Inicio de las prácticas recomendadas con la Evaluación de prácticas recomendadas (BPA) y la Garantía de seguridad

Version 9.1

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

March 5, 2020

Table of Contents

Introducción a las prácticas recomendadas..... 5
Identificar y priorizar las prácticas recomendadas..... 7
Acceder y ejecutar la Evaluación de prácticas recomendadas (BPA)..... 10
Acceda a la BPA desde el Portal de Atención al Cliente..... 10
Generar y descargar un informe BPA..... 12
Garantía de seguridad..... 15
Las siete capacidades de seguridad clave para adoptar..... 15
Comprobación de la adopción de las siete capacidades de seguridad clave..... 16
Mejorar la adopción de las siete capacidades de seguridad clave..... 18
Cómo activar la garantía de seguridad..... 19

Introducción a las prácticas recomendadas

Las prácticas recomendadas de seguridad previenen amenazas conocidas y desconocidas, reducen la superficie de ataque y brindan visibilidad del tráfico, para que sepa y controle qué aplicaciones, usuarios y contenido hay en su red. Cuando implementa las prácticas recomendadas de seguridad, usted:

- Minimiza las posibilidades de una intrusión exitosa.
- Identificar la presencia de atacantes.
- Protege sus datos valiosos.
- Protege a sus clientes, socios y empleados y, por lo tanto, protege la reputación de su empresa.
- Ayude a lograr un entorno de seguridad deZero Trust.

Para pasar a las prácticas recomendadas de seguridad, primero debe comprender su posición actual de seguridad de red e identificar áreas de mejora. Palo Alto Networks proporciona una ruta de transición guiada: la Evaluación de prácticas recomendadas (BPA) combinada con los Pasos para una transición segura y la documentación técnica de prácticas recomendadas.

Cuando se suscribe al servicio Premium (a partir del 1 de noviembre de 2019) o al Contrato de soporte Platinum, tiene la oportunidad de prepararse para la Garantía de seguridad. La Garantía de seguridad proporciona acceso a expertos en seguridad y herramientas de Palo Alto Networks para ayudar con la investigación inicial de incidentes.

- Identificar y priorizar las prácticas recomendadas
- Acceder y ejecutar la Evaluación de prácticas recomendadas (BPA)
- Garantía de seguridad

Identificar y priorizar las prácticas recomendadas

La Evaluación de prácticas recomendadas (BPA) de Palo Alto Networks utiliza su archivo de asistencia técnica para analizar los ajustes de configuración del cortafuegos de nueva generación y Panorama, y compara la configuración con las prácticas recomendadas de Palo Alto Networks. La BPA muestra el estado actual de la adopción de seguridad de prácticas recomendadas y sugiere cambios específicos para alinear la configuración con las prácticas recomendadas sobre seguridad. La ejecución de la BPA no solo le brinda una comprensión de dónde mejorar su estrategia de seguridad, sino que también establece una línea base para una comparación posterior y proporciona enlaces a documentación técnica que le muestran cómo llevar a cabo la transición de las recomendaciones de la BPA para obtener una configuración de prácticas recomendadas.

Con un enfoque iterativo y prioritario, puede transformar su posición de seguridad a un estado de práctica recomendada, paso a paso, midiendo el progreso y el nivel de comodidad conforme avanza:

STEP 1 | Cargue un archivo de asistencia técnica en el Portal de atención al cliente y Acceder y ejecutar la Evaluación de prácticas recomendadas (BPA) usted mismo, o comuníquese con su SE o socio de Palo Alto Networks para ejecutar la BPA en Panorama o sus cortafuegos de última generación.

Si ejecuta la BPA usted mismo, le recomendamos que se ponga en contacto con su SE de Palo Alto Networks o socio para que lo ayude a interpretar los resultados y comentar los próximos pasos.

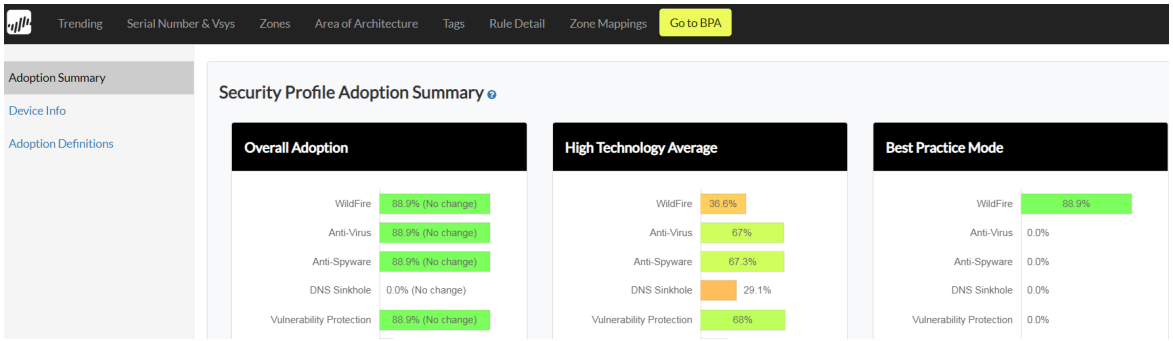
STEP 2 | Identifique y priorice la primera área de mejora para empezar la transición a las prácticas recomendadas.

Ya sea que su SE de Palo Alto Networks o socio ejecute la BPA, o usted ejecute la BPA, su SE o socio puede ayudarle a formular un plan priorizado para incorporar de manera segura las prácticas recomendadas. Planifique empezar primero con los cambios más seguros, fáciles y de mayor impacto, como la aplicación de los perfiles de antivirus, antispyware, la protección frente a vulnerabilidades y el análisis WildFire a sus reglas de política de seguridad.

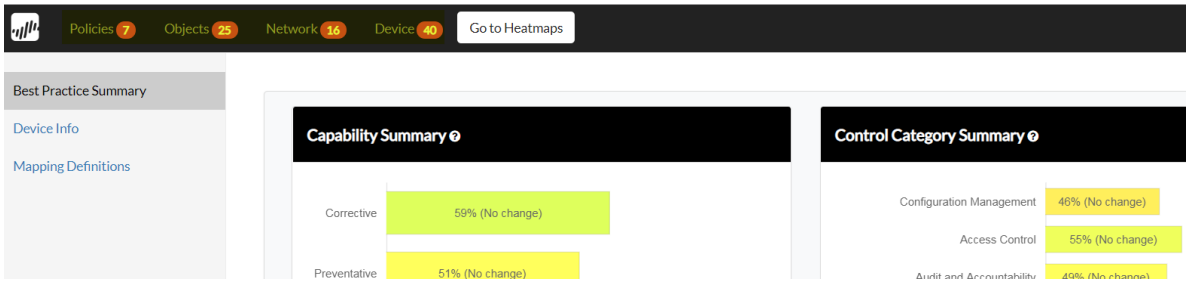
STEP 3 | Utilice los enlaces de BPA a la documentación técnica para configurar las prácticas recomendadas a las que ha de dar prioridad.

