildFire contienen información sobre muestras (archivos y enlaces de correo electrónico) cargados en la nube de WildFire para su análisis. Incluye artefactos, que son propiedades, actividades o comportamientos asociados con el evento registrado, como el tipo de aplicación o la dirección IP de un atacante, así como cualidades específicas de WildFire, como resultados de análisis de alto nivel, incluida la categorización de la muestra. como malware, phishing, grayware o información benigna, y detalla información de muestra. La revisión de los logs de envíos de WildFire también puede indicar si un usuario en sus redes descargó un archivo sospechoso. En el informe del análisis de WildFire se muestra información detallada de la muestra, además de información sobre los usuarios de destino, información del encabezado de correo electrónico (si está habilitado), la aplicación que entregó el archivo y todas las URL involucradas en la actividad de comando y control del archivo. Le informa de si el archivo es malintencionado, ha modificado las claves de registro, ha leído/escrito en archivos, ha creado nuevos archivos, ha abierto canales de comunicación de red, ha causado bloqueos de aplicaciones, ha generado procesos, ha descargado archivos o ha mostrado otro comportamiento malintencionado.

Los logs de WildFire se muestran como logs de envíos de WildFire en cortafuegos NGFW, mientras que en las plataformas de gestión en la nube, primero debe configurar el reenvío de logs para cargar los logs relevantes en Strata Logging Service, que a continuación, mostrará los logs de WildFire como logs de amenazas (tipo WildFire).

- Strata Cloud Manager
- PAN-OS y Panorama

Ver logs e informes de análisis de WildFire (PAN-OS y Panorama)

Las muestras que los cortafuegos envían para el análisis de WildFire se muestran como entradas en el log de **WildFire Submissions (Envíos de WildFire)** en la interfaz web del cortafuegos. Para cada entrada de WildFire puede abrir una vista del log ampliada que muestra los detalles del log y el informe de análisis de WildFire de la muestra.

Usuarios de Mozilla Firefox: El Informe de análisis de WildFire se muestra correctamente solo en Firefox v54 y versiones anteriores. Si tiene problemas para ver el informe, considere la posibilidad de usar un navegador web diferente, como Google Chrome. Alternativamente, puede descargar y abrir la versión en PDF o ver el informe a través del portal WildFire.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Reenviar archivos para Advanced WildFire Analysis.

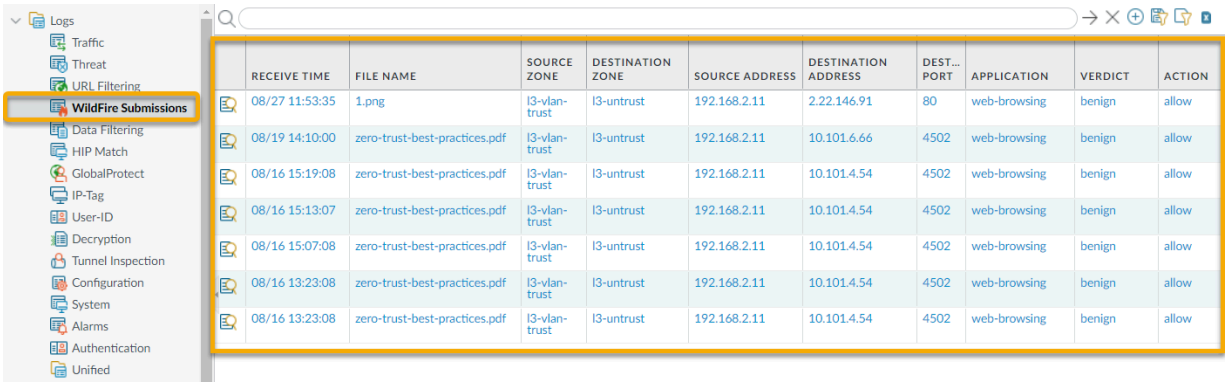
STEP 2 | Configuración de los ajustes del log de envíos a WildFire.

