paloalto
TECHDOCS

Política de seguridad recomendada de la puerta de enlace de Internet

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

July 24, 2023

Table of Contents

Práctica recomendada de política de seguridad de puerta de enlace de Internet

Una de las maneras más económicas y simples en las que un atacante obtiene acceso a su red es a través de usuarios que acceden a Internet. Al vulnerar con éxito un endpoint, un atacante puede ingresar a su red y moverse lateralmente hacia el objetivo final: robar el código fuente, filtrar los datos de los clientes o echar abajo la infraestructura. Para proteger su red contra los ciberataques y mejorar su postura de seguridad general, implemente una política de seguridad de puerta de enlace de Internet de prácticas recomendadas. Una política recomendada le permite habilitar de manera segura aplicaciones, usuarios y contenido al controlar todo el tráfico, en todos los puertos y en todo momento.

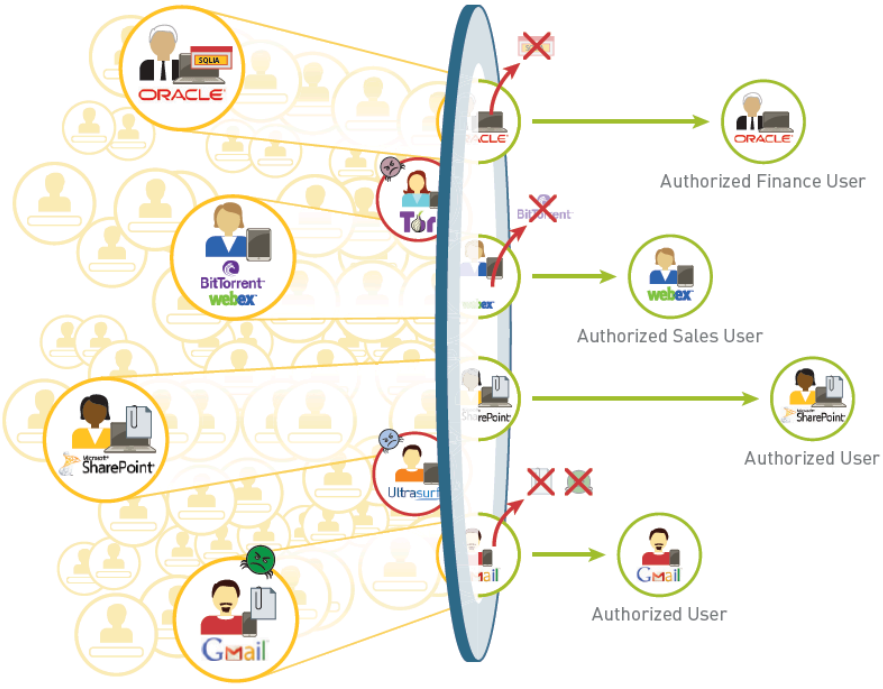
Consulte la serie de libros de prácticas recomendadas de Palo Alto Networks para obtener consejos sobre prácticas recomendadas en temas como descifrado, DoS y protección de zona (incluida la protección de búfer de paquetes) y mucho más.

¿Cuál es una política de seguridad de puerta de enlace de Internet de práctica recomendada?

Una política de seguridad recomendada para la puerta de enlace de Internet tiene dos objetivos principales de seguridad:

- **Minimizar la posibilidad de una intrusión:** a diferencia de las políticas de seguridad basadas en el puerto heredadas que bloquean todo en pos de la seguridad de la red o habilitan todo en pos del interés comercial, una política de seguridad basada en prácticas recomendadas aprovecha App-ID, User-ID, Content-ID y Device-ID (para IoT Security, que está más allá del alcance de este libro) para garantizar la habilitación segura de las aplicaciones en todos los puertos, para todos los usuarios, en todo momento, a la vez que simultáneamente analiza todo el tráfico para detectar amenazas conocidas y desconocidas.
- **Identificar la presencia de un atacante:** una política de seguridad de práctica recomendada para puerta de enlace de Internet brinda mecanismos integrados para ayudar a identificar brechas en la base de reglas y detectar actividad alarmante y posibles amenazas en la red.

Para lograr estos objetivos, una práctica recomendada de política de seguridad de puerta de enlace de Internet utiliza reglas basadas en la aplicación para permitir el acceso al usuario a aplicaciones específicas, analiza todo el tráfico para detectar y bloquear todas las amenazas conocidas, y envía los archivos desconocidos a WildFire para identificar nuevas amenazas y generar firmas para bloquearlas.



Las siguiente política de prácticas recomendadas garantizan la detección y prevención en varias etapas del ciclo de vida del ataque.

Metodología de prácticas recomendadas	¿Por qué es importante?
Inspección de todo el tráfico para lograr visibilidad	Debido a que no puede protegerse contra amenazas que no puede ver, asegúrese de tener una visibilidad total de todo el tráfico de todos los usuarios y aplicaciones en todo momento: • Implemente GlobalProtect para extender la plataforma de seguridad de última generación a los usuarios y dispositivos, independientemente de su ubicación. • Habilite el descifrado para que el cortafuegos pueda inspeccionar el tráfico cifrado (cada año, un mayor porcentaje del tráfico web empresarial está cifrado y más campañas de malware utilizan cifrado). • Habilite User-ID para asignar el tráfico de aplicaciones y las amenazas asociadas a usuarios/dispositivos y para permitir que la política siga a los usuarios dondequiera que vayan. • Si la política de la empresa permite dispositivos de los usuarios en la red (dispositivos personales [BYOD] o corporativos sin GlobalProtect u otras aplicaciones de gestión de seguridad), el control de acceso a dispositivos no gestionados en SaaS Security API permite a los usuarios acceder a sus aplicaciones SaaS en la nube desde dispositivos personales, desde cualquier ubicación, sin poner en riesgo de manera inadvertida sus datos u organización. El tráfico se redirige a través del cortafuegos para la aplicación de políticas y la prevención de amenazas. Con una visibilidad completa, el cortafuego podrá inspeccionar todo el tráfico —aplicaciones, amenazas y contenido— y asociarlo a los usuarios, independientemente de la ubicación o tipo de dispositivo, puerto, cifrado o técnicas evasivas empleadas, gracias a las tecnologías de App-ID, Content-ID y User-ID nativas. La visibilidad completa de las aplicaciones, el contenido y los usuarios de la red es el primer paso hacia un control de política informado.
Reducir la superficie de ataque	Después de obtener contexto sobre las aplicaciones, el contenido y los usuarios de la red, cree reglas de política de seguridad basadas en aplicaciones para permitir aplicaciones empresariales críticas y bloquear aplicaciones de alto riesgo que no tienen un caso de uso empresarial legítimo. Para reducir aún más la superficie de ataque, adjunte perfiles de bloqueo de archivos y filtrado de URL a todas las reglas que permiten el tráfico de aplicaciones, para impedir que los usuarios ingresen en sitios web propensos a amenazas y para evitar que carguen o descarguen tipos de archivos peligrosos (ya sea accidentalmente o a sabiendas). Para evitar que los atacantes ejecuten ataques de phishing con éxito, configure la prevención de phishing de credenciales.

Metodología de prácticas recomendadas	¿Por qué es importante?
Prevenir las amenazas conocidas	Adjunte perfiles de seguridad a todas las reglas de permisos para que el cortafuegos pueda detectar y bloquear vulnerabilidades de capa de red y aplicación, desbordamientos de búfer, ataques DoS, análisis de puertos y variantes de malware conocidas (incluidas las ocultas en archivos comprimidos o tráfico HTTP/HTTPS comprimido). Para habilitar la inspección de tráfico cifrado, habilite el descifrado. Además de las reglas de política de seguridad basadas en aplicaciones, cree reglas para bloquear direcciones IP malintencionadas conocidas sobre la base de la inteligencia contra amenazas de Palo Alto Networks y fuentes externas reconocidas.
Detección de amenazas desconocidas	Reenvíe todos los archivos desconocidos a WildFire para su análisis. WildFire identifica software malintencionado desconocido o dirigido (también denominado *amenazas avanzadas persistentes* o *APT [advanced persistent threats]*) oculto en archivos al observar directamente y ejecutar archivos desconocidos en un entorno virtualizado en la nube o en el dispositivo WildFire. Si WildFire detecta malware, automáticamente desarrolla una firma que puede entregarla en tiempo real o en un intervalo de tiempo de su elección.

¿Por qué necesito una política de seguridad de prácticas recomendadas de puerta de enlace de Internet?

Una política de seguridad de prácticas recomendadas le permite habilitar aplicaciones de forma segura mediante la clasificación de todo el tráfico, en todos los puertos, todo el tiempo, incluido el tráfico cifrado. Determine el caso de uso comercial para cada aplicación para crear reglas de política de seguridad que permiten y protegen el acceso a aplicaciones relevantes. Una política de seguridad de prácticas recomendadas aprovecha las tecnologías de nueva generación (App-ID, Content-ID, User-ID y Device-ID (para IoT Security, que está más allá del alcance de este libro)- en la plataforma de seguridad empresarial de Palo Alto Networks y:

- Identifica aplicaciones independientemente del puerto, el protocolo, la táctica evasiva o el cifrado.
- Identifica y controla usuarios independientemente de la dirección IP, la ubicación o el dispositivo.
- Protege frente a amenazas conocidas y desconocidas transmitidas a través de las aplicaciones
- Proporciona visibilidad detallada y control de política sobre el acceso a las aplicaciones y la funcionalidad.
- Sigue las Prácticas recomendadas de IoT Security si tiene una implementación de IoT.

Una política de seguridad de prácticas recomendadas utiliza un enfoque en capas para garantizar que habilite de forma segura las aplicaciones aprobadas mientras bloquea las aplicaciones que no tienen un caso de uso legítimo. Para mitigar el riesgo de que se interrumpan las aplicaciones al pasar de la aplicación basada en puertos a la aplicación basada en aplicaciones, la base de reglas de prácticas recomendadas incluye reglas de políticas de seguridad temporales que identifican lagunas en la base de reglas, detectan actividades sospechosas y amenazas potenciales, garantizan que las aplicaciones no se interrumpan durante la transición y le permiten supervisar el uso de las aplicaciones para que pueda crear las reglas adecuadas. Algunas aplicaciones permitidas por una política basada en puertos heredada pueden ser aplicaciones que no desea permitir o que desea limitar a un conjunto más granular de usuarios.

Una política de seguridad de prácticas recomendadas es más fácil de administrar y mantener porque cada regla cumple un objetivo empresarial específico y permite el acceso a una aplicación o grupo de aplicaciones para un grupo de usuarios o usuarios específicos. La aplicación de cada regla y los criterios de coincidencia de usuario facilitan la comprensión del tráfico al que se aplica la regla. Una práctica recomendada de base de regla de política de seguridad también aprovecha las etiquetas y objetos para que la base de reglas sea más fácil de analizar y mantener sincronizada con su entorno cambiante.

¿Cómo implemento la práctica recomendada de política de seguridad de puerta de enlace de Internet?

El objetivo es diseñar una política de seguridad de prácticas recomendadas basada en aplicaciones que se alinee con sus objetivos empresariales y políticas de uso aceptable, simplifique la administración, reduzca la posibilidad de error y aplique los principios de Zero Trust para el acceso a la red.

Al igual que con cualquier tecnología, suele haber un enfoque gradual para una implementación completa. Planifique cuidadosamente las fases de implementación para que la transición sea lo más fluida posible, con un impacto mínimo para los usuarios finales. En general, el flujo de trabajo para la implementación de una política de seguridad recomendada para la puerta de enlace de Internet es el siguiente:

- **Evalúe su negocio e identifique lo que necesita proteger**: el primer paso para implementar una arquitectura de seguridad es evaluar su negocio. Identifique sus activos más valiosos y las mayores amenazas para dichos activos. Por ejemplo, si se trata de una empresa de tecnología, la propiedad intelectual es el activo más valioso. En este caso, una de sus mayores amenazas es el robo de código fuente.
- Segmentar la red mediante interfaces y zonas: el tráfico puede fluir entre zonas solo si una regla de política de seguridad lo permite. Una defensa sólida para evitar que un atacante que ha obtenido acceso a su red se mueva de forma lateral a través de la red es definir zonas granulares y permitir el acceso solo a los grupos de usuarios específicos que necesitan acceso a una aplicación o un recurso en cada zona. La segmentación de su red en zonas pormenorizadas impide que un atacante establezca un canal de comunicación con la red (ya sea a través de software malintencionado o al vulnerar aplicaciones legítimas), lo que reduce la probabilidad de éxito de un ataque en la red.
- Identificar la lista de aplicaciones permitidas: antes de poder crear una política de seguridad de prácticas recomendadas de la puerta de enlace de Internet, cree un inventario de las aplicaciones que desea permitir en la red. Enumere por separado las aplicaciones que administra, autoriza oficialmente para la empresa y tolera para el uso de los empleados. Después de identificar las aplicaciones que desea permitir, si va a migrar desde una base de reglas basada en puertos, asigne las aplicaciones a las reglas basadas en puertos. Si una regla basada en puertos no tiene ninguna aplicación asignada, es posible que no necesite esa regla.
- Crear grupos de usuarios para acceder a Aplicaciones permitidas: una vez que identifique las aplicaciones que prevé permitir, identifique los grupos de usuarios que necesitan acceder a cada aplicación. Comprometer el sistema de un usuario final es una de las formas más baratas y fáciles para que un atacante obtenga acceso a su red. Para reducir significativamente la superficie expuesta a ataques, permita el acceso a la aplicación solo a los grupos de usuarios que tengan una necesidad empresarial legítima.
- Descifrar el tráfico para la visibilidad total y la inspección de amenazas: no es posible proteger su red frente a amenazas que no puede ver e inspeccionar. El tráfico cifrado es una forma común para que los atacantes entreguen amenazas. Por ejemplo, un atacante puede usar una aplicación web como Gmail, que utiliza cifrado TLS, para enviar por correo electrónico un exploit o software malintencionado para que los empleados accedan a esa aplicación en la red corporativa. O bien, un atacante puede alterar un sitio web que utiliza cifrado TLS para descargar sigilosamente un exploit o software malintencionado a los visitantes del sitio web.
- Crear perfiles de seguridad recomendados para la puerta de enlace de Internet: las aplicaciones legítimas ofrecen tráfico de comando y control, CVE, descargas no autorizadas de contenido malicioso,

ataques de phishing y APT. Para protegerse frente a amenazas conocidas y desconocidas, adjunte perfiles de seguridad estrictos a todas las reglas de política de seguridad que permitan el tráfico.

- Definir la política de seguridad de puerta de enlace de Internet inicial: con el inventario de aplicaciones y grupos de usuarios que ha elaborado, puede definir una política inicial que permita el acceso a todas las aplicaciones que desea incluir en la lista de permitidos para el usuario o grupo de usuarios. La base de regla de política inicial también debe incluir reglas para bloquear direcciones IP malintencionadas conocidas, así como reglas temporales que impiden que aplicaciones que quizás no conozca se interrumpan y para identificar brechas de la política y vulnerabilidades de seguridad en el diseño existente.
- Supervisar y ajustar la base de reglas de la política: una vez aplicadas las reglas temporales, supervise el tráfico que coincide con ellas para poder ajustar la política. Debido a que las reglas temporales están diseñadas para revelar el tráfico imprevisto de la red, tal como el tráfico que se ejecuta en puertos que no son por defecto o tráfico de usuarios desconocidos, debe evaluar el tráfico que coincide con estas reglas y ajustar las reglas de permiso de aplicaciones según corresponda.
- Eliminar las reglas temporales: después de un período de supervisión de varios meses, debería ver cada vez menos tráfico coincidente con las reglas temporales. Cuando llega al punto en que el tráfico ya no coincide con las reglas temporales, elimínelas para completar la política de seguridad recomendada para la puerta de enlace de Internet.
- Mantener la base de reglas: debido a la naturaleza dinámica de las aplicaciones, debe supervisar constantemente su lista de aplicaciones permitidas, adaptar las reglas para incluir nuevas aplicaciones y determinar de qué manera los App-ID nuevos o modificados afectan la política. Debido a que las reglas de una base de reglas de prácticas recomendadas se alinean con los objetivos comerciales y aprovechan los objetos de política para una administración simplificada, la inclusión de la compatibilidad para una nueva aplicación o un App-ID nuevos o modificados es tan simple como añadir o eliminar una aplicación de un grupo de aplicaciones o modificar un filtro de aplicaciones.

Identifique su Lista de aplicaciones permitidas

La lista de aplicaciones permitidas incluye las aplicaciones autorizadas que usted aprovisiona y administra para fines comerciales, de infraestructura y de trabajo de usuario, y las aplicaciones toleradas que elige permitir para uso personal. Antes de crear su política de seguridad de la pasarela de Internet, cree un inventario de las aplicaciones que desea permitir.

- Asignación de aplicaciones a objetivos comerciales para una base de reglas simplificada
- Uso de reglas temporales para el ajuste preciso de la Lista de permitidos
- Ejemplo de lista de aplicaciones permitidas

Asignación de aplicaciones a objetivos comerciales para una base de reglas simplificada

A medida que elabora el inventario de las aplicaciones de la red, tenga en cuenta los objetivos comerciales y las políticas de uso aceptable, e identifique las aplicaciones que corresponden a cada uno. Esto le permite crear una base de reglas basada en objetivos. Por ejemplo, un objetivo empresarial podría ser permitir que los grupos de ventas y soporte accedan a la base de datos de clientes. Cree una regla de permitidos que corresponda a cada objetivo y agrupe todas las aplicaciones que se alinean con el objetivo en una sola regla. Este enfoque le permite crear una base de reglas con un número menor de reglas individuales y cada regla tiene un propósito claro.

Dado que las reglas individuales que crea se alinean con sus objetivos comerciales, puede usar objetos de aplicación para agrupar aplicaciones permitidas para simplificar aún más la administración de la base de regla:

- Crear grupos de aplicaciones para cada conjunto de aplicaciones autorizadas: cree grupos de aplicaciones que incluyan explícitamente solo conjuntos de sus aplicaciones autorizadas. Los grupos de aplicaciones simplifican la administración de su política porque le permiten añadir y eliminar aplicaciones autorizadas sin modificar las reglas de política de seguridad individuales. En general, si las aplicaciones que se asignan al mismo objetivo tienen los mismos requisitos de acceso (por ejemplo, todas tienen una dirección de destino que apunta a Internet, todas permiten el acceso a cualquier usuario conocido y usted desea habilitarlas solo en los puertos por defecto), las añadirá al mismo grupo de aplicaciones.

  Etiquete todas las aplicaciones autorizadas *con la etiqueta Sanctioned (Sancionada) predefinida. Panorama y los cortafuegos consideran a las aplicaciones sin la etiqueta Sanctioned (Sancionada) como aplicaciones no sancionadas.*

- Crear un filtro de aplicaciones para permitir cada tipo de aplicación general: además de las aplicaciones que apruebe oficialmente, debe decidir a qué aplicaciones adicionales desea que los usuarios puedan acceder. Los filtros de aplicaciones le permiten habilitar de manera segura ciertas categorías de aplicaciones basándose en etiquetas, categoría, subcategoría, tecnología, factor de riesgo o característica. Separe diferentes tipos de aplicaciones en función del uso comercial y personal. Cree filtros separados para cada tipo de aplicación para facilitar la comprensión de cada regla de política.

Uso de reglas temporales para el ajuste preciso de la Lista de permitidos

El objetivo final de la política de seguridad basada en aplicaciones es permitir explícitamente el tráfico de aplicaciones que desea permitir y denegar implícitamente el tráfico que no desea. Sin embargo, la base

de reglas inicial requiere algunas reglas temporales que garantizan que tenga una visibilidad completa de todas las aplicaciones de la red, para que pueda ajustar correctamente la política. La base de reglas inicial necesita los siguientes tipos de reglas:

- Permita reglas para las aplicaciones que apruebe e implemente oficialmente con fines comerciales.
- Reglas de permitidos para habilitar de manera segura el acceso a aplicaciones toleradas que desea permitir de acuerdo con su política de uso aceptable.
- Reglas de bloqueo que bloquean aplicaciones sin un caso de uso legítimo. Estas reglas evitan que el tráfico malintencionado entre en la red, mientras que las reglas temporales detectan aplicaciones que la base de reglas de política aún no tiene en cuenta.
- Las reglas de permiso temporales le brindan visibilidad a todas las aplicaciones que se ejecutan en su red, para que pueda realizar el ajuste preciso de la base de reglas.

Normas temporales:

- Proporcione visibilidad de las aplicaciones que no sabía que estaban en su red.
- Evite que se bloqueen aplicaciones legítimas que no conocía.
- Identifique usuarios desconocidos, aplicaciones desconocidas y aplicaciones que se ejecutan en puertos no estándar (los atacantes suelen usar aplicaciones estándar en puertos no estándar como técnica de evasión para actividades maliciosas).

Identifique las aplicaciones legítimas que se ejecutan en puertos no estándar (por ejemplo, aplicaciones desarrolladas internamente) para que pueda modificar los puertos que usa la aplicación o crear una aplicación personalizada para usarla en la política.

Si tiene reglas de política de anulación de aplicaciones que creó para definir tiempos de espera de sesión personalizados para un conjunto de puertos, convierta las políticas de anulación de aplicaciones en políticas basadas en aplicaciones configurando tiempos de espera de sesión basados en servicios para mantener el tiempo de espera personalizado para cada aplicación. A continuación, migre cada regla a una regla basada en aplicaciones. Las políticas de anulación de aplicaciones se basan en puertos y no proporcionan visibilidad de la aplicación en el tráfico, por lo que no conoce ni controla qué aplicaciones usan los puertos. Los tiempos de espera de una sesión basados en el servicio logran tiempos de espera personalizados a la vez que conservan la visibilidad de la aplicación.

