Palo Alto Networks®
Guía del administrador de WildFire

Software del dispositivo WildFire 5.1

Información de contacto

Sede de la empresa:

Guía del administrador

3300 Olcott Street

Santa Clara, CA 95054

http://www.paloaltonetworks.com/contact/contact/

Acerca de esta guía

Esta guía describe las tareas administrativas necesarias para utilizar y mantener la función Palo Alto Networks WildFire. Los temas tratados incluyen información de licencias, la configuración de cortafuegos para reenviar archivos para su inspección, la visualización de informes y cómo configurar y gestionar el Dispositivo WF-500 WildFire.

Consulte las siguientes fuentes para obtener más información:

- Guía del administrador de Palo Alto Networks: Ofrece información sobre capacidades adicionales e instrucciones sobre la configuración de las funciones del cortafuegos.
- https://live.paloaltonetworks.com: Permite acceder a la base de conocimientos, la documentación al completo, foros de debate y vídeos.
- https://support.paloaltonetworks.com: Aquí podrá contactar con el servicio de asistencia técnica, informarse sobre los programas de asistencia y gestionar su cuenta o sus dispositivos.

Para enviar sus comentarios sobre la documentación, diríjase a:

documentation@paloaltonetoworks.com

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Número de pieza 810-000172-00A

Contenido

1 Descripción general de WildFire

Este capítulo proporciona una descripción general de la funcionalidad WildFire, incluidas las implementaciones compatibles, los requisitos de suscripción y descripción de los pasos que deben tomarse si se detecta malware en su entorno. Incluye las siguientes secciones:

Acerca de WildFire

El malware moderno es el eje de la mayoría de los ataques a la red más sofisticados de la actualidad, y cada vez se personaliza más para burlar las soluciones de seguridad tradicionales. Palo Alto Networks ha desarrollado un enfoque integrado que se encarga de todo el ciclo de vida del malware, lo que incluye la prevención de infecciones, la identificación de malware de día cero (es decir, malware que no han identificado anteriormente otros proveedores de antivirus) o malware específico (dirigido a un sector o corporación concretos), así como la localización y eliminación de infecciones activas.

El motor de WildFire de Palo Alto Networks expone el malware específico y de día cero mediante la observación directa en un entorno virtual en el sistema WildFire. La funcionalidad WildFire hace, además, un uso extensivo de la tecnología App-ID de Palo Alto Networks identificando las transferencias de archivos en todas las aplicaciones, no solo en los archivos adjuntos del correo electrónico o en las descargas de archivos del explorador.

Las principales ventajas de la funcionalidad WildFire de Palo Alto Networks son la detección de malware de día cero y generar rápidamente firmas para ofrecer protección frente a futuras infecciones de todo el malware que detecte. El cortafuegos proporciona alertas instantáneas en cualquier momento en que se detecte malware en su red mediante el envío de alertas de correo electrónico, alertas de Syslog o traps SNMP. Esto le permite identificar rápidamente qué usuario descargó el malware y eliminarlo antes de que cause mayores daños o se propague a otros usuarios. Además, cada firma generada por WildFire se propaga automáticamente a todos los cortafuegos de Palo Alto Networks protegidos con las suscripciones a Threat Prevention o WildFire, que ofrecen protección automatizada frente a malware incluso si no se ha detectado dentro de la red. Actualmente, Palo Alto Networks está descubriendo y generando nuevas firmas para miles de aplicaciones de malwares de día cero cada semana, y esta cifra sigue creciendo.

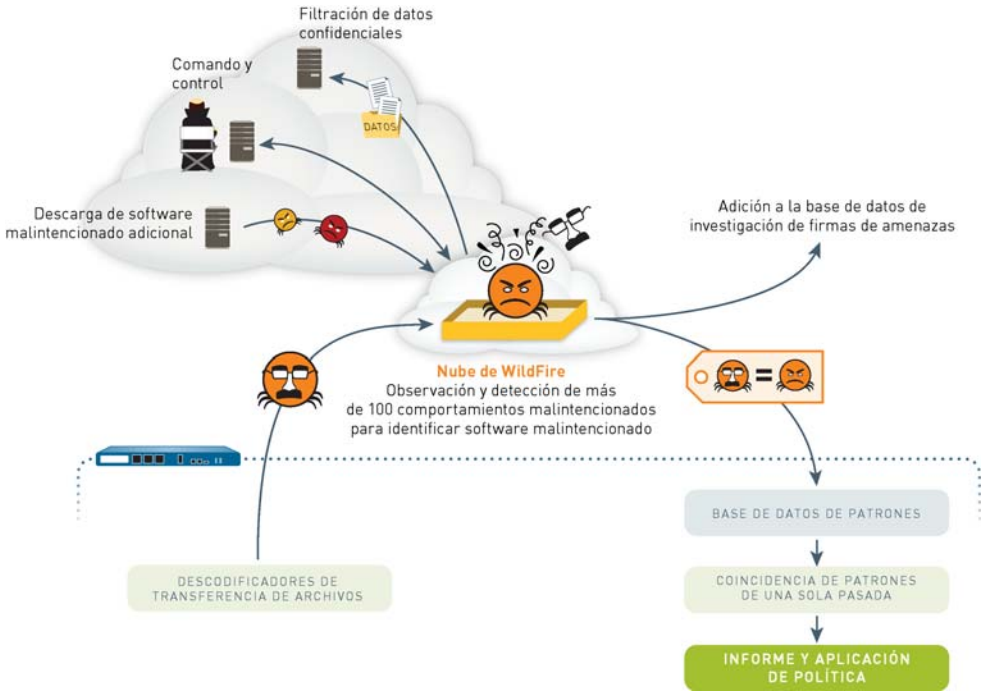
¿Cómo funciona WildFire?

Para usar WildFire en el cortafuegos, debe configurar un perfil de bloqueo de archivos para enviar archivos a WildFire definiendo la acción de reenvío en el tipo de archivo Win32 Portable Executable (PE). De forma alternativa, puede seleccionar la acción Continuar y reenviar para preguntar al usuario antes de descargar el archivo mediante HTTP. Dado que los ajustes de WildFire se configuran mediante un perfil de bloqueo de archivos, que después se adjunta a una política de cortafuegos, tiene un control muy detallado de las condiciones bajo las cuales se envían los archivos a WildFire. Por ejemplo, puede elegir reenviar solo archivos adjuntos de correo electrónico web o solo los procedentes de sitios web de determinadas categorías URL.

Siempre que se transfiere un archivo mediante una sesión que coincida con una regla de seguridad con un perfil de reenvío, el cortafuegos comprueba con WildFire si el archivo es nuevo. Si el archivo es nuevo, el cortafuegos lo reenvía automáticamente a WildFire, incluso si este se encontraba en un archivo ZIP o en HTTP comprimido. El cortafuegos también se puede configurar para que reenvíe archivos situados dentro de sesiones SSL descifradas. Cuando WildFire recibe un archivo, lo analiza en su entorno aislado virtualizado para determinar si muestra signos de comportamientos malintencionados, cambios en la configuración de seguridad del explorador, introducción de código en otros procesos, modificación de archivos en las carpetas del sistema de Windows o dominios que la muestra puede haber visitado. Cuando el motor de WildFire completa el análisis, genera un informe experto detallado que resume las actividades realizadas por la muestra en el host y la red, y asigna automáticamente un veredicto para indicar si se trata de malware o no.

Además, cuando el motor de WildFire identifica una muestra como malware, lo pasa al generador de firmas de WildFire, que automáticamente genera una firma en función de la carga de malware de la muestra y prueba su precisión y seguridad. Dado que el malware evoluciona rápidamente, las firmas que genera WildFire cubrirán diversas variantes de este. La nueva firma se distribuye entonces en 30-60 minutos a todos los cortafuegos de Palo Alto Networks con una suscripción de WildFire, o el día siguiente como parte de la actualización del antivirus para los cortafuegos que solo tienen una suscripción de Threat Prevention. En cuanto el cortafuegos se actualiza con la nueva firma, los archivos que contienen ese malware o una variante de este se eliminarán automáticamente. La información recopilada por WildFire durante el análisis del malware también se usa para fortalecer otras funciones de Threat Prevention, como las categorías de URL de malware PAN-DB, las firmas DNS y las firmas antispyware y antivirus. Palo Alto Networks también desarrolla firmas para el tráfico de comandos y control, lo que permite la interrupción inmediata de la comunicación de cualquier tipo de malware en la red. Si desea más información sobre las ventajas de tener una suscripción de WildFire, consulte "¿Cuáles son las ventajas de la suscripción de WildFire?" en la página 5.

El siguiente diagrama ilustra el flujo de trabajo de WildFire:



¿Qué contienen los informes de WildFire?

Por cada archivo que analiza WildFire, produce un informe detallado de comportamiento unos minutos después del envío del archivo. En función de cómo se haya enviado el archivo a WildFire y qué suscripciones estén activas en el cortafuegos, estos informes estarán disponibles en los logs de WildFire del cortafuegos, en el portal de WildFire (https://wildfire.paloaltonetworks.com) o a través de consultas a la API de WildFire. Los informes muestran información detallada de comportamiento sobre el archivo, información sobre el usuario de destino, la aplicación que entregó el archivo y todas las direcciones URL involucradas en la entrega o en la actividad phonehome del archivo. Si desea más información sobre cómo acceder a los informes y a las descripciones de los campos de los informes, consulte "Visualización de informes de WildFire" en la página 52.

¿Qué acciones debo tomar después de que se detecte malware?

Cuando se detecta malware en su red, es importante reaccionar rápido para evitar que se propague a otros sistemas. Para asegurarse de recibir alertas inmediatas de detección de malware en su red, configure sus cortafuegos para que envíen notificaciones de correo electrónico, traps SNMP o Syslog siempre que WildFire devuelva un veredicto de malware sobre un archivo reenviado desde un cortafuegos. Esto le permite ver rápidamente el informe del análisis de WildFire e identificar qué usuario descargó el malware, determinar si el usuario ejecutó el archivo infectado y evaluar si el malware ha intentado propagarse a otros hosts de la red. Si determina que el usuario ejecutó el archivo, puede desconectar rápidamente el equipo de la red para impedir que el malware se propague y seguir los procesos de respuesta a incidentes y reparación según sea necesario. Para obtener más información sobre los informes de WildFire y ver un ejemplo de WildFire en acción, consulte "Supervisión, control y prevención del malware en la red" en la página 47.

¿Qué implementaciones están disponibles?

El cortafuegos de próxima generación de Palo Alto Networks admite las siguientes implementaciones de WildFire:

- **Nube de Palo Alto Networks WildFire:** En esta implementación, el cortafuegos reenvía los archivos al entorno de WildFire alojado, que pertenece a Palo Alto Networks y está mantenido por este. Cuando WildFire detecta un nuevo malware, genera nuevas firmas en la hora próxima a la detección. Los cortafuegos equipados con una suscripción de WildFire pueden recibir las nuevas firmas en los siguientes 30-60 minutos; los cortafuegos con solo una suscripción de Threat Prevention pueden recibir las nuevas firmas en la siguiente actualización de firma del antivirus, en las próximas 24-48 horas. Para obtener más información, consulte "¿Cuáles son las ventajas de la suscripción de WildFire?" en la página 5.
- **Dispositivo WildFire:** En esta implementación, instalará un dispositivo WF-500 WildFire en su red empresarial y configurará sus cortafuegos para que reenvíen los archivos a este dispositivo en lugar de a la nube WildFire de Palo Alto Networks (opción predeterminada). Esta implementación impide que el cortafuegos tenga que enviar archivos fuera de la red para su análisis. De forma predeterminada, el dispositivo no enviará archivos fuera de su red a menos que habilite de forma explícita la función de envío automático, que reenviará automáticamente cualquier malware que detecte a la nube WildFire de Palo Alto Networks, donde los archivos se analizan para generar firmas de antivirus. Las firmas de antivirus se distribuirán entonces a todos los cortafuegos de Palo Alto Networks con una suscripción de Threat Prevention o WildFire. Un único dispositivo WildFire puede recibir y analizar archivos de hasta 100 cortafuegos de Palo Alto Networks.

Las principales diferencias entre la nube WildFire de Palo Alto Networks y el dispositivo WildFire son las siguientes:

- El dispositivo WildFire habilita el aislamiento local del malware para que los archivos que no resulten peligrosos nunca salgan de la red del cliente. De forma predeterminada, el dispositivo WildFire no reenvía archivos a la nube de WildFire y, por lo tanto, no se generan firmas para el malware detectado por este. Si desea generar firmas de WildFire para el malware detectado en su red, puede habilitar la función de envío automático en el dispositivo. Con esta opción habilitada, el dispositivo envía cualquier malware que detecte a la nube de WildFire para la generación de la firma correspondiente.
- La API de WildFire, que se proporciona con todas las suscripciones a WildFire, está disponible para todos los suscriptores de WildFire y puede utilizarse con la nube pública, pero no con el dispositivo WF-500.
- El envío manual de muestras puede realizarse en la nube pública a través del portal web (wildfire.paloaltonetworks.com), pero no existe ningún portal web local para el dispositivo WF-500.

¿Cuáles son las ventajas de la suscripción de WildFire?

WildFire ofrece detección y prevención de malware de día cero mediante una combinación de detección de malware basada en firmas y en aislamiento y bloqueo del malware. Para usar WildFire para obtener visibilidad del malware de día cero, todo lo que necesita es configurar un perfil de bloqueo de archivos para permitir al cortafuegos reenviar muestras a WildFire para su análisis. No se requiere ninguna suscripción para usar WildFire para el aislamiento de archivos enviados desde cortafuegos de Palo Alto Networks a la nube de WildFire.

Para realizar la detección y el bloqueo de malware conocido una vez detectado por WildFire, se requiere una suscripción de Threat Prevention o WildFire. La suscripción de Threat Prevention permite al cortafuegos recibir actualizaciones diarias de firma de antivirus, lo que proporciona protección para todas las muestras de malware detectadas por WildFire de forma general para todos los clientes con esta suscripción. Asimismo, la suscripción de Threat Prevention proporciona acceso a actualizaciones semanales de contenido que incluyen protección frente a vulnerabilidades y firmas antispyware.

Para beneficiarse al completo del servicio WildFire, cada cortafuegos debe tener una suscripción de WildFire, que ofrece las siguientes ventajas:

- **Actualizaciones dinámicas de WildFire**: nuevas firmas de malware con frecuencias inferiores a una hora. Se pueden configurar en **Dispositivo > Actualizaciones dinámicas**. En la hora siguiente a la detección del nuevo malware, WildFire crea una nueva firma de malware y la distribuye mediante las actualizaciones dinámicas de WildFire, que el cortafuegos puede sondear cada 15, 30 o 60 minutos. El cortafuegos se puede configurar para que realice acciones específicas con respecto a las firmas de malware aparte de las acciones habituales de firma de antivirus del perfil de antivirus. Las firmas de WildFire entregadas en la actualización dinámica incluyen las generadas para el malware detectado en archivos enviados a WildFire por todos los clientes de Palo Alto Networks WildFire, no solo las muestras de archivos que envía el cortafuegos a WildFire.

Una firma de WildFire tarda aproximadamente de 30 a 60 minutos en generarse y en estar disponible para los suscriptores de WildFire después de que el malware se detecte. Los cortafuegos equipados con una suscripción de WildFire pueden sondear la existencia de nuevas firmas de malware cada 15, 30 o 60 minutos. Por ejemplo, si el cortafuegos está definido para sondear actualizaciones de firmas de WildFire cada 30 minutos, puede que no reciba una firma de uno de los archivos enviados hasta el segundo intervalo de sondeo después de que se detecte debido al tiempo que tarda en generarse la firma. Si el cortafuegos solo tiene una suscripción de Threat Prevention, seguirá recibiendo firmas generadas por WildFire después de que las firmas de WildFire entren en las actualizaciones del antivirus, que se producen cada 24-48 horas.

Para los archivos analizados por un Dispositivo WF-500 WildFire, solo se pueden generar firmas para malware detectado en la red si ha habilitado explícitamente la función de envío automático (a menos que el mismo malware haya sido detectado por otro cliente y se haya enviado la misma muestra a la nube pública de WildFire). Si el envío automático está habilitado, el dispositivo reenviará todo el malware detectado a la nube de Palo Alto Networks WildFire, donde se usará para generar una firma de antivirus para detectar y bloquear futuras instancias de malware.

- **Logs de WildFire integrados**: cuando WildFire termina de analizar un archivo, envía un log de WildFire al cortafuegos que envió el archivo. Estos logs se pueden ver desde **Supervisar > Logs > WildFire**, y se puede obtener acceso directo al informe completo de análisis desde el sistema de WildFire haciendo clic en el botón **Ver informe de WildFire**. Tener los datos del log de WildFire sobre el cortafuegos hace que los logs de amenazas sean tan útiles como los demás, y permite configurar SNMP, Syslog, alertas de correo electrónico y el reenvío a Panorama. Sin la suscripción de WildFire, solo se puede acceder a los logs de WildFire con el portal web de WildFire, en wildfire.paloaltonetworks.com.
- **API de WildFire**: la suscripción de WildFire proporciona acceso a la API de WildFire, lo que permite tener un acceso directo programático al servicio WildFire en la nube de Palo Alto Networks WildFire. Puede usar la API de WildFire para enviar archivos a la nube de WildFire y recuperar informes de los archivos enviados. La API de WildFire admite hasta 100 envíos de archivos y hasta 1.000 consultas al día. Tenga en cuenta que no puede usar la API de WildFire para enviar archivos al dispositivo WildFire.
- **Dispositivo WildFire**: solo los cortafuegos con una suscripción de WildFire válida pueden reenviar archivos a un dispositivo WildFire para su análisis. Los cortafuegos que solo tienen una suscripción de Threat Prevention instalada pueden reenviar archivos a la nube de WildFire, pero no a un dispositivo WildFire.

2 Análisis de archivos mediante el dispositivo WF-500 WildFire

En este capítulo se describe el dispositivo WF-500 WildFire y se explica cómo configurarlo y gestionarlo para que pueda recibir y analizar archivos. Además, se explican los pasos necesarios para configurar un cortafuegos de Palo Alto Networks para que reenvíe archivos a un dispositivo WildFire, que los analizará.

Acerca del dispositivo WF-500 WildFire

El dispositivo WF-500 WildFire proporciona una nube privada de WildFire in situ, que le permite analizar archivos sospechosos en un entorno aislado sin que sea necesario su envío fuera de la red. Para utilizar un dispositivo WF-500 en lugar de la nube pública de WildFire, configure la nube de WildFire en el cortafuegos para que indique el dispositivo WF-500 en lugar del ajuste **default-cloud**. El dispositivo WF-500 aísla todos los archivos localmente y los analiza en busca de comportamientos malintencionados usando el mismo motor que el utilizado por el sistema de nube pública de WildFire. En minutos, el dispositivo devuelve los resultados del análisis al cortafuegos del log de WildFire.

De forma predeterminada, el dispositivo WF-500 no envía ningún archivo a la nube WildFire de Palo Alto Networks. Sin embargo, se debe enviar el malware a la nube pública de WildFire para poder recibir las firmas del antivirus relacionadas con este software descubierto por el dispositivo. El dispositivo WF-500 tiene una función de envío automático que solamente le permitirá enviar el malware confirmado a la nube pública para la generación de las firmas. Las firmas se distribuyen entonces a todos los clientes que reciben actualizaciones de las firmas de WildFire y del antivirus de Palo Alto Networks. Puede configurar el reenvío a un único dispositivo WildFire de hasta 100 cortafuegos de Palo Alto Networks; para que el reenvío de archivos a un dispositivo WildFire sea posible, cada cortafuegos debe tener una suscripción a WildFire válida.

El dispositivo de WildFire tiene dos interfaces:

- **MGT**: recibe todos los archivos reenviados desde los cortafuegos y devuelve a los cortafuegos los logs que detallan los resultados.
- **Interfaz de máquina virtual (interfaz vm)**: proporciona acceso a la red para que los elementos de aislamiento de análisis permitan a WildFire analizar mejor el comportamiento de los archivos que se ejecutan en ellos, ya que ello permite observar algunos comportamientos malintencionados que no se mostrarían sin acceso a la red, como la actividad teléfono-casa. Sin embargo, para evitar que el malware acceda a la red desde el elemento de aislamiento, debe configurar esta interfaz en una red aislada con una conexión a Internet para permitir que el malware que se ejecuta en las máquinas virtuales se comunique con Internet. Para obtener más información sobre la interfaz vm, consulte "Configuración de interfaz de la máquina virtual" en la página 17.

  Debe configurar esta interfaz para poder compilar los cambios en el dispositivo.

Configuración del dispositivo WF-500 WildFire

En esta sección se describen los pasos necesarios para configurar un dispositivo de WildFire en una red y cómo configurar un cortafuegos de Palo Alto Networks para que le reenvíe los archivos para su análisis.

Esta sección contiene los siguientes temas:

Antes de comenzar

- Monte en un rack el dispositivo WF-500 WildFire y conéctelo. Consulte la *WF-500 WildFire Appliance Hardware Reference Guide (Guía de referencia de hardware de WF-500 WildFire)*.
- Obtenga la información necesaria para configurar la conectividad de la red en el puerto MGT y la interfaz de la máquina virtual desde su administrador de red (dirección IP, máscara de subred, puerta de enlace, nombre de host, servidor DNS). Toda la comunicación entre los cortafuegos y el dispositivo se produce en el puerto MGT, incluidos los envíos de archivo, la distribución de logs de WildFire y la administración de dispositivos. Por lo tanto debe asegurarse de que los cortafuegos tienen conectividad con el puerto MGT del dispositivo. Además, el dispositivo se debe poder conectar al sitio updates.paloaltonetworks.com para recuperar las actualizaciones de software del sistema operativo.
- Debe tener preparado un ordenador con un cable de consola o cable Ethernet para conectarse al dispositivo para la configuración inicial.

Realización de la configuración inicial

En esta sección se describen los pasos necesarios para instalar un dispositivo WF-500 WildFire en una red y realizar una configuración básica.

INTEGRACIÓN DEL DISPOSITIVO WILDFIRE EN UNA RED		
Paso 1	Realice las tareas de la sección "Antes de comenzar" en la página 9.	• El dispositivo se ha montado en rack • La información de IP está preparada (interfaz MGT y dirección IP de la interfaz vm, máscara de subred, puerta de enlace, nombre de host, servidor DNS) • El ordenador de gestión está conectado al puerto MGT en el dispositivo o el puerto de la consola
Paso 2	Registre el dispositivo WildFire.	1. Obtenga el número de serie de la etiqueta de número de serie en el dispositivo o ejecute el siguiente comando de la CLI: `admin@WF-500> show system info` 2. Con un navegador, acceda a https://support.paloaltonetworks.com. 3. Registre el dispositivo de la siguiente forma: • Si es el primer dispositivo de Palo Alto Networks que registra y aún no tiene un inicio de sesión, haga clic en **Registrar** en el lado derecho de la página. Para el registro debe proporcionar una dirección de correo electrónico y el número de serie del dispositivo. Cuando se le solicite, establezca un nombre de usuario y una contraseña para acceder a la comunidad de asistencia técnica de Palo Alto Networks. • Con las cuentas existentes solo tiene que iniciar sesión y hacer clic en **Mis dispositivos**. Desplácese hasta la sección **Registrar dispositivo**, en la parte inferior de la pantalla, e introduzca el número de serie del dispositivo, su ciudad y su código postal, y haga clic en **Registrar dispositivo**.

INTEGRACIÓN DEL DISPOSITIVO WILDFIRE EN UNA RED (CONTINUACIÓN)		
Paso 3	Conecte el ordenador de gestión al dispositivo usando el puerto MGT o el puerto de consola y encienda el dispositivo.	1. Conéctese al puerto de la consola o al puerto MGT. Ambos se encuentran en la parte posterior del dispositivo. • **Puerto de la consola**: conector serie macho de 9 clavijas. Utilice la siguiente configuración en la aplicación de la consola: 9600-8-N-1. Conecte el cable proporcionado al puerto de serie en el dispositivo de gestión o al conversor USB-serie. • **Puerto MGT**: puerto RJ-45 Ethernet. De forma predeterminada, la dirección IP del puerto MGT es 192.168.1.1. La interfaz del ordenador de gestión debe estar en la misma subred que el puerto MGT. Por ejemplo, establezca la dirección IP del ordenador de gestión 192.168.1.5. 2. Conecte el dispositivo. **Nota** El dispositivo se activará tan pronto como se encienda la primera fuente de alimentación. Sonará un pitido de advertencia hasta que terminen de conectarse todas las fuentes de alimentación. Si el dispositivo ya está conectado, pero está apagado, utilice el botón de encendido de la parte frontal del dispositivo para encenderlo.
Paso 4	Restablezca la contraseña del administrador.	1. Inicie sesión en el dispositivo con un cliente de SSH o usando el puerto de la consola. Introduzca un nombre de usuario/contraseña de administrador/administrador. 2. Establezca una nueva contraseña ejecutando el comando: `admin@WF-500# set password` Introduzca la contraseña anterior, pulse Intro y, a continuación, introduzca y confirme la nueva contraseña. No hay necesidad de compilar la configuración porque se trata de un comando de operación. 3. Escriba `exit` para cerrar la sesión y, a continuación, vuelva a iniciarla para confirmar que se ha establecido la nueva contraseña.