La descarga del informe BPA le proporciona un archivo .zip que contiene el informe detallado en HMTL, un resumen ejecutivo y una hoja de cálculo de Excel que enumera las comprobaciones de prácticas recomendadas fallidas. Se puede vincular a la documentación técnica de dos maneras:

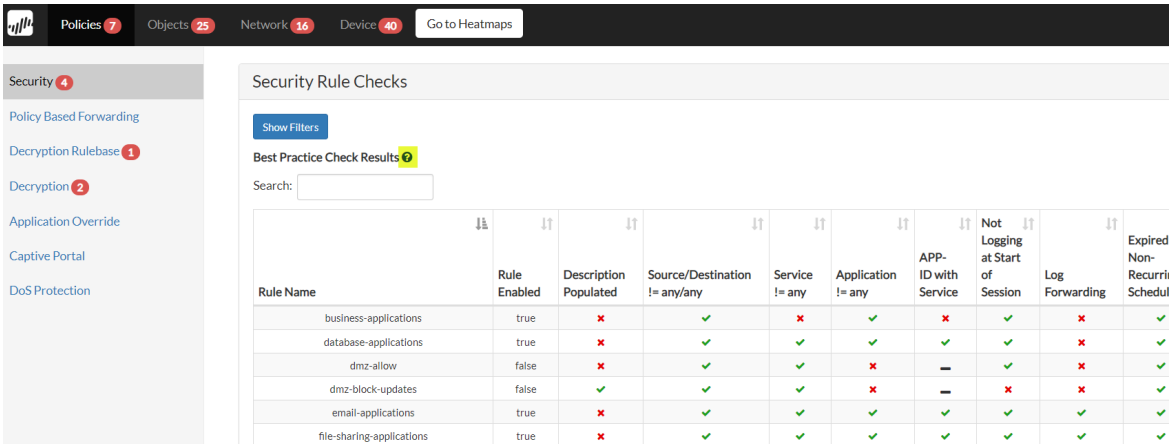
- Desde la hoja de cálculo: La pestaña Documentación proporciona enlaces para cada verificación no superada. Además, el número de identificación en la columna Comprobar ID en las pestañas Políticas, Objetos, Red y Dispositivo se enlaza directamente a la línea correspondiente en la pestaña Documentación.
- Del informe HTML, cuando abre el informe HTML, verá un mapa de calor que resume la adopción de las prácticas recomendadas. **Go to BPA (Ir a BPA)** Para acceder al informe.



Desde la página de resumen de la BPA, vea los informes detallados sobre **Policies (Políticas)**, **Objects (Objetos)**, **Network (Red)** o **Device (Dispositivo)** para la evaluación de configuración seleccionada.



De un informe detallado, haga clic en el signo **?** En un círculo azul para obtener descripciones y razonamientos sobre la verificación de la configuración y enlaces a la documentación técnica para la configuración de prácticas recomendadas.



Para los perfiles de seguridad (protección frente a vulnerabilidades, antivirus, antispyware, filtrado de URL, bloqueo de archivos), use los consejos para la transición segura para garantizar la disponibilidad de aplicaciones críticas para el negocio a medida que avanza hacia los perfiles de seguridad de prácticas recomendadas.

STEP 4 | Después de implementar el primer conjunto de cambios de prácticas recomendadas, ejecute nuevamente la BPA para medir el progreso y ayudar a verificar que los cambios funcionan como se esperaba.

Compare el primer resultado de la BPA y el siguiente resultado de la BPA para ver las mejoras en su estrategia de seguridad. Identifique y de prioridad a la siguiente área de mejora a tratar.

STEP 5 | Use los enlaces de BPA a la documentación técnica para configurar el siguiente conjunto de prácticas recomendadas que priorizó.

STEP 6 | Cuando considere adecuado, vuelva a ejecutar la BPA para medir el progreso e identificar y priorizar los próximos pasos, y luego configure las prácticas recomendadas utilizando la documentación técnica.

STEP 7 | Empiece ahora: Acceder y ejecutar la Evaluación de prácticas recomendadas (BPA) o póngase en contacto con su SE de Palo Alto Networks o socio y comience la transición a una red más segura hoy mismo.

Acceder y ejecutar la Evaluación de prácticas recomendadas (BPA)

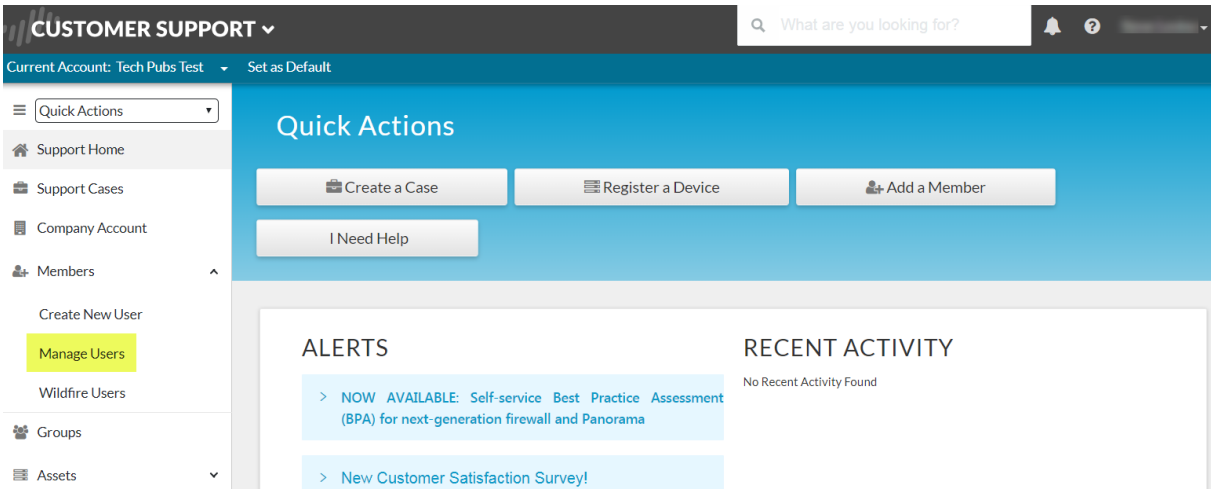
Acceda a la Evaluación de prácticas recomendadas (BPA) desde el Portal de atención al cliente. Las cuentas de superusuario tienen acceso automático a la BPA y pueden asignar la función de *Usuario BPA* a un perfil de un usuario estándar para que el usuario estándar pueda ejecutar la BPA. Este procedimiento muestra a los Superusuarios cómo dar acceso a los Usuarios estándar y cómo ejecutar la BPA. También puede ver vídeos cortos sobre cómo ejecutar una BPA y cómo entender los resultados.

Además, si se suscribe al servicio Premium (a partir del 1 de noviembre de 2019) o al Contrato de asistencia Platinum, tiene la oportunidad de prepararse y activar la Garantía de seguridad. La Garantía de seguridad proporciona acceso a expertos en seguridad y herramientas de Palo Alto Networks para ayudar con la investigación inicial de incidentes. Recomendamos encarecidamente que ejecute la BPA para medir su adopción de las siete capacidades de seguridad clave y para asegurarse de que su tasa de adopción sea al menos igual a la tasa de adopción media de su sector para que su red esté mejor protegida. La combinación del contrato de asistencia Premium o Platinum y una medición reciente de BPA que muestra que su tasa de adopción de las siete capacidades de seguridad clave cumple con la media de su sector activa automáticamente la Garantía de seguridad.

