Introducción a la BPA

10.0 (EoL)

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS

Contact Information

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

About the Documentation

- To ensure you are viewing the most current version of this document, or to access 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 15, 2020

Table of Contents

Evaluar la adopción de la capacidad de la política de seguridad

La herramienta de Evaluación de prácticas recomendadas (BPA) le ayuda a comprender su nivel actual de adopción de la capacidad de la política de seguridad y le ayuda a evaluar la madurez y la eficacia de su posición de seguridad. La adopción de capacidades como WildFire, protección frente a vulnerabilidades, descifrado SSL, etc., contribuye a detectar y prevenir ataques. Desarrollar un entendimiento sólido de cómo y dónde usar cada capacidad en diferentes entornos es fundamental para comprender cómo proteger mejor su red y sus valiosos activos.

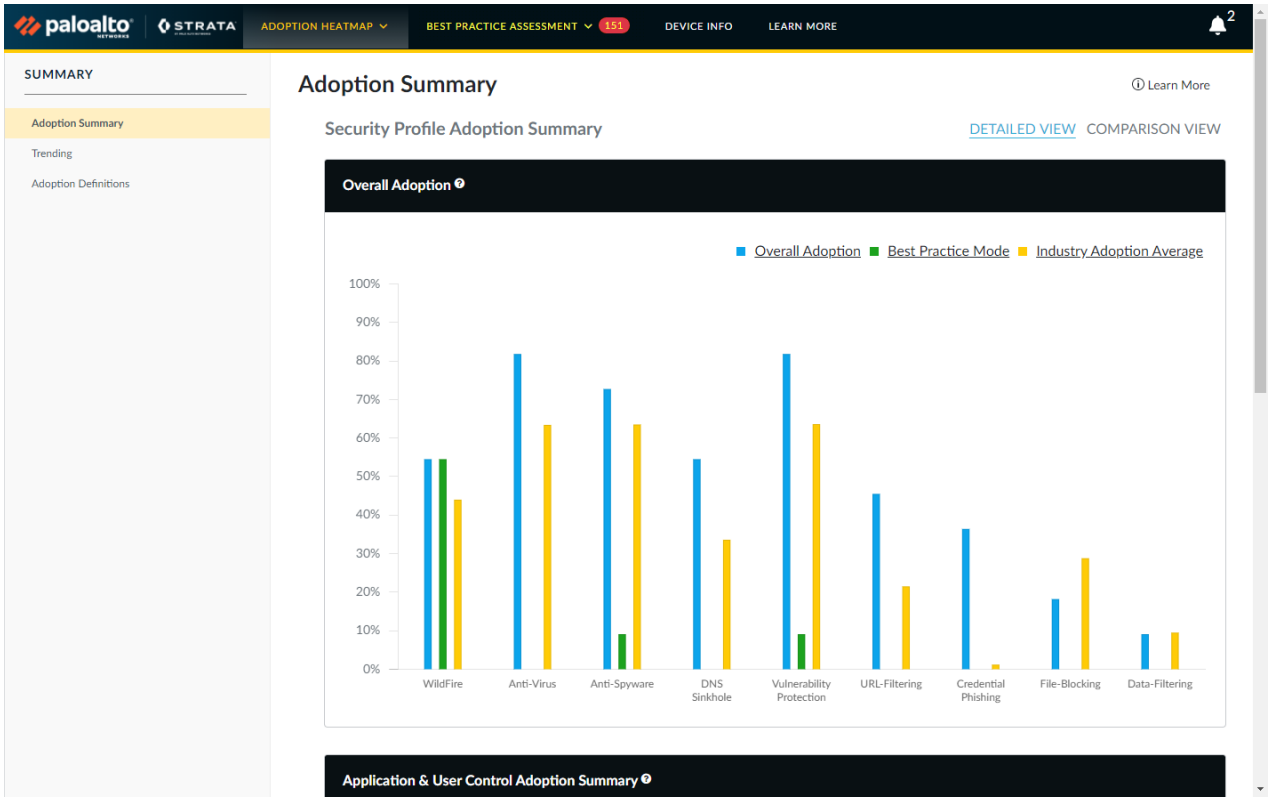
Introducción a las prácticas recomendadas muestra cómo acceder y ejecutar la BPA. La sección Mapas de calor de adopción de capacidades del informe de la BPA le permite revisar la adopción de estas capacidades en toda la base de reglas de la Política de seguridad. Vea el vídeo Introducción a Mapas de calor para obtener más información sobre Mapas de calor y aprovechar las ventajas de la Videoteca de BPA para aprender más sobre la herramienta.

Revise y analice la información en las pestañas de Mapa de calor para identificar las brechas en la adopción de capacidad de seguridad y determinar qué desea mejorar:

- Revisar el resumen de adopción
- Identificar brechas en la adopción
- Identificar reglas para mejorar

Revisar el resumen de adopción

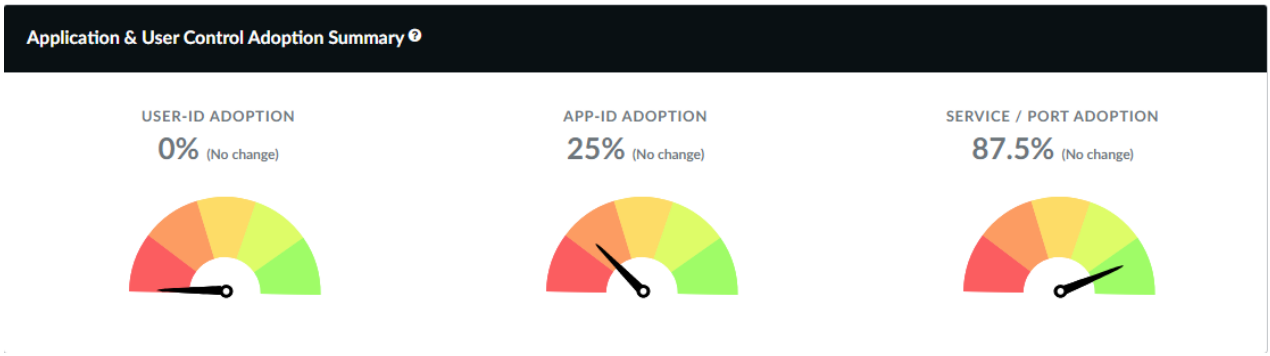
Después de que usted o su representante de Palo Alto Networks ejecute la BPA, el informe HTML resultante se abre en la página Mapa de calor de adopción, en el resumen de adopción. La vista Resumen de adopción proporciona una descripción general de la adopción general de las capacidades de seguridad de su dispositivo. El informe muestra el porcentaje de adopción actual para cada métrica (excepto el promedio de la industria, que proporciona los promedios de adopción en su sector), y entre paréntesis, el cambio porcentual en la adopción desde la última vez que ejecutó la BPA en el archivo de configuración del dispositivo (o **No change (Ningún cambio)** si el valor es el mismo que la última vez que ejecutó la BPA).



Adopción general: La adopción de perfiles de seguridad en las reglas de permiso de la política de seguridad. Los porcentajes se basan en el número de reglas de permiso que tienen uno o más perfiles habilitados como parte de la regla. La BPA no cuenta las reglas deshabilitadas o las reglas de bloqueo.

Promedio del sector: La media de adopción de perfiles de seguridad en las reglas de permiso para el sector de su empresa.

Modo de prácticas recomendadas: La adopción de los perfiles de seguridad configurados según las prácticas recomendadas en las reglas de permiso. La BPA solo cuenta las reglas con perfiles que pasan todas las comprobaciones de prácticas recomendadas.

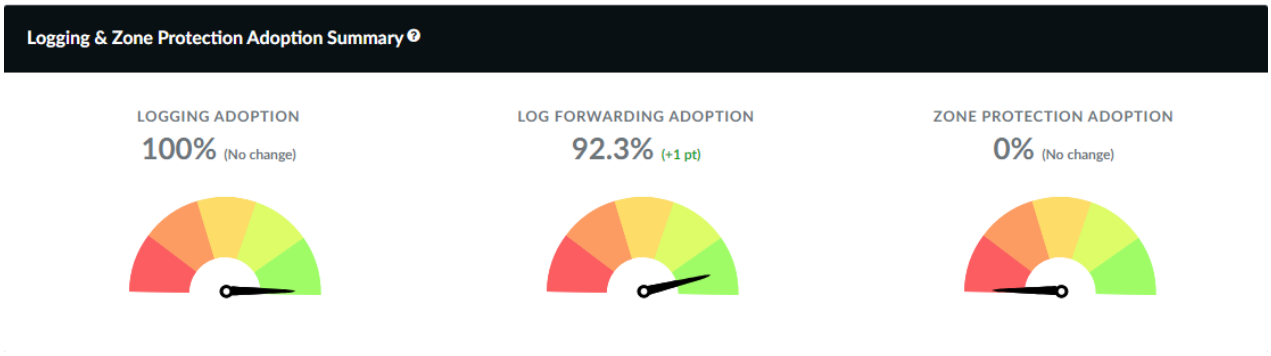


Adopción de App-ID: La adopción de App-ID en todas las reglas de política de seguridad. El valor porcentual se basa en el número total de reglas de permiso con una o más aplicaciones definidas (la Aplicación no es **any [cualquiera]**). La BPA no cuenta las reglas deshabilitadas.

Adopción de User-ID: La adopción de User-ID en todas las reglas de la política de seguridad. El valor porcentual se basa en el número total de reglas de permiso con los usuarios (incluidos los valores **known-user (usuario conocido)** y **unknown (desconocido)**) o grupos de usuarios. La BPA no cuenta las reglas deshabilitadas.

Adopción de servicio/puerto: La adopción de servicio/puerto en todas las reglas de la política de seguridad. El valor porcentual se basa en el número total de reglas de permiso con un servicio o puerto definido (el Servicio no es **any [cualquiera]**). La BPA no cuenta las reglas deshabilitadas.

La BPA no cuenta con App-ID, User-ID o la adopción de servicio/puerto para las reglas de bloqueo porque el razonamiento para el bloqueo difiere de una empresa a otra, por lo que la BPA no puede hacer recomendaciones basadas en las reglas de bloqueo.

