paloalto TECHDOCS

Prácticas recomendadas de la Política de seguridad

Contact Information

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

About the Documentation

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

Copyright

Last Revised

July 5, 2023

Table of Contents

Prácticas recomendadas de la Política de seguridad

La Política de seguridad determina qué tráfico permite en su red y cómo tratar dicho tráfico. Las prácticas recomendadas de la Política de seguridad limitan el tráfico que usted permite a solo tráfico autorizado requerido para su negocio y al tráfico tolerado para sus empleados. Esto reduce la superficie de ataque y ayuda a proteger su red y sus activos comerciales. La perspectiva de este documento es qué hacer para lograr la mejor seguridad de la red, dependiendo de que su empresa se base primero en la seguridad o en la disponibilidad de misión crítica.

Las prácticas recomendadas de la Política de seguridad siguen el principio de privilegio mínimo, lo que significa que solo las personas que necesitan acceso a aplicaciones, datos e infraestructura específicos tienen acceso, y que el tráfico se descifra, inspecciona y registra adecuadamente para proteger los activos, la propiedad intelectual y otras cosas que son críticas para su negocio. Todos los demás accesos aumentan el riesgo sin alcanzar los objetivos empresariales.

Este libro contiene las prácticas recomendadas simplificadas y paso a paso sobre cómo:

- Planificar la Política de seguridad
- Implementar la Política de seguridad
- Mantener la Política de seguridad

Los pasos que requieren configuración o para los que hay información conceptual en profundidad incluyen enlaces a la documentación correspondiente para obtener detalles. Obtenga información sobre las características, capacidades y funcionamiento de los productos de Palo Alto Networks en las guías del administrador del producto, notas informativas, guías de actualización, guías de interconexión, etc., que están disponibles en la página de inicio de la documentación técnica:

- PAN-OS
- Panorama
- Panorama Managed Prisma Access (incluida la documentación de la aplicación GlobalProtect)
- Cloud Managed Prisma Access
- Prisma SD-WAN
- Servicios de seguridad en la nube
- Motor de identidad en la nube
- GlobalProtect
- VM-SERIES
- CN-Series
- Centro de ayuda de Cortex
- Guías de hardware de cortafuegos y dispositivos

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

Planificación de las prácticas recomendadas de la Política de seguridad

Antes de crear reglas de políticas de seguridad de prácticas recomendadas, asegúrese de comprender las prácticas recomendadas para planificar una red segura, especialmente los principios de Zero Trust Network Access (ZTNA). La Política de seguridad define el tráfico que permite y bloquea. Sin embargo, se necesita un conjunto completo de herramientas y servicios para proteger completamente su red, incluidas herramientas que proporcionan:

- Visibilidad, como descifrado, App-ID, User-ID y Device-ID.
- Prevención avanzada de amenazas, como protección frente a vulnerabilidades, antivirus, antispyware, bloqueo de archivos, sandboxing, prevención de pérdida de datos (DLP), seguridad DNS y más.
- IoT Security para controlar dispositivos no gestionados y SaaS Security para controlar aplicaciones SaaS (CASB de nueva generación).

Asegúrese de tener el conjunto de herramientas adecuado para proteger su red y utilizarlo en y con la Política de seguridad.

STEP 1 | No puede defenderse de amenazas que no puede ver. Descifre todo el tráfico que pueda, de acuerdo con el cumplimiento normativo, las regulaciones locales, las regulaciones de privacidad y las consideraciones comerciales para obtener visibilidad del tráfico de forma que pueda inspeccionarlo y prevenir amenazas. Para el descifrado proxy SSL de reenvío (saliente), implemente primero User-ID y filtrado de URL para que pueda orientar el descifrado de manera efectiva. Parte del tráfico no se puede descifrar por motivos técnicos tales como certificados integrados, autenticación de clientes y certificados integrados en dispositivos IoT.

Si no descifra el tráfico, el cortafuegos no podrá identificar las aplicaciones de forma granular. Por ejemplo, el cortafuegos puede ver que la aplicación contenedor es Facebook, pero no puede ver la aplicación funcional, por lo que no sabe ni puede controlar si el usuario está cargando, descargando, publicando, etc. en Facebook. El cortafuegos tampoco puede ver ni inspeccionar la carga útil, por lo que no tiene visibilidad para defenderse frente a contenido malicioso. Para aprovechar al máximo sus otras suscripciones y lograr la mejor protección, debe descifrar el tráfico para obtener visibilidad de dicho tráfico.

El descifrado no requiere una licencia, pero para descifrar el tráfico saliente debe añadir una licencia de filtrado de URL, Advanced URL Filtering, para que pueda adoptar un enfoque granular para el descifrado, y elegir fácilmente qué tipos de tráfico descifrar y que no. El filtrado de URL le permite excluir categorías que no debe descifrar por motivos legales, personales, regulatorios o de otro tipo. El filtrado de URL también le permite bloquear el acceso de los usuarios a sitios web maliciosos.

Además, descifre el tráfico entrante para proteger servidores críticos y descifre el tráfico de proxy SSH para evitar el tráfico de gestión malicioso.

Siga las prácticas recomendadas de descifrado para prepararse, implementar y mantener el descifrado.

STEP 2 | Vea los procesos de planificación e implementación a través de una lente de acceso con privilegios mínimos y acceso a la red Zero Trust.

Comprenda quién necesita utilizar qué aplicaciones para acceder a qué datos y a qué infraestructura. Esto le permite crear reglas de Política de seguridad que permiten que solo las personas que necesitan

acceso con fines comerciales accedan únicamente a los datos y la infraestructura necesarios, mientras se bloquean todos los demás accesos.

Utilice los atributos disponibles en la Política de seguridad para definir el acceso con privilegios mínimos: usuarios, dispositivos, aplicaciones, origen y destino, servicio y URL (para el tráfico saliente, con el descifrado habilitado para que el cortafuegos tenga visibilidad de cada aplicación funcional, no solo de la aplicación contenedor).

STEP 3 | Obtenga las suscripciones adecuadas para su empresa para lograr la mejor estrategia de seguridad y prevención de amenazas.

- Advanced URL Filtering: servicio proporcionado en la nube que permite el acceso seguro a sitios web, protege a los usuarios de sitios peligrosos y ayuda a prevenir ataques de phishing de credenciales.
- Advanced Threat Prevention o servicio anterior de protección frente a amenazas activo: la prevención avanzada frente a amenazas, Advanced Threat Prevention, proporcionada en la nube utiliza modelos de aprendizaje profundo y aprendizaje automático en línea para el control en tiempo real de amenazas evasivas y de comando y control (C2) del primer día, e incluye todas las funciones estándar de Threat Prevention. La prevención de amenazas, Threat Prevention, estándar protege contra C2, malware y vulnerabilidades.

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

  Siga las prácticas recomendadas para las Actualizaciones de contenido de amenazas para asegurarse de tener las protecciones más recientes.
- DNS Security: (debe adquirir una licencia de Advanced Threat Prevention o tener una licencia de Threat Prevention anterior activa y una licencia de DNS Security para activarla) servicio en la nube que identifica y bloquea amenazas en el tráfico DNS e impide la conexión a sitios DNS maliciosos y que además se actualiza constantemente para prevenir nuevos tipos de ataques basados en DNS.
- Enterprise Data Loss Prevention (DLP): servicio proporcionado en la nube que protege los datos en todas las redes, nubes y usuarios empresariales, y que permite el cumplimiento de las normativas de seguridad de datos.
- Cortex Data Lake (CDL): almacenamiento de logs basado en la nube que se amplía a la par que su volumen de logs e ingiere logs de cortafuegos de nueva generación, Panorama, Prisma Access

y Cortex XDR. La mayoría de las aplicaciones de Cortex utilizan CDL para acceder, analizar e informar sobre los datos de red registrados.

- WildFire: entorno de análisis privado o basado en la nube que identifica malware conocido y desconocido (nuevo), y genera firmas que el cortafuegos utiliza para identificar y bloquear el tráfico malicioso.
- SaaS Security: servicio prestado en la nube que protege sus aplicaciones SaaS autorizadas con licencias que pueden ser independientes o en grupo:
  - La licencia de Data Security incluye SaaS Security API y Enterprise DLP.
  - La licencia complementaria SaaS Security Inline funciona con CDL para descubrir y controlar todas las aplicaciones SaaS en su red, incluidas las aplicaciones no autorizadas por TI, y habilita la Recomendación de políticas para SaaS para el administrador del cortafuegos.
  - Enterprise DLP para la protección frente a la pérdida de datos en aplicaciones SaaS.
- IoT Security: descubre y protege los dispositivos de IoT en su red y habilita recomendaciones automáticas de reglas de políticas de IoT para el administrador del cortafuegos. Siga las prácticas recomendadas de IoT Security para la planificación, implementación y supervisión.
- GlobalProtect: proporciona capacidades más allá de las funciones de VPN gratuitas, incluida la aplicación móvil de GlobalProtect, comprobaciones de HIP, VPN sin cliente y más.

STEP 4 | Revise su plan de segmentación de red.

Para Panorama Managed Prisma Access, en realidad solo hay dos zonas, trust y untrust (fiable y no fiable), y usted asigna todas las zonas de Panorama a la zona fiable de Prisma o a la zona de no fiable de Prisma.

En Panorama y cortafuegos, si una zona no es lo suficientemente granular e incluye dispositivos, usuarios y aplicaciones que requieren un tratamiento de seguridad diferente, considere rediseñar sus zonas para segmentar la red de una manera más granular. Coloque usuarios, aplicaciones y dispositivos que requieran un tratamiento similar en la misma zona. Las zonas pequeñas son más fáciles de defender que las zonas grandes.

En algunos entornos de nube, la arquitectura puede limitar la cantidad de zonas que puede configurar.

Siga las prácticas recomendadas de protección DoS y de zonas para evitar ataques de inundación y proteger los dispositivos en cada zona y los buffers de su cortafuegos.

Para Cloud Managed Prisma Access, base la microsegmentación en la identidad.

STEP 5 | Defina qué aplicaciones necesita permitir para fines comerciales (aplicaciones autorizadas) y qué aplicaciones permitir para otros fines (aplicaciones toleradas).

Utilice App-ID en la Política de seguridad (no se requiere suscripción) para identificar tanto las aplicaciones contenedor como sus aplicaciones funcionales (por ejemplo, no solo “facebook” sino “facebook-post”, “facebook-download”, etc.). Si utiliza SaaS Security, utilice App-ID Cloud Engine (ACE) para identificar aplicaciones en la nube (requiere suscripción a SaaS Security).

El cortafuegos da permiso a las aplicaciones que usted especifica en las reglas de la Política de seguridad cuya **Action (Acción)** es **Allow (Permitir)** y bloquea las aplicaciones especificadas en las reglas cuya **Action (Acción)** deniega, elimina o restablece el tráfico, según los criterios de la regla. El tráfico debe cumplir todos los criterios de una regla para coincidir con la regla. Si una aplicación no

coincide con ninguna regla, las dos reglas predeterminadas en la parte inferior de la base de reglas de la Política de seguridad controlan el tráfico. El tráfico entre zonas (el origen y el destino están en zonas diferentes) está denegado de forma predeterminada. El tráfico dentro de la zona (el origen y el destino están en la misma zona) está permitido de forma predeterminada.

Comunicar la política de acceso para que los empleados comprendan por qué es posible que no puedan acceder a determinadas aplicaciones.

STEP 6 | Identificar a todos los usuarios. Controle quién tiene acceso a qué aplicaciones y dispositivos en la Política de seguridad para garantizar que una política coherente siga a cada usuario en todas las partes de la red.

User-ID (no se requiere suscripción) combina información del usuario de múltiples fuentes para identificar a todos los usuarios en su red. Para ayudar a garantizar que la identificación del usuario sea coherente y se pueda ampliar a toda su red, utilice Cloud Identity Engine (CIE) (no se requiere suscripción) como fuente única y total para User-ID. CIE recopila y sincroniza datos de usuario de fuentes en toda su red. Todos los cortafuegos extraen exactamente la misma información de usuario de CIE, ya sea que estén en unas instalaciones o en la nube. CIE también proporciona autenticación junto con la mayoría de los principales proveedores de identidad (IdP), como Okta, Azure AD, PingID, etc.

En PAN-OS 10.2 y versiones anteriores, CIE proporciona servicios de sincronización de directorios (DSS) y autenticación en la nube (CAS). A partir de PAN-OS 11.0, también puede utilizar CIE como puntos de redistribución.

Al configurar grupos de usuarios, piense en quién necesita acceder a los mismos recursos de la misma manera para los mismos fines comerciales y siga las prácticas recomendadas para la asignación de grupos de usuarios y las prácticas recomendadas para grupos de usuarios dinámicos (DUG).

Utilice la VPN GlobalProtect en modo Siempre activado para obtener la mayor seguridad y una identificación de usuario fiable, si es posible. Utilice GlobalProtect para acceder de forma remota y con puertas de enlace internas para recopilar información de User-ID sin importar dónde se encuentren sus usuarios.

STEP 7 | Planifique adjuntar los perfiles de seguridad o el grupo de perfiles de seguridad adecuados a cada regla de Política de seguridad que permita el tráfico. (Si una regla bloquea el tráfico, el cortafuegos no inspecciona el tráfico bloqueado).

Los grupos de perfiles de seguridad son grupos de perfiles adaptados para un propósito particular que se aplican a las reglas de la Política de seguridad en lugar de aplicar cada perfil individualmente. Esto ahorra tiempo y ayuda a evitar una configuración errónea accidental.

STEP 8 | Planifique cómo almacenar logs (en CDL, en Recopiladores de logs, etc.) y a qué administradores notificar para los diferentes tipos y gravedades de eventos de registro de logs. Planifique para tener suficiente capacidad de almacenamiento de logs para permitir la investigación de eventos después de que ocurran.

STEP 9 | Utilice un único panel de administración, como Panorama o Cloud Managed Prisma Access, para gestionar su implementación y lograr una seguridad más sencilla y coherente.

STEP 10 | Siga las prácticas recomendadas de Acceso administrativo para garantizar el acceso con privilegios mínimos para los administradores de Panorama y cortafuegos.

STEP 11 | Las configuraciones del día 1, que están disponibles en el Portal de atención al cliente [**Tools (Herramientas)** > **Run Day 1 Configuration (Ejecutar configuración inicial)**] y que requieren inicio de sesión de soporte, son plantillas que proporcionan un modelo de configuración independiente del caso de uso para iniciar su camino hacia el acceso con privilegios mínimos. Las configuraciones del día 1 le ayudan a implementar las prácticas recomendadas básicas de seguridad de la red de inmediato, incluso para elementos críticos como actualizaciones dinámicas, perfiles de seguridad, registros y más.

Implementación de las prácticas recomendadas de la Política de seguridad

La implementación de las prácticas recomendadas de políticas de seguridad incluye:

- Prácticas recomendadas de las reglas de la Política de seguridad: se centra en todos los aspectos de la creación de reglas de políticas de seguridad, desde quién puede acceder a qué aplicaciones y recursos de qué manera hasta la aplicación de perfiles de amenazas que ayudan a proteger el tráfico del malware.
- Prácticas recomendadas de la base de reglas de la Política de seguridad: se centra en la secuencia de reglas de la Política de seguridad en la base de reglas y cómo eso afecta al tráfico que permite y bloquea.
- Prácticas recomendadas de Policy Optimizer: se centra en el uso de Policy Optimizer para ajustar y mantener la base de reglas.
- Prácticas recomendadas de App-ID Cloud Engine: se centra en cómo utilizar los App-ID en la nube en la Política de seguridad y cómo automatizar la adición de nuevos App-ID en la nube a la base de reglas. (App-ID Cloud Engine requiere una suscripción SaaS Security Inline).
- Prácticas recomendadas de recomendaciones de políticas se centra en las recomendación de políticas de SaaS y políticas de IoT. (La recomendación de políticas de SaaS requiere una suscripción a SaaS Security Inline y la recomendación de políticas de IoT requiere una suscripción a IoT Security).

Al planificar e implementar, tenga en cuenta estos principios:

- El principio de acceso con privilegios mínimos; limite el acceso únicamente a las personas adecuadas utilizando únicamente las aplicaciones adecuadas, desde únicamente las fuentes adecuadas hasta los destinos adecuados.
- Siga las Prácticas recomendadas de descifrado. Descifre todo el tráfico que sus consideraciones comerciales, regulaciones locales y de privacidad y el cumplimiento legal le permitan para obtener la máxima visibilidad del tráfico de forma que pueda inspeccionarlo y controlarlo. Para el descifrado proxy SSL de reenvío (saliente), implemente primero User-ID y filtrado de URL para que pueda orientar el descifrado de manera efectiva.

  

  Para el descifrado de salida, obtenga una licencia de filtrado de URL avanzado, Advanced URL Filtering, para que cuando el descifrado exponga un sitio web malicioso, el filtrado de URL pueda bloquear el acceso a él.

  

  Parte del tráfico no se puede descifrar por razones técnicas, debido a certificados anclados, autenticación de clientes, certificados integrados en dispositivos IoT, etc.
- Inspeccione todo el tráfico en ambas direcciones en busca de amenazas. No confíe en nada implícitamente.
- Automatice tanto como sea posible para ayudar a garantizar que la Política de seguridad se mantenga actualizada mediante grupos de direcciones dinámicas (DAG), listas dinámicas externas (EDL)y funciones de Supervisión de VM.

  Utilice el etiquetado automático para automatizar acciones de seguridad para usuarios y dispositivos en función de eventos de log. El etiquetado automático le permite automatizar las acciones a realizar cuando se produce un evento de log, por ejemplo, poner en cuarentena un dispositivo potencialmente infectado u obligar a un usuario a utilizar la autenticación MFA.

- Evite la sobrecarga de la configuración:
  - Reutilice objetos como perfiles de seguridad y grupos de perfiles, etiquetas, grupos de aplicaciones, filtros de aplicaciones, grupos de usuarios y grupos de direcciones. En Panorama, utilice objetos compartidos para evitar configurar los mismos objetos para varios grupos de dispositivos.
  - Antes de añadir una nueva regla de política a la base de reglas, verifique las reglas existentes para ver si puede añadir nuevas aplicaciones, usuarios o dispositivos a las reglas existentes en lugar de crear más reglas similares.

    Vea si una regla existente es la misma excepto por uno de los siguientes objetos: zona de origen, zona de destino, dirección IP de origen, dirección IP de destino, aplicación, puerto de servicio o usuario. Si solo uno de esos objetos es diferente, añada el nuevo objeto a la regla existente en lugar de crear una regla nueva.

    Por ejemplo, desea permitir una nueva aplicación de contabilidad. Cuando mira en la base de reglas existente, encuentra una regla para una aplicación de contabilidad diferente que permite el acceso desde el mismo origen al mismo destino, para los mismos grupos de usuarios, utilizando el puerto predeterminado de la aplicación. En lugar de escribir una nueva regla para la nueva aplicación, simplemente añada la nueva aplicación a la regla existente.

    

    Este método también funciona bien para consolidar reglas existentes.

  - Para el tráfico saliente, cree una regla basada en categorías de URL para múltiples aplicaciones que requieran el mismo tratamiento de seguridad. Por ejemplo, para permitir todo el tráfico de servicios financieros de bajo riesgo (suponiendo que desee inspeccionar y registrar el tráfico de la misma manera), cree una regla de permisos que especifique las categorías de URL de **financial-services (servicios financieros)** y **low risk (bajo riesgo)**.
  - Utilice Policy Optimizer para eliminar reglas no utilizadas.
- Utilice Panorama o Cloud Managed Prisma Access para gestionar implementaciones de cortafuegos de modo que pueda usar grupos de dispositivos para aplicar políticas de seguridad coherentes a cortafuegos individuales o a grupos de cortafuegos.

  Utilice reglas previas y reglas posteriores de manera correcta:

  - Reglas previas: los cortafuegos evalúan las reglas previas antes que las reglas definidas localmente y las reglas posteriores. (Las reglas definidas localmente en cortafuegos individuales se aplican solo a dichos cortafuegos). Coloque políticas que se apliquen a todas las implementaciones de cortafuegos en las reglas previas, como permitir DNS y otros servicios críticos y use EDL de amenazas definidas previamente para bloquear direcciones IP maliciosas y de alto riesgo conocidas.
  - Reglas posteriores: los cortafuegos evalúan estas reglas después de las reglas previas y de las reglas definidas localmente.

  

  *En las reglas de política de seguridad de Panorama, utilice la pestaña **Target (Destino)** para excluir cortafuegos específicos o subconjuntos de grupos de dispositivos de la regla [**Target to all but these specified devices (Destinar a todos menos a estos dispositivos indicados)**]. Esto le permite crear una regla amplia más arriba en la jerarquía en lugar de crear varias reglas similares más abajo en la jerarquía para hacer la excepción.*
- La política Anulación de aplicaciones no es la misma que la Política de seguridad de capa 7. No la use a menos que sea necesario porque la Anulación de aplicaciones elimina muchos controles de seguridad inherentes a la plataforma de Palo Alto Networks. La anulación de aplicaciones no le

permite inspeccionar el tráfico de capa 7, utilizar perfiles de seguridad para proteger el tráfico frente a amenazas ni utilizar App-ID, por lo que aumenta el riesgo. En la mayoría de los casos, es mejor crear una Aplicación personalizada o utilizar un tiempo de espera de servicio personalizado en vez de utilizar la Anulación de aplicación.

Revise su base de reglas existente. Si tiene alguna regla de Anulación de aplicación para el tráfico que no sea SMB o SIP, convierta la regla en una regla basada en App-ID para que pueda descifrar e inspeccionar el tráfico en la capa 7 y evitar amenazas. Si la regla es para tráfico SMB o SIP, asegúrese de que siga el principio de acceso con privilegios mínimos y que sea lo más restrictiva posible.

Prácticas recomendadas de las reglas de la Política de seguridad

Esta sección cubre la creación de reglas de la Política de seguridad, desde quién puede acceder a qué aplicaciones y recursos y de qué manera hasta la aplicación de perfiles de amenazas que ayudan a proteger el tráfico frente al malware.

Las reglas de la Política de seguridad definen criterios de coincidencia de tráfico, incluidas aplicaciones, usuarios, dispositivos, origen y destino, URL y servicios (puertos). La combinación de criterios coincidentes añade un contexto más granular a una regla, reduce el alcance de la regla y reduce la superficie de ataque. Los criterios coincidentes le permiten definir el tráfico exacto que desea controlar con la regla y cumplir con los principios de acceso a la red de confianza ceroZero Trust Network Access (ZTNA).

Las reglas de la Política de seguridad también definen acciones a tomar en el tráfico que coincide con los criterios de una regla, incluido si permitir o denegar el tráfico, creación de logs y reenvío de logs, inspección de amenazas y programación.

Cree reglas de la Política de seguridad lo más específicas posible para aplicar el principio de acceso con privilegios mínimos y segmentar la red.

- Conceptos críticos para la Política de seguridad: Cómo funcionan las reglas de la Política de seguridad.
- Nombre de regla, descripción, comentarios de auditoría y etiquetas: Prácticas recomendadas para la gestión de reglas de la Política de seguridad.
- Orígenes y destinos: Prácticas recomendadas para aplicar el principio de acceso con privilegios mínimos para restringir orígenes y destinos de tráfico.
- Aplicaciones y servicios: Prácticas recomendadas para añadir aplicaciones a las reglas.
- Acceso al sitio web (filtrado de URL): Prácticas recomendadas sobre cómo permitir el acceso de los usuarios a sitios web externos.
- Acciones de política y otras configuraciones: Prácticas recomendadas sobre cómo permitir o denegar tráfico, y aplicar QoS.
- Registro de logs y reenvío de logs: Prácticas recomendadas para registrar el tráfico y reenviar logs para su almacenamiento y análisis a largo plazo.
- Perfiles de seguridad: Prácticas recomendadas para aplicar perfiles de seguridad a reglas de la Política de seguridad.

Conceptos críticos para la Política de seguridad

Para crear una política de seguridad eficaz, es importante comprender conceptos críticos sobre lo que hacen las reglas de la Política de seguridad, cómo funcionan en la base de reglas de la Política de seguridad, cómo el tráfico empareja las reglas y las prácticas recomendadas para la creación de reglas.

- Descifre todo el tráfico permitido por las regulaciones locales, el cumplimiento, los requisitos comerciales y las consideraciones de privacidad. Para el descifrado proxy SSL de reenvío (saliente), implemente primero User-ID y filtrado de URL para que pueda orientar el descifrado de manera efectiva. Descifrar el tráfico proporciona visibilidad para que el cortafuegos pueda identificar aplicaciones funcionales (por ejemplo, no solo facebook sino facebook-post, facebook-download, facebook-file-sharing, etc.), identificar sitios web y aplicar perfiles de amenazas para inspeccionar y prevenir amenazas en el tráfico. Descifrar el tráfico le permite obtener la mayor protección y prevención de sus suscripciones frente a amenazas.
- **Reglas de permiso vs. reglas de bloqueo**: la Política de seguridad en los cortafuegos de Palo Alto Networks se basa en permitir explícitamente el tráfico en las reglas de políticas y denegar todo el tráfico que no permita explícitamente (lista de permitidos). El tráfico que no permite explícitamente se deniega implícitamente. El objetivo es permitir solo las aplicaciones, usuarios y dispositivos que desee en su red y dejar que el cortafuegos bloquee automáticamente lo que no desee.

  A medida que avance hacia una Política de seguridad basada en listas de permitidos, utilice reglas de bloqueo para impedir el acceso a direcciones IP, sitios web y aplicaciones de riesgo. Cree y pruebe reglas de bloqueo basadas en listas dinámicas externas (EDL) predefinidas para bloquear direcciones IP protegidas, direcciones IP de alto riesgo y direcciones IP maliciosas conocidas que se esconden dentro de categorías de aplicaciones que de otro modo serían benignas, y para evitar la autenticación en una URL o dominio malicioso. Utilice el Filtrado de URL avanzado para bloquear el acceso a sitios web peligrosos.