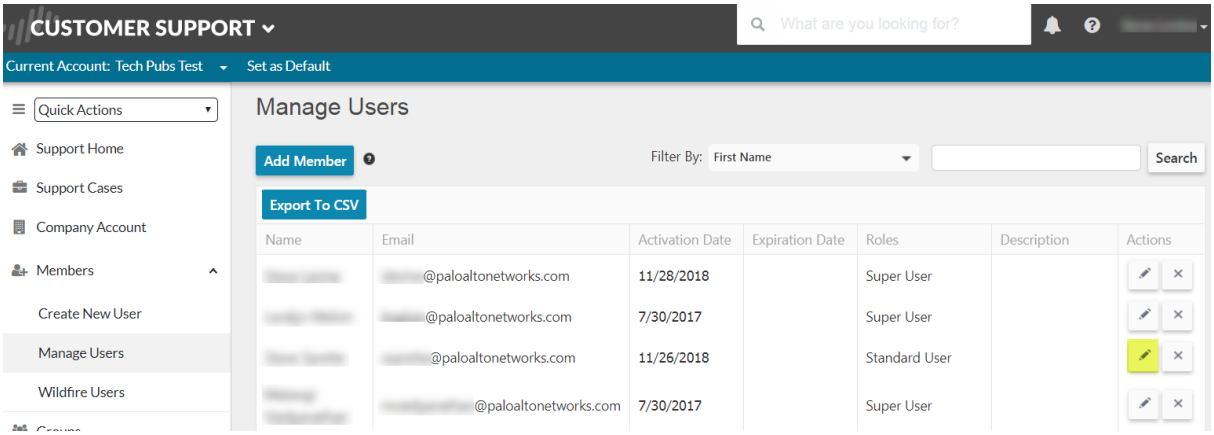
- Acceda a la BPA desde el Portal de Atención al Cliente
- Generar y descargar un informe BPA

Acceda a la BPA desde el Portal de Atención al Cliente

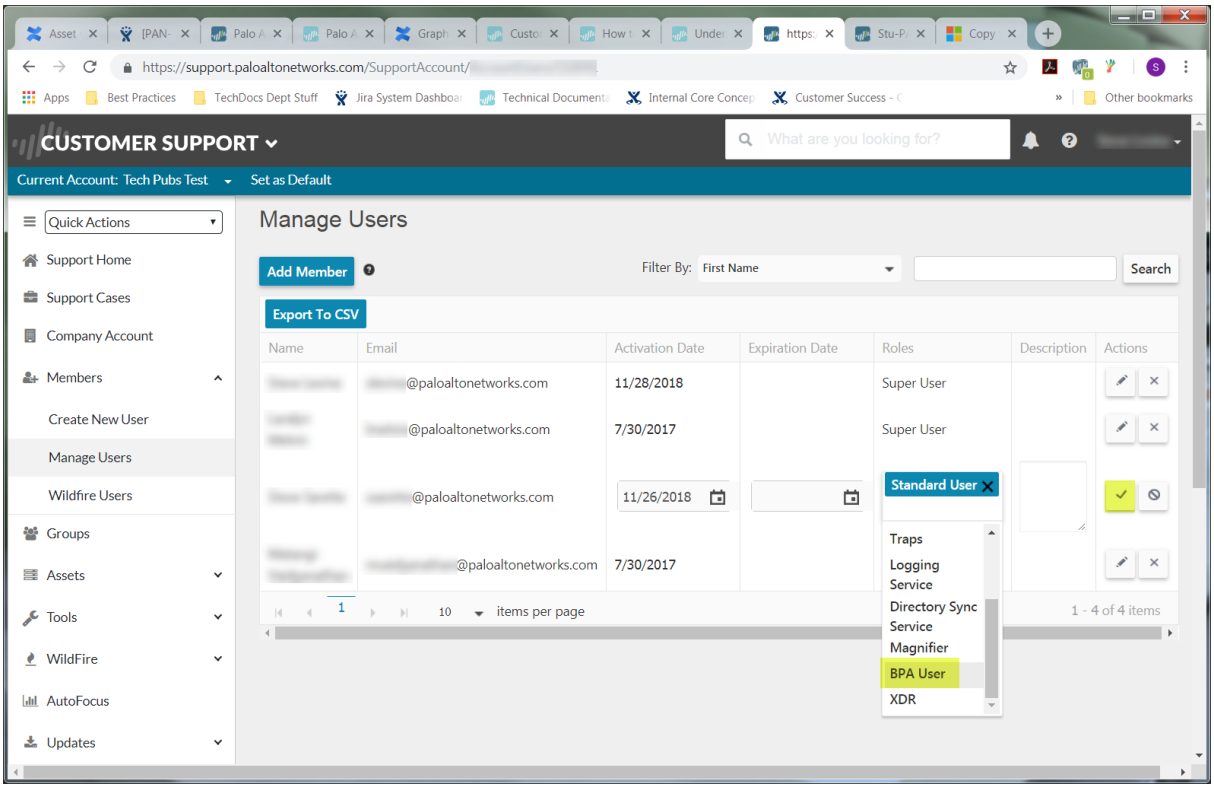
STEP 1 | Desde la pantalla de autenticación del Portal de atención al cliente, seleccione **Members (Miembros)** > **Manage Users (Gestionar usuarios)**.



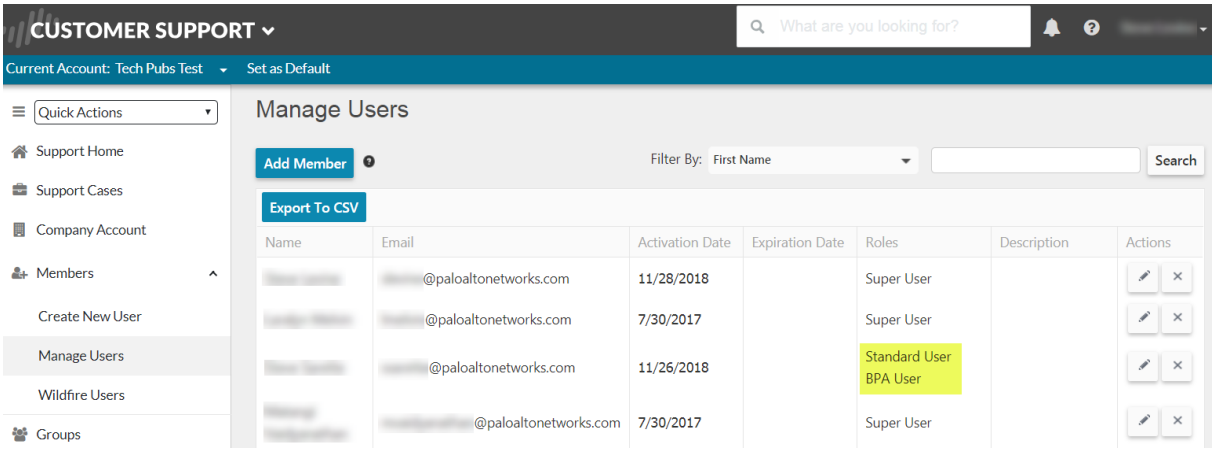
STEP 2 | Haga clic en el icono de lápiz para editar el usuario estándar al que desea asignar permisos BPA.



