paloalto
TECHDOCS

Introducción a Strata Cloud Manager

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Last Revised

February 6, 2025

Table of Contents

Introducción a Strata Cloud Manager

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW, incluidos los financiados por Créditos de NGFW de software • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Strata Cloud Manager de Palo Alto Networks le permite una gestión y operaciones unificadas impulsadas por IA para toda la implementación de seguridad de red. Con Strata Cloud Manager puede gestionar fácilmente toda su infraestructura de seguridad de red de Palo Alto Networks, sus NGFW y su entorno SASE, desde una única interfaz de usuario optimizada. Obtenga una visibilidad completa de los usuarios, las sucursales, las aplicaciones y las amenazas en todos los puntos de aplicación de la seguridad de la red; esto le brinda información práctica, mejor seguridad y fácil solución y resolución de problemas.

❑ **Predecir y prevenir las interrupciones de red**

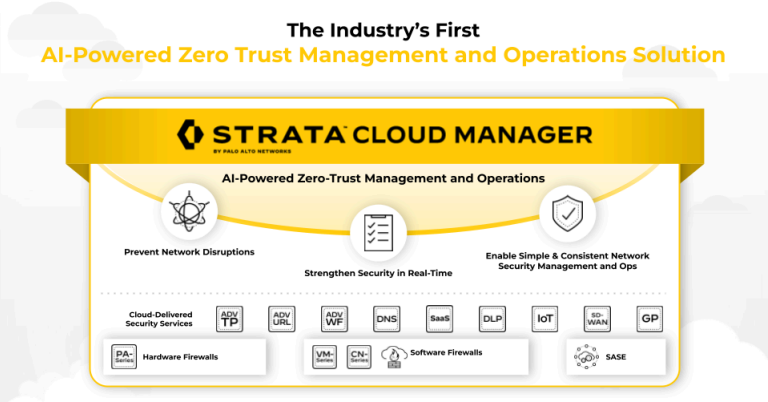
Strata Cloud Manager predice y previene las interrupciones de la red y remedia rápidamente los problemas, para que usted y sus usuarios puedan continuar con su negocio diario y mantenerse productivos.

❑ **Fortalecer la seguridad con las prácticas recomendadas en tiempo real**

Strata Cloud Manager identifica capacidades de seguridad vitales e infrautilizadas, y le guía para que las habilite basándose en las prácticas recomendadas que se ajusten a sus necesidades. Fortalezca su postura de seguridad con las prácticas recomendadas incorporadas y funciones de remediación en línea impulsadas por AIOps.

❑ **Gestión y operaciones de seguridad de red sencillas y coherentes**

Strata Cloud Manager consolida sus herramientas de seguridad para mejorar la operación y los conocimientos, de modo que pueda adoptar una experiencia de gestión simple y coherente para toda su pila de seguridad de red.



Cómo Strata Cloud Manager refuerza la seguridad

Maximice el uso de capacidades de seguridad

- Vea las características de seguridad que está utilizando e identifique las lagunas en la adopción de las características de seguridad que podría aprovechar. → Adopción de características
- Consulte las tasas de adopción de sus suscripciones a servicios de seguridad. → Adopción CDSS
- Vea cómo sus características de seguridad se adhieren a las prácticas recomendadas o dónde puede realizar mejoras para fortalecer su postura de seguridad. → Prácticas recomendadas incorporadas

Fortalecer y optimizar la configuración existente

Limpie y optimice fácilmente su política de seguridad en función de los datos de uso y las recomendaciones generadas automáticamente.

- Limpie los objetos a los que no se hace referencia en la política y las reglas sin que se produzca ningún acierto de tráfico; estos objetos y reglas pueden obstruir el rendimiento y complicar la gestión de políticas. → Limpieza de configuración
- Las reglas que son demasiado generales introducen lagunas de seguridad porque permiten aplicaciones que no están en uso en su red. El optimizador de políticas le permite convertir estas reglas excesivamente permisivas en reglas más específicas y enfocadas que solo permiten a las aplicaciones que está utilizando. → Optimizador de políticas

Guía en tiempo real para una configuración segura

- Los rieles de protección de prácticas recomendadas le brindan validación en vivo de que las reglas de su política de seguridad cumplen con las prácticas recomendadas. → Comprobaciones en vivo y en línea de la configuración de prácticas recomendadas

Cómo Strata Cloud Manager predice y previene las interrupciones de la red

Observabilidad integral

- Sepa cómo su red se mantiene segura gracias a la infraestructura de seguridad. → Centro de control
- Conozca el estado y el rendimiento de los usuarios, sitios de sucursales, aplicaciones, e infraestructura de TI, desde

  un único panel. → Panel de estado de SASE
- Conozca el estado y el rendimiento de los dispositivos desde un único panel. → Panel de estado de dispositivo

Previsión de estado y corrección de alteraciones

Los pronósticos automáticos previenen posibles interrupciones; cuando se detectan problemas, los conocimientos prácticos aceleran las resoluciones.

- Predicción asistida por máquina de interrupciones inminentes, con recomendaciones para su remediación. → Forecasting y detección de anomalías
- Reduzca el tiempo hasta la resolución con el análisis de causas probables. → Ver causas probables

Planificación de la evolución de las necesidades de seguridad

- Mejore la estabilidad identificando de forma proactiva la capacidad potencial. → Analizador de capacidad

Cómo funciona Strata Cloud Manager en todas partes de forma coherente

Configuración coherente

Aplicar políticas coherentes en todos los puntos de aplicación con procesos simplificados y eliminar la necesidad de realizar cambios individuales para los despliegues de NGFW y SASE.

- Configure e incorpore NGFW y Prisma Access para usuarios móviles y redes remotas, y planifique actualizaciones de software para NGFW. → Flujos de trabajo en Strata Cloud Manager
- Configure una política de seguridad que se comparta entre sus NGFW y Prisma Access. → Gestión compartida para NGFW y Prisma Access

Organización flexible de la configuración

Simplifique la gestión de la configuración a escala con flujos de trabajo de gestión de carpetas y dispositivos sencillos.

- Aplique los ajustes de configuración y aplique la política globalmente en todo su entorno, o los ajustes y la política de destino a ciertas partes de su organización. → Ámbito de configuración
- Agrupe lógicamente sus cortafuegos o tipos de implementación (usuarios móviles de Prime Access, redes remotas o conexiones de servicio) para una gestión de configuración simplificada. → Configuraciones de grupos
- Gestión de carpetas que puede enviar rápidamente a sus cortafuegos o implementaciones. → Fragmentos
- Tiene la flexibilidad de acomodar valores de configuración únicos que son específicos de dispositivos o implementaciones . → Variables

Logre visibilidad unificada de las amenazas

- Obtenga una visibilidad completa del tráfico de su red, suscripciones, usuarios, aplicaciones, redes, amenazas y mucho más. → Supervisión
- Obtenga una vista interactiva de las aplicaciones, los dispositivos ION, las amenazas, los usuarios y las suscripciones de seguridad en el trabajo en su red. Los paneles proporcionan visibilidad del estado, la postura de seguridad y la actividad que se produce en su implementación; lo que le ayuda a prevenir o abordar las deficiencias de rendimiento y seguridad en su red. → Paneles
- Obtenga informes sobre los patrones de tráfico de red, la utilización del ancho de banda, los datos de suscripción de seguridad y más. Los informes proporcionan información práctica sobre su red que puede utilizar para planificar y supervisar. → Informes

Productos que Strata Cloud Manager admite

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW, incluidos los financiados por Créditos de NGFW de software • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Prisma SD-WAN ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Strata Cloud Manager proporciona gestión y operaciones unificadas impulsadas por IA para sus dispositivos NGFW y red SASE, y las características de Strata Cloud Manager disponibles para usted dependen de sus licencias. Aquí están las licencias que permiten a Strata Cloud Manager gestionar dispositivos NGFW y SASE, y desbloquear las características de seguridad de la red de Strata Cloud Manager. → A continuación le indicamos cómo validar sus licencias

Table 1:

Strata Cloud Manager Essentials	Strata Cloud Manager Essentials ofrece funciones de gestión y seguridad, y estas funciones están disponibles para usted de forma gratuita con: • Cortafuegos de nueva generación (NGFW) • Prisma Access Strata Logging Service está disponible como complemento opcional para Strata Cloud Manager Essentials. *Strata Cloud Manager Essentials y Strata Cloud Manager Pro están disponibles para activar en cuentas del portal de atención al cliente (CSP) que no tienen: Servicio de registro de logs de Strata con almacenamiento dimensionado, AIOps para NGFW Free o Premium, o Prisma Access.*
Strata Cloud Manager Pro	Strata Cloud Manager Pro es la versión de pago que incluye todas las características de Strata Cloud Manager Essentials,

	además de funciones avanzadas para mejorar el estado operativo, prevenir interrupciones de la red, fortalecer la postura de seguridad en tiempo real y la gestión autónoma de la experiencia digital (ADEM) para supervisar el rendimiento de la experiencia del usuario. Strata Cloud Manager Pro incluye Strata Logging Service con un año de retención de logs y almacenamiento ilimitado, lo que permite el registro de logs centralizado y la recuperación de datos sin problemas en toda la implementación. Puede comprar Strata Cloud Manager Pro para los siguientes productos: • Cortafuegos de nueva generación (NGFW) • VM-Series financiada por créditos de NGFW de Software • Prisma Access
AIOps para NGFW Premium	Para los NGFW con licencia AIOps para NGFW Premium, Strata Cloud Manager le ofrece una visión general del estado y la seguridad de sus NGFW, y puede hacer cumplir controles proactivos para cerrar las brechas de seguridad. • **NGFW (Managed by PAN-OS or Panorama)** → Para los NGFW gestionados por PAN-OS y Panorama con una licencia AIOps para NGFW Premium, utilice Strata Cloud Manager para supervisar su estado de implementación y su postura de seguridad. • **NGFW (Managed by Strata Cloud Manager)** → Con una licencia AIOps para NGFW, también puede usar Strata Cloud Manager para la **gestión en nube para dispositivos NGFW**. • *Póngase en contacto con su equipo de cuentas para habilitar la Gestión en la nube para NGFW utilizando Strata Cloud Manager.* • *Strata Cloud Manager proporciona gestión y operaciones unificadas solo para NGFW utilizando la licencia AIOps para NGFW Premium. Continúe usando la aplicación AIOps para NGFW Free para dispositivos NGFW incorporados a AIOps para NGFW Free.*
Créditos NGFW de software	Para la VM-Series financiada con créditos de NGFW de software, Strata Cloud Manager admite características de AIOps para NGFW Premium, incluida la gestión en la nube para cortafuegos NGFW.

Prisma Access	Hay dos formas de gestionar Prisma Access: puede usar Strata Cloud Manager o Panorama. Strata Cloud Manager proporciona características de visibilidad de Prisma Access, y estás son compatibles independientemente de la interfaz de gestión que esté usando. Esto significa que si está utilizando Panorama para gestionar Prisma Access, todavía puede utilizar Strata Cloud Manager para la supervisión integral del entorno de Prisma Access. **Prisma Access (Managed by Strata Cloud Manager)** Utilice Strata Cloud Manager para la incorporación completa, la gestión y la supervisión de su entorno de Prisma Access. Esto incluye el uso de Strata Cloud Manager para gestionar y supervisar los servicios de seguridad en la nube que se incluyen con Prisma Access. Strata Cloud Manager le brinda una supervisión, alerta y visibilidad completas de su entorno de Prisma Access: • Autonomous DEM basado en IA • Supervisar Prisma Access en Strata Cloud Manager • Paneles de Strata Cloud Manager • Supervisión de Strata Cloud Manager • Informes de Strata Cloud Manager **Prisma Access (Managed by Panorama)** Si está utilizando Panorama para gestionar Prisma Access, debe continuar usando Panorama para gestionar su entorno. Sin embargo, puede utilizar Strata Cloud Manager para la supervisión, alerta y visibilidad completas de su entorno de Prisma Access: • Autonomous DEM basado en IA • Supervisar Prisma Access en Strata Cloud Manager • Paneles de Strata Cloud Manager • Supervisión de Strata Cloud Manager • Informes de Strata Cloud Manager
ADEM basado en IA	ADEM basado en IA es una licencia adicional de Prisma Access que automatiza operaciones de TI complejas, para aumentar la productividad y reducir el tiempo hasta la resolución de problemas. Strata Cloud Manager es compatible con ADEM basada en IA para todos los usuarios de Prisma Access (tanto Prisma Access gestionado por Panorama como Prisma Access Cloud Management).

	Si utiliza Panorama para gestionar Prisma Access, debe seguir utilizando Panorama para gestionar su entorno y puede utilizar Strata Cloud Manager para la supervisión ADEM.
Prisma SD-WAN	Utilice Strata Cloud Manager para Prisma SD-WAN. Prisma SD-WAN es un servicio en la nube que implementa SD-WAN autónoma y definida por aplicaciones para ayudarle a proteger y conectar sus sucursales, centros de datos y grandes campus sin aumentar el coste y la complejidad. AppFabric conecta sus sitios de forma segura con el conocimiento de la aplicación y le da la libertad de usar cualquier WAN, cualquier nube para una solución sucursal fina (seguridad desde la nube).
Servicios de seguridad en la nube • **Advanced Threat Prevention** • **Filtrado de URL avanzado** • **Advanced WildFire** • **DNS Security** • **DLP empresarial** • **IoT Security (Seguridad de IoT)** • **SaaS Security:**	Si tiene una licencia de Prisma Access o AIOps para NGFW Premium, puede usar Strata Cloud Manager para gestionar y supervisar sus suscripciones de seguridad. Strata Cloud Manager ofrece las protecciones que sus suscripciones de seguridad brindan de manera coherente en todo el tráfico de su empresa. Las características de Strata Cloud Manager disponibles para suscripciones de seguridad dependen de su licencia y pueden incluir: • Paneles e informes de Strata Cloud Manager para suscripciones de seguridad • Gestión unificada de Strata Cloud Manager para suscripciones de seguridad. Si utiliza Strata Cloud Manager para hacer cumplir una políticas de seguridad compartida en todas los NGFW o Prisma Access, puede utilizar una configuración única y centralizada para sus suscripciones de seguridad.

Primer vistazo a Strata Cloud Manager

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW, incluidos los financiados por Créditos de NGFW de software • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Prisma SD-WAN ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Este es un primer vistazo a Strata Cloud Manager. La interfaz de usuario de Strata Cloud Manager proporciona una visión completa de su red y le proporciona un flujo de trabajo unificado para gestionar NGFW y SASE. Muévase a través de la nueva navegación simplificada y coherente para interactuar con todos los datos de su red, obtener información útil que se muestre automáticamente y gestionar y supervisar colectivamente Prisma Access, sus NGFW y sus servicios de seguridad entregados en la nube.

Explore cada menú en la barra de navegación izquierda: estas rutas son ahora estándar en todos los productos de Palo Alto Networks o suscripciones que utilice con Strata Cloud Manager. Esto facilita:

- adoptar nuevas características y suscripciones
- incorporar nuevos usuarios, dispositivos, sitios o ubicaciones

ya que se insertarán directamente en su configuración de gestión existente.

Importante

Las características disponibles para usted en Strata Cloud Manager dependen de sus suscripciones. Puede revisar los documentos de Strata Cloud Manager para ver los requisitos de licencia para las funciones de Strata Cloud Manager.

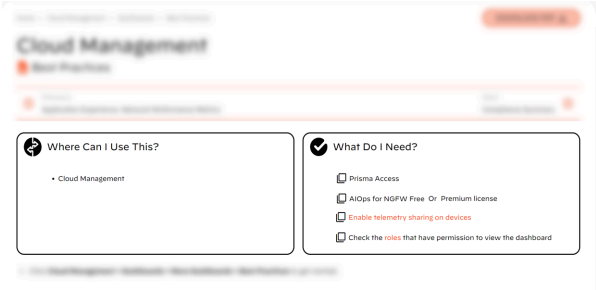
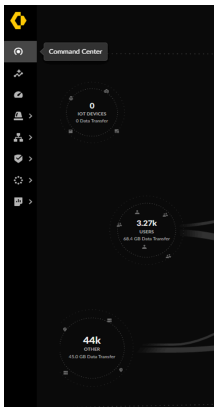
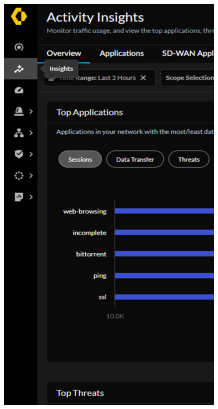
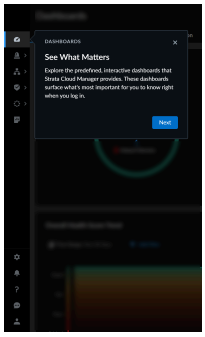
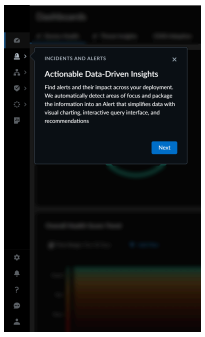
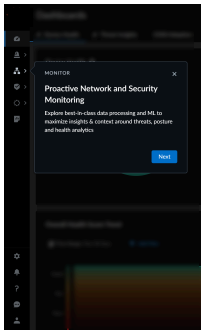
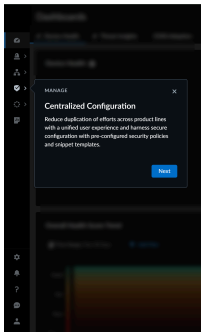
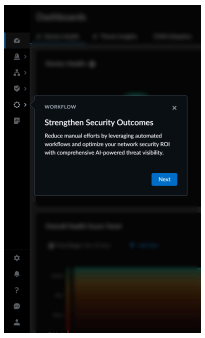
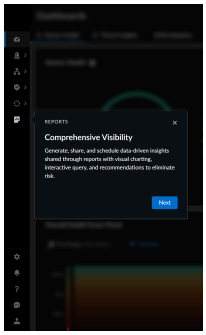
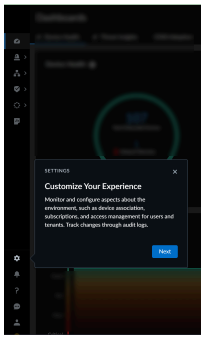


Table 2:

Centro de control:	**Su primera parada para evaluar el estado, seguridad y eficiencia de su red** El Centro de control es una visión general visualizada de su infraestructura de red y seguridad. Le proporciona cuatro vistas diferentes, cada una con sus propios datos rastreados, métricas y conocimientos prácticos para examinar e interactuar. • Centro de comando: Strata Cloud Manager	
Activity Insights	**Datos de red unificados, todo en un único lugar** Activity Insights le ofrece una visión en profundidad de las actividades de su red en implementaciones de Prisma Access y NGFW. Activity Insights unifica los datos de red, como el tráfico de red, el uso de aplicaciones, las amenazas y las actividades de los usuarios en un solo lugar. • Insights: Activity Insights	

Paneles	**Vea lo que importa, de inmediato** Los paneles de control resaltan lo que es más importante que sepa, justo cuando inicia sesión. Cada panel de control está diseñado para resaltar las áreas en las que puede tomar medidas para mejorar su postura de seguridad o el estado de la red. Explore todos los paneles interactivos predefinidos que se proporcionan y podrá fijar sus favoritos. • Paneles: Strata Cloud Manager	
Incidentes y alertas	**Información (Insights) procesable basada en datos** Strata Cloud Manager proporciona un marco unificado de incidentes y alertas. En un único lugar, vea, investigue y aborde las alertas e incidentes en su red, y salte a sus logs para examinar la actividad asociada. • Incidentes y alertas: Strata Cloud Manager	
Monitor (Supervisar)	**Supervisión proactiva de redes y seguridad** Supervise la salud y la seguridad de todo en su red, y use la búsqueda IoC para investigar el historial de un artefacto en su red y revisar los resultados del análisis global. Dependiendo de las suscripciones y los productos que utilice, puede supervisar: • Dispositivos NGFW • Prisma Access • Aplicaciones • Usuarios • Sucursales • Centros de datos • Servicios de red (como GlobalProtect y DNS)	

	• Sus suscripciones de Palo Alto Networks • Sus ubicaciones de Prisma Access • Prisma SD-WAN • Activos	
Gestionar	**Configuración centralizada** Gestione una política compartida en todos sus productos de seguridad de red y suscripciones; en el primer día, puede comenzar con una configuración segura basada en políticas y configuraciones de prácticas recomendadas predefinidas y comprobaciones de prácticas recomendadas en línea. • Gestionar: NGFW y Prisma Access • Gestionar: Recomendación de política de IoT: • Gestionar: DLP empresarial • Gestionar: SaaS Security:	
Flujos de trabajo	**Fortalecer los resultados de seguridad** Cuando navegue por primera vez a sus flujos de trabajo, el panel **Descubrimiento** mostrará las acciones críticas y recomendadas que puede realizar para mejorar la postura de seguridad u optimizar la gestión de la configuración, tan pronto como estén disponibles para usted. Continúe aquí para configurar e incorporar usuarios móviles y redes remotas de NGFW y Prisma Access, y planificar actualizaciones de software para NGFW. • Configurar Prisma Access • Configurar dispositivos NGFW • Planificador de actualización de software (AIOps para NGFW)	

Informes	**Visibilidad integral** Genere, comparta y programe información basada en datos compartida a través de informes con gráficos visuales, consultas interactivas y recomendaciones para eliminar el riesgo. • Informes: Strata Cloud Manager	
Configuración	**Configuración de incorporación y activación** Estas son las configuraciones a las que volverá cuando añada nuevos usuarios, licencias o administradores, o incluso cuando empiece a usar Strata Cloud Manager: • Suscripciones • Inquilinos • Asociaciones de dispositivos • identidad y acceso • Logs de auditoría	

Iniciar Strata Cloud Manager

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW, incluidos los financiados por Créditos de NGFW de software • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

La aplicación Strata Cloud Manager está disponible en el hub de Palo Alto Networks y puede acceder a ella directamente en stratacloudmanager.paloaltonetworks.com.

Una licencia de Prisma Access, una licencia AIOps para NGFW Premium o una licencia Prisma SD-WAN es un requisito básico para la gestión y operaciones unificadas de Strata Cloud Manager. Si tiene al menos una de estas licencias, puede acceder a Strata Cloud Manager para obtener visibilidad o gestionar sus productos.

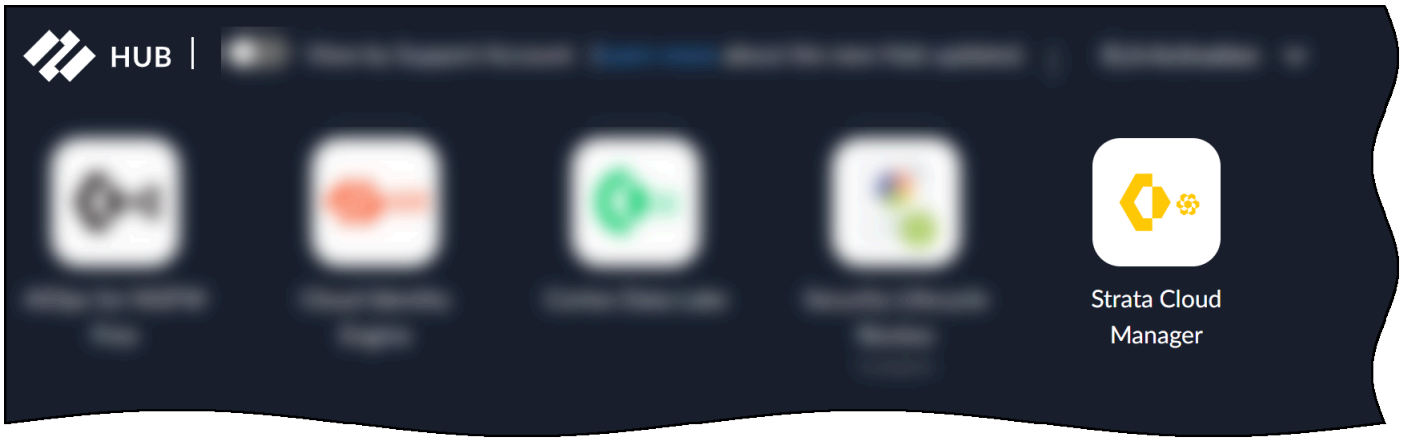
Si tiene más de una de estas licencias, Strata Cloud Manager le brinda una única interfaz para interactuar con estos productos, junto con licencias adicionales o suscripciones complementarias (como sus suscripciones de seguridad de Palo Alto Networks). → Consulte los productos y licencias compatibles *con la gestión y operaciones unificadas de Strata Cloud Manager*

Para iniciar o acceder aStrata Cloud Manager:

- Si es nuevo en Prisma Access, AIOps para NGFW Premium o Prisma SD-WAN en octubre de 2023 o posterior, aquí le mostramos cómo Iniciar Strata Cloud Manager por primera vez
- Si anteriormente usaba aplicaciones independientes y separadas en el hub para gestionar sus productos, aquí encontrará más información sobre cómo Cambiando a Strata Cloud Manager desde una aplicación de producto dedicada

Iniciar Strata Cloud Manager por primera vez

Después de activar una licencia de Prisma Access, AIOps para NGFW Premiumo Prisma SD-WAN, la aplicación Strata Cloud Managerestará disponible para usted en el hub de Palo Alto Networks o puede acceder a ella directamente en stratacloudmanager.paloaltonetworks.com.



Inicie la aplicación y tome una Primer vistazo a Strata Cloud Manager. Continúe incorporando su producto:

- Comience a utilizar AIOps para NGFW Premium, incluida la Gestión en la nube para dispositivos NGFW
- Comience a utilizar Prisma Access
- Comience a utilizar Prisma SD-WAN

Cambiando a Strata Cloud Manager desde una aplicación de producto dedicada

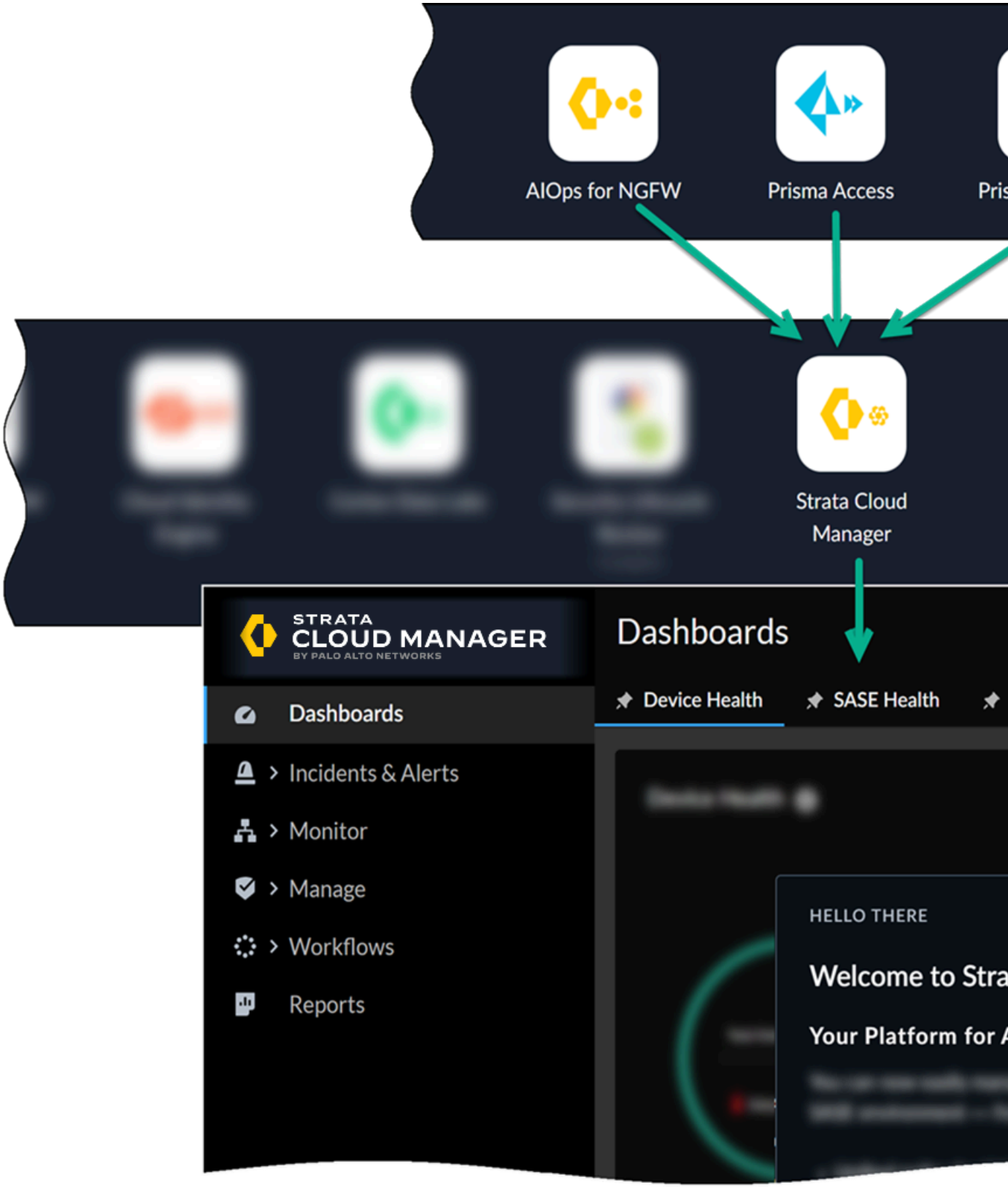
Importante

Esto solo se aplica si anteriormente utilizaba una aplicación independiente para gestionar o interactuar con su producto: la aplicación Prisma Access, la aplicación AIOps para NGFW Premium o la aplicación Prisma SD-WAN. Estas aplicaciones se han actualizado, o se actualizarán pronto, para brindarle una gestión y operaciones de Strata Cloud Manager unificadas.

Qué esperar al mudarse a Strata Cloud Manager desde una aplicación de producto dedicada:

- Strata Cloud Manager proporciona gestión y operaciones unificadas basadas en soporte de licencias: estos son los productos que puede supervisar o gestionar con Strata Cloud Manager.
- Las notificaciones dentro del producto le permitirán saber con anticipación que pronto habrá una actualización para brindarle Strata Cloud Manager.
- La actualización es perfecta y no afecta a sus datos, alertas ni activos.

- Una vez realizada la actualización, iniciará sesión en la aplicación Strata Cloud Manager en el hub; ya no utilizará aplicaciones independientes en el hub para Prisma Access, AIOps para NGFW Premium o Prisma SD-WAN.



- Su aplicación de producto le redirige automáticamente a stratacloudmanager.paloaltonetworks.com. Esta es la URL de Strata Cloud Manager.

  Si anteriormente usaba más de una aplicación de producto que se está actualizando para Strata Cloud Manager, las aplicaciones de producto actualizadas se redireccionarán a la misma instancia de Strata Cloud Manager.

- Strata Cloud Manager le ofrece una navegación completamente nueva que es común en todos sus productos de seguridad de red. Eche un primer vistazo a Strata Cloud Manager y explore la nueva experiencia de navegación y sus funciones.
- **Encuentre las características de su producto en la nueva interfaz de gestión unificada:**
  - AIOps para NGFW: ¿Dónde están mis funciones en Strata Cloud Manager?
  - Prisma SD-WAN: ¿Dónde están mis funciones en Strata Cloud Manager?
  - Insights de Prisma Access ¿Dónde están mis funciones en Strata Cloud Manager?
  - Prisma Access: ¿Dónde están mis funciones en Strata Cloud Manager?

Empezar con Strata Cloud Manager

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW, incluidos los financiados por Créditos de NGFW de software • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Strata Cloud Manager le ofrece gestión y operaciones unificadas basadas en IA para sus NGFW y su red SASE. Aquí tiene una hoja de trucos para empezar a utilizar Strata Cloud Manager por primera vez.

Si está planeando utilizar Strata Cloud Manager para incorporar y gestionar Prisma Access, cortafuegos NGFW (requiere AIOps para NGFW Premium) o ambos juntos, esto incluye lo que necesita saber para comenzar. Gestión compartida para Prisma Access y NGFW

❑ **(En el hub) Active sus licencias**

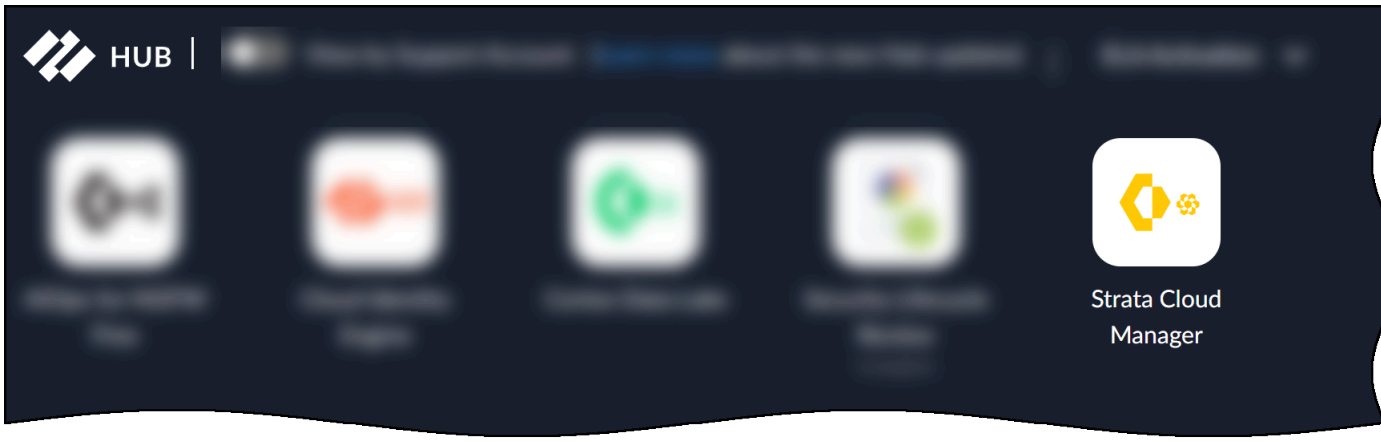
Después de comprar una licencia, recibirá un correo electrónico con un enlace de activación. El enlace inicia un flujo de trabajo guiado en el hub; siga el flujo de trabajo de activación para cada licencia que desee activar:

- Licencia AIOps para NGFW Premium
- Activar una licencia Prisma Access
- Prisma SD-WAN

La activación de cualquiera de estas licencias habilita Strata Cloud Manager. Después de haber activado al menos una de estas licencias, deberá activar cualquier licencia adicional o suscripciones complementarias.

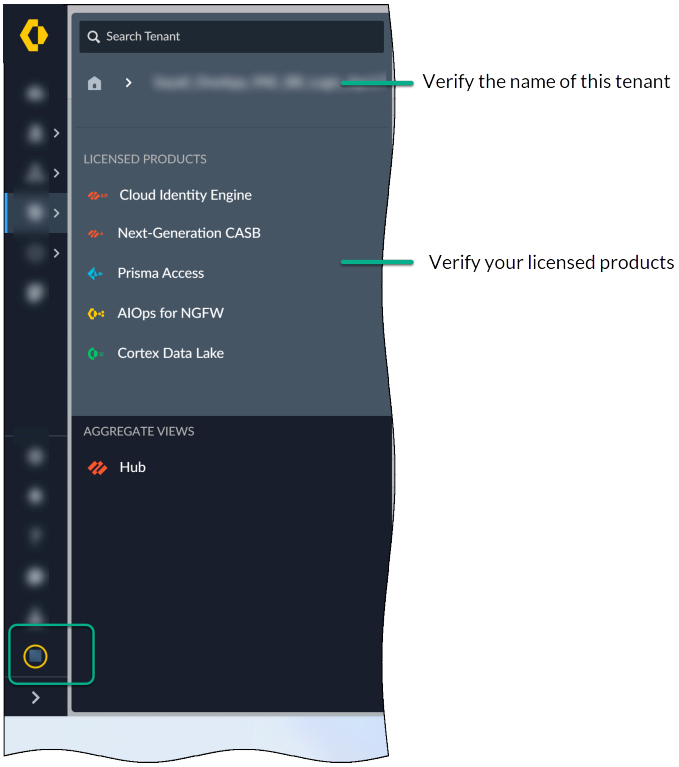
Iniciar Strata Cloud Manager

Después de activar una licencia de Prisma Access, AIOps para NGFW Premiumo Prisma SD-WAN, la aplicación Strata Cloud Managerestará disponible para usted en el hub de Palo Alto Networks, o puede acceder a ella directamente en stratacloudmanager.paloaltonetworks.com.



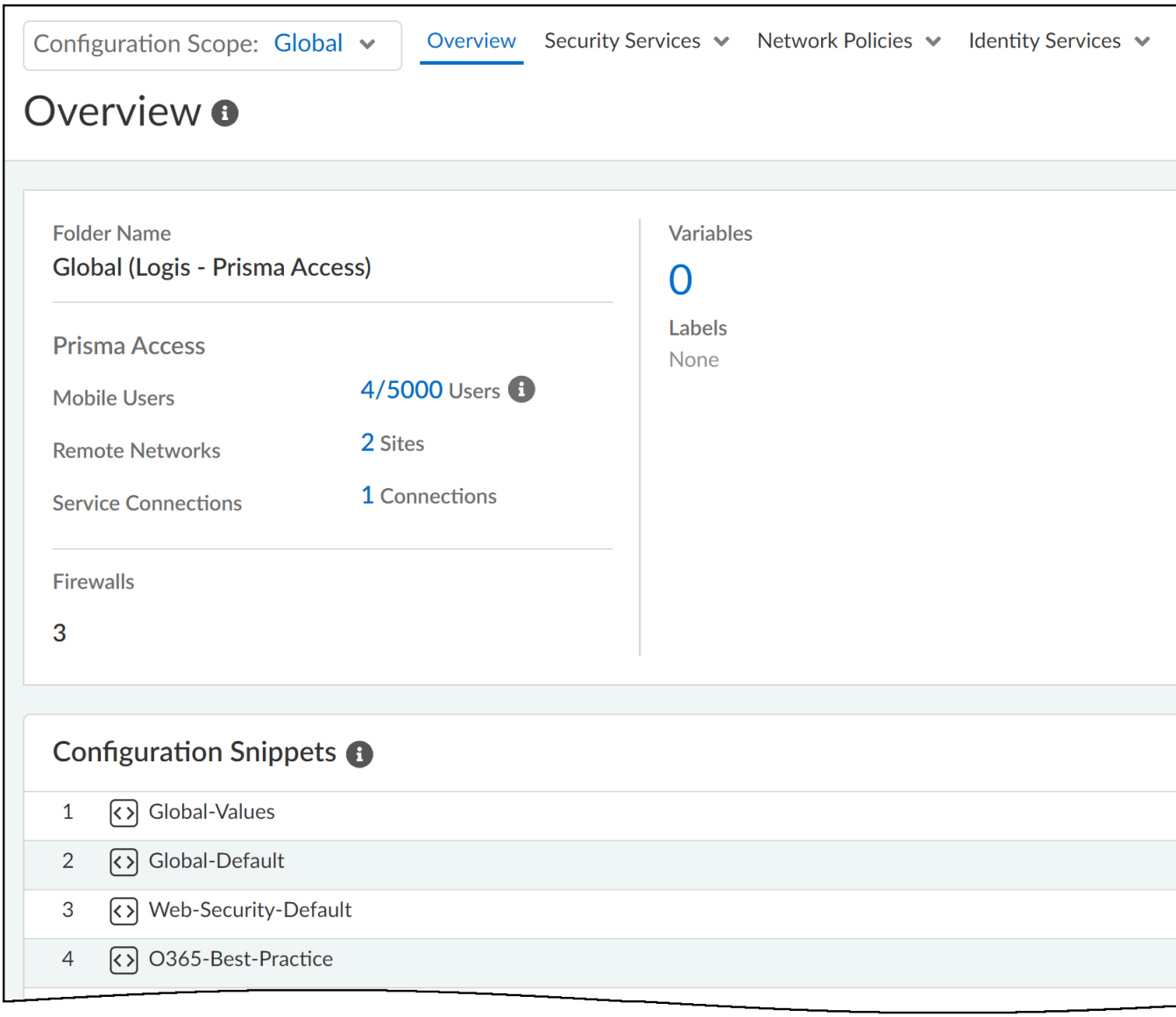
Valide sus licencias

- En la parte inferior del menú de navegación, seleccione los detalles de su inquilino y verifique el nombre del inquilino que está utilizando y sus productos con licencia. Aquí encontrará más información sobre la gestión de inquilinos y suscripciones.



- Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** para verificar el estado y los detalles de su licencia de Prisma Access, y ver qué otros detalles podrían estar disponibles.

Es posible que aún no vea muchos datos aquí si aún no ha incorporado NGFW o si su entorno Prisma Access aún se está aprovisionando. Si ese es el caso, vuelva a consultar pronto después de haber completado el resto de los pasos aquí.



- **Supervisión y visibilidad con Strata Cloud Manager**
  - Explore una representación visualizada de su red y su infraestructura de seguridad con el Centro de control.
  - Revise datos importantes de la red en Activity Insights.
  - Explora los paneles de control de Strata Cloud Manager disponibles para usted. Muchos paneles también admiten informes que puede programar o compartir con las partes interesadas.
  - Supervise su entorno Prisma Access, Prisma SD-WAN y sus NGFW.
  - Revise sus incidentes y alertas en Prisma Access, NGFW y Prisma SD-WAN.
- **Recomendaciones y flujos de trabajo de prácticas recomendadas en línea**

  Obtenga más información sobre la orientación y la automatización de las prácticas recomendadas integradas directamente en Strata Cloud Manager.

- **Configuración de incorporación de Strata Cloud Manager**

  Strata Cloud Manager reúne servicios comunes en el menú **Settings (Configuración)**. Vaya a **Settings (Configuración)** para gestionar:

  - Roles y permisos: obtenga más información sobre los roles disponibles en Strata Cloud Manager y los permisos asociados.
  - Asociaciones de dispositivos: asocie aplicaciones en la nube compatibles con sus dispositivos.
  - Gestión de inquilinos: cree y gestione su jerarquía de organizaciones y unidades comerciales, representadas por inquilinos.

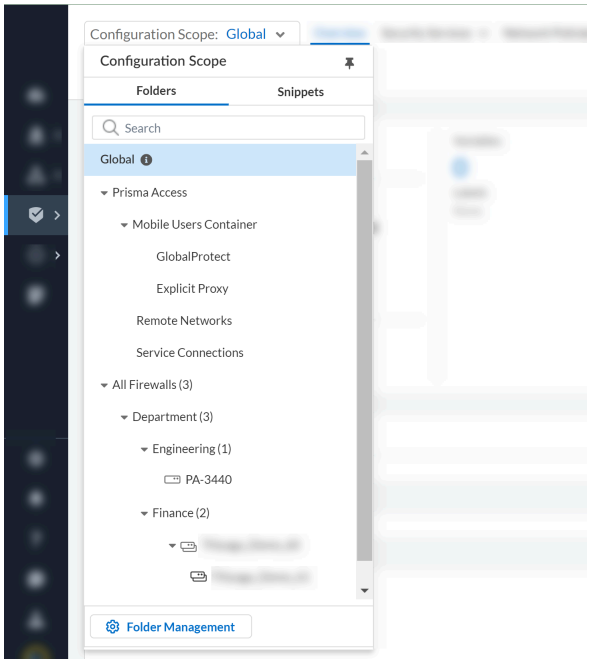
Gestión compartida para Prisma Access y NGFW

Para Prisma Access y NGFW, Strata Cloud Manager proporciona gestión compartida; NGFW integrados y usuarios de Prisma Access, redes remotas y conexiones de servicio a Strata Cloud Manager, y aplica una política de seguridad común.

- **Incorporación de dispositivos NGFW y Prisma Access a Strata Cloud Manager**
  - Configure Prisma Access e incorpore usuarios móviles, redes remotas y conexiones de servicio:
    - Configurar la infraestructura del servicio Prisma Access
    - Configurar los usuarios móviles de Prisma Access, incluidas las conexiones GlobalProtect y Proxy explicito
    - Configurar las redes remotas de Prisma Access
    - Configurar las conexiones del servicio Prisma Access
  - Incorporación y configuración de NGFW:
    - Incorporación y configuración para la gestión de la nube NGFW
- **Organizando su configuración**

  Cuando se trabaja con los ajustes de configuración de Strata Cloud Manager, la Gestionar: Alcance de la configuración actual siempre está visible para usted y puede alternar su vista para gestionar una configuración más amplia o más granular. El alcance de configuración le permite

aplicar políticas de forma global o proporcionar una aplicación específica para ciertos NGFW o implementaciones de Prisma Access.



Aquí encontrará más información sobre cómo comenzar a organizar su configuración de Strata Cloud Manager:

- **Flujos de trabajo: Gestión de carpetas**

  Utilice carpetas para agrupar lógicamente los NGFW para una gestión de configuración simplificada. Las carpetas de Prisma Access están predefinidas según el tipo de implementación. También puede habilitar la Seguridad web (una experiencia de gestión simplificada para administradores que gestionan el acceso a Internet y aplicaciones SaaS) a nivel de carpeta.

- **Gestionar: Fragmentos**

  Utilice fragmentos para agrupar configuraciones que pueda enviar rápidamente a sus NGFW o implementaciones de Prisma Access.

- **Gestionar: Variables**

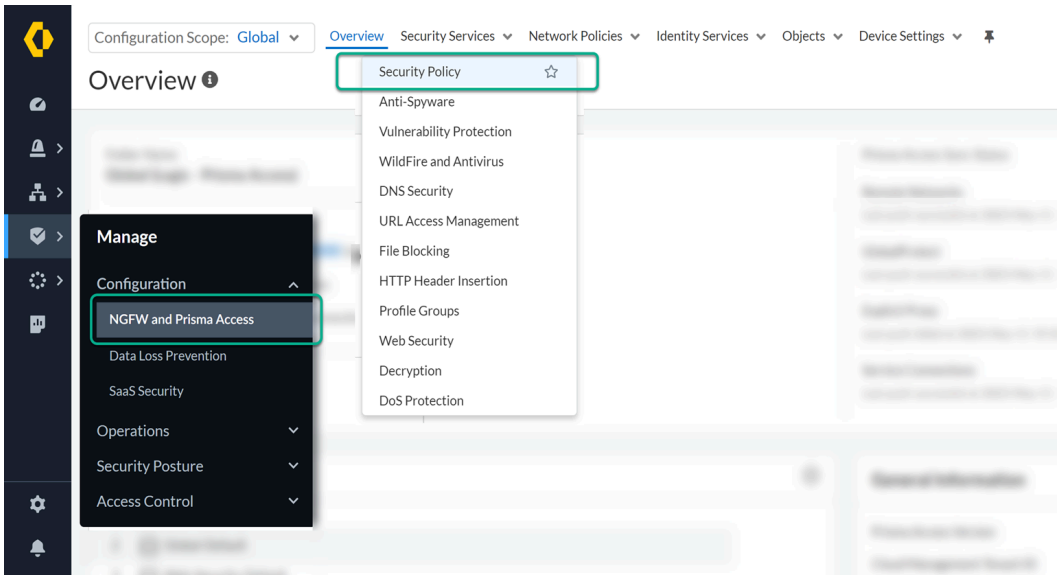
  Utilice variables en sus configuraciones para acomodar dispositivos u objetos de configuración específicos de la implementación.

- **Política de seguridad compartida para dispositivos NGFW y Prisma Access**

  Strata Cloud Manager le ofrece una gestión unificada para Prisma Access y sus NGFW. Su política de vsecurity de Strata Cloud Manager es compartida y se puede aplicar globalmente en

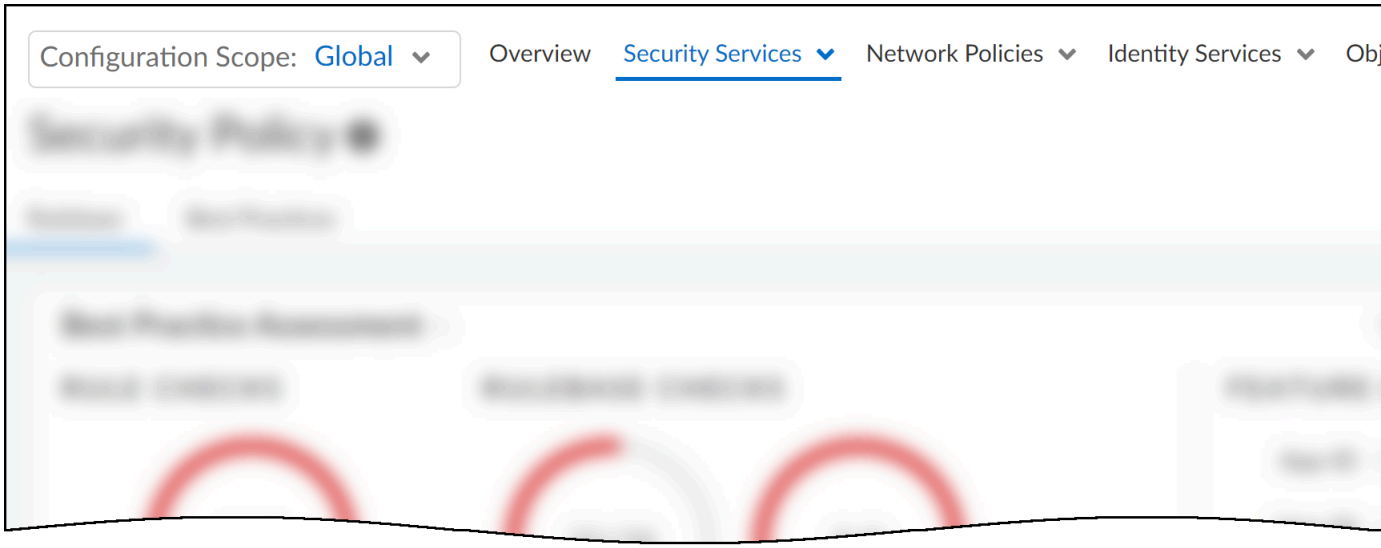
Prisma Access y NGFW, o bien apuntar a configuraciones específicas a implementaciones de Prisma Access o grupos específicos de cortafuegos.

Vaya a **Manage (Gestionar) > Configuration (Configuración) > NGFW and Prisma Access (NGFW y Prisma Access)** para comenzar.



- **Envío de cambios de configuración a dispositivos NGFW y Prisma Access**

  Al gestionar su configuración de Strata Cloud Manager, seleccione **Push Config (Enviar configuración)** para enviar los cambios de configuración a sus NGFW y Prisma Access:



Se le solicitará que establezca el alcance del envío de configuración, en función de sus carpetas. Aquí encontrará más información sobre cómo:

- Envíe sus cambios de configuración
- Revise el estado de un envío de configuración
- Vea cómo puede limpiar su configuración

Prácticas recomendadas integradas en Strata Cloud Manager

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW, incluidos los financiados por Créditos de NGFW de software • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Las prácticas recomendadas de Palo Alto Networks se han diseñado para ayudarle a obtener la red más segura posible al agilizar el proceso de verificación del cumplimiento de su infraestructura de red. Hemos creado comprobaciones de prácticas recomendadas directamente en Strata Cloud Manager, para que pueda obtener una evaluación en vivo de su configuración. Ajuste su postura de seguridad alineándose con las prácticas recomendadas. Puede aprovechar Strata Cloud Manager para evaluar sus configuraciones de seguridad de Panorama, NGFW y Prisma Access gestionadas por Panorama, en función de las prácticas recomendadas, y corregir las comprobaciones de prácticas recomendadas con errores.

La orientación sobre las prácticas recomendadas tiene como objetivo ayudarle a reforzar su postura de seguridad, pero también a gestionar su entorno de manera eficiente y a permitir la productividad de los usuarios. Evalúe continuamente su configuración comparándola con estas comprobaciones en línea, y cuando vea una oportunidad para mejorar su seguridad, tome medidas y hágalo.

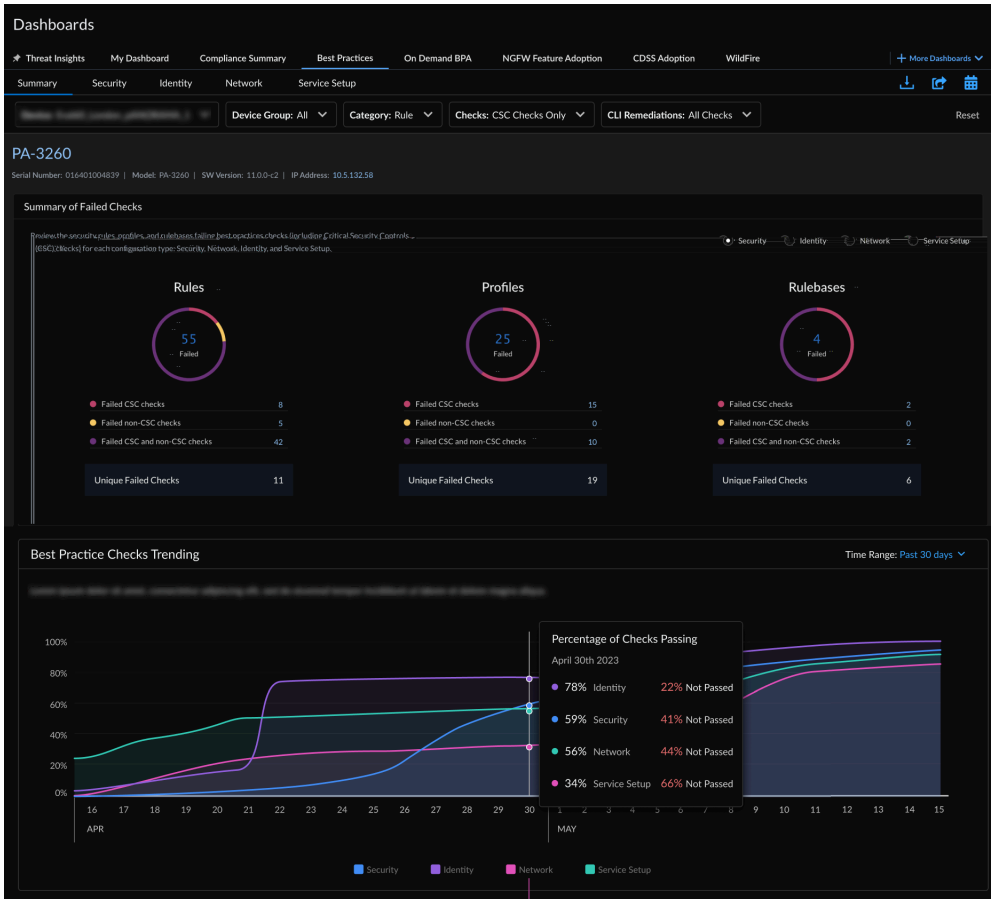
Visibilidad de la adopción y cumplimiento de las prácticas recomendadas

Para empezar, puede evaluar rápidamente su postura general de seguridad consultando los siguientes **Dashboards (Paneles)** de postura.

Vea cómo le va a un nivel alto y especifique las áreas donde es posible que desee comenzar a tomar medidas.

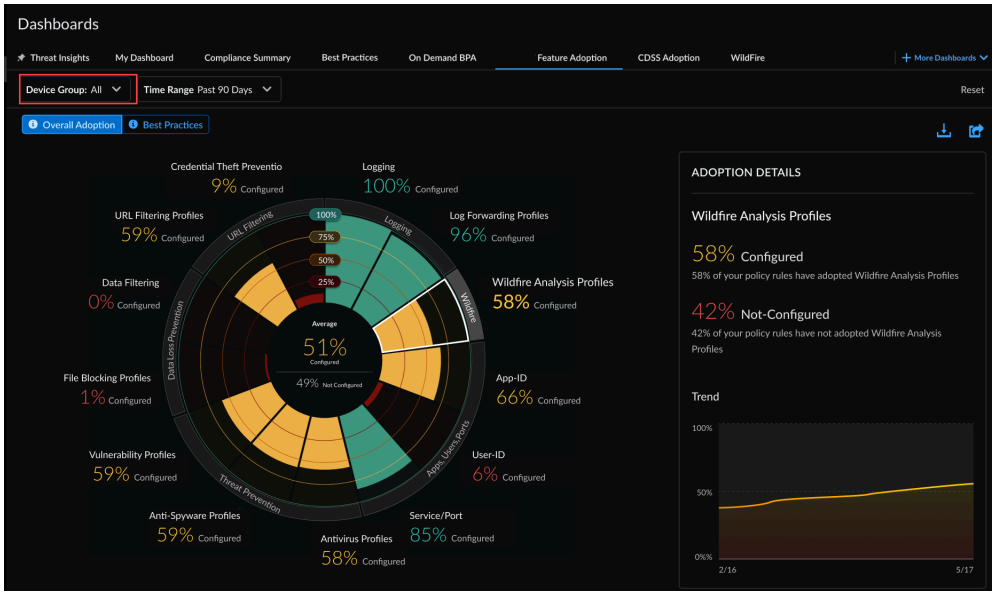
- Compruebe el panel de Panel: Prácticas recomendadas para obtener informes diarios de prácticas recomendadas y su asignación a las comprobaciones de controles de seguridad críticos (CSC) del Centro para la Seguridad de Internet, para ayudarle a identificar áreas en las que puede realizar cambios para mejorar el cumplimiento de sus prácticas recomendadas.

Comparta el informe de prácticas recomendadas en formato PDF y prográmelo para que se entregue regularmente en su bandeja de entrada.

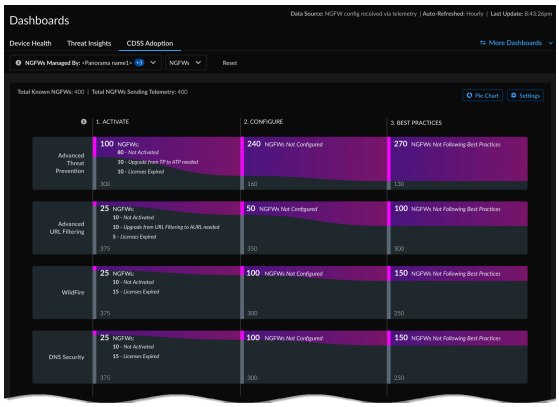


- Consulte el panel Resumen de cumplimiento para ver un historial de cambios en las comprobaciones de seguridad realizadas hasta 12 meses en el pasado, agrupados por los marcos del Centro para la Seguridad de Internet (CIS) y el Instituto Nacional de Estándares y Tecnología (NIST).

- Supervise la Panel: Adopción de características y manténgase al tanto de las características de seguridad que está utilizando en su implementación y de las posibles brechas en la cobertura.



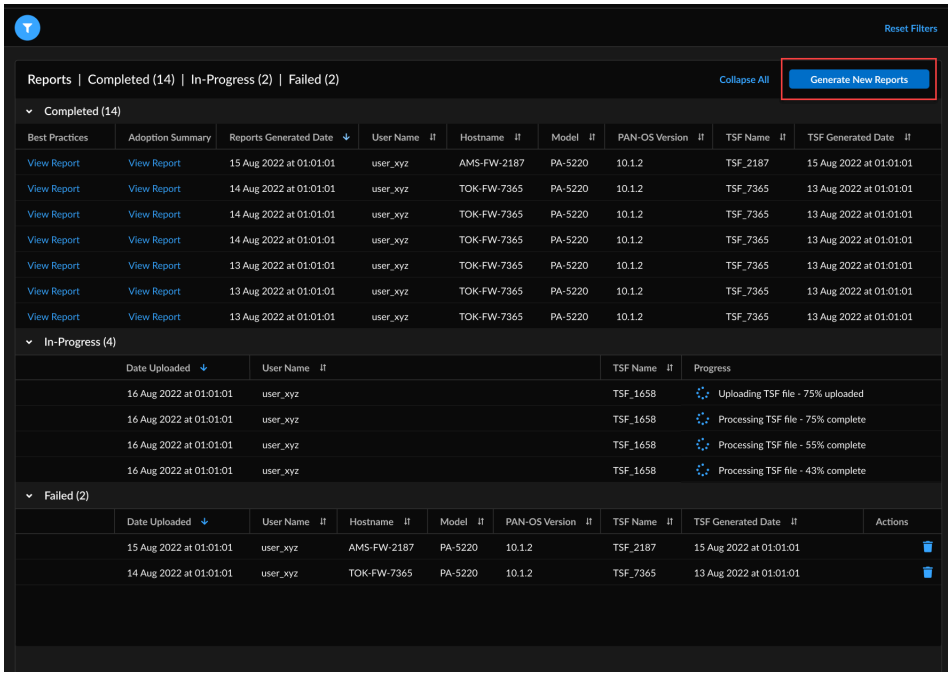
- Supervisar Panel: Adopción de CDSS: vea los servicios de seguridad o las suscripciones a funciones y su uso de licencias en sus dispositivos para identificar brechas de seguridad y fortalecer la postura de seguridad de su empresa.