STEP 3 | Para visualizar las muestras enviadas por un cortafuegos a una nube pública, privada o híbrida de WildFire, seleccione **Monitor (Supervisar)** > **Logs (Logs)** > **WildFire Submissions (Envíos de WildFire)**. Cuando WildFire completa el análisis de una muestra, los resultados se devuelven al cortafuegos que envió la muestra y se ponen a disposición en los logs de envíos de WildFire. Los logs de envío incluyen detalles sobre una muestra determinada, que incluye la siguiente información:

- La columna Verdict (veredicto) indica si la muestra es benigna, malintencionada, phishing o grayware.
- La columna Action (Acción) indica si el cortafuegos permitió o bloqueó la muestra.
- La columna Severity (Gravedad) indica el grado de amenaza que implica una muestra para una organización con los siguientes valores: crítico, alto, intermedio, bajo e informativo.

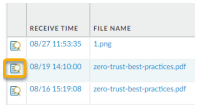
Los valores de los siguientes niveles de gravedad se determinan con una combinación de veredictos y valores de acción.

- *Baja: muestras de grayware con la acción allow (permitir).*
- *Alta: muestras maliciosas con la acción allow (permitir).*
- *Informativo:*
  - *Muestras benignas con la acción allow (permitir).*
  - *Muestras con cualquier veredicto y la acción block (bloquear).*

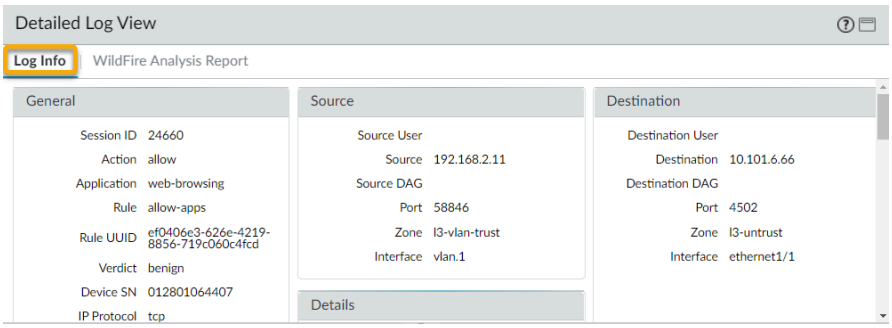


 ©2025 Palo Alto Networks, Inc.

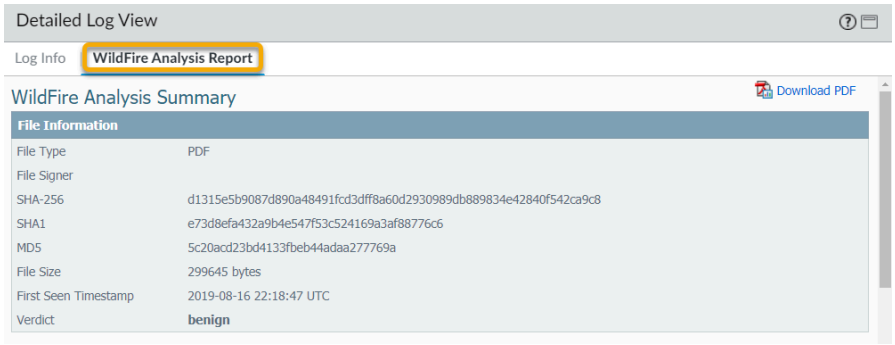
STEP 4 | En cualquiera de las entradas, seleccione el icono de detalles del log para abrir una vista detallada del log para cada entrada:



La vista detallada del log muestra la información del log y el informe de WildFire Analysis de la entrada. Si el cortafuegos tiene capturas de paquetes (PCAP) habilitadas, las PCAP de la muestra también se mostrarán.



Para todas las muestras, el informe del análisis de WildFire muestra información del archivo y la sesión. Para las muestras de malware, el informe de análisis de WildFire se amplía para incluir detalles sobre los atributos del archivo y el comportamiento que indicaron que el archivo era malintencionado.



STEP 5 | (Opcional) Haga clic en **Download PDF (Descargar PDF)** para descargar el informe de WildFire Analysis.