  > *Tenga especial cuidado con las aplicaciones para compartir archivos porque los delincuentes pueden utilizarlas para filtrar datos. Bloquee la mayoría de las aplicaciones para compartir archivos. Para las aplicaciones para compartir archivos que necesita para el desarrollo de su negocio, permita el acceso solo a los usuarios que necesitan esas aplicaciones con fines comerciales.*

  Para obtener la mayor seguridad, permita solo aplicaciones utilizadas con fines comerciales. Sin embargo, la mayoría de las empresas deben permitir algunas aplicaciones no comerciales para los empleados (aplicaciones toleradas). Considere qué aplicaciones toleradas permitir y pregúntese si esas aplicaciones representan alguna amenaza para la organización, como la capacidad de cargar o descargar datos. Descifre e inspeccione todo el tráfico que pueda en busca de amenazas.
- Las reglas de la Política de seguridad son específicas. Si el tráfico no coincide con todos los criterios especificados en una regla de Política de seguridad, el tráfico no coincide con la regla. Por ejemplo, si una regla especifica un usuario particular, una aplicación y un origen y destino, el tráfico debe cumplir todos esos criterios para cumplir con la regla. Si el usuario, el origen y el destino coinciden pero la aplicación no coincide, entonces el tráfico no coincide con la regla.
- Las reglas de la Política de seguridad segmentan su red definiendo quién tiene acceso a qué aplicaciones e infraestructura. Las reglas segmentan la red definiendo el origen, el destino, el usuario, el dispositivo, el servicio y la URL.
- Las reglas de la Política de seguridad aplican todos los perfiles de prevención de amenazas de Threat Prevention adjuntos al tráfico que coincide con las reglas.
- Las reglas de la Política de seguridad están en una base de reglas ordenada (usted elige el orden de las reglas). Los cortafuegos comparan el tráfico con las reglas de la Política de seguridad, comenzando con la primera regla en la base de reglas de la política de seguridad y avanzando hasta la última regla de la base de reglas. Cuando el tráfico coincide con los criterios de una regla, el cortafuegos toma la Acción

de la regla sobre el tráfico y no compara el tráfico con ninguna otra regla. Si ninguna regla coincide con el tráfico, el cortafuegos descarta el tráfico (denegación implícita).

- Coloque reglas de la Política de seguridad más específicas y granulares encima de las reglas generales en la base de reglas para evitar que solapen una regla. El solapamiento o superposición se produce cuando una regla amplia que incluye los mismos criterios coincidentes que una regla más específica se coloca más arriba en la base de reglas que la regla específica. En ese caso, el tráfico destinado a coincidir con la regla específica coincide primero con la regla general.
- Si el tráfico no coincide con otras reglas, dos reglas de la Política de seguridad predeterminadas en la parte inferior de la base de reglas descartan automáticamente todo el tráfico entre diferentes zonas [**interzone-default** (predeterminada interzonal)] y permiten automáticamente todo el tráfico entre la misma zona [**intrazone-default** (predeterminada intrazonal). Puede modificar las reglas predeterminadas entre zonas y dentro de la zona para registrar el tráfico, aplicar inspección de amenazas, etc. Si añade una regla que deniega todo el tráfico al principio en la base de reglas (reglas de cortafuegos local o reglas previas y posteriores de Panorama), ningún tráfico coincide con las reglas predeterminadas.
- Aplique el principio de acceso con privilegios mínimos a la construcción de reglas de la Política de seguridad (sea granular y preciso):
  - Controle qué administradores tienen acceso para administrar qué partes de qué cortafuegos y dispositivos Panorama. Prácticas recomendadas para proteger el acceso administrativo
  - Identifique a todos los usuarios (no debe haber usuarios desconocidos en su red), identifique las aplicaciones que desea permitir en su red y conozca su infraestructura (recursos a los que acceden los usuarios y las aplicaciones). Asigne quién necesita acceso a qué aplicaciones y recursos con fines comerciales, de modo que las reglas de su Política de seguridad no permitan accesos innecesarios. Permita el acceso a recursos comerciales y aplicaciones autorizadas solo a los usuarios que necesiten acceso con fines comerciales y permita solo el acceso mínimo requerido.
  - Permita el acceso a aplicaciones no comerciales que la empresa tolere en beneficio de sus empleados.
  - En la mayoría de los casos, utilice reglas de permiso en lugar de reglas de bloqueo: es más preciso y más fácil definir lo que desea permitir en su red y denegar implícitamente el resto que bloquear explícitamente el número cada vez mayor de aplicaciones que no desea en su red.
  - Optimice la base de reglas para editar reglas con aplicaciones no utilizadas y eliminar o deshabilitar reglas que no se utilizan.

Nombre de regla, descripción, comentarios de auditoría y etiquetas

Los campos Nombre, Descripción, Comentarios de auditoría y Etiquetas facilitan la gestión y navegación de la base de reglas de su Política de seguridad y la comprensión de lo que hace cada regla. También ayudan a los administradores nuevos y experimentados a comprender cuándo añadir una nueva aplicación, usuario o grupo de usuarios a una regla existente y cuándo crear una nueva regla.

STEP 1 | **Name (Nombre)**: identifica lo que hace cada regla.

Desarrolle una convención de nomenclatura estándar que utilice términos que faciliten la búsqueda en la base de reglas. Los nombres que muestran claramente a los administradores qué hace cada regla facilitan la comprensión del tráfico que controla cada regla y hacen que la búsqueda de una regla en particular sea más fácil e intuitiva.

STEP 2 | **Description (Descripción)**: describe el propósito de la regla para que cualquiera que examine la base de reglas pueda comprender por qué se creó la regla y el resultado previsto.

Para garantizar que todas las políticas tengan una descripción en PAN-OS y Panorama Managed Prisma Access, habilite **Require description on policies (Requerir descripción en las políticas)** en **Panorama** > **Setup (Configuración)** > **Management (Gestión)** > **Policy Rulebase Settings (Configuración de base de reglas de políticas)** [**Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** > **Policy Rulebase Settings (Configuración de base de reglas de políticas)** en cortafuegos individuales]. Para reglas existentes sin descripción, añada una la próxima vez que edite la regla.

En Cloud Managed Prisma Access, asegúrese de que los administradores introduzcan una descripción.

STEP 3 | **Tags (Etiquetas)**: descriptores de alto nivel para describir componentes basados en flujos, políticas basadas en aplicaciones, servicios internos, grupos de usuarios particulares, lo que tenga sentido para su negocio.

Las etiquetas organizan las políticas en grupos, lo que le permite filtrar y buscar políticas basadas en etiquetas.

Por ejemplo, si crea una etiqueta llamada **`deshabilitada`** y la aplica a todas las reglas deshabilitadas, puede filtrar la base de reglas y ver todas las reglas deshabilitadas según esa etiqueta. Usando la misma etiqueta, puede buscar en la base de reglas las reglas que están etiquetadas como **`deshabilitadas`** pero que se han reactivado filtrando por la etiqueta **`deshabilitada`** y **`núm de ec deshabilitada`**.

Para garantizar que todas las políticas tengan una etiqueta en PAN-OS y Panorama Managed Prisma Access, habilite **Require Tag on policies (Requerir etiqueta en las políticas)** en **Panorama** > **Setup (Configuración)** > **Management (Gestión)** > **Policy Rulebase Settings (Configuración de base de reglas de políticas)** [**Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** > **Policy Rulebase Settings (Configuración de base de reglas de políticas)** en cortafuegos individuales]. Para las reglas existentes sin etiqueta, añada una la próxima vez que edite la regla.

STEP 4 | Evite que los administradores confirmen políticas si no tienen etiquetas ni descripción.

En PAN-OS y Panorama Managed Prisma Access, habilite **Fail commit if policies have no tags or descriptions (Fallo de compilación si las políticas no tienen etiquetas o descripción)** en **Panorama** > **Setup (Configuración)** > **Management (Gestión)** > **Policy Rulebase Settings (Configuración de base de reglas de políticas)** [**Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** > **Policy Rulebase Settings (Configuración de base de reglas de políticas)** en cortafuegos individuales]. Para las reglas existentes, la confirmación falla si no añade una etiqueta y una descripción la próxima vez que edite la regla.

STEP 5 | **Audit Comments (Comentarios de auditoría)**: realiza un seguimiento de los cambios en las reglas y de por qué se realizaron los cambios para tener un historial de los cambios en las reglas y los fundamentos de los cambios. Esto es especialmente útil para documentar reglas que solo se utilizan en caso de recuperación ante desastres o de forma limitada.

En PAN-OS y Panorama Managed Prisma Access, asegúrese de que todas las políticas incluyan comentarios de auditoría, habilite **Require audit comment on policies (Exigir observaciones de auditoría sobre políticas)** en **Panorama** > **Setup (Configuración)** > **Management (Gestión)** > **Policy Rulebase Settings (Configuración de base de reglas de políticas)** [**Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** > **Policy Rulebase Settings (Configuración de base de reglas de políticas)** en cortafuegos individuales] y especifique un comentario de auditoría.

Para las reglas existentes sin comentarios de auditoría, deberá añadir los comentarios la próxima vez que edite la regla.

Los comentarios de auditoría permanecen con la regla de forma permanente. Haga clic en **Audit Comment Archive (Auditar archivo de comentarios)** en la regla para ver el historial, que no se puede eliminar.

Orígenes y destinos

Controlar el origen y el destino del tráfico consiste en seguir el principio de acceso con privilegios mínimos. Cree reglas de políticas de seguridad que especifiquen el origen y el destino exactos del tráfico de las aplicaciones que desea que coincidan con la regla. Permitir el tráfico en la regla desde orígenes y destinos que las aplicaciones no requieren para sus operaciones comerciales aumenta la superficie de ataque, lo que aumenta el riesgo. Limitar estrictamente los orígenes y destinos a aquellos estrictamente necesarios para fines comerciales reduce las superficies de ataque y disminuye el riesgo.

El control granular del origen y destino del tráfico le ayuda a implementar el acceso con privilegios mínimos:

- Orígenes: zonas, direcciones, usuarios y dispositivos, seguridad 5G, suscriptores, equipos y segmento de red.
- Destinos: zonas, direcciones y dispositivos.

En la medida de lo posible, utilice objetos de grupo de direcciones y de grupos de usuarios en lugar de direcciones y usuarios individuales para reducir el número de objetos de origen y destino. Esto simplifica la política y la hace más fácil de entender. Limite el número total de objetos de origen y destino para mayor claridad de la base de reglas.

STEP 1 | En PAN-OS, especifique las zonas de origen y destino lo más estrictamente posible para evitar el acceso innecesario a datos y aplicaciones.

Dedicar zonas para objetivos específicos, como una zona para todos los servidores web, facilita la creación de políticas granulares porque todos los servidores de la zona generalmente requieren la misma política de seguridad.

Panorama Managed Prisma Access utiliza dos zonas, trust y untrust, fiable y no fiable. Asigne zonas de Panorama a la zona trust de Prisma o a la zona untrust de Prisma.

Cloud Managed Prisma Access utiliza tres zonas: fiable, no fiable y VPN sin cliente, que se asigna a la zona fiable, trust, de forma predeterminada. En muchas integraciones SD-WAN de terceros, en el Visor de logs, la zona de origen utiliza el nombre de la red remota.

STEP 2 | Especifique las direcciones de origen y destino lo más estrictamente posible para evitar el acceso innecesario a datos y aplicaciones. Utilice grupos de direcciones en lugar de direcciones individuales tanto como sea posible para simplificar la política. Si la regla es para todos los dispositivos en una zona, para el tráfico entrante especifique la dirección de destino como **any (cualquiera)** y para el tráfico saliente especifique la dirección de origen como **any (cualquiera)**.

- Utilice objetos de dirección FQDN para hacer referencia a sistemas internos de modo que cuando las direcciones IP del sistema cambien, el cambio no afecte la política.

- Utilice grupos de direcciones dinámicas (DAG) en la política para adaptarse automáticamente a los cambios en las funciones del servidor o en la estrategia de seguridad en función de los eventos de registro de logs y el etiquetado automático. Piense en cómo agrupar servidores y desarrolle una estrategia de etiquetado que tenga sentido para su negocio.

  Cuando se produce un evento de registro específico, el cortafuegos mueve las direcciones IP de un DAG a otro DAG según el etiquetado automático. Los DAG se actualizan automáticamente y no requieren una acción de confirmación. Esto le permite tomar acciones de seguridad automatizadas, como mover un servidor o terminal potencialmente infectado desde un DAG en una regla de política que permite el acceso a recursos críticos a un DAG en una regla de política que bloquea ese acceso (poner en cuarentena un dispositivo).
- En entornos de centros de datos con automatización, utilice los DAG para controlar el acceso de las máquinas virtuales a medida que el centro de datos activa y desactiva los servidores virtualizados. Registre etiquetas dinámicamente utilizando la API XML nativa o el agente de supervisión de VM en el cortafuegos.
- En entornos de centros de datos, la segmentación combinada con la automatización puede dificultar la gestión de direcciones IP individuales. Como último recurso, si el entorno es demasiado difícil de gestionar, utilice subredes, pero éste es un método menos seguro.
- Utilice listas dinámicas externas (EDL) predefinidas de Palo Alto Networks como el origen o destino para bloquear el tráfico hacia y desde direcciones IP de alto riesgo, protegidas y otras direcciones IP maliciosas.
- Si el cumplimiento, la política comercial u otros motivos requieren que bloquee regiones geográficas, especifique la región o regiones como la dirección. (Para el tráfico entrante, especifique la región geográfica como origen y **any (cualquiera)** como destino. Para el tráfico saliente, especifique **any (cualquiera)** como origen y la región geográfica como destino).

STEP 3 | Especifique los usuarios de origen con User-ID para que la Política de seguridad sea válida tanto para el acceso local como remoto. La identificación coherente de los usuarios es fundamental para garantizar una política coherente independientemente de la ubicación del usuario y el método de conexión.

- Cree grupos de usuarios según el contexto, *¿qué debe hacer el usuario con fines comerciales? ¿Cuáles son los requisitos de acceso comunes?* Este punto de vista agrupa a los usuarios por

recursos a los que necesitan acceder y aplicaciones que necesitan usar para que pueda crear grupos lógicos y aplicarles políticas.

Haga que el equipo de seguridad de la red trabaje con el equipo que controla los grupos de usuarios para ayudar a garantizar que las agrupaciones tengan sentido para los controles de seguridad.

Especifique usuarios individuales en la política solo cuando no pueda usar grupos. Por ejemplo, su director ejecutivo y algunos otros ejecutivos de alto nivel podrían necesitar varios privilegios de acceso que otros usuarios y grupos no deberían tener.

- Si su implementación lo permite, utilice Cloud Identity Engine (CIE) para:
  - Sumar todas las fuentes de User-ID en su red, tanto en la nube como en las instalaciones.
  - Sincronizar las fuentes del directorio.
  - Proporcionar información de User-ID coherente en toda la red.

  El User-ID coherente permite que la política siga a los usuarios en todas partes de la red.

  

  CIE proporciona autenticación mediante la integración con proveedores de identidad como Okta, Azure AD y muchos otros.
- GlobalProtect es la fuente de asignación de User-ID con la información de usuario más precisa y completa, y la mayor precisión (también hay muchas otras posibles fuentes de asignación de User-ID).
- Utilice grupos de usuarios dinámicos (DUG) en la política para corregir automáticamente el comportamiento anómalo de los usuarios y la actividad maliciosa en función de los eventos de registro y etiquetado automático. Los DUG funcionan de manera similar a los DAG. Piense en qué actividades justifican la cuarentena o el acceso restringido y desarrolle una estrategia de etiquetado que tenga sentido para su negocio.

  Utilice también DUG para permitir el acceso periódico a grupos de usuarios. Por ejemplo, un DUG puede permitir el acceso para auditores (según lo definido por un grupo de usuarios para auditores) durante las auditorías trimestrales y bloquear el acceso en cualquier otro momento.
- En la configuración de la regla de la Política de seguridad, además de especificar usuarios y grupos particulares, puede especificar si la regla se aplica a **any (cualquier)** usuario, usuarios con **pre-logon (pre-inicio de sesión)**, **known-user (usuarios conocidos)** (autenticados) o **unknown (desconocidos)** (no autenticados):
  - Utilice **any (cualquier)** para reglas que se aplican a todos los usuarios de la red, por ejemplo, acceso a servicios básicos como DNS, NTP, OCSP, etc.
  - No permita usuarios **unknown (desconocidos)** en su red. Cree una regla para bloquear usuarios desconocidos. De forma alternativa, utilice **unknown (desconocido)** para el acceso de invitados siempre que no se permita el acceso a su red corporativa.
  - La VPN de acceso remoto con inicio de sesión previo es específica para los usuarios de GlobalProtect. Establece un túnel VPN antes de que el usuario inicie sesión en el dispositivo para autenticar el endpoint y permitir el acceso a servicios específicos como DHCP, DNS, etc., y requiere la instalación de certificados de máquina en cada endpoint. Las reglas de política que permiten el acceso de usuarios con "prelogon" deben permitir el acceso solo a los servicios de

autenticación de máquinas y a los servicios de red necesarios. Deniegue todos los demás accesos a los usuarios con "prelogon", o pre-inicio de sesión.

El principio general es el acceso con privilegios mínimos. Permita el acceso solo a usuarios y grupos que requieran acceso a aplicaciones y recursos con fines comerciales.

- Siga las Prácticas recomendadas de User-ID

STEP 4 | En Reglas de la Política de seguridad que rigen los dispositivos IoT (IoT Security requiere una suscripción), especifique los dispositivos IoT mediante Device-ID (PAN-OS 10.0 y posteriores).

Los objetos de dispositivo definen los Device-ID de dispositivos IoT e identifican los dispositivos de origen de la misma manera que el User-ID identifica a los usuarios de origen. Los objetos de dispositivo tienen seis métricas para usar como criterios de coincidencia. Un dispositivo debe coincidir con todas las métricas configuradas para coincidir con un Device-ID. En la mayoría de los casos, basta con definir una o dos métricas. Cuantas más métricas defina, mayores serán las posibilidades de que el filtro sea demasiado específico y no coincida con los dispositivos que desea que coincidan. Comprenda qué información envían los dispositivos al cortafuegos para saber qué métricas configurar para definir el objeto del dispositivo (no todos los dispositivos transmiten todas las métricas). Los siguientes comandos operativos muestran la información que los dispositivos IoT envían al cortafuegos:

- **`> show iot ip-device-mapping-mp all`**: vea todas las asignaciones de direcciones IP a dispositivos en el cortafuegos.
- **`> show iot ip-device-mapping-mp ip <ip-address>`**: permite ver la asignación de dirección IP a dispositivo para una dirección IP específica.

Siga las Prácticas recomendadas de IoT Security.

Aplicaciones y servicios

De forma predeterminada, una regla de denegación implícita en la parte inferior de la base de reglas de la Política de seguridad bloquea las aplicaciones que usted no permite explícitamente en una regla de la Política de seguridad. Para imponer el acceso con privilegios mínimos, ajuste las reglas de la Política de seguridad hasta que especifiquen solo las aplicaciones exactas que desea permitir por motivos comerciales (aplicaciones autorizadas) y para sus empleados (aplicaciones toleradas). Las reglas basadas en aplicaciones brindan un control granular de quién usa cada aplicación funcional y cómo la usan; para que pueda crear reglas precisas para la Política de seguridad a medida que avanza hacia un entorno de acceso a la red de Zero Trust. Las reglas basadas en puertos permiten cualquier aplicación en el puerto abierto; evítelas.

Debe habilitar el descifrado para que el cortafuegos vea la aplicación funcional en lugar de solo la aplicación "-base". Ver la aplicación funcional le permite controlar las aplicaciones de forma granular. Por ejemplo, en lugar de ver solo la aplicación contenedor "facebook", el cortafuegos puede ver "publicación en facebook", "descarga de facebook", "Uso compartido de archivos en facebook", etc. Esto le permite configurar la Política de seguridad basada en el acceso con privilegios mínimos; en lugar de dar a todos los empleados acceso a todas las aplicaciones funcionales de Facebook; puede restringir o bloquear el acceso a aplicaciones funcionales específicas para los usuarios adecuados.

Cuando añade una aplicación contenedor a una regla, todas sus aplicaciones funcionales se añaden implícitamente a la regla. Especifique las aplicaciones funcionales exactas que desea permitir para obtener un control más granular de las aplicaciones que permite y a quién permite usarlas.

La forma de aplicar los consejos de las prácticas recomendadas para las aplicaciones depende de si su entorno es nuevo, existente o una migración. Muchas de las recomendaciones reflejan el estado final de las prácticas recomendadas. En algunos casos, brindamos asesoramiento para la transición o asesoramiento sobre diferentes entornos. Sin embargo, cada entorno es único. El objetivo es comprender qué aplicaciones atraviesan su red, qué aplicaciones autorizadas y toleradas desea que atraviesen su red y utilizar esa información para realizar una transición segura a una base de reglas de la Política de seguridad que permita solo las aplicaciones que usted aprueba para fines comerciales y tolera para el acceso de los empleados.

Prácticas recomendadas de la base de reglas de la Política de seguridad *cubre dónde colocar las reglas en la base de reglas de la Política de seguridad.*

1. Utilice **grupos de aplicaciones** tanto como sea posible para simplificar y reforzar la creación de reglas de la Política de seguridad y reducir el tamaño de la base de reglas.

   Los grupos de aplicaciones son conjuntos de aplicaciones definidos por el usuario que requieren un tratamiento de seguridad similar. Añadir un grupo de aplicaciones a una regla de la Política de seguridad le permite controlar múltiples aplicaciones con una regla en lugar de crear una regla separada para cada aplicación. Si necesita añadir una aplicación al grupo o realizar cualquier otro cambio, solo tiene que realizar el cambio una vez en lugar de realizar el cambio en cada regla; porque cuando actualiza un grupo de aplicaciones, las reglas que hacen referencia a dicho grupo se actualizan automáticamente.
2. Ya sea que añada aplicaciones a un grupo de aplicaciones o a una regla de política de seguridad individual, especifique las aplicaciones funcionales exactas que desea, a menos que esté usando un grupo para bloquear una aplicación contenedor (que bloquea todas sus aplicaciones funcionales) o desee permitir acceso a todas las aplicaciones funcionales de una aplicación contenedor.
3. Las dependencias de aplicaciones ocurren cuando una aplicación necesita otras aplicaciones (aplicaciones dependientes) para funcionar correctamente. Las dependencias de las aplicaciones solo importan para las aplicaciones que usted permite, no para las aplicaciones que bloquea. Hay dos tipos de aplicaciones dependientes:

   - Aplicaciones explícitas, que el cortafuegos le muestra cuando añade una aplicación a la regla y que añade manualmente para que la aplicación funcione correctamente. Por ejemplo, la aplicación de chat de Facebook depende de añadir manualmente las aplicaciones Facebook-base y mqtt-base.
   - Aplicaciones implícitas, que el cortafuegos permite automáticamente para dar soporte a la aplicación especificada y que no es necesario añadir explícitamente a una regla. Por ejemplo, además de las

aplicaciones explícitas necesarias para que facebook-chat funcione correctamente, cuando añade facebook-chat a una regla, el cortafuegos permite automáticamente las aplicaciones jabber y web-browsing. (A menos que las añada explícitamente a una regla, jabber y web browsing no están permitidas para todo el tráfico, solo para el tráfico de chat de Facebook).

Tenga en cuenta qué aplicaciones permite implícitamente cuando permite una aplicación.

Puede ver las dependencias de una aplicación de varias maneras:

- El objeto **Applications (Aplicaciones)** proporciona una base de datos de aplicaciones con capacidad de búsqueda. Seleccione una aplicación para ver sus dependencias de aplicación explícitas [**Depends on (Depende de)**] y sus dependencias de aplicación implícitas [**Implicitly Uses (Usa implícitamente)**].
- La applipedia de Palo Alto Networks es una base de datos con capacidad de búsqueda para los App-ID entregados con contenido. Busque y seleccione una aplicación para ver sus dependencias de aplicación explícitas [**Depends on Applications (Aplicaciones de las que depende)**] y sus dependencias de aplicación implícitas [**Implicit use Applications (Aplicaciones de uso implícito)**].
- Cuando añade una aplicación a una regla de Política de seguridad, el cortafuegos le muestra las aplicaciones dependientes explícitas pero no las aplicaciones dependientes implícitas.
- **Commit Validate (validación de confirmación)** para ver las dependencias de las aplicaciones en base a toda la base de reglas de la Política de seguridad en lugar de en una sola regla.

Cada entorno de red y negocio es diferente, por lo que cómo gestionar las dependencias de las aplicaciones no es una recomendación única para valga para todos. Hay dos formas de abordar las dependencias de las aplicaciones, según su negocio y sus requisitos de seguridad:

- Centrarse en la disponibilidad: añada todas las aplicaciones dependientes que se muestran en una regla de la Política de seguridad a la regla para garantizar que la aplicación funcione correctamente. Por ejemplo, para la regla que controla el chat de Facebook, añada facebook-base y mqtt-base a la regla.

  Sin embargo, esto podría dar como resultado que algunas aplicaciones dependientes comunes, como SSL, se añadan a muchas reglas en lugar de solo a una regla, lo que añade desorden a la base de reglas. (Incluso si la base de reglas ya permite SSL, SSL aparece como una aplicación dependiente para muchas otras aplicaciones). Una buena forma de mitigar esto es utilizar Policy Optimizer para eliminar apariciones duplicadas de aplicaciones dependientes.
- Centrarse en la seguridad: para permitir el menor número de aplicaciones posible, ejecute una **Commit Validate (Validación de confirmación)** para ver todas las dependencias de las aplicaciones en la base de reglas de políticas de seguridad. Añada las dependencias que necesita según el resultado de Validación de confirmación. Considere la posibilidad de crear grupos de aplicaciones para diferentes conjuntos de dependencias de aplicaciones (por ejemplo, dependencias de VMware, dependencias de actualizaciones de software, etc.) que contengan todas las aplicaciones dependientes que desea permitir para poder controlar el acceso según los usuarios.

4. En implementaciones nuevas y existentes, bloquee inmediatamente el tráfico malicioso y peligroso conocido.

   - Bloquee el tráfico potencialmente malicioso basándose en fuentes fiables de inteligencia sobre amenazas, incluidas las listas dinámicas externas (EDL) integradas de Palo Alto Networks, que requieren una suscripción a Advanced Threat Prevention o Threat Prevention y bloquean direcciones IP protegidas, direcciones IP de alto riesgo, direcciones IP maliciosas conocidas y direcciones IP conocidas como nodos Tor de salida.