- Obtenga visibilidad del estado de seguridad y la tendencia de su implementación en función de las posturas de seguridad de los dispositivos NGFW incorporados con Panel: Información

sobre la postura de seguridad y reciba alertas cuando ocurran incidentes o la configuración de seguridad pueda necesitar un análisis más detallado.

- Genere Informes de BPA para dispositivos PAN-OS (que no son de telemetría) que ejecutan versiones 9.1 y posteriores, que ahora incluyen métricas de adopción de características.



Herramientas de prácticas recomendadas para Fortalecer la postura de seguridad

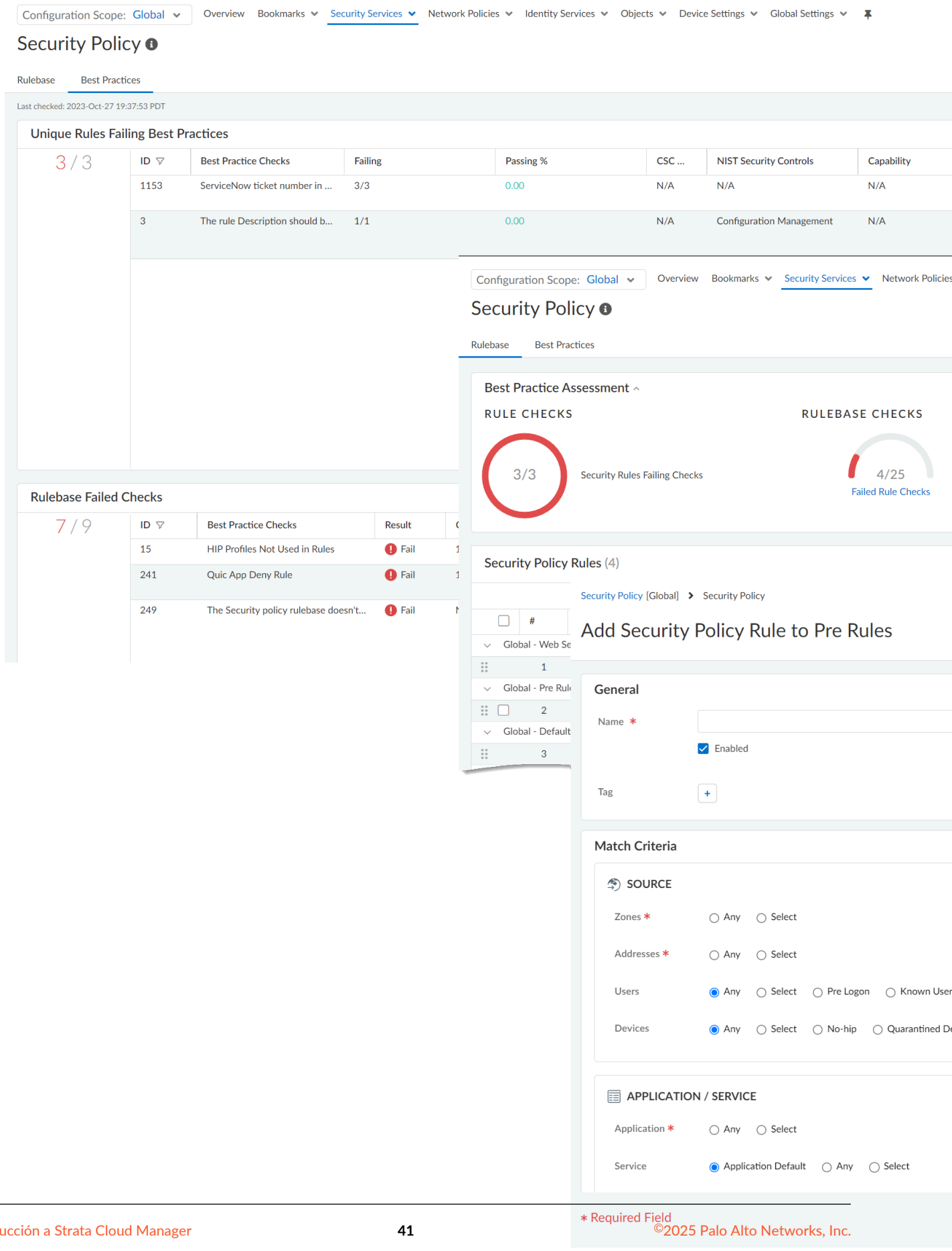
Encuentre una colección de herramientas para ayudarle a mejorar su postura de seguridad.

- Personalice las comprobaciones de postura de seguridad para su implementación a fin de maximizar las recomendaciones pertinentes en Gestionar: Configuración de la postura de seguridad
- Utilice la Limpieza de la configuración para identificar y eliminar objetos de configuración y reglas de políticas no utilizados.
- Configure la Configuración de Policy Optimizer para perfeccionar y optimizar las reglas de seguridad excesivamente permisivas de modo que solo permitan aplicaciones que se estén utilizando realmente en su red.

- Cree sus propias Comprobaciones de cumplimiento: personalice las comprobaciones de prácticas recomendadas existentes y cree y gestione exenciones especiales para alinearse mejor con los requisitos empresariales de su organización.
- Utilice un Analizador de políticas para asegurarse de que las actualizaciones que realice a sus reglas de Política de seguridad cumplan con sus requisitos y no introduzcan errores o configuraciones incorrectas (como cambios que resulten en reglas duplicadas o conflictivas).

Comprobaciones de configuración de prácticas recomendadas en línea en directo

La orientación sobre las prácticas recomendadas tiene como objetivo ayudarle a reforzar su postura de seguridad, pero también a gestionar su entorno de manera eficiente y a permitir la productividad de los usuarios. Evalúe continuamente su configuración comparándola con estas comprobaciones en línea, y cuando vea una oportunidad para mejorar su seguridad, tome medidas y hágalo.



- **Puntuaciones de prácticas recomendadas**

  Las puntuaciones de las prácticas recomendadas se muestran en un panel de funciones (política de seguridad, descifrado o control de acceso a URL, por ejemplo). Estas puntuaciones le dan una visión rápida de su progreso con las prácticas recomendadas. De un vistazo, puede identificar las áreas que requieren una investigación más profunda o en las que desea tomar medidas para mejorar su posición de seguridad.
- **Verificaciones de campo de las prácticas recomendadas**

  Las comprobaciones a nivel de campo le muestran exactamente dónde su configuración no se alinea con las prácticas recomendadas. Las pautas sobre las prácticas recomendadas se proporciona en línea, para que pueda tomar medidas inmediatamente.
- **Evaluación de prácticas recomendadas**

  Aquí puede obtener una vista completa de cómo la implementación de la función se alinea con las prácticas recomendadas. Examine los controles que han fallado para ver dónde puede realizar mejoras (también puede revisar los controles aprobados). Las comprobaciones de la base de reglas destacan los cambios de configuración que puede realizar fuera de las reglas individuales, por ejemplo, en un objeto de políticas que se utiliza en varias reglas.

Los controles de prácticas recomendadas están disponibles para:

- **Su base de reglas de la política de seguridad**

  Las comprobaciones de la base de reglas analizan cómo se organiza y gestiona la política de seguridad, incluidos los ajustes de configuración que se aplican a muchas reglas.
- **Reglas de seguridad**
- **Perfiles de seguridad**
  - Antispyware
  - Protección contra vulnerabilidades
  - WildFire y Antivirus
  - Gestión de acceso a URL
  - DNS Security
- **Autenticación**
- **descifrado**
- **GlobalProtect**

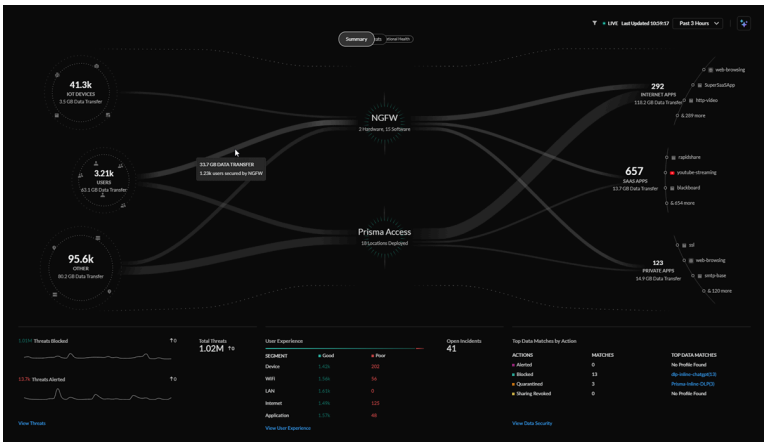
¿Busca más información sobre las prácticas recomendadas de Palo Alto Networks?

Esta es la Página principal de prácticas recomendadas, donde puede encontrar recursos para ayudarle a realizar la transición a las prácticas recomendadas e implementarlas.

Centro de comando: Strata Cloud Manager

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software • Prisma SD-WAN	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro ❑ Strata Cloud Manager Essentials ❑ Prisma SD-WAN Las demás licencias y requisitos previos necesarios para acceder al centro de control: ❑ Strata Logging Service ❑ Una licencia específica para ver ciertas métricas en el centro de control que se describe a continuación ❑ Un rol que tiene permiso para ver el Centro de control → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

El Centro de control de Strata Cloud Manager es su nueva página de inicio de NetSec; es un resumen visual interactivo que le ayudará a evaluar el estado, la seguridad y la eficiencia de su red. El centro de control proporciona una vista consolidada de la plataforma NetSec y le brinda una visibilidad completa de sus orígenes, aplicaciones, implementación de Prisma Access, sus NGFW y sus servicios de seguridad en un único lugar.



El centro de control le permite interactuar con los datos y visualizar las relaciones entre los eventos en la red, para que pueda tomar acciones inmediatas para reforzar su seguridad.

El centro de control está integrado con los nuevos paneles de Active Insights **(Insights > Activity Insights)**, y resaltará las anomalías detectadas por sus licencias y suscripciones incorporadas a través de información útil, y proporcionará una ruta para corregir esas anomalías.

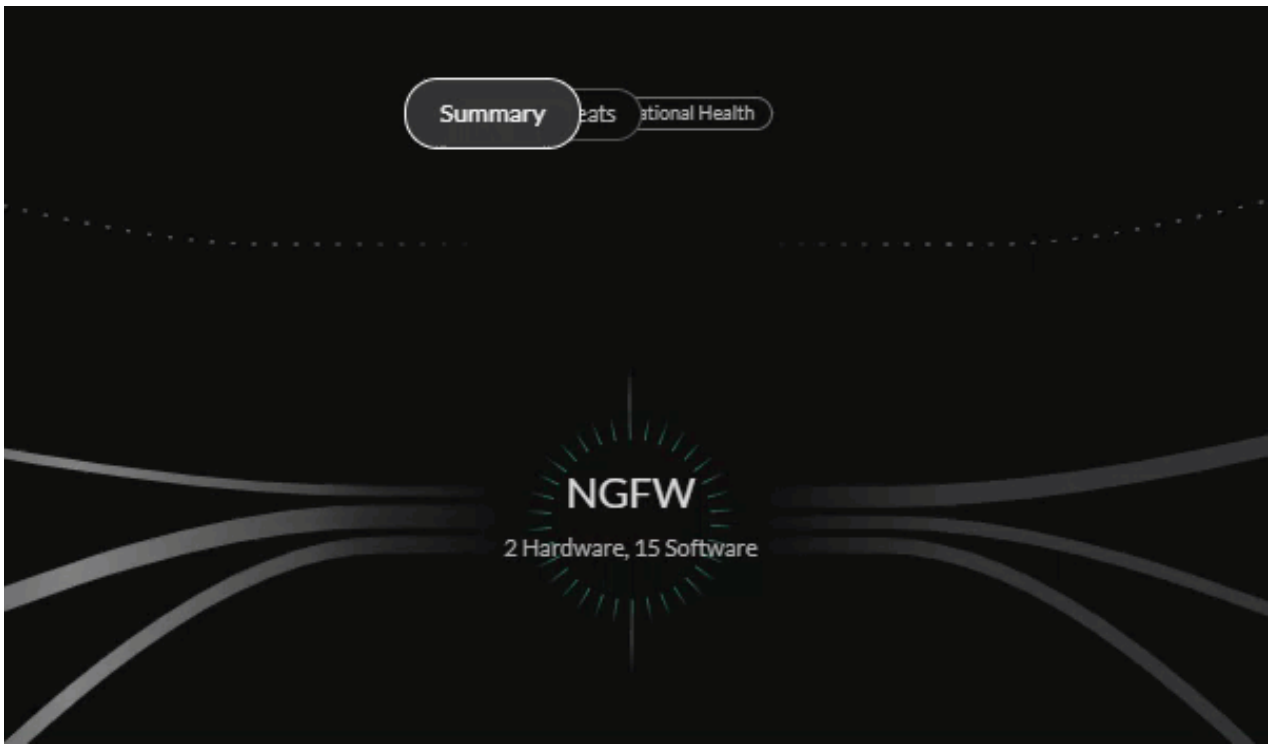
Desde la nueva página de inicio, puede ver:

- Una visión completa de todo el tráfico en su red que fluye de fuentes (usuarios, IoT, hosts externos) a aplicaciones (Internet, SaaS, privadas).
- Cómo se accede y protege a activos como usuarios, dispositivos y aplicaciones.
- Vaya a paneles específicos con contexto para comprender mejor los problemas que afectan a su red.
- Tipos de amenazas encontradas mientras los usuarios están trabajando.

Inicie Strata Cloud Manager y haga clic en **Command Center (Centro de control)** ( ) para comenzar.

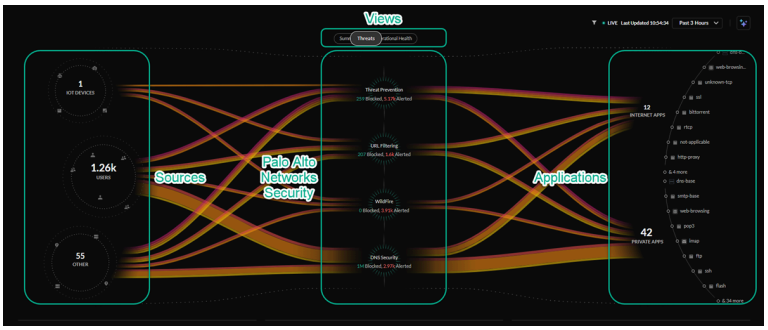
Cómo interactuar con el centro de control de Strata Cloud Manager

Cada vista en el centro de control desglosa cuidadosamente toda la información que necesitaría para evaluar el estado y la seguridad de su red.



Los datos en el centro de control se actualizan cada 5 minutos y por defecto muestran datos de las últimas 24 horas. También puede filtrar estos datos por las últimas 1 hora, 3 horas, 7 días o 30 días.

Cada vista del centro de control muestra diferentes tipos de datos visuales que fluyen desde las fuentes, a través de Prisma Access y NGFW o suscripciones de seguridad implementadas en su red, a las diversas aplicaciones de su red.



Las burbujas Sources (trabajadores híbridos, usuarios de oficina, dispositivos IoT y otros) están a la izquierda y las burbujas Applications (accesibles en Internet, SaaS y alojadas en la nube o in situ) están a la derecha. Las burbujas de aplicaciones muestran las tres aplicaciones más utilizadas en cada categoría.

Las fuentes incluyen:

- **IoT Devices (Dispositivos IoT)**: dispositivos descubiertos por una licencia de seguridad IoT activa y habilitada,
- **Users (Usuarios)**: usuarios remotos y de sucursales.
- **Others (Otros)**: anfitriones internos y externos que acceden a recursos en Internet.

Las aplicaciones incluyen:

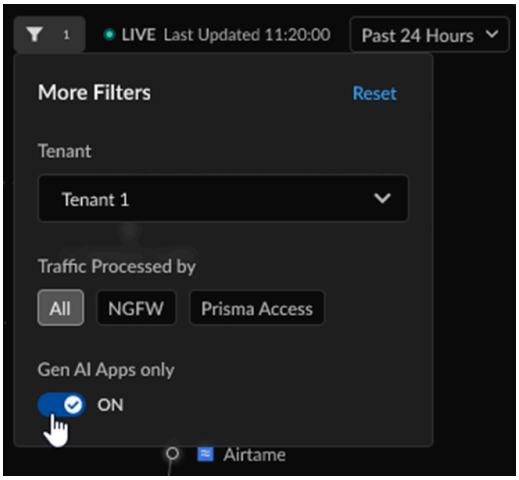
- **Internet Apps (Aplicaciones de internet)**: aplicaciones a las que se accede mediante un navegador web.
- **SaaS Apps (Aplicaciones SaaS)**: aplicaciones en la nube propiedad de y gestionadas por un proveedor de servicios de aplicaciones.
- **Private Apps (Aplicaciones privadas)**: aplicaciones alojadas en un centro de datos.

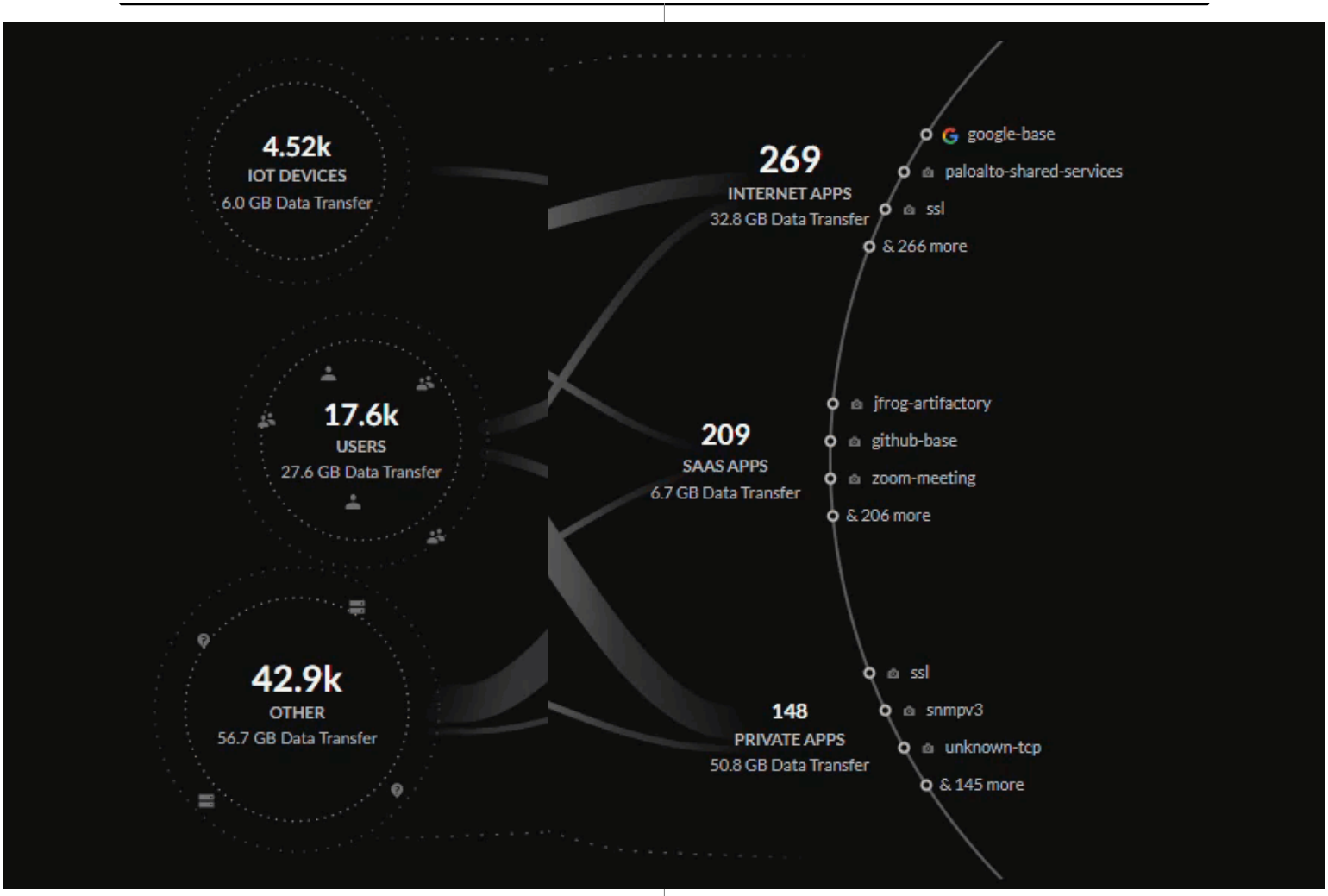
Puede filtrar los datos en la vista central haciendo clic en las burbujas para orígenes, implementaciones o aplicaciones. Esto le dará una vista más detallada de los datos rastreados para esa vista en relación con la burbuja seleccionada.

Seleccionando filtros (▼), puede filtrar los datos en las vistas del centro de control por datos específicos **Tenant (Inquilino)** o **NGFW** o **Prisma Access**.

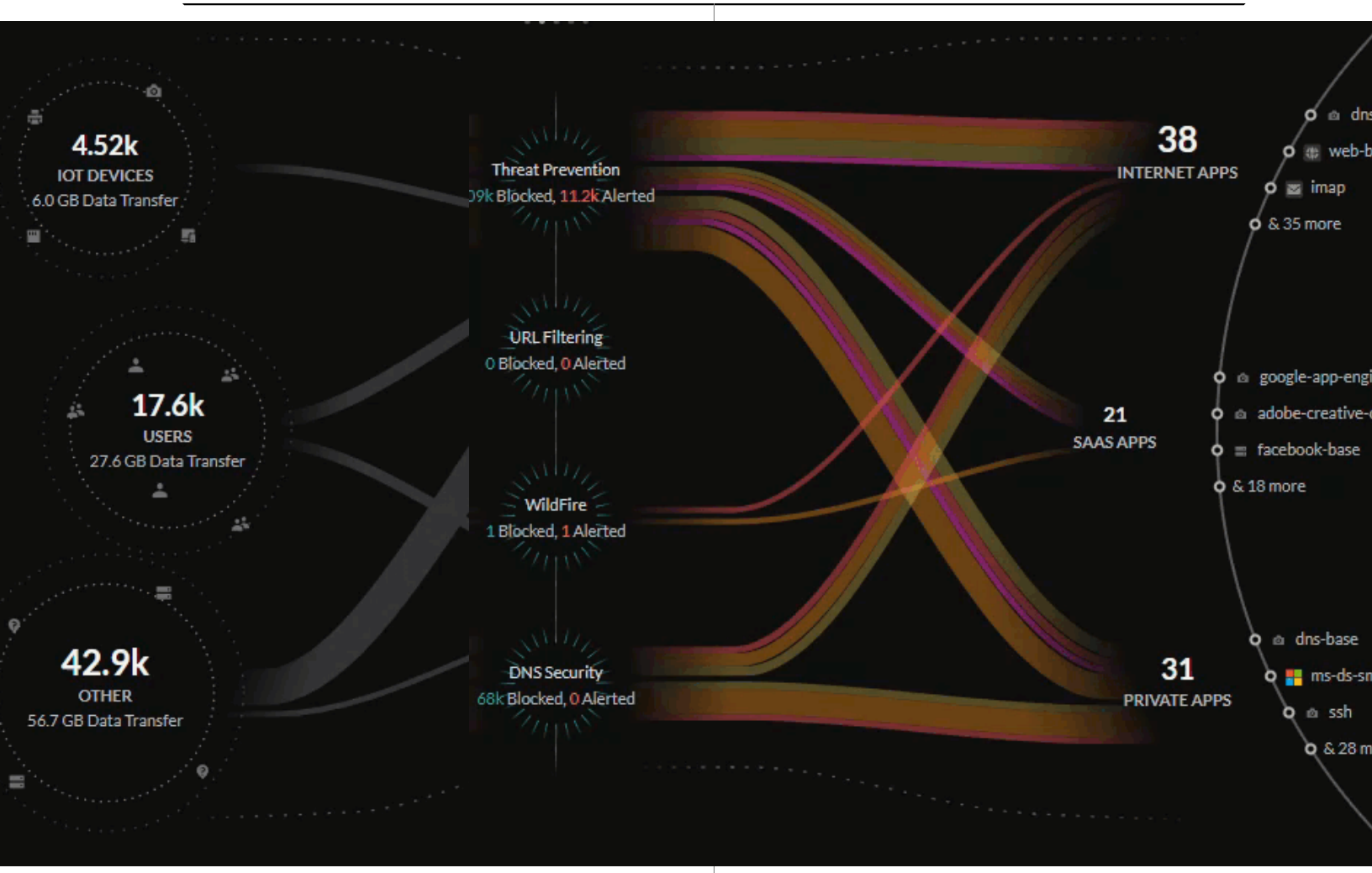
Con una licencia de AI Access, puede filtrar el tráfico en todas las vistas del centro de control por **GenAI Apps only (Solo aplicaciones GenAI)** para evaluar mejor cómo las aplicaciones GenAI que usan los usuarios de su red pueden estar afectando a la seguridad de sus datos.

Para obtener más información sobre las licencias de AI Access Security, haga clic aquí.

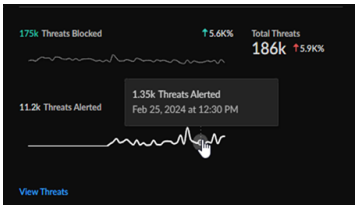




Al ver una de las vistas, puede pasar el ratón sobre las líneas para obtener más información sobre su red, como el tráfico o las amenazas bloqueadas o permitidas en su red.



Debajo del resumen visual central hay varias métricas clave rastreadas por las suscripciones que tiene activadas y que proporcionan información útil sobre su red. Estas métricas clave proporcionan la capacidad de navegar a una de las varias páginas de contexto detalladas donde se puede encontrar más información sobre las métricas que han surgido y profundizar en posibles soluciones.



Vistas del centro de control de Strata Cloud Manager

El centro de controls le proporciona cuatro vistas diferentes, cada una con sus propios datos y métricas rastreados para examinar e interactuar.

- Resumen
- Threats (Amenazas)
- Estado operativo
- Seguridad de datos

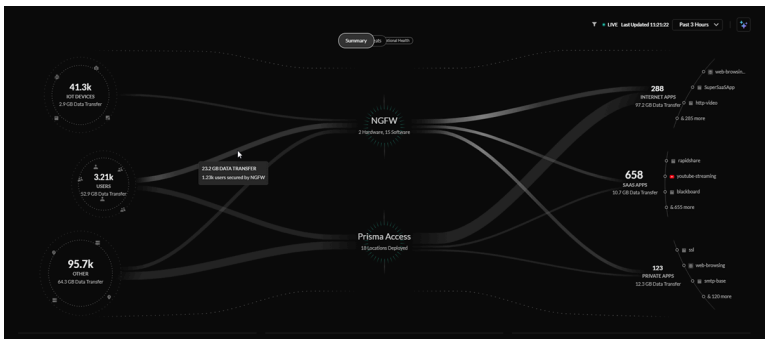
Centro de control (Resumen)

La vista **Summary (Resumen)** le ofrece un vistazo de alto nivel de todo el tráfico de sus usuarios, hosts externos, dispositivos IoT y aplicaciones, así como una vista previa de algunos de los problemas y anomalías en su red que las otras vistas destacan. Puede usar esta vista como el primer vistazo al estado de su red cada día.

Resumen de licencias	• Debe tener al menos una de estas licencias que viene con una licencia de Strata Logging Service para usar el centro de control de Strata: ❑ Licencia de Prisma Access ❑ Licencia de AIOps para NGFW Premium • O una licencia AIOPs para NGFW Free junto con una licencia de Strata Logging Service • Licencias necesarias para métricas adicionales en la vista Resumen: ❑ Suscripciones a CDSS (Cloud-Delivered Security Services) ❑ Suscripciones a Seguridad de datos ❑ Licencia ADEM ❑ Licencia de AI Access

Vista de resumen central

La vista Resumen central proporciona un vistazo a los datos que se transfieren entre los dispositivos de IoT, los usuarios, los hosts externos que acceden a recursos de Internet, las aplicaciones de Internet, las aplicaciones SaaS y las aplicaciones privadas de su red.



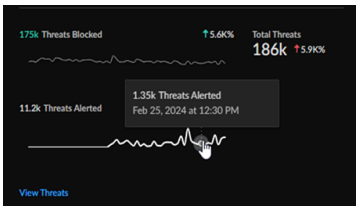
Las líneas de la vista Resumen central representan las transferencias de datos y el tráfico en su red, y el grosor de las líneas representa el volumen de datos transferidos desde fuentes y aplicaciones.

Puede ver cómo su infraestructura de red protege estas fuentes:

- Implementaciones de Prisma Access
- Cortafuegos de nueva generación de su inventario de Strata Logging Service

Recuento total de amenazas

El widget **Total Threats Count (Recuento total de amenazas)** le ofrece una vista rápida del número total de amenazas detectadas en su red, cuántas amenazas se han bloqueado, cuántas amenazas se han alertado y el cambio en las amenazas de un rango de tiempo seleccionado.



Haga clic en la pantalla Activities Insights **[Insights > Activity Insights > Threats (Amenazas)]** para obtener un desglose más detallado de las amenazas en su red.

Incidentes abiertos y experiencia de usuario

El widget **Open Incidents and User Experience (Incidentes abiertos y experiencia del usuario)** le ofrece una visión del recuento total de incidentes abiertos; el desglose de la experiencia del usuario, buena y potencialmente degradada, a partir de segmentos individuales de la cadena de prestación de servicios desde un dispositivo de usuario a una aplicación, y el cambio en los incidentes abiertos de un intervalo de tiempo seleccionado.

Haga clic en el panel de Experiencia de aplicación **[Dashboards (Paneles) > Application Experience (Experiencia de aplicación)]** para obtener un desglose más detallado de la experiencia de usuario y estado en su red y las métricas de rendimiento.

Principales perfiles de datos por acción

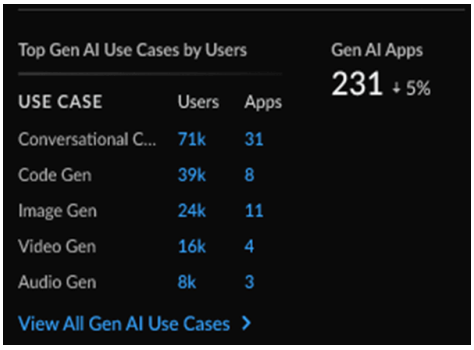
Los widgets **Top Data Profiles (Principales perfiles de datos)** le ofrecen una vista de los perfiles de filtrado de datos predefinidos superiores, el número de coincidencias encontradas en el tráfico de red y la acción realizada para los datos confidenciales basados en esos perfiles de datos.

Haga clic en la vista Seguridad de datos **[Command Center (Centro de control) > Data Security (Seguridad de datos)]** para obtener un desglose más detallado de los datos confidenciales de su red.

Principales casos de uso de GenAI por usuarios y aplicaciones GenAI

El widget **Top GenAI Use Cases by User (Casos de uso de GenAI por usuarios)** le ofrece una vista de los principales casos de uso para aplicaciones GenAI que utilizan los usuarios en sus redes, el número de usuarios para cada caso de uso y el número de aplicaciones GenAI que se incluyen en cada caso de uso.

También puede ver el número total de aplicaciones GenAI en sus redes, así como el cambio porcentual en las aplicaciones basado en el filtro de tiempo.



Haga clic en el panel de control de seguridad de acceso a la IA **[Insights > AI Access (Acceso de IA)]** en Activity Insights para obtener un desglose más detallado de la adopción de aplicaciones GenAI en su red y recomendaciones sobre cómo proteger mejor sus datos.

Para obtener más información sobre AI Access Security y cómo su organización puede adoptar aplicaciones GenAI de forma segura al tiempo que se mitigan los riesgos para la seguridad de sus datos, comience aquí.

Threats (Amenazas)

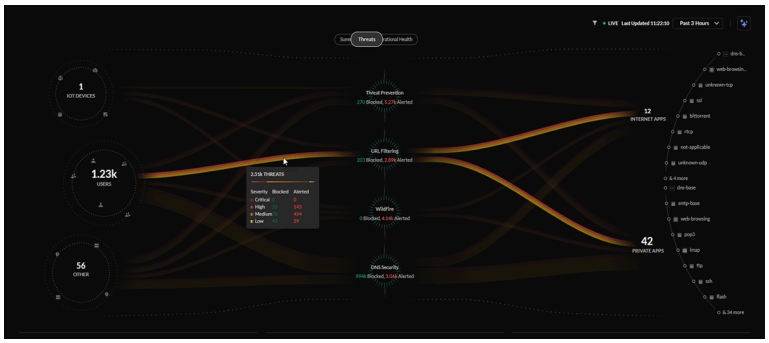
La vista **Threats (Amenazas)** muestra el tráfico inspeccionado en su red y las amenazas detectadas por sus suscripciones CDSS. Puede usar esta vista para supervisar las amenazas bloqueadas y alertadas en su red, o investigar áreas de su red que necesitan políticas actualizadas para bloquear de forma más efectiva cualquier amenaza alertada.

Licencias de amenazas	• Licencias de amenazas, incluidas: ❑ Licencia de prevención de amenazas ❑ Licencia de filtrado de URL ❑ Licencia WildFire ❑ Licencia DNS Security

Vista central de amenazas

La vista central de Amenazas proporciona un vistazo a todas las amenazas en su red que sus suscripciones de servicios de seguridad activas en la nube han identificado.

La vista Amenazas mostrará cómo sus suscripciones a Palo Alto Networks CDSS protegen su tráfico mediante la supervisión de amenazas potenciales en su red. El centro de control le ofrece información sobre el porcentaje de tráfico inspeccionado para sus dispositivos, usuarios y aplicaciones de IoT, y el número total de amenazas permitidas o alertadas.

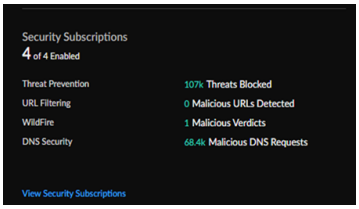


Las líneas de la vista central de Amenazas representan el tráfico supervisado por sus suscripciones de seguridad, y el grosor representa el volumen de amenazas detectadas y el color si las amenazas son de gravedad crítica, alta, media o baja.

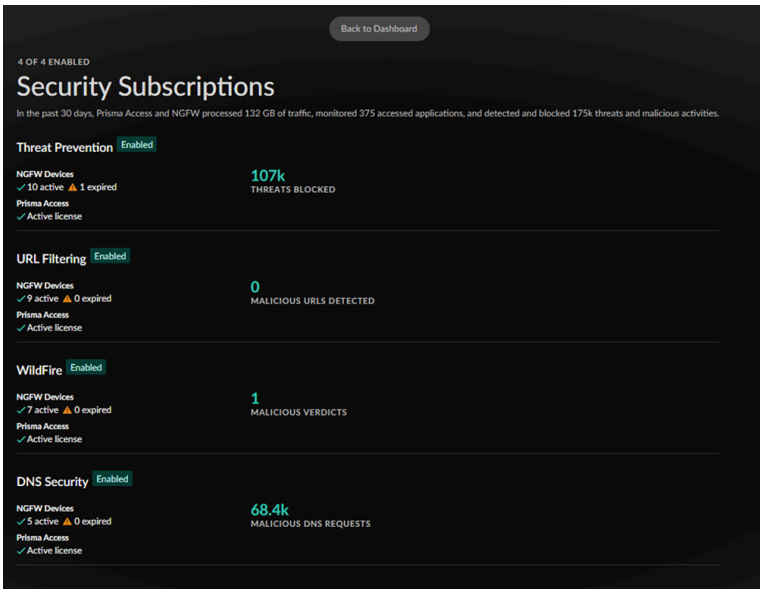
Suscripciones de seguridad:

El widget **Security Subscriptions (Suscripciones de seguridad)** le ofrece una vista de las suscripciones de seguridad entregadas en la nube, cuáles están activas y una instantánea de cómo protegen su red.

Subscripción	Descripción
Threat Prevention	Threat Prevention defiende su red contra amenazas de materias primas, que son generalizadas pero no sofisticadas, y amenazas avanzadas dirigidas perpetuadas por ciberadversarios organizados.
Filtrado de URL	Advanced URL Filtering es nuestra completa solución de filtrado de URL que protege su red y a los usuarios de amenazas basadas en la web.
WildFire	El servicio de análisis de malware WildFire entregado en la nube utiliza datos e inteligencia de amenazas de la comunidad global más grande del sector, y aplica análisis avanzados para identificar automáticamente amenazas desconocidas y detener a los atacantes.
DNS Security	Asegura automáticamente su tráfico DNS utilizando el servicio Palo Alto Networks DNS Security.

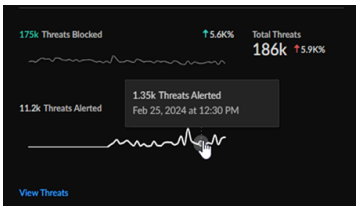


Al hacer clic en el widget **Security Subscriptions (Suscripciones de seguridad) [Command Center (Centro de control) > View Security Subscriptions (Ver suscripciones de seguridad)]**, obtendrá un informe detallado del estado de sus suscripciones en relación con sus implementaciones de NGFW y Prisma Access. Haga clic en **Back to the Dashboard (Volver al panel)** para volver a la vista **Threats (Amenazas)**.



Recuento total de amenazas

El widget **Total Threats Count (Recuento total de amenazas)** le ofrece una vista rápida del número total de amenazas detectadas en su red, cuántas amenazas se han bloqueado, cuántas amenazas se han alertado y el cambio en las amenazas de un rango de tiempo seleccionado.



Haga clic en Activities Insights **[Insights > Activity Insights > Threats (Amenazas)]** para obtener un desglose más detallado de las amenazas en su red.

Amenazas bloqueadas y alertadas

El widget **Amenazas bloqueadas y alertadas** le ofrece una vista de arriba hacia abajo de las amenazas que se detectan en su red, organizándolas por categoría, nivel de amenaza (crítico, alto, medio y bajo) y si las amenazas se han bloqueado o alertado.

Haga clic aquí para obtener una tabla más detallada de todas las amenazas que afectan a su red **[Insights > Activity Insights > Threats (Amenazas)]**.

Estado operativo

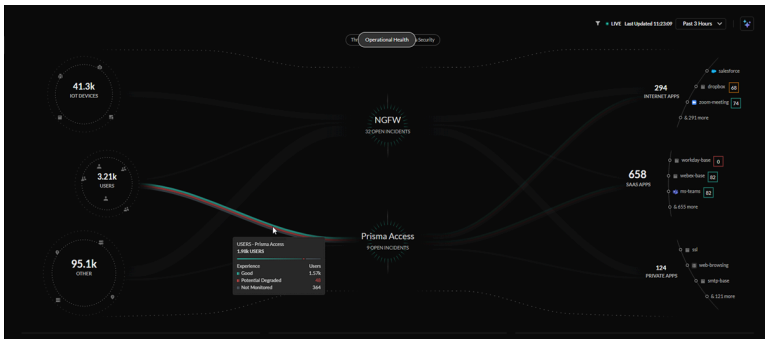
La vista **Estado operativo** muestra el estado de la infraestructura y la experiencia del usuario en su red. Puede usar esta vista para supervisar el estado de sus implementaciones de NGFW y Prisma Access, así como la experiencia del usuario en su red y revisar la gravedad de los incidentes abiertos en cada área.

Licencias de estado operativo	• Supervisión de suscripciones, incluyendo: ❑ Observabilidad de ADEM ❑ ADEM basado en IA ❑ IAOps para NGFW premium

Vista central del estado operativo

La vista central de estado operativo proporciona una visión del estado de la infraestructura y de la experiencia del usuario en su red. Si los usuarios tienen una licencia de la Gestión de la experiencia digital autónoma (ADEM), recibirán datos mejorados en esta vista.

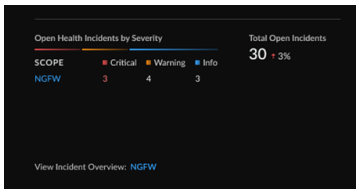
La vista Estado operativo mostrará cómo su suscripción a Palo Alto Networks ADEM supervisa la experiencia digital en todos los usuarios y aplicaciones de su entorno SASE.



Las líneas de la vista central de estado operativo representan a todos los usuarios de la red. Los usuarios están organizados por puntuación de experiencia del usuario, con los colores de las líneas representando una clasificación de buena, deficiente o no supervisada.

Número total de incidentes abiertos e incidentes por gravedad

El widget **Open Health Incidents by Severity (Abrir incidentes de estado por gravedad)** le ofrece una vista de todos los incidentes abiertos en su red, desglosados por alcance (NGFW, Prisma Access y Prisma SD-WAN), gravedad y número de incidentes.



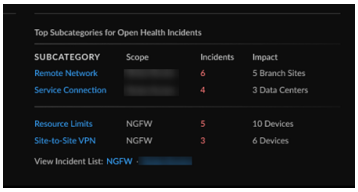
El widget rastrea el cambio porcentual en incidentes abiertos en función del período de tiempo seleccionado.

Haga clic en el panel **Incidents and Alerts (Incidentes y alertas)** para cada ámbito disponible **[Incidents and Alerts (Incidentes y alertas) > Prisma Access / NGFW > All Incidents (Todos los incidentes)]**.

Principales subcategorías de incidentes de estado abiertos

El widget **Top Subcategories for Open Health Incidents (Subcategorías principales para incidentes de estado abiertos)** le ofrece una vista de las subcategorías principales de los incidentes de estado abiertos en su red, organizadas por alcance, subcategoría, número de incidentes y lo que se ve afectado (centros de datos, sitios, dispositivos, etc.).

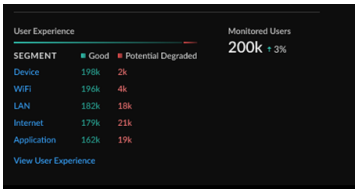
El widget mostrará las cinco subcategorías principales para un único alcance, o las dos subcategorías principales para varios alcances cuando estén disponibles.



Haga clic en el panel **Incidents and Alerts (Incidentes y alertas) [Incidents and Alerts (Incidentes y alertas) > Prisma Access / NGFW / Prisma SD-WAN)** para obtener más detalles sobre los incidentes.

Usuarios supervisados y experiencia de usuario

El widget **Open Incidents and User Experience (Incidentes abiertos y experiencia del usuario)** le ofrece una visión del recuento total de incidentes abiertos; el desglose de la experiencia del usuario, buena y potencialmente degradada, a partir de segmentos individuales de la cadena de prestación de servicios desde un dispositivo de usuario a una aplicación, y el cambio en los incidentes abiertos de un intervalo de tiempo seleccionado.



Haga clic en el panel de **Application Experience (Experiencia de aplicación) [Dashboards (Paneles) > Application Experience (Experiencia de aplicación)]** para obtener un desglose más detallado de la experiencia en su red y las métricas de rendimiento.

Prácticas recomendadas

Seguridad de datos

La vista **Data Security (Seguridad de datos)** muestra todos los datos confidenciales detectados en su red y varias aplicaciones SaaS conectadas. Puede usar esto para supervisar e identificar flujos de datos sensibles a riesgos elevados en su organización.

Licencias de seguridad de datos	• Licencias de seguridad de datos, incluidos: ❑ Licencia de seguridad SaaS ❑ Licencia de seguridad ❑ Licencia DLP Enterprise

Vista central de la seguridad de datos

La vista central de seguridad de datos proporciona el mapa de datos sensible y de alto riesgo en toda su red y aplicaciones SaaS conectadas. El centro de control le proporciona información sobre los usuarios de datos confidenciales de la organización, las aplicaciones específicas autorizadas, no autorizadas, toleradas o no etiquetadas en las que se detecta actividad de datos confidenciales (carga, descarga o exposición de activos), así como el número de activos permitidos, bloqueados, puestos en cuarentena, revocados o expuestos.

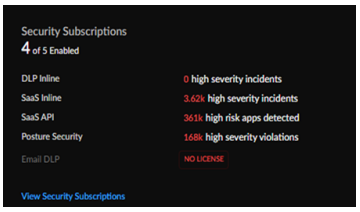
Las líneas de la vista central de Seguridad de datos representan los datos sensibles que se detectan a través de soluciones de seguridad de datos en reposo y datos en movimiento, y el grosor de las líneas representa la cantidad de datos y el color representa si esos datos se han marcado o clasificado como críticos, de alto, medio o bajo riesgo.

Suscripciones de seguridad:

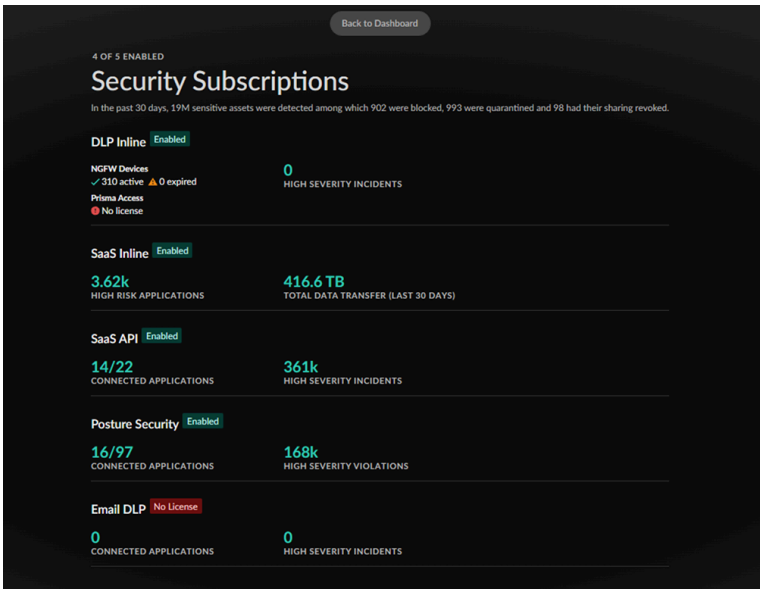
El widget **Security Subscriptions (Suscripciones de seguridad)** le ofrece una vista de las suscripciones de seguridad de datos, cuáles están activas y una instantánea de cómo protegen su red.

Suscripción	Descripción
DLP en línea	Enterprise DLP es un servicio basado en la nube que utiliza algoritmos de aprendizaje automático supervisados para clasificar documentos confidenciales en categorías,

Suscripción	Descripción
	para protegerse contra exposiciones, pérdida de datos y exfiltración de datos.
SaaS en línea	La solución SaaS en línea trabaja con Strata Logging Service para descubrir todas las aplicaciones SaaS que se están utilizando en su red.
SaaS API	SaaS API es un servicio basado en la nube que puede conectarse directamente a sus aplicaciones SaaS autorizadas mediante la API de la aplicación en la nube y proporcionar clasificación de datos, visibilidad de permisos o uso compartido y detección de amenazas dentro de la aplicación.
Seguridad de postura	SaaS Security Posture Management (SSPM) ayuda a detectar y remediar ajustes mal configurados en aplicaciones SaaS autorizadas a través de una supervisión continua.
Email DLP	Email DLP es un complemento de Enterprise DLP que evita la exfiltración de correos electrónicos que contienen información confidencial con detecciones de datos impulsadas por IA/ML.

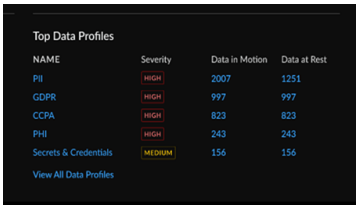


Al hacer clic en el widget **Security Subscriptions (Suscripciones de seguridad) [Command Center (Centro de control) > View Security Subscriptions (Ver suscripciones de seguridad)]**, obtendrá un informe detallado del estado de sus suscripciones en relación con sus implementaciones de NGFW y Prisma Access. Haga clic en **Back to the Dashboard (Volver al panel)** para volver a la vista **Data Security (Seguridad de datos)**.



Principales perfiles de datos

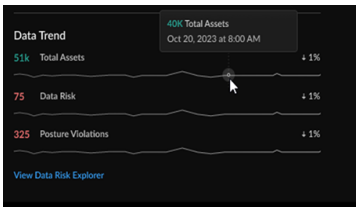
El widget **Top Data Profiles (Principales perfiles de datos)** muestra los perfiles de datos más importantes detectados en todos los datos confidenciales inspeccionados, la gravedad del perfil de datos y el número de coincidencias de activos detectadas en línea con los datos en movimiento frente a los datos en reposo.



Haga clic en el panel de **Data Loss Prevention (Prevención de pérdida de datos) [Manage (Gestionar) > Configuration (Configuración) > Data Loss Prevention (Prevención de pérdida de datos)]** para revisar todos los perfiles de datos predefinidos y añadir perfiles de datos personalizados.

Tendencia de datos

El widget **Data Trend (Tendencia de datos)** muestra la tendencia de los datos confidenciales supervisados por sus suscripciones de seguridad de datos, organizada por el cambio porcentual en los activos totales, los riesgos de datos y las violaciones de postura.



Haga clic en el panel **Data Risk (Riesgo de datos) [Manage (Gestionar) > Configuration (Configuración) > Data Loss Prevention (Prevención de pérdida de datos) > Data Risk (Riesgo de**

datos)] para comprender su puntuación general de riesgo de datos y revisar las recomendaciones procesables para mejorar la postura de seguridad de los datos de su organización.

Insights: Activity Insights

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software • Prisma SD-WAN	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Prisma SD-WAN ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro Las otras licencias y requisitos previos necesarios para acceder a ciertas vistas de Activity Insights son: ☐ Strata Logging Service ☐ Servicios de seguridad en la nube (CDSS) ☐ Observabilidad de ADEM ☐ Informes de WAN Clarity ☐ Un rol que tiene permiso para ver el panel → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Activity Insights le ofrece una visión en profundidad de las actividades de su red en implementaciones de Prisma Access y NGFW. Esta vista unifica los datos de red, como el tráfico de red, el uso de aplicaciones, las amenazas y las actividades de los usuarios en un solo lugar. Activity Insights le proporciona funciones de visualización, supervisión y generación de informes para que pueda llevar a cabo sus tareas fácilmente. Una vez que haya identificado las áreas que necesitan su enfoque con el Centro de control de Strata Cloud Manager, utilice los vínculos de contexto para navegar a Activity Insights u otros paneles para un análisis adicional.

Activity Insights cuenta con filtros avanzados para ayudarle a centrarse en los aspectos de seguridad que importan para su implementación. La funcionalidad avanzada de informes de Activity Insights le permite descargar, compartir y programar informes a partir de los datos de la pestaña Descripción general. El informe presenta los datos por separado para cada filtro aplicado en el panel. Alternativamente, puede programar informes para Activity Insights y paneles de control desde el menú de **Reports (Informes)** de **Strata Cloud Manager**.

Inicie Strata Cloud Manager y haga clic en **Insights** () para comenzar.

¿Qué le muestra Activity Insights?

Activity Insights muestra datos agregados por el inquilino de Strata Logging Service desplegados en entornos Prisma Access y NGFW. Puede filtrar los datos para una implementación específica. Activity Insights tiene diferentes pestañas. Cada una de estas pestañas proporciona una vista unificada de los datos de red en relación con las aplicaciones, los usuarios, las amenazas, las URL y el uso de la red.

- **Overview (Descripción general)**: muestra los datos de aplicaciones, amenazas, usuarios, URL y sesiones con el máximo número de actividades involucradas dentro del rango de tiempo seleccionado. Eche un vistazo a esta vista para identificar rápidamente cualquier irregularidad dentro de su red y luego profundice más para examinar las actividades que requieren investigación.
- **Applications (Aplicaciones)**: visión general de todo el uso de aplicaciones en la red, incluida la transferencia de datos, los riesgos de las aplicaciones y las capacidades de ADEM para supervisar la experiencia de las aplicaciones.
- **SD-WAN Applications (Aplicaciones SD-WAN)**: vea el rendimiento de las aplicaciones Prisma SD-WAN con detalles sobre la puntuación de salud en un intervalo de tiempo, estadísticas de transacciones y métricas de utilización del ancho de banda.
- **Threats (Amenazas)**: proporciona una visión holística de todas las amenazas que los servicios de seguridad de Palo Alto Networks detectaron y bloquearon en su red.
- **Users (Usuarios)**: proporciona información más profunda sobre el tráfico y las actividades de un usuario, incluidas las capacidades de ADEM para supervisar la experiencia del usuario.
- **URL**: muestra las URL a las que se accede en su red, cuántas de ellas son maliciosas, los usuarios y aplicaciones que acceden a las URL, las reglas que permiten las URL en su red y la aplicación por sus servicios de seguridad.
- **Rules (Reglas)**: proporciona información sobre las reglas de política de seguridad que permiten el tráfico generado por los usuarios y las aplicaciones, las amenazas detectadas en las sesiones de tráfico y las URL que afectan a la regla.
- **Regions (Regiones)**: muestra los detalles del tráfico de red en relación con aplicaciones, usuarios, amenazas y las URL.

¿Cómo puede utilizar los datos del panel?

Encontrar aquí puede ayudarle-

- Identifique las aplicaciones que desea supervisar, mejore la experiencia de usuario de las aplicaciones con puntuaciones bajas y controle las aplicaciones no autorizadas y peligrosas.
- Vea las amenazas más relevantes para su implementación y obtenga contexto sobre las amenazas para la investigación.
- Ajuste las reglas de la política seguridad y las reglas de tráfico en función de los resultados de los logs para cerrar las brechas de seguridad.
- Supervise la actividad del usuario para detectar y detener amenazas potenciales y proteger el uso indebido de información confidencial.

Activity Insights: Descripción general

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software • Prisma SD-WAN	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Prisma SD-WAN ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro Las otras licencias y requisitos previos necesarios para acceder a ciertas vistas de Activity Insights son: ☐ Strata Logging Service ☐ Servicios de seguridad en la nube (CDSS) ☐ Observabilidad de ADEM ☐ Informes de WAN Clarity ☐ Un rol que tiene permiso para ver el panel → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Vea el resumen de las aplicaciones, amenazas, usuarios, URL y reglas más vistos en su red durante el período de tiempo seleccionado. Eche un vistazo a esta vista para identificar rápidamente cualquier irregularidad dentro de su red y luego profundice más para examinar la actividad que requiere investigación. La vista general incluye:

- Top 5 aplicaciones y categorías de aplicaciones en su red que tienen la máxima actividad en términos de número de sesiones, transferencia de datos, amenazas detectadas, URL a las que se accede y usuarios que accedieron a las aplicaciones. Haga clic en **Ver todas las aplicaciones** para consultar los detalles de aplicación.

- Las 5 principales amenazas y categorías de amenazas que más afectan a las sesiones, usuarios y aplicaciones. Vea los detalles de las sesiones, los usuarios y las aplicaciones en las pestañas Visor de logs, Usuarios y Aplicaciones, respectivamente.

- Tendencia del tráfico de red de sesiones bloqueadas, permitidas y alertadas, la cantidad de datos transferidos y los usuarios que generan más tráfico.

- Top 5 de los usuarios con más sesiones de tráfico, datos transferidos, amenazas encontradas en el tráfico, URL accedidas y las puntuaciones de experiencia de usuario para aplicaciones supervisadas.
- URL a las que más se accede junto con detalles sobre la sesión, los usuarios y las aplicaciones que acceden a las URL.

- Las 5 reglas de política de seguridad más afectadas configuradas en su implementación con filtros para conocer las sesiones, usuarios, URL, amenazas, datos transferidos, aplicaciones involucradas en el tráfico que coinciden con las reglas.

Puede usar los filtros para ver los puntos de datos en los que desea centrarse y que son relevantes para su implementación. Estos filtros están disponibles en todas las pestañas del panel.

Filtros

Activity Insights cuenta con filtros avanzados para ayudarle a centrarse en los aspectos de seguridad que importan para su implementación. Los filtros disponibles son:

- **Time Range (Rango de tiempo)**: vea datos para un período de tiempo especificado
- **Scope Selection (Selección de alcance)**: datos específicos de una implementación: Prisma Access, NGFW
- **Subtenant (Subinquilino)**: la instancia de Prisma Access para la que se muestran los datos
- **User Name (Nombre de usuario)**: ver actividades relacionadas con un usuario individual
- **Application (Aplicación)**: eventos de red relativos a una aplicación específica
- **Application Type (Tipo de aplicación)**: tipo de aplicación; SaaS, internet, privada
- **Threat Category (Categoría de amenaza)**: datos de una categoría particular de amenaza
- **Threat Action (Acción de amenazas)**: vista específica de amenazas permitidas o bloqueadas
- **URL Risk Level (Nivel de riesgo de URL)**: datos relativos a las URL con nivel de riesgo específico; alto, medio o bajo
- **URL Category (Categoría de URL)**: filtra los datos en función de las categorías URL
- **Source Location (Ubicación de origen)**: ve la actividad que se originó en una ubicación específica
- **Destination Location (Ubicación de destino)**: vea la actividad dirigida a una región específica
- **URL**: actividad relacionada con una URL específica a la que se accede.
- **SaaS Application (Aplicación SaaS)**: datos relativos a una aplicación SaaS específica
- **Sanctioned Application (Aplicación sancionada)**: ver datos solo para aplicaciones autorizadas o no autorizadas

- **Port Type (Tipo de puerto)**: ordene el tráfico de aplicaciones que atraviesan puertos estándar o no estándar.
- **Protocol (Protocolo)**: vea el tráfico que utiliza un puerto TCP, UDP o HTTP específico
- **Source Type (Tipo de fuente)**: vea actividad generada desde un dispositivo particular, usuarios u otros.

Informes

Haga clic en uno de los iconos,  en la pestaña **Overview (Visión general)** para descargar, compartir y programar informes a partir de los datos de la pestaña **Overview (Visión general)**. También puede programar informes desde el menú de **Reports (Informes)** de **Strata Cloud Manager**; haga clic en el icono de y seleccione Activity Insights- Resumen en el menú desplegable **Type (Tipo)**.

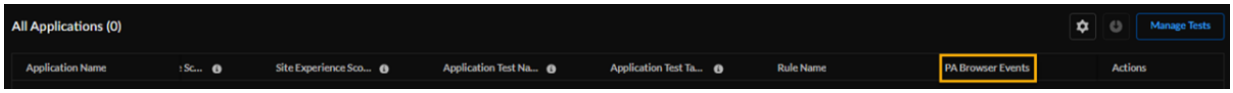
Activity Insights: Aplicaciones

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)* • Cortafuegos NGFW *(con gestión de la configuración de Strata Cloud Manager o Panorama)*	Debe tener al menos una de estas licencias para usar Activity Insights: ❑ Prisma Access ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) o AIOps for NGFW Premium license (use the Strata Cloud Manager app) Las otras licencias necesarias para ver la pestaña Activity Insights: Applications son: ❑ Strata Logging Service ❑ ADEM Observability desbloqueará funciones adicionales de Prisma Access

Supervise las aplicaciones en sus configuraciones de Prisma Access y NGFW, los usuarios que utilizan la aplicación, las puntuaciones de riesgo, la experiencia de usuario para cada aplicación y comprenda el impacto en la seguridad que representan las aplicaciones peligrosas. Los hallazgos sobre el uso de aplicaciones pueden ayudarle a perfeccionar su política de seguridad para controlar aplicaciones no autorizadas y peligrosas. Haga clic en **Activity Insights > Applications (Aplicaciones)** para ver la siguiente información:

- **Aplicaciones por puntuación de riesgo**: el número total de aplicaciones que se ejecutan en su organización y el número de aplicaciones que se consideran Bien, Regular y Deficiente. Las aplicaciones se clasifican como buenas, regulares y deficientes según las puntuaciones de experiencia de aplicación.
- **Application Data Transfer (Transferencia de datos de aplicación)**: descarga total de datos y carga en cortafuegos NGFW y Prisma Access durante el intervalo de tiempo seleccionado. Puede filtrar para ver la transferencia de datos que se origina en la categoría de aplicación y fluye a través del destino desde el dispositivo (centro de datos o Cortafuegos).
- **All Applications (Todas las aplicaciones)**: utilice este widget para ver qué aplicaciones de Prisma Access se supervisan con pruebas sintéticas que se ejecutan en ellas y aplicaciones que se ejecutan en sus entornos de NGFW. La tabla también muestra sus puntuaciones de experiencia, que le dan el estado de cada aplicación. Si tiene una suscripción a Prisma Access

Browser, verá una columna para **PA Browser Events (Eventos de PA Browser)**. Seleccione el número de eventos y le redirigirá a las páginas de gestión de Prisma Access Browser.



