paloalto TECHDOCS

Prácticas recomendadas para migrar a una política basada en aplicaciones

Version 10.1

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Last Revised

December 4, 2023

Table of Contents

Prácticas recomendadas para migrar a una política basada en aplicaciones

No tiene que sacrificar una mejor seguridad por la disponibilidad de la aplicación. En su lugar, utilice Expedition y Policy Optimizer para automatizar y reducir el tiempo y el esfuerzo necesarios para migrar de una política de seguridad basada en puertos en un cortafuegos heredado a una política de seguridad basada en aplicaciones en un cortafuegos de última generación de Palo Alto Networks o un dispositivo Panorama de forma gradual y segura.

- Habilitar aplicaciones de forma segura mediante una transición gradual
- Migrar una política basada en puertos a PAN-OS usando Expedition
- Migrar a una política basada en aplicaciones utilizando Policy Optimizer
- Siguientes pasos para adoptar las prácticas recomendadas de seguridad

Después de migrar la política heredada a una política basada en aplicaciones, utilice el informe BPA a petición en Strata Cloud Manager para identificar áreas para mejorar la seguridad, utilice el Resumen de adopción para identificar deficiencias en la adopción de capacidades de seguridad y visite el Portal de documentación de prácticas recomendadas, que proporciona pasos específicos de planificación, implementación y mantenimiento de prácticas recomendadas para una variedad de características, capacidades y objetivos de seguridad, incluidos:

- Descifrado (no puede defenderse de amenazas sobre las que no tiene visibilidad)
- Política de seguridad (incluye creación de reglas de políticas de seguridad, orden e higiene de la base de reglas, App-ID Cloud Engine (ACE), optimizador de políticas, recomendación de políticas de SaaS y recomendación de políticas de IoT)
- Zero Trust (cómo bloquear tu red)
- Protección DoS y de zonas (incluida la protección de búfer de paquetes)
- Acceso administrativo (proteger el acceso a cortafuegos y dispositivos de gestión)
- Prácticas recomendadas de IoT
- Prácticas recomendadas de la implementación de WildFire
- Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas

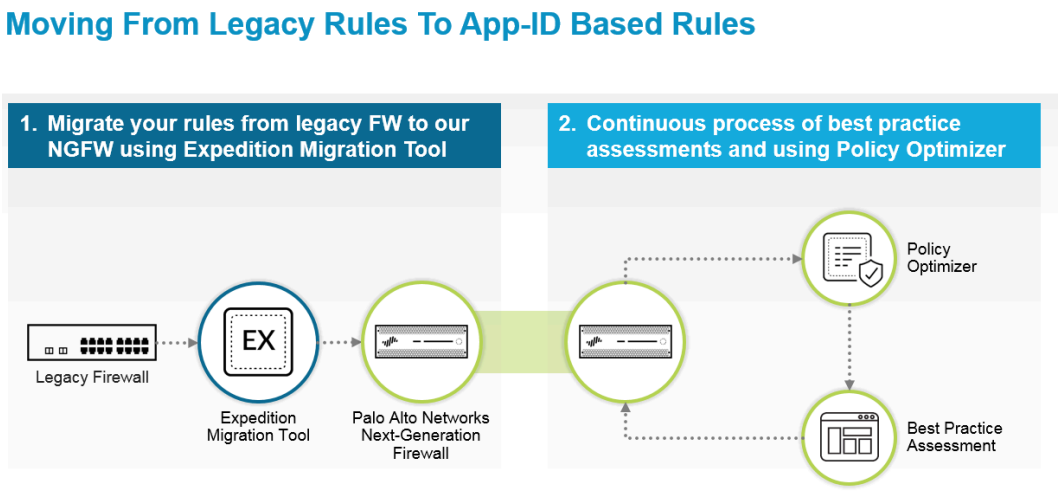
También asegúrese de tener las suscripciones adecuadas para respaldar la seguridad de su red, incluida prevención avanzada de amenazas, seguridad DNS, filtrado avanzado de URL, IoT security, GlobalProtect, SaaS Security, etc.

Habilitar aplicaciones de forma segura mediante una transición gradual

Las debilidades evidentes de la política de seguridad basada en puertos son bien conocidas: no puede ver qué aplicaciones usan un puerto, por lo que cualquier aplicación malintencionada puede obtener acceso a su red en puertos abiertos como el puerto 80 (HTTP) o el puerto 53 (DNS) . Esto hace que sea más fácil para los atacantes instalar malware, moverse lateralmente a través de la red, filtrar datos y comprometer su red porque no tiene visibilidad de las aplicaciones en su red, ni la capacidad para evitar las amenazas que oculta su tráfico.

Por el contrario, la política de seguridad basada en aplicaciones que utiliza App-ID™ brinda visibilidad de las aplicaciones independientemente del puerto, protocolo, cifrado (SSL o SSH) o tácticas evasivas, para que sepa exactamente qué aplicaciones están en su red y pueda inspeccionar su tráfico en busca de amenazas. Las políticas de aplicaciones específicas permiten un acceso seguro porque puede configurar reglas de política de seguridad que permiten que solo los usuarios correctos accedan a las aplicaciones correctas en los lugares correctos, y puede aplicar perfiles de prevención de amenazas a esas reglas. El uso de App-ID para clasificar las aplicaciones reduce la superficie de ataque porque permite el acceso a la red de solo las aplicaciones requeridas para respaldar su negocio y bloquea automáticamente las aplicaciones no deseadas. Permitir lo que desea y bloquear todo lo demás es mucho más fácil y más seguro que la interminable tarea de intentar bloquear todas las aplicaciones individuales que no desea.

Migre a App-ID en fases:



1. Use Expedition para importar una base de reglas heredada, limpiarla y lograr una migración similar a un cortafuegos de última generación de Palo Alto Networks o un dispositivo Panorama. Expedition se distribuye como una máquina virtual (VM).
2. Ejecute el cortafuegos o el dispositivo PAN-OS en su entorno de producción de red para que pueda aprender y catalogar las aplicaciones en su red.
3. Después de al menos una semana de tráfico de generación de logs, ejecute la Evaluación de prácticas recomendadas (BPA) para establecer una línea de base y luego utilizar Policy Optimizer para comenzar a convertir de forma segura las reglas basadas en puertos a reglas basadas en aplicaciones y proteger su red. (Puede convertir algunas sencillas reglas que permiten aplicaciones conocidas después de aproximadamente una semana; para otras reglas que ven muchas aplicaciones, como una regla general de acceso a Internet de salida, espere al menos 30 días para recopilar información de la aplicación).

Adopte un enfoque gradual para convertir de forma segura las reglas basadas en las necesidades y prioridades de su negocio.

4. (Opcional) Después de utilizar Policy Optimizer, convierta la base de reglas a App-ID, vuelva a importar la configuración a Expedition y use las funciones de enriquecimiento de reglas para simplificar y refinar aún más la base de reglas.
5. Mantenga la implementación de App-ID a medida que introduce nuevas aplicaciones en su red. Ejecute la BPA después de la primera conversión a través de las reglas basadas en puerto y posteriormente de forma periódica para medir el progreso y descubrir otras áreas para mejorar la seguridad.

Policy Optimizer está disponible a partir de PAN-OS 9.0. Si usa Panorama para gestionar sus cortafuegos de última generación, no tiene que actualizar los cortafuegos gestionados a PAN-OS 9.0 para usar Policy Optimizer. Solo necesita actualizar Panorama a PAN-OS 9.0, enviar logs de tráfico desde los cortafuegos gestionados a Panorama o Recopiladores de logs que ejecutan PAN-OS 9.0, y enviar la política de Panorama a los cortafuegos. Los cortafuegos gestionados deben ejecutar PAN-OS 8.1 o posterior, y si se conectan a los recopiladores de logs, los recopiladores de logs deben ejecutar PAN-OS 9.0. Esto proporciona una ruta rápida para la cualificación, por lo que puede usar Policy Optimizer para adoptar políticas basadas en App-ID rápidamente.

Strata Logging Service es compatible con Policy Optimizer en dispositivos Panorama que ejecuten PAN-OS 10.0.4 o posterior con el complemento Cloud Services 2.0 o posterior.

Los cortafuegos PA-7000 Series admiten dos tarjetas de logs: la tarjeta de procesamiento de logs (log processing card, LPC) para cortafuegos PA-7000 Series y la tarjeta de reenvío de logs (log forwarding card, LFC) de alto rendimiento para cortafuegos PA-7000 Series. A diferencia de la LPC, la LFC carece de discos locales para almacenar los logs. por lo que reeenvía todos los logs a un sistema externo (o varios) de almacenamiento de logs, como Panorama o un servidor de syslog. Si utiliza la LFC, la información sobre el uso de las aplicaciones del optimizador no se muestra en el cortafuegos porque los logs del tráfico no se almacenan en ninguna ubicación local. Si utiliza la LFC, los logs de tráfico se almacenan localmente en el cortafuegos, por lo que la información de uso de la aplicación del optimizador de políticas aparece en el cortafuegos. En ambos casos, el cortafuegos PA-7000 puede ejecutar PAN-OS 8.1 (o posterior) siempre que los Recopiladores de logs y Panorama ejecuten PAN-OS 9.0 o posterior.

Migrar una política basada en puertos a PAN-OS usando Expedition

Utilice Expedition para importar una base de reglas heredada, limpiarla y lograr una migración similar a un cortafuegos de última generación de Palo Alto Networks o un dispositivo Panorama como la primera fase de su migración a una política de seguridad basada en aplicaciones. Expedition es una excelente herramienta para realizar operaciones masivas en múltiples objetos en una configuración y admite la importación de configuraciones heredadas de la mayoría de los principales proveedores de cortafuegos.