Ejemplo de lista de aplicaciones permitidas

No es necesario capturar todas las aplicaciones que podrían estar en uso en la red en el inventario inicial. En su lugar, concéntrese en las aplicaciones que desea permitir. Las reglas temporales detectan otras aplicaciones que podrían estar en la red, para que no se vea inundado de quejas sobre aplicaciones rotas durante una transición a la política basada en aplicaciones. En la tabla siguiente se muestra un ejemplo de lista de aplicaciones permitidas para una implementación de puerta de enlace empresarial.

Tipo de aplicación	Práctica recomendada de seguridad
Aplicaciones SaaS	Los proveedores de servicios de aplicaciones SaaS tienen y administran el software y la infraestructura, pero usted conserva el control total de los datos, inclusive quién puede crearlos, compartirlos, transferirlos y acceder a ellos. Para controlar las aplicaciones SaaS, use SaaS Security (se requiere

Tipo de aplicación	Práctica recomendada de seguridad
	suscripción). Si utiliza la seguridad de SaaS, utilice la recomendación de política de SaaS para controlar las aplicaciones de SaaS en el cortafuegos. Si no tiene una suscripción de seguridad SaaS, genere un informe de uso de aplicaciones SaaS para comprobar si las aplicaciones SaaS actualmente en uso tienen características de hosting no favorables, como infracciones de datos anteriores o falta de certificados apropiados. De acuerdo con las necesidades de la empresa y el riesgo que esté dispuesto a asumir, use la información para lo siguiente: • Bloquee de inmediato aplicaciones existentes con características de hosting no favorables. • Cree políticas detalladas que bloqueen aplicaciones con características de hosting no favorables para evitar futuras infracciones. • Identifique las tendencias del tráfico de red de las aplicaciones principales con características de hosting no favorables de modo que pueda ajustar la política en consecuencia. Muchas aplicaciones SaaS tienen versiones empresariales y domésticas (personales), pero el uso sin restricciones aumenta el riesgo de que los datos confidenciales salgan de la red. La inserción de encabezados HTTP le permite controlar qué versiones de aplicaciones SaaS permite en su red. Por ejemplo, puede permitir la versión empresarial de Box u Office 365, y bloquear las versiones para consumidores. La inserción de encabezados HTTP reduce la superficie expuesta a ataques al permitir solo la versión de cada aplicación SaaS que desea autorizar o tolerar para el uso personal de los usuarios.

Aplicaciones autorizadas	Estas son aplicaciones que su departamento de TI gestiona específicamente con fines empresariales dentro de su organización, o para proporcionar infraestructura a su red y aplicaciones. Por ejemplo, en la implementación de una puerta de enlace de Internet, estas aplicaciones se dividen en las siguientes categorías:
	
	• **Aplicaciones de infraestructura**: aplicaciones que debe permitir para habilitar la conexión en red y la seguridad, tales como ping, NTP, SMTP y DNS.
	• **Aplicaciones autorizadas de TI**: Aplicaciones que suministra y administra para los usuarios. Se agrupan en dos categorías:
	  • **Aplicaciones autorizadas de TI locales**: aplicaciones que instala y aloja en su centro de datos para uso comercial. Con las aplicaciones autorizadas de TI locales, la infraestructura de aplicación y los datos residen en el equipo propiedad de la empresa. Entre ellas se incluyen Microsoft Exchange y la sincronización activa, además de las herramientas de autenticación como Kerberos y LDAP.
	  • **Aplicaciones SaaS autorizadas por el departamento de TI**: aplicaciones SaaS que su departamento de TI aprueba con fines comerciales, por ejemplo, Salesforce, Box y GitHub.

Tipo de aplicación	Práctica recomendada de seguridad
	• **Aplicaciones administrativas**: aplicaciones a las que solo debe poder acceder un grupo específico de usuarios administrativos para gestionar las aplicaciones y proporcionar soporte a los usuarios (por ejemplo, aplicaciones en escritorios remotos). Etiquete todas las aplicaciones autorizadas con la etiqueta *Sanctioned (Sancionada)* predefinida. Panorama y los cortafuegos consideran a las aplicaciones sin la etiqueta Sanctioned (Sancionada) como aplicaciones no autorizadas.
Tipos de aplicaciones toleradas	Además de las aplicaciones que autorice oficialmente, también debe permitir que los usuarios accedan de forma segura a otros tipos de aplicaciones toleradas: • **Aplicaciones empresariales generales**: por ejemplo, permita acceso a las actualizaciones de software, para las aplicaciones aceptadas, y a los servicios web como WebEx, Adobe online services y Evernote. • **Aplicaciones personales:** por ejemplo, es posible que permita a sus usuarios navegar por Internet o utilizar de manera segura un correo electrónico basado en la web, mensajería instantánea o aplicaciones de redes sociales, incluidas las versiones para consumidores de algunas aplicaciones SaaS. Comience con filtros de aplicaciones amplios para comprender qué aplicaciones están en su red. Decida cuánto riesgo está dispuesto a asumir y reduzca al máximo la lista de aplicaciones permitidas. Por ejemplo, es posible que tenga varias aplicaciones de mensajería en uso, cada una con el riesgo inherente de pérdida de datos, transferencia de archivos infectados con malware, etc. La mejor estrategia es sancionar una sola aplicación de mensajería y, a continuación, pasar lentamente de una política de permisos a una política de alertas y, después de avisar a los usuarios con suficiente antelación, a una política de bloqueo para eliminar gradualmente las demás aplicaciones de mensajería. Es posible que también desee permitir que un grupo reducido de usuarios continúe utilizando aplicaciones de mensajería adicionales según sea necesario para llevar a cabo funciones laborales con los socios.
Aplicaciones personalizadas específicas para su entorno	Cree aplicaciones personalizadas para aplicaciones propias o aplicaciones que se ejecuten en puertos no estándar. Esto le permite habilitar la aplicación como una aplicación autorizada (y aplicar la etiqueta predefinida de Sancionada) y bloquearla en su puerto predeterminado. De lo contrario, deberá abrir puertos adicionales (para las aplicaciones que se ejecutan en puertos no estándar) o permitir un tráfico desconocido (para las aplicaciones exclusivas), pero ninguna opción implica una política de seguridad de prácticas recomendadas. Si posee políticas existentes de anulación de aplicaciones que creó únicamente para definir los tiempos de espera personalizados de una sesión para un conjunto de puertos, convierta las políticas existentes de anulación de aplicaciones en políticas basadas en la aplicación configurando los tiempos de

Tipo de aplicación	Práctica recomendada de seguridad
	espera de una sesión basados en el servicio para conservar el tiempo de espera personalizado de cada aplicación. A continuación, migre cada regla a una regla basada en aplicaciones. Las políticas de anulación de aplicaciones se basan en puertos y no proporcionan visibilidad de la aplicación en el tráfico, por lo que no conoce ni controla qué aplicaciones usan los puertos. Los tiempos de espera de una sesión basados en el servicio logran tiempos de espera personalizados a la vez que conservan la visibilidad de la aplicación.

Crear grupos de usuarios para acceder a Aplicaciones permitidas

Habilitar aplicaciones de manera segura significa definir la lista de aplicaciones que desea permitir y habilitar el acceso solo a aquellos usuarios que tengan una necesidad comercial legítima. Por ejemplo, algunas aplicaciones, tales como las aplicaciones SaaS que habilitan el acceso a los servicios de Recursos Humanos tales como Workday o Service Now deben estar disponibles para todos los usuarios conocidos de la red. Sin embargo, para aplicaciones más sensibles, reduzca su superficie de ataque permitiendo el acceso solo a los usuarios que necesitan las aplicaciones para fines comerciales. Por ejemplo, el personal de soporte de TI podría necesitar legítimamente acceso a aplicaciones de escritorio remoto, pero la mayoría de los usuarios no. Limitar el acceso de los usuarios a las aplicaciones evita posibles brechas de seguridad que un atacante podría utilizar para obtener acceso y control sobre los sistemas de su red.

Para habilitar el acceso a las aplicaciones basado en los usuarios:

- Habilite User-ID en las zonas desde las que sus usuarios inician el tráfico.
- Para cada regla de aplicaciones permitidas que define, identifique los grupos de usuarios que tienen una necesidad comercial legítima para acceder a las aplicaciones. La asignación de reglas de permisos de aplicaciones a objetivos comerciales (lo que incluye considerar qué usuarios tienen una necesidad comercial para un tipo particular de aplicación) da como resultado un número menor de reglas para gestionar, en comparación con la asignación a usuarios de reglas basadas en puertos.
- Si no tiene grupos de usuarios existentes en su servidor Active Directory (AD), como alternativa, cree grupos LDAP personalizados para que coincidan con los grupos de usuarios que necesitan acceso a una aplicación en particular.
- Solo es necesario que un usuario final haga clic en un enlace de phishing e introduzca credenciales para permitir a un atacante obtener acceso a su red. Para defenderse de esta simple y eficaz técnica de ataque, realice la configuración de la protección de phishing de credenciales en todas las reglas de la política de seguridad que permiten el acceso de usuarios a Internet. Configure la detección de credenciales con el agente de User-ID basado en Windows para garantizar que pueda detectar cuando sus usuarios envían sus credenciales corporativas a un sitio en una categoría no autorizada.

Descifrar el tráfico para la visibilidad total y la inspección de amenazas

Descifre todo el tráfico excepto las categorías confidenciales, incluidas categorías de URL como servicios financieros, salud y medicina, gobierno y otro tráfico que no descifre por motivos comerciales, legales o normativos. Utilice categorías de URL, categorías de URL personalizadas y listas dinámicas externas (EDL) para especificar el tráfico que no descifra.

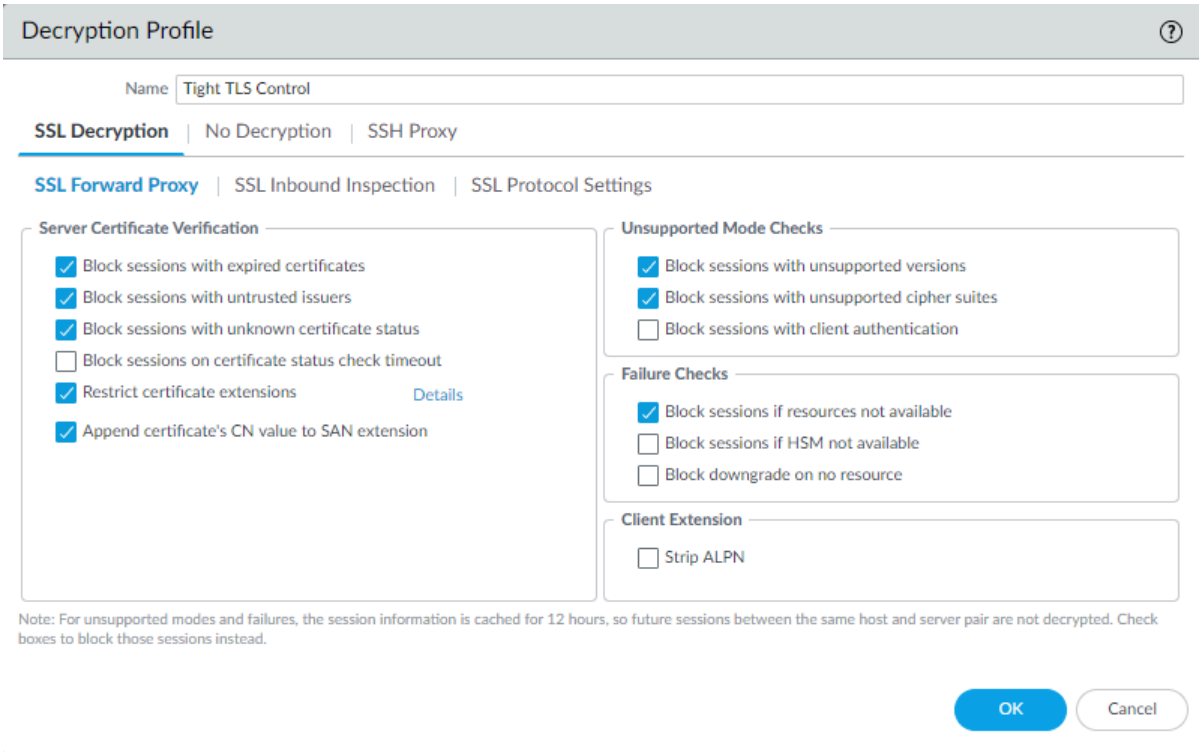
Utilice excepciones de descifrado solo cuando sea necesario. Sea preciso para asegurarse de limitar las excepciones a aplicaciones o usuarios específicos en función de las necesidades:

- Si el descifrado interrumpe una aplicación importante, cree una excepción para la dirección IP, dominio o nombre común específico en el certificado asociado a la aplicación.
- Si necesita excluir un usuario específico por motivos reglamentarios, comerciales o legales, cree una excepción solo para ese usuario.

Para garantizar que los certificados que se presentan durante el descifrado sean válidos, realice comprobaciones de CRL/OCSP.

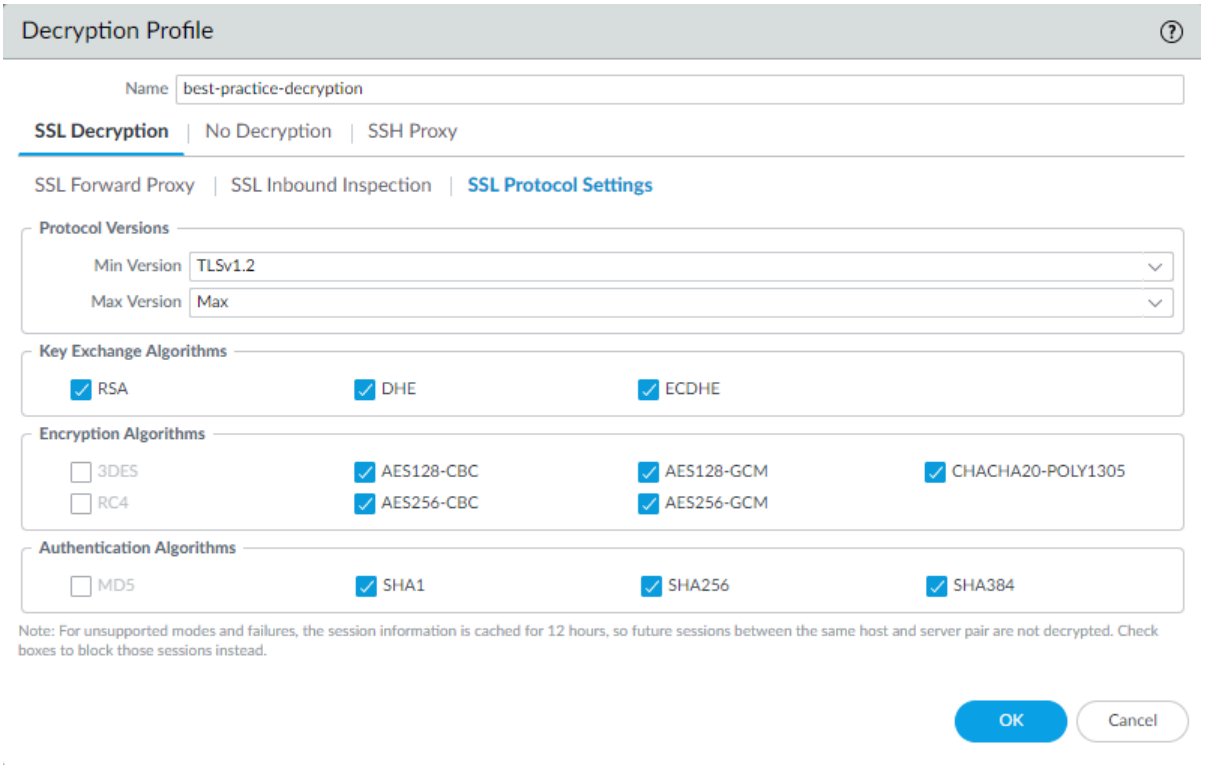
Añada un perfil de descifrado estricto a las reglas de política de descifrado. Antes de configurar el proxy de reenvío SSL, cree un perfil de descifrado recomendado [**Objects (Objetos)** > **Decryption Profile (Perfil de descifrado)**] para adjuntarlo a las reglas de su política de descifrado y seguir las prácticas recomendadas de descifrado:

STEP 1 | Realice la configuración de **SSL Decryption (Descifrado SSL)** > **SSL Forward Proxy (Proxy de reenvío SSL)** para bloquear las excepciones durante la negociación TLS y bloquear las sesiones que no pueden descifrarse:



Block sessions if resources not available (Bloquear sesiones si los recursos no están disponibles) impide permitir conexiones potencialmente peligrosas cuando el cortafuegos no tiene los recursos para realizar el descifrado mediante el bloqueo del tráfico que no se puede descifrar, lo que podría afectar a la experiencia del usuario.

STEP 2 | Realice la configuración de **SSL Decryption (Descifrado SSL)** > **SSL Protocol Settings (Configuración del protocolo SSL)** para bloquear el uso de versiones vulnerables SSL/TLS (TLSv1 0, TLSv1.1 y SSLv3) y evitar los algoritmos débiles (MD5, RC4, and 3DES):

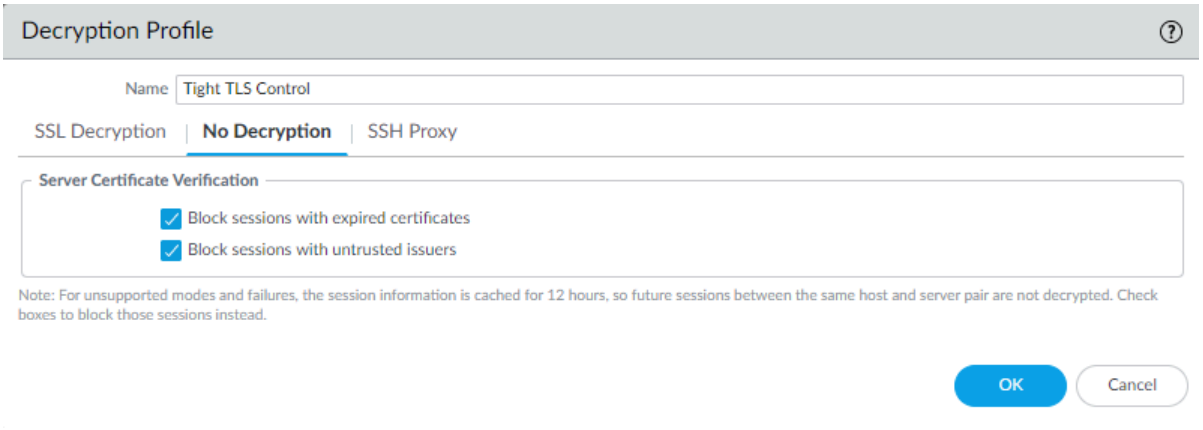


Utilice TLSv1.3 (el protocolo más seguro) cuando sea posible. Muchas aplicaciones móviles utilizan la fijación de certificados que impide el descifrado y hace que el cortafuegos descarte tráfico. Para ese tráfico, use TLSv1.2.

Revise los sitios a los que necesita acceder con fines comerciales. Si alguno de ellos usa TLSv1.1, cree una política y un perfil de descifrado separados para esos sitios, de modo que solo esos sitios a los que debe acceder por motivos de negocio puedan hacer uso del protocolo menos seguro.

No permita el algoritmo de autenticación SHA1 a menos que sea necesario. Cree una regla de política de descifrado y un perfil independientes para los sitios que usan SHA1 a los que debe acceder con fines comerciales.

STEP 3 | En el caso del tráfico que no se descifra, realice la configuración **No Decryption (Sin descifrado)** para bloquear las sesiones cifradas en los sitios con certificados vencidos o emisores que no sean de confianza:



Solo utilice un perfil sin descifrado para TLSv1.2 y versiones anteriores. No adjunte un perfil sin descifrado al tráfico TLSv1.3 que no descifre. TLSv1.3 cifra la información del certificado que no se cifró en versiones anteriores, por lo que el cortafuegos no puede bloquear sesiones basándose en la información del certificado.

Transición segura a los perfiles de seguridad de prácticas recomendadas

Los perfiles de seguridad le permiten inspeccionar el tráfico de la red en busca de amenazas como los exploits de vulnerabilidad, malware, comunicación de comando y control (C2) y amenazas desconocidas, y evitan que pongan en peligro su red utilizando varios tipos de firmas de amenazas, aprendizaje automático e IA (algunas protecciones requieren una suscripción).

El objetivo final es alcanzar un estado de prácticas recomendadas para todos sus perfiles de seguridad. Sin embargo, para garantizar la disponibilidad de aplicaciones críticas para el negocio, podría no ser factible implementar una configuración de perfil de seguridad de prácticas recomendadas desde el principio. En la mayoría de los casos, puede bloquear de forma segura algunas firmas, tipos de archivos o protocolos mientras alerta a otros hasta que obtenga la información y la confianza para finalizar una transición segura a los perfiles de seguridad de prácticas recomendadas sin afectar la disponibilidad.