- Bloquee DNS cifrado para mantener la visibilidad del tráfico e inspeccionarlo en busca de amenazas mediante Perfiles de amenazas. Los atacantes utilizan DNS para muchos tipos de ataques, por lo que debe inspeccionar el tráfico DNS. Bloquee DNS sobre HTTPS (DoH) y DNS sobre TLS (DoT) y utilice el Servicio DNS de Palo Alto Networks. Si no es posible bloquear el DNS cifrado inmediatamente, obtenga visibilidad del tráfico y realice la transición para bloquear el tráfico DoH y (DoT) .

  Debido a la granularidad de App-ID, puede permitir el tráfico DNS normal en una regla y bloquear el tráfico DoT y DoH en otra regla, porque cada uno tiene un App-ID diferente que puede especificar en una regla de la Política de seguridad.

- Los hackers suelen utilizar aplicaciones para el uso compartido de archivos para filtrar datos. Bloquee la mayoría de las aplicaciones para compartir archivos y permita el acceso a aplicaciones comerciales para compartir archivos solo a los usuarios que las necesiten por motivos comerciales. Una manera fácil de lograr esto es crear una regla que especifique los usuarios y tenga un filtro de aplicaciones que incluya la subcategoría **file-sharing (uso compartido de archivos)** y/o la etiqueta **Uploading (Cargando)**.

La creación de una política de seguridad basada en listas de permitidos bloquea implícitamente la mayoría de las aplicaciones no deseadas, por lo que no necesita muchas reglas de bloqueo. Base lo que bloquea en los requisitos de su negocio, permitiendo solo el tráfico de aplicaciones que desea en su red y pensando en quién necesita usar cada aplicación.

5. Configure el **Service (Servicio)** como **application-default** (aplicación predeterminada) en la mayoría de los casos. Debido a que App-ID se basa en firmas en lugar de puertos y protocolos (que pueden ser falsificados), App-ID es muy preciso, por lo que no es necesario especificar el puerto. El uso de la aplicación predeterminada evita que cualquier aplicación, excepto la legítima, utilice el puerto y evita que las aplicaciones evasivas utilicen puertos no estándar. Si en el futuro cambia el puerto predeterminado para la aplicación, application-default aplica automáticamente el nuevo puerto para que no tenga que volver a configurar los ajustes del puerto de servicio.

   Especifique puertos de servicio solo si tiene una aplicación personalizada, requisitos arquitectónicos especiales o si los requisitos de seguridad de su empresa así lo exigen.

6. Para aplicaciones internas y aplicaciones para las que no existe un App-ID, cree aplicaciones personalizadas para obtener visibilidad de capa 7 del tráfico. No utilice la política de anulación de aplicaciones porque omite el procesamiento de capa 7 y la inspección de amenazas. Los casos de uso para la anulación de aplicaciones son situaciones inusuales con tráfico SMB o SIP.

7. Utilice **filtros de aplicaciones** para descubrir tráfico en su red y gestionar nuevas aplicaciones.

   Los filtros de aplicaciones son conjuntos dinámicos de aplicaciones. Las aplicaciones coinciden con los filtros de aplicaciones en base a los atributos que usted defina, como categoría, subcategoría, riesgo, etiquetas (etiquetas predefinidas o etiquetas personalizadas) y características. El cortafuegos añade automáticamente nuevas aplicaciones a un filtro cuando coinciden con los criterios del filtro. Las reglas de la Política de seguridad con un filtro de aplicaciones controlan automáticamente las nuevas aplicaciones que coinciden con el filtro.

   Los filtros de aplicaciones son controles más flexibles que los grupos de aplicaciones. Usted controla exactamente qué aplicaciones están en un grupo de aplicaciones. Los atributos que usted define controlan qué aplicaciones están en un filtro de aplicaciones, lo que puede generar una pertenencia más

amplia y permitir más aplicaciones de las que necesita permitir. Por eso son mejores para descubrir el tráfico y poder controlarlo.

Los casos de uso incluyen:

- En implementaciones nuevas en las que aún no está familiarizado con el tráfico, utilice filtros de aplicaciones para analizar diferentes categorías y subcategorías de tráfico, para que pueda descubrir cuáles de esos tipos de aplicaciones están en su red.

  También puede crear filtros de aplicaciones para descubrir tráfico de diferentes tipos en implementaciones maduras.
- Filtrado de la base de reglas para nuevas aplicaciones. Cree un filtro que coincida con las nuevas aplicaciones y coloque la regla cerca de la parte superior de la base de reglas. Utilice Policy Optimizer para obtener visibilidad de las aplicaciones y controlarlas.

  

  Las actualizaciones de contenido controlan las nuevas aplicaciones. Cuando se publica una Actualización de contenido de aplicaciones, las nuevas aplicaciones se consideran nuevas hasta que se publique la siguiente actualización de contenido de aplicaciones. La publicación de versiones normalmente se produce alrededor del tercer martes de cada mes. Después del lanzamiento del siguiente conjunto de aplicaciones nuevas, el conjunto anterior de aplicaciones nuevas ya no se considera nuevo y el filtro de aplicaciones ya no coincide con ellas. Siga las Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas *y decida cómo gestionar las nuevas aplicaciones antes de la próxima actualización de contenido de aplicaciones.*
- En situaciones de migración, use filtros de aplicaciones para bloquear o permitir una amplia gama de tipos de aplicaciones específicas y luego use Policy Optimizer para acotarlas a solo las aplicaciones que desea en la red. Los filtros de aplicaciones también le permiten garantizar que ciertos tipos de aplicaciones nuevas se permitan automáticamente cuando coincidan con un filtro.
- Proteja las reglas para el futuro gestionando nuevas aplicaciones automáticamente cuando coinciden con un filtro. Esto es útil tanto en la fase de descubrimiento de aplicaciones en migraciones como en nuevas implementaciones y entornos maduros.

  Por ejemplo, cree una regla de permiso con un filtro de aplicaciones basado en la etiqueta de **Palo Alto Networks**. Esto garantiza que usted permite todas las aplicaciones actuales de Palo Alto Networks y todas las aplicaciones futuras de Palo Alto Networks.

  Otro ejemplo es la creación de una regla que filtre nuevos App-ID entregados con contenido para gestionarlos de forma segura hasta que pueda examinarlos más de cerca.

8. Las definiciones de aplicaciones no son estáticas. Las actualizaciones de contenido de las aplicaciones pueden cambiar la definición de una aplicación y, por lo tanto, la forma en que las reglas la tratan. Siga las prácticas recomendadas para las actualizaciones de contenido de aplicaciones para asegurarse de tener tiempo para realizar los cambios necesarios debido a la actualización.

Acceso al sitio web (filtrado de URL)

El filtrado de URL avanzado Advanced URL Filtering requiere una licencia. Utilice el filtrado de URL avanzado con PAN-OS, Prisma Access (generalmente incluido con la licencia de Prisma Access) y Cloud NGFW para AWS.

El filtrado de URL basado en categorías de sitios web simplifica la Política de seguridad saliente y lo protege de sitios web maliciosos. Cada Categoría de URL define un grupo de sitios que tienen el mismo

tipo de contenido, por ejemplo, **health-and-medicine** (sitios de salud y medicina), **games** (juegos) o **hacking** (jaqueo). También hay tres categorías que definen el nivel de riesgo relativo de los sitios dentro de una categoría particular: **low-risk** (riesgo bajo), **medium-risk** (riesgo medio) y **high-risk** (riesgo alto). Combinar una categoría con un nivel de riesgo le permite crear reglas de política de seguridad que bloquean o permiten el tráfico según el riesgo dentro de una categoría de URL.

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

STEP 1 | Dirija el tráfico para descifrarlo según las categorías de URL porque las categorías de URL le permiten identificar fácilmente el tráfico de riesgo.

Descifre primero las categorías de URL más peligrosas y descifre más tráfico a medida que adquiera experiencia.

STEP 2 | En las reglas de la Política de seguridad que controlan el tráfico que sale a Internet:

- Adjunte perfiles de Filtrado de URL para simplificar la Política de seguridad. Configure un perfil de filtrado de URL de prácticas recomendadas que bloquee todas las categorías de sitios web maliciosos (tanto para el acceso al sitio como para el envío de credenciales de usuario) y alerta sobre todas las demás categorías, y adjúntelo a todas las reglas que permiten el acceso web.
- Controle el tráfico que no puede descifrar por motivos legales, de cumplimiento, comerciales, de privacidad, regulatorios o de otro tipo con categorías de URL. Por ejemplo, cree una regla de política de seguridad, con los usuarios y aplicaciones apropiados, que especifique las categorías apropiadas como criterios de coincidencia y no descifre el tráfico que coincida con la regla.
- Configure categorías de URL personalizadas para poder crear excepciones a las reglas de la Política de seguridad basadas en filtrado de URL, URL Filtering. Añada la categoría de URL personalizada a un perfil de URL Filtering y asóciela a la regla de política de seguridad adecuada o utilice categorías personalizadas como criterios de coincidencia en la Política de seguridad. Las excepciones le permiten bloquear el acceso a categorías de URL para la mayoría de los usuarios, pero lo permiten para usuarios específicos, como los probadores de penetración y la seguridad de la información, bloquear una categoría completa, como las redes sociales, pero permitir el acceso a LinkedIn, o controlar qué descifrar. Por ejemplo:
  - Combine una categoría de URL con una categoría basada en riesgos como criterio de coincidencia para bloquear o permitir el tráfico de una categoría de URL basada en riesgo. Por ejemplo, para bloquear el acceso a sitios financieros de riesgo, cree una regla de política de seguridad que especifique tanto la categoría de URL de **financial-services (servicios financieros)** como la categoría **high-risk (alto riesgo)** como criterios de coincidencia y establezca la regla **Action (Acción)** en **Deny (Denegar)**. Coloque esta regla por encima de las reglas que permiten el acceso a la categoría de URL **financial-services** (servicios financieros) para que el cortafuegos bloquee los sitios de alto riesgo antes de permitir el acceso a los sitios de riesgo medio y bajo.
  - Si la disponibilidad de recursos del cortafuegos le impide descifrar todo el tráfico que puede descifrar legalmente y con fines comerciales, utilice categorías de URL personalizadas para crear reglas para la Política de seguridad que coincidan con el tráfico de bajo riesgo para el cual el descifrado tiene poco valor. Por ejemplo, para evitar el descifrado de servicios de transmisión de bajo riesgo, cree una regla de política de seguridad que especifique tanto la categoría de URL **streaming-media (medios de transmisión)** como la categoría **low-risk (bajo riesgo)** como

criterios de coincidencia y establezca la regla **Action (Acción)** en **Allow (Permitir)**. Si el tráfico utiliza TLSv1.2 o anterior, cree una política y un perfil de no descifrado para que el tráfico bloquee las sesiones incorrectas. Si el tráfico utiliza TLSv1.3 o posterior, no cree una política ni un perfil de No descifrado para el tráfico.

- Establezca la zona de origen en la regla de la Política de seguridad en una red interna protegida (zona trust). No especifique una zona externa ni **any (cualquier)** zona como origen porque aplica el filtrado de URL, URL Filtering, solo al tráfico saliente. (Aplicar el URL Filtering al tráfico entrante puede incluso provocar ataques DoS).

STEP 3 | Para realizar la transición de perfiles de URL Filtering de forma segura a la configuración de prácticas recomendadas y crear perfiles de URL Filtering de prácticas recomendadas:

1. Duplique el perfil de URL Filtering predeterminado [llamado **default (predeterminado)**] y edítelo.
2. Cambie el nombre del perfil de forma adecuada (p. ej., Perfil de URL Filtering de prácticas recomendadas).
3. Configure todas las acciones para las categorías de URL para alertar tanto para el acceso al sitio como para el envío de credenciales de usuario. (La acción de permitir predeterminada no genera registros). Debe configurar manualmente las categorías de URL para alertar para generar logs y obtener visibilidad del tráfico.

   Cuando se añade una nueva categoría al filtrado de URL, de forma predeterminada, la categoría está configurada para permitir el acceso al sitio y el envío de credenciales de usuario. Configure manualmente nuevas categorías para alertar sobre el acceso al sitio y el envío de credenciales de usuario y obtener sus logs de filtrado de URL. Actualice también las categorías de URL personalizadas según corresponda.
4. Establezca todas las acciones para categorías de URL maliciosas en bloquear, tanto el acceso al sitio como el envío de credenciales de usuario. Realice las excepciones apropiadas para las pruebas PEN, la investigación de amenazas y la seguridad de la información según sea necesario:
   - command-and-control (comando y control): las URL y los dominios que el malware o los sistemas comprometidos utilizan para comunicarse con el servidor remoto de un atacante.
   - Grayware: estos sitios no cumplen con la definición de virus ni representan una amenaza directa a la seguridad, pero influyen en los usuarios para que otorguen acceso remoto o realicen otras acciones no autorizadas. Los sitios de grayware incluyen estafas, actividades ilegales, actividades delictivas, adware y otras aplicaciones no deseadas y no solicitadas, incluidos dominios de “secuestros de URL”.
   - malware: sitios conocidos por alojar malware o usados para actividades de comando y control (C2).
   - phishing: sitios conocidos por albergar páginas de phishing de información personal y de credenciales, incluidas estafas de soporte técnico y scareware.
   - ransomware: sitios conocidos por distribuir ransomware.
   - actividad de escaneo: investigación de vulnerabilidades existentes o la realización de ataques dirigidos.
5. Algunas categorías de URL tienen grandes posibilidades de ser maliciosas, pero definitivamente no lo son. Configure todas las acciones para estas categorías de URL, para bloquear tanto el acceso al

sitio como el envío de credenciales de usuario. Realice las excepciones apropiadas para las pruebas PEN, la investigación de amenazas y la seguridad de la información según sea necesario:

- dynamic-dns (dns dinámico): sistemas con direcciones IP asignadas dinámicamente que a menudo se utilizan para entregar cargas útiles de malware o malware de comando y control.
- jaqueo: sitios relacionados con el acceso ilegal o cuestionable a software y equipos informáticos, así como para su uso. Incluye sitios que facilitan evitar los sistemas de licencias y derechos digitales.

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

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

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

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

6. Establezca la acción para el acceso al sitio y el envío de credenciales de usuario en bloquear, para que bloquee las siguientes categorías de URL según los requisitos legales o comerciales y el posible riesgo de responsabilidad. Si no bloquea estos sitios, alerte sobre ellos y aplique perfiles de seguridad estrictos al tráfico.
   - abused-Drugs (consumo de drogas): sitios que promueven el consumo de estupefacientes legales e ilegales.

- adult (adultos): todos los sitios que contienen contenido para adultos de cualquier tipo, incluidos juegos y cómics, así como material, medios, arte, foros y servicios sexualmente explícitos.
- copyright-infringement (violación de derechos de autor): dominios con contenido ilegal que plantea un riesgo de responsabilidad.
- extremism (extremismo): sitios web que promueven el terrorismo, el racismo, la explotación infantil, etc.
- gambling (juegos de azar): sitios web de loterías y juegos de azar.
- peer-to-peer: intercambio de torrents, programas de descarga, archivos multimedia u otras aplicaciones de software entre individuos. No incluye sitios de shareware o freeware.
- questionable (cuestionable): sitios que promueven el humor de mal gusto y contenido ofensivo dirigido a grupos demográficos específicos.
- weapons (armas): venta, revisión, descripciones o instrucciones sobre armas y su uso.

Considere también cómo desea gestionar las categorías de URL de criptomonedas, y alcohol y tabaco. Alerte sobre ellos y aplique perfiles de seguridad estrictos al tráfico o bloquéelos, según las necesidades de su negocio.

7. Bloquee el Envío de credenciales de usuario para la categoría de alto riesgo. (No bloquee el acceso al sitio para la categoría de alto riesgo).
8. Para la configuración del filtrado de URL en el perfil de URL Filtering:
   - Deshabilite **Solo la página del contenedor de logs**, que está habilitada de forma predeterminada. Si solo registra páginas contenedor, pierde visibilidad de las aplicaciones funcionales como publicación, carga, descarga, etc. Deshabilite **Log Container Page Only (Registrar solo página del contenedor)** para ver el log completo y ver la aplicación funcional real.
   - Si su entorno es un centro educativo que recibe fondos federales, habilite **Safe Search Enforcement (Aplicación de búsquedas seguras)** (requisito legal).
9. Habilite la **User Credential Detection (Detección de credenciales de usuario)** (requiere configurar y habilitar el User-ID).

STEP 4 | Aplique URL Filtering a las reglas de la Política de seguridad con Sumidero de DNS configurado en el perfil de seguridad antispyware (requiere una suscripción a Advanced Threat Protection o una suscripción anterior activa a Threat Protection, y una suscripción a DNS Security para usar la seguridad DNS basada en la nube) para ver qué máquinas están infectadas y donde intentaban conectarse para DNS.

Acciones de política y otras configuraciones

Las acciones de la Política de seguridad especifican si se permite o bloquea el tráfico y cómo bloquear el tráfico que no se permite. La Calidad de servicio (QoS) controla el ancho de banda, si es necesario, para garantizar que el tráfico que permite una regla reciba el ancho de banda adecuado.

STEP 1 | Defina una acción para cada regla de la Política de seguridad.

- **Allow (Permitir)** únicamente el tráfico autorizado y tolerado. Cuanto más tráfico permita que no esté relacionado con su negocio, mayor será el riesgo. El cortafuegos bloquea el tráfico que usted no permite de forma explícita en una regla de la Política de seguridad.
- Cuanto más sigan las reglas de su Política de seguridad el principio de acceso con privilegios mínimos, menos reglas de bloqueo necesitará. La forma de bloquear el tráfico depende de cómo quiera responder a la aplicación que está bloqueando.
  - Utilice **Deny (Denegar)**, que utiliza la acción predeterminada de la aplicación, a menos que desee que el cortafuegos responda a la aplicación de una manera específica, restableciendo el cliente, el servidor o ambos; o descartando silenciosamente el tráfico.
  - Utilice **Drop (Descartar)** cuando desee denegar el servicio de forma silenciosa, sin enviar una respuesta de restablecimiento. Cuando bloquea tráfico claramente malicioso, como cuando bloquea según las EDL predefinidas de Palo Alto Networks, la acción **Deny (Descartar)** evita que el extremo malicioso de la comunicación sepa por qué se bloqueó.
  - Si tiene un caso de uso para restablecer solo el cliente o solo el servidor, asegúrese de comprender la direccionalidad cliente-servidor (qué extremo de la comunicación inicia la conexión), que se basa en la configuración de origen y destino de la regla.

STEP 2 | Si es necesario, aplique QoS para controlar el ancho de banda para determinadas aplicaciones.

QoS es opcional. Comprenda las aplicaciones a las que desea dar prioridad para el ancho de banda y las aplicaciones cuyo ancho de banda desea limitar si aplica la QoS a la política. Por ejemplo, durante eventos populares como la Copa mundial de fútbol que utilizan aplicaciones de streaming específicas, puede permitir que los empleados vean el evento usando esas aplicaciones y limitar su ancho de banda para garantizar que haya un ancho de banda adecuado disponible para las actividades comerciales. Otro ejemplo es cuando se lanzan actualizaciones para aplicaciones populares, la descarga masiva puede afectar la disponibilidad del ancho de banda. Para evitarlo, aplique QoS para limitar el ancho de banda disponible para el tráfico de descarga de esa aplicación.

Registro de logs y reenvío de logs

El registro y el almacenamiento de logs es fundamental para investigar incidentes. Comuníquese con su:

- Centro de operaciones de seguridad (SOC) para asegurarse de que captura la información correcta para investigar eventos si es necesario.
- Audite el equipo de cumplimiento normativo para garantizar que captura la información correcta para las auditorías y el cumplimiento normativo.
- Equipo legal para garantizar que no almacene texto sin cifrar u otros datos que violen las normativas locales, el cumplimiento, los requisitos comerciales, la privacidad, etc.

STEP 1 | Tenga en cuenta la capacidad de almacenamiento de logs que necesita ahora y en el futuro y dimensione su capacidad de almacenamiento de logs en consecuencia.

- Planifique la capacidad de almacenamiento para poder conservar los logs el tiempo suficiente para investigar las amenazas. El período de tiempo depende de sus procedimientos de investigación.
- Asegúrese de que su SOC pueda ingerir logs desde el sitio donde los almacene. Cortex Data Lake (CDL) centraliza el almacenamiento y el análisis de logs y proporciona una solución que aumenta a medida que lo hace su volumen de logs.
- No duplique los mismos logs para almacenarlos en varios lugares. Utilice CDL o un espacio de almacenamiento independiente, como Log Collectors. Al mover logs de un espacio de almacenamiento a otro, no utilice la duplicación. En su lugar, prepare y ejecute una transición completa.

Si habilita el reenvío de logs duplicados en los cortafuegos o Panorama, los logs del sistema y de configuración no se envían a CDL, por lo que los logs de CDL estarán incompletos. Por este motivo, no habilite el reenvío de logs duplicados para la copia de seguridad de logs.

Si debe dividir el almacenamiento de logs, hágalo separando el reenvío de logs de manera coherente. Por ejemplo, envíe todos los logs de Prisma Access a CDL y envíe todos los registros del cortafuegos a Log Collectors.

STEP 2 | Piense en lo que desea registrar, cómo desea registrarlo y en lo que no desea o no puede registrar por motivos de cumplimiento o de espacio de almacenamiento.

Para la mayoría de las aplicaciones, registre toda la información que pueda para ayudar con las investigaciones del Centro de operaciones de seguridad (SOC). Sin embargo, existen algunas aplicaciones y circunstancias para las que no se pueden realizar registros completos:

- Evalúe si la regla necesita el registro de logs en función del cumplimiento, los requisitos comerciales, los requisitos de auditoría como ISO, consideraciones de privacidad (por ejemplo, PII, RGPD) y requisitos SOC. Tenga cuidado al registrar datos de números de la seguridad social, credenciales, información de identificación personal, etc., en texto sin cifrar si las aplicaciones no cifran dicha información.
- Los servicios básicos como DNS, NTP, syslog, etc. crean miles de pequeñas sesiones que generan muchos logs innecesarios, lo que afecta el almacenamiento de logs y dificulta la investigación de incidentes. Para estos servicios, configure solo el reenvío de logs de amenazas a menos que tenga la capacidad de almacenamiento para aceptar otros logs.

STEP 3 | En las reglas de la Política de seguridad, registre el tráfico al final de la sesión en lugar de al inicio para evitar registrar aplicaciones transitorias.

Log At Session Start (Registrar al iniciar sesión) también consume más recursos que el registro solo al final de la sesión. En la mayoría de los casos, solo utiliza **Log At Session End (Registrar al finalizar sesión)**. Habilite **Log At Session Start (Registrar al iniciar sesión)** y **Log At Session End (Registrar al finalizar sesión)** solo para solucionar problemas relacionados con la falta de coincidencia con una regla de la Política de seguridad, para sesiones de túnel de larga duración como túneles GRE (no puede ver estas sesiones en el ACC, a menos que cree logs al iniciar sesión) y para

obtener visibilidad de las sesiones de tecnología operativa/sistemas de control industrial (OT/ICS), que también son sesiones de larga duración.

Policy Optimizer y Cloud App-ID Engine (ACE) no cuentan las reglas que se registran al inicio de la sesión en sus estadísticas.

STEP 4 | Registre el tráfico que coincida con la regla intrazone-default (intrazona predeterminada), que permite todo el tráfico dentro de una zona de forma predeterminada, y la regla interzone-deny (denegar interzona), que bloquea todo el tráfico entre zonas que la regla de Política de seguridad no permite explícitamente de forma predeterminada.

STEP 5 | Configure perfiles de reenvío de logs y asígnelos a las reglas de la Política de seguridad para enviar logs al almacenamiento apropiado, como CDL o recopiladores de logs, y para alertar a los administradores apropiados sobre eventos, especialmente eventos de amenaza crítica, alta y media.

Cloud Managed Prisma Access reenvía todos los logs a CDL.

- Asegúrese de que cada regla de Política de seguridad tenga adjunto un perfil de reenvío de logs.

  Cree un perfil de reenvío de logs predeterminado básico para todas las nuevas reglas de Política de seguridad, asígnele el nombre **`predeterminado`** y asegúrese de que registre las amenazas. Al nombrar el perfil como **`predeterminado`**, el cortafuegos lo aplica automáticamente a todas las nuevas reglas de políticas de seguridad, de modo que garantiza que todas las reglas nuevas tengan perfiles de reenvío de logs.

  Es más fácil reemplazar o modificar el perfil para las pocas reglas que requieren un tratamiento de registro de logs diferente, como logs para el tráfico relacionado con el cumplimiento, información personal, regulaciones locales, requisitos comerciales, etc., o logs para servicios comunes como DNS o NTP, que adjuntar un perfil de reenvío de logs a cada nueva regla individualmente.

  *Para las reglas de la Política de seguridad que rigen la IoT Security, utilice el perfil de reenvío de logs predefinido**perfil predeterminado de IoT Security: habilitado por EAL**, que proporciona a IoT Security todos los tipos de logs que necesita, incluidos los* logs de aplicaciones mejorados.

- Utilice **Log Forwarding for Security Services (Reenvío de logs para servicios de seguridad)** en Policy Optimizer para identificar las reglas de políticas de seguridad que no tienen un perfil de reenvío de logs adjunto (seleccione **None (Ninguno)** en el filtro). Añada un perfil de reenvío de logs adecuado a cada regla que no tenga uno.

STEP 6 | Con fines de investigación, asegúrese de conocer el verdadero origen y destino del tráfico, no solo la dirección IP de un dispositivo proxy, como un balanceador de carga, un dispositivo NAT o un servidor DNS malicioso que se encuentra entre el verdadero origen y el cortafuegos. Si hay un dispositivo proxy entre el cortafuegos y el origen real, según la arquitectura de su red y la aplicación:

- Coloque cortafuegos frente a los balanceadores de carga para ver la dirección IP de origen real.
- Realice una Captura de paquetes previa a NAT configurando una etapa de recepción en la configuración de captura de paquetes.
- Aplique un perfil de URL Filtering que permita registrar el campo X-Forwarded-For (XFF) en la regla de la Política de seguridad [pestaña**URL Filtering Settings (Configuración de URL**

Filtering) en **Objects (Objetos)** > **Profiles (Perfiles)** > **URL Filtering**]. El campo XFF muestra la dirección IP de origen original. El registro XFF se encuentra en el registro de filtrado de URL.