Este tema resume el flujo de trabajo de Expedition. La Live community proporciona soporte para Expedition, incluido cómo obtener la herramienta y documentación detallada sobre cómo utilizar la herramienta.

La asistencia técnica de Palo Alto Networks (TAC) no proporciona soporte para Expedition.

Para obtener detalles sobre el flujo de trabajo de migración de Expedition, consulte la Guía del usuario de Expedition, que también incluye información sobre cómo importar objetos a una configuración mediante archivos CSV y cómo importar una configuración Iron-Skillet de Día 1.

Para gestionar Expedition, consulte la Guía del administrador de Expedition, que también incluye información sobre la interfaz del usuario, y la Guía de protección de Expedition, que brinda consejos sobre cómo proteger la VM de Expedition.

Antes de comenzar una migración, asegúrese de cumplir los siguientes requisitos previos:

- Descargue Expedition a un dispositivo de administración que admita la ejecución de una máquina virtual.
- La conectividad SSH y/o SSL a Palo Alto Networks Panorama y los cortafuegos a los que está migrando. El acceso SSH es para la conectividad a la CLI y el acceso SSL es para la conectividad a la interfaz web y para enviar comandos API.
- El acceso operativo a Palo Alto Networks Panorama y los cortafuegos a los que está migrando para que pueda enviar la configuración similar al dispositivo PAN-OS.

Los Servicios profesionales cuentan con una gran cantidad de experiencia en migración. Puede contratar al equipo de Servicios profesionales para ayudarle a cambiar una configuración de sus dispositivos heredados a los servidores de seguridad de nueva generación de Palo Alto Networks y los dispositivos de Panorama.

STEP 1 | Revise la configuración del cortafuego heredado.

Comprenda los objetivos de la base de reglas heredada. Documente los elementos que necesita saber para la migración, como las interfaces deshabilitadas en un dispositivo Juniper SRX o la verificación de que se permite el tráfico entre interfaces con los mismos niveles de seguridad, la verificación del estado de los túneles IPSec y la recopilación de claves previamente compartidas en un dispositivo Cisco ASA.

STEP 2 | Importe la configuración heredada a Expedition y realice las modificaciones necesarias en la configuración.

STEP 3 | Cree un nuevo **Project (Proyecto)** en Expedition.

STEP 4 | Importe la configuración de origen migrada (heredada) al **Project (Proyecto)** e inspecciónelo.

Compruebe el formato del archivo, asegúrese de que todos los archivos requeridos están incluidos y marque Logs y eventos de Expedition para asegurarse de que el archivo de configuración migrado se ha cargado correctamente. Si es necesario, modifique el archivo de origen migrado para solucionar problemas y luego verifique otra vez. Repita este paso hasta que se solucionen todos los problemas.

STEP 5 | Importe una configuración PAN-OS al **Project (Proyecto)** para que sea la configuración base para la migración.

Obtenga las actualizaciones de contenido más recientes y luego importe la configuración base desde un dispositivo PAN-OS existente (ya sea el archivo de configuración existente o el archivo de configuración PAN-OS predeterminado de fábrica).

El archivo de configuración debe coincidir con la versión de PAN-OS que desea utilizar. Por ejemplo, para ejecutar PAN-OS 9.0, importe un archivo de configuración PAN-OS 9.0.

STEP 6 | Limpie la configuración migrada para prepararla para fusionarla con la configuración Base PAN-OS.

- Elimine o sustituya objetos de servicio no válidos. PAN-OS reconoce solo los puertos de servicio TCP y UDP, y Expedition migra automáticamente los objetos de servicio TCP y UDP a las aplicaciones. Busque aplicaciones y servicios no basados en IP, como ping e ICMP, que algunos dispositivos heredados ven como servicios en lugar de aplicaciones. Sustitúyalos con App-ID para clasificarlos como aplicaciones y obtener visibilidad, inspeccionar y controlar el tráfico.
- Para simplificar la configuración y reducir su tamaño, elimine o reemplace otros objetos no válidos y objetos no utilizados y combine los objetos duplicados.
- Busque y elimine las reglas deshabilitadas para que no saturen la configuración.
- Cambie el nombre de las interfaces para que coincidan con las interfaces en el dispositivo PAN-OS. Los nombres de interfaz importados del dispositivo heredado generalmente no coinciden con las convenciones de nomenclatura de PAN-OS.
- Cuando importa la configuración heredada, Expedition asigna automáticamente nombres de zona. Cambie el nombre de las zonas para que describan el propósito que cumplen cuando migre la configuración al dispositivo PAN-OS. Asegúrese de que las zonas estén asignadas correctamente a las interfaces.

  Además, compruebe el enrutador virtual por rutas estáticas. Si existen muchas rutas estáticas, utilice Expedition para migrar las rutas a la configuración de PAN-OS. Si solo hay unas pocas rutas estáticas, anótelas y luego créelas manualmente después de migrar la configuración.

STEP 7 | Combine la configuración migrada con la configuración base de PAN-OS arrastrando y soltando objetos de la configuración migrada a la configuración base.

STEP 8 | Verifique que la configuración fusionada no tiene objetos duplicados que la fusión puede haber creado y elimínelos o combínelos.

STEP 9 | Antes de exportar la configuración combinada al dispositivo PAN-OS, borre la caché de ARP en los conmutadores y enrutadores conectados al dispositivo PAN-OS y en el dispositivo PAN-OS para actualizar sus tablas ARP.

En los dispositivos PAN-OS, utilice el comando CLI **`clear arp all`**. (Si es necesario, puede borrar la caché de ARP para cada interfaz utilizando el comando de la CLI **`clear arp <interface>`**)

STEP 10 | Exporte la configuración fusionada al dispositivo PAN-OS y cargue la configuración fusionada.

El método que utilice depende de cómo desea migrar la configuración fusionada:

- Para una nueva instalación en un dispositivo PAN-OS, debe **Generate XML & Set Output (Generar XML y establecer salida)**, importar el archivo XML (configuración) y luego cargarlo en el dispositivo PAN-OS.
- Para una instalación de PAN-OS existente o si desea migrar la configuración en partes en lugar de hacerlo de una sola vez, debe **Generate XML & Set Output (Generar XML y establecer salida)**, importar el archivo XML (configuración), y luego utilizar el comando CLI **`load config partial`** para seleccionar una parte específica de la configuración para cargar. Necesita acceso SSH para utilizar la CLI en un dispositivo PAN-OS.
- Si el dispositivo PAN-OS está conectado a Expedition, también puede utilizar llamadas API para enviar partes o la configuración completa al dispositivo.

STEP 11 | Después de exportar la configuración fusionada a un dispositivo PAN-OS y cargar la configuración, utilice Policy Optimizer para convertir la política basada en puertos a una política basada en aplicaciones.

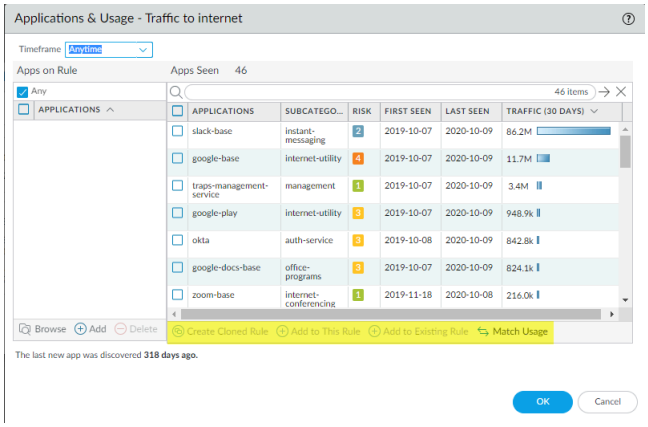
Migrar a una política basada en aplicaciones utilizando Policy Optimizer

Después de utilizar Expedition para migrar una configuración similar para un dispositivo PAN-OS, la siguiente fase es utilizar Policy Optimizer para simplificar la migración a las reglas de políticas de seguridad basadas en App-ID. Policy Optimizer hace que la conversión de reglas basadas en puertos heredadas sea mucho más sencilla porque automatiza la presentación de la información de aplicación para cada regla con el contexto que necesita para comprender la información y crear reglas basadas en aplicaciones inteligentes en una única vista. Policy Optimizer:

- Aprende y recuerda todas las aplicaciones que se ven en el tráfico para cada regla automáticamente, lo que elimina la necesidad de examinar cuidadosamente y analizar cientos de datos de registro. Incluso si los registros se transfieren, Policy Optimizer retiene la información de la aplicación, por lo que puede estar seguro de que está viendo todas las aplicaciones en una regla.
- Le permite migrar de forma segura a App-ID sin arriesgar la disponibilidad de la aplicación.
- Es nativa y compatible con los dispositivos PAN-OS, por lo que no tiene que mover configuraciones y datos del dispositivo a una herramienta no nativa.
- Proporciona opciones de clasificación y filtrado fáciles e intuitivas para ayudarle a identificar y priorizar qué reglas son las más fáciles y seguras de convertir primero.
- Se ejecuta en dispositivos Panorama, así como en cortafuegos individuales de nueva generación. Si administra sus cortafuegos de nueva generación que ejecutan PAN-OS 8.1 con Panorama, solo tiene que actualizar Panorama (y cualquier recopilador de logs conectado a los cortafuegos gestionados) a PAN-OS 9.0 para utilizar y obtener los beneficios de Policy Optimizer, así podrá cualificar y adoptar Policy Optimizer más rápido que si tuviera que cualificar todos sus cortafuegos.

  Strata Logging Service es compatible con Policy Optimizer en dispositivos Panorama que ejecuten PAN-OS 10.0.4 o posterior con el complemento Cloud Services 2.0 o posterior.

