

Introducción a la BPA

9.1

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

Palo Alto Networks, Inc.

www.paloaltonetworks.com

© 2019-2019 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

December 18, 2019

Table of Contents

Evaluar la adopción de la capacidad de la política de seguridad.....	5
Revisar el resumen de adopción.....	7
Identificar brechas en la adopción.....	9
Identificar reglas para mejorar.....	13
 Evaluar la configuración de prácticas recomendadas.....	 15
Revisar el resumen de prácticas recomendadas.....	17
Revisar la configuración de la política de prácticas recomendadas.....	19
Revisar la configuración de objetos de prácticas recomendadas.....	21
Revisar la configuración de red de prácticas recomendadas.....	22
Revisar la configuración de dispositivos de prácticas recomendadas y gestión de panorama.....	23
 Priorizar los cambios en las prácticas recomendadas.....	 25
Fortalecer la posición de la gestión de dispositivos.....	27
Mejorar la visibilidad del tráfico.....	28
Implementar controles de prácticas recomendadas iniciales.....	30
Ajustar y mejorar los controles de prácticas recomendadas.....	31

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

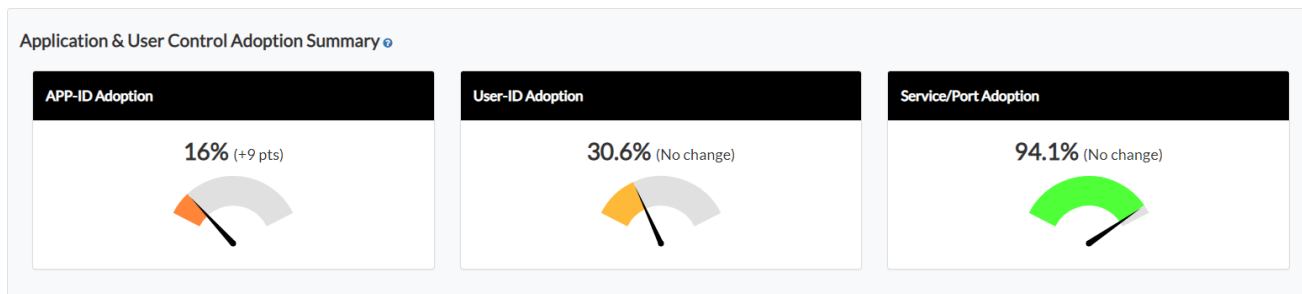
Después de que usted o su representante de Palo Alto Networks [ejecute la BPA](#), el informe HTML resultante se abre en la página Heatmap, en el resumen de adopción. La vista Resumen de adopción proporciona una descripción general de la adopción general de las capacidades de seguridad de su dispositivo. 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 para compararlos con su adopción), 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.

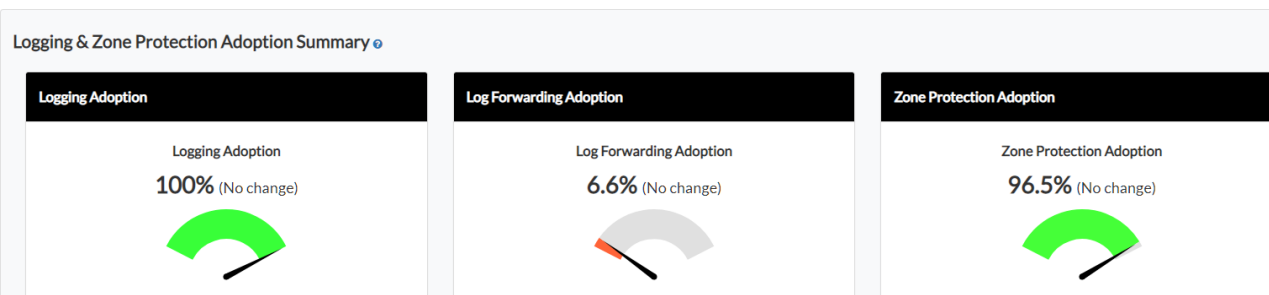
Adopción de User-ID: La adopción de User-ID en todas las reglas de la política de seguridad. El valor porcentual se basa en el número total de reglas de permiso con los usuarios (incluidos los valores **known-**

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.