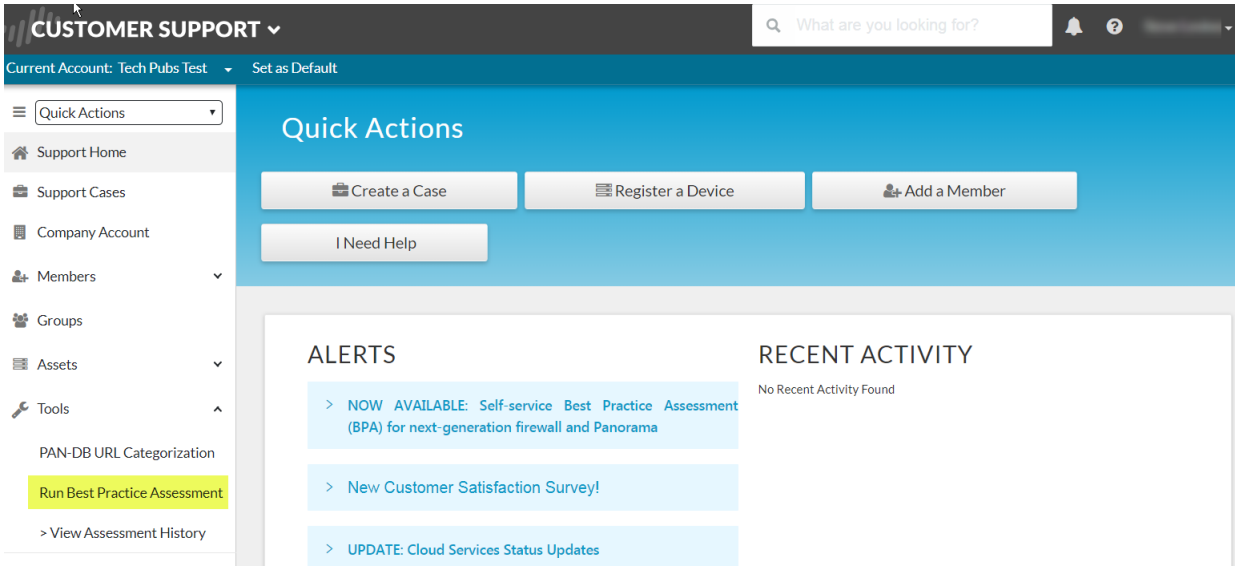
STEP 3 | Seleccione la función **BPA User (Usuario BPA)** y luego haga clic en la marca de verificación de actualización para añadir la nueva función.



STEP 4 | El usuario estándar ahora tiene los privilegios de rol de usuario BPA.



STEP 5 | Los superusuarios y los usuarios estándar con la función de usuario BPA pueden iniciar sesión en el Portal de atención al cliente para acceder y ejecutar las BPA [**Tools (Herramientas)** > **Run Best Practice Assessment (Ejecutar evaluación de prácticas recomendadas)**].



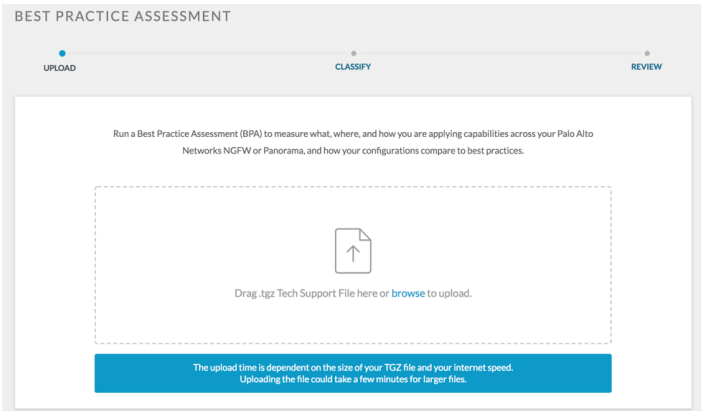
Generar y descargar un informe BPA

Después de obtener acceso a la BPA, puede generar un informe de BPA para un dispositivo Panorama o para un cortafuegos de próxima generación.

Si es posible, genere informes BPA para dispositivos Panorama en lugar de cortafuegos de última generación individuales, de forma que pueda obtener una visibilidad completa de todos los cortafuegos en su entorno en un único informe. Genere informes periódicamente para medir el progreso hacia la adopción de capacidades de seguridad y prácticas recomendadas de seguridad.

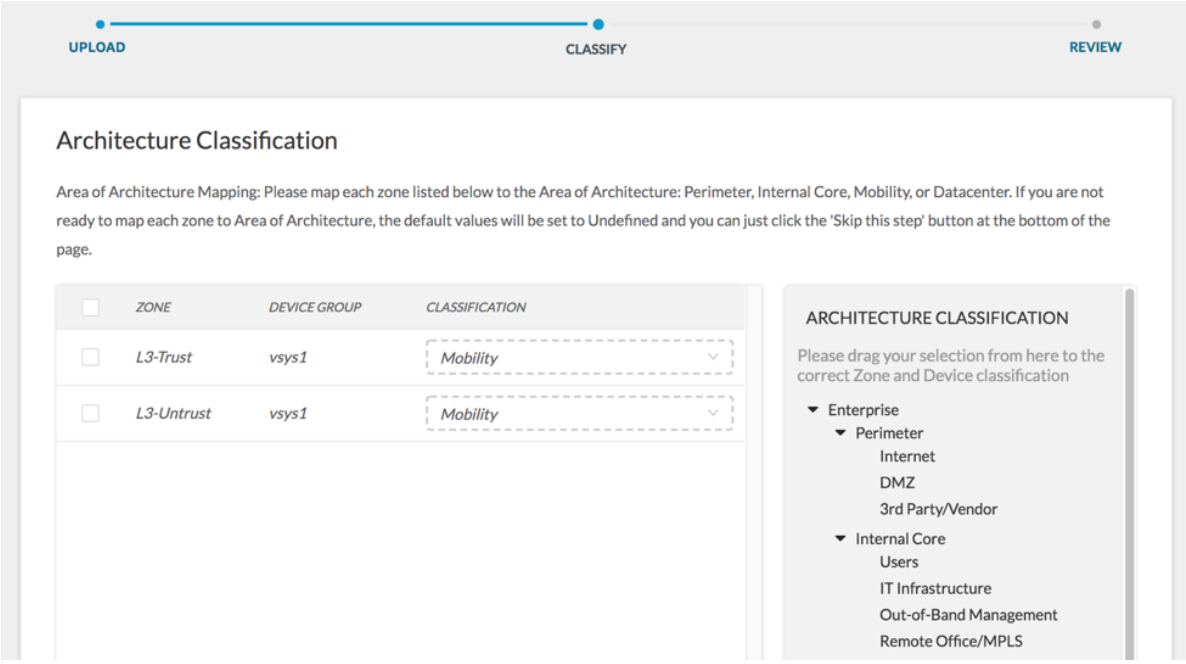
STEP 1 | Arrastre o suelte un Archivo de asistencia técnica (archivo .tgz) en la ventana del Portal de atención al cliente o busque un archivo de asistencia técnica.