INTEGRACIÓN DEL DISPOSITIVO WILDFIRE EN UNA RED (CONTINUACIÓN)	

Paso 5 Establezca la información de IP para la interfaz de gestión y el nombre de host para el dispositivo. Todos los cortafuegos que enviarán archivos al dispositivo WF-500 utilizarán el puerto MGT, por lo que debe asegurarse de que esta interfaz es accesible desde estos cortafuegos.
 	
En este ejemplo se utilizan los siguientes valores:
• Dirección IPv4: 10.10.0.5/22
• Máscara de subred: 255.255.252.0
• Puerta de enlace predeterminada: 10.10.0.1
• Nombre de host: wildfire-corp1
• Servidor DNS: 10.0.0.246
	1. Inicie sesión en el dispositivo con un cliente de SSH o usando el puerto de la consola y acceda al modo de configuración.
	`admin@WF-500> configure`
	2. Establezca la información de IP:
	`admin@WF-500# set deviceconfig system ip-address 10.10.0.5 netmask 255.255.252.0 default-gateway 10.10.0.1 dns-setting servers primary 10.0.0.246`
	Nota Puede configurar un servidor DNS secundario sustituyendo "primary" por "secondary" en el comando anterior, excluyendo el resto de parámetros IP. Por ejemplo:
	`admin@WF-500# set deviceconfig system dns-setting servers secondary 10.0.0.247`
	3. Establezca el nombre del host (wildfire-corp1 en este ejemplo):
	`admin@WF-500# set deviceconfig system hostname wildfire-corp1`
	4. Compile la configuración para activar la nueva configuración del puerto de gestión externo (MGT):
	`admin@WF-500# commit`
	5. Conecte el puerto de la interfaz de gestión a un conmutador de red.
	6. Vuelva a ubicar el PC de gestión en la red corporativa o en cualquier red necesaria para acceder al dispositivo en la red de gestión.
	7. Desde el ordenador de gestión, conéctese a la nueva dirección IP o nombre de host del puerto de gestión del dispositivo usando un cliente SSH. En este ejemplo, la nueva dirección IP es 10.10.0.5.

Paso 6 (opcional) Configure cuentas de usuario adicionales para gestionar el dispositivo WildFire. Se pueden asignar dos funciones: superusuario y superlector. El superusuario es equivalente al administrador, pero el superlector solo tiene acceso de lectura.	En este ejemplo, crearemos una cuenta de superlector para el usuario bsimpson:
	1. Introduzca el modo de configuración ejecutando el siguiente comando:
	`admin@WF-500> configure`
	2. Para crear la cuenta de usuario, introduzca el siguiente comando:
	`admin@WF-500# set mgt-config users bsimpson password`
	3. Introduzca y confirme la nueva contraseña.
	4. Para asignar la función de superlector, introduzca el siguiente comando y, a continuación, pulse Intro:
	`admin@WF-500# set mgt-config users bsimpson permissions role-based superreader yes`

INTEGRACIÓN DEL DISPOSITIVO WILDFIRE EN UNA RED (CONTINUACIÓN)		

Paso 7	Active el dispositivo con el código de autorización de WildFire que ha recibido de Palo Alto Networks.
	Nota El dispositivo WF-500 funcionará sin un código de autenticación, pero las nuevas actualizaciones de software no pueden instalarse sin un código de autenticación válido.
		1. Vaya al modo de operación para ejecutar los siguientes comandos:
		`admin@WF-500> exit`
		2. Obtenga e instale la licencia de WildFire:
		`admin@WF-500> request license fetch auth-code auth-code`
		3. Pulse Intro para obtener e instalar la licencia.
		4. Verifique la licencia:
		`admin@WF-500> request license info`
		Debe aparecer una licencia activa con una fecha posterior a la fecha actual.

Paso 8	Establezca la fecha/hora actual y la zona horaria.	1. Establezca la fecha y la hora:
		`admin@WF-500> set clock date YY/MM/DD time hh:mm:ss`
		2. Acceda al modo de configuración:
		`admin@WF-500> configure`
		3. Establezca la zona horaria local:
		`admin@WF-500# set deviceconfig system timezone timezone`
		Nota La marca de hora que aparecerá en el informe detallado de WildFire utilizará la zona horaria establecida en el dispositivo. Si hay varias personas viendo estos informes, puede que desee establecer la zona horaria en UTC.

Paso 9	(Opcional) Configure el envío automático para que el dispositivo WildFire envíe archivos que contengan malware a la nube WildFire de Palo Alto Networks. El sistema de nube de WildFire generará firmas, que se distribuyen mediante las actualizaciones de firma de WildFire y del antivirus.
	Nota Esta opción está deshabilitada de manera predeterminada.
		1. Para habilitar el envío automático, ejecute el comando:
		`admin@WF-500# set deviceconfig setting wildfire auto-submit yes`
		2. Para confirmar el ajuste, ejecute el siguiente comando desde el modo de operación:
		`admin@WF-500> show wildfire status`

INTEGRACIÓN DEL DISPOSITIVO WILDFIRE EN UNA RED (CONTINUACIÓN)	
Paso 10 Establezca una contraseña para la cuenta de administrador del portal. Esta cuenta se utiliza cuando se accede a los informes de WildFire desde un cortafuegos. El nombre de usuario y la contraseña predeterminados son admin/admin. **Nota** La cuenta del administrador del portal es la única cuenta utilizada para ver informes desde los logs. Solo se puede cambiar la contraseña de esta cuenta; no se pueden crear cuentas adicionales. No es la misma cuenta de administrador utilizada para gestionar el dispositivo.	Para cambiar la contraseña de la cuenta del administrador del portal de WildFire: 1. `admin@WF-500# set wildfire portal-admin password` 2. Pulse Intro y escriba y confirme la nueva contraseña.

¿Cuál es el siguiente paso?:

- Para verificar la configuración del dispositivo WF-500, consulte "Verificación de la configuración del dispositivo WF-500 WildFire" en la página 15.
- Para empezar a enviar archivos desde un cortafuegos, consulte "Reenvío de archivos a un dispositivo WF-500 WildFire" en la página 24.
- Para actualizar el software del dispositivo WildFire, consulte "Actualización del software del dispositivo WF-500 WildFire" en la página 22.
- Para configurar la interfaz vm que utiliza el dispositivo como parte de su análisis de malware, consulte "Configuración de interfaz de la máquina virtual" en la página 17.

Verificación de la configuración del dispositivo WF-500 WildFire

En esta sección se describen los pasos necesarios para verificar la configuración del dispositivo WildFire para garantizar que está listo para recibir archivos desde un cortafuegos de Palo Alto Networks. Para obtener información más detallada sobre los comandos de la CLI a los que se hace referencia en este flujo de trabajo, consulte "Referencia de la CLI del software del dispositivo WildFire" en la página 63.

VERIFICACIÓN DE LA CONFIGURACIÓN DEL DISPOSITIVO WILDFIRE	

Paso 1. Compruebe que el dispositivo está registrado y que la suscripción se ha activado.	1. Inicie una sesión SSH en la interfaz de gestión del dispositivo.
	2. Desde la CLI, introduzca el siguiente comando:
	`admin@WF-500> request license info`
	
	Compruebe que la licencia es válida y que el valor del campo `Expired:` aparece como `no`.
	Por ejemplo:
	`Feature: Premium`
	`Description: 24x7 phone support; advanced replacement hardware service`
	`Serial: 009707000000`
	`Issued: February 11, 2013`
	`Expires: February 11, 2016`
	`Expired?: no`
	3. En aquellos dispositivos habilitados para el envío automático, compruebe que el dispositivo WildFire se puede comunicar con la nube WildFire de Palo Alto Networks introduciendo el siguiente comando:
	`admin@WF-500> test wildfire registration`
	
	El siguiente resultado indica que el dispositivo está registrado en uno de los servidores de nube WildFire de Palo Alto Networks. Si el envío automático está habilitado, los archivos infectados con malware se enviarán a este servidor.
	`Test wildfire`
	`wildfire registration: successful`
	`download server list: successful`
	`select the best server:`
	`cs-s1.wildfire.paloaltonetworks.com`
	
	Nota El dispositivo sólo enviará archivos a la nube de WildFire si el envío automático está habilitado. Para obtener información sobre cómo habilitar el envío automático, consulte las instrucciones de "Realización de la configuración inicial" en la página 10.

VERIFICACIÓN DE LA CONFIGURACIÓN DEL DISPOSITIVO WILDFIRE (CONTINUACIÓN)

Paso 2 Compruebe el estado del servidor WildFire en el dispositivo.

1. El siguiente comando muestra el estado de WildFire:

```
admin@WF-500> show wildfire status
```

A continuación aparece un resultado de ejemplo:

```
Connection info:
        Wildfire cloud:           wildfire-public-cloud
        Status:                   Idle
        Auto-Submit:              enabled
        VM internet connection:   disabled
        Best server:
        Device registered:        yes
        Service route IP address: 192.168.2.20
        Signature verification:   enable
        Server selection:         enable
        Through a proxy:          no
```

En este ejemplo, el envío automático está habilitado, lo que significa que los archivos identificados como malware se reenviarán a la nube WildFire de Palo Alto Networks. Las firmas se pueden generar para proteger frente a futuras exposiciones a malware. El estado `Idle` indica que el dispositivo está listo para recibir archivos. `Device registered` muestra `yes`, lo que significa que el dispositivo está registrado en el sistema de nube de WildFire.

2. Para comprobar que el dispositivo está recibiendo archivos desde los cortafuegos y que está enviando archivos a la nube de WildFire para la generación de firmas (si el envío automático está habilitado), introduzca el siguiente comando:

```
admin@WF-500> show wildfire statistics
days 7
```

```
Last one hour statistics:
Total sessions submitted  :            0
Samples submitted         :            0
Samples analyzed          :            0
Samples pending           :            0
Samples (malicious)       :            0
Samples (benign)          :            0
Samples (error)           :            0
Malware sent to cloud     :            0

Last 7 days statistics:
Total sessions submitted  :           66
Samples submitted         :           34
Samples analyzed          :           34
Samples pending           :            0
Samples (malicious)       :            2
Samples (benign)          :           32
Samples (error)           :            0
Malware sent to cloud     :            0
```

3. Para ver estadísticas más detalladas, introduzca el siguiente comando:

```
admin@WF-500> show wildfire latest
[analysis |samples | sessions | uploads]
```

Por ejemplo, para mostrar detalles sobre los últimos 30 resultados del análisis, introduzca el siguiente comando:

```
admin@WF-500> show wildfire latest
analysis
```

VERIFICACIÓN DE LA CONFIGURACIÓN DEL DISPOSITIVO WILDFIRE (CONTINUACIÓN)	

Paso 3 Compruebe que los cortafuegos configurados para enviar archivos se han registrado correctamente en el dispositivo WildFire.	1. Introduzca el siguiente comando para que muestre una lista de cortafuegos registrados en el dispositivo:
	`admin@WF-500> show wildfire last-device-registration all`
	
	El resultado mostrará la siguiente información sobre cada cortafuegos registrado para enviar archivos al dispositivo: número de serie del cortafuegos, fecha de registro, dirección IP, versión de software, modelo de hardware y estado. Si no aparece ningún cortafuegos, puede que haya algún problema de conectividad entre los cortafuegos y el dispositivo. Compruebe la red para confirmar que los cortafuegos y el dispositivo WildFire se pueden comunicar.
	
	Utilice las pruebas de ping desde el dispositivo hasta la dirección de la puerta de enlace o a uno de los cortafuegos configurados para enviar al dispositivo Por ejemplo, si uno de los cortafuegos está en la dirección IP 10.0.5.254, las respuestas se mostrarán cuando se ejecute el siguiente comando de la CLI desde el dispositivo:
	`admin@WF-500> ping host 10.0.5.254`

Configuración de interfaz de la máquina virtual

La interfaz de la máquina virtual proporciona conectividad de red externa a las máquinas virtuales de los elementos de aislamiento en el dispositivo WF-500. En las siguientes secciones se describe la interfaz de la máquina virtual (interfaz vm) y se proporcionan las instrucciones necesarias para configurarla. También se proporcionan las instrucciones necesarias para conectar la interfaz a un puerto especializado en un cortafuegos de Palo Alto Networks para habilitar la conectividad a Internet.

- ¿Qué es la interfaz de la máquina virtual?
- Configuración de la interfaz de la máquina virtual
- Configuración del cortafuegos para controlar el tráfico de la interfaz de la máquina virtual

¿Qué es la interfaz de la máquina virtual?

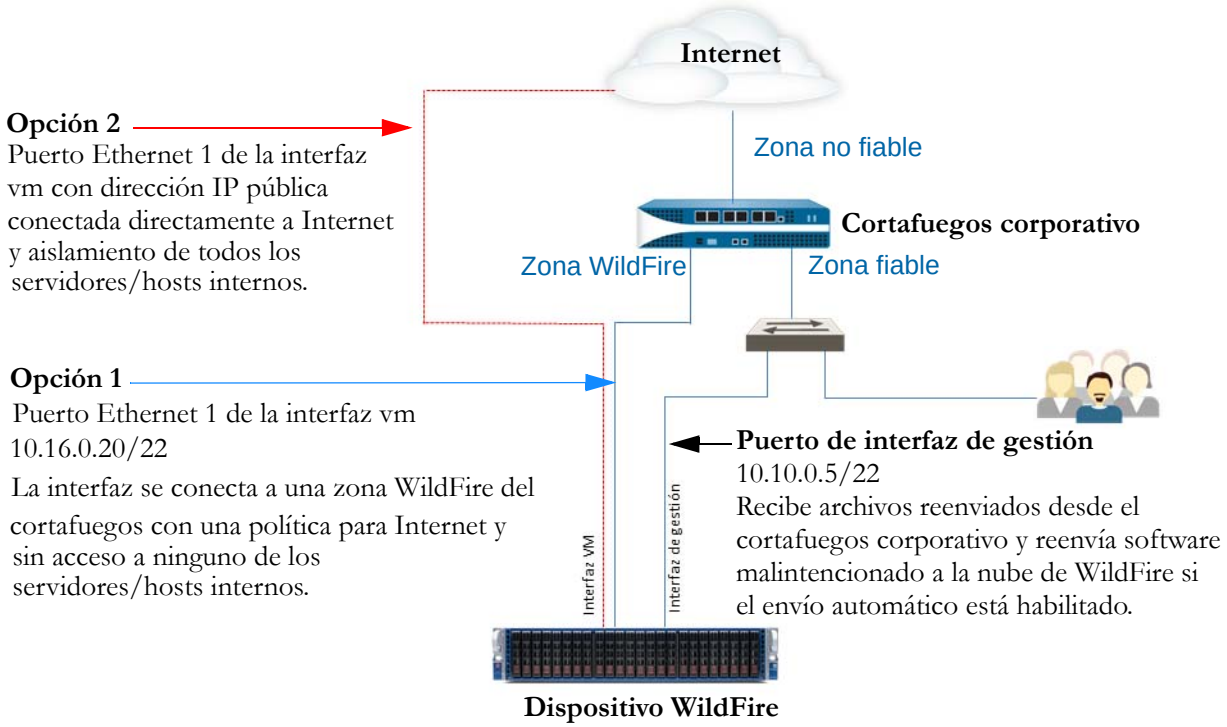
Cuando esté configurada y habilitada, la interfaz vm (con la etiqueta **1** en la parte posterior del dispositivo) contará con capacidades de detección de malware mejoradas. Esta interfaz permite que un archivo de muestra que se ejecuta en las máquinas virtuales de WildFire se comunique con Internet y permite a WildFire analizar mejor el comportamiento del archivo de muestra para determinar si muestra las características del malware.

Cuidado

Aunque se recomienda que la interfaz vm esté habilitada, es muy importante que no esté conectada a una red que permita el acceso a cualquiera de los servidores/hosts ya que el malware que se ejecuta en las máquinas virtuales de WildFire podría utilizar esta interfaz para propagarse.

Esta conexión puede ser una línea DSL especializada o un conexión de red que solo permita el acceso directo desde la interfaz a Internet y restrinja cualquier acceso a servidores internos/hosts de cliente.

En la siguiente ilustración se muestran dos opciones para conectar la interfaz vm a la red.



- **Opción 1 (recomendada):** La interfaz vm se conecta a un interfaz en una zona especializada de un cortafuegos con una política que solo permite el acceso a Internet. Es importante porque el malware que se ejecuta en las máquinas virtuales de WildFire puede utilizar potencialmente esta interfaz para propagarse. Es la opción recomendada porque los logs del cortafuegos proporcionarán visibilidad en cualquier tráfico generado por la interfaz vm.

- **Opción 2**: Utilice una conexión especializada del proveedor de Internet, como una conexión DSL, para conectar la interfaz vm a Internet. Asegúrese de que no hay acceso desde esta conexión a servidores/hosts internos. Aunque es una solución simple, el tráfico generado por la interfaz vm no se registrará a no ser que se coloque un cortafuegos o una herramienta de supervisión de tráfico entre el dispositivo WildFire y la conexión DSL.

Configuración de la interfaz de la máquina virtual

En esta sección aparecen las instrucciones necesarias para configurar la interfaz vm en el dispositivo WildFire usando la configuración de la opción 1 detallada en el flujo de trabajo anterior. Después de configurar la interfaz vm usando esta opción, también debe configurar una interfaz en un cortafuegos de Palo Alto Networks por el que se enrutará el tráfico desde la interfaz vm, según se describe en "Configuración del cortafuegos para controlar el tráfico de la interfaz de la máquina virtual" en la página 20.

De forma predeterminada, la interfaz vm está configurada usando los siguientes ajustes:
Dirección IP: 192.168.2.1
Máscara de red: 255.255.255.0
Puerta de enlace predeterminada: 192.168.2.254
DNS: 192.168.2.254
Si tiene pensado habilitar esta interfaz, configúrela con los ajustes adecuados para la red. Si no tiene pensando utilizar esta interfaz, respete los ajustes predeterminados. Si se elimina la configuración, se producirán fallos de compilación.

CONFIGURACIÓN DE LA INTERFAZ DE LA MÁQUINA VIRTUAL		

Paso 1	Establezca la información de la IP para la interfaz vm en el dispositivo WildFire. Se utilizará lo siguiente para este ejemplo:
	• Dirección IPv4: 10.16.0.20/22
	• Máscara de subred: 255.255.252.0
	• Puerta de enlace predeterminada: 10.16.0.1
	• Servidor DNS: 10.0.0.246
	Nota La interfaz vm no puede estar en la misma red que la interfaz de gestión (MGT).
		1. Introduzca el modo de configuración introduciendo el comando de la CLI:
		`admin@WF-500> configure`
		2. Establezca la información de IP para la interfaz vm:
		`admin@WF-500# set deviceconfig system vm-interface ip-address 10.16.0.20 netmask 255.255.252.0 default-gateway 10.16.0.1 dns-server 10.0.0.246`
		Nota Solo se puede asignar un servidor DNS a la interfaz vm. Se recomienda utilizar el servidor NS del ISP o un servicio DNS abierto.

Paso 2	Habilite la interfaz vm.	1. Para habilitar la interfaz vm.
		`admin@WF-500# set deviceconfig setting wildfire vm-network-enable yes`
		2. Confirme la configuración:
		`admin@WF-500# commit`

Paso 3	Continúe en la siguiente sección para configurar la interfaz del cortafuegos a la que se conectará la interfaz vm.	Consulte "Configuración del cortafuegos para controlar el tráfico de la interfaz de la máquina virtual" en la página 20.

Configuración del cortafuegos para controlar el tráfico de la interfaz de la máquina virtual

En el siguiente flujo de trabajo de ejemplo se describe cómo conectar la interfaz vm a un puerto en un cortafuegos de Palo Alto Networks. Antes de conectar la interfaz vm al cortafuegos, este debe tener una zona no fiable conectada a Internet. En este ejemplo, se configura una nueva zona denominada "wf-vm-zone" para conectar la interfaz vm del dispositivo al cortafuegos. La política asociada con la zona wf-vm solo permitirá la comunicación desde la interfaz vm hasta la zona no fiable.

CONFIGURACIÓN DE LA INTERFAZ DEL CORTAFUEGOS PARA LA RED DE LA MÁQUINA VIRTUAL		
Paso 1	Configure la interfaz en el cortafuegos al que se conectará la interfaz vm y establezca el enrutador virtual. **Nota** La zona wf-vm configurada en este paso solo se debe utilizar para conectar la interfaz vm desde el dispositivo al cortafuegos. No añada ninguna otra interfaz a la zona wf-vm porque el tráfico en el interior de la zona se habilitará de forma predeterminada, lo que permitiría al tráfico de la interfaz vm acceder a una red distinta a Internet.	1. En la interfaz web del cortafuegos, seleccione **Red > Interfaces** y, a continuación, seleccione una interfaz, por ejemplo **Ethernet1/3**. 2. Seleccione **Tipo de interfaz Capa3**. 3. En la pestaña **Configurar**, cuadro desplegable **Zona de seguridad**, seleccione **Nueva zona**. 4. En el campo **Name (Nombre)** del cuadro de diálogo Zona, introduzca **vf-vm-zone** y, a continuación, haga clic en **ACEPTAR**. 5. En el cuadro desplegable **Enrutador virtual**, seleccione **predeterminado**. 6. Para asignar una dirección IP a la interfaz, seleccione la pestaña **IPv4**, haga clic en **Añadir** en la sección IP e introduzca la dirección IP y la máscara de red para asignarlas a la interfaz, por ejemplo, 10.16.0.0/22. 7. Para guardar la configuración de la interfaz, haga clic en **Aceptar**.
Paso 2	Cree una política de seguridad en el cortafuegos para permitir el acceso desde la interfaz vm a Internet y bloquear todo el tráfico entrante. En este ejemplo, el nombre de la política es **Interfaz VM de WildFire**. Como no se creará una política de seguridad desde la zona no fiable a la zona de interfaz wf-vm, todo el tráfico entrante se bloqueará de forma predeterminada.	1. Seleccione **Políticas > Seguridad** y haga clic en **Añadir** 2. En la pestaña **General**, campo **Name (Nombre)**, introduzca **Interfaz VM de WildFire**. 3. En la pestaña **Origen**, establezca la **zona de origen** como **wf-vm-interface**. 4. En la pestaña **Destino**, establezca la **zona de destino** como **No fiable**. 5. En las pestañas **Aplicación** y **Categoría de URL/servicio**, deje de forma predeterminada **Cualquiera**. 6. En la pestaña **Acciones**, establezca **Configuración de acción** como **Permitir**. 7. En **Ajuste de log**, seleccione la casilla de verificación **Log al finalizar sesión**. **Nota** Si le preocupa que alguien pueda añadir de forma accidental otras interfaces a la zona wf-vm, clone la política de la seguridad de la interfaz VM de WildFire y, a continuación, en la pestaña **Acción** de la regla clonada, seleccione **Denegar**. Asegúrese de que esta nueva política de seguridad aparece bajo la política de seguridad de la interfaz VM de WildFire. Esto hará que la intrazona implícita active la regla que permite sobrescribir las comunicaciones entre interfaces de la misma zona y denegará/bloqueará cualquier comunicación intrazona.

CONFIGURACIÓN DE LA INTERFAZ DEL CORTAFUEGOS PARA LA RED DE LA MÁQUINA VIRTUAL (CONTINUACIÓN)		
Paso 3	Conecte los cables.	Conecte físicamente la interfaz vm del dispositivo WildFire al puerto que ha configurado en el cortafuegos (Ethernet 1/3 en este ejemplo) usando un cable RJ-45 directo. La interfaz vm aparece con la etiqueta **1** en la parte posterior del dispositivo.

Paso 4	Compruebe que la interfaz vm está transmitiendo y recibiendo tráfico.	1. Desde el modo de operación de la CLI del dispositivo WildFire ejecute el siguiente comando:
		`admin@WF-500> show interface vm-interface`
		2. Aparecerán todos los contadores de la interfaz. Compruebe que los contadores recibidos/transmitidos han aumentado. Ejecute el siguiente comando para generar tráfico ping:
		`admin@WF-500> ping source` *`vm-interface-ip`* `host` *`gateway-ip`*
		Por ejemplo:
		`admin@WF-500> ping source 10.16.0.20 host 10.16.0.1`

Actualización del software del dispositivo WF-500 WildFire

En esta sección se proporcionan las instrucciones necesarias para actualizar el software del dispositivo WildFire en un dispositivo WF-500 WildFire. Las actualizaciones de software contienen las últimas características y soluciones de problemas para el software. El dispositivo se puede actualizar usando el servidor de actualización de Palo Alto Networks o descargando e instalando las actualizaciones manualmente (consulte "Actualización manual del software" en la página 23). Para obtener detalles sobre una versión específica del software, consulte las notas de la versión correspondiente.