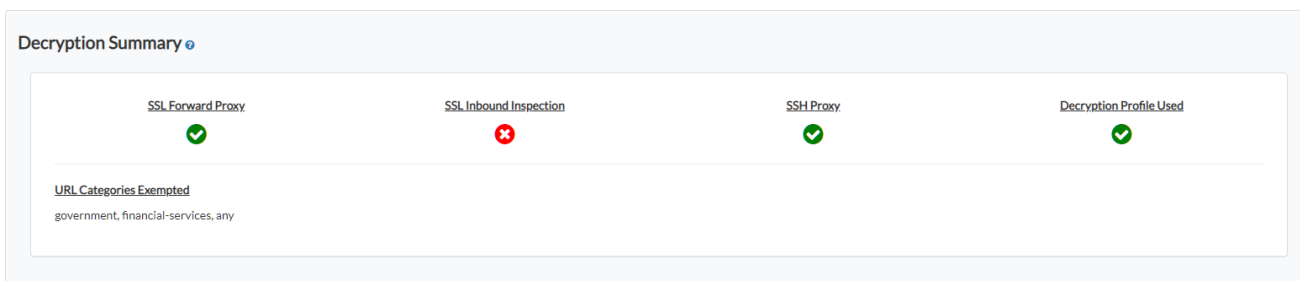


Adopción de generación de logs: La adopción de **Log at Session End (Log al finalizar sesión)** en todas las reglas de la política de seguridad. El valor porcentual se basa en el número total de reglas con **Log at Session End (Log al finalizar sesión)** habilitado. La BPA no cuenta las reglas deshabilitadas.

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, 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

El mapa de calor muestra 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 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 y etiquetas. Los **Column Filters (Filtros de columna)** filtran los grupos de dispositivos, los dispositivos, las zonas, las áreas de la arquitectura y las etiquetas para reducir el alcance e identificar las brechas.

paloalto

Trending

Device Group

Serial Number & Vsys

Zones

Area of Architecture

Tags

Rule Detail

Zone Mappings

Go to Best Practice Assessment

Security Policy Capability Adoption Heatmaps

Help

Column Filters

Source Area of Architecture	Destination Area of Architecture	Total Rule Count	Allow Rule Count	Deny Rule Count	WildFire					Threat Prevention (IPS)					URL Filtering			User ID Adoption %	App ID Adoption %	Service / Port Adoption %	Logging Adoption %	Log Forwarding %	Zone Protection Profile Adoption %	
					WildFire Adoption %	Anti-Spyware Adoption %	DNS Sinkhole Adoption %	Anti-Virus Adoption %	Vulnerability Protection Adoption %	URL Filtering Adoption %	Credential Theft Adoption %	File Blocking Adoption %	Data Filtering Adoption %											
Internal Core	Datacenter	314	314	0	79.6	79.6	79.6	79.6	79.6	0.0	0.0	79.6	0.0	0.0	0.0	30.6	9.6	94.6	100.0	0.0	100.0			
any	any	9	3	6	0.0	33.3	33.3	0.0	33.3	0.0	0.0	0.0	0.0	0.0	0.0	33.3	66.7	100.0	77.8	0.0				
Remote Users/VPN, Internal Core	Internet	8	6	2	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0			
Internet	DMZ	3	3	0	66.7	0.0	0.0	66.7	100.0	0.0	0.0	33.3	0.0	0.0	0.0	100.0	100.0	100.0	100.0	66.7	100.0			
Out-of-Band Management, Users, Remote Office/MPLS, Internal Core	IT Infrastructure	3	3	0	66.7	100.0	100.0	66.7	100.0	0.0	0.0	66.7	0.0	0.0	0.0	100.0	100.0	100.0	100.0	66.7	100.0			
DMZ	Datacenter	2	2	0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0	100.0	100.0	100.0	0.0	0.0			
DMZ	Internet	2	2	0	50.0	50.0	50.0	100.0	50.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0	100.0	100.0	100.0	100.0	0.0			
Undefined	Undefined	2	2	0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	50.0	100.0	100.0	100.0	0.0	50.0			
Web-tier	App-tier	1	1	0	100.0	100.0	100.0	100.0	100.0	0.0	0.0	100.0	0.0	0.0	0.0	100.0	100.0	100.0	100.0	0.0	0.0			
App-tier	DB-tier	1	1	0	100.0	100.0	100.0	100.0	100.0	0.0	0.0	100.0	0.0	0.0	0.0	100.0	100.0	100.0	100.0	0.0	0.0			
Remote Users/VPN, Internal Core	DMZ	1	1	0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0			
Remote Office/MPLS	Internal Core	1	1	0	100.0	100.0	100.0	100.0	100.0	0.0	0.0	100.0	0.0	0.0	0.0	0.0	0.0	100.0	0.0	0.0				
Internal Core	Internet	1	0	1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0	0.0	0.0	100.0	100.0	0.0			
Remote Office/MPLS	PCI	1	1	0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0	100.0	0.0	0.0			
Internal Core	Remote Office/MPLS	1	1	0	100.0	100.0	100.0	100.0	100.0	0.0	0.0	100.0	0.0	0.0	0.0	0.0	0.0	100.0	0.0	0.0	100.0			
Grand Total:		350	341	9	78.0	78.0	78.0	78.3	78.9	2.1	2.1	77.4	0.0	0.0	2.1	2.1	77.4	0.0	30.6	16.0	94.1	100.0	6.6	96.5