Los superusuarios pueden crear archivos de asistencia técnica [**Device (Dispositivo)** > **Support (Asistencia técnica)** > **Tech Support File (Archivo de asistencia técnica)** o **Panorama** > **Support (Asistencia técnica)** > **Tech Support File (Archivo de asistencia técnica)**].



STEP 2 | Opcionalmente, asigne cada zona al área de la arquitectura o haga clic en **Skip this step (Omitir este paso)** para ejecutar la BPA sin asignar zonas.

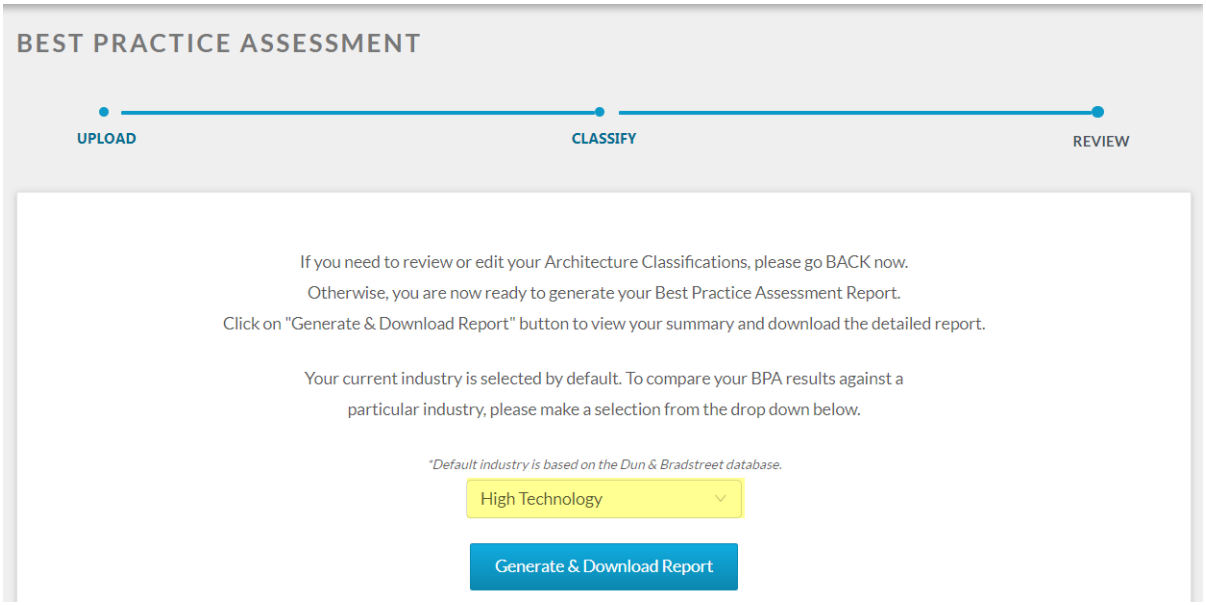
Arrastre y suelte el valor de arquitectura desde Clasificación de arquitectura, use el menú desplegable **Classification (Clasificación)** para seleccionar un valor, o seleccione varias casillas de verificación para seleccionar varias zonas y luego aplique un valor a todas las zonas seleccionadas al mismo tiempo .



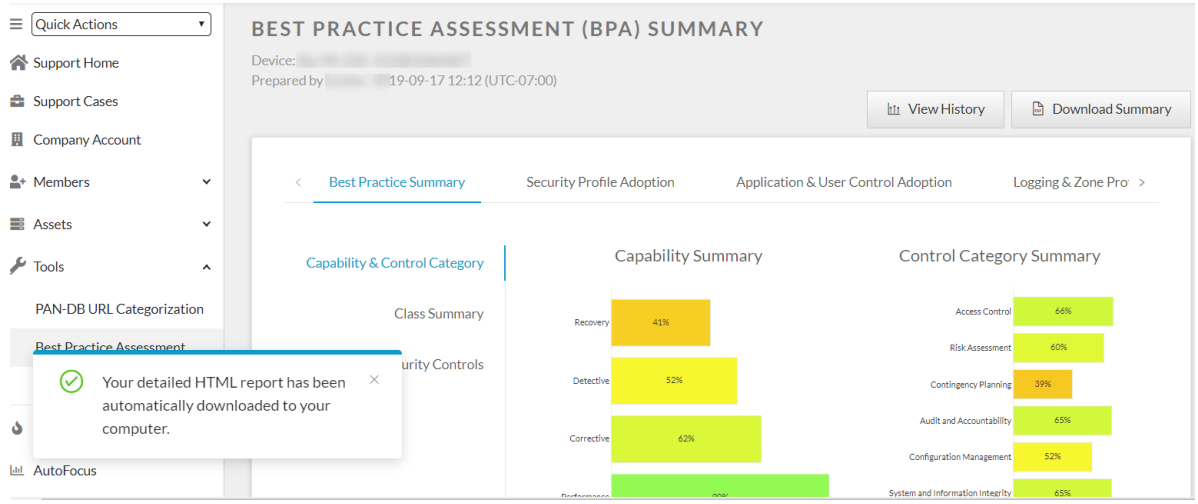
STEP 3 | Identifique el sector asignado a su cuenta y genere y descargue el informe BPA [**Generate & Download Report (Generar y descargar informe)**].

Puede cambiar el sector frente al que la BPA compara sus resultados utilizando el menú desplegable. Si desea cambiar algo antes de generar el informe, también puede volver y hacer esos cambios.

Generate & Download Report (Generar y descargar informe) descarga el informe detallado de la BPA, el informe de resumen ejecutivo y una hoja de cálculo que muestra las comprobaciones de prácticas recomendadas fallidas en el sistema desde el que accedió y ejecutó la BPA.



STEP 4 | La BPA generada muestra el Resumen Ejecutivo y le informa que el informe HTML detallado se descargó en su equipo informático.



STEP 5 | Ahora que ya sabe cómo ejecutar la BPA, vaya al Portal de atención al cliente y pruébelo hoy mismo (o póngase en contacto con su SE de Palo Alto Networks o socio para ejecutar la BPA) para comenzar la transición a una red más segura.

Si se suscribe al servicio Premium (a partir del 1 de noviembre de 2019) o al Contrato de soporte Platinum, use la BPA para preparar su estrategia de seguridad para aprovechar Garantía de seguridad, que ayuda con las investigaciones iniciales de incidentes.