Perfiles de seguridad

Los perfiles de seguridad analizan el tráfico permitido en busca de amenazas como virus, malware, spyware, tipos de archivos maliciosos y otras amenazas conocidas y desconocidas, y evita esas amenazas. Adjunte perfiles de seguridad a reglas de la Política de seguridad que permitan al tráfico aplicar prevención de amenazas al tráfico que coincida con la regla.

Utilice las configuraciones del día 1 para plantillas que proporcionen prácticas recomendadas independientes de casos de uso y perfiles de seguridad para permitir el tráfico de manera correcta. Las configuraciones del día 1 están disponibles en el portal de atención al cliente (**Tools (Herramientas)** > **Run Day 1 Configuration (Ejecutar configuración del día 1)**) y requieren un inicio de sesión de soporte. A partir de ahí, realice la transición a las prácticas recomendadas de bloqueo de amenazas, como se describe aquí.

Para identificar y prevenir amenazas, el cortafuegos debe tener visibilidad del tráfico de aplicaciones. Descifre *todo el tráfico que permitan las regulaciones locales, las consideraciones comerciales, las consideraciones de privacidad y la capacidad técnica. Para el descifrado* proxy SSL de reenvío *(saliente), implemente primero User-ID y filtrado de URL para que pueda orientar el descifrado de manera efectiva. Si no descifra el tráfico, el cortafuegos no podrá analizar los encabezados cifrados ni la información de la carga útil.*

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

Obtenga la suscripción al servicio en la nube Advanced Threat Prevention para prevenir amenazas que incluyen comando y control desconocido y amenazas de vulnerabilidad de día cero en tiempo real. Advanced Threat Prevention está disponible para PAN-OS y para Prisma Access 3.2 Innovation e implementaciones posteriores de Innovation. Si ejecuta una versión anterior de Prisma Access, utilice la suscripción normal a Threat Prevention.

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

Las recomendaciones de perfiles de seguridad de prácticas recomendadas para Cloud Managed Prisma Access *difieren ligeramente de las recomendaciones para PAN-OS y Panorama Managed Prisma Access. Además, en Cloud Managed Prisma Access, no es posible aplicar perfiles de seguridad individuales a reglas de políticas de seguridad, solo puede aplicar grupos de perfiles. Los grupos de perfiles incluyen los* Perfiles de seguridad *que usted incluye en el grupo.*

Los consejos sobre prácticas recomendadas se centran en qué hacer para estar más seguro, y ese es el objetivo final de sus perfiles de seguridad. Sin embargo, para garantizar la disponibilidad de las aplicaciones críticas para el negocio, comience por bloquear el tráfico malicioso conocido y alertar sobre la mayoría del resto del tráfico. Siga los consejos de transición del perfil de seguridad de las prácticas recomendadas para pasar de forma segura de alertas a perfiles de seguridad de prácticas recomendadas que bloqueen el tráfico, y tenga cuidado al pasar de alerta a bloqueo para evitar afectar las aplicaciones críticas para el negocio.

El momento para realizar la transición de una configuración de perfil de seguridad de alerta a bloqueo es cuando esté seguro de que el perfil está ajustado adecuadamente, ha realizado las excepciones necesarias y no activará inadvertidamente una firma que bloquee una aplicación crítica para el negocio.

Esta sección simplificada le muestra las configuraciones de prácticas recomendadas. Creación de perfiles de seguridad de prácticas recomendadas proporciona información más detallada sobre los motivos de la configuración.

- Perfil de antivirus (incluye la firma de WildFire y acciones de aprendizaje automático en tiempo real)
- Perfil antispyware (incluye políticas de DNS/sumidero y análisis en la nube en tiempo real)

  Para proporcionar una cobertura completa, obtenga una suscripción a Advanced URL Filtering y una suscripción a DNS Security para obtener visibilidad y protección contra URL, dominios maliciosos y abusos del protocolo DNS.
- Perfil de protección de vulnerabilidades (incluye análisis en la nube en tiempo real)
- Perfil de bloqueo de archivos
- Perfil de análisis de WildFire

STEP 1 | Duplique el Perfil de antivirus predeterminado predefinido, cámbiele el nombre y edítelo a medida que realiza la transición segura del Perfil de antivirus a la configuración de prácticas recomendadas.

Para realizar la transición del Perfil de antivirus a un perfil de prácticas recomendadas de forma segura:

1. Los falsos positivos son raros. Implemente el Perfil antivirus de prácticas recomendadas para aplicaciones que no son críticas para su negocio de inmediato.
2. Para las aplicaciones críticas para el negocio, comience enviando alertas para asegurarse de que no afecta la disponibilidad de las aplicaciones críticas. Realice la transición a bloqueo cuando tenga la certeza de que el Perfil de antivirus no bloquea dichas aplicaciones.
3. Si tiene una implementación existente o está migrando, y tiene un bloqueo existente, duplíquelo porque ya tiene claro el tráfico y por qué lo está bloqueando.
4. Si trata las aplicaciones internas de manera diferente a las aplicaciones externas, es posible que necesite un perfil de antivirus para el tráfico de Internet y un perfil de antivirus diferente para el tráfico interno.

Supervise los logs de amenazas para ver si alguna aplicación crítica para el negocio provoca alertas o bloqueos. Supervise los logs de envíos de WildFire si tiene una suscripción de Advanced WildFire o una suscripción anterior de WildFire, y utilice la configuración de acciones de WildFire.

Un perfil antivirus de prácticas recomendadas bloquea malware, virus y bots de ransomware conocidos:

- Habilite la búsqueda de firmas en tiempo real en todo el dispositivo y en el perfil de antivirus, para retener archivos hasta que el cortafuegos reciba la última firma de antivirus en tiempo real desde la nube:
  - Habilitar globalmente: **Device (Dispositivo)** > **Setup (Configuración)** > **Content-ID** > **Content-ID Settings (Ajustes de Content-ID)** > **Realtime Signature Lookup (Consulta de firma en tiempo real)**, habilite **Hold for WildFire Real Time Signature Lookup ((Mantener pulsado para buscar la firma en tiempo real de WildFire)** y ponga la **Action On Real Time Signature Timeout (Acción sobre el tiempo de espera de firma de WildFire en tiempo real)**

en **Reset Both (Restablecer Ambos)**. Debe habilitar la búsqueda de firmas en tiempo real a nivel global para habilitar los perfiles de antivirus.

- Habilitar en Antivirus Profile (Perfil de antivirus): **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Antivirus** y habilitar **Hold for WildFire Real Time Signature Look Up (Mantener pulsado para buscar la firma en tiempo real de WildFire)**.

Retener archivos para garantizar que WildFire obtenga las firmas antivirus más recientes le protege frente al malware de día cero y firmas de antivirus obsoletas a las que podría estar expuesto si reenvía archivos sin retenerlos para obtener las firmas más recientes.

- Configure las acciones que deberá tomar cuando el cortafuegos detecte virus en ciertos protocolos. La acción más segura es restablecer tanto el cliente como el servidor para asegurarse de que la sesión ha finalizado:
  - Cambie la **Signature Action (Acción de firma)** a **reset-both (restablecer, ambos)** para los protocolos smtp, pop3 e imap, cuya acción predeterminada es alertar. Deje la **Signature Action (Acción de firma)** para los otros protocolos en **reset-both (restablecer-ambos)**.
  - Cambie la **WildFire Signature Action (Acción de firma de WildFire)** a **reset-both (restablecer ambos)** para los protocolos smtp, pop3 e imap, cuya acción predeterminada es alertar. Deje la **WildFire Signature Action (Acción de firma de WildFire)** para los otros protocolos en **reset-both (restablecer ambos)**.
  - Cambie la **WildFire Inline ML Action (Acción de WildFire Inline ML)** a **reset-both (restablecer ambos)** para los protocolos smtp, pop3 e imap, cuya acción predeterminada es alertar. Deje la **WildFire Inline ML Action (Acción de WildFire Inline ML)** para los otros protocolos en **reset-both (restablecer ambos)**.

Adjunte un perfil de prácticas recomendadas a todas las reglas de permiso.

Se requiere una suscripción a WildFire para configurar la Acción de firma de WildFire y la Acción de WildFire Inline ML.

En Cloud Managed Prisma Access, Antivirus y WildFire se combinan en un perfil en lugar de tener perfiles separados.

STEP 2 | Duplique el Perfil antispyware predeterminado predefinido, cámbiele el nombre y edítelo a medida que realiza la transición segura del Perfil antispyware a la configuración de prácticas recomendadas. Además de las políticas de firma antispyware, el perfil también controla las políticas de sumidero de DNS.

Para realizar la transición del Perfil antispyware de forma segura a un perfil de prácticas recomendadas, en **Signature Policies (Políticas de firmas)**:

1. Los falsos positivos son relativamente raros. Para aplicaciones que no son críticas para su empresa, bloquee firmas críticas y de gravedad alta desde el principio.
2. Las firmas de gravedad media pueden generar falsos positivos, por lo que requieren una supervisión inicial. Alerte sobre las firmas de gravedad media para el tráfico interno y bloquee las firmas de gravedad media para el tráfico externo. Supervise los logs de amenazas [**Monitor (Supervisar)** > **Logs** > **Threat (Amenaza)**] para ver si puede bloquear las aplicaciones para las que recibe alertas o si necesita permitirlas.
3. Para aplicaciones críticas para el negocio, establezca la **Action (Acción)** en **alert (alerta)** para garantizar la disponibilidad de la aplicación. Sin embrago, si ya protege las aplicaciones con un perfil Antispyware que bloquea firmas críticas, altas o medias, y está seguro de que el perfil

satisface sus necesidades empresariales y de seguridad, utilice un perfil similar para bloquear el spyware y proteger esas aplicaciones.

4. Habilite la captura de paquetes simple para todas las firmas de gravedad durante la transición para que pueda investigar los eventos con mayor detalle si es necesario y si tiene los recursos. A medida que pasa a los perfiles de prácticas recomendadas, si los eventos bajos e informativos crean demasiada actividad de captura de paquetes (un volumen de tráfico demasiado grande) y la información no es particularmente útil, realice la transición para desactivar la captura de paquetes en estas gravedades.

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

5. Cree excepciones según sea necesario para corregir cualquier falso positivo confirmado antes de implementar perfiles antispyware de prácticas recomendadas completos.

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

Realice la transición de las **Políticas DNS** del perfil a las prácticas recomendadas tan pronto como esté seguro de que comprende el tráfico que está bloqueando:

- Establezca la **Policy Action (Acción de política)** para firmas DNS en **sinkhole (sumidero)** para poder 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. Establezca **Packet Capture (Captura de paquetes)** en **extended-capture (captura extendida)**.

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

- Realice un sinkhole de todos los tipos de dominio de **DNS Security (Seguridad DNS)** y establezca la **Packet Capture (Captura de paquetes)** en **extended-capture** (captura extendida) para dominios de comando y control y **single-packet** ((paquete simple) para todos los demás tipos de dominio, excepto Dominios estacionados (PAN-OS 10.0 y posteriores).
- Bloquee todos los tipos de registros DNS, que se utilizan en consultas DNS cifradas, para evitar que los clientes cifren el saludo del cliente durante el proceso de resolución DNS.

Configure el **Inline Cloud Analysis (Análisis en la nube en tiempo real)** del perfil (requiere suscripción a Advanced Threat Prevention y PAN-OS 10.2 y posterior) para **Enable cloud inline**

analysis (Habilitar el análisis en la nube en tiempo real) en todo el tráfico saliente. Establezca la **Action (Acción)** en **Reset-both (Restablecer ambos)** para todos los modelos.

En el perfil antispyware de transición, si tiene controles antispyware existentes que bloquean el tráfico y satisfacen sus necesidades comerciales, implemente esos controles inmediatamente porque ya tiene claro el tráfico y por qué lo está bloqueando.

Un perfil Antispyware de prácticas recomendadas detecta el tráfico de comando y control (C2), evita que los sistemas comprometidos establezcan una conexión saliente y habilita DNS sinkholing para identificar hosts infectados. Utilice GlobalProtect para poner en cuarentena automáticamente un dispositivo comprometido en PAN-OS y con Panorama Managed Prisma Access, y también puede poner en cuarentena dispositivos comprometidos en Cloud Managed Prisma Access.

Para **Signature Policies (Políticas de firma)**:

1. Establezca la **Action (Acción)** para gravedades críticas, altas y medias en **reste-both (restablecer ambos)** y establezca la **packet-capture (captura de paquetes)** en **single-packet (paquete simple)**.
2. Establezca la **Action (Acción)** para gravedades bajas e informativas en **default (valor predeterminado)** y desactive **packet-capture (captura de paquetes)**.

Para **DNS Policies (Políticas DNS)**, utilice la misma configuración recomendada para el período de transición. Establezca la **Policy Action (Acción de política)** en sumidero para todas las fuentes de firmas, establezca **Packet Capture (Captura de paquetes)** en **extended-capture (captura extendida)** para **Palo Alto Networks Content (Contenido de Palo Alto Networks)** y dominios de comando y control, y establezca **Packet Capture (Captura de paquetes)** en **single-packet (paquete simple)** para todos los demás dominios de seguridad DNS, excepto los dominios Estacionados.

La configuración de prácticas recomendadas para **Inline Cloud Analysis (Análisis en la nube en tiempo real)** es la misma que la configuración de transición. Habilite la función en todo el tráfico saliente y establezca la acción en **reset-both (restablecer ambos)**.

Utilice el servicio de DNS Security para protegerse frente a amenazas avanzadas basadas en DNS (requiere una licencia de DNS Security y Advanced Threat Prevention o una suscripción activa a Threat Prevention).

Adjunte un perfil de prácticas recomendadas a todas las reglas de permiso.

STEP 3 | Duplique el perfil estricto de Protección frente a vulnerabilidades predefinido, cámbiele el nombre y edítelo a medida que realiza la transición del perfil de Protección frente a vulnerabilidades de forma segura a la configuración de prácticas recomendadas.

Los perfiles de protección frente a vulnerabilidades protegen contra desbordamientos de búfer, ejecución de código ilegal y otros intentos de aprovechar vulnerabilidades del lado del cliente y del

servidor. Para realizar la transición del perfil de Protección frente a vulnerabilidades de forma segura a un perfil de prácticas recomendadas:

1. Las tasas de falsos positivos son bajas. Establezca reglas para que las aplicaciones que no son críticas para su negocio se bloqueen [**reset-both (restablecer ambas)**] de inmediato.
2. Para las aplicaciones críticas para el negocio, comience enviando alertas para asegurarse de que no afecta la disponibilidad de las aplicaciones críticas. Realice la transición a bloqueo cuando tenga la certeza de que el Perfil de protección frente a vulnerabilidades no bloquea dichas aplicaciones.
3. Si tiene una implementación existente o está migrando, y tiene un bloqueo existente, duplíquelo porque ya tiene claro el tráfico y por qué lo está bloqueando.
4. Establezca firmas en la categoría de **brute-force (fuerza bruta)** para gravedades críticas, altas y medias para alertarlas y ajustarlas hasta que pueda realizar una transición cómoda al bloqueo. Establezca **Packet Capture (Captura de paquetes)** en **extended-capture (captura extendida)**.
5. Fije firmas para reglas críticas y de alta gravedad en **reset-both (restablecer ambas)** y fije **Packet Capture (Captura de paquetes)** en **single-packet (paquete simple)**.
6. Fije firmas para reglas de gravedad media en **alert (alertar)** y fije **Packet Capture Captura de paquetes)** en **extended-capture (captura extendida)**.
7. Fije las firmas para las reglas de gravedad baja e informativa en **default (predeterminada)** y fije **Packet Capture (Captura de paquetes)** en **single-packet (paquete simple)**.
8. Para el **Inline Cloud Analysis (Análisis en la nube en tiempo real)**, utilice los mismos criterios para alertar frente a bloquear aplicaciones empresariales que utiliza para las reglas iniciales de protección frente a vulnerabilidades. Si tiene controles existentes, duplíquelos para bloquear el tráfico. Para nuevos controles, alerte durante al menos una semana antes de pasar al bloqueo. Pase al bloqueo tan pronto como considere.

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

Supervise los logs de amenazas para ver si alguna aplicación crítica para el negocio provoca alertas o bloqueos. Supervise los logs de envíos de WildFire si tiene una suscripción a WildFire y utiliza las acciones de WildFire.

El perfil de protección frente a vulnerabilidades de prácticas recomendadas controla cómo gestionar las vulnerabilidades del lado del cliente y del servidor para gravedades de eventos críticos, altos, medios, bajos e informativos. En el perfil, configure seis reglas:

1. Cree las mismas tres reglas que previenen ataques de fuerza bruta en el perfil de transición y establezca la **Action (Acción)** en **reset-both (restablecer ambos)** y **Packet Capture (Captura de paquetes)** en **single-packet (paquete simple)**.
2. Combine gravedades simple-cliente-crítica, simple-cliente-alta, simple-cliente-media, simple-servidor-crítica, simple-servidor-alta y simple-servidor-baja en una única regla. Establezca la **Action**

(Acción) en **reset-both (restablecer ambos)** y establezca **Packet Capture (Captura de paquetes)** en **single-packet (paquete simple)**.

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

3. Para gravedades bajas de cliente simple y servidor simple, establezca la **Action (Acción)** en **default (valor predeterminado)** y establezca **Packet Capture (Captura de paquetes)** en **single-packet (paquete simple)**.
4. Para gravedades informativas simples de cliente y de servidor, establezca la **Action (Acción)** en **default (valor predeterminado)** y elija **disable (deshabilitar)** la captura de paquetes. (La actividad informativa puede generar un volumen relativamente alto de tráfico de captura de paquetes que no es particularmente útil en comparación con las capturas de paquetes de amenazas potenciales).
5. Establezca las acciones de **Inline Cloud Analysis (Análisis en la nube en tiempo real)** en **reset-both** (restablecer ambos).

Para controlar los perfiles de protección frente a vulnerabilidades de manera más granular y ajustar la protección frente a las vulnerabilidades para un caso de uso particular, cree reglas separadas en el perfil para cada gravedad para la detección tanto del lado del cliente como del lado del servidor. Cuando los ajustes de acción y captura de paquetes son los mismos, tiene sentido combinarlos en una regla para simplificar la configuración.

Adjunte un perfil de prácticas recomendadas a todas las reglas de permiso.

STEP 4 | Realice la transición de sus perfiles de Bloqueo de archivos de alerta a bloqueo de todos los tipos de archivos potencialmente maliciosos.

Cloud Managed Prisma Access no admite perfiles de Bloqueo de archivos para las reglas de políticas de seguridad.

Los Perfiles de bloqueo de archivos bloquean tipos de archivos potencialmente maliciosos utilizados en ataques cibernéticos. Para realizar la transición de perfiles de bloqueo de archivos de forma segura a la configuración de prácticas recomendadas y a un perfil de prácticas recomendadas:

- Para aplicaciones críticas para el negocio, alerte sobre todos los tipos de archivos y pase a un Perfil de bloqueo de archivos de prácticas recomendadas lo antes posible. Si ya tiene controles de bloqueo implementados, duplíquelos y continúe bloqueando el tráfico que ya sabe que desea bloquear.
- Para aplicaciones que no son críticas para el negocio, inicie la transición a un perfil de bloqueo de archivos de prácticas recomendadas:
  - **Tráfico entrante y saliente**: bloquee archivos 7z, bat, chm, class, cpl, dll, dlp, hta, jar, ocx, pif, scr, torrent, vbe y wsf. Alerta en todos los demás archivos.
  - **Tráfico interno**: bloquee archivos 7z, bat, chm, class, cpl, dlp, hta, jar, ocx, pif, scr, torrent, vbe y wsf (es lo mismo que el perfil de tráfico entrante y saliente excepto que alerta acerca de archivos .dll en lugar de bloquearlos). Alerta en todos los demás archivos.
  - Bloquee cualquiera de los siguientes tipos de archivos que pueda para los usuarios que no los necesitan para fines comerciales: cab, exe, flash, msi, codificación multinivel, PE, rar, tar, rar-cifrado y zip-cifrado.

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

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

El perfil de **strict file blocking (bloqueo de archivos estricto)** predefinido bloquea los tipos de archivos que normalmente se utilizan en ataques cibernéticos y que no tienen casos de uso reales para carga y descarga. Sin embargo, es posible que también se requieran algunos protocolos utilizados con fines maliciosos para actividades como las actualizaciones de Windows. El perfil de **strict file blocking (bloqueo de archivos estricto)** bloquea archivos .exe., .dll, .pe y .cab. Para hacer excepciones para permitir protocolos para una actividad específica, como actualizaciones de Windows:

1. Cree una regla de política de seguridad específica que permita solo a los usuarios que necesitan acceso con fines comerciales y a las aplicaciones comerciales que utilizan los protocolos que desea bloquear para otro tráfico.
2. Adjunte un perfil de Bloqueo de archivos que permita los protocolos necesarios a la regla.
3. Coloque la regla encima de una regla de política de seguridad con un perfil de Bloqueo de archivos que bloquee los protocolos para el resto del tráfico.

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

Adjunte un perfil de prácticas recomendadas a todas las reglas de permiso.

STEP 5 | Adjunte el perfil predeterminado de WildFire Analysis a todas las reglas de permiso para detectar y prevenir el malware de día cero.

Para obtener actualizaciones en tiempo real y otras funciones avanzadas, obtenga una suscripción a Advanced WildFire (PAN-OS 10.0 o posterior) o una suscripción a WildFire.

Implemente el perfil WildFire predeterminado, que es el perfil de prácticas recomendadas. WildFire no afecta el tráfico de la red, por lo que no se requiere un período de transición. (Sin embargo, la configuración de acciones de prácticas recomendadas de WildFire en el Perfil de antivirus afectan el tráfico que genera firmas que resultan en una acción de restablecimiento o descarte o en una retención para buscar la firma de antivirus más reciente). Adjunte un perfil de análisis de WildFire a todas las reglas de permiso para enviar todos los archivos a WildFire para su análisis.

En Cloud Managed Prisma Access, WildFire y Antivirus se combinan en un perfil, que se añade a un grupo de perfiles de Prisma Access.

STEP 6 | Los grupos de Perfiles de seguridad constan de perfiles de seguridad individuales combinados en un grupo con nombre, lo que le permite aplicar perfiles de seguridad de forma más sencilla y coherente a las reglas de la Política de seguridad.

Cree grupos de perfiles de seguridad para diferentes condiciones, según la lógica de su base de reglas:

- Cada grupo de perfiles deberá tener un propósito distinto, como crear grupos de perfiles específicos para el flujo de tráfico. Por ejemplo, un grupo de perfiles para el tráfico entrante no necesita un perfil de URL Filtering, pero un grupo de perfiles para el tráfico saliente sí.

  Los grupos de perfiles que son específicos del flujo de tráfico facilitan la creación de excepciones si desea tratar el tráfico interno y externo de manera diferente. Por ejemplo, es posible que desee bloquear algo para el tráfico interno que utiliza y permite para el tráfico externo. En ese caso, utilizaría perfiles diferentes para el tráfico interno y externo. La necesidad de perfiles separados dependerá de cómo desee tratar el tráfico.
- Para facilitar la transición de perfiles de alerta a bloqueo, cree grupos de perfiles para alertas iniciales y grupos de perfiles para bloqueos de prácticas recomendadas. Esto facilita la alerta sobre amenazas en todas las reglas de permiso. A medida que se sienta lo suficientemente cómodo para pasar de una alerta a un bloqueo, los grupos de perfiles facilitan el cambio porque solo tiene que intercambiar un objeto en lugar de cada perfil individual.
- Considere la posibilidad de crear un grupo de perfiles predeterminado con el nombre **`predeterminado`**. Por ejemplo, cree un grupo con perfiles que alerten pero no bloqueen la mayor parte del tráfico, en base al consejo sobre la transición de perfiles de seguridad a prácticas recomendadas. El cortafuegos aplica automáticamente el grupo de perfiles predeterminado a todas las nuevas reglas de la Política de seguridad que permiten el tráfico. (El cortafuegos no aplica el perfil predeterminado a las reglas existentes). Esto garantiza que todas las nuevas reglas de permiso tengan algún nivel de prevención de amenazas. Edite o reemplace el perfil predeterminado según sea necesario.

Prácticas recomendadas de la base de reglas de la Política de seguridad

La base de reglas de la Política de seguridad es una lista ordenada de sus reglas de Política de seguridad. El orden de las reglas determina cómo el cortafuegos gestiona el tráfico.

Los cortafuegos comparan el tráfico con las reglas de la Política de seguridad, comenzando con la primera regla en la parte superior de la base de reglas de la política de seguridad. Cuando el tráfico coincide con los

criterios de una regla, el cortafuegos ejecuta la acción de la regla en el tráfico y no lo compara con ninguna otra regla. Si ninguna regla coincide con el tráfico, el cortafuegos descarta el tráfico (denegación implícita). La forma en que ordena las reglas en la base de reglas es fundamental porque el cortafuegos toma medidas sobre el tráfico basándose en la primera coincidencia de reglas y luego deja de comparar el tráfico con la base de reglas.

Si migró la Política de seguridad desde el cortafuegos de otro proveedor, es posible que el cortafuegos anterior haya evaluado el tráfico según su base de reglas de manera diferente. Por ejemplo, es posible que el orden de las reglas no haya marcado la diferencia en su antiguo cortafuegos, pero son cruciales en los cortafuegos de Palo Alto Networks.

Comprender cómo desea gestionar los diferentes tipos de tráfico y #unique_18 le ayudará a evaluar cómo ordenar las reglas en la base de reglas. Diseñe y optimice su base de reglas de la Política de seguridad de manera lógica, como se describe en esta sección. Para las bases de reglas existentes, si la base de reglas no está tan optimizada como podría estarlo, planifique y pruebe los cambios de acuerdo con los consejos de esta sección. Si planifica implementar los cambios en fases, hágalos en el momento o momentos apropiados.

Esta sección cubre cómo:

- Ordenar reglas de la Política de seguridad en la base de reglas
- Evitar la sobrecarga de la base de reglas
- Posicionarse para hacer excepciones a una regla
- Prevenir y remediar el solapamiento de reglas
- Usar las jerarquías de grupos de dispositivos en Panorama para simplificar la base de reglas

STEP 1 | Ordene las reglas de la Política de seguridad de forma lógica en la base de reglas.

