paloalto
TECHDOCS

Gestión de Advanced Threat Prevention

Contact Information

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

About the Documentation

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

Copyright

Last Revised

May 18, 2023

Table of Contents

Advanced Threat Prevention

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia de Advanced Threat Prevention (para un mejor soporte de funciones) o Threat Prevention

Las suscripciones de prevención de intrusiones de amenazas de cortafuegos de nueva generación de Palo Alto Networks® protegen y defienden su red de las amenazas de productos básicos y las amenazas avanzadas persistentes (APT) utilizando mecanismos de detección múltiples para combatir toda la gama del panorama de amenazas. La solución de prevención de amenazas de Palo Alto Networks se compone de las siguientes suscripciones:

- **Advanced Threat Prevention**: el servicio en la nube de Advanced Threat Prevention utiliza modelos de aprendizaje profundo y aprendizaje automático en línea para la detección en tiempo real de amenazas C2 evasivas y desconocidas nunca antes vistas, así como de vulnerabilidades de día cero. Como servicio nativo en la nube de latencia ultra baja, esta solución extensible e infinitamente escalable siempre se mantiene actualizada con las mejoras de entrenamiento de modelos. También es compatible con el aprendizaje profundo local, el cual complementa el componente basado en nube del análisis en línea en la nube de Advanced Threat Prevention al proporcionar un mecanismo para realizar análisis rápidos y locales basados en el aprendizaje profundo de amenazas de día cero y otras amenazas evasivas. La licencia de Advanced Threat Prevention incluye todos los beneficios incluidos con Threat Prevention.
- **Threat Prevention**: la suscripción básica de Threat Prevention se basa en firmas generadas a partir de datos de tráfico maliciosos recopilados de varios servicios de Palo Alto Networks. Estas firmas son utilizadas por el cortafuegos para hacer cumplir las políticas de seguridad basadas en amenazas específicas, que incluyen: comando y control (C2), varios tipos de malware conocido y vulnerabilidades; y combinado con las tecnologías de identificación de ID de aplicación e ID de usuario en el cortafuegos, puede hacer referencias cruzadas a datos de contexto para producir políticas detalladas. Como parte de sus políticas de mitigación de amenazas, también puede identificar y bloquear tipos de archivos y direcciones IP conocidos o riesgosos, de los cuales hay varias categorías prefabricadas disponibles, incluidas listas que especifican proveedores de servicios a prueba de balas e IP maliciosas conocidas. En los casos en que se utilizan herramientas y software especializados, puede crear sus propias firmas de vulnerabilidad para personalizar sus capacidades de prevención de intrusiones según los requisitos únicos de su red.

Para maximizar la prevención de amenazas, Palo Alto Network también recomienda los siguientes servicios de suscripción, además de Advanced | Threat Prevention:

- **DNS Security**: el servicio DNS Security en la nube diseñado para proteger a su organización de amenazas avanzadas basadas en DNS. Al aplicar el aprendizaje automático avanzado y el análisis predictivo a una amplia gama de fuentes de inteligencia de amenazas, DNS Security genera un conjunto de firmas DNS mejorado y proporciona un análisis en tiempo real de las solicitudes de DNS para defender su red contra los dominios maliciosos recién generados. DNS Security puede detectar varias amenazas C2, incluidos túneles DNS, ataques de reenlace de DNS, dominios creados mediante generación automática, hosts de malware y mucho más. DNS Security requiere y funciona con su suscripción a Advanced Threat Prevention o Threat Prevention para obtener una cobertura completa de amenazas DNS.

Las suscripciones de prevención de intrusiones de Palo Alto Networks trabajan juntas para proporcionar una solución integral que intercepta y rompe la cadena en varias etapas del proceso de ataque y proporciona visibilidad para evitar infracciones de seguridad en su infraestructura de red.

Servicios de detección de Advanced Threat Prevention

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	☐ Licencia de Advanced Threat Prevention (para un mejor soporte de funciones) o Threat Prevention

Advanced Threat Prevention es un sistema de prevención de intrusiones (IPS en inglés) que puede detectar y bloquear malware, vulnerabilidades y mando y control (C2 en inglés) en todos los puertos y protocolos, utilizando un sistema de prevención de múltiples capas con componentes que operan en el cortafuegos y en la nube. La nube de Threat Prevention opera una multitud de servicios de detección que utilizan los datos de amenazas combinados de los servicios de Palo Alto Networks para crear firmas, cada una de las cuales posee patrones identificables específicos, y son utilizados por el cortafuegos para hacer cumplir las políticas de seguridad cuando se detectan amenazas coincidentes y comportamientos maliciosos. Estas firmas se clasifican en función del tipo de amenaza y se les asignan números de identificador únicos. Para detectar amenazas que se corresponden con estas firmas, el cortafuegos opera motores de análisis que inspeccionan y clasifican el tráfico de red que exhibe rasgos anómalos.

Además del mecanismo de detección basado en firmas, Advanced Threat Prevention proporciona un sistema de detección en línea para evitar amenazas C2 desconocidas y evasivas, incluidas las producidas a través del marco Empire, así como vulnerabilidades de inyección de comandos e inyección SQL. La nube de Advanced Threat Prevention opera modelos de aprendizaje profundo extensibles que permiten capacidades de análisis en línea en el cortafuegos, por solicitud, para evitar que las amenazas de día cero entren a la red así como para distribuir protecciones. Esto le permite prevenir amenazas desconocidas mediante la inspección del tráfico en tiempo real con detectores en línea. Estos motores de detección basados en el aprendizaje automático y aprendizaje profundo en la nube de Advanced Threat Prevention analizan el tráfico en busca de C2 desconocidos y vulnerabilidades que utilizan la inyección SQL y la inyección de comandos para protegerse frente a las amenazas de día cero. Para proporcionar un contexto de amenaza y detalles completos de detección, se generan informes que pueden incluir las herramientas/técnicas utilizadas por el atacante, el alcance y el impacto de la detección; así como la clasificación de ciberataque correspondiente según lo definido por el marco MITRE ATT&CK®.

MITRE ATT&CK® es una base de conocimientos seleccionada y un modelo para el comportamiento de los adversarios cibernéticos. Este trabajo se reproduce y distribuye con el permiso de The MITRE Corporation. Por la presente, MITRE Corporation (MITRE) le otorga una licencia no exclusiva y libre de regalías para usar ATT&CK® con fines comerciales, de investigación y desarrollo. Cualquier copia que realice para tales fines está autorizada siempre que reproduzca la designación de derechos de autor de MITRE y esta licencia en dicha copia.

Al operar motores de detección basados en la nube, puede acceder a una amplia gama de mecanismos de detección que se actualizan e implementan automáticamente sin necesidad de que el usuario descargue contenido de actualización u opere analizadores basados en cortafuegos que requieren un uso intensivo de procesos que consumen recursos. La lógica del motor de detección basada en la nube se monitorea y actualiza continuamente utilizando conjuntos de datos de tráfico C2 de WildFire, con soporte adicional de los investigadores de amenazas de Palo Alto Networks que brindan intervención humana para mejoras de detección altamente acusadas. Los motores de aprendizaje profundo de Advanced Threat Prevention admiten el análisis de amenazas basadas en C2 a través de aplicaciones HTTP, HTTP2, SSL, unknown-UDP y unknown-TCP. Los modelos de análisis adicionales se entregan a través de actualizaciones de contenido, sin embargo, las mejoras a los modelos existentes se realizan como una actualización del lado de la nube, que no requiere actualización del cortafuegos.

Advanced Threat Prevention también es compatible con el aprendizaje profundo local, que proporciona un mecanismo para realizar análisis rápidos y locales basados en el aprendizaje profundo de amenazas de día cero y otras amenazas evasivas, como una característica complementaria al componente de Análisis en línea en la nube basado en la nube de Advanced Threat Prevention. El tráfico malintencionado conocido que coincide con el conjunto de firmas publicadas de Palo Alto Networks se descarta (o se les aplica otra acción definida por el usuario); sin embargo, cierto tráfico que coincide con los criterios de contenido sospechoso se redirige para su análisis mediante el módulo de detección de análisis de Deep Leaning. Si es necesario un análisis más detallado, el tráfico se envía a la nube de Advanced Threat Prevention para un análisis adicional, así como para las comprobaciones de falsos positivos y falsos negativos necesarias. El módulo de detección de Deep Learning se basa en los módulos de detección probados que operan en la nube de Advanced Threat Prevention y, como tal, tiene las mismas capacidades de detección de amenazas avanzadas y de día cero. Sin embargo, también tienen la ventaja añadida de procesar un volumen de tráfico mucho mayor, sin el retraso asociado a las consultas en la nube. Esto le permite inspeccionar más tráfico y recibir veredictos en un período de tiempo más corto. Esto es especialmente beneficioso cuando se enfrenta a condiciones de red desafiantes.

Palo Alto Networks también ofrece la suscripción a Threat Prevention que no incluye las funciones que se encuentran en la licencia Advanced Threat Prevention basada en la nube.

Las firmas de amenazas utilizadas por el cortafuegos se clasifican ampliamente en tres tipos: antivirus, antispyware y vulnerabilidad, y son utilizadas por los perfiles de seguridad correspondientes para hacer cumplir las políticas definidas por el usuario.

Los servicios de seguridad entregados en la nube de Palo Alto Networks también generan firmas WildFire y DNS C2 para sus respectivos servicios, así como firmas de formato de archivo, que pueden designar tipos de archivos en lugar de firmas de amenazas, por ejemplo, como excepciones de firma.

- Las firmas antivirus detectan varios tipos de malware y virus, incluidas descargas de gusanos, troyanos y spyware.
- Las firmas antispyware detectan el spyware C2 en hosts comprometidos al intentar llamar a casa o balizar a un servidor C2 externo.
- Las firmas de vulnerabilidad detectan vulnerabilidades del sistema de explotación.

Las firmas tienen un nivel de gravedad predeterminado con una acción predeterminada asociada; por ejemplo, en el caso de una amenaza malintencionada alta, la acción predeterminada es Restablecer ambos. Esta configuración se basa en las recomendaciones de seguridad de Palo Alto Networks.

En implementaciones en las que hay aplicaciones internas especializadas o en casos en los que la inteligencia externa se alimenta utilizando reglas de código abierto Snort y Suricata, se pueden crear Firmas personalizadas para una protección específica.

Los cortafuegos reciben actualizaciones de firmas de dos formas paquetes de actualización: el contenido antivirus diario y las actualizaciones semanales de contenido de aplicaciones y amenazas. Las actualizaciones de contenido antivirus incluyen firmas antivirus y firmas DNS (C2) utilizadas por los perfiles de seguridad antivirus y antispyware, respectivamente. Las actualizaciones de contenido para aplicaciones y amenazas incluyen firmas de vulnerabilidad y antispyware, utilizadas por los perfiles de seguridad de vulnerabilidad y antispyware, respectivamente. Los paquetes de actualización también incluyen contenido adicional aprovechado por otros servicios y subfunciones. Para obtener más información, consulte Actualizaciones de contenido dinámico.

Categorías de firma de amenazas

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia de Advanced Threat Prevention (para un mejor soporte de funciones) o Threat Prevention

Existen tres tipos de firmas de amenazas de Palo Alto Networks; cada una diseñada para detectar diferentes amenazas a medida que el cortafuegos analiza el tráfico de red:

- Firmas de antivirus: detectan antivirus y malware encontrados en tipos de archivos y ejecutables.
- Firmas antispyware: detectan actividad de comando y control (command-and-control, C2), en la que el spyware en un cliente infectado recopila datos o se comunica con un atacante remoto sin el consentimiento del usuario.
- Firmas de vulnerabilidades: detecta fallos en el sistema que un atacante podría intentar aprovechar.

La gravedad de una firma indica el riesgo del evento detectado, y la acción predeterminada de una firma (por ejemplo, bloquear o alertar) es la forma en que Palo Alto Networks recomienda que aplique el tráfico coincidente.

Debe Configuración de antivirus, antispyware y protección frente a vulnerabilidades para definir qué acción tomar cuando se detecta una amenaza, y puede utilizar fácilmente los perfiles de seguridad predeterminados para comenzar a bloquear amenazas según las recomendaciones de Palo Alto Networks. Para cada tipo de firma, categoría e incluso firmas específicas, puede continuar modificando o creando perfiles nuevos para detectar de manera más detallada amenazas potenciales.

La siguiente tabla detalla todas las posibles categorías de firma por tipo (antivirus, spyware y vulnerabilidades) e incluye la actualización de contenido (aplicaciones y amenazas, antivirus o WildFire) que proporcionan las firmas en cada categoría. También puede visitar la base de datos de amenazas de Palo Alto Networks para Más información sobre las firmas de amenazas.

Categoría de amenaza	Actualización de contenido que proporciona estas firmas	Description (Descripción)
Firmas de antivirus		

Categoría de amenaza	Actualización de contenido que proporciona estas firmas	Description (Descripción)
apk	Antivirus WildFire	Archivos maliciosos de las Aplicaciones de Android (Android Application, APK).
MacOSX	Antivirus WildFire	Archivos maliciosos de MacOSX, que incluyen: • Archivos de imagen de disco (DMG) de Apple. • Los archivos de objeto Mach (Mach-O) son ejecutables, bibliotecas y código objeto. • Paquetes de instalación de software de Apple (PKG)
flash	Antivirus Wildfire o Wildfire privado	Los applets de Adobe Flash y el contenido de Flash insertado en páginas web.
jar	Antivirus Wildfire	Applets de Java (tipos de archivo JAR/Class).
ms-office	Antivirus Wildfire o Wildfire privado	Archivos de Microsoft Office, como documentos (DOC, DOCX, RTF), libros (XLS, XLSX) y presentaciones de PowerPoint (PPT, PPTX). Esto también incluye documentos de Office Open XML (OOXML) 2007+.
pdf	Antivirus Wildfire o Wildfire privado	Archivos con formato de documento portable (Portable document format, PDF).
pe	Antivirus Wildfire o Wildfire privado	Los archivos Ejecutables portátiles (Portable executable, PE) pueden ejecutarse automáticamente en un sistema de Microsoft Windows y solo deben permitirse cuando están autorizados. Estos tipos de archivos incluyen: • Código objeto. • Fuentes (FON). • Archivos de sistema (SYN). • Archivos de controladores (DRV). • Elementos del panel de control de Windows (CPL). • Bibliotecas de enlaces dinámicos (dynamic-link libraries, DLL). • OCX (bibliotecas para controles personalizados OLE o controles ActiveX).

Categoría de amenaza	Actualización de contenido que proporciona estas firmas	Description (Descripción)
		• Archivos de salvapantallas de Windows (SCR). • Archivos de la Interfaz de firmware extensible (Extensible Firmware Interface, EFI), que se ejecutan entre un SO y el firmware para facilitar actualizaciones de dispositivos y operaciones de inicio. • Archivos de información de programa (Program information files, PIF).
Linux	Antivirus Wildfire	Archivos de formato ejecutable (Executable and Linkable Format, ELF).
archive	Antivirus Wildfire	Archivos de almacenamiento Roshal Archive (RAR) and 7-Zip (7z).
Firmas de spyware		
Adware	Aplicaciones y amenazas	Detecta programas que muestran anuncios potencialmente no deseados. Algunos adware modifican los exploradores para destacar e incluir un hipervínculo a las palabras claves buscadas con más frecuencia en páginas web; estos enlaces redirigen a los usuarios a los sitios web de anuncios. El adware también puede recuperar actualizaciones de un servidor de comando y control (command-and-control, C2) e instalar estas actualizaciones en un explorador o en el sistema de un cliente. Las protecciones nuevas en esta categoría son escasas.
autogen	Antivirus	Estas firmas basadas en la carga útil detectan el tráfico de comando y control (command-and-control, C2) y se generan automáticamente. En gran medida, las firmas autogeneradas pueden detectar el tráfico de C2 incluso cuando el host de C2 es desconocido o cambia con rapidez.
backdoor	Aplicaciones y amenazas	Detecta un programa que permite a un atacante obtener acceso remoto no autorizado a un sistema.
Botnet	Aplicaciones y amenazas	Indica la actividad de botnet. Un botnet es una red de ordenadores infectados con malware ("bots") que un atacante controla. El atacante puede controlar de

Categoría de amenaza	Actualización de contenido que proporciona estas firmas	Description (Descripción)
		manera central cada ordenador de un botnet para llevar a cabo una acción coordinada simultáneamente (por ejemplo, iniciar un ataque DoS).
browser-hijack	Aplicaciones y amenazas	Detecta un complemento o software que modifica la configuración del explorador. Un secuestrador de explorador podría controlar la búsqueda automática o realizar un seguimiento de la actividad de los usuarios y enviar esta información a un servidor de C2. Las protecciones nuevas en esta categoría son escasas.
cryptominer (criptominado)	Aplicaciones y amenazas	(A veces conocido como cryptojacking o minería) Detecta el intento de descarga o el tráfico de red generado por programas maliciosos diseñados para utilizar recursos informáticos para extraer criptomonedas sin el conocimiento del usuario. Los binarios de criptominado se entregan con frecuencia mediante un descargador de scripts de shell que intenta determinar la arquitectura del sistema y eliminar otros procesos de minería en el sistema. Algunas minerías se ejecutan dentro de otros procesos, como un navegador web que representa una página web maliciosa.
data-theft	Aplicaciones y amenazas	Detecta a un sistema que envía información a un servidor de C2 conocido. Las protecciones nuevas en esta categoría son escasas.
dns	Antivirus	Detecta solicitudes de DNS para conectarse a dominios maliciosos. Las firmas de dns y dns-wildfire detectan los mismos dominios maliciosos; sin embargo, las firmas dns están incluidas en la actualización de contenido de antivirus diaria y las firmas dns-wildfire están incluidas en las actualizaciones de WildFire que emite protecciones cada 5 minutos.
dns-security	Antivirus	Detecta solicitudes de DNS para conectarse a dominios maliciosos. dns-security incluye firmas de dns y de dns-wildfire, además de las firmas únicas que genera el servicio DNS Security.

Categoría de amenaza	Actualización de contenido que proporciona estas firmas	Description (Descripción)
dns-wildfire	Wildfire o Wildfire privado	Detecta solicitudes de DNS para conectarse a dominios maliciosos. Las firmas de dns y dns-wildfire detectan los mismos dominios maliciosos; sin embargo, las firmas dns están incluidas en la actualización de contenido de antivirus diaria y las firmas dns-wildfire están incluidas en las actualizaciones de WildFire que emite protecciones cada 5 minutos.
downloader (descargador)	Aplicaciones y amenazas	(También conocido como droppers [instaladores troyanos], stagers [escalonamientos] o loaders [cargadores]) Detecta programas que usan una conexión a Internet para conectarse a un servidor remoto para descargar y ejecutar malware en el sistema comprometido El caso de uso más común es que un descargador se implemente como la culminación de la *etapa uno* de un ciberataque, donde la ejecución de la carga útil obtenida del descargador se considera *etapa dos*. Los scripts de shell (Bash, PowerShell, etc.), los troyanos y los documentos de señuelos maliciosos (también conocidos como maldocs), como archivos PDF y Word, son tipos de descargadores comunes.
fraud (fraude)	Aplicaciones y amenazas	(Incluidos el robo de formularios, el phishing y las estafas) Detecta el acceso a sitios web comprometidos para los que se ha determinado que incorporan código JavaScript malicioso para recopilar información confidencial del usuario (por ejemplo, nombre, dirección, correo electrónico, número de tarjeta de crédito, CVV y fecha de vencimiento) de los formularios de pago que se capturan en las páginas de pago de los sitios web de comercio electrónico.
hacktool (herramienta de hackeo)	Aplicaciones y amenazas	Detecta el tráfico generado por las herramientas de software que utilizan los actores malintencionados para realizar reconocimientos, atacar u obtener acceso a sistemas vulnerables, exfiltrar datos o crear un canal de comando y control para controlar de forma secreta un sistema informático sin autorización. Estos programas están fuertemente asociados con malware y ciberataques. Las herramientas de hacking pueden implementarse de manera benigna cuando se utilizan en operaciones de Red y Blue Team, pruebas de penetración e I+D. El uso o posesión de estas

Categoría de amenaza	Actualización de contenido que proporciona estas firmas	Description (Descripción)
		herramientas puede ser ilegal en algunos países, independientemente de su intención.
Registrador de pulsaciones de teclas	Aplicaciones y amenazas	Detecta programas que permiten a los atacantes rastrear la actividad del usuario de manera secreta mediante el registro de pulsaciones de teclas y capturas de pantalla. Los registradores de pulsaciones de teclas usan varios métodos de C2 para enviar periódicamente logs e informes a una dirección de correo electrónico predefinida o a un servidor de C2. Mediante la vigilancia de las pulsaciones de teclas, un atacante podría recuperar las credenciales que le brindarían el acceso a la red.
networm	Aplicaciones y amenazas	Detecta un programa que se replica automáticamente y se transmite de sistema en sistema. Los networm podrían usar recursos compartidos o aprovechar fallas de seguridad para acceder a los sistemas objetivo.
Kit de phishing (suplantación de identidad)	Aplicaciones y amenazas	Detecta cuando un usuario intenta conectar a una página de destino del kit de phishing (generalmente después de recibir un correo electrónico con un enlace al sitio malicioso). Un sitio web de phishing engaña a los usuarios para enviar credenciales que un atacante puede robar para obtener acceso a la red. *Además de bloquear el acceso a las páginas de destino del kit de phishing, habilite la autenticación multifactor y la prevención de phishing de credenciales para evitar los ataques de phishing en todas las etapas.*
post-exploitation	Aplicaciones y amenazas	Detecta la actividad que indica la etapa de post-exploitation de un ataque, en el que un atacante intenta evaluar el valor de un sistema en riesgo. Esto podría incluir evaluar la confidencialidad de los datos almacenados en el sistema, y la utilidad del sistema en comprometer más la red.
webshell	Aplicaciones y amenazas	Detecta web shells y tráfico web shell, incluida la detección de implantes y la interacción de comando y control. Los web shells primero deben implantarlos un actor malintencionado en el host comprometido,

Categoría de amenaza	Actualización de contenido que proporciona estas firmas	Description (Descripción)
		la mayoría de las veces apuntando a un servidor web o marco. La comunicación posterior con el archivo de web shell con frecuencia permite que un actor malintencionado establezca un punto de apoyo en el sistema y realice la enumeración de servicios y redes, la exfiltración de datos y la ejecución remota de código en el contexto del usuario del servidor web. Los tipos de web shell más comunes son los scripts de marcado PHP, .NET y Perl. Los atacantes también pueden utilizar servidores web infectados con web shells (los servidores web pueden ser sistemas internos o conectados a Internet) para atacar otros sistemas internos.
spyware	Aplicaciones y amenazas	Detecta una comunicación C2 de salida. Estas firmas están autogeneradas o creadas manualmente por los investigadores de Palo Alto Networks. *Las firmas de spyware y autogen detectan la comunicación de C2 saliente; sin embargo, las firmas de autogen están basadas en la carga útil y pueden detectar exclusivamente comunicaciones de C2 con hosts de C2 que sean desconocidas o cambien con rapidez.*
Firmas de vulnerabilidad		
brute force	Aplicaciones y amenazas	Una firma brute-force detecta varias incidencias de una condición en un período de tiempo determinado. Mientras la actividad aislada podría ser benigna, la firma brute-force indica que la frecuencia y velocidad en la cual ocurre la actividad es sospechosa. Por ejemplo, un solo fallo de inicio de sesión en el FTP no indica una actividad maliciosa. Sin embargo, varios inicios de sesión en el FTP con errores en un breve período de tiempo probablemente indiquen que un atacante está probando combinaciones de contraseñas para acceder al servidor FTP. Puede ajustar la acción y las condiciones del activador para las firmas brute force.
code execution	Aplicaciones y amenazas	Detecta una vulnerabilidad de ejecución de código que un atacante puede aprovechar para ejecutar código

Categoría de amenaza	Actualización de contenido que proporciona estas firmas	Description (Descripción)
		en un sistema con los privilegios de un usuario con la sesión iniciada.
code-obfuscation	Aplicaciones y amenazas	Detecta código que se transformó para ocultar determinados datos y, al mismo tiempo, conserva su función. El código oculto es difícil o imposible de leer, por lo que no es evidente qué comandos ejecuta el código o con qué programa está diseñado para interactuar. Lo más común es que los actores maliciosos oculten código para disimular malware. Con menor frecuencia, algunos programadores legítimos podrían ocultar código para proteger la privacidad y la propiedad intelectual o para mejorar la experiencia del usuario. Por ejemplo, determinados tipos de ocultación (como la minificación) reducen el tamaño del archivo, lo que disminuye los tiempos de carga del sitio web y el uso del ancho de banda.
dos	Aplicaciones y amenazas	Detecta un ataque de denegación de servicio (denial-of-service, DoS), en el que un atacante intenta que un sistema objetivo no esté disponible, interrumpiendo temporalmente el sistema y los servicios y aplicaciones dependientes. Para llevar a cabo un ataque DoS, un atacante podría producir una inundación de tráfico en un sistema objetivo o enviar información que provoque fallos. Los ataques DoS despojan a los usuarios legítimos (como empleados, miembros y titulares de cuenta) del servicio o recursos al cual esperan acceder.
exploit-kit	Aplicaciones y amenazas	Detecta una página de destino del kit de exploits. Las páginas de destino del kit de exploits con frecuencia contienen varios exploits que apuntan a una o varias vulnerabilidades y exposiciones comunes (common vulnerabilities and exposures, CVE), para varios exploradores y complementos. Debido a que las CVE objetivo cambian con rapidez, las firmas exploit-kit se activan sobre la base de la página de destino del kit de exploits y no de las CVE. Cuando un usuario visita un sitio web con un kit de exploits, este analiza las CVE objetivo e intenta proporcionar de forma silenciosa una carga útil maliciosa al ordenador de la víctima.

Categoría de amenaza	Actualización de contenido que proporciona estas firmas	Description (Descripción)
info-leak	Aplicaciones y amenazas	Detecta una vulnerabilidad de software que un atacante podría aprovechar para robar información confidencial o de propiedad. Con frecuencia, podría existir un info-leak porque las comprobaciones integrales no existen para proteger los datos, y los atacantes pueden aprovechar las info-leaks enviando solicitudes manipuladas.
insecure-credentials (credenciales no seguras)	Aplicaciones y amenazas	Detecta el uso de contraseñas débiles, comprometidas y predeterminadas del fabricante para software, dispositivos de red y dispositivos de IoT.
Desbordamiento	Aplicaciones y amenazas	Detecta una vulnerabilidad de desbordamiento, en la que el atacante podría aprovechar la falta de comprobaciones apropiadas. Un ataque exitoso podría conllevar una ejecución remota de código con los privilegios de aplicación, servidor o sistema operativo.
phishing	Aplicaciones y amenazas	Detecta cuando un usuario intenta conectar a una página de destino del kit de phishing (generalmente después de recibir un correo electrónico con un enlace al sitio malicioso). Un sitio web de phishing engaña a los usuarios para enviar credenciales que un atacante puede robar para obtener acceso a la red. *Además de bloquear el acceso a las páginas de destino del kit de phishing, habilite la autenticación multifactor y la prevención de phishing de credenciales para evitar los ataques de phishing en todas las etapas.*
protocol-anomaly	Aplicaciones y amenazas	Detecta anomalías de protocolo, en las que el comportamiento de un protocolo se desvía del uso estándar y de cumplimiento. Por ejemplo, un paquete con formato incorrecto, una aplicación escrita de manera deficiente o una aplicación que se ejecuta en un puerto no estándar se considerarían anomalías y podrían usarse como herramientas de evasión. La acción recomendada es bloquear las anomalías de protocolo de cualquier gravedad.
sql-injection	Aplicaciones y amenazas	Detecta una técnica de hacking común en la que un atacante inserta consultas SQL en las solicitudes de una aplicación para leer o modificar una base de datos.

Categoría de amenaza	Actualización de contenido que proporciona estas firmas	Description (Descripción)
		Este tipo de técnica se usa con frecuencia en sitios web que no realizan limpiezas integrales de las entradas de usuario.