Garantía de seguridad

Si detecta actividad sospechosa en su red, la Garantía de seguridad le proporciona ayuda adicional de Palo Alto Networks cuando más la necesita. La Garantía de seguridad proporciona:

- Acceso a los expertos en seguridad de Palo Alto Networks y sus herramientas especializadas de inteligencia de amenazas y prácticas de búsqueda de amenazas.
- Análisis avanzado de logs e indicadores de riesgo (IOC).
- Evaluación de la configuración que incluye recomendaciones personalizadas de seguridad de los productos.
- Recomendaciones del siguiente paso para acelerar la transición a su proveedor de respuesta a incidentes (IR) para ayudar a gestionar y resolver el incidente.

Para aprovechar la Garantía de seguridad, debe suscribirse al Contrato de asistencia Premium (a partir del 1 de noviembre de 2019) o al Contrato de asistencia Platinum.

El primer paso hacia la Garantía de seguridad es ejecutar laEvaluación de prácticas recomendadas (BPA) para medir su adopción de siete capacidades de seguridad clave: WildFire, antivirus, antispyware, DNS Sinkhole, filtrado de URL, protección frente a vulnerabilidades y creación de logs. Le recomendamos que se asegure de que su tasa de adopción para esas capacidades de seguridad sea al menos igual a la tasa de adopción media de su sector.

La ejecución de la BPA y adopción de niveles más altos de capacidades de seguridad clave proporcionan una mejor protección para su red y ayuda a evitar incidentes. La BPA también mide el nivel de adopción de muchas otras capacidades de seguridad, como ID de aplicación e ID de usuario, configuración de zona, otros perfiles de seguridad como bloqueo de archivos y perfiles de protección DoS, y la BPA hace recomendaciones sobre cómo mejorar su estrategia de seguridad.

Ejecute la BPA periódicamente (por ejemplo, mensualmente o trimestralmente) para medir la adopción de capacidades de seguridad clave, comprender el estado de la seguridad de su red y priorizar las mejoras de seguridad.

Cuando se suscribe al Contrato de asistencia Premium (a partir del 1 de noviembre de 2019) o al Contrato de asistencia Platinum y ejecuta la BPA, si muestra que ha adoptado las siete capacidades de seguridad clave a una tasa que cumple con la media de su sector, la Garantía de seguridad se habilita automáticamente. Si necesita asistencia para adoptar estas capacidades clave a un ritmo que cumpla con la media de su sector, comuníquese con su representante de ventas de Palo Alto Networks para obtener ayuda para definir los requisitos, proporcionar criterios de justificación, etc. Si motivos comerciales le impiden adoptar las capacidades de seguridad clave en este nivel, trabaje con su representante de ventas de Palo Alto Networks sobre cómo obtener acceso a los beneficios de la Garantía de seguridad.

- Las siete capacidades de seguridad clave para adoptar
- Comprobación de la adopción de las siete capacidades de seguridad clave
- Mejorar la adopción de las siete capacidades de seguridad clave
- Cómo activar la garantía de seguridad

Las siete capacidades de seguridad clave para adoptar

Recomendamos encarecidamente adoptar las siguientes siete capacidades de seguridad clave por los siguientes motivos:

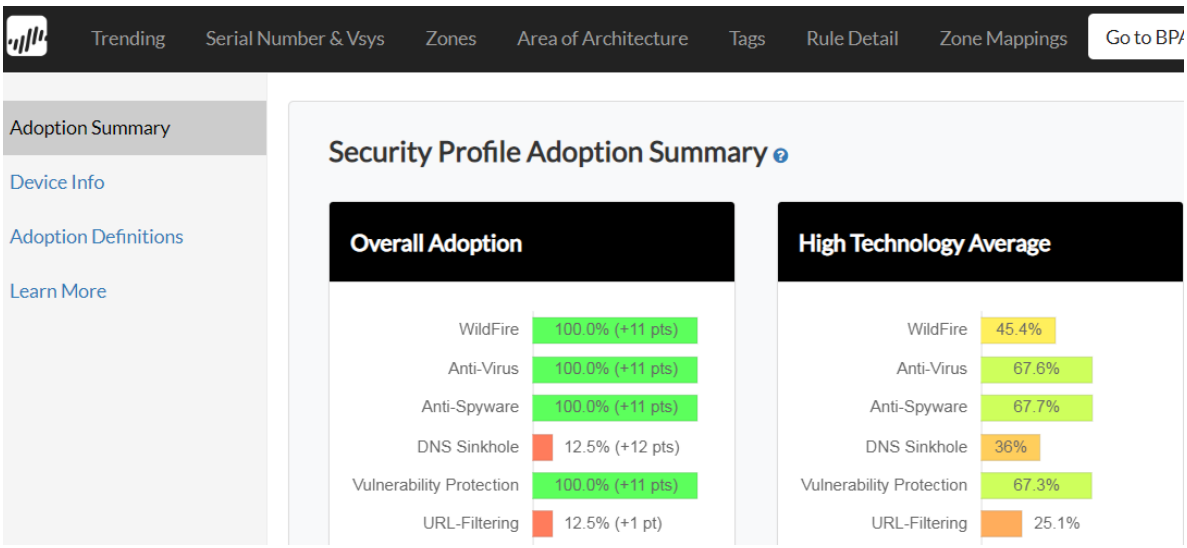
- **WildFire**: adjunte un perfil de seguridad WildFire a las reglas de política de seguridad que permiten el tráfico para proteger su red de amenazas nuevas y desconocidas. WildFire es una defensa sólida contra las amenazas avanzadas persistentes (ATP).

- **Antivirus**: adjunte un perfil de seguridad de antivirus a las reglas de política de seguridad que permiten el tráfico para bloquear archivos maliciosos conocidos como malware, ransomware, bots y virus.
- **Antispyware**: adjunte un perfil de seguridad antispyware a las reglas de política de seguridad que permiten que el tráfico detecte el tráfico de comando y control (C2) iniciado por código malicioso que se ejecuta en un servidor o endpoint, y que evitan que los sistemas comprometidos establezcan una conexión saliente desde su red.
- **DNS Sinkhole**: configure la porción de DNS Sinkhole de un perfil de seguridad antispyware que se adjunta a las reglas de política de seguridad que permiten el tráfico. DNS Sinkhole permite identificar los hosts potencialmente en riesgo que intentan acceder a dominios sospechosos realizando el seguimiento de los hosts y evitando que accedan a esos dominios.
- **Filtrado de URL**: adjunte un perfil de filtrado de URL a las reglas de política de seguridad que permiten el tráfico para evitar el acceso a contenido web peligroso (sitios que pueden contener contenido malicioso). Los perfiles de filtrado de URL y las categorías de URL le brindan un control granular sobre los tipos de sitios web a los que permite el acceso.
- **Protección frente a vulnerabilidades**: adjunte un perfil de seguridad de protección frente a vulnerabilidades a las reglas de política de seguridad que permiten el tráfico para evitar que los atacantes aprovechen las vulnerabilidades del lado del cliente y del servidor y entreguen cargas mal intencionadas a su red y usuarios, y para evitar que los atacantes usen vulnerabilidades para moverse lateralmente dentro de su red.
- **Creación de logs**: permite la creación de logs de todo el tráfico (permitido y denegado) para proporcionar una pista de auditoría con marca de tiempo para eventos del sistema y eventos de tráfico de red. Los logs proporcionan información crítica para investigar incidentes. Reenvío de logs le permite enviar logs desde todos sus cortafuegos a Panorama o al exterior para añadir los logs para su análisis.