Puede descargar los datos de la tabla en formato csv (solo aplicaciones Prisma Access). Haga clic en el botón **Gestionar pruebas** para ver todas las pruebas sintéticas que están configuradas para todas las aplicaciones de Prisma Access en la tabla Pruebas de aplicaciones. Si desea crear una prueba para supervisar una aplicación, haga clic en **Supervisar la aplicación para ver el estado** en la columna Experiencia del usuario.

- **Application Details (Detalles de aplicación)**: vea detalles generales de la aplicación junto con detalles sobre la actividad de la aplicación y la experiencia de la aplicación.
  - La pestaña **Activity (Actividad)** muestra el número total de amenazas observadas en la aplicación, el total de usuarios que acceden a la aplicación, los datos transferidos a través de la aplicación, los eventos de datos del navegador de PA y los eventos de acceso al Prisma Access Browser.

    La siguiente imagen muestra los detalles de aplicación sobre los **PA Browser Data Events (Eventos de datos de PA Browser)** y **PA Browser Data Events (Eventos de datos de PA Browser)**. La vista predeterminada muestra un **Aggregate (Agregado)** de todos los eventos y eventos bloqueados, o puede elegir ver un **Breakdown (Desglose)** por **Event Type (Tipo de evento)** y **Count (Recuento)**.

  - La pestaña **Experience (Experiencia)** muestra la puntuación de experiencia de la aplicación, la tendencia de puntuación durante el intervalo de tiempo seleccionado y las métricas de rendimiento de la red.

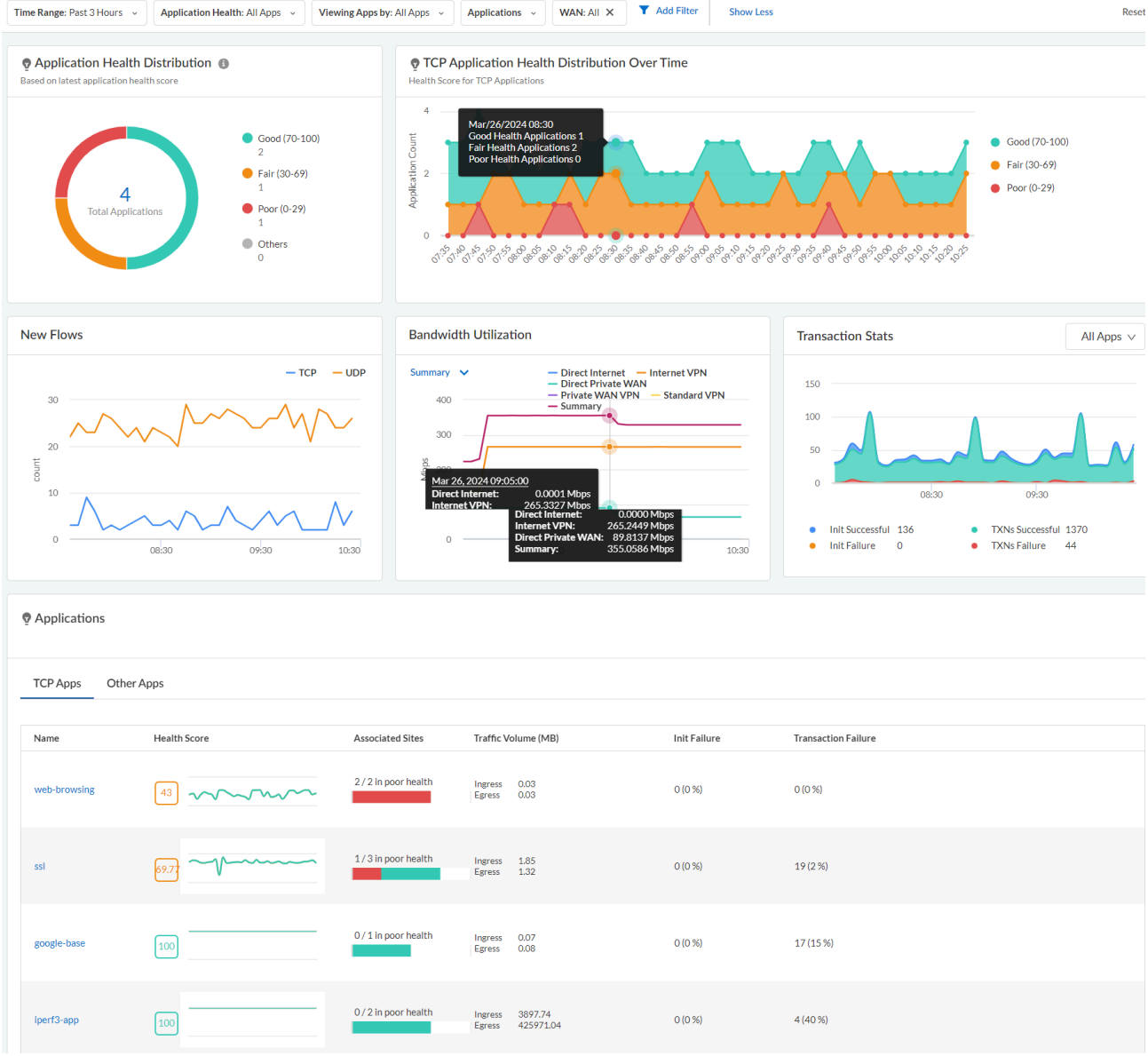
Si una aplicación es una aplicación contenedora, las estadísticas que se muestran son un resumen de todas las aplicaciones en el contenedor. Por ejemplo, gmail es una aplicación contenedora (no hay App-ID para gmail). Agrupa aplicaciones como gmail-posting, gmail-downloading, gmail-uploading, etc. La puntuación de riesgo establecida para esta aplicación contenedora es la puntuación de riesgo más alta encontrada para las aplicaciones contenidas. Todas las demás métricas se calculan sumando los valores encontrados para las aplicaciones contenidas.

Informes: no puede generar un informe que cubra los datos de esta vista. Sin embargo, puede usar el informe de **uso de aplicaciones** para ver los datos de uso de aplicaciones en su red. Para programar un informe, en el menú **Strata Cloud Manager** > **Reports (Informes)**, haga clic en el icono de y seleccione Uso de la aplicación en el menú desplegable **Type (Tipo)**.

Activity Insights: Aplicaciones SD-WAN

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma SD-WAN	❑ Licencia de Prisma SD-WAN ❑ Licencia de WAN Clarity Reporting para ver ciertos widgets

Vea las principales aplicaciones que no están funcionando bien en Prisma SD-WAN. Consulte la puntuación de estado determinada de todas las solicitudes deficientes, la lista de solicitudes deficientes para un inquilino basada en la puntuación de estado y la puntuación de estado promedio de las solicitudes deficientes en las últimas 3 horas en intervalos de 5 minutos.



- **Distribución del estado de la aplicación** (requiere licencia WAN Clarity): La distribución de solicitudes, Buena, Regular y Deficiente, para un inquilino específico.
- **Distribución del estado de la aplicación TCP a lo largo del tiempo** (requiere licencia WAN Clarity): La distribución del estado de las aplicaciones TCP, Buena, Regular y Deficiente durante un período de tiempo. El gráfico de serie temporal debe calcularse y actualizarse en función de la duración seleccionada. Por ejemplo, las duraciones admitidas son una hora, tres horas, 1 día, siete días, 30 días y 90 días y el intervalo es de un minuto, cinco minutos, una hora y un día, respectivamente.
- **Nuevos flujos**: Muestra los nuevos flujos TCP y UDP para una aplicación, un conjunto específico de aplicaciones o todas las aplicaciones durante un período determinado. Un flujo TCP se considera un flujo nuevo cuando ve el primer paquete SYN. Un flujo UDP se considera un flujo nuevo cuando ve el primer paquete UDP en cualquier dirección. Un flujo es una secuencia de paquetes en ambas direcciones identificados por la IP de origen y destino, el puerto de origen y destino y el protocolo.
- **Utilización del ancho de banda**: El gráfico de utilización del ancho de banda muestra la cantidad de ancho de banda utilizado en un rastro en una red. Utilice el gráfico para identificar la congestión WAN en una red que puede obstaculizar el rendimiento de la aplicación. Es una representación visual del pico de ancho de banda, el ancho de banda total consumido por un sitio en particular y la aplicación; si la carga está en la dirección de entrada o salida. Mueva el cursor en el gráfico de utilización del ancho de banda para obtener una vista más detallada de la utilización del ancho de banda con una aplicación o sello de tiempo. Normalmente, las aplicaciones se enumeran en orden de utilización del ancho de banda.
- **Estadísticas de transacción**: Proporciona estadísticas de transacciones sobre flujos TCP, incluidas acciones correctas y fallidas de iniciación/transacción para una aplicación específica o todas las aplicaciones, una ruta particular o todas las rutas y todos los eventos de estado.
- **Aplicaciones**: Enumera todos los detalles de las aplicaciones, como el nombre, el perfil de la aplicación, la puntuación de estado, los sitios afectados, el volumen de tráfico, el inicio/fallo y la transacción/fallo. Cuando haga clic en el nombre de la aplicación, podrá ver los detalles individuales de la aplicación en una nueva página.

Activity Insights: Threats (Amenazas)

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)* • Cortafuegos NGFW *(con gestión de la configuración de Strata Cloud Manager o Panorama)*	Debe tener al menos una de estas licencias para usar Activity Insights: ❑ Prisma Access ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) o AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro Las otras licencias necesarias para ver la pestaña Activity Insights:Amenazas son: ❑ Strata Logging Service ❑ Licencias CDSS ❑ ADEM Observability desbloqueará características adicionales de Prisma Access

Obtenga una visión holística de la actividad de amenazas y de los distintos tipos de amenazas que se observan en su red. La pestaña muestra el número total de sesiones de amenazas observadas en sus implementaciones de Prisma Access y NGFW, el desglose de los números según la categoría de amenaza y la gravedad de la amenaza durante el período de tiempo seleccionado. Puede buscar en un artefacto de seguridad (hash de archivo, una dirección URL, un dominio o una dirección IP (IPv4 o IPv6) asociada a una amenaza para conocer el análisis de inteligencia de amenazas de Palo Alto Networks y los resultados del análisis de terceros.

Revise los siguientes detalles de las amenazas únicas en su red:

- **Threat Name (Nombre de amenaza)**. nombre de la firma de la amenaza. Úsalo para encontrar la información más reciente de las amenazas en la Bóveda de amenazas, incluidas todas las sesiones de amenaza durante un intervalo de tiempo.
- **Threat ID (ID de amenaza)**: ID de firma de amenaza único. Utilice el ID de amenaza para buscar la información más reciente que la base de datos de amenazas de Palo Alto Networks tiene para esta firma.
- **Threat Category and Subcategory (Categoría y subcategoría de amenazas)**: el tipo de amenazas basado en firmas de amenazas (antivirus, spyware (C2) y vulnerabilidades).
- **Licenses (Licencias)**: los Servicios de seguridad de Palo Alto Networks que detectaron la amenaza.

- **Severity (Gravedad)**: la gravedad de la amenaza se determina en función de la facilidad con la que se explota la vulnerabilidad, el impacto en la vulnerabilidad, la omnipresencia del producto vulnerable, el impacto de la vulnerabilidad, etc. Las gravedades se clasifican como:
  - Crítica: cuando la vulnerabilidad afecta a las instalaciones predeterminadas de software implementado muy ampliamente y las vulnerabilidades pueden hacer que la raíz esté en riesgo. El código de exploit (información sobre cómo vulnerar el código del sistema, los métodos, la prueba de concepto (POC)) está ampliamente disponible y es fácil de aprovechar. El atacante no necesita ninguna credencial de autenticación especial ni conocimientos sobre las víctimas individuales.
  - Alta: amenazas que tienen la habilidad de convertirse en críticas pero que tienen factores atenuantes; por ejemplo, pueden ser difíciles de explotar, no conceder privilegios elevados o no tener un gran grupo de víctimas.
  - Media: amenazas menores en las que se minimiza el impacto, como ataques DoS que no comprometen al objetivo o vulnerabilidades que requieren que el atacante esté en la misma LAN que la víctima, afectan solo a configuraciones no estándar o aplicaciones oscuras u ofrecen acceso muy limitado.
  - Baja: amenazas con nivel de advertencia baja que tienen muy poco impacto en la infraestructura de la organización. Suelen requerir acceso local o físico al sistema y con frecuencia suelen ocasionar problemas en la privacidad de las víctimas, problemas de DoS y fugas de información.
  - Informativa: eventos sospechosos que no suponen una amenaza inmediata, pero que se registran para indicar que podría haber problemas más serios.
- **Total Sessions (Número total de sesiones)**: el número de sesiones en las que se ha detectado la amenaza. Haga clic en el nombre de la amenaza para ver todas las sesiones de amenazas relacionadas en el intervalo de tiempo especificado. La tabla de sesión de amenazas proporciona contexto sobre la amenaza, como la hora en que los servicios de seguridad de Palo Alto Network detectaron las amenazas, los usuarios, las reglas, las aplicaciones, los dispositivos afectados por la amenaza y las acciones realizadas (permitidas o bloqueadas) sobre la amenaza.
- **Total Users (Total de usuarios)**: número de usuarios expuestos a la amenaza.
- **Allowed Threats and Blocked Threats (Amenazas permitidas y amenazas bloqueadas)**: revise la acción aplicada a la amenaza para asegurarse de que las acciones no desencadenen falsos positivos en su red.
- **Actions (Acciones)**: investigue el historial de logs de la amenaza en el Visor de logs.

Informes: no puede generar informes que cubran los datos de esta vista.

Activity Insights: Usuarios

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)* • Cortafuegos NGFW *(con gestión de la configuración de Strata Cloud Manager o Panorama)*	Debe tener al menos una de estas licencias para usar Activity Insights: ❑ Prisma Access ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) o AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro Las otras licencias necesarias para ver la pestaña Activity Insights: La pestaña Usuarios son: ❑ Strata Logging Service ❑ Licencia de Advanced URL Filtering ❑ Licencia d Cloud Identity Engine ❑ Licencia de Advanced Threat Prevention ❑ ADEM Observability desbloqueará características adicionales de Prisma Access

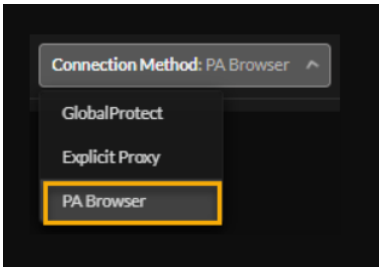
Supervise la actividad de los usuarios en sus entornos Prisma Access y NGFW. Puede ver los datos de los usuarios que se conectan a los servicios de seguridad de Prisma Access y NGFW a través de la aplicación GlobalProtect en sus dispositivos o a través del proxy explícito mediante un navegador web en sus dispositivos. Supervisar la actividad del usuario ayuda a detectar y detener amenazas potenciales, proteger el uso indebido de información confidencial y ajustar su regla de política de seguridad para cerrar las brechas de seguridad.

Puede filtrar los datos de usuario en función de:

- Implementación; Prisma Access, NGFW
- Métodos y versiones de conexión; GlobalProtect, Proxy explícito, Prisma Access Browser
- Nombre de usuario
- Nombre del dispositivo
- Ubicación de origen del tráfico y ubicaciones de Prisma Access
- Aplicaciones a las que acceden los usuarios y filtros de puntuación de experiencia del usuario

Vea los siguientes detalles aquí:

- **Usuarios conectados/activos**: supervise los datos agregados sobre su GlobalProtect, Usuarios móviles de proxy explícito y Prisma Access Browser conectados actualmente.



  Vea el número de usuarios conectados a su red en el momento en que se obtuvieron los datos o como se indica en la marca de tiempo. Puede **Ver tendencia por Usuarios** o por **Dispositivos de usuario**. Seleccione el número para ver la tabla **Connected Users | Connected User Devices (Usuarios conectados | Dispositivos de usuario conectados)** para obtener detalles sobre todos los usuarios conectados y todos sus dispositivos.

  Ver datos de acceso dinámico a privilegios en **Ver tendencia por usuarios** o por **dispositivos de usuario**, **Connected Users | Connected User Devices (Usuarios conectados | dispositivos de usuario conectados)** y **Project Distribution by Theater (Distribución de proyectos por teatro)**.
- **Usuarios supervisados**: vea el número total de usuarios o dispositivos de usuario supervisados por ADEM y su experiencia promedio de usuario, que es la puntuación de experiencia agregada en todos los usuarios supervisados en ADEM. Haga clic en el número para ver los detalles de la actividad del usuario en relación con la experiencia del usuario.
- **Usuarios peligrosos**: vea el número de usuarios afectados por amenazas. La flecha Arriba o Abajo compara este rango de tiempo con un rango de tiempo anterior para determinar la diferencia, en porcentaje, del número de dispositivos conectados. Seleccione Ver más detalles para las versiones de GlobalProtect o la utilización de grupo de IP para ver detalles sobre los usuarios de riesgo en su entorno.
- **Detalles de la versión de GlobalProtect** muestra las versiones de GlobalProtect instaladas en sus dispositivos. Puede ver cuántos usuarios se conectan con cada versión. Utilice los datos para hacer cumplir la última versión de la aplicación GlobalProtect. Pase el cursor sobre las líneas de tendencia de distribución para ver las direcciones IP de los usuarios conectados en ese momento.
- **Consulte la utilización del grupo de direcciones IP** por diferentes teatros de asignación de grupos IP según el número de usuarios conectados en ese momento. El porcentaje de utilización del grupo de direcciones IP en el gráfico es el número de bloques del grupo de direcciones IP utilizados de todos los bloques del grupo IP que están disponibles en todas las subredes. Puede tomar medidas proactivas añadiendo subredes cuando vea una barra de agrupación IP que se acerca a la capacidad máxima de cualquier región.
- La tabla **Usuarios** muestra información sobre los usuarios que iniciaron sesión durante el intervalo de tiempo. Haga clic en el nombre de usuario para obtener visibilidad de los patrones

de navegación de un usuario individual: sus sitios visitados con más frecuencia, los sitios con los que transfieren datos e intentos de acceder a sitios de alto riesgo.

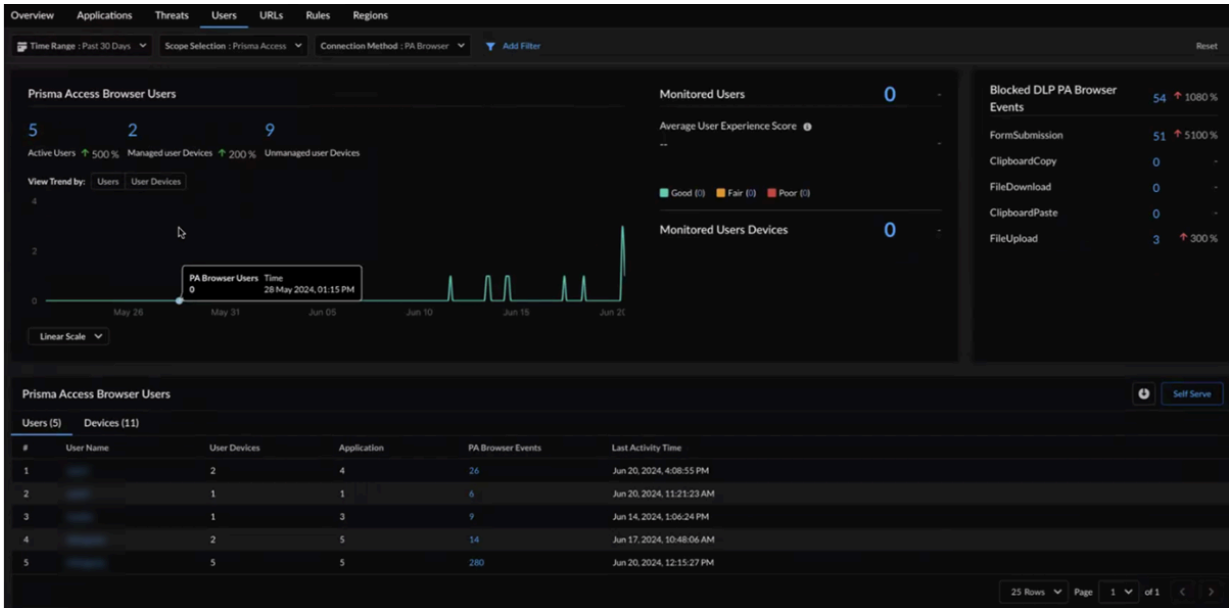
- **Threats (Amenazas)**
  - **Resumen de navegación**: vea los números de los tipos de sitios con los que el usuario tuvo la mayor transferencia de datos y el número de visitas al sitio por el usuario.
  - **10 principales categorías de URL más visitadas**: vea las principales categorías URL para el usuario en función de la transferencia de datos. También puede ver el número de URL únicas visitadas que pertenecen a cada categoría de URL.
  - **Resumen de navegación de URL**: fuera de las URL únicas visitadas por el usuario, tenga cuidado con las visitas a URL maliciosas y de alto riesgo: estos sitios pueden exponer su red a amenazas, pérdida de datos y violaciones de cumplimiento. Si ve más visitas a estos sitios de las que esperaba, ajuste la regla de la política de seguridad para cerrar las brechas.
  - **10 URL principales**: Revise el nivel de riesgo de los sitios visitados con más frecuencia por el usuario. Las URL de alto riesgo deben ser supervisadas ya que es probable que expongan su red a amenazas.
  - **URL bloqueadas por riesgo**: son las URL bloqueadas a las que el usuario intentó acceder con más frecuencia. Revise los logs de filtrado de URL y vea si necesita ajustar la regla de políticas de seguridad para cambiar la acción.
  - **Amenazas severas**: vea el número total de amenazas detectadas para el usuario y los números en función de la gravedad de las amenazas. Compare el número con otros usuarios. Ajuste la regla de la política de seguridad si los números son inusualmente altos.
  - **Principales amenazas graves**: estas son las amenazas detectadas con mayor frecuencia por el usuario.
- **Conectividad**: muestra la tendencia de los dispositivos en los que el usuario ha iniciado sesión durante un período de tiempo específico y los detalles de conexión del dispositivo para cada evento de inicio de sesión y cierre de sesión del usuario.
- **Experiencia** : proporciona los datos de experiencia del usuario para el dispositivo, la puntuación de experiencia y la tendencia para cada una de las aplicaciones supervisadas, y la métrica de rendimiento para el usuario supervisado y las aplicaciones para dispositivos individuales.

- Prisma Access Browser - Seleccione el **Prisma Access Browser Connection Method (Método de conexión de Prisma Access Browser)** para ver información sobre sus usuarios de Prisma Access Browser.

  El gráfico de tendencias de actividad de **Prisma Access Browser Users (Usuarios de Prisma Access Browser)** muestra el número de usuarios que han estado activos en algún momento del filtro de rango de tiempo seleccionado. El gráfico muestra el desglose de los dispositivos de estos usuarios activos instalados con un agente de conectividad Prisma Access (dispositivos gestionados) y sin ningún usuario agente (no gestionado).

  El Prisma Access Browser ofrece una visibilidad inigualable de las acciones de un usuario del navegador, indicando si las acciones del usuario en su dispositivo, con respecto a los activos de datos de la empresa, están permitidas o bloqueadas por la políticas DLP de la empresa. El widget **Blocked DLP PA Browser Events (Eventos del navegador de PA DLP bloqueados)**

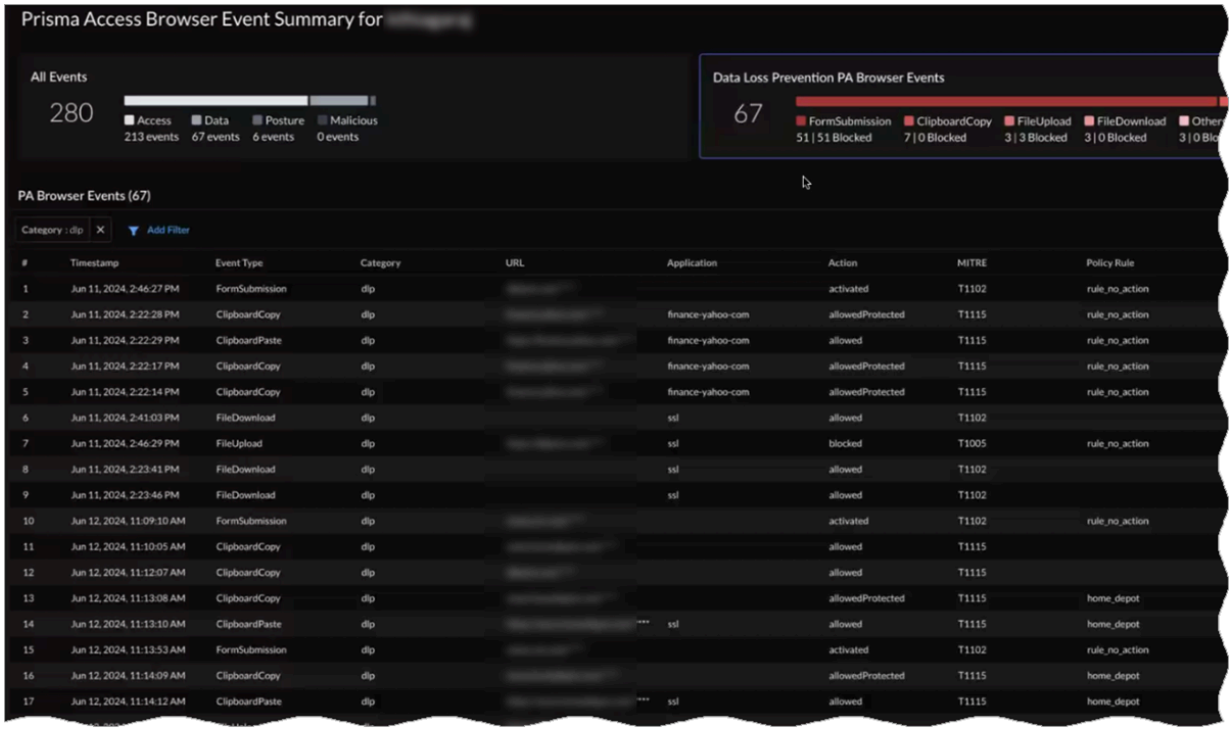
muestra los eventos que indican las acciones de usuario realizadas en el navegador que están bloqueadas por las políticas.



La tabla **Prisma Access Browser Users (Usuarios de Prisma Access Browser)** muestra la lista de usuarios activos que acceden a las aplicaciones a través del Prisma Access Browser. Haga clic en cualquier **User Name (Nombre de usuario)** para ver la **Activity (Actividad)** de dicho usuario en la página **User Details (Detalles de usuario)** > **Activity (Actividad)**.

La página **Resumen de eventos de Prisma Access Browser** enumera todas las acciones del navegador realizadas por el usuario a través del navegador en el intervalo de tiempo seleccionado. La vista predeterminada de la tabla **Eventos de PA Browser** muestra la lista de todos los **Eventos de Browser** de DLP permitidos o bloqueados por la políticas. Puede cambiar las vistas a otras categorías de eventos, como **Access Events (Eventos de acceso)**, **Posture Events (Eventos de posición)** o **Malicious Events (Eventos maliciosos)**, seleccionando la categoría de evento adecuada. En cada categoría de **Event (Evento)**, puede ver el desglose de los tipos de evento, junto con la marca de tiempo que muestra cuándo se realizó el evento

del navegador, información sobre la URL de la aplicación a la que se accede, el nombre de la aplicación y cualquier nota de ataque de MITRE asociada relevante.

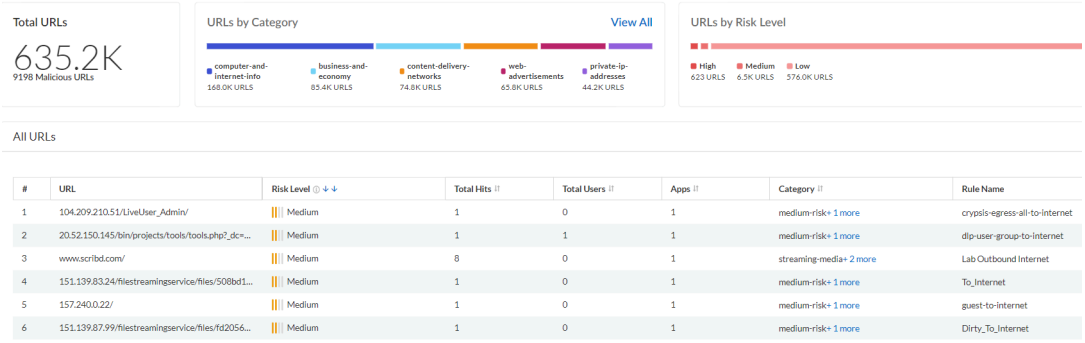


Informes: no puede generar un informe que cubra los datos de esta vista. Sin embargo, puede usar el informe Actividad del usuario para ver la actividad específica de un usuario en su red. Para programar un informe desde el menú **Strata Cloud Manager** > **Reports (Informes)**, haga clic en el icono de y seleccione Usuarios en el menú desplegable **Type (Tipo)**.

Activity Insights: URL

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)* • Cortafuegos NGFW *(con gestión de la configuración de Strata Cloud Manager o Panorama)*	Debe tener al menos una de estas licencias para usar Activity Insights: ❑ Prisma Access ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) o AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro Las otras licencias necesarias para ver la pestaña Activity Insights: Pestaña URL son: ❑ Strata Logging Service ❑ licencia de Advanced URL Filtering

Esta vista resume la actividad de URL en las implementaciones de Prisma Access y NGFW que detectó el servicio Advanced URL Filtering. Puede obtener visibilidad del número total de URL detectadas en su red durante el período de tiempo especificado, el desglose de estas URL por categoría de URL y nivel de riesgo. Utilice las opciones de filtrado para filtrar la vista en el panel.



Utilice los datos aquí para:

- Identificar las categorías de URL a las que más se accede, URL únicas con la categoría de URL, historial de URL en su red junto con hallazgos de análisis global. Según las URL maliciosas filtradas por el servicio de filtrado de URL, es probable que estas categorías de URL expongan su red a contenido malicioso y que se puede vulnerar. Es una práctica recomendada bloquear estas categorías de URL.
- Revise las URL de alto riesgo, su impacto en los usuarios, las aplicaciones y las reglas. No se confirma que los sitios de URL de alto riesgo sean maliciosos; sin embargo, pueden exponer su red a amenazas (un sitio que no es malicioso, pero está alojado por un ISP blindado, es un

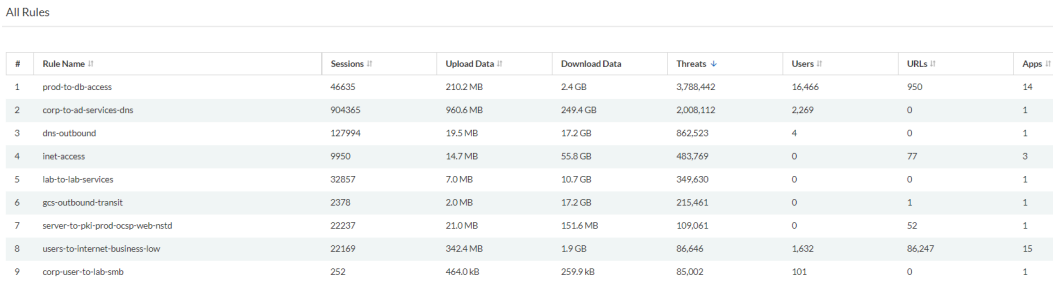
ejemplo de un sitio de alto riesgo). Considere dirigirse a estos sitios con normas de descifrado y políticas de seguridad estrictas.

Informes: no puede generar informes que cubran los datos de esta vista.

Activity Insights: Reglas

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)* • Cortafuegos NGFW *(con gestión de la configuración de Strata Cloud Manager o Panorama)*	Debe tener al menos una de estas licencias para usar Activity Insights: ❑ Prisma Access ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) o AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro Las otras licencias necesarias para ver la pestaña Activity Insights: Las pestañas de reglas son: ❑ Strata Logging Service

Vea las reglas de política de seguridad que coinciden con todo el tráfico de la red. Las reglas de política de seguridad determina si una sesión se bloqueará o se permitirá basándose en atributos del tráfico, como la dirección IP de origen y destino, la aplicación, el usuario y el servicio. Todo el tráfico que pasa por su red se compara con una sesión y cada sesión con una regla de la política de seguridad. Cuando se produce una coincidencia de sesión, se aplica la regla de política de seguridad.


All Rules

#	Rule Name	Sessions	Upload Data	Download Data	Threats	Users	URLs	Apps
1	prod-to-db-access	46635	210.2 MB	2.4 GB	3,788,442	16,466	950	14
2	corp-to-ad-services-dns	904365	960.6 MB	249.4 GB	2,008,112	2,269	0	1
3	dns-outbound	127994	19.5 MB	17.2 GB	862,523	4	0	1
4	inet-access	9950	14.7 MB	55.8 GB	483,769	0	77	3
5	lab-to-lab-services	32857	7.0 MB	10.7 GB	349,630	0	0	1
6	gcs-outbound-transit	2378	2.0 MB	17.2 GB	215,461	0	1	1
7	server-to-pki-prod-ocsp-web-nstd	22237	21.0 MB	151.6 MB	109,061	0	52	1
8	users-to-internet-business-low	22169	342.4 MB	1.9 GB	86,646	1,632	86,247	15
9	corp-user-to-lab-smb	252	464.0 kB	259.9 kB	85,002	101	0	1

El panel muestra los siguientes detalles del evento de red que coincide con la regla de política de seguridad:

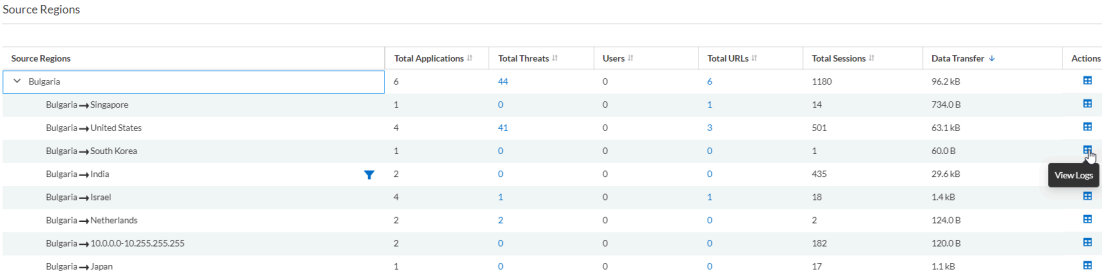
Sesiones de tráfico, datos transferidos, amenazas detectadas en las sesiones, usuarios afectados, URL visitadas y aplicaciones a las que se accede. Revise las reglas que más coincidan con las sesiones de tráfico, analice esas sesiones para comprender si la regla es demasiado permisiva y optimizar la regla si es necesario.

Informes: no puede generar informes que cubran los datos de esta vista.

Activity Insights: regions

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)* • Cortafuegos NGFW *(con gestión de la configuración de Strata Cloud Manager o Panorama)*	Debe tener al menos una de estas licencias para usar Activity Insights: ❑ Prisma Access ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) o AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro Las otras licencias necesarias para ver la pestaña Activity Insights: La pestaña Regiones son: ❑ Strata Logging Service

Estas son las regiones desde las que se originó el tráfico en su red. La vista proporciona información sobre amenazas, usuarios, URL, sesiones de red y transferencia de datos que se originan en estas ubicaciones. También puede profundizar para conocer la ubicación objetivo del tráfico. Haga clic en Acciones para ver los logs de tráfico para la sesión. Puede utilizar los datos para identificar y reducir las regiones que son objetivos de amenazas que intentan infiltrarse en su red. Optimice la regla que se aplica a las regiones seleccionadas.



Hay opciones de filtrado para reducir el tráfico hacia y desde una región de origen y destino específica. Las otras opciones de filtrado incluyen:

- tráfico visto en una implementación específica; Prisma Access, NGFW
- tráfico hacia y desde aplicaciones autorizadas o no autorizadas
- tráfico utilizando puerto y protocolos específicos
- tráfico que implica tipos específicos de amenazas, categoría de amenazas, URL y categoría de URL

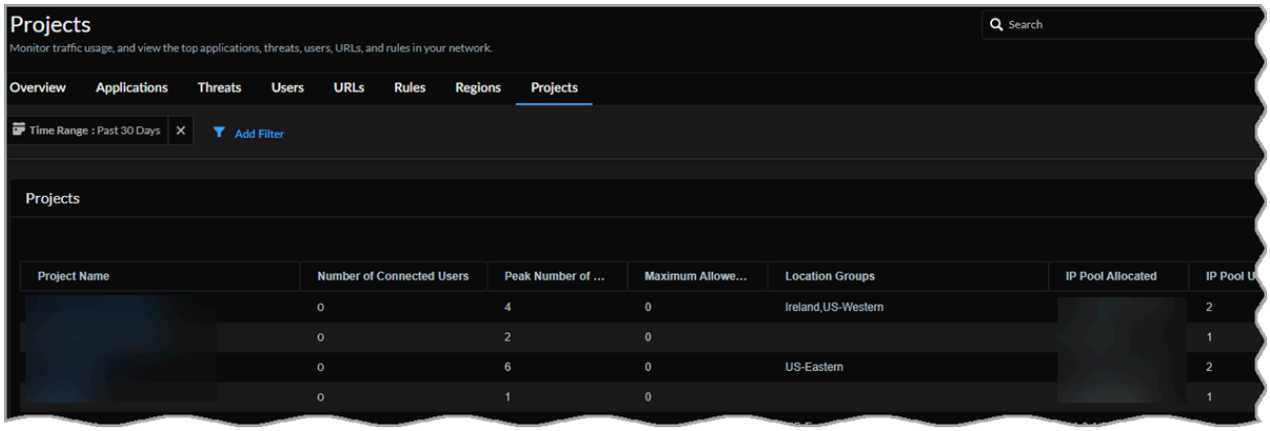
Informes: no puede generar informes que cubran los datos de esta vista. Sin embargo, puede utilizar el informe Uso de la red para conocer detalles sobre el tráfico de red. Para programar el

informe, en el menú **Strata Cloud Manager** > **Reports (Informes)**, haga clic en el icono de y seleccione Uso de red en el menú desplegable **Type (Tipo)**.

Activity Insights: Proyectos

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)* • Cortafuegos NGFW *(con gestión de la configuración de Strata Cloud Manager o Panorama)*	Debe tener al menos una de estas licencias para usar Activity Insights: ☐ Prisma Access ☐ AIOps for NGFW Free (use the AIOps for NGFW Free app) o AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro

Obtenga visibilidad de su implementación del agente de Prisma Access mediante el uso de Strata Cloud Manager para supervisar la actividad de su proyecto de Acceso dinámico a privilegios.



- La tabla **Projects (Proyectos)** proporciona una descripción general de los proyectos a los que acceden los usuarios de Dynamic Privilege Access mediante Prisma Access. Seleccione el nombre de cualquier proyecto para ver su página de detalles.
- La página de detalles del proyecto muestra:
  - **Overview (Visión general)**: vea el número máximo de usuarios permitidos y el número máximo de usuarios durante el intervalo de tiempo seleccionado para este proyecto.
  - **IP Pools Utilization (Utilización de grupos de IP)**: vea el número de direcciones IP en uso y el número de direcciones IP que aún están disponibles para los grupos de este proyecto.
  - **Connected Users (Usuarios conectados)**: vea un gráfico de los usuarios conectados durante el intervalo de tiempo seleccionado.
  - **Connected Users by Location Group (Usuarios conectados por grupo de ubicaciones)**: vea el número de usuarios según el grupo de ubicaciones de Prisma Access en el que se encuentran.

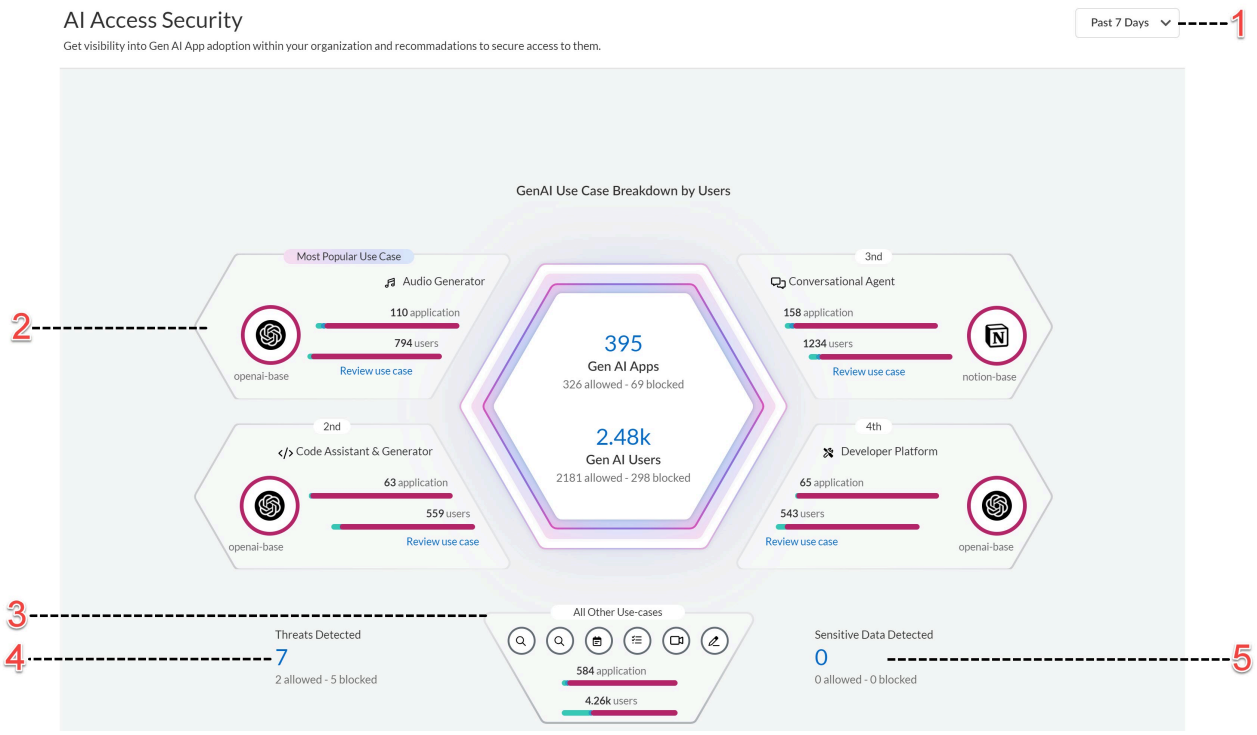
Insights: AI Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)* • Cortafuegos NGFW *(con gestión de la configuración de Strata Cloud Manager o Panorama)*	Una de las siguientes licencias: ❑ Licencia de AI Access Security ❑ Licencia CASB-PA ❑ Licencia CASB-X Para obtener más información sobre las licencias compatibles con AI Access Security, haga clic aquí.

Las aplicaciones de inteligencia artificial generativa (GenAI) son aplicaciones de IA capaces de generar texto, imágenes, vídeos y otras formas de datos en respuesta a las indicaciones del usuario, además de aprender continuamente en función de las entradas de datos del usuario. Su uso está proliferando a un ritmo asombroso y ofrece oportunidades ilimitadas para las empresas. Sin embargo, la naturaleza por la que las aplicaciones de GenAI mejoran de manera polémica presenta un nuevo peligro para las empresas y los administradores de seguridad: ¿cómo puede asegurarse de que sus empleados no expongan datos confidenciales o patentados a las aplicaciones de GenAI?

Palo Alto Networks presenta AI Access Security para habilitar la adopción segura de las aplicaciones de GenAI en toda la organización.

Utilice la función AI Access Security Insights para filtrar el uso de la aplicación GenAI en su red. El panel de información de AI Access Security proporciona detalles detallados para ayudarle a comprender qué aplicaciones de GenAI se están utilizando y quién las utiliza.



Para obtener más información sobre cómo proteger sus datos confidenciales de las aplicaciones de GenAI, haga clic aquí.

Insights: AI Runtime Security

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)* • Cortafuegos NGFW *(con gestión de la configuración de Strata Cloud Manager o Panorama)*	☐ Active su licencia de AI Runtime Security ☐ Requisitos previos de configuración de AI Runtime Security ☐ Incorporar y activar una cuenta en la nube en SCM

Palo Alto Networks AI Runtime Security es una solución de seguridad centralizada especialmente diseñada para proteger la arquitectura de red en la nube de su organización de ataques de red convencionales y específicos de IA aprovechando la seguridad en tiempo real impulsada por IA. Protege sus modelos de IA de nueva generación, aplicaciones de IA y conjuntos de datos de IA de amenazas de red como Inyecciones de mensajes en solicitudes, fuga de datos confidenciales, salida no segura (por ejemplo, malware y URL) y ataques DoS de modelos.

Utilice el panel AI Runtime Security Insights para comprender la superficie de ataque de su red en la nube y defender sus activos en la nube contra amenazas maliciosas.

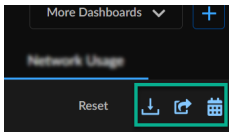
Para obtener más información sobre cómo proteger su flujo de tráfico de red de IA y no IA de posibles ataques, haga clic aquí.

Paneles: Strata Cloud Manager

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software • Prisma SD-WAN	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN Las otras licencias y requisitos previos necesarios para acceder a ciertos Paneles son: ❑ Servicios de seguridad en la nube (CDSS) ❑ Observabilidad ADEM ❑ Un rol que tiene permiso para ver el panel → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Strata Cloud Manager proporciona un conjunto de paneles interactivos que le brindan una vista completa de las aplicaciones, los dispositivos ION, las amenazas, los usuarios y las suscripciones de seguridad que funcionan en su red. Los paneles proporcionan visibilidad del estado, la postura de seguridad y la actividad que se produce en su implementación; lo que le ayuda a prevenir o abordar las deficiencias de rendimiento y seguridad en su red. La compatibilidad con el panel de control se extiende a través de los Productos y suscripciones de Palo Alto Networks compatibles con la gestión en la nube y también de otras fuentes, como Traps, Cortex XDR, Prisma SaaS y Proofpoint. Los datos que ve a menudo dependen de su suscripción. Puede revisar cada tema del panel para ver cuáles son los requisitos de licencia para ese panel, si los permisos de rol pueden afectar a los datos visibles y para obtener información sobre los diferentes tipos de datos que cada suscripción desbloquea.

Puede acceder a los paneles desde el menú **Dashboards (Paneles)** en el panel de navegación izquierdo. El panel de estado de SASE está anclado a la página de aterrizaje de forma predeterminada. Haga clic en **More Dashboards (Más paneles)** y active o desactive la casilla de verificación situada junto al nombre de un panel para anclar o desanclar el panel a la página de aterrizaje del panel. También puede crear su propio panel de control utilizando la opción **Crear mi panel de control**. Algunos de los paneles también tienen la opción de descargar y compartir informes que puede compartir sin conexión y programar actualizaciones periódicas. Para ver si Informes es compatible con un panel de control, compruebe estos iconos:



Integración con Cloud Identity Engine

Le recomendamos que configure Cloud Identity Engine (Directory Sync) para aprovechar al máximo los paneles. Cloud Identity Engine es una aplicación gratuita de Palo Alto Networks que otorga a otras aplicaciones acceso de solo lectura a su información de Active Directory y le permite:

- **Obtener datos de actividad del usuario**: Cloud Identity Engine le permite especificar el usuario para el que desea ejecutar un informe.
- **Comparta informes de forma fácil y segura con otros miembros de su organización** con la configuración de Cloud Identity Engine, puede añadir destinatarios fácilmente a un informe programado. Los destinatarios de su informe se comparan con Cloud Identity Engine y, si no encuentra una coincidencia, realiza un paso de validación adicional al comparar el dominio de la dirección de correo electrónico con los dominios de direcciones de correo electrónico asociados con su cuenta de asistencia. Estas comprobaciones garantizan que los informes no se envíen fuera de la organización.

Las aplicaciones integradas se deben implementar en la misma región. En cualquier momento, puede ir al hub para integrar Cloud Identity Engine con Prisma Access o Directory Sync. # Integración de aplicaciones de Palo Alto Networks

Compatibilidad con paneles de control

Algunos de las compatibilidades del panel de control del producto están pendientes de migrar a Strata Cloud Manager.

Función	Compatible con				Licencias y otros requisitos	Alcance de los datos agregados
	Prisma Access (gestionado en la nube)	Prisma Access (gestionado por Panorama)*	AIOps for N(	Plataforma multiinquilin Prisma SASE		
	• Documentos para Prisma Access (Managed by Strata Cloud Manager) y Prisma Access (Managed by Panorama)		• Documentos para AIOps for NGFW	• Documentos para la plataforma multiinquilino Prisma SASE		
Estado de SASE	Sí	Sí	Sí		• Observabilidad ADEM • ADEM basado en IA	
Prácticas recomendadas	Sí	No	Versiones de PAN-OS: 10.0 o posterior	Sí	[Solo para AIOps for NGFW] Habilite el uso compartido de telemetría en dispositivos	• Prisma Access (Manage por inquilino • AIOps for NGFW: por NGFW/ Panorama asociado a una instancia de AIOps for NGFW
Resumen de cumplimiento	No	No	Sí	No	[Solo para AIOps para NGFW] Habilite el uso compartido de telemetría	AIOps para NGFW: por NGFW/ Panorama asociado con la instancia

Función	Compatible con				Licencias y otros requisitos	Alcance de los datos agregados
	Prisma Access (gestionado en la nube)	Prisma Access (gestionado por Panorama)*	AIOps for N(	Plataforma multiinquilin Prisma SASE		
					en dispositivos	AIOps para NGFW
BPA bajo demanda	No	No	Sí	No	TSF	AIOps para NGFW: por NGFW/ Panorama asociado con la instancia AIOps para NGFW
Resumen ejecutivo	Sí	Sí	Sí	Sí	• Licencia de Strata Logging Service • Licencia de Prevención de amenazas • Licencia de Filtrado de URL • Licencia de WildFire • Licencia Enterprise DLP	Por arrendatario de Strata Logging Service
WildFire	Sí	No	Sí	Sí**	Licencia de WildFire	Por Grupo de servicios de inquilino (TSG)
DNS SecuritySí		Sí	Sí	Sí**	Licencia de DNS Security	Por Grupo de servicios

Función	Compatible con				Licencias y otros requisitos	Alcance de los datos agregados
	Prisma Access (gestionado en la nube)	Prisma Access (gestionado por Panorama)*	AIOps for N(	Plataforma multiinquilin Prisma SASE		
						de inquilino (TSG)
Visor de logs	Sí	Sí	Sí	Sí	Licencia de Strata Logging Service	Por arrendatario de Strata Logging Service
Búsqueda del COI	Sí	No	Sí	Sí**	Requisitos para ver el gráfico de tendencias en la búsqueda: • Licencia DNS • Licencia WildFire • Licencia Strata Logging Service • Filtrado de URL	
Descargar/ Compartir/ Programar	Sí	Sí	Sí	Sí		Consulte la columna de características correspondiente en esta tabla
SaaS Security	Sí	No	No	No	• Licencia de Saas Security • Strata Logging Service	Por arrendatario de Prisma Access

Función	Compatible con				Licencias y otros requisitos	Alcance de los datos agregados
	Prisma Access (gestionado en la nube)	Prisma Access (gestionado por Panorama)*	AIOps for N(	Plataforma multiinquilin Prisma SASE		
Incidentes de DLP	Sí	No	No	No	Licencia Enterprise DLP	Por arrendatario de Prisma Access
Estado del dispositivo	No	No	Sí	No	• [Solo para AIOps for NGFW] Habilite el uso compartido de telemetría en dispositivos	AIOps for NGFW: por NGFW/ Panorama asociado a una instancia de AIOps for NGFW
Información sobre la postura de seguridad	No	No	Sí	No		AIOps for NGFW: por NGFW/ Panorama asociado a una instancia de AIOps for NGFW
Advanced Threat Prevention	No	No	Sí	No	• Licencia de Prevención de amenazas o Advanced Threat Prevention • Strata Logging Service	Por arrendatario de Strata Logging Service
IoT Security (Seguridad de IoT)	Sí	Sí	Sí	No	Licencia de IoT Security	Por arrendatario de IoT Security

Función	Compatible con				Licencias y otros requisitos	Alcance de los datos agregados
	Prisma Access (gestionado en la nube)	Prisma Access (gestionado por Panorama)*	AIOps for NG	Plataforma multiinquilino Prisma SASE		
Prisma SD-WAN	No	No	No	Sí	Licencia de Prisma SD-WAN	Por arrendatario de Prisma SD-WAN
CVE de PAN-OS	No	Sí	Sí		[Solo para AIOps para NGFW] Habilite el uso compartido de telemetría en dispositivos	• AIOps para NGFW: por NGFW/ Panorama asociado con la instancia AIOps para NGFW • Base de datos PSIRT de CVE mediante acceso a la API
Adopción de CDSS	Sí	Sí	Sí		[Solo para AIOps para NGFW] Habilite el uso compartido de telemetría en dispositivos	AIOps para NGFW: por NGFW/ Panorama asociado con la instancia AIOps para NGFW
Adopción de características	No	Sí	Sí		[Solo para AIOps para NGFW] Habilite el uso compartido	AIOps para NGFW: por NGFW/ Panorama asociado con la

Función	Compatible con				Licencias y otros requisitos	Alcance de los datos agregados
	Prisma Access (gestionado en la nube)	Prisma Access (gestionado por Panorama)*	AIOps for N(	Plataforma multiinquilin Prisma SASE		
					de telemetría en dispositivos	instancia AIOps para NGFW

Prisma Access (gestionado por Panorama)*:

- Para los usuarios de Prisma Access (gestionado por panorama) con Strata Logging Service alojado en la región no perteneciente a las Américas, debe dar su consentimiento para permitir que Prisma Access lea y procese los datos del Strata Logging Service en la región no americana. Revise y acepte el aviso de privacidad en la página de inicio del panel para proporcionar su consentimiento y ver más paneles y logs. Solo los administradores de aplicaciones, instancias y cuentas pueden ver y aceptar el aviso de privacidad.
- Los paneles no son compatibles con el entorno multiinquilino de Prisma Access (gestionado por Panorama).

Sí*: Sí significa que todas las versiones de Prisma Access y PAN-OS son compatibles.

Sí**: en la plataforma multiinquilino, los inquilinos se identifican como grupos de servicios de inquilinos (TSG) y asignados con ID de TSG. Se puede asociar uno o varios inquilinos por portal de atención al cliente (CSP). Los datos que se muestran en el panel dependen de los siguientes escenarios:

- La aplicación desde la que accede al panel de control debe ser compatible con TSG y se debe acceder a ella a través de la Plataforma SASE o la vista del inquilino en el hub.
- Usted tiene Dispositivos asociados con el inquilino utilizando Servicios comunes en el hub.
- Verifique si sus inquilinos tienen una asignación de uno a uno o de varios a uno con CSP.
  - Si los inquilinos tienen una asignación uno a uno con CSP, puede ver los datos del panel en todos los orígenes (por ejemplo, en el panel de WildFire, se muestran los datos de muestras de cortafuegos de Palo Alto Networks, Prisma Access, Traps, Cortex XDR, Prisma SaaS, Proofpoint y las cargas manuales).
  - Si hay varios inquilinos asociados por CSP, el panel muestra solo datos de Prisma Access, cortafuegos de Palo Alto Networks y dispositivos Panorama asociados a inquilinos específicos y no de otros orígenes.

AIOps for NGFW*: los paneles disponibles en AIOps for NGFW dependen de si tiene una versión de licencia Gratuita o Premium https://docs.paloaltonetworks.com/aiops/aiops-for-ngfw/get-started-with-aiops/premium-features.

Panel: Creación de un panel personalizado

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software • Prisma SD-WAN	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN Las otras licencias y requisitos previos necesarios para la visibilidad son: ❑ Licencias para desbloquear ciertos widgets en el panel ❑ Un rol que tiene permiso para ver el panel → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Además de los paneles predeterminados, puede crear paneles personalizados para obtener visibilidad en áreas de su interés en su red mediante widgets. Los widgets son componentes que se utilizan para crear un panel. Los widgets se clasifican y almacenan en la biblioteca de widgets. Haga clic en **Dashboard (Paneles)** > **+** y seleccione una categoría de la lista desplegable para ver los widgets. Los widgets disponibles en la biblioteca de widgets dependen de sus suscripciones a servicios de seguridad. Por ejemplo, si tiene licencias de AIOps for NGFW Premium y Advanced WildFire, puede ver y usar todos los widgets de la categoría WildFire para crear un panel.

Estas son las categorías de widgets disponibles para crear un panel. Consulte los enlaces a continuación para conocer los requisitos de licencia para acceder a los widgets de estas categorías y obtener más información sobre ellos.

- Panel: Advanced Threat Prevention
- Panel: DNS Security
- Panel: WildFire

Crear un panel de control

Puede añadir hasta 10 widgets en un panel personalizado y crear 10 paneles personalizados por usuario. El panel de control y los widgets se pueden personalizar en cualquier momento. Puede

personalizar el mosaico del widget, la descripción, mostrar u ocultar filtros, configuraciones del panel como el diseño, el nombre del panel y las descripciones, y también incluir filtros en el panel.

STEP 1 | Haga clic en **Dashboards (Paneles)** > **+**.

STEP 2 | Introduzca un nombre para el panel.

STEP 3 | Seleccione una categoría de widget del menú desplegable Biblioteca de widgets.

STEP 4 | Añada el widget al panel: pase el ratón sobre el widget para obtener más información sobre él. Arrastre y suelte el widget en el lienzo del panel.

Puede añadir más widgets del mismo tipo o de tipos diferentes de otra categoría de widgets al lienzo del panel.

STEP 5 | Cambie entre la vista **Datos de muestra** y **Datos reales** para saber cómo se ve su widget del panel. Los datos de muestra le ayudan a ver cómo va a quedar el panel y qué tipo de información puede ver. Utilice la opción **Datos reales** para ver los datos reales de su implementación.

STEP 6 | (Opcional) Puede personalizar el panel en la vista del editor:

- Reorganice los widgets en el panel: seleccione el widget y arrástrelo y suéltelo donde sea necesario en el lienzo.
- Editar un widget: utilice el icono de edición en la esquina superior derecha de cada widget para editar la configuración del widget. Las configuraciones disponibles dependen del widget y no son las mismas en todos los widgets. Por ejemplo, puede editar el nombre del widget, la descripción y las opciones para filtrar y ordenar los datos del widget, como veredicto y acción.

  Puede editar la configuración del widget en la vista del editor o después de guardar el panel.

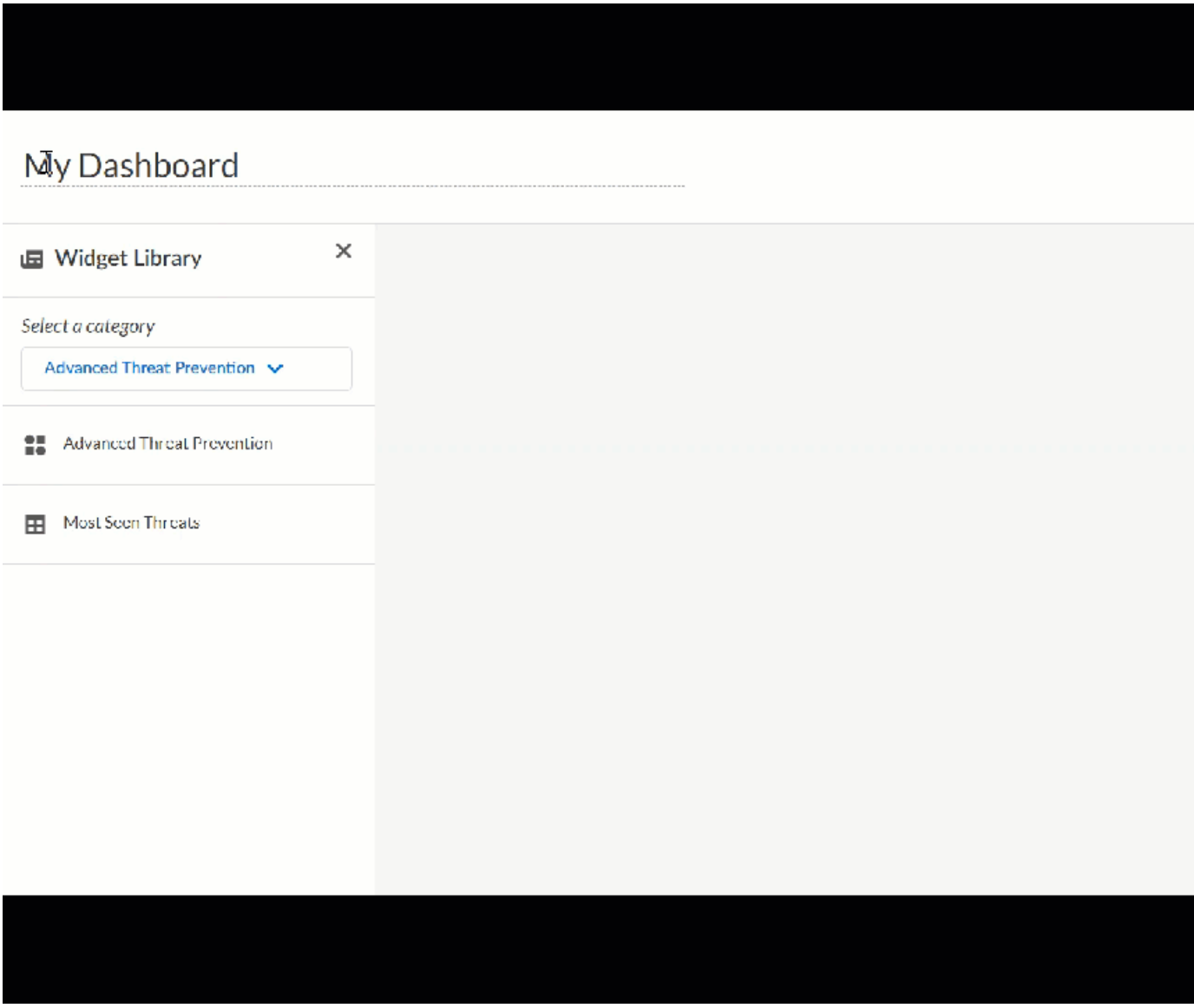
STEP 7 | Guarde el panel y haga clic en **Go to see dashboard (Ir a ver el panel)** en la parte superior de la página para abrirlo.