Estas capacidades dan como resultado una herramienta fácil de utilizar que ahorra tiempo y evita errores al convertir reglas basadas en puertos a reglas basadas en App-ID. Policy Optimizer proporciona varios métodos de conversión de reglas:



- **Create Cloned Rule (Crear Regla duplicada)**: La duplicación de una regla conserva la regla original basada en el puerto y coloca la nueva regla basada en App-ID por encima de la regla duplicada. Puede duplicar varias reglas basadas en App-ID de una regla basada en puerto. Por ejemplo, puede duplicar

múltiples reglas de App-ID basadas en subcategorías de aplicación de una regla general de navegación web para agrupar aplicaciones que requieren un acceso y un tratamiento de amenazas similares en lugar de tratar de controlar todo el acceso web para todos los usuarios en todos los lugares en una sola regla general no segura.

No existe ningún riesgo para la disponibilidad de las aplicaciones porque la regla basada en puerto debajo de la regla duplicada actúa como una red de seguridad. Si la regla basada en la duplicación (App-ID) no coincide con todas las aplicaciones que debe permitir, verá que esas aplicaciones alcanzan la regla basada en puerto debajo de la regla duplicada y puede realizar los ajustes necesarios. Puede eliminar la regla basada en puerto cuando el tráfico que desea permitir no coincida con la regla basada en puerto durante un período de tiempo razonable, completando la conversión de esa regla a una regla basada en App-ID.

- **Add to This Rule (Añadir a esta regla)**: La adición de aplicaciones a la regla sustituye la regla basada en puerto con una regla basada en App-ID, que elimina la regla basada en puerto de la base de reglas y no proporciona la red de seguridad que proporciona la duplicación. Utilice **Add to This Rule (Añadir a esta regla)** solo cuando esté seguro de que conoce todas las aplicaciones que desea que controle la regla. Las reglas que solo han visto unas pocas aplicaciones y para las que está seguro de saber que aplicaciones requeridas para su negocio son candidatas para **Add to This Rule (Añadir a esta regla)**. Es más seguro duplicar reglas que han visto muchas aplicaciones y reglas que pueden ver más aplicaciones de las que necesita permitir. Si omite añadir una aplicación a una regla, perderá la disponibilidad de esa aplicación, a menos que otra regla lo permita, mientras que la duplicación de la regla conserva la regla basada en el puerto como una red de seguridad.
- **Add to Existing Rule (Añadir a regla existente)**: Añadir aplicaciones a una regla existente no reemplaza la regla original basada en el puerto, que permanece en la base de reglas. **Add to Existing Rule (Añadir a regla existente)** le permite seleccionar cualquier regla configurada previamente y añadir aplicaciones en ella.

  Cuando añade aplicaciones a una regla basada en aplicaciones existente, el cortafuegos elimina esas aplicaciones de la regla basada en puertos y las añade a la regla basada en aplicaciones seleccionada. Las aplicaciones añadidas utilizan el mismo origen, destino, servicio, etc., que las otras aplicaciones en la regla basada en aplicaciones.

  Cuando añade aplicaciones a otra regla basada en puertos existente, el cortafuegos elimina esas aplicaciones de la regla basada en puertos original y las añade a la otra regla basada en puertos. Esto convierte la otra regla basada en puertos en una regla basada en aplicaciones que controla solo las aplicaciones que añadió a la regla. Si convierte parte de una regla basada en puertos de esta manera, vaya a la regla y cambie el Servicio a application-default para evitar que las aplicaciones usen puertos no estándar (además, es posible que el Servicio configurado en la regla no coincida con la aplicación).
- **Match Usage (Hacer coincidir el uso)**: La coincidencia de uso de una regla basada en puerto sustituye la regla basada en puerto con una regla basada en App-ID que contiene todas las aplicaciones que se ven en esa regla. Utilice **Match Usage (Hacer coincidir el uso)** solo cuando la regla ha visto una pequeña cantidad de aplicaciones conocidas que tienen propósitos comerciales legítimos. Un buen ejemplo es el puerto TCP 22, que debería permitir solo el tráfico SSH. Si SSH es la única aplicación vista en una regla basada en puerto para el puerto 22, puede **Match Usage (Hacer coincidir el uso)** y convertir la regla en una regla de App-ID.

Para **Create Cloned Rule (Crear regla duplicada)**, **Add to This Rule (Añadir a esta regla)** o **Add to Existing Rule (Añadir a regla existente)**, debe seleccionar al menos una aplicación de **Apps seen (Aplicaciones vistas)**.

Las aplicaciones utilizadas solo para eventos trimestrales o anuales pueden no aparecer en la información de la aplicación si el historial no es lo suficientemente largo para capturar su actividad más reciente. Tenga en cuenta estos tipos de aplicaciones cuando convierta reglas.

Cuando convierte una regla basada en puerto en una regla basada en aplicación, Policy Optimizer no realiza ningún otro cambio en la regla, aparte de la conversión de servicios a App-ID. En la mayoría de los casos, después de convertir una regla, debe cambiar el **Service (Servicio)** a **application-default (aplicación predeterminada)** para que solo las aplicaciones que utilizan legítimamente el puerto pueden acceder al puerto y evitar que las aplicaciones evasivas obtengan acceso a la red mediante el uso de un puerto no estándar.

Si las necesidades comerciales requieren que se permitan aplicaciones, como aplicaciones personalizadas internas en puertos no estándar, entre clientes y servidores particulares; restrinja la excepción a solo las aplicaciones, fuentes y destinos requeridos. Considere volver a crear las aplicaciones personalizadas para utilizar los puertos predeterminados de las aplicaciones.

Antes de utilizar Policy Optimizer para convertir las reglas basadas en puertos en reglas basadas en App-ID:

1. Complete la migración similar de la configuración heredada a un cortafuegos Palo Alto Networks de nueva generación o un dispositivo Panorama desde Expedition.
2. Ejecute el dispositivo PAN-OS en su red de producción durante aproximadamente una semana antes de comenzar a convertir las reglas a App-ID, para que el dispositivo pueda comenzar a aprender y clasificar las aplicaciones en la red. Puede convertir algunas reglas simples rápidamente (por ejemplo, una regla del puerto 22 solo debería permitir el tráfico SSH y es fácil de convertir), mientras que debe permitir que el cortafuegos recopile datos de aplicaciones del tráfico durante un período de tiempo más largo para otras reglas, como su regla de acceso a internet (puerto 80/433).
3. Ejecute la Evaluación de prácticas recomendadas (BPA) para establecer una línea de base con la que comparar el progreso.
4. Establezca objetivos reales. Piense en cómo quiere que se vea el resultado final. Cuando alcance el objetivo, ejecute nuevamente la BPA para confirmar que alcanzó el objetivo, y luego vuelva a evaluar si puede ir más lejos y hacer que su red sea incluso más segura. Con Policy Optimizer no sacrifica la disponibilidad a cambio de la seguridad, solo mejora la seguridad.

Convertir reglas por etapas. Puede convertir algunas reglas simples basadas en puertos que permiten aplicaciones conocidas a reglas basadas en App-ID después de que el dispositivo PAN-OS tenga tan solo una semana de logs (Policy Optimizer descubre las aplicaciones que se ven en las reglas mediante la lectura de los logs). Para otras reglas que ven muchas aplicaciones, como una regla general de acceso web, espere al menos 30 días para recopilar información de la aplicación.

Los Servicios profesionales cuentan con una gran cantidad de experiencia en migración. Puede contratar al equipo de Servicios profesionales para ayudarle a cambiar una configuración de sus dispositivos heredados a los servidores de seguridad de nueva generación de Palo Alto Networks y los dispositivos de Panorama.

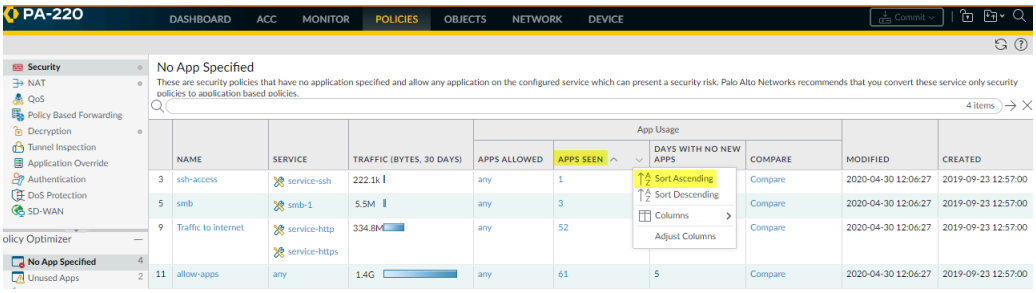
- Convertir reglas simples con aplicaciones conocidas después de una semana
- Reglas para iniciar la conversión después de 30 días

Convertir reglas simples con aplicaciones conocidas después de una semana

Después de una semana de control del tráfico de producción, puede comenzar de manera segura a convertir reglas simples basadas en puertos a reglas basadas en App-ID. Los buenos candidatos incluyen reglas para las que solo una o una pequeña cantidad de aplicaciones conocidas deben usar el puerto legítimamente porque es bastante fácil determinar qué aplicaciones desea permitir en una regla simple. Los ejemplos incluyen el puerto 21 (FTP), el puerto 22 (SSH) y el puerto 53 (DNS).

Instale las Actualizaciones de contenido más recientes antes de comenzar a convertir las reglas para asegurarse de tener las firmas de aplicaciones más recientes en su dispositivo PAN-OS. Este ejemplo muestra cómo ordenar las reglas basadas en puertos para encontrar candidatos para una conversión segura y las opciones para convertir esas reglas basadas en puertos directamente en reglas basadas en App-ID.