ACTUALIZACIÓN DEL SOFTWARE DEL DISPOSITIVO WF-500 WILDFIRE		

Paso 1	Consulte la versión actual del software del dispositivo WildFire en el dispositivo y compruebe si hay una nueva versión disponible.	1. Introduzca el siguiente comando y compruebe el campo `sw-version`:
		`admin@WF-500> show system info`
		2. Introduzca el siguiente comando para ver las últimas versiones:
		`admin@WF-500> request system software check`
		Nota Si el dispositivo no puede ponerse en contacto con el servidor de actualización de Palo Alto Networks, asegúrese de que cuenta con una licencia y de que el DNS está resolviendo correctamente. También puede probar desde el dispositivo haciendo ping al servidor de actualización de Palo Alto Networks para asegurarse de que es posible acceder. Ejecute el siguiente comando de la CLI:
		`admin@WF-500> ping host updates.paloaltonetworks.com`

Paso 2	Descargue e instale una nueva versión del software del dispositivo WildFire.	1. Para instalar una nueva versión del software, utilice el siguiente comando:
		`admin@WF-500> request system software download file` *`nombre de archivo`*
		Por ejemplo:
		`admin@WF-500> request system software download file WildFire_m-5.1.0`
		2. Compruebe que el archivo ha terminado de descargarse utilizando el siguiente comando:
		`admin@WF-500> show jobs pending`
		o
		`admin@WF-500> show jobs all`
		3. Después de se descargue el archivo, instálelo usando el siguiente comando:
		`admin@WF-500> request system software install file` *`nombre de archivo`*
		Por ejemplo:
		`admin@WF-500> request system software install file WildFire_m-5.1.0`

ACTUALIZACIÓN DEL SOFTWARE DEL DISPOSITIVO WF-500 WILDFIRE (CONTINUACIÓN)	

Paso 3 Después de que se instale la nueva versión, reinicie el dispositivo.	1. Supervise el estado de la actualización usando el siguiente comando:
	`admin@WF-500> show jobs pending`
	2. Después de se actualice el archivo, reinicie el dispositivo usando el siguiente comando:
	`admin@WF-500> request restart system`
	3. Después de reiniciar, verifique que la nueva versión está instalada ejecutando el siguiente comando de la CLI y compruebe el campo `sw-version`:
	`admin@WF-500> show system info`

Actualización manual del software

Si el dispositivo WildFire no cuenta con conectividad de red a los servidores de actualización de Palo Alto Networks, puede actualizar manualmente el software.	1. Acceda a https://support.paloaltonetworks.com/ y en la sección **Manage Devices (Gestionar dispositivos)**, haga clic en **Software Updates (Actualizaciones de software)**.
	2. Descargue el archivo de imagen del software de WildFire que desea instalar en un ordenador que ejecuta el software del servidor SCP.
	3. Importe el archivo de imagen del software desde el servidor SCP:
	`scp import software from` *`nombredeusuario@direccion_ip/archivo de imagen del nombre de carpeta`*
	
	Por ejemplo:
	`admin@WF-500> scp import software from user1@10.0.3.4:/tmp/WildFire_m-5.1.0`
	4. Instale el archivo de imagen:
	`admin@WF-500> request system software install file` *`nombredelarchivodeimagen`*
	5. Después de que finalice la actualización, reinicie el dispositivo.
	`admin@WF-500> request restart system`
	6. Después de reiniciar, verifique que la nueva versión está instalada introduciendo el siguiente comando de la CLI y compruebe el campo `sw-version`:
	`admin@WF-500> show system info`

Reenvío de archivos a un dispositivo WF-500 WildFire

En esta sección se describen los pasos necesarios para la configuración de un cortafuegos de Palo Alto Networks para que empiece a reenviar archivos a un dispositivo WF-500 WildFire y se describe cómo verificar la configuración del dispositivo.

Aunque el cortafuegos puede reenviar a cualquier dispositivo WildFire (es necesaria la suscripción a WildFire) o a la nube de WildFire, para obtener una mayor visibilidad, asegúrese de que todos los cortafuegos indican el mismo sistema WildFire. En los cortafuegos gestionados por Panorama, simplifique la administración de WildFire usando plantillas de Panorama para introducir la información del servidor WildFire, el tamaño de archivo permitido y los ajustes de información de la sesión en los cortafuegos. Utilice los grupos de dispositivos de Panorama para configurar e introducir los perfiles de bloqueo de los archivos y las reglas de las políticas de seguridad. Panorama solo puede indicar un sistema WildFire (dispositivo o nube).

Si hay un cortafuegos entre el cortafuegos que está reenviando los archivos a WildFire y la nube de WildFire o el dispositivo WildFire, asegúrese de que el cortafuegos intermedio permite los puertos necesarios.

- Nube de WildFire: Utiliza el puerto 443 para registro y envío de archivos.
- Dispositivo WildFire: Utiliza el puerto 443 para registro y el 10443 para envío de archivos.

Siga estas instrucciones en todos los cortafuegos que reenviarán archivos al dispositivo WildFire:

CONFIGURACIÓN DEL REENVÍO AL DISPOSITIVO WF-500 WILDFIRE		
Paso 1	Compruebe que el cortafuegos tiene una suscripción a WildFire y que las actualizaciones dinámicas están programadas y actualizadas.	1. Acceda a **Dispositivo > Licencias** y confirme que el cortafuegos tiene instaladas suscripciones WildFire y de prevención de amenazas válidas. 2. Acceda a **Dispositivo > Actualizaciones dinámicas** y haga clic en **Comprobar ahora** para asegurarse de que el cortafuegos tiene las actualizaciones más recientes del antivirus, aplicaciones y amenazas y WildFire. 3. Si las actualizaciones no están programadas, hágalo ahora. Asegúrese de escalonar la programación de las actualizaciones porque solo se puede realizar una cada vez. Consulte "Recomendaciones para actualizaciones dinámicas" en la página 28 para conocer la configuración recomendada.

CONFIGURACIÓN DEL REENVÍO AL DISPOSITIVO WF-500 WILDFIRE (CONTINUACIÓN)		
Paso 2	Defina el servidor WildFire al que reenviará archivos el cortafuegos para su análisis.	1. Acceda a **Dispositivo > Configuración > WildFire**. 2. Haga clic en el icono de edición **Configuración general**. 3. En el campo **Servidor WildFire**, introduzca la dirección IP o FQDN del dispositivo WF-500 WildFire. **Nota** La mejor forma de devolver el campo **Servidor WildFire** a sus valores predeterminados es borrar el campo y hacer clic en **ACEPTAR**. Así se garantiza que se añade el valor correcto. Del mismo modo, cuando utilice un dispositivo WildFire, asegúrese de que no está habilitada la opción Deshabilitar selección de servidor o de lo contrario el cortafuegos no podrá enviar archivos desde el dispositivo. Ejecute el siguiente comando y confirme que Deshabilitar selección de servidor no está establecido en "**sí**": `admin@PA-200# show deviceconfig setting wildfire` Esta opción está desactivada de forma predefinida, de modo que no mostrará la configuración a no ser que lo establezca en "no" o en "sí". También puede comprobar su configuración actual ejecutando el comando: `admin@PA-200# show config running | match wildfire` Con este comando se mostrarán todos los parámetros de WildFire.

CONFIGURACIÓN DEL REENVÍO AL DISPOSITIVO WF-500 WILDFIRE (CONTINUACIÓN)

Paso 3 Configure el perfil de bloqueo del archivo para definir qué aplicaciones y tipos de archivos activarán el reenvío a WildFire.

Nota Al seleccionar **PE** en la columna Tipos de archivos del perfil de objetos para seleccionar una categoría o tipos de archivos, no añada un tipo de archivo individual que forme parte de esa categoría porque esto produciría entradas redundantes en los logs Filtrado de datos. Por ejemplo, si selecciona PE, no seleccione también **exe** porque es parte de la categoría de PE. Esto también es aplicable al tipo de archivo **zip**, ya que los tipos de archivos admitidos que se compriman se envían automáticamente a WildFire.

Al seleccionar una categoría en lugar de un tipo de archivo individual también se garantiza que, como la compatibilidad con un nuevo tipo de archivo se añade a una categoría específica, automáticamente pasará a formar parte del perfil de bloqueo del archivo. Si selecciona **Cualquiera**, todos los tipos de archivos admitidos se reenviarán a WildFire.

1. Desplácese hasta **Objetos > Perfiles de seguridad > Bloqueo de archivos**.
2. Haga clic en **Añadir** para añadir un nuevo perfil e introduzca un **Nombre** y una **Descripción**.
3. Haga clic en **Añadir** en la ventana **Perfil de bloqueo de archivo** y, a continuación, haga clic en **Añadir** de nuevo. Haga clic en el campo **Nombres** e introduzca un nombre para la regla.
4. Seleccione las **aplicaciones** que coincidirán con este perfil. Por ejemplo, si selecciona **navegación web** como la aplicación, el perfil coincidirá con cualquier tráfico de la aplicación identificado como "navegación web".
5. En el campo **Tipo de archivo**, seleccione los tipos de archivos que activarán la acción de reenvío. Seleccione **Cualquiera** para reenviar todos los tipos de archivo admitidos por WildFire o seleccione **PE** para que solo reenvíe archivos Portable Executable.
6. En el campo **Dirección**, seleccione **cargar**, **descargar** o **ambos**. Si selecciona **ambos** se activará el reenvío siempre que un usuario trate de cargar o descargar un archivo.
7. Defina una **acción** de la siguiente forma (seleccione **Reenviar** para este ejemplo):
   - **Reenviar**: el cortafuegos reenviará automáticamente cualquier archivo que coincida con este perfil a WildFire para su análisis, además de distribuir el archivo al usuario.
   - **Continuar y reenviar**: se le indica al usuario que debe hacer clic en **Continuar** antes de que se produzca la descarga y que se reenvíe el archivo a WildFire. Como aquí se necesita de la acción del usuario en un navegador web, solo es compatible con aplicaciones de navegación web.

   Nota Cuando utilice **Continuar y reenviar**, asegúrese de que la interfaz de entrada (la que recibe en primer lugar el tráfico para sus usuarios) tiene un perfil de gestión adjunto que permite páginas de respuesta. Para configurar un perfil de gestión, seleccione **Red > Perfiles de red > Gestión de interfaz** y seleccione la casilla de verificación **Páginas de respuesta**. Instale el perfil de gestión en la pestaña **Avanzado** en la configuración de la interfaz de entrada.
8. Haga clic en **ACEPTAR** para guardar los cambios.

CONFIGURACIÓN DEL REENVÍO AL DISPOSITIVO WF-500 WILDFIRE (CONTINUACIÓN)		
Paso 4	Para reenviar archivos a WildFire desde sitios web usando el cifrado SSL, habilite el reenvío de contenido descifrado. Para obtener información sobre la configuración del descifrado, consulte la Palo Alto Networks Getting Started Guide (Guía de inicio de Palo Alto Networks). **Nota** Solo puede habilitar esta opción un superusuario.	1. Vaya a **Dispositivo > Configuración > ID de contenido**. 2. Haga clic en el icono de edición de las opciones **Filtrado de URL** y habilite **Permitir reenvío de contenido descifrado**. 3. Haga clic en **ACEPTAR** para guardar los cambios. **Nota** Si el cortafuegos tiene múltiples sistemas virtuales, debe habilitar esta opción por VSYS. En esta situación, acceda a **Dispositivo > Sistemas virtuales**, haga clic en el sistema virtual que desea modificar y seleccione la casilla de verificación **Permitir reenvío de contenido descifrado**.
Paso 5	Adjunte el perfil de bloqueo de archivos a una política de seguridad.	1. Desplácese hasta **Políticas > Seguridad**. 2. Haga clic en **Añadir** para crear una nueva política para las zonas a las que está aplicando el reenvío de WildFire o seleccione una política de seguridad existente. 3. En la pestaña **Acciones**, seleccione el perfil **Bloqueo de archivo** en el menú desplegable. **Nota** Si esta regla de seguridad no tiene ningún perfil adjunto, seleccione **Perfiles** en el menú **Tipo de perfil** para habilitar la selección de un perfil de bloqueo de archivos.
Paso 6	(Opcional) Modifique el tamaño máximo del archivo que puede cargar el cortafuegos en WildFire.	1. Acceda a **Dispositivo > Configuración > WildFire**. 2. Haga clic en el icono de edición **Configuración general**. 3. En el campo **Tamaño de archivo máximo (MB)**, introduzca el tamaño máximo de archivo para los archivos enviados a WildFire para su análisis (intervalo 1-10 MB; de forma predeterminada 2 MB).
Paso 7	(Opcional) Modifique las opciones de la sesión que definen qué información de sesión se debe registrar en los informes de análisis de WildFire.	1. Haga clic en el icono de edición de **Ajustes de información de sesión**. 2. De forma predeterminada, todos los elementos de información de la sesión aparecerán en los informes. Borre las casillas de verificación que correspondan a campos que desee eliminar de los informes de análisis de WildFire. 3. Haga clic en **ACEPTAR** para guardar los cambios.
Paso 8	Compile la configuración.	Haga clic en **Compilar** para aplicar los cambios. Durante la evaluación de la política de seguridad, todos los archivos que cumplan los criterios definidos en la política de bloqueo de archivos se reenviarán a WildFire para su análisis. Para obtener información sobre cómo consultar los informes de los archivos que se han analizado, consulte "Supervisión, control y prevención del malware en la red" en la página 47. Para obtener instrucciones sobre cómo comprobar la configuración, consulte "Comprobación de la configuración de WildFire en el cortafuegos" en la página 29.

Recomendaciones para actualizaciones dinámicas

En la siguiente lista se detallan recomendaciones para conseguir actualizaciones dinámicas en un cortafuegos típico que utilice WildFire y que tenga suscripciones a WildFire y prevención de amenazas. Para un flujo de trabajo más dinámico, utilice Panorama para introducir programaciones de actualización dinámicas en los cortafuegos gestionados usando plantillas de Panorama. Así se garantiza la consistencia entre todos los cortafuegos y se simplifica la gestión de la programación de actualizaciones.

Estas orientaciones proporcionan dos opciones de programación: la programación mínima recomendada y una más agresiva. Si elige un enfoque más agresivo, el dispositivo realizará actualizaciones más frecuentemente, algunas de las cuales pueden ser de gran volumen (más de 100 MB para las actualizaciones de antivirus). De igual forma, raramente se podrían producir errores. Por lo tanto, considere retrasar la instalación de nuevas actualizaciones hasta que se no hayan publicado un determinado número de horas. Utilice el campo **Umbral (horas)** para especificar cuánto tiempo se debe esperar tras una publicación antes de realizar una actualización de contenido.

- **Antivirus**: se publican nuevas actualizaciones de contenido antivirus diariamente. Para obtener el contenido más reciente, programe estas actualizaciones diariamente como mínimo. Se puede realizar una programación más agresiva cada hora.
- **Aplicaciones y amenazas**: App-ID nuevo, protección de vulnerabilidad y firmas antispyware se publican como actualizaciones de contenido semanales (normalmente los martes). Para obtener el contenido más reciente, programe estas actualizaciones semanalmente como mínimo. Si desea un enfoque más agresivo, realice una programación diaria que garantice que el cortafuegos recibe el contenido más reciente tan pronto como es publicado (incluidas publicaciones ocasionales de contenido urgente fuera de programación).
- **WildFire**: se publican nuevas firmas de antivirus de WildFire cada 30 minutos. Dependiendo de cuándo se descubre el malware en el ciclo de publicación, la cobertura se proporcionará en forma de firma de WildFire 30-60 minutos después de que WildFire lo descubra. Para conseguir las firmas de WildFire más recientes, programe estas actualizaciones cada hora o cada media hora. Para que la programación sea más agresiva, puede programar la búsqueda de actualizaciones del cortafuegos con una frecuencia de 15 minutos.

Aunque las actualizaciones de WildFire pueden entrar en conflicto con la actualización de un antivirus o firma de amenazas, la actualización debe ser finalizar con éxito, ya que es mucho más pequeña que la típica actualización de aplicación/antivirus y firma de amenazas. Cada actualización de WildFire suele contener firmas generadas en los últimos 7 días; en ese momento entran a formar parte de la actualización de la firma antivirus cada 24-48 horas.

Comprobación de la configuración de WildFire en el cortafuegos

En esta sección se describen los pasos necesarios para comprobar la configuración de WildFire en el cortafuegos.

COMPROBACIÓN DE LA CONFIGURACIÓN DE WILDFIRE EN EL CORTAFUEGOS		

Paso 1	Compruebe las suscripciones de WildFire y prevención de amenazas y el registro de WildFire.
	Nota El cortafuegos debe tener una suscripción a WildFire para reenviar archivos a un dispositivo WildFire.
		1. Acceda a **Dispositivo > Licencias** y confirme que se ha instalado una suscripción válida de WildFire y prevención de amenazas. Si no hay instaladas licencias válidas, vaya a la sección **Gestión de licencias** y haga clic en **Recuperar claves de licencia del servidor de licencias**.
		2. Para comprobar que el cortafuegos se puede comunicar con un sistema WildFire, de forma que los archivos se puedan reenviar para su análisis, ejecute el siguiente comando de la CLI:
		`admin@PA-200> test wildfire registration`
		En la siguiente salida, el cortafuegos indica un dispositivo WildFire. Si el cortafuegos indica la nube de WildFire, mostrará el nombre de host de uno de los sistemas WildFire en la nube de WildFire.
		`Test wildfire`
		`wildfire registration: successful`
		`download server list: successful`
		`select the best server: 192.168.2.20:10443`
		3. Si los problemas con las licencias continúan, póngase en contacto con su distribuidor o con un ingeniero de sistemas de Palo Alto Networks para confirmar todas las licencias y conseguir un nuevo código de autorización si es necesario.

Paso 2	Confirme que el cortafuegos está enviando archivos al sistema WildFire correcto.	1. Para determinar si el cortafuegos está reenviando archivos (a la nube WildFire de Palo Alto Networks o a un dispositivo WildFire), vaya a **Dispositivo > Configuración > WildFire**. 2. Haga clic en el botón de edición **Configuración general**. 3. Si el cortafuegos está reenviando archivos a la nube de WildFire, este campo debería aparecer como **default-cloud**. Si está reenviando archivos a un dispositivo WildFire, aparecerán la dirección IP o FQDN del dispositivo WildFire. En Panorama, el nombre predeterminado de la nube es **wildfire-public-cloud**. **Nota** Si ha modificado el valor de este campo, pero quiere volver al ajuste **default-cloud**, borre el campo **Servidor WildFire** y haga clic en **ACEPTAR**. Así restaurará el campo a su valor predeterminado. Cuando utilice un dispositivo WildFire, asegúrese de que no está habilitada la opción Deshabilitar selección de servidor o de lo contrario el dispositivo no podría recibir archivos desde el cortafuegos. Compruebe el siguiente ajuste y asegúrese de que está establecido como “no”: `admin@PA-200# set deviceconfig setting wildfire disable-server-select`

COMPROBACIÓN DE LA CONFIGURACIÓN DE WILDFIRE EN EL CORTAFUEGOS (CONTINUACIÓN)	
Paso 3 Compruebe los logs.	1. Vaya a **Supervisar > Logs > Filtrado de datos**. 2. Confirme que los archivos se están reenviando a WildFire consultando la columna **Acción**: • **Reenviar**. Aparece si el perfil de bloqueo del archivo y la política de seguridad reenvían el archivo de forma correcta. • **Wildfire-upload-success**. Aparecerá si el archivo se ha enviado a WildFire. Esto significa que el archivo no está firmado por un firmante de archivo fiable y que WildFire no lo ha analizado anteriormente. • **Wildfire-upload-skip**. Aparecerá en todos los archivos que se identifiquen como aptos para enviarse a WildFire por un perfil de bloqueo de archivos o una política de seguridad, pero que no fue necesario que WildFire analizase porque ya se habían analizado previamente. En este caso, la acción de **reenviar** aparecerá en el registro de **Filtrado de datos** porque era una acción de reenvío válida, pero que no se envió y analizó en WildFire porque el archivo ya se envió a la nube WildFire desde otra sesión, posiblemente desde otro cortafuegos. 3. Consulte los logs de WildFire (se necesita suscripción) seleccionando **Supervisar > Logs > WildFire**. Si los logs de WildFire están disponibles, el cortafuegos está reenviando correctamente los archivos a WildFire y WildFire está devolviendo los resultados del análisis de archivos. **Nota** Para obtener más información sobre los logs relacionados con WildFire, consulte "Acerca de los logs de WildFire" en la página 48.
Paso 4 Cree la política de bloqueo de archivos.	1. Acceda a **Objetos > Perfiles de seguridad > Bloqueo de archivo** y haga clic en el perfil de bloqueo de archivo para modificarlo. 2. Confirme que la acción está establecida en **Reenviar** o en **Continuar y reenviar**. Si está establecida en **Continuar y reenviar**, solo se reenviará el tráfico http/https porque es el único tipo de tráfico que permite solicitar al usuario que haga clic para continuar.
Paso 5 Compruebe la política de seguridad.	1. Acceda a **Políticas > Seguridad** y haga clic en la regla de política de seguridad que activa el reenvío de archivos a WildFire. 2. Haga clic en la pestaña **Acciones** y asegúrese que la política de bloqueo de archivos está seleccionada en el menú desplegable **Bloqueo de archivo**.

COMPROBACIÓN DE LA CONFIGURACIÓN DE WILDFIRE EN EL CORTAFUEGOS (CONTINUACIÓN)

Paso 6 Compruebe el estado de WildFire.	Ejecute los siguientes comandos de la CLI para comprobar el estado de WildFire y verificar que las estadísticas están aumentando:
	• Compruebe el estado de WildFire:
	`admin@PA-200> show wildfire status`
	Cuando reenvíe los archivos a la nube de WildFire, el resultado debería ser el siguiente:
	`Connection info:`
	`Wildfire cloud: default cloud`
	`Status: Idle`
	`Best server: ca-s1.wildfire.paloaltonetworks.com`
	`Device registered: yes`
	`Valid wildfire license: yes`
	`Service route IP address: 192.168.2.1`
	`Signature verification: enable`
	`Server selection: enable`
	`Through a proxy: no`
	`Forwarding info:`
	`file size limit (MB): 2`
	`file idle time out (second): 90`
	`total file forwarded: 0`
	`forwarding rate (per minute): 0`
	`concurrent files: 0`
	Nota Si el cortafuegos está reenviando archivos a un dispositivo WildFire, el campo `Wildfire cloud:` mostrará la dirección IP o nombre de host del dispositivo y `Best server:` no mostrará ningún valor.
	• Utilice el siguiente comando para comprobar las estadísticas y determinar si los valores han aumentado:
	`admin@PA-200> show wildfire statistics`
	Este es el resultado de un cortafuegos en funcionamiento. Si no aparece ningún valor, el cortafuegos no está reenviando archivos.
	`Total msg rcvd: 8819`
	`Total bytes rcvd: 7064822`
	`Total msg read: 8684`
	`Total bytes read: 6756221`
	`Total msg lost by read: 135`
	`DP receiver reset count: 2`
	`Total file count: 42`
	`CANCEL_FILE_DUP 31`
	`CANCEL_FILESIZE_LIMIT 2`
	`DROP_NO_MATCH_FILE 135`
	`FWD_CNT_LOCAL_FILE 9`
	`FWD_CNT_LOCAL_DUP 30`
	`FWD_CNT_REMOTE_FILE 9`
	`FWD_CNT_REMOTE_DUP_CLEAN 24`
	`FWD_CNT_REMOTE_DUP_TBD 3`
	`FWD_CNT_CACHE_SYNC 1`
	`FWD_ERR_CONN_FAIL 16776`
	`LOG_ERR_REPORT_CACHE_NOMATCH 47`
	`Service connection reset cnt: 1`
	`data_buf_meter 0%`
	`msg_buf_meter 0%`
	`ctrl_msg_buf_meter 0%`
	`fbf_buf_meter 0%`

COMPROBACIÓN DE LA CONFIGURACIÓN DE WILDFIRE EN EL CORTAFUEGOS (CONTINUACIÓN)	
Paso 7 Compruebe el estado y las programaciones de las actualizaciones dinámicas, para asegurarse de que el cortafuegos está recibiendo automáticamente las firmas generadas por WildFire.	1. Acceda a **Dispositivo > Actualizaciones dinámicas**. 2. Asegúrese de que el antivirus, las aplicaciones y amenazas y WildFire tienen las actualizaciones más recientes y que se ha establecido la programación para cada elemento. Escalone la programación de las actualizaciones porque solo se puede realizar una cada vez. 3. Haga clic en **Comprobar ahora** en la parte inferior de las ventanas para ver si hay alguna actualización disponible, lo que también confirma que el cortafuegos se puede comunicar con updates.paloaltonetworks.com. Si el cortafuegos no tiene conectividad con el servidor de actualización, descargue las actualizaciones directamente desde Palo Alto Networks. Inicie sesión en https://support.paloaltonetworks.com y en la sección **Dispositivos gestionados**, haga clic en **Actualizaciones dinámicas** para ver las actualizaciones disponibles. Para obtener más información sobre las actualizaciones dinámicas, consulte la sección Gestión de la actualización de contenidos de la Palo Alto Networks Getting Started Guide (Guía de inicio de Palo Alto Networks).

3 Análisis de archivos mediante la nube de WildFire

En este capítulo se describen los pasos necesarios para empezar a cargar archivos en la nube WildFire de Palo Alto Networks para su análisis directamente desde el cortafuegos, manualmente desde el portal o de forma programada mediante la API de WildFire. Incluye las siguientes secciones:

Envío de archivos a la nube de WildFire

Para configurar un cortafuegos para el envío automático de archivos desconocidos a WildFire, configure un perfil de bloqueo de archivo con la acción Reenviar o Continuar y reenviar y, a continuación, adjúntelo a las reglas de seguridad que desea inspeccionar en busca de un malware de día cero. Por ejemplo, podría configurar una política con un perfil de bloqueo de archivo que active el cortafuegos para reenviar cualquier archivo exe que intenten descargar los usuarios durante una sesión de navegación web. El reenvío de archivos con cifrado SSL también es compatible, siempre que el cifrado SSL esté configurado en el cortafuegos y la opción de reenviar archivos cifrados esté activada.

Si hay un cortafuegos entre el cortafuegos que está reenviando los archivos a WildFire y la nube de WildFire o el dispositivo WildFire, asegúrese de que el cortafuegos intermedio permite los puertos necesarios.