STEP 8 | (Opcional) Después de guardar el panel, puede:

- Cambiar el intervalo de tiempo para el cual desea ver los datos del panel.

  Puede cambiar la hora solo después de guardar el panel. En la vista del editor, el rango de tiempo predeterminado es 24 horas.

- Utilice el icono editar o eliminar para modificar o eliminar el panel personalizado.



Panel: Estado del dispositivo

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW, incluidos los financiados por Créditos de NGFW de software	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium o Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

- Haga clic en **Dashboards (Paneles)** > **Device Health (Estado del dispositivo)** para comenzar.

¿Qué le muestra este panel?

El panel muestra los datos añadidos de todos los cortafuegos incorporados a su inquilino y también están enviando datos de telemetría.

El panel Estado del dispositivo le muestra el estado de salud acumulativo y el rendimiento de su implementación en función de las puntuaciones de salud de los NGFW incorporados. El estado del dispositivo está determinada por la gravedad de la puntuación de estado, o salud, (0-100) y su grado de estado correspondiente (bueno, regular, deficiente, crítico). La puntuación de salud se calcula en función de la prioridad, número, tipo y estado de las alertas abiertas.

¿Cómo puede utilizar los datos del panel?

Este panel le ayuda a:

- Comprender las mejoras de implementación que ha realizado durante un período al ver los datos históricos de puntuación de salud.
- Acotar los dispositivos que requieren atención en su implementación y priorizar los problemas para resolverlos.

La funcionalidad de informe (descargar, compartir y programar informe) no es compatible con este panel.

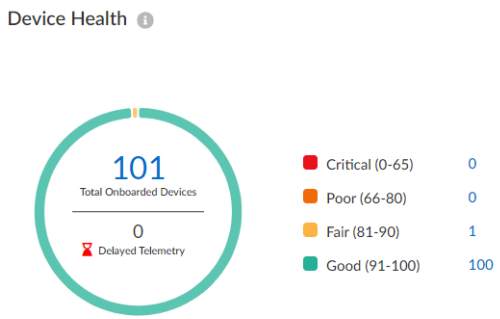
Panel de estado del dispositivo: Puntuaciones del estado del dispositivo

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW, incluidos los financiados por Créditos de NGFW de software	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium o Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

- Haga clic en **Dashboards (Paneles)** > **Device Health (Estado del dispositivo)** para ver el panel.

El widget del panel muestra:

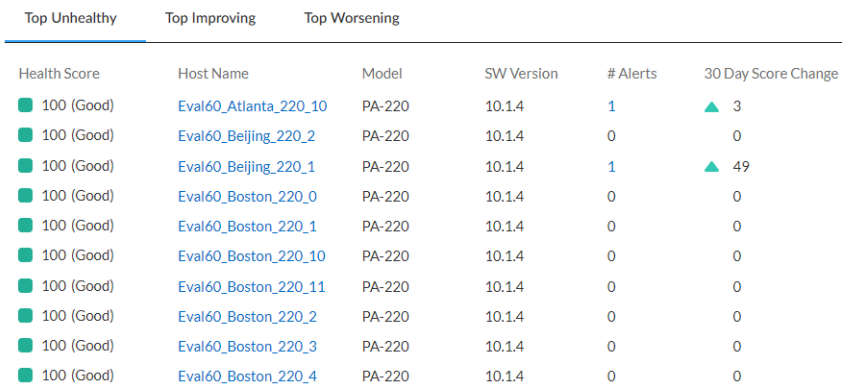
- El número total de cortafuegos NGFW incorporados.
- El número de dispositivos que no han enviado datos de telemetría durante más de 12 horas.
- La gravedad de la puntuación de estado de los dispositivos incorporados en su implementación. Haga clic en el enlace numérico para conocer los detalles del dispositivo, las estadísticas de estado del dispositivo y las alertas en el dispositivo que necesitan atención.



Panel de estado del dispositivo: Estadísticas de dispositivos

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW, incluidos los financiados por Créditos de NGFW de software	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium o Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

- Haga clic en **Dashboards (Paneles)** > **Device Health (Estado del dispositivo)** para ver el panel.



Principales dispositivos en mal estado

Estos son los dispositivos con más problemas de salud y rendimiento en su implementación. También puede profundizar para ver los detalles del dispositivo y las alertas en el dispositivo. Arreglar las alertas críticas para mejorar la puntuación de estado y el estado de implementación.

Principales dispositivos mejorando

Vea los 10 dispositivos principales durante el período de 30 días con puntuaciones de estado mejoradas en comparación con las puntuaciones de estado actuales de los dispositivos.

Principales dispositivos empeorando

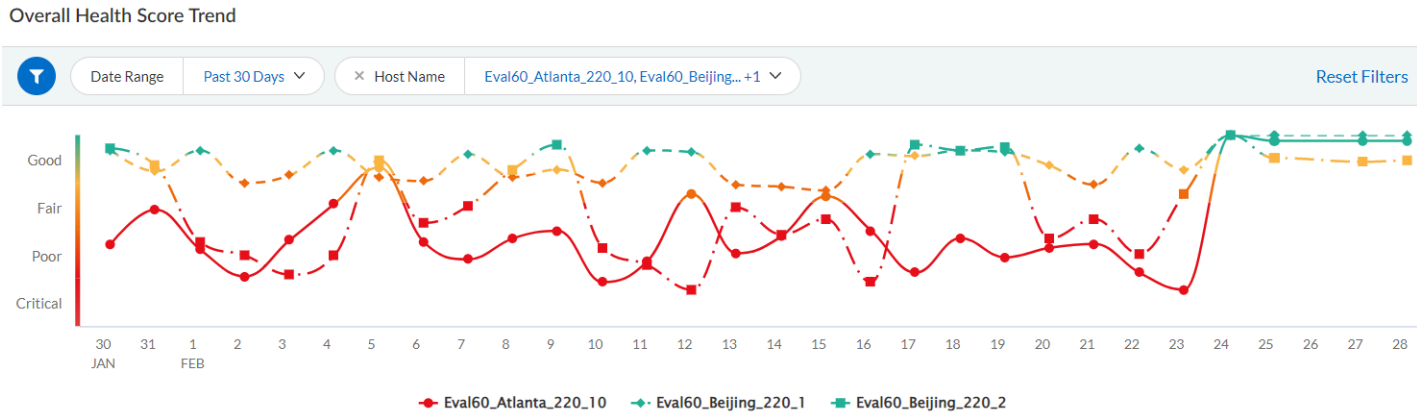
Revise el estado de los dispositivos en el intervalo de 30 días. Estos son los 10 dispositivos principales con las puntuaciones de estado disminuidas en comparación con las puntuaciones de estado actuales de los dispositivos.

Panel de estado del dispositivo: Tendencia de puntuación

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW, incluidos los financiados por Créditos de NGFW de software	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium o Strata Cloud Manager Pro

¿Dónde puedo usar esto?	¿Qué necesito?
	→ Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

- Haga clic en **Dashboards (Paneles)** > **Device Health (Estado del dispositivo)**para ver el panel.



El gráfico muestra la tendencia del estado de su implementación durante el período de tiempo seleccionado. Coloque el cursor sobre el punto de activación para conocer los dispositivos que contribuyen a la gravedad de la puntuación de estado. Puede ver las tendencias de uno o más dispositivos filtrados por el nombre de host, el modelo o la versión de software.

Panel: Resumen ejecutivo

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software • Prisma SD-WAN	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro ☐ Prisma SD-WAN Las otras licencias y requisitos previos necesarios para la visibilidad son: ☐ Licencias para desbloquear ciertos widgets en el panel ☐ Un rol que tiene permiso para ver el panel → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

- Haga clic en **Strata Cloud Manager** > **Dashboards (Paneles)** > **More Dashboards (Más paneles)** > **Executive Summary (Resumen ejecutivo)** para empezar.

¿Qué le muestra este panel?

El panel muestra datos agregados por inquilino de Strata Logging Service.

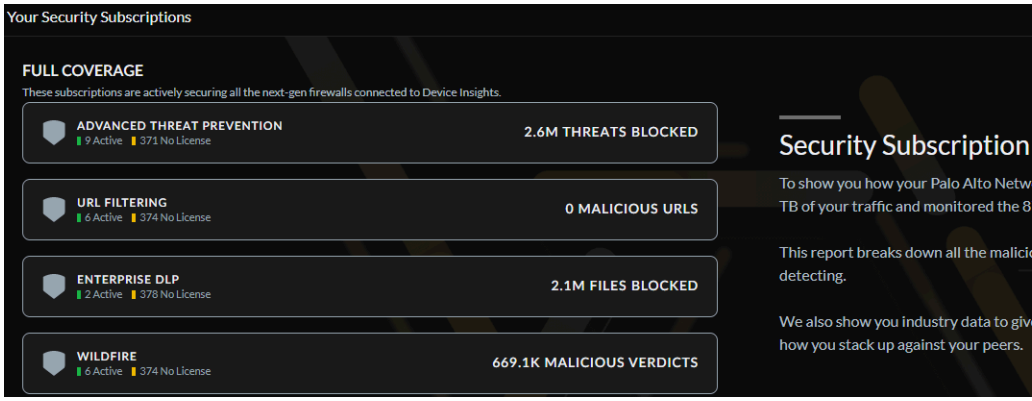
El panel Resumen ejecutivo muestra cómo le protegen sus suscripciones de seguridad de Palo Alto Networks. En este informe se desglosa la actividad maliciosa en la red que detectan estas suscripciones: **WildFire**, **Advanced Threat Prevention**, **Advanced URL Filtering** y **DLP empresarial**. El panel muestra datos para cada uno de estos servicios con enlaces a paneles de servicios de seguridad para profundizar en la investigación más profunda.

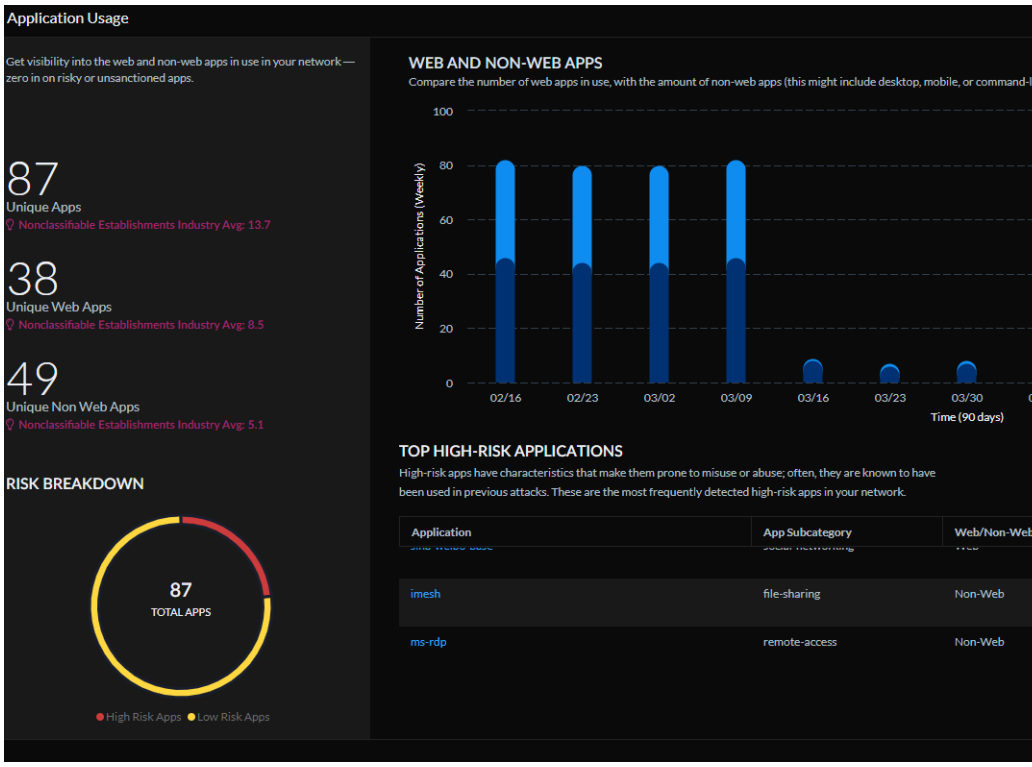
Este panel admite informes. Estos iconos,  en la parte superior derecha de un panel, indican qué los informes son compatibles con este panel. Puede compartir, descargar y programar informes que cubran los datos que muestra este panel.

¿Cómo puede utilizar los datos del panel de control?

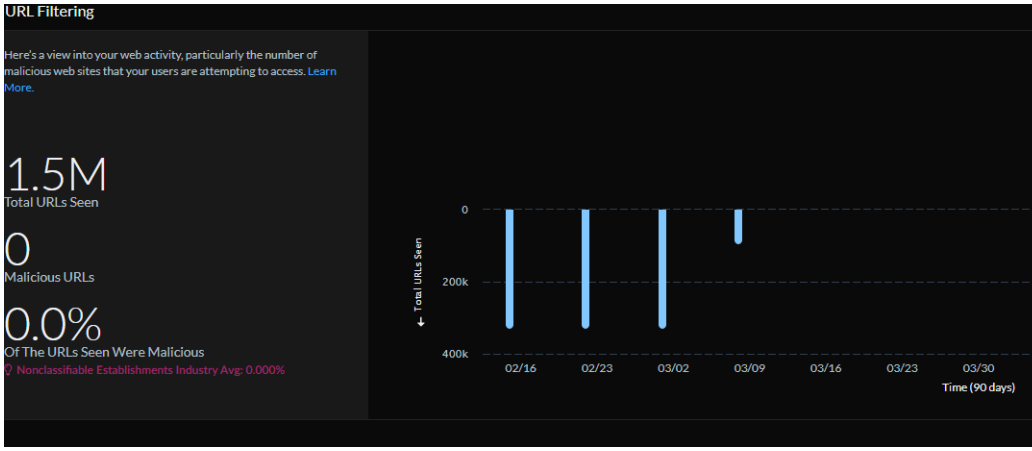
- Revise toda la actividad maliciosa que detectan las suscripciones activas de Palo Alto Networks. Vea si necesita refinar la configuración de la suscripción o la configuración de las reglas de seguridad para cerrar las brechas de seguridad.
- Le muestra los datos de la industria para darle una perspectiva sobre el panorama de amenazas al que se enfrenta y cómo se compara con su par.

El panel proporciona los siguientes datos.

Panel de Resumen Ejecutivo: Sus suscripciones de seguridad	Este informe proporciona las cifras de la actividad maliciosa que sus suscripciones están detectando y previniendo: • aplicaciones de alto riesgo • amenazas graves (exploits, malware y C2) • actividad web maliciosa • Amenazas basadas en archivos (incluidas amenazas nunca antes vistas) • pérdida de datos 

Panel de Resumen Ejecutivo: Application Usage (Uso de aplicación)	Revise los logs de tráfico de las aplicaciones de alto riesgo y vea cómo puede reforzar la posición de seguridad. 
Panel de Resumen Ejecutivo: Advanced Threat Prevention *Requiere una licencia de Advanced Threat Prevention.*	Examine las reglas de la política de seguridad que permiten la mayoría de las amenazas. Revise estas reglas para ver dónde puede habilitar una aplicación de amenazas más estricta. Más información
Panel de Resumen Ejecutivo: URL Filtering *Requiere una licencia de Advanced URL Filtering.*	Revise la actividad web maliciosa en su red, en particular el número de sitios web malintencionados

a los que los usuarios intentan acceder.

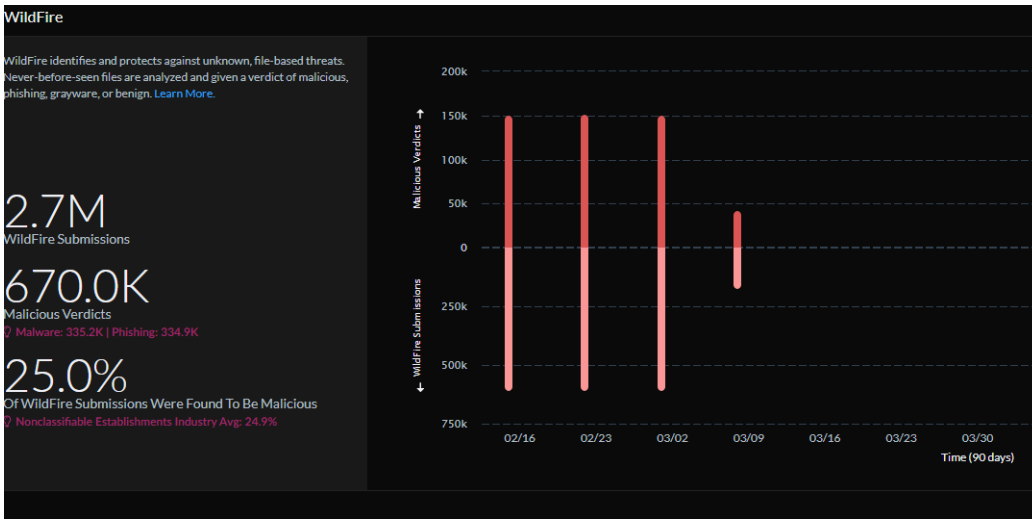


Panel de Resumen Ejecutivo: WildFire

Requiere licencia de Advanced WildFire.

Los datos de pares en este panel le brindan una vista del panorama de amenazas de su sector y cómo se compara su cobertura de seguridad con organizaciones similares. Estos datos del sector también se muestran para las suscripciones que no se utilizan; esto le ayuda a ver si hay lugares donde puede aumentar la cobertura para cerrar las brechas de seguridad.

Aquí hay un primer plano del tipo de datos que proporciona este panel: aquí puede ver el trabajo que WildFire está haciendo para proteger su red y su sector. Obtener más información. #

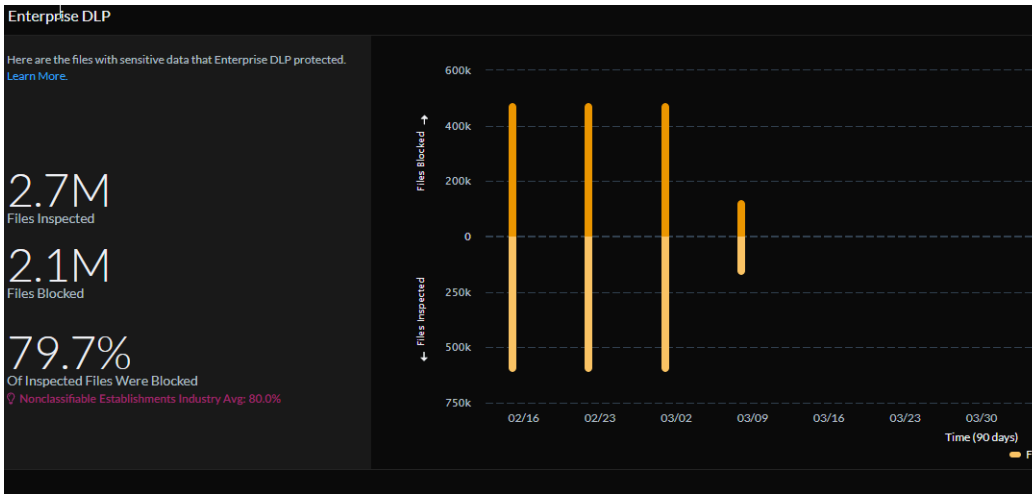


Panel de Resumen Ejecutivo: DLP empresarial

Requiere una licencia Enterprise DLP.

Vea cómo su servicio de DLP empresarial de Palo Alto Networks protege sus datos mediante la aplicación de estándares de seguridad de datos. El panel proporciona información sobre las aplicaciones en las que DLP impide la mayoría de las cargas y el número total de archivos que DLP bloquea en su red. También puede usar estos datos para comparar con sus pares de la industria y comparar sus estándares de postura de seguridad.

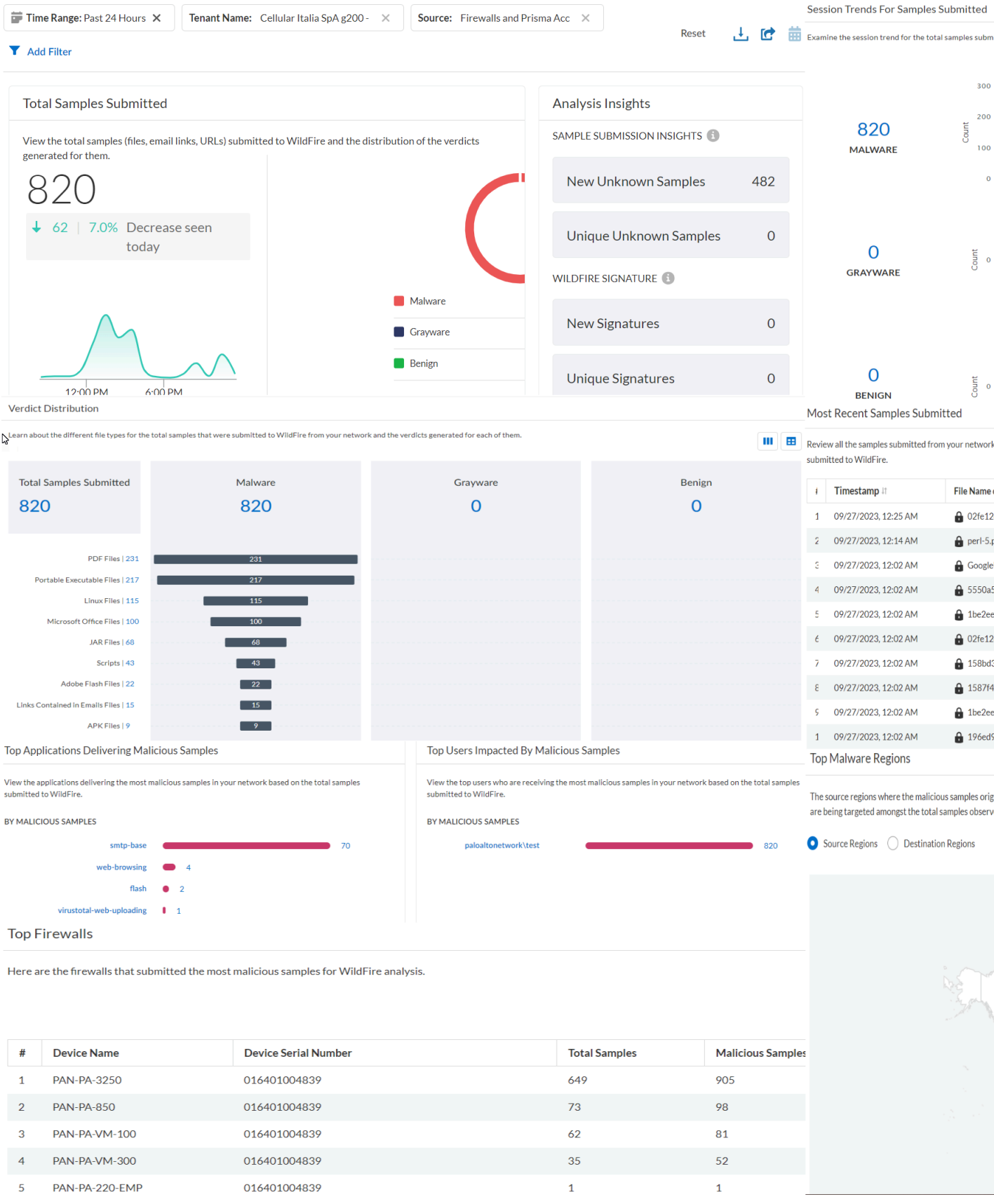
Revise las aplicaciones y los nombres de usuario de origen para comprender mejor dónde se originaron los Incidentes de DLP y gestionarlos.



Panel: WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro Las otras licencias y requisitos previos necesarios para la visibilidad son: ☐ Un rol que tiene permiso para ver el panel de control ☐ Advanced WildFire → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

- Haga clic en **Strata Cloud Manager** > **Dashboards (Paneles)** > **More Dashboards (Más paneles)** > **WildFire** para empezar.



#	Device Name	Device Serial Number	Total Samples	Malicious Samples
1	PAN-PA-3250	016401004839	649	905
2	PAN-PA-850	016401004839	73	98
3	PAN-PA-VM-100	016401004839	62	81
4	PAN-PA-VM-300	016401004839	35	52
5	PAN-PA-220-EMP	016401004839	1	1

¿Qué le muestra este panel?

El panel muestra datos agregados por Grupo de servicios de inquilino (TSG). El panel de control muestra los datos de Prisma Access, los cortafuegos de Palo Alto Networks y los dispositivos Panorama asociados con el inquilino, siempre que los inquilinos tengan una asignación de uno a uno con su cuenta de Customer Support Portal. El panel no muestra datos de otras fuentes si hay varios inquilinos asociados por Portal de atención al cliente.

El panel de control de WildFire le muestra cómo WildFire le protege del malware nuevo oculto en archivos y ejecutables. Este panel admite informes. Estos iconos,  en la parte superior derecha de un panel, indican qué los informes son compatibles con este panel. Puede compartir, descargar y programar informes que cubran los datos que muestra este panel.

¿Cómo puede utilizar los datos del panel?

Utilice este panel de control para:

- (Requiere licencia AIOps for NGFW Premium)supervisar los envíos de WildFire y obtener detalles de las muestras de WildFire enviadas a la nube de WildFire para su análisis.
- ver los detalles de los usuarios destinatarios, las aplicaciones que entregaron los archivos, los cortafuegos que enviaron las muestras para su análisis y todas las URL involucradas en la actividad de comando y control de los archivos.
- (Requiere licencia de AIOps for NGFW Premium)Vea los logs de WildFire y el informe de análisis y ajuste la configuración de WildFire para su implementación en función del informe.

Panel WildFire: Filtros

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro Las otras licencias y requisitos previos necesarios para la visibilidad son: ☐ Un rol que tiene permiso para ver el panel de control ☐ Advanced WildFire → Las características y capacidades disponibles para usted en Strata Cloud

¿Dónde puedo usar esto?	¿Qué necesito?
	Manager depende de qué licencia(s) esté usando.

El panel WildFire proporciona estas opciones de filtro para reducir los datos específicos del panel.

- **Intervalo de tiempo**: seleccione entre las **últimas 24 horas**, los **últimos 7 días**, los **últimos 30 días** o el **intervalo de tiempo personalizado** para mostrar datos para un periodo de tiempo específico.
- **Nombre de inquilino**: el inquilino para el que se muestran los datos del panel.
- **Origen**: el alcance de los datos del panel proviene de los cortafuegos de Palo Alto Networks y Prisma Access.
- **Muestras**: seleccione la opción **Pública** o **Privada** para ver los datos enviados desde la nube pública o el entorno de nube privada de Wildfire.
- **Veredicto**: vea las muestras que se identifican como **Benignas**, **Malware** o **Grayware** en el análisis de WildFire.
- **Acción**: seleccione la opción **Permitir** o **Bloquear** para mostrar las muestras de WildFire permitidas o bloqueadas por su regla de políticas.
- **Tipo de archivo**: vea los datos basados en el tipo de archivo de la muestra analizada por WildFire. Obtenga información sobre los tipos de archivos compatibles para el análisis WildFire.
- **Hash de archivo**: vea los datos de un hash de archivo analizado por WildFire. A continuación, se enumeran las versiones hash que genera WildFire para cada archivo analizado:
  - **SHA-1**: muestra la información SHA-1 del archivo.
  - **SHA-256**: muestra la información SHA-256 del archivo.
  - **MD5**: muestra la información MD5 del archivo.
- **Nombre de aplicación**: filtra datos basados en las muestras que entrega una aplicación.
- **Región de origen**: filtro para ver las muestras que se envían desde una ubicación específica.
- **Región de destino**: filtro para ver las muestras que se reciben en una ubicación específica.
- **Nombre de usuario**: introduzca el nombre de usuario para filtrar los datos del usuario que está dirigido a entregar la muestra en su red.
- **Número de serie del dispositivo**: filtre los datos del dispositivo que envió la muestra para su análisis en WildFire.

Panel WildFire: Número total de muestras enviadas

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
	❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro Las otras licencias y requisitos previos necesarios para la visibilidad son: ❑ Un rol que tiene permiso para ver el panel de control ❑ Advanced WildFire → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

- Haga clic en **Dashboards (Paneles)** > **More Dashboards (Más paneles)** > **WildFire** para ver el panel.

El número total de muestras presentadas para el análisis de WildFire durante el período de tiempo seleccionado. El widget muestra el número de muestras enviadas desde cada fuente y el veredicto generado para las muestras. El widget también muestra el pico en las muestras enviadas para el análisis de WildFire. Investigue los picos en las muestras de malware y tome medidas para mitigar los efectos de las amenazas en su red.

Panel WildFire: Insights de análisis

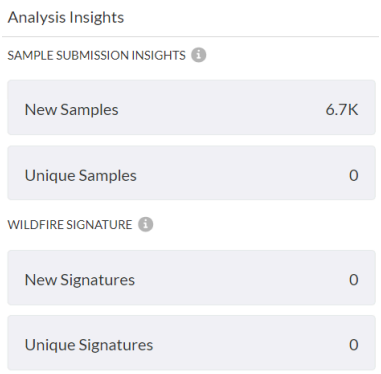
¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro Las otras licencias y requisitos previos necesarios para la visibilidad son: ❑ Un rol que tiene permiso para ver el panel de control ❑ Advanced WildFire

¿Dónde puedo usar esto?	¿Qué necesito?
	→ Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

- Haga clic en **Dashboards (Paneles)** > **More Dashboards (Más paneles)** > **WildFire** para ver el panel.

Obtenga información sobre las muestras únicas de WildFire enviadas desde su red y las firmas generadas. Utilice los datos para comprender las nuevas amenazas que se observaron solo en su red en el período de tiempo seleccionado y el número de veces que su red se ha protegido con las firmas generadas.

- **Muestras únicas desconocidas**: número de muestras enviadas a WildFire desde su red que solo se ven en su red, que son previamente desconocidas para WildFire, y que no están disponibles en otras fuentes públicas o privadas.
- **Nuevas muestras desconocidas**: número de muestras nuevas enviadas a WildFire desde su red que son previamente desconocidas para WildFire (con sha256 distinto).
- **Firmas únicas**: número de firmas generadas a partir de muestras únicas de su entorno.
- **Nuevas firmas**: número de nuevas firmas creadas por WildFire a partir de todas las muestras cargadas.



Panel WildFire: Tendencias de sesión para muestras enviadas

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro

¿Dónde puedo usar esto?	¿Qué necesito?
	Las otras licencias y requisitos previos necesarios para la visibilidad son: ☐ Un rol que tiene permiso para ver el panel de control ☐ Advanced WildFire → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

- Haga clic en **Dashboards (Paneles)** > **More Dashboards (Más paneles)** > **WildFire** para ver el panel.

Examine las tendencias de todas las muestras enviadas a WildFire desde su red y los veredictos de esas muestras. Puede realizar una búsqueda de IOC en estas muestras para conocer el historial de la muestra en su red y los resultados del análisis global de la muestra.

Panel WildFire: Distribución de veredictos

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app)

¿Dónde puedo usar esto?	¿Qué necesito?
	❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro Las otras licencias y requisitos previos necesarios para la visibilidad son: ❑ Un rol que tiene permiso para ver el panel de control ❑ Advanced WildFire → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

- Haga clic en **Dashboards (Paneles)** > **More Dashboards (Más paneles)** > **WildFire** para ver el panel.

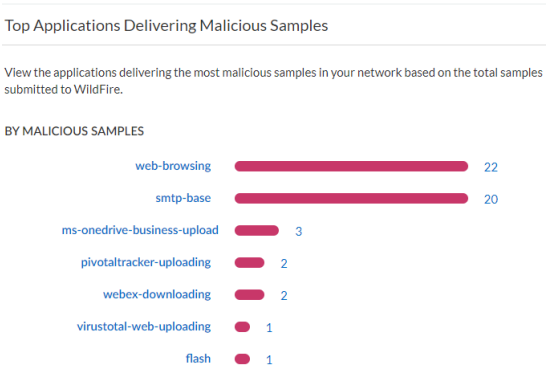
Obtenga más información sobre los veredictos de las nuevas muestras netas que WildFire detectó por primera vez en su red. Céntrese en los tipos de muestra que ocultan malware con mayor frecuencia. Haga clic en el enlace para obtener más información sobre la muestra.

Panel WildFire: Principales aplicaciones entregando muestras maliciosas

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro Las otras licencias y requisitos previos necesarios para la visibilidad son: ❑ Un rol que tiene permiso para ver el panel de control ❑ Advanced WildFire → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

- Haga clic en **Dashboards (Paneles)** > **More Dashboards (Más paneles)** > **WildFire** para ver el panel.

Revise los detalles de las aplicaciones que entregaron la mayoría de las muestras malintencionadas en su red. Haga clic en el recuento de muestras maliciosas para obtener más información sobre las muestras.



Panel WildFire: Principales usuarios afectados por muestras maliciosas

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro Las otras licencias y requisitos previos necesarios para la visibilidad son: ☐ Un rol que tiene permiso para ver el panel de control ☐ Advanced WildFire → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

- Haga clic en **Dashboards (Paneles)** > **More Dashboards (Más paneles)** > **WildFire** para ver el panel.

Esto muestra las cuentas de usuario que se usan con más frecuencia para entregar muestras malintencionadas en la red. Haga clic en el nombre de usuario para investigar los patrones de actividad del usuario.

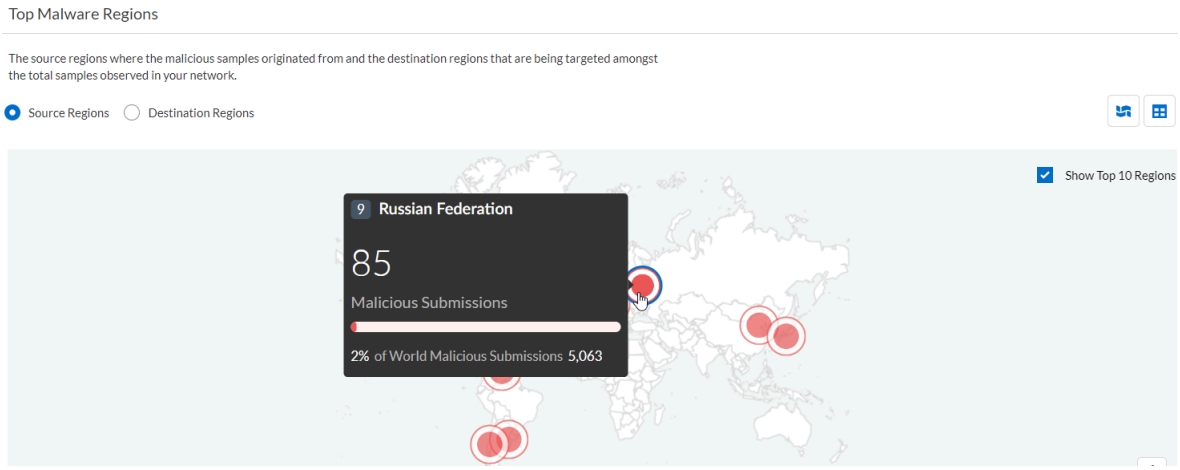
Panel WildFire: Principales regiones de malware

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app)

¿Dónde puedo usar esto?	¿Qué necesito?
	❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro Las otras licencias y requisitos previos necesarios para la visibilidad son: ❑ Un rol que tiene permiso para ver el panel de control ❑ Advanced WildFire → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

- Haga clic en **Dashboards (Paneles)** > **More Dashboards (Más paneles)** > **WildFire** para ver el panel.

Revise las ubicaciones desde las que se originaron las muestras maliciosas o a las que se entregaron en la red. Puede ver el recuento de muestras para las regiones de origen y destino en un formato de mapa o tabla. Utilícelo para reducir las regiones objetivo de malware y el tipo de ataque de malware.



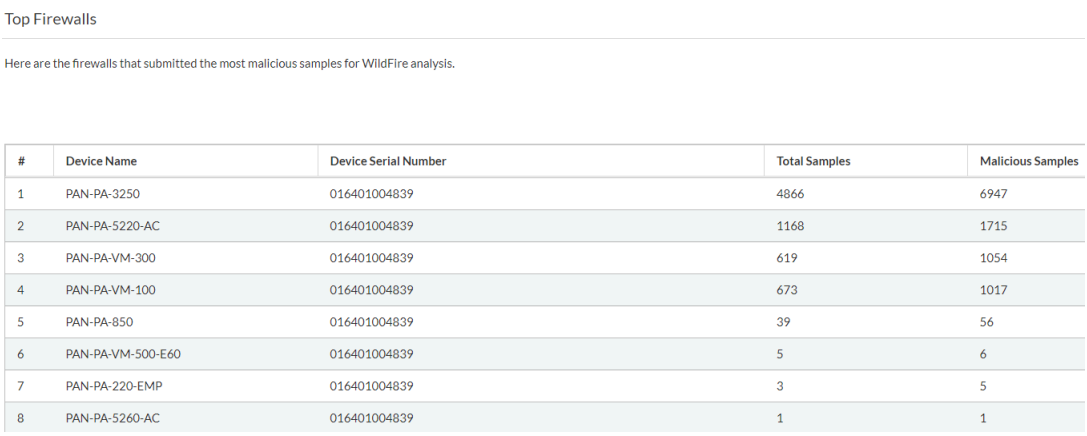
Panel WildFire: Cortafuegos principales

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro

¿Dónde puedo usar esto?	¿Qué necesito?
	Las otras licencias y requisitos previos necesarios para la visibilidad son: ☐ Un rol que tiene permiso para ver el panel de control ☐ Advanced WildFire → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

- Haga clic en **Dashboards (Paneles)** > **More Dashboards (Más paneles)** > **WildFire** para ver el panel.

Vea los cortafuegos que están enviando las muestras más maliciosas para su análisis a WildFire. Revise estos cortafuegos para rastrear los endpoints afectados y reconfigure las reglas de políticas para mitigar las amenazas y contener los archivos maliciosos en el origen.



Top Firewalls

Here are the firewalls that submitted the most malicious samples for WildFire analysis.

#	Device Name	Device Serial Number	Total Samples	Malicious Samples
1	PAN-PA-3250	016401004839	4866	6947
2	PAN-PA-5220-AC	016401004839	1168	1715
3	PAN-PA-VM-300	016401004839	619	1054
4	PAN-PA-VM-100	016401004839	673	1017
5	PAN-PA-850	016401004839	39	56
6	PAN-PA-VM-500-E60	016401004839	5	6
7	PAN-PA-220-EMP	016401004839	3	5
8	PAN-PA-5260-AC	016401004839	1	1

Panel: DNS Security

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro Las otras licencias y requisitos previos necesarios para la visibilidad son: ☐ Un rol que tiene permiso para ver el panel de ☐ DNS Security o Advanced DNS Security → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

- Haga clic en **Strata Cloud Manager** > **Dashboards (Paneles)** > **More Dashboards (Más paneles)** > **DNS Security** para empezar.

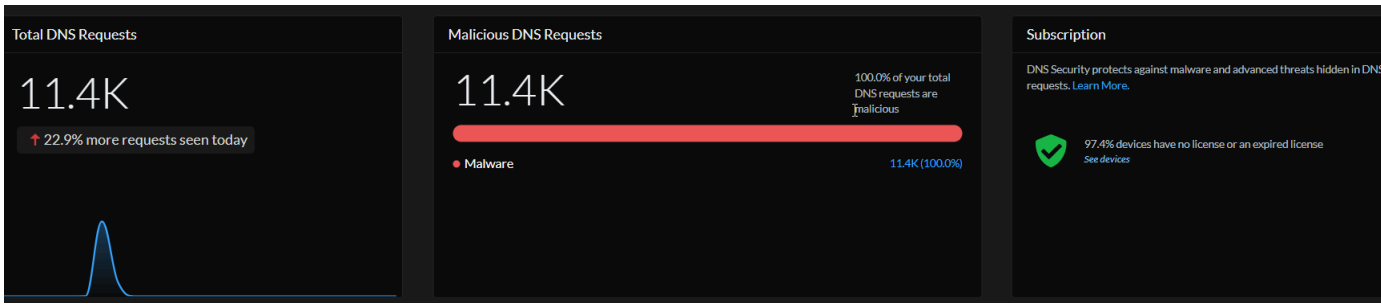
¿Qué le muestra este panel?

El panel muestra datos agregados por Grupo de servicios de inquilino (TSG). El panel muestra datos de Prisma Access, cortafuegos de Palo Alto Networks y dispositivos Panorama asociados con su inquilino.

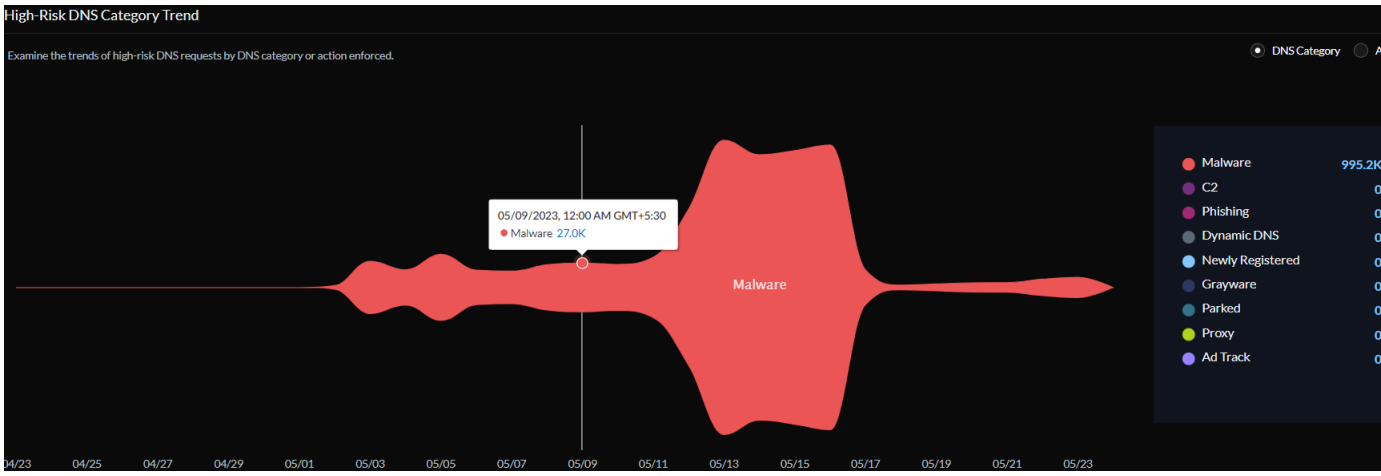
El nuevo panel de DNS Security muestra cómo su suscripción a DNS Security le protege de las amenazas avanzadas y el malware que utiliza DNS. También puede filtrar la información que se muestra en el panel por intervalo de tiempo, acción realizada, dominio, IP de resolución y categoría de DNS. El nombre del origen y del inquilino para los que se muestran los datos en el panel se muestran en los filtros Nombre del inquilino y Origen. Puede ver:Estadísticas y tendencias de solicitudes de DNS

- **Número total de solicitudes de DNS**: muestra el número total de solicitudes de DNS que procesa DNS Security. El gráfico de líneas dibuja el número de solicitudes de DNS según el rango de tiempo definido por el usuario. Al especificar un rango de tiempo personalizado, el gráfico de líneas se actualiza en consecuencia.

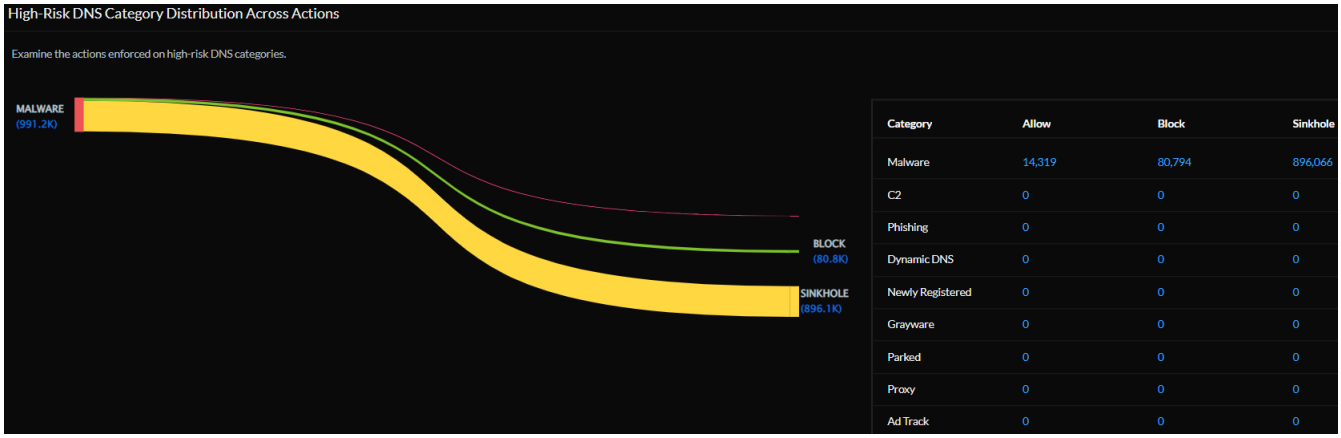
- **Solicitudes de DNS maliciosas**: muestra un gráfico de barras apiladas que muestra las solicitudes de DNS que se clasifican como maliciosas. Haga clic en el enlace del número para ver los detalles de las solicitudes de DNS.
- **Suscripción**: muestra el número de dispositivos de la red con una suscripción activa a DNS Security. También se muestra, con un enlace a una lista completa, un porcentaje de dispositivos que no están equipados con DNS Security o tienen una suscripción caducada.



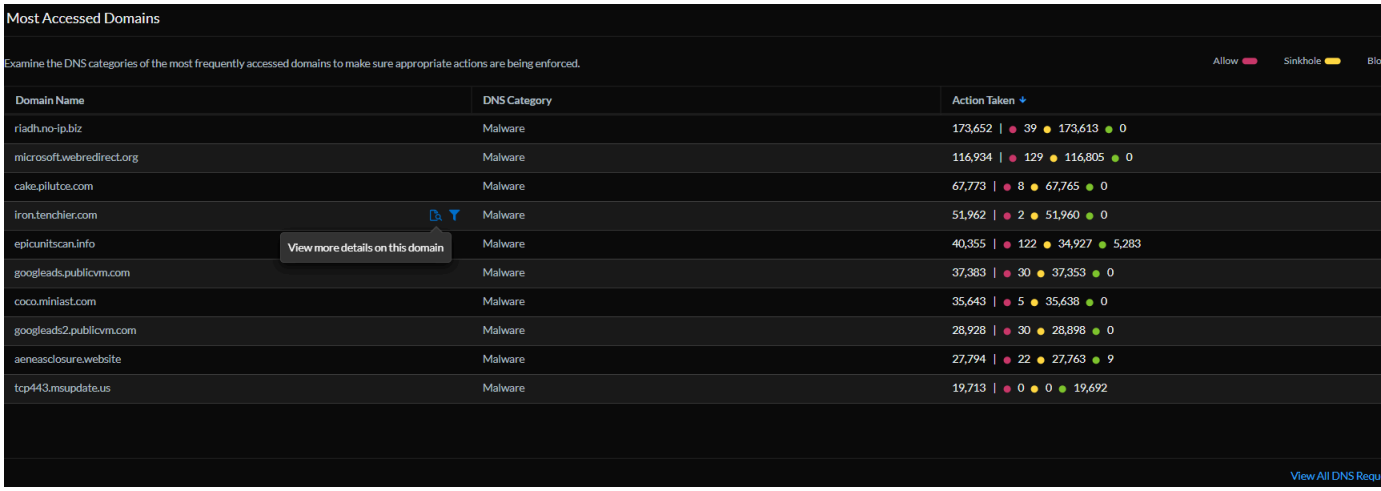
- **Tendencias de la categoría de DNS de alto riesgo**: examine la tendencia de las solicitudes de DNS de alto riesgo según la categoría de DNS o según las medidas adoptadas frente a ellas. Pase el cursor sobre un flujo específico para abrir una ventana emergente que muestre el número de solicitudes o el tipo de acción aplicada.



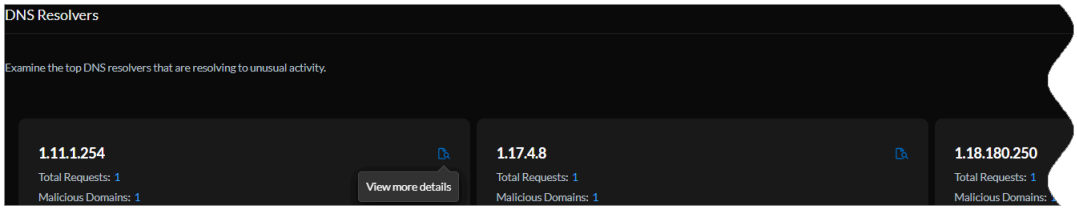
- **Distribución de categorías de DNS de alto riesgo entre acciones**: examine las acciones que el cortafuegos está tomando contra categorías particulares de DNS de alto riesgo.



- **Dominios más visitados** : proporciona una lista de los 10 dominios más solicitados de su red junto con la categoría de DNS y la acción realizada. Puede ver más detalles y los logs pertinentes para un dominio. Seleccione **View All DNS Requests (Ver todas las solicitudes de DNS)** para obtener una lista completa de los dominios a los que se ha accedido.



- **Solucionadores de DNS**: Supervise la actividad de resolución de DNS maliciosa y sospechosa en su red. Vea los principales solucionadores de DNS que resuelven dominios maliciosos y los solucionadores que resuelven una cantidad sospechosamente baja de solicitudes de DNS. Haga clic en el icono de búsqueda para Ver más detalles en el artefacto (dirección IP). Puede ver el historial del artefacto en su red y los resultados del análisis global.



- **Usuarios que visitan dominios maliciosos**: examine los hosts de su red que intentan resolver el nombre de host o el dominio de una URL maliciosa.
- **(Requiere licencia de Advanced DNS Security) Dominios secuestrados**: proporciona una lista de dominios secuestrados según lo determinado por Advanced DNS Security. Para cada

entrada, hay un motivo para la clasificación y un recuento de resultados de tráfico basado en la IP de origen.

Hijacked Domains

Hijacked	Hits
xyz.test-ipv4-wildcard.hijacking.testpanw.com	117
www.test-ipv4-wildcard.hijacking.testpanw.com	118
www.test-cname-rrname-sub-wc.hijacking.testpanw.com	353
test.test-ipv4-wildcard.hijacking.testpanw.com	118
test-ipv6.hijacking.testpanw.com	469
test-ipv4.hijacking.testpanw.com	472
test-cname-rrname.hijacking.testpanw.com	234
test-cname-rrname-wc.hijacking.testpanw.com	117
qpwc.test-ipv4-wildcard.hijacking.testpanw.com	118

- **(Requiere licencia de Advanced DNS Security) Dominios mal configurados**: Proporciona una lista de Dominios que no se pueden resolver asociada a los dominios principales de cara al público especificados por el usuario. Para cada entrada, hay un motivo para la mala configuración y un recuento de resultados de tráfico basado en la IP de origen.

Misconfigured Domains

Misconfigured Domains	Misconfigured Reasons	Hits
demo.test-dnsmisconfig-zone-dangling.testpanw.com	test-dnsmisconfig-zone-dangling.testpanw.com:A:1.2.3.4 the IP 1.2.3.4 is allocatable	117
adns-demo.test-dnsmisconfig-zone-dangling.testpanw...	test-dnsmisconfig-zone-dangling.testpanw.com:A:1.2.3.4 the IP 1.2.3.4 is allocatable	117
abc.test-dnsmisconfig-zone-dangling.testpanw.com	test-dnsmisconfig-zone-dangling.testpanw.com:A:1.2.3.4 the IP 1.2.3.4 is allocatable	589
123demo.test-dnsmisconfig-zone-dangling.testpanw.c...	test-dnsmisconfig-zone-dangling.testpanw.com:A:1.2.3.4 the IP 1.2.3.4 is allocatable	0
123.test-dnsmisconfig-zone-dangling.testpanw.com	test-dnsmisconfig-zone-dangling.testpanw.com:A:1.2.3.4 the IP 1.2.3.4 is allocatable	471

Este panel admite informes. Estos iconos,  en la parte superior derecha de un panel, indican qué los informes son compatibles con este panel. Puede compartir, descargar y programar informes que cubran los datos que muestra este panel.

¿Cómo puede utilizar los datos del panel de control?

Este panel le ayuda a:

- examinar cómo se procesan y categorizan las solicitudes de DNS
- obtener información sobre las amenazas basadas en DNS
- detectar solicitudes de DNS de dominios secuestrados y mal configurados con Advanced DNS Security

Panel: AI Runtime Security

El panel del centro de control de Strata Cloud Manager (SCM) proporciona una vista consolidada de las cargas de trabajo en la nube implementadas en clústeres y máquinas virtuales, como los módulos, los modelos, las aplicaciones, las máquinas virtuales y los espacios de nombres.

¿Dónde puedo usar esto?	¿Qué necesito?
• AI Runtime Security	☐ Active su licencia de AI Runtime Security ☐ Requisitos previos de configuración de AI Runtime Security ☐ Incorporar y activar una cuenta en la nube en SCM

Descubra recursos en la nube

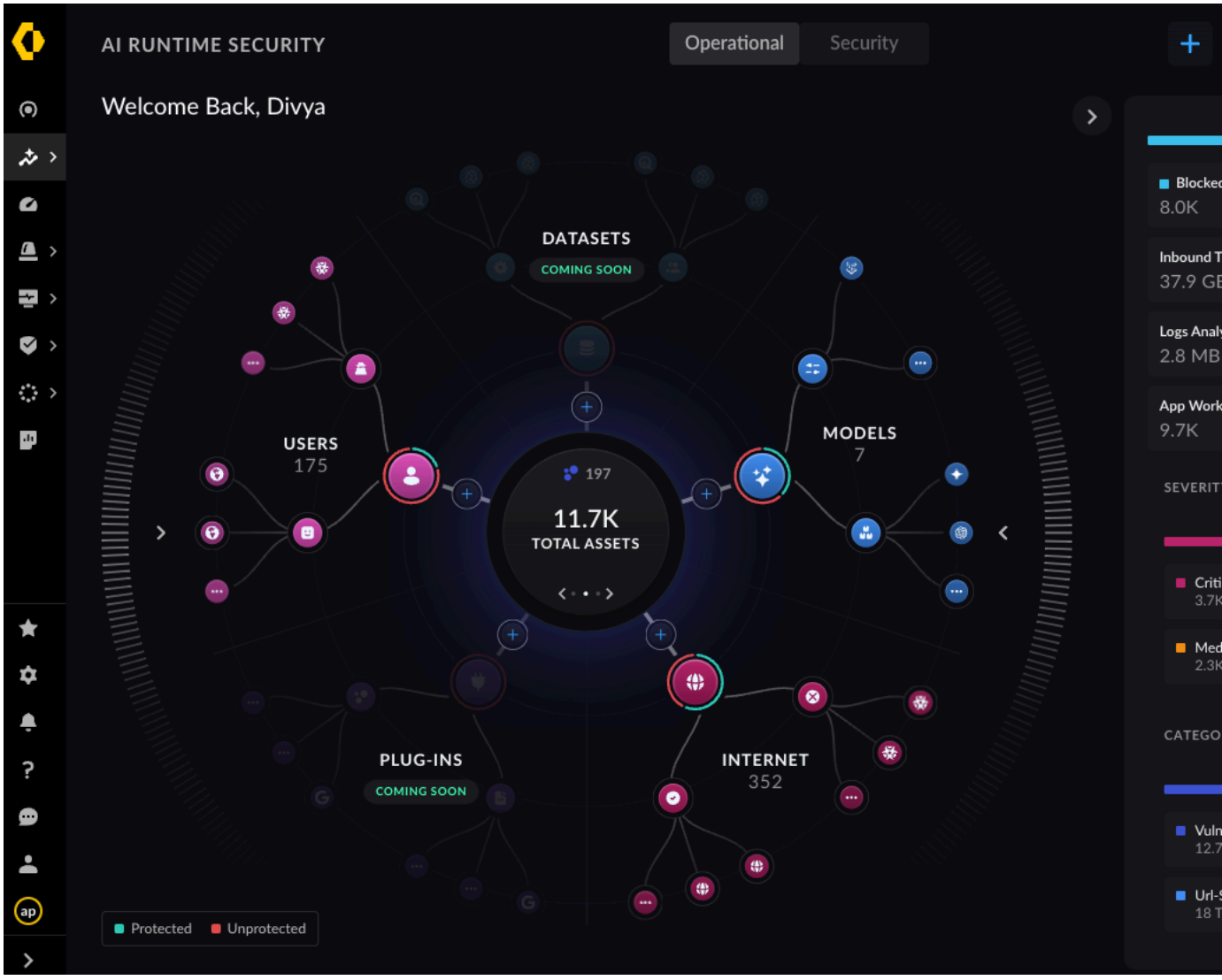
AI incorporar correctamente su cuenta en la nube en SCM y activar su cuenta de servicio, el panel de control de SCM proporciona un descubrimiento unificado de activos en tiempo real de sus cargas de trabajo en la nube.

El **Centro de control de aplicaciones en la nube** en SCM en **Insights (Informaciones) → AI Runtime Security (Seguridad de IA de tiempo de ejecución)** proporciona información práctica para descubrir todos los activos en la nube en su cuenta en la nube incorporada.

El descubrimiento de activos en el panel de control de SCM se clasifica en la vista operativa y la vista de seguridad.

El descubrimiento muestra el desglose de amenazas según la urgencia de la amenaza y las categorías de riesgo, como la detección de vulnerabilidades, la seguridad de URL y la inyección inmediata.

1. La **vista operativa** es una vista agregada de:
    1. Un recuento total y desglose de los activos descubiertos en los entornos de nube integrados
    2. Flujos de tráfico - protegidos y desprotegidos por la instancia de seguridad de IA en tiempo de ejecución
    3. Cargas de trabajo de las aplicaciones (contenedores, funciones sin servidor y máquinas virtuales)
    4. Modelos de IA que se consultan
    5. Aplicaciones de usuario que acceden a los destinos de Internet
    6. Aplicaciones de usuarios de aplicaciones a las que se accede desde aplicaciones externas
    7. Estadísticas de tráfico entrante y saliente



2. En **Vista de seguridad**:
   1. Puede agregar una instancia de (icono "+") AI Runtime Security para proteger el tráfico de red no protegido identificado en la vista operativa.