El camino para implementar los perfiles de seguridad de prácticas recomendadas es:

1. Utilice AIOps para generar un informe de evaluación de prácticas recomendadas (BPA) bajo demanda sobre su postura de seguridad. Revise la adopción de sus prácticas recomendadas, identifique lagunas en la adopción y revise la configuración del perfil de seguridad.
2. Utilice los siguientes pasos de transición segura para avanzar hacia el estado de prácticas recomendadas para sus perfiles de seguridad.

Hágase las siguientes preguntas para ayudar a determinar el enfoque correcto para habilitar los perfiles de seguridad para un segmento de red determinado o un conjunto de reglas de políticas de seguridad:

1. ¿Ya tengo perfiles de seguridad habilitados en reglas que protegen aplicaciones similares o segmentos de red? Si la respuesta es afirmativa, es posible que pueda duplicar esas configuraciones de perfil, incluidas las acciones de bloqueo que ya determinó como seguras para habilitar.
2. ¿El segmento de red que estoy protegiendo es crítico para mi negocio? Si la respuesta es sí y no tiene perfiles probados habilitados en segmentos similares, es posible que prefiera alertar primero, examinar el tráfico que genera las alertas para asegurarse de que el perfil no bloquee aplicaciones críticas, y luego bloquee cuando lo considere.
3. ¿Estoy implementando perfiles de seguridad para contrarrestar una amenaza inmediata? Si la respuesta es afirmativa, es posible que desee bloquear como la acción inicial en lugar de alertar.
4. ¿Existe un proceso de cambio de cortafuegos en curso que permita la investigación y corrección de falsos positivos de manera adecuada? Si la respuesta es afirmativa, es posible que pueda bloquear como la acción inicial en lugar de alertar.

La mayoría de los "falsos positivos" son intentos de ataque contra una vulnerabilidad que no existe en su red. El ataque es real, pero el peligro no lo es porque la vulnerabilidad no está presente, por lo que el ataque a menudo se considera un falso positivo. Las firmas de ataque de fuerza bruta también pueden generar falsos positivos, si establece el umbral de ataque demasiado bajo.

Considere su posición de seguridad actual en combinación con la guía para cada tipo de perfil de seguridad para decidir cómo implementar los perfiles inicialmente y luego pasar a la guía de prácticas recomendadas.

- Transición segura de los perfiles de protección de vulnerabilidades a las prácticas recomendadas
- Transición segura de perfiles antispyware a las prácticas recomendadas

- Transición segura de perfiles de antivirus a las prácticas recomendadas
- Transición segura de perfiles de WildFire a las prácticas recomendadas
- Transición segura de perfiles de filtrado URL a las prácticas recomendadas
- Transición segura de perfiles de bloqueo de archivos a las prácticas recomendadas

Transición segura de los perfiles de protección de vulnerabilidades a las prácticas recomendadas

La decisión de bloquear o alertar cuando aplique por primera vez los perfiles de Protección frente a vulnerabilidades al tráfico depende de su posición de seguridad actual y de los requisitos de su negocio con respecto a la seguridad frente a la disponibilidad. La siguiente guía ayuda a determinar si debe comenzar con acciones de bloqueo o alerta a medida que comienza la transición hacia los perfiles de protección de vulnerabilidades de prácticas recomendadas.

La protección de vulnerabilidades requiere una suscripción a Advanced Threat Prevention o una suscripción activa a la anterior Threat Prevention.

Para identificar y prevenir amenazas, el cortafuegos debe tener visibilidad del tráfico de aplicaciones. Descifre *todo el tráfico que permitan las regulaciones locales, las consideraciones comerciales, las consideraciones de privacidad y la capacidad técnica. Si no descifra el tráfico, el cortafuegos no podrá analizar los encabezados cifrados ni la información de la carga útil.*

Además, siga las prácticas recomendadas de Actualización de contenido de amenazas *para asegurarse de que las firmas del perfil de seguridad estén actualizadas.*

- **Aplicaciones críticas para el negocio**: generalmente es mejor establecer la **Action (Acción)** de regla inicial en **Alert (Alerta)** para garantizar la disponibilidad de la aplicación. Sin embargo, en algunas situaciones puede utilizar la acción de **bloqueo** desde el principio. Por ejemplo, cuando ya está protegiendo aplicaciones similares con un perfil de protección frente a vulnerabilidades que bloquea las

firmas de vulnerabilidades y tiene la certeza que el perfil satisface sus necesidades empresariales y de seguridad, puede usar un perfil similar para bloquear vulnerabilidades y proteger aplicaciones similares.

Las alertas le permiten analizar logs de amenazas y crear excepciones cuando sea necesario antes de comenzar a bloquear el tráfico. Alertar y supervisar antes de pasar al bloqueo le da confianza de que:

- *El perfil inicial no bloqueará las aplicaciones críticas para el negocio cuando lo implemente.*
- *Las excepciones necesarias se crean a medida que se pasa al estado de bloqueo para mantener la disponibilidad de la aplicación.*

Mantenga el periodo de tiempo que mantiene la acción de alerta inicial al mínimo para reducir la posibilidad de una violación de la seguridad. Cambie al estado de bloqueo tan pronto como crea que ha identificado las excepciones que necesita para hacer y configurar el perfil en consecuencia.

- **Firmas críticas y de gravedad alta**: las tasas de falsos positivos para firmas críticas y de alta gravedad suelen ser bajas y generalmente indican un ataque contra una vulnerabilidad que no existe en su red. Para aplicaciones que no son críticas para su empresa, como el acceso a Internet, bloquee [**reset-both (restablecer ambas)**] firmas críticas y de gravedad alta desde el principio.
- **Firmas de gravedad media**: pueden generar falsos positivos y requieren un control inicial. Comience por alertar acerca de firmas de gravedad media y controle los logs de amenazas (**Monitor [Supervisar]** > **Logs** > **Threat [Amenaza]**) para ver si debería bloquear aplicaciones para las que recibe alertas o si necesita permitirlas.
- Ajuste las reglas de perfil que alertan antes de pasar a bloquearlas, especialmente para el tráfico de centros de datos y que se conecta a Internet. Pase a bloquear tan pronto como considere.
- Configure firmas en la categoría de fuerza bruta para alertar y luego pase a bloquear tan pronto como considere. Los eventos de fuerza bruta son eventos colectivos que se activan cuando una acción ocurre varias veces en un corto período de tiempo. Por ejemplo, un intento de inicio de sesión SSH es un evento informativo, pero 100 intentos de inicio de sesión en 10 segundos activan la firma de fuerza bruta. Aunque puede llevar tiempo ajustar el perfil para que el tráfico normal de la red no active una

firma de fuerza bruta, realice la transición para bloquear estas firmas lo antes posible de forma segura, según su nivel de confianza.

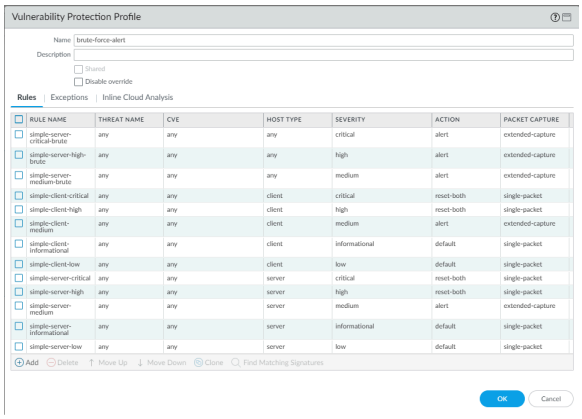


Figure 1: Perfil de protección frente a vulnerabilidades de alerta de fuerza bruta

- La **Action (Acción)** predeterminada para la mayoría de las firmas de gravedad baja e informativas es **alert (alertar)** o **allow (permitir)**. A menos que tenga una necesidad específica de alertar en todas las firmas informativas y de gravedad bajas, configure la **Action (Acción)** como **default (predeterminada)**.
- Si los recursos están disponibles, habilite la captura de paquetes extendida para firmas de gravedad crítica, alta y media sobre las que se realiza las alertas. Habilite la captura de paquetes simple para firmas bloqueadas y para firmas de gravedad baja e informativa. La habilitación de la captura de paquetes permite investigar eventos con mayor detalle si es necesario. A medida que pasa a los perfiles de prácticas recomendadas, si los eventos informativos crean demasiada actividad de captura de paquetes (un volumen de tráfico demasiado grande) y la información no es particularmente útil, proceda a desactivar la captura de paquetes en eventos informativos.

  *Las capturas de paquetes consumen recursos del plano de gestión. Compruebe los recursos del sistema [por ejemplo, **Dashboard (Panel)** > **System Resources (Recursos del sistema)**] para comprender el uso antes y después de implementar la captura de paquetes, para asegurarse de que su sistema tenga recursos suficientes para realizar todas las capturas de paquetes.*
- Para el **Inline Cloud Analysis (Análisis en línea en la nube)**, utilice los mismos criterios para alertar frente a bloquear aplicaciones empresariales que utiliza para las reglas de protección frente a vulnerabilidades. Si tiene controles existentes, puede replicarlos para bloquear el tráfico. Para nuevos

controles, alerte durante al menos una semana antes de pasar al bloqueo. Pase al bloqueo tan pronto como considere.

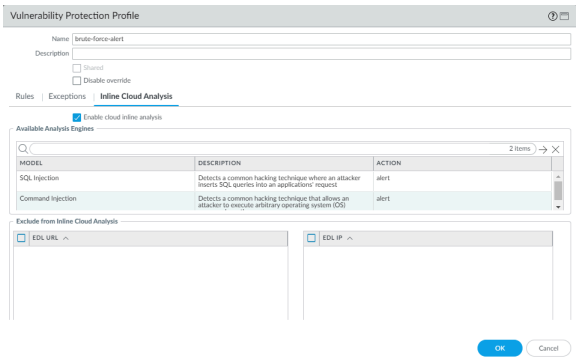


Figure 2: Análisis en línea en la nube alerta el perfil de protección frente a vulnerabilidades

Cuando tenga los perfiles iniciales en su lugar, controle los registros de amenazas durante el tiempo suficiente para estar seguro de que comprende si alguna de las aplicaciones críticas para la empresa genera alertas o bloqueos. Cree excepciones (abra una incidencia de soporte si es necesario) en cada perfil según sea necesario para corregir los falsos positivos confirmados antes de realizar la transición a perfiles de protección frente a vulnerabilidades con prácticas recomendadas. Como de rápido completa su transición a perfiles de prácticas recomendadas depende de su negocio, aplicaciones y nivel de comodidad. Tenga en cuenta que algunas aplicaciones solo se utilizan semanal, mensual, trimestral o anualmente para auditorías, eventos periódicos, reuniones, etc.

Transición segura de perfiles antispyware a las prácticas recomendadas

La siguiente guía le ayuda a determinar si debe comenzar con las acciones de bloqueo o alerta a medida que define los perfiles iniciales de antispyware y comienza con la transición a los perfiles de prácticas recomendadas.

Anti-Spyware requiere una suscripción a Advanced Threat Prevention o a una suscripción activa a Threat Prevention anterior.

Para identificar y prevenir amenazas, el cortafuegos debe tener visibilidad del tráfico de aplicaciones. Descifre *todo el tráfico que permitan las regulaciones locales, las consideraciones comerciales, las consideraciones de privacidad y la capacidad técnica. Si no descifra el tráfico, el cortafuegos no podrá analizar los encabezados cifrados ni la información de la carga útil.*

Además, siga las prácticas recomendadas de Actualización de contenido de amenazas *para asegurarse de que las firmas del perfil de seguridad estén actualizadas.*

- **Aplicaciones críticas para el negocio**: establezca la acción inicial en alerta para garantizar la disponibilidad de la aplicación. Sin embargo, en algunas situaciones puede utilizar la acción de **bloqueo** desde el principio. Por ejemplo, cuando ya está protegiendo aplicaciones con un perfil Antispyware que bloquea firmas críticas, altas o medias, y está seguro de que el perfil satisface sus necesidades

empresariales y de seguridad, puede usar un perfil similar para bloquear el spyware y proteger esas aplicaciones.

> *La acción de alerta le permite analizar los registros de amenazas y crear excepciones cuando sea necesario antes de pasar a una acción de bloqueo. Alertar y supervisar antes de pasar al bloqueo le da la confianza de que:*
>
> - *El perfil no bloqueará las aplicaciones críticas para la empresa cuando lo implemente.*
> - *Las excepciones necesarias se crean a medida que se pasa al estado de bloqueo para mantener la disponibilidad de la aplicación.*
>
> *Cambie al estado de prácticas recomendadas tan pronto como crea que ha identificado las excepciones que necesita para hacer y configure el perfil en consecuencia.*

- **Firmas críticas y de gravedad alta**: Las tasas de falsos positivos son típicamente bajas. Para aplicaciones que no son críticas para su empresa, bloquee firmas críticas y de gravedad alta desde el principio.
- **Firmas de gravedad media**: pueden generar falsos positivos y requieren un control inicial. Comience por alertar sobre las firmas de gravedad media para el tráfico interno y bloquear las firmas de gravedad media para el tráfico externo. Supervise los logs de amenazas [**Monitor (Supervisar)** > **Logs** > **Threat (Amenaza)**] para ver si debe bloquear las aplicaciones para las que recibe alertas o si necesita permitirlas.
- **Firmas de gravedad baja e informativa**: la acción predeterminada para la mayoría de estas firmas es alertar o permitir. A menos que tenga una necesidad específica de alertar en todas las firmas informativas y de gravedad bajas, empiece con la acción predeterminada.
- Habilite la captura de paquetes simple para todas las firmas de gravedad durante la transición si tiene los recursos. La habilitación de la captura de paquetes le permite investigar eventos con mayor detalle si es necesario. A medida que pasa a los perfiles de prácticas recomendadas, si los eventos bajos e informativos crean demasiada actividad de captura de paquetes (un volumen de tráfico demasiado grande) y la información no es útil, puede decidir desactivar la captura de paquetes en estas gravedades.

  > *Las capturas de paquetes consumen recursos del plano de gestión. Compruebe los recursos del sistema [por ejemplo, **Dashboard (Panel)** > **System Resources (Recursos del sistema)**] para comprender el uso antes y después de implementar la captura de paquetes, para asegurarse de que su sistema tenga recursos suficientes para realizar todas las capturas de paquetes.*
- Si trata las aplicaciones internas de manera diferente a las aplicaciones externas, es posible que necesite un perfil Antispyware para el tráfico de Internet y otro perfil Antispyware para el tráfico interno.
- **DNS Policies (Políticas de DNS)**:
  - establezca la **Policy Action (Acción de política)** para las firmas DNS en **Sinkhole** para identificar los hosts potencialmente comprometidos que intentan acceder a dominios sospechosos. DNS Sinkhole le permite realizar un seguimiento de los hosts y evitar que accedan a esos dominios. (Habilitar DNS Sinkhole inmediatamente es la práctica recomendada). Establezca **Packet Capture (Captura de paquetes)** en **extended-capture (captura extendida)**.

- Redirija todos los tipos de dominio de seguridad de **DNS Security (Seguridad DNS)** y establezca la **Packet Capture (Captura de paquetes)** como se muestra en la Figura 1 (PAN-OS 10.0 y versiones posteriores).
- Además, bloquee todos los tipos de registros DNS porque son utilizados por consultas DNS cifradas. Esto evita que los clientes cifren el mensaje de bienvenida del cliente durante el proceso de resolución de DNS, lo que bloquea el intercambio de información clave.

Permitir el tráfico solo a servidores DNS autorizados. Utilice el servicio de seguridad DNS para evitar conexiones a servidores DNS maliciosos.

En los sistemas basados en PAN-OS, establezca la dirección de DNS Sinkhole como el FQDN, por ejemplo, sinkhole.paloaltonetworks.com, de modo que si la dirección IP cambia, la configuración siga siendo válida. Para Prisma Access, utilice la dirección IP del sinkhole.

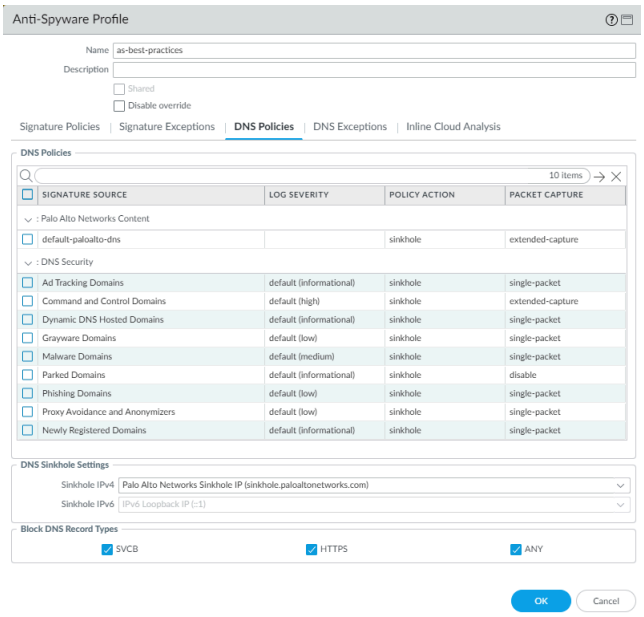


Figure 3: Políticas DNS de perfiles de antispyware

- **Inline Cloud Analysis (Análisis en línea en la nube)** (requiere una suscripción a Advanced Threat Prevention y PAN-OS 10.2 o posterior):**habilite el análisis en línea en la nube** en todo el tráfico saliente. Establezca la **Action (Acción)** en **Reset-both (Restablecer ambos)** para todos los modelos.

Los entornos aislados no pueden usar Advanced Threat Prevention porque es un servicio en la nube y requiere una conexión a la nube.

Cuando tenga los perfiles iniciales en su lugar, controle los registros de amenazas durante el tiempo suficiente para estar seguro de que comprende si alguna de las aplicaciones críticas para la empresa genera alertas o bloqueos. Realice la transición a los perfiles antispyware con prácticas recomendadas tan pronto como se sienta cómodo haciéndolo. Cree excepciones (abra una incidencia de soporte técnico si es necesario) en cada perfil según sea necesario para corregir los falsos positivos confirmados antes de implementar los perfiles de antispyware de prácticas recomendadas.

Transición segura de perfiles de antivirus a las prácticas recomendadas

La siguiente guía ayuda a determinar si se debe comenzar con acciones de bloqueo o alerta cuando se duplica el perfil de antivirus predeterminado y se modifica para definir los perfiles iniciales y comenzar la transición a perfiles de prácticas recomendadas.

El antivirus requiere una suscripción a Advanced Threat Prevention o a Threat Prevention.

Para identificar y prevenir amenazas, el cortafuegos debe tener visibilidad del tráfico de aplicaciones. Descifre todo el tráfico que permitan las regulaciones locales, las consideraciones comerciales, las consideraciones de privacidad y la capacidad técnica. Si no descifra el tráfico, el cortafuegos no podrá analizar los encabezados cifrados ni la información de la carga útil.

Además, siga las prácticas recomendadas de Actualización de contenido de amenazas para asegurarse de que las firmas del perfil de seguridad estén actualizadas.

- **Aplicaciones críticas para el negocio**: establezca la acción inicial en alerta para garantizar la disponibilidad de la aplicación. Sin embargo, en algunas situaciones puede bloquear las firmas de antivirus desde el principio. Por ejemplo, cuando ya está protegiendo aplicaciones similares con un perfil de antivirus y está seguro de que el perfil satisface sus necesidades empresariales y de seguridad, puede usar un perfil similar para proteger aplicaciones similares porque ya entiende que está bloqueando.

  *La acción de alerta le permite analizar los registros de amenazas (**Monitor (Supervisar)** > **Logs** > **Threat (Amenaza)**) y cree excepciones cuando sea necesario antes de pasar a una acción de bloqueo. Alertar y supervisar antes de pasar al bloqueo le da confianza de que:*

  - *El perfil no bloqueará las aplicaciones críticas para la empresa cuando lo implemente.*
  - *Las excepciones necesarias se crean a medida que se pasa al estado de bloqueo para mantener la disponibilidad de la aplicación.*

  Mantenga el periodo de tiempo que mantiene la acción de alerta inicial al mínimo para reducir la posibilidad de un incidente de seguridad. Cambie al estado de prácticas recomendadas tan pronto como crea que ha identificado las excepciones que necesita para hacer y configure el perfil en consecuencia.
- **Firmas críticas y de gravedad alta**: es seguro implementar Perfiles de antivirus de prácticas recomendadas para bloquear el tráfico malicioso de aplicaciones que no son críticas para su negocio de inmediato, dado que las tasas de falsos positivos son raras y por tanto rara vez se produce un bloqueo innecesario.
- Si trata las aplicaciones internas de manera diferente a las externas, es posible que necesite un perfil de antivirus para el tráfico orientado a Internet y otro perfil de antivirus para el tráfico interno.

- Habilite la búsqueda de firmas en tiempo real en todo el dispositivo y en el perfil de antivirus, para retener archivos hasta que el cortafuegos reciba la última firma de antivirus en tiempo real desde la nube:
  - Habilitar globalmente: **Device (Dispositivo)** > **Setup (Configuración)** > **Content-ID** > **Content-ID Settings (Ajustes de Content-ID)** > **Realtime Signature Lookup (Consulta de firma en tiempo real)**, habilite **Hold for WildFire Real Time Signature Lookup ((Mantener pulsado para buscar la firma en tiempo real de WildFire)** y ponga la **Action On Real Time Signature Timeout (Acción sobre el tiempo de espera de firma de WildFire en tiempo real)** en **Reset Both (Restablecer Ambos)**. Debe habilitar la búsqueda de firmas en tiempo real a nivel global para habilitar los perfiles de antivirus.
  - Habilitar en Antivirus Profile (Perfil de antivirus): **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Antivirus** y habilitar **Hold for WildFire Real Time Signature Look Up (Mantener pulsado para buscar la firma en tiempo real de WildFire)**.