Debido a que el cortafuegos ejecuta la acción de una regla de política en el tráfico cuando ese tráfico coincide con los criterios de la regla, el orden de las reglas es crítico y determina qué regla coincide con el tráfico y, por lo tanto, qué acción realiza el cortafuegos sobre el tráfico y cómo este inspecciona el tráfico. :

1. Coloque reglas que bloqueen el tráfico malicioso en la parte superior de la base de reglas para evitar permitir accidentalmente tráfico inadecuado más adelante en la base de reglas. Si tiene una licencia activa de Advanced Threat Prevention o una versión activa de Threat Prevention, cree reglas de bloqueo basadas en las listas dinámicas externas (EDL) predefinidas y pruébelas para asegurarse de que no bloqueen el tráfico que desea permitir. En Panorama, coloque estas reglas en las reglas previas para que se ejecuten antes que cualquier regla específica del cortafuegos.
2. Permita que las aplicaciones de infraestructura básica y los servicios comunes, como DNS y NTP, estén cerca de la parte superior de la base de reglas para evitar bloquearlos accidentalmente. Estas reglas generalmente permiten el tráfico desde cualquier zona de origen a cualquier zona de destino y se aplican a todo y a todos.

   En Panorama, coloque estas reglas en las reglas previas para que se ejecuten antes que cualquier regla definida localmente en el cortafuegos.
3. La lógica para todas las demás reglas es colocar las reglas más específicas cerca de la parte superior de la base de reglas y las reglas más generales más cerca de la parte inferior de la base de reglas. Si coloca reglas generales antes que reglas específicas en la base de reglas, el tráfico que desea que coincida con la regla específica podría coincidir con la regla general, lo que podría suponer

aplicar una acción diferente y una inspección del tráfico diferente a la que desea. A esto se le llama shadowing o solapamiento: otra regla “solapa” a la regla que desea que coincida el tráfico.

4. Si aún no ha convertido o no puede convertir todas sus reglas de Política de seguridad basadas en puertos y servicios a reglas basadas en App-ID, coloque las reglas basadas en App-ID antes que las reglas basadas en puertos y servicios.

STEP 2 | Mantenga la base de reglas lo más pequeña posible para facilitar la gestión y evitar la sobrecarga de la base de reglas.

1. Si cinco de los seis objetos siguientes son iguales en varias reglas, combine esas reglas en una sola regla:
   - Zona de origen
   - Zona de destino
   - Dirección IP origen
   - Dirección IP de destino
   - Puerto de servicio
   - Aplicación

   Por ejemplo, si tres reglas especifican aplicaciones diferentes pero tienen la misma zona de origen y destino, direcciones IP de origen y destino y puerto de servicio, entonces puede combinar las reglas en una regla que especifique las aplicaciones de cada una de las reglas originales.
2. Utilice objetos de grupo para simplificar la creación de políticas y reducir el tamaño de la base de reglas.

   Utilice grupos de aplicaciones y grupos de direcciones para ayudar a consolidar reglas que se aplican a todos los miembros del grupo.

   Si utiliza tanto objetos individuales como objetos de grupo en la política, tenga en cuenta que la pertenencia de un objeto a un grupo puede causar elsolapamiento de las reglas si el objeto se especifica individualmente en una regla y también se especifica en una regla como parte de un grupo de objetos. En este caso, es posible que el cortafuegos no realice la acción prevista porque el tráfico podría coincidir primero con la regla incorrecta. Si es posible, combine las reglas, a menos que su proceso de control de cambios requiera una política específica para realizar un seguimiento del acceso. Si desea tratar un objeto de manera diferente a otros objetos de un grupo, elimine el objeto del grupo.
3. Deshabilite o elimine reglas de la base de reglas de la Política de seguridad cuando ya no las necesite.

   Las reglas de la Política de seguridad pueden volverse innecesarias cuando una organización cambia las aplicaciones o la infraestructura, o cuando ya no necesita reglas de prueba temporales. Si no desactiva o elimina dichas reglas, estas podrían provocar acciones inesperadas en el tráfico. Es más seguro deshabilitar una regla primero para poder habilitarla nuevamente si deshabilitarla causa problemas. Cuando deshabilita las reglas, se aplica una etiqueta con la fecha en que se deshabilitaron las reglas. Utilice periódicamente la función Uso de reglas de Policy Optimizer para

comprobar cuánto tiempo lleva sin utilizar una regla. Si tras un período de tiempo usted considera que realmente no necesita la regla, elimínela.

*Tenga en cuenta las reglas con aplicaciones que utiliza solo para eventos periódicos, como reuniones trimestrales o conferencias anuales. Podría ser adecuado configurar una **Schedule (Programación)** que habilite la regla solo durante el período de tiempo del evento.*

4. Utilice Policy Optimizer para optimizar la base de reglas. Policy Optimizer encuentra reglas no utilizadas, reglas con aplicaciones no utilizadas, reglas que no se han utilizado con el tiempo y reglas que no tienen perfiles de reenvío de logs, además de permitirle gestionar nuevas aplicaciones SaaS en la Política de seguridad si tiene una suscripción a SaaS Security.
5. En Panorama, utilice grupos de dispositivos globales comunes que se apliquen a múltiples VSYS y cortafuegos en toda la organización para reglas de políticas de seguridad globales comunes, como reglas que controlan servicios básicos comunes y cualquier otro servicio o aplicación que desee aplicar a grupos amplios de dispositivos. Cree la jerarquía del grupo de dispositivos para no tener que repetir reglas entre grupos; use la jerarquía para escribir una regla una vez y aplicarla a todos los grupos de cortafuegos correspondientes.
6. Revise la base de reglas de la Política de seguridad periódicamente como parte de un mantenimiento programado periódicamente.

STEP 3 | Para hacer una excepción a una regla, coloque la regla más específica delante de la regla más general.

Por ejemplo, desea impedir que sus empleados accedan a sitios web maliciosos, por lo que crea una regla de Política de seguridad general que bloquea el acceso a todos los sitios web maliciosos para todos los empleados. Sin embargo, su equipo de InfoSec y los probadores de penetración necesitan acceso para realizar pruebas. En este caso, crea una regla que permite el acceso a los sitios web maliciosos requeridos solo para esos usuarios (descifrando el tráfico, aplicando los perfiles de amenazas más estrictos a la regla y especificando solo las aplicaciones utilizadas para las pruebas) y coloca esa regla por encima de la regla general en la base de reglas.

Cuando InfoSec y los probadores de penetración intentan acceder a los sitios maliciosos para realizar pruebas, se les permite, pero ningún otro usuario coincide con los criterios de la regla, por lo que la regla general los bloquea. Si coloca la regla de acceso del equipo de InfoSec y de prueba de penetración después de la regla de bloqueo general, la regla general solapa la regla específica y el tráfico de InfoSec/probador de penetración coincidirá con la regla general y se bloqueará.

STEP 4 | Evite que las reglas generales solapen reglas más específicas.

El solapamiento se produce cuando coloca una regla amplia que incluye los mismos criterios de coincidencia que una regla más específica que se encuentra más arriba en la base de reglas que la regla específica, de modo que el tráfico destinado a coincidir con la regla específica coincide primero con la regla general y nunca se compara con la regla específica. El resultado es que el cortafuegos

ejecuta la acción e inspección configurada en la regla general cuando la intención es ejecutar la acción e inspección en la regla específica. La regla general *solapa* la regla específica.

Una regla de solapamiento puede superponerse a más de una regla en la base de reglas.

La forma más sencilla de evitar el solapamiento es construir la base de reglas correctamente desde el principio. Sin embargo, las bases de reglas existentes y las bases de reglas migradas pueden tener reglas de solapamiento. Para prevenir y corregir los solapamientos:

1. Comprenda la acción que desea realizar en el tráfico y cómo desea inspeccionarlo.

   Si la acción y la inspección en la regla específica son la forma en que desea gestionar el tráfico, ponga la regla específica por encima de la regla general en la base de reglas. Si la acción y la inspección en la regla general son la forma en que desea gestionar el tráfico, entonces no necesita la regla específica.
2. Coloque reglas de la Política de seguridad más específicas por encima de las reglas generales en la base de reglas. Si coloca la regla general primero, esta se superpondrá a la regla específica, por ejemplo:

   1. Cree una regla general que bloquee todo acceso a Facebook.
   2. Cree una regla específica que permita a los grupos de marketing y relaciones públicas acceder a Facebook, pero coloque la regla debajo de la regla general de Facebook en la base de reglas.
   3. La regla general bloquea todo el acceso a Facebook independientemente del grupo de usuarios, por lo que el tráfico nunca coincide con la regla específica que permite el acceso a los grupos específicos que desea permitir.

   La solución es mover la regla específica por encima de la regla general en la base de reglas.
3. Revise y resuelva las reglas que se solapan para asegurarse de que el cortafuegos ejecute la acción que desea e inspeccione el tráfico de la manera que desee.

   Cuando escribe una nueva regla de la Política de seguridad:

   1. Seleccione una opción de confirmación y realice una **Confirm (Confirmación)** en el cortafuegos o una **Validate Commit (validación de confirmación)** en Panorama para comprobar si hay problemas de configuración. No confirme la configuración. Resuelva los problemas que la comprobación de validación descubra antes de continuar.
   2. Haga clic en **Commit (Confirmar)** o **Commit and Push (Confirmar y enviar)** para confirmar y enviar los cambios de configuración.
   3. Cuando finalice la confirmación, seleccione **Tasks (Tareas)** en la cinta inferior derecha para abrir el Administrador de tareas.
   4. En la columna **Type (Tipo)**, haga clic en **Commit All (Confirmar todo)** para que aparezca **Job Status (Estado del trabajo)**. (Commit and Push no proporciona información de seguimiento).
   5. Haga clic en el mensaje de la columna **Status (Estado)** para abrir los **Last Push State Details (Detalles del último estado de envío)** y seleccione la pestaña **Rule Shadow (Solapamiento de regla)**. Si no hay una pestaña **Rule Shadow (Solapamiento de regla)**, entonces el cortafuegos no tiene reglas solapadas.
   6. El lado izquierdo de **Last Push State Details (Detalles del estado del último envío)** muestra las reglas que solapan, o se superponen, a otras reglas. El nombre de cada regla que solapamiento es un vínculo a la regla. Para cada regla de solapamiento, haga clic en el número en la columna

Count (Recuento) para mostrar las reglas que solapa. Se enumeran los nombres de las reglas solapadas, pero no son enlaces a dichas reglas.

7. La lista de reglas de solapamiento no es persistente en todas las operaciones de confirmación, por lo que es fundamental capturar la lista de reglas solapadas de cada regla de solapamiento. Por ejemplo, obtenga el estado a través de una API usando un script, copie y pegue la lista en un editor de texto, tome una captura de pantalla, tome una fotografía o escriba los nombres de las reglas que solapan y las reglas solapadas.

   *La operación de **Commit (Enviar)** de la configuración PAN-OS valida las reglas de solapamiento. Si se detecta el solapamiento de reglas, se genera un mensaje de advertencia que identifica las reglas afectadas. Si realiza otra operación de confirmación antes de capturar la lista de solapamientos, la información de solapamiento se pierde. Asegúrese de capturar esta información de inmediato.*

8. Encuentre cada regla que solapa y solapada en la base de reglas de la Política de seguridad y capture la configuración de cada regla.
9. Compare cada regla de solapamiento con las reglas a las que solapa, una al lado de la otra, para comprender el propósito de cada regla. Esto le permite evaluar juntas las reglas relacionadas y comprender cómo desea gestionar las aplicaciones que controlan las reglas.
10. Cuando tenga claro cómo desea gestionar las aplicaciones en una regla de solapamiento y las reglas a las que solapa, combine reglas para simplificar la base de reglas, deshabilite o elimine reglas duplicadas y mueva reglas específicas por encima de las reglas generales para resolver el solapamiento o superposición.
11. Repita para corregir cualquier solapamiento restante.
12. Repita el proceso para cada regla de solapamiento.

En sistemas de prueba que no son de producción, es posible que desee mantener el solapamiento y las reglas solapadas para probar nuevas reglas de políticas y para otros fines de prueba.

STEP 5 | En Panorama, coloque las reglas de la Política de seguridad de manera adecuada dentro de las jerarquías de grupos de dispositivos.

Coloque las reglas de modo que no tenga que repetir la misma regla innecesariamente en varios grupos de dispositivos. Las reglas que son comunes a varios grupos de dispositivos pertenecen a esos grupos en la jerarquía, por lo que una regla se aplica a todos los grupos.

- Diseñe la jerarquía de una manera cuidadosa que solo brinde acceso a los grupos de cortafuegos a los que desea tener acceso. Piense en el acceso que cada cortafuegos necesita cuando cree grupos de dispositivos y piense en el acceso que cada grupo de dispositivos necesita cuando crea la jerarquía de grupos de dispositivos. La clave para la construcción es los aspectos en común: qué cortafuegos necesitan acceso similar, qué grupos de cortafuegos necesitan acceso similar y cómo construir una jerarquía que permita a los grupos superiores en la jerarquía contener reglas que se apliquen a los niveles inferiores y eliminar la necesidad de duplicar normas.
- Coloque reglas que se apliquen a todos los cortafuegos en el grupo más alto de la jerarquía para evitar la duplicación de reglas.

- Coloque reglas que se apliquen a conjuntos de grupos de cortafuegos lo suficientemente altos en la jerarquía para que no tenga que duplicar reglas.

La Guía del administrador de Panorama proporciona información detallada sobre los grupos de dispositivos, incluida una ilustración de ejemplo de una jerarquía de grupos de dispositivos .

Prácticas recomendadas de Policy Optimizer

Policy Optimizer le ayuda a convertir reglas de la Política de seguridad basadas en puertos en reglas basadas en aplicaciones, y realizar la transición a reglas de política de acceso con privilegios mínimos:

- Descubra y convierta reglas basadas en puertos [la aplicación es **any (cualquiera)** en lugar de una aplicación específica] en reglas basadas en aplicaciones que siguen el principio de acceso con privilegios mínimos [**Policies (Políticas)** > **Security (Seguridad)** > **Policy Optimizer** > **Rules Without App Controls (Reglas sin controles de aplicación)**).
- Descubra y elimine aplicaciones no utilizadas de reglas sobreaprovisionadas [**Policies (Políticas)** > **Security (Seguridad)** > **Policy Optimizer** > **Unused Apps (Aplicaciones no utilizadas)**]
- Descubra y elimine las reglas que no utiliza y comprenda el uso de las reglas de políticas [**Policies (políticas)** > **Security (Seguridad)** > **Policy Optimizer** > **Rule Usage (Uso de reglas)**].
- Descubra nuevas aplicaciones que coincidan con los filtros de aplicaciones y los grupos de aplicaciones utilizados en las reglas de la Política de seguridad. Evalúe nuevas aplicaciones y si desea permitirlas o bloquearlas [**Policies (Políticas)** > **Security (Seguridad)** > **Policy Optimizer** > **New App Viewer (Visor de aplicaciones nuevas)**].

  Si tiene una suscripción SaaS Security Inline y utiliza App-ID Cloud Engine (ACE), utilice Policy Optimizer para integrar App-ID de ACE en su base de reglas de la Política de seguridad.
- Descubra las reglas de la Política de seguridad que no tienen un perfil de reenvío de logs adjunto y añada perfiles de reenvío de logs a esas reglas [**Policies (Políticas)** > **Security (Seguridad)** > **Policy Optimizer** > **Log Forwarding for Security Services (Reenvío de logs para servicios de seguridad)**].

Policy Optimizer está disponible en PAN-OS 9.0 y posteriores para los cortafuegos Panorama y PAN-OS (los cortafuegos pueden estar en PAN-OS 8.1 si Panorama ejecuta PAN-OS 9.0 o posterior). Prisma Access no es compatible con Policy Optimizer.

Para la compatibilidad con Cortex Data Lake, Panorama requiere PAN-OS 10.0.3 o posterior con el complemento Cloud Services 2.0 Innovation o posterior.

Las prácticas recomendadas de Policy Optimizer cubren:

- Cómo utilizar Policy Optimizer: principales casos de uso, cómo añadir aplicaciones a las reglas de la Política de seguridad, reglas de clasificación y filtrado, y uso de filtros y grupos de aplicaciones.
- Flujos de trabajo de la base de reglas de Policy Optimizer: cómo planificar una transición a reglas basadas en aplicaciones, convertir reglas basadas en puertos en reglas basadas en aplicaciones, eliminar reglas no utilizadas y eliminar aplicaciones no utilizadas para reforzar la base de reglas.

Descifre *lo antes posible todo el tráfico que las regulaciones locales, el cumplimiento, los requisitos comerciales y las consideraciones de privacidad permiten para proporcionar información más precisa sobre las aplicaciones y obtener visibilidad de las aplicaciones que controla con Policy Optimizer. Sin descifrado, el cortafuegos a menudo puede identificar las aplicaciones principales, pero generalmente no puede identificar las aplicaciones funcionales. Por ejemplo, el cortafuegos ve "facebook", pero no ve facebook-post, facebook-download, facebook-file-sharing, etc. Debe descifrar el tráfico para obtener visibilidad y control de las aplicaciones funcionales. Para el descifrado* proxy SSL de reenvío *(saliente), implemente primero User-ID y filtrado de URL para que pueda orientar el descifrado de manera efectiva.*

Cómo utilizar Policy Optimizer

Esta sección describe los principales casos de uso de Policy Optimizer y cómo utilizar la herramienta. Flujos de trabajo de la base de reglas de Policy Optimizer describe los flujos de trabajo.

Los casos de uso de Policy Optimizer incluyen:

- **Migración desde reglas basadas en aplicaciones basadas en puertos**: vea las aplicaciones de capa 7 que coinciden con cada regla basada en puertos, seleccione las aplicaciones que desea permitir y convierta cada regla en una o más reglas basadas en aplicaciones.
- **Nuevas implementaciones**: descubra aplicaciones en su red y realice la transición a una política basada en aplicaciones a lo largo del tiempo.
- **Implementaciones maduras**: examine su base de reglas, convierta reglas amplias basadas en filtros de aplicaciones en reglas estrictas basadas en grupos de aplicaciones que permitan solo las aplicaciones que usted apruebe y elimine las reglas y aplicaciones no utilizadas.
- **DevOps**: comprenda las aplicaciones nuevas o modificadas en su entorno de prueba. Aprenda cómo gestionarlos en las reglas de la Política de seguridad antes de realizar cambios en su entorno de producción. Pruebe las reglas nuevas y modificadas antes de aplicarlas en un entorno de producción.

STEP 1 | Trabaje con las personas adecuadas para comprender las aplicaciones autorizadas que desea permitir en su red con fines comerciales y las aplicaciones toleradas que desea permitir para los empleados.

Sea consciente de qué aplicaciones son críticas para el negocio. Conozca qué aplicaciones solo se utilizan periódicamente para eventos trimestrales, anuales u otros, y evalúe las reglas relevantes el tiempo suficiente para ver la actividad de estas aplicaciones. Conocer la lógica empresarial para dar permiso a aplicaciones le ayudará a comprender cómo construir una Política de seguridad. Para comprender mejor las aplicaciones, busque los App-ID de contenido entregado en applipedia o en **Objects (Objetos)** > **Applications (Aplicaciones)** en el cortafuegos o en Panorama.

STEP 2 | Conozca cómo clasificar, filtrar y examinar la información y las estadísticas de Policy Optimizer utilizando diferentes métricas para diferentes propósitos.

Las estadísticas del Policy Optimizer no se informan en tiempo real. Se tarda aproximadamente una hora o más, según el volumen de tráfico de la aplicación y el tamaño de la base de reglas, en actualizar la lista de aplicaciones. Cuando añada una aplicación a una regla, espere al menos una hora antes de

ejecutar los logs de tráfico para ver la información de la aplicación. Si no ve la información, espere un momento y vuelva a comprobarla.

*Policy Optimizer ignora el tráfico de reglas que solo se **Log at Session Start (Registran al inicio de la sesión)** para evitar contar aplicaciones transitorias. (Para las reglas que también se **Log at Session End (Registran al finalizar la sesión)**, Policy Optimizer recoge las estadísticas de las reglas).*

STEP 3 | Entienda cómo utilizar filtros de aplicaciones y grupos de aplicaciones en la Política de seguridad.

Utilice filtros de aplicaciones en reglas de la Política de seguridad para descubrir aplicaciones en su red. Luego, convierta esas reglas de filtros de aplicaciones a grupos de aplicaciones para que pueda especificar las aplicaciones exactas que desea permitir.

- Utilice **grupos de aplicaciones** tanto como sea posible para simplificar y reforzar las reglas de la Política de seguridad y reducir el tamaño de la base de reglas.

  Los grupos de aplicaciones son conjuntos de aplicaciones específicas definidas por el usuario que desea controlar en una regla con un tratamiento de seguridad similar. Añada aplicaciones a reglas usando grupos de aplicaciones (el tema vinculado se centra en las aplicaciones de ACE pero se aplica a todas las aplicaciones) para controlar múltiples aplicaciones con una regla en lugar de crear una regla independiente para cada aplicación. Reutilice grupos de aplicaciones en diferentes reglas para dar diferentes accesos a las aplicaciones a diferentes usuarios, orígenes y destinos. La reutilización de grupos automatiza la adición de aplicaciones a múltiples reglas (cuando realiza cualquier cambio en un grupo de aplicaciones, el cambio se refleja en todas las reglas incluidas en el grupo de aplicaciones).
- Utilice **filtros de aplicaciones** para:
  - Descubrir aplicaciones en su red.
  - Proteja las reglas para el futuro gestionando nuevas aplicaciones automáticamente cuando coinciden con un filtro. Esto es útil tanto en la fase de descubrimiento de aplicaciones en migraciones como en nuevas implementaciones y entornos maduros.

    Por ejemplo, cree una regla de permiso con un filtro de aplicaciones basado en la etiqueta de **Palo Alto Networks**. Esto garantiza que usted permite todas las aplicaciones actuales de Palo Alto Networks y todas las aplicaciones futuras de Palo Alto Networks.

    Otro ejemplo es la creación de una regla que filtre nuevos App-ID entregados con contenido para gestionarlos de forma segura hasta que pueda examinarlos más de cerca.
  - En bases de reglas maduras, añada aplicaciones a las reglas utilizando filtros de aplicaciones para bloquear tipos de aplicaciones no deseadas. Utilice grupos de aplicaciones para permitir tráfico de forma intencionada (el tema vinculado se centra en las aplicaciones de ACE pero se aplica a todas las aplicaciones).

  Los filtros de aplicaciones son conjuntos dinámicos de aplicaciones. Las aplicaciones coinciden con los filtros de aplicaciones en base a los atributos que usted defina, como categoría, subcategoría, riesgo, etiquetas (etiquetas predefinidas o etiquetas personalizadas) y características. El cortafuegos añade automáticamente nuevas aplicaciones a un filtro cuando coinciden con los criterios del filtro. Las reglas de la Política de seguridad con un filtro de aplicaciones controlan automáticamente las nuevas aplicaciones que coinciden con el filtro.

  Los filtros de aplicaciones son controles más laxos que los grupos de aplicaciones. Usted controla exactamente qué aplicaciones están en un grupo de aplicaciones. Los atributos que usted

defina controlan las aplicaciones en un filtro de aplicaciones, lo que puede llevar a permitir más aplicaciones de las necesarias. Es por eso que los filtros son mejores para descubrir tráfico y para bloquear subcategorías de aplicaciones del tráfico. Reutilice filtros de aplicaciones en diferentes reglas para dar diferentes accesos a las aplicaciones a diferentes usuarios, orígenes y destinos.

Utilice grupos de aplicaciones y filtros de aplicaciones tanto como pueda en lugar de añadir aplicaciones individuales a las reglas. A partir de PAN-OS 10.1, puede añadir aplicaciones a grupos de aplicaciones y filtros directamente desde Policy Optimizer, lo cual es una práctica recomendada porque le brinda visibilidad de todas las aplicaciones que ve una regla.

Anterior a PAN-OS 10.1, añada aplicaciones a grupos y filtros usando **Objects (Objetos)** > **Application Groups (Grupos de aplicaciones)** y **Objects (Objetos)** > **Application Filters (Filtro de aplicaciones)**.

STEP 4 | Decida qué aplicaciones añadir a una regla según el objetivo de la regla. El objetivo de la regla ayuda a determinar quién necesita acceso a las aplicaciones y cómo (origen, destino, inspección, registro) otorgar acceso.

STEP 5 | Reutilice los objetos de los filtros de aplicaciones y de los grupos de aplicaciones en la política para brindar a diferentes grupos de usuarios diferentes niveles de acceso a esas aplicaciones y/o tratar diferentes combinaciones de origen y destino de manera diferente.

User-ID es fundamental para crear prácticas recomendadas de la Política de seguridad basada en el principio de acceso con privilegios mínimos. Sin User-ID, no puede especificar quién puede usar las aplicaciones.

La reutilización de objetos del filtro de aplicaciones y de grupos de aplicaciones reduce la sobrecarga de la base de reglas al simplificarla.

Flujos de trabajo de la base de reglas de Policy Optimizer

Esta sección describe la transición de reglas basadas en puertos a reglas basados en aplicaciones y flujos de trabajo para la herramienta Policy Optimizer. Cómo utilizar Policy Optimizer describe los principales casos de uso y cómo utilizar la herramienta.

El objetivo final es restringir las reglas para que solo permitan aplicaciones autorizadas y aplicaciones que usted tolere para el uso de los empleados. En conjunto con eso, restringir a los usuarios que tengan motivos comerciales legítimos para acceder a diferentes aplicaciones. Utilice los logs de tráfico y el ACC para limitar el alcance de las reglas a usuarios específicos, para evitar un aprovisionamiento excesivo del acceso de los usuarios. Trabaje con propietarios de aplicaciones y otros grupos para comprender quién tiene motivos comerciales para acceder a las aplicaciones.

STEP 1 | Planifique una transición gradual de reglas basadas en puertos a reglas basadas en aplicaciones y comprenda los conceptos y métodos clave de transición.