La adopción de estas capacidades clave mejora enormemente su estrategia de seguridad, reduce su superficie de ataque, aumenta su visibilidad del tráfico de red, previene ataques conocidos y nuevos, y protege sus datos, activos, aplicaciones y servicios que son muy valiosos para su red.

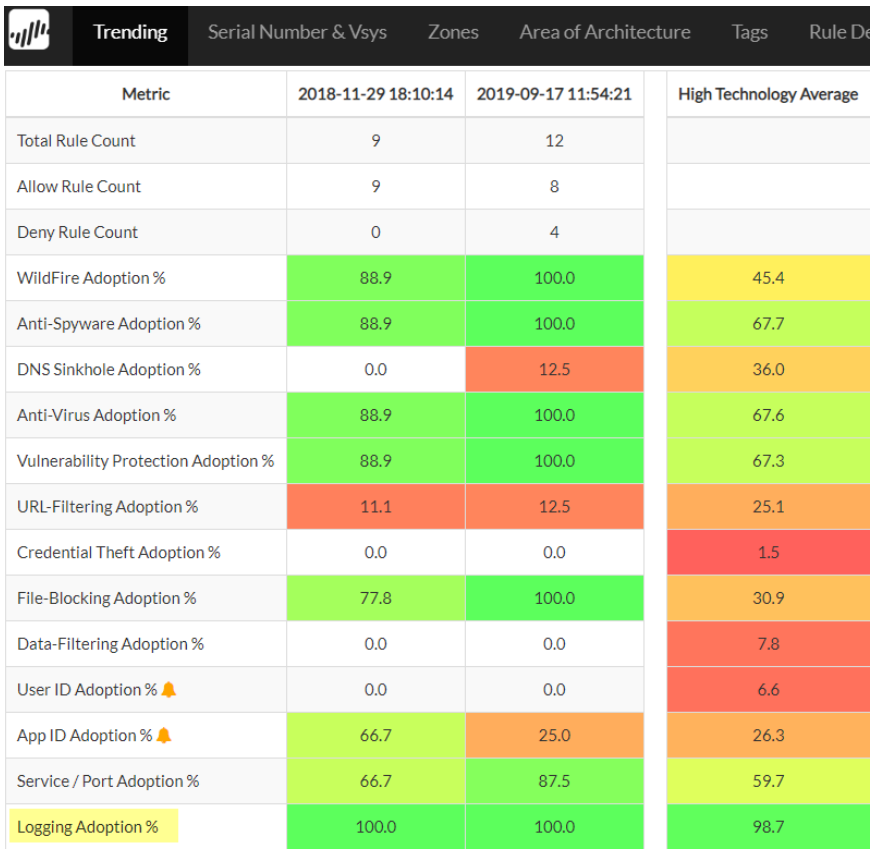
Comprobación de la adopción de las siete capacidades de seguridad clave

En el informe detallado de BPA (formato HTML) que recibe cuando genera y descarga sus resultados de BPA, vaya a la Página de resumen de adopción para verificar su adopción general de los seis perfiles de seguridad (WildFire, antivirus, antispyware, DNS Sinkhole, protección frente a vulnerabilidades y filtrado de URL) y la media de adopción de esas capacidades por parte de su sector (la creación de logs es una verificación por separado). La página Resumen de adopción muestra la adopción de sus capacidades de seguridad en comparación con su sector y le ayuda a identificar las brechas en la adopción. Por ejemplo, si su sector es la Alta tecnología:



Los resultados muestran que la configuración cumple con la adopción media del sector para cuatro capacidades: Perfiles de WildFire, antivirus, antispyware y perfil de protección frente a vulnerabilidades. Los resultados también muestran que la configuración no llega a la adopción media del sector para dos capacidades: DNS Sinkhole y filtrado de URL. Esto indica el siguiente curso de acción: configure el DNS sinkhole en el perfil antispyware y aplique el filtrado de URL al tráfico de Internet.

En el informe detallado de la BPA, en formato HTML, vaya a la página **Trending (Tendencias)** para verificar su adopción general de las capacidades de creación de logs y la adopción media de dicha capacidad en el sector.



Metric	2018-11-29 18:10:14	2019-09-17 11:54:21	High Technology Average
Total Rule Count	9	12	
Allow Rule Count	9	8	
Deny Rule Count	0	4	
WildFire Adoption %	88.9	100.0	45.4
Anti-Spyware Adoption %	88.9	100.0	67.7
DNS Sinkhole Adoption %	0.0	12.5	36.0
Anti-Virus Adoption %	88.9	100.0	67.6
Vulnerability Protection Adoption %	88.9	100.0	67.3
URL-Filtering Adoption %	11.1	12.5	25.1
Credential Theft Adoption %	0.0	0.0	1.5
File-Blocking Adoption %	77.8	100.0	30.9
Data-Filtering Adoption %	0.0	0.0	7.8
User ID Adoption %	0.0	0.0	6.6
App ID Adoption %	66.7	25.0	26.3
Service / Port Adoption %	66.7	87.5	59.7
Logging Adoption %	100.0	100.0	98.7

Esta página muestra no solo su nivel de adopción en comparación con su sector, sino también su nivel de adopción en comparación con la última vez que ejecutó la BPA. Esta es una medida de la mejora de la seguridad a lo largo del tiempo, así como un llamado a la acción si sus resultados indican que su seguridad no es tan estricta como usted desea.

Si el perfil y los resultados de la creación de logs muestran que su adopción de las siete capacidades cumple con la media del sector, la Garantía de seguridad se habilita automáticamente. Si necesita asistencia para adoptar estas capacidades clave a un ritmo que cumpla con la media de su sector, comuníquese con su representante de ventas de Palo Alto Networks para obtener ayuda para definir los requisitos, proporcionar criterios de justificación, etc. Si motivos comerciales le impiden adoptar las capacidades de seguridad clave en este nivel, trabaje con su representante de ventas de Palo Alto Networks sobre cómo obtener acceso a los beneficios de la Garantía de seguridad.

Mejorar la adopción de las siete capacidades de seguridad clave

Use la BPA junto con la documentación técnica de Palo Alto Networks para identificar las capacidades de seguridad que necesitan mejoras y para realizar las mejoras necesarias, especialmente en las siete capacidades de seguridad clave. Mejorar su estrategia de seguridad ayuda a proteger a sus usuarios y sus valiosos dispositivos, activos, aplicaciones y servicios.