STEP 1 | En **Policies (Políticas)** > **Security (Seguridad)** > **Policy Optimizer** > **No App Specified (Ninguna aplicación especificada)**, seleccione **Apps Seen (Aplicaciones vistas)** y **Sort Ascending (Orden ascendente)** (o haga clic en **Apps seen (Aplicaciones vistas)** para invertir el orden de visualización actual) para encontrar las reglas basadas en puertos que han visto la menor cantidad de aplicaciones.

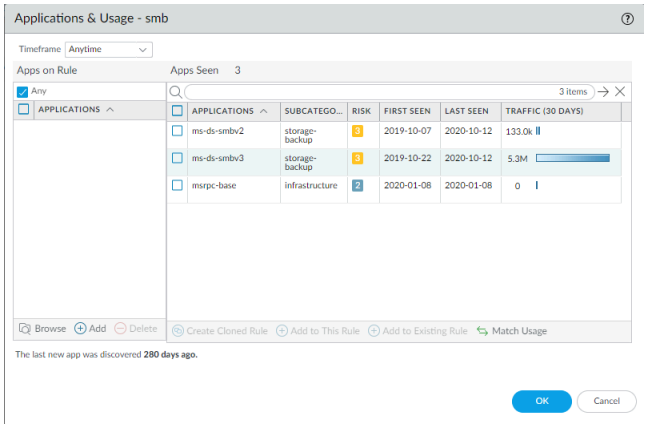


Las reglas basadas en puertos que han visto la menor cantidad de aplicaciones se muestran en la parte superior de la pantalla **No App Specified (Ninguna aplicación especificada)**. Puede convertir de forma segura las reglas para servicios específicos, como SSH, directamente a reglas basadas en aplicaciones, y puede examinar las reglas que han visto pocas aplicaciones para ver si puede convertirlas de manera segura.

La regla basada en puerto destinada a permitir el tráfico del Bloque de mensajes del servidor (SMB) solo ha visto tres aplicaciones desde que migró la configuración al dispositivo PAN-OS y, por lo tanto, es un candidato para la conversión.

STEP 2 | Haga clic en el número de **Apps Seen (Aplicaciones vistas)** o **Compare (Comparar)** para examinar las aplicaciones vistas en la regla.

Applications & Usage (Aplicaciones y uso) muestra las aplicaciones que se ven en el tráfico que coinciden con la regla.



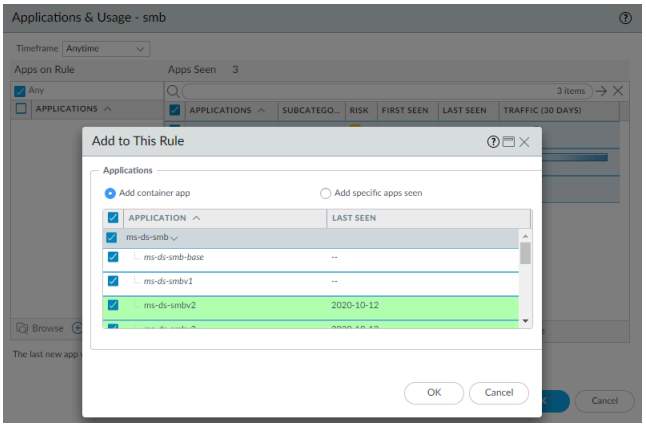
STEP 3 | Evalúe si desea permitir todas, algunas o ninguna de las aplicaciones que se ven en la regla y seleccione las aplicaciones que desea permitir.

Puede igualar el uso exacto de la regla, probar la regla en el futuro añadiendo las aplicaciones de contenedor o seleccionar aplicaciones individuales para añadir a la regla.

- Si desea que la regla permita que todas las aplicaciones coincidan exactamente con la regla:
  1. Seleccione todas las **Applications (Aplicaciones)** en **Apps Seen (Aplicaciones vistas)**.
  2. Haga clic en **Match Usage (Hacer coincidir el uso)**.
  3. Haga clic en **OK (Aceptar)** para convertir la regla basada en puerto en una regla basada en App-ID.
  4. Establezca el **Service (Servicio)** en **application-default (aplicación predeterminada)** de modo que ninguna aplicación malintencionada y evasiva pueda usar el puerto.
- Si desea permitir todas o algunas de las aplicaciones que se ven en la regla o respaldarla de cara al futuro añadiendo sus aplicaciones de contenedor (de modo que se permitan todas las aplicaciones

dentro de cada contenedor y las aplicaciones que se añadan a la aplicación de contenedor más adelante):

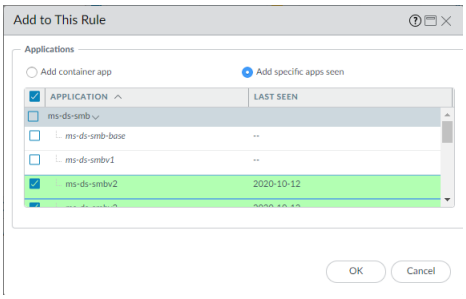
1. Seleccione todas las aplicaciones y luego **Add to This Rule (Añadir a esta regla)**.



   Las aplicaciones sombreadas en gris son las aplicaciones de contenedor. Las aplicaciones sombreadas en verde son las aplicaciones que se ven en la regla. Las aplicaciones sin sombrear pertenecen a la misma aplicación de contenedor pero no se han visto en la regla.

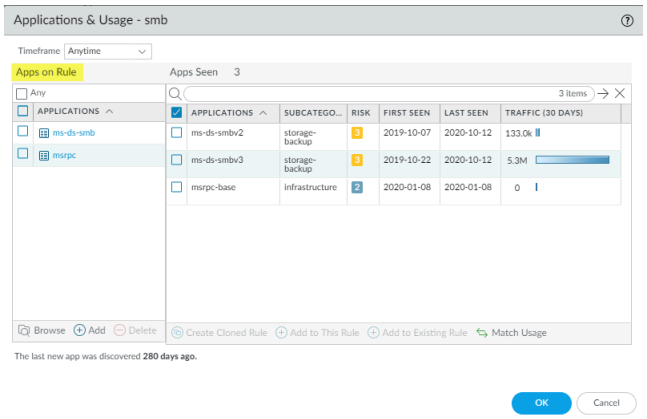
   Add container app (Añadir aplicación de contenedor) se selecciona de forma predeterminada por lo que todas las aplicaciones en el contenedor también se seleccionan de forma predeterminada.

2. Si solo desea que la regla incluya las aplicaciones que coinciden con la regla, seleccione **Add container app (Añadir aplicación de contenedor)**. Solo las aplicaciones que se ven en la regla se añaden a la regla. La aplicación de contenedor y las aplicaciones en la regla que no coinciden con la regla no se seleccionan. Haga clic en **OK (Aceptar)** para seleccionar solo las aplicaciones que se ven en la regla.



   Si desea incluir la aplicación de contenedor y todas sus aplicaciones en la regla, deje la selección como **Add container app (Añadir aplicación de contenedor)** y luego haga clic en **OK (Aceptar)**. Solo las aplicaciones de contenedor aparecen en **Apps on Rule (Aplicaciones en la**

regla) porque incluyen (permiten) todas las aplicaciones que contienen, lo que también "protege de cara al futuro" la regla al permitir que se añadan aplicaciones al contenedor en el futuro:

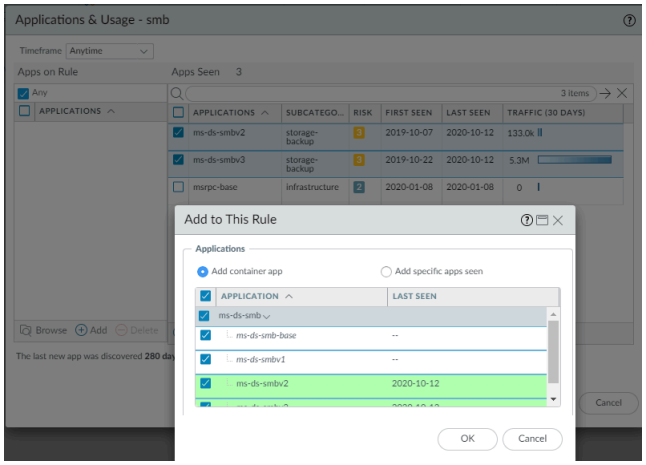


3. Haga clic en **OK (Aceptar)** en la pestaña **Usage (Uso)** para convertir la regla.
4. Establezca el **Service (Servicio)** en **application-default (aplicación predeterminada)** de modo que ninguna aplicación malintencionada y evasiva pueda usar el puerto.