Ver logs e informes de análisis de WildFire (Cloud Management)

***Si está utilizando Panorama para gestionar Prisma Access,**, puede seguir el proceso a continuación para acceder al contenido en Prisma Access o cambie a la pestaña **PAN-OS** y siga las instrucciones allí.*

STEP 1 | Utilice las credenciales asociadas con su cuenta de asistencia técnica de Palo Alto Networks e inicie sesión en la aplicación de Strata Cloud Manager en el hub.

Para obtener más información sobre la Actividad de uso, consulte el Visor de logs.

 ©2025 Palo Alto Networks, Inc.

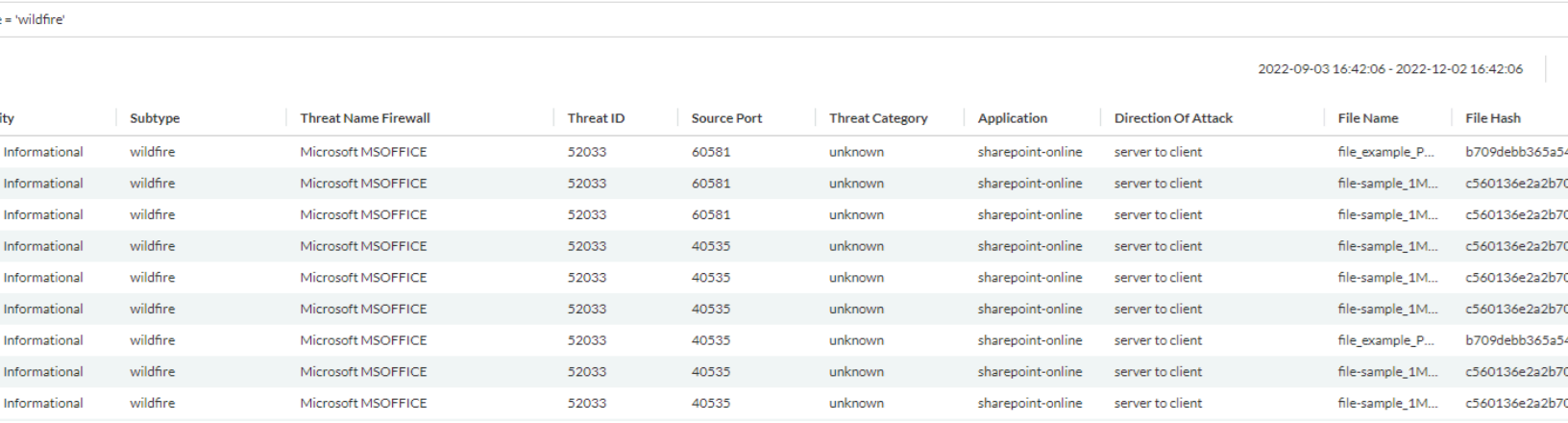
STEP 2 | Filtrar los logs de amenazas para mostrar los envíos de muestras de WildFire en Prisma Access.

1. Seleccione **Incidents and Alerts (Incidentes y alertas)** > **Log Viewer (Visor de logs)**.
2. Cambie el tipo de log que se buscará a **Threat (Amenaza)**.
3. Cree un filtro de búsqueda utilizando el subtipo WildFire utilizado para indicar un envío de muestra de WildFire utilizando el generador de consultas. Por ejemplo, puede utilizar `sub_type.value = 'wildfire'` para ver sus logs de WildFire. Ajuste los criterios de

 ©2025 Palo Alto Networks, Inc.

búsqueda según sea necesario para su búsqueda, incluidos parámetros de consulta adicionales (como el nivel de gravedad y la acción) junto con un rango de fechas.

Para ver el informe de análisis de WildFire, debe iniciar sesión en el portal de WildFire y utilizar el valor hash o el nombre del archivo para recuperar el archivo del informe. Para obtener más información, consulte Visualización de informes en el portal de WildFire.