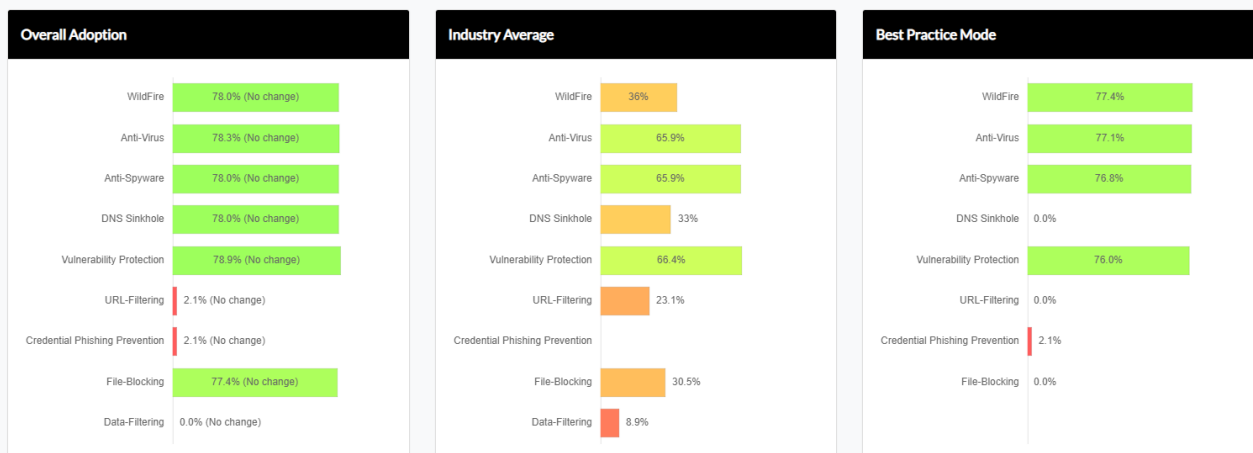
Showing 1 to 15 of 15 entries

Export Data

Previous1Next

En el [Resumen de adopción](#) del perfil de seguridad del mapa de calor, verifique las tasas de adopción de las siguientes capacidades y utilice las recomendaciones como criterios de identificación de brecha; si la tasa de adopción real no coincide con las recomendaciones, planifique cerrar la brecha.

Security Profile Adoption Summary



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

La configuración de perfiles de seguridad en todas las reglas de permiso permite que el cortafuegos inspeccione todo 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.