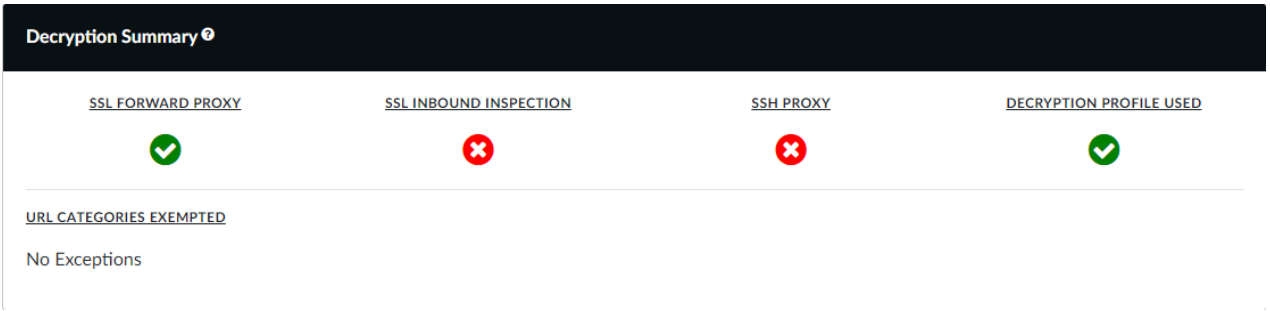


Adopción de generación de logs: La adopción de **Log at Session End (Log al finalizar sesión)** en todas las reglas de la política de seguridad. El valor porcentual se basa en el número total de reglas con **Log at Session End (Log al finalizar sesión)** habilitado. La BPA no cuenta las reglas deshabilitadas.

Adopción de reenvío de logs: La adopción de perfiles de reenvío de logs en todas las reglas de la política de seguridad. El valor porcentual se basa en el número total de reglas con un perfil de reenvío de logs configurado. La BPA no cuenta las reglas deshabilitadas.

Adopción de Protección de zona: La adopción de protección de zonas en todas las reglas de permiso de las políticas de seguridad. El valor porcentual se basa en el número total de reglas de permiso en las que la zona de origen tiene un perfil de Protección de zona configurado. La BPA no cuenta las reglas deshabilitadas.

Para cada una de estas métricas, el valor entre paréntesis junto a cada porcentaje es el cambio porcentual en la adopción desde la última vez que ejecutó la BPA en el archivo de configuración del dispositivo (o **No change [Ningún cambio]** si el valor es el mismo que la última vez que ejecutó la BPA).



Resumen de descifrado: Muestra si la configuración incluye reglas de política de descifrado para SSL Forward Proxy, SSL Inbound Inspection y SSH Proxy. El resumen también muestra si la configuración incluye perfiles de descifrado e identifica las categorías de URL que el dispositivo exime del descifrado.

Si no descifra una categoría de URL (o aplicaciones individuales), no puede inspeccionar su tráfico porque el cortafuegos no puede ver qué hay dentro del tráfico cifrado. El cortafuegos solo puede inspeccionar el tráfico que usted descifre.

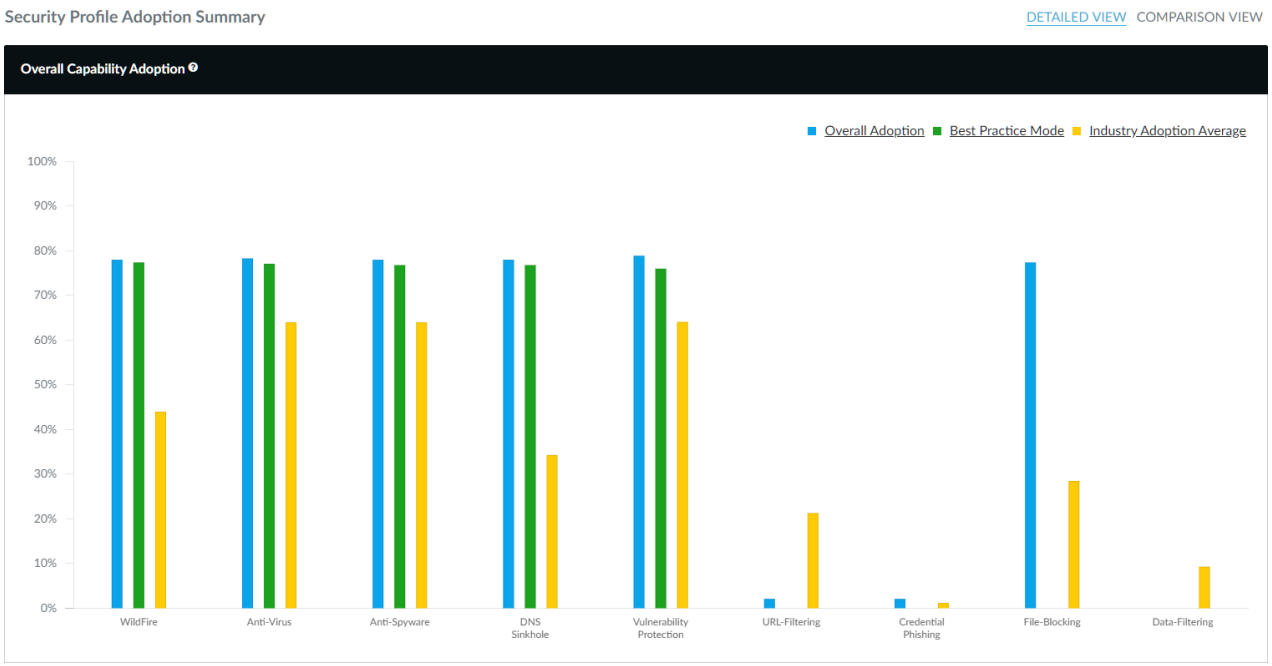
Siguiente: Identificar brechas en la adopción para entender donde se puede mejorar la seguridad.

Identificar brechas en la adopción

Las opciones de Mapa de calor de adopción muestran dónde está fuerte su política de seguridad y dónde hay brechas en la adopción de la capacidad de la política de seguridad en las que puede concentrarse en mejorar. Para obtener la máxima visibilidad del tráfico y la máxima protección contra ataques, establezca objetivos para la adopción de la capacidad de seguridad y utilice las siguientes recomendaciones como una línea base de prácticas recomendadas. Evalúe su posición actual con respecto a la línea base para identificar las brechas en la adopción de la capacidad de la política de seguridad.

Los Mapas de calor de adopción ayudan a identificar dispositivos, zonas y áreas donde puede mejorar la adopción de la capacidad de la política de seguridad. Puede revisar la información de adopción por grupo de dispositivos, número de serie y Vsys, zonas, áreas de arquitectura, etiquetas, detalles de reglas y asignaciones de zonas. Los **Local Filters (Filtros locales)** filtran por grupo de dispositivos, área de arquitectura de origen, área de arquitectura de destino, destino, zona de origen, zona de destino y etiquetas para reducir el alcance e identificar brechas. A continuación, se muestra el mapa de calor de adopción por área de arquitectura [**Adoption Heatmap (Mapa de calor de adopción)** > **Areas of Architecture (Áreas de arquitectura)**]:

En **Adoption Heatmap (Mapa de calor de adopción)** > **Summary (Resumen)**, haga clic en Adoption Summary (Resumen de adopción) para marcar las tasas de adopción de las siguientes capacidades. Use las recomendaciones como criterios de identificación de brechas; si la tasa de adopción real no coincide con las recomendaciones, planifique cerrar la brecha:



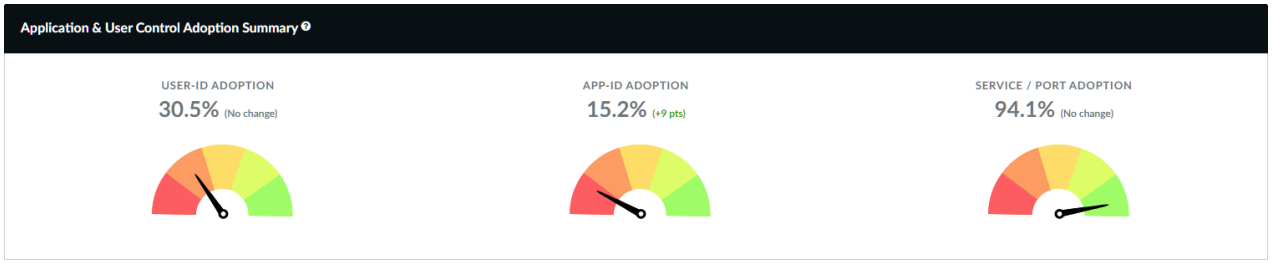
- Aplique los perfiles de seguridad de WildFire, antivirus, antispyware, protección frente a vulnerabilidades y bloqueo de archivos a todas las reglas que permiten el tráfico, con un objetivo de 100% o casi 100% de adopción. Si no aplica un perfil a una regla para permitir, asegúrese de que haya una buena razón comercial para no aplicarlo.

  La configuración de perfiles de seguridad en todas las reglas de permitir habilita que el cortafuegos inspeccione el tráfico descifrado en busca de amenazas, independientemente de la aplicación o el servicio/puerto. Después de actualizar la configuración, ejecute la BPA para medir el progreso y detectar nuevas reglas que no tengan perfiles de seguridad adjuntos.

  Puede aplicar los perfiles de WildFire a las reglas sin una licencia de WildFire. La cobertura se limita a los archivos PE, pero esto todavía proporciona una visibilidad útil de los archivos maliciosos desconocidos.