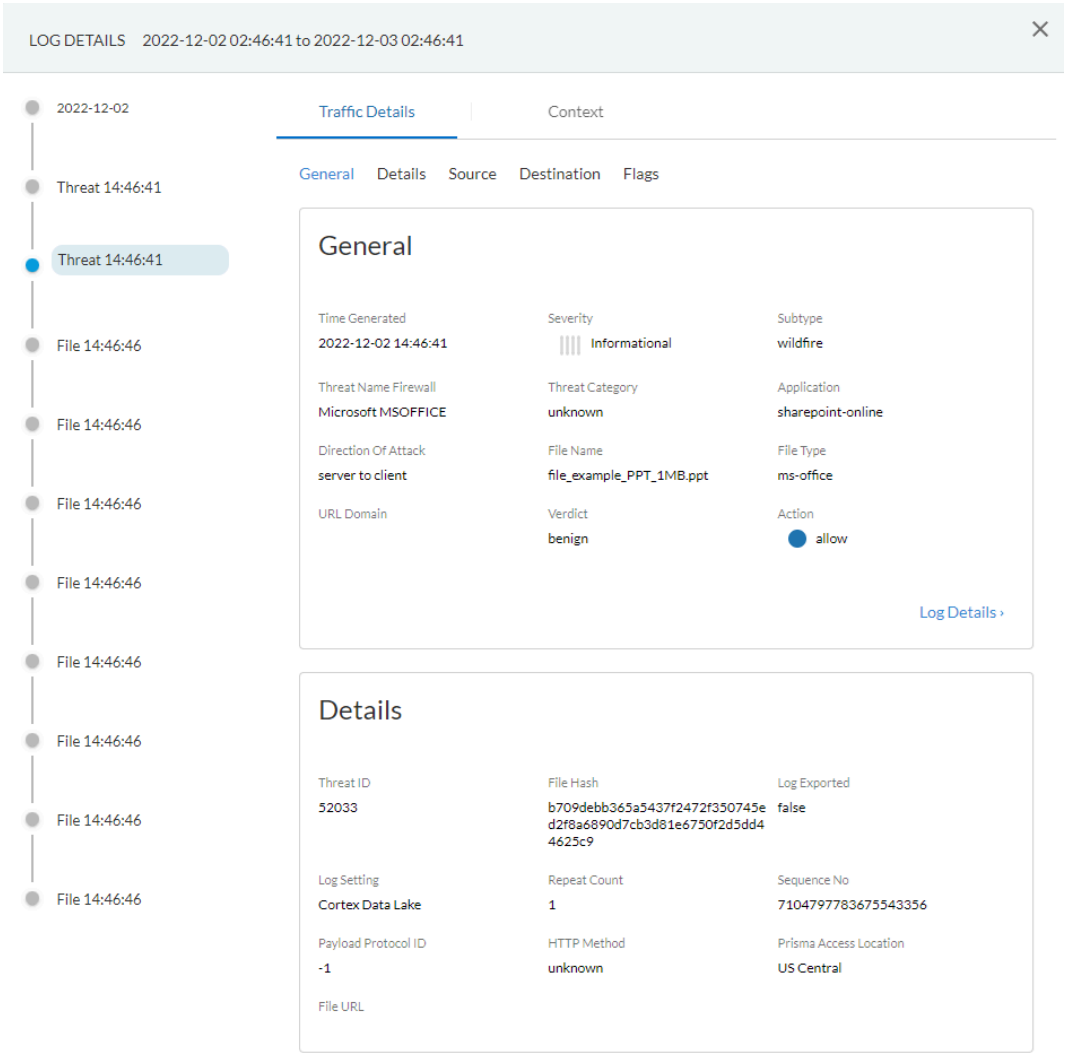

= 'wildfire'