- Nube de WildFire: Utiliza el puerto 443 para registro y envío de archivos.
- Dispositivo WildFire: Utiliza el puerto 443 para registro y el 10443 para envío de archivos.

Siga estas instrucciones en todos los cortafuegos que reenviarán archivos a WildFire:

CONFIGURACIÓN DE UN PERFIL DE BLOQUEO DE ARCHIVOS Y POSTERIOR ADICIÓN DEL MISMO A UN PERFIL DE SEGURIDAD		
Paso 1	Compruebe que el cortafuegos tiene suscripciones a WildFire y prevención de amenazas y que las actualizaciones dinámicas están programadas y actualizadas.	1. Acceda a **Dispositivo > Licencias** y confirme que el cortafuegos tiene suscripciones a WildFire y prevención de amenazas válidas. 2. Acceda a **Dispositivo > Actualizaciones dinámicas** y haga clic en **Comprobar ahora** para asegurarse de que el cortafuegos tiene las actualizaciones más recientes del antivirus, aplicaciones y amenazas y WildFire. 3. Si las actualizaciones no están programadas, hágalo ahora. Asegúrese de escalonar la programación de las actualizaciones porque solo se puede realizar una cada vez. Consulte "Recomendaciones para actualizaciones dinámicas" en la página 37 para conocer la configuración recomendada.
Nota	Aunque el cortafuegos puede reenviar archivos a WildFire sin una suscripción a WildFire, los logs de WildFire no estarán disponibles en el cortafuegos y el cortafuegos no recibirá actualizaciones de firmas de malware de WildFire con una frecuencia inferior a la hora. Para obtener más información sobre las suscripciones, consulte "¿Cuáles son las ventajas de la suscripción de WildFire?" en la página 5.	

CONFIGURACIÓN DE UN PERFIL DE BLOQUEO DE ARCHIVOS Y POSTERIOR ADICIÓN DEL MISMO A UN PERFIL DE SEGURIDAD (CONTINUACIÓN)

Paso 2 Configure el perfil de bloqueo del archivo para definir qué aplicaciones y tipos de archivos activarán el reenvío a WildFire.

Nota Al seleccionar **PE** en la columna Tipos de archivos del perfil de objetos para seleccionar una categoría o tipos de archivos, no añada un tipo de archivo individual que forme parte de esa categoría porque esto produciría entradas redundantes en los logs Filtrado de datos. Por ejemplo, si selecciona PE, no seleccione **exe** porque es parte de la categoría de PE. Esto también es aplicable al tipo de archivo **zip**, ya que los tipos de archivos admitidos que se compriman se envían automáticamente a WildFire.

Al seleccionar una categoría en lugar de un tipo de archivo individual también se garantiza que, como la compatibilidad con un nuevo tipo de archivo se añade a una categoría específica, automáticamente pasará a formar parte del perfil de bloqueo del archivo. Si selecciona **Cualquiera**, todos los tipos de archivos admitidos se reenviarán a WildFire.

1. Desplácese hasta **Objetos > Perfiles de seguridad > Bloqueo de archivos**.
2. Haga clic en **Añadir** para añadir un nuevo perfil e introduzca un **Nombre** y una **Descripción**.
3. Haga clic en **Añadir** en la ventana **Perfil de bloqueo de archivo** y, a continuación, haga clic en **Añadir** de nuevo. Haga clic en el campo **Nombres** e introduzca un nombre para la regla.
4. Seleccione las **aplicaciones** que coincidirán con este perfil. Por ejemplo, si selecciona **navegación web** como la aplicación, el perfil coincidirá con cualquier tráfico de la aplicación identificado como "navegación web".
5. En el campo **Tipo de archivo**, seleccione los tipos de archivos que activarán la acción de reenvío. Seleccione **Cualquiera** para reenviar todos los tipos de archivo admitidos por WildFire o seleccione **PE** para que solo reenvíe archivos Portable Executable.
6. En el campo **Dirección**, seleccione **cargar**, **descargar** o **ambos**. La opción **ambos** activará el reenvío siempre que un usuario trate de cargar o descargar un archivo.
7. Defina una **acción** de la siguiente forma:
   - **Reenviar**: el cortafuegos reenviará automáticamente cualquier archivo que coincida con este perfil a WildFire para su análisis, además de distribuir el archivo al usuario.
   - **Continuar y reenviar**: se le indica al usuario que debe hacer clic en Continuar antes de que se produzca la descarga y que se reenvíe el archivo a WildFire. Como aquí se necesita de la acción del usuario en un navegador web, solo es compatible con aplicaciones de navegación web.

   Nota Cuando utilice **Continuar y reenviar**, asegúrese de que la interfaz de entrada (la que recibe en primer lugar el tráfico para sus usuarios) tiene un perfil de gestión adjunto que permite páginas de respuesta. Para configurar un perfil de gestión, seleccione **Red > Perfiles de red > Gestión de interfaz** y seleccione la casilla de verificación **Páginas de respuesta**. Instale el perfil de gestión en la pestaña **Avanzado** en la configuración de la interfaz de entrada.
8. Haga clic en **ACEPTAR** para guardar los cambios.

CONFIGURACIÓN DE UN PERFIL DE BLOQUEO DE ARCHIVOS Y POSTERIOR ADICIÓN DEL MISMO A UN PERFIL DE SEGURIDAD (CONTINUACIÓN)		
Paso 3	Para reenviar archivos a WildFire desde sitios web usando el cifrado SSL, habilite el reenvío de contenido descifrado. Para obtener información sobre la configuración del descifrado, consulte la Palo Alto Networks Getting Started Guide (Guía de inicio de Palo Alto Networks). **Nota** Solo puede habilitar esta opción un superusuario.	1. Vaya a **Dispositivo > Configuración > ID de contenido**. 2. Haga clic en el icono de edición de las opciones **Filtrado de URL** y habilite **Permitir reenvío de contenido descifrado**. 3. Haga clic en **ACEPTAR** para guardar los cambios. **Nota** Si el cortafuegos tiene múltiples sistemas virtuales, debe habilitar esta opción por VSYS. En esta situación, acceda a **Dispositivo > Sistemas virtuales**, haga clic en el sistema virtual que desea modificar y seleccione la casilla de verificación **Permitir reenvío de contenido descifrado**.
Paso 4	Adjunte el perfil de bloqueo de archivos a una política de seguridad.	1. Desplácese hasta **Políticas > Seguridad**. 2. Haga clic en **Añadir** para crear una nueva política para las zonas a las que desea aplicar el reenvío de WildFire o seleccione una política de seguridad existente. 3. En la pestaña **Acciones**, seleccione el perfil **Bloqueo de archivo** en el menú desplegable. **Nota** Si esta regla de seguridad no tiene ningún perfil adjunto, seleccione **Perfiles** en el menú **Tipo de perfil** para habilitar la selección de un perfil de bloqueo de archivos.
Paso 5	(Opcional) Modifique el tamaño máximo del archivo permitido para cargar en WildFire.	1. Acceda a **Dispositivo > Configuración > WildFire**. 2. Haga clic en el icono de edición **Configuración general**. 3. En el campo **Tamaño de archivo máximo (MB)**, introduzca el tamaño máximo de archivo para los archivos que se enviarán a WildFire para su análisis (intervalo 1-10 MB; de forma predeterminada 2 MB).
Paso 6	(Opcional) Modifique las opciones de la sesión que definen qué información de sesión se debe registrar en los informes de análisis de WildFire.	1. Haga clic en el icono de edición de **Ajustes de información de sesión**. 2. De forma predeterminada, todos los elementos de información de la sesión aparecerán en los informes. Borre las casillas de verificación que correspondan a campos que desee eliminar de los informes de análisis de WildFire. 3. Haga clic en **ACEPTAR** para guardar los cambios.
Paso 7	Compile la configuración.	Haga clic en **Compilar** para aplicar los cambios. Durante la evaluación de la política de seguridad, todos los archivos que cumplan los criterios definidos en la política de bloqueo de archivos se reenviarán a WildFire para su análisis. Para obtener información sobre cómo consultar los informes de los archivos que se han analizado, consulte "Supervisión, control y prevención del malware en la red" en la página 47. Para obtener instrucciones sobre cómo comprobar la configuración, consulte "Comprobación de la configuración de WildFire en el cortafuegos" en la página 38.

Recomendaciones para actualizaciones dinámicas

En la siguiente lista se detallan recomendaciones para conseguir actualizaciones dinámicas en un cortafuegos típico que utilice WildFire y que tenga suscripciones a WildFire y prevención de amenazas. Para un flujo de trabajo más dinámico, utilice Panorama para introducir programaciones de actualización dinámicas en los cortafuegos gestionados usando plantillas de Panorama. Así se garantiza la consistencia entre todos los cortafuegos y se simplifica la gestión de la programación de actualizaciones.

Estas orientaciones proporcionan dos opciones de programación: la programación mínima recomendada y una más agresiva. Si elige un enfoque más agresivo, el dispositivo realizará actualizaciones más frecuentemente, algunas de las cuales pueden ser de gran volumen (más de 100 MB para las actualizaciones de antivirus). De igual forma, raramente se podrían producir errores. Por lo tanto, considere retrasar la instalación de nuevas actualizaciones hasta que se no hayan publicado un determinado número de horas. Utilice el campo **Umbral (horas)** para especificar cuánto tiempo se debe esperar tras una publicación antes de realizar una actualización de contenido.

- **Antivirus**: se publican nuevas actualizaciones de contenido antivirus diariamente. Para obtener el contenido más reciente, programe estas actualizaciones diariamente como mínimo. Se puede realizar una programación más agresiva cada hora.
- **Aplicaciones y amenazas**: App-ID nuevo, protección de vulnerabilidad y firmas antispyware se publican como actualizaciones de contenido semanales (normalmente los martes). Para obtener el contenido más reciente, programe estas actualizaciones semanalmente como mínimo. Si desea un enfoque más agresivo, realice una programación diaria que garantice que el cortafuegos recibe el contenido más reciente tan pronto como es publicado (incluidas publicaciones ocasionales de contenido urgente fuera de programación).
- **WildFire**: se publican nuevas firmas de antivirus de WildFire cada 30 minutos. Dependiendo de cuándo se descubre el malware en el ciclo de publicación, la cobertura se proporcionará en forma de firma de WildFire 30-60 minutos después de que WildFire lo descubra. Para conseguir las firmas de WildFire más recientes, programe estas actualizaciones cada hora o cada media hora. Para que la programación sea más agresiva, puede programar la búsqueda de actualizaciones del cortafuegos con una frecuencia de 15 minutos.

Comprobación de la configuración de WildFire en el cortafuegos

En esta sección se describen los pasos necesarios para comprobar la configuración de WildFire en el cortafuegos.

COMPROBACIÓN DE LA CONFIGURACIÓN DE WILDFIRE EN EL CORTAFUEGOS		

Paso 1	Compruebe las suscripciones a WildFire y prevención de amenazas y el registro de WildFire.	1. Acceda a **Dispositivo > Licencias** y confirme que se ha instalado una suscripción válida a WildFire y prevención de amenazas. Si no hay instaladas licencias válidas, vaya a la sección **Gestión de licencias** y haga clic en **Recuperar claves de licencia del servidor de licencias**.
		2. Para comprobar que el cortafuegos se puede comunicar con un sistema WildFire, de forma que los archivos se puedan reenviar para su análisis, ejecute el siguiente comando de la CLI:
		`admin@PA-200> test wildfire registration`
		
		En la siguiente salida, el cortafuegos indica la nube de WildFire. Si el cortafuegos está indicando un dispositivo WildFire, mostrará el nombre de host o la dirección IP del dispositivo.
		`Test wildfire`
		`wildfire registration: successful`
		`download server list: successful`
		`select the best server: ca-s1.wildfire`
		3. Si los problemas con las licencias continúan, póngase en contacto con su distribuidor o con un ingeniero de sistemas de Palo Alto Networks para confirmar todas las licencias y conseguir un nuevo código de autorización si es necesario.

Paso 2	Confirme que el cortafuegos está enviando archivos al sistema WildFire correcto.	1. Para determinar si el cortafuegos está reenviando archivos (a la nube WildFire de Palo Alto Networks o a un dispositivo WildFire), vaya a **Dispositivo > Configuración > WildFire**. 2. Haga clic en el botón de edición **Configuración general**. 3. Si el cortafuegos está reenviando archivos a la nube de WildFire, este campo debería aparecer como **default-cloud**. Si está reenviando archivos a un dispositivo WildFire, aparecerán la dirección IP o FQDN del dispositivo WildFire. En Panorama, el nombre predeterminado de la nube es **wildfire-public-cloud**. **Nota** Si ha modificado el valor de este campo, pero quiere volver al ajuste **default-cloud**, borre el campo **Servidor WildFire** y haga clic en **ACEPTAR**. Así restaurará el campo a su valor predeterminado. Si el campo no permite la edición, compruebe el siguiente ajusta y asegúrese de que está establecido en “no”: `admin@PA-200# set deviceconfig setting wildfire disable-server-select`

COMPROBACIÓN DE LA CONFIGURACIÓN DE WILDFIRE EN EL CORTAFUEGOS (CONTINUACIÓN)	
Paso 3 Compruebe los logs.	1. Vaya a **Supervisar > Logs > Filtrado de datos**. 2. Confirme que los archivos se están reenviando a WildFire consultando la columna **Acción**: • **Reenviar**. Aparece si el perfil de bloqueo del archivo y la política de seguridad reenvían el archivo de forma correcta. • **Wildfire-upload-success**. Aparecerá si el archivo se ha enviado a WildFire. Esto significa que el archivo no está firmado por un firmante de archivo fiable y que WildFire no lo ha analizado anteriormente. • **Wildfire-upload-skip**. Aparecerá en todos los archivos que se identifiquen como aptos para enviarse a WildFire por un perfil de bloqueo de archivos o una política de seguridad, pero que no fue necesario que WildFire analizase porque ya se habían analizado previamente. En este caso, la acción de **reenviar** aparecerá en el registro de **Filtrado de datos** porque era una acción de reenvío válida, pero que no se envió y analizó en WildFire porque el archivo ya se envió a la nube WildFire desde otra sesión, posiblemente desde otro cortafuegos. 3. Consulte los logs de WildFire (se necesita suscripción) seleccionando **Supervisar > Logs > WildFire**. Si los logs de WildFire están disponibles, el cortafuegos está reenviando correctamente los archivos a WildFire y WildFire está devolviendo los resultados del análisis de archivos. **Nota** Para obtener más información sobre los logs relacionados con WildFire, consulte "Acerca de los logs de WildFire" en la página 48.
Paso 4 Cree la política de bloqueo de archivos.	1. Acceda a **Objetos > Perfiles de seguridad > Bloqueo de archivo** y haga clic en el perfil de bloqueo de archivo para modificarlo. 2. Confirme que la acción está establecida en **Reenviar** o en **Continuar y reenviar**. Si está establecida en **Continuar y reenviar**, solo se reenviará el tráfico http/https porque es el único tipo de tráfico que permite solicitar al usuario que haga clic para continuar.
Paso 5 Compruebe la política de seguridad.	1. Acceda a **Políticas > Seguridad** y haga clic en la regla de política de seguridad que activa el reenvío de archivos a WildFire. 2. Haga clic en la pestaña **Acciones** y asegúrese que la política de bloqueo de archivos está seleccionada en el menú desplegable **Bloqueo de archivo**.

COMPROBACIÓN DE LA CONFIGURACIÓN DE WILDFIRE EN EL CORTAFUEGOS (CONTINUACIÓN)

Paso 6 Compruebe el estado de WildFire.

Ejecute los siguientes comandos de la CLI para comprobar el estado de WildFire y verificar que las estadísticas están aumentando:

- Compruebe el estado de WildFire:

```
admin@PA-200> show wildfire status
```

Cuando reenvíe los archivos a la nube de WildFire, el resultado debería ser el siguiente:

```
Connection info:
        Wildfire cloud:                 default cloud
        Status:                         Idle
        Best server:        ca-s1.wildfire.paloaltonetworks.com
        Device registered:              yes
        Valid wildfire license:         yes
        Service route IP address:       192.168.2.1
        Signature verification:         enable
        Server selection:               enable
        Through a proxy:                no

Forwarding info:
        file size limit (MB):           2
        file idle time out (second):    90
        total file forwarded:           0
        forwarding rate (per minute):   0
        concurrent files:               0
```

Nota Si el cortafuegos está reenviando archivos a un dispositivo WildFire, el campo `Wildfire cloud:` mostrará la dirección IP o nombre de host del dispositivo y `Best server:` no mostrará ningún valor.

- Utilice el siguiente comando para comprobar las estadísticas y determinar si los valores han aumentado:

```
admin@PA-200> show wildfire statistics
```

Este es el resultado de un cortafuegos en funcionamiento. Si no aparece ningún valor, el cortafuegos no está reenviando archivos.

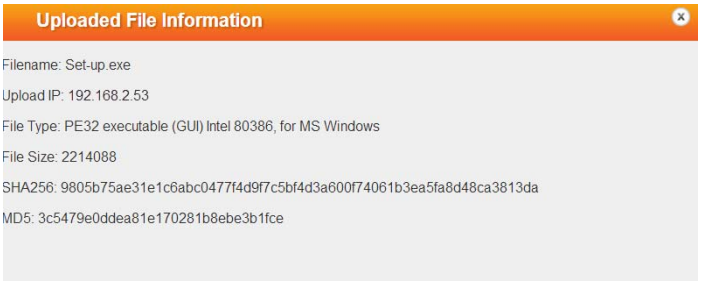
```
        Total msg rcvd:                          8819
        Total bytes rcvd:                     7064822
        Total msg read:                          8684
        Total bytes read:                     6756221
        Total msg lost by read:                  135
        DP receiver reset count:                   2
        Total file count:                         42
        CANCEL_FILE_DUP                           31
        CANCEL_FILESIZE_LIMIT                      2
        DROP_NO_MATCH_FILE                       135
        FWD_CNT_LOCAL_FILE                         9
        FWD_CNT_LOCAL_DUP                         30
        FWD_CNT_REMOTE_FILE                        9
        FWD_CNT_REMOTE_DUP_CLEAN                  24
        FWD_CNT_REMOTE_DUP_TBD                     3
        FWD_CNT_CACHE_SYNC                         1
        FWD_ERR_CONN_FAIL                      16776
        LOG_ERR_REPORT_CACHE_NOMATCH              47
        Service connection reset cnt:              1
        data_buf_meter                            0%
        msg_buf_meter                             0%
        ctrl_msg_buf_meter                        0%
        fbf_buf_meter                             0%
```

COMPROBACIÓN DE LA CONFIGURACIÓN DE WILDFIRE EN EL CORTAFUEGOS (CONTINUACIÓN)		
Paso 7	Compruebe el estado y las programaciones de las actualizaciones dinámicas, para asegurarse de que el cortafuegos está recibiendo automáticamente las firmas generadas por WildFire.	1. Acceda a **Dispositivo > Actualizaciones dinámicas**. 2. Asegúrese de que el antivirus, las aplicaciones y amenazas y WildFire tienen las actualizaciones más recientes y que se ha establecido la programación para cada elemento. Escalone la programación de las actualizaciones porque solo se puede realizar una cada vez. 3. Haga clic en **Comprobar ahora** en la parte inferior de las ventanas para ver si hay alguna actualización disponible, lo que también confirma que el cortafuegos se puede comunicar con updates.paloaltonetworks.com. Si el cortafuegos no tiene conectividad con el servidor de actualización, descargue las actualizaciones directamente desde Palo Alto Networks. Inicie sesión en https://support.paloaltonetworks.com y en la sección **Dispositivos gestionados**, haga clic en **Actualizaciones dinámicas** para ver las actualizaciones disponibles. Para obtener más información sobre las actualizaciones dinámicas, consulte la sección Gestión de la actualización de contenidos de la Palo Alto Networks Getting Started Guide (Guía de inicio de Palo Alto Networks).

Carga de archivos en el portal de la nube de WildFire

Todos los clientes de Palo Alto Networks con una cuenta de asistencia técnica pueden cargar archivos manualmente en el portal de Palo Alto Networks WildFire para su análisis. El portal de WildFire admite la carga manual de los archivos Win32 PE con un máximo de 10MB.

El siguiente procedimiento describe los pasos necesarios para cargar archivos manualmente:

CARGA MANUAL EN WILDFIRE		
Paso 1	Cargue un archivo para su análisis en WildFire.	1. Acceda a https://wildfire.paloaltonetworks.com/ e inicie sesión. 2. Haga clic en el botón **Cargar archivo** en la parte superior derecha de la página y haga clic en **Choose File (Seleccionar archivo)**. 3. Acceda al archivo, resáltelo y, a continuación, haga clic en **Abrir**. El nombre del archivo aparecerá junto a **Choose File (Seleccionar archivo)**. 4. Haga clic en el botón **Upload (Cargar)** para cargar el archivo en WildFire. Si el archivo se carga correctamente, aparecerá un cuadro de diálogo emergente **Uploaded File Information (Información sobre archivo cargado)** parecido al siguiente:  Uploaded File Information Filename: Set-up.exe Upload IP: 192.168.2.53 File Type: PE32 executable (GUI) Intel 80386, for MS Windows File Size: 2214088 SHA256: 9805b75ae31e1c6abc0477f4d9f7c5bf4d3a600f74061b3ea5fa8d48ca3813da MD5: 3c5479e0ddea81e170281b8ebe3b1fce 5. Cierre el cuadro de diálogo emergente **Uploaded File Information (Información sobre archivo cargado)**.
Paso 2	Vea los resultados del análisis. WildFire tardará unos 5 minutos en completar el análisis del archivo. **Nota** Como no se asocia la carga manual con un cortafuegos específico, las cargas manuales aparecerán de forma separada de los cortafuegos registrados.	1. Actualice la página del portal en el navegador. 2. Aparecerá un elemento de línea **Manual** en la lista **Dispositivo** de la página del portal; también aparecerá el resultado del análisis como **malware** o **no peligroso**. Haga clic en la palabra **Manual**. 3. La página del informe mostrará una lista de todos los archivos que se han cargado en su cuenta. Encuentre el archivo cargado y haga clic en el icono de detalles a la izquierda del campo de fecha. El portal muestra un informe completo del análisis de archivo que detalla el comportamiento observado del archivo, incluido el usuario al que estaba destinado, la aplicación que distribuyó el malware y todas las URL relacionadas en la distribución o la actividad teléfono-hogar de la muestra. Si WildFire identifica el archivo como malware, genera una firma que se distribuirá a todos los cortafuegos de Palo Alto Networks configurados para la prevención de amenazas. Los cortafuegos con una suscripción a WildFire pueden descargar estas firmas con una frecuencia inferior a la hora.

Carga de archivos usando la API de WildFire

Usando la API de WildFire, puede enviar tareas de análisis de archivos de forma programada a la nube de WildFire y pedir al sistema datos de informes mediante una interfaz de API REST sencilla.

Esta sección contiene los siguientes temas:

Acerca de las suscripciones a WildFire y claves API

Se proporciona acceso a la clave API si al menos un cortafuegos de Palo Alto Networks cuenta con una suscripción a Wildfire activa y registrada a nombre de un titular de cuenta de su organización. Puede compartir la misma clave API en la organización. La clave API aparece en la sección **My Account (Mi cuenta)** del portal web de WildFire, junto con estadísticas como cuántas cargas y consultas se han realizado usando la clave. La clave se debe considerar secreta y no debe compartirse fuera de los canales autorizados.

¿Cómo usar la API de WildFire?

La API de WildFire es una API REST que utiliza solicitudes HTTP estándar para enviar y recibir datos. Las llamadas de la API se pueden realizar directamente desde utilidades de la línea de comandos como cURL o usando cualquier secuencia de comandos o marco de aplicaciones que sea compatible con los servicios de la REST.

Los métodos de la API se alojan en https://wildfire.paloaltonetworks.com/ y el protocolo HTTPS (no HTTP) es necesario para proteger su clave API y cualquier otro dato intercambiado con el servicio.

Una clave API de WildFire le permite hasta 100 cargas de muestra por día y hasta 1000 informes por día.

Métodos de envío de la API de WildFire

Utilice los siguiente métodos para enviar archivos a WildFire:

Envío de un archivo a la nube de WildFire usando el método de envío de archivo

La API de WildFire admite archivos ejecutables Win32. Al enviar, es necesario el archivo y la clave API para que WildFire abra el archivo en un entorno aislado y lo analice en busca de comportamientos potencialmente malintencionados. El método de envío de archivo devuelve código que un indica un estado satisfactorio o erróneo. Si el resultado es un código 200 OK, significa que el envío ha tenido éxito y que el resultado estará disponible para su consulta en 5 minutos.

URL	https://wildfire.paloaltonetworks.com/submit-file	
Método	POST	
Parámetros	file	Archivo de muestra que se debe analizar
	apikey	Su clave API de WildFire
Resultado	200 OK	Correcto; WildFire procesará el envío
	401 Unauthorized	Clave API no válida
	402 Payment Required	Clave API caducada
	403 Forbidden	Clave API revocada
	405 Method Not Allowed	Se ha utilizado un método distinto a POST
	406 Not Acceptable	Error de clave API
	413 Request Entity Too Large	Tamaño de archivo de muestra sobre el límite máximo de 10 MB
	418 Unsupported File Type	No se admite el tipo de archivo de muestra
	419 Max Request Reached	Se ha superado el número máximo de cargas por día

Envío de un archivo a WildFire usando el método de envío de URL

Utilice el método de envío de URL para enviar un archivo para su análisis mediante una URL Este método es idéntico, en cuanto a interfaz y funcionalidad, al método de envío de archivo, aunque un parámetro de URL sustituye al parámetro de archivo. El parámetro de URL debe indicar a un tipo de archivo admitido accesible (archivos ejecutables Win32). Si el resultado es un código 200 OK, significa que el envío ha tenido éxito; el resultado suele estar disponible para su consulta en 5 minutos.