Planificación y metodología de migraciones y nuevas implementaciones:

- Para las migraciones de reglas basadas en puertos a reglas basadas en aplicaciones, comience con su base de reglas de la Política de seguridad basada en puertos. Para nuevas implementaciones y migraciones, cree reglas basadas en filtros de aplicaciones para obtener visibilidad de diferentes tipos de aplicaciones y añada una regla general en la parte inferior de la base de reglas para no bloquear accidentalmente aplicaciones de misión crítica. Aplique las prácticas recomendadas de perfiles de Prevención de amenazas (en ambas direcciones) y perfiles de filtrado de URL (tráfico saliente) a estas reglas. A medida que las aplicaciones coincidan con las reglas generales, siga los consejos del Paso 2 para priorizar qué reglas comenzar a convertir y ajustar primero, y durante

cuánto tiempo observar las reglas con diferentes tipos de aplicaciones antes de realizar la transición a reglas basadas en aplicaciones.

Policy Optimizer le muestra las aplicaciones específicas de capa 7 (App-ID) que coinciden con cada regla basada en puerto.

- Ejecute informes de evaluación de prácticas recomendadas directamente en AIOps para establecer una línea de referencia que le permita comprender el estado actual de sus prácticas recomendadas. Ejecute informes periódicos para medir el progreso. El progreso significa menos reglas basadas en puertos, menos reglas no utilizadas y menos reglas con aplicaciones no utilizadas a lo largo del tiempo.

Planificación y metodología de implementaciones existentes:

- Si la implementación consta de reglas basadas en puertos o principalmente de reglas basadas en puertos, siga los consejos anteriores para migrar a una política basada en aplicaciones.
- Si la implementación consta principalmente de reglas basadas en aplicaciones, coloque una regla general en la parte inferior de la base de reglas de la Política de seguridad para descubrir y obtener visibilidad de las aplicaciones que no coinciden con otras reglas, con perfiles de seguridad estrictos para detener el tráfico malicioso. Siga los consejos de priorización del Paso 2 para endurecer las reglas.

Después de mover aplicaciones desde reglas basadas en puertos a reglas basadas en aplicaciones, seleccione las reglas basadas en puertos en Policy Optimizer y seleccione **Reset Rule Hit Counter (Restablecer recuento de resultados de reglas)**. Esto restablece el contador de **Days with no new apps (Días sin aplicaciones nuevas)** para que pueda ver cuándo más aplicaciones nuevas coinciden con las reglas originales basadas en puertos y evaluar si desea permitirlas o bloquearlas.

Después de ajustar una regla, espere hasta que **Days with no new apps (Días sin aplicaciones nuevas)** alcance al menos siete días antes de volver a revisar la regla para continuar ajustándola. Cuando las reglas generales y las reglas basadas en puertos ya no ven las aplicaciones que desea permitir, deshabilítelas o elimínelas. Tenga en cuenta las aplicaciones que su empresa utiliza solo para eventos periódicos antes de deshabilitar o eliminar una regla.

STEP 2 | Priorice y convierta reglas de la Política de seguridad basadas en puertos [reglas con la aplicación configurada en **any (cualquiera)**] en reglas basadas en aplicaciones de capa 7.

Priorice qué reglas convertir de reglas basadas en puertos a reglas basadas en aplicaciones y en qué fase de la transición. Estas técnicas son válidas para migraciones y nuevas implementaciones, y para implementaciones existentes basadas en aplicaciones donde necesita reforzar su base de reglas:

1. En implementaciones nuevas y existentes, bloquee inmediatamente el tráfico malicioso y peligroso conocido.
2. Implemente reglas generales basadas en filtros de aplicaciones.
3. Convierta reglas simples con aplicaciones conocidas después de una semana Por ejemplo, las reglas que controlan el puerto 21 (FTP), el puerto 53 (DNS) y el puerto 22 (SSH) son buenas candidatas

para una conversión rápida. Cuanto menos y más conocidas sean las aplicaciones en una regla basada en puertos, más confianza podrá tener al convertirla en una regla basada en aplicaciones.

4. Después de 30 días, convierta las reglas más estables. Las reglas que no ven nuevas solicitudes durante un período de 30 días y que controlan relativamente pocas solicitudes son buenas candidatas.
5. Después de al menos 30 días, comience a convertir las reglas de acceso a Internet (ssl, navegación web) y las reglas que reciben la mayor cantidad de tráfico.
6. Después de un período de tiempo apropiado para las aplicaciones vistas en la regla, convierta las reglas con pocas aplicaciones vistas.
7. A medida que convierte reglas, revise cada regla cuando **Days with no new apps (Días sin aplicaciones nuevas)** alcance al menos siete días (más tiempo para reglas complejas o reglas con muchas aplicaciones) y gestione nuevas aplicaciones según sea necesario.

La duplicación de reglas es la forma más segura de realizar la transición de reglas basadas en puertos a reglas basadas en aplicaciones. La duplicación conserva la regla original basada en puerto y coloca la regla clonada directamente encima de la regla original. Esto le permite crear reglas específicas basadas en aplicaciones a partir de la regla original, sin poner en riesgo la disponibilidad de la aplicación, como se muestra en este ejemplo de caso de uso de duplicación para migrar su navegación web y tráfico SSL a reglas basadas en aplicaciones. Las aplicaciones que no coinciden con las reglas duplicadas siguen coincidiendo con la regla basada en puertos original. Cuando la regla original deja de ver las aplicaciones que desea en su red durante un período de tiempo adecuado, puede desactivar o eliminar la regla original de forma segura.

Utilice grupos de aplicaciones y filtros de aplicaciones de forma adecuada a medida que convierte reglas.

Para escenarios de migración, siga las prácticas recomendadas para migrar a una política basada en aplicaciones.

STEP 3 | A medida que examina las reglas, utilice filtros de aplicaciones para bloquear los tipos de aplicaciones que sabe que no desea en su red. Bloquee el tráfico según subcategorías, etiquetas y características. Utilice filtros de aplicaciones para hacer excepciones a las reglas de bloqueo. No utilice el riesgo como criterio de filtro de bloqueo; utilícelo para determinar cómo inspeccionar, registrar y controlar el tráfico de forma adecuada.

Además de las reglas de bloqueo recomendadas para detener el tráfico malicioso conocido, revise sus reglas con regularidad y bloquee otro tráfico que sepa que no desea:

1. Identifique los tipos de aplicaciones que no desea en su red y cree filtros de aplicaciones que coincidan con ellos. Cree reglas de bloqueo basadas en esos filtros de aplicaciones y colóquelas delante de cualquier regla general (o duplique la regla a partir de una regla existente y coloque la regla duplicada directamente encima de la regla original en la base de reglas).
2. Determine si hay aplicaciones específicas dentro de los tipos de aplicaciones bloqueadas que desea permitir en su red. Duplique la regla de bloqueo, cambie la **Action (Acción)** a **Allow (Permitir)**y elimine todas las aplicaciones excepto las que desea permitir. Coloque la regla de permitir directamente encima de la regla de bloqueo para crear excepciones a la regla de bloqueo.
3. Supervise la regla de bloqueo para ver si desea permitir otras aplicaciones bloqueadas. Si creó una regla de permitir para excepciones, añada las aplicaciones que desea permitir a dicha regla. De lo

contrario, cree una nueva regla de permitir para las aplicaciones y colóquela directamente encima de la regla de bloqueo en la base de reglas.

Por ejemplo, las aplicaciones para compartir archivos pueden ser particularmente arriesgadas. Descifre el tráfico y, en la regla de la Política de seguridad, permita solo las aplicaciones específicas para compartir archivos que utiliza con fines comerciales, solo para los usuarios necesarios e inspeccione y registre el tráfico. En la siguiente regla de la base de reglas, utilice un filtro de aplicaciones basado en la subcategoría **file-sharing (uso compartido de archivos)** para bloquear todas las aplicaciones de uso compartido de archivos que no permita explícita y expresamente.

STEP 4 | Elimine las aplicaciones no utilizadas de las reglas sobreaprovisionadas.

Comprenda el propósito de una aplicación antes de eliminarla de una regla.

- Compare las **Apps Used (Aplicaciones utilizadas)** con las **Apps Allowed (Aplicaciones permitidas)**. Si la regla permite más aplicaciones de las que utiliza, examine las aplicaciones no utilizadas y determine si puede eliminarlas.
- Tenga en cuenta las aplicaciones que se utilizan únicamente para eventos trimestrales, anuales u otros eventos periódicos. Asegúrese de capturar un historial lo suficientemente largo de la regla para ver esas aplicaciones. También tenga en cuenta las aplicaciones que están activas en su entorno de prueba y que se han añadido a su entorno de producción en previsión de la autorización de la aplicación.

STEP 5 | Elimine las reglas no utilizadas de la base de reglas de la Política de seguridad.

Las reglas no utilizadas desordenan y complican la base de reglas. Uso de reglas le muestra información sobre reglas no utilizadas en diferentes períodos de tiempo. Evalúe las aplicaciones en las reglas para ver si las necesita aunque no se hayan utilizado. Antes de eliminar reglas no utilizadas, tenga en cuenta:

- **Bloquear reglas sin resultados**: no deshabilite ni elimine estas reglas. Por ejemplo, una regla de bloqueo que utiliza una EDL de amenazas no recibe ningún resultado. Eso está bien, pero desea continuar bloqueando en caso de que tráfico malicioso intente acceder a su red.
- **Reglas temporales**: por ejemplo, reglas para contratistas o auditores. En lugar de eliminar esas reglas, si hay un tiempo de acceso regular, configure un horario para controlar cuándo la regla está en vigor. Si el acceso es intermitente, deshabilite las reglas y habilítelas cuando sea necesario.
- **Reglas de políticas deshabilitadas**: aplique una etiqueta con la fecha en que se deshabilitaron las reglas. Si las reglas no se utilizan dentro de un período de tiempo determinado, por ejemplo, más de un año, es posible que la regla se pueda eliminar. Añada una **Description (Descripción)** para indicar por qué la regla está deshabilitada y por qué o cuándo puede ser necesario habilitarla, por ejemplo, para el acceso de un auditor o un contratista.
- **Aplicaciones utilizadas periódicamente**: algunas aplicaciones solo se utilizan para eventos trimestrales, anuales u otros eventos periódicos. Capture un historial lo suficientemente largo de reglas que controlan este tipo de aplicaciones para asegurarse de que ya no estén en uso.

STEP 6 | Asegúrese de que cada regla tenga adjunto un perfil de reenvío de logs adecuado.

Identifique reglas sin perfiles de reenvío de logs y añádales perfiles [**Policies (Políticas)** > **Security (Seguridad)** > **Policy Optimizer** > **Log Forwarding for Security Services (Reenvío de logs para servicios de seguridad)**].

STEP 7 | Convierta reglas amplias basadas en filtros de aplicaciones en reglas acotadas basadas en grupos de aplicaciones.

Utilice Estadísticas de uso de reglas para comprender cómo se usan las reglas y use Policy Optimizer para añadir aplicaciones a grupos de aplicaciones [PAN-OS 10.1 y posteriores; para PAN-OS 10.0 y anteriores, añada aplicaciones a grupos de aplicaciones en **Objects (Objetos)** > **Application Groups (Grupo de aplicaciones)**] y cree reglas más estrictas.

El objetivo final es permitir solo las aplicaciones que se autorizan en lugar de permitir una gama más amplia de aplicaciones que coincidan con un filtro de aplicaciones. Utilice filtros de aplicaciones para descubrir aplicaciones en su red y bloquear subcategorías amplias de aplicaciones, y utilice grupos de aplicaciones para especificar las aplicaciones exactas que desea permitir. Para convertir reglas basadas en filtros de aplicaciones en reglas basadas en grupos de aplicaciones mediante Policy Optimizer:

- Examine las aplicaciones que coinciden con las reglas basadas en filtros de aplicaciones y decida qué aplicaciones desea permitir.
- Para cada regla basada en un filtro de aplicaciones, seleccione las aplicaciones que desea permitir y añada las aplicaciones a un grupo de aplicaciones en una regla duplicada o existente.
- Después de mover las aplicaciones de reglas basadas en filtros de aplicaciones, a reglas basadas en grupos de aplicaciones. seleccione esas reglas en Policy Optimizer y elija **Reset Rule Hit Counter (Restablecer contador de resultados de reglas)**. Esto restablece el contador **Days with no new apps (Días sin aplicaciones nuevas)** para que pueda ver cuándo las aplicaciones nuevas coinciden con las reglas basadas en filtros de aplicaciones.
- Supervise las reglas basadas en filtros de aplicaciones hasta que el contador **Days with no new apps (Días sin aplicaciones nuevas)** alcance un umbral que indique que una regla ya no ve nuevas aplicaciones. El umbral depende de su entorno y de los tipos de aplicaciones con las que coincida el filtro de aplicaciones. Tenga en cuenta las aplicaciones utilizadas solo en determinados períodos, como eventos trimestrales o anuales, y deje el filtro activado el tiempo suficiente para ver esas aplicaciones y poder añadirlas a los grupos de aplicaciones correspondientes. Si la regla del filtro de aplicaciones no coincide con ninguna aplicación que desee en su red, deshabilite o elimine la regla, según la política de su empresa.

STEP 8 | Revise y actualice las reglas de la Política de seguridad a medida que nuevas aplicaciones se implementan a su entorno.

Revise los nuevos App-ID con regularidad en el Visor de aplicaciones nuevas. Añada aplicaciones a grupos de aplicaciones nuevos y existentes o añada aplicaciones directamente a reglas de la Política de seguridad existentes. Continúe convirtiendo filtros de aplicaciones en grupos de aplicaciones.

Prácticas recomendadas de App-ID Cloud Engine

El App-ID Cloud Engine (ACE) identifica miles de aplicaciones SaaS que el cortafuegos identificaba previamente como ssl o tráfico de navegación web, no como aplicaciones específicas. ACE proporciona a estas aplicaciones SaaS los App-ID específicos para que usted pueda obtener visibilidad de ellos, controlarlos y utilizarlos explícitamente en la política de seguridad.

ACE requiere PAN-OS 10.1 o posterior y una suscripción a SaaS Security Inline. ACE está disponible en Prisma Access Cloud Services 3.0 Innovation *para Panorama Managed Prisma Access y también en* Cloud Managed Prisma Access*.*

Los App-ID de ACE solo son compatibles con la Política de seguridad. No puede usar los App-ID de ACE en ningún otro tipo de regla de políticas.

El cortafuegos descarga todo el catálogo de App-ID de ACE, pero solo descarga las firmas de App-ID de ACE para las aplicaciones que se ven en el entorno.

ACE controla las aplicaciones SaaS en los flujos salientes y actúa como un agente de seguridad de acceso a la nube (CASB). En las nuevas implementaciones, ACE identifica las aplicaciones SaaS de su red para simplificar el paso a la política basada en aplicaciones de capa 7.

En implementaciones existentes, ACE proporciona herramientas para comprender y gestionar de forma segura las posiblemente muchas aplicaciones SaaS que se identificaron a priori como ssl o tráfico de navegación web, y controlarlas explícitamente en la Política de seguridad.

Descifre *todo el tráfico que las regulaciones locales, las normativas, los requisitos comerciales y las consideraciones de privacidad permiten tan pronto como sea posible para proporcionar información de aplicaciones más precisa y obtener visibilidad de las aplicaciones ACE. Sin descifrado, el cortafuegos a menudo puede identificar las aplicaciones principales, pero generalmente no puede identificar las aplicaciones funcionales. Por ejemplo, el cortafuegos ve "facebook", pero no ve facebook-post, facebook-download, facebook-file-sharing, etc. Debe descifrar el tráfico para obtener visibilidad y control de las aplicaciones funcionales. Para el descifrado* proxy SSL de reenvío *(saliente), implemente primero User-ID y filtrado de URL para que pueda orientar el descifrado de manera efectiva.*

STEP 1 | Comprenda cómo funcionan los App-ID de ACE en el cortafuegos antes de habilitar ACE.

Lea el Procesamiento ACE y uso de la política para aprender cómo el cortafuegos gestiona los App-ID de ACE, incluido:

- Cómo y cuándo el cortafuegos descarga los App-ID de ACE.
- Las diferencias entre los App-ID de ACE y los App-ID del contenido entregado.
- Cómo resuelve el cortafuegos los conflictos entre los App-ID de ACE, los App-ID del contenido entregado y los App-ID personalizados; incluidas las aplicaciones contenedor (por ejemplo, facebook) y sus aplicaciones funcionales (por ejemplo, facebook-post, facebook-download, etc.).
- Comportamiento HA.
- Comportamiento de Panorama al confirmar o enviar.

ACE identifica aplicaciones SaaS específicas que el cortafuegos identificó previamente como ssl o tráfico de navegación web. Cuando habilite ACE:

- Si tiene una regla de políticas de seguridad que permite el tráfico ssl y de navegación web, los App-ID de ACE descargados coinciden con esa regla a menos que coincidan con un filtro de aplicaciones utilizado en una regla. Los App-ID de ACE coinciden con un filtro de aplicaciones basado en los criterios del filtro, incluidas las etiquetas, al igual que los App-ID entregados con contenido. Si un App-ID de ACE coincide con un filtro de aplicaciones en una regla, la aplicación se añade

implícitamente a la regla. Esa regla controla la aplicación de ACE en lugar de la regla de navegación ssl/web, incluida la acción de la regla (permitir o denegar), los usuarios que pueden acceder a la aplicación, los orígenes y destinos, y cómo se inspecciona y registra la aplicación.

- Hasta que añade un App-ID de ACE explícitamente a una regla o un App-ID de ACE coincida con un filtro de aplicaciones que lo añada implícitamente a una regla, una aplicación ACE seguirá coincidiendo con la regla que permite la navegación ssl/web, al igual que antes de habilitar ACE.
- Si no tiene ninguna regla que permita el tráfico ssl y de navegación web, siga los consejos del Paso 3 para descubrir y controlar los App-ID de ACE.

Cuando usa un el App-ID de ACE explícitamente en la política, el cortafuegos trata la aplicación de la misma manera que trata las aplicaciones entregadas con contenido.

STEP 2 | Revise su base de reglas de políticas de seguridad para encontrar reglas que utilicen filtros de aplicaciones antes de habilitar ACE.

Los filtros de aplicaciones permiten aplicaciones basadas en criterios de filtro coincidentes, incluidas las etiquetas, por lo que añaden automáticamente aplicaciones a las reglas y hay que examinar esas reglas para ver qué aplicaciones específicas permite cada filtro y quién tiene acceso a dichas aplicaciones. Cuando un App-ID de ACE coincide con un filtro de aplicaciones en una regla, es posible que esa regla no permita los mismos usuarios que la regla de navegación ssl y web. Los usuarios que tenían acceso a la aplicación en la regla ssl y de navegación web pueden perder el acceso a la aplicación porque ya no coincide con esa regla, y esos usuarios no están especificados en la regla explícita.

Es fundamental entender quién necesita usar qué aplicaciones para fines empresariales, especialmente en entornos con muchas reglas, aplicaciones y grupos de usuarios. Por ejemplo, si usa la etiqueta ***Web Apps (Aplicaciones web)*** *en un grupo de aplicaciones en una regla, la etiqueta añade implícitamente a la regla aplicaciones de ACE coincidentes. Esas aplicaciones de ACE no coinciden con la regla de navegación ssl y web y solo los usuarios especificados en la regla* ***Web Apps (Aplicaciones web)*** *pueden acceder a ellas.*

Si ninguna regla tiene filtros de aplicaciones, no hay riesgo de que las aplicaciones de ACE coincidan automáticamente con las reglas existentes después de habilitar ACE porque aún no ha añadido ninguna aplicación de ACE explícitamente a las reglas.

Si utiliza filtros de aplicaciones en las reglas de políticas de seguridad, cuando habilita ACE:

- Para las reglas de denegación, las aplicaciones de ACE que coinciden con la regla se bloquean, que es exactamente lo que pretende hacer con las aplicaciones que coinciden con la regla de denegación. La regla es más efectiva porque ahora bloquea aplicaciones SaaS no autorizadas que el cortafuegos no podría identificar sin ACE.
- Para permitir reglas, supervise de cerca las aplicaciones que la regla permite. Añadir aplicaciones implícitamente con un filtro se basa en criterios, no en que un administrador añada aplicaciones específicas a propósito. Las reglas más afectadas son las reglas con filtros basados en etiquetas

amplias como **Web App (Aplicación web)**, que se aplica a la mayoría de las App-ID tanto de ACE como de contenido entregado.

En implementaciones existentes, tenga en cuenta que si tiene una regla que permite el tráfico ssl y de navegación web, entonces estaba permitiendo todas las aplicaciones que ACE ahora identifica. Use filtros para bloquear los tipos de tráfico que sabe que no quiere y continúe permitiendo el resto de aplicaciones mientras evalúa lo que desea autorizar y lo que quiere bloquear.

El paso 3, el paso 4 y el paso 5 muestran cómo usar filtros de aplicaciones para añadir App-ID de ACE a reglas de forma segura.

STEP 3 | Permita explícitamente que las aplicaciones de ACE utilicen filtros de aplicaciones para que pueda evaluar las aplicaciones de manera controlada.

Crear filtros de aplicaciones para permitir los tipos de aplicaciones que desea en su red es más fácil que revisar periódicamente todas las nuevas aplicaciones de ACE para determinar qué aplicaciones específicas permitir. Los filtros de aplicaciones le permiten examinar los mismos tipos de aplicaciones, una al lado de la otra, y determinar cuáles desea permitir para fines comerciales.

1. Cree un filtro de aplicaciones basado en la etiqueta **App-ID Cloud Engine**, que coincida con todos los App-ID de ACE (aplicaciones que se identificaron como ssl o navegación web antes de ACE). Adjunte el filtro a una regla de Política de seguridad con los perfiles de seguridad y el registro apropiados, y coloque la regla en la parte inferior de la base de reglas de la Política de seguridad. Esto garantiza que la regla coincida y permita todos los App-ID de ACE nuevos y existentes a menos que se especifiquen en una regla anterior. También garantiza que las reglas de bloqueo del cortafuegos entren en vigor antes de que el cortafuegos compare el tráfico con la regla de permitir de ACE.
2. A medida que se familiarice con las aplicaciones de ACE, cree reglas de filtro de aplicaciones más específicas basadas en subcategorías, etiquetas, riesgos y características para adaptarse a grupos más pequeños de aplicaciones. Coloque estas reglas para permitir directamente encima de la regla general permitir de ACE basada en la etiqueta **App-ID Cloud Engine**. Reducir las aplicaciones que coinciden con un filtro le permite examinar las aplicaciones más similares unas con otras y determinar cuáles desea permitir para fines comerciales.
3. Revise el Nuevo visor de aplicaciones en Policy Optimizer con frecuencia para ver qué App-ID de ACE descargadas coinciden con las reglas de la Política de seguridad y para obtener una mayor visibilidad de esas aplicaciones. Evaluar las aplicaciones y determinar si permitirlas o bloquearlas.

No añada usuarios a reglas que tengan filtros de aplicaciones para ampliarlas porque eso permite más acceso del necesario a las aplicaciones. Sobre aprovisionar el acceso de los usuarios aumenta el riesgo y va en contra de los principios de acceso a la red de la confianza cero Zero Trust. Permitir solo usuarios que necesitan acceso para fines comerciales.

STEP 4 | Utilice filtros de aplicaciones para bloquear los tipos de aplicaciones que no desea en su red, en función de las subcategorías, etiquetas y características. No utilice el riesgo como criterio de filtro de bloqueo (el riesgo es una evaluación del riesgo relativo dentro de una categoría o subcategoría, no

necesariamente de uso malicioso). Utilice el riesgo para determinar cómo inspeccionar, registrar y controlar el tráfico adecuadamente.

El bloqueo basado en filtros de aplicaciones es más fácil que revisar periódicamente todas las nuevas aplicaciones de ACE para determinar lo que hace y no hacer en su red. Usar filtros de aplicaciones significa que el cortafuegos bloquea inmediatamente nuevas aplicaciones que usted sabe que no quiere.

1. Determine los tipos de aplicaciones de ACE que no desea en su red. Cree reglas de bloqueo basadas en esos tipos de aplicación y colóquelas por encima de las reglas generales.
2. Determine si hay aplicaciones específicas dentro de esos tipos que desea permitir en su red. Si desea permitir algunas de las aplicaciones:
    1. Duplique la regla de bloqueo.
    2. Cambie la **Action (Acción)** a **Allow (Permitir)**.
    3. Elimine todas las aplicaciones de la regla excepto las aplicaciones que desea permitir.
    4. Especifique los usuarios que necesitan acceso a las aplicaciones permitidas, añada los perfiles de seguridad apropiados y configure el registro de logs.
    5. Coloque la nueva regla para permitir directamente encima de la regla bloquear para crear excepciones a la regla de bloqueo.
3. Supervise la regla de bloqueo para ver si hay otras aplicaciones específicas que desee permitir y añádalas a una regla de permitir existente o cree una nueva regla de permitir para realizar dichas excepciones.

Por ejemplo, las aplicaciones para compartir archivos pueden ser particularmente arriesgadas. Permita que solo las aplicaciones de intercambio de archivos que utiliza para fines comerciales, solo para los usuarios necesarios, e inspeccione y registre el tráfico. En la siguiente regla de la base de reglas de políticas de seguridad, utilice un filtro de aplicaciones basado en la subcategoría **file-sharing (uso compartido de archivos)** para bloquear todas las aplicaciones de uso compartido de archivos que no permita explícita y expresamente. Supervise la regla de bloqueo para asegurarse de que no bloquea las aplicaciones de intercambio de archivos que desea permitir.

STEP 5 | Convierta reglas amplias basadas en filtros de aplicaciones en reglas acotadas basadas en grupos de aplicaciones.

Las Estadísticas de uso de reglas muestran cómo se usan las reglas en su entorno. Utilice Policy Optimizer para añadir aplicaciones a grupos de aplicaciones (PAN-OS 10.1 y posterior) o añadir aplicaciones a grupos de aplicaciones de forma manual para crear reglas más estrictas.