- **WildFire**: Transición segura de perfiles de WildFire a las prácticas recomendadas e implementación de las Prácticas recomendadas de WildFire. El perfil de prácticas recomendadas de WildFire es el perfil predeterminado.
- **Antivirus**: Transición segura de perfiles de antivirus a las prácticas recomendadas e implementación de las Prácticas recomendadas de antivirus (o ligeramente más estrictas prácticas recomendadas de antivirus para el centro de datos).
- **Antispyware y DNS Sinkhole**: la configuración de DNS Sinkhole se encuentra en la pestaña **DNS Signatures (Firmas DNS)** en el perfil de seguridad antispyware. Cambie de forma segura los perfiles antispyware a las prácticas recomendadas y luego implemente prácticas recomendadas antispyware (o ligeramente más estrictas prácticas recomendadas antispyware para el centro de datos).
- **Filtrado de URL**: Transición segura de perfiles de filtrado de URL a las prácticas recomendadas e implementación de las Prácticas recomendadas de filtrado de URL.
- **Protección frente a vulnerabilidades**: Transición segura de perfiles de protección frente a vulnerabilidades a las prácticas recomendadas e implementación de las Prácticas recomendadas de protección frente a vulnerabilidades (o ligeramente más estrictas prácticas recomendadas de protección frente a vulnerabilidad para los datos centro).
- **Creación de logs**: las reglas de política de seguridad generan un log al final de la sesión de forma predeterminada.

Además, la BPA y la documentación técnica le muestran cómo mejorar muchas otras capacidades de seguridad, como App-ID, User-ID, perfiles de bloqueo de archivos, DoS y protección de zona, y protección contra robo de credenciales. Algunos recursos clave son:

- Introducción a la BPA: le muestra cómo utilizar la BPA para revisar la adopción de capacidades de seguridad e identificar brechas en la adopción, evaluar su configuración, incluidas las políticas, los objetos, la red y la configuración de dispositivos y Panorama, y priorizar cambios que incluyen fortalecer la estrategia de gestión de su dispositivo, mejorar la visibilidad del tráfico e implementar controles iniciales de prácticas recomendadas.
- Prácticas recomendadas de descifrado: le muestra cómo aumentar su visibilidad descifrando todo el tráfico que permite su modelo de negocio, consideraciones de privacidad y regulaciones para que pueda inspeccionar la cantidad máxima de tráfico y proteger su red frente a amenazas cifradas.
- Prácticas recomendadas de protección de zonas y DoS: le muestra cómo adoptar un enfoque por capas para protegerse contra los ataques de denegación de servicio (DoS) que intentan derribar su red y defender su perímetro, zonas y dispositivos individuales.

- Prácticas recomendadas para actualizaciones de contenido de aplicaciones y amenazas: la implementación de contenido y de actualizaciones de aplicaciones de la mejor manera para los requisitos de su empresa garantiza que su red esté protegida contra las últimas amenazas e identifica las aplicaciones más recientes.

Puede encontrar todos estos documentos y mucho más en el Portal de prácticas recomendadas y en la página Transición a las prácticas recomendadas.

Cómo activar la garantía de seguridad

Si experimenta actividad sospechosa, cuando activa la Garantía de seguridad, debe proporcionar un conjunto específico de datos sobre el incidente sospechoso para que los expertos de Palo Alto Networks puedan investigar la actividad.

- Datos a recopilar antes de activar la Garantía de seguridad
- Activación de la Garantía de seguridad

Datos a recopilar antes de activar la Garantía de seguridad

Los expertos de Palo Alto Networks necesitan, como mínimo, la siguiente información sobre la actividad sospechosa para comenzar a diagnosticar el posible problema. Recopile estos datos antes de activar la Garantía de seguridad.

Detalles básicos sobre la actividad sospechosa:

- **El tipo y vector del ataque sospechoso**: ¿Qué evidencia de actividad sospechosa alertó a su equipo administrativo o de respuesta?
- **Línea de tiempo**:
  - Fecha y hora del presunto ataque inicial, si se conoce.
  - La hora en que identificó el posible problema.
- **Detalles del incidente**:
  - Direcciones IP conocidas de los sistemas afectados.
    - Las direcciones IP de los hosts afectados que están disponibles públicamente a través de NAT.
    - Servicios críticos que podrían hacer que el sistema o los sistemas sean un objetivo, por ejemplo, bases de datos, servicios web, servidores de acceso remoto (RDP, Citrix, etc.).
  - Direcciones IP sospechosas o conocidas que pueden estar relacionadas con el ataque.
  - Las User-ID de las cuentas de usuario comprometidas (si las hay).
- **Diagrama de topología o descripción general**: La ubicación del cortafuegos en relación con los hosts afectados. (No se requiere un diagrama de topología de red completo).
- **Malware e indicadores de compromiso**:
  - Muestras.
  - Hashes.

Datos del cortafuegos:

- **Archivos de asistencia técnica**:
  - Genere y cargue archivos de Asistencia técnica desde los cortafuegos en la ruta a dispositivos potencialmente afectados en el momento de la actividad sospechosa.
  - Si utiliza Panorama para gestionar los cortafuegos, genere y cargue el archivo de Asistencia técnica de Panorama.
- **Logs del cortafuegos**: Exporte logs desde el cortafuegos y los dispositivos Panorama de dos horas antes de la actividad sospechosa. Antes de exportar los logs, compruebe que la El ajuste de fila del CSV esté en el valor máximo de 65535 filas [**Device (Dispositivo)** > **Setup (Configuración)** > **Management (Administración)** > **Logging and Reporting Settings (Configuración de log e informes)**]. Si el valor es

menor, Aumente al máximo de 65535 filas. Exporte logs para cada una de las siguientes categorías básicas de logs (si los logs están habilitados) en función de la información de la dirección IP y los detalles de la marca de tiempo (puede filtrar logs para mostrar las entradas de logs en función de la dirección IP y la hora):

- Logs de filtrado de datos
- Logs de tráfico
- Logs de amenazas
- Logs de filtrado de URL
- Logs de User-ID (si sospecha que hay movimiento lateral involucrado)
- Logs de envíos a Wildfire

Es importante comprender la política de retención de logs y la capacidad de retención de logs de su implementación para garantizar que no se examinen datos relevantes. Es posible que los administradores deban tomar medidas adicionales, como exportar datos desde el cortafuegos u otros servidores de logs para garantizar la continuidad y la integridad de los datos durante la investigación.

Más formas de identificar datos significativos sobre actividades sospechosas:

- **Use el Centro de control de aplicaciones (ACC)** . El ACC puede mostrar picos de tráfico, anomalías y cambios en el tiempo antes, durante y después de la actividad sospechosa.
- **Utilice el Informe del supervisor de amenazas** para ver las principales amenazas durante el período anterior, durante y después de la actividad sospechosa.

Activación de la Garantía de seguridad

Después de recopilar datos sobre la actividad sospechosa para garantizar el análisis oportuno de la información relevante, está listo para activar la Asistencia de seguridad. Puede activar la Asistencia de seguridad de dos maneras:

- Inicie sesión en el Portal de atención al cliente. Haga clic en **Create a Case (Crear un caso)** para abrir un caso de asistencia. Cuando complete el formulario, seleccione **Threat (Amenaza)**.
- Su ingeniero de ventas (SE) puede abrir un caso de asistencia en su nombre.