URL	https://wildfire.paloaltonetworks.com/submit-url	
Método	POST	
Parámetros	url	URL del archivo que se debe analizar
	apikey	Su clave API de WildFire

Resultado	200 OK	Correcto; WildFire procesará el envío
	401 Unauthorized	Clave API no válida
	402 Payment Required	Clave API caducada
	403 Forbidden	Clave API revocada
	405 Method Not Allowed	Se ha utilizado un método distinto a POST
	406 Not Acceptable	Error de clave API
	413 Request Entity Too Large	Tamaño de archivo de muestra sobre el límite máximo de 10 MB
	418 Unsupported File Type	No se admite el tipo de archivo de muestra
	419 Max Request Reached	Se ha superado el número máximo de cargas por día

Consulta de un informe XML de WildFire

Utilice el método de obtención de informe XML para buscar un informe XML de los resultados del análisis de una muestra concreta. Utilice el hash MD5 o SHA-256 del archivo de muestra como consulta de búsqueda.

URL	https://wildfire.paloaltonetworks.com/get-report-xml	
Método	POST	
Parámetros	md5	Hash MD5 del informe solicitado o el hash sha256 según aparece en la siguiente fila.
	sha256	Hash SHA-256 del informe solicitado
	`apikey`	Su clave API de WildFire
Resultado	200 OK	Correcto; WildFire procesará el envío
	401 Unauthorized	Clave API no válida
	404 Not Found	No se ha encontrado el informe
	405 Method Not Allowed	Se ha utilizado un método distinto a POST

Los informes también se pueden recuperar de la nube de WildFire según el número de serie (device_ID) del cortafuegos que envió el archivo y el ID del informe (tid). El valor tid se puede encontrar en el CSV, Syslog o exportación de API de un log de amenazas.

URL	https://wildfire.paloaltonetworks.com/publicapi/report
Método	POST

Parámetros	device_id	Número de serie del cortafuegos que envió el archivo a WildFire.
	report_id	El ID de informe (tid) se puede encontrar en el CSV, Syslog o exportación de API de un log de amenazas.
	format	XML
Resultado	200 OK	Correcto; WildFire procesará el envío
	401 Unauthorized	Clave API no válida
	404 Not Found	No se ha encontrado el informe
	405 Method Not Allowed	Se ha utilizado un método distinto a POST

Ejemplos de código para envío y consulta

El siguiente ejemplo de código Shell muestra un comando simple para enviar un archivo a la API de WildFire para su análisis. La clave API se proporciona como el primer parámetro y la ruta del archivo es el segundo parámetro:

```
#manual upload sample to WildFire with APIKEY
#Parameter 1: APIKEY
#Parameter 2: location of the file

key=$1
file=$2

/usr/bin/curl -i -k -F apikey=$key -F file=@$file
https://wildfire.paloaltonetworks.com/submit-file
```

El siguiente comando cURL muestra una consulta de un informe XML que usa el hash MD5 de la muestra de interés:

```
curl -i -k -F md5=[MD5 HASH] -F apikey=[API KEY] -F
https://wildfire.paloaltonetworks.com/get-report-xml
```

El siguiente comando cURL muestra una consulta de un informe XML que usa device_ID y report_ID de la muestra de interés:

```
curl -i -k -F device_id=[SERIAL NUMBER] -F report_id=[TID FROM LOG] -F format=xml
https://wildfire.paloaltonetworks.com/publicapi/report
```

4 Supervisión, control y prevención del malware en la red

Este capítulo describe el sistema de elaboración de informes y logs de WildFire, y en él se mostrará a los administradores cómo usar esta información para localizar amenazas e identificar a los usuarios atacados por malware.

Acerca de los logs de WildFire

Cada cortafuegos configurado para reenviar archivos a WildFire registrará la acción de reenvío en logs de filtrado de datos y, después de que WildFire analice el archivo, los resultados se volverán a enviar al cortafuegos y aparecerán en los logs de WildFire (se requiere suscripción a WildFire). Puede encontrar el informe de análisis detallado de cada archivo en el log correspondiente de WildFire; para ello, haga clic en el botón **Ver informe de WildFire**. El informe se obtendrá entonces del dispositivo WildFire o de la nube de WildFire. Si no hay una suscripción a WildFire instalada y el cortafuegos reenvía archivos a la nube de WildFire, el informe de análisis puede verse en el portal de WildFire, en https://wildfire.paloaltonetworks.com.

Si sus cortafuegos reenvían archivos a un dispositivo WildFire para su análisis, los resultados del log solo pueden verse desde el cortafuegos; no hay un acceso directo de portal web al dispositivo.

- **Logs de acción de reenvío**: los logs de filtrado de datos ubicados en **Supervisar > Logs > Filtrado de datos** mostrarán los archivos que se han bloqueado/reenviado en función del perfil de bloqueo del archivo. Para determinar qué archivos se han reenviado a WildFire, busque los siguientes valores en la columna **Action (Acción)** del log:

Log	Descripción
wildfire-upload-success	El archivo se ha enviado a la nube. Esto significa que el archivo no está firmado por un firmante de archivo fiable y que WildFire no lo ha analizado anteriormente.
wildfire-upload-skip	aparecerá en todos los archivos que se identifiquen como aptos para enviarse a WildFire por un perfil de bloqueo de archivos o una política de seguridad, pero que no fue necesario que WildFire analizase porque ya se habían analizado previamente. En este caso, la acción de **reenviar** aparecerá en el registro de **Filtrado de datos** porque era una acción de reenvío válida, pero que no se envió y analizó en WildFire porque el archivo ya se envió a la nube WildFire desde otra sesión, posiblemente desde otro cortafuegos. Si está habilitado el registro de archivos, **wildfire-upload-skip** también se mostrará para archivos buenos que se hayan encontrado antes, por lo que no es necesario que se envíen a la nube para su análisis. El registro de archivos se activa desde la CLI ejecutando `set deviceconfig setting wildfire report-benign-file`.

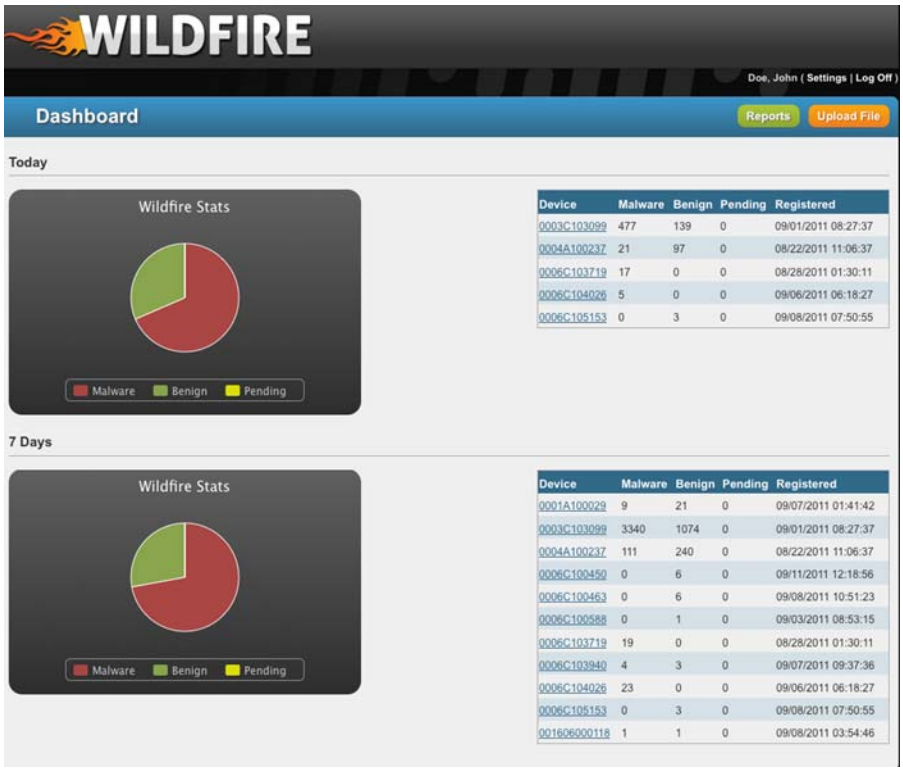
- **Logs de WildFire**: los resultados del análisis de los archivos analizados por WildFire se devuelven a los logs del cortafuegos (se requiere suscripción a WildFire) una vez se complete el análisis. Estos logs se escriben en el cortafuegos que reenvió el archivo en **Supervisar > Logs > WildFire**. Si los logs se reenvían desde el cortafuegos a Panorama, se escriben en el servidor de Panorama, en **Supervisar > Logs > WildFire Submissions (Presentaciones de WildFire)**. La columna **Category (Categoría)** de los logs de WildFire mostrará **benign (Bueno)**, lo que significa que el archivo es seguro, o **malicious (Malintencionado)**, lo que indica que WildFire ha determinado que el archivo contiene código malintencionado. Si se determina que el archivo es malintencionado, el generador de firmas de WildFire generará una firma. Si usa un dispositivo de WildFire, el envío automático debe estar habilitado en el dispositivo para que los archivos infectados con malware se envíen a la nube de WildFire para la generación de la firma.

Para ver el informe detallado de un archivo analizado por WildFire, localice la entrada del log en el log de WildFire, haga clic en el icono que aparece a la izquierda de la entrada del log para mostrar los detalles y, a continuación, haga clic en el botón **Ver informe de WildFire**. Aparecerá un mensaje de inicio de sesión para acceder al informe y, tras introducir las credenciales correspondientes, el informe se recuperará del sistema WildFire y se mostrará en su explorador. Para obtener información sobre cuentas de portal para acceder a la nube de WildFire, consulte "Cuentas de usuario del portal de WildFire" en la página 51. Para obtener información sobre la cuenta de administrador usada para recuperar informes de un dispositivo WildFire, consulte "Realización de la configuración inicial" en la página 10 y el paso que describe la cuenta portal-admin.

Supervisión de envíos con la nube de WildFire

Vaya a la nube WildFire de Palo Alto Networks, en https://wildfire.paloaltonetworks.com, e inicie sesión usando 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 asistencia técnica específica (así como los archivos que se hayan cargado manualmente). Para cada dispositivo, se mostrarán estadísticas del número de archivos de malware detectados, archivos buenos analizados y archivos pendientes en espera para su análisis. También aparecerán la fecha y la hora que registró el cortafuegos la primera vez con el portal para comenzar el reenvío de archivos a WildFire.

Para obtener información sobre la configuración de cuentas de WildFire adicionales que pueden usarse para revisar información de informes, consulte "Cuentas de usuario del portal de WildFire" en la página 51.



Personalización de la configuración del portal de WildFire

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

CONFIGURACIÓN DEL PORTAL DE WILDFIRE		
Paso 1	Configure la zona horaria para la cuenta del portal.	1. Vaya al portal, en https://wildfire.paloaltonetworks.com, e inicie sesión usando sus credenciales de inicio de sesión de asistencia técnica de Palo Alto Networks o su cuenta de usuario de WildFire. 2. Haga clic en el vínculo **Settings (Configuración)**, situado en la parte superior derecha de la ventana del portal. 3. Seleccione la zona horaria del menú desplegable y, a continuación, haga clic en **Update Time Zone (Actualizar zona horaria)** para guardar el cambio. **Nota** La marca de hora que aparecerá en el informe detallado de WildFire utilizará la zona horaria establecida en su cuenta del portal. 4. Haga clic de nuevo en el vínculo **Settings (Configuración)** para volver a la página de configuración.
Paso 2	Elimine los logs de WildFire de cortafuegos específicos. Con esto eliminará todos los logs y las notificaciones del cortafuegos seleccionado.	1. En el menú desplegable **Delete WildFire Logs (Eliminar logs de WildFire)**, seleccione el cortafuegos (por número de serie). 2. Haga clic en el botón **Delete Logs (Eliminar logs).** 3. Haga clic en **ACEPTAR** para continuar con la eliminación.
Paso 3	Configure las notificaciones de correo electrónico que se generarán en función de los resultados de los archivos enviados a WildFire.	1. En la página de configuración del portal, localice la sección **Email Notifications (Notificaciones de correo electrónico)**. Aparecerá una tabla con los encabezados de columna **Device** (Dispositivo), **Malware (Malware)** y **Benign (Bueno)**. 2. El primer elemento de la fila mostrará **Manual**. Seleccione **Malware (Malware)** o **Benign (Bueno)** para obtener una notificación de los archivos que se han cargado manualmente a la nube de WildFire, o que se han enviado mediante la API de WildFire. Para recibir notificaciones de cortafuegos que reenvían archivos a la nube de WildFire, active las casillas de verificación **Malware (Malware)** o **Benign (Bueno)** junto a cada cortafuegos. **Nota** Active las casillas de verificación directamente debajo de los encabezados de columna **Malware (Malware)** y **Benign (Bueno)** para activar todas las casillas de verificación de los dispositivos mostrados.

Cuentas de usuario del portal de WildFire

Las cuentas del portal de WildFire las crea un superusuario (o el propietario registrado de un dispositivo de Palo Alto Networks) para permitir que otros usuarios inicien sesión en el portal web de WildFire y vean datos de WildFire de dispositivos concedidos de forma específica por el superusuario o el propietario registrado. Un superusuario es la persona que ha registrado un cortafuegos de Palo Alto Networks y tiene la principal cuenta de asistencia técnica del dispositivo o los dispositivos. El usuario de WildFire puede ser un usuario del sitio de asistencia técnica existente que pertenezca a cualquier cuenta (incluidas la cuenta secundaria, la principal o cualquier otra cuenta del sistema), o puede ser un usuario que no tenga una cuenta de asistencia técnica de Palo Alto Networks, pero se le ha otorgado acceso solo para el portal de WildFire y un conjunto concreto de cortafuegos.

Adición de cuentas de usuario de WildFire

Esta sección describe los pasos necesarios para añadir cuentas adicionales de WildFire a la nube de WildFire.

ADICIÓN DE CUENTAS DE USUARIO DE WILDFIRE		
Paso 1	Acceda a la sección para gestionar usuarios y cuentas en el sitio de asistencia técnica y seleccione una cuenta.	1. Inicie sesión en https://support.paloaltonetworks.com/. 2. En **Manage Account (Gestionar cuenta)**, haga clic en **Users and Accounts (Usuarios y cuentas)**. 3. Seleccione una cuenta o una cuenta secundaria existente.
Paso 2	Añada un usuario de WildFire.	1. Haga clic en el botón **Add WildFire User (Añadir usuario de WildFire)**. 2. Introduzca la dirección de correo electrónico del usuario destinatario que desea añadir. **Nota** El usuario puede ser un usuario de sitio de asistencia técnica existente que pertenezca a cualquier cuenta (incluidas la cuenta secundaria, la cuenta principal, Palo Alto Networks o cualquier otra cuenta del sistema), así como cualquier dirección de correo electrónico que no disponga de una cuenta de asistencia técnica. La única restricción es que la dirección de correo electrónico no puede proceder de una cuenta de correo electrónico gratuita basada en web (Gmail, Hotmail, Yahoo, etc.). Si se introduce una cuenta de correo electrónico de un dominio no compatible, se mostrará un mensaje de advertencia.

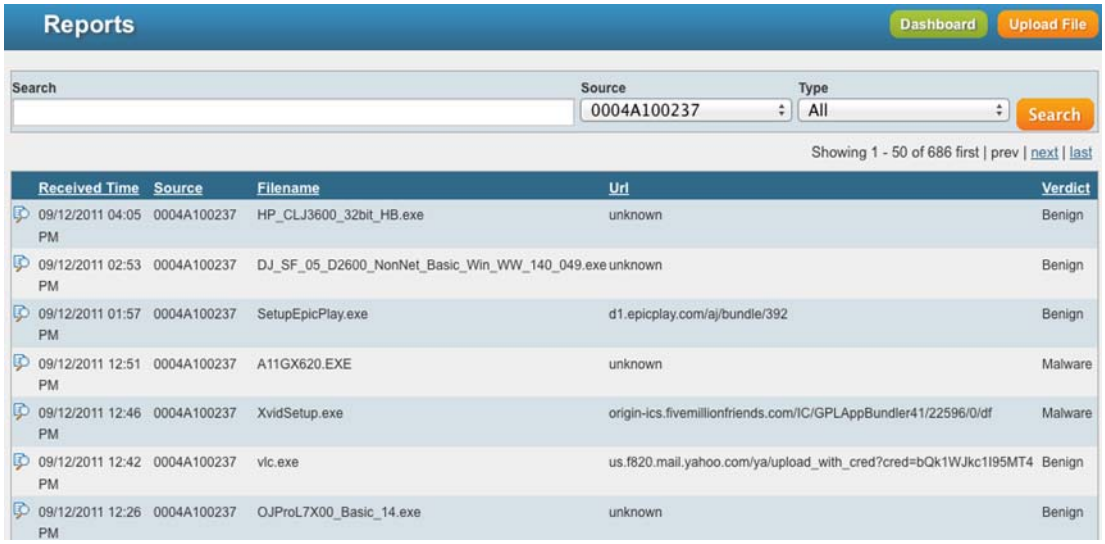
ADICIÓN DE CUENTAS DE USUARIO DE WILDFIRE (CONTINUACIÓN)		
Paso 3	Asigne cortafuegos a la nueva cuenta de usuario y acceda al portal de WildFire.	1. Seleccione el o los cortafuegos por número de serie a los que desea conceder acceso y cumplimente los detalles de cuenta opcionales. 2. Se enviará un correo electrónico al usuario. Los usuarios con una cuenta de asistencia técnica existente recibirán un correo electrónico con una lista de los cortafuegos de los cuales ahora pueden ver los informes de WildFire. Si el usuario no tiene una cuenta de asistencia técnica, se le enviará un correo electrónico con instrucciones sobre cómo acceder al portal y cómo configurar una nueva contraseña. 3. El usuario podrá entonces iniciar sesión en https://wildfire.paloaltonetworks.com 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 buenos.

Visualización de informes de WildFire

El método principal para ver informes de WildFire enviados a la nube de WildFire o a un dispositivo WildFire es acceder al cortafuegos que ha reenviado el archivo a WildFire y, después, ver los logs de WildFire desde la pestaña Supervisar. Haga clic en el icono de detalles del log, a la izquierda de la entrada del log de WildFire, para ver más detalles sobre la sesión. A continuación, haga clic en el icono **Ver informes de WildFire** para ver el informe detallado del análisis de WildFire. Si el cortafuegos reenvía logs a Panorama, estos pueden verse en Panorama, en la misma área.

Al enviar archivos al portal de WildFire (mediante el reenvío de cortafuegos, la carga manual o la API de WildFire), es posible acceder a los informes desde el cortafuegos, así como desde el portal de WildFire. Para acceder a los informes desde el portal, inicie sesión en https://wildfire.paloaltonetworks.com y haga clic en el botón **Informes**, en la parte superior de la página del portal de WildFire. Aparecerá una lista que muestre la fecha en la que se ha recibido el archivo, el número de serie del cortafuegos que ha reenviado el archivo (o manual, si el archivo se ha cargado manualmente o mediante la API de WildFire) y el nombre de archivo o URL. También tiene a su disposición opciones de búsqueda en la parte superior de la página y se incluyen controles de paginación.

Para ver un informe individual desde el portal, haga clic en el icono **Informes**, situado a la izquierda del nombre del informe. Para imprimir un informe detallado, use la opción de impresión del explorador. A continuación puede ver un informe de muestra:



¿Qué contienen los informes de WildFire?

Los informes muestran información detallada de comportamiento sobre el archivo que se ejecutó en el sistema WildFire, así como información sobre el usuario de destino, la aplicación que entregó el archivo y todas las direcciones URL involucradas en la entrega o en la actividad teléfono-casa del archivo. La siguiente tabla describe cada sección que aparece en un informe de análisis de WildFire típico. La organización del informe puede variar en función de la versión del software del dispositivo WildFire instalado en dicho dispositivo, o de si los informes se ven desde la nube de WildFire. El informe contendrá parte o la totalidad de la siguiente información, en función de la información de sesión definida en el cortafuegos que reenvió el archivo, y también en función del comportamiento observado.

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

Encabezado del informe	Descripción

Información del archivo	• **SHA-256**: muestra la información SHA del archivo. La información SHA es muy similar a una huella digital, que identifica exclusivamente un archivo para garantizar que este no se ha modificado de ninguna forma. Si la información de SHA se compara con el archivo original y se encuentran diferencias, este archivo se ha modificado de algún modo.
	• **Antivirus Coverage (cobertura antivirus)**: haga clic en este vínculo para ver si el archivo se ha identificado anteriormente. Esto le llevará al sitio web https://www.virustotal.com/en/, que contiene información sobre varios proveedores de antivirus y le mostrará si estos ofrecen cobertura o no para el archivo infectado. Si el archivo no se ha detectado nunca antes por ninguno de los proveedores mostrados, aparecerá **file not found (archivo no encontrado)**.
	• **Verdict (veredicto)**: muestra el veredicto del análisis:
	  • **Benign (bueno)**: el archivo es seguro y no muestra comportamiento malintencionado.
	  • **Malware (malware)**: WildFire ha identificado el archivo como malware y generará una firma que proteja contra futuras exposiciones. Si un dispositivo WildFire ha analizado el archivo y el envío automático está deshabilitado, el archivo no se reenviará a la nube de WildFire, por lo que no se generará ninguna firma.

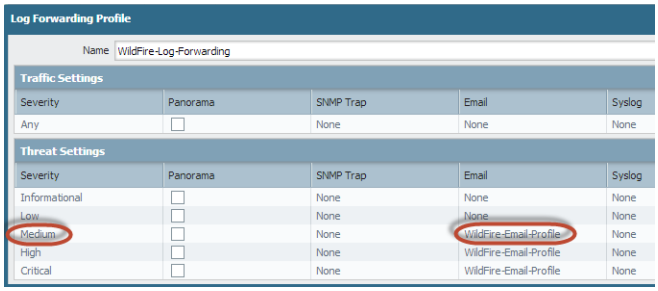
Información de sesión	Muestra la información de sesión que aparecerá en los informes de WildFire. La configuración de estas opciones se define en el cortafuegos que envía el archivo de muestra a WildFire, y se realiza en la pestaña **Dispositivo > Configuración > WildFire**, en la sección **Ajustes de información de sesión**. A continuación se enumeran las opciones disponibles: • IP de origen • Puerto de origen • IP de destino • Puerto de destino • Sistema virtual (si VSYS múltiple está configurado en el cortafuegos) • Aplicación • Usuario (si el ID de usuarios está configurado en el cortafuegos) • URL • Nombre de archivo
Behavioral Summary (Resumen de comportamientos)	Muestra los distintos comportamientos que ha tenido el archivo. Por ejemplo, si ha creado o modificado archivos, iniciado un proceso, generado procesos nuevos, modificado el registro o instalado objetos de ayuda del explorador.
Network Activity (Actividad de red)	Muestra la actividad de la red generada por la muestra, como el acceso a otros hosts de la red y la actividad teléfono-casa del archivo.
Host Activity (Actividad de host)	Muestra las claves de registro que se han definido, modificado o eliminado.
Process (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.

Configuración de alertas para el malware detectado

Esta sección describe los pasos necesarios para configurar un cortafuegos de Palo Alto Networks para enviar una alerta cada vez que WildFire devuelva un log de amenaza al cortafuegos que indica que se ha detectado malware. Este ejemplo describe cómo configurar una alerta de correo electrónico Para configurar los registros de Syslog, los traps SNMP o el reenvío de logs a Panorama, asegúrese de que el cortafuegos está configurado con información de servidor SNMP y de que este cortafuegos está gestionado por Panorama. Panorama, Syslog o SNMP se pueden seleccionar después junto con el correo electrónico, según se describe en los siguientes pasos:

Para obtener más información sobre alertas y reenvío de logs, consulte las secciones "Configuración de alertas de correo electrónico" "Definición de servidores Syslog" y "Configuración de los destinos de Trap SNMP" de la Palo Alto Networks Getting Started Guide (Guía de inicio de Palo Alto Networks).