Prácticas recomendadas para proteger su red ante evasiones de capa 4 y capa 7

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia de Advanced Threat Prevention (para un mejor soporte de funciones) o Threat Prevention

Para supervisar y proteger su red de la mayoría de ataques de capa 4 y capa 7, aquí tiene un par de recomendaciones.

- ❑ Actualice a la última versión del software PAN-OS y la última versión de publicación de contenido para asegurarse de que tiene las últimas actualizaciones de seguridad. Consulte Instalación de las actualizaciones de contenido y software.
- ❑ Habilite DNS Security (requiere una licencia de Threat Prevention y suscripción a DNS Security) para capturar solicitudes de DNS maliciosas. Palo Alto Networks recomienda utilizar las siguientes opciones de configuración de la categoría de seguridad DNS en su perfil de antispyware:

SIGNATURE SOURCE	LOG SEVERITY	POLICY ACTION	PACKET CAPTURE
: Palo Alto Networks Content			
default-paloalto-dns		sinkhole	extended-capture
: DNS Security			
Command and Control Domains	default (high)	sinkhole	extended-capture
Dynamic DNS Hosted Domains	default (informational)	sinkhole	disable
Grayware Domains	default (low)	sinkhole	disable
Malware Domains	default (medium)	sinkhole	disable
Parked Domains	default (informational)	sinkhole	disable
Phishing Domains	default (low)	sinkhole	disable
Proxy Avoidance and Anonymizers	default (low)	sinkhole	disable
Newly Registered Domains	default (informational)	sinkhole	disable

  - Para la configuración de la gravedad de logs, utilice la configuración predeterminada:
  - Para la acción de política, configure todas las fuentes de firmas en **sinkhole**.
  - Para la captura de paquetes, configure Command and Control Domains (Dominios de comando y control) en **extended-capture** (captura ampliada). Deje todas las demás categorías en la configuración predeterminada.

  Para obtener más información sobre la configuración antispyware relacionada, consulte Perfil de antispyware recomendado para la puerta de enlace de Internet.
- ❑ Si tiene una suscripción activa a Advanced Threat Prevention, habilite Análisis en línea en la nube y Aprendizaje profundo local, si está disponible, para bloquear las amenazas avanzadas de C2 y spyware en tiempo real. La acción predeterminada para cada motor de análisis es **alerta**, que genera un log de amenazas cuando se detecta una amenaza correspondiente; sin embargo,

Palo Alto Networks recomienda establecer todas las acciones del modelo de análisis en **Reset-Both**. Esto elimina los paquetes coincidentes y envía un RST al cliente y al servidor, rompiendo la conexión, así como generando una entrada de log de amenazas.

- ❑ Configure el cortafuegos para que actúe como proxy DNS y habilite las firmas de evasión.

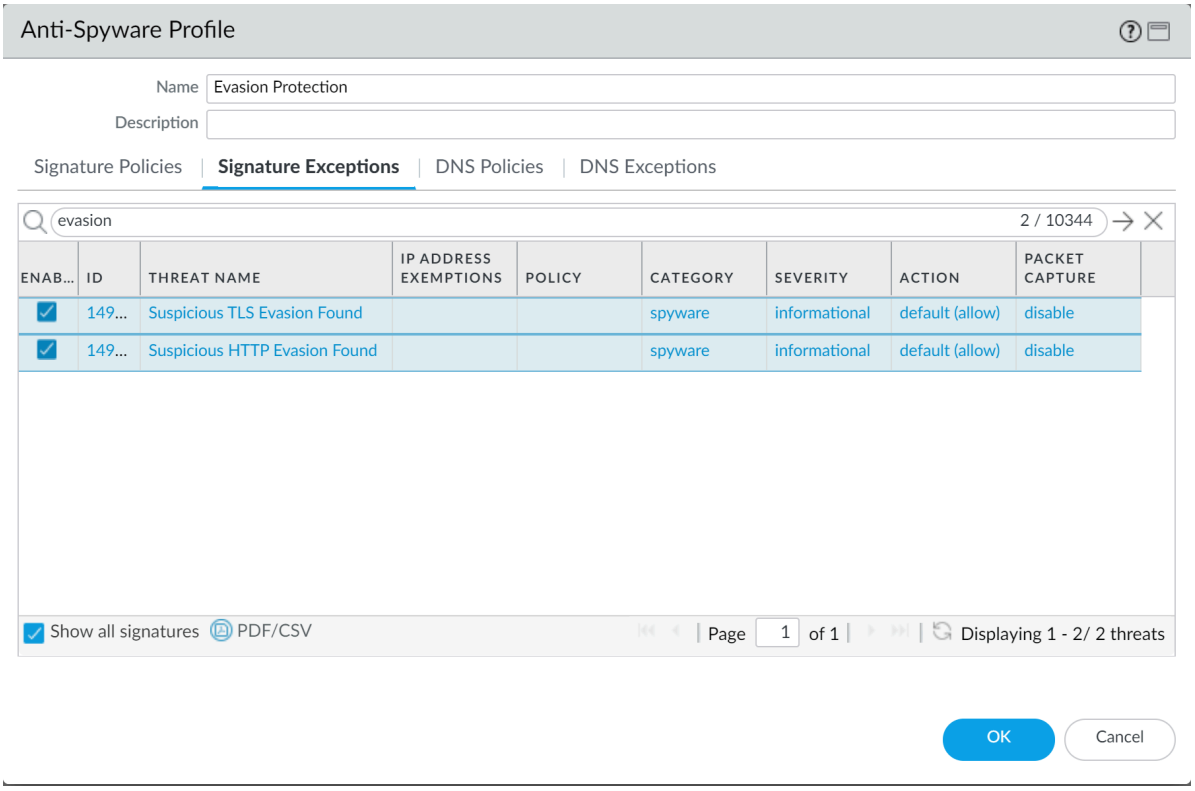
  El proxy DNS no forma parte del motor de políticas de seguridad del cortafuegos; en su lugar, indica al cortafuegos que resuelva los nombres de host DNS mientras mantiene la asignación de dominio a IP, algo que es fundamental para evitar la evasión de TLS/HTTP.

  - Configuración de un objeto proxy DNS.

    Cuando actúa como proxy DNS, el cortafuegos resuelve las solicitudes DNS y almacena en caché las asignaciones de nombre de host y direcciones IP para resolver de manera rápida y eficiente futuras consultas DNS.
  - Habilitación de las firmas de evasión

    Las firmas de evasión que detectan solicitudes HTTP o TLS elaboradas pueden enviar alertas cuando los clientes se conectan a un domino que no sea el dominio especificado en la solicitud DNS original. Asegúrese de configurar el proxy DNS antes de habilitar las firmas de evasión. Sin el proxy DNS, las firmas de evasión pueden activar alertas cuando un servidor DNS de la configuración de equilibrio de carga DNS devuelve direcciones IP diferentes (para

los servidores que alojan recursos idénticos) al cortafuegos y cliente en respuesta a la misma solicitud DNS.

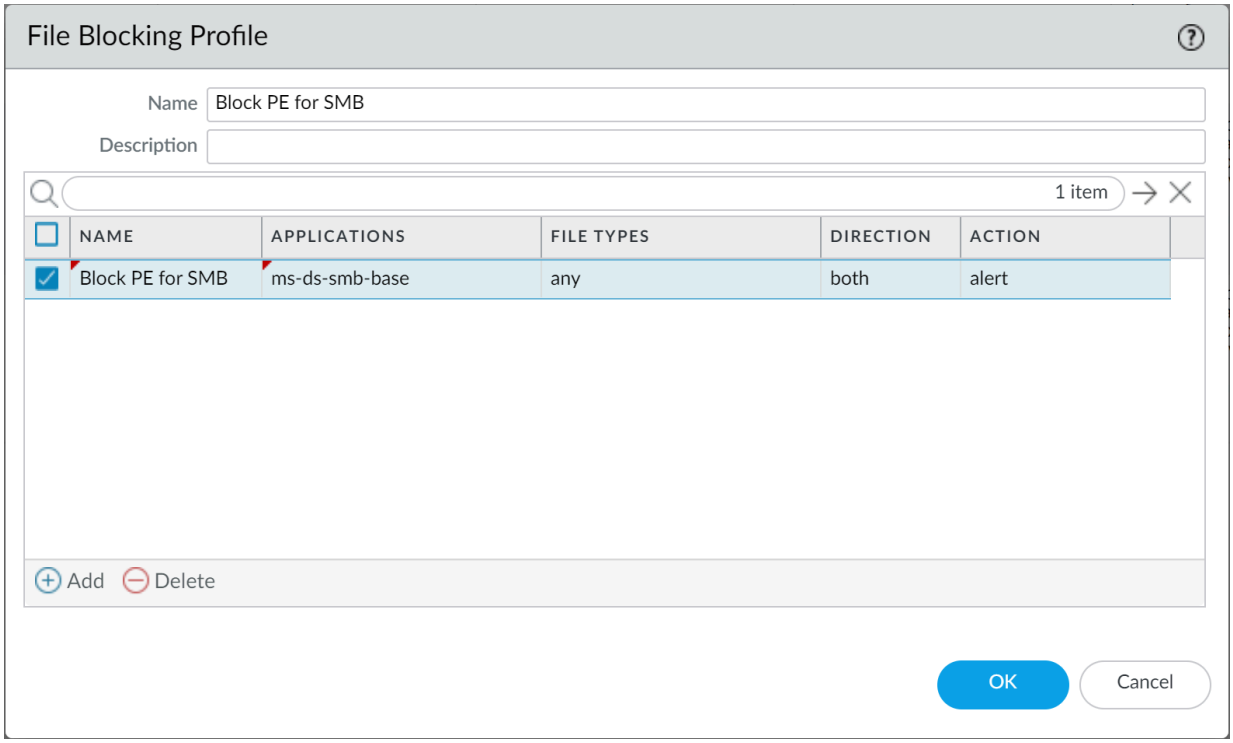


- Para implementaciones que operan Prisma Access o redes sin un servidor DNS interno, configure su política DNS para usar la dirección IP del sinkhole de Palo Alto Networks (72.5.65.111) en lugar del FQDN de sinkhole predeterminado (sinkhole.paloaltonetworks.com).

  El sinkhole DNS utilizado por el perfil antispyware permite al cortafuegos una respuesta a una consulta DNS para dominios que coinciden con la categoría configurada para una acción de sinkhole al servidor de sinkhole especificado, para ayudar a identificar hosts comprometidos. Cuando se utiliza el FQDN de sinkhole predeterminado, el cortafuegos envía el registro CNAME como respuesta al cliente, con la expectativa de que un servidor DNS interno resuelva el registro CNAME, lo que permite que las comunicaciones maliciosas del cliente al servidor de sinkhole configurado se registren y sean fácilmente identificables. Sin embargo, si los clientes están operando Prisma Access, están en redes sin un servidor DNS interno o utilizando otro software o herramientas que no se pueden resolver correctamente un CNAME en una respuesta de registro A, la solicitud de DNS se elimina, lo que genera detalles de log de tráfico incompletos que son cruciales para el análisis de amenazas.
- Para los servidores, cree reglas de política de seguridad que permitan solo las aplicaciones que usted apruebe en cada servidor. Verifique que el puerto estándar para la aplicación coincida

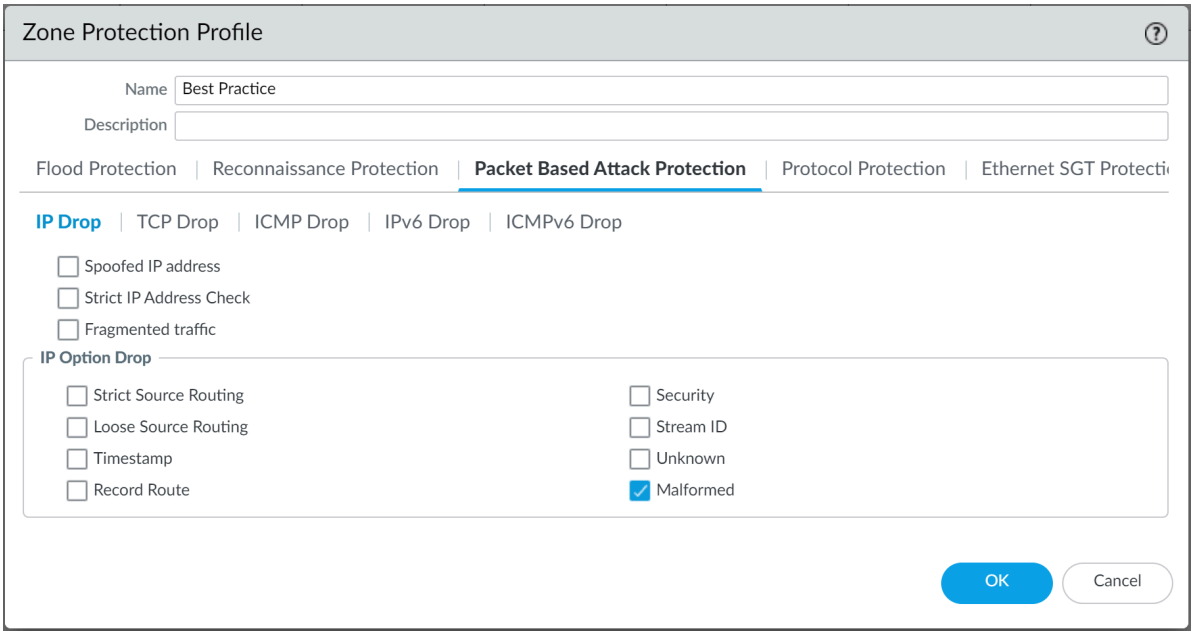
con el puerto de escucha del servidor. Por ejemplo, para garantizar que solo se permita el tráfico SMTP en su servidor de correo electrónico, configure la aplicación en **smtp** y configure el servicio en **application-default**. Si su servidor utiliza solo un subconjunto de los puertos estándar (por ejemplo, si su servidor SMTP utiliza solo el puerto 587 mientras la aplicación SMTP tiene puertos estándar definidos como 25 y 587), cree un nuevo servicio personalizado que incluya solo el puerto 587 y utilice ese nuevo servicio en su regla de política de seguridad en lugar de la opción predeterminada de la aplicación Además, asegúrese de restringir el acceso a zonas de origen y destino específicas, y a conjuntos específicos de direcciones IP.

- Bloquee todas las aplicaciones o tráfico desconocidos mediante la política de seguridad. Normalmente, las únicas aplicaciones clasificadas como tráfico desconocido son aplicaciones internas o personalizadas de su red, o posibles amenazas. El tráfico desconocido puede ser una aplicación no compatible, un protocolo anómalo o anormal, o una aplicación conocida que utiliza puertos no estándar. En cualquiera de estos casos debe bloquearse. Consulte Gestión de aplicaciones personalizadas o desconocidas.
- Configure un bloqueo de archivo para impedir que los tipos de archivo portables ejecutables (Portable Executable, PE) para el tráfico de bloque de mensajes del servidor (Server Message Block, SMB) pasen de zonas fiables a zonas no fiables (aplicaciones ms-ds-smb).



- Bloquee variantes maliciosas de PE (portables ejecutables), archivos ELF y MS Office, y scripts de PowerShell y shell en tiempo real. La habilitación de WildFire Inline ML le permite analizar archivos de forma dinámica mediante el aprendizaje automático en el cortafuegos. Esta capa adicional de protección antivirus complementa las firmas basadas en WildFire para proporcionar una cobertura ampliada para archivos cuyas firmas aún no existen.

- Cree un perfil de protección de zona configurado para ofrecer protección frente a los ataques basados en paquetes (**Network [Red]** > **Network Profiles [Perfiles de red]** > **Zone Protection [Protección de zona]**):
  - Seleccione la opción para descartar los paquetes IP **Malformed (Con formato incorrecto)** (**Packet Based Attack Protection [Protección contra ataque basado en paquetes]** > **IP Drop [Descarte de IP]**).



  - Habilite la opción de descarte **Mismatched overlapping TCP segment (Segmento TCP superpuesto no coincidente)** (**Packet Based Attack Protection [Protección contra ataque basado en paquetes]** > **TCP Drop [Descarte de IP]**).

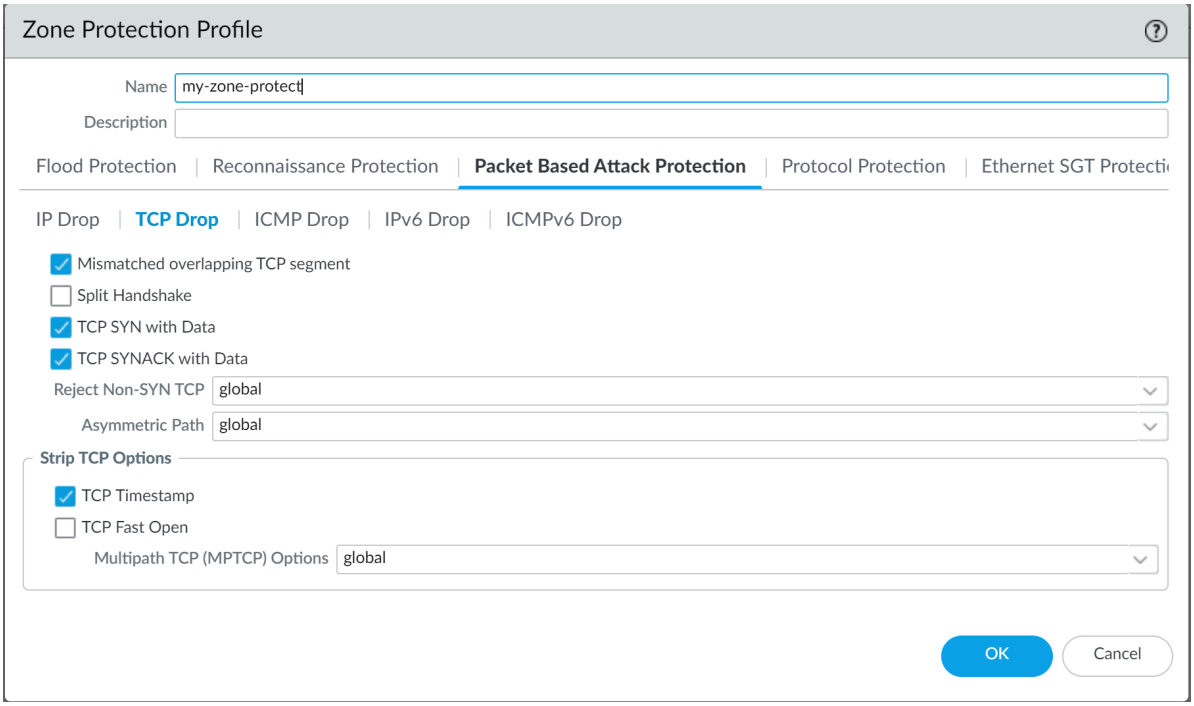
    Al establecer deliberadamente conexiones con datos superpuestos pero diferentes en ellas, los atacantes pueden intentar causar una interpretación equivocada de la intención de la conexión e inducir deliberadamente falsos positivos o falsos negativos. Los atacantes utilizan también la replicación de IP y la predicción de números de secuencia para interceptar la conexión de un usuario e introducir sus propios datos en la conexión. La selección de la opción **Mismatched overlapping TCP segment (Segmento TCP superpuesto no coincidente)** especifica que PAN-OS descarta las tramas con datos superpuestos y no coincidentes. Los segmentos recibidos son descartados cuando están dentro de otro segmento, cuando se superponen con parte de otro segmento o cuando contienen otro segmento completo.

- Habilite las opciones de descarte **TCP SYN with Data (TCP SYN con datos)** y **TCP SYNACK with Data (TCP SYNACK con datos)** (**Packet Based Attack Protection (Protección contra ataque basado en paquetes)** > **TCP Drop (Descarte de TCP)**).

  El descarte de paquetes SYN y SYN-ACK que contienen datos en la carga durante un protocolo de tres direcciones aumenta la seguridad al bloquear malware incluido en la carga y prevenir que extraiga datos no autorizados antes de que se complete el protocolo TCP.

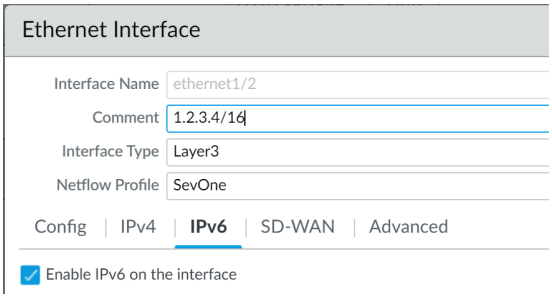
- Quite las marcas de tiempo TCP de los paquetes SYN antes de que el cortafuegos envíe el paquete (**Packet Based Attack Protection [Protección contra ataque basado en paquetes]** > **TCP Drop [Descarte de TCP]**).

  Cuando habilita la opción **Strip TCP Options - TCP Timestamp (Quitar opciones TCP - Marca de tiempo TCP)**, la pila TCP en ambos extremos de la conexión TCP no admitirá marcas de tiempo TCP. Esto evita los ataques que utilizan distintas marcas de tiempo en varios paquetes para el mismo número de secuencia.

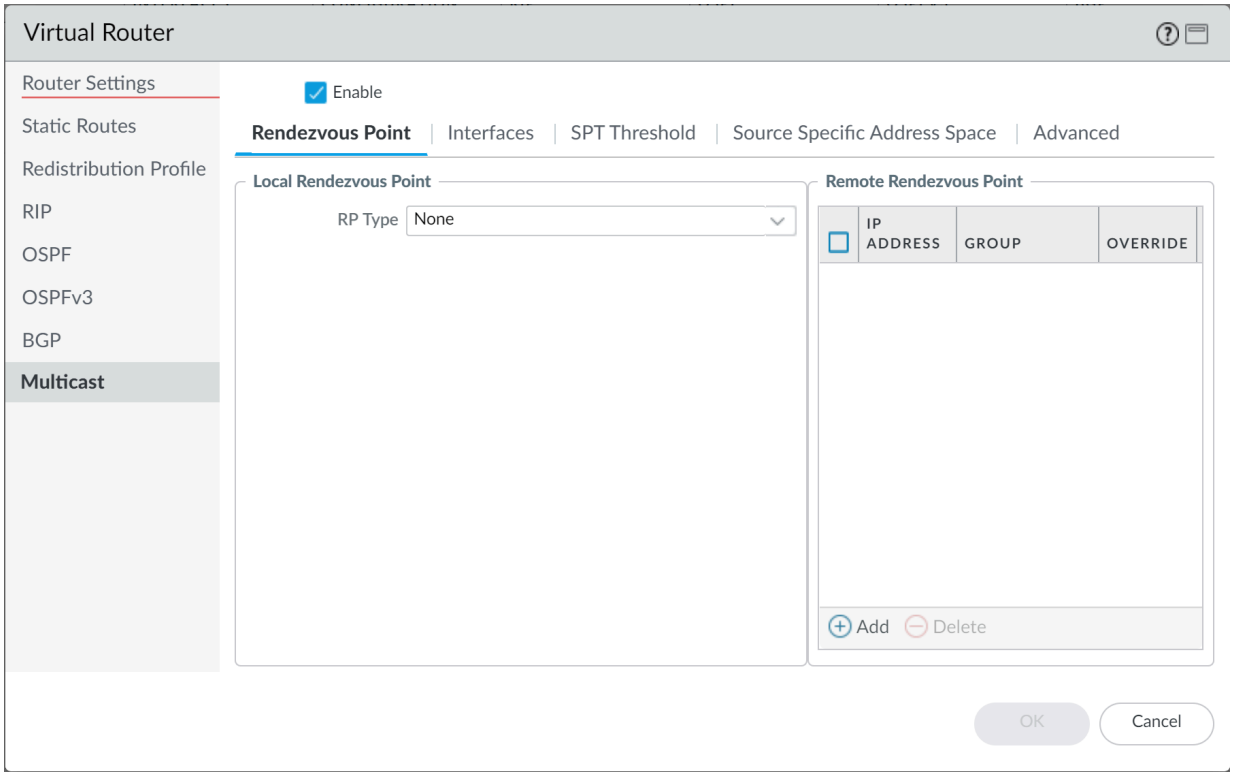


- Si configura direcciones IPv6 en sus hosts de red, asegúrese de habilitar el soporte para IPv6 si aún no está habilitado (**Network [Red]** > **Interfaces** > **Ethernet > IPv6**).

  La habilitación de la compatibilidad con IPv6 permite el acceso a hosts IPv6 y también filtra paquetes IPv6 encapsulados en paquetes IPv4, lo cual evita que las IPv6 en direcciones de multidifusión IPv4 se utilicen para el reconocimiento de la red.



- Habilite la compatibilidad con tráfico de multidifusión para que el cortafuegos pueda aplicar la política sobre tráfico de multidifusión (**Network [Red]** > **Virtual Router [Enrutador virtual]** > **Multicast [Multidifusión]**).



- Deshabilite las opciones **Forward datagrams exceeding UDP content inspection queue (Reenviar datagramas que superen la cola de inspección de contenido UDP)** y **Forward**

segments exceeding TCP content inspection queue (Reenviar segmentos que superen la cola de inspección de contenido TCP), disponibles en **Device (Dispositivo)** > **Setup (Configuración)** > **Content-ID (ID de contenido)** > **Content-ID Settings (Configuración de Content-ID)**.

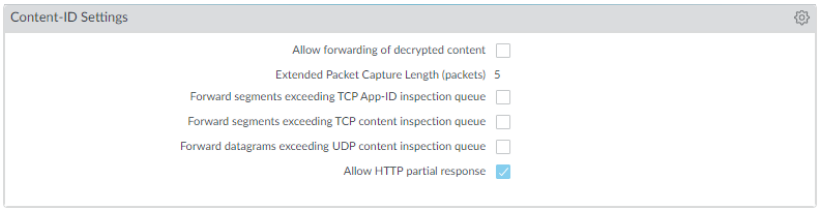
De manera predeterminada, cuando la cola de inspección de contenido TCP o UDP está llena, el cortafuegos omite la inspección en los segmentos TCP o los datagramas UDP que superen el límite de la cola de 64. Si deshabilita esta opción, garantiza la inspección del contenido de todos los datagramas TCP y UDP que permite el cortafuegos. Solo en circunstancias concretas (por ejemplo, si la plataforma del cortafuegos no tiene el tamaño apropiado para un caso de uso), afecta al rendimiento deshabilitar este ajuste.

- Deshabilite **Allow HTTP partial response (Habilitar respuesta parcial HTTP)** (**Device [Dispositivo]** > **Setup [Configurar]** > **Content-ID [ID de contenido]** > **Content-ID Settings [Configuración de ID de contenido]**).

  La opción de respuesta parcial HTTP permite a un cliente recuperar solo parte de un archivo. Cuando un cortafuegos de próxima generación en una transferencia identifica y omite un archivo malicioso, finaliza la sesión TCP con un paquete RST. Si el explorador web implementa la opción de intervalo de encabezado HTTP, puede comenzar una nueva sesión para recuperar solo la parte restante del archivo, lo cual evita que el cortafuegos active la misma firma nuevamente debido a la falta de contexto en la sesión inicial y, al mismo tiempo, permite que el explorador web vuelva a armar el archivo y envíe el contenido malintencionado. Al deshabilitar esta opción, evita que esto pase.

  La opción Allow HTTP partial response (Permitir respuesta parcial de HTTP) está habilitada de forma predeterminada en el cortafuegos. Esto proporciona la máxima disponibilidad, pero aumenta el riesgo de sufrir un ciberataque exitoso. Para obtener la máxima seguridad, deshabilite esta opción a fin de evitar que el navegador web inicie una nueva sesión para recuperar el resto de un archivo después de que el cortafuegos finalice la sesión original debido a una actividad maliciosa. Deshabilitar la respuesta parcial de HTTP afecta las transferencias de datos basadas en HTTP que usan el encabezado RANGE, lo que puede causar anomalías en el servicio para determinadas aplicaciones. Después de deshabilitar la respuesta parcial de HTTP, debe validar el funcionamiento de sus aplicaciones críticas para el negocio.