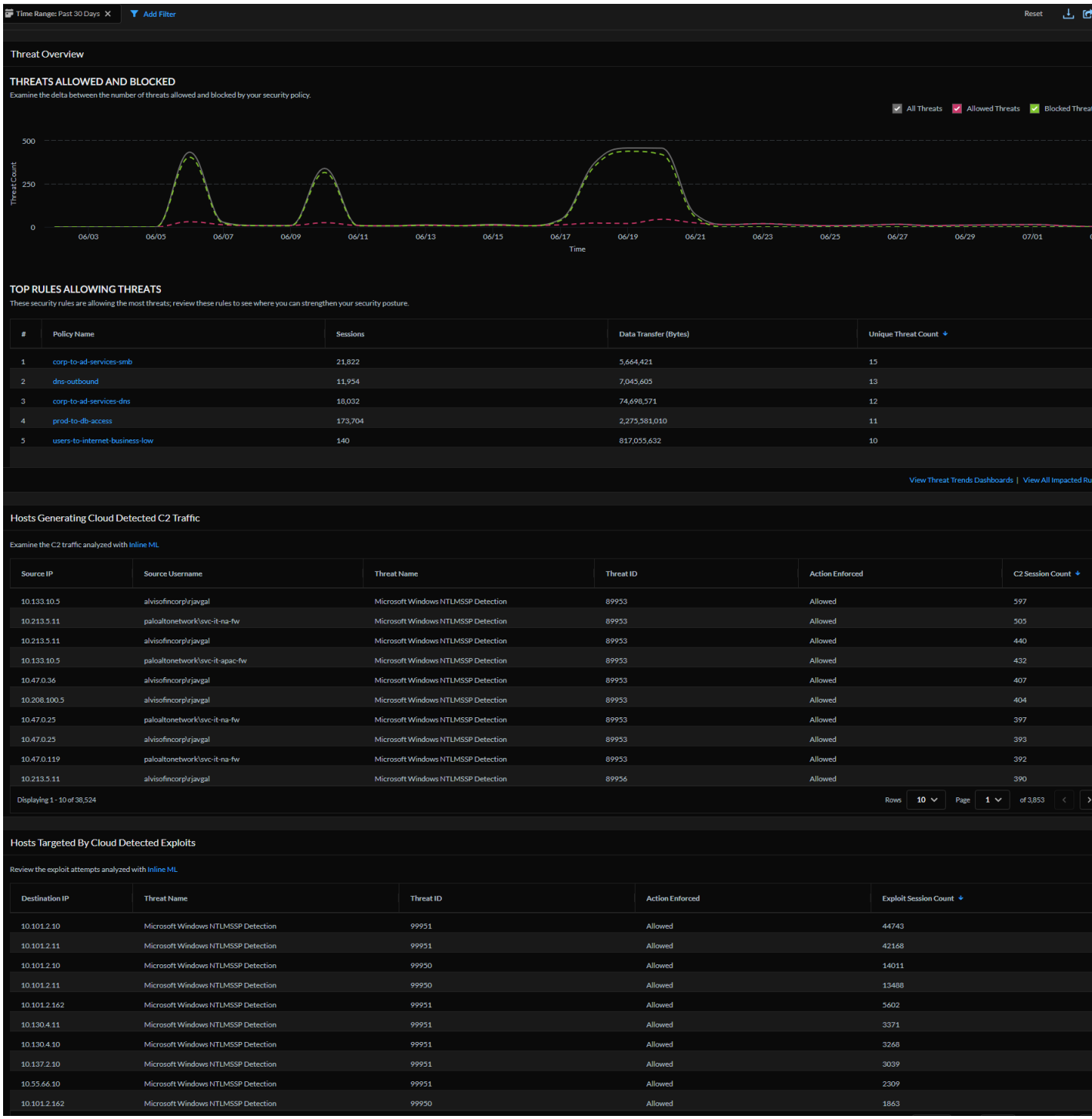
      Si ya existe la protección de instancia de AI Runtime Security, redireccione el tráfico no protegido a través de la instancia de AI Runtime Security disponible.

A continuación, detecte las rutas de flujo de red arriesgadas entre las aplicaciones de usuario, los modelos de IA e Internet. Consulte AI Traffic Network Risk Analysis e Deploy an AI Runtime Security instance para supervisar y defender su arquitectura de red en la nube.

Panel: Advanced Threat Prevention

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro Las otras licencias y requisitos previos necesarios para la visibilidad son: ☐ Un rol que tiene permiso para ver el panel ☐ Prevención de amenazas o Advanced Threat Prevention → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

- Haga clic **Strata Cloud Manager** > **Dashboards (Paneles de control)** > **More Dashboards (Más paneles de control)** > **Advanced Threat Prevention** para comenzar.



¿Qué le muestra este panel?

El panel muestra datos agregados por inquilino de Strata Logging Service.

El panel Advanced Threat Prevention brinda información sobre las amenazas detectadas en su red e identifica oportunidades para fortalecer su postura de seguridad. Las amenazas se detectan

utilizando modelos de análisis en línea en la nube y firmas de amenazas generadas a partir de datos de tráfico malicioso recopilados de varios servicios de Palo Alto Networks. Este panel proporciona una vista cronológica de las amenazas permitidas y bloqueadas y una lista de hosts que generan tráfico C2 detectado en la nube y hosts que son el objetivo de exploits detectados en la nube.

Este panel admite informes. Estos iconos,  en la parte superior derecha de un panel, indican qué los informes son compatibles con este panel. Puede compartir, descargar y programar informes que cubran los datos que muestra este panel.

¿Cómo puede utilizar los datos del panel de control?

Utilice este panel para:

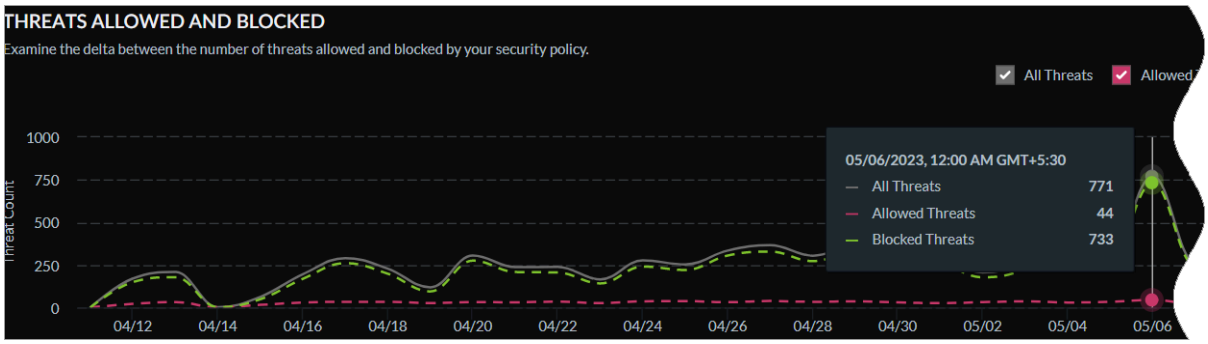
- obtener visibilidad de amenazas en el tráfico de su red
- analizar sesiones de amenazas para mejorar la precisión de sus reglas de políticas
- obtener información sobre las amenazas en tiempo real detectadas por el análisis en línea de la nube
- obtener contexto sobre la amenaza a partir de logs e informes en la nube y usar estos datos para mejorar su proceso de respuesta a incidentes.

Panel de Advanced Threat Prevention: Descripción general de amenazas

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro Las otras licencias y requisitos previos necesarios para la visibilidad son: ❑ Un rol que tiene permiso para ver el panel ❑ Prevención de amenazas o Advanced Threat Prevention → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

- Haga clic en **Strata Cloud Manager** > **Dashboards (Paneles)** > **More Dashboards (Más paneles)** > **Advanced Threat Prevention** para visualizar el panel.

Compare la diferencia entre las amenazas permitidas y bloqueadas por las reglas de seguridad.

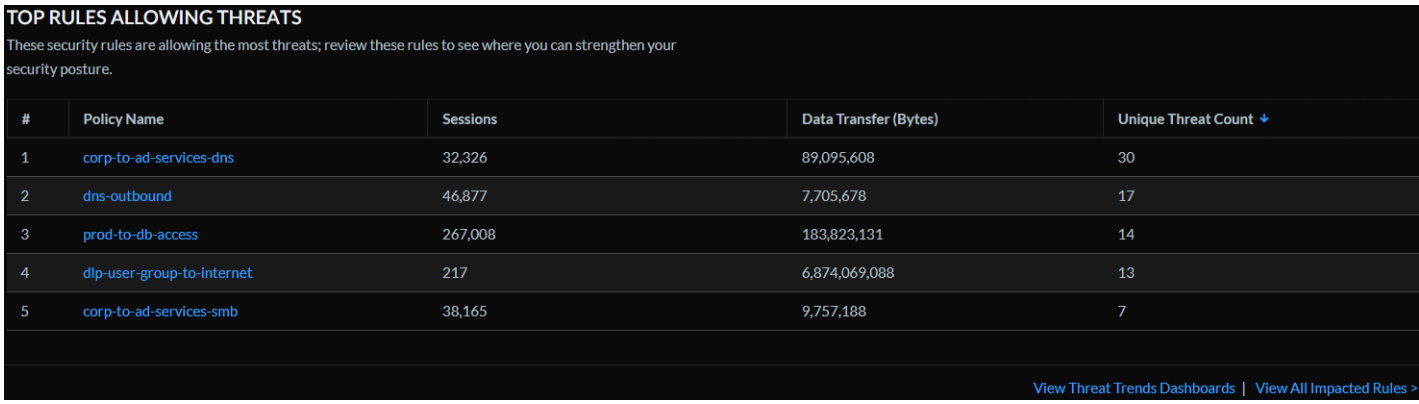


Panel de Advanced Threat Prevention: Principales reglas que permiten amenazas

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro Las otras licencias y requisitos previos necesarios para la visibilidad son: ❑ Un rol que tiene permiso para ver el panel ❑ Prevención de amenazas o Advanced Threat Prevention → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

- Haga clic en **Strata Cloud Manager** > **Dashboards (Paneles)** > **More Dashboards (Más paneles)** > **Advanced Threat Prevention** para visualizar el panel.

Examine las sesiones de amenazas que coincidan con la regla de la política de seguridad y vea si necesita modificar la regla para fortalecer su postura de seguridad. Puede analizar más a fondo las amenazas y las reglas coincidentes en Activity Insights.



Columna	Description (Descripción)
Nombre de la política	La regla de política de seguridad que está permitiendo las amenazas correspondientes.
Sesiones	El número de sesiones de amenazas que coinciden con la regla de la política de seguridad.
Transferencia de datos (bytes)	La cantidad de datos que fluyó a través de las sesiones que coincidió con la regla de la política de seguridad.
Recuento de amenazas únicas	El número de amenazas que coincidían con la regla de la política de seguridad.

Panel de Advanced Threat Prevention: Hosts que generan tráfico C2 detectado en la nube

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro Las otras licencias y requisitos previos necesarios para la visibilidad son: ☐ Un rol que tiene permiso para ver el panel

¿Dónde puedo usar esto?	¿Qué necesito?
	☐ Prevención de amenazas o Advanced Threat Prevention → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

- Haga clic en **Strata Cloud Manager** > **Dashboards (Paneles)** > **More Dashboards (Más paneles)** > **Advanced Threat Prevention** para visualizar el panel.

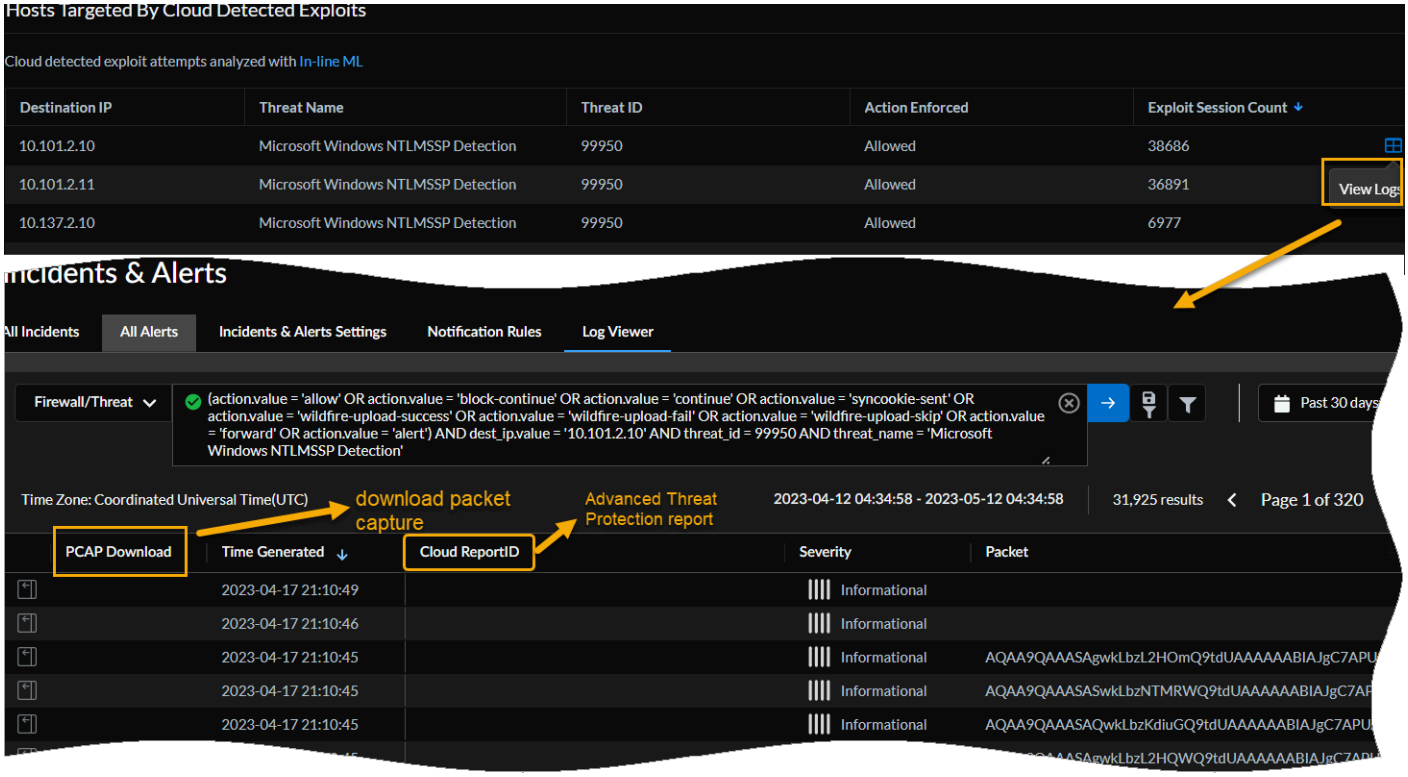
Examine las IPs de origen y los usuarios responsables de generar tráfico de comando y control (C2). Advanced Threat Prevention utiliza motores basados en la nube y análisis en línea en nube para detectar y analizar el tráfico en busca de C2 desconocido y vulnerabilidades. Haga clic en el icono de búsqueda junto a la IP de origen para revisar los patrones de uso relacionados con la IP de origen. Un enlace contextual al Visor de logs ayuda a analizar las sesiones de amenazas, descargar la captura de paquetes y el informe en la nube para obtener contexto adicional y aprovechar los datos de análisis de amenazas de Palo Alto Networks y mejorar sus procesos de respuesta a incidentes.

Panel de Advanced Threat Prevention: Hosts a los que se dirigen los exploits detectados en la nube

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro Las otras licencias y requisitos previos necesarios para la visibilidad son: ☐ Un rol que tiene permiso para ver el panel ☐ Prevención de amenazas o Advanced Threat Prevention → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

- Haga clic en **Strata Cloud Manager** > **Dashboards (Paneles)** > **More Dashboards (Más paneles)** > **Advanced Threat Prevention** para visualizar el panel.

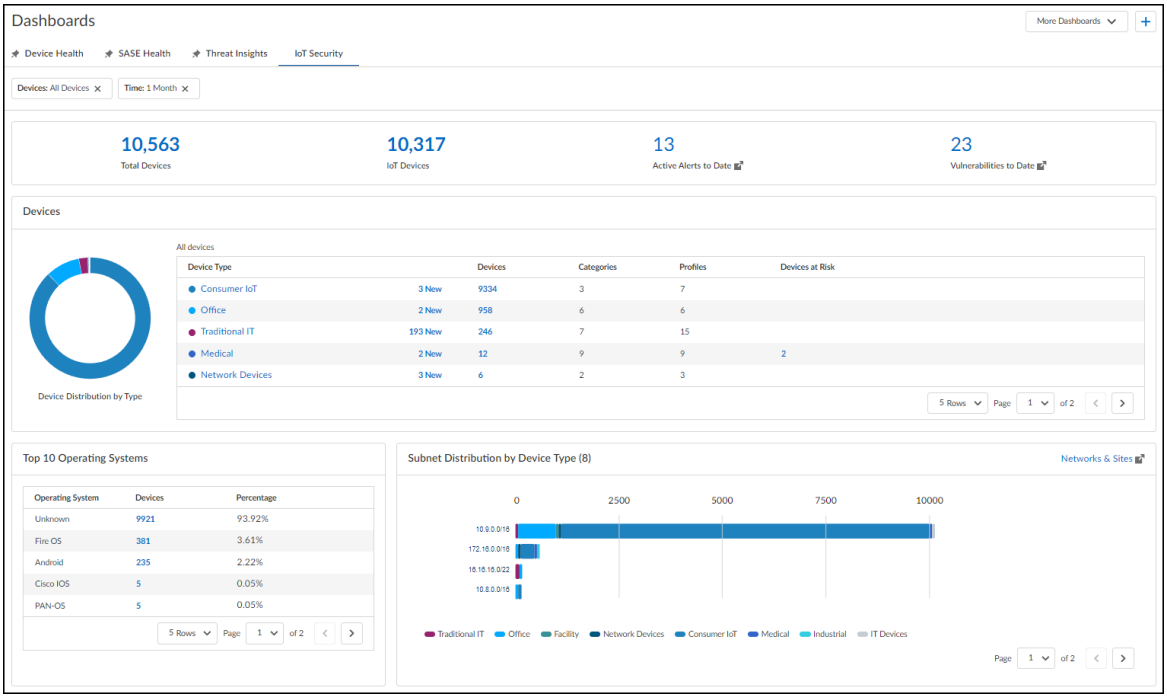
Estas son las IP a las que se dirigen los exploits de vulnerabilidad. Advanced Threat Prevention utiliza motores basados en la nube y análisis en línea en la nube para detectar y analizar este tráfico. Pase el cursor sobre la dirección IP de destino y haga clic en el icono de búsqueda para revisar los patrones de uso relacionados con la IP de destino. Vea los logs para obtener contexto alrededor de la amenaza. Descargue el informe en la nube y la captura de paquetes de los logs para obtener contexto adicional y utilice los datos analíticos de amenazas de Palo Alto Networks y la inteligencia de amenazas para mejorar sus procesos de respuesta a incidentes.



Panel: IoT Security (Seguridad de IoT)

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro Las otras licencias y requisitos previos necesarios para la visibilidad son: ☐ Un rol que tiene permiso para ver el panel ☐ IoT Security → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Para comenzar, seleccione **Dashboards (Paneles)** > **More Dashboards (Más paneles)** > **IoT Security**.



¿Qué le muestra este panel?

El panel de IoT Security proporciona información sobre los dispositivos en la red, sus perfiles de dispositivos y sistemas operativos, y cómo se distribuyen por tipo de dispositivo en las subredes. Para productos de IoT Security avanzados (IoT Security Enterprise Plus, Industrial IoT Security o Medical IoT Security), el panel de IoT Security también muestra el número total de alertas activas hasta la fecha y las vulnerabilidades hasta la fecha.

El texto en color azul es interactivo. Esto es lo que sucede cuando hace clic:

- Resumen (en la parte superior): el **Total Devices (Número total de dispositivos)** y **IoT Devices (Dispositivos IoT)** se vinculan a la página **Monitor (Supervisar)** > **Assets (Activos)** con filtros aplicados para mostrar el inventario de todos los dispositivos o todos los dispositivos IoT. El texto en azul para Alertas activas hasta la fecha y Vulnerabilidades activas hasta la fecha abre las páginas correspondientes en su portal de IoT Security. (Cuando no hay alertas ni vulnerabilidades, el número es 0 y no hay ningún vínculo).
- Dispositivos: haga clic en una sección del gráfico o en una entrada de la columna Tipo de dispositivo para hacer zoom y ver las categorías de dispositivos dentro de un tipo elegido, y desde allí para ver los perfiles de dispositivos dentro de una categoría elegida. Al hacer clic en**back (volver)** dentro del gráfico o hacer clic en la ruta de navegación sobre la tabla, se vuelve a un nivel más amplio de clasificación de dispositivos.

  Los números en las columnas Dispositivos y Dispositivos en riesgo se vinculan a la página **Monitor (Supervisar)** > **Assets (Activos)**. Strata Cloud Manager aplica automáticamente un filtro para mostrar los dispositivos que coinciden con la columna y fila elegidas, que puede ser Tipo de dispositivo, Nombre de categoría o Nombre de perfil según el nivel actual en pantalla.

  A veces ve los números de nuevos dispositivos que IoT Security detecta en la red. Estos números aparecen a la izquierda de los números en la columna Dispositivos. IoT Security considera que los dispositivos son "Nuevos" si los detecta por primera vez en la red dentro del filtro de tiempo establecido en la parte superior del panel.
- Los 10 principales sistemas operativos: los números en la columna Dispositivos se vinculan a la página **Monitor (Supervisar)** > **Assets (Activos)** con un filtro aplicado para mostrar solo los dispositivos con el sistema operativo elegido.
- Distribución de subred por tipo de dispositivo: pase el cursor sobre la barra de una subred para ver el número de dispositivos agrupados por tipo de dispositivo que hay en la subred. Esta información le ayudará a decidir si hay demasiados tipos de dispositivos no relacionados mezclados en la misma subred. Por ejemplo, si ve dispositivos IoT de instalaciones industriales, de consumo y de servicios públicos en una subred, es posible que desee segmentar los dispositivos de cada tipo en sus propias subredes independientes. Al hacer clic en **Networks & Sites (Redes y sitios)**, se abre una nueva ventana del navegador y se abre **Networks (Redes)** > **Networks and Sites (Redes y sitios)** > , **Networks (Redes)** en el portal de IoT Security.

¿Cómo puede utilizar los datos de este panel?

Utilice los datos de este panel para obtener más información sobre los dispositivos de su red:

Filters (Filtros) (en la parte superior de la página)

- Filtre los datos que se muestran en el panel por tipo de dispositivo y período de tiempo (último año, mes, semana, día u hora) para ver datos sobre los dispositivos de interés.

Summary (Resumen) (en la parte superior del panel de control)

- Vea el número total de dispositivos que han estado activos en su red según lo determinado por el tipo de dispositivo y los filtros de tiempo.
- Del número total de dispositivos activos, vea cuántos son específicamente dispositivos IoT.
- Desarrolle una idea del panorama de seguridad en el que operan los dispositivos al ver la cantidad de alertas activas y vulnerabilidades detectadas hasta la fecha.

Dispositivos

- Conozca cuántos dispositivos hay entre varios tipos de dispositivos y profundice para saber cuántos dispositivos hay entre varias categorías de dispositivos y luego entre varios perfiles de dispositivos. Descubra cuántos dispositivos de riesgo crítico hay en cada nivel cada vez más granular de clasificación de dispositivos y qué tipo de dispositivos son.

Los 10 sistemas operativos principales

- De todos los dispositivos cuyo sistema operativo IoT Security ha detectado, vea los 10 sistemas operativos más comunes, cuántos dispositivos usan cada uno y cuál es ese porcentaje.

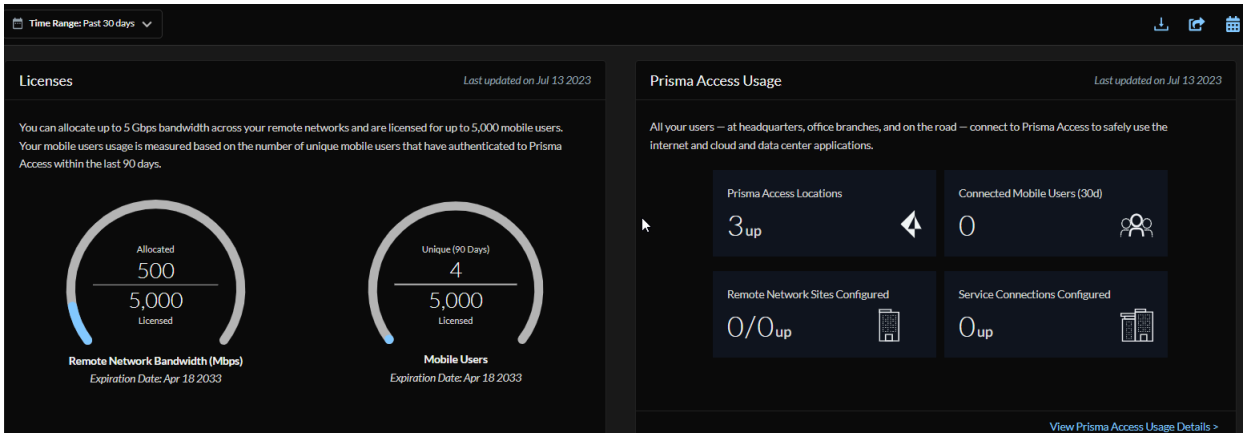
Distribución de subredes por tipo de dispositivo

- Vea cómo se distribuyen los diferentes tipos de dispositivos en subredes a lo largo de la red. Si ve una gran combinación de tipos de dispositivos en la misma subred, plantéese segmentarlos en sus propias subredes separadas.

Panel: Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	Uno de estos: ☐ Licencia de Prisma Access ☐ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

- Haga clic en **Strata Cloud Manager** > **Dashboards (Paneles)** > **More dashboards (Más paneles)** > **Prisma Access** para empezar.



¿Qué le muestra este panel?

Vea cómo aprovechar lo que tiene disponible con su licencia y obtenga una visión general del estado y el rendimiento de su entorno de Prisma Access.

Los datos de uso de Prisma Access incluyen:

- Una descripción general de su uso de Prisma Access: sus licencias, ubicaciones de Prisma Access y capacidad de usuarios móviles y/o utilización del ancho de banda
- Las mejores ubicaciones de Prisma Access para usuarios móviles y redes remotas
- Consumo general de ancho de banda para sitios de conexión de red y servicio remotos, y los sitios de conexión de red y servicio remotos de mayor consumo
- Tendencias de desconexión de túneles, incluidos los túneles más afectados

El panel muestra los datos agregados por inquilino de Prisma Access.

Este panel admite informes. Estos iconos,  en la parte superior derecha de un panel, indican qué los informes son compatibles con este panel. Puede compartir, descargar y programar informes que cubran los datos que muestra este panel.

¿Cómo puede utilizar los datos del panel de control?

Este panel ayuda a obtener visibilidad del uso de Prisma Access en su red y a ajustar los parámetros de configuración en función de los datos del panel.

Panel: Experiencia de aplicación

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)*	❑ Licencia de Prisma Access ❑ Licencia de ADEM Observability para ver los datos de las aplicaciones supervisadas ❑ Licencia de redes remotas *(Necesario para ver los datos de experiencia de sitios remotos)*

- Haga clic en **Strata Cloud Manager** > **Dashboards (Paneles)** > **More Dashboards (Más paneles)** > **Application Experience (Experiencia de aplicación)** para empezar.

¿Qué le muestra este panel?

Los datos que se muestran en este panel cambiarán y corresponderán a la tarjeta que seleccione: Experiencia del usuario móvil o Experiencia del sitio remoto. Si es nuevo en AI-Powered ADEM, es posible que desee comenzar por realizar una encuesta de las aplicaciones que se utilizan en toda su organización y utilizar esta información para identificar para qué aplicaciones quiere crear pruebas de aplicaciones. Además, si tiene usuarios o sitios remotos que informan acerca de problemas con las aplicaciones, este panel es un buen lugar para comenzar a aislar el problema. Los datos de uso de la aplicación se extraen del tráfico de usuario real que atraviesa Prisma Access. Incluye el tráfico de usuarios móviles y sitios remotos.

Puede añadir un filtro para reducir los resultados y mostrar datos solo para aplicaciones específicas, tipo de implementación, puntuación de experiencia, usuarios móviles, grupos o ubicaciones de Prisma Access. Vea la puntuación de la experiencia individual de la aplicación y el número de usuarios y sitios remotos que se están viendo afectados por cualquier problema de rendimiento existente.

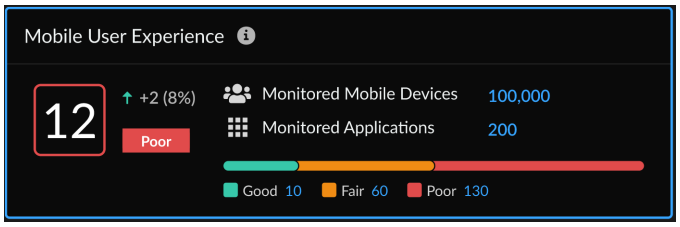
¿Cómo puede utilizar los datos del panel de control?

Una vez que haya encuestado las aplicaciones que se ejecutan en su red y determinado qué aplicaciones quiere supervisar, puede crear una prueba de aplicación. A medida que crea pruebas de aplicaciones, tenga en cuenta que, aunque puede crear pruebas de aplicaciones dirigidas a varios usuarios o sitios, el número de pruebas se basa en el número de pruebas de aplicaciones que realiza cada usuario individual o dispositivo ION (por ejemplo, si tiene una prueba de aplicaciones para Slack y la dirige a 1000 usuarios, esto contaría en su licencia como 1000 pruebas).

Panel de experiencia de aplicación: Tarjeta de experiencia de usuario móvil

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)*	❑ Licencia de Prisma Access ❑ Licencia de ADEM Observability para ver los datos de **Monitored Applications (Aplicaciones supervisadas)**

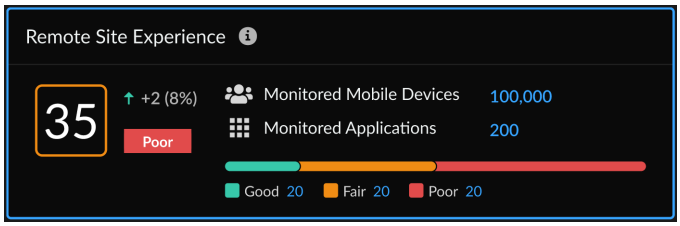
Este widget muestra el promedio de la puntuación del segmento de aplicación para todos los usuarios móviles para todas las aplicaciones supervisadas. También muestra un desglose de las experiencias buenas, aceptables y deficientes por número de dispositivos de usuario. Puede explorar en profundidad a los usuarios que experimentan un rendimiento regular o deficiente para comenzar a investigar. La puntuación de experiencia de esta tarjeta le dará una indicación de la experiencia digital general del usuario. Para cada aplicación que se supervisa por usuario móvil, ADEM calcula una puntuación basada en las 5 métricas críticas: disponibilidad de la aplicación, tiempo de resolución DNS, tiempo de conexión TCP, tiempo de conexión SSL y latencia HTTP. Si la aplicación no supera la prueba de disponibilidad (la aplicación no está disponible), la puntuación de experiencia es 0. Si se puede acceder a la aplicación, solo entonces se calcularán las cuatro métricas restantes. Cada una de las métricas anteriores (aparte de la accesibilidad de la aplicación) tiene una ponderación y umbrales inferior y superior de referencia diferentes, y su ponderación combinada es igual a 100. La suma de estas puntuaciones de métricas individuales determina la puntuación de la experiencia de la aplicación para un usuario. Un promedio de todos los resultados de la muestra de prueba para cada aplicación determina la puntuación de experiencia de un usuario.



Panel de experiencia de aplicación: Tarjeta de experiencia de sitio remoto

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)*	❑ Licencia de Prisma Access ❑ Licencia de ADEM Observability para ver los datos de **Monitored Applications (Aplicaciones supervisadas)** ❑ Licencia de redes remotas

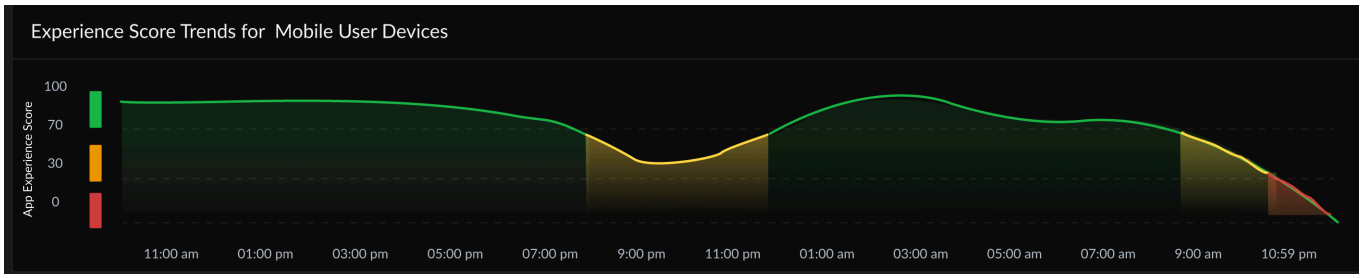
La puntuación de la experiencia del sitio remoto es una puntuación media de todas las aplicaciones supervisadas en todas las rutas de acceso WAN activas. Es un promedio de todos los resultados de muestras de prueba que se recopilan de aplicaciones individuales supervisadas para ese sitio remoto. Es la puntuación general de la experiencia (contenido en un cuadrado codificado por colores) del sitio remoto o sucursal, que es un promedio de las puntuaciones de experiencia de todas las muestras de prueba recopiladas en las rutas activas de todas las aplicaciones supervisadas para ese sitio. Aunque la puntuación de experiencia de cada ruta de copia de seguridad se calculará individualmente y estará disponible para cada sitio y aplicación remotos, la puntuación de experiencia de las rutas de copia de seguridad no se tiene en cuenta al calcular la puntuación de experiencia de un sitio remoto. Puede profundizar en los sitios que experimentan un rendimiento regular o deficiente haciendo clic en el número junto a Regular o Deficiente.



Panel de experiencia de aplicación: Tendencias de la puntuación de la experiencia

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)*	❑ Licencia de Prisma Access ❑ Licencia de ADEM Observability para ver los datos de **Monitored Applications (Aplicaciones supervisadas)**

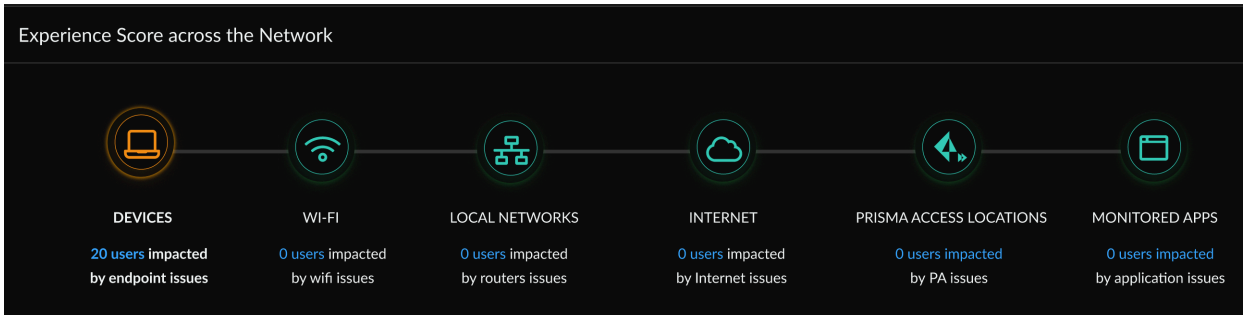
Este widget muestra un gráfico de series de tiempo de la experiencia promedio de todos los usuarios móviles. La puntuación de experiencia se calcula y se muestra a intervalos establecidos durante el rango de tiempo seleccionado. El eje y está codificado por colores según el rango de puntuación para mostrarle la calidad de su puntuación de experiencia (Rojo = Deficiente, Amarillo = Regular y Verde = Buena). Pase el cursor del ratón sobre la línea de tendencia para ver la puntuación de experiencia en el momento en el que se coloca el cursor.



Panel de experiencia de aplicación: Puntuación de experiencia en toda la red

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)*	❑ Licencia de Prisma Access ❑ Licencia de ADEM Observability para ver los datos de **Monitored Applications (Aplicaciones supervisadas)**

Identifique el segmento de la red que podría estar causando problemas dentro de su organización desde los endpoints (para usuarios móviles) o la sucursal (sitios remotos) hasta las aplicaciones. Puede ver qué segmento de la red podría estar causando problemas dentro de su organización desde los endpoints y los sitios remotos de Prisma SD-WAN hasta la aplicación. Puede ver qué segmento, como una interrupción de ISP o de ubicación informática o una interrupción de una aplicación SaaS, está afectando la experiencia digital dentro de su organización y también el número preciso de usuarios o sitios que se ven afectados por ella. Los iconos están codificados por colores y se basan en el promedio de la puntuación de estado del segmento para todos los usuarios móviles. Un icono verde representa Buena (puntuación es >=70), amarillo representa Regular (puntuación es 30-70), rojo representa Deficiente (puntuación <30).



Dispositivos: métricas de estado del dispositivo (CPU/memoria/espacio en disco/cola de disco/batería)

Wi-Fi: métricas WIFI (calidad de señal, Tx, Rx, SSID, BSSID, canal)

Redes locales: métricas de rendimiento de red (latencia/pérdida/fluctuación)

Internet: métricas de rendimiento de red (latencia/pérdida/fluctuación) si un dispositivo no está conectado a GlobalProtect, el segmento de Internet, las métricas de rendimiento de red serán las mismas que la prueba ping de TCP ejecutada para el segmento de aplicación.

Ubicaciones de Prisma Access: métricas de rendimiento de red (latencia/pérdida/fluctuación). La prueba para este segmento no se ejecuta si el dispositivo no está conectado a GlobalProtect.

Aplicaciones supervisadas: métricas de rendimiento de red (latencia/pérdida/fluctuaciones), métricas de rendimiento de aplicaciones (disponibilidad, búsqueda DNS, TCP Connect, SSL Connect, latencia HTTP, tiempo hasta el primer byte,tiempo hasta el último byte,transferencia de datos)

Panel de experiencia de aplicación: Distribución global de las puntuaciones de la experiencia de las aplicaciones

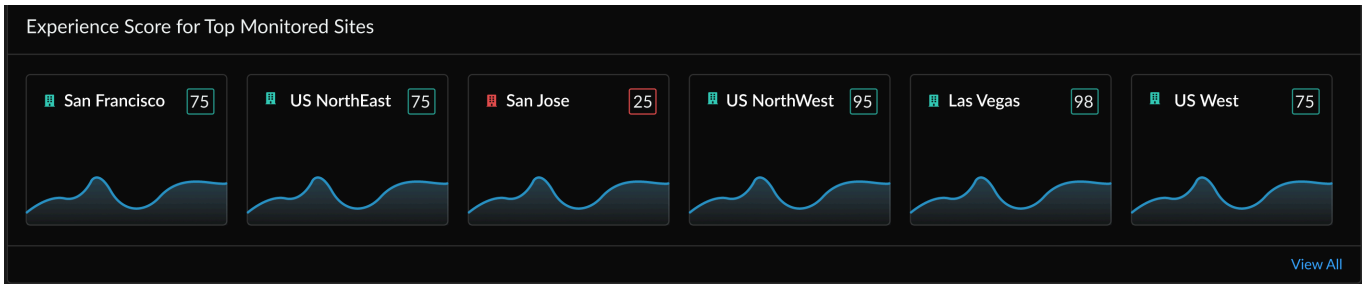
¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)*	❑ Licencia de Prisma Access ❑ Licencia de ADEM Observability para ver los datos de **Monitored Applications (Aplicaciones supervisadas)**

Dependiendo de la tarjeta que seleccione, la vista del mapa en este widget le muestra la experiencia de las ubicaciones de Prisma Access en función de la cantidad total de usuarios móviles y aplicaciones supervisadas o el número total de sitios remotos y aplicaciones supervisadas en una ubicación de Prisma Access específica. Las ubicaciones de Prisma Access están marcadas con círculos codificados por colores para representar el estado de los puntuaciones del segmento de aplicación de todos los usuarios móviles supervisados y los sitios remotos conectados a esa ubicación de Prisma Access específica donde aparece el círculo. Pase el cursor del ratón sobre un círculo para ver los puntuaciones de experiencia para la ubicación, así como la cantidad total de dispositivos de usuario móvil o sitios remotos supervisados y el número total de aplicaciones que se supervisan para esa ubicación. Varias ubicaciones que están geográficamente muy cerca una de otra se representan mediante un círculo con un número dentro. El número indica cuántas ubicaciones se agruparon en esa zona. Para ver exactamente qué ubicaciones se agruparon, amplíe el mapa.

Panel de experiencia de aplicación: Puntuación de experiencia para los sitios más supervisados

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)*	❑ Licencia de Prisma Access ❑ Licencia de ADEM Observability para ver los datos de **Monitored Applications (Aplicaciones supervisadas)**

Este widget muestra una tarjeta por aplicación y muestra los sitios con las puntuaciones más altas. Este widget muestra la tendencia de la puntuación de experiencia de los sitios remotos durante el rango de tiempo seleccionado. Pase el cursor del ratón sobre la línea de tendencia para ver la puntuación de experiencia para ese punto específico en el tiempo.

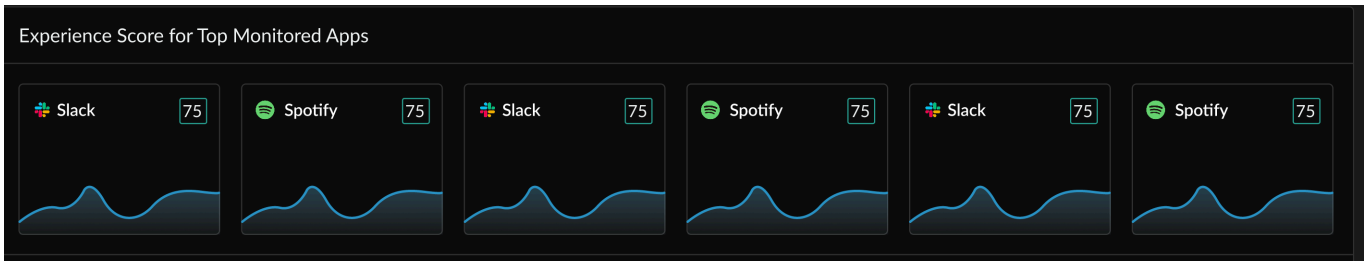


Panel de experiencia de aplicación: Puntuación de experiencia para las principales aplicaciones supervisadas

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)*	❑ Licencia de Prisma Access ❑ Licencia de ADEM Observability para ver los datos de **Monitored Applications (Aplicaciones supervisadas)**

Cada tarjeta de aplicación le muestra la puntuación promedio del segmento de aplicación (el número incluido en el cuadrado) para todos los usuarios móviles supervisados para esa aplicación en particular en el sitio remoto. La puntuación de experiencia se calcula como un promedio de las puntuaciones de experiencia de la aplicación de todas las aplicaciones supervisadas. La puntuación de experiencia representa la experiencia de extremo a extremo para las rutas activas de la aplicación. Es la media de todas las muestras de ensayo recogidas en las vías activas sólo para esa aplicación específica. La línea de tendencia muestra el promedio de todas las muestras de datos de APM de 5 minutos para el marco de tiempo seleccionado.

Puede ver cuántas aplicaciones está supervisando y también cuántas rutas activas y de respaldo se supervisan. Cada tarjeta de solicitud muestra el número de rutas que se ven afectadas. Haga clic en una tarjeta de aplicación para ver las métricas de esa aplicación específica.

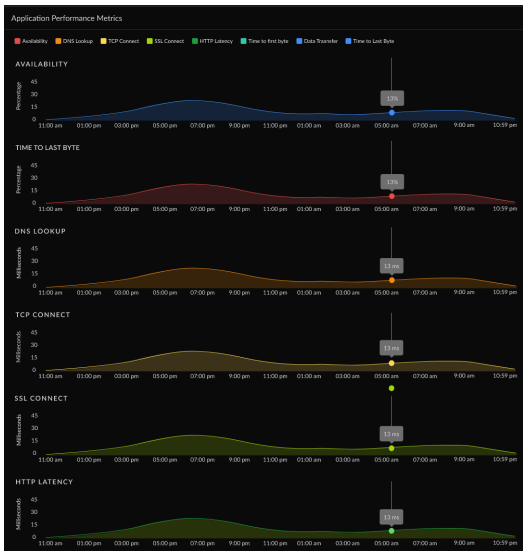


Panel de experiencia de aplicación: Métricas de rendimiento de las aplicaciones

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)*	❑ Licencia de Prisma Access ❑ Licencia de ADEM Observability para ver los datos de **Monitored Applications (Aplicaciones supervisadas)**

Autonomous DEM utiliza TCP ping y Curl para determinar el rendimiento de la aplicación de un extremo a otro.

Métrica	Description (Descripción)
Disponibilidad	Disponibilidad de la aplicación (en porcentaje) durante el **Time Range (Rango de tiempo)**.
Búsqueda de DNS	Tiempo de resolución de DNS.
Conexión TCP	Tiempo que se tarda en establecer una conexión TCP.
Conexión SSL	Tiempo que se tarda en establecer una conexión SSL.
Latencia HTTP	Tiempo que se tarda en establecer una conexión HTTP.
Tiempo hasta el primer byte	El total de la búsqueda de DNS, la conexión TCP, la conexión SSL y el tiempo de latencia HTTP da como resultado el tiempo hasta el primer byte.
Transferencia de datos	Tiempo total que se tarda en transferir la totalidad de los datos.
Tiempo hasta el último byte	Tiempo hasta el primer byte + tiempo de transferencia de datos.

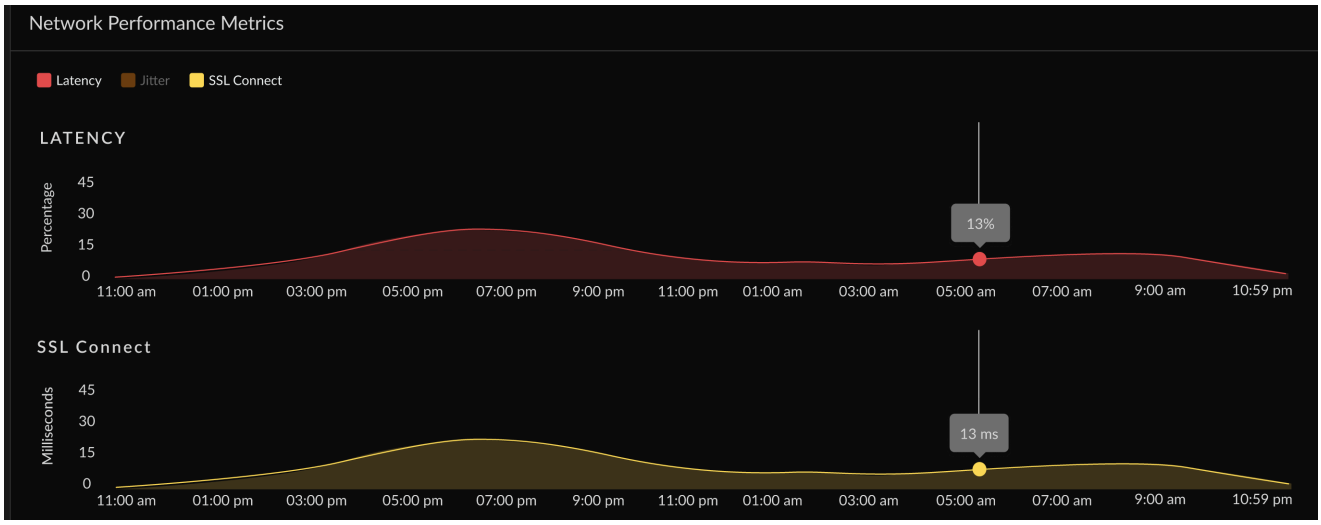


Panel de experiencia de aplicación: Métricas de rendimiento de la red

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)*	❑ Licencia de Prisma Access ❑ Licencia de ADEM Observability para ver los datos de **Monitored Applications (Aplicaciones supervisadas)**

ADEM utiliza pings ICMP para determinar el rendimiento de la red en cada segmento.

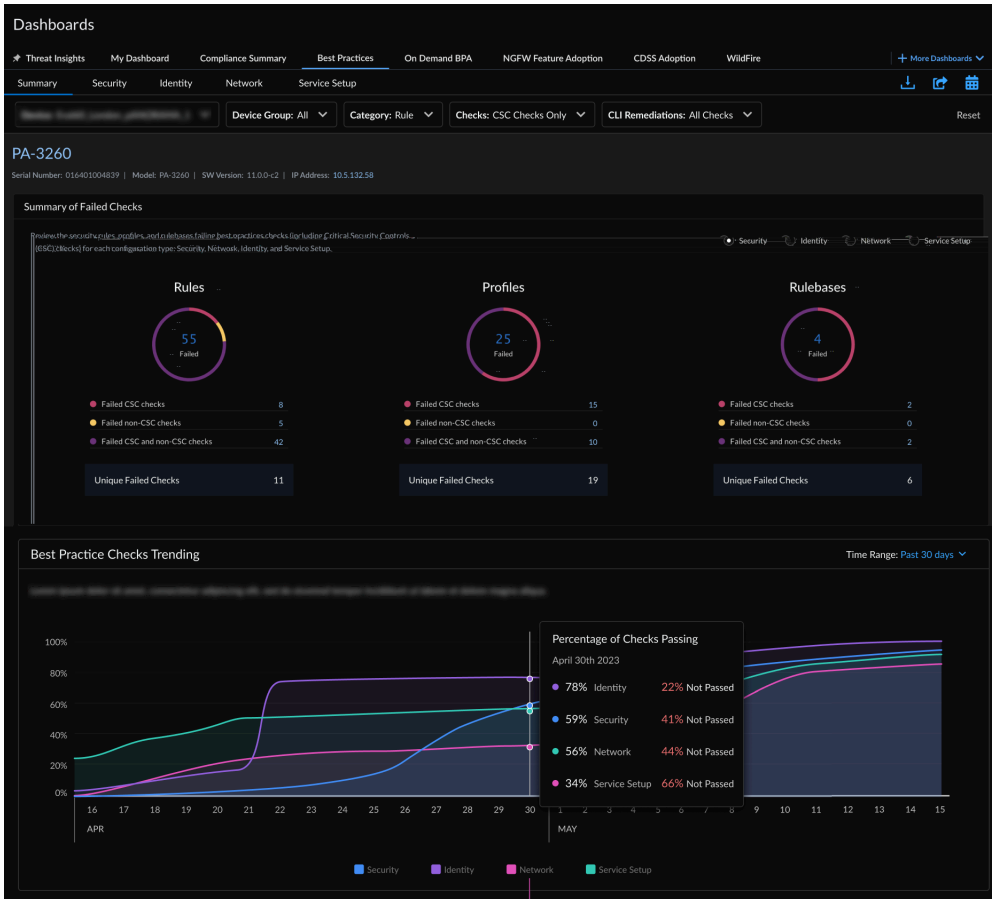
Métrica	Description (Descripción)
Disponibilidad	Métricas de disponibilidad de la red durante el **Time Range (Intervalo de tiempo)**.
Latencia de red	Tiempo necesario para transferir los datos a través de la red.
Pérdida de paquetes	Pérdida de paquetes durante la transmisión de datos.
Vibración	Cambio en la latencia durante el **Time Range (Intervalo de tiempo)**.



Panel: Prácticas recomendadas

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ☐ Prisma Access ☐ AIOps for NGFW Premium ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

- Haga clic en **Strata Cloud Manager** > **Dashboards (Paneles)** > **More Dashboards (Más paneles)** > **Best Practices (Prácticas recomendadas)** para empezar.



¿Qué le muestra este panel?

El panel muestra los datos añadidos por Prisma Access y NGFW/Panorama asociados con su inquilino.

El panel de prácticas recomendadas mide su postura de seguridad en comparación con la guía de prácticas recomendadas de Palo Alto Networks. Es importante destacar que la evaluación de las prácticas recomendadas incluye verificaciones para los controles de seguridad críticos (CSC) del Centro de Seguridad en Internet. Los controles CSC se miran por separado de otros controles de prácticas recomendadas, por lo que puede seleccionar y priorizar fácilmente las actualizaciones que lo llevarán al cumplimiento de CSC.

El panel de prácticas recomendadas se divide en cinco secciones:

- **Resumen**

  Le da una visión completa de todas las comprobaciones que han fallado para un dispositivo en todos los tipos de configuración (Seguridad, Red, Identidad y Configuración de servicios). Le permite vea gráficos de tendencias históricos para las comprobaciones de BPA y evaluar su tasa de adopción de prácticas recomendadas para áreas de características clave.

- **Seguridad**

  Muestra las reglas, bases de reglas o perfiles que no superan las prácticas recomendadas y las comprobaciones CSC para el dispositivo y la ubicación seleccionados. Cuando esté disponible, las correcciones de la CLI le permiten resolver problemas con las reglas de su política. Las correcciones de la CLI se generan con los datos de TSF que usted carga al generar un informe de BPA bajo demanda.

  - **Bases de reglas**

    Mire cómo está organizada su política y si los ajustes de configuración que se aplican en muchas reglas se ajustan a las prácticas recomendadas (incluidas las comprobaciones de CSC).

  - **Reglas**

    Le muestra las reglas que fallan las prácticas recomendadas y las comprobaciones CSC. Vea dónde puede tomar medidas rápidas para corregir las comprobaciones fallidas. Las reglas se ordenan en función del número de sesiones, por lo que puede comenzar revisando y actualizando las reglas que más están afectando al tráfico.

  - **Perfiles**

    Le muestra cómo se acumulan sus perfiles en comparación con las prácticas recomendadas, incluidas las comprobaciones CSC. Los perfiles realizan una inspección avanzada del tráfico que coincide con una regla de seguridad o descifrado.

- **Identidad**

  Muestra si la configuración de aplicación de autenticación (regla de autenticación, perfil de autenticación y portal de autenticación) para un dispositivo cumple con las prácticas recomendadas y las comprobaciones CSC.

- **Red**

  Comprueba si la aplicación anula las reglas y la configuración de red de acuerdo con las prácticas recomendadas y las comprobaciones CSC.

- **Configuración del servicio**

  Vea cómo las suscripciones que ha habilitado en sus dispositivos se alinean con las prácticas recomendadas y las comprobaciones CSC. Puede revisar la configuración de WildFire, las configuraciones del portal de GlobalProtect y la puerta de enlace de GlobalProtect aquí y corregir las comprobaciones con error.

Este panel admite informes. Estos iconos,  en la parte superior derecha de un panel, indican qué los informes son compatibles con este panel. Puede compartir, descargar y programar informes que cubran los datos que muestra este panel.

¿Cómo puede utilizar los datos del panel?

Si bien la orientación sobre las prácticas recomendadas tiene como objetivo ayudarle a reforzar su postura de seguridad, las conclusiones de este informe también pueden ayudarle a identificar áreas en las que puede realizar cambios para gestionar su entorno de manera más eficaz.

Panel: Resumen de cumplimiento

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW, incluidos los financiados por Créditos de NGFW de software	❑ AIOps for NGFW Premium o Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Puede ver un historial de cambios en las comprobaciones de seguridad realizadas hasta 12 meses en el pasado, agrupados por los marcos del Centro para la Seguridad de Internet (CIS) y el Instituto Nacional de Estándares y Tecnología (NIST). Para cada marco, verá una lista de controles, así como el porcentaje de la tasa de cumplimiento actual y promedio, el número total de comprobaciones de procedimientos recomendados y el número de comprobaciones fallidas para cada control.

Interactúe con el gráfico y la lista para ver la relación entre los controles y sus estadísticas históricas. Vea los detalles de los controles individuales y sus comprobaciones asociadas, y seleccione una comprobación de las mejores prácticas para ver la configuración del cortafuegos que está fallando la comprobación.

El marco de **los controles de seguridad críticos del CIS** es un conjunto priorizado de acciones recomendadas y prácticas recomendadas que ayudan a proteger a las organizaciones y sus datos de los vectores de ciberataque conocidos. Puede ver los resúmenes de comprobación de 11 de los 16 controles CIS básicos y fundamentales:

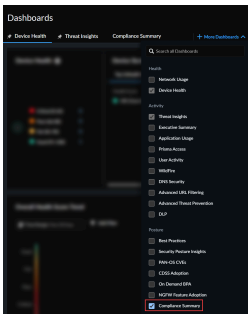
- CSC 3: Gestión continua de vulnerabilidades
- CSC 4: Uso controlado de privilegios administrativos
- CSC 6: Mantenimiento, supervisión y análisis de logs de auditoría
- CSC 7: Protecciones de correo electrónico y navegador web
- CSC 8: Defensas frente a malware
- CSC 9: Limitación y control de puertos, protocolos y servicios de red
- CSC 11: Configuración segura para dispositivos de red, como cortafuegos, enrutadores y conmutadores
- CSC 12: Defensa de borde
- CSC 13: Protección de datos
- CSC 14: Acceso controlado basado en la necesidad de saber
- CSC 16: Supervisión y control de cuentas

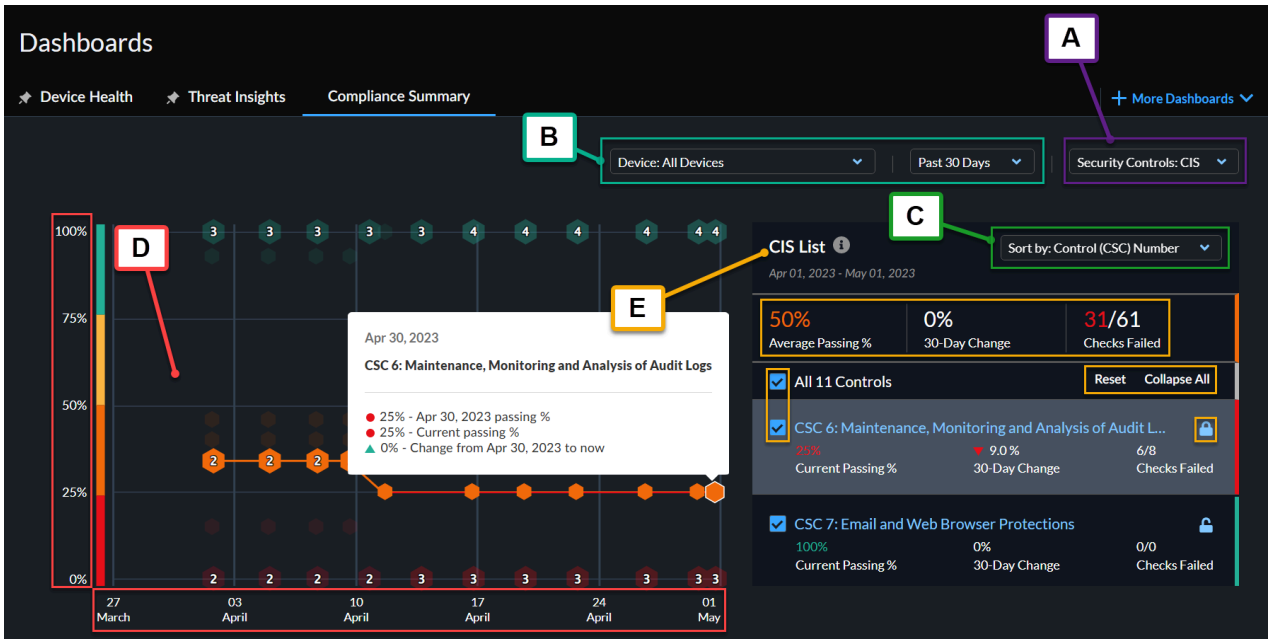
El marco de **Los controles SP 800-53 del Marco de Ciberseguridad del NIST** proporciona orientación a las agencias federales y otras organizaciones para implementar y mantener controles de seguridad y privacidad para sus sistemas de información. Puede ver resúmenes de comprobaciones de ocho familias de controles NIST:

- SC: Control de acceso
- AU: Auditoría y responsabilidad
- CM: gestión de la configuración
- CP: Planificación de contingencias
- IA: Identificación y autenticación
- RA: Evaluación de riesgos
- SC: Protección de sistemas y comunicaciones
- SI: Integridad del sistema y de la información

Para acceder al panel de resumen de cumplimiento, vaya a**Dashboards (Paneles)** y, a continuación, seleccione la pestaña **Resumen de cumplimiento** .