  Retener archivos para garantizar que WildFire obtenga las firmas antivirus más recientes le protege frente al malware de día cero y firmas de antivirus obsoletas a las que podría estar expuesto si reenvía archivos sin retenerlos para obtener las firmas más recientes.
- La configuración de la acción de WildFire en el perfil de antivirus puede afectar al tráfico si el tráfico genera una firma WildFire que resulta en una acción de restablecimiento o descarte.

Cuando tenga los perfiles iniciales en su lugar, controle los registros de amenazas durante el tiempo suficiente para estar seguro de que comprende si alguna de las aplicaciones críticas para la empresa genera alertas o bloqueos. También supervise los logs de envíos de WildFire [**Monitor (Supervisar)** > **Logs** > **WildFire Submissions (Envíos de WildFire)**] durante el tiempo suficiente para estar seguro de que comprende si alguna de las aplicaciones críticas para la empresa genera alertas o bloqueos debido a la acción del perfil de antivirus de WildFire. Cree excepciones (abra una incidencia de soporte técnico si es necesario) en cada perfil según sea necesario para corregir los falsos positivos confirmados antes de implementar los perfiles de antivirus completos de prácticas recomendadas. La velocidad de su transición a perfiles de prácticas recomendadas depende de su negocio, aplicaciones y nivel de comodidad. Tenga en cuenta que algunas aplicaciones solo se utilizan semanal, mensual, trimestral o anualmente para auditorías, eventos periódicos, reuniones, etc.

Transición segura de perfiles de WildFire a las prácticas recomendadas

La siguiente guía ayuda a definir la configuración inicial de los perfiles de análisis de WildFire.

Los cortafuegos de nueva generación de Palo Alto Networks incluyen el servicio básico de WildFire y no requieren una suscripción a Advanced WildFire (o a WildFire heredado activo). El servicio básico permite que el cortafuegos reenvíe archivos PE para su análisis y recupera firmas avanzadas de WildFire solo con una actualización de antivirus y/o prevención de amenazas cada 24-48 horas. Una suscripción a Advanced WildFire (PAN-OS 10.0 o posterior) o una suscripción anterior a WildFire incluye muchas más funciones, como recibir actualizaciones en tiempo real, compatibilidad con más tipos de archivos y una API.

Para identificar y prevenir amenazas, el cortafuegos debe tener visibilidad del tráfico de aplicaciones. Descifre todo el tráfico que permitan las regulaciones locales, las consideraciones comerciales, las consideraciones de privacidad y la capacidad técnica. Si no descifra el tráfico, el cortafuegos no podrá analizar los encabezados cifrados ni la información de la carga útil.

La generación de firmas de WildFire es altamente precisa y los falsos positivos son raros. La implementación del perfil de análisis de WildFire predeterminado (que es el perfil de prácticas recomendadas) no afecta al tráfico de red. Sin embargo, la configuración de la acción de WildFire en el Perfil de antivirus podría afectar al tráfico si el tráfico genera una firma WildFire que resulta en una acción de restablecimiento o caída.

Cuando tenga los perfiles iniciales en su lugar, controle los logs de envíos de WildFire [**Monitor (Supervisar)** > **Logs** > **WildFire Submissions (Envíos de WildFire)**] durante el tiempo suficiente para estar seguro de que comprende si alguna de las aplicaciones críticas para la empresa genera alertas o bloqueos debido a la acción del perfil de Antivirus de WildFire. Cree excepciones (abra una incidencia de soporte técnico si es necesario) en el perfil del antivirus según sea necesario para corregir cualquier falso positivo confirmado.

Transición segura de perfiles de filtrado URL a las prácticas recomendadas

Utilice la siguiente guía para determinar si debe comenzar con las acciones de bloqueo o alerta a medida que define los perfiles de filtrado de URL iniciales e inicia la transición a los perfiles de prácticas recomendadas. Aplique los archivos de filtrado de URL al tráfico de Internet (no aplique los perfiles de filtrado de URL al tráfico interno).

Debe habilitar el descifrado para aprovechar el filtrado de URL porque debe descifrar el tráfico para revelar la URL exacta, de forma que el cortafuegos pueda tomar la acción adecuada. Como mínimo, descifrar el tráfico de riesgo alto y medio.

El Filtrado de URL avanzado requiere una suscripción.

- Las categorías de URL predefinidas son precisas, por lo que es seguro implementar perfiles de filtrado de URL con acciones de categoría configuradas de acuerdo con la política de su empresa para permitir o denegar el acceso a diferentes tipos de sitios web.
- Bloquee el**Site Access (Acceso al sitio)** y el **User Credential Submission (Envío de credenciales de usuario)** desde el principio para categorías de URL malas conocidas, que incluyen: malware, comando y control, violación de derechos de autor, extremismo, phishing, ransomware, dynamic-dns, hackeo (pero haga excepciones para los evaluadores internos de PEN), y evitación de proxy y anonimizadores.
- Para las categorías de URL desconocidas (sitios que PAN-DB aún no ha identificado), estacionadas (a menudo se usan para el phishing de credenciales), grayware (malicioso o dudoso) y de dominios recién registrados (a menudo utilizados para actividades maliciosas), alerte desde el principio para que pueda controlar los logs de filtrado de URL [**Monitor (Supervisar)** > **Logs** > **URL Filtering (Filtrado de URL)**] en caso de que sitios web legítimos activen alertas antes de cambiar a las prácticas recomendadas de bloqueo de estas categorías.

- Configure todas las demás categorías de URL para que generen **alerts (alertas)** y generen logs para el tráfico. El cortafuegos no registra el tráfico cuando el acceso está configurado en **allow (permitir)**. Supervise los logs de filtrado de URL para ver si desea bloquear otras categorías.

  Puede combinar las categorías de riesgo alto, medio y bajo con otras categorías para determinar qué tráfico permitir, bloquear y descifrar. Por ejemplo, podría bloquear el acceso a todos los sitios web que sean tanto de alto riesgo como de servicios financieros. O si su cortafuegos necesita conservar recursos, puede descifrar todo el tráfico de riesgo alto y medio para algunas categorías y no descifrar el tráfico de bajo riesgo para esas categorías.

Cuando tenga los perfiles iniciales en su lugar, controle los logs de filtrado de URL durante el tiempo suficiente para estar seguro de que entiende que se bloquearán los sitios críticos para la empresa si cambia de la alerta al bloqueo y a los Perfiles de filtrado de URL de prácticas recomendadas. Si cree que un URL específico no está catalogado correctamente, solicite el recatalogado del URL para tener el URL colocado en la categoría correcta. La velocidad de su transición a perfiles de prácticas recomendadas depende de su negocio, sus aplicaciones y su nivel de comodidad.

Transición segura de perfiles de bloqueo de archivos a las prácticas recomendadas

La siguiente guía ayuda a determinar si debe comenzar con las acciones de bloqueo o alerta a medida que define los perfiles iniciales de bloqueo de archivos e inicia la transición a los perfiles de prácticas recomendadas. Alertar en lugar de permitir que los tipos de archivos generen logs y obtengan visibilidad del tráfico.

- Las prácticas recomendadas para perfiles de bloqueo de archivos suelen ser diferentes para diferentes tipos de aplicaciones y pueden ser diferentes para el tráfico entrante, saliente e interno. Por ejemplo:
  - Si las aplicaciones internas dependen de las transferencias de tipo de archivo que el perfil de Bloqueo de archivos de las prácticas recomendadas recomienda bloquear, permita esos tipos de archivos para esas aplicaciones internas; un buen ejemplo son los archivos .dll. Permita esos tipos de transferencia de archivos solo para las aplicaciones internas necesarias, no para todas las aplicaciones.
  - Para el tráfico basado en Internet, utilice un enfoque más restrictivo para evitar que los atacantes entreguen archivos maliciosos y para reducir la superficie de ataque.
  - Para el tráfico del centro de datos, adopte un enfoque más restrictivo (excepto para las aplicaciones internas que dependen de los tipos de transferencia de archivos que de otro modo bloquearía) para reducir la superficie de ataque y proteger sus activos más valiosos.
  - Cuando cree excepciones, siga el principio de privilegio mínimo y aplique las excepciones solo a las aplicaciones y usuarios que necesitan acceso al tipo de archivo por motivos comerciales.
- **Aplicaciones críticas para el negocio**: comience con la acción alertar para todos los tipos de archivos y pase a los perfiles de bloqueo de archivos con prácticas recomendadas lo antes posible. Si ya tiene controles de bloqueo implementados, duplíquelos y continúe bloqueando el tráfico que ya sabe que desea bloquear.

- Para aplicaciones que no son críticas para el negocio, inicie la transición a un perfil de bloqueo de archivos con prácticas recomendadas:
  - **Tráfico entrante y saliente**: establezca la **Action (Acción)** en **block (bloquear)** para archivos 7z, bat, chm, class, cpl, dll, dlp, hta, jar, ocx, pif, scr, torrent, vbe y wsf. Establezca la **Action (Acción)** en **alert (alertar)** para todos los demás archivos.
  - **Tráfico interno**: bloquee archivos 7z, bat, chm, class, cpl, dlp, hta, jar, ocx, pif, scr, torrent, vbe y wsf (es lo mismo que el perfil de tráfico entrante y saliente excepto que alerta acerca de archivos .dll en lugar de bloquearlos). Alerta en todos los demás archivos.
  - Bloquee todos los siguientes tipos de archivos que pueda para los usuarios que no los necesitan para fines comerciales: cab, exe, flash, msi, codificación multinivel, PE, rar, tar, rar-cifrado y zip-cifrado.

Si es necesario, cree excepciones para grupos de TI y otras personas que necesiten acceso comercial legítimo a cualquiera de estos tipos de archivos. Si ya bloquea otros tipos de archivos, continúe bloqueándolos.

Realice la transición a un perfil de bloqueo de archivos con prácticas recomendadas tan pronto como se sienta cómodo haciéndolo.

Ajuste las reglas de perfil que alertan y haga la transición a bloquear tan pronto como considere, especialmente para el tráfico de centros de datos y de Internet. Supervise los logs de filtrado de datos [**Monitor (Supervisar)** > **Logs** > **Data Filtering (Filtrado de datos)**] para comprender el uso de los tipos de archivos antes de configurar las acciones de bloqueo para tipos de archivo específicos. Cuando sea conocedor de qué tipos de archivos requieren sus aplicaciones personalizadas internas y críticas para el negocio, realice la transición hacia una configuración de bloqueo de archivos con prácticas recomendadas, modificada según sea necesario para satisfacer sus necesidades comerciales.

Crear perfiles de seguridad recomendados para la puerta de enlace de Internet

La mayoría del software malintencionado ingresa furtivamente en la red en aplicaciones o servicios legítimos. Para habilitar aplicaciones de forma segura, debe escanear todo el tráfico permitido en busca de amenazas. Adjunte Perfiles de seguridad a todas las reglas de política de seguridad para permitir el tráfico, a fin de que pueda detectar amenazas (tanto conocidas como desconocidas) en el tráfico de su red. Las siguientes recomendaciones de prácticas recomendadas se centran en la seguridad más estricta. Adjunte un perfil de filtrado de URL a todas las reglas que permitan el tráfico de y a Internet, y adjunte los otros perfiles a todas las reglas de permiso.

Más del 90 por ciento del tráfico web está cifrado. Habilite el descifrado para obtener visibilidad del tráfico, utilice perfiles de seguridad para inspeccionar la carga útil y evitar eventos maliciosos.

Considere añadir sus perfiles de seguridad de prácticas recomendadas a un grupo de perfiles de seguridad predeterminado. Cuando asigna un nombre ***predeterminado*** *a un grupo de perfiles de seguridad, el cortafuegos lo adjunta automáticamente a cada nueva regla de política de seguridad que crea y garantiza que el cortafuegos inspeccione el tráfico en busca de actividad maliciosa.*

Considere también la posibilidad de crear grupos de perfiles de seguridad diseñados específicamente para diferentes tipos de tráfico. Los grupos de perfiles de seguridad facilitan la aplicación de todos los perfiles necesarios a las reglas de políticas de seguridad y garantizan que no se deje atrás ningún perfil crítico.

- Perfil de bloqueo de archivos recomendado para la puerta de enlace de Internet
- Perfil de antivirus recomendado para la puerta de enlace de Internet
- Perfil de protección de vulnerabilidades recomendado para la puerta de enlace de Internet
- Perfil de antispyware recomendado para la puerta de enlace de Internet
- Perfil de filtrado de URL recomendado para la puerta de enlace de Internet
- Perfil de análisis de WildFire recomendado para la puerta de enlace de Internet

Perfil de bloqueo de archivos recomendado para la puerta de enlace de Internet

Use el perfil de **bloqueo de archivos estricto** predefinido para bloquear los tipos de archivos que se incluyen comúnmente en las campañas de ataque de malware que no tienen un caso de uso real para la carga y descarga. Bloquear estos tipos de archivos reduce la superficie de ataque. El perfil predefinido estricto bloquea los archivos por lotes, DLL, archivos de clase Java, archivos de ayuda, accesos directos de Windows (.lnk), archivos .rar, archivos .tar, archivos cifrados rar y zip, archivos de varios niveles codificados (archivos codificados o comprimidos hasta cuatro veces), archivos .hta, y archivos portable ejecutable (Portable Executable, PE) de Windows, que incluyen archivos .exe, .cpl, .dll, .ocx, .sys, .scr, .drv, .efi, .fon y .pif. El perfil predefinido alerta sobre todos los demás tipos de archivos para brindar visibilidad de otras transferencias de archivo que puede determinar si desea introducir cambios en la política.

En algunos casos, es probable que la necesidad de admitir aplicaciones críticas evite que bloquee todos los tipos de archivos del perfil estricto. Siga los consejos de Transición segura de perfiles de bloqueo de archivos a las prácticas recomendadas *para ayudar a determinar si necesita hacer excepciones en diferentes áreas de la red. Revise los logs de filtrado de datos [**Monitor (Supervisar)** > **Logs** > **Data Filtering (Filtrado de datos)**] para identificar los tipos de archivos y analizar con las partes interesadas de la empresa los tipos de archivos que necesitan sus aplicaciones. En función de esta información, duplique el perfil estricto y modifíquelo según sea necesario para permitir solo el otro tipo de archivos que deben admitir las aplicaciones críticas. Puede usar el ajuste de **Direction (Dirección)** para evitar que determinados tipos de archivos fluyan en ambas direcciones o para bloquear a los archivos en una dirección, pero no en otra.*

NAME	LOCATION	RULE NAME	APPLICATIONS	FILE TYPES	DIRECTION	ACTION
basic file blocking	Predefined	Block high risk file types	any	7z, bat, chm, class, cpl, dll, exe, hlp, hta, jar, ocx, PE, pif, rar, scr, torrent, vbe, wsf	both	block
		Continue prompt encrypted files	any	encrypted-rar, encrypted-zip	both	continue
		Log all other file types	any	any	both	alert
strict file blocking	Predefined	Block all risky file types	any	7z, bat, cab, chm, class, cpl, dll, exe, flash, hlp, hta, jar, msi, Multi-Level-Encoding, ocx, PE, pif, rar, scr, tar, torrent, vbe, wsf	both	block
		Block encrypted files	any	encrypted-rar, encrypted-zip	both	block
		Log all other file types	any	any	both	alert

También es posible que necesite algunos protocolos que se utilizan a menudo con fines maliciosos para actividades como las actualizaciones de Windows. El perfil de **strict file blocking (bloqueo de archivos estricto)** bloquea archivos .exe., .dll, .pe y .cab. Para hacer excepciones para permitir protocolos para una actividad específica, como actualizaciones de Windows:

1. Cree una regla de política de seguridad específica que permita solo a los usuarios y aplicaciones comerciales necesarios que utilizan los protocolos que desea bloquear para otro tráfico.
2. Duplique su perfil estricto de bloqueo de archivos, modifíquelo para permitir los protocolos requeridos y luego adjúntelo a la regla.
3. Coloque la regla encima de una regla de política de seguridad con un perfil de Bloqueo de archivos que bloquee los protocolos para el resto del tráfico.

Este método le permite utilizar tipos de archivos potencialmente maliciosos de una manera segura que habilita las aplicaciones comerciales mientras bloquea el tráfico malicioso. Ajuste los perfiles y la base de reglas para permitir las excepciones necesarias.

¿Por qué necesito este perfil?

Los atacantes pueden entregar archivos maliciosos de muchas maneras:

- Archivos adjuntos o enlaces en correo electrónico corporativo o personal.
- Enlaces o mensajes instantáneos en redes sociales y otras fuentes.
- Kits de exploits.
- Aplicaciones para compartir archivos (como FTP, Google Drive o Dropbox).
- Unidades USB.
-

Adjuntar un perfil estricto de bloqueo de archivos previene este tipo de ataques y reduce la superficie de ataque.

Si elige no bloquear todos los archivos de Windows PE, envíe todos los archivos desconocidos a WildFire para analizarlos. Configure la acción en **continue (continuar)** para evitar descargas inadvertidas, que se

producen cuando un usuario final descarga contenido que instala archivos malintencionados, tales como applets Java o archivos ejecutables, sin el conocimiento del usuario. Las descargas inadvertidas pueden producirse cuando los usuarios entran en sitios web, ven mensajes de correo electrónico o hacen clic en ventanas emergentes diseñadas para engañarles. Informe a los usuarios que si les aparece un mensaje que les indica continuar con la transferencia de un archivo que no iniciaron intencionadamente, podrían quedar sujetos a una descarga malintencionada. Además, utilice el bloqueo de archivos con filtrado de URL para limitar las categorías en las que los usuarios pueden transferir archivos para reducir la superficie de ataque, si no le queda otra opción que permitir tipos de archivos que puedan contener amenazas.

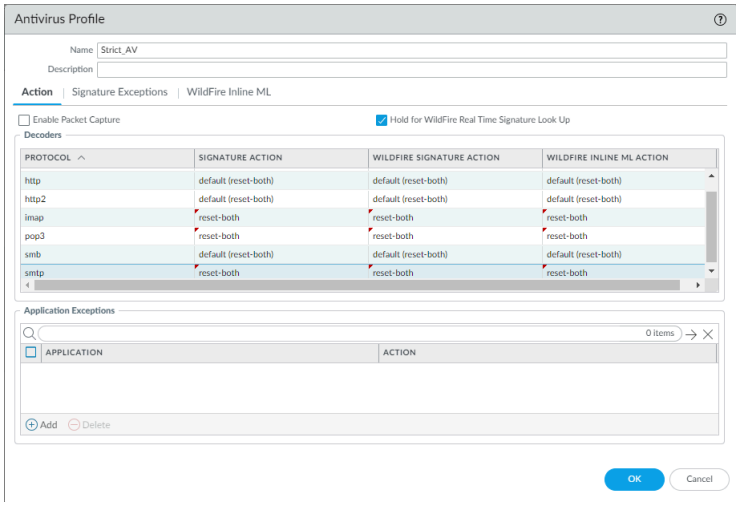
Perfil de antivirus recomendado para la puerta de enlace de Internet

Para garantizar la disponibilidad para aplicaciones críticas para el negocio, siga el consejo de Transición segura de perfiles de antivirus a las prácticas recomendadas a medida que pasa de su estado actual al perfil de prácticas recomendadas. El objetivo es realizar la transición al perfil como se muestra aquí y adjuntarlo a todas las reglas de política de seguridad que permiten tráfico. Los decodificadores de protocolos del perfil de antivirus detectan e impiden la transferencia de virus y malware a través de siete protocolos: FTP, HTTP, HTTP2, IMAP, POP3, SMB y SMTP.

Configure las acciones de WildFire Signature y WildFire Inline ML para los siete protocolos (el perfil antivirus también aplica acciones basadas en firmas WildFire) y, si aún no lo ha hecho, habilite la búsqueda de firmas en tiempo real como se muestra en Transición segura de perfiles de antivirus a las prácticas recomendadas.

Configure el perfil de antivirus duplicado para restablecer tanto el cliente como el servidor en los siete decodificadores de protocolo y acciones de WildFire, y luego adjunte el perfil a las reglas de permiso de la política de seguridad.

Si trata las aplicaciones internas de manera diferente a las aplicaciones externas, es posible que necesite un perfil de antivirus para el tráfico de Internet y un perfil de antivirus diferente para el tráfico interno.



Habilite la búsqueda de firmas en tiempo real a nivel global y en el perfil de Antivirus para retener archivos hasta que el cortafuegos reciba la última firma antivirus en tiempo real desde la nube:

- Habilitar globalmente: **Device (Dispositivo)** > **Setup (Configuración)** > **Content-ID** > **Content-ID Settings (Configuración de Content-ID)** > **Realtime Signature Lookup (Consulta de firma**

en tiempo real), habilite **Hold for WildFire Real Time Signature Look Up (Mantener pulsado para buscar la firma en tiempo real de WildFire)** y configure el **Action on Real Time Siganture Timeout (Acción en el tiempo de espera de firma en tiempo real)** para **Reset Both (Restablecer ambos)**. Debe habilitar la búsqueda de firmas en tiempo real a nivel global para habilitarla en los perfiles de antivirus.