2022-09-03 16:42:06 - 2022-12-02 16:42:06

ity	Subtype	Threat Name Firewall	Threat ID	Source Port	Threat Category	Application	Direction Of Attack	File Name	File Hash
Informational	wildfire	Microsoft MSOFFICE	52033	60581	unknown	sharepoint-online	server to client	file_example_P...	b709debb365a5
Informational	wildfire	Microsoft MSOFFICE	52033	60581	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70
Informational	wildfire	Microsoft MSOFFICE	52033	60581	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70
Informational	wildfire	Microsoft MSOFFICE	52033	40535	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70
Informational	wildfire	Microsoft MSOFFICE	52033	40535	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70
Informational	wildfire	Microsoft MSOFFICE	52033	40535	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70
Informational	wildfire	Microsoft MSOFFICE	52033	40535	unknown	sharepoint-online	server to client	file_example_P...	b709debb365a5
Informational	wildfire	Microsoft MSOFFICE	52033	40535	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70
Informational	wildfire	Microsoft MSOFFICE	52033	40535	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70

4. Ejecute la consulta una vez que haya terminado de ensamblar su filtro.
5. Seleccione una entrada de registro de los resultados para ver los detalles del registro.
6. El **Subtype (Subtipo)** de log de amenazas se muestra en el panel **General** junto con otra información sobre la muestra. Otros detalles relevantes sobre la amenaza se muestran en sus correspondientes ventanas.

 ©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

Uso del portal de WildFire para supervisar el malware

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

Inicie sesión en el portal de WildFire de Palo Alto Networks utilizando sus credenciales de asistencia técnica de Palo Alto Networks o su cuenta de WildFire. El portal se abrirá para mostrar el panel, que enumera información de informes de resumen de todos los cortafuegos asociados a la suscripción a WildFire o cuenta de soporte específica. Para cada dispositivo incluido, el portal mostrará estadísticas del número de archivos de malware detectados, muestras benignas analizadas y la cantidad de archivos pendientes en espera de análisis. Su cuenta del portal de WildFire muestra los datos de todas las muestras reenviadas por los cortafuegos en la red que están conectados a la nube pública de WildFire, además de los datos para las muestras reenviadas manualmente al portal. Además, si tiene habilitado un dispositivo WildFire para reenviar malware a la nube pública de WildFire para la generación y distribución de firmas, también se puede acceder a los informes de esas muestras de malware a través del portal.

Consulte las secciones siguientes para obtener detalles sobre el uso del portal de WildFire para supervisar la actividad de WildFire:

- Configuración de los ajustes del portal de WildFire
- Cómo añadir usuarios al portal de WildFire
- Visualización de informes en el portal de WildFire

Configuración de los ajustes del portal de WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

©2025 Palo Alto Networks, Inc.

Esta sección describe los ajustes que pueden personalizarse para una cuenta de nube de WildFire, como la zona horaria y las notificaciones de correo electrónico de cada cortafuegos conectado a la cuenta. También puede eliminar logs de cortafuegos almacenados en la nube.

STEP 1 | Acceda a los ajustes del portal.

1. Inicie sesión en el portal de WildFire.
2. Seleccione **Settings (Configuración)** en la barra del menú.

STEP 2 | Configure la zona horaria para la cuenta de la nube de WildFire.

Seleccione una zona horaria en la lista desplegable **Set Time Zone (Establecer zona horaria)** y haga clic en **Update Time Zone (Actualizar zona horaria)** para guardar los cambios.

La marca de hora que aparece en los informes de análisis de WildFire se basa en la zona horaria configurada en la cuenta de la nube de WildFire.

STEP 3 | (Opcional) Elimine los logs de WildFire alojados en la nube para cortafuegos específicos.

1. En la lista desplegable **Delete WildFire Reports (Eliminar informes de WildFire)**, seleccione un cortafuegos (por número de serie) y haga clic en **Delete Reports (Eliminar informes)** para eliminar los logs de ese cortafuegos del portal de WildFire. Esta acción no elimina los logs almacenados en el cortafuegos.
2. Haga clic en **OK (Aceptar)** para continuar con la eliminación.

STEP 4 | (Opcional) Configure las notificaciones de correo electrónico en función de los veredictos del análisis de WildFire.

El portal de WildFire no envía las alertas de los archivos bloqueados que reenvió el cortafuegos para el análisis de WildFire.