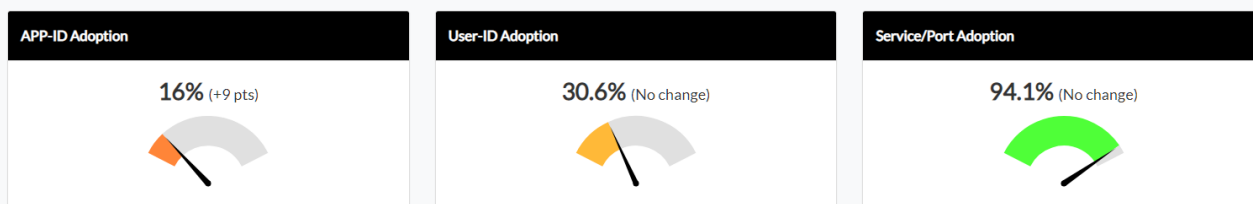


Puede aplicar los perfiles de WildFire a las reglas sin una licencia de WildFire. La cobertura se limita a los archivos PE, pero esto todavía proporciona una visibilidad útil de los archivos maliciosos desconocidos.

- 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.

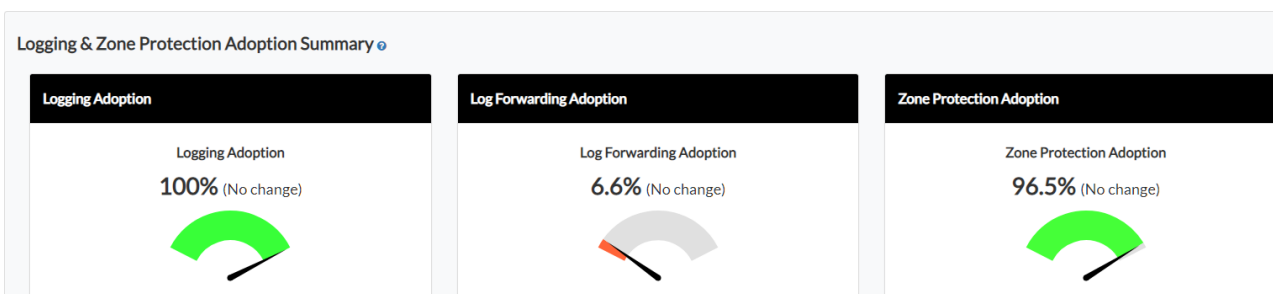
En el [Resumen de adopción](#) de la aplicación y control del usuario del mapa de calor, compruebe las tasas de adopción de las siguientes capacidades. Use las recomendaciones como criterios de identificación de brechas; si la tasa de adopción real no coincide con las recomendaciones, planifique cerrar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

Application & User Control Adoption Summary



- ❑ 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 de lista blanca (regla de permiso) 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 mapa de calor, verifique 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

Utilice **Column Filters (Filtros de columna)** para acotar 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 refinar 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:

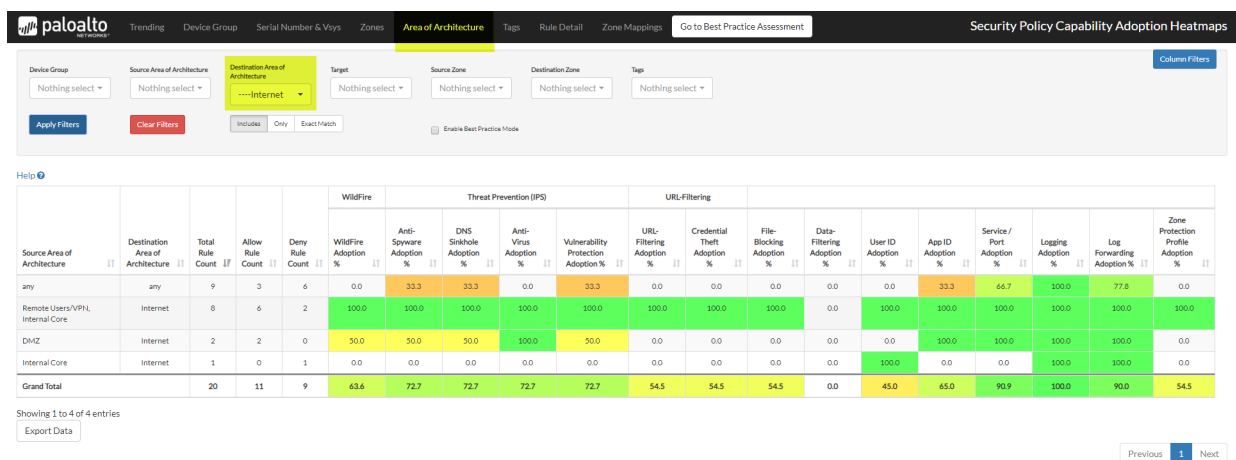
STEP 1 | En la sección Heatmaps de la BPA, haga clic en **Areas of Architecture (Áreas de arquitectura)**.