- Habilite **Hold for WildFire Real Time Signature Lookup (Mantener pulsado para buscar la firma en tiempo real de WildFire)** en el perfil de antivirus. Retener archivos para garantizar que WildFire obtenga las firmas antivirus más recientes le protege frente al malware de día cero y firmas de antivirus obsoletas a las que podría estar expuesto si reenvía archivos sin retenerlos para obtener las firmas más recientes.

¿Por qué necesito este perfil?

Al adjuntar perfiles de antivirus a todas las reglas de seguridad, bloquea archivos malintencionados conocidos (software malintencionado, bots de ransomware y virus) a medida que ingresan en la red. Las maneras habituales en que los usuarios reciben archivos malintencionados incluyen documentos adjuntos malintencionados en correos electrónicos, enlaces para descargar archivos malintencionados o amenazas silenciosas proporcionadas por Exploit Kits que aprovechan una vulnerabilidad y luego descargan automáticamente cargas útiles malintencionadas en el dispositivo del usuario final.

Perfil de protección de vulnerabilidades recomendado para la puerta de enlace de Internet

Adjunte un perfil de protección de vulnerabilidad a todo el tráfico permitido para proteger contra los desbordamientos de búfer, ejecución de código ilegal y otros intentos de aprovechar vulnerabilidades del lado del cliente y del lado del servidor. Para garantizar la disponibilidad para aplicaciones críticas para el negocio, siga los consejos de Transición segura de los perfiles de protección de vulnerabilidades a las prácticas recomendadas a medida que pasa de su estado actual al perfil de prácticas recomendadas. Duplique el perfil de Protección frente a vulnerabilidades predefinido y edítelo para crear el perfil de prácticas recomendadas:

- Cambie la **Action (Acción)** en las tres reglas de fuerza bruta para **reset-both (restablecer ambos)** y **Packet Capture (Captura de paquetes** a **single-packet (un solo paquete)** para pasar de alertar sobre eventos de ataque de fuerza bruta a bloquearlos.
- Consolide eventos de gravedad crítica, alta y media para servidores y clientes en una única regla. Configure la **Action (Acción)** para **reset-both (restablecer ambos)** y configure la **Packet Capture (Captura de paquetes)** en **single-packet (un solo paquete)**. Esto simplifica el perfil y funciona porque el perfil utiliza la misma acción y la misma configuración de captura de paquetes para estas gravedades.

  *Para los perfiles que controlan el tráfico interno (este-oeste), el bloqueo de eventos de gravedad media podría afectar las aplicaciones empresariales. Si el bloqueo afecta las aplicaciones empresariales, cree una regla independiente en el perfil para eventos de gravedad media con la **Action (Acción)** establecida en **alert (alerta)**. Aplique el perfil solo al tráfico interno.*

- Para simplificar el perfil, consolide los eventos de baja gravedad para servidores y clientes en una única regla. Establezca la **Action (Acción)** en **default (predeterminada)** y establezca la **Packet Capture (Captura de paquetes)** en **single-packet (un solo paquete)**.

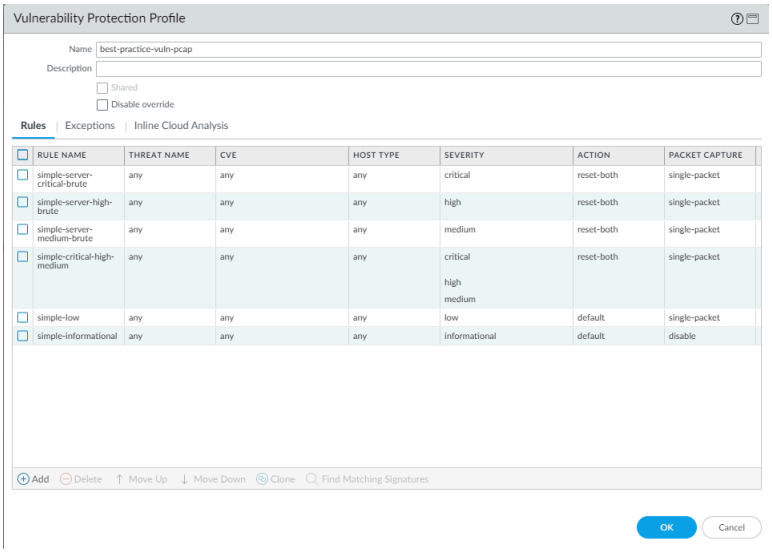
- Consolide eventos informativos para servidores y clientes en una única regla. Establezca la **Action (Acción)** en **default (predeterminada)** y establezca la **Packet Capture (Captura de paquetes)** en **disable (deshabilitar)**.

  Las PCAP para eventos informativos generan un volumen de tráfico relativamente alto que normalmente no es útil, en comparación con las capturas relacionadas con amenazas potenciales.
- Aplique PCAP extendida (opuesta a la PCAP simple) al tráfico de valor elevado al que aplica la Acción **alert (alertar)**. Aplique la PCAP usando la misma lógica que usa para decidir qué trafico registrar y tome las capturas de paquetes (PCAP) del tráfico que registra. Aplique PCAP única al tráfico que bloquea. El número predeterminado de paquetes que registra y envía un PCAP amplio al plano de gestión es de cinco paquetes, que es el valor recomendado. En la mayoría de los casos, capturar cinco paquetes proporciona suficiente información para analizar una amenaza. Si se envía demasiado tráfico de PCAP al plano de gestión, capturar más de cinco paquetes podría provocar el descarte de PCAP.

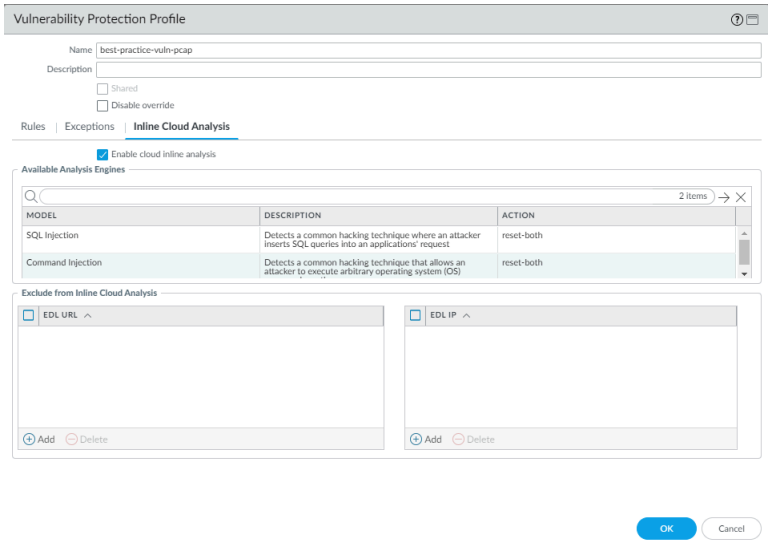
*Si desea obtener más granularidad para ajustar el perfil, cree reglas separadas con las configuraciones de **Action (Acción)** y **Packet Capture (Captura de paquetes)** como se describe. Por ejemplo, cree una regla para gravedades críticas, altas y medias para servidores y otra regla similar para clientes, o cree reglas separadas para cada gravedad para clientes y servidores para lograr el nivel de granularidad y control que desea.*

*Las capturas de paquetes consumen recursos del plano de gestión. Compruebe los recursos del sistema [por ejemplo, **Dashboard (Panel)** > **System Resources (Recursos del sistema)**] para comprender el uso antes y después de implementar la captura de paquetes, para asegurarse de que su sistema tenga recursos suficientes para realizar las capturas de paquetes que desea.*

Habilite la captura de paquetes (PCAP) para cada regla para que pueda rastrear el origen de los posibles ataques. Descargue actualizaciones de contenido automáticamente e instálelas cuanto antes, de modo que la firma siempre permanezca actualizada.



Para **Inline Cloud Analysis (Análisis en línea en la nube)**, establezca la **Action (Acción)** en **reset-both (restablecer ambas)** para bloquear técnicas de jaqueo comunes.



¿Por qué necesito este perfil?

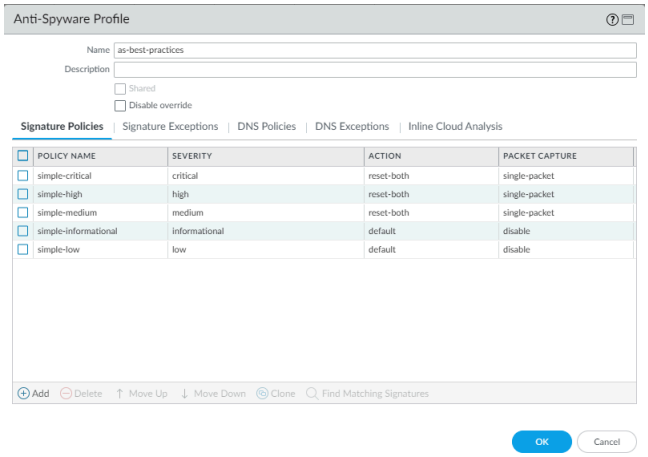
Sin protección estricta contra las vulnerabilidades, los atacantes pueden aprovechar las vulnerabilidades del lado del cliente y del lado del servidor para afectar a los usuarios finales. Por ejemplo, un atacante podría aprovechar una vulnerabilidad para instalar código malintencionado en sistemas cliente o usar un Exploit Kit para suministrar automáticamente cargas útiles malintencionadas a los usuarios finales. Los perfiles de protección de vulnerabilidad evitan que un atacante utilice las vulnerabilidades en hosts internos para moverse lateralmente por la red.

Perfil de antispyware recomendado para la puerta de enlace de Internet

Adjunte un perfil de antispyware a todo el tráfico permitido para detectar tráfico de comando y de control (C2) iniciado desde código malintencionado que se ejecuta en un servidor o extremo, y evitar que los sistemas afectados establezcan una conexión saliente desde su red. Duplique el perfil antispyware estricto predefinido y edítelo. Para garantizar la disponibilidad de aplicaciones críticas para el negocio, realice una transición segura de los perfiles antispyware a las prácticas recomendadas. Edite el perfil para habilitar el sinkhole DNS y la captura de paquetes (PCAP) a fin de facilitar el rastreo de endpoints que intentan resolver dominios malintencionados. Conserve la **Action (Acción)** predeterminada para restablecer la conexión cuando el cortafuegos detecte una amenaza de gravedad media, alta o crítica y habilite PCAP simple para dichas amenazas.

Permita el tráfico solo a servidores DNS autorizados. Utilice el servicio de seguridad DNS para evitar conexiones a servidores DNS maliciosos.

Si trata las aplicaciones internas de manera diferente a las aplicaciones externas, es posible que necesite un perfil Antispyware para el tráfico de Internet y un perfil Antispyware diferente para el tráfico interno.



No habilite PCAP para la actividad informativa debido a que genera un volumen relativamente elevado de tráfico y normalmente no es útil en comparación con los PCAP para posibles amenazas. Aplique PCAP extendida (opuesta a la PCAP simple) al tráfico de valor elevado al que aplica la Acción **alert (alertar)**. Aplique la PCAP usando la misma lógica que usa para decidir qué trafico registrar y tome las capturas de paquetes (PCAP) del tráfico que registra. Aplique PCAP única al tráfico que bloquea. El número predeterminado de paquetes que registra y envía un PCAP amplio al plano de gestión es de cinco paquetes, que es el valor recomendado. En la mayoría de los casos, capturar cinco paquetes proporciona suficiente información para analizar una amenaza. Si se envía demasiado tráfico de PCAP al plano de gestión, capturar más de cinco paquetes podría provocar el descarte de PCAP.

*Las capturas de paquetes consumen recursos del plano de gestión. Compruebe los recursos del sistema [por ejemplo, **Dashboard (Panel)** > **System Resources (Recursos del sistema)**] para comprender el uso antes y después de implementar la captura de paquetes, para asegurarse de que su sistema tenga recursos suficientes para realizar todas las capturas de paquetes que desee.*

Configure las políticas DNS para proteger su red de consultas de DNS a dominios maliciosos. Para obtener la mejor seguridad, utilice el servicio de seguridad DNS para proteger su tráfico DNS. De lo contrario, utilice conjuntos de firmas DNS descargables y disponibles localmente (incluidos con las actualizaciones de antivirus y WildFire).

Redirija el tráfico malicioso en lugar de bloquearlo para identificar hosts potencialmente comprometidos que intentan acceder a dominios sospechosos rastreando los hosts e impidiéndoles acceder a esos dominios. Para las categorías de dominio que representan una amenaza mayor, configure un nivel de gravedad de registro más alto y/o ajustes de captura de paquetes para ayudar a determinar si el ataque fue exitoso, identificar los métodos de ataque y proporcionar un mejor contexto general.

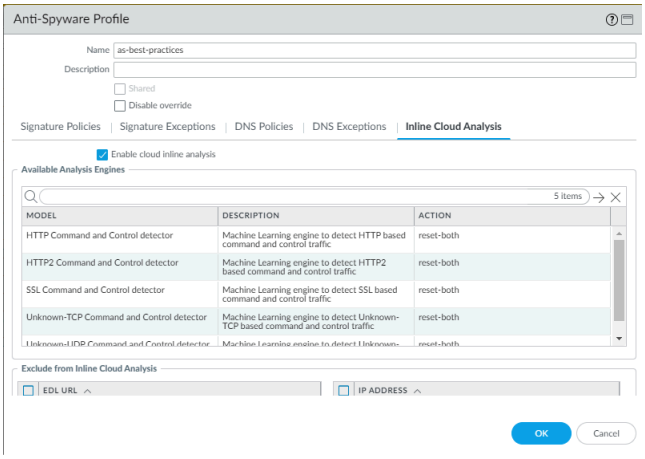
Configure el DNS predeterminado de Palo Alto Networks y las categorías de origen de firma DNS individuales (PAN-OS 10.0 y posteriores):

Origen de firma DNS	Gravedad de logs	Acción de política	Captura de paquetes
Contenido de Palo Alto Networks			
default-paloalto-dns	predeterminado	sinkhole	extended-capture

Origen de firma DNS	Gravedad de logs	Acción de política	Captura de paquetes
DNS Security			
Dominios de comando y control	alto (predeterminado)	sinkhole	extended-capture
Dominios alojados en el DNS dinámico	informativo (predeterminado)	sinkhole	paquete simple
Dominios de grayware	bajo (opción predeterminada)	sinkhole	paquete simple
Dominios de malware	medio (predeterminado)	sinkhole	paquete simple
Dominios estacionados	informativo (predeterminado)	sinkhole	deshabilitado (predeterminado)
Dominios de phishing	bajo (opción predeterminada)	sinkhole	paquete simple
Evitación de proxy y anonimizadores	bajo (opción predeterminada)	sinkhole	paquete simple
Dominios recién registrados	informativo (predeterminado)	sinkhole	paquete simple
Dominios de seguimiento de anuncios	informativo (predeterminado)	sinkhole	paquete simple

Para el **Inline Cloud Analysis (Análisis en línea de la nube)** (requiere una suscripción a Advanced Threat Prevention), habilite el **Cloud inline analysis (Análisis en línea de la nube)** para todo el tráfico saliente. Establezca la **Action (Acción)** en **Reset-both (Restablecer ambos)** para todos los modelos.

Los entornos aislados no pueden utilizar la prevención avanzada de amenazas, Advanced Threat Prevention, porque es un servicio en la nube y requiere una conexión a la nube.



Perfil de filtrado de URL recomendado para la puerta de enlace de Internet

Utilice el Filtrado de URL avanzado para evitar el acceso a contenido web con alto riesgo de actividad maliciosa. Adjunte un perfil de filtrado URL para todas las reglas que permiten el acceso a las aplicaciones basadas en la web, para proteger contra URL que Palo Alto Netwoks ha observado que alojan software malintencionado, malware en potencia, riesgo de responsabilidad y contenido vulnerable.

Debe habilitar el descifrado para aprovechar el filtrado de URL porque debe descifrar el tráfico para revelar la URL exacta, de forma que el cortafuegos pueda tomar la acción adecuada. Como mínimo, descifrar el tráfico de riesgo alto y medio.

Para garantizar la disponibilidad de aplicaciones críticas para el negocio, Transición segura de perfiles de filtrado URL a las prácticas recomendadas. Un perfil de filtrado de URL de prácticas recomendadas establece todas las categorías de URL peligrosas conocidas y envíos de credenciales en bloquear. El objetivo es bloquear las siguientes categorías:

- Establezca todas las acciones para categorías de URL maliciosas en bloquear, tanto el acceso al sitio como el envío de credenciales de usuario. Realice las excepciones apropiadas para las pruebas PEN, la investigación de amenazas y la seguridad de la información según sea necesario:
  - **command-and-control** (comando y control): las URL y los dominios que el malware o los sistemas comprometidos utilizan para comunicarse con el servidor remoto de un atacante.
  - **Grayware**: estos sitios no cumplen con la definición de virus ni representan una amenaza directa a la seguridad, pero influyen en los usuarios para que otorguen acceso remoto o realicen otras acciones no autorizadas. Los sitios de grayware incluyen estafas, actividades ilegales, actividades delictivas, adware y otras aplicaciones no deseadas y no solicitadas, incluidos dominios de “secuestros de URL”.
  - **malware**: sitios conocidos por alojar malware o usados para actividades de comando y control (C2).
  - **phishing**: sitios conocidos por albergar páginas de phishing de información personal y de credenciales, incluidas estafas de soporte técnico y scareware.
  - **ransomware**: sitios conocidos por distribuir ransomware.
  - **scanning-activity** (actividad de análisis): sitios que exploran en busca de vulnerabilidades existentes o que llevan a cabo ataques dirigidos.

- Algunas categorías de URL tienen grandes posibilidades de ser maliciosas, pero definitivamente no lo son. Configure todas las acciones para estas categorías de URL, para bloquear tanto el acceso al sitio como el envío de credenciales de usuario. Realice las excepciones apropiadas para las pruebas PEN, la investigación de amenazas y la seguridad de la información según sea necesario:
  - **dynamic-dns** (dns dinámico): sistemas con direcciones IP asignadas dinámicamente que a menudo se utilizan para entregar cargas útiles de malware o malware de comando y control.

    Si tiene un propósito comercial para un dominio DNS dinámico, asegúrese de permitir esos URL en su perfil de filtrado de URL.
  - **hacking** (jaqueo): sitios relacionados con el acceso ilegal o cuestionable a software y equipos informáticos, así como para su uso. Incluye sitios que facilitan evitar los sistemas de licencias y derechos digitales.

    Haga excepciones a esta categoría para los usuarios apropiados de pruebas PEN e investigación de amenazas.
  - **insufficient-content** (contenido insuficiente): sitios web y servicios que presentan páginas de prueba, sin contenido, brindan acceso a la API no destinado a la visualización del usuario final o requieren autenticación sin mostrar ningún otro contenido.
  - **newly-registered-domains** (dominios recién registrados): dominios que los algoritmos de generación de dominios suelen generar o que los ciberdelincuentes generan para actividades maliciosas.
  - **not-resolved** (no resuelto): si no se puede acceder a la nube PAN-DB y la URL no está en la caché de filtrado de URL del cortafuegos, el cortafuegos no puede resolver ni identificar la categoría de URL.

    *Para mayor seguridad, habilite **Hold client request for category lookup (Retener solicitud del cliente para consulta de categoría)** para darle al cortafuegos más tiempo para resolver la categoría de URL. Esto extiende el tiempo que el cortafuegos tiene para consultar el tipo de categoría desde la nube y da como resultado una mejor seguridad, aunque podría aumentar la latencia.*
  - **parked** (estacionado): dominios que a menudo se utilizarán para phishing de credenciales o robo de información personal.
  - **proxy-avoidance-and-anonymizers (Evasión de proxy y anonimizadores)**: URL y servicios a menudo utilizados para desviar productos de filtrado de contenido.
  - **unkown** (desconocido): sitios aún no identificados por Palo Alto Networks (PAN-DB).

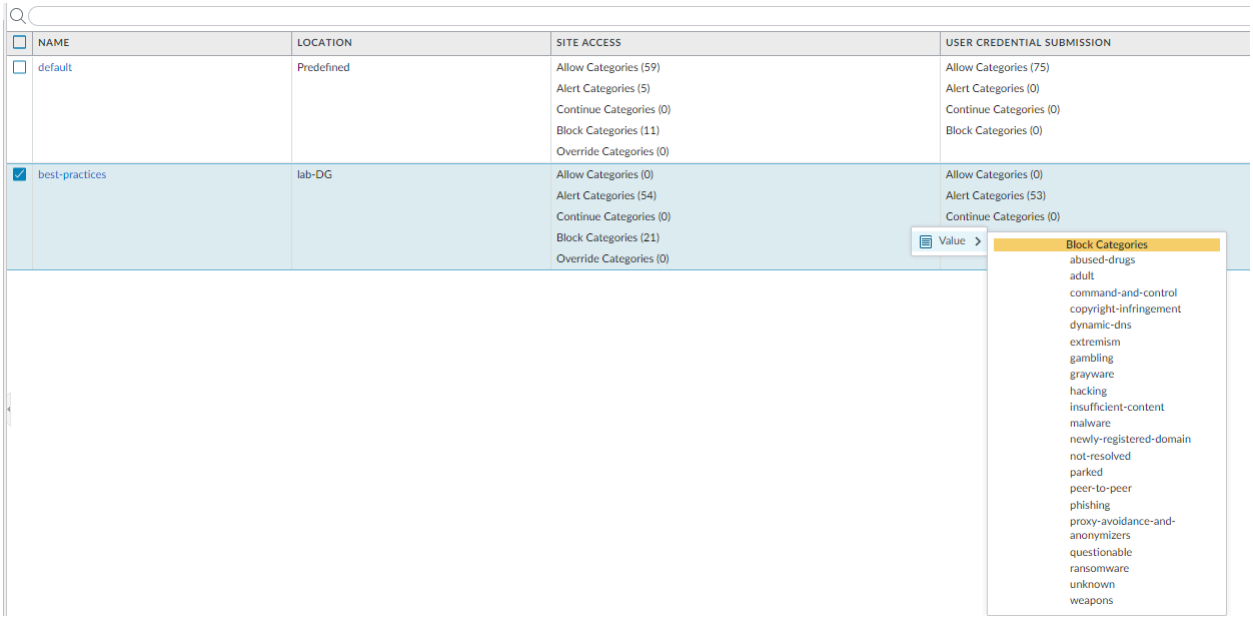
    Las actualizaciones en tiempo real de PAN-DB detectan sitios desconocidos después del primer intento de acceder a uno de ellos, por lo que el cortafuegos identifica las URL desconocidas rápidamente y luego las maneja según la categoría de URL real del sitio.