  Si experimenta una interrupción en la transferencia de datos HTTP en una aplicación crítica para el negocio, puede crear una política de cancelación de aplicaciones para ese caso específico. Debido a que la cancelación de aplicaciones ignora App-ID (incluida la inspección de contenidos y amenazas), solo debe crear esta política para determinadas aplicaciones críticas para el negocio. También debe especificar los orígenes y los destinos para limitar la regla (principio de acceso con privilegios mínimos). No cree una política de cancelación de aplicaciones a menos que sea necesario. Para obtener información sobre las políticas de cancelación de aplicaciones, consulte https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVLCA0.



- ❑ Cree un perfil de protección frente a vulnerabilidades que bloquee las anomalías del protocolo y todas las vulnerabilidades con gravedad baja y alta.

  Una anomalía de protocolo ocurre cuando el comportamiento de un protocolo se desvía del uso estándar y de cumplimiento. Por ejemplo, un paquete con formato incorrecto, una aplicación escrita de manera deficiente o una aplicación que se ejecuta en un puerto no estándar se considerarían anomalías y podrían usarse como herramientas de evasión.

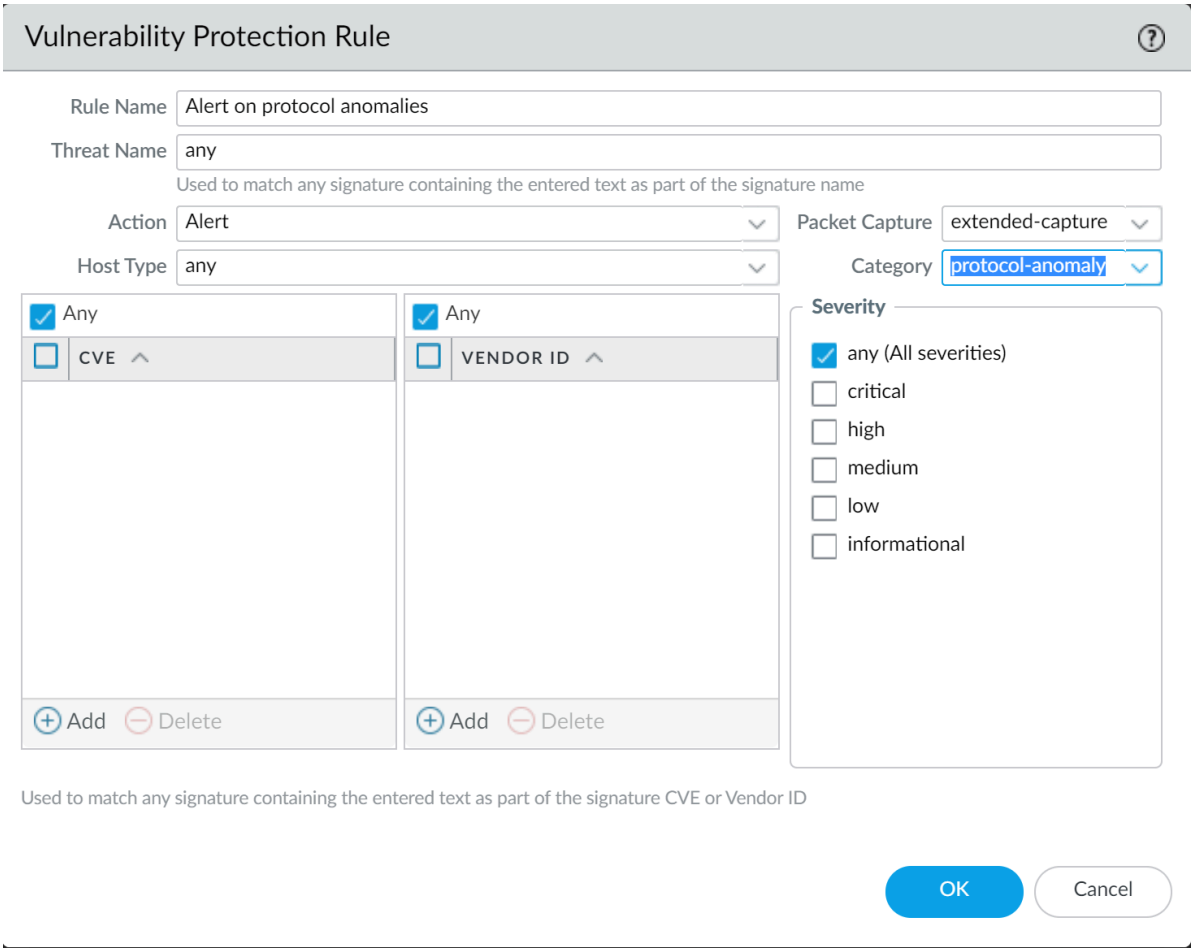
  Si su red es crítica; es decir, si la prioridad más alta de la empresa es la disponibilidad de la aplicación, debe comenzar por alertar sobre las anomalías del protocolo durante un periodo para garantizar que no haya aplicaciones internas críticas que utilicen protocolos establecidos de una manera no estándar. Si detecta que ciertas aplicaciones críticas activan firmas de anomalía de protocolo, puede excluir dichas aplicaciones del cumplimiento de anomalía de protocolo. Para esto, añada otra regla al perfil de protección de vulnerabilidades que permita las anomalías del protocolo y adjunte el perfil a la regla de política de seguridad que aplica el tráfico hacia y desde las aplicaciones críticas.

  Asegúrese de que las reglas del perfil de protección de vulnerabilidades y las reglas de la política de seguridad que permita las anomalías de protocolo para las aplicaciones internas críticas se indiquen por encima de las reglas que bloquean las anomalías de protocolo. El tráfico se evalúa en función de las reglas de política de seguridad y las reglas de los perfiles de protección de vulnerabilidades desde arriba hacia abajo, y se aplica en función de la primera regla de coincidencia.

  - Comience por alertas sobre las anomalías de protocolo:

    Cree una regla de perfil de protección de vulnerabilidades con la opción **Action (Acción)** configurada en Alert (Alerta), la opción **Category (Categoría)** configurada en protocol-anomaly (protocolo-anomalía) y la opción **Severity (Gravedad)** configurada en Any (Cualquiera). Supervise el tráfico para determinar si alguna aplicación interna crítica utiliza protocolos establecidos de maneras no estándar. Si detecta que esto es así, continúe

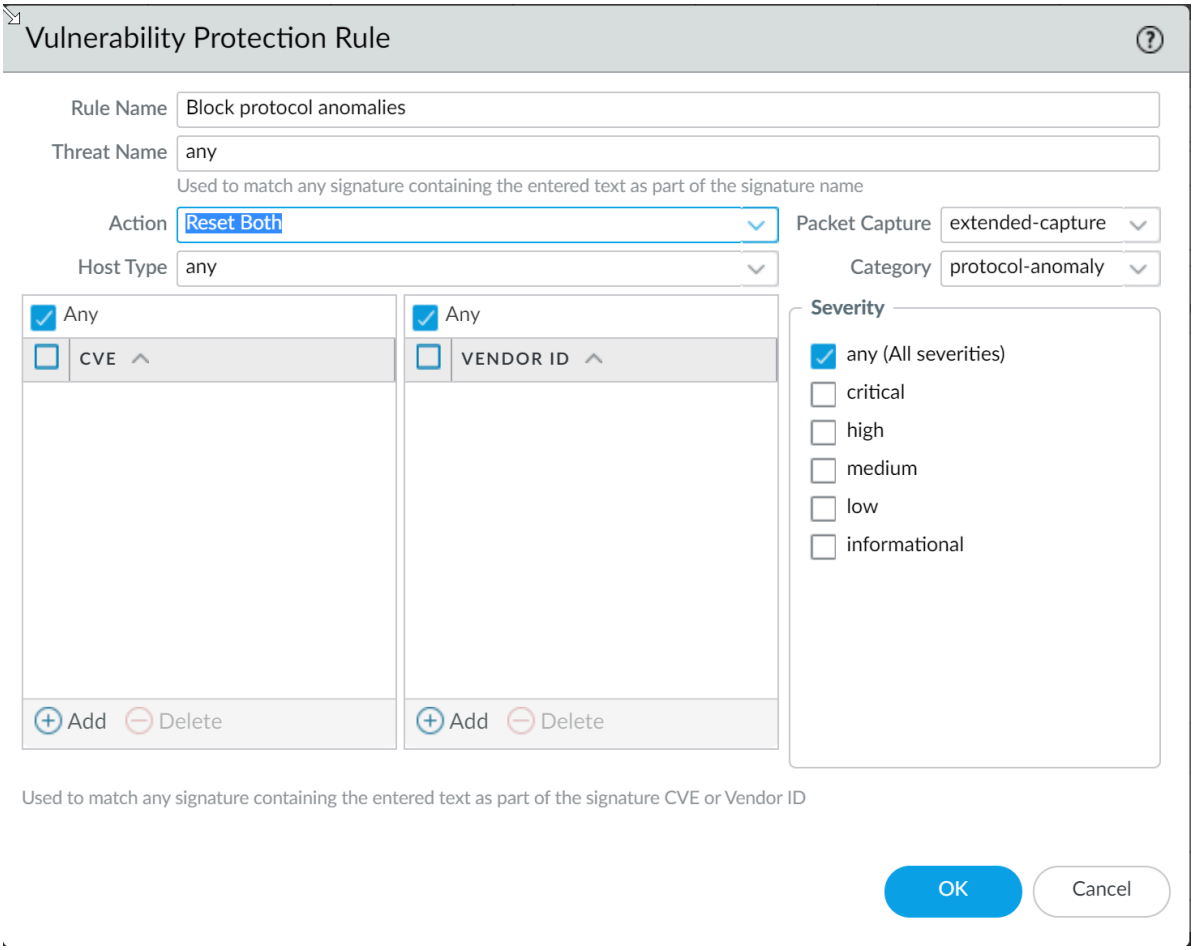
permitiendo las anomalías de protocolo para dichas aplicaciones y luego bloquee las anomalías de protocolo para las demás aplicaciones.



- Bloquee las anomalías de protocolo:

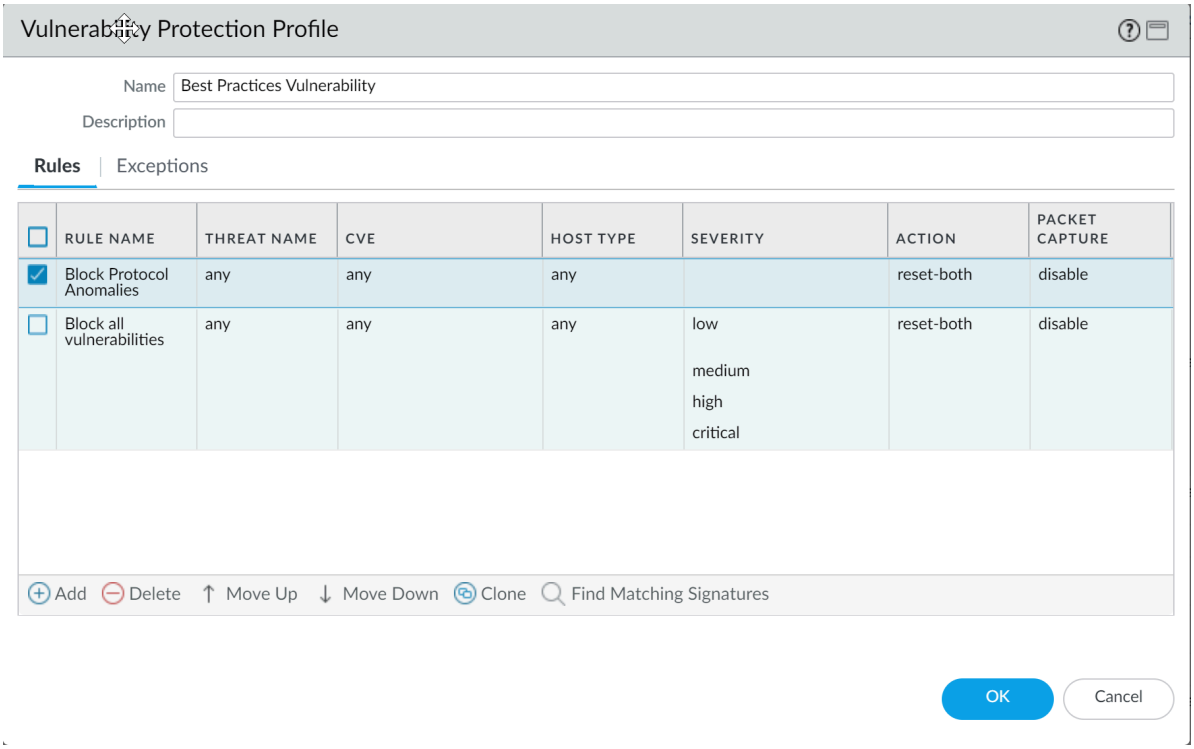
  Cree una regla de perfil de protección de vulnerabilidades con la opción **Category (Categoría)** configurada en protocol-anomaly (protocolo-anomalía), la regla **Action (Acción)**

configurada en Reset Both (Restablecer ambos) y la opción **Severity (Gravedad)** configurada en Any (Cualquiera).



- Opcionalmente, permita las anomalías de protocolo para las aplicaciones críticas que utilizan protocolos establecidos de una manera no estándar. Para ello, cree una regla de perfil de protección de vulnerabilidades que permita anomalías de protocolo: configure la regla **Action (Acción)** en Allow (Permitir), la opción **Category (Categoría)** en protocol-anomaly (protocolo-anomalía) y la opción **Severity (Gravedad)** en any (cualquiera). Adjunte la regla de perfil de protección de vulnerabilidad a la regla de política de seguridad que aplique el tráfico hacia y desde las aplicaciones críticas.

- Añada otra regla al perfil de protección contra vulnerabilidades para bloquear todas las vulnerabilidades con gravedad baja y alta. Esta regla debe indicarse después de la regla que bloquea las anomalías de protocolo.



- Continúe adjuntando los siguientes perfiles de seguridad a sus reglas de políticas de seguridad para proporcionar una protección basada en firmas:
  - Cree un perfil antyspyware para bloquear todo el spyware con gravedad baja y alta.
  - Cree un perfil de antivirus para bloquear todo el contenido que coincida con una firma de antivirus.

Uso compartido de inteligencia de amenazas con Palo Alto Networks

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia de Advanced Threat Prevention (para un mejor soporte de funciones) o Threat Prevention

La telemetría es el proceso de recolección y transmisión de datos para su análisis. Cuando habilita la telemetría en el cortafuegos, el cortafuegos recopila y envía periódicamente información sobre aplicaciones, amenazas y el estado del dispositivo a Palo Alto Networks. El uso compartido de la inteligencia de amenazas ofrece los siguientes beneficios:

- Mejor vulnerabilidad y firmas de spyware para usted y otros clientes del mundo. Por ejemplo, cuando un evento de amenaza desencadena firmas de vulnerabilidad o spyware, el cortafuegos comparte las URL asociadas a la amenaza con el equipo de investigación de amenazas de Palo Alto Networks para que puedan clasificar adecuadamente las URL como maliciosas.
- Pruebas y evaluaciones rápidas de las firmas de amenazas experimentales sin impacto en su red, de modo que se pueden suministrar firmas de prevención de amenazas críticas a todos los clientes de Palo Alto Networks con mayor rapidez.
- Mejora la precisión y la capacidad para detectar malware dentro del filtrado de URL de PAN-DB, las firmas de comando y control (C2) basadas en DNS y WildFire.

Palo Alto Networks utiliza la inteligencia de amenazas que se extrae de la telemetría para proporcionarle estos beneficios a usted y a otros usuarios de Palo Alto Networks. Todos los usuarios de Palo Alto Networks se benefician con el uso compartido de los datos de telemetría de cada usuario, lo que convierte a la telemetría en un enfoque impulsado por una comunidad para la prevención de amenazas. Palo Alto Networks no comparte sus datos de telemetría con otros clientes u organizaciones externas.

Para leer más sobre la telemetría, incluidos sus beneficios, usos y configuración, consulte Telemetría del dispositivo.

Recursos de Advanced Threat Prevention

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia de Advanced Threat Prevention (para un mejor soporte de funciones) o Threat Prevention

Para obtener más información sobre las prácticas recomendadas de prevención de amenazas, consulte las siguientes fuentes:

- Creación de firmas de amenazas personalizadas
- Prácticas recomendadas para proteger su red ante evasiones de capa 4 y capa 7
- Prácticas recomendadas de filtrado de URL
- Prácticas recomendadas para Zero Trust
- Prácticas recomendadas de protección DoS y de zonas

Para ver una lista de las amenazas y aplicaciones que los productos de Palo Alto Networks pueden identificar, utilice los siguientes enlaces:

- Applipedia: ofrece información sobre las aplicaciones que Palo Alto Networks puede identificar.
- Threat Vault: enumera todas las amenazas que pueden identificar los productos de Palo Alto Networks. Puede buscar por Vulnerabilidad, Spyware o Virus. Haga clic en el icono de detalles junto al número de ID para obtener más información acerca de una amenaza.

Configuración de Threat Prevention

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia de Advanced Threat Prevention (para un mejor soporte de funciones) o Threat Prevention

Para poder habilitar y configurar el análisis en línea en la nube, debe obtener e instalar Threat Prevention o Advanced Threat Prevention (para acceder a las características basadas en la nube del análisis en línea en la nube) además de las licencias de plataforma desde las que se opera. Las licencias se activan desde el Portal de atención al cliente de Palo Alto Networks y deben estar activas para poder habilitar cualquiera de las características de prevención de amenazas. Además, Threat Prevention (similar a otros servicios de seguridad de Palo Alto Networks) se gestiona a través de perfiles de seguridad, que a su vez dependen de la configuración de las políticas de aplicación de red definidas a través de las reglas de las políticas de seguridad. Antes de habilitar Threat Prevention, se recomienda familiarizarse con los componentes principales de la plataforma de seguridad en la que están habilitadas las suscripciones de seguridad. Consulte su documentación del producto para obtener más información.

Para habilitar y configurar la suscripción a Threat Prevention para que funcione de forma óptima en la implementación de seguridad de red, consulte las tareas a continuación. Si bien puede no ser necesario implementar todos los procesos que se muestran aquí, Palo Alto Networks recomienda revisar todas las tareas para familiarizarse con las opciones disponibles para una implementación correcta. Además, se recomienda que siga las prácticas recomendadas proporcionadas por Palo Alto Networks para una óptima usabilidad y seguridad.

Configuración de antivirus, antispyware y protección frente a vulnerabilidades

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia de Advanced Threat Prevention (para un mejor soporte de funciones) o Threat Prevention

Todos los cortafuegos de próxima generación de Palo Alto Networks incluyen perfiles predefinidos de antivirus, antispyware y protección de vulnerabilidades que puede incluir en las reglas de políticas de seguridad. Incluye un perfil de antivirus predefinido, **predeterminado**, que usa la acción predeterminada para cada protocolo (bloquear tráfico HTTP, FTP y SMB y alerta de tráfico SMTP, IMAP y POP3). Hay dos perfiles predefinidos de antispyware y protección contra vulnerabilidades:

- **default (predeterminado)**: aplica la acción predeterminada a todo el spyware y eventos de protección de vulnerabilidades de gravedad crítica, alta y media de cliente y servidor. No detecta los niveles bajo e informativo.
- **estricto**: Aplica la respuesta de bloqueo a todo el spyware y eventos de protección de vulnerabilidades de gravedad crítica, alta y media de cliente y servidor y usa la acción predeterminada para los eventos bajos e informativos.

Para garantizar que el tráfico que entra en su red está libre de amenazas, incluya los perfiles predefinidos en sus políticas básicas de acceso web. Al supervisar el tráfico en su red y ampliar su base de reglas de políticas, puede diseñar perfiles más granulares para hacer frente a sus necesidades de seguridad específicas.

Use el siguiente flujo de trabajo para configurar los perfiles de seguridad de antivirus, antispyware y protección de vulnerabilidades.

- Strata Cloud Manager
- PAN-OS y Panorama

Configuración de antivirus, antispyware y protección frente a vulnerabilidades (Cloud Management)

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

La suscripción de Threat Prevention reúne en una licencia las funciones de antivirus, antispyware y protección frente a vulnerabilidades, y forma parte de la suscripción de Prisma Access. Para obtener información sobre las aplicaciones y los servicios ofrecidos con Prisma Access, consulte Todas las aplicaciones y servicios disponibles. Para verificar las suscripciones para las que tiene licencias activas actualmente, Compruebe lo que es compatible con su licencia.

STEP 2 | (Opcional) Cree perfiles de seguridad personalizados para antivirus, antispyware y protección de vulnerabilidades.

De forma alternativa, puede utilizar los perfiles de prácticas recomendadas predefinidas.

Para apostar por una estrategia de seguridad óptima, realice una transición segura a los perfiles de seguridad recomendados.

- Para crear Perfiles de WildFire y antivirus personalizados, seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and (NGFW y) Prisma Access** > **Security Services (Servicios de seguridad)** > **WildFire and Antivirus (WildFire y antivirus)** y **Add Profile (Añadir perfil)**. Siga los pasos para realizar la transición al perfil de antivirus adecuado para alcanzar su objetivo sin problemas.
- Para crear Perfiles antispyware personalizados, seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and (NGFW y) Prisma Access** > **Security Services (Servicios de seguridad)** > **Anti-spyware (Antispyware)** y **Add Profile (Añadir perfil)**. Siga los pasos para realizar la transición al perfil de antispyware adecuado para alcanzar su objetivo sin problemas.
- Para crear Perfiles de protección frente a vulnerabilidades personalizados, seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and (NGFW y) Prisma Access** > **Security Services (Servicios de seguridad)** > **Vulnerability Protection (Protección frente a vulnerabilidades)** y **Add Profile (Añadir perfil)**. Siga los pasos para realizar la transición al perfil de protección frente a vulnerabilidades adecuado para alcanzar su objetivo sin problemas.

STEP 3 | Adjunte perfiles de seguridad a sus **Security Policy Rules (Reglas de políticas de seguridad)**. Prisma Access aplica las reglas de la política de seguridad de prácticas recomendadas de forma predeterminada.

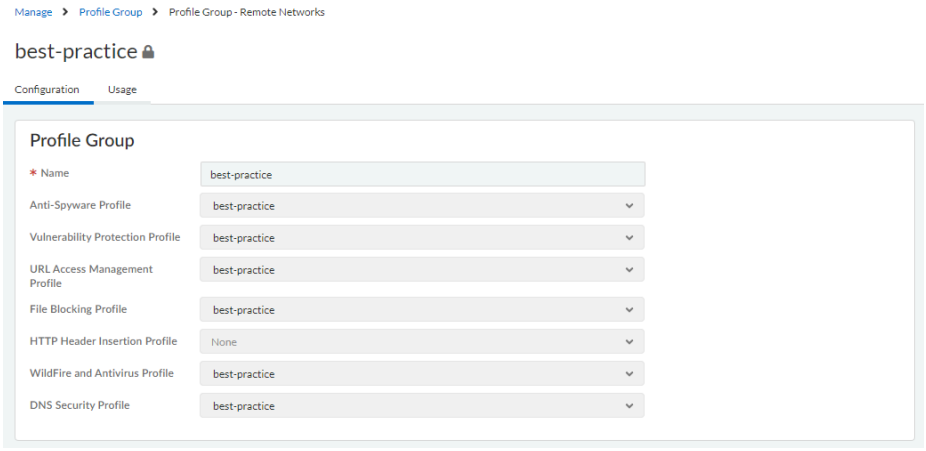
Cuando configura una regla de política de la seguridad que utiliza un perfil de protección de vulnerabilidades para bloquear conexiones cuando se detectan exploits o intentos de obtener acceso no autorizado, Prisma Access bloquea automáticamente ese tráfico y registra esos incidentes (consulte Supervisar direcciones IP bloqueadas).

1. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and (NGFW y) Prisma Access** > **Security Services (Servicios de seguridad)** > **Security Policy (Política de seguridad)** y seleccione la regla que desea modificar o la opción **Add Rule (Añadir regla)**.
2. En **Action and Advanced Inspection (Acción e inspección avanzada)**, seleccione el **Profile Group (Grupo de perfiles)** que incluya los siguientes perfiles de seguridad:

WildFire and Antivirus (WildFire y antivirus), **Anti-Spyware (Antispyware)** y **Vulnerability Protection (Protección frente a vulnerabilidades)**.

*Puede crear nuevos grupos de perfiles en **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and (NGFW y) Prisma Access** > **Security Services (Servicios de seguridad)** > **Profile Groups (Grupos de perfiles)**. Para obtener más información, consulte* Enable a Security Profile (Habilitar un perfil de seguridad).

*De forma predeterminada, el grupo de perfiles de **prácticas recomendadas** se habilita con la configuración de prácticas recomendadas para todos los perfiles de seguridad disponibles.*



STEP 4 | Confirme los cambios.

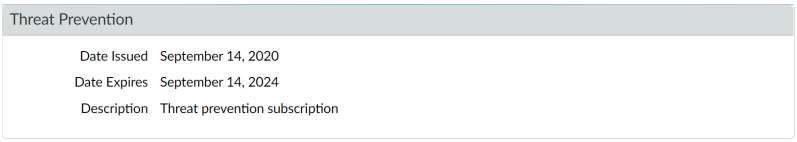
Configuración de antivirus, antispyware y protección frente a vulnerabilidades (NGFW (Managed by PAN-OS or Panorama))

*Palo Alto Networks define una acción predeterminada para todas las firmas antispyware y de protección de vulnerabilidades. Para ver la acción predeterminada, seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Anti-Spyware (Antispyware)** u **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Vulnerability Protection (Protección de vulnerabilidades)** y luego seleccione un perfil. Haga clic en la pestaña Exceptions (Excepciones) y después en Show all signatures (Mostrar todas las firmas) para ver la lista de todas las firmas y la **Action (Acción)** predeterminada correspondiente. Para cambiar la acción predeterminada, debe crear un nuevo perfil y, a continuación, especificar una **Action (Acción)** y/o añadir excepciones de firma individuales a las **Exceptions (Excepciones)** en el perfil.*

STEP 1 | Compruebe que tiene una suscripción de prevención de amenazas.

La suscripción de prevención de amenazas reúne en una licencia las funciones de antivirus, antispyware y protección contra vulnerabilidades. Para comprobar si posee una suscripción activa de prevención de amenazas, seleccione **Device (Dispositivo)** > **Licenses (Licencias)**

y verifique que la fecha de caducidad de **Threat Prevention (Prevención de amenazas)** sea futura.



STEP 2 | Descargue la última actualización de contenido.

1. Seleccione **Device (Dispositivo)** > **Dynamic Updates (Actualizaciones dinámicas)** y haga clic en **Check Now (Comprobar ahora)** en la parte inferior de la página para recuperar las firmas más recientes.
2. En la columna **Actions (Acciones)**, haga clic en **Download (Descargar)** e instale las actualizaciones de antivirus más recientes y luego descargue y seleccione **Install (Instalar)** para instalar las actualizaciones más recientes de aplicaciones y protección contra amenazas.

STEP 3 | Programe actualizaciones de contenido.

Lea Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas *para obtener información importante sobre la implementación de actualizaciones.*

1. Seleccione **Device (Dispositivo)** > **Dynamic Updates (Actualizaciones dinámicas)** y luego haga clic en **Schedule (Programar)** para recuperar automáticamente las actualizaciones de firmas de **antivirus** y **aplicaciones y amenazas**.
2. Especifique la frecuencia y momento de las actualizaciones:
   - **download-only (solo descarga)**: el cortafuegos descarga automáticamente las actualizaciones más recientes según el cronograma que usted defina, pero debe **instalarlas** manualmente.
   - **download-and-install (descargar e instalar)**: el cortafuegos descarga e instala automáticamente las actualizaciones según el cronograma que usted defina.
3. Haga clic en **OK (Aceptar)** para guardar el cronograma actualizado, no se necesita confirmar.
4. (Opcional) Defina un **Threshold (Umbral)** para indicar una cantidad mínima de horas transcurridas desde que una actualización está disponible para que el cortafuegos la descargue. Por ejemplo, configurar el **Threshold (Umbral)** en **10** significa que el cortafuegos no descargará una actualización hasta que tenga al menos 10 horas, independientemente del cronograma.
5. (HA únicamente) Decida si elegirá la opción **Sync To Peer (Sincronizar con el peer)**, que permite que el peer sincronice las actualizaciones de contenido después de descargar e instalar (el cronograma de actualización no sincroniza entre los peers; usted debe configurar manualmente el cronograma en ambos peers).