STEP 2 | Haga clic en **Column Filters (Filtros de columna)** 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 Filter (Aplicar filtro)**.

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 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 | Siguiendo: **Identificar reglas para mejorar**.

12 INTRODUCCIÓN A LA BPA | Evaluar la adopción de la capacidad de la política de seguridad

Identificar reglas para mejorar

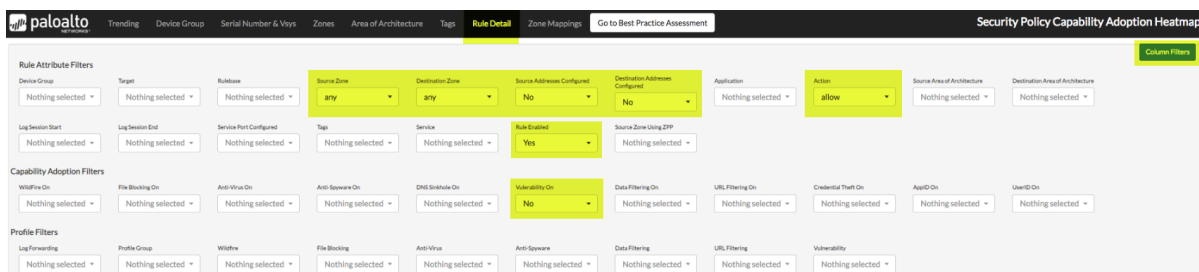
Después de identificar una brecha en la adopción de la capacidad de la política de seguridad, utilice la vista **Rule Detail (Detalle de la regla)** para enumerar las reglas que requieren una mayor investigación o corrección. Configure **Column Filters (Filtros de columna)** para que coincida con los 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 la sección de Mapas de calor de la BPA, haga clic en **Rule Detail (Detalle de regla)**.

STEP 2 | Haga clic en **Column Filters (Filtros de columna)** para expandir las opciones de filtro y luego seleccionar 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:

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.

Cuando abre el informe BPA por primera vez, se abre en la sección Mapa de calor. Haga clic en **Go to Best Practice Assessment (Ir a Evaluación de prácticas recomendadas)** para ir a 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.