*Si no ve el **Resumen de cumplimiento** entre las opciones de pestaña, seleccione **Más paneles** y, a continuación, active la casilla de verificación **Resumen de cumplimiento** entre las opciones enumeradas en **Postura**.*





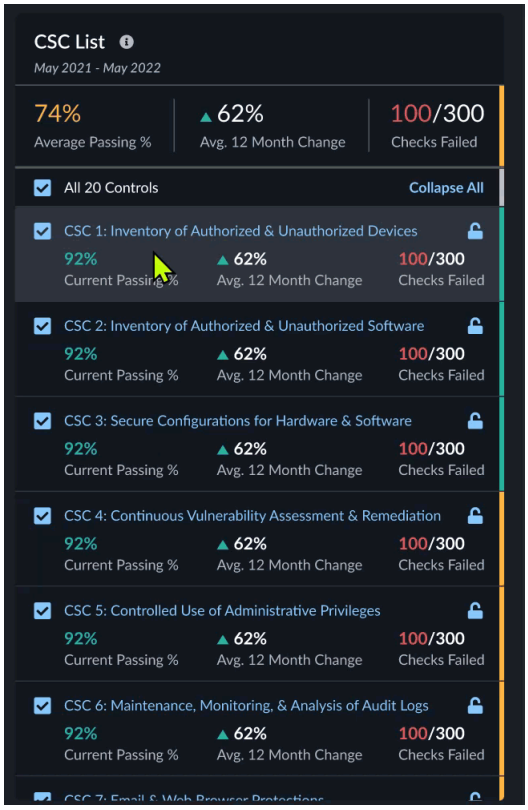
A) Selector de controles de seguridad	Seleccione controles CIS o NIST

B) Filtrar por	• Dispositivo
	• Período de tiempo
	  • Últimos 7 días
	  • Últimos 30 días
	  • Últimos 90 días
	  • Últimos 6 meses
	  • Últimos 12 meses

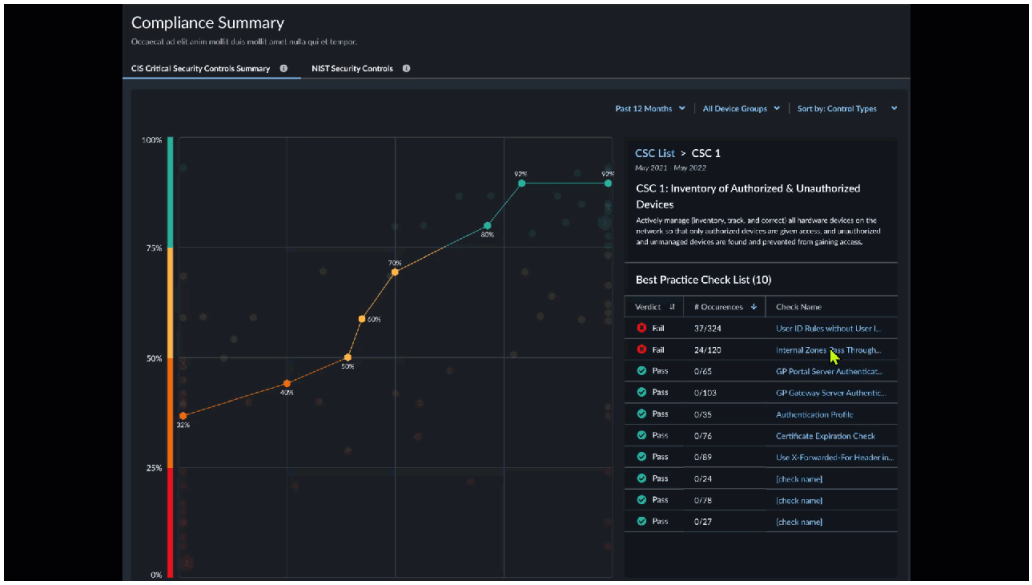
C) Ordenar por	• Número de CSC de control • % de aprobación actual • % de cambio • Número de comprobaciones fallidas
D) Gráfico de línea	• % de aprobación: muestra el porcentaje de aprobación para un tipo de comprobación específico. • Línea de tiempo: muestra cuándo se midió el porcentaje para un tipo de comprobación determinado.

E) Lista de comprobación	• Estadísticas
	  • % de aprobación promedio: muestra el porcentaje promedio de aprobación de las comprobaciones.
	  • Cambio de 12 meses: muestra el cambio durante un período de 12 meses.
	  • Comprobaciones fallidas: muestra el número de comprobaciones fallidas.
	• Controles seleccionados: una marca de verificación muestra un control en el gráfico de líneas.
	• Restablecer: elimina todos los bloqueos.
	• Contraer todo/expandir todo: muestra/oculta estadísticas en la lista.
	• Gráfico de línea de bloqueo: mantiene las comprobaciones bloqueadas a la vista en el gráfico de líneas.

- *Seleccione un control en la lista para ver las comprobaciones de prácticas recomendadas que incluye.*



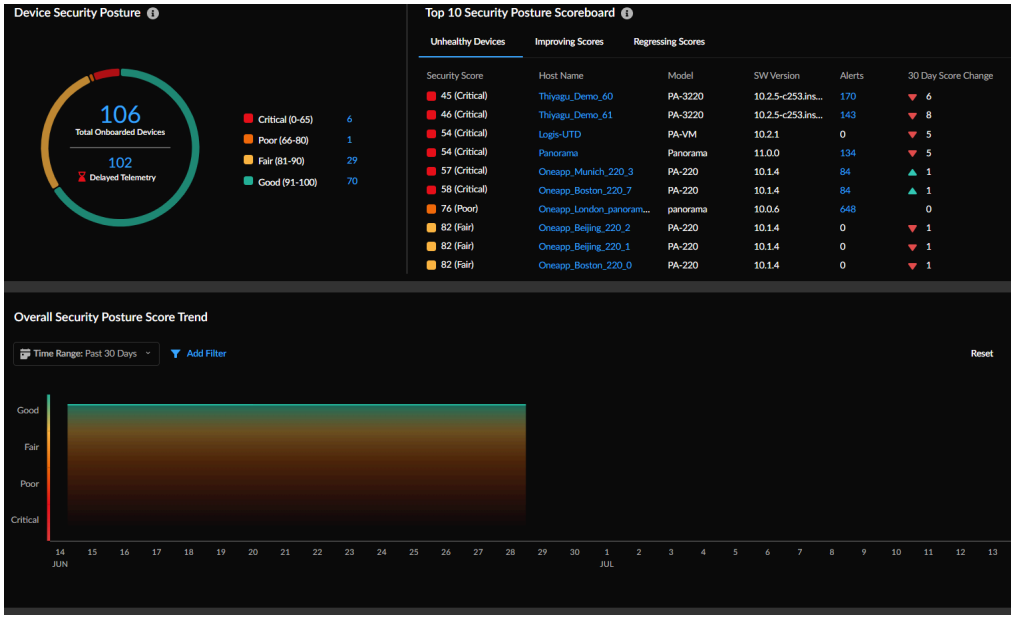
- *Seleccione una comprobación de prácticas recomendadas para ver la configuración del cortafuegos que está fallando la comprobación.*



Panel: Información sobre la postura de seguridad

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW, incluidos los financiados por Créditos de NGFW de software	☐ Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium o Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

- Haga clic en **Strata Cloud Manager** > **Dashboards (Paneles)** > **More Dashboards (Más paneles)** > **Security Posture Insights (Postura de seguridad de Insights)** para empezar.



¿Qué le muestra este panel?

El panel muestra los datos agregados de todos los cortafuegos asociados con su inquilino y también está enviando datos de telemetría.

Obtenga visibilidad del estado de seguridad y la tendencia de su implementación en función de las posturas de seguridad de los dispositivos NGFW integrados. La gravedad de la puntuación de seguridad (0-100) y su grado de seguridad correspondiente (bueno, regular, malo, crítico) determinan la postura de seguridad de un dispositivo. La puntuación de seguridad se calcula en función de la prioridad, la cantidad, el tipo y el estado de las alertas abiertas.

¿Cómo puede utilizar los datos del panel?

Utilice este panel para:

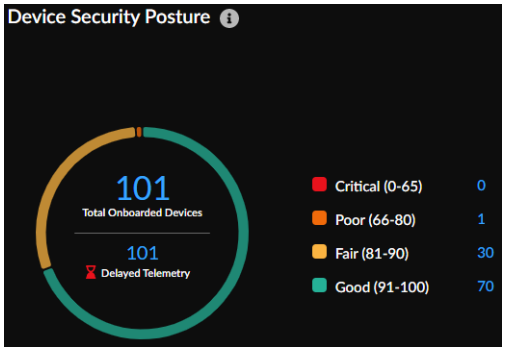
- Conozca la tendencia de problemas que afectan la postura de seguridad de su implementación.
- Comprender las mejoras de seguridad que ha realizado en su implementación mirando los datos históricos de puntuación de seguridad.
- Reducir los dispositivos donde exista la oportunidad de mejorar la postura de seguridad y dar prioridad a los problemas para resolverlos.

La funcionalidad de informe (descargar, compartir y programar informe) no es compatible con este panel.

Panel de Información de la postura de seguridad: Postura de seguridad del dispositivo

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW, incluidos los financiados por Créditos de NGFW de software	☐ Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium o Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

- Haga clic en **Strata Cloud Manager** > **Dashboards (Paneles)** > **More Dashboards (Más paneles)** > **Security Posture Insights (Postura de seguridad de Insights)** para ver el panel.



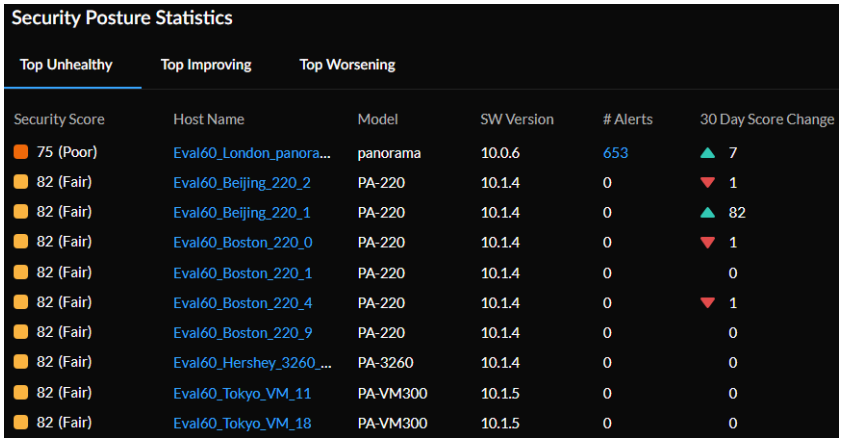
El widget del panel muestra:

- El número total de dispositivos NGFW incorporados.
- El número de dispositivos que no han enviado datos de telemetría durante más de 12 horas.
- La prioridad de la puntuación de seguridad para los dispositivos integrados en la implementación. Haga clic en el enlace del número para conocer los detalles del dispositivo y las estadísticas de seguridad.

Panel de Información de la postura de seguridad: Estadísticas de postura de seguridad

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW, incluidos los financiados por Créditos de NGFW de software	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium o Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

- Haga clic en **Strata Cloud Manager** > **Dashboards (Paneles)** > **More Dashboards (Más paneles)** > **Security Posture Insights (Postura de seguridad de Insights)** para ver el panel.



Principales dispositivos en mal estado

Estos son los 10 dispositivos que más afectan a la posición de seguridad de su implementación. Profundice para ver los detalles del dispositivo y las alertas en el dispositivo. Realice los pasos de corrección para que las alertas críticas en los dispositivos mejoren la postura de seguridad.

Principales dispositivos mejorando

Vea los 10 dispositivos principales con puntuaciones de posición de seguridad mejoradas durante un período de tiempo de 30 días, en comparación con las puntuaciones de seguridad actuales de los dispositivos.

Principales dispositivos empeorando

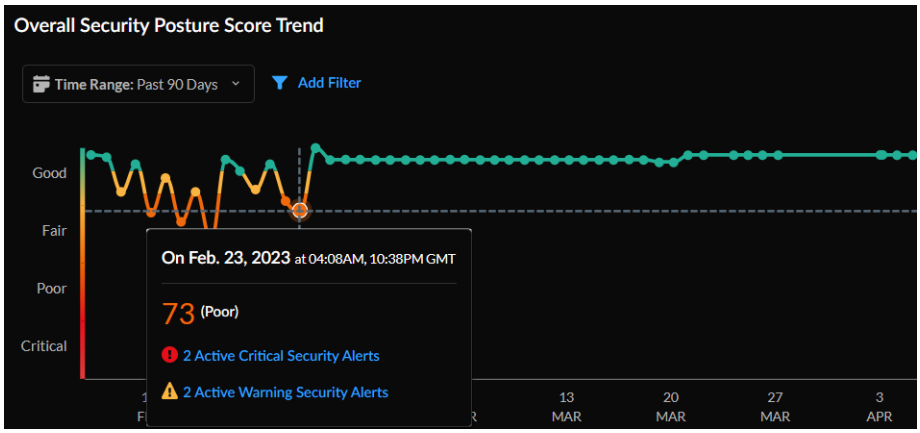
Estos son los dispositivos con las puntuaciones de posición de seguridad degradadas en comparación con las puntuaciones de seguridad actuales de los dispositivos. Revise las alertas en estos dispositivos y priorice para repararlos.

Panel de Información de la postura de seguridad: Tendencia de puntuación

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW, incluidos los financiados por Créditos de NGFW de software	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium o Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

- Haga clic en **Strata Cloud Manager** > **Dashboards (Paneles)** > **More Dashboards (Más paneles)** > **Security Posture Insights (Postura de seguridad de Insights)** para ver el panel.

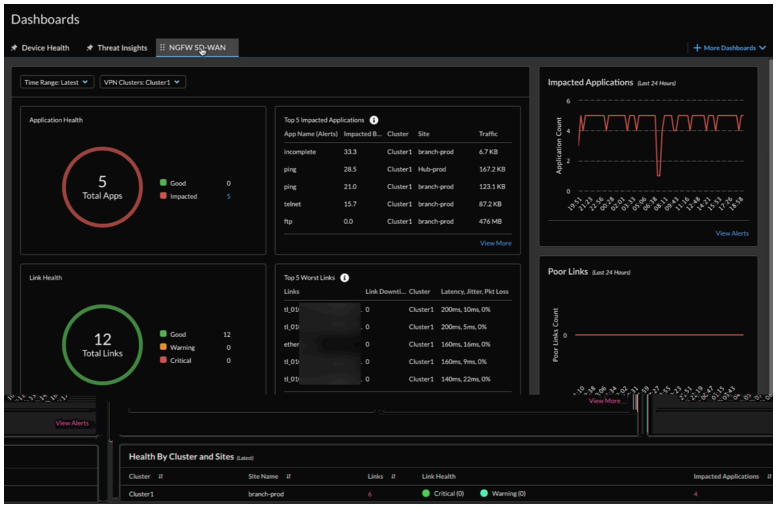
El gráfico muestra la tendencia de la postura de seguridad de la implementación durante el período de tiempo seleccionado. Coloque el cursor sobre el punto de activación para conocer los dispositivos y las alertas activas que contribuyen a la tendencia de la postura de seguridad. Puede ver las tendencias de uno o más dispositivos filtrados por el nombre de host, el modelo o la versión de software.



Panel: NGFW SD-WAN

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW, incluidos los financiados por Créditos de NGFW de software	☐ AIOps for NGFW Premium o Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

- Haga clic en **Dashboards > More Dashboards > NGFW SD-WAN (Paneles > Más paneles > NGFW SD-WAN)** para comenzar.



Para utilizar este panel, puede configurar una red de área amplia definida por software (SD-WAN) en Strata Cloud Manager para sus cortafuegos de nueva generación de Palo Alto Networks.

¿Qué le muestra este panel?

El panel de **NGFW SD-WAN (SD-WAN de NGFW)** le muestra las métricas de rendimiento de los enlaces y el tráfico de aplicaciones para los cortafuegos gestionados en la nube con SD-WAN.

¿Cómo puede utilizar los datos del panel?

Este panel le ayuda con:

- Visibilidad de las métricas de rendimiento de las aplicaciones y los vínculos en sus clústeres de VPN para solucionar problemas mediante la visualización de la información resumida de todos los clústeres de VPN.
- Analizar en profundidad para aislar los problemas en los sitios, aplicaciones y enlaces afectados.
- Generar alertas prácticas para investigar y remediar enlaces y aplicaciones deficientes. Con la detección de anomalías, banda de normalidad y pronósticos basados en el aprendizaje

automático, las alertas procesables se basan en umbrales basados en datos y obtendrá información sobre las tendencias.

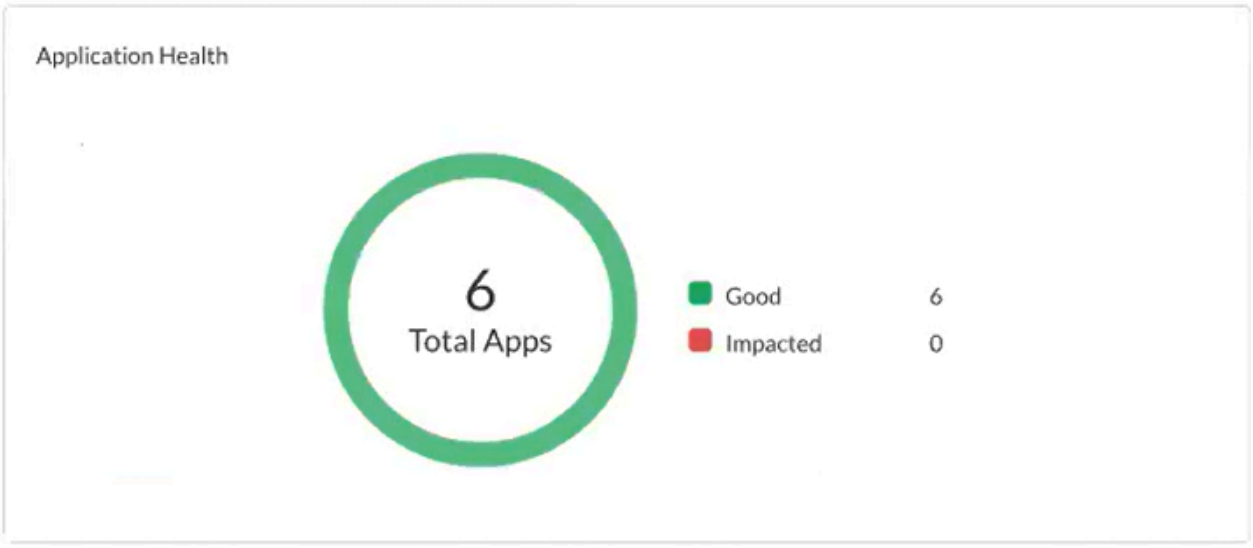
Aquí hay un video que muestra cómo supervisar el panel SD-WAN de NGFW.

Panel de SD-WAN para NGFW: Estado de la aplicación

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW, incluidos los financiados por Créditos de NGFW de software	❑ AIOps for NGFW Premium o Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

El panel muestra:

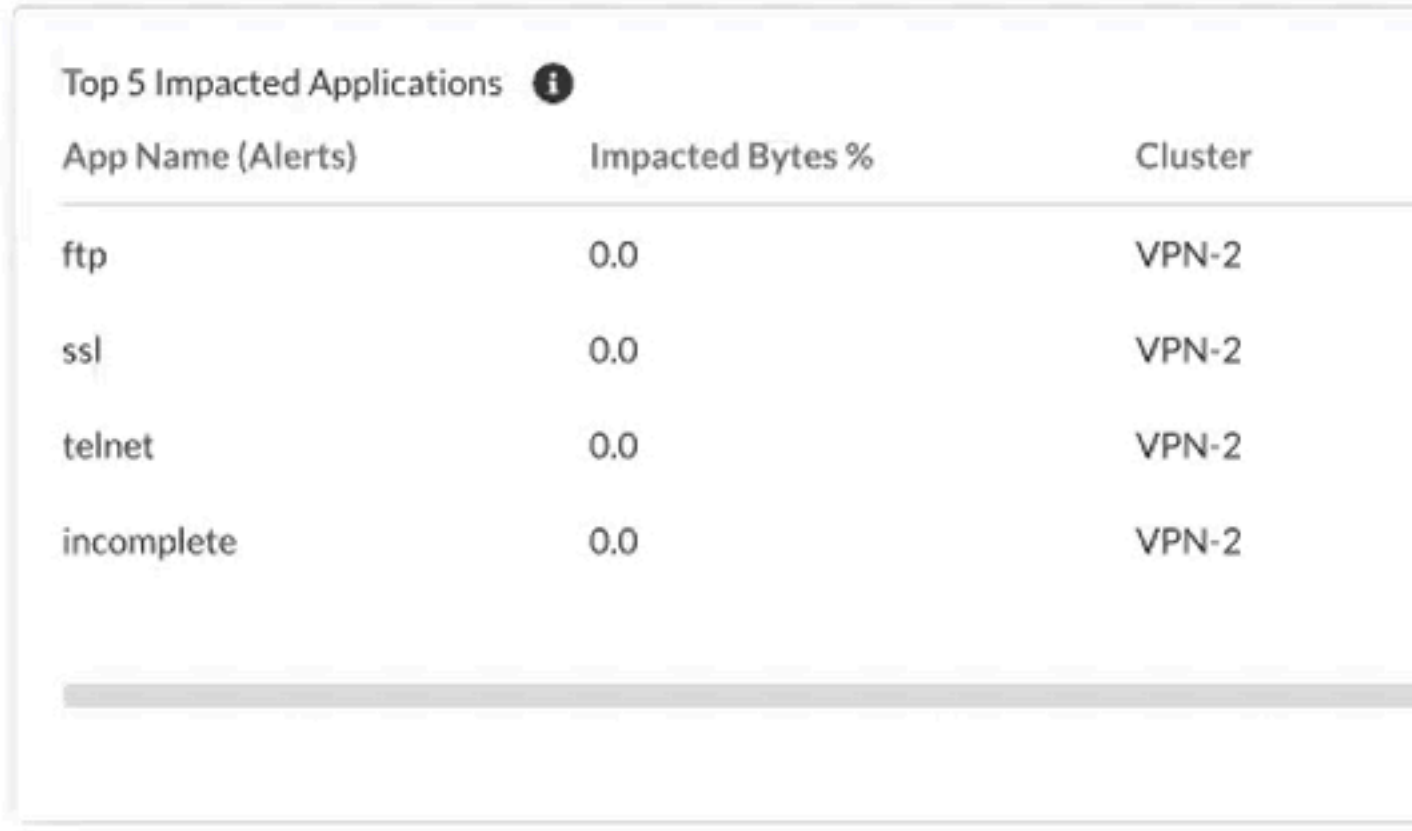
- El número total de aplicaciones para la duración de tiempo seleccionada y el clúster VPN.
- El número de aplicaciones afectadas, es decir, una o más aplicaciones del clúster de VPN para las que ninguna de las rutas tiene vibración, latencia o rendimiento de pérdida de paquetes que cumplen con los umbrales especificados en el perfil de calidad de ruta en la lista de rutas a partir de las que el cortafuegos puede elegir.
- El número de aplicaciones cuyo estado es bueno, es decir, aplicaciones en el clúster VPN que no están experimentando fluctuación, latencia o problemas de rendimiento de pérdida de paquetes.



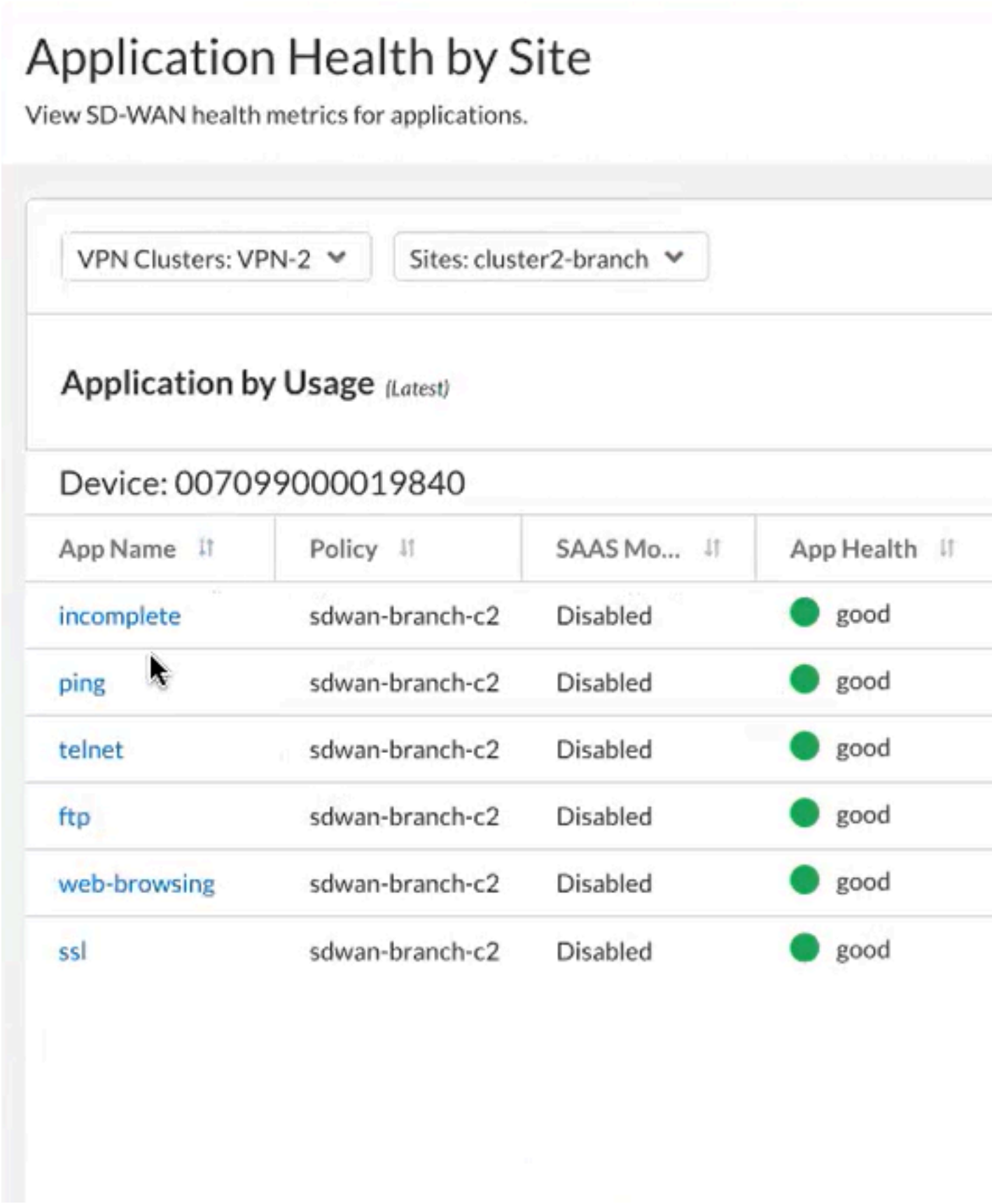
Panel de SD-WAN para NGFW: Principales aplicaciones afectadas

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW, incluidos los financiados por Créditos de NGFW de software	☐ AIOps for NGFW Premium o Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

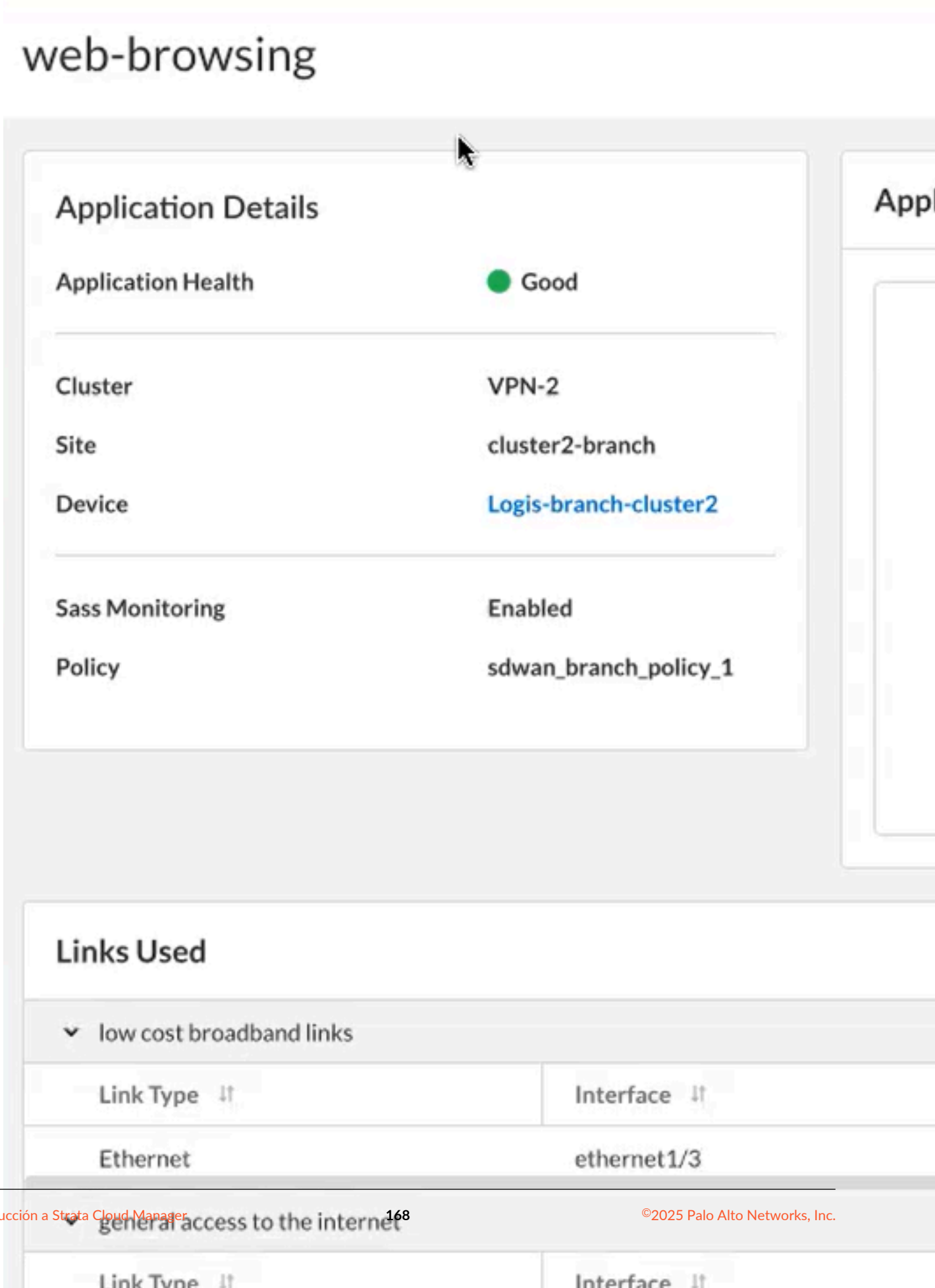
Para la duración de tiempo y el clúster VPN seleccionados, Strata Cloud Manager muestra las 5 aplicaciones afectadas principales en función de su porcentaje calculado del tráfico impactado del total de bytes. Un mayor porcentaje calculado indica un mayor impacto en la aplicación.



Haga clic en **Ver más** para comprobar todas las aplicaciones afectadas.



Además, haga clic en una aplicación para ver sus detalles, incluido el tráfico y los enlaces utilizados. También puede hacer clic en un enlace usado para ver sus detalles.



Panel de SD-WAN para NGFW: Aplicaciones afectadas

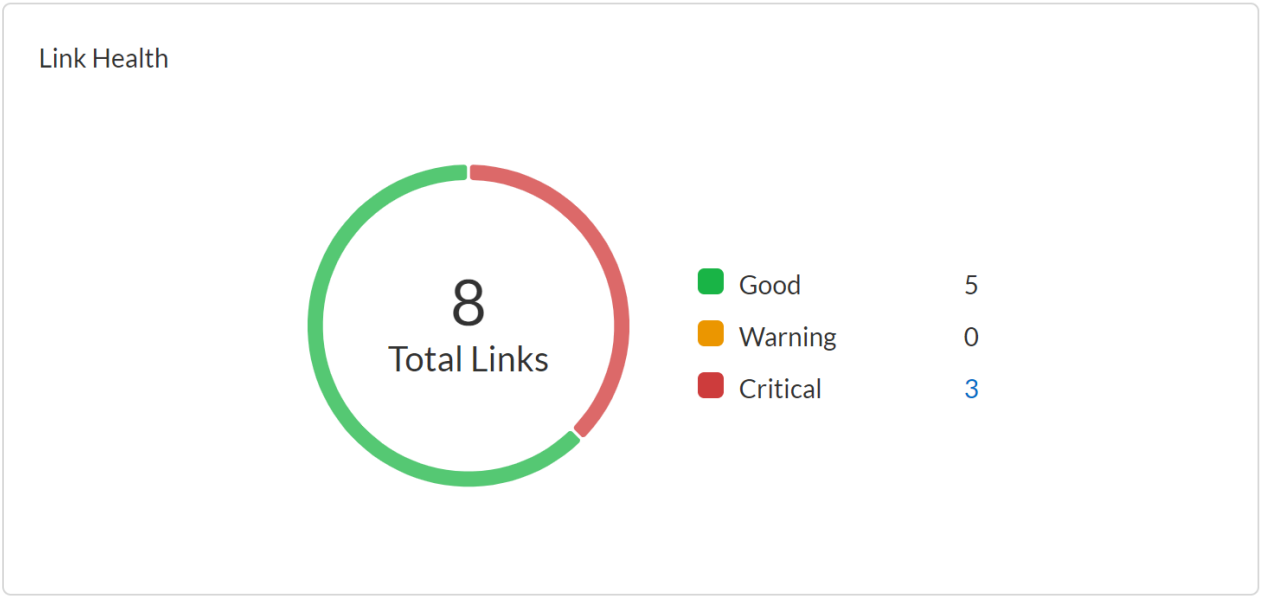
¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW, incluidos los financiados por Créditos de NGFW de software	❑ AIOps for NGFW Premium o Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

- El gráfico muestra una tendencia que muestra las aplicaciones afectadas en las últimas 24 horas. Coloque el cursor sobre la línea de tendencia para ver las aplicaciones afectadas en un momento específico.
- Haga clic en **Ver alertas** para ver las alertas asociadas que se generan debido a las aplicaciones afectadas.

Panel de SD-WAN para NGFW: Estado del enlace

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW, incluidos los financiados por Créditos de NGFW de software	❑ AIOps for NGFW Premium o Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

- El número total de enlaces para la duración seleccionada y el clúster de VPN.
- El número de enlaces clasificados como Crítico, Advertencia y Bueno.
- Haga clic en el enlace numérico de **Crítico** para ver las alertas generadas debido al rendimiento del enlace SD-WAN.



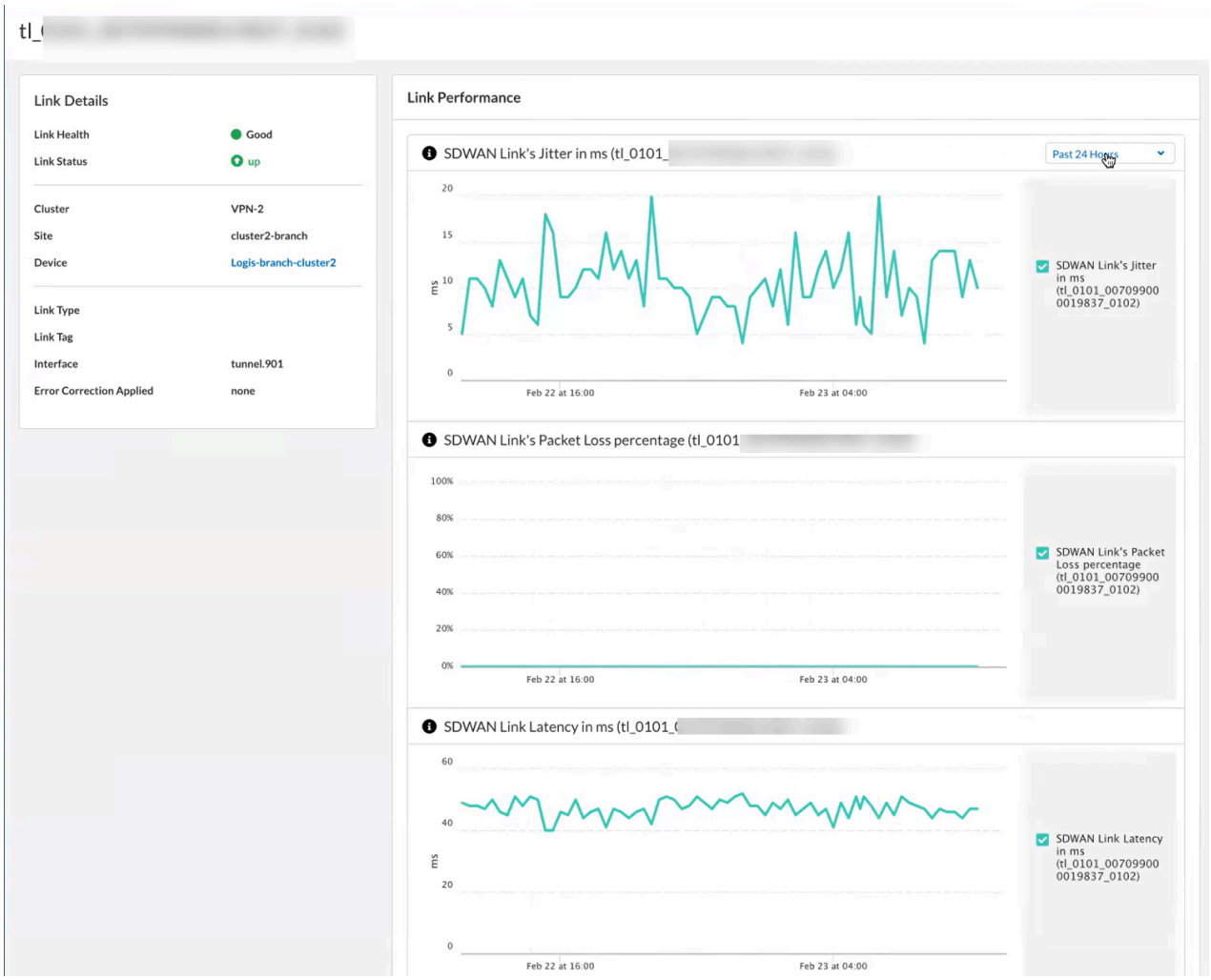
Panel de SD-WAN para NGFW: Los peores enlaces

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW, incluidos los financiados por Créditos de NGFW de software	❑ AIOps for NGFW Premium o Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Para la duración de tiempo y el clúster VPN seleccionados, Strata Cloud Manager muestra los 5 peores enlaces según el promedio calculado de las métricas de la interfaz (tiempo de inactividad del túnel, latencia, fluctuación, vibración y pérdida de paquetes). Los enlaces se clasifican en función de la prioridad del tiempo de inactividad del túnel, latencia, pérdida de paquetes y fluctuación. Un promedio calculado más alto indica la mala calidad de los enlaces.

Haga clic en **View more (Ver más)** para comprobar todos los enlaces afectados.

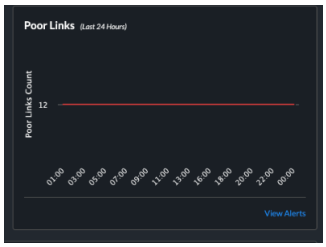
Además, haga clic en un enlace para ver sus detalles, incluidos los gráficos basados en el rendimiento del enlace.



Panel de SD-WAN para NGFW: Enlaces deficientes

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW, incluidos los financiados por Créditos de NGFW de software	❑ AIOps for NGFW Premium o Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

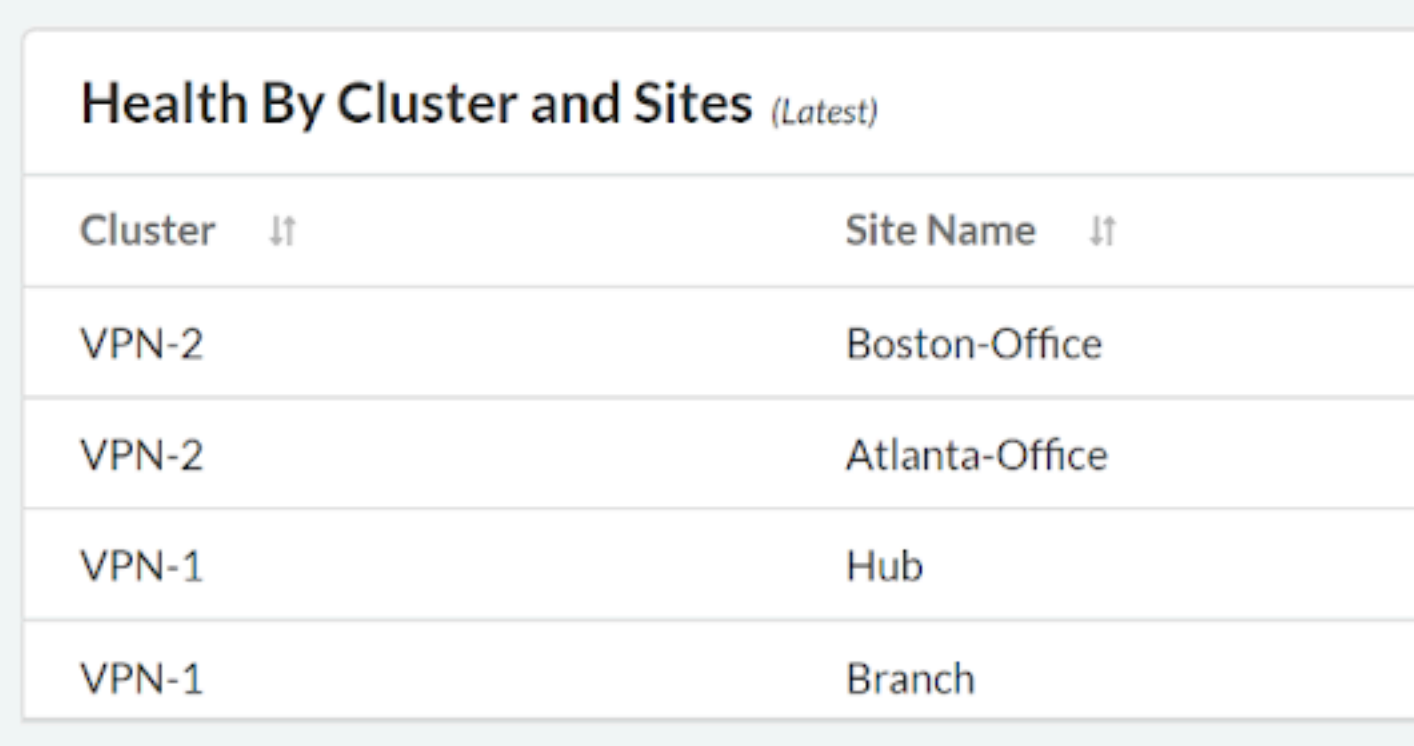
- El gráfico muestra una tendencia que muestra los enlaces deficientes detectados en las últimas 24 horas. Pase el cursor sobre la línea de tendencia para ver los enlaces deficientes en un momento específico.
- Haga clic en **Ver alertas** para ver las alertas asociadas que se generan debido a los enlaces deficientes.



Panel de SD-WAN para NGFW: Estado por grupo y sitios

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW, incluidos los financiados por Créditos de NGFW de software	❑ AIOps for NGFW Premium o Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Vea el número de enlaces, su estado y las aplicaciones afectadas para cada sitio.



Haga clic en los enlaces numéricos debajo de estas columnas para ver detalles sobre ellos.

Panel: Prisma SD-WAN

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma SD-WAN	❑ Licencia de Prisma SD-WAN Las otras licencias y requisitos previos necesarios para la visibilidad son: ❑ Licencias para desbloquear ciertos widgets en el panel ❑ WAN Clarity para análisis predictivo ❑ Un rol que tiene permiso para ver el panel → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

¿Qué le muestra este panel?

El Panel le muestra una vista gráfica y de alto nivel de las métricas de red, dispositivo y métricas de aplicaciones de Prisma SD-WAN. Además, le muestra:

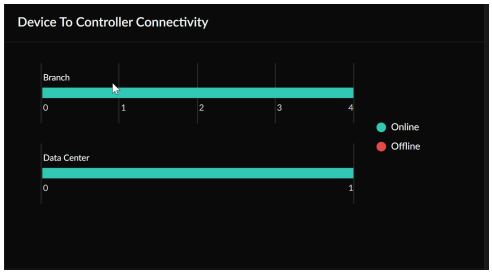
- El estado de la conectividad de los dispositivos de su sucursal y de centro de datos al controlador.
- Los datos de uso de la aplicación para su tráfico de entrada y salida.
- Información básica de la red e informes para todos los sitios de sucursales en un inquilino de la semana pasada.
- Información sobre la sucursal superior y los sitios del centro de datos por el número de incidentes generados.
- Las métricas de calidad del enlace en sus sitios como puntuación MOS, pérdida de paquetes, fluctuación y latencia.
- La utilización de la capacidad predictiva a nivel de sitio en base a los últimos tres a seis meses de información.

Panel de Prisma SD-WAN: Conectividad de dispositivo a controlador

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma SD-WAN	❑ Licencia de Prisma SD-WAN Las otras licencias y requisitos previos necesarios para la visibilidad son:

¿Dónde puedo usar esto?	¿Qué necesito?
	❑ Licencias para desbloquear ciertos widgets en el panel ❑ WAN Clarity para análisis predictivo ❑ Un rol que tiene permiso para ver el panel → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

El widget Conectividad de dispositivo a controlador representa el número de dispositivos ION en línea y sin conexión conectados al controlador Prisma SD-WAN para una sucursal y un centro de datos. Con este gráfico interactivo, puede ver el estado en línea o sin conexión de un dispositivo reclamado para la sucursal y el centro de datos correspondientes.

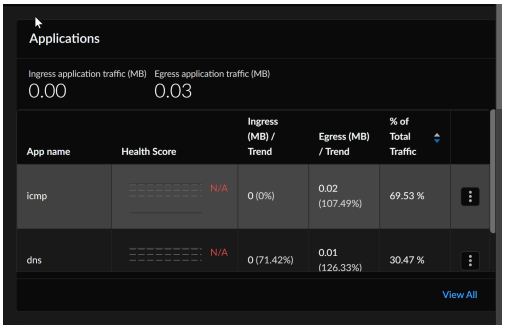


Al hacer clic en **Branch (Sucursal)** o en **Data Center (Centro de datos)** en el gráfico interactivo, puede ver el nombre de los dispositivos reclamados y no reclamados, el estado, la versión de software instalada, la última actividad y el estado de redundancia del dispositivo.

Panel de Prisma SD-WAN: Aplicaciones

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma SD-WAN	❑ Licencia de Prisma SD-WAN Las otras licencias y requisitos previos necesarios para la visibilidad son: ❑ Licencias para desbloquear ciertos widgets en el panel ❑ WAN Clarity para análisis predictivo ❑ Un rol que tiene permiso para ver el panel → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

El widget Applications muestra información sobre el uso de la aplicación en el sitio durante el intervalo de tiempo seleccionado. Se muestra el tráfico total de entrada y salida de aplicaciones para el intervalo de tiempo. Las 10 principales aplicaciones por volumen de tráfico se muestran junto con el otro tráfico. Haga clic en **View All (Ver todo)** para ver la distribución del estado de la aplicación, la distribución del estado de la aplicación TCP a lo largo del tiempo, los nuevos flujos, la utilización del ancho de banda, las estadísticas de transacciones para el rango de tiempo seleccionado junto con las aplicaciones principales. Puede profundizar para ver el rendimiento de una aplicación y las métricas por sitio para el rango de tiempo seleccionado en el panel.

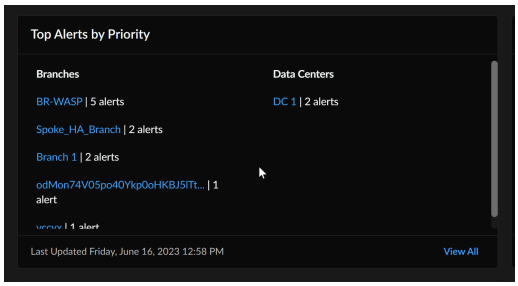


Las métricas para todas las aplicaciones TCP se muestran inicialmente, pero, cualquiera de las 10 aplicaciones TCP principales se puede seleccionar para centrarse más estrictamente en una aplicación superior específica.

Panel de Prisma SD-WAN: Principales alertas por prioridad

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma SD-WAN	☐ Licencia de Prisma SD-WAN Las otras licencias y requisitos previos necesarios para la visibilidad son: ☐ Licencias para desbloquear ciertos widgets en el panel ☐ WAN Clarity para análisis predictivo ☐ Un rol que tiene permiso para ver el panel → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

El widget **Principales alertas por prioridad** muestra las 5 alertas principales por prioridad. Puede ver información sobre las principales sucursales y centros de datos por el número de alertas generadas en el intervalo de tiempo seleccionado. Puede explorar en profundidad para ver la información de alerta por sitio para el intervalo de tiempo seleccionado.



Haga clic en **View All (Ver todo)** para ver la siguiente información sobre las alertas:

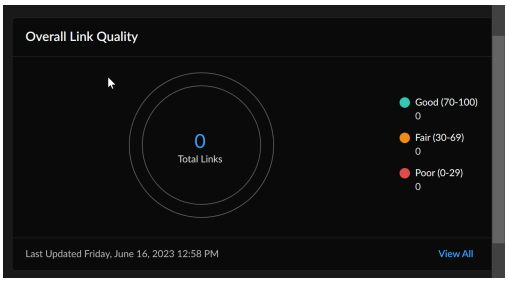
- Cuándo se creó la alerta.
- Nombre del incidente.
- El objeto principal afectado.
- La gravedad de la alerta.
- La prioridad de la alerta.

Haga clic en los puntos suspensivos para solucionar el problema de la alerta.

Panel de Prisma SD-WAN: Calidad general del enlace

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma SD-WAN	❑ Licencia de Prisma SD-WAN Las otras licencias y requisitos previos necesarios para la visibilidad son: ❑ Licencias para desbloquear ciertos widgets en el panel ❑ WAN Clarity para análisis predictivo ❑ Un rol que tiene permiso para ver el panel → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

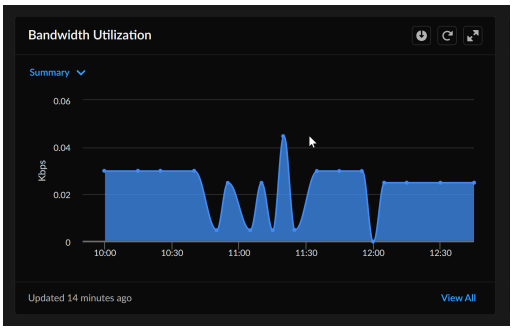
El widget **Calidad general del enlace** proporciona una instantánea general del estado actual de los enlaces de todos sus sitios durante el rango de tiempo seleccionado. Puede explorar en profundidad para ver el rendimiento del enlace, la pérdida de paquetes del enlace, la fluctuación del enlace y la latencia del enlace, y le permite analizar la información que desea ver con mayor detalle en el panel Métricas de calidad del enlace.



Panel de Prisma SD-WAN: Utilización del ancho de banda

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma SD-WAN	❑ Licencia de Prisma SD-WAN Las otras licencias y requisitos previos necesarios para la visibilidad son: ❑ Licencias para desbloquear ciertos widgets en el panel ❑ WAN Clarity para análisis predictivo ❑ Un rol que tiene permiso para ver el panel → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

El widget de Utilización del ancho de banda muestra la cantidad de ancho de banda utilizado en un rastro en una red. Es una representación visual del pico de ancho de banda, el ancho de banda total consumido por un sitio en particular y la aplicación; si la carga está en la dirección de entrada, salida o ambas.



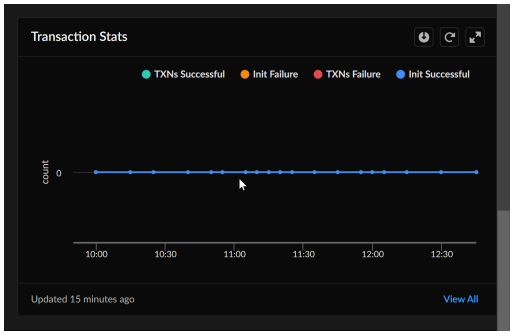
Mueva el cursor en el gráfico **Bandwidth Utilization (Utilización de ancho de banda)** para obtener una vista más granular de la utilización del ancho de banda con una aplicación o marca de tiempo. Normalmente, las aplicaciones se enumeran en orden de utilización del ancho de banda. El gráfico muestra el ancho de banda consumido a lo largo del tiempo. La vista 1H proporciona datos granulares por minuto, y la imagen 1D muestra datos cada 5 minutos. Los datos del gráfico 1D tienen un promedio superior a 5 minutos para cada muestra. Si la utilización se mantiene por encima de 5 minutos, puede ver la utilización máxima correspondiente en ambos gráficos.

Puede utilizar la opción de descarga del widget para descargar el gráfico de utilización de ancho de banda en formatos PDF, CSV, XLS o PNG.

Panel de Prisma SD-WAN: Estadísticas de transacciones

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma SD-WAN	❑ Licencia de Prisma SD-WAN Las otras licencias y requisitos previos necesarios para la visibilidad son: ❑ Licencias para desbloquear ciertos widgets en el panel ❑ WAN Clarity para análisis predictivo ❑ Un rol que tiene permiso para ver el panel → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

El widget Estadísticas de transacciones proporciona estadísticas de transacciones sobre flujos TCP, incluidas acciones correctas y fallidas de iniciación/transacción para una aplicación específica o todas las aplicaciones, una ruta particular o todas las rutas y todos los eventos de estado. Mide el rendimiento y la disponibilidad de las redes y aplicaciones que se ejecutan en rutas de redes. Para cada solicitud en una ruta determinada, Prisma SD-WAN supervisa, en tiempo real, las tasas de error de transacción para las transacciones de iniciación y transferencia de datos.



Desde el gráfico de Estadísticas de transacciones, vea la lista de aplicaciones por utilización de ancho de banda o por ruta. Puede filtrar las transacciones realizadas correctamente para obtener una vista granular de las estadísticas de fallos de transacciones. El gráfico muestra el recuento de transacciones realizas correctamente o fallidas para las siguientes categorías:

- **Init Sucessful (Inicialización realizada correctamente)**: Realización correcta del protocolo de enlace de tres vías.
- **TXNs Sucessful (TXN realizadas correctamente)**: Transferencia de datos realizada correctamente después de la finalización del protocolo de enlace de tres vías.

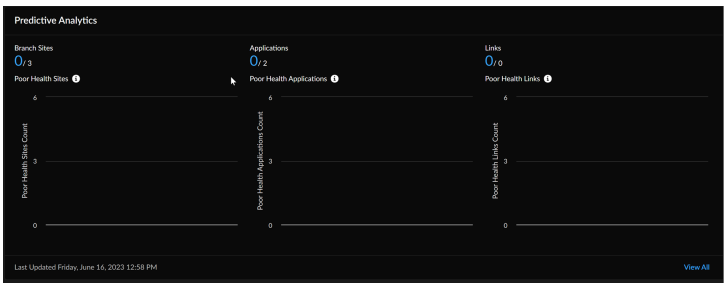
- **Init Failure (Fallo de inicialización)**: No se pudo completar el protocolo de enlace de tres vías. Las razones del fallo pueden incluir una configuración incorrecta del cortafuegos, un problema con el servidor de aplicaciones, una configuración incorrecta de la lista de control de acceso a la red o un problema con el proveedor de la red WAN.
- **TXNs Failure (Fallo de TXN)**: Fallo de transferencia de datos después de la finalización del protocolo de enlace de tres vías. Las razones del fallo pueden incluir un cortafuegos mal configurado, un problema con el servidor de aplicaciones, una lista de control de acceso a la red mal configurada o un problema con el proveedor de red WAN.

Puede utilizar la opción de descarga del widget para descargar el gráfico de utilización de ancho de banda en formatos PDF, CSV, XLS o PNG.

Panel de Prisma SD-WAN: Análisis predictivo

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma SD-WAN	❑ Licencia de Prisma SD-WAN Las otras licencias y requisitos previos necesarios para la visibilidad son: ❑ Licencias para desbloquear ciertos widgets en el panel ❑ WAN Clarity para análisis predictivo ❑ Un rol que tiene permiso para ver el panel → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

El widget Análisis predictivo proporciona información sobre el estado de los sitios y aplicaciones, y una supervisión proactiva para identificar problemas críticos y solucionarlos más rápidamente, mejorando así los niveles de servicio. Identifica sitios críticos, enlaces y aplicaciones y los clasifica como **Good (Buenos)**, **Fair (Regulares)** y **Poor (Deficientes)** a nivel de inquilino, según las puntuaciones de estado de IA/ML. El widget incluye la predicción de la utilización de la capacidad a nivel del sitio de la sucursal en función de los tres a seis meses anteriores de información.



El intervalo de tiempo predeterminado para ver las métricas es de tres horas; sin embargo, puede ajustarlo a períodos más cortos o más largos según el alcance deseado de la información. Obtenga información sobre los 10 principales sitios cuya utilización del ancho de banda aumentó en los

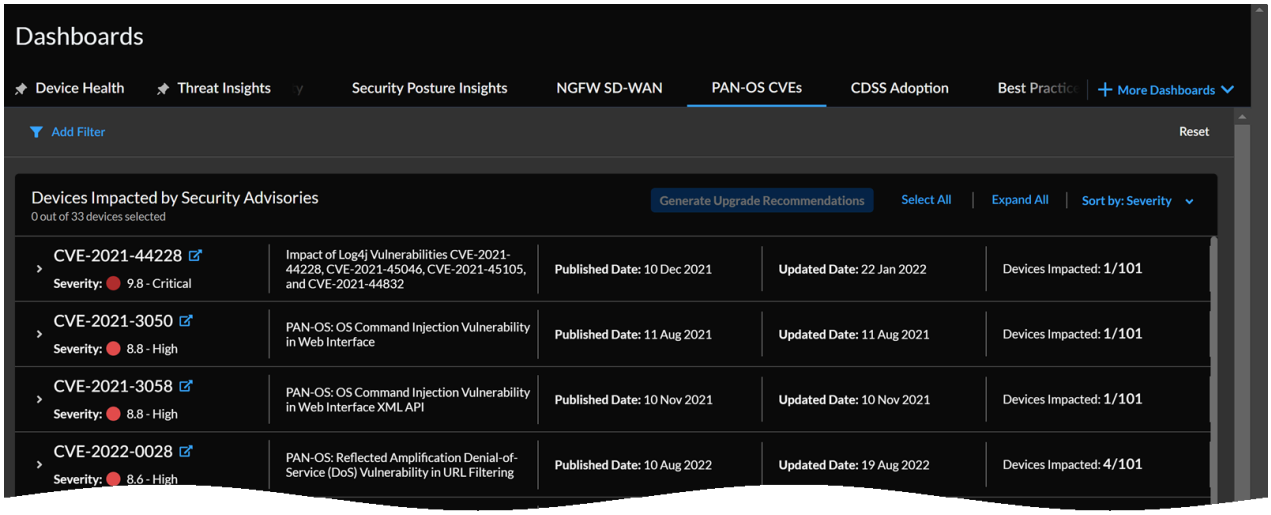
últimos 28 días; puede ver la previsión a siete días cada vez que la previsión a 28 días no esté disponible y predecir la futura utilización de la capacidad de la sucursal.

Haga clic en **View All (Ver todo)** para obtener información sobre sitios de sucursales, aplicaciones, enlaces, información de red, sitios principales con crecimiento del volumen de tráfico en los últimos 30 días y predicción y anomalía de la capacidad del sitio.

Panel: CVE de PAN-OS

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW, incluidos los financiados por Créditos de NGFW de software	☐ Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium o Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

- Haga clic en **Dashboards (Paneles) > More Dashboards (Más paneles) > PAN-OS CVE** para comenzar.



¿Qué le muestra este panel?

El panel muestra los datos añadidos de todos los cortafuegos y Panorama incorporados a su inquilino y también están enviando datos de telemetría. Además, muestra los datos de telemetría de la base de datos NGFW PSIRT de las CVE.

El panel **PAN-OS CVEs (CVE de PAN-OS)** muestra el número de dispositivos afectados por una vulnerabilidad específica en función de las características que se han habilitado en los dispositivos. Strata Cloud Manager analiza las características que se han habilitado para determinar los dispositivos afectados por el CVE.

Después de comprender las vulnerabilidades de los dispositivos afectados, puede planificar sus parches utilizando la función Recomendaciones de actualización. Expanda las CVE y seleccione los cortafuegos que desea actualizar para corregir las vulnerabilidades, y haga clic en **Generate Upgrade Recommendations (Generar recomendaciones de actualización)**. Se le redirige a NGFW - Recomendaciones de actualización para ver el informe generado.