CONFIGURACIÓN DE ALERTAS PARA MALWARE	
Paso 1. Configure un perfil de servidor de correo electrónico si no hay uno ya configurado.	1. Vaya a **Dispositivo > Perfiles de servidor > Correo electrónico**. 2. Haga clic en **Añadir** y, a continuación, introduzca un **Nombre** para el perfil. Por ejemplo, **WildFire-Correoelectronico-Perfil**. 3. (Opcional) Seleccione el sistema virtual al que se aplica este perfil en el menú desplegable **Ubicación**. 4. Haga clic en **Añadir** para añadir una nueva entrada de servidor de correo electrónico e introduzca la información necesaria para conectar con el servidor SMTP y enviar mensajes de correo electrónico (puede añadir hasta cuatro servidores de correo electrónico al perfil): • **Servidor**: nombre para identificar el servidor de correo electrónico (1-31 caracteres). Este campo es solamente una etiqueta y no tiene que ser el nombre de host de un servidor SMTP existente. • **Mostrar nombre**: el nombre que aparecerá en el campo De del correo electrónico. • **De**: la dirección de correo electrónico desde la que se enviarán las notificaciones de correo electrónico. • **Para**: la dirección de correo electrónico a la que se enviarán las notificaciones de correo electrónico. • **Destinatarios adicionales**: introduzca una dirección de correo electrónico para enviar notificaciones a un segundo destinatario. • **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 **ACEPTAR** para guardar el perfil de servidor. 6. Haga clic en **Compilar** para guardar los cambios en la configuración actual.
Paso 2 Pruebe el perfil del servidor de correo electrónico.	1. Vaya a **Supervisar > Informes en PDF > Programador de correo electrónico**. 2. Haga clic en **Añadir** y seleccione el nuevo perfil de correo electrónico en el menú desplegable **Perfil de correo electrónico**. 3. Haga clic en el botón **Enviar correo electrónico de prueba** y un correo electrónico de prueba se enviará a los destinatarios definidos en el perfil de correo electrónico.

CONFIGURACIÓN DE ALERTAS PARA MALWARE (CONTINUACIÓN)		
Paso 3	Configure un perfil de reenvío de logs. El perfil de reenvío de logs determina qué tráfico se supervisa y qué gravedad activará una notificación de alerta.	1. Vaya a **Objetos > Reenvío de logs**. 2. Haga clic en **Añadir** e indique un nombre para el perfil. Por ejemplo, **WildFire-Reenvio-Log**. 3. En la sección **Configuración de amenaza**, elija el perfil de correo electrónico de la columna **Correo electrónico** para el tipo de gravedad de nivel **Medio**. El motivo por el que se usa la gravedad media aquí es porque los logs de malware de WildFire tienen una gravedad de tipo **Medio**. Para enviar alertas sobre logs bueno de WildFire, seleccione el tipo de gravedad **Informativo**. 4. Haga clic en **ACEPTAR** para guardar los cambios.  **Nota** Si el cortafuegos está gestionado por Panorama, active la casilla de verificación **Panorama**, situada a la derecha de la gravedad de tipo **Medio** para permitir el reenvío de logs a Panorama. Si hay un servidor SNMP configurado, seleccione el servidor en el menú desplegable **Trap SNMP** a la derecha del tipo de gravedad **Medio** para reenviar traps al servidor SNMP.
Paso 4	Aplique el perfil de reenvío de logs al perfil de seguridad que contiene el perfil de bloqueo de archivos.	1. Vaya a **Políticas > Seguridad** y haga clic en la política usada para el reenvío de WildFire. 2. En la sección **Ajuste de log** de la pestaña **Acciones**, haga clic en el menú desplegable **Reenvío de logs** y seleccione el nuevo perfil de reenvío de logs. En este ejemplo, el perfil se denomina **WildFire-Reenvio-Log**. 3. Haga clic en **ACEPTAR** para guardar los cambios y, a continuación, haga clic en **Compilar** para confirmar la configuración. Las alertas de correo electrónico deberían recibirse ahora para los logs de amenaza y WildFire con una gravedad media.

WildFire en acción

El siguiente caso de ejemplo resume todo el ciclo de vida de 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 el cortafuegos de Palo Alto Networks junto con WildFire puede detectar malware de día cero descargado por sus usuarios incluso cuando el tráfico tiene cifrado SSL. Una vez identificado el malware, se le notifica al administrador, se avisa al usuario que descargó el archivo y el cortafuegos descarga automáticamente una nueva firma que proteja frente a futuras exposiciones del malware. 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".

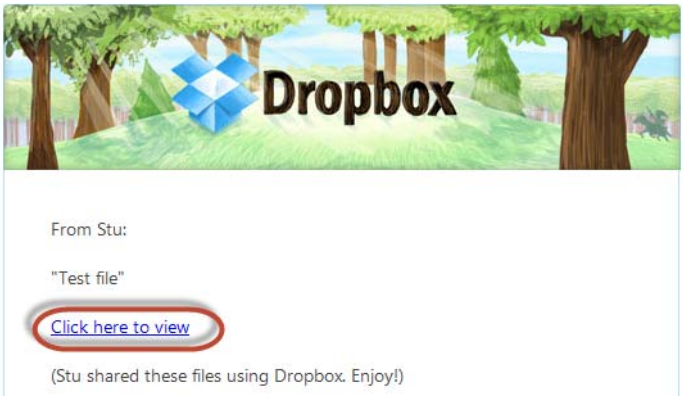
Si desea más información sobre la configuración de WildFire, consulte "Envío de archivos a la nube de WildFire" en la página 34 o "Reenvío de archivos a un dispositivo WF-500 WildFire" en la página 24.

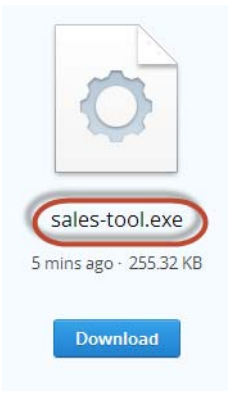
Este ejemplo usa un sitio web que utiliza cifrado SSL, por lo que el descifrado debe configurarse en el cortafuegos y la opción **Permitir reenvío de contenido descifrado** debe estar habilitada. Para obtener más información sobre la configuración del descifrado, consulte la *Palo Alto Networks Getting Started Guide (Guía de inicio de Palo Alto Networks)*. Para obtener más información sobre cómo habilitar el reenvío de datos descifrados, consulte "Envío de archivos a la nube de WildFire" en la página 34 o "Reenvío de archivos a un dispositivo WF-500 WildFire" en la página 24.

CASO DE EJEMPLO DE WILDFIRE

Paso 1. El representante de ventas de la empresa asociada carga un archivo de una herramienta de ventas denominado **sales-tool.exe** en su cuenta de Dropbox y, después, envía un correo electrónico a la representante de ventas de Palo Alto Networks con un enlace al archivo.

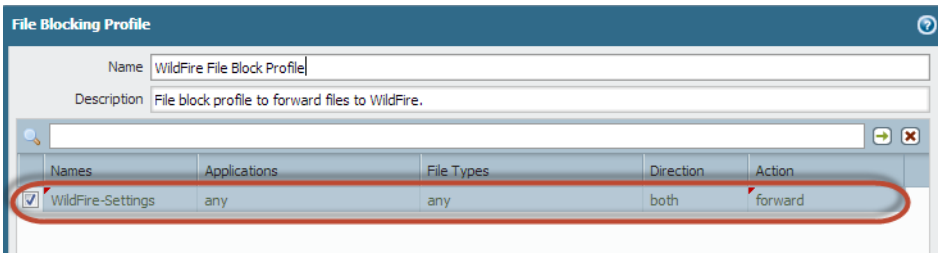
Paso 2 La representante de ventas de Palo Alto recibe el correo electrónico del socio de ventas y hace clic en el vínculo descargado, que le lleva al sitio de Dropbox. A continuación, hace clic en **Descargar** y el archivo se guarda en su escritorio.

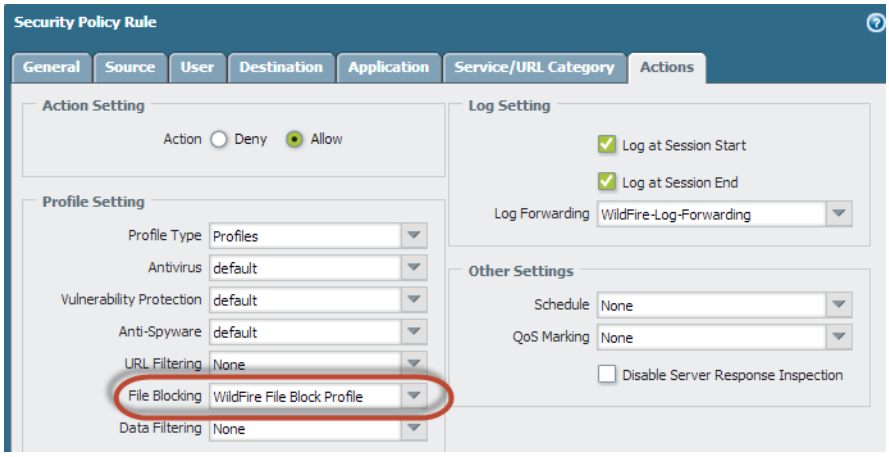


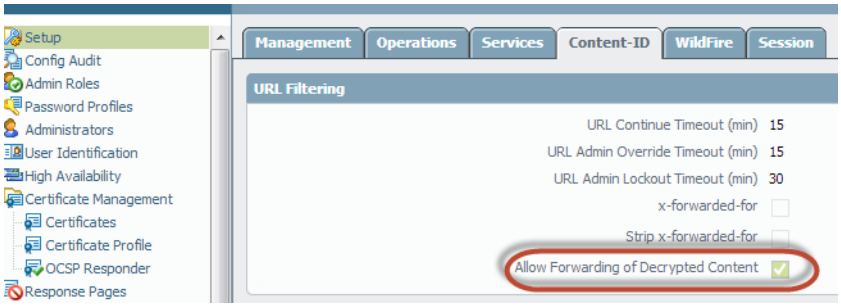


CASO DE EJEMPLO DE WILDFIRE (CONTINUACIÓN)

Paso 3 El cortafuegos que protege a la representante de ventas de Palo Alto tiene un perfil de bloqueo de archivos adjunto a una política de seguridad que busca archivos en cualquier aplicación utilizada para descargar o cargar cualquier tipo de archivo Portable Executable (PE). En cuanto la representante de ventas hace clic en Descargar, la política del cortafuegos también reenvía el archivo sales-tool.exe a WildFire para su análisis. Aun cuando la representante de ventas use Dropbox, que tiene cifrado SSL, el cortafuegos está configurado para el descifrado, por lo que todo el tráfico se puede revisar y los archivos se pueden reenviar a WildFire. Las siguientes capturas de pantalla muestran el perfil de bloqueo de archivos, la política de seguridad configurada con el perfil de bloqueo de archivos y la opción para permitir el reenvío de contenido descifrado.





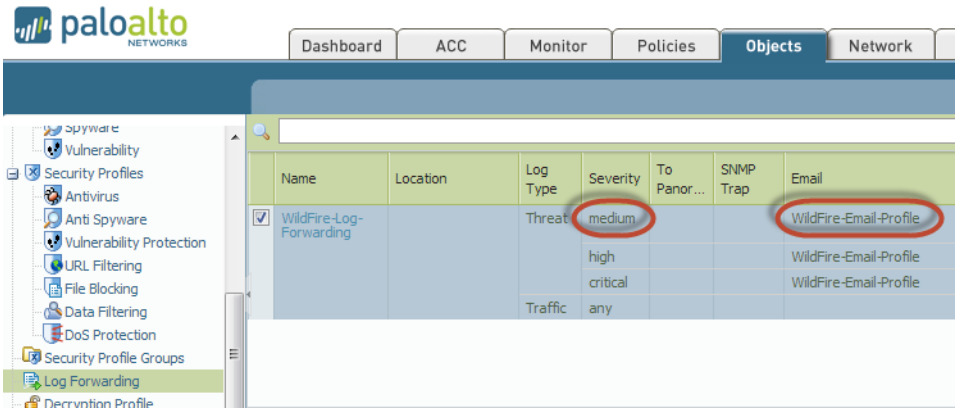


CASO DE EJEMPLO DE WILDFIRE (CONTINUACIÓN)

Paso 4 En este momento, WildFire ha recibido el archivo y está analizándolo en busca de más de 100 comportamientos malintencionados distintos. Para ver que el archivo se ha reenviado correctamente, consulte **Supervisar > Logs > Filtrado de datos** en el cortafuegos.

Paso 5 En aproximadamente cinco minutos, WildFire ha terminado el análisis del archivo y envía un log de WildFire al cortafuegos con los resultados del análisis. En este ejemplo, el log de WildFire muestra que el archivo es malintencionado.

Paso 6 También hay configurado un perfil de reenvío de logs para alertas de amenaza media de correo electrónico, de modo que el administrador de seguridad recibe inmediatamente un correo electrónico en relación al malware que ha descargado la representante de ventas.



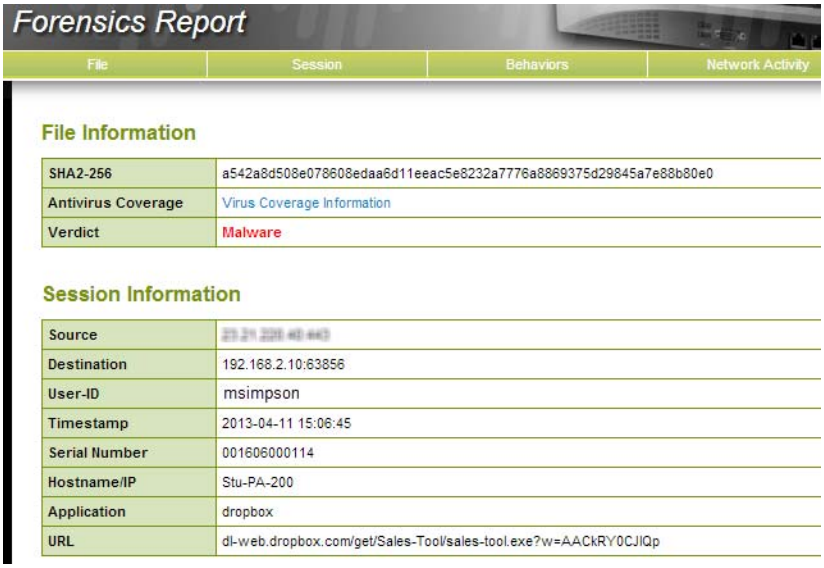
CASO DE EJEMPLO DE WILDFIRE (CONTINUACIÓN)

Paso 7 El administrador de seguridad identificará el usuario por el nombre si el ID de usuarios está configurado o, en caso contrario, por dirección IP. En este punto, el administrador puede apagar la red o la conexión VPN que está usando la representante de ventas y, a continuación, se pondrá 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 WildFire, el técnico del grupo de asistencia técnica puede comprobar si el malware se ha ejecutado en el sistema examinando los archivos, los procesos y la información de registro detallados en el informe del análisis. Si se ha ejecutado el malware, el técnico puede intentar limpiar el sistema manualmente o volver a crear una imagen de este.

Para obtener detalles de los campos del informe de WildFire, consulte "¿Qué contienen los informes de WildFire?" en la página 53.

Vista parcial del informe de análisis de WildFire



Forensics Report

File | Session | Behaviors | Network Activity

File Information

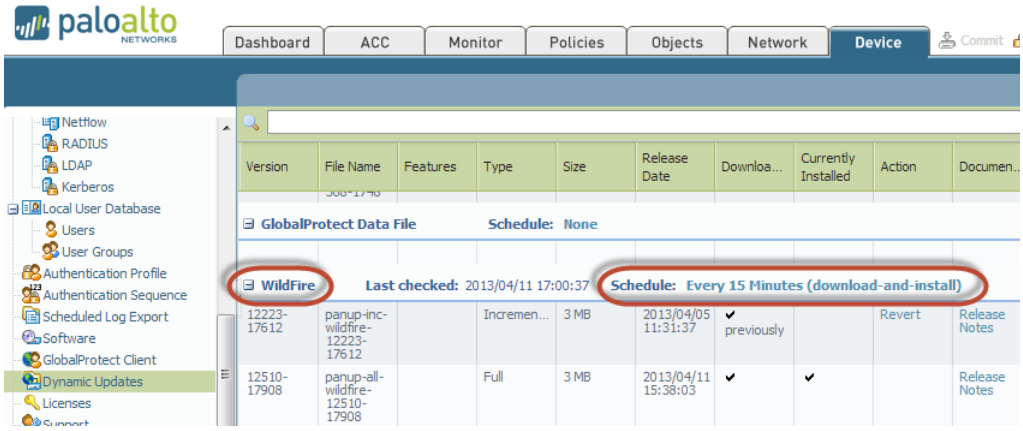
SHA2-256	a542a8d508e078608edaa6d11eeac5e8232a7776a8869375d29845a7e88b80e0
Antivirus Coverage	Virus Coverage Information
Verdict	Malware

Session Information

Source	[redacted]
Destination	192.168.2.10:63856
User-ID	msimpson
Timestamp	2013-04-11 15:06:45
Serial Number	001606000114
Hostname/IP	Stu-PA-200
Application	dropbox
URL	dl-web.dropbox.com/get/Sales-Tool/sales-tool.exe?w=AACkRY0CJlQp

CASO DE EJEMPLO DE WILDFIRE (CONTINUACIÓN)

Paso 8 Una vez identificado el malware y comprobado el sistema del usuario, ¿cómo 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 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, 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 WildFire proporcionada por Palo Alto Networks y el cortafuegos ha descargado la nueva firma. Este cortafuegos y cualquier otro cortafuegos de Palo Alto Networks configurado para descargar firmas de WildFire protege ahora a los usuarios frente a este malware detectado recientemente.



Todo esto tiene lugar mucho antes de que la mayoría de los proveedores de antivirus perciban incluso la existencia de malware de día cero. En este ejemplo, el malware ya no se considera de día cero, ya que Palo Alto Networks sabe de su existencia y ya ha proporcionado la protección correspondiente a sus clientes.

5 Referencia de la CLI del software del dispositivo WildFire

En este capítulo se describen los comandos de la CLI específicos para el software del dispositivo WF-500 WildFire. El resto de comandos, tales como las interfaces de configuración, confirmación de la configuración y el ajuste de la información del sistema, son idénticos a PAN-OS y también se muestran en la jerarquía. Para obtener más información sobre los comandos de PAN-OS, consulte la *Guía de referencia de la interfaz de línea de comandos de PAN-OS de Palo Alto Networks*.

Acerca del software del dispositivo WildFire

En esta sección se presenta la interfaz de línea de comandos (CLI) del software del dispositivo WildFire y se describe su uso:

Acerca de la estructura de la CLI del software del dispositivo WildFire

La CLI del software del dispositivo WildFire se usa manejar dicho dispositivo. La CLI es la única interfaz del dispositivo. Sirve para ver información de estado y configuración y modificar la configuración del dispositivo. Acceda a la CLI del software del dispositivo WildFire a través de SSH o de un acceso directo a la consola usando el puerto de la consola.

La CLI del software del dispositivo WildFire tiene dos modos de funcionamiento:

- **Modo de operación**: Permite ver el estado del sistema, navegar por la CLI del software del dispositivo WildFire y acceder al modo de configuración.
- **Modo de configuración**: Permite ver y modificar la jerarquía de configuración.

Si desea más información sobre estos modos, consulte "Modos de comando de la CLI" en la página 71.

Acceso a la CLI

En esta sección se describe cómo acceder y comenzar a usar la CLI del software del dispositivo WildFire:

- Establecimiento de una conexión directa con la consola
- Establecimiento de una conexión de SSH

Establecimiento de una conexión directa con la consola

Consulte la *WF-500 WildFire Appliance Hardware Reference Guide (Guía de referencia de hardware de WF-500 WildFire)* para obtener información acerca de la instalación del hardware e Inicio rápido para información sobre configuración inicial del dispositivo.

Utilice la siguiente configuración en la conexión directa de la consola:

- Tasa de datos: 9600
- Bits de datos: 8
- Paridad: no
- Bits de terminación: 1
- Control de flujo: Ninguna

Establecimiento de una conexión de SSH

Para acceder a la CLI del software del dispositivo WildFire:

1. Abra la conexión de la consola.
2. Introduzca el nombre del usuario administrativo. El valor predeterminado es admin.
3. Introduzca la contraseña administrativa. El valor predeterminado es admin.
4. La CLI del software del dispositivo WildFire se abre en el modo de operación y se muestra el siguiente mensaje de la CLI:
   `nombreusuario@nombrehost>`

Uso de los comandos de la CLI del software del dispositivo WildFire

- Convenciones de comandos de la CLI del software del dispositivo WildFire
- Mensajes de comandos de la CLI
- Acceso a los modos de operación y configuración
- Mostrar opciones de comandos de la CLI del software del dispositivo WildFire

Convenciones de comandos de la CLI del software del dispositivo WildFire

El mensaje de comandos básico incluye el nombre de usuario y de host del dispositivo:

```
nombreusuario@nombrehost>
```

Ejemplo:

```
msimpson@wf-corp1>
```

Al entrar en el modo de configuración, el mensaje cambia de > a #:

```
nombreusuario@nombrehost>          (modo de operación)
nombreusuario@nombrehost> configurar
Entrando en el modo de configuración.
[editar]
nombreusuario@nombrehost#          (modo de configuración)
```

En el modo de configuración, el contexto de jerarquía actual se muestra en el titular `[editar...]` que aparece entre corchetes cuando se emite un comando.

Mensajes de comandos de la CLI

Pueden aparecer mensajes al emitir un comando. Los mensajes ofrecen información de contexto y pueden ayudar a corregir comandos no válidos. En los siguientes ejemplos, el mensaje se muestra en negrita.

Ejemplo: Comando desconocido

```
nombreusuario@nombrehost# grupo de aplicaciones
Comando desconocido: grupo de aplicaciones
[editar red]
nombreusuario@nombrehost#
```

Ejemplo: Modos de cambio

```
nombreusuario@nombrehost# salir
Saliendo del modo de configuración

nombreusuario@nombrehost>
```

Ejemplo: Sintaxis no válida

```
nombreusuario@nombrehost> depurar 17
Comando no reconocido
Sintaxis no válida.
nombreusuario@nombrehost>
```

La CLI comprueba la sintaxis de cada comando. Si la sintaxis es correcta, se ejecuta el comando y se registran los cambios de la jerarquía del candidato. Si la sintaxis no es correcta, aparece un mensaje de sintaxis no válida, como en el siguiente ejemplo:

```
nombreusuario@nombrehost# establecer aplicación de zona 1.1.2.2
Comando no reconocido
Sintaxis no válida.
[editar]
nombreusuario@nombrehost#
```

Acceso a los modos de operación y configuración

Al iniciar sesión, la CLI del software del dispositivo WildFire se abre en el modo de operación. Puede alternar entre los modos de operación y navegación en cualquier momento.

- Para entrar en el modo de configuración desde el modo de operación, use el comando **configurar**:

  ```
  nombreusuario@nombrehost> configurar
  Entrando en el modo de configuración.

  [editar]
  nombreusuario@nombrehost#
  ```

- Para salir del modo de configuración y regresar al modo de operación, use el comando **abandonar** o el comando **salir**:

  ```
  nombreusuario@nombrehost# abandonar
  Saliendo del modo de configuración

  nombreusuario@nombrehost>
  ```

Para introducir un comando del modo de operación mientras está en el modo de configuración, use el comando **ejecutar**. Por ejemplo, para mostrar recursos del sistema desde el modo de configuración, use `ejecutar mostrar recursos del sistema`.

Mostrar opciones de comandos de la CLI del software del dispositivo WildFire

Use ? (o **Meta-H**) para mostrar una lista de opciones de comandos, basada en el contexto:

- Para mostrar una lista de comandos de operación, introduzca **?** en el mensaje del comando.

  ```
  nombreusuario@nombrehost> ?
    clear       Borrar los parámetros de tiempo de ejecución
    configure   Modificar la información de la configuración de software
    debug       Depurar y diagnosticar
    exit        Salir de esta sesión
    grep        Buscar en el archivo líneas que contengan una coincidencia de patrones
    less        Examinar el contenido del archivo depurado
    ping        Hacer ping a hosts y redes
    quit        Abandonar esta sesión
    request     Hacer solicitudes en el nivel de sistema
  ```

```
  scp          Usar ssh para copiar el archivo en otro host
  set          Establecer parámetros opcionales
  show         Mostrar parámetros opcionales
  ssh          Iniciar una shell para otro host
 tail       Imprimir las últimas 10 líneas del contenido del archivo de depuración
nombreusuario@nombrehost>
```

- Para mostrar las opciones disponibles de un comando especificado, introduzca el comando seguido de **?**.

  Ejemplo:

```
nombreusuario@nombrehost> ping ?
+ bypass-routing     Derivar tabla de enrutamiento; usar interfaz especificada
+ count              Número de solicitudes para enviar (1..2000000000 paquetes)
+ do-not-fragment    No fragmentar paquetes de solicitud de eco (IPv4)
+ inet               Forzar a destino IPv4
+ interface          Interfaz de origen (multicast, all-ones, paquetes sin enrutar)
+ interval           Retraso entre solicitudes (segundos)
+ no-resolve         No intentar imprimir las direcciones simbólicamente
+ pattern            Patrón de relleno hexadecimal
+ record-route       Registrar y elaborar informe de la ruta de un paquete (IPv4)
+ size               Tamaño de los paquetes de solicitud (0..65468 bytes)
+ source             Fuente de dirección para la solicitud de eco
+ tos                Valor de tipo de servicio IP (0..255)
+ ttl                Valor de contador interno de tiempo de vida (valor de límite de
                     salto de IPv6) (saltos 0..255)
+ verbose            Muestra información de salida detallada
+ wait               Retraso después de mandar el último paquete del ultimo proyecto
                     (segundos)
  <host>             Nombre de host o dirección IP de host remoto
```

Símbolos de opciones de comandos

El símbolo que precede a una opción puede proporcionar información adicional acerca de la sintaxis de comandos.