- Si desea seleccionar las aplicaciones que va a permitir dentro de una aplicación de contenedor, seleccione esas aplicaciones y luego haga clic en **Add to This Rule (Añadir a esta regla)**. Por ejemplo, si decide no permitir msrpc-base y selecciona solo ms-ds-smbv2 y ms-ds-smbv3 para **Add to Rule (Añadir a la regla)**, Policy Optimizer le muestra las aplicaciones relacionadas en la aplicación de contenedor (ms-ds-smb, sombreado en gris) y le da la oportunidad de proteger la regla a futuro añadiendo esas aplicaciones:

  1. Seleccione las aplicaciones que desea permitir y luego haga clic en **Add to This Rule (Añadir a esta regla)**.

     Por ejemplo, si decide no permitir msrpc-base y selecciona solo ms-ds-smbv2 y ms-ds-smbv3 para **Add to This Rule (Añadir a esta la regla)**, Policy Optimizer le muestra las aplicaciones relacionadas en la aplicación de contenedor (ms-ds-smb, sombreado en gris) y le da la oportunidad de proteger la regla de cara al futuro con la aplicación de contenedor con todas sus aplicaciones presentes y futuras:

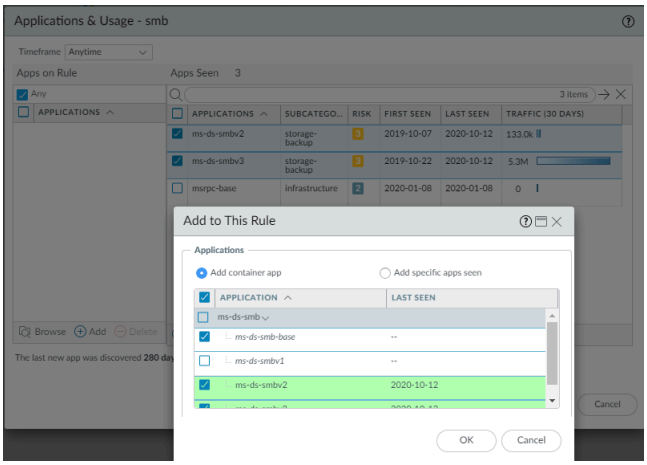


     Las aplicaciones sombreadas en verde son las aplicaciones que se ven en la regla. Las aplicaciones sin sombrear pertenecen a la misma aplicación de contenedor pero no se han visto en la regla.

2. Puede permitir todas las aplicaciones o seleccionar qué aplicaciones permitir.

   Para permitir toda la aplicación de contenedor y todas sus aplicaciones actuales y futuras, haga clic en **OK (Aceptar)**. **Apps on Rule (Aplicaciones en regla)** muestra las aplicaciones seleccionadas. Haga clic en **OK (Aceptar)** para convertir la regla.

   Para permitir solo las aplicaciones seleccionadas, deseleccione las aplicaciones no deseadas. Si deselecciona una aplicación en un contenedor, la aplicación de contenedor también se deselecciona para que no dé permiso automáticamente a sus aplicaciones secundarias.



3. Haga clic en **OK (Aceptar)**. **Apps on Rule (Aplicaciones en regla)** muestra las aplicaciones seleccionadas.
4. Haga clic en **OK (Aceptar)** para convertir la regla.
5. Establezca el **Service (Servicio)** en **application-default (aplicación predeterminada)** de modo que ninguna aplicación malintencionada y evasiva pueda usar el puerto.

Reglas para iniciar la conversión después de 30 días

Después de 30 días de controlar el tráfico de producción, puede comenzar a convertir de manera segura el resto de las reglas basadas en puertos en reglas basadas en App-ID y limpiar la base de reglas. Un buen lugar para comenzar es limpiar las reglas no utilizadas para reducir la superficie de ataque. Después de eso, comience a convertir las reglas a App-ID en el perímetro con su regla de acceso a Internet de salida (puerto 80/443), ya que esa regla probablemente ve más tráfico con más aplicaciones que cualquier otra regla, lo que también significa que es la regla que tiene mayor riesgo.

Instale las Actualizaciones de contenido más recientes antes de comenzar a convertir las reglas para asegurarse de tener las firmas de aplicaciones más recientes en su dispositivo PAN-OS.

Policy Optimizer ofrece muchas formas intuitivas de ordenar, filtrar y priorizar qué reglas convertir primero. Después de eliminar las reglas no utilizadas y convertir la regla de acceso web a App-ID, las reglas que seleccione para priorizar dependerán de su negocio y los requisitos de seguridad. Piense en qué aplicaciones son críticas para su negocio y el riesgo de un incidente y las posibles consecuencias a medida que prioriza.

Las siguientes secciones proporcionan ideas y métodos para usar opciones de clasificación y filtrado simples pero potentes para identificar y priorizar las reglas que va a convertir después de los primeros 30 días:

- Retirar reglas no utilizadas (reglas que no coinciden con el tráfico)

- Convertir las reglas más estables (reglas que no ven nuevas aplicaciones durante un período de tiempo)
- Convertir las reglas de acceso a Internet (reglas que controlan el tráfico en el puerto HTTP 80 y el puerto HTTPS 443)
- Convertir reglas que vean el mayor tráfico (reglas que ven más tráfico durante un período de tiempo)
- Convertir reglas con pocas aplicaciones vistas a lo largo de un período de tiempo (fácil de identificar y convertir)

Retirar reglas no utilizadas

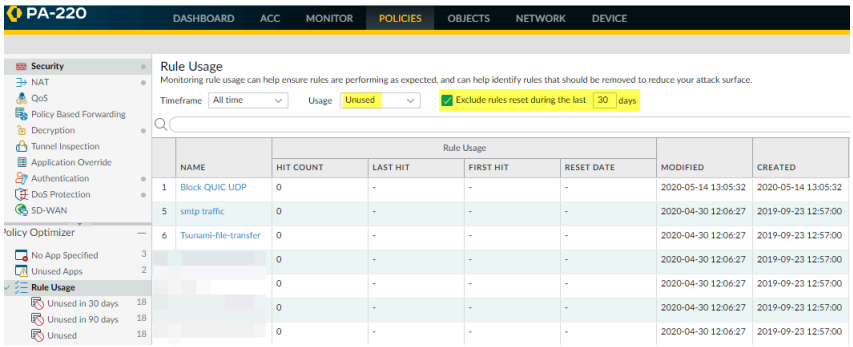
La base de reglas migrada a menudo contiene reglas que no están en uso porque ningún tráfico de aplicaciones coincide con esas reglas. Las reglas no utilizadas saturan la base de reglas y ofrecen avenidas de ataque a los adversarios. Elimine estas reglas para limpiar la base de reglas y reducir la superficie de ataque, o modifíquelas para que se apliquen al tráfico de aplicaciones y tengan un objetivo legítimo en la base de reglas.

Las reglas no utilizadas pueden existir por varias razones. Las reglas que rigen los servicios y aplicaciones que una vez utilizó la empresa pero que se sustituyeron con otras aplicaciones pueden estar en la base de reglas. Una regla que precede a una regla no utilizada puede controlar las aplicaciones que, de lo contrario, coincidirían con la regla no utilizada. En algunos casos, las reglas no utilizadas son reglas antiguas creadas por administradores que ya no están en la empresa y además, los administradores actuales no conocen el objetivo de dichas reglas.

Ver reglas en cualquier **Timeframe (Periodo de tiempo)** que elija (**Policies [Políticas]** > **Security [Seguridad]** > **Policy Optimizer** > **Rule Usage [Uso de regla]**). Establezca el **Use (Uso)** en **Unused (No usado)** para eliminar las reglas que han visto tráfico de aplicaciones.

STEP 1 | Identifique reglas no utilizadas.

En **Policies (Políticas)** > **Security (Seguridad)** > **Policy Optimizer** > **Rule Usage (Uso de regla)**, establezca el **Timeframe (Periodo de tiempo)**en **All time (Todo el tiempo)**, establezca el **Usage (Uso)** en **Unused (No usado)** (para mostrar solo las reglas con un recuento de resultados de cero), y **Exclude rules reset during the last 30 days (Excluir reglas reiniciadas durante los últimos 30 días)** (para evitar mostrar las reglas recientemente restablecidas que pueden no haber visto tráfico en los últimos días pero que pueden ver tráfico en un período de tiempo más largo). El resultado es una lista de reglas que no han visto tráfico de aplicaciones en el **Timeframe (Periodo de tiempo)** seleccionado.



STEP 2 | Evalúe las reglas que no han visto tráfico y determine si son necesarias o si puede deshabilitarlas.

En este ejemplo, la empresa usó la aplicación de transferencia de archivos Tsunami en el pasado, pero la investigación muestra que la empresa ya no usa Tsunami, por lo que no hay razón para permitir el tráfico de la aplicación Tsunami en la red.

STEP 3 | Puede **Disable (Deshabilitar)** o **Delete (Eliminar)**) la regla.

En **Policies (Políticas)** > **Security (Seguridad)**, seleccione la regla de transferencia de archivos Tsunami y seleccione **Disable (Desactivar)** o **Delete (Eliminar)** la regla.

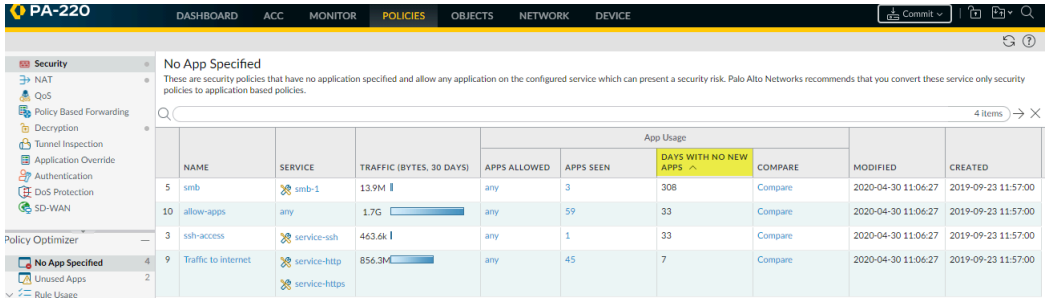
La deshabilitación de la regla es más seguro en caso de que su empresa necesite la aplicación más adelante, aunque no haya visto ningún tráfico. (Esto puede suceder si no tiene en cuenta los eventos trimestrales y anuales al investigar si la empresa utiliza una aplicación, o si la aplicación es necesaria para un proveedor o socio cuyo tráfico solo accede a la red periódicamente). Después de un período de tiempo razonable, elimine las reglas no utilizadas que desactivó anteriormente.