A continuación se muestra cómo evaluar las vulnerabilidades que afectan a los dispositivos y generar recomendaciones de actualización para corregirlas.

¿Cómo puede utilizar los datos del panel?

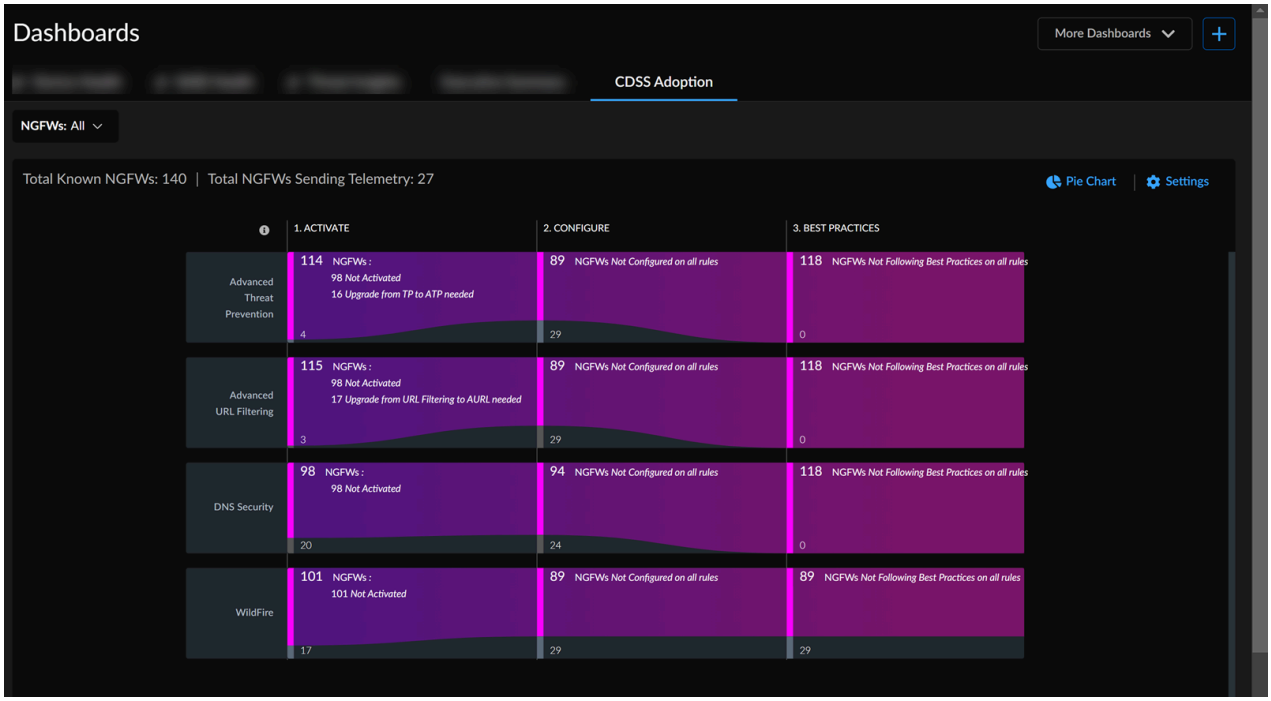
Este panel le ayuda a:

- Decidir qué dispositivos actualizar para mitigar una vulnerabilidad.
- Ver detalles sobre un dispositivo afectado, como el nombre del host, el modelo, el número de serie, la versión SW y la última actualización de telemetría expandiendo un CVE.
- Filtrar las CVE y ordenarlas aún más por **Severity (Gravedad)** o **Devices Impacted (Dispositivos afectados)**.
- Ver la asesoría asociada con una CVE haciendo clic en ella.

Panel: Adopción de CDSS

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW, incluidos los financiados por Créditos de NGFW de software	☐ Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium o Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

- Haga clic en **Dashboards (Paneles)** > **Posture (Postura)** > **CDSS Adoption (Adopción de CDSS)** para empezar.



¿Qué le muestra este panel?

- *El panel muestra los datos añadidos de todos los cortafuegos incorporados a su inquilino y también están enviando datos de telemetría.*
- *Actualmente, este panel solo admite cuatro suscripciones de seguridad: Advanced Threat Prevention, Advanced URL Filtering, DNS Security y Wildfire.*

El panel **CDSS Adoption (Adopción de CDSS)** muestra las suscripciones recomendadas a los servicios de seguridad entregados en la nube (CDSS) y su uso en sus dispositivos. Esto le ayuda a identificar brechas de seguridad y a endurecer la postura de seguridad de su empresa. Después de

navegar por esta página, verá un pop-up que le pedirá que confirme o actualice sus roles de zona en los NGFW para obtener recomendaciones precisas de los servicios de seguridad. Puedes seguir el enlace en esta ventana emergente para asignar zonas a roles.

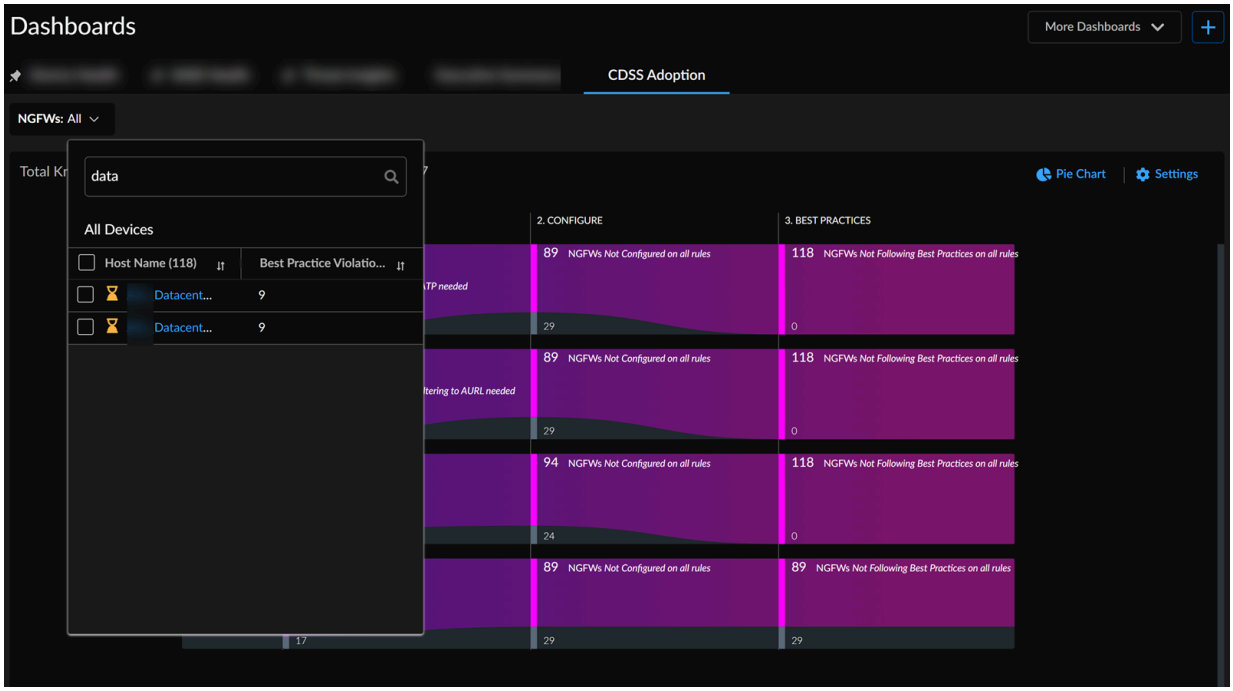
Aquí hay un video que muestra cómo supervisar las suscripciones de seguridad usando el panel de **CDSS Adoption (Adopción CDSS)**:

¿Cómo puede utilizar los datos del panel?

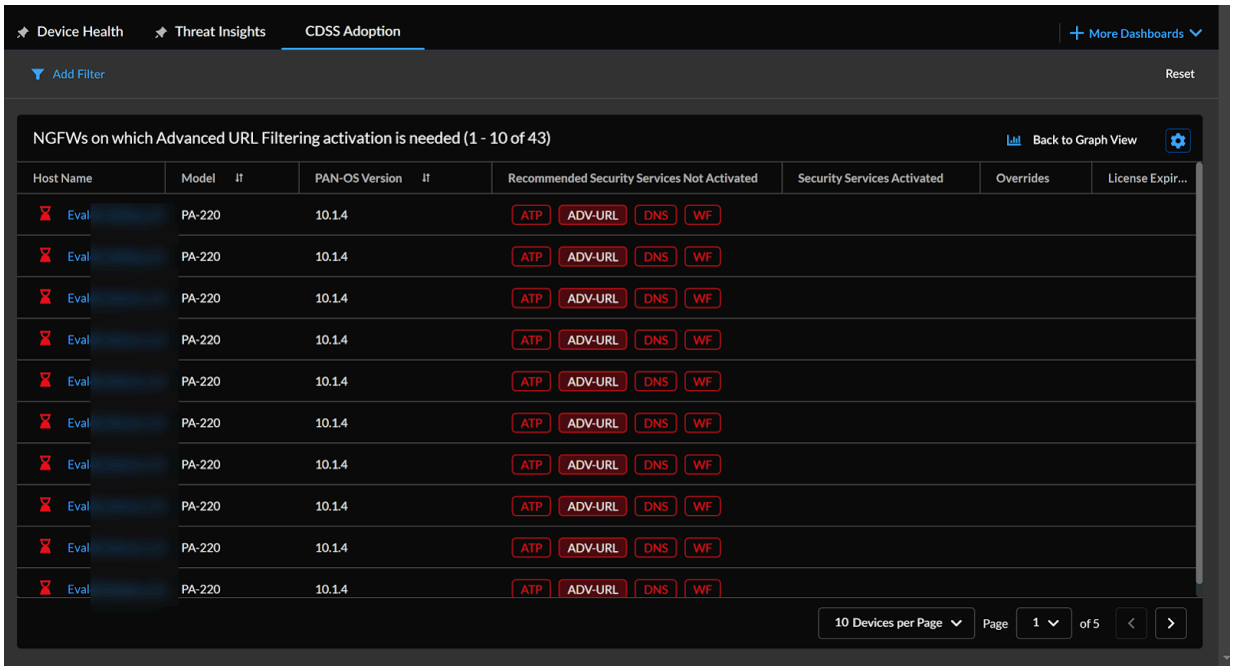
Este panel le ayuda con lo siguiente:

- En la parte superior de la página de Descripción general, puede ver el número total de cortafuegos NGFW conocidos y el número de NGFW que envían telemetría en su instancia de AIOps para NGFW. La adopción del CDSS implica avanzar mediante la activación, configuración y adhesión a las prácticas recomendadas. Para hacer un seguimiento del progreso de cada suscripción, simplemente haga clic en los números del gráfico para ver una lista de dispositivos que requieren actualizaciones a lo largo de este viaje. Para utilizar una licencia de suscripción de seguridad en un dispositivo, debe activarla y, a continuación, configurar el servicio o la función en consecuencia.

  Para centrarse en los datos de los servicios de seguridad de un NGFW específico, filtre el gráfico en función de ellos. En esta lista desplegable también puede ver las infracciones de las prácticas recomendadas para un dispositivo.

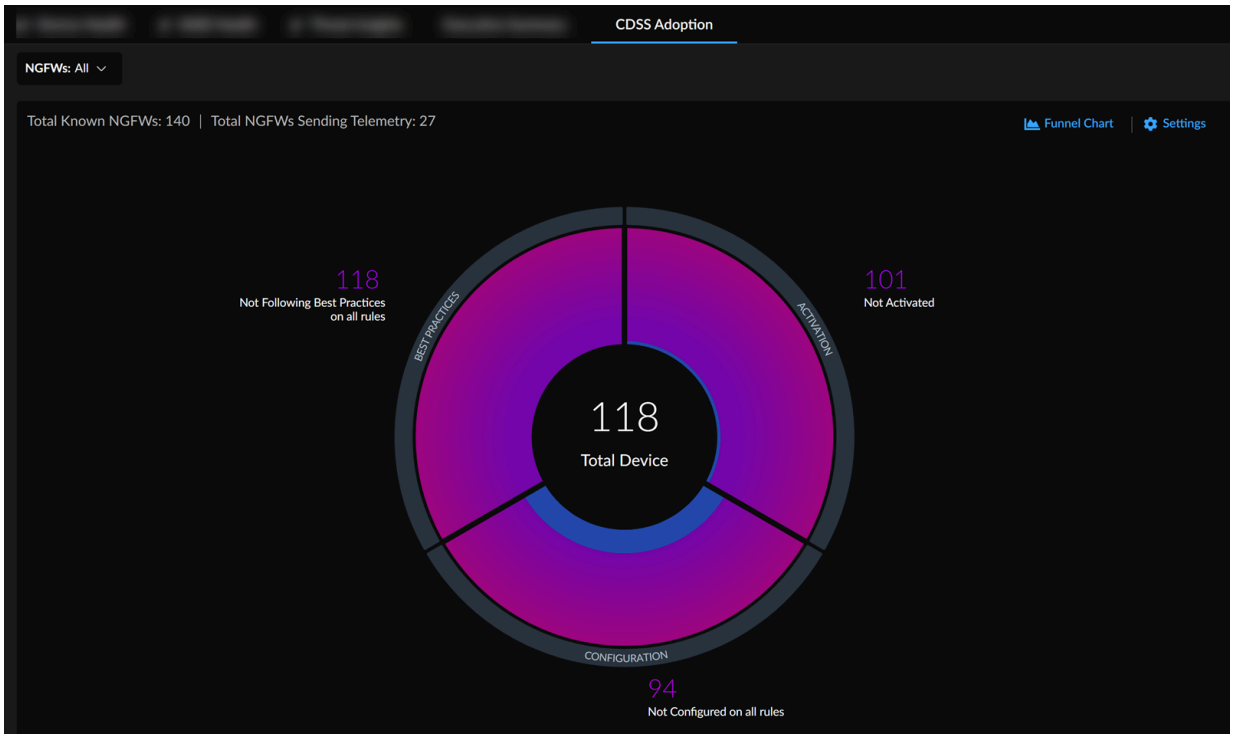


- Puede hacer clic en uno de los valores en **ACTIVATE (ACTIVAR)**, **CONFIGURE (CONFIGURAR)** o **BEST PRACTICES (PRÁCTICAS RECOMENDADAS)** para ver los detalles en un formato tabular.

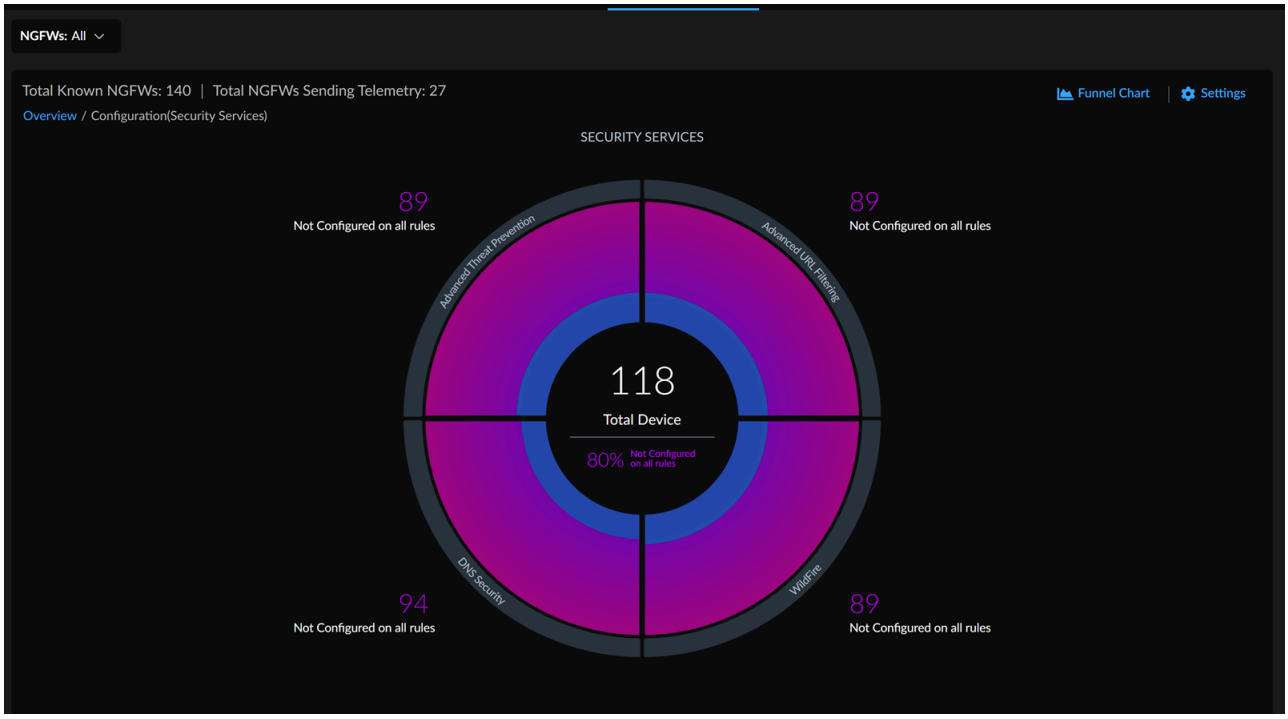


En este ejemplo, AIOps para NGFW recomienda la activación de Advanced URL Filtering (ADV-URL) junto con los servicios de seguridad Advanced Threat Protection (ATP), Domain Name System (DNS) y WildFire (WF) para NGFW. Puede hacer clic en **Back to Graph View (Volver a vista de gráfico)** para navegar a la página Descripción general.

- También puede ver los mismos datos de postura de seguridad en un formato de gráfico circular. Haga clic en el icono del gráfico circular para ver la información sobre los servicios de seguridad recomendados en un formato de gráfico circular.



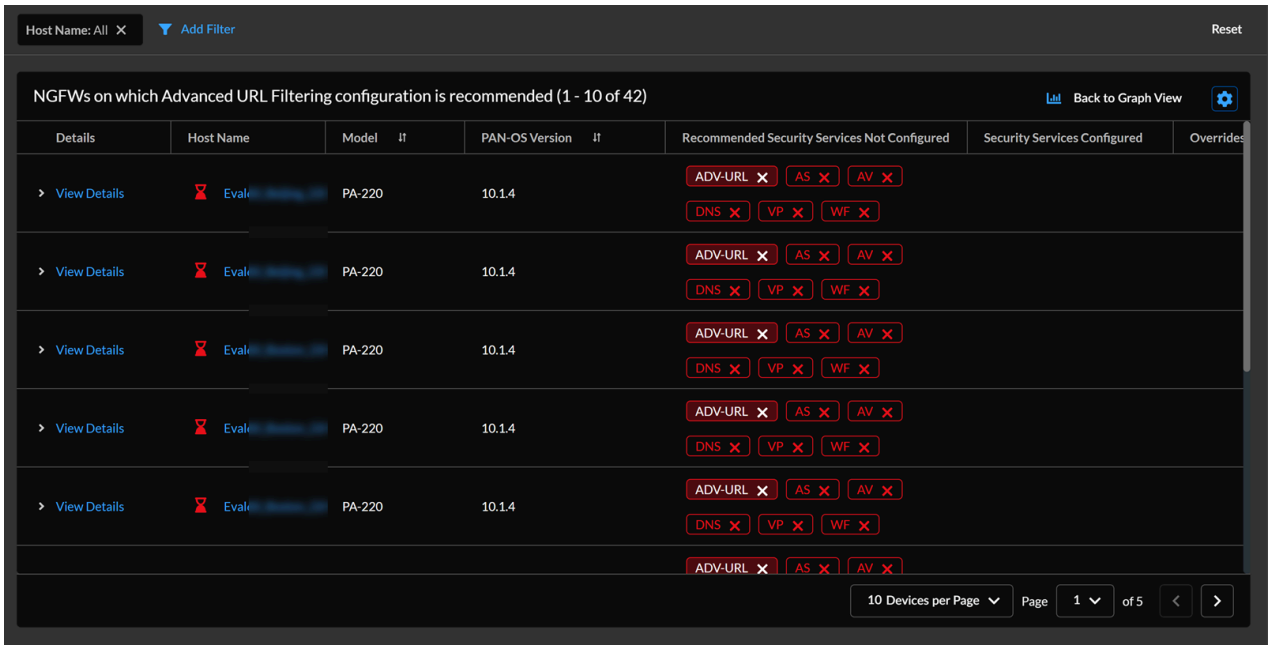
- Puede hacer clic en las secciones del gráfico circular para ver la información sobre el servicio de seguridad individual.



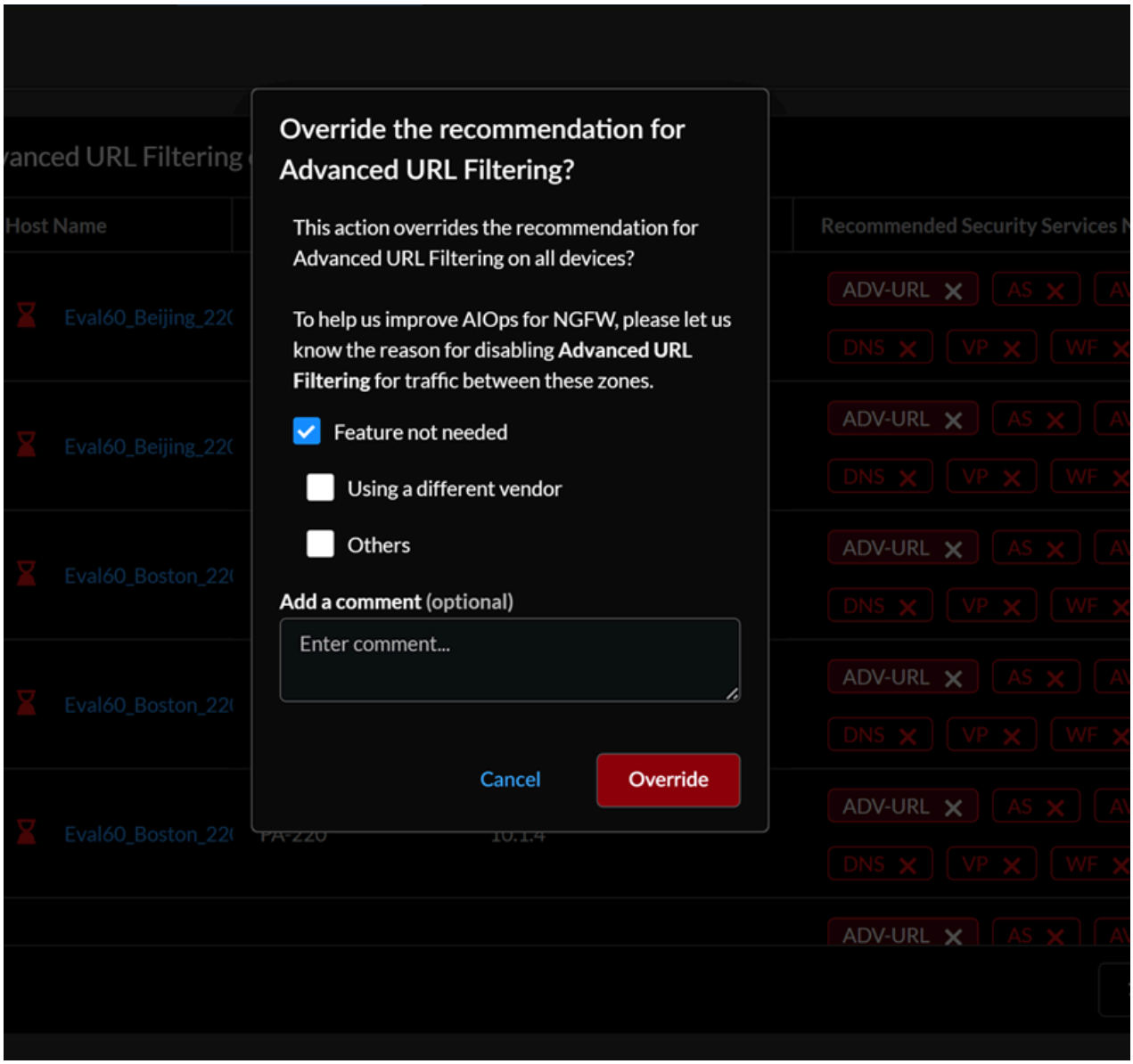
En este ejemplo, para ver el NGFW donde DNS Security no está configurado, puede hacer clic en el valor situado encima de la sección **DNS Security** de un gráfico circular o en la sección **DNS Security** de un gráfico circular.

Anular el servicio de seguridad recomendado

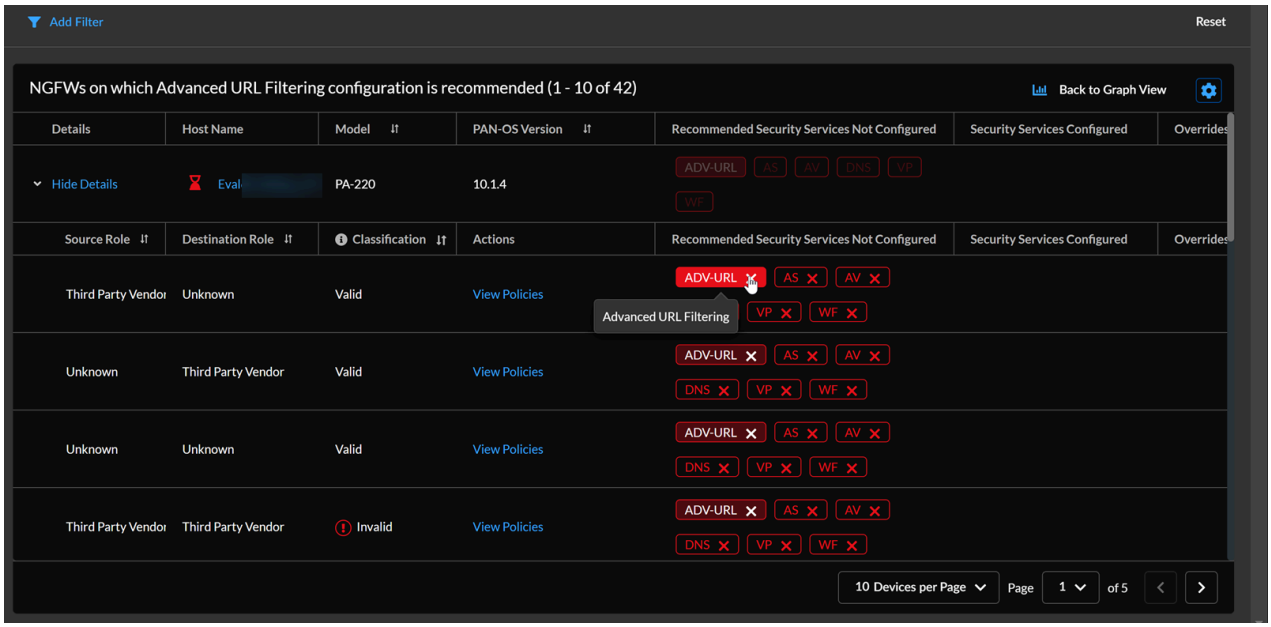
Cuando no necesite un servicio de seguridad recomendado por algún motivo, puede anularlo. Haga clic en un valor en **CONFIGURE (CONFIGURAR)** para ver los detalles en un formato tabular, puede anular el servicio de seguridad recomendado.



En este ejemplo, AIOps para NGFW recomienda la configuración de Advanced URL Filtering (ADV-URL) junto con otros servicios de seguridad para un dispositivo. Puede cancelar el servicio de seguridad ADV-URL para el dispositivo NGFW y todas las zonas que cubre.

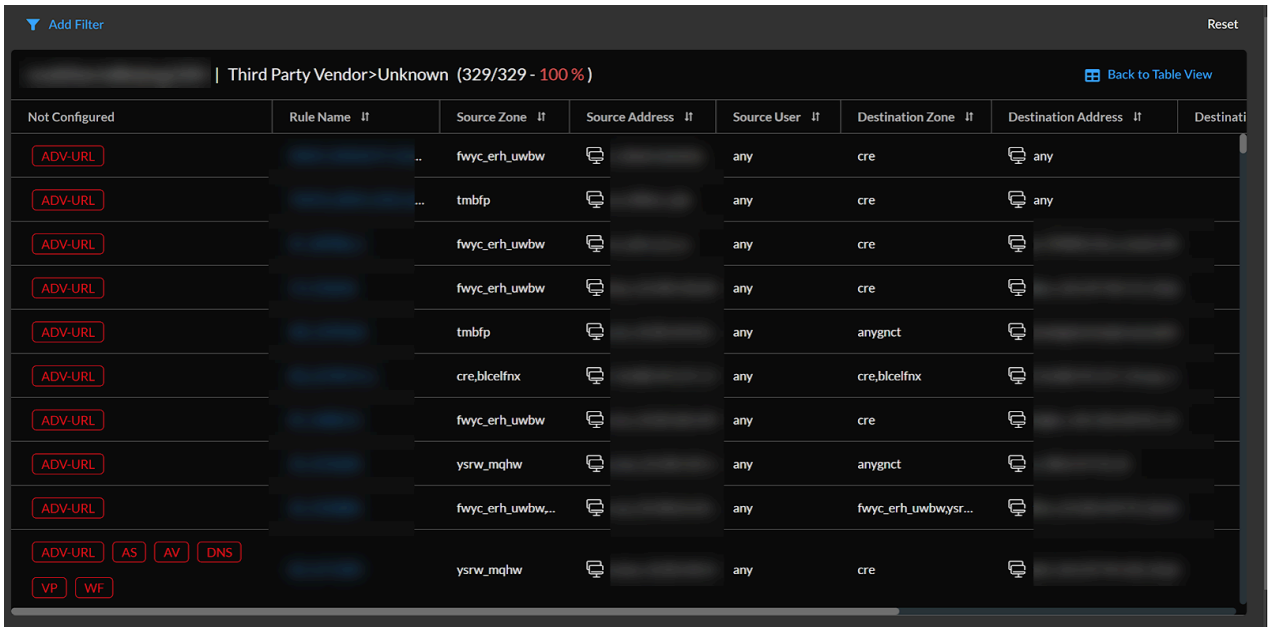


También puede anular el servicio de seguridad recomendado a nivel de zona. **View Details (Ver detalles)** para que un NGFW vea los roles de origen y destino, las políticas y los servicios de seguridad recomendados.



En este ejemplo, puede anular el servicio de seguridad **ADV-URL** para el rol de origen como **Third Party Vendor (Proveedor externo)** y el rol de destino como **Unknown (Desconocido)**. También puede restaurar la recomendación anulada haciendo clic en el servicio de seguridad en la columna **Overrides (Anulaciones)**.

Puede **View Policies (Ver las políticas)** asociadas con roles. Seleccione una regla para ver sus detalles sin necesidad de salir de la aplicación.



Haga clic en **Back to Table View (Volver a vista de tabla)** para ver los servicios de seguridad en un formato tabular.

Panel: Adopción de características

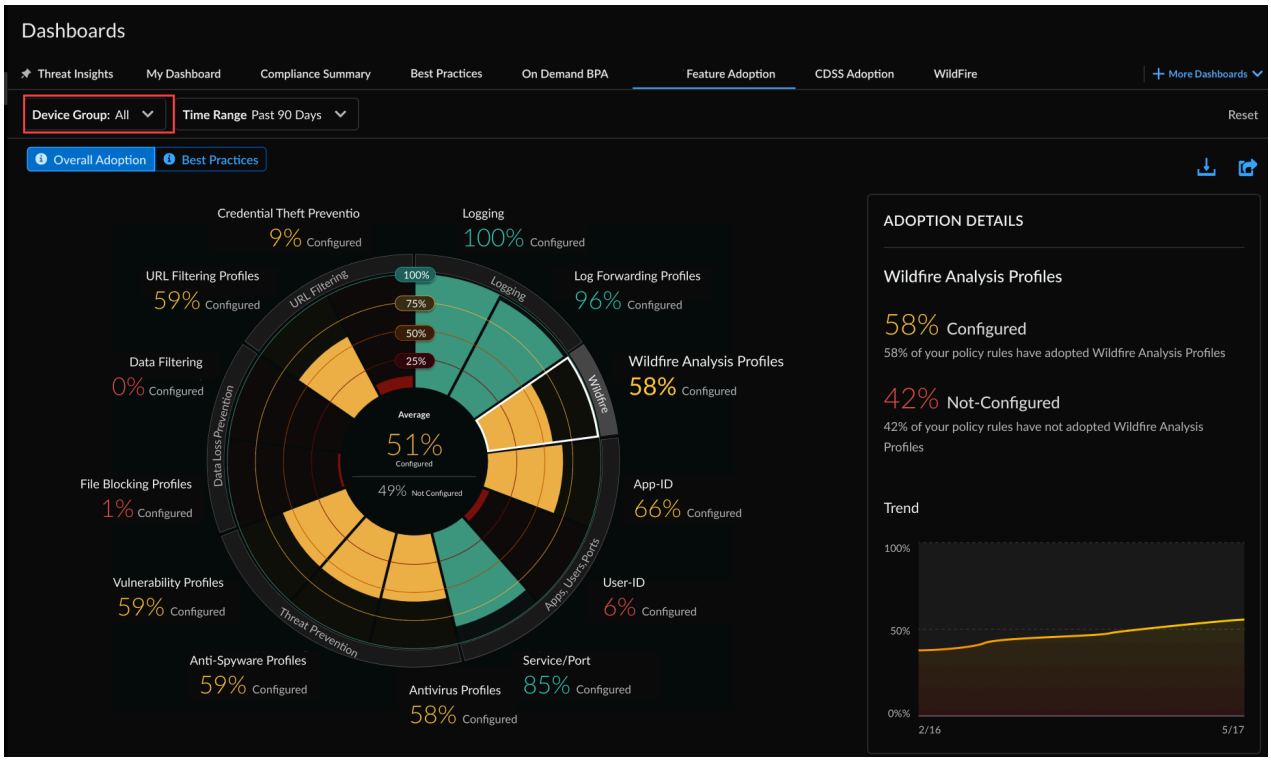
¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW, incluidos los financiados por Créditos de NGFW de software	☐ Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium o Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

- Haga clic en **Dashboards (Paneles)** > **Feature Adoption (Adopción de funciones)** para comenzar.

¿Qué le muestra este panel?

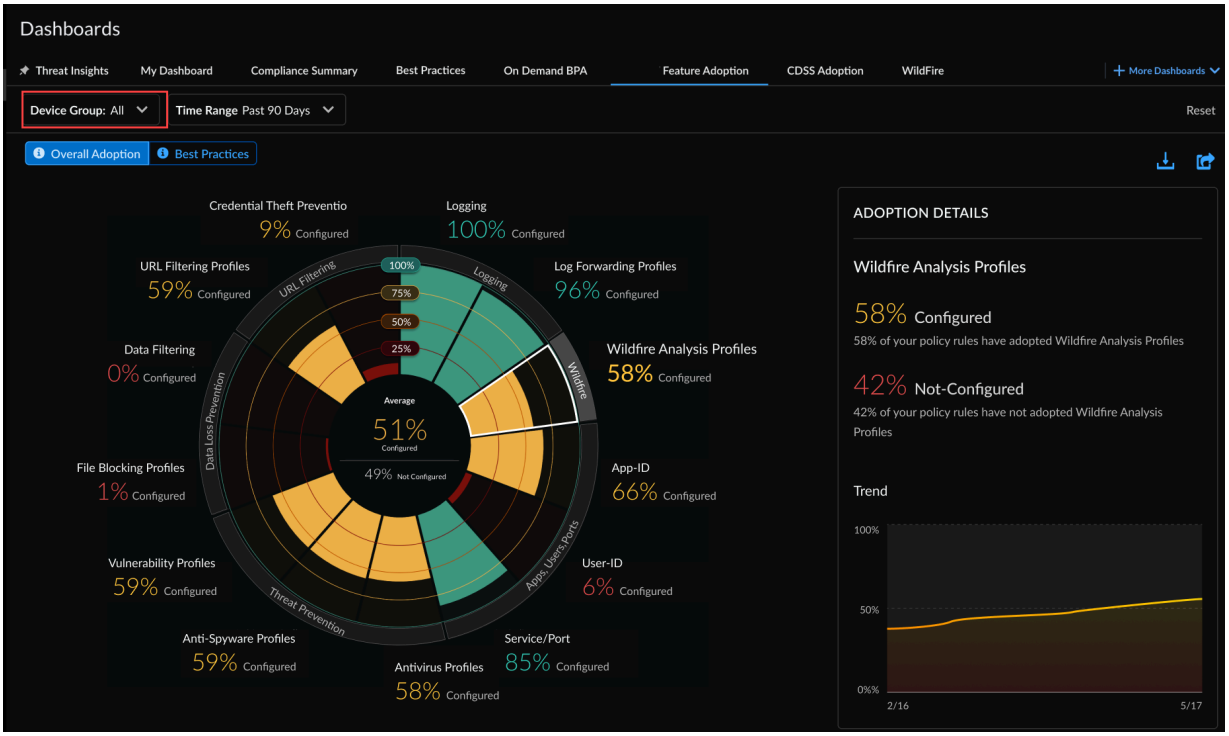
El panel muestra los datos añadidos de todos los cortafuegos incorporados a su inquilino y también están enviando datos de telemetría.

El panel **Feature Adoption (Adopción de funciones)** le muestra las funciones de seguridad que está utilizando en su implementación y puede usarlo para identificar brechas en la adopción. Esto le ayuda a asegurarse de aprovechar al máximo sus suscripciones de seguridad y funciones de cortafuegos de Palo Alto Networks.



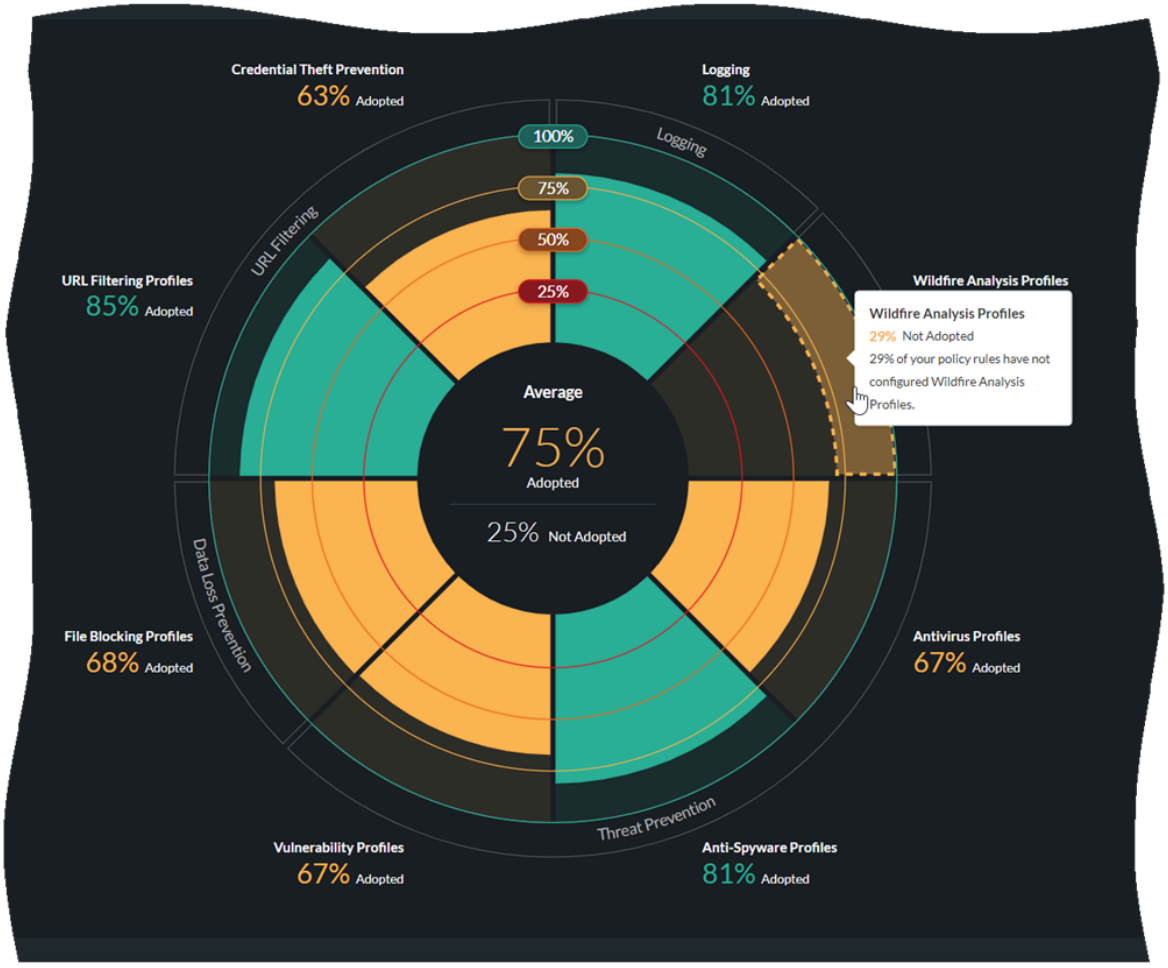
Cómo utilizar este panel

- Para centrarse en la adopción de funciones para un conjunto específico de cortafuegos, puede filtrar el gráfico según el grupo de dispositivos, incluidos los dispositivos gestionados por Panorama. También puede ver gráficos del historial de tendencias de adopción.

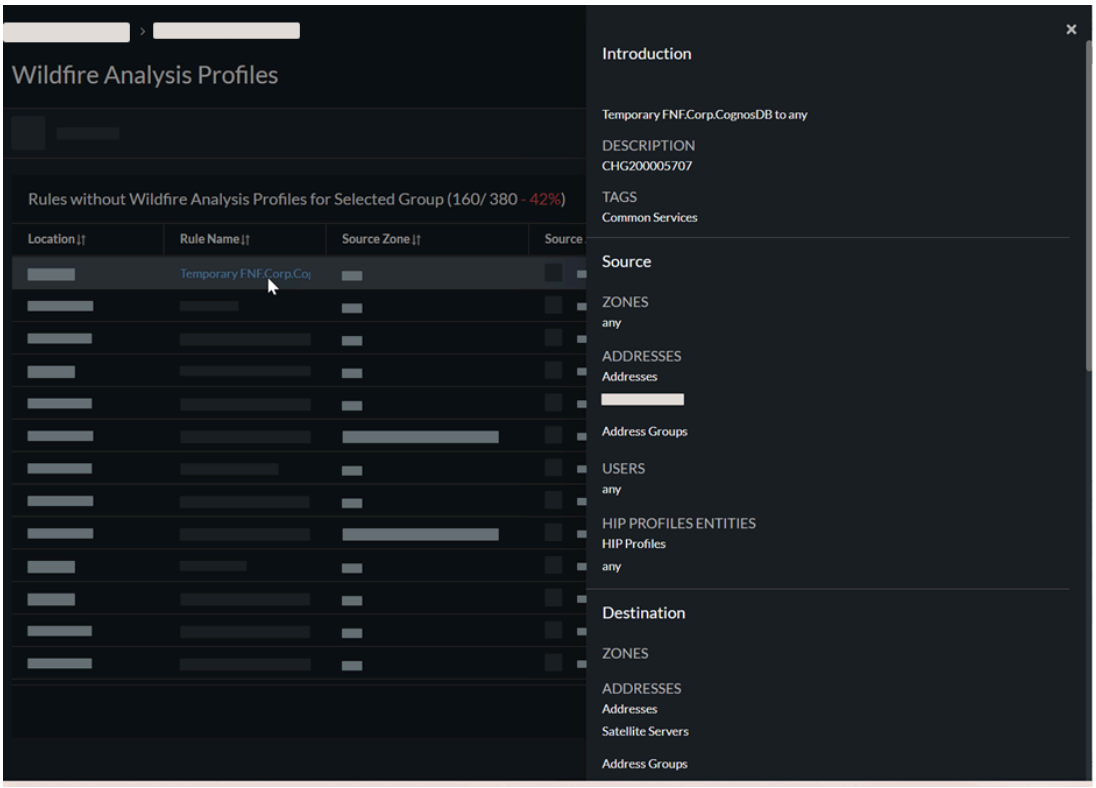


- *Cuando genera un informe BPA a demanda utilizando un TSF, la información de adopción de su TSF se refleja en el panel de adopción de funciones. (PAN-OS 9.1 y TSF superiores)*
- *Puede exportar datos de adopción en formato .csv para utilizarlos en aplicaciones de terceros como Microsoft Excel*

- Seleccione la sección de una característica en el gráfico para ver qué reglas de política carecen de esa característica.



- Seleccione una regla para ver sus detalles sin necesidad de salir de la aplicación.

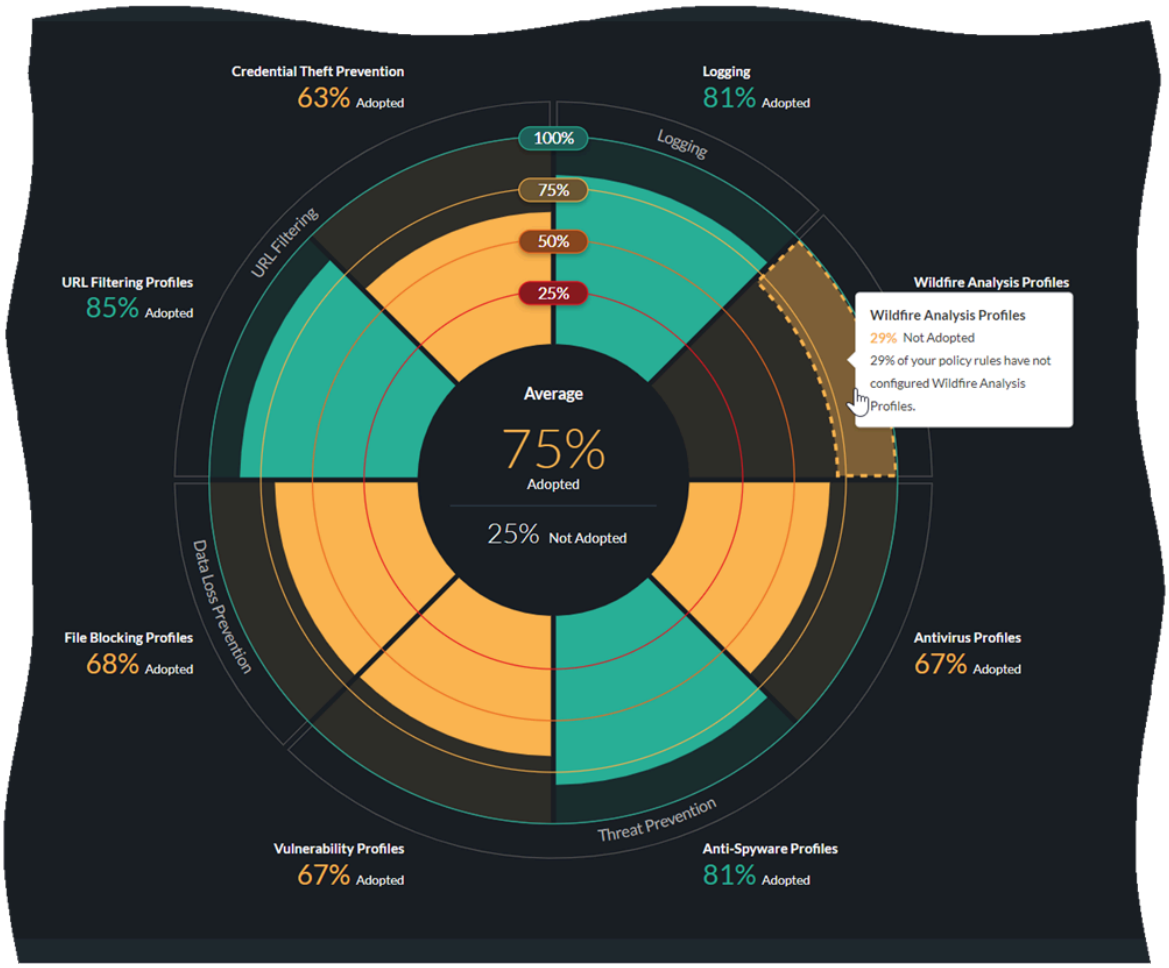


Identificar brechas en la adopción

Este panel muestra dónde su política de seguridad es sólida y dónde hay brechas en la adopción de capacidades que usted puede enfocar en mejorar. Para obtener la máxima visibilidad del tráfico y la máxima protección contra ataques, establezca objetivos para la adopción de la capacidad de seguridad y utilice las siguientes recomendaciones como una línea base de prácticas recomendadas. Evalúe su posición actual con respecto a la línea base para identificar las brechas en la adopción de la capacidad de la política de seguridad.

El resumen de adopción ayuda a identificar dispositivos, zonas y áreas donde puede mejorar la adopción de la capacidad de la política de seguridad. Puede revisar la información de adopción por grupo de dispositivos, número de serie y Vsys, zonas, áreas de arquitectura, etiquetas, detalles de reglas y asignaciones de zonas. Filtre por grupo de dispositivos para limitar el alcance e identificar brechas.

En **Dashboard (Panel)** > **Feature Adoption (Adopción de característica)**, seleccione **Overall Adoption (adopción general)** para verificar las tasas de adopción de las siguientes capacidades. Seleccione **Best Practices (Prácticas recomendadas)** para ver las tasas de adopción de estas capacidades que se adhieren a las prácticas recomendadas de Palo Alto Networks. Utilice esta información como criterios de identificación de brechas; si la tasa de adopción real no coincide con las recomendaciones, planifique cerrar la brecha:



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

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

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

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

En el resumen de aplicaciones, usuarios y puertos del resumen de adopción, verifique las tasas de adopción para las siguientes capacidades. Use las recomendaciones como criterios de identificación de brechas; si la tasa de adopción real no coincide con las recomendaciones, planifique cerrar la brecha:

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

En el resumen de registro de logs del Resumen de adopción, verifique las tasas de adopción para las siguientes capacidades. Use las recomendaciones como criterios de identificación de brechas; si la tasa de adopción real no coincide con las recomendaciones, planifique cerrar la brecha:

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

En resumen:

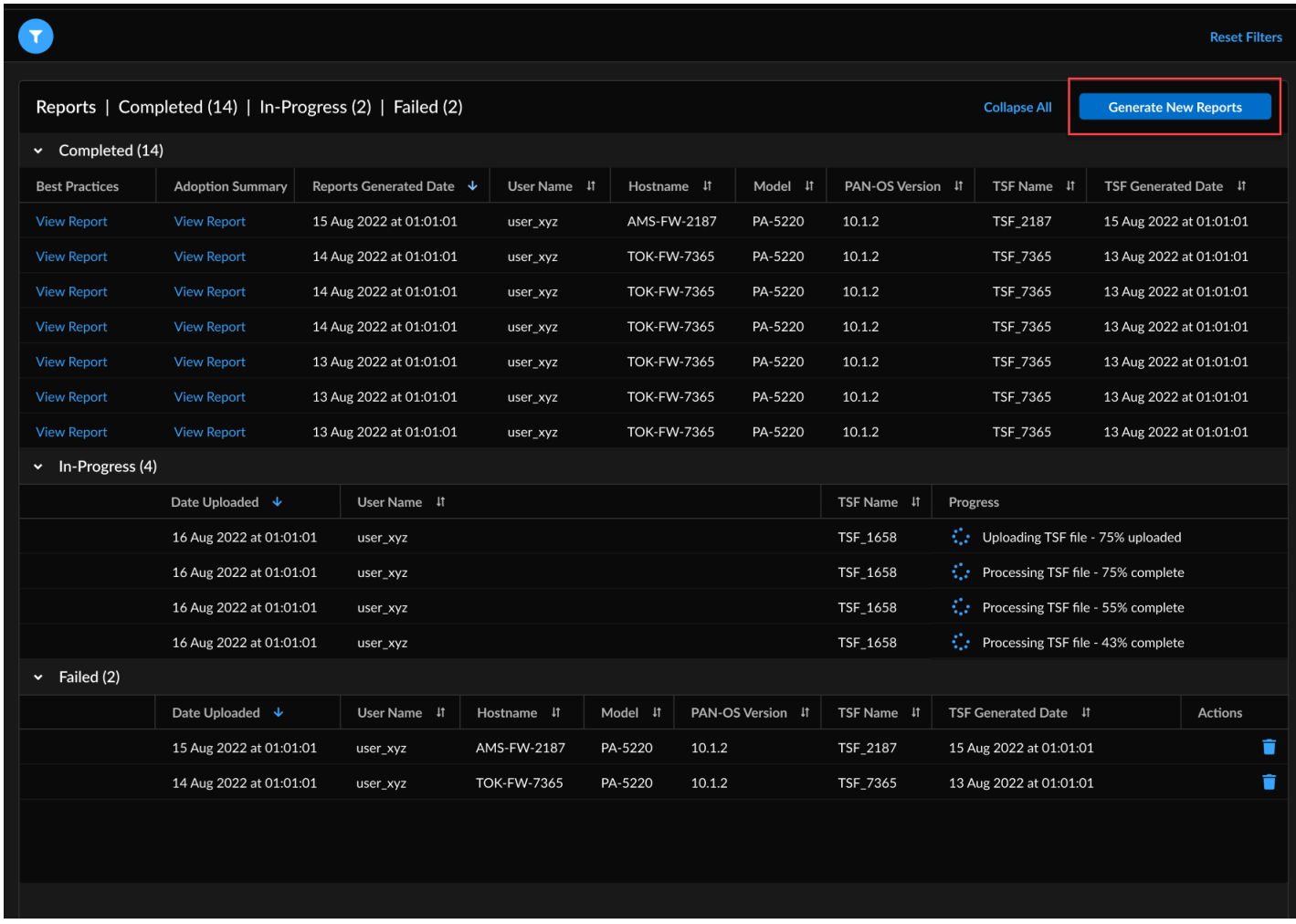
Función	Objetivo de adopción
WildFire	Lo más cerca posible al 100% de las reglas de la política de seguridad
Antivirus	Lo más cerca posible al 100% de las reglas de la política de seguridad
Antispyware	Lo más cerca posible al 100% de las reglas de la política de seguridad
vulnerabilidad	Lo más cerca posible al 100% de las reglas de la política de seguridad
Bloqueo de archivos	Lo más cerca posible al 100% de las reglas de la política de seguridad
Filtrado de URL y robo de credenciales	Todo el tráfico saliente de internet
App-ID	Lo más cerca posible al 100% de las reglas de la política de seguridad
User-ID	Todas las reglas con zonas de origen o rangos de direcciones que tienen presencia del usuario

Función	Objetivo de adopción
Servicio/puerto	Lo más cerca posible al 100% de las reglas de la política de seguridad
de creación de logs	Lo más cerca posible al 100% de las reglas de la política de seguridad
Log Forwarding	Lo más cerca posible al 100% de las reglas de la política de seguridad
Protección de zona	Todas las zonas

Panel: BPA bajo demanda

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW, incluidos los financiados por Créditos de NGFW de software	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium o Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

- Vaya a **Dashboards (Paneles)** > **On Demand BPA (BPA bajo demanda)** para comenzar.



¿Qué le muestra este panel?

El panel muestra el informe de Evaluación de prácticas recomendadas (BPA) basado en los archivos TSF cargados de los dispositivos.

Ahora puede ejecutar la Evaluación de prácticas recomendadas (BPA) y el resumen de Adopción de funciones directamente desde Strata Cloud Manager. Solo tiene que cargar un archivo de asistencia técnica (TSF). Puede generar el informe BPA bajo demanda para dispositivos que no envían datos de telemetría o están incorporados a AIOps para NGFW.

¿Cómo puede utilizar los datos del panel?

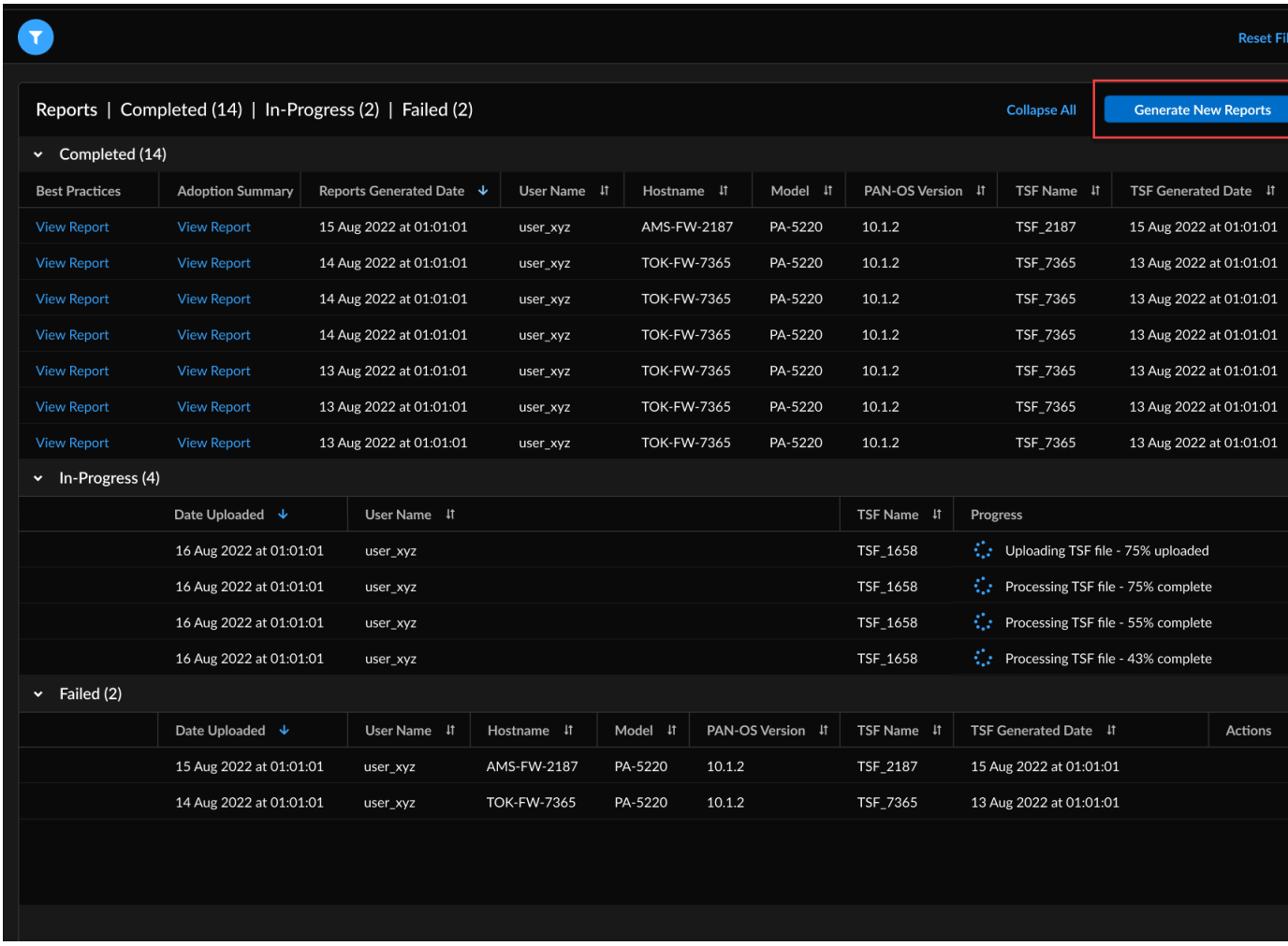
La BPA evalúa su postura de seguridad frente a las prácticas recomendadas de Palo Alto Networks y prioriza las mejoras para los dispositivos. Las prácticas recomendadas de seguridad previenen amenazas conocidas y desconocidas, reducen la superficie de ataque y proporcionan visibilidad del tráfico, para que pueda saber y controlar qué aplicaciones, usuarios y contenido hay en su red. Además, las prácticas recomendadas incluyen verificaciones para los controles críticos de seguridad (CSC) del Centro de Seguridad en Internet. Consulte la orientación sobre prácticas recomendadas para reforzar la postura de seguridad e implementar mejoras.

Generar informe BPA bajo demanda

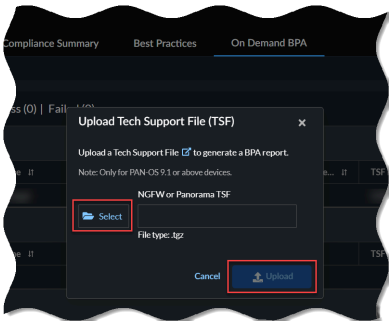
Siga estos pasos para generar el informe BPA bajo demanda.