1. En la sección Configure Alerts (Configuración de alertas), seleccione las casillas de verificación **Malware**, **Grayware** o **Benign (Benigno)** para recibir notificaciones de correo electrónico basadas en esos veredictos:
   - Seleccione las casillas de verificación de veredicto en la fila **All (Todos)** para recibir notificaciones de veredicto para todas las muestras cargadas en la nube de WildFire.
   - Seleccione las casillas de verificación de veredicto en la fila **Manual** para recibir notificaciones de veredicto para todas las muestras cargadas manualmente en la nube pública de WildFire utilizando el portal de WildFire.
   - Seleccione las casillas de verificación de veredicto para uno o varios números de serie de cortafuegos para recibir notificaciones de veredicto para las muestras enviadas por esos cortafuegos.
2. Seleccione **Update Notification (Actualizar notificación)** para habilitar el envío por correo electrónico de las notificaciones de veredicto a la dirección de correo electrónico asociada a su cuenta de soporte.

 ©2025 Palo Alto Networks, Inc.

Cómo añadir usuarios al portal de WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

Las cuentas del portal de WildFire son creadas por un superusuario (el propietario registrado de un dispositivo de Palo Alto Networks) para permitir que otros usuarios inicien sesión en la nube de WildFire y vean datos de WildFire de dispositivos a los que obtuvieron acceso a través del superusuario. Un usuario de WildFire puede ser un usuario asociado con una cuenta existente de Palo Alto Networks o un usuario no asociado a una cuenta de soporte de Palo Alto Networks, que puede tener acceso a las nubes públicas de WildFire y a un conjunto específico de datos de los cortafuegos.

STEP 1 | Seleccione la cuenta para la cual desea añadir usuarios que puedan acceder al portal de WildFire.

Los usuarios del portal de WildFire pueden visualizar datos para todos los cortafuegos asociados con la cuenta de soporte.

1. Inicie sesión en el Portal de soporte de Palo Alto Networks.
2. En **Manage Account (Gestionar cuenta)**, haga clic en **Users and Accounts (Usuarios y cuentas)**.
3. Seleccione una cuenta o una cuenta secundaria existente.

STEP 2 | Añada un usuario de WildFire.

1. Haga clic en **Add WildFire User (Añadir usuario de WildFire)**.
2. Introduzca la dirección de correo electrónico para el usuario que desea añadir.

La única restricción al agregar un usuario es que la dirección de correo electrónico no puede ser de una cuenta de correo electrónico web gratuito (como Gmail, Hotmail y Yahoo). Si se introduce una cuenta de correo electrónico de un dominio no compatible, se mostrará un mensaje de advertencia.

STEP 3 | Asigne cortafuegos a la nueva cuenta de usuario y acceda a la nube de WildFire.

Seleccione los cortafuegos por número de serie a los que desea conceder acceso y cumplimente los detalles de cuenta opcionales.

Los usuarios con una cuenta de soporte existente recibirán un mensaje de correo electrónico con una lista de los cortafuegos de los cuales ahora pueden ver los informes de WildFire. Si el usuario no tiene

 ©2025 Palo Alto Networks, Inc.

una cuenta de soporte, el portal enviará un mensaje de correo electrónico con instrucciones sobre cómo acceder al portal y configurar una nueva contraseña.

El nuevo usuario podrá entonces iniciar sesión en la nube de WildFire y ver informes de WildFire de los cortafuegos a los que se le ha concedido acceso. Además, podrá configurar alertas de correo electrónico automáticas para estos dispositivos con el fin de recibir alertas sobre los archivos analizados. También es posible elegir la opción de recibir informes sobre archivos con malware o benignos.