El objetivo final es permitir solo las aplicaciones que se autorizan en lugar de permitir una gama más amplia de aplicaciones que coincidan con un filtro de aplicaciones. Utilice filtros de aplicaciones para descubrir aplicaciones en su red y grupos de aplicaciones para especificar las aplicaciones exactas que desea permitir. Para usar Policy Optimizer para convertir reglas basadas en filtros de aplicaciones en reglas basadas en grupos de aplicaciones:

- Examine las aplicaciones que coinciden con las reglas basadas en filtros de aplicaciones y decida qué aplicaciones desea permitir.
- Para cada regla basada en un filtro de aplicaciones, seleccione las aplicaciones que desea permitir y añada las aplicaciones a un grupo de aplicaciones en una regla duplicada o existente.
- Después de mover las aplicaciones a reglas basadas en grupos de aplicaciones, seleccione las reglas basadas en filtros de aplicaciones originales en Policy Optimizer y elija **Reset Rule Hit Counter (Restablecer contador de resultados de reglas)**. Esto restablece el contador de **Days with no new**

apps (Días sin aplicaciones nuevas) para que pueda ver cuándo las nuevas aplicaciones coinciden con las reglas basadas en filtros de aplicaciones.

- Supervise las reglas basadas en filtros de aplicaciones para ver cuándo el contador **Days with no new apps (Días sin aplicaciones nuevas)** alcanza un umbral que indica que una regla ya no ve nuevas aplicaciones. El umbral depende de su entorno y de los tipos de aplicaciones con las que coincida el filtro de aplicaciones. Tenga en cuenta las aplicaciones utilizadas solo en ciertos períodos, como eventos trimestrales o anuales, y deje el filtro en su lugar el tiempo suficiente para ver dichas aplicaciones. Si la regla del filtro de aplicaciones no coincide con ninguna aplicación que desee en su red, deshabilite o elimine la regla, según la política de su empresa.

*Mantenga la regla basada en la etiqueta **App-ID Cloud Engine** en la parte inferior de la base de reglas como regla general para permitir nuevas aplicaciones de ACE. Después de pasar de reglas basadas en filtros de aplicaciones a reglas basadas en grupos de aplicaciones, todos los nuevos App-ID de ACE coinciden con la regla general. Examine periódicamente la regla para determinar qué aplicaciones añadir a las reglas y grupos de aplicaciones existentes, qué aplicaciones requieren nuevas reglas y qué aplicaciones desea bloquear.*

STEP 6 | Compruebe el **New App Viewer (Visor de aplicaciones nuevas)** con frecuencia para obtener visibilidad y control explícito de los nuevos App-ID de ACE que anteriormente se identificaban como aplicaciones ssl o de navegación web. Utilice los nuevos App-ID de ACE explícitamente en la política en lugar de como ssl o aplicaciones de navegación web.

Revise los nuevos App-ID de ACE que el cortafuegos descarga regularmente en el Nuevo visor de aplicaciones de Policy Optimizer. Utilice Policy Optimizer para añadir aplicaciones a grupos de aplicaciones existentes y nuevos, o para añadir aplicaciones directamente a las reglas de políticas de seguridad existentes. Siga utilizando Policy Optimizer para convertir filtros de aplicaciones a grupos de aplicaciones.

Prácticas recomendadas de recomendaciones de políticas

La Recomendación de políticas para SaaS y la Recomendación de políticas de IoT permiten a los administradores de SaaS Security y de IoT Security crear recomendaciones de políticas de seguridad y enviarlas a:

- Cortafuegos PAN-OS y Panorama (Recomendación de políticas de IoT y SaaS).
- Panorama Managed Prisma Access (Recomendación de política de SaaS e IoT).
- Cloud Managed Prisma Access (solo recomendación de política SaaS).

Los servicios basados en la nube, como la recomendación de políticas de IoT y SaaS, no se pueden utilizar en entornos aislados porque requieren una conexión a la nube.

En entornos aislados, para la IoT Security, considere usar Panorama como motor de gestión para interactuar con el servicio en la nube y recibir recomendaciones de políticas. Luego envíe las recomendaciones a los cortafuegos gestionados que no están conectados a la nube. Esta solución solo se aplica a las recomendaciones de políticas en sí. Funciones como la asignación device-to-IP requieren conectividad en la nube para los dispositivos gestionados.

La Recomendación de política de SaaS controla las aplicaciones SaaS no autorizadas en PAN-OS y Prisma Access. La Recomendación de política de IoT controla los dispositivos de red no gestionados en PAN-OS y Panorama Managed Prisma Access. Sus flujos de trabajo tienen muchas similitudes.

Requisitos:

- Recomendación de política de SaaS
  - Licencia de SaaS Security Inline

    La licencia de SaaS Security Inline incluye App-ID Cloud Engine (ACE), que proporciona miles de App-ID de SaaS para recomendaciones de políticas. La Recomendación de política de SaaS requiere la Implementación de ACE.
  - PAN-OS 10.1 o posterior para PAN-OS y Panorama Managed Prisma Access.
  - Enterprise Data Loss Prevention (DLP) para implementar las prácticas recomendadas de prevención de pérdida de datos y obtener visibilidad de los datos.
  - Configure Azure AD para User-ID para especificar usuarios en las recomendaciones de reglas de políticas (no puede crear reglas de políticas basadas en usuarios sin User-ID).
- Recomendación de política de IoT:
  - Licencia de IoT Security.
  - Requisitos previos de IoT Security.
  - Garantice el soporte adecuado para PAN-OS y/o soporte en Panorama Managed Prisma Access.
  - Habilite Device-ID en cada zona en la que desee controlar los dispositivos IoT. (Device- ID es para la IoT Security lo que el User-ID es para SaaS Security; Device-ID es el "quién" de IoT Security).

Panorama puede enviar recomendaciones de políticas de IoT y SaaS solo a cortafuegos que tengan las licencias adecuadas, por lo que deben estar instaladas en cortafuegos que utilicen recomendaciones de políticas de IoT y SaaS. Si los dispositivos gestionados no tienen las licencias adecuadas, el envío falla.

Además de las licencias, para funcionar correctamente y siguiendo las prácticas recomendadas, las recomendaciones de políticas tanto de IoT como de SaaS requieren:

- Un certificado de dispositivo válido en cada dispositivo que utilice la recomendación de política de IoT o SaaS.
- Una conexión a Cortex Data Lake (CDL) para visibilidad del tráfico.
- Reenvío de logs a CDL configurado en cada recomendación de regla de Política de seguridad. Para SaaS Security, reenvíe logs de tráfico, logs de filtrado de URL y logs de amenazas como mínimo.

La recomendación de políticas de SaaS le ayuda a controlar las aplicaciones no autorizadas.

Para proteger las aplicaciones SaaS autorizadas*, utilice la* API de seguridad SaaS*. La API de SaaS Security proporciona seguridad para* aplicaciones SaaS compatibles normalmente aprobadas *y le permite* gestionar políticas para dichas aplicaciones SaaS.

- Conceptos de recomendaciones de políticas: ideas cruciales que se deben comprender antes de recomendar políticas.
- Flujo de trabajo de recomendaciones de políticas: flujos de trabajo de SaaS e IoT y prácticas recomendadas de flujo de trabajo.

Conceptos de recomendaciones de políticas

Las recomendaciones de políticas de SaaS e IoT tienen muchas similitudes en sus flujos de trabajo y objetivos. Los flujos de trabajo y el proceso de pensamiento para la recomendación de políticas en PAN-OS y Prisma Access también tienen muchas similitudes. Revise Prácticas recomendadas de las reglas de la Política de seguridad para comprender mejor las prácticas recomendadas para los componentes de las reglas.

Cloud Managed Prisma Access no admite la recomendación de políticas de IoT.

Los administradores de SaaS Security e IoT Security envían recomendaciones de políticas a PAN-OS y Prisma Access. Los administradores de PAN-OS importan recomendaciones de políticas de SaaS y recomendaciones de políticas de IoT en PAN-OS y Panorama Managed Prisma Access. Los administradores de Cloud Managed Prisma Access importan recomendaciones de políticas de SaaS en la plataforma en la nube. A menudo, diferentes administradores deben cooperar para recomendar e implementar reglas de políticas, por lo que una buena comunicación entre administradores es fundamental.

Las prácticas recomendadas generales para la recomendación de la política de IoT incluyen:

- Sepa si los dispositivos descubiertos pertenecen a su red.
- Asegúrese de que las aplicaciones descubiertas que ve para los dispositivos sean apropiadas para dichos dispositivos.
- Comprender las vulnerabilidades detectadas en los dispositivos.
- Deje suficiente tiempo para que IoT Security recopile suficientes datos sobre los dispositivos para identificarlos con alta fiabilidad.

Las prácticas recomendadas generales para la recomendación de la política de SaaS incluyen:

- Conozca las aplicaciones y los tipos de aplicaciones que deberían y no deberían estar en su red. Cree una lista formal de aplicaciones y tipos de aplicaciones autorizadas, toleradas y no autorizadas, y etiquete las aplicaciones de forma adecuada a medida que obtenga visibilidad de ellas. Vea datos de uso de aplicaciones no autorizadas y use filtros para ver quién usa las aplicaciones y cómo se usan. Utilice las herramientas de **Visibility (Visibilidad)** para ver las aplicaciones descubiertas y luego etiquetar las aplicaciones descubiertas.
- Comprenda los datos que desea buscar en los archivos para poder crear perfiles DLP adecuados para las recomendaciones de reglas de políticas.
- La mayoría de las recomendaciones de reglas de políticas de SaaS son para bloquear el tráfico. Aplicar el principio de acceso con privilegios mínimos a las aplicaciones SaaS es más complejo que aplicarlo solo a aplicaciones de contenido entregado porque hay decenas de miles de aplicaciones SaaS que controlar. Si las recomendaciones de políticas de SaaS son demasiado estrictas, estas pueden afectar a

las aplicaciones comerciales. Asegúrese de comprender las aplicaciones y los tipos de aplicaciones que desea bloquear antes de hacerlo.

Utilice filtros para centrarse en categorías de alto riesgo, como la transferencia de archivos y aplicaciones de CMS, y para comprobar qué aplicaciones tienen el mayor uso. Céntrese primero en esas categorías y subcategorías.

- Utilice tantos componentes basados en contexto como sea posible para crear recomendaciones de políticas de acceso con privilegios mínimos. Implemente User-ID mediante Cloud Identity Engine (CIE) (requiere Azure AD) para realizar las excepciones de acceso necesarias a usuarios y grupos. Utilice Enterprise DLP para evitar la pérdida de datos confidenciales.
- Para Cloud Managed Prisma Access, si la política administrativa de su organización lo permite, añada la aplicación SaaS Security a la consola de gestión de la nube. Utilice la consola de gestión de la nube para gestionar las recomendaciones de políticas de SaaS (y SaaS Security y otras aplicaciones de la nube) en lugar de usar aplicaciones independientes para obtener los siguientes beneficios:
  - Gestionar todos los elementos de seguridad de la nube desde una única interfaz en lugar de desde diferentes interfaces de aplicaciones.
  - Un administrador puede realizar todas las acciones de recomendación de políticas SaaS, incluida la adición de la regla a la base de reglas de Prisma Access. Si gestiona con la aplicación independiente, puede crear la recomendación de política, pero debe cambiar a otra aplicación o transferirla a otro administrador para añadir la regla a Prisma Access.

Para utilizar SaaS Security y Enterprise DLP en la consola de gestión de la nube, debe habilitar Web Security en la consola. (Esta es una función gratuita, no una suscripción).

Puede crear recomendaciones de políticas de SaaS utilizando recomendaciones de políticas predefinidas y creando recomendaciones de políticas creadas por el usuario.

Flujo de trabajo de recomendaciones de políticas

Este flujo de trabajo es válido para IoT Security, para la aplicación SaaS Security (PAN-OS, Panorama Managed Prisma Access) y para la consola de gestión de la nube (Cloud Managed Prisma Access). Cada paso indica qué administradores están involucrados. Es útil que cada administrador comprenda las responsabilidades de otros administradores que participan en las recomendaciones de políticas.

STEP 1 | (*Todos los administradores*) Cree líneas abiertas de comunicación entre los administradores que administren diferentes partes de la recomendación de políticas.

La recomendación de políticas a menudo requiere que diferentes administradores trabajen juntos para recomendar, importar e integrar nuevas reglas de políticas de SaaS Security y IoT Security en la base de reglas de PAN-OS o Prisma Access. Diseñe un proceso que garantice una buena comunicación cuando un administrador de IoT Security o SaaS Security entregue una recomendación de política a un administrador de Panorama, Prisma Access o de cortafuegos. El traspaso se produce después de que un administrador de IoT Security o SaaS Security crea una nueva regla, modifica una regla existente o elimina una regla y habilita (envía en SaaS Security) o activa (IoT Security) la regla.

El flujo de trabajo de administración es:

1. **Los administradores de SaaS Security** crean nuevas recomendaciones de reglas, añaden aplicaciones, usuarios/grupos de usuarios y perfiles DLP, y configuran la acción. Revisan las recomendaciones de reglas y luego las envían a PAN-OS, Panorama Managed Prisma Access o

Cloud Managed Prisma Access. Revise las pautas para la colaboración y autoría de administradores de SaaS Security.

Los administradores de IoT Security evalúan las recomendaciones de reglas generadas automáticamente, las modifican según sea necesario, crean conjuntos de políticas (grupos de recomendaciones de reglas basadas en el tráfico de dispositivos IoT en el mismo perfil de dispositivo) y las envían a PAN-OS y Panorama Managed Prisma Access.

2. **Los administradores de PAN-OS y Prisma Access** importan recomendaciones de políticas de SaaS e IoT. Evalúan recomendaciones de reglas, las importan y añaden grupos del Perfil de seguridad y otros objetos a las reglas. También ordenan las reglas en la base de reglasde la Política de seguridad. Cuando Panorama envía recomendaciones de políticas a los cortafuegos y a Prisma Access, los administradores del cortafuegos y de Prisma importan las reglas recomendadas.

   Los administradores deben comunicarse para añadir los objetos apropiados a las reglas recomendadas y comprender el propósito de esas reglas.

   Para Cloud Managed Prisma Access, el mismo administrador puede gestionar tanto las recomendaciones de políticas de SaaS como las tareas de Prisma Access, especialmente si el administrador gestiona ambas aplicaciones en la consola de gestión en la nube.

3. **Los administradores de SaaS Security e IoT Security** actualizan o eliminan una recomendación de regla y luego envían el cambio a PAN-OS o Prisma Access.

   Los administradores de PAN-OS y Prisma Access ven la actualización o eliminación de la regla e importan la regla actualizada o eliminan la regla de PAN-OS o Prisma Access.

La comunicación entre administradores es crucial para que todas las partes comprendan el propósito de las reglas recomendadas, el propósito de las actualizaciones de las reglas y por qué se elimina una regla. La comunicación entre administradores ayuda a garantizar que las recomendaciones de políticas de SaaS e IoT no se queden en PAN-OS o Prisma Access esperando que un administrador note su presencia y las importe a la base de reglas.

STEP 2 | (*Administrador de SaaS Security y IoT Security*) Los administradores de SaaS Security deben evaluar los riesgos de las aplicaciones SaaS no autorizadas y los administradores de IoT Security deben comprender los perfiles de dispositivos, que describen los tipos de dispositivos no gestionados en la red y su comportamiento.

IoT Security aprende automáticamente sobre los dispositivos no gestionados en la red y crea un perfil de dispositivo para cada conjunto de dispositivos similares. El perfil describe las características de los dispositivos.

Familiarícese con las aplicaciones SaaS y los dispositivos IoT en su red:

- SaaS: espere al menos siete días hábiles de datos antes de analizar una solicitud para recomendar una política. Recopile suficientes datos para comprender la aplicación y su uso comercial.

  IoT: supervise la lista de perfiles de dispositivos para ver cuáles son elegibles para la recomendación de políticas. Puede crear una recomendación de política cuando la clasificación de confianza para un perfil de dispositivo alcance el 90 %, lo que indica una alta confianza en el comportamiento del dispositivo. Algunos dispositivos producen menos tráfico y pueden tardar en alcanzar una clasificación de confianza alta. Deje tiempo para que IoT Security recopile datos suficientes para lograr una clasificación de confianza del 90 %.

- SaaS: comprenda cómo y por qué los usuarios utilizan aplicaciones SaaS específicas y si existen motivos comerciales para permitir dichas aplicaciones.

  IoT: comprenda si los dispositivos descubiertos pertenecen a su red. Si su empresa es bancaria, entonces ver un dispositivo médico en su red puede indicar un problema.
- SaaS: evalúe la seguridad y privacidad, gestión de acceso a identidades y atributos de cumplimiento de las aplicaciones SaaS en función de la tolerancia al riesgo.

  IoT: en entornos médicos, evalúe el riesgo de cumplimiento de los dispositivos médicos de IoT.
- SaaS:etiquete aplicaciones autorizadas, toleradas y no autorizadas para clasificarlas.

STEP 3 | (*Administrador de SaaS Security*) Configure las recomendaciones de políticas de SaaS predefinidas. (Administradores de IoT Security ir al Paso 5).

Las recomendaciones de reglas de políticas de SaaS predefinidas bloquean el acceso a aplicaciones, el acceso a cuentas personales y el acceso y uso compartido de contenido; y exigen el acceso de solo lectura para los usuarios apropiados. Añadir aplicaciones a recomendaciones predefinidas es una manera fácil de comenzar a bloquear aplicaciones SaaS.

Para utilizar SaaS Security y Enterprise DLP en la consola de gestión de la nube, debe habilitar Web Security en la consola. (Esta es una función gratuita).

En la consola de gestión en la nube, el mismo administrador puede crear recomendaciones de políticas de SaaS e importarlas a Prisma Access.

1. Seleccione una regla predefinida. (**Discovered Apps (Aplicaciones descubiertas)** > **Policy Recommendations (Recomendaciones de políticas)** en la consola de gestión en la nube o **Visibility (visibilidad)** > **Security Rules (Reglas de seguridad)** en la consola de SaaS Security).
2. Seleccione y añada aplicaciones a la regla. Si la regla no se aplica a todos los usuarios, añada usuarios y grupos de usuarios. Asegúrese de entender las aplicaciones y los tipos de aplicaciones que desea bloquear antes de bloquearlas, y de comprender quién necesita utilizar determinadas aplicaciones con fines comerciales.

   Céntrese primero en los tipos de aplicaciones peligrosas, como las aplicaciones para compartir archivos, gestión de contenidos y, colaboración y productividad. Reduzca las cargas a sitios que comparten archivos para que solo los usuarios que necesitan cargar archivos con fines comerciales tengan acceso únicamente a las aplicaciones para compartir archivos utilizadas con fines comerciales.
3. Si tiene una licencia Enterprise DLP (práctica recomendada), añada un perfil DLP para inspeccionar el tráfico en busca de información confidencial y protegerlo frente el acceso no autorizado, incluidos perfiles predefinidos para aplicaciones DLP compatibles.
4. Verifique que la regla haga lo que usted desea que haga de la manera que usted desea hacerlo.
5. **Save (Guardar)** la regla predeterminada.
6. Debe **Enable (Habilitar)** la regla para enviarla a PAN-OS o Prisma Access. Debe habilitar reglas para que los administradores de PAN-OS o Prisma Access las importen.

   Comuníquese sobre las reglas habilitadas con el administrador responsable de verificar, evaluar e importar las recomendaciones de políticas de SaaS.

STEP 4 | (*Administrador de SaaS Security*) Configure las recomendaciones de políticas de SaaS definidas por el usuario. (Administradores de IoT Security ir al Paso 5).

Utilice los filtros en la vista Aplicaciones descubiertas para buscar aplicaciones y sus métricas de uso y para ayudarle a saber si debe bloquear o permitir una aplicación. Céntrese en las categorías de aplicaciones más peligrosas, como transferencia de archivos, gestión de contenidos y aplicaciones de colaboración y productividad. Las aplicaciones de alto **Risk (Riesgo)** que también tienen un alto

Usage (Uso) tienden a tener el mayor potencial de riesgo. Seleccione aplicaciones para ver quién usa la aplicación y cómo la usa.

Cuando configura recomendaciones de políticas y las envía, PAN-OS y Prisma Access crean automáticamente los perfiles, etiquetas y grupos de aplicaciones HIP adjuntos. Si tiene una licencia Enterprise DLP en los cortafuegos de destino, también se crea el perfil DLP (de lo contrario, el envío falla). El envío falla si el administrador de SaaS Security añade otros tipos de perfiles a una recomendación de regla y esos perfiles aún no existen en el cortafuegos. Si los objetos de perfil adjuntos existen en el cortafuegos, el envío se realiza correctamente. (El administrador de PAN-OS o Prisma Access puede añadir perfiles a las recomendaciones de reglas importadas. En Cloud Managed Prisma Access, solo puede añadir grupos de perfiles, no perfiles individuales).

Las licencias adecuadas para los perfiles deben estar en todos los cortafuegos que importen recomendaciones de políticas de SaaS.

*Los grupos de usuarios de CIE son coherentes en toda su organización. Si no utiliza CIE o si no puede sincronizar desde CIE, la configuración de **Users & Groups (Usuarios y grupos)** no está disponible en SaaS Security y no puede basar las recomendaciones de políticas de SaaS en los usuarios. La práctica recomendada es utilizar CIE y crear una política de aplicaciones basada en quién necesita acceder a las aplicaciones con fines comerciales.*

Para aplicar SaaS Security y Enterprise DLP, debe habilitar Web Security en la consola de gestión en la nube. (Esta es una función gratuita).

En la consola de gestión en la nube, el mismo administrador puede crear recomendaciones de políticas de SaaS e importarlas a Prisma Access.

Para configurar las recomendaciones de prácticas recomendadas para la política de SaaS:

1. Cree nuevas recomendaciones de políticas de SaaS Security:
   - Consola de SaaS Security: **Visibility (Visibilidad)** > **Security Rules (Reglas de seguridad)** > **Create New Rule (Crear nueva regla)**
   - Consola de gestión en la nube: **Discovered Apps (Aplicaciones descubiertas)** > **Policy Recommendations (Recomendaciones de políticas)** > **Add Policy (Añadir política)**
2. Siga las prácticas recomendadas para especificar el Name (Nombre) y la Description (Descripción) de la regla.
3. Añada aplicaciones a la regla.

   Utilice los filtros de categoría, riesgo y capacidades para encontrar aplicaciones SaaS. Añada aplicaciones a la regla directamente desde los resultados del filtro. Céntrese primero en las aplicaciones menos seguras y de mayor uso.
4. Seleccione la **User Activity (Actividad del usuario)** a detectar. Todas las aplicaciones seleccionadas para la regla deben admitir las actividades del usuario seleccionadas. Si una aplicación no admite una actividad, la interfaz devuelve un error.
5. Configure el resto de parámetros de la regla:

- **Users & Groups (Usuarios y grupos)**: debe utilizar y sincronizar desde CIE para especificar usuarios y grupos en la recomendación de política de SaaS.
- **Device Posture (Postura del dispositivo)**: especifique qué tipos de dispositivos pueden acceder a las aplicaciones de la regla. Cuando se importa una regla en PAN-OS o Prisma Access, la postura del dispositivo crea automáticamente un objeto de perfil de información de host (HIP) para dispositivos móviles.
- **Data Profile (Perfil de datos)**: debe tener una licencia Enterprise DLP en SaaS Security y en cortafuegos de destino específicos para utilizar esta función. Con una suscripción Enterprise DLP, puede crear reglas para un perfil DLP específico y bloquear aplicaciones solo si contienen datos que coincidan con el perfil.
- **Response (Respuesta)**:**Allow (Permitir)** o **Block (Bloquear)** el tráfico que coincida con la regla. La mayoría de las recomendaciones son reglas de bloqueo para evitar el aprovisionamiento excesivo de acceso.

6. Verifique que la regla haga lo que usted desea que haga de la manera que usted desea hacerlo.
7. Seleccione **Save (Guardar)** la regla.
8. Debe **Enable (Habilitar)** la regla para enviarla a PAN-OS o Prisma Access. Debe habilitar reglas para que los administradores de PAN-OS o Prisma Access las importen.

   Informe sobre las reglas habilitadas al administrador de PAN-OS o Prisma Access, quien es responsable de verificar, evaluar e importar las recomendaciones de políticas de SaaS.

   Crear recomendaciones de reglas de políticas de SaaS *proporciona más detalles sobre el flujo de trabajo.*

STEP 5 | (*Administrador de IoT Security*) Configure las recomendaciones de políticas de IoT (solo PAN-OS y Panorama Managed Prisma Access) en la aplicación IoT Security.

IoT Security genera automáticamente Recomendaciones de políticas de IoT basadas en el comportamiento de los dispositivos que pertenecen a un perfil de dispositivo cuando IoT Security alcanza una puntuación de confianza (el nivel de confianza que IoT Security tiene en su identificación de un dispositivo) del 90 % o más para el perfil. La puntuación de confianza aumenta con el tiempo a medida que IoT Security recopila más información sobre los dispositivos. Puede editar las reglas generadas automáticamente antes de enviarlas a Panorama, a los cortafuegos o a Prisma Access.

IoT Security no proporciona recomendaciones de políticas para dispositivos de TI como ordenadores PC, teléfonos inteligentes o tabletas, pero IoT Security sí los identifica.

Utilice las recomendaciones de políticas automáticas para crear conjuntos de reglas de políticas basadas en el comportamiento de los dispositivos IoT en el mismo perfil de dispositivo en varios inquilinos de

IoT Security. Un conjunto de reglas de políticas incluye las recomendaciones de reglas de políticas que usted selecciona para controlar los dispositivos en un perfil de dispositivo.

1. Cree nuevas recomendaciones de políticas de IoT Security de dos maneras:
   - Vaya a la página Perfiles, coloque el cursor sobre el nombre de un perfil y haga clic en **Create Policy Set (Crear conjunto de políticas)** en la ventana emergente.
   - **Profiles (Perfiles)** > **<profile-name>** > **Behaviors (Comportamientos)**, seleccione **Outbound Behaviors (Comportamientos de salida)**, seleccione **Create Policy (Crear política)**y luego haga clic en **Next (Siguiente)**.
2. **Select Policies (Seleccionar políticas)** muestra las recomendaciones de políticas generadas automáticamente para el perfil del dispositivo seleccionado, incluidas las aplicaciones que utilizan los dispositivos.
   1. Asegúrese de que las aplicaciones que ve en la lista sean apropiadas para los dispositivos. Por ejemplo, no debería ver la aplicación iTunes cuando está mirando impresoras o cámaras. Si ve aplicaciones inesperadas en la lista, es posible que el dispositivo esté comprometido.