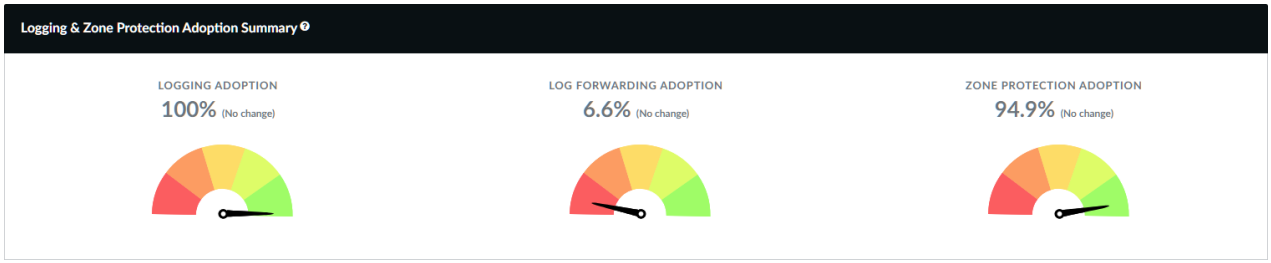
- En el perfil Antispyware, aplique DNS Sinkhole a todas las reglas para evitar que los hosts internos comprometidos envíen consultas de DNS para dominios maliciosos y personalizados, para identificar y rastrear los hosts potencialmente en peligro y para evitar brechas en la inspección de DNS. La habilitación de DNS Sinkhole protege su red sin afectar la disponibilidad, por lo que puede y debe habilitarla de inmediato.
- Aplique el filtrado de URL y la protección contra robo de credenciales (phishing) a todo el tráfico de internet saliente.

En el Resumen de adopción del control de usuario y aplicación del Resumen de adopción, compruebe las tasas de adopción de las siguientes capacidades. Use las recomendaciones como criterios de identificación de brechas; si la tasa de adopción real no coincide con las recomendaciones, planifique cerrar la brecha:



- Aplique App-ID al 100% o a la mayor cantidad posible de reglas. Aplique User-ID a todas las reglas con zonas de origen o rangos de direcciones que tengan presencia del usuario (es posible que algunas zonas no tengan orígenes de usuarios; por ejemplo, las fuentes en las zonas del centro de datos deberían ser servidores y no usuarios). Aproveche App-ID y User-ID para crear políticas que permitan a los usuarios apropiados autorizar (y tolerar) aplicaciones. Bloquee explícitamente las aplicaciones maliciosas y no deseadas.
- Apunte al 100% o cerca del 100% de adopción del servicio/puerto: no permita aplicaciones en puertos no estándar a menos que haya una buena razón comercial para ello.

En el Resumen de adopción de generación de logs y protección de zonas del Resumen de adopción, compruebe las tasas de adopción de las siguientes capacidades. Use las recomendaciones como criterios de identificación de brechas; si la tasa de adopción real no coincide con las recomendaciones, planifique cerrar la brecha:



- Intente obtener el 100 % o cerca del 100 % de adopción para la generación y el reenvío de logs.
- Configure perfiles de protección de zona en todas las zonas.

En resumen:

Función	Objetivo de adopción
WildFire	Lo más cerca posible al 100% de las reglas de la política de seguridad
Antivirus	Lo más cerca posible al 100% de las reglas de la política de seguridad
Antispyware	Lo más cerca posible al 100% de las reglas de la política de seguridad
vulnerabilidad	Lo más cerca posible al 100% de las reglas de la política de seguridad
Bloqueo de archivos	Lo más cerca posible al 100% de las reglas de la política de seguridad
Filtrado de URL y robo de credenciales	Todo el tráfico saliente de internet
App-ID	Lo más cerca posible al 100% de las reglas de la política de seguridad

Función	Objetivo de adopción
User-ID	Todas las reglas con zonas de origen o rangos de direcciones que tienen presencia del usuario
Servicio/puerto	Lo más cerca posible al 100% de las reglas de la política de seguridad
de creación de logs	Lo más cerca posible al 100% de las reglas de la política de seguridad
Log Forwarding	Lo más cerca posible al 100% de las reglas de la política de seguridad
Protección de zona	Todas las zonas

Cuando se visualizan Mapas de calor de adopción, use **Local Filters (Filtros locales)** para limitar el alcance. Utilice la información resultante para identificar las brechas en la capacidad de la política de seguridad, comparar con los criterios de identificación de brechas y ajustar o establecer nuevos criterios de identificación de brechas para una mayor investigación. Por ejemplo, para crear un filtro que muestre la adopción de reglas que controlan el tráfico al área de arquitectura de internet:

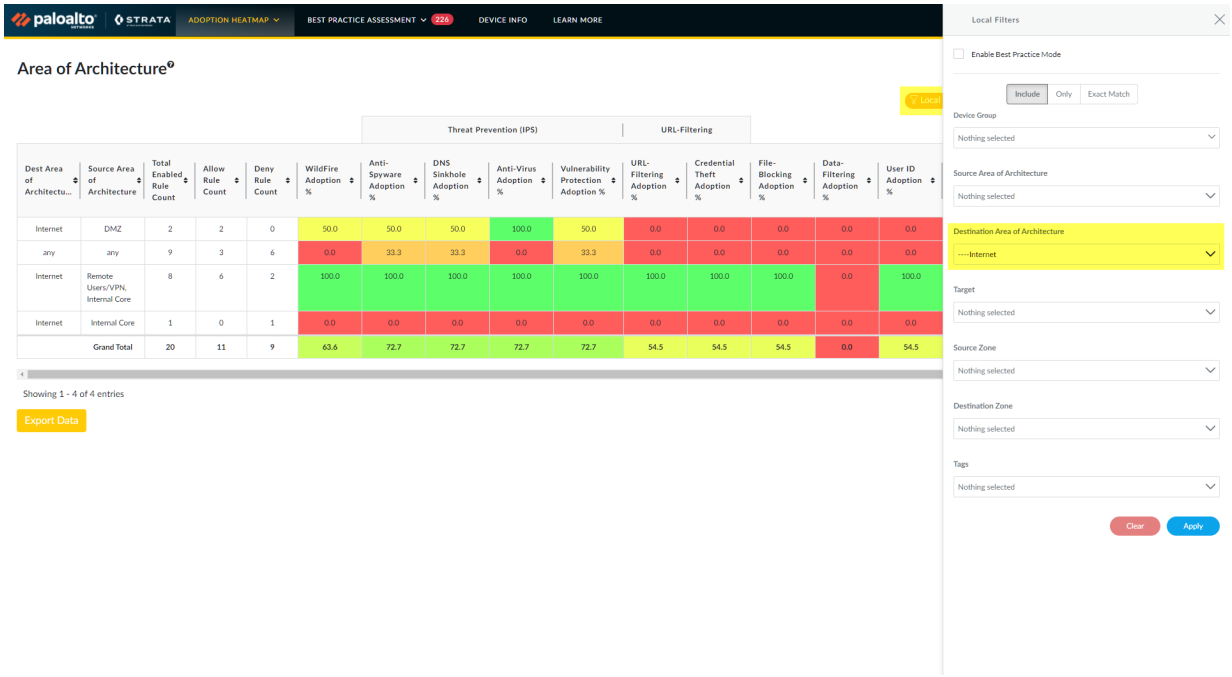
STEP 1 | Seleccione **Adoption Heatmap (Mapa de calor de adopción)** > **Areas of Architecture (Áreas de arquitectura)**.

STEP 2 | Haga clic en **Local Filters (Filtros locales)** para expandir las opciones de filtro.

STEP 3 | Establezca **Destination Area of Architecture (Área de destino de la arquitectura)** en **Internet**.

STEP 4 | Haga clic en **Apply (Aplicar)**.

La BPA filtra los resultados:



Interprete los resultados en función de sus objetivos y criterios de seguridad. Por ejemplo, si su objetivo es aplicar WildFire al 100% de sus reglas de permiso, el mapa de calor de adopción filtrado revela que solo el 50% de sus reglas de permiso de DMZ tienen perfiles de WildFire, por lo que ha identificado una brecha a la que se debe aplicar mejoras.

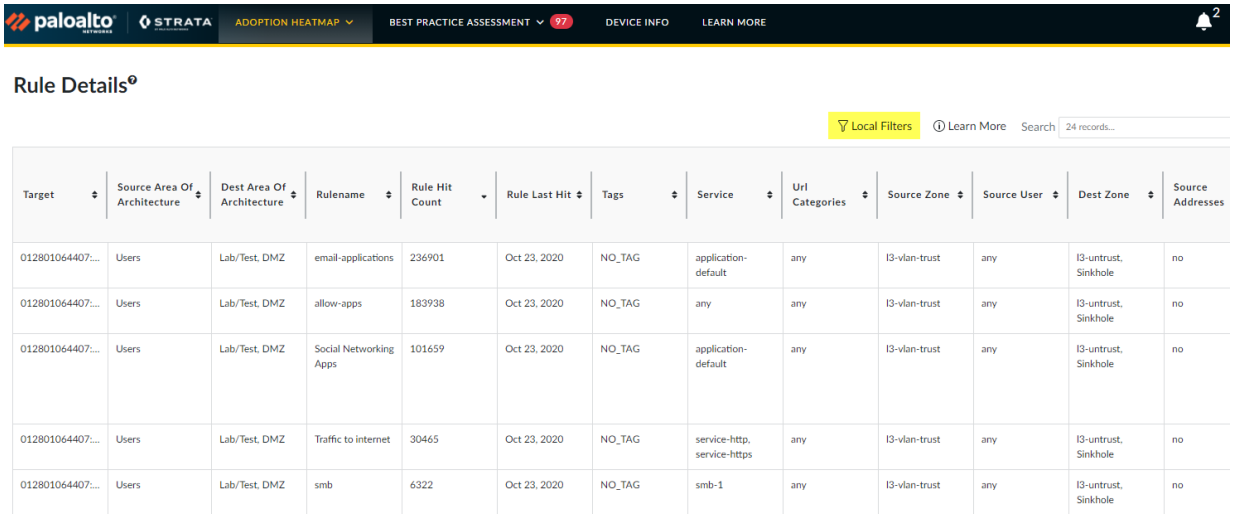
STEP 5 | Siguiente: Identificar reglas para mejorar.

Identificar reglas para mejorar

Después de identificar una brecha en la adopción de la capacidad de la política de seguridad, utilice la vista **Adoption Heatmap (Mapa del calor de adopción)** > **Rule Detail (Detalles de la regla)** para enumerar las reglas que requieren una mayor investigación o corrección. Configure los **Local Filters (Filtros locales)** para que coincida con los criterios de identificación de brechas que desarrolló cuando identificó brechas en la adopción. Esto da como resultado listas de reglas que puede exportar y entregar al equipo operativo a cargo de la política de seguridad del cortafuegos.