Visualización de informes en el portal de WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia avanzada de WildFire *Para Prisma Access, esto generalmente se incluye con su licencia de Prisma Access.*

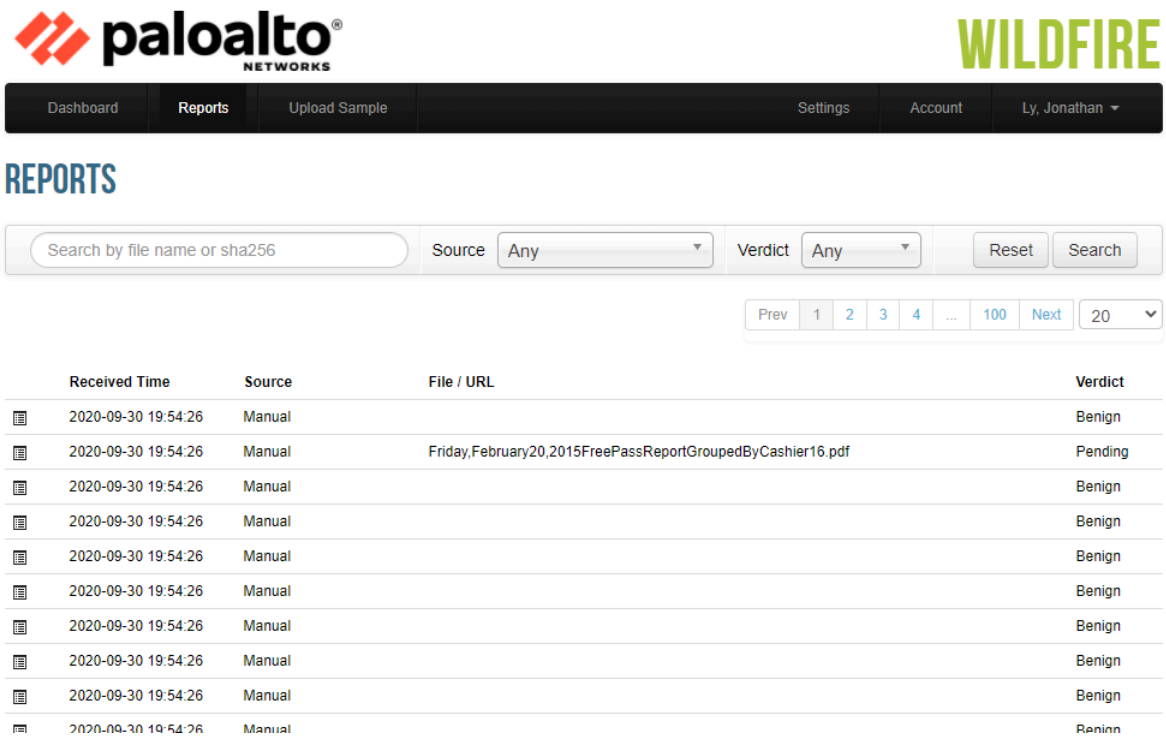
El portal de WildFire muestra informes para las muestras enviadas desde los cortafuegos, subidas manualmente o cargadas con la API de WildFire. Seleccione **Reports (Informes)** para mostrar los informes más recientes para las muestras analizadas por la nube de WildFire. Para cada muestra enumerada, la entrada del informe muestra la fecha y hora en que la nube recibió la muestra, el número de serie del cortafuegos que envió el archivo, el nombre de archivo o URL, y el veredicto asignado por WildFire (benigno, grayware, malware o phishing).

Use la opción de búsqueda para buscar informes basados en el nombre de archivo o el valor hash de la muestra. También puede acotar los resultados visualizados al mostrar únicamente los informes de las muestras enviadas por una **Source (Fuente)** específica (visualizar solo los resultados enviados manualmente o por un cortafuegos específico) o de las muestras que recibieron un **Verdict (Veredicto)** específico de WildFire (todos, benigno, malware, grayware, phishing o pendiente).

Para ver un informe individual desde el portal, haga clic en el icono **Reports (Informes)**, situado a la izquierda del nombre del informe. Para guardar el informe detallado, haga clic en el botón **Download as PDF (Descargar como PDF)** en la esquina superior derecha de la página del informe. Para obtener detalles sobre los informes de análisis de WildFire, consulte Informes de WildFire Analysis: detallados.

A continuación se muestra una lista de archivos de muestra enviados por un cortafuegos específico:

 ©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.