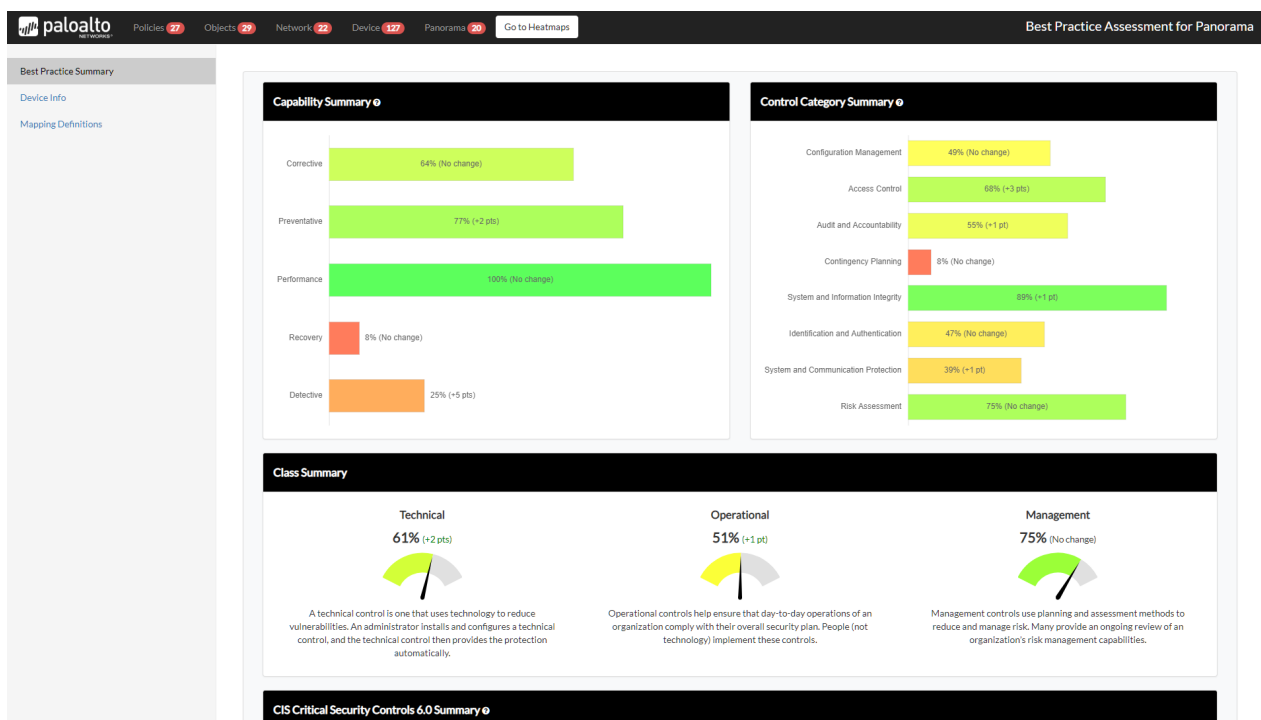
Además de esta documentación, puede ver la Demostración de BPA y un breve vídeo sobre cómo ejecutar una BPA para aprender más sobre el uso del BPA.

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

Cuando cambia la vista de Mapas de calor al informe de BPA, el informe muestra 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 todas 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.

Policies 27
Objects 29
Network 22
Device 127
Panorama 20
Go to Heatmaps

Best Practice Assessment for Panorama

Best Practice Summary

Device Info

Mapping Definitions

Show Filters

Top Nav

Left Nav

Capability

Class

Control Category

CSC Controls

Nothing selected

Nothing selected

Nothing selected

Nothing selected

Nothing selected

Nothing selected

Apply Filters

Clear Filters

Show 10 entries

ID	Best Practice Check Name	Top Nav	Left Nav	Capability	Class	Control Category	CSC Controls	Passing %
3	Description Populated	Policies	Security	Corrective	Operational			0
4	Source/Destination = any/any	Policies	Security	Preventative, Corrective	Technical			99.7
5	Service != any	Policies	Security	Preventative, Corrective	Technical			94.6
6	Log at Start of Session	Policies	Security	Performance	Technical			99.7
7	Log Forwarding	Policies	Security	Recovery, Detective	Operational, Technical	Contingency Planning, Audit and Accountability	6.2, 6.6, 10.1	6.8
8	Expired Non-Recurring Schedules	Policies	Security	Preventative	Operational	Configuration Management	N/A	100
9	Disable Server Response Inspection	Policies	Security	Preventative	Operational	System and Information Integrity	8.1, 8.5, 11.1	100
11	Disabled Rules	Policies	Security	Preventative	Operational	Configuration Management	N/A	55.6
12	Interzone Deny Rule with Logging	Policies	Security	Preventative, Detective	Technical	Audit and Accountability, System and Information Integrity	6.2, 6.4, 6.6	100
13	Intrazone Allow Rules with Logging	Policies	Security	Preventative, Detective	Technical	Audit and Accountability, System and Information Integrity	6.2, 6.6, 8.1	0
							Total:	62.8

Showing 1 to 10 of 202 entries

Export Mappings

Previous

1

2

3

4

5

...