   Existen consideraciones adicionales para decidir si usará la opción **Sync To Peer (Sincronizar con el peer)** y cómo, según su implementación HA:

   - **HA activo/pasivo**: si los cortafuegos utilizan el puerto MGT para las actualizaciones de contenido, programe ambos cortafuegos para que descarguen e instalen las

actualizaciones de forma independiente. Sin embargo, si los cortafuegos utilizan un puerto de datos para las actualizaciones de contenido, el cortafuegos pasivo no descargará ni instalará actualizaciones, a menos y hasta que esté activo. Para mantener los cronogramas sincronizados en ambos cortafuegos al usar un puerto de datos para las actualizaciones, programa actualizaciones en ambos cortafuegos y luego habilite **Sync To Peer (Sincronizar con el peer)** para que, sea cual fuera el cortafuegos activo, este descargue e instale las actualizaciones, y también las envíe al cortafuegos pasivo.

- **HA activo/activo**: si los cortafuegos utilizan la interfaz MGT para las actualizaciones de contenido, seleccione **download-and-install (descargar a instalar)** en ambos cortafuegos, pero no habilite **Sync To Peer (Sincronizar con el peer)**. Sin embargo, si los cortafuegos usan un puerto de datos, seleccione **download-and-install (descargar e instalar)** en ambos cortafuegos y habilite **Sync To Peer (Sincronizar con el peer)** para que si un cortafuegos asume un estado activo-secundario, el cortafugos activo-primario descargue e instale las actualizaciones y las envíe al cortafuegos activo-secundario.

STEP 4 | (Opcional) Cree perfiles de seguridad personalizados para antivirus, antispyware y protección de vulnerabilidades.

O bien, puede usar los perfiles estricto o predeterminado predefinido.

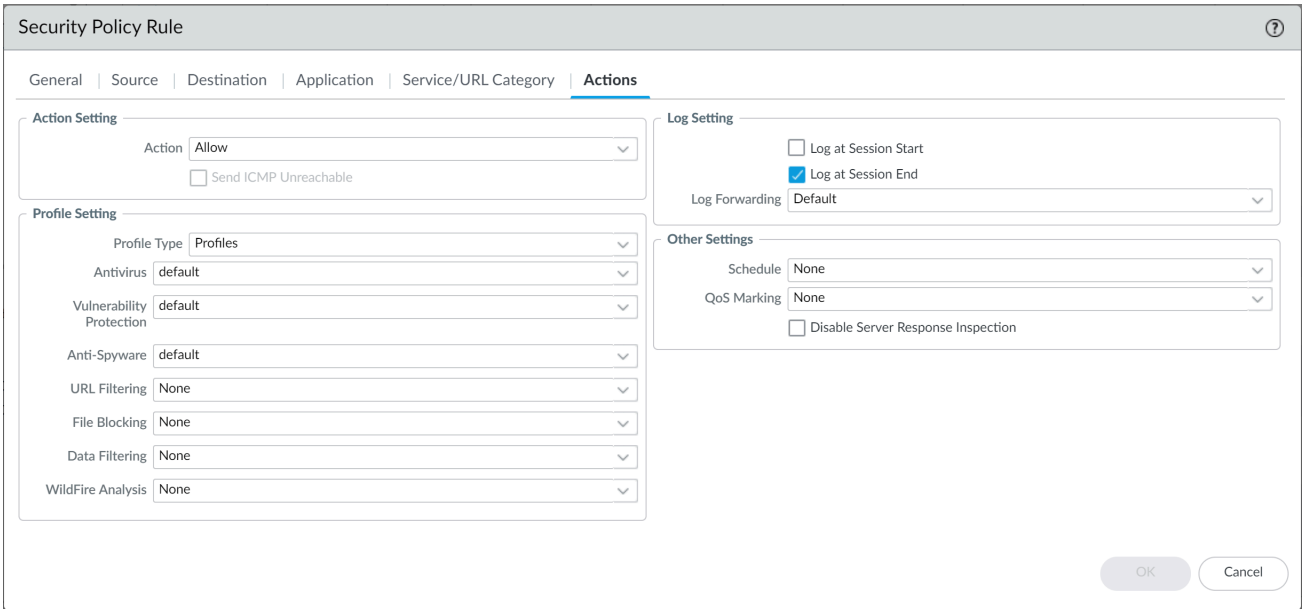
Para apostar por una estrategia de seguridad óptima, realice una transición segura a los perfiles de seguridad recomendados.

- Para crear perfiles antivirus personalizados, seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Antivirus** y **Add (Añadir)** un nuevo perfil. Siga los pasos para realizar la transición al perfil de antivirus adecuado para alcanzar su objetivo sin problemas.
- Para crear Perfiles antispyware personalizados, seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Anti-Spyware (Antispyware)** y **Add (Añadir)** un nuevo perfil. Siga los pasos para realizar la transición al perifil de antispyware adecuado para alcanzar su objetivo sin problemas.
- Para crear Perfiles de protección de vulnerabilidades personalizados, seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Vulnerability Protection (Protección frente a vulnerabilidades)** y **Add (Añadir)** un nuevo perfil. Siga los pasos para realizar la transición al perifil de protección frente a vulnerabilidades adecuado para alcanzar su objetivo sin problemas.

STEP 5 | Adjunte perfiles de seguridad a sus reglas de política de seguridad.

Cuando configura el cortafuegos con una regla de política de seguridad que utiliza un perfil de protección de vulnerabilidades para bloquear las conexiones, el cortafuegos automáticamente bloquea el tráfico en el hardware (consulte Supervisión de direcciones IP bloqueadas).

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y seleccione la regla que desea modificar.
2. En la pestaña **Actions (Acciones)**, seleccione **Profiles (Perfiles)** como el **Profile Type (Tipo de perfil)**.
3. Seleccione los perfiles de seguridad que creó para **Antivirus**, **Anti-Spyware** y **Vulnerability Protection (Protección de vulnerabilidades)**.



STEP 6 | Confirme los cambios.

Haga clic en **Commit (Confirmar)**.

Configuración del análisis en línea en la nube

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced Threat Prevention (para un mayor soporte de funciones)

El análisis en línea en la nube es una función de Advanced Threat Prevention que permite la detección de amenazas avanzadas de comando y control (C2) de día cero y vulnerabilidades de inyección de comandos e inyección SQL en tiempo real consultando el servicio en la nube de Advanced Threat Prevention. La protección de análisis en línea en la nube se ofrece a través de sus perfiles de seguridad antispyware y protección de vulnerabilidades, con amenazas avanzadas de C2 (comando y control) y spyware gestionadas por el primero y vulnerabilidades de inyección de comandos e inyección de SQL por el segundo.

Los cortafuegos compatibles con PAN-OS 11.2 y posteriores implementaciones también pueden acceder al Aprendizaje profundo local para Advanced Threat Prevention. El aprendizaje profundo local, Local Deep Learning, complementa el componente basado en nube del análisis en línea en la nube de Advanced Threat Prevention al proporcionar un mecanismo para realizar análisis rápidos y locales basados en el aprendizaje profundo de amenazas de día cero y otras amenazas evasivas. Las actualizaciones de los modelos locales de aprendizaje profundo se entregan a través de actualizaciones de contenido. Debido a los recursos adicionales del sistema necesarios para ejecutar módulos de detección de aprendizaje profundo locales, el aprendizaje profundo local solo está disponible en las siguientes plataformas:

- Serie PA-5400, excepto el dispositivo PA-5450.
- VM-Series (debe asignar al menos 16 GB de memoria total)
- VM-Series en nube pública
- VM-Series en nube privada

Para habilitar y configurar el análisis en línea en la nube y el aprendizaje profundo local, debe activar su licencia de Advanced Threat Prevention y crear (o modificar) el perfil de seguridad antispyware y de protección frente a vulnerabilidades. A continuación, configure los ajustes de la política para cada motor de análisis de categorías y luego adjunte los perfiles a una regla de la política de seguridad.

Para obtener más información sobre la creación de reglas de políticas de seguridad, consulte el capítulo de Políticas de la Guía del administrador de PAN-OS®.

- Strata Cloud Manager
- PAN-OS y Panorama

Configuración del análisis en línea en la nube (PAN-OS y Panorama)

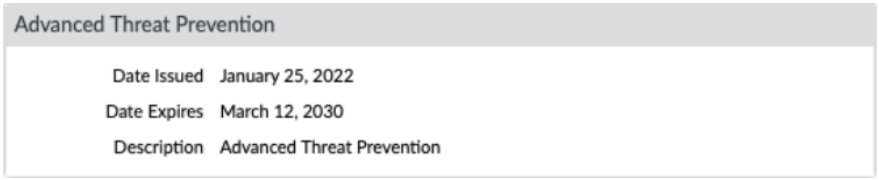
El análisis en línea en la nube de Advanced Threat Prevention admite varios motores de detección, que requieren diferentes versiones mínimas de PAN-OS para habilitar:

- *La detección de amenazas avanzadas C2 (comando y control) y spyware requiere PAN-OS 10.2 y versiones posteriores.*
- *La detección de amenazas de exploits de día cero requiere PAN-OS 11.0 y versiones posteriores.*
- *La compatibilidad con LDL (aprendizaje profundo local) requiere PAN-OS 11.2 y versiones posteriores.*

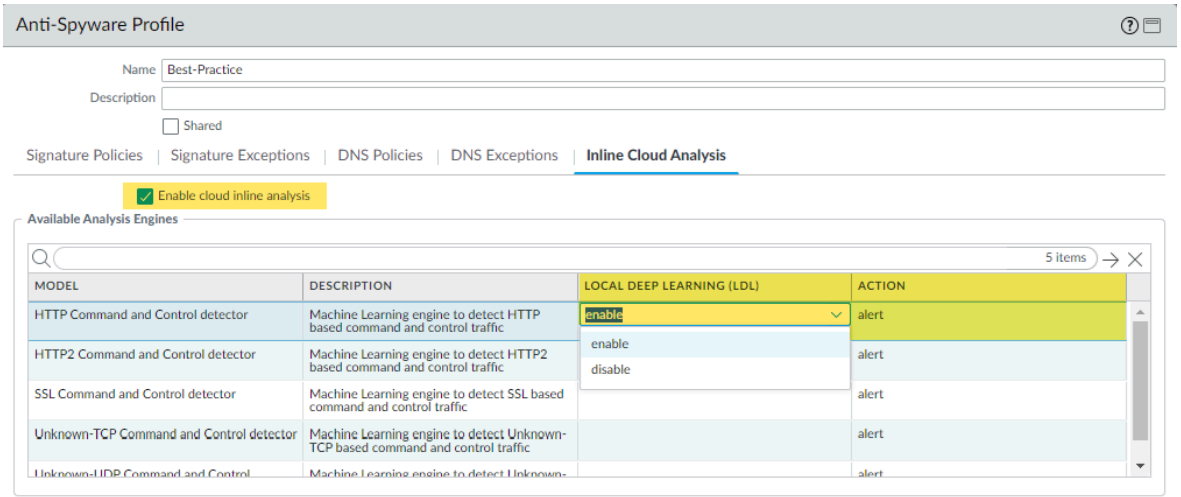
STEP 1 | Inicie sesión en la interfaz web de PAN-OS.

STEP 2 | Para aprovechar el análisis en línea de la nube, debe tener una suscripción activa a Advanced Threat Prevention.

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



STEP 3 | Actualice o cree un nuevo perfil de seguridad antispyware para habilitar el análisis en línea en la nube (para analizar el tráfico en busca de amenazas avanzadas de C2 (comando y control) y spyware en tiempo real).



1. Seleccione un **perfil antispyware existente** o **añada** uno nuevo (**Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Anti-Spyware**).
2. Seleccione su perfil antispyware y, a continuación, vaya a **Inline Cloud Analysis (Análisis en línea de la nube)** y **habilítelo**.
3. (Aprendizaje profundo local [compatible con PAN-OS 11.2 y versiones posteriores]) Seleccione **enable (habilitar)** para cada motor de análisis disponible con una opción **Local Deep Learning (LDL) [Aprendizaje profundo local (LDL)]**. Actualmente hay dos motores de análisis disponibles con un modo LDL opcional: **HTTP Command and Control detector (Detector de comando y control HTTP)** y **HTTP2 Command and Control detector (Detector de comando y control HTTP2)**.
4. Especifique una **acción** que se debe realizar cuando se detecte una amenaza mediante un motor de análisis correspondiente.

   *La acción predeterminada para cada motor de análisis es **alert (alertar)**, sin embargo, Palo Alto Networks recomienda configurar todas las acciones en **Reset-Both (Restablecer ambos)** para la mejor postura de seguridad.*

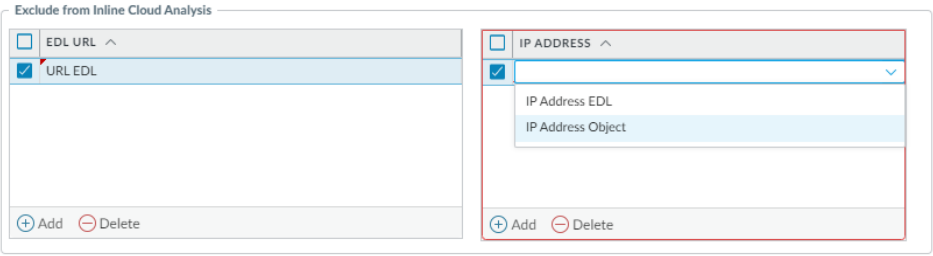
   - **Allow (Permitir)**: la solicitud está permitida y no se genera ninguna entrada de log.
   - **Alert (Alertar)**: se permite la solicitud y se genera una entrada de log de amenazas.
   - **Drop (Soltar)**: elimina la solicitud; no se envía una acción de restablecimiento al host/aplicación.
   - **Reset Client (Restablecer cliente)**: restablece la conexión de la parte del cliente.
   - **Reset Server (Restablecer servidor)**: restablece la conexión de la parte del servidor.
   - **Reset-Both (Restablecer ambos)**: restablece la conexión tanto en el extremo del cliente como en el del servidor.
5. Haga clic en **OK (Aceptar)** para salir del cuadro de diálogo de configuración del perfil antispyware y **compilar** sus cambios.

STEP 4 | (Opcional) Añada excepciones de URL o dirección IP a su perfil antispyware si el análisis en línea de la nube produce falsos positivos. Puede agregar excepciones especificando una lista dinámica externa (tipos de lista de direcciones URL o IP) o un objeto **Addresses (Direcciones)**.

1. Añada una excepción de objeto de **Listas dinámicas externas** o **Direcciones [IP].**
2. Seleccione)**Objects (Objetos) > Security Profiles (Perfiles de seguridad) > Anti-Spyware**.
3. Seleccione un perfil antispyware para el que desee excluir direcciones URL o IP específicas y, a continuación, seleccione **Inline Cloud Analysis (Análisis en línea de la nube)**.
4. **Añada** una **URL EDL** o **dirección IP**, según el tipo de excepción que desee añadir, y, a continuación, seleccione una lista dinámica externa de dirección URL o dirección IP preexistente. Si no hay ninguno disponible, cree una nueva lista dinámica externa. Para

las excepciones de dirección IP, puede, opcionalmente, seleccionar una lista de objeto **Addresses (Direcciones)**.

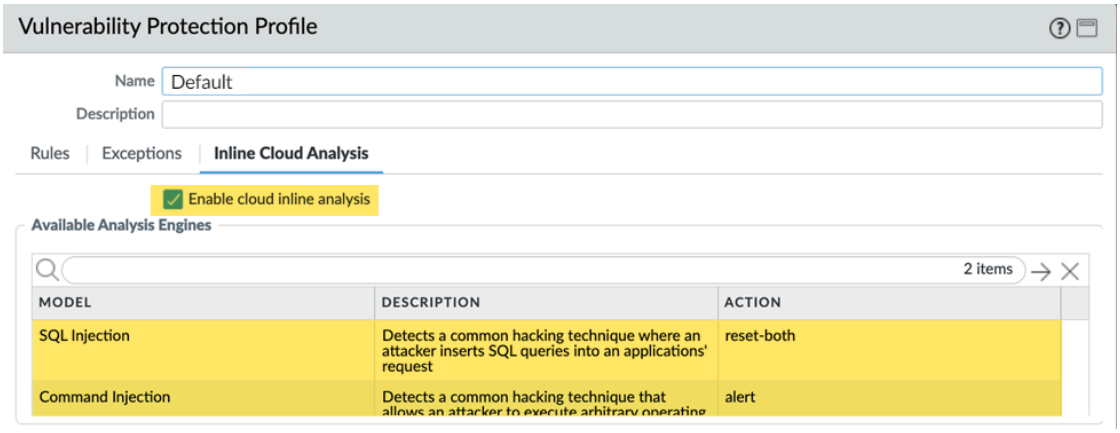
*Los perfiles antispyware que se configuran como **Shared (Compartido)** en los cortafuegos gestionados por Panorama no se pueden tener objetos de dirección IP añadidos a la lista de excepciones de análisis en línea en la nube.*



5. Haga clic en **OK (Aceptar)** para guardar el perfil antispyware y **compilar** los cambios.

STEP 5 | (Compatible con PAN-OS 11.0 y versiones posteriores) Actualice o cree un nuevo perfil de seguridad de protección frente a vulnerabilidades para habilitar el análisis en línea en la nube

(para analizar el tráfico para la inyección de comandos y las vulnerabilidades de inyección SQL en tiempo real).



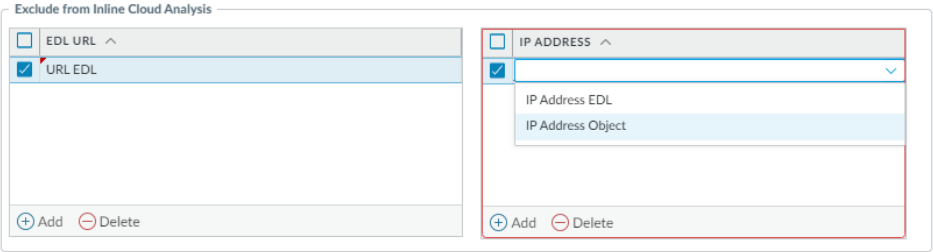
1. Seleccione un perfil de seguridad de protección frente a vulnerabilidades existente o elija **Add (Añadir)** uno nuevo [**Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Vulnerability Protection (Protección frente a vulnerabilidades)**].
2. Seleccione su perfil de protección frente a vulnerabilidades y, a continuación, vaya a **Inline Cloud Analysis (Análisis en línea en la nube)** y **Enable cloud inline analysis (Habilitar el análisis en línea en la nube)**.
3. Especifique una **Action (Acción)** a tomar cuando se detecte un exploit de vulnerabilidad utilizando un motor de análisis correspondiente. Actualmente hay dos motores de análisis disponibles: **SQL Injection (Inyección SQL)** e **Command Injection (Inyección de comandos)**.
   - **Allow (Permitir)**: la solicitud está permitida y no se genera ninguna entrada de log.
   - **Alert (Alertar)**: se permite la solicitud y se genera una entrada de log de amenazas.
   - **Reset Client (Restablecer cliente)**: restablece la conexión de la parte del cliente.
   - **Reset Server (Restablecer servidor)**: restablece la conexión de la parte del servidor.
   - **Reset-Both (Restablecer ambos)**: restablece la conexión tanto en el extremo del cliente como en el del servidor.
4. Haga clic en **OK (Aceptar)** para salir del cuadro de diálogo de configuración del perfil de protección frente a vulnerabilidades y luego en **Commit (Confirmar)** para confirmar sus cambios.

STEP 6 | (Opcional) Añada excepciones de URL y/o dirección IP a su perfil de protección frente a vulnerabilidades si el análisis en línea en la nube produce falsos positivos. Puede agregar excepciones especificando una lista dinámica externa (tipos de lista de direcciones URL o IP) o un objeto **Addresses (Direcciones)**.

1. Añada una excepción de objeto de **Listas dinámicas externas** o **Direcciones [IP].**
2. Seleccione **Objects > Security Profiles > Vulnerability (Objetos > Perfiles de seguridad > Vulnerabilidad)** para volver a su perfil de Protección frente a vulnerabilidades.
3. Seleccione un perfil de vulnerabilidad para el que desee excluir direcciones URL o direcciones IP específicas y, a continuación, seleccione **Inline Cloud Analysis (Análisis en línea en la nube)**.

4. **Añada** una **URL EDL** o **dirección IP**, según el tipo de excepción que desee añadir, y, a continuación, seleccione una lista dinámica externa de dirección URL o dirección IP preexistente. Si no hay ninguno disponible, cree una nueva lista dinámica externa. Para las excepciones de dirección IP, puede, opcionalmente, seleccionar una lista de objeto **Addresses (Direcciones)**.

   *No se puede añadir objetos de dirección IP a la lista de excepciones de análisis en la nube en línea de los perfiles de vulnerabilidad que se configuran como **Shared (Compartido)** en los cortafuegos gestionados por Panorama.*



5. Haga clic en **OK (Aceptar)** para guardar el perfil de protección frente a vulnerabilidades y **Commit (Confirmar)** sus cambios.

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

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Content-ID** > **Threat Prevention Inline Cloud Analysis (Análisis en línea en la nube de Threat Prevention)**.
2. Especifique el valor de tiempo de espera y la acción asociada que se debe realizar cuando se alcancen los límites de latencia para las solicitudes de análisis en línea en la nube:
   - Latencia máxima (ms): especifique el tiempo de procesamiento máximo aceptable, en segundos, para que el análisis en línea en la nube devuelva un resultado.
   - Permitir en latencia máxima: permite que el cortafuegos realice la acción de permitir, cuando se alcanza la latencia máxima. Al anular la selección de esta opción, se establece que la acción del cortafuegos se bloquee.
   - Registrar tráfico no analizado: permite que el cortafuegos registre las solicitudes de tráfico que muestren características anómalas que indiquen la presencia de amenazas de mando y control (C2) avanzadas y evasivas, pero que no hayan sido procesadas por el análisis en línea en la nube de Threat Prevention.
3. Haga clic en **OK (Aceptar)** para confirmar los cambios.

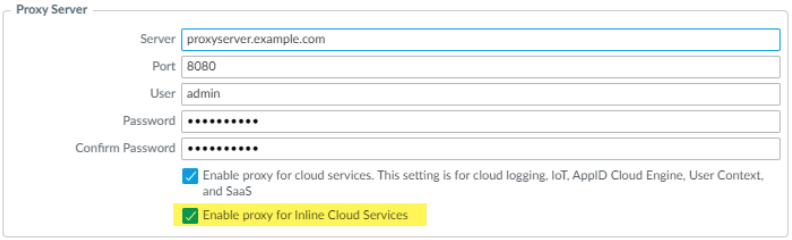
STEP 8 | Instalar un certificado de dispositivo Repita el procedimiento para todos los cortafuegos habilitados para el análisis en línea en la nube.

STEP 9 | (Necesario cuando el cortafuegos se implementa con un servidor proxy explícito) Configure el servidor proxy utilizado para acceder a los servidores que facilitan las solicitudes generadas por todas las características de análisis en la nube configuradas. Se puede especificar un único servidor proxy que se aplica a todos los servicios de actualización

de Palo Alto Networks, incluidos todos los servicios de registro de logs y nube en línea configurados.

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

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

   3. Haga clic en **OK (Aceptar)**.
2. (Solo para las siguientes versiones: PAN-OS 10.2.11 y versiones posteriores y PAN-OS 11.1.5 y versiones posteriores) Configure el servidor proxy a través de la CLI del cortafuegos.
   1. Acceda a la CLI del cortafuegos.
   2. Configure los ajustes del servidor proxy base mediante los siguientes comandos de la CLI:

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



```
set deviceconfig system secure-proxy-user <value> set
deviceconfig system secure-proxy-password <value>
```

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

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

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

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

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

Por ejemplo:

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

STEP 10 | (Opcional) Establezca el nombre de dominio completo (FQDN) de contenido en la nube que utiliza el cortafuegos para gestionar las solicitudes de servicio de análisis en línea de la nube. El FQDN predeterminado se conecta a hawkeye.services-edge.paloaltonetworks.com y, a continuación, se resuelve en el servidor de servicios en la nube más cercano. Puede invalidar

la selección automática del servidor especificando un servidor de contenido en la nube regional que mejor se adapte a sus requisitos de residencia y rendimiento de datos.

El FQDN de contenido en la nube es un recurso utilizado globalmente y afecta a la forma en que otros servicios que dependen de esta conexión envían cargas útiles de tráfico.

Verifique que el cortafuegos use el FQDN de Content Cloud correcto (**Device [Dispositivo]** > **Setup [Configuración]** > **Content-ID** > **Content Cloud Setting [Configuración de Content Cloud]**) para su región y cambie el FQDN si es necesario:

Si su NGFW está configurado en línea para facilitar una implementación de seguridad SaaS, tenga en cuenta que los FQDN ubicados en Francia y Japón no admiten actualmente la funcionalidad de seguridad SaaS.

- Centro de EE. UU. (Iowa, EE. UU.): **us.hawkeye.services-edge.paloaltonetworks.com**
- Europa (Fráncfort, Alemania): **eu.hawkeye.services-edge.paloaltonetworks.com**
- APAC (Singapur): **apac.hawkeye.services-edge.paloaltonetworks.com**
- India (Mumbai): **in.hawkeye.services-edge.paloaltonetworks.com**
- Reino Unido (Londres, Inglaterra): **uk.hawkeye.services-edge.paloaltonetworks.com**
- Francia (París, Francia): **fr.hawkeye.services-edge.paloaltonetworks.com**
- Japón (Tokio, Japón): **jp.hawkeye.services-edge.paloaltonetworks.com**
- Australia (Sídney, Australia): **au.hawkeye.services-edge.paloaltonetworks.com**
- Canadá (Montreal, Canadá): **ca.hawkeye.services-edge.paloaltonetworks.com**
- Suiza (Zúrich, Suiza): **ch.hawkeye.services-edge.paloaltonetworks.com**

STEP 11 | (Opcional) Compruebe el estado de la conectividad del cortafuegos con el servicio en la nube Advanced Threat Prevention.

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

```
show ctd-agent status security-client
```

Por ejemplo:

```
show ctd-agent status security-client ... Security Client
 AceMlc2(1) Current cloud server: hawkeye.services-
edge.paloaltonetworks.com Cloud connection: connected ...
```

Salida de CLI acortada por brevedad.

Si no puede conectarse al servicio en la nube Advanced Threat Prevention, compruebe que no se está bloqueando el siguiente dominio: hawkeye.services-edge.paloaltonetworks.com.

STEP 12 | (Opcional) Supervisar Advanced Threat Prevention

Configuración del análisis en línea en la nube (Strata Cloud Manager)

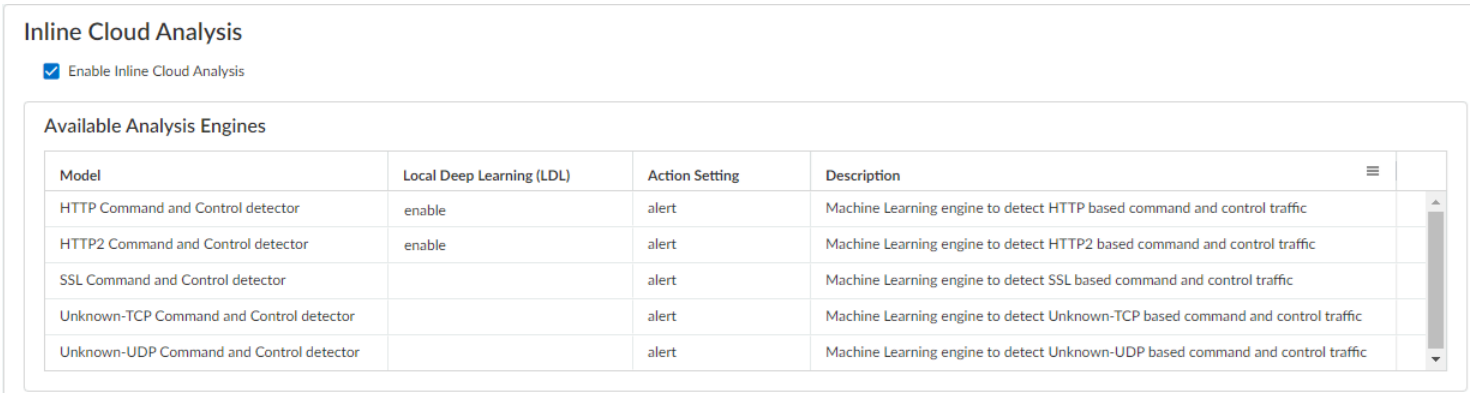
STEP 1 | Para aprovechar el análisis en línea en la nube, debe tener una suscripción a Prisma Access, que proporciona acceso a las funciones de Advanced Threat Prevention. Para obtener información sobre las aplicaciones y los servicios ofrecidos con Prisma Access, consulte Todas las aplicaciones y servicios disponibles.