    Si la disponibilidad es vital para la empresa y debe permitir el tráfico, avise sobre los sitios desconocidos, aplique al tráfico los perfiles recomendados de seguridad e investigue las alertas relacionadas con el tráfico.

- Establezca la acción para el acceso al sitio y el envío de credenciales de usuario en bloquear, para que bloquee las siguientes categorías de URL según los requisitos legales o comerciales y el posible riesgo de responsabilidad. Si no bloquea estos sitios, alerte sobre ellos y aplique perfiles de seguridad estrictos al tráfico.
  - **abused-Drugs** (consumo de drogas): sitios que promueven el consumo de estupefacientes legales e ilegales.
  - **adult** (adultos): todos los sitios que contienen contenido para adultos de cualquier tipo, incluidos juegos y cómics, así como material, medios, arte, foros y servicios sexualmente explícitos.
  - **copyright-infringement** (violación de derechos de autor): dominios con contenido ilegal que plantea un riesgo de responsabilidad.
  - **extremism** (extremismo): sitios web que promueven el terrorismo, el racismo, la explotación infantil, etc.
  - **gambling** (juegos de azar): sitios web de loterías y juegos de azar.
  - **peer-to-peer**: intercambio de torrents, programas de descarga, archivos multimedia u otras aplicaciones de software entre individuos. (No incluye sitios de shareware o freeware).
  - **questionable** (cuestionable): sitios que promueven el humor de mal gusto y contenido ofensivo dirigido a grupos demográficos específicos.
  - **weapons** (armas): venta, revisión, descripciones o instrucciones sobre armas y su uso.

  Considere también cómo desea gestionar las categorías de URL de criptomonedas, y alcohol y tabaco. Alerte sobre ellos y aplique perfiles de seguridad estrictos al tráfico o bloquéelos, según las necesidades de su negocio.
- Bloquee el Envío de credenciales de usuario para la categoría de alto riesgo. (No bloquee el acceso al sitio para la categoría de alto riesgo).

Además de bloquear categorías de riesgo conocidas, también debe alertar sobre todas las demás categorías para tener visibilidad de los sitios que sus usuarios visitan. Si necesita introducir gradualmente una política de bloqueo, configure las categorías para continuar y cree una página de respuesta personalizada para informar a los usuarios sobre sus políticas de uso aceptable y alertarlos sobre el hecho de que están entrando en un sitio que podría suponer una amenaza. Esto preparará el camino para que bloquee las categorías después de un período de supervisión.



Deshabilite **Log Container Page Only (Registrar solo página del contenedor)** en el perfil dado que está habilitada de forma predeterminada. Si solo registra páginas de contenedores, pierde la visibilidad de aplicaciones funcionales como publicación, carga, descarga, etc. Deshabilite **Log Container Page Only (Registrar solo página del contenedor)** para ver el log completo y ver la aplicación funcional real.

Si su entorno es un centro educativo que recibe fondos federales, habilite **Safe Search Enforcement (Aplicación de búsquedas seguras)** (requisito legal).

Si ejecuta PAN-OS 9.0.4 o posterior, habilite la opción para retener las solicitudes de los clientes (introduzca **`config`** y luego **`set deviceconfig setting ctd hold-client-request yes`**) para asegúrese de que el cortafuegos gestione las solicitudes web de los usuarios de la manera más segura posible. De forma predeterminada, el cortafuegos permite solicitudes mientras busca una categoría de URL no almacenada en la caché en PAN-DB y luego aplica la política apropiada cuando el servidor responde. Retenga las solicitudes durante esta búsqueda para maximizar la seguridad (esto podría aumentar la latencia, pero es la opción más segura). Para obtener más información, consulte Configuración del filtrado de URL.

¿Qué sucede si no puedo bloquear todas las categorías recomendadas?

Si los usuarios necesitan acceder a sitios en categorías bloqueadas por motivos comerciales, cree una lista de permitidos solo para los sitios específicos en una regla que permita solo a los usuarios y aplicaciones necesarios, si cree que el riesgo está justificado. Recuerde que las leyes y regulaciones locales que rigen los tipos de sitios que puede bloquear, no pueden bloquear y debe bloquear. En las categorías de riesgo a las que decide permitir el acceso, configure la protección frente a phishing de credenciales para garantizar que los usuarios no envíen credenciales corporativas a un sitio que pueda albergar un ataque de phishing.

Si permite el tráfico a categorías de URL maliciosas y potencialmente maliciosas, o a sitios web que plantean posibles problemas de responsabilidad, los riesgos incluyen:

- Categorías de URL maliciosas:
  - **command-and-control (Comando y control)**: los dominios y URL de comando y control utilizados por software malintencionado y sistemas afectados para comunicarse de manera furtiva con el servidor remoto de un atacante y recibir comandos malintencionados o filtrar datos.
  - **grayware**: sitios web y servicios que no cumplen con la definición de virus, pero que son maliciosos o cuestionables y podrían reducir el rendimiento del dispositivo y causar riesgos de seguridad. Antes de la versión de lanzamiento de contenido 8206, el cortafuegos colocaba el grayware en la categoría de malware o URL cuestionable. Si no está seguro sobre si bloquear el grayware, comience por alertar sobre el grayware, investigue las alertas y, después, decida si bloquear el grayware o continuar alertando sobre el grayware.
  - **malware**: sitios conocidos por alojar malware o usados para actividades de comando y control (C2), y que pueden exhibir kits de vulneración.
  - **phishing**: conocidos por alojar páginas de suplantación de identidad o phishing para identificación personal.
  - **ransomware**: sitios conocidos por distribuir ransomware.
  - **scanning-activity** (actividad de análisis): sitios que exploran en busca de vulnerabilidades existentes o que llevan a cabo ataques dirigidos.
- Categorías de URL potencialmente maliciosas:
  - **dynamic-dns**: hosts y nombres de dominio para sistemas que asignan direcciones IP dinámicamente y que a menudo se usan para enviar cargas de malware o tráfico C2. Además, los dominios DNS dinámicos no atraviesan el mismo proceso de examen que los dominios que están registrados por una empresa de registro de dominios reconocida, por lo cual son menos fiables.
  - **hacking** (jaqueo): sitios relacionados con el acceso ilegal o cuestionable a software y equipos informáticos, así como para su uso. Incluye sitios que facilitan evitar los sistemas de licencias y derechos digitales.

    Haga excepciones a esta categoría para los usuarios apropiados de pruebas PEN e investigación de amenazas.
  - **insufficient-content** (contenido insuficiente): sitios web y servicios que presentan páginas de prueba, sin contenido, brindan acceso a la API no destinado a la visualización del usuario final o requieren autenticación sin mostrar ningún otro contenido.
  - **newly-registered-domain (dominio recién registrado)**: dominios nuevos que, a menudo, se generan a propósito o con algoritmos de generación de dominios para destinarlos a actividades malintencionadas.
  - **not-resolved** (no resuelto): si no se puede acceder a la nube PAN-DB y la URL no está en la caché de filtrado de URL del cortafuegos, el cortafuegos no puede resolver ni identificar la categoría de URL.

    *Para mayor seguridad, habilite **Hold client request for category lookup (Retener solicitud del cliente para consulta de categoría)** para darle al cortafuegos más tiempo para resolver la categoría de URL. Esto extiende el tiempo que el cortafuegos tiene para consultar el tipo de categoría desde la nube y da como resultado una mejor seguridad, aunque podría aumentar la latencia.*
  - **parked**: dominios registrados por personas, que a menudo más tarde se descubre que se usan para el phishing de credenciales. Estos dominios pueden ser similares a dominios legítimos, por

ejemplo, pal0alto0netw0rks.com, con la intención de realizar phishing para obtener credenciales o información de identificación personal. O bien, podrían ser dominios para los cuales una persona compra los derechos con la esperanza de que un día pudiesen ser valiosos, como por ejemplo, panw.net.

- **proxy-avoidance-and-anonymizers (Evasión de proxy y anonimizadores)**: URL y servicios a menudo utilizados para desviar productos de filtrado de contenido.
- **unknown (desconocido)**: sitios que PAN-DB no ha identificado todavía. Si la disponibilidad es vital para la empresa y debe permitir el tráfico, avise sobre los sitios desconocidos, aplique al tráfico los perfiles recomendados de seguridad e investigue las alertas.

Las actualizaciones en tiempo real de PAN-DB obtienen información de los sitios desconocidos tras el primer intento de acceso. Así, las URL desconocidas se identifican al instante y se convierten en URL conocidas que puede manejar el cortafuegos según la categoría que les corresponda.

- Categorías de URL con riesgo potencial de responsabilidad:
  - **Abused-Drugs** (consumo de drogas): sitios web que promueven el consumo de drogas legales e ilegales, la venta y el uso de parafernalia relacionada con estupefacientes, y la producción o venta de drogas.
  - **adulto** (adultos): sitios web que podrían no ser adecuados para el lugar de trabajo.
  - **copyright-infringement (infracción de derechos de autor)**: dominios con contenido ilegal, como contenido que permite la descarga ilegal de software u otra propiedad intelectual, que podría acarrear una responsabilidad civil. Esta categoría se introdujo para permitir el cumplimiento con las leyes de protección infantil requeridas en el sector de la educación, así como también las leyes en países que exigen que los proveedores de Internet eviten que los usuarios compartan material con derechos de autor a través de su servidor.
  - **extremism (extremismo)**: sitios web que promueven el terrorismo, el racismo, el fascismo u otras visiones extremistas que discriminan a personas o grupos de diferentes orígenes étnicos, religiones u otras creencias. Esta categoría se introdujo para permitir el cumplimiento con las leyes de protección infantil requeridas en el sector de la educación. En algunas regiones, la legislación y las normativas prohíben que se permita el acceso a sitios extremistas, lo que podría acarrear una responsabilidad civil.
  - **gambling** (juegos de azar): sitios web de loterías o juegos de azar que facilitan el intercambio de dinero real y/o virtual. También sitios web que proporcionan tutoriales, consejos u otra información sobre juegos de azar, incluidas probabilidades y grupos de apuestas.
  - **peer-to-peer**: sitios web a los que se accede o que se utilizan para el intercambio de torrents, programas de descarga, archivos multimedia u otras aplicaciones de software entre individuos, principalmente para proteger contra las capacidades de descarga de bitTorrent. No incluye sitios de shareware o freeware.
  - **questionable** (cuestionable): sitios web que contienen contenido potencialmente ofensivo dirigido a grupos demográficos específicos o individuos, actividad delictiva, actividad ilegal y esquemas para hacerse rico rápidamente.
  - **weapons** (armas): sitios web que venden, revisan, describen o proporcionan instrucciones sobre armas y su uso y que podrían no ser apropiados en el lugar de trabajo.

El perfil de filtrado de URL predeterminado bloquea las categorías de malware, phishing y URL de comando y control, pero no el resto de las categorías recomendadas para bloquear como categorías para bloquear. Este perfil también bloquea otras categorías, como las de contenido sospechoso, contenido para adultos, abuso de drogas, apuestas y armas. El bloqueo de estas categorías de URL depende de los requisitos de su empresa. Por ejemplo, una universidad probablemente no restringirá el acceso de los estudiantes a la mayoría de estos sitios porque la disponibilidad es importante, pero un negocio que primero valora la seguridad podría bloquear a todos ellos.

Ejemplos de URL Filtering

El filtrado de URL funciona con el bloqueo de archivos, el descifrado, las listas dinámicas externas (EDL), la generación de logs y otras capacidades de seguridad para crear políticas granulares que pueden ir más allá de simplemente bloquear o permitir categorías completas de URL. Utilice los pasos de transición seguros para el filtrado de URL para evaluar qué sitios desea permitir y qué sitios desea bloquear, luego implemente políticas que se ajusten a los requisitos de su negocio. Por ejemplo:

- Utilice categorías de URL basadas en riesgos (riesgo alto, riesgo medio y riesgo bajo) en combinación con otras categorías de URL para centrarse en el descifrado o en el bloqueo del tráfico. Por ejemplo, usted puede:
  - Bloquear el tráfico a sitios web de alto riesgo en la categoría de servicios financieros.
  - Descifrar todo el tráfico web de alto y medio riesgo.
  - Descifrar el tráfico de riesgo alto y medio a categorías de URL específicas si el cortafuegos no tiene recursos suficientes para descifrar todo el tráfico deseado.
- Registre todos los agentes de usuario y las referencias, todos los URL y todas las descargas de archivos para dominios de categorías de alto y medio riesgo para aumentar la visibilidad.
- Permita el acceso a categorías como sitios personales y blogs mientras aplica un perfil de bloqueo de archivos al tráfico para evitar la descarga de contenido peligroso como archivos .exe, .scr y otros archivos potencialmente maliciosos.
- Utilice la EDL predefinida de **Palo Alto Networks: direcciones IP blindadas** para evitar el acceso a sitios alojados en ISP blindados, especialmente si permite el acceso a sitios financieros de alto o medio riesgo.
- Utilice combinaciones de categorías de URL para simplificar la política.

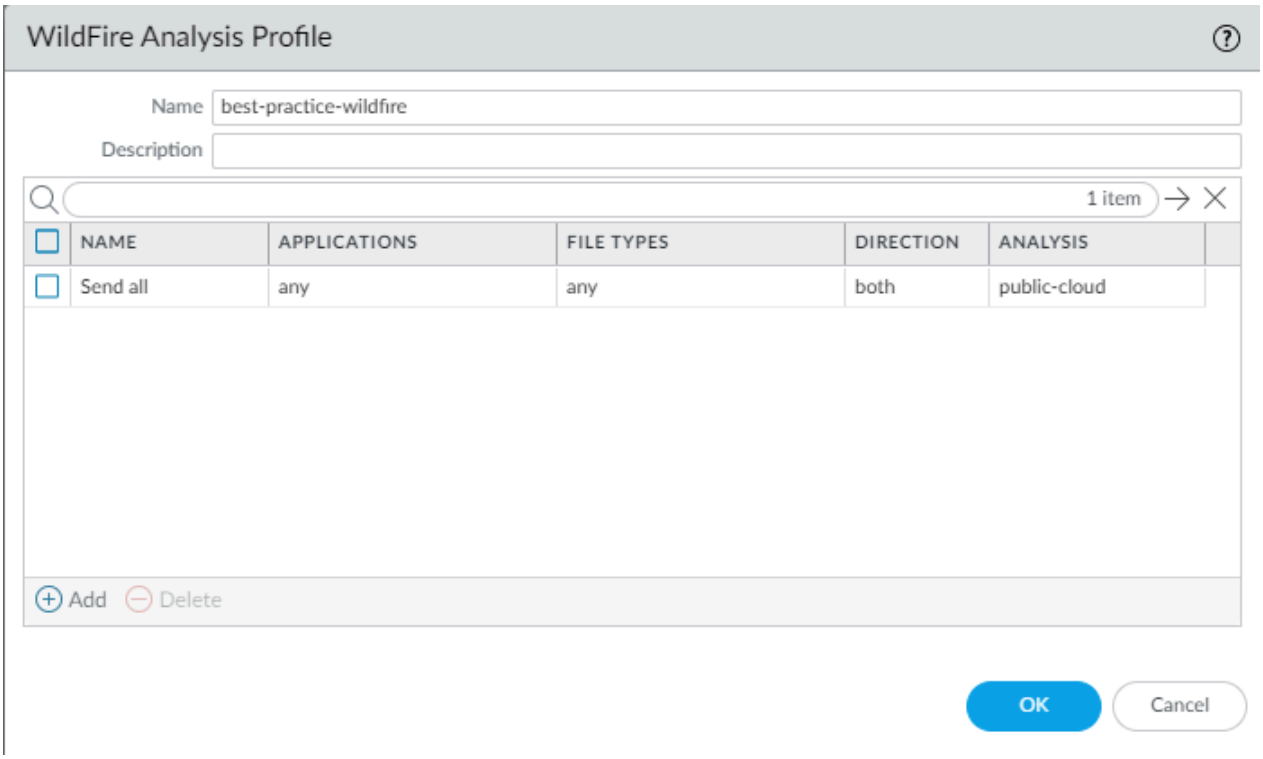
Perfil de análisis de WildFire recomendado para la puerta de enlace de Internet

Envíe archivos a WildFire para su análisis y para proteger su red de amenazas desconocidas. Sin esta protección, los atacantes pueden infiltrarse en la red y aprovechar las vulnerabilidades en las aplicaciones que sus empleados usan a diario. Debido a que WildFire protege contra las amenazas desconocidas, es su mejor defensa frente a las amenazas avanzadas persistentes (advanced persistent threats, APT).

Configure las actualizaciones de contenido en el dispositivo WildFire para que se descarguen e instalen automáticamente en tiempo real, de modo que siempre tenga el soporte más reciente.

El perfil de análisis de WildFire recomendado envía todos los archivos en ambas direcciones (carga y descarga) a WildFire para su análisis. Específicamente, asegúrese de enviar todos los archivos PE (si no los está bloqueando de acuerdo con las prácticas recomendadas de bloqueo), archivos Adobe Flash y Reader

(PDF, SWF), archivos Microsoft Office (PowerPoint, Excel, Word, RTF), archivos Java (Java, CLASS) y archivos Android (.APK).



Establezca alertas de malware a través de correos electrónicos, SNMP o un servidor syslog, de modo que el cortafuegos notifique automáticamente cuando encuentre un posible problema. Cuanto antes aísle un host en riesgo, menor será la probabilidad de que el malware antes desconocido se propague a otros dispositivos en el centro de datos y será más fácil solucionar el problema.

De ser necesario, puede limitar las aplicaciones y los tipos de archivos que se envían para analizar según la dirección del tráfico.

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

Definir la política de seguridad de puerta de enlace de Internet inicial

El objetivo de la política de seguridad para la puerta de enlace de Internet de prácticas recomendadas es usar el cumplimiento positivo de las aplicaciones que están permitidas. Sin embargo, lleva tiempo identificar las aplicaciones exactas que se ejecutan en su red, qué aplicaciones son críticas para su negocio y quién necesita acceder a cada aplicación. Para crear una política de seguridad basada en reglas de autorización de aplicaciones; comience con una base de reglas que permita libremente el uso de las aplicaciones que usted autoriza oficialmente para los usuarios, así como las aplicaciones comerciales generales y aplicaciones personales toleradas (si es lo adecuado para su negocio).

La política inicial incluye reglas que bloquean explícitamente aplicaciones y direcciones IP maliciosas conocidas, y reglas de permiso temporales que ayudan a ajustar su política y preservar la disponibilidad de las aplicaciones mientras realiza la transición a una política de prácticas recomendadas.

Para aplicar políticas de seguridad coherentes en varias ubicaciones, reutilice las plantillas y pilas de plantillas *de modo que se apliquen las mismas políticas en cada cortafuegos de puerta de enlace de Internet de cada ubicación. Las plantillas usan variables para aplicar valores para dispositivos específicos como direcciones IP, FQDN, etc., conservar una política de seguridad global y reducir el número de plantillas y pilas de plantillas que debe gestionar.*

Los siguientes temas describen cómo crear la base de reglas inicial, describen por qué cada regla es necesaria y muestra los riesgos que supone ignorar las recomendaciones de las prácticas recomendadas:

- PASO 1: Crear reglas basadas en las fuentes fiables de inteligencia de amenazas
- Paso 2: Crear las Reglas de aplicaciones permitidas
- Paso 3: Crear las reglas de bloqueo de aplicaciones
- Paso 4: Crear reglas de ajuste temporales
- Paso 5: Habilitar la creación de logs para el tráfico que no coincide con ninguna regla

PASO 1: Crear reglas basadas en las fuentes fiables de inteligencia de amenazas

Bloquee el tráfico de hosts que Palo Alto Networks y fuentes de terceros fiables consideren maliciosos. Una licencia de prevención de amenazas avanzada, Advanced Threat Prevention, (o una licencia de Prevención de amenazas heredada activa) incluye listas dinámicas externas (EDL) integradas que contienen direcciones IP maliciosas conocidas. Utilice EDL en la política para bloquear el tráfico malicioso. Palo Alto Networks compila y actualiza dinámicamente las listas basándose en la inteligencia sobre amenazas más reciente. Los cortafuegos reciben e implementan actualizaciones dinámicas sin necesidad de un reinicio.