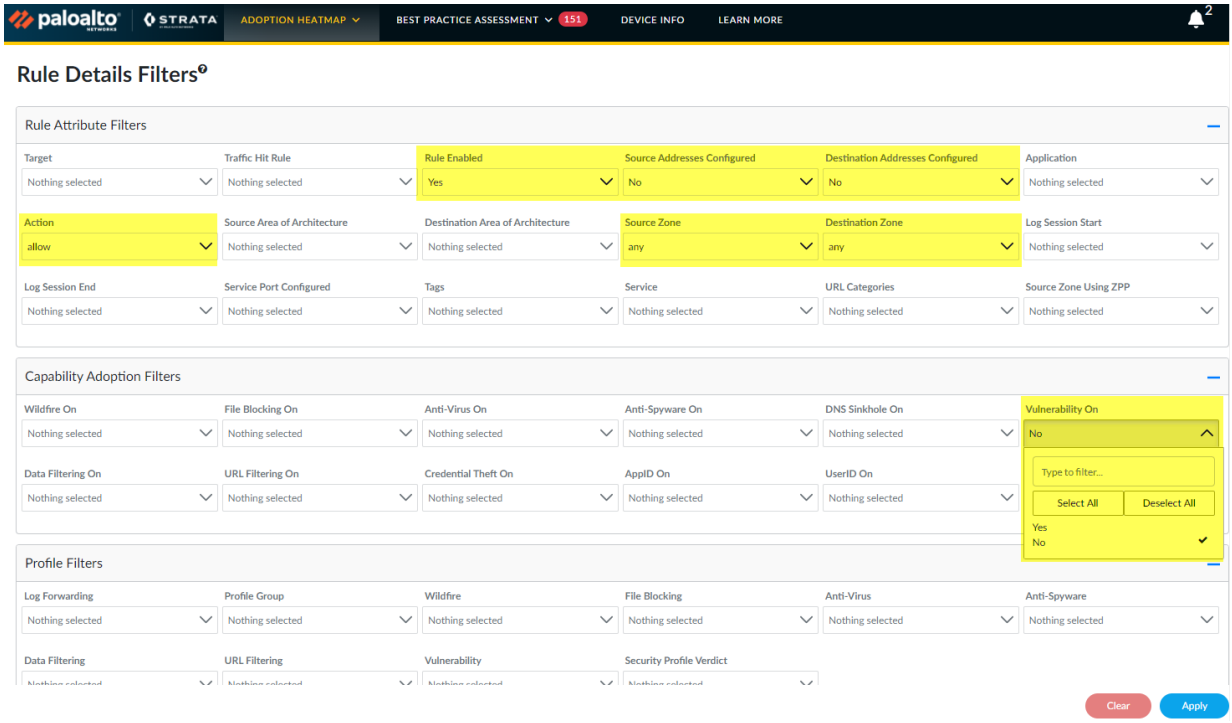
Por ejemplo, para crear un filtro de Detalle de Regla para identificar las reglas que permiten todo el tráfico y no tienen un perfil de Protección frente a vulnerabilidades configurado:

STEP 1 | En el menú del Mapa de calor de adopción, seleccione **Rule Detail (Detalle de la regla)** para ver la página Detalles de la regla.



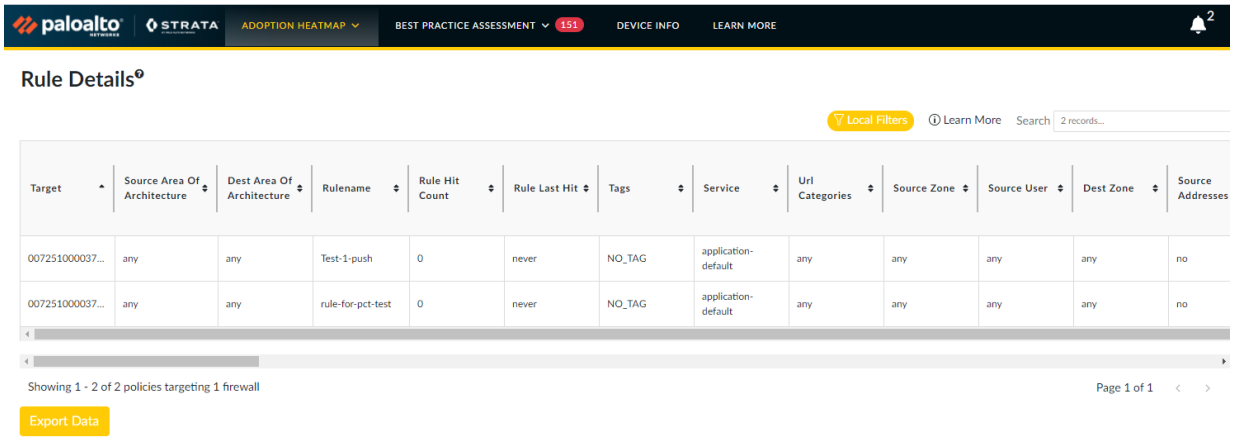
STEP 2 | Haga clic en **Local Filters (Filtros locales)** para ver las opciones de filtro y luego seleccione los siguientes filtros:

- Zona de origen = **any (cualquiera)**
- Zona de destino = **any (cualquiera)**
- Dirección de origen configurada = **No**
- Dirección de destino configurada = **No**
- Acción = **allow (permitir)**
- Regla habilitada = **Yes (Sí)**
- Vulnerabilidad habilitada = **No**



STEP 3 | Haga clic en **Apply Filter (Aplicar filtro)**.

La BPA enumera las reglas que coinciden con los filtros:



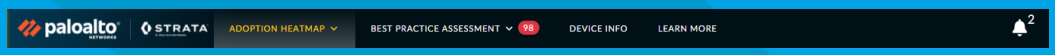
STEP 4 | Para exportar la lista de reglas filtrada a un archivo .csv, haga clic en **Export Data (Exportar datos)**.

STEP 5 | Siguiente: Evaluar la configuración de prácticas recomendadas.

Evaluar la configuración de prácticas recomendadas

La herramienta de evaluación de prácticas recomendadas (BPA) le ayuda a comprender el nivel actual de configuración de prácticas recomendadas en su política de seguridad para que pueda evaluar la madurez de su posición de seguridad. Vea el vídeo Introducción a BPA para obtener más información sobre BPA y aprovechar la Videoteca de BPA para aprender aún más sobre la herramienta.

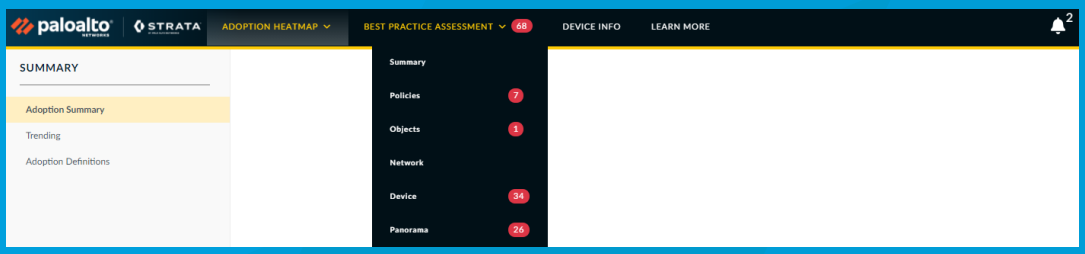
El informe BPA se abre primero en la página Mapa de calor de adopción. Haga clic en **Best Practice Assessment (Evaluación de prácticas recomendadas)** para ver la sección de BPA del informe, que se centra en la adopción de las prácticas recomendadas de configuración para los cortafuegos de nueva generación y Panorama.



Además de esta documentación, puede ver la Demostración de BPA y un breve vídeo sobre cómo ejecutar una BPA para aprender más sobre el uso del BPA.

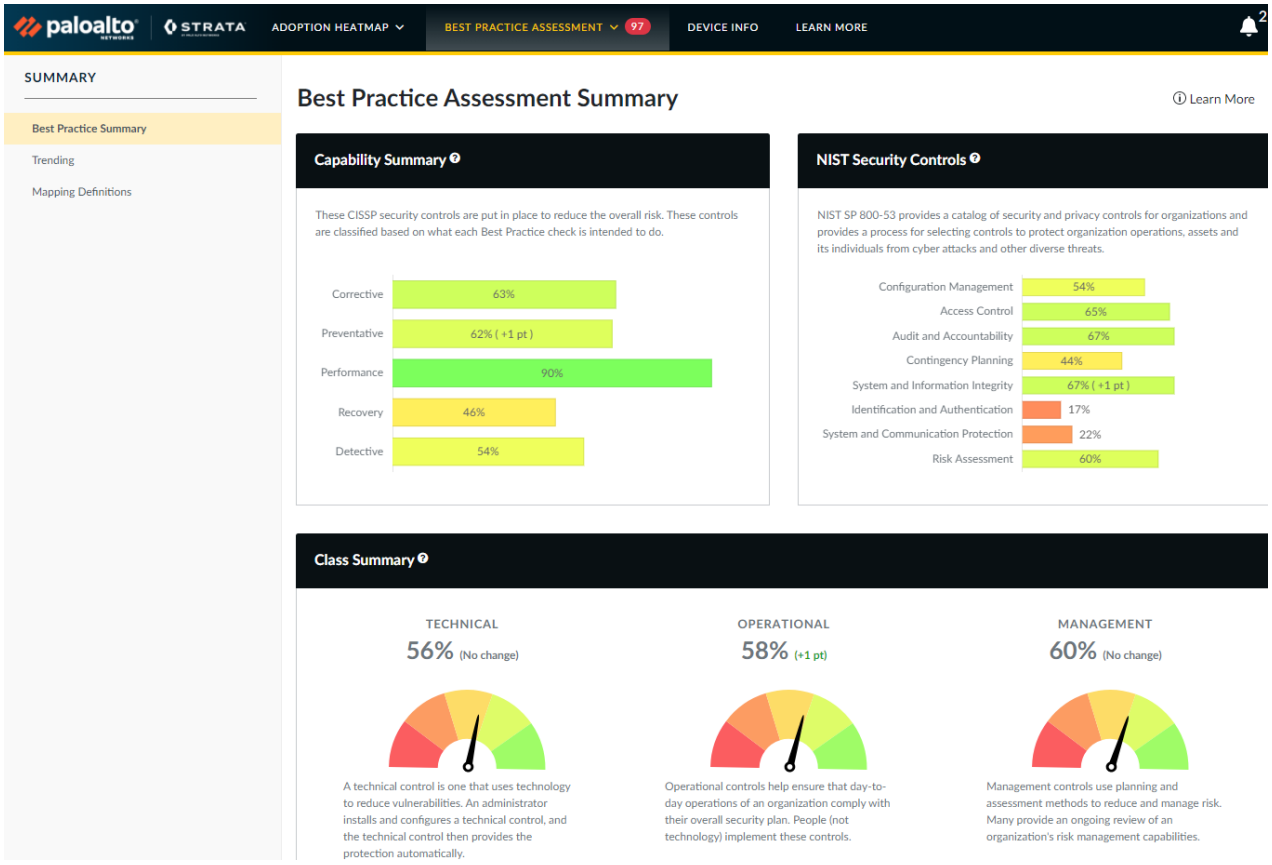
Un informe BPA evalúa un cortafuegos de última generación o un archivo de configuración de Panorama en comparación con más de 200 verificaciones de prácticas recomendadas. La BPA agrupa los resultados de la evaluación por políticas, objetos, red e información de dispositivo/Panorama, similar a la interfaz de usuario de PAN-OS. Revise y analice la información para encontrar áreas en la que centrarse y mejorar:

- Revisar el resumen de prácticas recomendadas
- Revisar la configuración de la política de prácticas recomendadas
- Revisar la configuración de objetos de prácticas recomendadas
- Revisar la configuración de red de prácticas recomendadas
- Revisar la configuración de dispositivos de prácticas recomendadas y gestión de panorama



Revisar el resumen de prácticas recomendadas

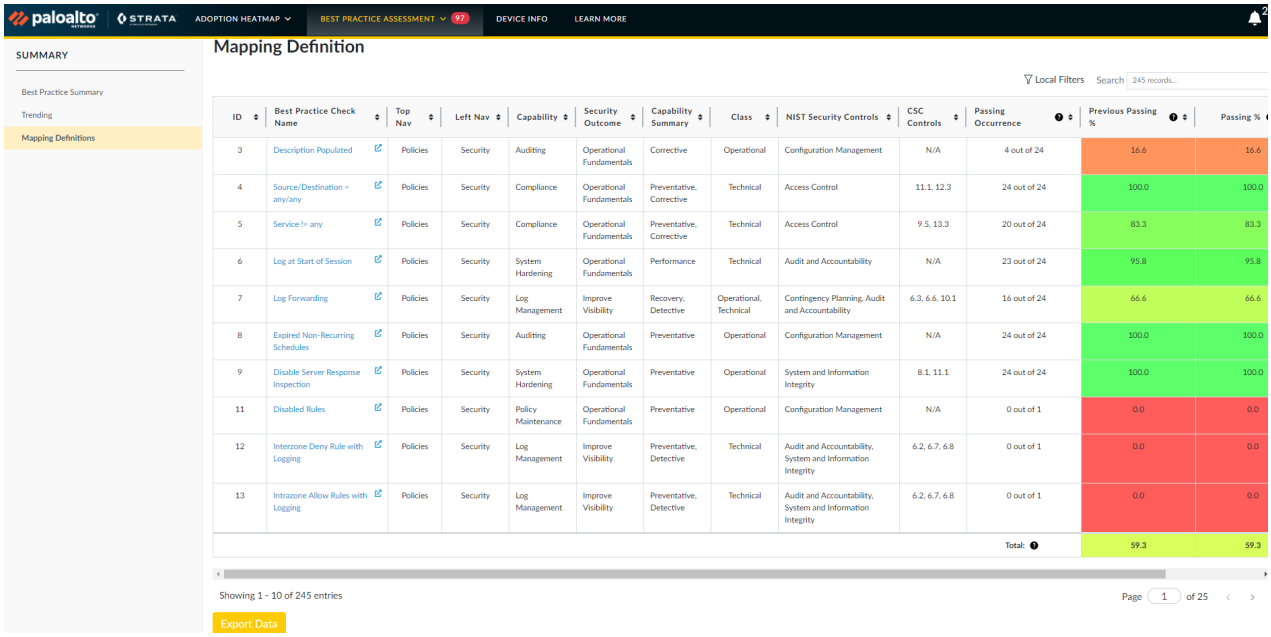
Seleccione **Summary (Resumen)** del menú **Best Practice Assessment (Evaluación de prácticas recomendadas)** para ver el Resumen de prácticas recomendadas.



El resumen presenta los resultados de la verificación de la configuración de prácticas recomendadas asignados a las categorías de control de los estándares de la industria, como por ejemplo los controles críticos de seguridad del Centro para la Seguridad de Internet (CIS) y la publicación del Instituto Nacional de Estándares y Tecnología (NIST) sobre controles de seguridad y procedimientos de evaluación. El propósito de esta información es proporcionar una buena manera de aprender cómo las comprobaciones de BPA están relacionadas con los estándares de la industria, no el de actuar como una auditoría.

Al igual que el Resumen de adopción, el Resumen de prácticas recomendadas incluye métricas que muestran su tasa de adopción actual y el progreso de la adopción (entre paréntesis) desde la última vez que generó la BPA en la configuración del dispositivo.

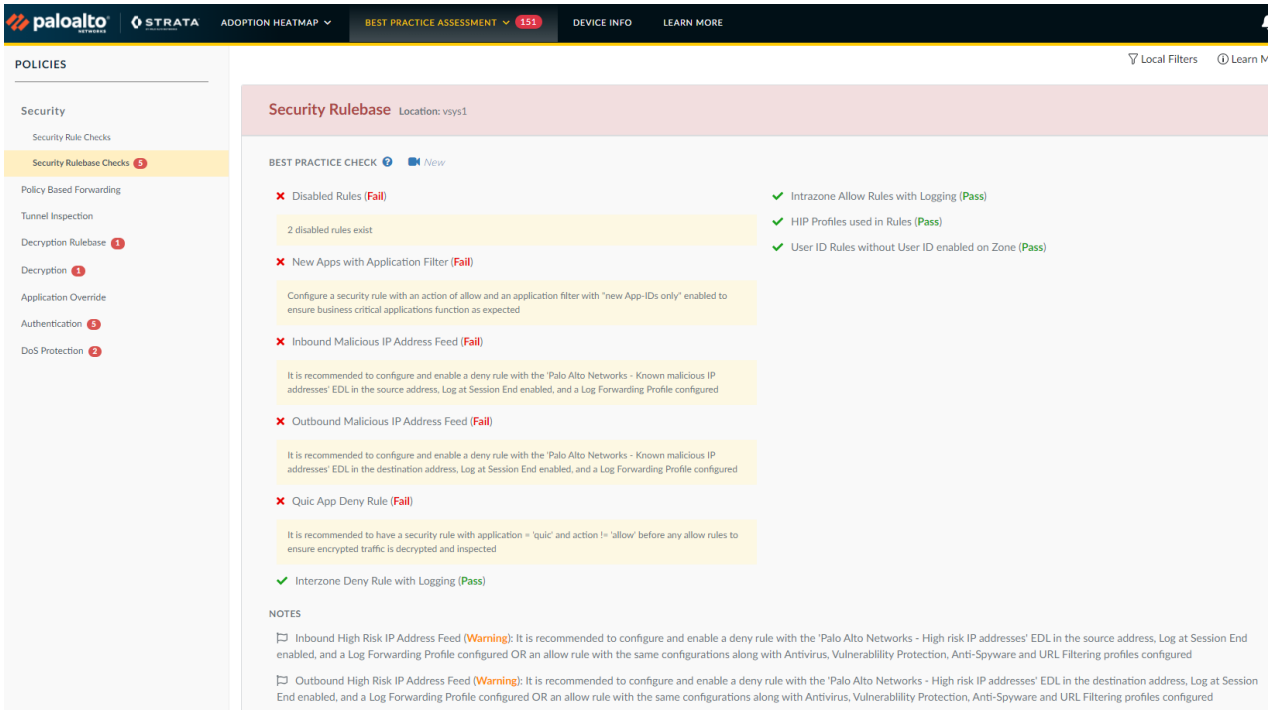
Haga clic en **Mapping Definitions (Definiciones de asignaciones)** (barra lateral izquierda) para ver una lista completa de todos las comprobaciones asignadas y sus puntuaciones individuales. **Show Filters (Mostrar filtros)** para establecer filtros, **Apply Filters (Aplicar filtros)** al resultado, y **Export Mappings (Exportar asignaciones)** para exportar las asignaciones a un archivo .csv.



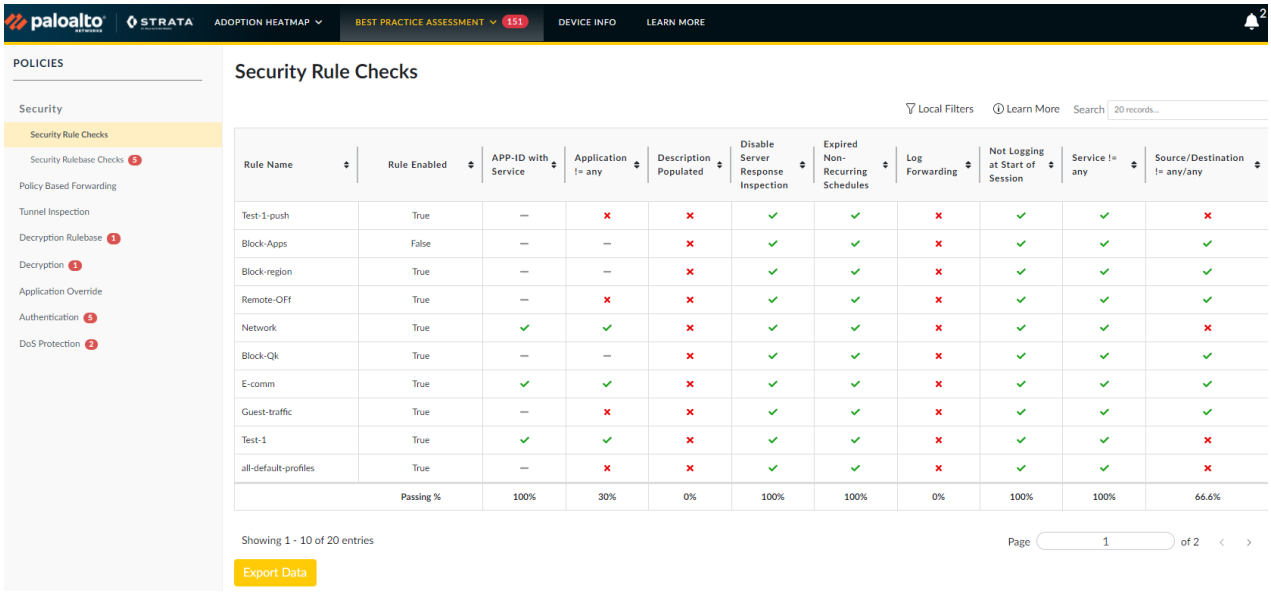
Siguiente: Revisar la configuración de la política de prácticas recomendadas.