Convertir las reglas más estables

Convierta las reglas basadas en puertos que no han visto nuevas aplicaciones durante un período de tiempo razonable, lo que significa que las reglas se han estabilizado y es menos probable que vean nuevas aplicaciones en ellas. Duplique estas reglas para asegurarse de que si más aplicaciones coinciden con la regla más adelante, la regla basada en puerto permanezca en la base de reglas durante el tiempo que sea necesario como una red de seguridad.

Tenga en cuenta las aplicaciones que se utilizan solo para eventos trimestrales, anuales y otros eventos periódicos cuando considere si las nuevas aplicaciones coincidirán con la regla.

STEP 1 | En **Policies (Políticas)** > **Security (Seguridad)** > **Policy Optimizer** > **No App Specfied (Ninguna aplicación especificada)**, ordene las reglas (descendente) para mostrar las reglas con el mayor número de **Days with No New Apps (Días sin nuevas aplicaciones)** al inicio de la lista.

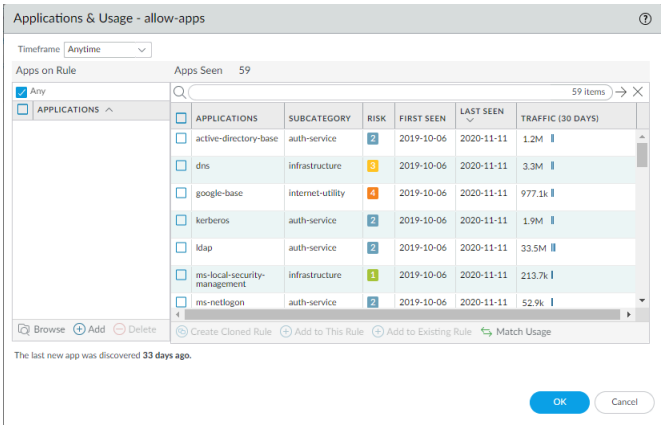


Las primeras tres reglas no han visto nuevas aplicaciones durante más de 30 días y son candidatas para la conversión a App-ID. [Convertir reglas simples con aplicaciones conocidas después de una semana describe las reglas de conversión con pocas **Apps Seen (Aplicaciones vistas)**, como la regla smb, por lo que este ejemplo se centra en la regla para permitir aplicaciones].

*Compruebe la fecha **Modified (Modificada)** porque las reglas que no han sido modificadas durante un largo tiempo también pueden ser más estables. Es posible que las reglas que se han modificado recientemente no hayan visto todas las aplicaciones que podrían coincidir con la regla.*

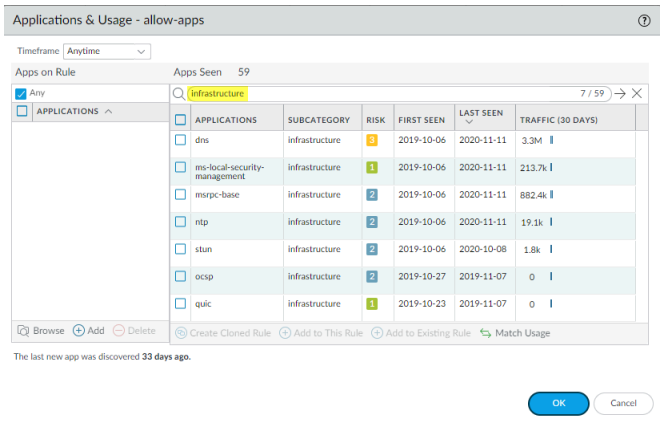
Dado que varias aplicaciones han sido vistas en la regla, duplique la regla en lugar de convertirla directamente en una regla basada en App-ID.

STEP 2 | Haga clic en el número de **Apps Seen (Aplicaciones vistas)** para abrir el cuadro de diálogo **Applications & Usage (Aplicaciones y uso)**.



STEP 3 | Ordene y filtre las **Apps Seen (Aplicaciones vistas)** en la regla para determinar cómo gestionar las aplicaciones.

Ordenar o filtrar por subcategoría le ayuda a comprender el tráfico que se ve en las reglas que ven varias aplicaciones. Por ejemplo, puede filtrar por la subcategoría de infraestructura para ver todas las aplicaciones de infraestructura y duplicar una regla basada en App-ID para controlarlas.



STEP 4 | Siga del Paso 4 al Paso 7 en Convertir las reglas de acceso a Internet para crear una regla duplicada que controle cada subcategoría (o subcategorías relacionadas) de las aplicaciones que desea tratar de manera similar.

Convertir las reglas de acceso a Internet

Una regla de acceso a Internet controla el tráfico en el puerto 80 (HTTP) y el puerto 443 (HTTPS). Esta regla generalmente ve la mayor cantidad de aplicaciones y la mayor cantidad de tráfico en bytes. Una regla de acceso a Internet basada en puertos puede permitir aplicaciones que no desea en su red y exponerlas a ataques. Controle y habilite de forma segura las aplicaciones que permite en esos puertos convirtiendo la regla de acceso a Internet basada en puertos en un conjunto de reglas basadas en aplicaciones. Para hacer esto, debe comprender qué aplicaciones autoriza su empresa para uso comercial y qué aplicaciones tolera su empresa para otros fines.

Un buen método de conversión es agrupar las aplicaciones que requieren un tratamiento similar en la misma regla en lugar de crear reglas separadas para cada aplicación para ayudar a prevenir el

sobredimensionamiento de la base de reglas. Utilice Policy Optimizer para ordenar las aplicaciones que se ven en una regla por subcategoría de aplicación, para que pueda ver todas las aplicaciones en una regla para una subcategoría en particular, seleccione las aplicaciones que utiliza su empresa y luego duplique una regla para controlar esas aplicaciones. Policy Optimizer ofrece muchas opciones de clasificación y filtrado para organizar y analizar las aplicaciones vistas en una regla.

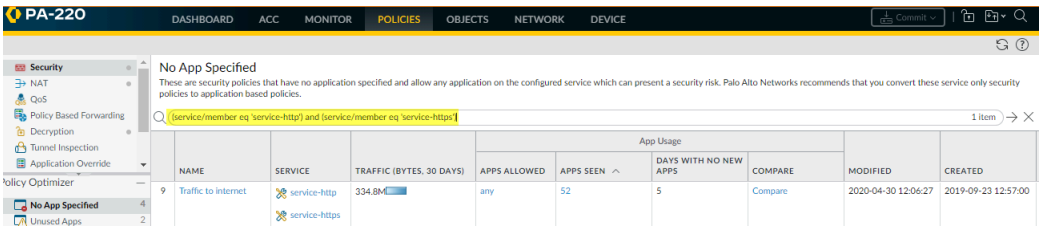
Duplique la regla en lugar de convertirla directamente para garantizar la disponibilidad de la aplicación. La duplicación de una regla conserva la regla original basada en el puerto y coloca la regla basada en la aplicación duplicada directamente sobre la regla basada en el puerto en la base de reglas de seguridad. Creer diferentes reglas de acceso a internet a partir de la regla original basada en puerto para grupos de aplicaciones que desea tratar de manera diferente, sin arriesgar la disponibilidad de la aplicación. Fácilmente qué aplicaciones coinciden con la regla duplicada y qué aplicaciones se filtran a través de la regla original basada en el puerto y luego ajuste las reglas según sea necesario. Cuando ninguna de las aplicaciones que desea permitir coincida con la regla basada en puertos durante un período de tiempo suficientemente largo para estar seguro de que ha contabilizado todas las aplicaciones que la empresa requiere, puede desactivar (o eliminar) la regla basada en puertos. Esto finalizaría la conversión sin arriesgar la disponibilidad de la aplicación.

Utilice el mismo método para convertir otras reglas que han visto varias aplicaciones conocidas. Utilice la información de **Policies (Políticas)** > **Security (Seguridad)** > **Policy Optimizer** > **No App Specified (Ninguna aplicación especificada)** para ayudarle a priorizar las reglas que desea convertir después de convertir las reglas de acceso a internet. Por ejemplo, podría priorizar en base a una combinación de la mayoría de las **Apps seen (Aplicaciones vistas)** y la mayoría del tráfico en los últimos 30 días [**Traffic (Bytes, 30 days) [Tráfico (Bytes, 30 días)]**] para convertir las reglas más usadas, o puede mirar a los **Days with No New Apps (Días sin nuevas aplicaciones)** y la fecha **Modified (Modificada)** para encontrar reglas que han visto muchas aplicaciones pero también que sean más estables.

Este ejemplo muestra cómo duplicar una regla basada en la aplicación que controla las aplicaciones típicas de una empresa desde una regla de acceso a internet basada en puerto. Utilice el mismo proceso de duplicación para crear reglas basadas en aplicaciones de forma segura para diferentes subcategorías y aplicaciones individuales que se ven en cualquier regla basada en puertos.

STEP 1 | Vaya a **Policies (Políticas)** > **Security (Seguridad)** > **Policy Optimizer** > **No App Specfied (Ninguna aplicación especificada)** y encuentre las reglas basadas en puertos que controlan el acceso a internet.

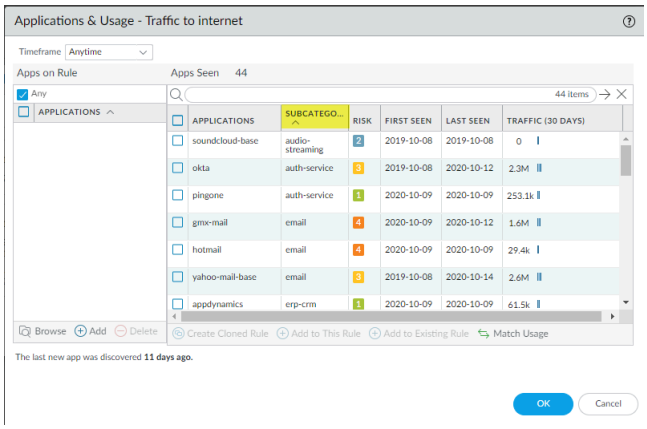
Utilice el filtro **`(service / member eq 'service-http') y (service / member eq 'service-https')`** para encontrar las reglas basadas en puerto configuradas con **service-http** y **service-https**, que es o son las reglas de acceso a internet.