Para verificar las suscripciones para las que tiene licencias activas actualmente, Compruebe lo que es compatible con su licencia.

STEP 2 | Utilice las credenciales asociadas con su cuenta de asistencia técnica de Palo Alto Networks e inicie sesión en Strata Cloud Manager en el hub.

STEP 3 | Actualice o cree un nuevo perfil de seguridad antispyware para habilitar el análisis en línea en la nube (para analizar el tráfico en busca de amenazas avanzadas de C2 [comando y control] y spyware en tiempo real).

1. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and (NGFW y) Prisma Access** > **Security Services (Servicios de Seguridad)** > **Anti-Spyware (Antispyware)**.
2. Seleccione su perfil de seguridad antispyware y navegue hasta el panel de **Inline Cloud Analysis (Análisis en línea en la nube)** y seleccione **Enable Inline Cloud Analysis (Habilitar el análisis en línea en la nube)**.



3. Seleccione **enable (habilitar)** para cada motor de análisis disponible con una opción **Local Deep Learning (LDL) [Aprendizaje profundo local (LDL)]**. Actualmente hay dos motores de análisis disponibles con un modo LDL opcional: **HTTP Command and Control detector**

(Detector de comando y control HTTP) y **HTTP2 Command and Control detector (Detector de comando y control HTTP2)**.

4. Especifique una **acción** que se debe realizar cuando se detecte una amenaza mediante un motor de análisis correspondiente.

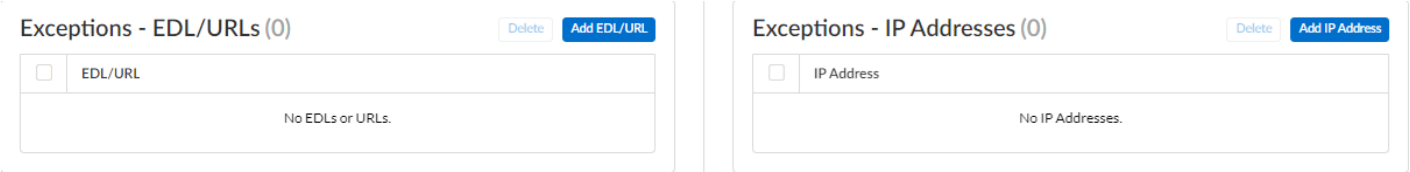
   *La acción predeterminada para cada motor de análisis es **alert (alertar)**, sin embargo, Palo Alto Networks recomienda configurar todas las acciones en **Reset-Both (Restablecer ambos)** para la mejor postura de seguridad.*

   - **Allow (Permitir)**: la solicitud está permitida y no se genera ninguna entrada de log.
   - **Alert (Alertar)**: se permite la solicitud y se genera una entrada de log de amenazas.
   - **Drop (Soltar)**: elimina la solicitud; no se envía una acción de restablecimiento al host/aplicación.
   - **Reset Client (Restablecer cliente)**: restablece la conexión de la parte del cliente.
   - **Reset Server (Restablecer servidor)**: restablece la conexión de la parte del servidor.
   - **Reset-Both (Restablecer ambos)**: restablece la conexión tanto en el extremo del cliente como en el del servidor.

5. Haga clic en **OK (Aceptar)** para salir del cuadro de diálogo de configuración del perfil de seguridad antispyware y seleccione **Commit (Confirmar)** para confirmar sus cambios.

STEP 4 | (Opcional) Añada excepciones de URL o dirección IP a su perfil antispyware si el análisis en línea de la nube produce falsos positivos. Puede añadir excepciones especificando un Lista dinámica externa (tipos de lista de direcciones IP y URL) o un objeto de política de **Addresses (Direcciones)**.

1. Añada una excepción de objeto de **Listas dinámicas externas** o **Direcciones [IP]**.
2. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **Anti-spyware (Antispyware)**.
3. Seleccione un perfil antispyware para el que desee excluir direcciones URL o IP específicas y, a continuación, vaya al panel **Inline Cloud Analysis (Análisis en línea de la nube)**.
4. Deberá **Add EDL/URL (Añadir EDL/URL)** o **Add IP Address (Añadir dirección IP)**, en función del tipo de excepción que desee añadir y, a continuación, seleccione una URL o una lista dinámica externa de direcciones IP preexistente. Si no hay ninguna disponible, cree un nuevo objeto de política de la lista dinámica externa. Para las excepciones de dirección IP, puede, opcionalmente, seleccionar una lista de objeto **Addresses (Direcciones)**.



5. Haga clic en **OK (Aceptar)** para guardar el perfil antispyware y **compilar** los cambios.

STEP 5 | (Opcional) Supervisar Advanced Threat Prevention

Prevención de ataques de fuerza bruta

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia de Advanced Threat Prevention (para un mejor soporte de funciones) o Threat Prevention

Un ataque de fuerza bruta utiliza un gran volumen de solicitudes/respuestas de la misma dirección IP de origen o destino para introducirse en un sistema. El atacante emplea un método de ensayo y error para adivinar la respuesta a un reto o una solicitud.

El perfil de protección frente a vulnerabilidades incluye firmas para protegerle de ataques de fuerza bruta. Cada firma tiene un ID, nombre de amenaza y gravedad, y se activa cuando se registra un patrón. El patrón especifica las condiciones y el intervalo en los que el tráfico se identifica como un ataque de fuerza bruta; algunas firmas están asociadas a otra firma secundaria de una gravedad menor que especifica el patrón con el que debe coincidir. Cuando un patrón coincide con la firma o la firma secundaria, activa la acción predeterminada de la firma.

Para aplicar la protección:

- Adjunte el perfil de protección frente a vulnerabilidades a una regla de la política de seguridad. Consulte Configuración de antivirus, antispyware y protección frente a vulnerabilidades.
- Instale actualizaciones de contenido que incluyan nuevas firmas para proteger el cortafuegos frente a amenazas emergentes. Consulte Instalación de las actualizaciones de contenido y software.

Personalización de la acción y las condiciones de activación para una firma de fuerza bruta

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia de Advanced Threat Prevention (para un mejor soporte de funciones) o Threat Prevention

El cortafuegos incluye dos tipos de firmas de fuerza bruta predefinidas: firma principal y firma secundaria. Una firma secundaria es una única incidencia de un patrón de tráfico que coincide con la firma. Una firma principal está asociada a una firma secundaria y se activa cuando se producen varios eventos dentro de un intervalo de tiempo, que coinciden con el patrón de tráfico definido en la firma secundaria.

Por lo general, una firma secundaria tiene de manera predeterminada la acción *permitir*, porque un único evento no es indicativo de un ataque. Esto garantiza que el tráfico legítimo no se bloquee y evita generar logs de amenaza para los eventos que no merecen atención. Palo Alto Networks le recomienda que no cambie la acción predeterminada sin antes considerarlo detenidamente.

En la mayoría de los casos, la firma de fuerza bruta es un evento destacado debido a su patrón recurrente. Si fuera necesario, puede realizar una de las siguientes opciones para personalizar la acción para una firma de fuerza bruta:

- Cree una regla para modificar la acción predeterminada para todas las firmas de la categoría de fuerza bruta. Puede optar por permitir, alertar, bloquear, restablecer o descartar el tráfico.
- Defina una excepción para una firma específica. Por ejemplo, puede buscar y definir una excepción para CVE.

Para una firma principal, puede modificar tanto las condiciones de activación como la acción; para una firma secundaria, solamente puede modificar la acción.

Para mitigar un ataque de manera eficaz, especifique la acción Bloquear dirección IP en lugar de la acción Eliminar o Restablecer para la mayoría de firmas de fuerza bruta.

STEP 1 | Cree un nuevo perfil de protección contra vulnerabilidades.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Vulnerability Protection (Protección frente a vulnerabilidades)** y **Add (Añadir)** para añadir un perfil.
2. Especifique un nombre en **Name** para el perfil de protección frente a vulnerabilidades.
3. (Opcional) Introduzca una **descripción**.
4. (Opcional) Especifique que el perfil sea **Shared (Compartido)** con:
   - **Every virtual system (vsys) on a multi-vsys firewall (Cada sistema virtual [vsys] en un cortafuegos de varios vsys)**: si no está marcada (deshabilitada), el perfil está disponible únicamente para el sistema virtual seleccionado en la pestaña **Objects (Objetos)**.

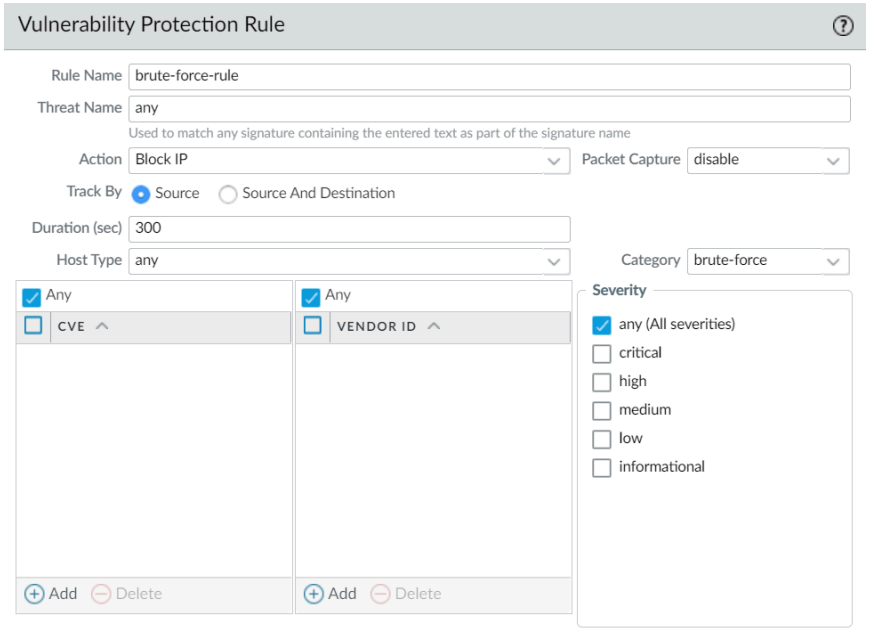
- **Every device group on Panorama (Cada grupo de dispositivos en Panorama)**: si no está marcada (deshabilitada), el perfil está disponible únicamente para el grupo de dispositivos seleccionado en la pestaña **Objects (Objetos)**.

5. (Opcional, Panorama únicamente) Seleccione **Disable override (Deshabilitar cancelación)** para evitar que los administradores cancelen la configuración de este perfil de protección frente a vulnerabilidades en los grupos de dispositivos que lo heredan. Esta opción no está seleccionada de manera predeterminada, lo que significa que los administradores pueden cancelar la configuración de cualquier grupo de dispositivos que hereda el perfil.

STEP 2 | Cree una regla que defina la acción para todas las firmas de una categoría.

1. En la pestaña **Rules (Reglas)**, seleccione **Add (Añadir)** e ingrese un **Rule Name (Nombre de regla)** para una nueva regla.
2. (Opcional) Especifique un nombre de amenaza específico (el valor predeterminado es **any [cualquiera]**).
3. Establezca la **Acción**. En este ejemplo, está establecida como **Block IP**.

   Si configura un perfil de protección frente a vulnerabilidades para bloquear IP, el cortafuegos primero utiliza hardware para bloquear las direcciones IP. Si el tráfico de ataques excede la capacidad de bloqueo del hardware, el cortafuegos utiliza mecanismos de bloqueo de software para bloquear las direcciones IP restantes.
4. Establezca la **Categoría** como **Fuerza bruta**.
5. (Opcional) Si bloquea, especifique el **Host Type (Tipo de host)** en el cual desea bloquear: **server (servidor)** or **client (cliente)** (el predeterminado es **any (cualquiera)**).
6. Consulte Paso 3 para personalizar la acción de una firma específica.
7. Consulte Paso 4 para personalizar el umbral de activación de una firma principal.



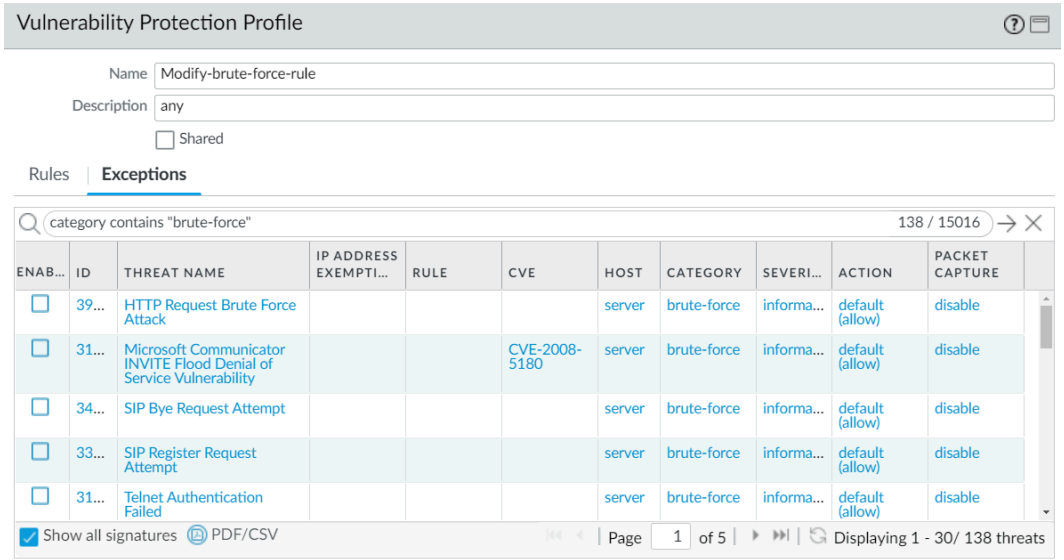
8. Haga clic en **OK (Aceptar)** para guardar la regla y el perfil.

STEP 3 | (Opcional) Personalice la acción para una firma específica.

1. En la pestaña **Exceptions (Excepciones)**, seleccione **Show all signatures (Mostrar todas las firmas)** para buscar la firma que desee modificar.

   Para ver todas las firmas de la categoría de fuerza bruta, busque por `category contains 'brute-force'`.

2. Para editar una firma específica, haga clic en la acción predeterminada predefinida en la columna Acción.



3. Defina la acción. **Allow (Permitir)**, **Alert (Alertar)**, **Block Ip (Bloquear IP)** o **Drop (Descartar)**. Si selecciona **Block Ip (Bloquear IP)**, realice estas tareas adicionales:

   1. Especifique el **Time (Tiempo)** (en segundos) después del cual activar la acción.
   2. Especifique **Track By (Rastrear por)** y bloquee la dirección IP usando **IP source (Origen de IP)** o **IP source and destination (Origen y destino de IP)**.

4. Haga clic en **OK (Aceptar)**.
5. Para cada firma modificada, seleccione la casilla de verificación de la columna **Enable (Habilitar)**.
6. Haga clic en **OK (Aceptar)**.

STEP 4 | Personalice las condiciones de activación para una firma principal.

Una firma principal que pueda editarse se marcará con este icono: .

En este ejemplo, los criterios de búsqueda fueron la categoría brute force y CVE-2008-1447.

1. Modifique ( ) el atributo de tiempo y los criterios de agregación para la firma.
2. Para modificar el umbral de activación, especifique el **Number of Hits (Número de resultados)** por cantidad de **seconds (segundos)**.
3. Especifique si agregar el número de resultados (**Aggregation Criteria [Criterios de agregación]**) por **source (origen)**, **destination (destino)** u **source-and-destination (origen y destino)**.
4. Haga clic en **OK (Aceptar)**.

STEP 5 | Añada este nuevo perfil a una regla de política de seguridad.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y **Add (Añadir)** o modifique una regla de política de seguridad.
2. En la pestaña **Actions (Acciones)**, seleccione **Profiles (Perfiles)** como el **Profile Type (Tipo de perfil)** para el Profile Setting (Ajuste de perfil).
3. Seleccione su perfil de **Vulnerability Protection (Protección frente a vulnerabilidades)**.
4. Haga clic en **OK (Aceptar)**.

STEP 6 | Confirme los cambios.

1. Haga clic en **Commit (Confirmar)**.

Habilitación de las firmas de evasión

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	☐ Licencia de Advanced Threat Prevention (para un mejor soporte de funciones) o Threat Prevention

Las firmas de evasión de Palo Alto Networks detectan solicitudes HTTP o TLS manipuladas y pueden alertar en instancias en las que un cliente se conecta a un dominio que no es el dominio especificado en la solicitud DNS. Las firmas de evasión son eficaces únicamente cuando el cortafuegos está habilitado para actuar como un proxy DNS y resolver las solicitudes de nombre de dominio. La práctica recomendada es realizar los siguientes pasos para habilitar las firmas de evasión.

STEP 1 | Habilite un cortafuegos que sea un intermediario entre los clientes y los servidores, y que actúe como proxy DNS.

Realice la Configuración de un objeto proxy DNS, que incluye los siguientes pasos:

- Especifique las interfaces en las cuales desea que el cortafuegos escuche las solicitudes DNS.
- Defina el servidor DNS con el que se comunicará el cortafuegos para resolver las solicitudes DNS.
- Configure las entradas estáticas de FQDN a dirección IP que el cortafuegos puede resolver localmente, sin tener que conectarse con un servidor DNS.
- Habilite el almacenamiento en caché de asignaciones resueltas de nombre de host a dirección IP.

STEP 2 | Obtenga la versión más reciente de contenido sobre aplicaciones y amenazas (versión 579 o posterior).

1. Seleccione **Device** > **Dynamic Updates** (Dispositivo > Actualizaciones dinámicas).
2. Seleccione **Check Now** para descargar las últimas actualizaciones de contenido de aplicaciones y amenazas.
3. Descargue e instale la versión de contenido 579 de aplicaciones y amenazas (o posterior).

STEP 3 | Defina cómo el cortafuegos debe aplicar acciones al tráfico que coincide con las firmas de evasión.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Anti-Spyware (Antispyware)** y **Add (Añadir)** para añadir o modificar un perfil antispyware.
2. Seleccione **Exceptions (Excepciones)** y seleccione **Show all signatures (Mostrar todas las firmas)**.
3. Filtre las firmas en función de la palabra clave `evasion`.
4. Para todas las firmas de evasión, configure **Action (Acciones)** en un ajuste que no sea el de permitir o la acción por defecto (la acción por defecto para las firmas de evasión es permitir). Por ejemplo, establezca que la **Action (Acción)** para las ID de firmas 14978 y 14984 sea **alert (alertar)** o **drop (descartar)**.
5. Haga clic en **OK (Aceptar)** para guardar el perfil de antispyware actualizado.
6. Adjunte el perfil de antispyware a una regla de política de seguridad: Seleccione **Policies (Políticas)** > **Security (Seguridad)**, seleccione la política deseada para modificarla y, a continuación, haga clic en la pestaña **Actions (Acciones)**. En Profile Settings (Configuración del perfil), haga clic en el menú desplegable junto a **Anti-Spyware**, seleccione el perfil antispyware que acaba de modificar para aplicar las firmas de evasión.

STEP 4 | Confirme los cambios.

Haga clic en **Commit (Confirmar)**.

Creación de excepciones de amenazas

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia de Advanced Threat Prevention (para un mejor soporte de funciones) o Threat Prevention

Palo Alto Networks define una acción predeterminada recomendada (como un bloqueo o una alerta) para las firmas de amenazas. Puede utilizar una ID de amenaza para excluir una firma de amenaza de la aplicación o modificar la acción que se aplica a esa firma de amenaza. Por ejemplo, puede modificar la acción para las firmas de amenazas que causan falsos positivos en su red.

Configure las excepciones de las amenazas para antivirus, vulnerabilidad, spyware y firmas de DNS para cambiar la aplicación para una amenaza. Sin embargo, antes de comenzar, asegúrese de que las amenazas se detectan y aplican correctamente en función de la configuración de firma predeterminada o de las prácticas recomendadas para una postura de seguridad óptima:

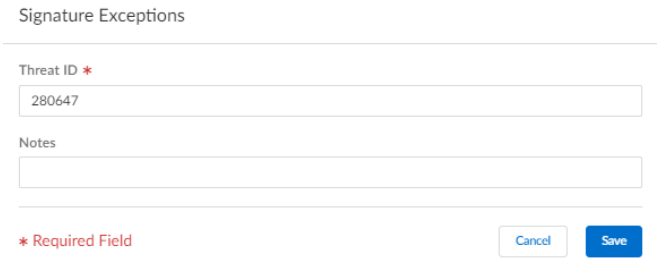
- Obtenga las actualizaciones más recientes de antivirus, amenazas y aplicaciones, y actualizaciones de firmas de WildFire (para el cortafuegos).
- Configuración de antivirus, antispyware y protección frente a vulnerabilidades y aplique estos perfiles de seguridad a su política de seguridad.
- Strata Cloud Manager
- PAN-OS y Panorama

Creación de excepciones de amenazas (Strata Cloud Manager)

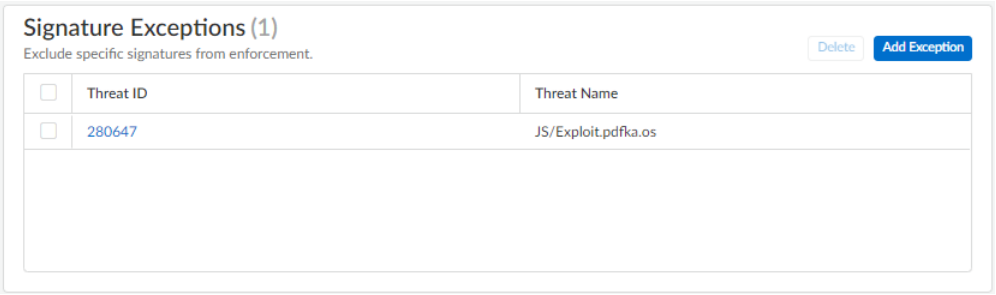
STEP 1 | Excluya las firmas del antivirus de la aplicación de acciones.

Si bien puede usar un perfil de WildFire y antivirus para excluir la aplicación de firmas de antivirus, no puede cambiar la acción que se aplica para una firma de antivirus específica. Sin embargo, puede definir la acción exigible cuando se encuentran virus en diferentes tipos de tráfico mediante la edición del perfil de seguridad ***Enforcement Actions (Acciones de aplicación)****.*

1. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and (NGFW y) Prisma Access** > **Security Services (Servicios de seguridad)** > **WildFire y Antivirus (WildFire y antivirus)**.
2. Deberá **Add Profile (Añadir perfil)** o seleccione un perfil existente de WildFire y antivirus del cual desea excluir una firma de amenazas y vaya a la pestaña **Advanced Settings (Configuración avanzada)**.
3. En el menú de **Signature Exceptions (Excepciones de firma)**, seleccione **Add Exception (Añadir excepción)** y proporcione el **Threat ID** para la firma de amenaza para la cual desea excluir su aplicación. Opcionalmente, puede añadir notas a la excepción de firma.



4. Debe **Save (Guardar)** la excepción de firma cuando haya terminado.
5. Una identificación de firma de amenazas válida completa automáticamente el campo de nombre de amenaza. Puede ver una lista completa de excepciones de firma activas, así como **Delete (Eliminar)** entradas que ya no sean necesarias.



6. Repita para añadir excepciones adicionales o haga clic en **Save (Guardar)** después de que se hayan añadido todas las excepciones de amenazas.

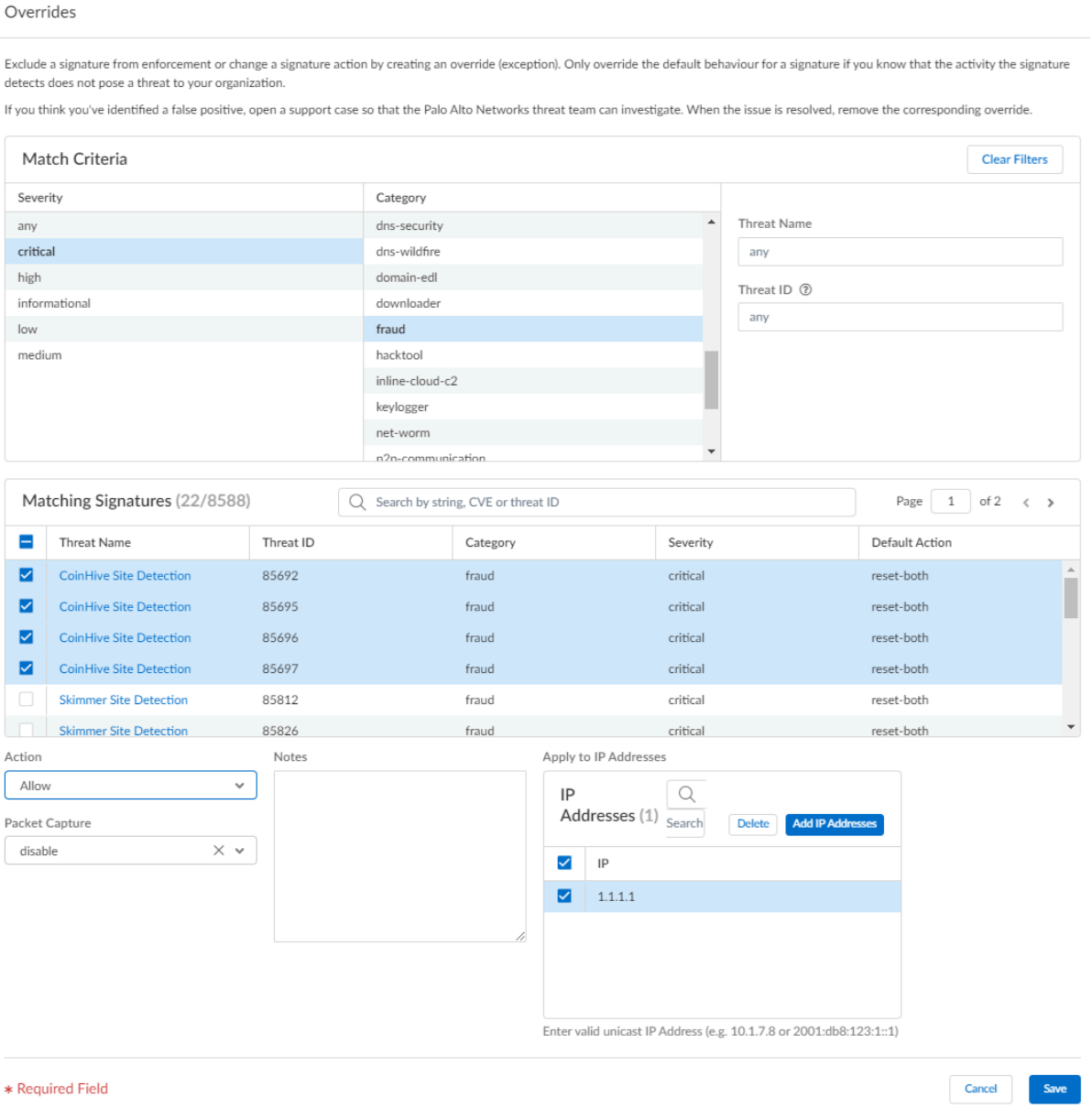
STEP 2 | Modifique la aplicación de las firmas de vulnerabilidad y spyware (excepto las firmas DNS; si bien son un tipo de firma de spyware, las firmas DNS se gestionan a través de la suscripción de DNS Security en Prisma Access).

1. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and (NGFW y)Prisma Access** > **Security Services (Servicios de seguridad)** > **Anti-Spyware**

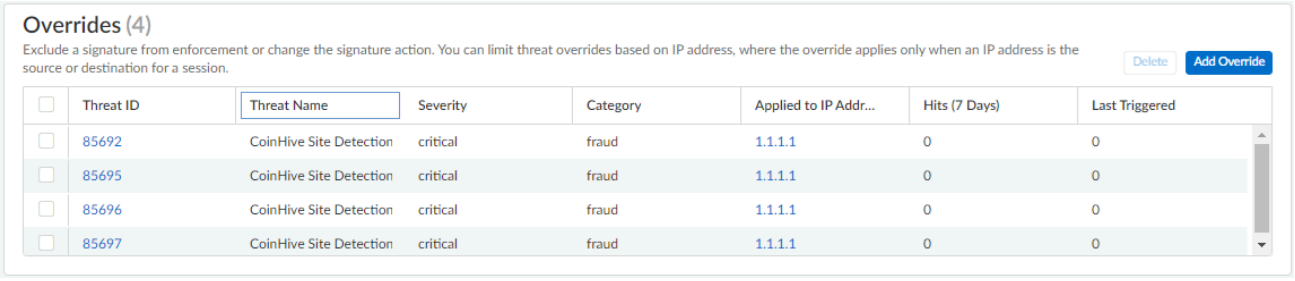
(Antispyware) o **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and (NGFW y) Prisma Access** > **Security Services (Servicios de seguridad)** > **Vulnerability Protection (Protección frente a vulnerabilidades)**, según el tipo de firma.

2. Elija **Add Profile (Añadir perfil)** para añadir un perfil nuevo o seleccione un perfil existente de antispyware o protección frente a vulnerabilidades desde el cual desea modificar la aplicación de la firma y luego seleccione **Add Override (Añadir anulación)**.
3. Busque firmas de spyware o vulnerabilidad proporcionando los **Match Criteria (Criterios de coincidencia)** pertinentes. Esto filtra automáticamente las firmas disponibles y muestra los resultados en la sección **Matching Signatures (Firmas coincidentes)** .
4. Seleccione la casilla de verificación correspondiente a la(s) firma(s) cuya aplicación desea modificar.

5. Proporcione la **Action (Acción)**, **Packet Capture (Captura de paquetes)** y **IP Addresses (Direcciones IP)** actualizadas a las que desea aplicar las reglas de aplicación modificadas para las firmas seleccionadas.



6. Debe **Save (Guardar)** su configuración de aplicación de firma actualizada.
7. Puede ver una lista completa de **Overrides (Anulaciones)**, incluidas varias estadísticas, así como **Delete (Eliminar)** entradas que ya no son necesarias.

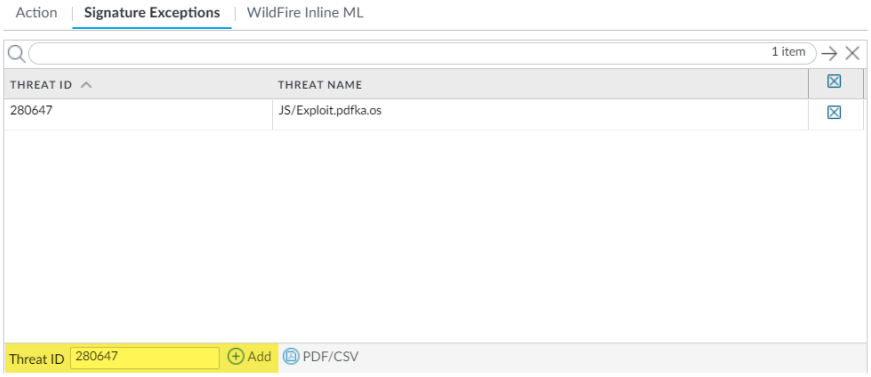


Creación de excepciones de amenazas (NGFW (Managed by PAN-OS or Panorama))

STEP 1 | Excluya las firmas del antivirus de la aplicación de acciones.

*A pesar de que puede utilizar un perfil de antivirus para excluir firmas de antivirus, no puede cambiar la acción que aplica el cortafuegos a una firma de antivirus determinada. Sin embargo, puede definir la acción que el cortafuegos aplicará a los virus que encuentre en diferentes tipos de tráfico editando los decodificadores (**Objects [Objetos] > Security Profiles [Perfiles de seguridad] > Antivirus > <antivirus-profile> > Antivirus**).*

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Antivirus**.
2. Haga clic en **Add (Añadir)** para añadir un nuevo perfil de antivirus o modifique uno existente en el que desea excluir una firma de amenazas, y seleccione **Signature Exception (Excepción de firma)**.
3. Haga clic en **Add (Añadir)** para añadir la **Threat ID (ID de amenazas)** de la firma de amenazas que desea excluir de la aplicación de acciones del cortafuegos.



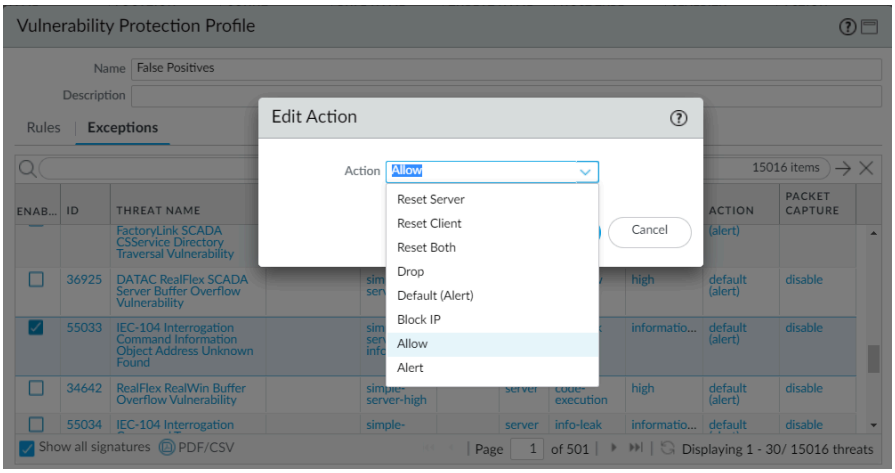
4. Haga clic en **OK (Aceptar)** para guardar el perfil de antivirus.

STEP 2 | Modifique la aplicación de acciones para las vulnerabilidades y las firmas de spyware (excepto las firmas de DNS; pase a la próxima opción para modificar la aplicación de acciones para las firmas de DNS, que son un tipo de firma de spyware).

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Anti-Spyware (Antispyware)** u **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Vulnerability Protection (Protección frente a vulnerabilidades)**.
2. **Añada** o modifique un perfil existente de protección frente a vulnerabilidades o antispyware del que desee excluir la firma de amenazas y, a continuación, seleccione

Signature Exceptions (Excepciones de firma) para los perfiles de protección antispyware o **excepciones** para los perfiles de protección frente a vulnerabilidades.

3. Haga clic en **Show all signatures (Mostrar todas las firmas)** y realice el filtro para seleccionar la firma en la que desea modificar las reglas de aplicación.
4. Marque la casilla de la columna **Enable (Habilitar)** que corresponde a la firma cuya aplicación desea modificar.
5. Seleccione la **Action (Acción)** que desea que aplique el cortafuegos en esta firma de amenaza.



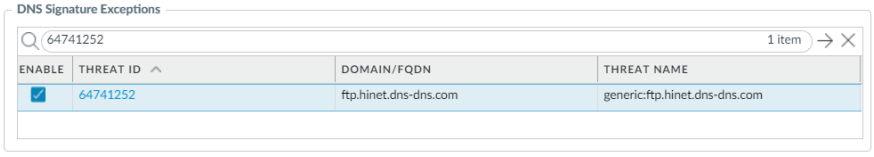
En el caso de las firmas que desea excluir de la aplicación de acciones debido a que provocan falsos positivos, configure **Allow (Permitir)** como **Action (Acción)**.

6. Haga clic en **OK (Aceptar)** para guardar su perfil nuevo o modificado antispyware o de protección frente a vulnerabilidades.

STEP 3 | Modifique la aplicación para las firmas de DNS.

De manera predeterminada, el DNS busca los nombres de host maliciosos que las firmas de DNS detectan y envían a un sinkhole.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Anti-Spyware**.
2. Haga clic en **Add (Añadir)** para añadir un nuevo perfil de antispyware o modifique uno existente en el que desea excluir una firma de amenazas, y seleccione **DNS Exceptions (Excepciones de DNS)**.
3. Busque el ID de amenaza de DNS para la firma de DNS que desee excluir de la aplicación y seleccione la casilla de la firma correspondiente:



4. Haga clic en **OK (Aceptar)** para guardar el perfil de antispyware modificado o uno nuevo.

Uso de consultas de DNS para identificar hosts infectados en la red

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia de Advanced Threat Prevention (para un mejor soporte de funciones) o Threat Prevention

La acción de sinkhole de DNS de los perfiles de antispyware permite que el cortafuegos genere respuestas falsas a las consultas de DNS de dominios malintencionados conocidos o dominios personalizados, de modo que se identifiquen los hosts de la red infectados con malware. Un host comprometido puede iniciar la comunicación con un servidor de comando y control (command-and-control, C2); si logra establecer la conexión, un atacante puede controlar de forma remota el host infectado con el fin de infiltrase más en la red o de filtrar datos.

Las consultas DNS a cualquier dominio incluido en la lista de firmas de DNS de Palo Alto Networks se envían a un sinkhole a una dirección IP de servidor de Palo Alto Networks.

El cortafuegos puede recurrir a dos orígenes de firmas de DNS para identificar los dominios malintencionados y de C2:

- (Requiere una suscripción a Advanced | Threat Prevention) Firmas DNS locales: el cortafuegos puede usar este conjunto descargado y limitado de firmas de DNS para identificar los dominios maliciosos. El cortafuegos obtiene nuevas firmas de DNS como parte de las actualizaciones diarias del antivirus.
- (Requiere una suscripción a DNS Security) Firmas de DNS Security: el cortafuegos accede al servicio en la nube DNS Security de Palo Alto Networks para buscar dominios malintencionados en la base de datos completa de firmas de DNS. DNS Security proporciona algunas firmas en exclusiva para detectar ataques de C2 que usan técnicas de aprendizaje automático, como los algoritmos de generación de dominios (domain generation algorithm, DGA) y la tunelización de DNS. Para obtener más información sobre la suscripción a DNS Security, consulte la guía de DNS Security.

  Si desea especificar una acción de sinkholing para las firmas de DNS Security, puede configurar esos ajustes como parte de su perfil de DNS Security.

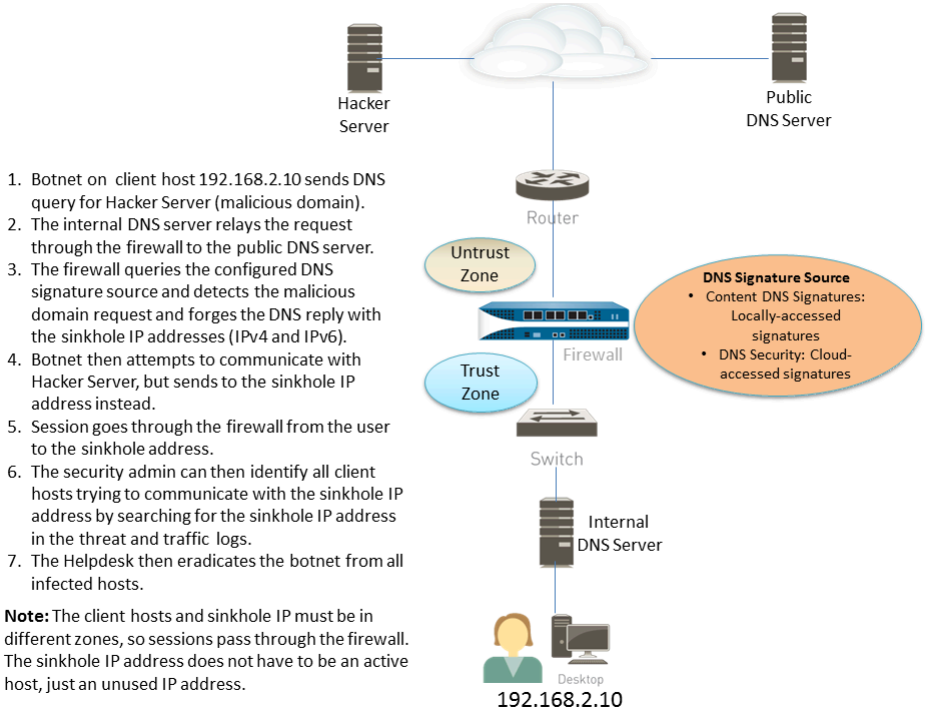
Las consultas de DNS de dominios realizadas en el conjunto local de firmas de DNS o en el conjunto de firmas de DNS Security se redirigen a un servidor de Palo Alto Networks, y el host no puede acceder al dominio malintencionado. Los temas siguientes aportan información para habilitar el sinkholing de DNS con el fin de identificar los hosts infectados.

- Funcionamiento del sinkholing de DNS
- Configuración del sinkholing de DNS
- Configuración del sinkholing de DNS para una lista de dominios personalizados
- Configuración de la dirección IP del sinkhole en un servidor local de la red
- Consulta de hosts infectados que intentan conectar a dominios malintencionados

Funcionamiento del sinkholing de DNS

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia de Advanced Threat Prevention (para un mejor soporte de funciones) o Threat Prevention

La función de sinkholing de DNS facilita la identificación de hosts infectados en la red protegida mediante tráfico DNS en situaciones en las que el cortafuegos no puede ver la consulta de DNS del cliente infectado (es decir, el cortafuegos no puede ver el originador de la consulta de DNS). En una implementación típica, donde el cortafuegos está antes del servidor DNS local, el log de amenazas identificará la resolución DNS local como el origen del tráfico en lugar del host infectado. Al hacer el sinkholing de las consultas de DNS de malware, se resuelve este problema de visibilidad, ya que se generan respuestas falsas a las consultas de los hosts clientes dirigidas a dominios malintencionados. De ese modo, si los clientes intentan conectarse a dominios malintencionados (mediante comando y control [command-and-control, C2], por ejemplo), se conectan, en cambio, a la dirección IP predeterminada de sinkhole de Palo Alto Networks o a la dirección IP que defina el usuario según el procedimiento Configuración del sinkholing de DNS para una lista de dominios personalizados. Así, resulta muy sencillo identificar los hosts infectados en los logs de tráfico.



Configuración del sinkholing de DNS

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia de Advanced Threat Prevention (para un mejor soporte de funciones) o Threat Prevention

Para habilitar el sinkholing de DNS, adjunte el perfil anti-spyware predeterminado a una regla de la política de seguridad del cortafuegos (consulte Configuración de antivirus, antispyware y protección frente a vulnerabilidades). Las consultas de DNS sobre cualquier dominio incluido en el origen de firmas de DNS de Palo Alto Networks que especifique se resuelven en la dirección IP predeterminada de sinkhole de Palo Alto Networks. En la actualidad, se utilizan una dirección IPv4 (sinkhole.paloaltonetworks.com) y una dirección IPv6 de bucle invertido (::1). Esta dirección está sujeta a cambios y puede actualizarse con actualizaciones de contenido.

STEP 1 | Habilite el sinkholing de DNS para la lista personalizada de dominios en una lista dinámica externa.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Anti-Spyware**.
2. Modifique un perfil existente o seleccione uno de los perfiles por defecto existentes y duplíquelo.
3. Asigne un nombre al perfil en **Name (Nombre)** y, a continuación, seleccione la pestaña **DNS Policies (Políticas DNS)**.
4. Verifique que **default-paloalto-dns** esté presente en el **origen de firma**.
5. (Opcional) En la lista desplegable **Packet Capture (Captura de paquetes)**, seleccione **single-packet (un solo paquete)** para capturar el primer paquete de la sesión o **extended-capture (captura extendida)** para configurar entre 1 y 50 paquetes. A continuación, puede usar las capturas de paquete para un análisis más detallado.

STEP 2 | Verifique los ajustes de sinkholing en el perfil de antispyware.

1. En la pestaña **DNS Policies (Políticas DNS)**, verifique que **Policy Action (Acción de políticas)** en las consultas DNS sea **sinkhole**.
2. En la sección DNS Sinkhole Settings (Configuración de sinkhole de DNS), verifique que está habilitada la opción **Sinkhole**. Para su conveniencia, la dirección IP del sinkhole por defecto se configura para acceder a un servidor de Palo Alto Networks. Palo Alto Networks puede actualizar automáticamente esta dirección IP a través de actualizaciones de contenido.

   Si desea cambiar la dirección de **Sinkhole IPv4 (IPv4 de sinkhole)** o **Sinkhole IPv6 (IPv6 de sinkhole)** por un servidor local de la red o por una dirección de bucle invertido, consulte Configuración de la dirección IP del sinkhole en un servidor local de la red.
3. Haga clic en **OK (Aceptar)** para guardar el perfil de antispyware.

STEP 3 | Adjunte el perfil de antispyware a una regla de política de seguridad.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y seleccione una regla de la política de seguridad.
2. En la pestaña **Actions**, seleccione la casilla de verificación **Log at Session Start** para habilitar el registro de logs.
3. En la sección Profile Setting, haga clic en el menú desplegable **Profile Type** para ver todos los **Profiles**. Haga clic en el menú desplegable **Anti-Spyware** y seleccione el nuevo perfil.
4. Haga clic en **OK (ACEPTAR)** para guardar la regla de política.

STEP 4 | Para comprobar que se aplica la acción de la política, supervise la actividad del cortafuegos.

1. Seleccione **ACC** y añada un dominio de URL como filtro global para ver la actividad de amenazas y la actividad bloqueada para el dominio al cual accedió.
2. Seleccione **Monitor (Supervisar)** > **Logs** > **Threat (Amenaza)** y filtre por `(action eq sinkhole)` para visualizar los logs en los dominios de sinkhole.

Configuración del sinkholing de DNS para una lista de dominios personalizados

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	☐ Licencia de Advanced Threat Prevention (para un mejor soporte de funciones) o Threat Prevention

Para habilitar el sinkholing para una lista personalizada de dominios, debe crear una lista externa dinámica que incluya los dominios, habilite la acción de sinkhole en un perfil antispyware y adjunte el perfil a una regla de política de seguridad. Cuando un cliente intenta acceder a un dominio malintencionado de la lista, el cortafuegos falsifica la dirección IP de destino en el paquete al servidor por defecto de Palo Alto Networks o a una dirección IP definida por el usuario para el sinkholing.

Para cada dominio personalizado incluido en la lista dinámica externa, el cortafuegos general las firmas de spyware basadas en DNS. La firma se denomina Custom Malicious DNS Query <domain name> y es del tipo spyware con gravedad media; cada firma es un hash de 24 bytes del nombre de dominio.

Para obtener información sobre los límites de entrada de la lista de dominios, consulte Lista dinámica externa.

STEP 1 | Habilite el sinkholing de DNS para la lista personalizada de dominios en una lista dinámica externa.

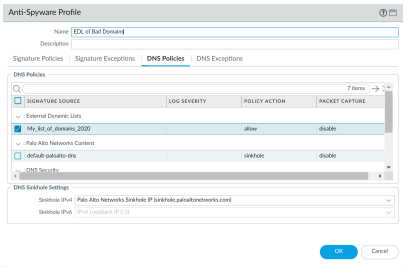
1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Anti-Spyware**.
2. Modifique un perfil existente o seleccione uno de los perfiles por defecto existentes y duplíquelo.
3. Asigne un nombre al perfil en **Name (Nombre)** y, a continuación, seleccione la pestaña **DNS Policies (Políticas DNS)**.
4. Seleccione una EDL a partir del origen de firma de **External Dynamic Lists (Listas dinámicas externas)**.

   *Si ya ha creado una lista dinámica externa de tipo: **Domain List (Lista de dominio)**, puede seleccionarla aquí. La lista no muestra listas dinámicas externas de tipo URL o direcciones IP que pueda haber creado.*
5. Configure la lista dinámica externa del perfil Anti-Spyware (consulte Configuración del cortafuegos para acceder a una lista dinámica externa). El **Type (Tipo)** está preconfigurado en **Domain List (Lista de dominios)**.
6. (Opcional) En la lista desplegable **Packet Capture (Captura de paquetes)**, seleccione **single-packet (un solo paquete)** para capturar el primer paquete de la sesión o **extended-capture (captura extendida)** para configurar entre 1 y 50 paquetes. A continuación, puede usar las capturas de paquete para un análisis más detallado.

STEP 2 | Verifique los ajustes de sinkholing en el perfil de antispyware.

1. En la pestaña **DNS Policies (Políticas DNS)**, verifique que **Policy Action (Acción de políticas)** en las consultas DNS sea **sinkhole**.
2. En la sección DNS Sinkhole Settings (Configuración de sinkhole de DNS), verifique que está habilitada la opción **Sinkhole**. Para su conveniencia, la dirección IP del sinkhole por defecto se configura para acceder a un servidor de Palo Alto Networks. Palo Alto Networks puede actualizar automáticamente esta dirección IP a través de actualizaciones de contenido.

   Si desea modificar la dirección de **Sinkhole IPv4** o **Sinkhole IPv6** en un servidor local de su red o en una dirección de bucle invertido, consulte Configuración de la dirección IP de sinkhole en un servidor local o en su red.



3. Haga clic en **OK (Aceptar)** para guardar el perfil de antispyware.

STEP 3 | Adjunte el perfil de antispyware a una regla de política de seguridad.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y seleccione una regla de la política de seguridad.
2. En la pestaña **Actions**, seleccione la casilla de verificación **Log at Session Start** para habilitar el registro de logs.
3. En la sección Profile Setting, haga clic en el menú desplegable **Profile Type** para ver todos los **Profiles**. Haga clic en el menú desplegable **Anti-Spyware** y seleccione el nuevo perfil.
4. Haga clic en **OK (ACEPTAR)** para guardar la regla de política.

STEP 4 | Compruebe que la acción de política esté forzada.

1. Visualice las entradas de lista dinámica externa que pertenezcan a la lista de dominio y acceda a un dominio desde la lista.
2. Para supervisar la actividad del cortafuegos:
   1. Seleccione **ACC** y añada un dominio de URL como filtro global para ver la actividad de amenazas y la actividad bloqueada para el dominio al cual accedió.
   2. Seleccione **Monitor (Supervisar)** > **Logs** > **Threat (Amenaza)** y filtre por `(action eq sinkhole)` para visualizar los logs en los dominios de sinkhole.

STEP 5 | Verifique si las entradas en la lista dinámica externa se ignoraron u omitieron.

Use el siguiente comando CLI en el cortafuegos para revisar los detalles de la lista.

```
request system external-list show type domain name <list_name>
```

Por ejemplo:

```
request system external-list show type domain name
 My_List_of_Domains_2015 vsys1/EBLDomain: Próxima actualización
 en: Jue 21 de mayo 10:15:39 2015 Fuente: https://1.2.3.4/
My_List_of_Domains_2015 Con referencia: Sí Válido : Sí Número de
 entradas: 3 dominios:www.example.com baddomain.com qqq.abcedfg.com
```

STEP 6 | (Opcional) Recupere la lista dinámica externa a pedido.

Para forzar que el cortafuegos recupere la lista actualizada a pedido en lugar de hacerlo en el siguiente intervalo de actualización (la frecuencia de **Repeat** que definió para la lista dinámica externa), use el siguiente comando CLI:

```
request system external-list refresh type domain name  <list_name>
```

Como alternativa, puede usar la interfaz del cortafuegos para recuperar una lista dinámica externa del servidor web.

Configuración de la dirección IP del sinkhole en un servidor local de la red

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia de Advanced Threat Prevention (para un mejor soporte de funciones) o Threat Prevention

Por defecto, la función de sinkholing está habilitada para todas las firmas DNS de Palo Alto Network, y la dirección IP de sinkhole está configurada para acceder a un servidor de Palo Alto Network. Use las instrucciones de esta sección si desea configurar la dirección IP de sinkhole en un servidor local de la red.

Debe obtener las direcciones IPv4 e IPv6 para usar como direcciones IP de sinkhole, debido a que el software malintencionado puede realizar consultas de DNS mediante uno o ambos protocolos. La dirección de sinkhole de DNS debe estar una zona distinta de la de los hosts de cliente para garantizar que, cuando un host infectado intentar iniciar una sesión con la dirección IP de sinkhole, se enrutará a través del cortafuegos.

Las direcciones de sinkhole se deben reservar con este fin y no es necesario asignarlas a un host físico. Además, puede utilizar un servidor honey-pot (trampa) como host físico para analizar más detenidamente el tráfico malintencionado.

Para los siguientes pasos de configuración, se utilizan las siguientes direcciones de sinkhole de DNS de ejemplo:

Dirección de sinkhole de DNS IPv4: 10.15.0.20

Dirección de sinkhole de DNS IPv6: fd97:3dec:4d27:e37c:5:5:5:5

STEP 1 | Configure la interfaz de sinkhole y la zona.

El tráfico de la zona en la que se encuentran los hosts de cliente se debe enrutar a la zona en la que se ha definido la dirección IP de sinkhole para que se registre el tráfico.

Utilice una zona específica para el tráfico de sinkhole, ya que el host infectado enviará tráfico a esta zona.

1. Seleccione **Network (Red)** > **Interfaces** y seleccione una interfaz para configurar como su interfaz de sinkhole.
2. En la lista desplegable **Tipo de interfaz**, seleccione **Capa3**.
3. Para añadir una dirección IPv4, seleccione la pestaña **IPv4**, seleccione **Static (Estático)** y, a continuación, haga clic en **Add (Añadir)**. En este ejemplo, añada 10.15.0.20 como la dirección IPv4 de DNS sinkhole.

4. Seleccione la pestaña **IPv6**, haga clic en **Static (Estático)** y, a continuación, haga clic en **Add (Añadir)** y especifique una dirección IPv6 y una máscara de subred. En este ejemplo, fd97:3dec:4d27:e37c::/64 es la dirección de sinkhole IPv6.
5. Haga clic en **OK (Aceptar)** para guardar.
6. Para añadir una zona para el sinkhole, seleccione **Network (Red)** > **Zones (Zonas)** y haga clic en **Add (Añadir)**.
7. Especifique un **Name (Nombre)** para la zona.
8. En la lista desplegable **Type (Tipo)**, seleccione **Layer3**.
9. En la sección **Interfaces**, haga clic en **Añadir** y añada la interfaz que ha configurado.
10. Haga clic en **OK (Aceptar)**.

STEP 2 | Habilite el sinkholing DNS.

Por defecto, el sinkholing está habilitado para todas las firmas DNS de Palo Alto Networks. Para cambiar la dirección de sumidero a su servidor local, consulte el Paso 2 en Configurar sinkholing de DNS para una lista de dominios personalizados.

STEP 3 | Edite la regla de la política de seguridad que permite el tráfico de los hosts de cliente de la zona fiable a la zona no fiable para incluir la zona de sinkhole como un destino y adjuntar el perfil de antispyware.

La modificación de las reglas de política de seguridad que permiten el tráfico desde hosts clientes en la zona fiable hacia la zona no fiable garantiza la identificación del tráfico de hosts infectados. Al añadir la zona de sinkhole como un destino en la regla, permite que los clientes infectados envíen consultas de DNS falsas al sinkhole de DNS.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)**.
2. Seleccione una regla existente que permita el tráfico de la zona del host de cliente a la zona que no es de confianza.
3. En la pestaña **Destination (Destino)**, seleccione **Add (Añadir)** para añadir la zona de sinkhole. Esto permite que el tráfico del host de cliente fluya hasta la zona de sinkhole.
4. En la pestaña **Actions**, seleccione la casilla de verificación **Log at Session Start** para habilitar el registro de logs. De este modo, garantiza que el tráfico de los hosts de cliente de la zona de confianza se registre al acceder a las zonas que no son de confianza o de sinkhole.
5. En la sección **Profile Setting (Ajuste de perfil)**, seleccione el perfil de **Antispyware** en el que ha habilitado el sinkholing de DNS.
6. Haga clic en **OK (Aceptar)** para guardar la regla de política de seguridad y, a continuación, en **Commit (Confirmar)**.