Revisar la configuración de la política de prácticas recomendadas

Best Practice Assessment (Evaluación de prácticas recomendadas) > **Policies (Políticas)** muestra todas las comprobaciones relacionadas con los diferentes tipos de políticas de cortafuegos y comienza en la página **Security Rulebase checks (Comprobaciones de la base de reglas de seguridad)**. Las **Security Rulebase Checks (Comprobaciones de base de reglas de seguridad)** resumen los resultados de la verificación de prácticas recomendadas por grupo de dispositivos, con un estado de aprobado/suspenso y recomendaciones sobre qué hacer con las revisiones no aprobadas. Haga clic en la ayuda ( ) para ver la descripción y el razonamiento de cada resultado, junto con un enlace a la documentación técnica como referencia.



Seleccione el tipo de política que desea revisar del menú izquierdo para identificar posibles mejoras a la regla. Por ejemplo, **Security Rule Checks (Comprobaciones de reglas de seguridad)** muestra los resultados de las comprobaciones basadas en reglas. Haga clic en **Local Filters (Filtros locales)** para configurar filtros que limitan los resultados a las reglas que suspendieron una o más verificaciones particulares. Usted puede **Export Data (Exportar datos)** para exportar la lista a un archivo .csv para el análisis de corrección.



Cuando repase la información de **Policy (Política)**, como mínimo, revise los siguientes elementos para ayudar a comprender el alcance de la corrección de políticas (cambiar entre vistas):

- **Seguridad**: Identificar las reglas que no superan la comprobación **Source/Destination !=any/any (Origen/Destino ! = any/any)**.
- **Seguridad**: Identificar las reglas que no superan la comprobación **App-ID with Service (App-ID con servicio)**.
- **Seguridad**: Identificar las reglas de User-ID que no superan la comprobación **User-ID Rules without User ID enabled on Zone (Reglas de User-ID sin la habilitación de User-ID en la zona**.
- **Base de reglas de descifrado**: Comprobaciones de descifrado de SSH Proxy.
- **Descifrado**: Cada regla de política de descifrado debe tener un perfil de descifrado asociado.

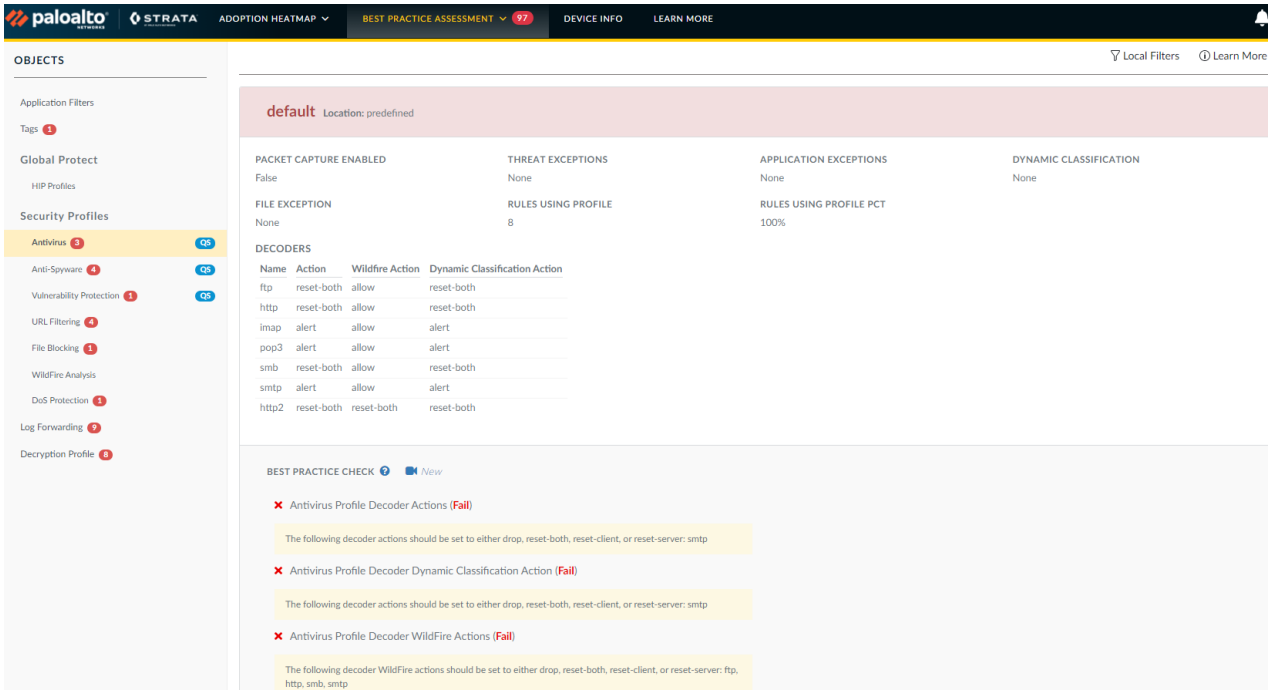
> *La excepción es el tráfico TLSv1.3 que elige no descifrar mediante la aplicación de una política de No descifrado al tráfico. Cuando adjunta un perfil de No descifrado a la política, el perfil verifica la información del certificado y bloquea las sesiones de descifrado que utilizan certificados incorrectos. Sin embargo, debido a que TLSv1.3 cifra la información del certificado, el cortafuegos no puede bloquear el tráfico no cifrado según la información del certificado, por lo que no tiene sentido adjuntar el perfil a la política.*

- **Anulación de la aplicación**: Las reglas de anulación de la aplicación que usan una inspección de nivel 7 de bypass de aplicación personaliza simple para el tráfico coincidente. Reduzca o elimine las reglas de anulación de aplicaciones que usan una aplicación personalizada simple para que pueda Mejorar la visibilidad del tráfico e inspeccionar las aplicaciones y contenidos que controlan estas reglas.

Siguiente: Revisar la configuración de objetos de prácticas recomendadas.

Revisar la configuración de objetos de prácticas recomendadas

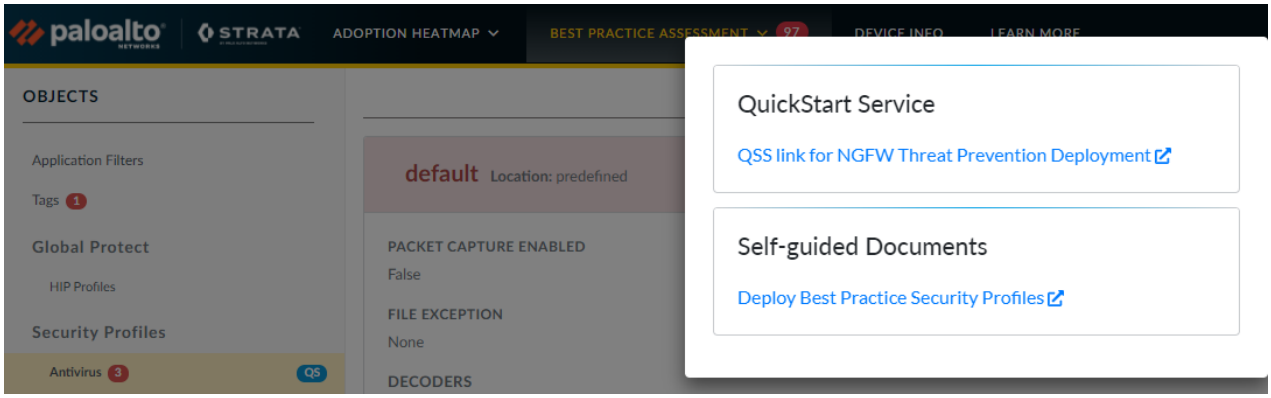
Best Practice Assessment (Evaluación de prácticas recomendadas) > **Objects (Objetos)** muestra todas las comprobaciones relacionadas con diferentes tipos de objetos de cortafuegos y comienza en la página **Application Filters (Filtros de aplicación)**. Seleccione el objeto que desea revisar para comprender la configuración existente e identificar brechas potenciales en la configuración de prácticas recomendadas relacionadas con filtro de aplicaciones, etiquetas, GlobalProtect, perfiles de seguridad, reenvío de logs y perfiles de descifrado. El siguiente ejemplo muestra el resultado cuando selecciona el objeto de perfil de seguridad de antivirus.



Para cada perfil de antivirus, el informe muestra la configuración actual y cuántas reglas utilizan el perfil. El informe muestra los resultados de la verificación de prácticas recomendadas debajo de la configuración actual con estado de aprobado/suspenso y recomendaciones para las verificaciones de prácticas recomendadas suspensas. Haga clic en la ayuda ( ) para conocer el razonamiento de cada verificación y los enlaces a la documentación de prácticas recomendadas.

Cuando una o más verificaciones suspenden, el título del perfil se torna rojo. El informe enumera los perfiles que no están en uso en la parte inferior con un título en amarillo.

El botón "QS" junto a algunos de los enlaces de la página de perfil, a la izquierda de la pantalla, le conecta a las opciones del Servicio QuickStart. El **QuickStart Service (Servicio QuickStart)** le ayuda a aumentar sus capacidades de seguridad e inversión al ayudarle a planificar y ejecutar su implementación de cortafuegos como plataforma. Los **Self-guided Documents (Documentos autoguiados)** le ayudan a comprender, crear e implementar el objeto.