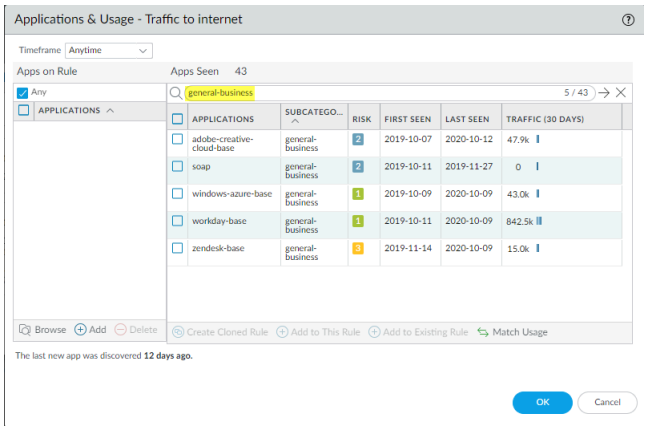
STEP 2 | Haga clic en**Compare (Comparar)** o en el número de **Apps Seen (Aplicaciones vistas)** para abrir el cuadro de diálogo **Applications & Usage (Aplicaciones y uso)**.

STEP 3 | Ordene **Apps Seen (Aplicaciones vistas)** por subcategoría de aplicación para agrupar aplicaciones similares que pueden ser apropiadas para controlar en la misma regla de política de seguridad.

Ordene por **subcategory (Subcategoría)** para agrupar las aplicaciones vistas en la regla:



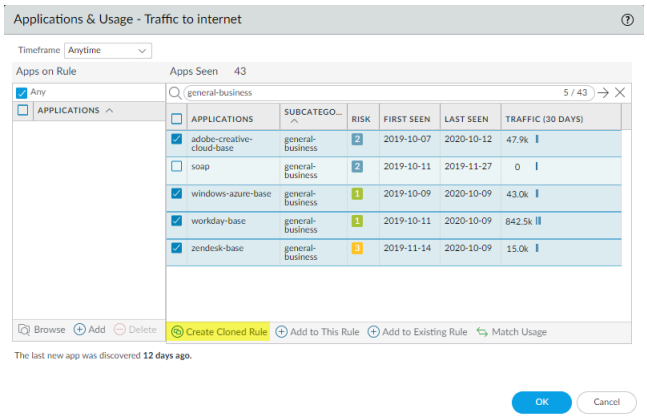
También puede filtrar por una subcategoría particular para ver solo las aplicaciones que pertenecen a esa subcategoría. En este ejemplo, para crear una regla basada en App-ID para controlar las aplicaciones típicas de una empresa, filtre para ver solo las aplicaciones típicas de una empresa que se ven en la regla:



STEP 4 | Seleccione las aplicaciones que desea permitir y luego **Create Cloned Rule (Crear Regla duplicada)** para duplicar la nueva regla basada en aplicación a partir de la regla basada en puerto.

En este ejemplo, la empresa usa cuatro de las aplicaciones, pero no ha usado una de las aplicaciones durante un largo período de tiempo, lo que puede ver en las columnas **Last Seen (Vista por última**

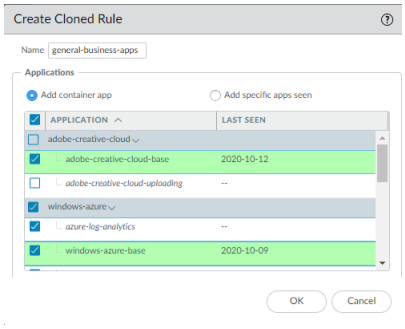
vez) y **Traffic (30 Days) [Tráfico (30 días)]**. Según el uso y las aplicaciones autorizadas por la empresa, la empresa elige no permitir la aplicación que no está utilizando.



STEP 5 | En el cuadro de diálogo **Clone (Duplicar)**, seleccione las aplicaciones asociadas con cada aplicación de contenedor que desee permitir.

Asigne un **Name (Nombre)**a la nueva regla que describa su propósito; en este ejemplo, general-business-apps. Decida si desea permitir solo aplicaciones específicas de cada aplicación de contenedor o si desea permitir la aplicación de contenedor. Si proporciona permisos a la aplicación de contenedor entonces todas las aplicaciones en el contenedor también tienen permiso. Esto protege la regla a futuro ya que permite automáticamente nuevas aplicaciones si se añaden a la aplicación de contenedor que ayuda a garantizar la disponibilidad de la aplicación. Por defecto, todas las aplicaciones están seleccionadas. Las aplicaciones de contenedor para cada aplicación están sombreadas en gris, las aplicaciones que se han visto en la regla están sombreadas en verde, y las aplicaciones en la aplicación de contenedor que no se han visto en la regla están en cursiva y no están sombreadas.

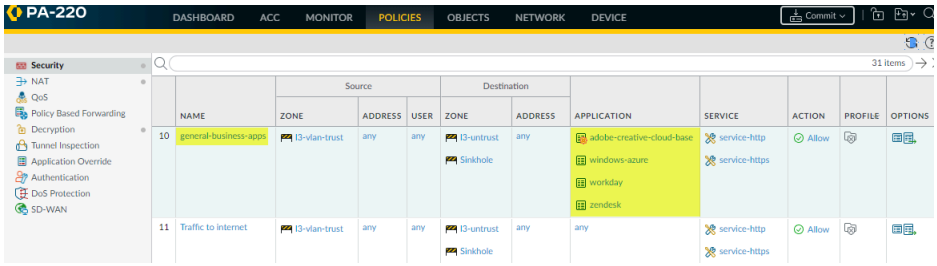
En la ilustración de este ejemplo, puede ver las aplicaciones de contenedor "adobe-creative-cloud" y "windows-azure" atenuadas, las aplicaciones que se ven en la regla en verde ("adobe-creative-cloud-base" y "windows-azure -base") y dos aplicaciones que no se han visto en la regla en cursiva (“adobe-creative-cloud-uploading” y “azure-log-analytics”). El ejemplo muestra que la aplicación "adobe-creative-cloud-uploading" no está seleccionada, lo que también deselecciona automáticamente su aplicación de contenedor ("adobe-creative-cloud") mientras que todas las aplicaciones de "windows-azure" permanecen seleccionadas, por lo que la aplicación de contenedor windows-azure” permanece seleccionada.



Anule la selección de una aplicación si no desea que los usuarios tengan acceso a esa aplicación en particular. Sin embargo, si se añaden nuevas aplicaciones a la aplicación de contenedor "adobe-creative-cloud", el cortafuegos no las permitirá de forma automática porque la aplicación de contenedor

no está seleccionada. Por el contrario, si se añaden nuevas aplicaciones a la aplicación de contenedor "windows-azure", el cortafuegos las aceptará automáticamente, lo que protege la regla de cara al futuro.

STEP 6 | Haga clic en **OK (Aceptar)** para volver a la pestaña Uso de la regla de la política de seguridad y luego haga clic en **OK (Aceptar)** nuevamente para crear la regla. El cortafuegos coloca la regla por encima de la regla basada en el puerto en la base de reglas de la política de seguridad (**Policies (Políticas)** > **Security (Seguridad)**).



Si selecciona una aplicación de contenedor, Policy Optimizer añade solo la aplicación de contenedor a la regla porque la regla de seguridad incluye todas las aplicaciones. El engranaje rojo para "adobe-creative-cloud-base" indica que es una aplicación individual, no una aplicación contenedora.

STEP 7 | Haga clic en la regla **Name (Nombre)** o en **Service (Servicio)** y cambie el **Service (Servicio)** a **application-default (aplicación predeterminada)** para evitar que las aplicaciones evasivas obtengan acceso a un puerto no estándar.

STEP 8 | Siempre que necesite permitir a otras aplicaciones típicas de una empresa autorizadas, añádalas a la regla general-business-apps y elimine las aplicaciones de la regla si ya no las usa.

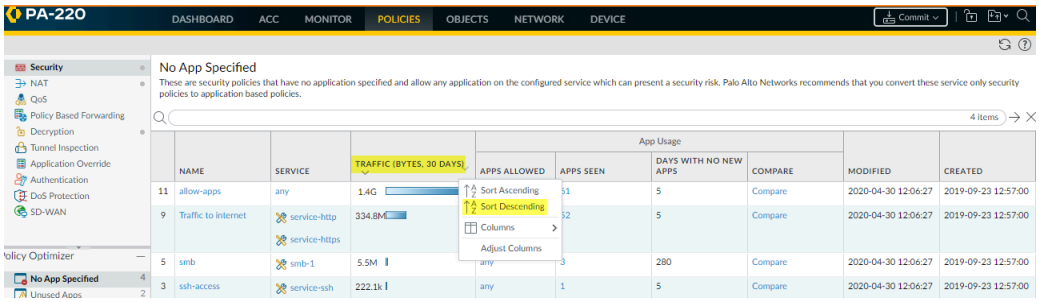
Convertir reglas que vean el mayor tráfico

La clasificación de las reglas que han visto el mayor tráfico en los últimos 30 días (**Traffic (Bytes, 30 days) [Tráfico (Bytes, 30 días)]**) le muestra las reglas actuales más activas. (Un periodo de tiempo más largo pueden inducirle al error al poner énfasis en las reglas más antiguas que permanecen en la parte superior de la lista porque tienen grandes totales acumulados, incluso si ya no ven mucho tráfico). La conversión de estas reglas a reglas basadas en App-ID protege la mayor cantidad de tráfico para su esfuerzo.