Símbolo	Descripción
*	Esta opción es obligatoria.
>	Hay opciones adicionales anidadas para este comando.
+	Hay opciones de comando adicionales para este comando en este nivel.
|	Hay una opción para especificar un "valor de excepción" o un "valor de coincidencia" para restringir el comando.
" "	Aunque las comillas dobles no son un símbolo de opción de comando, debe usarse al introducir frases de varias palabras en comandos de CLI. Por ejemplo, para crear un nombre de grupo de dirección llamado Grupo de prueba y añadir el usuario llamado nombre1 a este grupo; debe escribir el nombre del grupo con comillas dobles alrededor del siguiente modo: establecer grupo de direcciones "Grupo de prueba" usuario1. Si no coloca comillas dobles alrededor del nombre del grupo, la CLI podría interpretar la palabra Prueba como el nombre del grupo y Grupo como el nombre de usuario y se mostraría el siguiente mensaje de error: "prueba no es un nombre válido". Nota: Las comillas simples tampoco serían válidas en este ejemplo.

Los siguientes ejemplos muestran cómo se usan estos símbolos.

Ejemplo: En el siguiente comando, es obligatoria la palabra clave `from`:

```
nombreusuario@nombrehost> scp import configuration ?
+ remote-port   número de puerto de SSH en el host remoto
* from          Origen (nombreusuario@host:ruta)
nombreusuario@nombrehost> scp import configuration
```

Ejemplo: El resultado de este comando muestra opciones designadas con + y >.

```
nombreusuario@nombrehost# set rulebase security rules rule1 ?
+ action                acción
+ application           aplicación
+ destination           destino
+ disabled              deshabilitado
+ from                  de
+ log-end               fin del log
+ log-setting           ajuste de log
+ log-start             inicio de log
+ negate-destination    negar destino
+ negate-source         negar origen
+ schedule              programación
+ service               servicio
+ source                origen
+ to                    para
```

```
> profiles              perfiles
  <Intro>               Finalizar entrada
[editar]
nombreusuario@nombrehost# set rulebase security rules rule1
```

Cada opción de la lista marcada con + se puede añadir al comando.

La palabra clave perfiles (con >) tiene opciones adicionales:

```
nombreusuario@nombrehost# set rulebase security rules rule1 profiles ?
+ virus            Cadena de ayuda para virus
+ spyware          Cadena de ayuda para spyware
+ vulnerability    Cadena de ayuda para vulnerabilidad
+ group            Cadena de ayuda para grupo
  <Intro>          Finalizar entrada
[editar]
nombreusuario@nombrehost# set rulebase security rules rule1 profiles
```

Restricción de resultados de comandos

Algunos comandos de operación incluyen una opción para restringir el resultado que aparece. Para restringir el resultado, introduzca un símbolo de barra vertical seguido de **excepto** o **coincidencia** y el valor que se debe incluir o excluir:

Ejemplo:
El siguiente resultado de muestra pertenece al comando **mostrar información del sistema**:

```
nombreusuario@nombrehost> mostrar información del sistema
nombrehost: wf-corp1
ip-address: 192.168.2.20
netmask: 255.255.255.0
default-gateway: 192.168.2.1
mac-address: 00:25:90:95:84:76
vm-interface-ip-address: 10.16.0.20
vm-interface-netmask: 255.255.252.0
vm-interface-default-gateway: 10.16.0.1
vm-interface-dns-server: 10.0.0.247
time: Mon Apr 15 13:31:39 2013
uptime: 0 days, 0:02:35
family: m
model: WF-500
serial: 009707000118
sw-version: 5.1.0
logdb-version: 5.0.2
platform-family: m

nombreusuario@nombrehost>
```

El siguiente ejemplo muestra solo información del modelo del sistema:

```
nombreusuario@nombrehost> show system info | match model
model: WF-500

nombreusuario@nombrehost>
```

Niveles de privilegio

Los niveles de privilegio determinan los comandos que el usuario tiene permitido ejecutar y la información que el usuario tiene permitido ver.

Nivel	Descripción
superlector	Tiene solo acceso de lectura completo al dispositivo.
superusuario	Tiene acceso de escritura completo al dispositivo.

Modos de comando de la CLI

En este capítulo se describen los modos usados para interactuar con la CLI del software del dispositivo WildFire:

- Acerca del modo de configuración
- Acerca del modo de operación

Acerca del modo de configuración

Al introducir comandos en el modo de configuración se modifica la configuración del candidato. La configuración del candidato modificada se almacena en la memoria del dispositivo y se conserva mientras el dispositivo esté en funcionamiento.

Cada comando de configuración implica una acción, y también puede incluir palabras clave, opciones y valores.

En esta sección se describen el modo de configuración y la jerarquía de configuración:

- Uso de comandos del modo de configuración
- Acerca de la jerarquía de configuración
- Navegación por la jerarquía

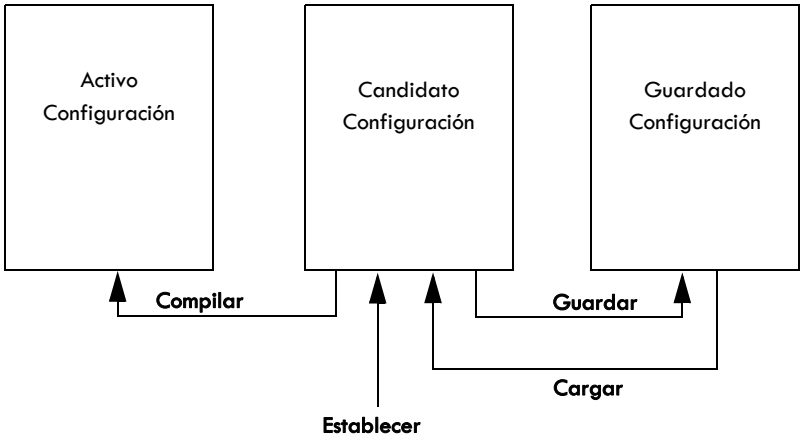
Uso de comandos del modo de configuración

Use los siguientes comandos para almacenar y aplicar cambios de configuración:

- Comando **guardar**: Guarda la configuración del candidato en la memoria permanente del dispositivo. La configuración guardada se conserva hasta que se vuelva a usar el comando **guardar** para sobrescribirla. Tenga en cuenta que este comando no activa la configuración.
- comando **compilar**: Aplica la configuración de lcandidato al dispositivo. Una configuración compilada vuelve activa la configuración del dispositivo.

- comando **establecer**: Cambia un valor en la configuración del candidato.
- comando **cargar**: Asigna la última configuración guardada o una configuración especificada para ser la configuración del candidato.

Cuando se cambia el modo de configuración sin emitir el comando guardar o compilar, los cambios de configuración podrían perderse si se interrumpe la alimentación del dispositivo.



Mantener la configuración de un candidato y separar los pasos de guardado y compilación conlleva importantes ventajas en comparación con las arquitecturas CLI tradicionales:

- Distinguir entre los conceptos de **guardado** y **compilación** permite hacer múltiples cambios simultáneos y reduce la vulnerabilidad del sistema.
- Los comandos se pueden adaptar fácilmente para funciones similares.

  Por ejemplo, al configurar dos interfaces Ethernet, cada una con una dirección IP, puede editar la configuración de la primera interfaz, copiar el comando, modificar solo la interfaz y la dirección IP y, a continuación, aplicar el cambio a la segunda interfaz.
- La estructura de comandos siempre es constante.

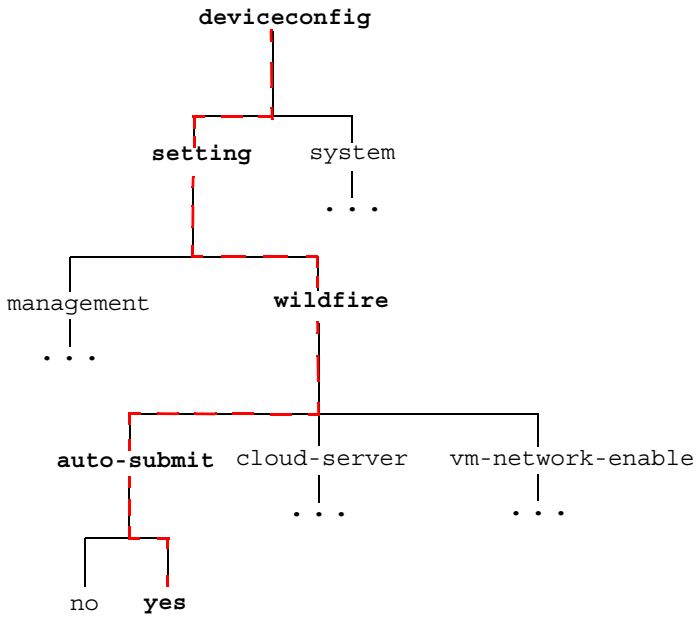
Dado que la configuración del candidato siempre es exclusiva, todos los cambios autorizados de la configuración del candidato serán coherentes entre sí.

Acerca de la jerarquía de configuración

La configuración del dispositivo se organiza con una estructura jerárquica. Para mostrar un segmento del nivel actual de la jerarquía, use el comando **mostrar**. Al introducir **mostrar** aparece la jerarquía completa, mientras que al introducir **mostrar** con palabras clave aparece un segmento de la jerarquía. Por ejemplo, cuando se ejecuta el comando **mostrar** desde el nivel más alto del modo de configuración, se muestra toda la configuración. Si se ejecuta el comando **editar configuración de gestión** y se introduce **mostrar**, o se ejecuta el comando **mostrar configuración de gestión**, solo aparece la parte de la jerarquía relativa a la configuración de gestión.

Rutas de jerarquía

Al introducir comandos, la ruta se traza a través de la jerarquía del siguiente modo:

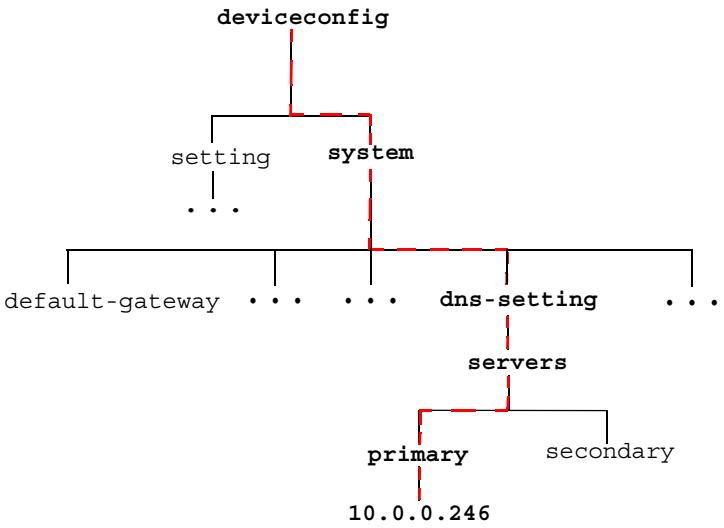


Por ejemplo, el siguiente comando asigna el servidor de DNS principal 10.0.0.246 para el dispositivo:

```
[editar]
nombreusuario@nombrehost# establecer servidores principales para configuración de DNS
10.0.0.246 para el sistema deviceconfig
```

Este comando genera un nuevo elemento en la jerarquía y en los resultados del siguiente comando **mostrar**:

```
[editar]
nombreusuario@nombrehost# show deviceconfig system dns-settings
dns-setting {
    servers {
      primary 10.0.0.246
      }
  }
[editar]
nombreusuario@nombrehost#
```



Navegación por la jerarquía

El titular [editar...] presentado a continuación de la línea del símbolo de sistema del modo de configuración muestra el contexto de jerarquía actual. Por ejemplo, el titular

```
[editar]
```

indica que el contexto relativo es el máximo nivel de la jerarquía, mientras que

```
[editar deviceconfig]
```

indica que el contexto relativo está al nivel de deviceconfig.

Use los comandos de la lista para navegar por la jerarquía de configuración.

Nivel	Descripción
editar	Establece el contexto para la configuración dentro de la jerarquía de comandos.
arriba	Cambia el contexto al nivel superior de la jerarquía.
máximo	Cambia el contexto al nivel más alto de la jerarquía.

Si se emite el comando establecer después de usar los comandos arriba y principal, se inicia desde un nuevo contexto.

Acerca del modo de operación

La primera vez que se inicia sesión en el dispositivo, la CLI del software del dispositivo WildFire se abre en el modo de operación. Los comandos del modo de operación tienen que ver con acciones que se ejecutan inmediatamente. No suponen cambios en la configuración, y no es necesario guardarlos o compilarlos.

Los comandos del modo de operación son de diversos tipos:

- **Acceso a la red**: Abre una ventana a otro host. Es compatible con SSH.
- **Supervisión y solución de problemas**: Realizar diagnósticos y análisis. Incluye los comandos **depurar** y **ping**.
- **Mostrar comandos**: Muestra o borra la información actual. Incluye los comandos **borrar** y **mostrar**.
- **Comandos de navegación de la CLI del software del dispositivo WildFire**: Entrar en el modo de configuración o salir de la CLI del software del dispositivo WildFire. Incluye los comandos **configurar**, **salir** y **abandonar**.
- **Comandos del sistema**: Hace solicitudes en el nivel del sistema o reinicia. Incluye los comandos **establecer** y **solicitud**.

Establecimiento del formato de salida para comandos de configuración

Cambia el formato de salida para los comandos de configuración usando el comando **establecer formato de salida de la configuración de cli** en el modo de operación. Las opciones incluyen el formato predefinido, json (JavaScript Object Notation), formato establecido y formato XML. El formato predefinido es un formato jerárquico donde las secciones de configuración tienen sangría y están entre llaves.

Comandos del modo de configuración

Esta sección contiene información de consulta sobre comandos para los siguientes comandos del modo de configuración que son específicos del software del dispositivo WildFire. El resto de comandos que forman parte del software del dispositivo WildFire son idénticos a PAN-OS, consulte la *Guía de referencia de la interfaz de línea de comandos de PAN-OS de Palo Alto Networks* para obtener información sobre esos comandos.

Todos los comandos específicos de WildFire están en color azul en el resultado de la siguiente jerarquía y tienen un hiperenlace a la descripción.

```
deviceconfig {
  system {
    login-banner <valor>;
    hostname <valor>;
    domain <valor>;
    speed-duplex
auto-negotiate|10Mbps-half-duplex|10Mbps-full-duplex|100Mbps-half-duplex|100Mbps-full-
duplex|
    1Gbps-full-duplex;
    ip-address <ip/máscara_de_red>;
    netmask <valor>;
    default-gateway <ip/máscara_de_red>;
    interfaz vm{
      ip-address <ip/máscara_de_red>;
      netmask <valor>;
      default-gateway <ip/máscara_de_red>;
      mtu 576-1500;
      speed-duplex
      auto-negotiate|10Mbps-half-duplex|10Mbps-full-duplex|100Mbps-half-duplex|100Mbps
     -full-duplex|
      1Gbps-full-duplex;
      link-state up|down;
      dns-server <ip/máscara_de_red>;
    }
    geo-location {
      latitude <float>;
      longitude <float>;
    }
    timezone
    dns-setting {
        servers {
          primary <ip/máscara_de_red>;
          secondary <ip/máscara_de_red>;
        }
    }
    ntp-server-1 <valor>;
    ntp-server-2 <valor>;
    update-server <valor>;
    secure-proxy-server <valor>;
    secure-proxy-port 1-65535;
    secure-proxy-user <valor>;
```

```
    secure-proxy-password <valor>;
    service {
      disable-ssh yes|no;
      disable-icmp yes|no;
    }
  }
  setting {
    wildfire {
      cloud-server <valor>;
      auto-submit yes|no;
      vm-network-enable yes|no;
    }
    management {
      admin-lockout {
        failed-attempts 0-10;
        lockout-time 0-60;
      }
      idle-timeout 1-1440;
    }
  }
}

mgt-config {
  users {
    REPETIR...
    <nombre> {
      phash <valor>;
      permissions {
        role-based {
          superreader yes;
          O BIEN...
          superuser yes;
        }
      }
    }
  }
}

predefined;

shared {
  log-settings {
    system {
      informational {
        send-syslog {
          using-syslog-setting <valor>;
        }
      }
      low {
        send-syslog {
          using-syslog-setting <valor>;
        }
```

```
      }
      medium {
        send-syslog {
          using-syslog-setting <valor>;
        }
      }
      high {
        send-syslog {
          using-syslog-setting <valor>;
        }
      }
      critical {
        send-syslog {
          using-syslog-setting <valor>;
        }
      }
    }
    config {
      any {
        send-syslog {
          using-syslog-setting <valor>;
        }
      }
    }
    syslog {
      REPETIR...
      <nombre> {
        server {
          REPETIR...
          <nombre> {
            server <valor>;
            port 1-65535;
            facility
LOG_USER|LOG_LOCAL0|LOG_LOCAL1|LOG_LOCAL2|LOG_LOCAL3|LOG_LOCAL4|LOG_LOCAL5|LOG_LOCAL6|
LOG_LOCAL7;
          }
        }
      }
    }
  }
}
```

interfaz vm

Descripción

La interfaz vm sirve para permitir que el software malintencionado que se ejecuta en las máquinas virtuales de WildFire acceda a Internet para habilitar análisis de archivos más exhaustivos. Se recomienda la activación de este puerto, que a su vez ayudará a WildFire a identificar mejor la actividad maliciosa si el software malintencionado accede a Internet para phone-home u otra actividad. Es importante que esta interfaz esté en una red aislada para Internet. Para obtener más información acerca de la interfaz vm, consulte "Configuración de interfaz de la máquina virtual" en la página 17.

Tras configurar la interfaz vm, habilítela ejecutando el siguiente comando:

```
set deviceconfig setting wildfire vm-network-enable yes
```

Ubicación de jerarquía

establecer sistema de deviceconfig

Sintaxis

```
set vm-interface {
    ip-address <dirección_ip>;
    netmask <dirección_ip>;
    default-gateway <dirección_ip>;
    dns-server <dirección_ip>;
```

Opciones

```
admin@wf-corp1# establecer interfaz vm
+ default-gateway   Puerta de enlace predefinida
+ dns-server        Servidor dns
+ ip-address        Dirección IP para interfaz de descarga vm wildfire
+ link-state        Estado del enlace activo o inactivo
+ mtu               Unidad de transmisión máxima para la interfaz de gestión
+ netmask           Máscara de red de IP para la interfaz de descarga vm wildfire
+ speed-duplex      Velocidad y duplex para la interfaz de descarga vm wildfire
```

Resultado de muestra

A continuación se muestra una interfaz vm configurada.

```
vm-interface {
  ip-address 10.16.0.20;
  netmask 255.255.252.0;
  default-gateway 10.16.0.1;
  dns-server 10.0.0.246;
}
```

Nivel de privilegios requerido

superusuario, superlector

wildfire

Descripción

Configure los ajustes de Wildfire para que envía automáticamente el software malintencionado a la Nube de Palo Alto Networks WildFire para generar firmas, definir el servidor de la Nube que recibirá los archivos infectados por software malintencionado y habilitar o deshabilitar la interfaz vm. Lea la descripción de la interfaz vm antes de habilitarla.

Ubicación de jerarquía

establecer configuración de deviceconfig

Sintaxis

```
wildfire {
      cloud-server <valor>;
      auto-submit yes|no;
      vm-network-enable yes|no;
      }
```

Opciones

```
admin@wf-corp1# establecer wildfire
+ auto-submit envía automáticamente todo el veredicto incorrecto/software malicioso a
la Nube pública
+ cloud-server Nombre de host para el servidor de la Nube. De manera predefinida es
wildfire-public-cloud
+ vm-network-enable habilitar/deshabilitar
```

Resultado de muestra

El siguiente resultado muestra que el envío automático no está habilitado en el dispositivo WildFire, de modo que los archivos infectados por software malintencionado no se enviarán a la Nube de WildFire. Si el envío automático estuviera habilitado, se enviarían los archivos a la Nube de WildFire porque el servidor de la Nube de la Nube pública de wildfire está definido. También muestra que la interfaz vm está habilitada, lo cual permitirá que el software malintencionado que se ejecuta en máquinas virtuales de WildFire accedan a Internet.

```
wildfire {
  auto-submit no;
  vm-network-enable yes;
  cloud-server wildfire-public-cloud;
}
```

Nivel de privilegios requerido

superusuario, superlector

Comandos del modo de operación

Esta sección contiene información de consulta sobre comandos para los siguientes comandos del modo de operación que son específicos del software del dispositivo WildFire. El resto de comandos que forman parte del software del dispositivo WildFire son idénticos a PAN-OS, consulte la *Guía de referencia de la línea de comandos de PAN-OS de Palo Alto Networks* para obtener información sobre esos comandos.