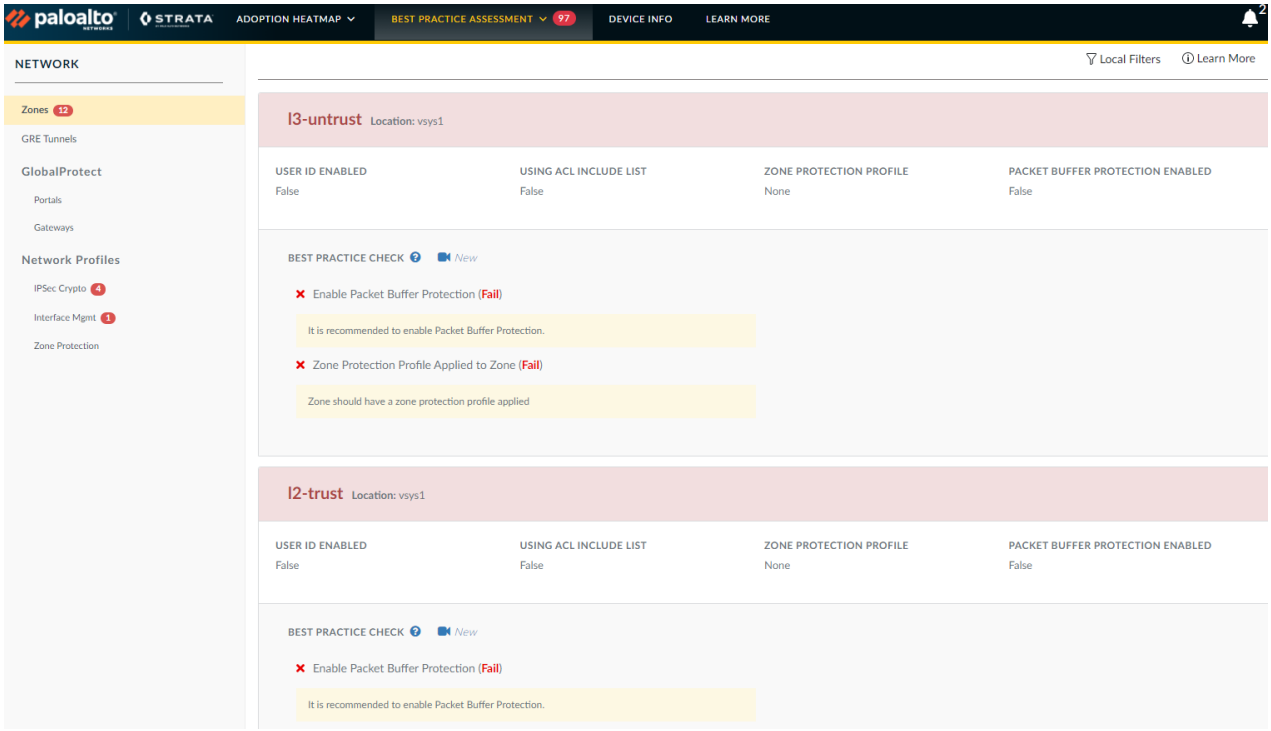
Cuando revise la pestaña **Objects (Objetos)**, como mínimo, revisa los siguientes elementos para poder comprender el alcance potencial de la corrección:

- **Antivirus**: Acciones de decodificadores tanto para antivirus como para WildFire.
- **Anti-Spyware**: Perfil estricto, Sinkhole DNS.
- **Protección frente a vulnerabilidades**: Perfil estricto.
- **Filtrado de URL**: Si las malas categorías conocidas están bloqueadas.
- **Análisis de WildFire**: Tipos de archivo de perfil (todos los tipos deben enviarse a WildFire para su análisis).
- **Reenvío de logs**: Si todos los tipos de logs se envían (enviar todos los tipos de logs).

Siguiente: Revisar la configuración de red de prácticas recomendadas.

Revisar la configuración de red de prácticas recomendadas

Best Practice Assessment (Evaluación de prácticas recomendadas) > **Network (Red)** muestra todas las comprobaciones de la configuración relacionada con la red y comienza en la página **Zones (Zonas)**. En la barra de navegación izquierda, seleccione la verificación de red que desea revisar para comprender la configuración existente e identificar posibles brechas en la configuración de prácticas recomendadas relacionadas con los perfiles de Zonas,Túneles GRE y con GlobalProtect, IPsec Crypto, gestión de la interfaz y los perfiles de protección de zonas. El siguiente ejemplo muestra el resultado para Zones.



El informe muestra la configuración actual de cada elemento. Los resultados de verificación de prácticas recomendadas para cada elemento aparecen debajo de su configuración actual. Puede especificar un **Device Group (Grupo de dispositivos)** o **Template (Plantilla)** para limitar el alcance de la información mostrada.

Cada verificación tiene el estado de aprobado/suspenso y recomendaciones para verificaciones de prácticas recomendadas fallidas. Haga clic en la ayuda ( ) para conocer el razonamiento de cada verificación y los enlaces a la documentación de prácticas recomendadas. Cuando una o más verificaciones fallan, el título del elemento se vuelve rojo.

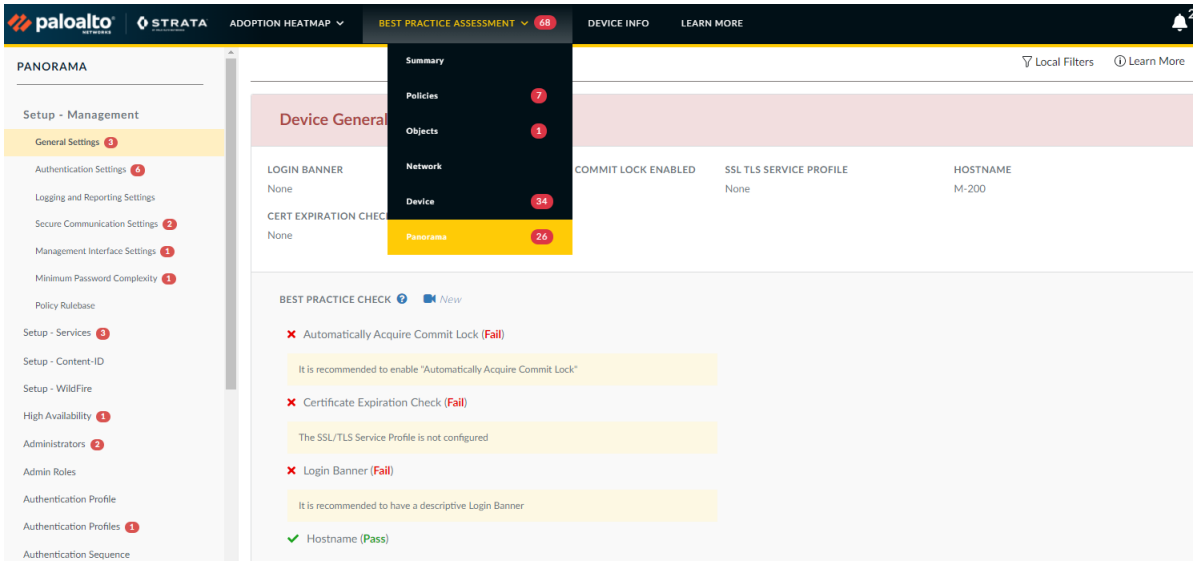
Cuando revise la pestaña **Network (Red)**, como mínimo, revise los siguientes elementos para ayudar a comprender el alcance potencial de la corrección:

- **Zonas**: Ya sea que cada zona tenga habilitada la Protección de búfer de paquetes y tenga un perfil de Protección de zonas.
- **Protección de zona**: si la Protección frente a inundaciones y la Protección de ataques basados en paquetes están habilitadas.

Siguiente: Revisar la configuración de dispositivos de prácticas recomendadas y gestión de panorama.

Revisar la configuración de dispositivos de prácticas recomendadas y gestión de panorama

Las páginas **Best Practice Assessment (Evaluación de prácticas recomendadas)** > **Device (Dispositivo)** y **Best Practice Assessment (Evaluación de prácticas recomendadas)** > **Panorama** muestran todas las comprobaciones relacionadas con la instalación y configuración de la gestión de dispositivos. En los cortafuegos independientes, **Best Practice Assessment (Evaluación de prácticas recomendadas)** > **Device (Dispositivo)** comienza en la página de Configuración general para la configuración de gestión del dispositivo del cortafuegos. En Panorama, **Best Practice Assessment (Evaluación de prácticas recomendadas)** > **Device (Dispositivo)** comienza en la página que muestra la configuración general de cada pila de plantillas. **Best Practice Assessment (Evaluación de prácticas recomendadas)** > **Panorama** comienza en la página Configuración general para la configuración de gestión del dispositivo. Seleccione la verificación que desea revisar para comprender la configuración existente e identificar posibles brechas en la configuración de prácticas recomendadas relacionadas con el cortafuegos y la gestión de dispositivos de Panorama. El siguiente ejemplo muestra el resultado de la Configuración general en un dispositivo Panorama.



El informe muestra la configuración actual de cada elemento. Los resultados de verificación de prácticas recomendadas para cada elemento aparecen debajo de su configuración actual. Al ver la información de un **Device (Dispositivo)**, puede especificar una **Template (Plantilla)** para limitar el alcance de la información mostrada.

Cada verificación tiene el estado de aprobado/suspenso y recomendaciones para verificaciones de prácticas recomendadas fallidas. Haga clic en la ayuda ( ) para conocer el razonamiento de cada verificación y los enlaces a la documentación de prácticas recomendadas. Cuando una o más verificaciones fallan, el título del elemento se vuelve rojo.

Cuando revise las pestañas **Device (Dispositivo)** or **Panorama**, como mínimo, revise los siguientes elementos para ayudar a comprender el alcance potencial de la corrección:

- **Dynamic Updates (Actualizaciones dinámicas)**: Actualizaciones de antivirus, aplicaciones, amenazas y WildFire.
- **Management Interface Settings (Configuración de la interfaz de gestión)**: Servicios de conectividad de red, direcciones IP permitidas.