Si varias reglas ven mucho tráfico, use la información de **Policies (Políticas)** > **Security (Seguridad)** > **Policy Optimizer** > **No App Specified (Ninguna aplicación especificada)** para ayudar a priorizar qué reglas convertir primero. Por ejemplo, podría dar prioridad a las reglas con la mayor cantidad de **Apps Seen (Aplicaciones vistas)** (potencialmente las reglas con mayor riesgo) o las reglas con la mayoría de **Days with No New Apps (Días sin nuevas aplicaciones)** y la fecha **Modified (Modificada)** más antiguo (las reglas de alto tráfico más estables).

STEP 1 | En **Policies (Políticas)** > **Security (Seguridad)** > **Policy Optimizer** > **No App Specfied (Ninguna aplicación especificada)**, ordene las reglas en orden descendente por **Traffic (Bytes, 30 days)**

[Tráfico (Bytes, 30 días)] para colocar las reglas con actividad más reciente en la parte superior de la lista.



STEP 2 | Seleccione una regla para comenzar la conversión y haga clic en el número de **Apps Seen (Aplicaciones vistas)**.

STEP 3 | En el cuadro de diálogo **Applications & Usage (Aplicaciones y uso)**, ordene y filtre las **Apps Seen (Aplicaciones vistas)** en la regla para determinar cómo gestionar las aplicaciones.

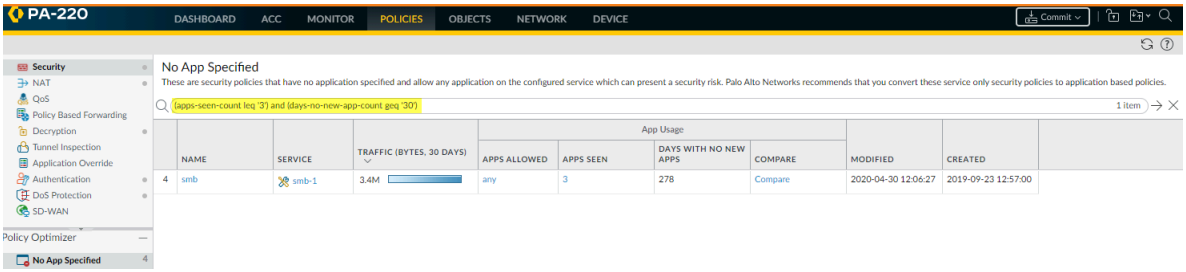
Ordene o filtre por subcategoría de aplicación para agrupar las aplicaciones que puedan requerir un tratamiento similar y que se puedan controlar en una regla basada en aplicación. Ordene por **Traffic (30 days) [Tráfico (30 días)]** para ver la cantidad de tráfico reciente en aplicaciones individuales para dar prioridad a las aplicaciones más activas en este momento.

STEP 4 | Siga del Paso 4 al Paso 7 en Convertir las reglas de acceso a Internet para crear una regla duplicada que controle cada subcategoría (o subcategorías relacionadas) de las aplicaciones que desea tratar de manera similar.

Convertir reglas con pocas aplicaciones vistas a lo largo de un período de tiempo

Reglas con relativamente pocas **Apps Seen (Aplicaciones vistas)** y sin nuevas aplicaciones vistas durante un período de tiempo suficientemente largo, pueden ser fáciles de convertir, relativamente estables y fáciles de identificar mediante filtros.

STEP 1 | En **Policies (Políticas)** > **Security (Seguridad)** > **Policy Optimizer** > **No App Specfied (Ninguna aplicación especificada)**, filtre las reglas para mostrar solo las reglas con un número bajo de **Apps Seen (Aplicaciones vistas)** y que no han visto aplicaciones en un período de tiempo específico.



Este ejemplo filtra las reglas que han visto tres o menos aplicaciones. **`(apps seen count leq '3')`** y para las que no se han visto aplicaciones durante al menos 30 días. **`(days no new app count geq '30')`**.

STEP 2 | Seleccione una regla para convertir y haga clic en el número de **Apps Seen (Aplicaciones vistas)**.

STEP 3 | En el cuadro de diálogo **Applications & Usage (Aplicaciones y uso)**, decida si desea permitir todas las aplicaciones y si deberían estar en la misma regla; es decir, decida si las aplicaciones requieren un tratamiento similar en términos de acceso y seguridad.

Si desea permitir todas las aplicaciones y estas requieren un tratamiento similar, puede **Match Usage (Hacer coincidir el uso)** y sustituir la regla basada en puerto con la nueva regla basada en App-ID.

Si desea permitir todas las aplicaciones pero estas requieren un tratamiento diferente, duplique la regla para cada conjunto de aplicaciones que requiera un tratamiento diferente. Por ejemplo, si una regla basada en puerto permite tres aplicaciones y dos de ellas son aplicaciones de correo electrónico y una es una aplicación de infraestructura, es posible que desee duplicar una regla para las aplicaciones de correo electrónico y otra para la aplicación de infraestructura.

Si desea permitir algunas aplicaciones y denegar a otras:

- Duplique una o más reglas para las aplicaciones que desea conservar y supervise la regla original basada en puerto para asegurarse de que las aplicaciones que no desea conservar son las únicas que coinciden con esa regla. Cuando haya transcurrido el tiempo suficiente para estar seguro de que ninguna de las aplicaciones que desea permitir coincida con la regla basada en el puerto, puede inhabilitarla o eliminarla. Los pasos 4 al 7 en Convertir las reglas de acceso a Internet muestran cómo crear una regla duplicada.
- Si está seguro de saber qué aplicaciones desea permitir y qué aplicaciones desea bloquear:
  - Si las aplicaciones que desea permitir requieren un tratamiento similar, utilice **Add to This Rule (Añadir a esta regla)** para sustituir la regla basada en puerto con una regla basada en la aplicación que permita solo las aplicaciones que añadió a la regla. Las aplicaciones que no añada a la regla se bloquean a menos que las permita en otra regla.
  - Si las aplicaciones que desea permitir requieren un tratamiento diferente, duplique las reglas basadas en la aplicación para las aplicaciones que desea permitir desde la regla basada en puerto. Si continúa seguro de que está bien bloquear las aplicaciones restantes, puede deshabilitar (o eliminar) la regla basada en puerto.

Siguientes pasos para adoptar las prácticas recomendadas de seguridad

Después de terminar su primer paso en la conversión de reglas basadas en puertos a reglas basadas en aplicaciones, considere los siguientes pasos para fortalecer la base de reglas de su Política de seguridad y mejorar la seguridad de la red:

- Utilice la Capacidad de enriquecimiento de reglas de Expedition, que utiliza el aprendizaje automático para examinar y consolidar la configuración de su política.
- Ejecute la Evaluación de las prácticas recomendadas (BPA) regularmente para medir el progreso hacia el logro de su objetivo de adopción de App-ID e identificar puntos débiles adicionales. Cuando alcance su objetivo, use la BPA para identificar las áreas donde puede continuar mejorando la adopción y proteger aún más su red.
- Policy Optimizer convierte las reglas basadas en puertos en reglas basadas en App-ID pero no cambia nada más sobre las reglas. Después de convertir las reglas heredadas en reglas basadas en App-ID, ajuste las reglas para reducir la superficie de ataque y aumentar la visibilidad:
  - Establezca el **Service (Servicio)** en **application-default (aplicación predeterminada)** para evitar que las aplicaciones utilicen puertos no estándar. Para aplicaciones internas personalizadas, defina puertos predeterminados y luego aplique **application-default (aplicación predeterminada)**.
  - En el perímetro (puerta de enlace de internet), para aplicaciones web, utilice categorías de Filtrado de URL para evitar el acceso a sitios web peligrosos.
  - Configure User-ID para controlar quién tiene acceso a las aplicaciones.
  - Configure el Reenvío de logs para centralizar los registros de múltiples dispositivos PAN-OS, para enviar alertas de correo electrónico a administradores específicos o grupos para alertas específicas, y para preservar los logs para análisis históricos.
  - Configure los perfiles de seguridad de prácticas recomendadas para antivirus, antispyware, protección frente a vulnerabilidades, bloqueo de archivos y análisis de WildFire y aplíquelos a las reglas de política de seguridad de App-ID.
  - Considere utilizar plantillas de Iron-Skillet, disponibles en GitHub, para empezar y arrancar su configuración inicial de prácticas recomendadas.
- Mantenga la implementación de App-ID. A medida que añade reglas para nuevas aplicaciones, incluidas las aplicaciones internas personalizadas, cree reglas basadas en App-ID que ayuden a mantener su red segura. No vuelva a usar las reglas basadas en puertos que no le dan visibilidad del tráfico de aplicaciones ni le permiten inspeccionar y controlarlas. Aprenda más acerca de App-ID en la Guía del administrador de PAN-OS.
- A medida que refuerza la base de reglas de la política de seguridad, considere aplicar otras protecciones a su red, como por ejemplo las prácticas recomendadas para descifrar el tráfico y para protección de DoS y zonas.

Si necesita ayuda para migrar la configuración de su dispositivo heredado a los dispositivos de Palo Alto Networks, póngase en contacto con el Grupo de servicios profesionales de Palo Alto Networks, que cuenta con una gran experiencia en migración que le puede servir para lograr una migración y una conversión a App-ID exitosas.