21

Next

Siguiente: [Revisar la configuración de la política de prácticas recomendadas.](#)

Revisar la configuración de la política de prácticas recomendadas

La pestaña **Políticas (Políticas)** muestra todas las comprobaciones relacionadas con diferentes tipos de políticas de cortafuegos. Seleccione el tipo de política que desea revisar para identificar posibles mejoras a la regla. La vista de política de **Security (Seguridad)** muestra los resultados de la verificación basada en reglas (**Security Rule Checks [Comprobaciones de la regla de seguridad]**). **Show Filters (Mostrar filtros)** 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.

Haga clic en ayuda (?) para ver la descripción y el razonamiento de cada verificación, junto con un enlace a la documentación técnica sobre la capacidad que examina cada verificación.

Rule Name	Rule Enabled	Description Populated	Source/Destination != any/any	Service != any	Application != any	APP-ID with Service	Not Logging at Start of Session	Log Forwarding	Expired Non-Recurring Schedules	Disable Server Response Inspection
all-default-profiles	true	✗	✗	✓	✗	—	✓	✗	✓	✓
Allow-Den-Users	true	✗	✓	✓	✗	—	✗	✗	✓	✓
Block-apps	true	✗	✓	✓	—	✓	✓	✗	✓	✓
Block-Apps	false	✗	✓	✓	—	✓	✓	✗	✓	✓
Block-Qik	true	✗	✓	✓	—	✓	✓	✗	✓	✓
Block-Region	true	✗	✓	✓	—	—	✗	✓	✗	✓
Block-region	true	✗	✓	✓	—	—	✓	✗	✓	✓
Byod-users	true	✗	✓	✓	✗	—	✗	✓	✓	✓
Commerce-E	true	✗	✓	✓	✓	✓	✓	✗	✓	✗
dummy-deny	true	✗	✓	✓	—	—	✓	✗	✓	✓
E-comm	true	✗	✓	✓	✓	✓	✓	✗	✓	✓
Guest-traffic	true	✗	✓	✓	✗	—	✓	✗	✓	✓
High-risk-IPS	true	✗	✓	✓	—	✗	✓	✗	✓	✓
Hip-check	true	✗	✓	✓	✗	—	✓	✗	✓	✓
Intrazone-default	true	—	—	—	—	—	✓	✗	—	—
N rule	true	✗	✓	✓	✗	—	✓	✗	✓	✓
Network	true	✗	✗	✓	✓	✓	✓	✗	✓	✓
Networking	true	✗	✓	✓	✓	✓	✓	✗	✓	✗

Passing %: 0% 73.3% 93.3% 33.3% 84.6% 87% 9.6% 96.6% 90%

Bajo la **Security Rule Checks (Comprobaciones de la regla de seguridad)**, las **Security Rulebase Checks (Comprobaciones de base de reglas de seguridad)** resume los resultados de la verificación de prácticas recomendadas por grupo de dispositivos, con un estado de aprobado/suspense 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.

Security Rulebase vsys: vsys1

Best Practice Check Results

- ✗ Disabled Rules (Fail): 1 disabled rules exist
- ✓ Intrazone Deny Rule with Logging (Pass)
- ✗ Intrazone Allow Rules with Logging (Fail): It is recommended to override the intrazone-default rule with Action set to 'allow', Log at Session End enabled, and IPS capability enabled.
- ✓ HIP Profiles used in Rules (Pass)
- ✓ User ID Rules without User ID enabled on Zone (Pass)

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.
 - ❑ **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

La pestaña **Objects (Objetos)** muestra todas las comprobaciones relacionadas con los diferentes tipos de objetos del cortafuegos. Seleccione el tipo de objeto que desea revisar para comprender la configuración existente e identificar brechas potenciales en la configuración de prácticas recomendadas relacionadas con etiquetas, GlobalProtect, perfiles de seguridad, reenvío de logs y perfiles de descifrado. El siguiente ejemplo muestra el resultado de un perfil de seguridad de antivirus.