      Conozca sus dispositivos y sus perfiles para poder elaborar recomendaciones adecuadas para controlarlos.
   2. Verifique las **Alerts Raised (Alertas generadas)**. Investigue las aplicaciones con una gran cantidad de alertas antes de añadirlas al conjunto de políticas, especialmente si las alertas son de gravedad alta o crítica.
   3. Seleccione las políticas que desea aplicar a los dispositivos. Estas políticas se incluyen en el conjunto de políticas para el perfil del dispositivo.

      Si no ve una aplicación que desee incluir en el conjunto de políticas, elija **Add Rule (Añadir regla)** para seleccionar manualmente una aplicación y un tipo de destino y **Create (Crear)** la regla.
   4. De forma predeterminada, la regla se aplica a todos [**Any (Cualquiera)**] los destinos detectados en el tráfico para el perfil del dispositivo. Si desea restringir los destinos de una aplicación, haga clic en **Destination (Destino)** > **Any (Cualquiera)**, desactive **Allow any destination (Permitir cualquier destino)** y desmarque los destinos que no desea permitir en la lista.
   5. Cuando tenga claro de que el conjunto de políticas contiene las reglas que desea, seleccione **Next (Siguiente)**.
3. En **Firewall Configuration (Configuración del cortafuegos)** > **Policy configurations (Configuraciones de políticas)**, modifique las recomendaciones generadas automáticamente según sea necesario. Las **Policy configurations (Configuraciones de políticas)** muestran las aplicaciones seleccionadas.
   - Siga las prácticas recomendadas para especificar el Name (Nombre) y la Description (Descripción) del conjunto de políticas. Asegúrese de que el nombre identifique lo que hace la regla y que la descripción indique el propósito de la regla.
   - Deje los **Services (Servicios)** como **application-default** (aplicación predeterminada) para evitar que las aplicaciones utilicen puertos no estándar, lo que es una indicación de comportamiento evasivo y potencialmente malicioso.

- Añada perfiles de seguridad y grupos de perfiles de seguridad, perfiles de reenvío de logs y otros objetos en Panorama o en cortafuegos, no en la aplicación IoT Security.

4. Revise el conjunto de políticas. Cuando esté seguro de que está configurado como lo desea, puede **Create (Crear)** el conjunto de políticas, que también lo guarda.
5. **Activate Policy Set (Activar el conjunto de políticas)** para que la recomendación de regla de política esté disponible para importar en Panorama y cortafuegos individuales.

   Informe sobre las reglas habilitadas al administrador de PAN-OS o Prisma Access, quien es responsable de verificar, evaluar e importar las recomendaciones de políticas de IoT.

Crear un conjunto de políticas de IoT *proporciona más detalles sobre el flujo de trabajo.*

STEP 6 | (Administradores de panorama y cortafuegos) (Administrador de Cloud Managed Prisma Access solo para SaaS Security) Evalúe, importe y, si es necesario, modifique las recomendaciones de reglas de políticas.

Debido a que la consola de gestión de la nube permite la gestión de todas las aplicaciones de la nube en un único lugar, el administrador de Cloud Managed Prisma Access puede ser el mismo administrador que creó las recomendaciones de la política de SaaS Security.

Antes de importar reglas:

- Cree Grupos de perfiles de seguridad en Panorama, cortafuegos y/o la consola de gestión en la nube que estén listos para que usted los aplique a las recomendaciones de políticas de SaaS Security e IoT Security importadas. Como mínimo, cree grupos de perfiles que alerten sobre la mayor parte del tráfico y bloqueen el tráfico malicioso conocido para mantener la disponibilidad. A medida que comprenda mejor las recomendaciones de políticas con el tiempo, siga las Prácticas recomendadas de perfiles de seguridad para que los grupos de perfiles sean lo más estrictos posible, sin poner en peligro la capacidad de acceder a puntos críticos. aplicaciones y dispositivos empresariales.

  Para los grupos de perfiles SaaS, conozca los tipos de aplicaciones y comprenda quiénes utilizan las aplicaciones para determinar qué perfiles usar y qué tan estrictos deben ser al principio.

  Para los grupos de perfiles de IoT, conozca sus dispositivos y sus perfiles para poder crear grupos de perfiles de seguridad adecuados para controlarlos. Comprenda lo que significa la aplicación en la regla para poder aplicar los perfiles de seguridad adecuados al grupo.

  Cuando cree grupos de perfiles de seguridad, consulte con el administrador de IoT Security y/o de SaaS Security para asegurarse de que los grupos de perfiles de seguridad tengan sentido para las recomendaciones de políticas de IoT y SaaS.
- En las implementaciones de IoT Security, habilite Device-ID en cada zona en la que desee controlar los dispositivos IoT. Device-ID es para los dispositivos IoT lo que User-ID es para los usuarios y App-ID para las aplicaciones: un identificador único. En zonas sin Device-ID habilitado, no puede aplicar la Política de seguridad en dispositivos IoT.
- La recomendación de políticas SaaS requiere App-ID Cloud Engine (ACE), que identifica decenas de miles de aplicaciones SaaS para que pueda crear una Política de seguridad para controlarlas. ACE

requiere el reenvío de logs a Cortex Data Lake. Siga las prácticas recomendadas de reenvío de logs cuando cree el perfil CDL.

Si utiliza App-ID de ACE en cualquier regla de la Política de seguridad, incluso si la regla se aplica solo a un usuario o grupo de usuarios, el cortafuegos aplica el App-ID de ACE a todos los usuarios. (Una vez que utiliza el App-ID de ACE en la política, el cortafuegos aplica el App-ID de la misma manera que aplica los App-ID proporcionados por contenido).

Para importar recomendaciones de políticas de SaaS e IoT:

1. Verifique periódicamente las reglas importadas. Actualice la página de recomendaciones de políticas de IoT o SaaS para asegurarse de que ve las recomendaciones de políticas más recientes:
   - Panorama: **Panorama** > **Policy Recommendation (Recomendación de políticas)** > **SaaS** o **Panorama** > **Policy Recommendation (Recomendación de políticas)** > **IoT**.
   - Cortafuegos: **Device (Dispositivo)** > **Policy Recommendation (Recomendación de políticas)** > **SaaS** o **Device (dispositivos)** > **Policy Recommendation (Recomendación de políticas)** > **IoT**.
   - Cloud Managed Prisma Access (solo recomendación de políticas de SaaS): Seleccione **Policy Recommendation (Recomendación de políticas)** > **Manage (Gestionar)** > **Web Security (Seguridad web)** > **Web Access Policy (Política de acceso web)**, y luego seleccione la pestaña **Policy Recommendations (Recomendaciones de políticas)** para ver las **New SaaS Rule Recommendations (Nuevas recomendaciones de reglas SaaS)**.
2. Seleccionar y evaluar nuevas reglas. Asegúrese de que todos los objetos, direcciones, etc. de la regla importada tengan sentido. Si no está seguro de algo en la recomendación, hable con el administrador

de IoT Security o de SaaS Security para asegurarse de que comprende el objetivo de la regla y sus componentes.

Para las recomendaciones de reglas de políticas de SaaS, asegúrese de que el acceso de los usuarios a las aplicaciones no sea demasiado amplio.

3. El proceso de importación de reglas le permite modificar la regla y colocarla en la base de reglas de la Política de seguridad. Seleccione una regla o reglas para importar y luego:

   - Cortafuegos Panorama y PAN-OS: **Import Policy Rule (Importar regla de políticas)**.

     Puede importar hasta diez reglas de políticas de IoT a la vez.

   - Cloud Managed Prisma Access (solo recomendación de políticas de SaaS): **Actions (Acciones)** > **Import (Importar)**.

     No finalice la importación de la regla hasta que complete los siguientes pasos para añadir perfiles de seguridad y reenvío de logs, evaluar la regla y seleccionar su orden en la base de reglas de políticas de seguridad.

   Cuando importa una regla, PAN-OS y Prisma Access crean automáticamente algunos de los objetos de la regla en la regla de política:

   - La importación de recomendaciones de políticas de IoT crea automáticamente el objeto Dispositivo, incluidas las asignaciones de dispositivo a IP, según el perfil del dispositivo IoT.

     Después de que Panorama importa el objeto del Dispositivo y lo envía a los cortafuegos gestionados, los cortafuegos despliegan la asignación de dispositivo a IP directamente desde la nube. Panorama no participa en la actualización de la asignación de dispositivo a IP.

   - La importación de recomendaciones de políticas de SaaS crea automáticamente los perfiles, etiquetas y grupos de aplicaciones HIP necesarios. Para los perfiles de Enterprise DLP, los dispositivos de destino deben tener una licencia Enterprise DLP. Cualquier otro perfil solo se puede importar si ya existe en el dispositivo de destino.

4. Añada un grupo de perfil de seguridad a cada regla.

   Usar grupos de perfiles en lugar de perfiles individuales es más rápido, más fácil y evita omitir accidentalmente un perfil de una regla. También le permite comenzar con un grupo de perfiles que

principalmente alerta y reemplazarlo fácilmente con un grupo de perfiles más estricto a medida que adquiere experiencia con aplicaciones SaaS y dispositivos IoT.

La aplicación de perfiles a aplicaciones SaaS y reglas de dispositivos IoT difiere:

- **Recomendaciones de reglas de política de SaaS Security**:
  - PAN-OS y Panorama Managed Prisma Access: aplique perfiles de prácticas recomendadas de Advanced Threat Prevention y Filtrado avanzado de URL al tráfico de aplicaciones SaaS.
  - Cloud Managed Prisma Access: puede aplicar grupos de perfiles de seguridad a recomendaciones de políticas, pero no perfiles de seguridad individuales. Añada perfiles de seguridad a un grupo de perfiles y aplique el grupo a una regla.

    Las recomendaciones de perfiles de seguridad de prácticas recomendadas para Cloud Managed Prisma Access difieren ligeramente de las recomendaciones para PAN-OS y Panorama Managed Prisma Access.
- **Recomendaciones de reglas de políticas de IoT Security**: para evitar comportamientos maliciosos, asegúrese de que los perfiles de seguridad sean apropiados para el dispositivo. Trabaje con el administrador de IoT Security para comprender el comportamiento y las alertas de los diferentes dispositivos que se muestran en los perfiles de dispositivo. Aplique perfiles a las recomendaciones de políticas de IoT basadas en comportamientos y alertas. Busque debilidades comunes en los dispositivos de IoT, como credenciales débiles del fabricante, conexiones a URL peligrosas, antivirus desactualizados, que permiten el acceso a dispositivos no autorizados, protocolos no seguros y sistemas operativos EOL, así como dispositivos que no están parcheados o que no pueden ser parcheados.
  - Aplique perfiles de protección de vulnerabilidades y perfiles antispyware (para evitar malware de comando y control) a todos los dispositivos.
  - Si un dispositivo tiene tráfico saliente a Internet, especialmente hacia destinos desconocidos, aplique el filtrado de URL avanzado, Advanced URL Filtering, y la prevención de amenazas avanzada, Advanced Threat Prevention. Si el dispositivo puede enviar archivos, añada perfiles de Advanced WildFire y bloqueo de archivos.

- Si el dispositivo tiene puertos de servidor y acepta conexiones entrantes, aplique Protección DoS además de los perfiles de bloqueo de archivos, Advanced WildFire y Advanced Threat Prevention.

5. Añada un perfil de reenvío de logs a cada regla.

   - Para obtener recomendaciones de políticas de IoT, añada el perfil de reenvío de logs predefinido **perfil predeterminado de IoT Security: habilitado por EAL**, que proporciona todos los tipos de logs que requiere la IoT Security, incluidos los logs de aplicaciones mejorados.
   - La recomendación de la política SaaS requiere que ACE identifique las aplicaciones SaaS. ACE requiere el reenvío de logs a CDL, por lo que las reglas de políticas de seguridad basadas en aplicaciones SaaS también requieren el reenvío de logs a CDL.

   

   *Después de importar reglas, puede aplicar perfiles de reenvío de logs a varias reglas a la vez utilizando el**Log Forwarding for Security Services (Reenvío de logs para servicios de seguridad)** en Policy Optimizer para identificar las reglas de políticas de seguridad que no tienen un perfil de reenvío de logs adjunto [seleccione **None (Ninguno)** en el filtro].*

6. En Panorama y Cloud Managed Prisma Access, seleccione si la regla es una regla previa o posterior. (No se aplica a cortafuegos independientes).

   El orden de prioridad para las reglas que evalúan es reglas previas, luego reglas específicas de la implementación y luego reglas posteriores. Las reglas previas y posteriores de Cloud Managed Prisma Access residen en la carpeta de configuración compartida. Las reglas previas y posteriores de Panorama residen en **Policies (Políticas)** > **Security (Seguridad)**. En Panorama, puede especificar grupos de dispositivos para la regla.

7. Seleccione la regla que desea que vaya anterior a la regla importada en la base de reglas de la Política de seguridad. Siga las prácticas recomendadas de la base de reglas.

   

   *No elija **No Rule Selection (Sin selección de regla)**, que coloca la regla en la parte superior de la base de reglas de la Política de seguridad. La parte superior de la base de reglas suele ser el lugar equivocado para una nueva regla. Por ejemplo, una nueva regla de permiso no estará sujeta a reglas críticas que bloqueen el tráfico malicioso conocido. Una nueva regla de bloqueo puede bloquear el acceso de usuarios legítimos si no se coloca después de una regla de permiso para los usuarios legítimos de la aplicación. Ordene cada regla adecuadamente en la base de reglas.*

8. Verifique la regla y, si está satisfecho con ella, impórtela.

   - **Cloud Managed Prisma Access**:**Import (Importar)**.
   - **Panorama y cortafuegos independientes**:**OK (Aceptar)**.

     Después de importar las reglas, los administradores de Panorama deben enviar las reglas a los cortafuegos gestionados, y los administradores de cortafuegos deben importarlas antes de que se activen en el cortafuegos. Actualice **Device (Dispositivo)** > **Policy Recommendation**

(Recomendación de política) > **IoT** o **Device (Dispositivo)** > **Policy Recommendation (Recomendación de política)** > **SaaS** para ver las recomendaciones más recientes.

Es posible que los administradores del cortafuegos necesiten modificar las reglas después de importarlas. Los administradores de cortafuegos deben consultar con los administradores de Panorama, SaaS Security o IoT Security si no están seguros del propósito de la regla.

Consulte la base de reglas de la Política de seguridad para asegurarse de que la regla esté en el orden correcto.

9. (Solo IoT Security) Después de importar la regla, vea el **Device Object (Objeto del dispositivo)** para verificar los filtros de atributos del dispositivo.

   Utilice los atributos del dispositivo IoT en la Política de seguridad para identificar mejor los dispositivos. Al importar una regla de política de IoT, se importan automáticamente los atributos asociados con el dispositivo y se crea su Device-ID. Device-ID es para los dispositivos IoT lo que User-ID es para las personas. Aunque hay seis atributos de dispositivo, los cortafuegos suelen recibir solo un atributo de un dispositivo. Si el objeto de dispositivo [**Objects (Objetos)** > **Devices (Dispositivos)**] especifica atributos que el dispositivo no envía al cortafuegos, entonces el tráfico no coincide con el dispositivo y la regla no controla el dispositivo, por lo tanto, solo especifique los atributos que los dispositivos envían al cortafuegos. .

   *Haga clic en el **Device-ID** en la regla para que aparezca su Objeto de dispositivo asociado.*

   Ejecute el comando de la CLI **`show iot ip-device-mapping-mp all`** o **`show iot ip-device-mapping-mp ip <IP-address>`** para validar que el cortafuegos reciba los atributos importados con la regla. Si el cortafuegos no recibe un atributo configurado en el objeto de dispositivo, elimine el atributo del objeto de dispositivo.

Para conocer los procedimientos de configuración detallados, consulte la Guía del administrador correspondiente:

- **IoT Security**:
  - Procedimiento de importación
  - Importar un conjunto de políticas a Panorama
  - Configuración de Device-ID
- **SaaS Security**:
  - PAN-OS y Panorama Managed Prisma Access: importe recomendaciones de políticas de SaaS (para cortafuegos independientes; en Panorama, también puede especificar si la regla importada es una regla anterior o posterior, y enviar la regla a los cortafuegos después de importarla en Panorama).
  - Cloud Managed Prisma Access: vea recomendaciones de políticas de SaaSe importe nuevas recomendaciones de políticas de SaaS.

STEP 7 | (Todos los administradores) Actualice y elimine las recomendaciones de políticas según sea necesario para mantener actualizada la base de reglas de políticas de seguridad.

La importación de recomendaciones de políticas es un proceso continuo. Los administradores recomiendan nuevas reglas, modifican reglas y eliminan reglas antiguas. El número de dispositivos de IoT crece y las posturas de los dispositivos cambian a lo largo del tiempo. El número de aplicaciones

SaaS aumenta y las aplicaciones que su empresa etiqueta como autorizadas, toleradas y no autorizadas cambian con el tiempo. Cree listas de verificación de elementos diarios, semanales y mensuales para supervisar y mantener la visibilidad de los dispositivos IoT y las aplicaciones SaaS.

Procedimientos para importar recomendaciones de políticas actualizadas:

- IoT Security: Modificar y actualizar las recomendaciones de reglas de políticas de IoT incluye los pasos de IoT Security y PAN-OS.
- SaaS Security:
  - SaaS Security Inline: modificar las recomendaciones de reglas de políticas de SaaS activas muestra cómo modificar una regla existente en SaaS Security.
  - Cloud Managed Prisma Access: actualice las recomendaciones de reglas de políticas de SaaS importadas en Cloud Managed Prisma Access.

    Si el mismo administrador es el administrador de recomendaciones de políticas de SaaS y el de Prisma Access, puede habilitar las actualizaciones automáticas para aplicar automáticamente los cambios en las recomendaciones de reglas.
  - Panorama Managed Prisma Access y PAN-OS: Importar recomendación de política para SaaS actualizada muestra cómo buscar e importar recomendaciones de políticas de SaaS Security actualizadas.

Procedimientos para retirar recomendaciones de políticas eliminadas:

- IoT: Eliminar y quitar las recomendaciones de reglas de políticas incluye los pasos de IoT Security y PAN-OS.
- SaaS Security:
  - SaaS Security Inline:Eliminar recomendaciones de reglas de políticas de SaaS muestra cómo eliminar una regla existente en SaaS Security.
  - Cloud Managed Prisma Access: retire recomendaciones de reglas de políticas SaaS eliminadas en Cloud Managed Prisma Access.
  - Panorama Managed Prisma Access y PAN-OS: Retirar la recomendación de política SaaS eliminada.

Prácticas recomendadas para mantener la política de seguridad

Después de planificar e implementar las prácticas recomendadas de políticas de seguridad, mantenga su implementación de las prácticas recomendadas a medida que cambien la red y sus aplicaciones, los usuarios, los dispositivos y la infraestructura.

STEP 1 | Mantenga actualizadas todas las suscripciones de seguridad para evitar lagunas en la cobertura.

STEP 2 | Manténgase al día con las actualizaciones de contenido de Aplicaciones y Amenazas y siga las prácticas recomendadas para actualizaciones de contenido de Aplicaciones y Amenazas.

STEP 3 | Revise las notas de la versión para conocer las últimas características, cambios en el comportamiento predeterminado, problemas, etc.

STEP 4 | Cree listas de verificación de mantenimiento diarias, semanales, mensuales (y cualquier otro período que necesite).

El mantenimiento de la implementación de políticas de seguridad es una tarea recursiva porque se añaden y eliminan continuamente nuevas aplicaciones, usuarios y dispositivos de IoT a su entorno, a medida que las cosas cambian con el tiempo. Por ejemplo, las listas de verificación pueden incluir:

- Evaluar actualizaciones de contenido de aplicaciones y amenazas
- Usar Policy Optimizer para gestionar aplicaciones.
- Revisar las recomendaciones y actualizaciones de políticas de IoT y SaaS. La postura de los dispositivos IoT puede cambiar con el tiempo y las aplicaciones SaaS utilizadas pueden cambiar con el tiempo o necesitar un tratamiento diferente y requerir actualizaciones. Mantenga actualizadas las etiquetas de autorizadas/toleradas/no autorizadas para las aplicaciones.
- Establecer horarios para ejecutar herramientas de análisis de la estrategia de seguridad.
- Revisar los cambios de comportamiento y los problemas documentados en las notas de la versión.
- Revisar las reglas de la Política de seguridad para ver si puede ajustarlas o si ya no son necesarias.

STEP 5 | Mantener App-ID en la Política de seguridad:

- Revise los App-ID nuevos y modificados y ajuste las reglas según sea necesario.
- A medida que añada nuevas aplicaciones a su red, inclúyalas en reglas de políticas específicas y detalladas. Utilice etiquetas y filtros de aplicaciones para automatizar la adición de aplicaciones autorizadas, incluidas las nuevas aplicaciones de App-ID Cloud Engine, a las reglas.
- Cuando su empresa deje de usar una aplicación, elimínela de las reglas de permiso para evitar el uso no autorizado.
- Revise periódicamente las aplicaciones sus reglas de Política de seguridad permiten.

STEP 6 | Mantener User-ID en la Política de seguridad:

- A medida que añada nuevos usuarios a su red, añádalos a los grupos de usuarios apropiados para controlar su acceso e incluirlos en la política, o agréguelos directamente a las reglas si no pertenecen a ningún grupo.
- A medida que los usuarios abandonan la empresa o cuando finalizan sus contratos, elimínelos de los grupos de usuarios para impedir el acceso. Elimine individuos de las reglas si no fueron añadidos como parte de un grupo.
- Continúe utilizando las prácticas recomendadas para la asignación de grupos de usuarios y las prácticas recomendadas para grupos de usuarios dinámicos (DUG) a medida que añade y elimina usuarios de grupos y reglas de política.

STEP 7 | Mantenga y actualice los perfiles de seguridad y los grupos de perfiles a medida que su red y objetivos evolucionan. Cuando añada nuevas reglas de permiso, asegúrese de que tengan los perfiles de seguridad adecuados adjuntos.

STEP 8 | Actualice el reenvío de logs, Log Forwarding, según sea necesario para nuevas reglas y aplicaciones:

- Aplique un perfil de reenvío de logs apropiado a cada nueva regla de la Política de seguridad o utilice un perfil de reenvío de logs predeterminado para aplicar automáticamente un perfil de reenvío de logs a nuevas reglas. Si utiliza un perfil predeterminado, compruebe la regla para asegurarse de que el perfil predeterminado es adecuado y, si no lo es, sustitúyalo por un perfil adecuado.
- Revise periódicamente lo que está registrando y lo que no, y cómo lo está haciendo. Asegúrese de registrar los logs de tráfico que desea registrar y de registrar toda la información que desea registrar para las operaciones del Centro de operaciones de seguridad (SOC).
- Actualice los perfiles de reenvío de logs a medida que los administradores se unen y abandonan la empresa.
- A medida que lleguen nuevas aplicaciones a su red, actualice el reenvío de logs, Log Forwarding, para incluirlas.

STEP 9 | Utilice herramientas de análisis de la estrategia de seguridad para comprobar la implementación de sus prácticas recomendadas:

- En PAN-OS y Prisma Access, utilice Strata Cloud Manager para comprobar la Política de seguridad a medida que la crea.
- Ejecute periódicamente la Evaluación de prácticas recomendadas (BPA) a petición de Strata Cloud Manager para medir el progreso hacia la implementación de las prácticas recomendadas.
- Ejecute el análisis Security Lifecyle review (SLR) trimestralmente para obtener una mejor visual de su red.

STEP 10 | Utilice herramientas de cortafuegos para comprobar la actividad y ajustar la Política de seguridad según sea necesario.

- Utilice la información de los logs en PAN-OS (también se aplica a Panorama Managed Prisma Access) y Cloud Managed Prisma Access para investigar y supervisar el tráfico.
- Utilice el Centro de control de aplicaciones para ver resúmenes gráficos de aplicaciones, usuarios, amenazas, URL y contenido que atraviesa su red.
- Utilice los informes de App Scope para ayudar a comprender los cambios en el uso de la aplicación y la actividad del usuario, el uso del ancho de banda y las amenazas de red.
- Cree Informes personalizados para ver los datos exactos que desea investigar.

STEP 11 | Compruebe Policy Optimizer regularmente para examinar la base de reglas y encontrar y corregir reglas no utilizadas, reglas sobreaprovisionadas y reglas con aplicaciones no utilizadas. Añada la comprobación de Policy Optimizer a su mantenimiento programado periódicamente.

STEP 12 | Utilice las herramientas y servicios de SecOps para supervisar toda su estrategia de seguridad de forma proactiva, ayudar a prevenir amenazas e investigar problemas:

- Cortex XSIAM combina análisis SOC para una supervisión proactiva con capacidades SIEM.
- Cortex XSOAR proporciona una completa orquestación de seguridad, automatización y respuesta; incluidos los manuales de respuesta, para la gestión integral de la inteligencia de amenazas y la colaboración en tiempo real.
- Cortex XDR proporciona una plataforma de detección y respuesta extendida que supervisa y gestiona eventos y datos en la nube, la red y los endpoints.
- Servicios SOC tales como la evaluación de la estrategia de prevención de SecOps, optimización y talleres de aprendizaje.

STEP 13 | Los siguientes recursos proporcionan más información sobre las plataformas, características y soporte de Palo Alto Networks:

- El Portal de documentación de prácticas recomendadas de seguridad contiene libros independientes como Prácticas recomendadas de IoT Security, Prácticas recomendadas de acceso administrativo y Prácticas recomendadas de descifrado, y enlaces a temas de prácticas recomendadas en varias guías del administrador.

- Guías del administrador:
  - Guía del administrador de PAN-OS
  - Guía del administrador de Prisma Access (Panorama Managed y Cloud Managed Prisma Access)
  - Guía del administrador de SaaS Security
  - Guía del administrador de IoT Security
- Portales de documentación:
  - Portal de documentación de Cloud Delivered Security Services (CDSS)
  - Portal de documentación de Cloud Identity Engine (CIE)
  - Portal de documentación GlobalProtect
  - Portal de atención al cliente de Palo Alto Networks
- Supervise su implementación de IoT Security utilizando las prácticas recomendadas
- Estructura de la solución IoT Security (resumen de cómo funciona la solución IoT Security)
- SaaS Security en Prisma Access (gestionado por Panorama y en la nube)
- Resolución de problemas en SaaS Security Inline