- **Administrators (Administradores)**: Administradores locales, perfil de contraseña del administrador. Compruebe **Device (Dispositivo)** > **Administrators (Administradores)** o **Panorama** > **Administrators (Administradores)** para asegurarse de que las contraseñas de los Administradores estén configuradas con la complejidad mínima requerida.
- **Minimum Password Complexity (Complejidad de contraseña mínima)**: Verificación de requisitos de complejidad mínimos para la contraseña.

Siguiente: Priorizar los cambios en las prácticas recomendadas.

Priorizar los cambios en las prácticas recomendadas

La cantidad de información en un informe BPA puede ser abrumadora. Este capítulo proporciona recomendaciones para ayudarle a priorizar la mejora de su configuración para que pueda cerrar las brechas de seguridad, implementar primero las mejoras de mayor valor y avanzar hacia la obtención de una posición de seguridad de prácticas recomendadas.

Los siguientes temas se centran en cómo mejorar su posición de seguridad en el orden en que generalmente se implementan las nuevas implementaciones, centrándose primero en la administración, luego en la visibilidad, el control y la aplicación. Las implementaciones existentes ya pueden haber alcanzado cierta madurez en cada área.

> Fortalecer la posición de la gestión de dispositivos
> Mejorar la visibilidad del tráfico
> Implementar controles de prácticas recomendadas iniciales
> Ajustar y mejorar los controles de prácticas recomendadas

Fortalecer la posición de la gestión de dispositivos

El fortalecimiento de la posición de administración de dispositivos protege el cortafuegos al evitar el acceso no autorizado que podría comprometerlo, reduce el impacto operacional de eventos inesperados y proporciona una mayor visibilidad del funcionamiento del cortafuegos.

- Siga las prácticas recomendadas para proteger el acceso administrativo. para evitar el acceso no autorizado y no seguro a la interfaz de administración del dispositivo.
- Envíe todos los registros de sistema y configuración a Panorama y a las soluciones de control de terceros para mantener un seguimiento de los eventos relacionados con el sistema y los cambios de configuración.
- Cree una programación de copia de seguridad de configuración para que pueda solucionar los problemas relacionados con la configuración y las interrupciones del sistema de forma más eficiente.

Después de configurar los cambios, Ejecute la BPA para validar los cambios, medir el progreso y priorizar los próximos cambios.

Siguiente: Mejorar la visibilidad del tráfico.

Mejorar la visibilidad del tráfico

No puede protegerse contra amenazas que no puede ver, por lo que debe asegurarse de tener una visibilidad completa del tráfico en todos los usuarios y aplicaciones en todo momento. La visibilidad completa de las aplicaciones, el contenido y los usuarios de la red es el primer paso hacia un control de política informado:

- Maximizar la adopción del perfil de seguridad. Después de Revisar el resumen de adopción e identifique brechas en la adopción, corrija las brechas utilizando los pasos de transición segura para avanzar hacia una implementación de perfiles de seguridad de prácticas recomendadas.
- Maximizar la adopción de generación de logs (incluido el Reenvío de logs) a través de la base de reglas de política de seguridad para inspeccionar *todo* el tráfico.
- Configure las prácticas recomendadas para las actualizaciones de contenido dinámico para garantizar que el cortafuegos tenga la aplicación más reciente y firmas de amenazas para proteger su red y que implemente actualizaciones basadas en los requisitos de seguridad y disponibilidad de su red.
- Planifique su implementación de descifrado SSL basada en las prácticas recomendadas.
- Habilite User-ID en las zonas de usuario (zonas internas y de confianza desde donde los usuarios inician el tráfico) para asignar el tráfico de la aplicación y las amenazas asociadas a los usuarios y dispositivos.

  No habilite User-ID en zonas externas no fiables. Si habilita User-ID (o el sondeo de clientes como WMI) en una zona externa no fiable, las sondas podrían enviarse fuera de su red protegida y exponer la información de User-ID como el nombre de la cuenta de servicio del Agente User-ID, el nombre de dominio y hash de contraseña cifrado; lo que podría permitir a un atacante obtener acceso no autorizado a recursos protegidos.
- Reduzca o elimine las reglas de Cancelación de aplicaciones para que pueda inspeccionar las aplicaciones y el contenido que controlan estas reglas (una regla de Anulación de aplicaciones es una regla de capa 4 que no permite que el cortafuegos inspeccione el tráfico). Elimine la necesidad o reduzca el alcance de las reglas básicas de la Anulación de la aplicación:
  - Valide si el caso de uso para la regla todavía existe. A menudo, se creaba una regla de Anulación de la aplicación para superar un problema específico relacionado con el rendimiento, los decodificadores de protocolo o aplicaciones desconocidas. Con el tiempo, las actualizaciones de PAN-OS, las actualizaciones de contenido o las actualizaciones de hardware pueden eliminar la necesidad de algunas reglas de Anulación de la aplicación. Si ejecuta PAN-OS 9.0 o posterior en cortafuegos o PAN-OS 9.0 o posterior en cortafuegos gestionados por Panorama que ejecuta PAN-OS 8.1 (o posterior), puede usar Policy Optimizer para transformar la regla en una regla de capa 7.
  - Reduzca el alcance de la regla de cancelación de la aplicación para que solo afecte la cantidad mínima de tráfico posible. Las reglas que se definen demasiado ampliamente pueden cancelar más tráfico del necesario o previsto. Defina las zonas de origen y destino, la dirección y/o los puertos en cada regla de cancelación de la aplicación para limitar el alcance de la regla tanto como sea posible.
  - Cree aplicaciones personalizadas de capa 7 para aplicaciones internas.
  - Cree objetos de servicio con valores de tiempo de espera personalizados.
- Planifique la implementación de DoS y protección de zona, y tome medidas de CPS de línea de base para que pueda establecer umbrales razonables de protección contra inundaciones.

Al implementar estas capacidades nativas de App-ID, Content-ID, User-ID y descifrado de SSL, el cortafuegos obtiene visibilidad y puede inspeccionar todo su tráfico (aplicaciones, amenazas y contenido) y vincular eventos con el usuario, independientemente de ubicación, tipo de dispositivo, puerto, cifrado o técnicas evasivas de un atacante.

La mejora de la adopción de capacidades, como el descifrado SSL, la generación de logs, la protección contra inundaciones, los perfiles de seguridad, etc., puede resultar en un consumo adicional de recursos del cortafuegos. Comprenda la capacidad de sus

cortafuegos y asegúrese de que tengan el tamaño adecuado para gestionar cualquier carga adicional. Su SE de Palo Alto Networks o CE puede ayudarle a dimensionar la implementación. También es posible que necesite espacio de almacenamiento de logs adicional.

Después de configurar los cambios, Ejecute la BPA para validar los cambios, medir el progreso y priorizar los próximos cambios.

Siguiente: Implementar controles de prácticas recomendadas iniciales.

Implementar controles de prácticas recomendadas iniciales

Después de obtener visibilidad y contexto acerca del tráfico en su red (aplicaciones, contenido, amenazas y usuarios), implemente controles estrictos para reducir la superficie de ataque y evitar amenazas conocidas y desconocidas para completar la transición a una configuración de prácticas recomendadas.

- Después de Revisar el resumen de adopción y identificar brechas en la adopción, siga los pasos de transición seguros para ir a los perfiles de seguridad de prácticas recomendadas para bloquear amenazas y reducir la superficie de ataque, incluida la implementación de controles estrictos en el centro de datos para proteger los activos más valiosos de su negocio.
- Cree reglas de política de seguridad basadas en aplicaciones para centro de datos y cortafuegos de perímetro; use las recomendaciones de prácticas recomendadas de cortafuegos de perímetro para otros cortafuegos que no están en el centro de datos. Si ejecuta PAN-OS 9.0 o posterior en cortafuegos o PAN-OS 9.0 o posterior en un cortafuegos que gestiona Panorama que se ejecuta en PAN-OS 8.1 (o posterior), puede usar Policy Optimizer para convertir reglas basadas en puertos a reglas basadas en aplicaciones.
- Cree políticas de acceso basadas en usuarios..
- Implemente perfiles de protección de zonas de prácticas recomendadas en todas las zonas.
- Implemente descifrado SSL para que el cortafuegos puede obtener más visibilidad (descifrar) e inspeccionar el tráfico cifrado.

Después de implementar las capacidades de control, el cortafuegos puede analizar todo el tráfico permitido, y detectar y bloquear las vulnerabilidades de seguridad en el nivel de la aplicación, los desbordamientos de búfer, los ataques DoS, las exploraciones de puertos y las variantes de malware conocidas y desconocidas. El cortafuegos controla la aplicación y el acceso de los usuarios, así como el bloqueo de aplicaciones maliciosas y no deseadas.

Después de configurar los cambios, Ejecute la BPA para validar los cambios, medir el progreso y priorizar los próximos cambios.

Siguiente: Ajustar y mejorar los controles de prácticas recomendadas.

Ajustar y mejorar los controles de prácticas recomendadas

Después de que implemente el control sobre el tráfico de su red (aplicaciones, contenido, amenazas y usuarios), comience a ajustar los controles e implemente funcionalidades adicionales para mejorar su postura de seguridad.

- Si no ha convertido las aplicaciones internas en aplicaciones personalizadas para obtener visibilidad y control del tráfico, convierta las aplicaciones internas a aplicaciones personalizadas.
- Cambie los perfiles de seguridad a las prácticas recomendadas después de los pasos de transición seguros para comenzar la transición a perfiles de prácticas recomendadas.
- Bloquee direcciones IP maliciosas conocidas basado en inteligencia de amenazas de Palo Alto Networks y fuentes de terceros de buena reputación.
- Implemente GlobalProtect o el Servicio en la nube de GlobalProtect para ampliar la plataforma de seguridad de última generación a usuarios y dispositivos, independientemente de su ubicación.
- Habilite la prevención de robo de credenciales.
- Configure la Autenticación multifactor basada en red.

Siguiente: Ejecute la BPA para validar cambios, medir el progreso y priorizar los próximos cambios, obtenga más información sobre prácticas recomendadas y aprenda más sobre las múltiples capacidades de seguridad de Panorama y los cortafuegos de última generación de PAN-OS..