The screenshot displays the Palo Alto Networks management console. The top navigation bar shows 'Policies 27', 'Objects 29', 'Network 22', 'Device 127', and 'Panorama 20'. The left sidebar lists various configuration categories: Tags (1), GlobalProtect, HIP Profiles (1), Security Profiles, and several protection modules like Anti-Spyware (3), Vulnerability Protection (4), URL Filtering (1), File Blocking (3), WildFire Analysis (1), DoS Protection (5), Log Forwarding (4), and Decryption Profile (3). The 'Antivirus' security profile is selected. The main content area shows the configuration for the 'InternalCore' device group. It includes a table of decoders with columns for Name, Action, and WildFire Action. The 'Best Practice Check Results' section at the bottom indicates that the Antivirus Profile Decoder Actions passed, but the Antivirus Profile Decoder WildFire Actions failed, providing a list of recommended actions for smtp, smb, http, and ftp.

Para cada perfil, 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 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.

Cuando revise la pestaña **Objects (Objetos)**, como mínimo, revise 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

La pestaña **Network (Red)** muestra todas las comprobaciones de la configuración relacionadas con la red. 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 Zones, GlobalProtect, IPsec Crypto y perfiles de protección de zonas. El siguiente ejemplo muestra el resultado para Zones.

The screenshot displays the Palo Alto Networks Best Practice Assessment for Panorama interface. The top navigation bar includes tabs for Policies (27), Objects (29), Network (32), Device (127), and Panorama (20), along with a 'Go to Heatmaps' button. The left sidebar shows a navigation menu with 'Zones (19)' selected, and sub-items for GlobalProtect, Portals, Gateways, Network Profiles, IPsec Crypto, and Zone Protection (3). The main content area is titled 'Best Practice Assessment for Panorama' and shows configuration details for three device groups: Internet, LAN, and GlobalProtect. Each group is associated with the 'vsys1' template and the 'Perimeter' template. The configuration details include 'User Id Enabled' (True), 'Using Acl Include List' (False), and 'Zone Protection Profile' (zpp-hq-Internet for Internet, None for LAN and GlobalProtect). Below the configuration details, the 'Best Practice Check Results' section shows a list of checks with their status (Pass/Fail) and a 'Notes' section with additional information.

Device Group	Template	User Id Enabled	Using Acl Include List	Zone Protection Profile
Internet device group: vsys1 template: Perimeter	All	True	False	zpp-hq-Internet
LAN device group: vsys1 template: Perimeter	All	True	False	None
GlobalProtect device group: vsys1 template: Perimeter	All	True	False	None

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 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 pestañas **Device (Dispositivo)** y **Panorama** muestran todas las comprobaciones relacionadas con la configuración de gestión de dispositivos. Seleccione la verificación de gestión de dispositivos 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 del cortafuegos (haga clic en **Panorama** para ver los resultados de la comprobación de Panorama).

The screenshot shows the Palo Alto Networks Best Practice Assessment for Panorama interface. The top navigation bar includes tabs for Policies (27), Objects (29), Network (32), Device (137), and Panorama (20). The left sidebar lists various setup categories with counts: General Settings (11), Authentication Settings (12), Logging and Reporting Settings (3), Secure Communication Settings (8), Management Interface Settings, Minimum Password Complexity (4), Setup - Services (6), Setup - Content-ID (6), Setup - WildFire (25), Setup - Session (4), Setup - Telemetry (4), High Availability, Administrators, Admin Roles, Authentication Profile (2), Authentication Profiles (3), Authentication Sequence, Authentication Sequences (4), User Identification, Log Settings, and System (12). The main content area displays 'Template General Settings' for three templates: Perimeter, Internal Core, and Datacenter. Each template section shows configuration details for Login Banner, Auto Acquire Commit Lock, and Ssl/Tls Service Profile, along with 'Best Practice Check Results' indicating failures for 'Automatically Acquire Commit Lock', 'Certificate Expiration Check', and 'Login Banner'.

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/suspenseo y recomendaciones para verificaciones de prácticas recomendadas fallidas. Haga clic en el signo de interrogación para 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](#).