STEP 1 | Bloquee el tráfico desde y hacia las direcciones IP que Palo Alto Networks identifica como maliciosas.

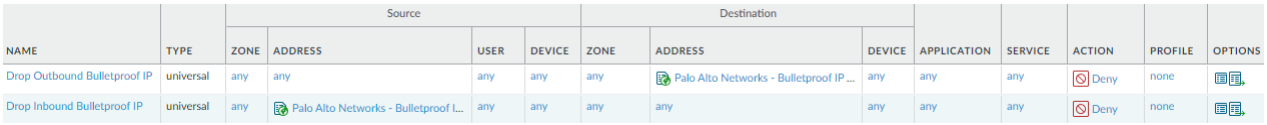
¿Por qué necesito estas reglas?	Aspectos destacados de las reglas
❑ Esta regla lo protege contra direcciones IP que Palo Alto Networks comprobó que se utilizan casi exclusivamente para distribuir malware, iniciar actividades de comando y control, e iniciar ataques.	• Una regla bloquea el tráfico saliente hacia direcciones IP maliciosas conocidas, mientras que la otra regla bloquea el tráfico entrante de esas direcciones. • Establezca la lista dinámica externa **Palo Alto Networks - Known malicious IP addresses (Palo Alto Networks: direcciones IP malintencionadas conocidas)** como la dirección de destino de la regla para tráfico saliente y como la dirección de origen de la regla para el tráfico entrante. • Deniegue el tráfico que coincida con estas reglas. • Habilite la generación de logs para el tráfico que coincide con estas reglas, para poder investigar las posibles amenazas en su red. • Debido a que estas reglas detienen el tráfico malicioso, protegen el tráfico de cualquier usuario que se ejecute en cualquier puerto.

		Source				Destination							
NAME	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Drop Outbound Malicious IP	universal	any	any	any	any	any	Palo Alto Networks - Known malicio...	any	any	any	Deny	none	
Drop Inbound Malicious IP	universal	any	Palo Alto Networks - Known malic...	any	any	any	any	any	any	any	Deny	none	

STEP 2 | Bloquee el tráfico hacia y desde los proveedores de alojamiento a prueba de balas.

¿Por qué necesito estas reglas?	Aspectos destacados de las reglas
❑ Esta regla lo protege contra las direcciones IP que Palo Alto Networks ha demostrado que pertenecen a proveedores de alojamiento a prueba de balas. Los proveedores de alojamiento a prueba de balas tienen restricciones de contenido limitadas o no tienen restricciones, y no registran eventos. Los sitios a prueba de balas son lugares ideales desde donde lanzar ataques de comando y control (C2) y realizar actividades ilegales porque todo vale y no se controla nada.	• Una regla bloquea el tráfico saliente hacia direcciones de hospedaje a prueba de balas, mientras que otra regla bloquea el tráfico entrante a esas direcciones. • Establezca la lista dinámica externa **Palo Alto Networks - Bulletproof IP addresses (Palo Alto Networks: direcciones IP a prueba de balas)** como la dirección de Destino para la regla de tráfico saliente y como la dirección de Origen para la regla de tráfico entrante. • Deniegue el tráfico que coincida con estas reglas.

¿Por qué necesito estas reglas?	Aspectos destacados de las reglas
	• Habilite la creación de logs para el tráfico que coincide con esta regla, para poder investigar las posibles amenazas en su red. • Debido a que estas reglas detienen el tráfico malicioso, protegen el tráfico de cualquier usuario que se ejecute en cualquier puerto.



		Source				Destination							
NAME	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Drop Outbound Bulletproof IP	universal	any	any	any	any	any	Palo Alto Networks - Bulletproof IP ...	any	any	any	Deny	none	
Drop Inbound Bulletproof IP	universal	any	Palo Alto Networks - Bulletproof I...	any	any	any	any	any	any	any	Deny	none	

STEP 3 | Bloquee y registre el tráfico desde y hacia las direcciones IP de alto riesgo de asesores de confianza sobre amenazas.

¿Por qué necesito estas reglas?	Aspectos destacados de las reglas
A pesar de que Palo Alto Networks no cuenta con evidencia directa de la maldad de las direcciones IP en la fuente de direcciones IP de alto riesgo, los asesores de amenazas las han vinculado con comportamientos maliciosos. ❑ Bloquee y registre el tráfico como se muestra en este ejemplo. ❑ Si debe permitir una dirección IP de alto riesgo por motivos comerciales, cree una regla de política de seguridad con perfiles de seguridad estrictos que permita solo esa dirección IP, y colóquela delante de la regla de bloqueo de direcciones IP de alto riesgo en la base de reglas. Supervise y registre de cerca cualquier dirección IP de alto riesgo que elija permitir.	• Una regla registra el tráfico saliente bloqueado hacia direcciones IP de alto riesgo y otra regla registra el tráfico entrante a dichas direcciones. • Establezca la lista dinámica externa **Palo Alto Networks - High risk IP addresses (Palo Alto Networks: direcciones IP de alto riesgo)** como la dirección de destino de la regla para tráfico saliente y como la dirección de origen de la regla para el tráfico entrante. • Si permite el tráfico, aplique perfiles de seguridad de prácticas recomendadas. • Dado que estas reglas detienen el tráfico malicioso, protegen el tráfico de cualquier usuario que se ejecute en cualquier puerto y para cualquier aplicación.

		Source				Destination							
NAME	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Block Outbound High Risk IPs	universal	any	any	any	any	any	Palo Alto Networks - High risk IP addresses	any	any	any	Deny	none	
Block Inbound High Risk IPs	universal	any	Palo Alto Networks - Known malicious IP addresses	any	any	any	any	any	any	any	Deny	none	

STEP 4 | Igualmente, cree dos reglas que bloqueen y registren el tráfico hacia y desde los nodos de salida de Tor, que a menudo (pero no siempre) están asociados con actividad maliciosa, especialmente en entornos empresariales, utilizando la lista dinámica externa **Palo Alto Networks - Tor exit IP addresses (Direcciones IP de salida de Tor de Palo Alto Networks)**.

Paso 2: Crear las Reglas de aplicaciones permitidas

Identifique su lista de aplicaciones permitidas antes de crear reglas de permisos de aplicación. Crear reglas de permiso basadas en aplicaciones, no en puertos. Excepto para ciertas aplicaciones de infraestructura que requieren acceso de usuario antes de que el cortafuegos pueda identificar al usuario, permita el acceso solo a usuarios conocidos. Cree grupos de usuarios para acceder a aplicaciones permitidas y limite el acceso de los usuarios solo a los usuarios o grupos de usuarios específicos que tienen una necesidad empresarial de acceder a cada aplicación.

Para convertir las reglas basadas en puertos a reglas basadas en aplicaciones o migrar desde un cortafuegos basado en puertos, siga los consejos de Prácticas recomendadas para migrar a políticas basadas en aplicaciones*, que aprovecha el* Policy Optimizer*. Policy Optimizer le ayuda a analizar las reglas basadas en puertos y le muestra las aplicaciones exactas que coinciden con dichas reglas. También le ayuda a encontrar reglas no utilizadas, reglas con aplicaciones no utilizadas (reglas sobreaprovisionadas) y reglas basadas en puertos existentes.*

Coloque reglas específicas por delante de las reglas generales en la base de reglas de políticas de seguridad. De lo contrario, una regla general podría hacer sombra a una regla específica. (La vigilancia es cuando coloca una regla amplia que incluye los mismos criterios de coincidencia que una regla más específica, más alto en la base de reglas que la regla específica, por lo que el tráfico destinado a coincidir con la regla específica coincide con la regla general).

La parte de la base de reglas incluye las reglas que dan permiso a las aplicaciones que identificó como parte de su lista de aplicaciones permitidas, incluidas:

- Las aplicaciones autorizadas que usted aprovisiona y administra para fines comerciales y de infraestructura.
- Los usuarios de aplicaciones empresariales generales pueden necesitar hacer su trabajo.
- Las aplicaciones toleradas que usted decida permitir para uso personal.

Etiquete todas las aplicaciones autorizadas *con la etiqueta Sanctioned (Sancionada) predefinida. Panorama y los cortafuegos consideran a las aplicaciones sin la etiqueta Sanctioned (Sancionada) como aplicaciones no autorizadas.*

Adjunte perfiles de seguridad de prácticas recomendadas para analizar todo el tráfico permitido en busca de amenazas conocidas y desconocidas. Si no ha creado estos perfiles, entonces debe Crear perfiles de seguridad de prácticas recomendadas para la puerta de enlace de Internet. Debido a que no es posible inspeccionar lo que no puede ver, configure el cortafuegos para descifrar tráfico para visibilidad completa e inspección de amenazas.

STEP 1 | Permita el acceso a sus servidores DNS corporativos.

Permita el tráfico solo a servidores DNS autorizados. Utilice el servicio de seguridad DNS para evitar conexiones a servidores DNS maliciosos.

¿Por qué necesito esta regla?	Aspectos destacados de las reglas
❑ El acceso a DNS proporciona servicios de infraestructura de red y es comúnmente aprovechado por los atacantes. ❑ El permitir el acceso únicamente a su servidor DNS interno reduce la superficie de ataque.	• Debido a que la regla es muy específica, colóquela cerca de la parte superior de la base de reglas. • Cree un objeto de dirección para usar para la dirección de destino, a fin de garantizar que los usuarios solo accedan al servidor DNS de su centro de datos. • Debido a que los usuarios necesitan acceso a estos servicios antes de iniciar sesión, permita el acceso a cualquier usuario.

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
IT DNS Services	Best Practice	universal	Users	any	any	any	IT Infrastructure	DNS Servers	any	dns	application-default	Allow		

STEP 2 | Permita el acceso a otros recursos de infraestructura de TI necesarios.

¿Por qué necesito esta regla?	Aspectos destacados de las reglas
❑ Habilite las aplicaciones que proporcionan infraestructura de red y funciones de administración, como NTP, OCSP, STUN y ping. ❑ Si bien el tráfico DNS permitido en la regla anterior se limita a la dirección de destino en el centro de datos, es posible que estas aplicaciones no residan en su centro de datos y, por lo tanto, requieran una regla separada.	• Debido a que estas aplicaciones se ejecutan en el puerto predeterminado, permiten el acceso a cualquier usuario (es posible que los usuarios aún no hayan iniciado sesión y no sepan cuándo se necesitan estos servicios) y tienen una dirección de destino de **any (cualquiera)**, añádalas a un grupo de aplicaciones y cree una regla para permitir el acceso a todos ellas.

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Required Infrastructure	Best Practice	universal	Users	any	any	any	Internet	any	any	Required Infrastructure	application-default	Allow		

STEP 3 | Permita el acceso a aplicaciones SaaS autorizadas de TI.

¿Por qué necesito esta regla?	Aspectos destacados de las reglas
❑ Con las aplicaciones SaaS, los datos patentados residen en la nube. Esta regla garantiza que	• Cree un grupo de aplicaciones para controlar todas las aplicaciones SaaS autorizadas.

¿Por qué necesito esta regla?	Aspectos destacados de las reglas
solo los usuarios conocidos tengan acceso a estas aplicaciones (y a los datos subyacentes). ❑ Analice el tráfico SaaS permitido en busca de amenazas.	• Las aplicaciones SaaS siempre deben ejecutarse en el puerto predeterminado de la aplicación. • Restrinja el acceso a usuarios conocidos. Consulte Crear grupos de usuarios para acceder a Aplicaciones permitidas.

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
IT Sanctioned SaaS Apps	Best Practice	universal	Users	any	known-user	any	Internet	any	any	IT Sanctioned SaaS Applica...	application-default	Allow		

STEP 4 | Permitir el acceso a aplicaciones locales aprovisionadas por TI.

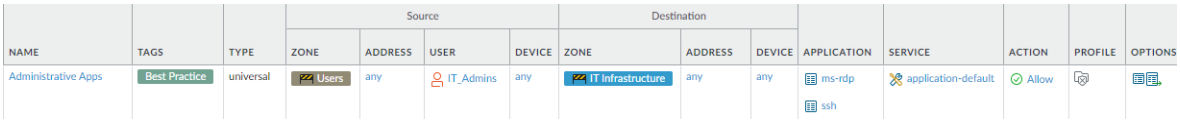
¿Por qué necesito esta regla?	Aspectos destacados de las reglas
❑ Los ataques a menudo utilizan aplicaciones de centro de datos críticas para el negocio, como FTP, durante la etapa de filtración o aprovechan las vulnerabilidades de la aplicación para moverse lateralmente. ❑ Muchas aplicaciones de centros de datos utilizan múltiples puertos. Establecer el Servicio en **application-default** (aplicación predeterminada) habilita de forma segura las aplicaciones en sus puertos estándar. No permita aplicaciones en puertos no estándar, ya que a menudo se asocian con comportamientos evasivos.	• Cree un grupo de aplicaciones para agrupar todas las aplicaciones del centro de datos. • Cree un grupo de direcciones para sus direcciones de servidor de centro de datos. • Restrinja el acceso a usuarios conocidos. Consulte Crear grupos de usuarios para acceder a Aplicaciones permitidas.

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
IT Deployed Apps	Best Practice	universal	Users	any	known-user	any	Business Apps	Data Center	any	IT Deployed Apps	application-default	Allow		

STEP 5 | Permita el acceso a las aplicaciones que necesitan sus usuarios administrativos.

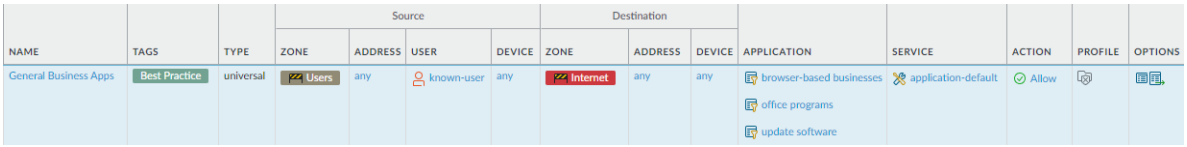
¿Por qué necesito esta regla?	Aspectos destacados de las reglas
❑ Para reducir la superficie de ataque, cree grupos de usuario para el acceso a aplicaciones permitidas. ❑ Debido a que los administradores a menudo necesitan acceder a datos de cuenta delicados y acceder de forma remota a otros sistemas (por ejemplo, RDP), para reducir la superficie de ataque, permita el acceso únicamente a	• Esta regla limita el acceso a los usuarios del grupo IT_admins. • Cree una aplicación personalizada para cada aplicación interna o aplicación que se ejecute en puertos no estándar, para que pueda aplicarlas en los puertos por defecto en lugar de abrir puertos adicionales en la red.

¿Por qué necesito esta regla?	Aspectos destacados de las reglas
los administradores que tienen una necesidad comercial.	• Si tiene diferentes grupos de usuarios para diferentes aplicaciones, cree reglas separadas para un control pormenorizado.



STEP 6 | Habilite el acceso a las aplicaciones comerciales generales.

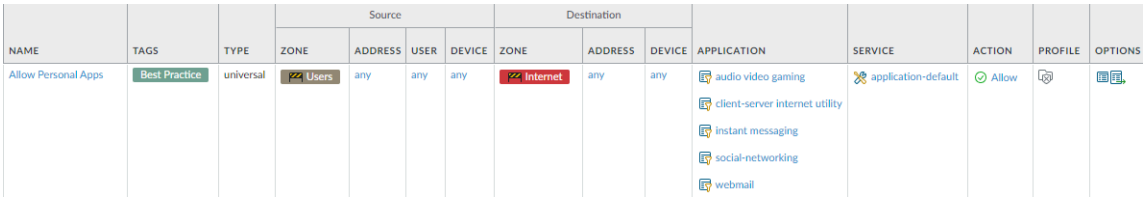
¿Por qué necesito esta regla?	Aspectos destacados de las reglas
❑ Además de las aplicaciones que autoriza y administra para los usuarios, los usuarios a menudo necesitan acceso a otras aplicaciones empresariales, como Zoom, Adobe online services o G Suite. ❑ Esta regla le ayuda a que pueda permitir la navegación segura mientras busca amenazas. Consulte Crear perfiles de seguridad recomendados para la puerta de enlace de Internet.	• Restringir el acceso solo a usuarios conocidos. Consulte Crear grupos de usuarios para acceder a Aplicaciones permitidas. • Para mayor visibilidad, cree un filtro de aplicaciones para cada tipo de aplicación que desee permitir. • Adjunte Perfiles de seguridad de prácticas recomendadas para prevenir amenazas conocidas y desconocidas en todo el tráfico.



STEP 7 | (Opcional) Permita el acceso a aplicaciones personales.

¿Por qué necesito esta regla?	Aspectos destacados de las reglas
❑ Debido a que la línea que divide los dispositivos de trabajo y personales es borrosa, asegurarse de que todas las aplicaciones a las que acceden sus usuarios se habiliten de manera segura y estén libres de amenazas. ❑ Use filtros de aplicaciones para habilitar de manera segura el acceso a aplicaciones personales cuando crea esta base de reglas inicial. Una vez que evalúa las aplicaciones que se están usando, puede usar la información para decidir si eliminará el filtro y permitirá un	• Restringir el acceso solo a usuarios conocidos. Consulte Crear grupos de usuarios para acceder a Aplicaciones permitidas. • Para mayor visibilidad, cree un filtro de aplicaciones para cada tipo de aplicación que desee permitir. • Adjunte Perfiles de seguridad de prácticas recomendadas para prevenir amenazas conocidas y desconocidas en todo el tráfico.

¿Por qué necesito esta regla?	Aspectos destacados de las reglas
subconjunto menor de aplicaciones personales apropiadas para sus políticas de uso aceptable.	



STEP 8 | Permita la navegación web general.

¿Por qué necesito esta regla?	Aspectos destacados de las reglas
❑ La regla anterior permitía el acceso a aplicaciones personales (muchas de ellas basadas en navegador). Esta regla permite la navegación web general. ❑ La navegación web general presenta más riesgos que otros tipos de tráfico de aplicaciones. Cree perfiles de seguridad de prácticas recomendadas y adjúntelos a esta regla para permitir la navegación web de forma segura. ❑ Debido a que las amenazas a menudo se ocultan en el tráfico cifrado, descifre el tráfico para una visibilidad completa e inspección de amenazas para habilitar la navegación web de forma segura.	• Utilice los mismos perfiles de seguridad recomendados que las otras reglas y ajuste el perfil de filtrado de URL tanto como sea posible. • Para prevenir que dispositivos con software malintencionado o dispositivos incrustados lleguen a Internet, solo proporcione permisos a usuarios conocidos. • Use filtros de aplicación para permitir el acceso a tipos de aplicaciones generales. • Permita explícitamente SSL como una aplicación para permitir a los usuarios navegar a sitios HTTPS que seleccione para excluir del descifrado. • Establezca el servicio en **application-default (aplicación predeterminada)**.

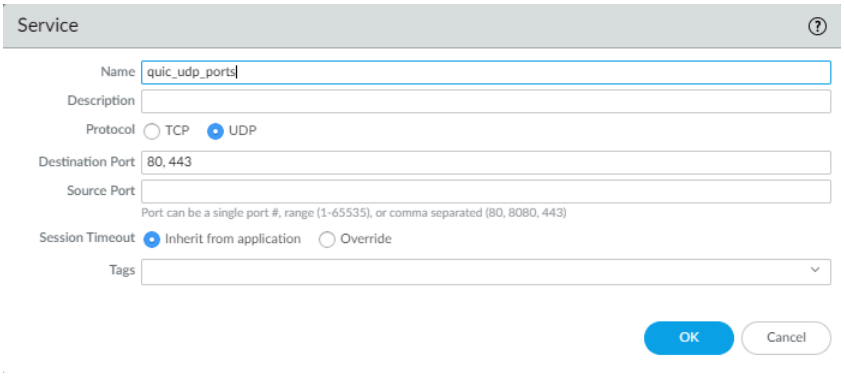
Paso 3: Crear las reglas de bloqueo de aplicaciones

Las reglas de bloqueo de aplicaciones le protegen de aplicaciones evasivas y comúnmente vulneradas mientras desarrolla y ajusta su base de reglas de políticas de seguridad. Las reglas de ajuste temporales ayudan a encontrar lagunas en las políticas e identificar posibles ataques. Debido a que detectan el tráfico de aplicaciones que usted no sabía que se estaba ejecutando en su red, estas permiten el tráfico que podría representar riesgos de seguridad. Las siguientes reglas de bloqueo bloquean explícitamente aplicaciones y protocolos potencialmente maliciosos que los atacantes utilizan habitualmente, como DNS y SMTP públicos, túneles cifrados, acceso remoto y aplicaciones no autorizadas para compartir archivos.

STEP 1 | Bloquee el protocolo de Conexiones UDP rápidas en Internet (QUIC).

¿Por qué necesito esta regla?	Aspectos destacados de las reglas
❑ Chrome y algunos otros navegadores establecen sesiones utilizando QUIC en lugar de TLS. QUIC utiliza cifrado propio que el cortafuegos no puede descifrar, por lo que podría introducir a la red tráfico cifrado potencialmente peligroso. ❑ Bloquear QUIC obliga al explorador a volver a TLS y permite que el cortafuegos descifre el tráfico.	• Cree un servicio [**Objects (Objetos)** > **Services (Servicios)**] que especifique los puertos UDP 80 y 443. • La primera regla bloquea QUIC en sus puertos de servicio UDP (80 y 443) y utiliza el servicio que creó para especificar esos puertos. • La segunda regla bloquea la aplicación QUIC.