Todos los comandos específicos de WildFire están en color azul en el resultado de la siguiente jerarquía y tienen un hiperenlace a la descripción.

```
test {
  wildfire {
    registration;
  }
}
set {
  wildfire {
     portal-admin {
       password <valor>;
     }
  }
  O BIEN...
  management-server {
    unlock {
      admin <valor>;
    }
    O BIEN...
    logging on|off|import-start|import-end;
  }
  O BIEN...
  password;
  O BIEN...
  ssh-authentication {
    public-key <valor>;
  }
  O BIEN...
  cli {
    config-output-format default|xml|set|json;
    O BIEN...
    pager on|off;
    O BIEN...
    confirmation-prompt on|off;
    O BIEN...
    scripting-mode on|off;
    O BIEN...
    timeout {
      idle 1-1440;
    }
```

```
    O BIEN...
    hide-ip;
    O BIEN...
    hide-user;
  }
  O BIEN...
  clock {
    date <valor>;
    time <valor>;
  }
}

request {
  system {
    software {
      info;
      O BIEN...
      check;
      O BIEN...
      download {
        version <valor>;
        O BIEN...
        file <valor>;
      }
      O BIEN...
      install {
          version <valor>;
          O BIEN...
          file <valor>;
        load-config <valor>;
      }
    }
    O BIEN...
    raid {
      remove <valor>;
      O BIEN...
      copy {
        from <valor>;
        to <valor>;
      }
      O BIEN...
      add {
        REPETIR...
        <nombre> {
          force {
            no-format;
          }
        }
      }
    }
  }
```

```
O BIEN...
password-hash {
  password <valor>;
  username <valor>;
}
O BIEN...
commit-lock {
  add {
    comment <valor>;
  }
  O BIEN...
  remove {
    admin <valor>;
  }
}
O BIEN...
config-lock {
  add {
    comment <valor>;
  }
  O BIEN...
  remove;
}
O BIEN...
tech-support {
  dump;
}
O BIEN...
stats {
  dump;
}
O BIEN...
shutdown {
  system;
}
O BIEN...
system {
  software {
    info;
    O BIEN...
    check;
    O BIEN...
    download {
      version <valor>;
      O BIEN...
      file <valor>;
    }
    O BIEN...
    install {
        version <valor>;
        O BIEN...
        file <valor>;
```

```
        load-config <valor>;
      }
    }
  }
  O BIEN...
  license {
    info;
    O BIEN...
    fetch {
      auth-code <valor>;
    }
    O BIEN...
    install <valor>;
  }
  O BIEN...
  restart {
    system;
    O BIEN...
    software;
  }
  O BIEN...
  support {
    info;
    O BIEN...
    check;
  }
}

check {
  pending-changes;
  O BIEN...
  data-access-passwd {
    system;
  }
}

save {
  config {
    to <valor>;
  }
}

load {
  config {
    key <valor>;
      last-saved;
      O BIEN...
      from <valor>;
      O BIEN...
      version <valor>1-1048576;
      O BIEN...
      partial {
```

```
        from <valor>;
        from-xpath <valor>;
        to-xpath <valor>;
        mode merge|replace|append;
      }
  }
  O BIEN...
  device-state;
}

load {
  config {
    key <valor>;
      last-saved;
      O BIEN...
      from <valor>;
      O BIEN...
      version <valor>;
      O BIEN...
      partial {
        from <valor>;
        from-xpath <valor>;
        to-xpath <valor>;
        mode merge|replace|append;
      }
      O BIEN...
      repo {
        device <valor>;
          file <valor>;
          O BIEN...
          version <valor>;
      }
  }
}

delete {
  config {
    saved <valor>;
    O BIEN...
    repo {
      device <valor>;
        file <valor>;
        O BIEN...
        running-config;
    }
  }
  O BIEN...
  software {
    image <valor>;
    O BIEN...
    version <valor>;
  }
}
```

```
clear {
  job {
    id 0-4294967295;
  }
  O BIEN...
  log {
    config;
    O BIEN...
    system;
  }
  O BIEN...
  counter {
    device;
  }
}

show {
  arp management|ethernet1/1|ethernet1/2|all;
  O BIEN...
  neighbor management|ethernet1/1|ethernet1/2|all;
  O BIEN...
  web-server {
    log-level;
  }
  O BIEN...
  config {
    diff;
    O BIEN...
    running {
      xpath <valor>;
    }
    O BIEN...
    candidate;
  }
  O BIEN...
  interface management|ethernet1/1;
  O BIEN...
  management-clients;
  O BIEN...
  counter {
    management-server;
    O BIEN...
    interface management|ethernet1/1;
    O BIEN...
    device;
  }
  O BIEN...
  ntp;
  O BIEN...
  clock;
  O BIEN...
```

```
wildfire {
    sample-status {
      sha256 {
        equal <valor>;
      }
    }
    O BIEN...
    status;
    O BIEN...
    statistics;
    O BIEN...
    latest {
      analysis {
        filter malicious|benign;
        sort-by SHA256|Submit Time|Start Time|Finish Time|Malicious|Status;
        sort-direction asc|desc;
        limit 1-20000;
        days 1-7;
      }
      O BIEN...
      sessions {
        filter malicious|benign;
        sort-by SHA256|Create Time|Src IP|Src Port|Dst Ip|Dst Port|File|Device
        ID|App|Malicious|Status;
        sort-direction asc|desc;
        limit 1-20000;
        days 1-7;
      }
      O BIEN...
      samples {
        filter malicious|benign;
        sort-by SHA256|Create Time|File Name|File Type|File Size|Malicious|Status;
        sort-direction asc|desc;
        limit 1-20000;
        days 1-7;
      }
      O BIEN...
      uploads {
        sort-by SHA256|Create Time|Finish Time|Status;
        sort-direction asc|desc;
        limit 1-20000;
        days 1-7;
      }
    }
    O BIEN...
    last-device-registration {
      all;
    }
  }
  O BIEN...
```

```
cli {
  info;
  O BIEN...
  idle-timeout;
  O BIEN...
  hide-ip;
  O BIEN...
  hide-user;
  O BIEN...
  permissions;
}
O BIEN...
jobs {
  all;
  O BIEN...
  pending;
  O BIEN...
  processed;
  O BIEN...
  id 1-4294967296;
}
O BIEN...
location {
  ip <ip/máscara_de_red>;
}
O BIEN...
system {
  software {
    status;
  }
  O BIEN...
  masterkey-properties;
  O BIEN...
  info;
  O BIEN...
  resources {
    follow;
  }
  O BIEN...
  raid {
      detail;
  }
  O BIEN...
  disk-space;
  O BIEN...
  disk-partition;
  O BIEN...
  files;
  O BIEN...
  state {
      filter <valor>;
      O BIEN...
```

```
        filter-pretty <valor>;
        O BIEN...
        browser;
    }
    O BIEN...
    environmentals {
        fans;
        O BIEN...
        thermal;
        O BIEN...
        power;
    }
    O BIEN...
    setting {
      multi-vsys;
    }
  }
  O BIEN...
  high-availability {
    all;
    O BIEN...
    state;
    O BIEN...
    control-link {
      statistics;
    }
    O BIEN...
    transitions;
    O BIEN...
    path-monitoring;
    O BIEN...
    local-state;
  }
  O BIEN...
  log {
    config {
      direction {
        equal forward|backward;
      }
      csv-output {
        equal yes|no;
      }
      query {
        equal <valor>;
      }
      receive_time {
        in
last-60-seconds|last-15-minutes|last-hour|last-6-hrs|last-12-hrs|last-24-hrs|last-cale
ndar-day|last-7-days|last-30-days|last-calendar-month;
      }
      start-time {
        equal <valor>;
```

```
      }
      end-time {
        equal <valor>;
      }
      serial {
        equal <valor>;
        O BIEN...
        not-equal <valor>;
      }
      client {
        equal web|cli;
        O BIEN...
        not-equal web|cli;
      }
      cmd {
        equal
add|clone|commit|create|delete|edit|get|load-from-disk|move|rename|save-to-disk|set;
        O BIEN...
        not-equal
add|clone|commit|create|delete|edit|get|load-from-disk|move|rename|save-to-disk|set;
      }
      result {
        equal succeeded|failed|unauthorized;
        O BIEN...
        not-equal succeeded|failed|unauthorized;
      }
    }
    O BIEN...
    system {
      direction {
        equal forward|backward;
      }
      csv-output {
        equal yes|no;
      }
      query {
        equal <valor>;
      }
      receive_time {
        in
last-60-seconds|last-15-minutes|last-hour|last-6-hrs|last-12-hrs|last-24-hrs|last-cale
ndar-day|last-7-days|last-30-days|last-calendar-month;
      }
      start-time {
        equal <valor>;
      }
      end-time {
        equal <valor>;
      }
      serial {
        equal <valor>;
        O BIEN...
        not-equal <valor>;
```

```
      }
      opaque {
        contains <valor>;
      }
      severity {
        equal critical|high|medium|low|informational;
        O BIEN...
        not-equal critical|high|medium|low|informational;
        O BIEN...
        greater-than-or-equal critical|high|medium|low|informational;
        O BIEN...
        less-than-or-equal critical|high|medium|low|informational;
      }
      subtype {
        equal <valor>;
        O BIEN...
        not-equal <valor>;
      }
      object {
        equal <valor>;
        O BIEN...
        not-equal <valor>;
      }
      eventid {
        equal <valor>;
        O BIEN...
        not-equal <valor>;
      }
      id {
        equal <valor>;
        O BIEN...
        not-equal <valor>;
      }
    }
  }
}

debug {
  web-server {
    reset-cache;
    O BIEN...
    log-level {
      info;
      O BIEN...
      warn;
      O BIEN...
      crit;
      O BIEN...
      debug;
    }
  }
```

```
O BIEN...
delete {
  sample {
    sha256 {
      equal <valor>;
    }
  }
}
O BIEN...
swm {
  list;
  O BIEN...
  log;
  O BIEN...
  history;
  O BIEN...
  status;
  O BIEN...
  unlock;
  O BIEN...
  revert;
}
O BIEN...
tac-login {
    permanently-disable;
    O BIEN...
    challenge;
    O BIEN...
    response;
}
O BIEN...
software {
  restart {
    management-server;
    O BIEN...
    web-server;
    O BIEN...
    ntp;
  }
  O BIEN...
  core {
    management-server;
    O BIEN...
    web-server;
  }
  O BIEN...
  trace {
    management-server;
    O BIEN...
    web-server;
  }
}
```

```
O BIEN...
cli on|off|detail|show;
O BIEN...
system {
  maintenance-mode;
  O BIEN...
  disk-sync;
  O BIEN...
  ssh-key-reset {
    management;
    O BIEN...
    all;
  }
}
O BIEN...
device {
  set queue|all;
  O BIEN...
  unset queue|all;
  O BIEN...
  on error|warning|info|debug|dump;
  O BIEN...
  off;
  O BIEN...
  show;
  O BIEN...
  clear;
  O BIEN...
  dump {
    queues;
    O BIEN...
    queue-stats;
    O BIEN...
    queue <valor>;
  }
  O BIEN...
  flush {
    queue <valor>;
  }
  O BIEN...
  set-watermark {
    queue <valor>;
    type high|low;
    value 0-4000;
  }
}
O BIEN...
vardata-receiver {
  set {
    third-party libcurl|all;
    O BIEN...
    all;
```

```
    }
    O BIEN...
    unset {
      third-party libcurl|all;
      O BIEN...
      all;
    }
    O BIEN...
    on normal|debug|dump;
    O BIEN...
    off;
    O BIEN...
    show;
    O BIEN...
    statistics;
  }
  O BIEN...
  wildfire {
    reset {
      forwarding;
    }
  }
  O BIEN...
  management-server {
    client {
      disable authd|useridd|ha_agent;
      O BIEN...
      enable authd|useridd|ha_agent;
    }
    O BIEN...
    conn;
    O BIEN...
    on error|warn|info|debug|dump;
    O BIEN...
    off;
    O BIEN...
    clear;
    O BIEN...
    show;
    O BIEN...
    set {
      all;
      O BIEN...
      comm basic|detail|all;
      O BIEN...
      panorama basic|detail|all;
      O BIEN...
      proxy basic|detail|all;
      O BIEN...
      server basic|detail|all;
    }
```

```
    O BIEN...
    unset {
      all;
      O BIEN...
      comm basic|detail|all;
      O BIEN...
      panorama basic|detail|all;
      O BIEN...
      proxy basic|detail|all;
      O BIEN...
      server basic|detail|all;
    }
  }
}

upload {
  generic_chunks {
    todir <valor>;
    tofile <valor>;
    offset 0-419430600;
    endoffile yes|no;
    content <valor>;
  }
  O BIEN...
  generic {
    name <valor>;
    path <valor>;
    content <valor>;
    todir <valor>;
    tofile <valor>;
  }
  O BIEN...
  config {
    name <valor>;
    path <valor>;
    content <valor>;
  }
  O BIEN...
  software {
    name <valor>;
    path <valor>;
    content <valor>;
  }
  O BIEN...
  license {
    name <valor>;
    path <valor>;
    content <valor>;
  }
```

```
O BIEN...
certificate {
  name <valor>;
  passphrase <valor>;
  path <valor>;
  content <valor>;
  certificate-name <valor>;
  format pkcs12|pem;
}
O BIEN...
private-key {
  name <valor>;
  passphrase <valor>;
  path <valor>;
  content <valor>;
  certificate-name <valor>;
  format pkcs12|pem;
}
O BIEN...
keypair {
  name <valor>;
  passphrase <valor>;
  path <valor>;
  content <valor>;
  certificate-name <valor>;
  format pkcs12|pem;
}
O BIEN...
ssl-optout-text {
  name <valor>;
  path <valor>;
  content <valor>;
}
O BIEN...
ssl-cert-status-page {
  name <valor>;
  path <valor>;
  content <valor>;
}
O BIEN...
logo {
  name <valor>;
  path <valor>;
  content <valor>;
}
O BIEN...
custom-logo {
    login-screen {
      name <valor>;
      path <valor>;
    }
```

```
      O BIEN...
      main-ui {
        name <valor>;
        path <valor>;
      }
      O BIEN...
      pdf-report-header {
        name <valor>;
        path <valor>;
      }
      O BIEN...
      pdf-report-footer {
        name <valor>;
        path <valor>;
      }
  }
}

download {
  certificate {
    certificate-name <valor>;
    include-key yes|no;
    format pem|pkcs12;
    passphrase <valor>;
  }
  O BIEN...
  csv;
  O BIEN...
  techsupport;
  O BIEN...
  statsdump;
  O BIEN...
  generic {
    file <valor>;
  }
}

scp {
  import {
    configuration {
      from <valor>;
      remote-port 1-65535;
      source-ip <ip/máscara_de_red>;
    }
    O BIEN...
    license {
      from <valor>;
      remote-port 1-65535;
      source-ip <ip/máscara_de_red>;
    }
```

```
    O BIEN...
    software {
      from <valor>;
      remote-port 1-65535;
      source-ip <ip/máscara_de_red>;
    }
  }
  O BIEN...
  export {
    mgmt-pcap {
      from <valor>;
      to <valor>;
      remote-port 1-65535;
      source-ip <ip/máscara_de_red>;
    }
    O BIEN...
    configuration {
      from <valor>;
      to <valor>;
      remote-port 1-65535;
      source-ip <ip/máscara_de_red>;
    }
    O BIEN...
    tech-support {
      to <valor>;
      remote-port 1-65535;
      source-ip <ip/máscara_de_red>;
    }
  }
}

tftp {
  import {
    configuration {
      from <valor>;
      file <valor>;
      remote-port 1-65535;
      source-ip <ip/máscara_de_red>;
    }
    O BIEN...
    certificate {
      from <valor>;
      file <valor>;
      remote-port 1-65535;
      source-ip <ip/máscara_de_red>;
      certificate-name <valor>;
      passphrase <valor>;
      format pkcs12|pem;
    }
```

```
    O BIEN...
    private-key {
      from <valor>;
      file <valor>;
      remote-port 1-65535;
      source-ip <ip/máscara_de_red>;
      passphrase <valor>;
      certificate-name <valor>;
      format pkcs12|pem;
    }
    O BIEN...
    keypair {
      from <valor>;
      file <valor>;
      remote-port 1-65535;
      source-ip <ip/máscara_de_red>;
      passphrase <valor>;
      certificate-name <valor>;
      format pkcs12|pem;
    }
    O BIEN...
    license {
      from <valor>;
      file <valor>;
      remote-port 1-65535;
      source-ip <ip/máscara_de_red>;
    }
    O BIEN...
    software {
      from <valor>;
      file <valor>;
      remote-port 1-65535;
      source-ip <ip/máscara_de_red>;
    }
  }
  O BIEN...
  export {
    config-bundle {
      to <valor>;
      remote-port 1-65535;
      source-ip <ip/máscara_de_red>;
    }
    O BIEN...
    core-file {
      control-plane {
        from <valor>;
        to <valor>;
        remote-port 1-65535;
        source-ip <ip/máscara_de_red>;
      }
    }
```

```
O BIEN...
    device-state {
      to <valor>;
      remote-port 1-65535;
      source-ip <ip/máscara_de_red>;
    }
    O BIEN...
    mgmt-pcap {
      from <valor>;
      to <valor>;
      remote-port 1-65535;
      source-ip <ip/máscara_de_red>;
    }
    O BIEN...
    configuration {
      from <valor>;
      to <valor>;
      remote-port 1-65535;
      source-ip <ip/máscara_de_red>;
    }
    O BIEN...
    tech-support {
      to <valor>;
      remote-port 1-65535;
      source-ip <ip/máscara_de_red>;
    }
    O BIEN...
    log-file {
      management-plane {
        to <valor>;
        remote-port 1-65535;
        source-ip <ip/máscara_de_red>;
      }
    }
  }
}

load {
  config {
    key <valor>;
      last-saved;
      O BIEN...
      from <valor>;
      O BIEN...
      version <valor>1-1048576;
      O BIEN...
      partial {
        from <valor>;
        from-xpath <valor>;
        to-xpath <valor>;
        mode merge|replace|append;
      }
```

```
  }
  O BIEN...
  device-state;
}

less {
    mp-log <valor>;
    O BIEN...
    mp-backtrace <valor>;
}

grep {
  invert-match yes|no;
  line-number yes|no;
  ignore-case yes|no;
  no-filename yes|no;
  count yes|no;
  max-count 1-65535;
  context 1-65535;
  before-context 1-65535;
  after-context 1-65535;
  pattern <valor>;
    mp-log <valor>;
    O BIEN...
    dp-log <valor>;
}

tail {
  follow yes|no;
  lines 1-65535;
    mp-log <valor>;
}

ssh {
  inet yes|no;
  port 0-65535;
  source <valor>;
  v1 yes|no;
  v2 yes|no;
  host <valor>;
}

telnet {
  8bit yes|no;
  port 0-65535;
  host <valor>;
}

traceroute {
  ipv4 yes|no;
  first-ttl 1-255;
  max-ttl 1-255;
```

```
  port 1-65535;
  tos 1-255;
  wait 1-99999;
  pause 1-2000000000;
  do-not-fragment yes|no;
  debug-socket yes|no;
  gateway <ip/máscara_de_red>;
  no-resolve yes|no;
  bypass-routing yes|no;
  source <valor>;
  host <valor>;
}

netstat {
  route yes|no;
  interfaces yes|no;
  groups yes|no;
  statistics yes|no;
  verbose yes|no;
  numeric yes|no;
  numeric-hosts yes|no;
  numeric-ports yes|no;
  numeric-users yes|no;
  symbolic yes|no;
  extend yes|no;
  programs yes|no;
  continuous yes|no;
  listening yes|no;
  all yes|no;
  timers yes|no;
  fib yes|no;
  cache yes|no;
}

ping {
  bypass-routing yes|no;
  count 1-2000000000;
  do-not-fragment yes|no;
  interval 1-2000000000;
  source <valor>;
  no-resolve yes|no;
  pattern <valor>;
  size 0-65468;
  tos 1-255;
  ttl 1-255;
  verbose yes|no;
  host <valor>;
}
```

test wildfire registration

Descripción

Ejecute una prueba para verificar si se han registrado correctamente el dispositivo WildFire o un firewall con un servidor WildFire. Si la prueba es satisfactoria, se mostrarán la dirección IP o el nombre del servidor WildFire, lo que indica que el dispositivo/firewall podrán enviar archivos al servidor de WildFire para su análisis.

Ubicación de jerarquía

Nivel máximo del modo de operaciones.

Sintaxis

```
test {
  wildfire {
    registration;
  }
}
```

Opciones

```
No hay opciones adicionales.
```

Resultado de muestra

A continuación se muestra un resultado satisfactorio de un firewall que puede comunicarse con un dispositivo WildFire. Si es un dispositivo WildFire apuntando a la Nube de WildFire de Palo Alto Networks, el nombre del servidor de uno de los servidores de la Nube se muestra en el campo `seleccione el mejor servidor:`.

```
Test wildfire
        registro de wildfire:         successful
        download server list:          successful
        select the best server:        ca-s1.wildfire.paloaltonetworks.com
```

Nivel de privilegios requerido

superusuario, superlector

set wildfire portal-admin

Descripción

Establece la contraseña de la cuenta de administrador del portal que servirá para ver los informes de WildFire desde un firewall. El nombre de usuario y la contraseña predeterminados son admin/admin. Tras introducir el comando, pulse Intro y aparecerá un mensaje para cambiar la contraseña.

Esta cuenta se usa cuando se ven los detalles del log de WildFire en el firewall o Panorama y se hace clic en **Ver informe WildFire**. Después de la autenticación, se recupera el informe de análisis detallado de WildFire y se muestra en su explorador.

La cuenta de administrador del portal es la única cuenta para ver informes desde los logs; es posible cambiar la contraseña, pero no se puede cambiar el nombre de cuenta ni crear cuentas adicionales.

Ubicación de jerarquía

Nivel máximo del modo de operaciones.

Sintaxis

```
set {
  wildfire {
    portal-admin {
      password <valor>;
    }
  }
```

Opciones

```
No hay opciones adicionales.
```

Resultado de muestra

A continuación se muestra el resultado de este comando.

```
admin@wf-corp1> set wildfire portal-admin password
Enter password   :
Confirm password :
```

Nivel de privilegios requerido

superusuario, superlector

raid

Descripción

Use esta opción para manejar los pares de RAID instalados en el dispositivo WildFire. El dispositivo WF-500 WildFire se entrega con cuatro unidades en las cuatro primeras bahías de unidades (A1, A2, B1, B2). Las unidades A1 y A2 son el par RAID 1 y las unidades B1 y B2 son el segundo par RAID 1.

Ubicación de jerarquía

request system

Sintaxis

```
raid {
      remove <valor>;
      O BIEN...
      copy {
        from <valor>;
        to <valor>;
      }
      O BIEN...
        add {
```

Opciones

```
> add      Añade una unidad al par de discos RAID correspondiente
> copy     Copia y migra de una unidad a otra en la bahía
> remove   unidad que se eliminará del par de discos RAID
```

Resultado de muestra

El siguiente resultado muestra un dispositivo WildFire WF-500 con una RAID configurada correctamente.

```
admin@wf-corp1> show system raid

Disk Pair A                          Available
   Disk id A1                          Present
   Disk id A2                          Present
Disk Pair B                          Available
   Disk id B1                          Present
   Disk id B2                          Present
```

Nivel de privilegios requerido

superusuario, superlector

show wildfire

Descripción

Muestra la información de registro del dispositivo WildFire, actividad, muestras recientes que se han analizado e información de la máquina virtual.

Ubicación de jerarquía

show wildfire

Sintaxis

```
sample-status {
      sha256 {
        equal <valor>;
      }
    }
    O BIEN...
    status;
    O BIEN...
    statistics;
    O BIEN...
    latest {
      analysis {
        filter malicious|benign;
        sort-by SHA256|Submit Time|Start Time|Finish Time|Malicious|Status;
        sort-direction asc|desc;
        limit 1-20000;
        days 1-7;
      }
      O BIEN...
      sessions {
        filter malicious|benign;
        sort-by SHA256|Create Time|Src IP|Src Port|Dst Ip|Dst Port|File|Device
ID|App|Malicious|Status;
        sort-direction asc|desc;
        limit 1-20000;
        days 1-7;
      }
      O BIEN...
      samples {
        filter malicious|benign;
        sort-by SHA256|Create Time|File Name|File Type|File Size|Malicious|Status;
        sort-direction asc|desc;
```

```
        limit 1-20000;
        days 1-7;
      }
      O BIEN...
      uploads {
        sort-by SHA256|Create Time|Finish Time|Status;
        sort-direction asc|desc;
        limit 1-20000;
        days 1-7;
      }
    O BIEN...
    last-device-registration {
      all;
    }
  }
```

Opciones

```
admin@wf-corp1> show wildfire
> last-device-registration     Muestra una lista de las últimas actividades de
                              registro
> latest                      Muestra las últimas 30 actividades, que
                              incluyen las últimas 30 actividades de
                              análisis, los últimos 30 archivos que se
                              analizaron, información de la sesión de red en
                              archivos que fueron analizados y archivos que
                              fueron cargados al servidor en la Nube pública.
> sample-status               Muestra un estado de ejemplo de wildfire
> statistics                  Muestra estadísticas básicas de wildfire
> status                      Estado
```

Resultado de muestra

A continuación se muestra el resultado de este comando.

```
admin@wf-corp1> show wildfire last-device-registration all

+--------------+---------------------+-------------+------------+----------+--
--
----+
| Device ID    | Last Registered     | Device IP   | SW Version | HW Model | Sta
tus |
+--------------+---------------------+-------------+------------+----------+--
--
----+
| 001606000114 | 2013-03-12 08:34:09 | 192.168.2.1 | 5.0.2      | PA-200   | OK
    |
+--------------+---------------------+-------------+------------+----------+--
--

admin@wf-corp1> show wildfire latest
> analysis   Muestra los últimos 30 análisis
> samples    Muestra los últimos 30 ejemplos
> sessions   Muestra las últimas 30 sesiones
> uploads    Muestra las últimas 30 cargas
```

```
show wildfire sample-status sha256 equal
c08ec3f922e26b92dac959f672ed7df2734ad7840cd40dd72db72d9c9827b6e8

Sample information:
+---------------------+------------------+-----------+-----------+-----------+-------
------------+
| Create Time       | File Name       | File Type | File Size | Malicious | Status
|
+---------------------+------------------+-----------+-----------+-----------+-------
------------+
| 2013-03-07 10:22:00 | 5138e1fa13a66.exe | PE        | 261420    | No        | analysis
complete |
| 2013-03-07 10:22:00 | 5138e1fa13a66.exe | PE        | 261420    | No        | analysis
complete |
+---------------------+------------------+-----------+-----------+-----------+-------
------------+

Session information:
+---------------------+---------------+----------+-------------+----------+---------
----------+-------------+-------------+-----------+-----------+
| Create Time        | Src IP        | Src Port | Dst IP      | Dst Port | File
| Device ID    | App           | Malicious | Status    |
+---------------------+---------------+----------+-------------+----------+---------
----------+-------------+-------------+-----------+-----------+
| 2013-03-07 10:22:42 | 46.165.211.184 | 80       | 192.168.2.10 | 53620    |
5138e223a1069.exe | 001606000114 | web-browsing | No        | completed |
| 2013-03-07 10:22:02 | 46.165.211.184 | 80       | 192.168.2.10 | 53618    |
5138e1fb3e5fb.exe | 001606000114 | web-browsing | No        | completed |
| 2013-03-07 10:22:00 | 46.165.211.184 | 80       | 192.168.2.10 | 53617    |
5138e1fa13a66.exe | 001606000114 | web-browsing | No        | completed |
+---------------------+---------------+----------+-------------+----------+---------
----------+-------------+-------------+-----------+-----------+

Analysis information:
+---------------------+---------------------+---------------------+-----------+-------
----+
| Submit Time         | Start Time          | Finish Time         | Malicious | Status
|
+---------------------+---------------------+---------------------+-----------+-------
----+
| 2013-03-07 10:22:01 | 2013-03-07 10:22:01 | 2013-03-07 10:27:02 | No        |
completed |
+---------------------+---------------------+---------------------+-----------+-------
----+

admin@wf-corp1> show wildfire statistics days 7

Last one hour statistics:
Total sessions submitted  :           0
Samples submitted         :           0
Samples analyzed          :           0
Samples pending           :           0
Samples (malicious)       :           0
Samples (benign)          :           0
```

```
Samples (error)           :            0
Malware sent to cloud     :            0

Last 7 days statistics:
Total sessions submitted  :           23
Samples submitted         :            3
Samples analyzed          :            3
Samples pending           :            0
Samples (malicious)       :            0
Samples (benign)          :            3
Samples (error)           :            0
Malware sent to cloud     :            0

admin@wf-corp1> show wildfire status

Connection info:
        Wildfire cloud:                 wildfire-public-cloud
        Status:                         Idle
        Auto-Submit:                    disabled
        VM internet connection:         disabled
        Best server:
        Device registered:              no
        Service route IP address:       192.168.2.20
        Signature verification:         enable
        Server selection:               enable
        Through a proxy:                no
```

Nivel de privilegios requerido

superusuario, superlector

show system raid

Descripción

Muestra la configuración RAID del dispositivo. El dispositivo WF-500 WildFire se entrega con cuatro unidades en las cuatro primeras bahías de unidades (A1, A2, B1, B2). Las unidades A1 y A2 son el par RAID 1 y las unidades B1 y B2 son el segundo par RAID 1.

Ubicación de jerarquía

show system

Sintaxis

```
raid{
        detail;
```

Opciones

```
No hay opciones adicionales.
```

Resultado de muestra

A continuación se muestra la configuración RAID en un dispositivo WildFire WF-500.

```
admin@wf-corp1> show system raid detail

Disk Pair A                             Available
   Status                                   clean
   Disk id A1                             Present
       model         : ST91000640NS
       size          : 953869 MB
       partition_1   : active sync
       partition_2   : active sync
   Disk id A2                             Present
       model         : ST91000640NS
       size          : 953869 MB
       partition_1   : active sync
       partition_2   : active sync
Disk Pair B                             Available
   Status                                   clean
   Disk id B1                             Present
       model         : ST91000640NS
       size          : 953869 MB
       partition_1   : active sync
```

```
    partition_2  : active sync
Disk id B2                          Present
    model        : ST91000640NS
    size         : 953869 MB
    partition_1  : active sync
    partition_2  : active sync
```

Nivel de privilegios requerido

superusuario, superlector