STEP 4 | Para confirmar que podrá identificar los hosts infectados, compruebe si el tráfico desde el host cliente de la zona de confianza hasta la nueva zona de sinkhole se está registrando.

En este ejemplo, el cliente de host infectado es 192.168.2.10 y la dirección IPv4 de sinkhole es 10.15.0.20.

1. En un host de cliente de la zona de confianza, abra un símbolo del sistema y ejecute el siguiente comando:

   ```
   C:\>ping <sinkhole address>
   ```

   La salida del siguiente ejemplo muestra la solicitud de ping a la dirección de sinkhole de DNS en 10.15.0.2 y el resultado, que es `Request timed out` debido a que en este ejemplo la dirección IP de sinkhole no se ha asignado a un host físico:

   ```
   C:\>ping 10.15.0.20 Pinging 10.15.0.20 with 32 bytes of data:
    Request timed out. Request timed out. Ping statistics for
    10.15.0.20: Packets: Sent = 4, Received = 0, Lost = 4 (100%
    loss)
   ```

2. En el cortafuegos, seleccione **Monitor (Supervisar)** > **Logs** > **Traffic (Tráfico)** y encuentre la entrada de log con el origen 192.168.2.10 y el destino 10.15.0.20. Esto confirma que el tráfico para la dirección IP de sinkhole atraviesa las zonas del cortafuegos.

   *Puede buscar o filtrar los logs y mostrar solo los logs con el destino 10.15.0.20. Para ello, haga clic en la dirección IP (10.15.0.20) en la columna **Destination (Destino)**, lo que añadirá el filtro (addr.dst en 10.15.0.20) al campo de búsqueda. Haga clic en el icono Aplicar filtro a la derecha del campo de búsqueda para aplicar el filtro.*

STEP 5 | Compruebe que el sinkholing de DNS esté configurado correctamente.

Está simulando la acción que un host cliente infectado realizaría cuando una aplicación malintencionada intenta una notificación de instalación.

1. Detecte un dominio malintencionado que esté incluido en la base de datos de firmas de antivirus actual del cortafuegos para comprobar el sinkholing.

   1. Seleccione **Device (Dispositivo)** > **Dynamic (Dinámico) Updates (Actualizaciones)** y en la sección **Antivirus**, haga clic en el enlace **Release Notes (Notas de versión)** para la base de datos de antivirus instalada actualmente. También puede buscar las notas de versión del antivirus que enumeran las actualizaciones de firma incrementales en la sección de actualizaciones dinámicas del sitio de asistencia técnica de Palo Alto Networks.
   2. En la segunda columna de las notas de la versión, busque un elemento de línea con una extensión de dominio (por ejemplo, com, edu o net). En la columna de la izquierda se muestra el nombre del dominio. Por ejemplo, en la versión de antivirus 1117-1560,

hay un elemento en la columna de la izquierda llamado "tbsbana" y en la columna de la derecha se muestra "net".

A continuación se muestra el contenido de las notas de la versión para este elemento de línea:

```
conficker:tbsbana 1 variants: net
```

2. En el host de cliente, abra un símbolo del sistema.
3. Realice la acción NSLOOKUP para una dirección URL identificada como un dominio malintencionado conocido.

   Por ejemplo, si se usa la dirección URL `track.bidtrk.com`:

```
C:\>nslookup track.bidtrk.com Server: my-local-
dns.local Address: 10.0.0.222 Non-authoritative
 answer: Name: track.bidtrk.com.org Addresses:
 fd97:3dec:4d27:e37c:5:5:5:510.15.0.20
```

   En la salida, observe que la acción NSLOOKUP para el dominio malintencionado se ha falsificado mediante las direcciones IP de sinkhole que configuramos (10.15.0.20). Dado que el dominio coincide con una firma DNS malintencionada, se realiza la acción sinkhole.
4. Seleccione **Monitor (Supervisar)** > **Logs** > **Threat (Amenaza)** y busque la entrada de log de amenaza correspondiente para comprobar si se ha realizado la acción correcta en la solicitud NSLOOKUP.
5. Haga ping a **`track.bidtrk.com`**, lo que genera tráfico de red para la dirección de sinkhole.

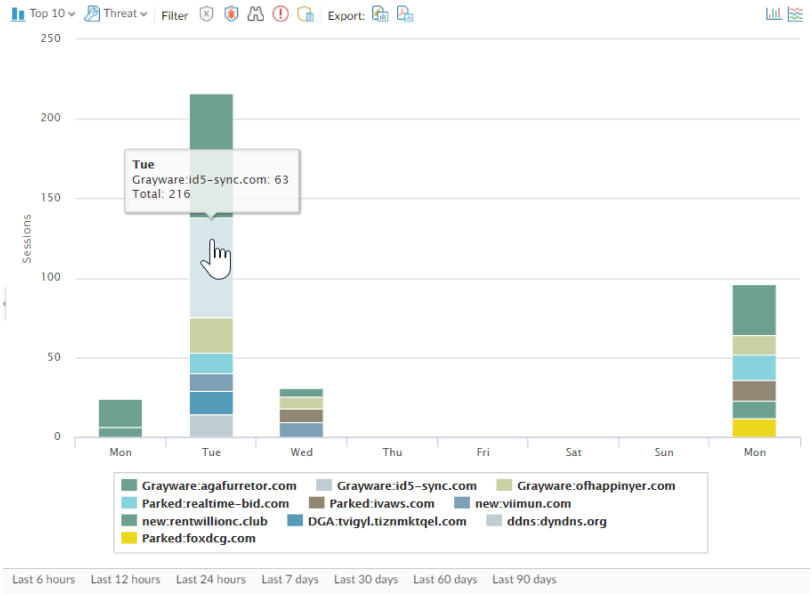
Consulta de hosts infectados que intentan conectar a dominios malintencionados

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	☐ Licencia de Advanced Threat Prevention (para un mejor soporte de funciones) o Threat Prevention

Después de configurar la función de sinkholing de DNS y comprobar si el tráfico para un dominio malintencionado se dirige a la dirección de sinkhole, debe supervisar regularmente el tráfico para la dirección de sinkhole para poder hacer un seguimiento de los hosts infectados y eliminar la amenaza.

- Utilice Appscope para identificar los hosts de cliente infectados.
  1. Seleccione **Monitor (Supervisar)** > **App Scope** y seleccione **Threat Monitor (Supervisor de amenazas)**.
  2. Haga clic en el botón **Mostrar spyware** de la parte superior de la página mostrada.
  3. Seleccione un intervalo de tiempo.

     En la siguiente captura de pantalla se muestran tres casos de consultas de DNS sospechosas, generadas cuando el host de cliente de prueba realizó una acción NSLOOKUP en un dominio malintencionado conocido. Haga clic en el gráfico para ver más detalles del evento.



- Configure un informe personalizado para identificar todos los hosts de cliente que envían tráfico a la dirección IP de sinkhole, que es 10.15.0.20 en este ejemplo.

  Reenvíe la información a un gestor de SNMP, a un servidor Syslog o a Panorama para habilitar las alertas para estos eventos.

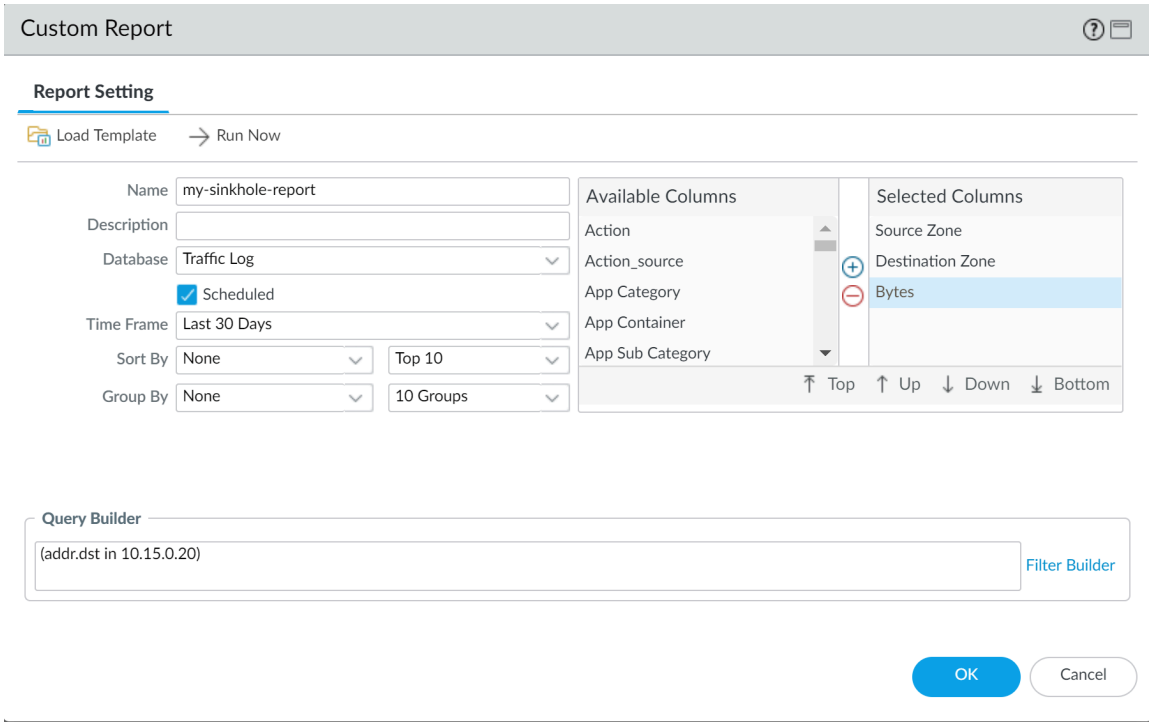
  En este ejemplo, el host de cliente infectado realiza una acción NSLOOKUP para un dominio malintencionado conocido incluido en la base de datos de firmas DNS de Palo Alto Networks. A continuación, la consulta se envía al servidor DNS local, el cual reenvía la solicitud a través del cortafuegos a un servidor DNS externo. La política de seguridad del cortafuegos con el perfil de antispyware configurado coincide con la consulta enviada a la base de datos de firmas DNS, la cual falsifica a continuación la respuesta mediante la dirección de sinkhole de 10.15.0.20 y fd97:3dec:4d27:e37c:5:5:5:5. El cliente intenta iniciar una sesión y el log de tráfico registra la actividad con el host de origen y la dirección de destino, que ahora se dirige a la dirección de sinkhole falsa.

  La visualización del log de tráfico en el cortafuegos permite identificar cualquier host de cliente que envíe tráfico a la dirección de sinkhole. En este ejemplo, los logs muestran que la dirección de origen 192.168.2.10 ha enviado la consulta de DNS malintencionada. A continuación, el host se puede buscar y limpiar. Sin la opción de sinkhole de DNS, el administrador solo vería el servidor DNS local como el sistema que ha realizado la consulta y no vería el host de cliente

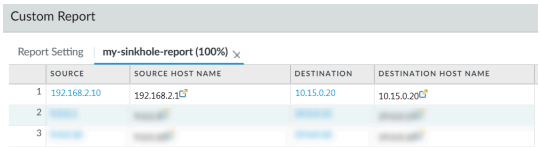
infectado. Si intenta ejecutar un informe en el log de amenazas mediante la acción “sinkhole”, el log muestra el servidor DNS local, pero no el host infectado.

1. Seleccione **Monitor (Supervisar)** > **Manage Custom Reports (Gestionar informes personalizados)**.
2. Haga clic en **Add (Añadir)** y asigne un **Name (Nombre)** al informe.
3. Defina un informe personalizado que capture el tráfico para la dirección de sinkhole del modo siguiente:
   - **Base de datos**: seleccione **Registro de tráfico**.
   - **Scheduled (Programado)**: habilite **Scheduled (Programado)** para que el informe se ejecute cada noche.
   - **Período de tiempo**: 30 días.
   - **Selected Columns (Columnas seleccionadas)**: seleccione **Source address (Dirección de origen)** o **Source User (Usuario de origen)** (si ha configurado User-ID) para identificar el host de cliente infectado en el informe y seleccione **Destination address (Dirección de destino)**, la cual será la dirección de sinkhole.
   - En la sección de la parte inferior de la pantalla, cree una consulta personalizada para el tráfico de la dirección de sinkhole (10.15.0.20 en este ejemplo). Puede especificar la dirección de destino en la ventana **Query Builder (Generador de consultas)** (**addr.dst en 10.15.0.20**) o seleccionar lo siguiente en cada columna y hacer clic en **Add**

(Añadir): Connector = and, Attribute = Destination Address, Operator = in y Value = 10.15.0.20. Haga clic en **Add (Añadir)** para añadir la consulta.



4. Haga clic en **Run Now (Ejecutar ahora)** para ejecutar el informe. El informe muestra todos los hosts de cliente que han enviado tráfico a la dirección de sinkhole, lo que indica que es probable que estén infectados. A continuación, puede hacer un seguimiento de los hosts y comprobarlos para detectar spyware.



5. Para ver los informes programados que se han ejecutado, seleccione **Monitor (Supervisar)** > **Reports (Informes)**.

Firmas personalizadas

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia de Advanced Threat Prevention (para un mejor soporte de funciones) o Threat Prevention

Puede crear firmas de amenazas personalizadas para detectar y bloquear tráfico específico. Cuando un servidor de gestión Panorama es el encargado de administrar el cortafuegos, el ThreatID se asigna a la amenaza personalizada correspondiente en el cortafuegos para permitir que este genere un log de amenazas con el ThreatID personalizado configurado. Visite nuestra guía para obtener más información sobre las firmas de amenazas y aplicaciones personalizadas.

Supervisar Advanced Threat Prevention

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia de Advanced Threat Prevention (para un mejor soporte de funciones) o Threat Prevention

Palo Alto Networks ofrece varias opciones para supervisar la actividad procesada por Advanced Threat Prevention para acomodar la recuperación de información para una gama de productos que dependen de Advanced Threat Prevention y los datos asociados. Dependiendo de la plataforma del producto, es posible acceder a paneles de alto nivel que también proporcionan estadísticas de solicitud de DNS y tendencias de uso, incluido el contexto en la actividad de red, y detalles de solicitudes de DNS de usuarios específicos.

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

Para obtener una vista de alto nivel de la actividad de la red, puede ver el panel que proporciona visibilidad de los datos generales de gestión de amenazas de la red, así como de varias tendencias DNS. Cada tarjeta de panel proporciona una vista única del impacto de una amenaza en su red, en un formato de informe gráfico. Esto proporciona una visión general de las entidades más afectadas por las amenazas, según la aplicación, el usuario y qué reglas de seguridad están hacen cumplir las políticas de su organización.

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

- Centro de control de Strata Cloud Manager
- Ver Logs de amenazas
- Ver informe de Advanced Threat Prevention
- Supervisión de direcciones IP bloqueadas
- Más información sobre las firmas de amenazas
- Crear informes personalizados basados en categorías de amenazas

Ver Logs de amenazas

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia de Advanced Threat Prevention (para un mejor soporte de funciones) o Threat Prevention

Las categorías de amenazas clasifican los diferentes tipos de firmas de amenazas para ayudarle a comprender y establecer conexiones entre los eventos que detectan las firmas de amenazas. Las categorías de amenazas son subconjuntos de tipos de firmas de amenazas más amplios: spyware, vulnerabilidad y antivirus. Las entradas de log de amenazas muestran la **categoría de amenaza** de cada evento registrado.

Puede explorar, buscar y visualizar los logs de Advanced Threat Prevention que se generan automáticamente cuando se detecta una amenaza. Por lo general, esto incluye cualquier coincidencia de firma de amenaza cualificada que una característica de prevención de amenazas, incluido el aprendizaje automático en línea, analiza a menos que esté configurada específicamente con un nivel de gravedad de log de ninguno. Las entradas de log proporcionan numerosos detalles sobre el evento, incluido el nivel de amenaza y, si corresponde, la naturaleza de la amenaza.

- Strata Cloud Manager
- PAN-OS y Panorama

Ver Logs de amenazas (Cloud Management)

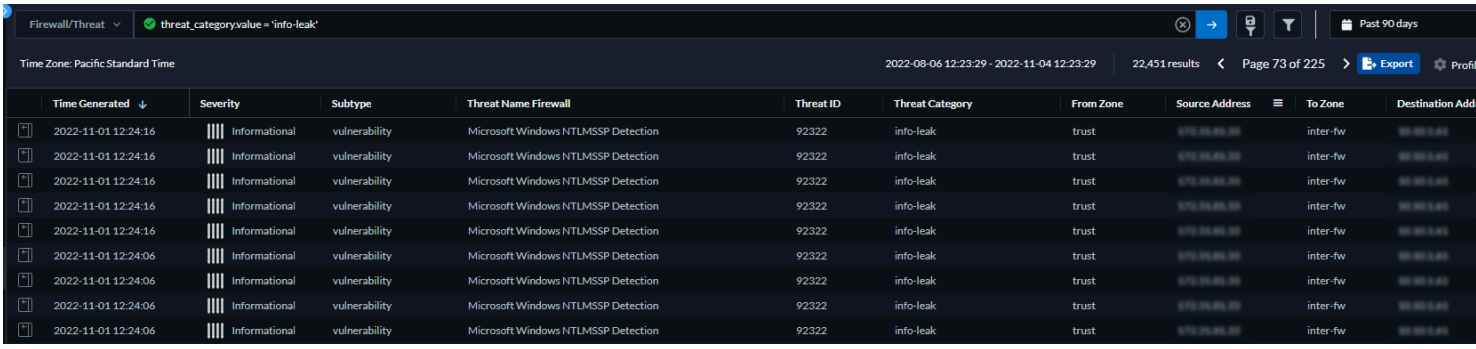
STEP 1 | Utilice las credenciales asociadas con su cuenta de asistencia técnica de Palo Alto Networks e inicie sesión en Strata Cloud Manager en el hub.

> *Para obtener más información sobre el uso de los paneles de Activity (Actividad), consulte el Visor de logs.*

STEP 2 | Filtre los logs de amenazas en función de la **Threat Category (Categoría de amenaza)** o el **Subtype (Subtipo)** en Prisma Access.

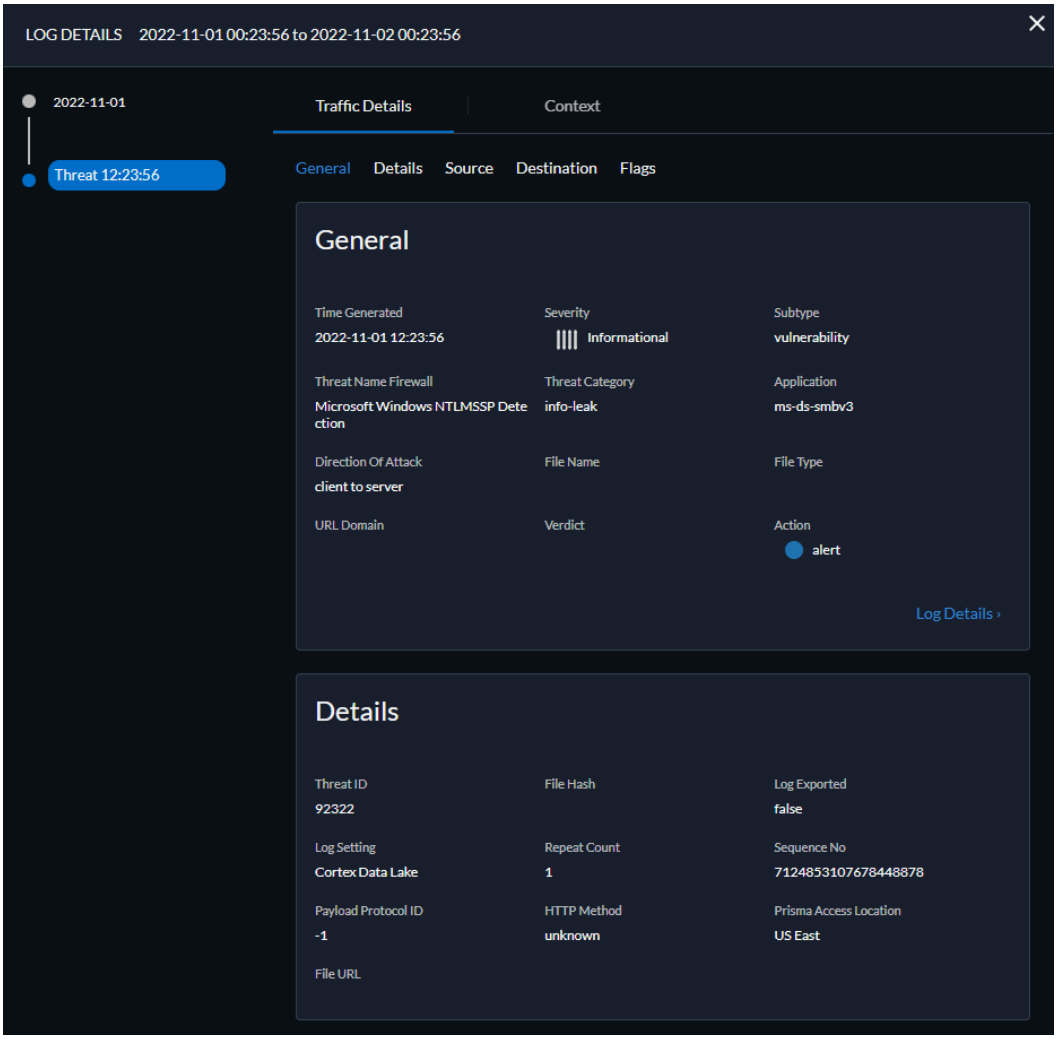
1. Seleccione **Incidents & Alerts (Incidentes y alertas)** > **Log Viewer (Visor de logs)**.
2. Cambie el tipo de log que se buscará a **Threat (Amenaza)**.
3. Cree un filtro de búsqueda mediante uno de los subtipos de firma de amenazas utilizados por los perfiles de antivirus, antispyware o protección frente a vulnerabilidades [**antivirus**, **spyware**y **vulnerability (vulnerabilidad)** respectivamente] o en función de la categoría de amenazas mediante el generador de consultas. Por ejemplo, puede usar `sub_type.valor = 'spyware'` para ver los logs de amenazas que se han

determinado como spyware. Para buscar otros subtipos, reemplace el spyware del ejemplo anterior por otro subtipo compatible [**vulnerability (vulnerabilidad)** o **spyware**]. También puede buscar en función de un **Threat Category (Categoría de amenaza)**, como una vulnerabilidad de fuga de información mediante la siguiente consulta `threat_category.value = 'info-leak'`. Para obtener una lista de las categorías válidas que puede utilizar, consulte Categorías de firma de amenazas. Ajuste los criterios de búsqueda según sea necesario para su búsqueda, incluidos parámetros de consulta adicionales (como el nivel de gravedad y la acción) junto con un rango de fechas.



4. Ejecute la consulta una vez que haya terminado de ensamblar sus filtros.

5. Seleccione una entrada de registro de los resultados para ver los detalles del registro.



6. La **Category (Categoría)** de amenaza se muestra en el panel **Details (Detalles)** de la vista de log detallada. Otros detalles relevantes sobre la amenaza se muestran en sus correspondientes ventanas.

STEP 3 | Filtrar los logs de amenazas por [categorías] de amenazas que se han detectado mediante el análisis en línea en la nube (spyware).

> *El tráfico C2 basado en HTTP que originalmente se clasificó con el nombre de amenaza Detección de tráfico de comando y control HTTP analizado en línea en la nube y está asociado con varios ID de amenazas, ahora está separado en tres nombres de amenazas únicos que se corresponden con las identificaciones de amenazas únicas y describen con mayor precisión las detecciones realizadas por Advanced Threat Prevention:* ***Detección de tráfico HTTP C2 evasivo*** *(ID de amenaza: 89950),* ***Detección de tráfico Cobalt Strike C2 evasivo*** *(ID de amenaza: 89955, 89956 y 89957) y* ***Detección de tráfico Empire C2 evasivo*** *(ID de amenaza: 89958).*
>
> *Los logs de tráfico C2 basados en HTTP generados antes del 11 de diciembre de 2023 seguirán clasificándose con el nombre de amenaza Detección de tráfico de comando y control HTTP analizado en línea en la nube.*

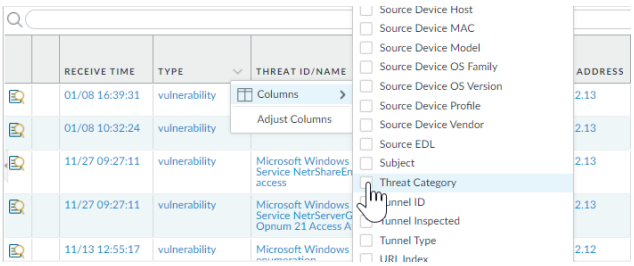
1. Seleccione **Incidents & Alerts (Incidentes y alertas)** > **Log Viewer (Visor de logs)**.
2. Cambie el tipo de log que se buscará a **Threat (Amenaza)**.
3. Cree un filtro de búsqueda utilizando una categoría de amenaza utilizada exclusivamente por Análisis en línea en la nube (spyware): `threat_category.valor = 'inline-cloud-c2'`. Puede restringir aún más la búsqueda haciendo una referencia cruzada de un valor de Threat-ID que corresponda a un tipo de C2 específico. Por ejemplo `threat_category.value = 'inline-cloud-c2' Y Threat ID = 89958`, donde 89958 indica el ID de amenaza del tráfico empire C2 evasivo.
4. Seleccione una entrada de log para ver los detalles de una amenaza C2 detectada.
5. La **Category (Categoría)** de amenaza se muestra en el panel **General** de los detalles del log. Las amenazas C2 que se han detectado mediante el análisis en línea de la nube tienen una categoría de amenaza de inline-cloud-c2. Puede hacer una referencia cruzada del valor de **ID** de amenazas en el panel **Details (Detalles)** para determinar el tipo específico de C2 que se ha detectado.

STEP 4 | Filtre los logs de amenazas por [categorías] de amenazas que se han detectado mediante el análisis en línea en la nube (vulnerabilidad).

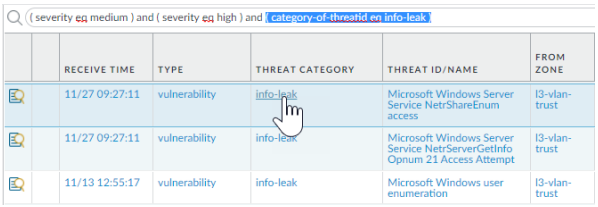
1. Seleccione **Incidents & Alerts (Incidentes y alertas)** > **Log Viewer (Visor de logs)**.
2. Cambie el tipo de log que se buscará a **Threat (Amenaza)**.
3. Cree un filtro de búsqueda utilizando una categoría de amenaza utilizada exclusivamente por el Análisis en línea en la nube (vulnerabilidad): `threat_category.valor = 'exploit-en-línea-de-nube'`.
4. Seleccione una entrada de log para ver los detalles de las vulnerabilidades detectadas de inyección de comandos e inyección de SQL. Las amenazas de exploits en línea (inyección SQL) tienen un ID de 99950, mientras que las amenazas de exploits en línea (inyección de comandos) tienen un ID de 99951.