El Servicio especifica los puertos UDP que se bloquearán para QUIC.



La primera regla especifica el servicio que configuró para QUIC y la segunda regla bloquea la aplicación QUIC:

			Source				Destination								
	NAME	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
1	Block QUIC UDP	universal	l3-vlan-trust	any	any	any	l3-untrust	any	any	any	quic_udp_ports	Deny	none	
2	Block QUIC	universal	l3-vlan-trust	any	any	any	l3-untrust	any	any	quic	application-default	Deny	none	

STEP 2 | Bloquee las aplicaciones que no tengan un caso de uso legítimo.

¿Por qué necesito esta regla?	Aspectos destacados de las reglas
❑ Bloquee aplicaciones potencialmente maliciosas, como túneles cifrados, intercambio de archivos entre peers y aplicaciones para compartir archivos basadas en web que TI no haya autorizado. ❑ Debido a que las reglas de ajuste temporales pueden permitir tráfico con intenciones maliciosas, así como tráfico legítimo que no coincide con las reglas de su política como se esperaba, estas podrían permitir tráfico	• Use la acción **Drop (Descartar)** para descartar silenciosamente el tráfico sin enviar una señal al cliente o al servidor. • Habilite la creación de logs para el tráfico que coincide con esta regla, para poder investigar posibles amenazas y el uso inadecuado de las aplicaciones en su red. • Dado que esta regla está destinada a detectar tráfico malicioso, coincide con el tráfico de

¿Por qué necesito esta regla?	Aspectos destacados de las reglas
peligroso o malicioso. Esta regla bloquea el tráfico que no tiene un caso de uso legítimo y que un atacante o un usuario negligente podría utilizar.	cualquier usuario que se ejecute en cualquier puerto.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
Block Bad Apps	Best Practice	universal	Users	any	any	any	Internet	any	any	encrypted tunnels file sharing remote access	any	Drop	none	

STEP 3 | Bloquee las aplicaciones de DNS público y SMTP.

Permita el tráfico solo a servidores DNS autorizados. Utilice el servicio de seguridad DNS *para evitar conexiones a servidores DNS maliciosos.*

¿Por qué necesito esta regla?	Aspectos destacados de las reglas
❑ Bloquee las aplicaciones DNS/SMTP para evitar la tunelización de DNS, el tráfico de comando y control, y las aplicaciones de gestión remotas.	• Use la acción **Reset both client and server (Restablecer cliente y servidor)** para enviar un mensaje de restablecimiento de TCP a los dispositivos del lado del cliente y del lado del servidor. • Habilite el registro del tráfico que coincida con esta regla para que pueda investigar posibles amenazas.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
Block Public DNS and SMTP	Best Practice	universal	Users	any	any	any	Internet	any	any	dns smtp	any	Reset Both	none	

Paso 4: Crear reglas de ajuste temporales

Las reglas de ajuste temporales le ayudan a supervisar la base de reglas de prácticas recomendadas inicial en busca de lagunas y le alertan sobre comportamientos sospechosos.

Por ejemplo, las reglas temporales identifican el tráfico que proviene de usuarios desconocidos o de aplicaciones que se ejecutan en puertos inesperados. Supervise el tráfico que coincida con las reglas temporales para obtener una comprensión completa de todas las aplicaciones en uso en su red (y garantizar la disponibilidad de las aplicaciones mientras realiza la transición a una base de reglas basada en prácticas recomendadas). Utilice esta información para ayudarle a ajustar la lista de permitidos, ya sea añadiendo nuevas reglas de permisos para aplicaciones que no sabía que necesitaba o para acotar las reglas de permisos y reemplazar los filtros de aplicaciones por grupos de aplicaciones o aplicaciones específicas. Cuando el tráfico ya no coincida con estas reglas, puede eliminar las reglas temporales.

Algunas reglas de ajuste temporales van más allá de las reglas que bloquean las aplicaciones malas y otras van después para garantizar que el tráfico fijado como objetivo coincida con la regla adecuada, al tiempo que garantizan que el tráfico malo no entre en su red.

STEP 1 | Permita la navegación web y SSL en puertos no estándar para usuarios conocidos para determinar si existen aplicaciones legítimas que se ejecutan en puertos no estándar.

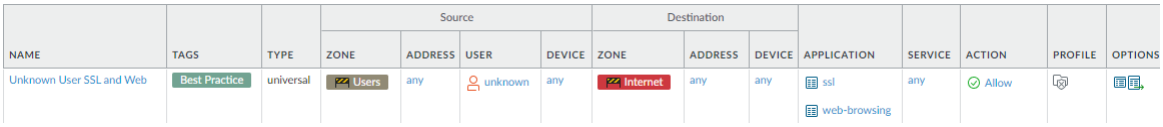
¿Por qué necesito esta regla?	Aspectos destacados de las reglas
❑ Esta regla ayuda a determinar si tiene lagunas en la política en las que los usuarios no pueden acceder a aplicaciones legítimas porque se ejecutan en puertos no estándar. ❑ Supervise todo el tráfico que coincida con esta regla. Para el tráfico legítimo, agregue las aplicaciones adecuadas a las reglas de permiso adecuadas. Cree una aplicación personalizada cuando corresponda.	• A diferencia de las reglas de permitidos que admiten aplicaciones solo en el puerto predeterminado, esta regla permite la navegación web y el tráfico SSL en cualquier puerto, para detectar brechas en su lista de permitidos. • Dado que esta regla encuentra lagunas en la política, limítela a los usuarios conocidos de la red. • Permita de forma explícita SSL como una aplicación en esta regla si desea permitir que los usuarios puedan ingresar en sitios HTTPS que no están descifrados (por ejemplo, sitios de servicios financieros o de salud). • Adjunte perfiles de seguridad de prácticas recomendadas para buscar amenazas. • Añada esta regla por encima de las reglas de bloqueo de aplicaciones o, de lo contrario, no habrá tráfico que coincida con esta regla.

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected Port SSL and Web	Best Practice	universal	Users	any	known-user	any	Internet	any	any	ssl web-browsing	any	Allow		

STEP 2 | Permita la navegación web y el tráfico SSL en puertos no estándar de usuarios desconocidos para destacar a todos los usuarios desconocidos, independientemente del puerto.

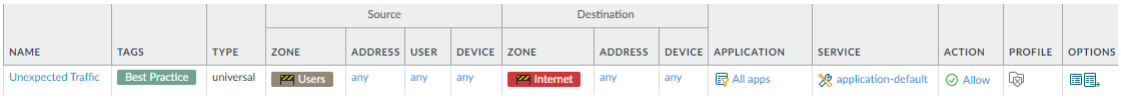
¿Por qué necesito esta regla?	Aspectos destacados de las reglas
❑ Esta regla ayuda a determinar si existen brechas en su cobertura de User-ID. ❑ Esta regla ayuda a identificar los dispositivos comprometidos o integrados que intentan acceder a Internet.	• Si bien la mayoría de las reglas de aplicaciones permitidas se aplican a usuarios conocidos o a grupos de usuarios específicos, esta regla explícitamente busca la coincidencia con el tráfico de usuarios **desconocidos**.

¿Por qué necesito esta regla?	Aspectos destacados de las reglas
❑ Es importante bloquear el uso de puertos no estándar, incluso para el tráfico de navegación web, debido a que es una técnica de evasión.	• Esta regla debe ir por encima de las reglas de bloqueo de aplicaciones o, de lo contrario, el tráfico nunca coincidirá con ella. • Adjunte perfiles de seguridad de prácticas recomendadas para buscar amenazas.



STEP 3 | Permita todas las aplicaciones en el puerto de aplicación-por defecto para identificar aplicaciones imprevistas.

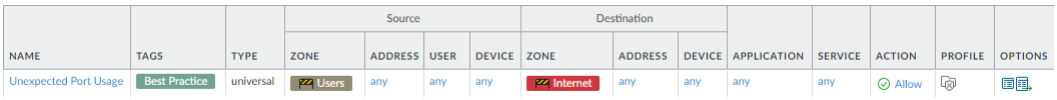
¿Por qué necesito esta regla?	Aspectos destacados de las reglas
❑ Esta regla aporta visibilidad sobre aplicaciones que no sabía que se estaban ejecutando en su red, a fin de que pueda ajustar la lista de aplicaciones permitidas. ❑ Supervise todo el tráfico que coincide con esta regla, para determinar si representa una posible amenaza o si necesita modificar sus reglas de permiso para habilitar el acceso a más aplicaciones.	• Debido a que esta regla permite todas las aplicaciones, debe añadirla después de las reglas de bloqueo de aplicación para prevenir que las aplicaciones nocivas se ejecuten en la red. • Si ejecuta PAN-OS 7.0.x o una versión anterior, para identificar adecuadamente las aplicaciones imprevistas debe crear un filtro de aplicaciones que incluya todas las aplicaciones, en lugar de configurar la regla para permitir **any (cualquier)** aplicación.



STEP 4 | Permita que cualquier aplicación en cualquier puerto identifique las aplicaciones que se ejecutan en puertos no estándar.

¿Por qué necesito esta regla?	Aspectos destacados de las reglas
❑ Esta regla ayuda a identificar aplicaciones legítimas y conocidas que se ejecutan en puertos desconocidos. ❑ Esta regla ayuda a identificar aplicaciones desconocidas para las cuales debe crear una aplicación personalizada, y añadir a su aplicación reglas de permiso. ❑ El tráfico que coincide con esta regla es procesable. Rastree el origen del tráfico y	• Dado que esta es una regla muy general que permite cualquier aplicación de cualquier usuario en cualquier puerto, colóquela en la parte inferior de la base de reglas. • Habilite la creación de logs para el tráfico que coincide con esta regla, para que pueda investigar el uso indebido de aplicaciones y las posibles amenazas, o identificar aplicaciones

¿Por qué necesito esta regla?	Aspectos destacados de las reglas
asegúrese de no permitir tráfico tcp, udp o non-syn-tcp desconocido.	legítimas que requieren una aplicación personalizada.



Paso 5: Habilitar la creación de logs para el tráfico que no coincide con ninguna regla

El tráfico de puerta de enlace de Internet que no coincide con las reglas definidas coincide con la regla predeterminada entre zonas predefinida en la parte inferior de la base de reglas y se deniega. Para obtener visibilidad sobre el tráfico que no coincide con las reglas que creó, habilite la creación de logs en la regla de interzona-por defecto:

STEP 1 | Seleccione la fila de la regla predeterminada entre zonas en la base de reglas y elija **Override (Anular)** la regla para editarla.

STEP 2 | Seleccione el nombre de la regla **interzone-default** (interzona-por defecto) para abrir la regla para su edición.

STEP 3 | En la pestaña **Actions (Acciones)**, seleccione **Log at Session End (Log al finalizar sesión)** y haga clic en **OK (Aceptar)**.

STEP 4 | Cree un informe personalizado para supervisar el tráfico que coincida con la regla:

1. Seleccione **Monitor (Supervisar)** > **Manage Custom Reports (Gestionar informes personalizados)**.
2. Seleccione **Add** para añadir un informe y **Name** para asignarle un nombre descriptivo.
3. Configure la **Database (Base de datos)** en **Traffic Summary (Resumen de tráfico)**.
4. Seleccione la casilla de verificación **Scheduled (Programado)**.
5. Añada **Rule (Regla)**, **Application (Aplicación)**, **Bytes**, **Sessions (Sesiones)** a la lista Columnas seleccionadas.
6. Establezca los campos **Time Frame (Periodo)**, **Sort By (Ordenar por)** y **Group By (Agrupar por)** deseados.
7. Defina la consulta para que coincida con el tráfico que corresponda a la regla interzone-default (interzona-predeterminada):

   ```
   (rule eq 'interzone-default')
   ```

STEP 5 | Seleccione **Commit (Confirmar)** para confirmar los cambios que realizó en la base de reglas.

Supervisión y ajuste la base de reglas de la política

La creación de una política de seguridad de prácticas recomendadas es un proceso iterativo. Después de Definir la política de seguridad de puerta de enlace de Internet inicial, debe comenzar a supervisar el tráfico que coincide con las reglas temporales diseñadas para identificar las brechas de la política y el comportamiento alarmante, y ajustar la política según corresponda. La supervisión del tráfico que coincide con estas reglas le permite realizar los ajustes adecuados a las reglas permanentes y asegurarse de que todo el tráfico coincide con las reglas de aplicaciones permitidas, o evaluar si debe permitir aplicaciones que no coincidan con ninguna regla.

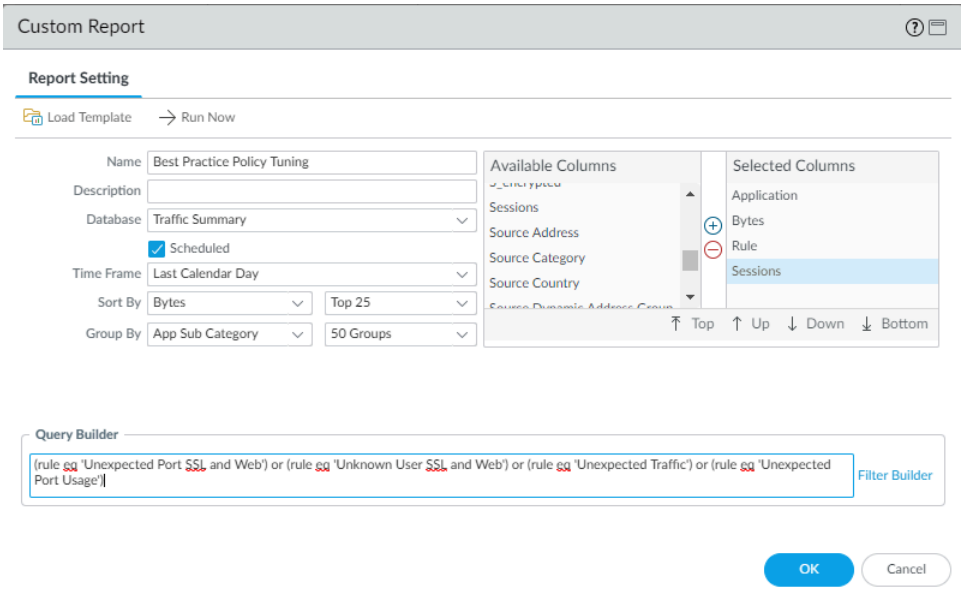
A medida que ajuste su base de reglas, verá cada vez menos tráfico que desea permitir que coincida con las reglas temporales. Cuando vea que ya no hay el tráfico que desea permitir que coincida con estas reglas, las reglas de permiso de aplicación positiva se completan y ya puede retirar las reglas temporales (la regla de denegación predeterminada entre zonas deniega automáticamente el tráfico que ninguna regla permite explícitamente).

Dado que las versiones mensuales de contenido añaden nuevos identificadores de aplicación, revise el impacto que tienen los cambios de identificador de aplicación en la política de seguridad.

STEP 1 | Cree informes personalizados para supervisar el tráfico que coincida con las reglas que identifican las lagunas de las políticas.

1. Seleccione **Monitor (Supervisar)** > **Manage Custom Reports (Gestionar informes personalizados)**.
2. Elija **Add (Añadir)** un informe y asígnele un **Name (Nombre)** descriptivo que indique la brecha de política que está investigando.
3. Configure la **Database (Base de datos)** en **Traffic Summary (Resumen de tráfico)**.
4. Seleccione **Scheduled (Programado)**.
5. Añada **Rule (Regla)**, **Application (Aplicación)**, **Bytes**, **Sessions (Sesiones)** a la lista Columnas seleccionadas.
6. Establezca los campos **Time Frame (Periodo)**, **Sort By (Ordenar por)** y **Group By (Agrupar por)** deseados.
7. Defina la consulta para que coincida con el tráfico que coincide con las reglas que encuentran lagunas de la política y comportamientos sospechosos. Puede crear un único informe que da detalles del tráfico que coincide con cualquiera de las reglas (usando el operador **or**) crear informes individuales para supervisar cada regla. En las siguientes consultas de ejemplo se usan los nombres de regla definidos en la política de ejemplo:
   - `(rule eq 'Unexpected Port SSL and Web')`
   - `(rule eq 'Unknown User SSL and Web')`
   - `(rule eq 'Unexpected Traffic')`

- `(rule eq 'Unexpected Port Usage')`



STEP 2 | Revise el informe con regularidad para comprender por qué el tráfico coincide con cada una de las reglas de ajuste. Actualice las reglas para incluir aplicaciones y usuarios legítimos, o use la información del informe para evaluar el riesgo de la aplicación e implementar cambios en las políticas.

Eliminar las reglas temporales

Después de varios meses de supervisar la política de seguridad de prácticas recomendadas de su puerta de enlace de Internet inicial y ajustar la base de reglas, deberá ver un menor volumen del tráfico que desea permitir que coincida con las reglas temporales. Cuando ya no vea tráfico que coincida con estas reglas, habrá alcanzado su objetivo de lograr la transición a una base de reglas de política de seguridad basadas en la aplicación. Ahora puede eliminar las reglas temporales, incluidas las reglas de bloqueo de aplicaciones para aplicaciones que no tienen un caso de uso legítimo y para aplicaciones DNS y SMTP públicas porque la regla de denegación predeterminada entre zonas bloquea automáticamente ese tráfico, ya que no coincide con las reglas de permiso explícitas. (Mantenga las reglas que QUIC.)

STEP 1 | Seleccione **Policies (Políticas)** > **Security (Seguridad)**.

STEP 2 | Seleccione la regla y haga clic en **Delete**.

O bien, seleccione **Disable (Deshabilitar)** para deshabilitar las reglas durante cierto período antes de eliminarlas. Esto le permite **Enable (Habilitar)** las reglas nuevamente si los logs de tráfico muestran que el tráfico que desea permitir coincide con la regla de denegación predeterminada entre zonas.

STEP 3 | Haga clic en **Commit (Confirmar)** para confirmar los cambios.

Mantener la base de reglas

Las empresas y las aplicaciones evolucionan, por lo que su base de reglas de políticas de seguridad también debe evolucionar. Cuando sus aplicaciones autorizadas cambien, realice los cambios correspondientes en las reglas de políticas existentes que se alineen con el caso de uso comercial de la aplicación, siempre que sea posible en lugar de añadir nuevas reglas. A menudo, el cambio es tan simple como añadir una nueva aplicación a un grupo de aplicaciones o eliminar una aplicación obsoleta de un grupo de aplicaciones.

En Panorama o en un cortafuegos independiente, use el contador de coincidencias de la regla de política *para analizar los cambios en la base de reglas. Por ejemplo, cuando añade una aplicación nueva, antes de permitir el tráfico de la aplicación en la red, añada la regla de permiso en la base de reglas. Si el tráfico coincide con la regla y aumenta el valor del contador, el tráfico que coincide con la regla ya se encuentra en la red incluso si aún no se activó la aplicación, es posible que necesite ajustar la red. Compruebe los widgets de* ***ACC > Threat Activity (Actividad de amenazas) > Applications Using Non Standard Ports (Aplicaciones que usan puertos no estándar)*** *y* ***ACC > Threat Activity (Actividad de amenazas) > Rules Allowing Apps On Non Standard Ports (Reglas que permiten aplicaciones en puertos no estándar)*** *para comprobar si el tráfico en los puertos no estándar provocó las coincidencias inesperadas con la regla.*

La clave para usar el contador de coincidencias de la regla de la política es restablecer el contador cuando realiza un cambio, como la introducción de una nueva aplicación o el cambio del significado de una regla. Restablecer el contador garantiza que verá el resultado del cambio, no resultados que incluyen el cambio y los eventos que se produjeron antes del cambio.

Si usa Panorama para gestionar los cortafuegos, supervisar el estado del cortafuegos *para comparar los dispositivos con el rendimiento de referencia y entre sí para identificar las desviaciones del comportamiento normal.*

Configure las actualizaciones de contenido de Palo Alto Networks para que se descarguen automáticamente y programe la instalación en los cortafuegos lo antes posible. Las actualizaciones de contenido de aplicaciones y amenazas se producen cada vez que sea necesario actualizar las firmas de los perfiles de seguridad. Las actualizaciones de contenido enviadas el tercer martes de cada mes también contienen los App-ID nuevos y modificados (actualizaciones de aplicaciones; en casos excepcionales, una actualización de aplicación se puede retrasar uno o dos días). Evalúe cómo los App-ID nuevos y modificados afectan su base de reglas de políticas de seguridad en un entorno que no es de producción y modifique las reglas según sea necesario.

Siga las prácticas recomendadas de actualizaciones de contenido, instale actualizaciones tan pronto como pueda para proteger su puerta de enlace de Internet y configure el reenvío de logs para todas las actualizaciones de contenido.

STEP 1 | Antes de instalar una nueva actualización de contenido, revise los App-ID nuevos y modificados para determinar si los cambios afectan la política.

STEP 2 | Si es necesario, modifique las reglas existentes en la política de seguridad para adaptarse a los cambios del App-ID. Puede deshabilitar App-ID seleccionados si algunos App-ID requieren más pruebas e instalar el resto de los App-ID nuevos y modificados. Finalice las pruebas y revisiones de

políticas necesarias antes de la siguiente versión de contenido mensual con los nuevos App-ID (el tercer martes de cada mes) para evitar la superposición.

STEP 3 | Prepare actualizaciones de la política para tener en cuenta los cambios de App-ID en una versión de contenido, para añadir nuevas aplicaciones autorizadas, para eliminar aplicaciones de las reglas de permiso.