Ver Logs de amenazas (NGFW (Managed by PAN-OS or Panorama))

- Filtre los logs de amenaza por categoría de amenaza.
  1. Select **Monitor (Supervisar)** > **Logs** > **Threat (Amenaza)**.
  2. Añada la columna Threat Category (Categoría de amenaza) para ver la categoría de amenaza de cada entrada de log:



  3. Para implementar un filtro en función de la categoría de amenaza:
     - Utilice el generador de consultas de log para añadir un filtro con la categoría de amenaza **Attribute (Atributo)** y en el campo **Value (Valor)**, introduzca una categoría de amenaza.
     - Seleccione la categoría de amenaza de cualquier entrada del log para añadir esa categoría al filtro:



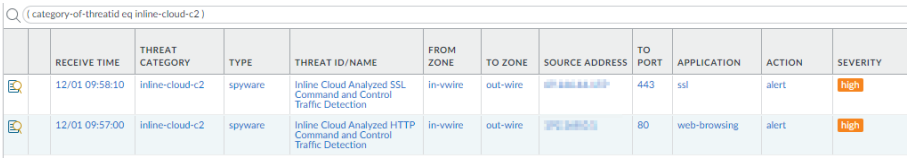
- Filtrar logs de amenazas por tipo de firma de amenaza.
  1. Select **Monitor (Supervisar)** > **Logs** > **Threat (Amenaza)**.
  2. Añada la columna **Type (Tipo)**, si no está presente, para que pueda ver la categoría de firma de amenaza para cada entrada de log:
  3. Para filtrar según el tipo de firma:
     - Utilice el generador de consultas de log para añadir un filtro con el **Attribute (Atributo)** de la categoría de firma de amenaza y, en el campo **Value (Valor)**, introduzca un tipo de firma de amenaza. Puede seleccionar entre **vulnerability (vulnerabilidad)**, **virus** y **spyware**, que corresponden a las firmas gestionas por sus perfiles de seguridad de Protección frente a vulnerabilidades, antivirus y antispyware.
     - Seleccione el **Type (Tipo)** de cualquier entrada de log para añadir ese tipo de firma de amenaza al filtro. También puede crear manualmente su consulta utilizando el filtro y el tipo de firma de amenaza.

- Filtrar los logs de amenazas por [categorías] de amenazas que se han detectado mediante el análisis en línea en la nube (spyware).

  El tráfico C2 basado en HTTP que originalmente se clasificó con el nombre de amenaza Detección de tráfico de comando y control HTTP analizado en línea en la nube y está asociado con varios ID de amenazas, ahora está separado en tres nombres de amenazas únicos que se corresponden con las identificaciones de amenazas únicas y describen con mayor precisión las detecciones realizadas por Advanced Threat Prevention: ***Detección de tráfico HTTP C2 evasivo*** *(ID de amenaza: 89950),* ***Detección de tráfico Cobalt Strike C2 evasivo*** *(ID de amenaza: 89955, 89956 y 89957) y* ***Detección de tráfico Empire C2 evasivo*** *(ID de amenaza: 89958).*

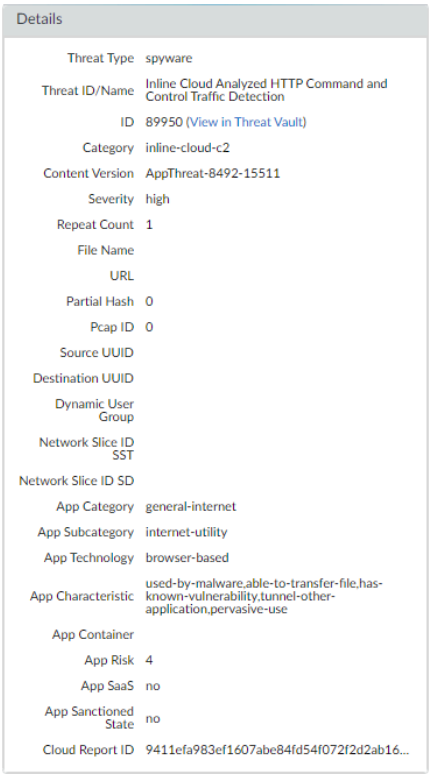
  Si no instala el contenido de actualización o está revisando los logs de tráfico C2 basados en HTTP generados antes del 11 de diciembre de 2023 (la fecha de lanzamiento de la actualización de contenido), todo el tráfico C2 basado en HTTP seguirá estando clasificado con el nombre de la amenaza Detección de tráfico HTTP de comando y control en línea en la nube.

  1. Seleccione **Monitor (Supervisar)** > **Logs (Logs)** > **Threat (Amenaza)**. Puede filtrar los logs según determinadas características de la amenaza. Considere los siguientes ejemplos:
     - Filtre utilizando `( category-of-threatid eq inline-cloud-c2 )` para ver los logs de amenazas C2 que se han analizado utilizando el mecanismo de análisis en línea em la nube de Advanced Threat Prevention.
     - Puede restringir aún más la búsqueda haciendo una referencia cruzada de un valor de Threat-ID que corresponda a un tipo de C2 específico. Por ejemplo, `(categoría-de-amenaza eq inline-cloud-c2) y (nombre-de-amenaza eq 89958)`, donde 89958 indica el ID de amenaza del tráfico empire C2 evasivo.
     - Filtre usando `(local_deep_learning eq yes)` para ver los logs de amenazas que se han analizado mediante el mecanismo de análisis profundo local de Advanced Threat Prevention.

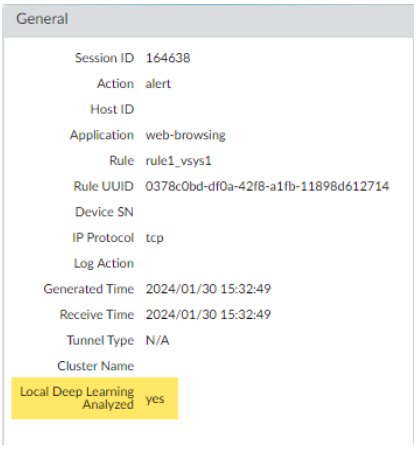
     

  2. Seleccione una entrada de log para ver los detalles de una amenaza C2 detectada.
  3. La **categoría** de amenaza se muestra en el panel **Details (Detalles)** de la vista de log detallada. Las amenazas C2 que se han detectado mediante el análisis en línea de la nube tienen una categoría de amenaza de inline-cloud-c2. Puede hacer una referencia

cruzada del valor de **ID** de amenazas para determinar el tipo específico de C2 que se ha detectado.

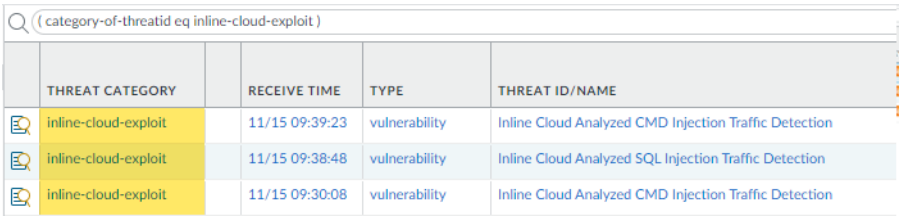


4. Si la amenaza se analizó utilizando aprendizaje profundo local, el campo **Local Deep Learning Analyzed (Aprendizaje profundo local analizado)** indica sí.

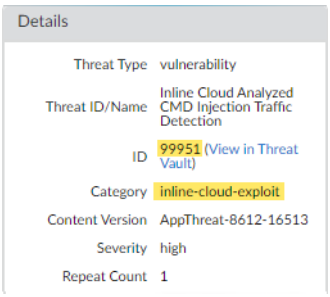


- Supervisar la actividad en el cortafuegos para detectar vulnerabilidades que se hayan detectado mediante el análisis en línea en la nube (vulnerabilidad).
  1. Seleccione **Monitor (Supervisar)** > **Logs (Logs)** > **Threat (Amenaza)** y filtre por `( category-of-threatid eq inline-cloud-exploit )` para ver los logs que se han analizado mediante el mecanismo de análisis en línea en la nube de Advanced Threat Prevention. Las amenazas de exploits en línea (inyección SQL) tienen un ID de

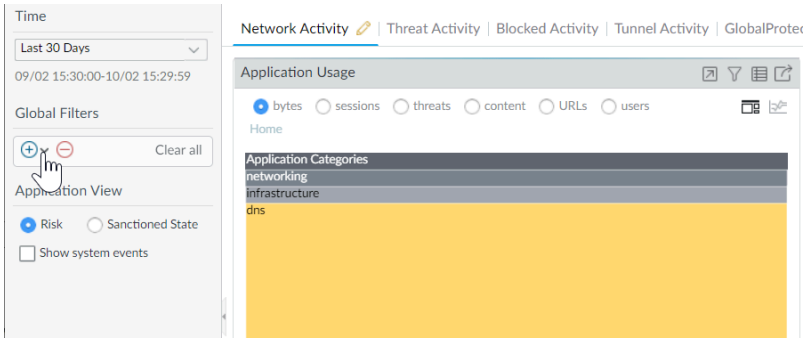
99950, mientras que las amenazas de exploits en línea (inyección de comandos) tienen un ID de 99951.



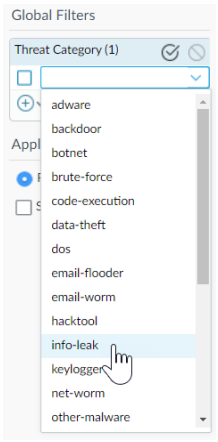
2. Seleccione una entrada de log para ver los detalles de un exploit de vulnerabilidad.
3. La **categoría** de amenaza se muestra en el panel **Details (Detalles)** de la vista de log detallada. Los exploits de vulnerabilidades que se han detectado mediante el análisis en línea en la nube tienen una categoría de amenaza de inline-cloud-exploit.



- Filtre la actividad del ACC por categoría de amenaza.
  1. Seleccione **ACC** y añada una categoría de amenaza como filtro global:



  2. Seleccione la categoría de amenaza que se utilizará para filtrar todas las pestañas de ACC.



Ver informe de Advanced Threat Prevention

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia de Advanced Threat Prevention (para un mejor soporte de funciones) o Threat Prevention

El Informe de Advanced Threat Prevention está disponible a través de la API de Threat Vault y proporciona información detallada de análisis y detección, así como información sobre la transacción, la sesión y otros procesos relacionados. El informe contiene parte o toda la información descrita en la siguiente tabla según la información de la sesión configurada en el cortafuegos que procesó el archivo y los detalles del análisis del archivo en formato JSON.

Los NGFW no tienen acceso directo a los informes a través de PAN-OS; en su lugar, debe hacer referencia al cloud_reportid asociado con el log de amenazas y usar la API de Threat Vault para buscar y recuperar el informe.

*Para Prisma Access (a través del Strata Cloud Manager), el informe se puede ver desde el visor de logs (Ver Logs de amenazas). Las entradas de log con un informe de Advanced Threat Prevention generado tienen un enlace de descarga junto al valor de ID del informe debajo de la columna **Cloud ReportID**.*

Encabezado del informe	Description (Descripción)
Información general	Contiene información sobre la plataforma de seguridad/ cortafuegos que procesó la amenaza. • El número de identificación del informe en la nube que contiene los datos del informe de Advanced Threat. • Mensajes de error que podrían haberse generado durante la creación del informe.
Información sobre PAN-OS	Contiene información sobre la plataforma de seguridad/ cortafuegos que procesó la amenaza. • Interfaz del cortafuegos (IPv4/IPv6) • Versión del paquete de contenido • Nombre de host de cortafuegos

Encabezado del informe	Description (Descripción)
	• Modelo de cortafuegos: • Número de serie • Versión de PAN-OS
Session information (Información de la sesión)	Contiene información de la sesión basada en el tráfico a medida que atravesó el cortafuegos/plataforma de seguridad que reenvió la amenaza. Las siguientes opciones están disponibles: • IP de origen • Puerto de origen • IP de destino • Puerto de destino • Session ID (ID de sesión) • Marca de tiempo de la sesión • Tipo de carga útil
Datos de la transacción	Los datos de la transacción proporcionan una descripción general de los detalles de la carga útil y contienen el o los informes del servicio de detección. Las siguientes opciones están disponibles: • ID de transacción • Hash SHA256 de la carga útil
Resultados del servicio de detección	Cuando el análisis de amenazas lo realiza la nube de Advanced Threat Prevention, esta sección contiene entradas que muestran los resultados del análisis. Esto incluye los informes del servicio de detección, que además proporcionan las técnicas clasificadas de MITRE ATT&CK® empleadas, así como los detalles de la carga útil. Las detecciones de comando y control para el marco Empire C2 muestran información contextual adicional. Esto incluye informes generados tanto en la fase de preparación como en la de comando (posterior a la vulneración) de un ataque que ocurre en sesiones separadas. Las siguientes entradas de información están disponibles: • Descripción del ataque: describe la naturaleza del ataque C2. • Detalles del ataque: indica la fase del ataque Empire C2 y describe los intercambios entre el servidor y el cliente.

Encabezado del informe	Description (Descripción)
	• Evidencias de ataque: enumera comportamientos y acciones coherentes con el conocido Empire C2. *El C2 basado en Empire se detecta utilizando un detector de submódulo incluido en el motor de análisis **Detección de tráfico de comando y control HTTP analizado en línea en la nube** con un ID de amenaza único de 89958.*

Supervisión de direcciones IP bloqueadas

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia de Advanced Threat Prevention (para un mejor soporte de funciones) o Threat Prevention

El cortafuegos mantiene una lista de bloqueo de las direcciones IP de origen que está bloqueando. Cuando el cortafuegos bloquea una dirección IP de origen, tal como cuando configura alguna de las siguientes reglas de política, bloquea el tráfico en el hardware antes de que esos paquetes utilicen recursos de búfer de paquetes o CPU:

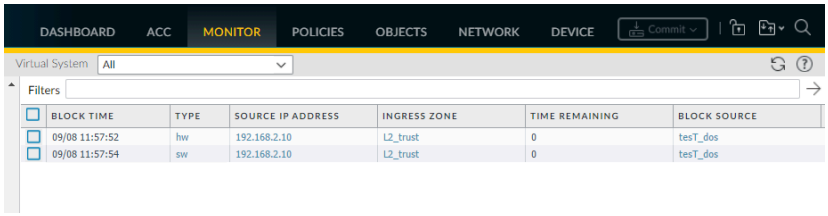
- Una regla de política de protección DoS clasificada con la acción de **Protect (Proteger)** (una política de protección DoS clasificada especifica que las conexiones entrantes coinciden con una dirección IP, dirección IP de destino o par de dirección IP de origen y destino, y está asociada con un perfil de protección DoS clasificado, según se describe en Protección DoS contra inundaciones de nuevas sesiones).
- Una regla de política de seguridad que utiliza un perfil de protección frente a vulnerabilidades.

El bloqueo de direcciones IP de hardware es compatible con los cortafuegos de las series PA-3200 Series, PA-5200 Series, PA-5400 Series (excepto PA-5450) y PA-7000 Series.

Puede ver la lista de bloqueo, obtener información detallada sobre una dirección IP en la lista de bloqueo o ver cuentas de direcciones que el hardware y software están bloqueando. Puede eliminar una dirección IP de la lista si considera que no deben bloquearse. Puede cambiar el origen de la información detallada sobre direcciones en la lista. También puede cambiar por cuánto tiempo el hardware bloqueará las direcciones IP.

- Visualice las entradas en la lista de bloqueo.
  1. Seleccione **Monitor (Supervisar)** > **Block IP List (Lista de bloqueo de IP)**.

     Las entradas en la lista de bloqueo indican en la columna Type (Tipo) si fueron bloqueadas por hardware (hw) o software (sw).
  2. Observe lo siguiente en la parte inferior de la pantalla:
     - Recuento de **Total Blocked IPs (IP totales bloqueadas)** en relación con el número de direcciones IP bloqueadas que admite el cortafuegos.
     - El porcentaje de la lista de bloqueo que ha usado el cortafuegos.
  3. Para filtrar las entradas mostradas, seleccione un valor en una columna (que crea un filtro en el campo **Filters [Filtros]**) y aplique el filtro (→). De lo contrario, el cortafuegos muestra las primeras 1000 entradas.
  4. Ingrese un número de **Page (Página)** o haga clic en las flechas en la parte inferior de la pantalla para avanzar en las páginas de entradas.
  5. Para ver detalles sobre una dirección en la lista de bloqueo, pase el ratón sobre una dirección IP de origen y haga clic en la flecha hacia abajo. Haga clic en el enlace **Who Is**, que muestra información de Network Solutions Who Is acerca de la dirección.



- Elimine entradas de la lista de bloqueo.

  Elimine una entrada si determina que no se debe bloquear la dirección IP. Luego, revise la regla de la política que ha provocado que el cortafuegos bloquee la dirección.

  1. Seleccione **Monitor (Supervisar)** > **Block IP List (Lista de bloqueo de IP)**.
  2. Seleccione una o más entradas y haga clic en **Delete (Eliminar)**.
  3. (Opcional) Seleccione **Clear All (Borrar todo)** para eliminar todas las entradas de la lista.

- Deshabilite o vuelva a habilitar el bloqueo de direcciones IP de hardware para fines de solución de problemas.

  Si bien el bloqueo de direcciones IP de hardware está deshabilitado, el cortafuegos continúa realizando el bloqueo de direcciones IP de software que usted ha configurado.

```
> set system setting hardware-acl-blocking [enable | disable]
```

  Para conservar los recursos de la CPU y del búfer de paquetes, deje habilitado el bloqueo de direcciones IP de hardware, a menos que el servicio técnico de Palo Alto Networks le pida que lo deshabilite, por ejemplo, si se va a depurar un flujo de tráfico.

- Ajuste la cantidad de segundos que las direcciones IP bloqueadas por el hardware permanecerán en la lista de bloqueo (el intervalo es de 1 a 3600; el valor predeterminado es 1).

```
> set system setting hardware-acl-blocking duration <seconds>
```

Mantenga una duración más breve para las entradas de lista de bloqueo de hardware que para las entradas de lista de bloqueo de software, a fin de reducir la probabilidad de superar la capacidad de bloqueo del hardware.

- Cambie el sitio web predeterminado para encontrar más información sobre una dirección IP de Network Solutions Who Is a otro sitio web.

```
# set deviceconfig system ip-address-lookup-url <url>
```

- Visualice los recuentos de direcciones IP bloqueadas por hardware y software; por ejemplo, para ver la tasa de ataques.

  Visualice la suma total de entradas de direcciones IP en la tabla de bloqueo de hardware y la lista de bloqueo (bloqueadas por hardware y software):

```
> show counter global name flow_dos_blk_num_entries
```

  Visualice el recuento de entradas de direcciones IP en la tabla de bloqueo de hardware que fueron bloqueadas por hardware:

```
> show counter global name flow_dos_blk_hw_entries
```

  Visualice el recuento de entradas de direcciones IP en la lista de bloqueo que fueron bloqueadas por software:

```
> show counter global name flow_dos_blk_sw_entries
```

- Visualice la información de la lista de bloqueo por ranura en un cortafuegos de la serie PA-7000.

```
> show dos-block-table software filter slot <slot-number>
```


Más información sobre las firmas de amenazas

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	☐ Licencia de Advanced Threat Prevention (para un mejor soporte de funciones) o Threat Prevention

Los logs de amenazas del cortafuegos registran todas las amenazas que el cortafuegos detecta en función de las firmas de amenazas (Configuración de antivirus, antispyware y protección frente a vulnerabilidades) y el ACC muestra una descripción general de las principales amenazas en su red. Cada evento que registra el cortafuegos incluye una ID que identifica la firma de amenaza asociada.

Puede utilizar el ID de amenazas encontrada con un log de amenaza o entrada de ACC para realizar las siguientes tareas:

- Compruebe de forma segura si una firma de amenazas se configuró como una excepción a su política de seguridad (Creación de excepciones de amenazas).
- Busque la información de Threat Vault más reciente sobre una amenaza específica. Debido a que Threat Vault está integrada con el cortafuegos, puede ver detalles de las amenazas directamente en el contexto del cortafuegos o iniciar una búsqueda de Threat Vault en una nueva ventana del explorador para detectar una amenaza registrada por el cortafuegos.

Si se deshabilita una firma, la firma UTID podría reutilizarse para una nueva firma.

Revise las notas de versión de la actualización de contenido para obtener notificaciones relacionadas con las firmas nuevas y deshabilitadas. Las firmas podrían deshabilitarse en los siguientes casos: la actividad que detecta la firma proviene de atacantes, la firma generó importantes falsos positivos o la firma se consolidó con otras firmas similares en una sola firma (optimización de la firma).

STEP 1 | Confirme que el cortafuegos está conectado a Threat Vault.

Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y edite la configuración **Logging and Reporting (Creación de logs e informes)** como **Enable Threat Vault Access (Habilitar el acceso a la cámara de amenazas)**. El acceso a Threat Vault se habilita de manera predeterminada.

STEP 2 | Busque el ID de amenazas de las amenazas que detecta el cortafuegos.

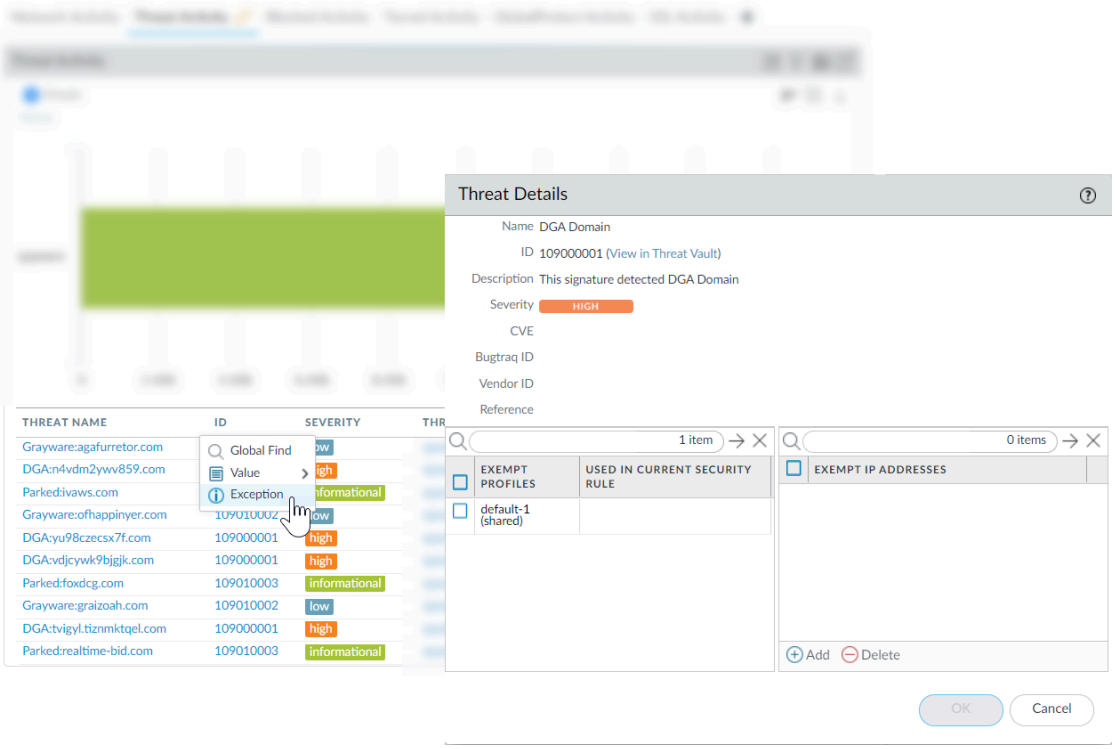
- Para ver cada evento de amenaza que detecta el cortafuegos basado en las firmas de amenazas, seleccione **Monitor (Supervisar)** > **Logs** > **Threat (Amenaza)**. Puede encontrar el ID de una entrada de amenaza de la columna ID o seleccionar la entrada de log para ver los detalles del log, que incluye el ID de amenaza.
- Para acceder a una descripción general de las amenazas principales de la red, seleccione **ACC** > **Threat Activity (Actividad de amenazas)** y observe el widget de Threat Activity

(Actividad de amenazas). La columna ID muestra el ID de amenazas de cada amenaza que se muestra.

- Para ver los detalles de las amenazas que puede configurar como excepciones de amenazas (es decir, el cortafuegos aplica la amenaza de manera diferente a la acción predeterminada definida para la firma de amenazas) seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Anti-Spyware/Vulnerability Protection (Antispyware/protección contra vulnerabilidades)**. Haga clic en **Add (Añadir)** para añadir un perfil o modifique uno existente, y haga clic en la pestaña **Exceptions (Excepciones)** para ver las excepciones configuradas. Si no se configuran excepciones, puede filtrar por firmas de amenazas o seleccione **Show all signatures (Mostrar todas las firmas)**.

STEP 3 | Coloque el cursor sobre un **Threat Name (Nombre de amenaza)** o el **ID** de amenazas para abrir el menú desplegable, y haga clic en **Exception (Excepción)** para revisar los detalles de la amenaza y cómo se configura el cortafuegos para aplicar la amenaza.

Por ejemplo, obtenga más información sobre una amenaza principal ilustrada en el ACC:



STEP 4 | Revise los **Threat Details (Detalles de amenaza)** más recientes de la amenaza e inicie una búsqueda de Threat Vault en función del ID de amenazas.

- Los detalles de amenazas que se muestran incluyen la información de Threat Vault más reciente para la amenaza, los recursos que puede utilizar para obtener más información sobre la amenaza y los CVE asociados a la amenaza.
- Seleccione **View in Threat Vault (Ver en Threat Vault)** para abrir una búsqueda Threat Vault en una nueva ventana del explorador y buscar la información más reciente que tiene la base de datos de amenazas de Palo Alto Networks para esta firma de amenazas.

STEP 5 | Compruebe si una firma de amenazas se configuró como una excepción de su política de seguridad.

- Si la columna **Used in current security rule (Utilizada en la regla de seguridad actual)** está vacía, el cortafuegos aplica la amenaza en función de la acción de la firma predeterminada recomendada (por ejemplo, bloquear o crear alerta).
- Una marca de verificación en la columna **Used in current security rule (Utilizada en la regla de seguridad actual)** indica que una regla de la política de seguridad se configuró para aplicar una acción no predeterminada a la amenaza (por ejemplo, permitir), en función de la configuración de **Exempt Profiles (Perfiles de exclusión)** asociada.

*La columna **Used in security rule (Utilizada en la regla de seguridad actual)** no indica si la regla de la política de seguridad está habilitada; solo indica si la regla de la política de seguridad se configuró con una exención de amenaza. Seleccione **Policies (Políticas)** > **Security (Seguridad)** para comprobar si una regla indicada de la política de seguridad está habilitada.*

STEP 6 | Haga clic en **Add (Añadir)** para añadir una dirección IP para filtrar la excepción de amenaza o ver las **Exempt IP Addresses (Direcciones IP exentas)** existentes.

Configure una dirección IP de exención para aplicar una excepción de amenaza solo cuando la sesión asociada cuente con una dirección IP de origen o de destino coincidente; en el caso de las otras sesiones, la amenaza se aplica en función de la acción de la firma predeterminada.

Crear informes personalizados basados en categorías de amenazas

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia de Advanced Threat Prevention (para un mejor soporte de funciones) o Threat Prevention

Puede crear informes personalizados en el cortafuegos para generar (a petición) o programar (cada noche) informes basados en atributos o elementos clave de información que desea recuperar y analizar.

- Cree informes personalizados basados en las categorías de amenazas para recibir información sobre tipos específicos de amenazas que detectó el cortafuegos.
  1. Seleccione **Monitor (Supervisar)** > **Manage Custom reports (Gestionar informes personalizados)** para añadir un nuevo informe personalizado o modificar uno existente.
  2. Seleccione la **Database (Base de datos)** que se utilizará como el origen del informe personalizado. En este caso, seleccione **Threat (Amenaza)** de cualquiera de los dos tipos de orígenes de la base de datos, base de datos de resumen y logs detallados. Los datos de la base de datos de resumen se resumen para permitir una respuesta más rápida cuando se generan informes. La generación de logs detallados requiere más tiempo, pero estos proporcionan un conjunto de datos detallados y completos de cada entrada del log.
  3. En el generador de consultas de log, añada un filtro de informes con el atributo **Threat Category (Categoría de amenaza)** y en el campo Value (Valor), seleccione una categoría de amenaza en la que se basará su informe.
  4. Para comprobar la configuración del nuevo informe, seleccione **Run now (Ejecutar ahora)**.
  5. Haga clic en **OK (Aceptar)** para guardar el informe.