STEP 1 | Vaya a **Dashboards (Paneles)** > **On Demand BPA (BPA bajo demanda)**.

STEP 2 | **Generate New BPA Report (Generar nuevo informe de BPA).**



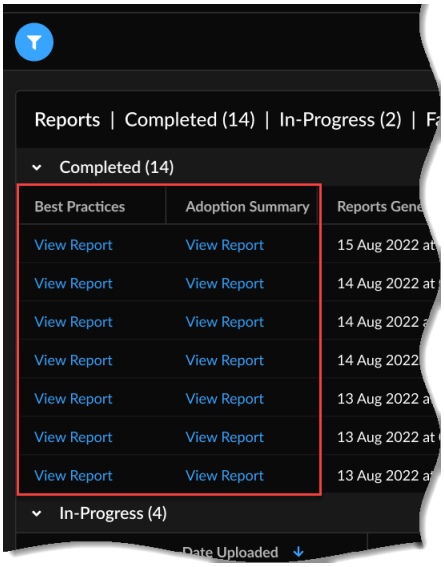
STEP 3 | Deberá **Select TSF (Seleccionar TSF)** y **Upload TSF (Cargar el archivo TSF)**.



El tiempo de carga depende del tamaño de su archivo .tgz y la velocidad de Internet. Cargar el archivo podría tardar unos minutos para archivos más grandes. Expanda **In-Progress (En curso)** para ver el estado de los archivos TSF.

- *BPA bajo demanda admite solo los archivos de asistencia técnica (TSF) en el formato de archivo .tgz.*
- *BPA bajo demanda admite TSF desde dispositivos con la versión 9.1 o superior de PAN-OS para la generación de informes.*
- *Para obtener información sobre la captura, el procesamiento y el almacenamiento de telemetría de datos de Palo Alto Networks, consulte la* Privacidad de AIOps para NGFW *en el* Centro de confianza.

STEP 4 | **View Report (Ver informe)** debajo de **Completed (Completado)** para ver los resultados.



Panel: Estado de SASE

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	• Uno de estos: ❑ Prisma Access y Observabilidad ADEM ❑ Strata Cloud Manager Pro • Un rol que tiene permiso para ver el panel → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

¿Qué le muestra este panel?

Este panel le muestra el estado general de sus usuarios móviles, sitios remotos y aplicaciones (si ha comprado una licencia de AI-Powered ADEM) que están actualmente conectados a Prisma Access. Los números en los círculos representan el número de usuarios o sitios que están conectados actualmente desde la ubicación de Prisma Access donde aparecen. Un punto representa un solo usuario o sitio. Las áreas del mapa que tienen un fondo azul indican que los números mostrados en esa región son una predicción o pronóstico.

Filtra los datos que se muestran en este panel con uno o más de los siguientes filtros

- el intervalo de tiempo
- Ubicación de Prisma Access
- Ubicación de la fuente

¿Cómo puede utilizar los datos del panel de control?

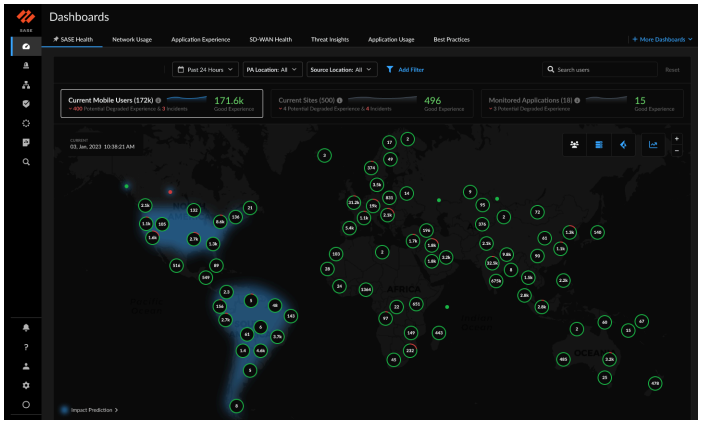
Utilice el panel de control para obtener una descripción general y el estado general de cuántos usuarios móviles y sitios remotos están conectados a Prisma Access, categorizados por su ubicación en el mapa. También puede ver su estado general en este panel.

Panel de estado de SASE: Usuarios móviles actuales: vista de mapa

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	• Uno de estos: ❑ Prisma Access y Observabilidad ADEM ❑ Strata Cloud Manager Pro • Un rol que tiene permiso para ver el panel

¿Dónde puedo usar esto?	¿Qué necesito?
	→ Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

La pestaña **Current Mobile Users (Usuarios móviles actuales)** en el panel de **SASE Health (Estado de SASE)** le muestra una descripción general del desglose de la experiencia de los usuarios móviles en todas las ubicaciones. El número en los círculos corresponde a la cantidad de usuarios móviles que están actualmente conectados a Prisma Access usando GlobalProtect. Un punto representa un solo usuario móvil. Un círculo o punto verde indica una buena puntuación de experiencia de usuario. Del mismo modo, un color rojo indica una puntuación de experiencia degradada. Las puntuaciones de experiencia degradadas comprenden puntuaciones Regular y Deficientes combinadas. El gráfico de líneas a la derecha de **Current Mobile Users (Usuarios móviles actuales)** muestra una tendencia de los puntuaciones de experiencia promedio de todos los usuarios móviles durante el **Time Range (Rango de tiempo)** seleccionado.



Haga clic en el número (que representa el número de usuarios con experiencia potencialmente degradada) junto a **Potential Degraded Experience (Experiencia potencial degradada)** o **Incidents (Incidentes)** para ver los detalles de la experiencia del usuario degradada en un panel que se abre a la izquierda.

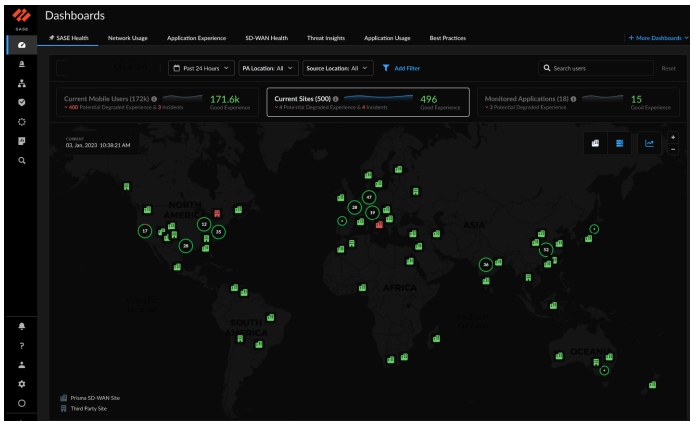
Panel de estado de SASE: Sitios actuales - Vista de mapa

¿Dónde puedo usar esto?	¿Qué necesito?

• Prisma Access (Managed by Panorama or Strata Cloud Manager)	• Uno de estos:
	  ❑ Prisma Access y Observabilidad ADEM
	  ❑ Strata Cloud Manager Pro
	• Un rol que tiene permiso para ver el panel
	→ Las características y capacidades disponibles para usted en Strata Cloud

¿Dónde puedo usar esto?	¿Qué necesito?
	Manager depende de qué licencia(s) esté usando.

Este panel muestra el número de sitios configurados que se conectan a ubicaciones de Prisma Access en todo el mundo. El número incluido entre paréntesis es el número total de sitios conectados y el número a la derecha en la tarjeta es el número de sitios que están con puntuaciones de Buena experiencia. Los sitios cuyas puntuaciones de experiencia no se pueden obtener por ningún motivo no se excluyen al calcular el número de sitios conectados. El gráfico de la línea azul indica la tendencia de la puntuación media de experiencia de todos los sitios a lo largo del tiempo. Debajo de los Sitios actuales se ve el número de sitios con puntuación de experiencia degradada (deficiente) junto con el número de Incidentes para todos los sitios. Los incidentes pueden incluir una o más de las siguientes categorías: Infraestructura, servicios de red, centros de datos y sitios de terceros (los centros de datos están caídos).



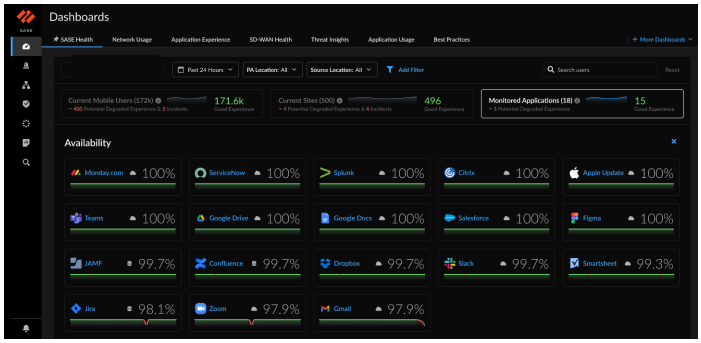
Panel de estado de SASE: Aplicaciones supervisadas

¿Dónde puedo usar esto?	¿Qué necesito?

• Prisma Access (Managed by Panorama or Strata Cloud Manager)	• Uno de estos:
	  ❑ Prisma Access y Observabilidad ADEM
	  ❑ Strata Cloud Manager Pro
	• Un rol que tiene permiso para ver el panel
	→ Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Consulte las métricas de disponibilidad de aplicaciones en la pestaña **Monitored Applications (Aplicaciones supervisadas)** del panel **SASE Health (Estado de SASE)**. Este panel le muestra cuántas aplicaciones se supervisan a través de ADEM y cuántas de ellas están experimentando una puntuación degradada. Este número tiene en cuenta la experiencia de aplicación tanto para usuarios móviles como para sitios remotos. Las aplicaciones con puntuaciones de experiencia de

aplicación Deficientes o Regulares se consideran como experiencia degradada. También puede ver la disponibilidad de la aplicación durante el intervalo de tiempo que seleccione con el filtro.



El número a la derecha del nombre de la aplicación le indica el porcentaje de tiempo durante el **intervalo de tiempo** que la aplicación estuvo disponible.

Supervisar Strata Cloud Manager

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software • Prisma SD-WAN	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN Las otras licencias y requisitos previos necesarios para la visibilidad son: ❑ Observabilidad de ADEM ❑ DEM autónomo para redes remotas ❑ ADEM con tecnología de IA ❑ Informes de claridad de WAN ❑ Un rol que tiene permiso para ver el panel → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Obtenga una visibilidad completa del tráfico de su red y de los productos y suscripciones que gestiona con Strata Cloud Manager. Puede supervisar de forma protectora el estado de conectividad y el estado de sus redes remotas, aplicaciones, dispositivos NGFW y usuarios móviles en Prisma Access. Strata Cloud Manager también proporciona funciones para supervisar el rendimiento de los servicios de red comunes, los detalles de consumo de sus licencias de suscripción y gestionar la herramienta utilizada para analizar los problemas de conectividad. Los usuarios de Prisma SD-WAN también pueden supervisar el estado de conectividad de las aplicaciones Prisma SD-WAN, dispositivos ION, centros de datos aquí en un único lugar.

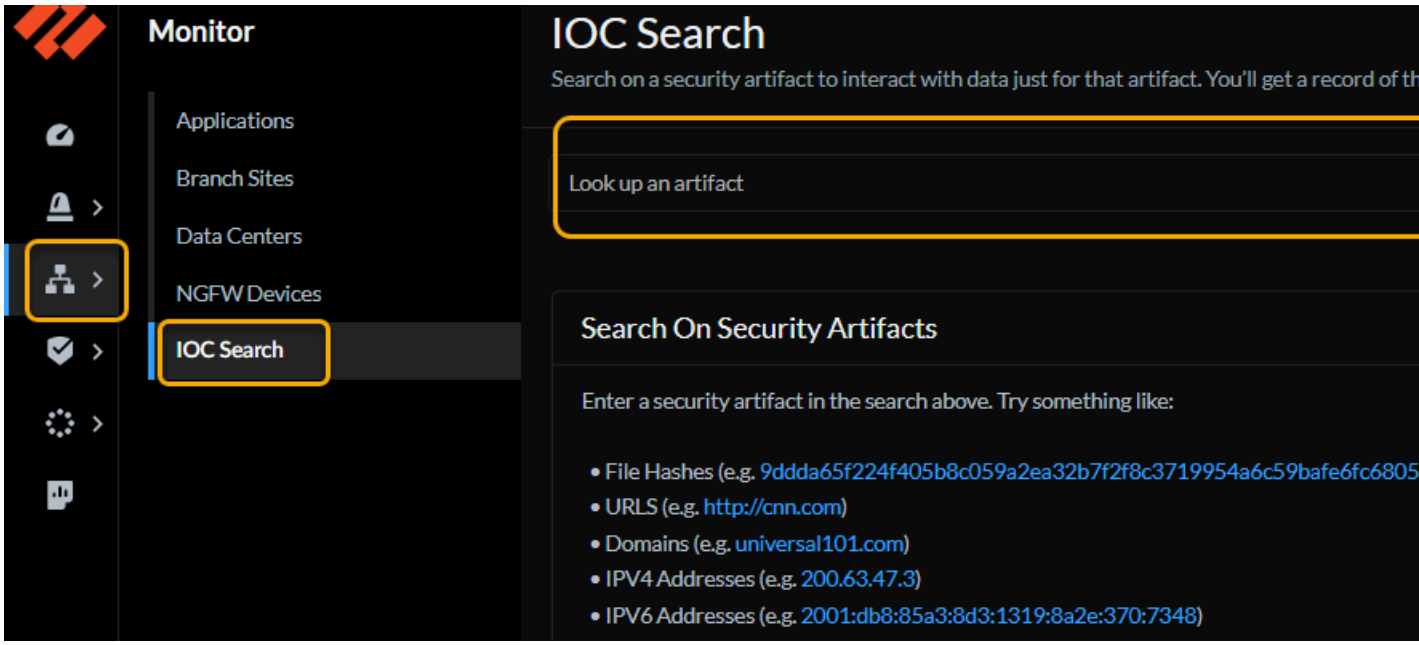
Supervisar Búsqueda del COI

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software • Prisma SD-WAN	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN Las otras licencias y requisitos previos necesarios para la visibilidad son: ❑ Observabilidad de ADEM ❑ DEM autónomo para redes remotas ❑ ADEM con tecnología de IA ❑ Informes de claridad de WAN ❑ Un rol que tiene permiso para ver el panel → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Puede buscar un artefacto de seguridad para interactuar con los datos solo para ese artefacto. Los resultados de búsqueda incluyen:

- Historial y actividad del artefacto en su red. *Evalúe cuán prevalente es el artefacto en su red y compárelo con los pares del sector.*
- Inteligencia de amenazas de Palo Alto Networks sobre el artefacto, basado en el análisis de todo el tráfico que Palo Alto Networks procesa y analiza.
- Hallazgos consolidados de análisis de terceros para el artefacto.

Haga clic en **Monitor (Supervisar)** > **IOC Search (Búsqueda de IOC)** para comenzar.

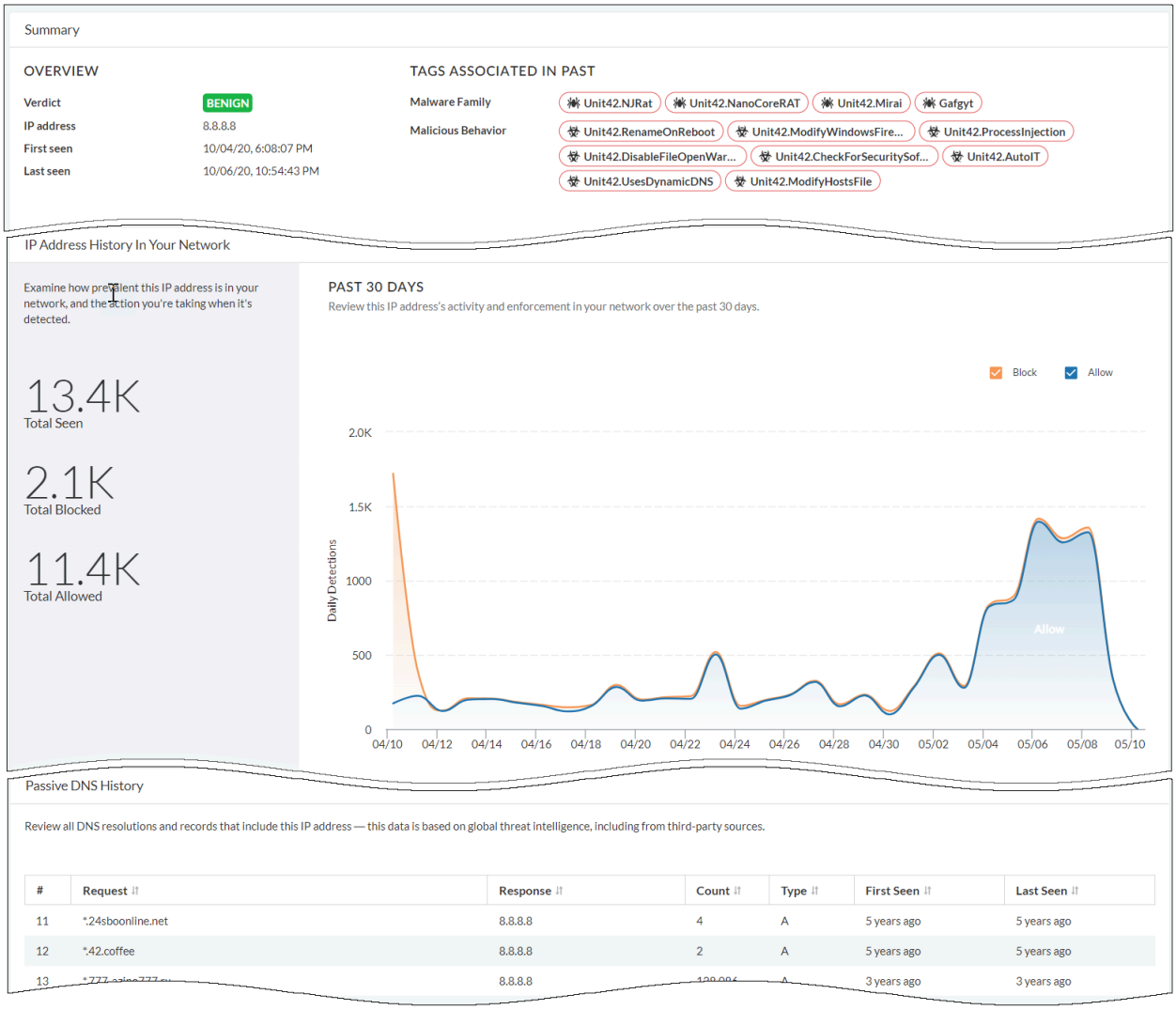


Para empezar, busque uno de estos tipos de artefactos: un **hash de archivo**, una **URL**, un **dominio** o una **dirección IP** (IPv4 o IPv6).

Dirección IP

Puede buscar una dirección IP para analizar la información de amenazas relacionada con las actividades de dirección IP en su red. En el resultado de la búsqueda se muestran los siguientes datos:

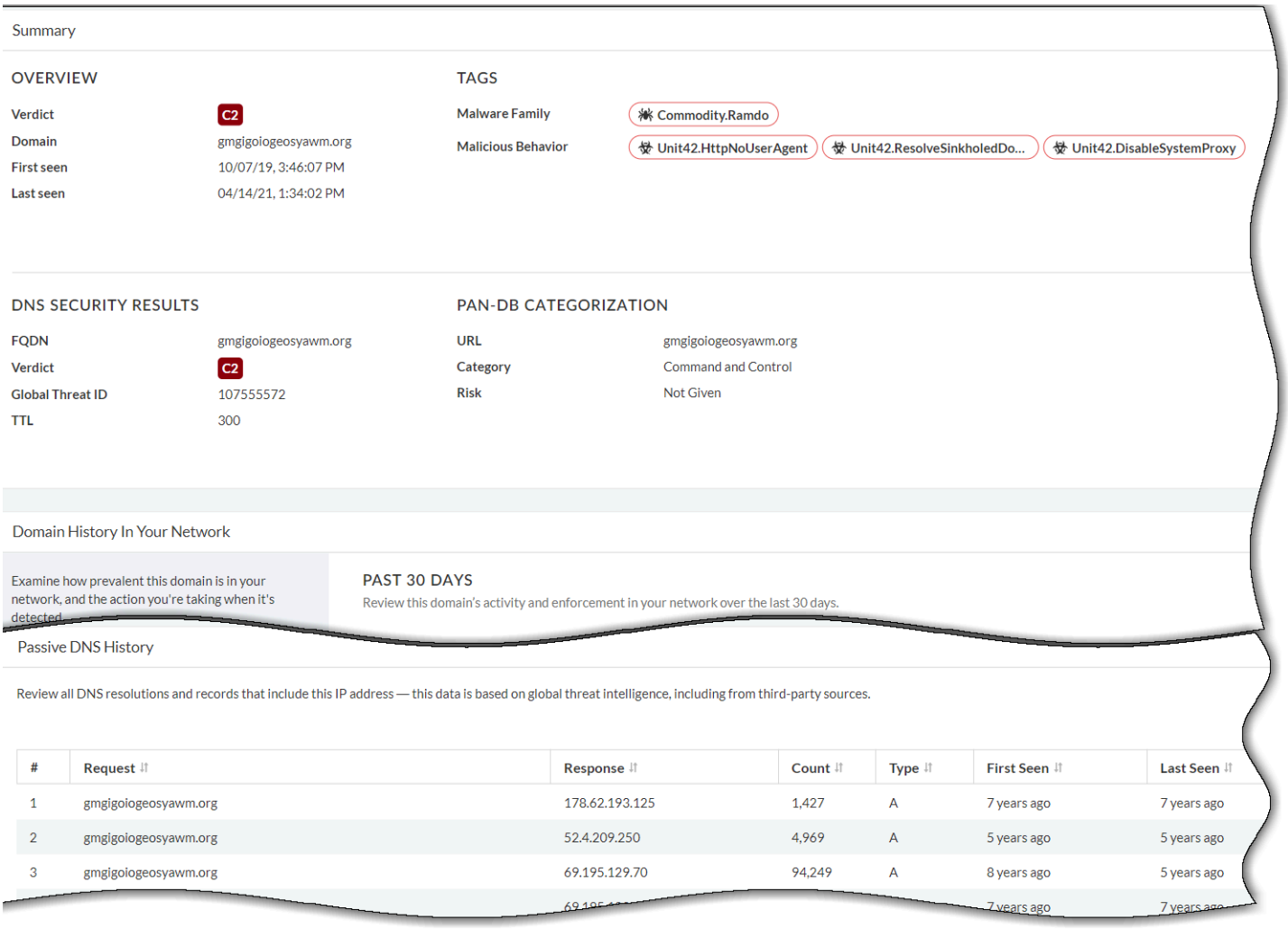
- Número total de veces que se detectó una dirección IP en su red en los últimos 30 días.
- Representación gráfica de la acción realizada (permitir o bloquear) en la dirección IP.
- Lista de solicitudes de DNS que contienen la dirección IP basada en la inteligencia de amenazas de Palo Alto Networks y fuentes de terceros.



Dominio

Vea un resumen de las actividades asociadas al dominio en su red. Los resultados de la búsqueda incluyen:

- Clasificación del dominio en su red basada en el análisis de muestra WildFire.
- Número total de actividades asociadas al dominio en los últimos 30 días.
- Imposición aplicada a cada actividad en un formato gráfico.
- Información del análisis de WildFire que respalda los datos utilizados para asignar el veredicto para el dominio.
- Actividad DNS recopilada de todos los envíos de WildFire que contienen instancias de este dominio.


Summary

OVERVIEW

Verdict C2
Domain gmgigoiogeosyawm.org
First seen 10/07/19, 3:46:07 PM
Last seen 04/14/21, 1:34:02 PM

TAGS

Malware Family Commodity.Ramdo
Malicious Behavior Unit42.HttpNoUserAgent Unit42.ResolveSinkholedDo... Unit42.DisableSystemProxy

DNS SECURITY RESULTS

FQDN gmgigoiogeosyawm.org
Verdict C2
Global Threat ID 107555572
TTL 300

PAN-DB CATEGORIZATION

URL gmgigoiogeosyawm.org
Category Command and Control
Risk Not Given

Domain History In Your Network

Examine how prevalent this domain is in your network, and the action you're taking when it's detected.

PAST 30 DAYS

Review this domain's activity and enforcement in your network over the last 30 days.

Passive DNS History

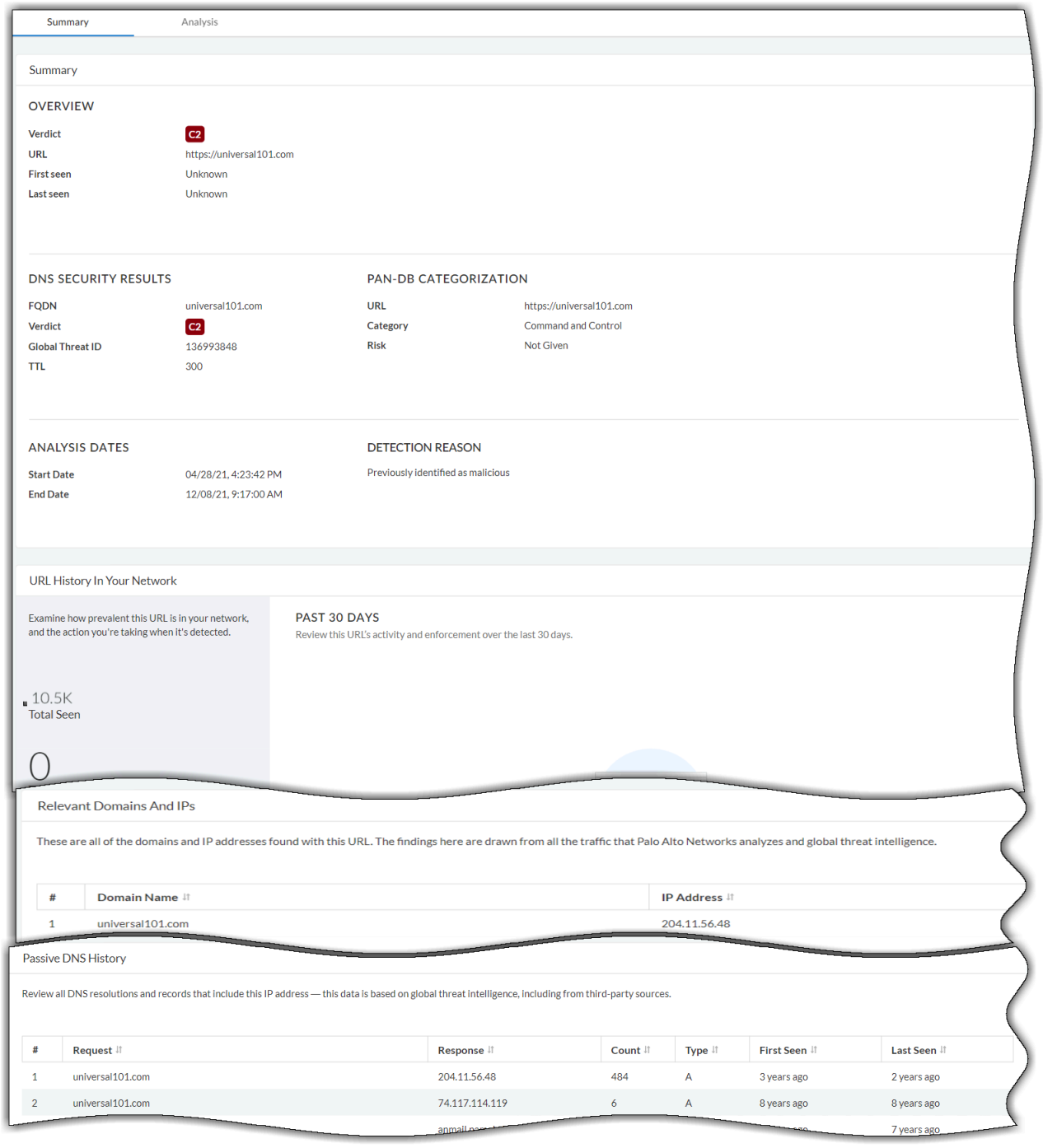
Review all DNS resolutions and records that include this IP address — this data is based on global threat intelligence, including from third-party sources.

#	Request	Response	Count	Type	First Seen	Last Seen
1	gmgigoiogeosyawm.org	178.62.193.125	1,427	A	7 years ago	7 years ago
2	gmgigoiogeosyawm.org	52.4.209.250	4,969	A	5 years ago	5 years ago
3	gmgigoiogeosyawm.org	69.195.129.70	94,249	A	8 years ago	5 years ago
		69.195			7 years ago	7 years ago

URL

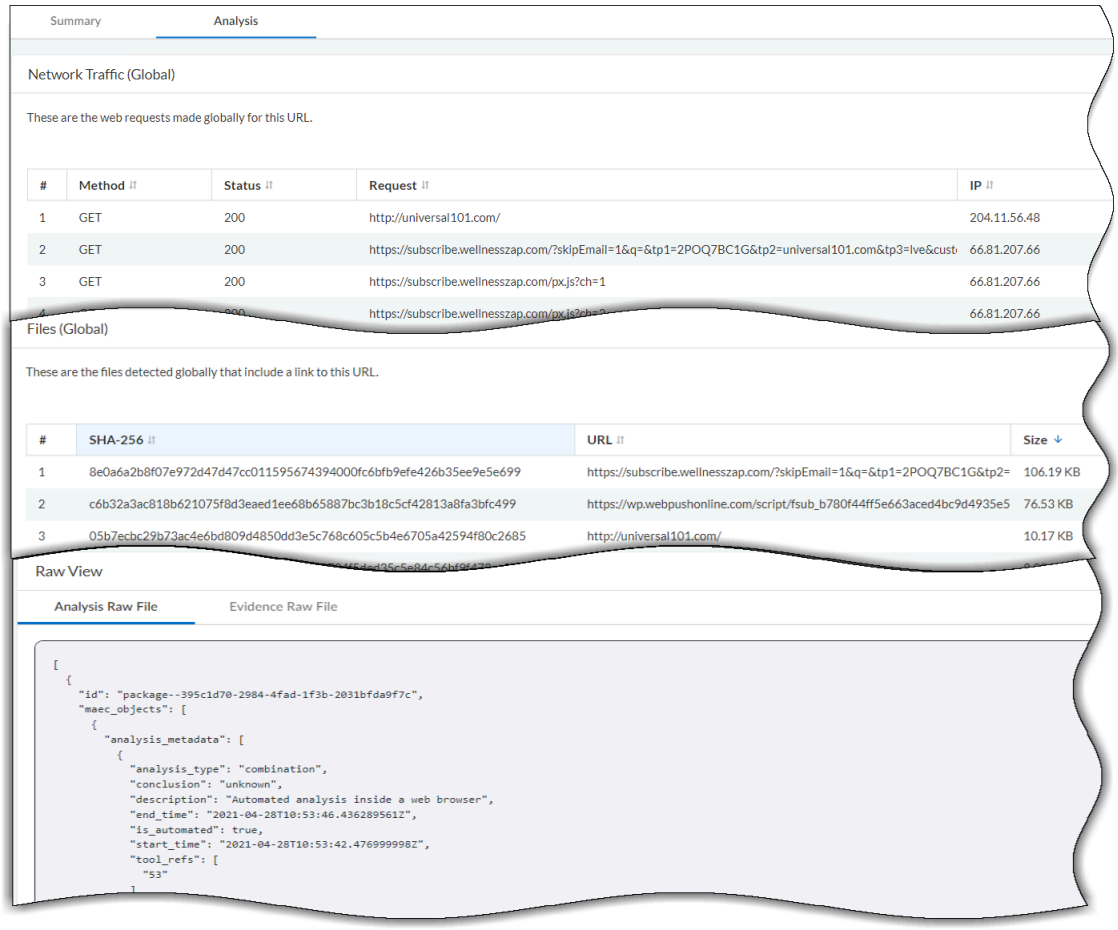
Obtenga información sobre la actividad de la URL en todo el tráfico que Palo Alto Networks analiza. Los resultados de la búsqueda incluyen:

Resumen: revisa un resumen de la actividad de la URL en su red. Los datos incluyen: Hallazgos de DNS Security para la URL y la categorización de PAN-DB.



Captura de pantalla: muestra una instantánea del sitio web cuando se busca en un artefacto URL.

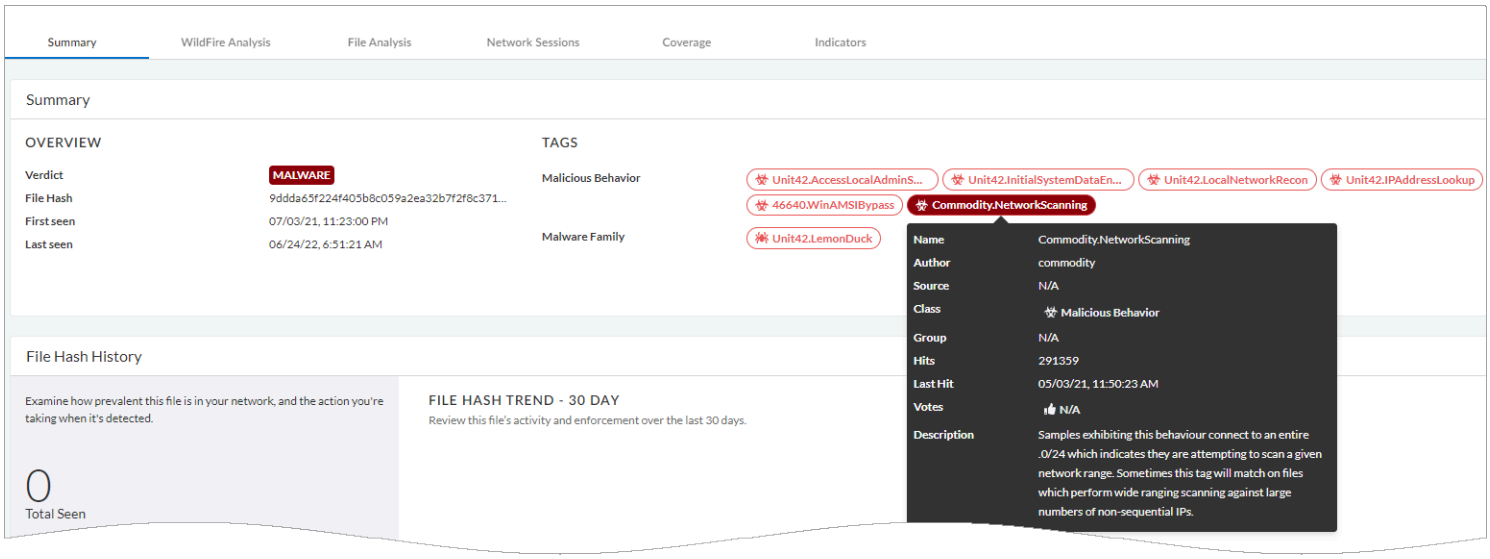
Análisis: consulte los datos de análisis de archivos que incluyen las solicitudes realizadas globalmente para esta URL, y los archivos detectados con esta URL. Puede usar el valor hash del archivo o la vista de archivo para saber más.



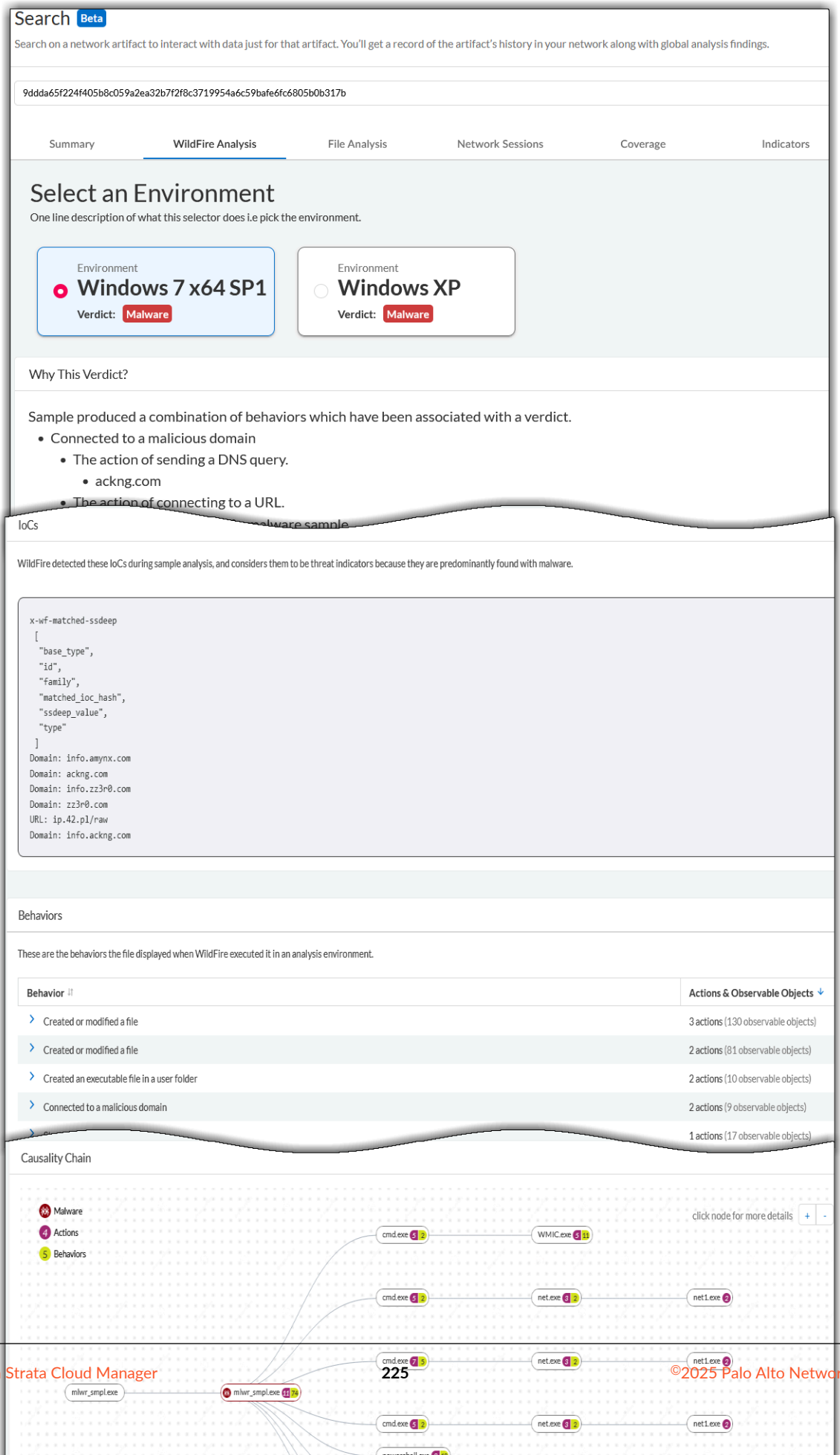
Hash de archivo

La búsqueda de hash de archivos resume la actividad del archivo, el análisis de las propiedades del archivo y los detalles del análisis de muestras de WildFire. Puede profundizar en el resultado de la búsqueda para revisar los siguientes datos:

Resumen: vea el veredicto hash del archivo y el historial de la actividad del archivo en su red. Haga clic en el nombre de la etiqueta para ver los detalles de la etiqueta. Las etiquetas pueden ayudarle a entender si el archivo es parte de alguna familia, campaña o actor de amenazas.



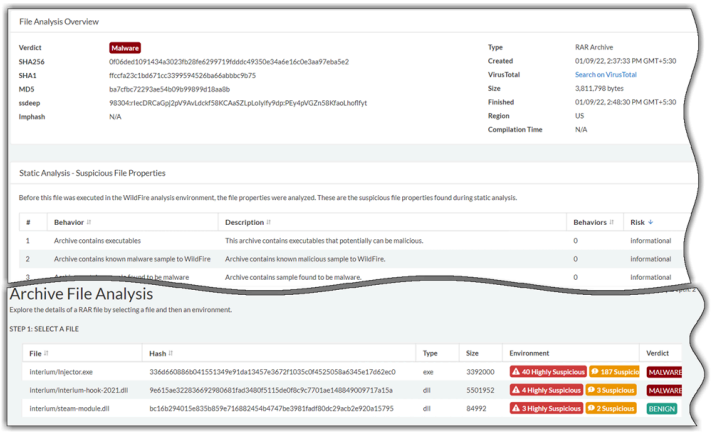
Análisis WildFire: evalúe cómo se comportó la muestra (archivo) durante el análisis de WildFire. Puede ver la información sobre el veredicto de la muestra, los indicadores de amenaza detectados durante el análisis de la muestra y el comportamiento durante el procesamiento de la muestra en el entorno de análisis. También puede ver las capturas de pantalla de los diversos hitos del proceso capturados durante el análisis de muestra de WildFire.



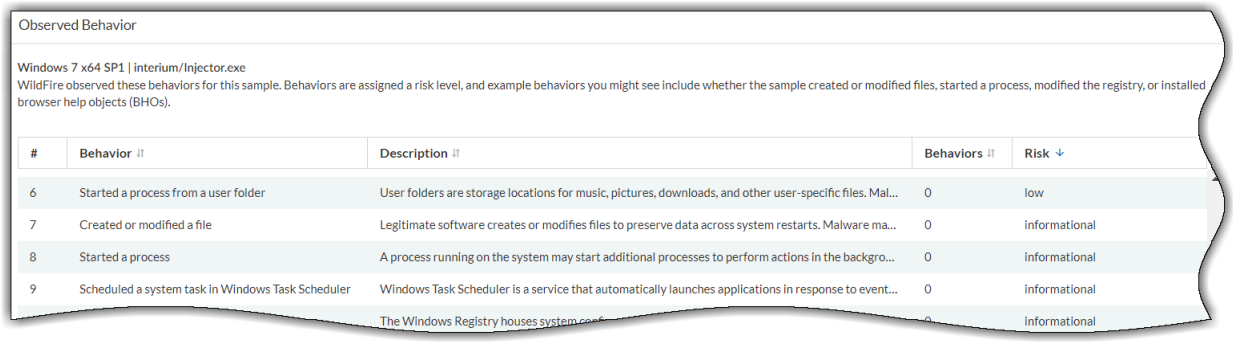
Análisis de archivos: compare el análisis antes y después de la ejecución de la muestra (archivo) en el entorno de análisis de WildFire.

Descripción general: compruebe el veredicto de la muestra aquí. Si el veredicto se clasifica incorrectamente, solicite un cambio de veredicto. El equipo de amenazas de Palo Alto Networks investiga más a fondo la muestra y actualiza el veredicto si se considera incorrecto.

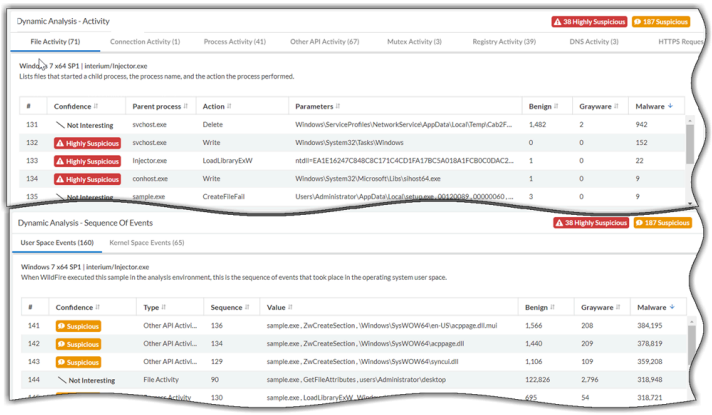
Análisis estático: el análisis estático analiza el contenido de un archivo específico antes de ejecutarlo en el entorno de análisis WildFire. La búsqueda también muestra las propiedades sospechosas del archivo encontradas durante el análisis estático. El resultado de la búsqueda varía según el tipo de archivo. La captura de pantalla muestra un análisis estático de un archivo de fichero.



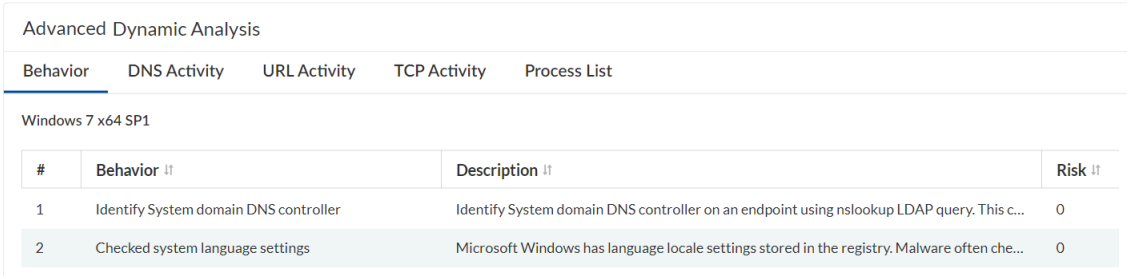
Comportamiento observado: revise el análisis de comportamiento de WildFire de la muestra en un entorno particular.



Análisis dinámico: inspecciona el archivo en detalle extrayendo información e indicadores adicionales para una red comprometida. Puede comprobar las actividades de proceso involucradas y la secuencia de eventos que tuvieron lugar en su sistema mientras ejecutaba el archivo.

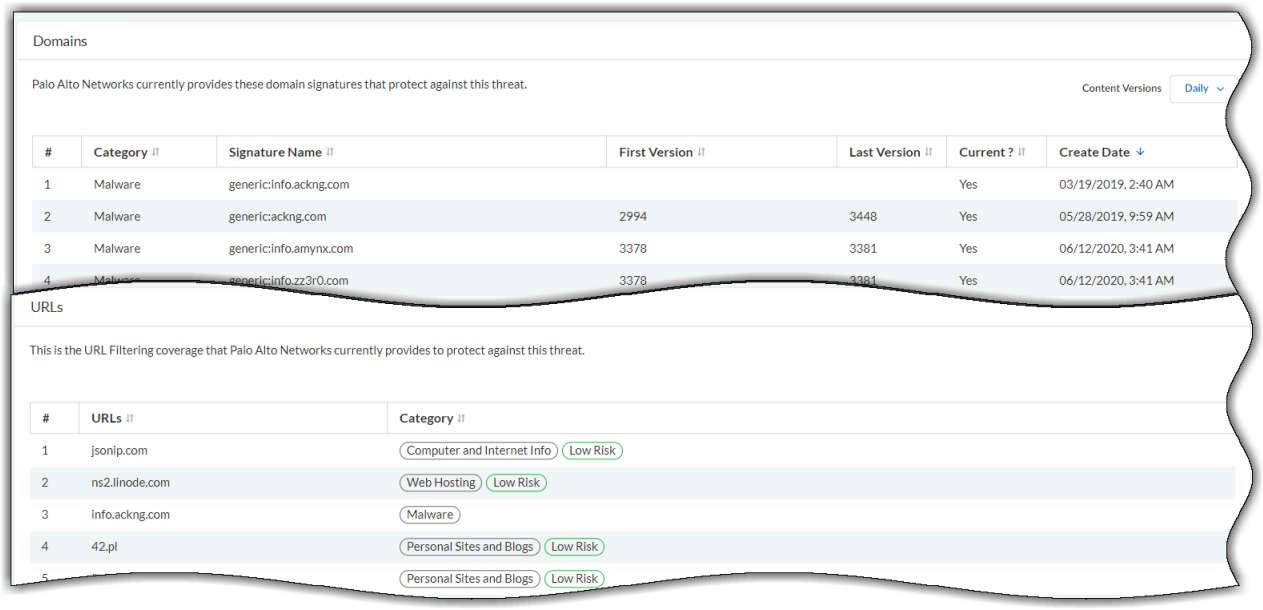


Análisis dinámico avanzado: vea los resultados del análisis de muestras analizadas por técnicas de Advanced WildFire (análisis inteligente de memoria en tiempo de ejecución, análisis dinámico de hipervisor, emulación de dependencias, etc.), un motor basado en la nube que detecta y previene amenazas de malware altamente evasivas. Puede ver los comportamientos observados y utilizar esta información para el análisis posterior a la ejecución.



Sesiones de red: obtenga información sobre la sesión de red para una muestra. Utilice estos datos para obtener más información sobre el contexto de la amenaza, conocer los hosts y clientes afectados y las aplicaciones utilizadas para entregar el malware.

Cobertura: compruebe la cobertura de firma para una muestra para evaluar el nivel de protección contra amenazas. Puede ver las firmas etiquetadas en los dominios desde donde se descargó la muestra y las URL a las que accede la muestra.



Indicadores: vea los artefactos que son indicadores de una red existente. Los indicadores se clasifican en función de los tipos de artefactos; dominio, dirección IP, URL, encabezados de agente de usuario y objetos de exclusión mutua. Los artefactos de alto riesgo se etiquetan como sospechosos o altamente sospechosos.

Domain

2 Highly Suspicious 4 Suspicious 4 Interesting

These domains - seen when this sample was executed in the WildFire analysis environment - are predominantly found with malware, and can indicate a compromised network.

#	Confidence	Indicator	Matching Indicators	Benign	Grayware	Malware
1	Highly Suspicious	info.ackng.com		0	0	234
2	Highly Suspicious	42.pl		97	5	499
3	Suspicious	ns3.epik.com		555	43	28,611
					44	28,595

IPv4

1 Highly Suspicious 2 Suspicious

These IP addresses - seen when this sample was executed in the WildFire analysis environment - are predominantly found with malware, and can indicate a compromised network.

#	Confidence	Indicator	Matching Indicators	Benign	Grayware	Malware
1	Highly Suspicious	88.214.207.96		30	1	277
2	Suspicious	127.0.0.1		273,674	891,030	7,528,431
					8	562

URL

1 Highly Suspicious 4 Interesting

These URLs - seen when this sample was executed in the WildFire analysis environment - are predominantly found with malware, and can indicate a compromised network.

#	Confidence	Indicator	Matching Indicators	Benign	Grayware	Malware
1	Highly Suspicious	/e.png?id=		0	0	233
2	Suspicious	ip.42.pl/raw		104	7	507
3	Interesting	zz3r0.com/e.png?id=GVZ823834177364.GVZ823834177364.local&ma...		--	--	--

1 Suspicious User-Agent

ninantly found with malware, and can indicate a compromised network.

	Benign	Grayware	Malware
	5,162	26,246	54,432

These user agent headers - seen for HTTP requests that were sent when this sample was executed in the WildFire analysis environment - are predor

#	Confidence	Indicator	Matching Indicators
1	Suspicious	Python-urllib/2.7	

5 Interesting

ltaneously. These mutexes are predominantly found with malware, and can indicate

	Benign	Grayware	Malware
	1	0	0
	--	--	--
		--	--

Mutex

A mutex (mutual exclusion object) allows programs to share the same resource, though the resource cannot be used by more than one program simu a compromised network.

#	Confidence	Indicator	Matching Indicators
1	Interesting	testmutex_{D0E858DF-985E-4907-B7FB-8D732C3FC3B9}	
2	Interesting	Local\c:!users!jgs9ctxe4snol!appdata!roaming!microsoft!windows!cookies!	

Supervisar Sucursales

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software • Prisma SD-WAN	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro ☐ Prisma SD-WAN Las otras licencias y requisitos previos necesarios para la visibilidad son: ☐ Observabilidad de ADEM ☐ DEM autónomo para redes remotas ☐ ADEM con tecnología de IA ☐ Informes de claridad de WAN ☐ Un rol que tiene permiso para ver el panel → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Sucursales: Prisma Access

Seleccione **Monitor (Supervisar)** > **Branch Sites (Sucursales)** > **Prisma Access** para ver el estado y la conectividad de sus redes remotas y el uso de todas sus Redes remotas implementadas en diferentes ubicaciones de Prisma Access. Muestra el estado de la conectividad en tiempo real y los detalles de consumo de ancho de banda, junto con otros detalles de implementación. Los usuarios móviles, las sucursales y los comercios minoristas se conectan a redes remotas. También puede ver el estado de los túneles configurados en las redes remotas y los usuarios móviles.

Además de los widgets que se muestran con la licencia de Prisma Access, este panel muestra la puntuación de la experiencia del sitio y detalles de la sucursal Prisma SD-WAN solo si tiene la página ADEM Observability o la licencia AI-Powered ADEM.

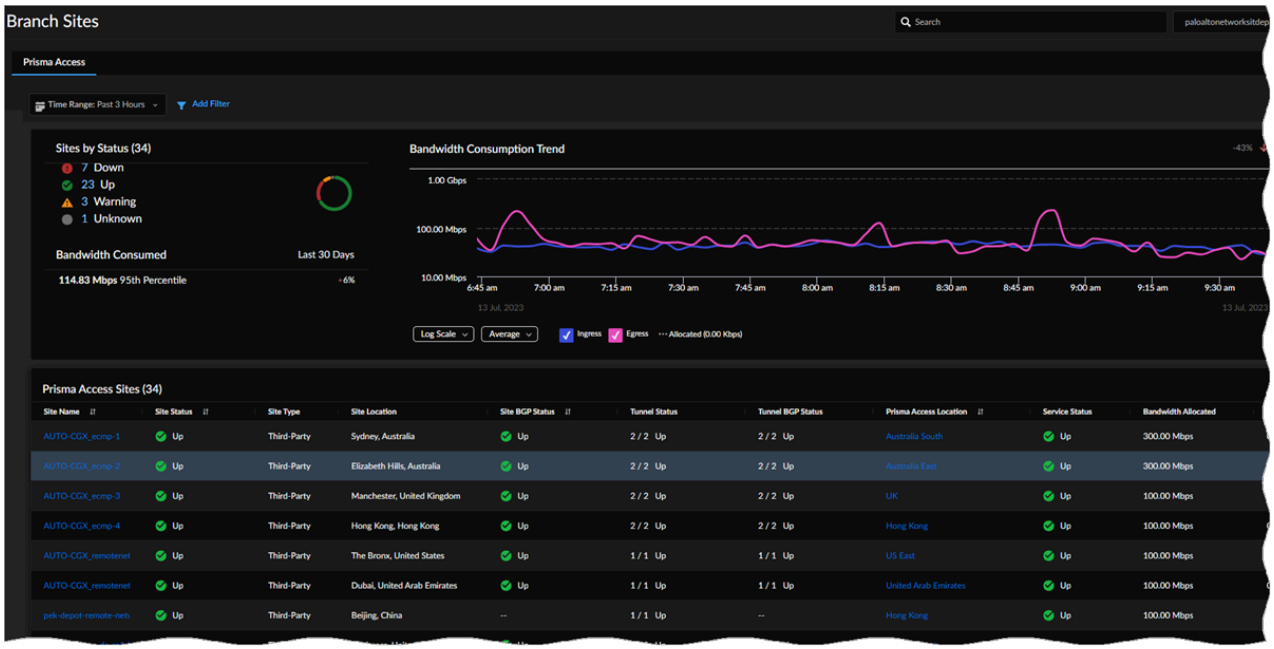
Sucursales: Prisma SD-WAN

Seleccione **Monitor (Supervisar)** > **Branch Sites (Sucursales)** > **Prisma SD-WAN** para configurar una sucursal en Prisma SD-WAN. Los sitios de sucursales incluyen las sucursales que tiene en su red de área amplia en Prisma SD-WAN. Puede configurar una sucursal antes o después de que los dispositivos ION lleguen a un sitio determinado. La sucursal en Prisma SD-WAN proporciona las siguientes vistas:

- La vista de **Mapa** de la sucursal proporciona el estado de conectividad de los dispositivos de la sucursal con el controlador y el estado de alarma del sitio.
- La vista **Lista** muestra cuántos sitios estaban activos durante el **Time Range (Intervalo de tiempo)** seleccionado y las métricas de estado general de las sucursales.
- La vista **Actividad** presenta los análisis clave de la aplicación, la puntuación de estado del sitio más reciente y la distribución del estado del sitio a lo largo del tiempo.
- Prisma Access
- Prisma SD-WAN

Sucursales (Prisma Access)

Seleccione **Branch Sites (Sucursales)** > **Prisma Access** para ver el estado y la conectividad de sus redes remotas y el uso de todas sus Redes remotas desplegadas en diferentes ubicaciones de Prisma Access.



Muestra el estado de la conectividad en tiempo real y los detalles de consumo de ancho de banda, junto con otros detalles de implementación. Los usuarios móviles, las sucursales y los comercios minoristas se conectan a redes remotas. También puede ver el estado de los túneles configurados en las redes remotas y los usuarios móviles. Para obtener una descripción detallada de estos widgets, consulte Ver y supervisar sucursales.

Usted puede:

- Consulte sus sitios de redes remotas por estado.
- Vea las tendencias en el consumo de ancho de banda de redes remotas.
- Vea sus sitios de Prisma Access y seleccione cualquier sitio para ver más detalles.
- Abra los **IPSec Termination Node Utilization Details (Detalles de utilización del nodo de terminación IPSec)** para ver los detalles de consumo de ancho de banda de cada SPN en el sitio.

- Ver datos de túnel y tendencias de túnel para un sitio.
- Vea la información sobre el estado del sitio, la salud, la conectividad y el consumo.

Sucursales (Prisma SD-WAN)

Puede configurar una sucursal antes o después de que los dispositivos ION lleguen a un sitio determinado. La sucursal en Prisma SD-WAN proporciona las siguientes vistas:

- La vista de **Mapa** de la sucursal proporciona el estado de conectividad de los dispositivos de la sucursal con el controlador y el estado de alarma del sitio. Cuando se selecciona una sucursal, se muestra la siguiente información:
  - Resumen del sitio: se utiliza para el análisis y la resolución de problemas.
  - Configuraciones: se utiliza para la configuración del sitio y del dispositivo.
  - Conexiones superpuestas: se utiliza para ver el estado de todas las conexiones VPN superpuestas.
- La vista **Lista** muestra cuántos sitios estaban activos durante el **Time Range (Intervalo de tiempo)** seleccionado y las métricas de estado general de las sucursales. La puntuación media de un sitio deficiente es el promedio de todas las muestras deficientes de los sitios identificados como deficientes. El gráfico de serie temporal se calcula y actualiza en función de la duración seleccionada. Por ejemplo, las duraciones admitidas son una hora, tres horas, 24 horas, siete días, 30 días y 90 días y el intervalo es de un minuto, cinco minutos, una hora y un día, respectivamente.
  - **Site Connectivity Health Distribution (Distribución del estado de la conectividad del sitio)**: Gráfico de distribución de sitios clasificados como bueno, regular y deficiente para un inquilino determinado en función de la distribución más reciente del estado de la conectividad del sitio.
  - **Site Connectivity Health Distribution Over Time (Distribución del estado de la conectividad del sitio a lo largo del tiempo)**: El gráfico de serie temporal de la puntuación de estado de los dispositivos que ejecutan el software 5.6.1 o superior.
  - **Puntuación de la experiencia de la aplicación del sitio** La puntuación de la experiencia de la aplicación del sitio.
  - **Sucursales de Prisma SD-WAN**: Vea el estado del sitio, estado de la conectividad del sitio, estado del circuito, estado del tejido seguro y acercándose al umbral de capacidad de una sucursal. Puede explorar en profundidad y filtrar una sucursal por predicción del sitio, estado de alarma y estado de ADEM.

- La vista **Actividad** presenta los análisis clave de la aplicación, la puntuación de estado del sitio más reciente y la distribución del estado del sitio a lo largo del tiempo. Estas incluyen:
  - Distribución del estado del sitio: muestra el gráfico de distribución de sitios buenos, regulares y deficientes para un inquilino determinado según la última puntuación del estado del sitio.
  - Distribución del estado del sitio a lo largo del tiempo: muestra el gráfico de serie temporal de la distribución del estado del sitio a lo largo del tiempo para un inquilino determinado en función de la puntuación de estado de una sucursal.
  - Utilización del ancho de banda: muestra la utilización del ancho de banda de cada aplicación en un sitio y una ruta WAN, con datos sobre las diez aplicaciones principales que consumen la mayor cantidad de ancho de banda en la red.
  - Estadísticas de transacciones: muestra estadísticas de transacciones sobre flujos TCP, incluidas acciones correctas y fallidas de iniciación/transacción para una aplicación específica o todas las aplicaciones, una ruta particular o todas las rutas y todos los eventos de estado.
  - Nuevos flujos: muestra los nuevos flujos TCP y UDP para una aplicación, un conjunto específico de aplicaciones o todas las aplicaciones durante un período determinado.
  - Flujos simultáneos: le ayuda a comprender cuántas conexiones están activas en su red por aplicación.

Supervisar Centros de datos

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software • Prisma SD-WAN	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN Las otras licencias y requisitos previos necesarios para la visibilidad son: ❑ Observabilidad de ADEM ❑ DEM autónomo para redes remotas ❑ ADEM con tecnología de IA ❑ Informes de claridad de WAN ❑ Un rol que tiene permiso para ver el panel → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

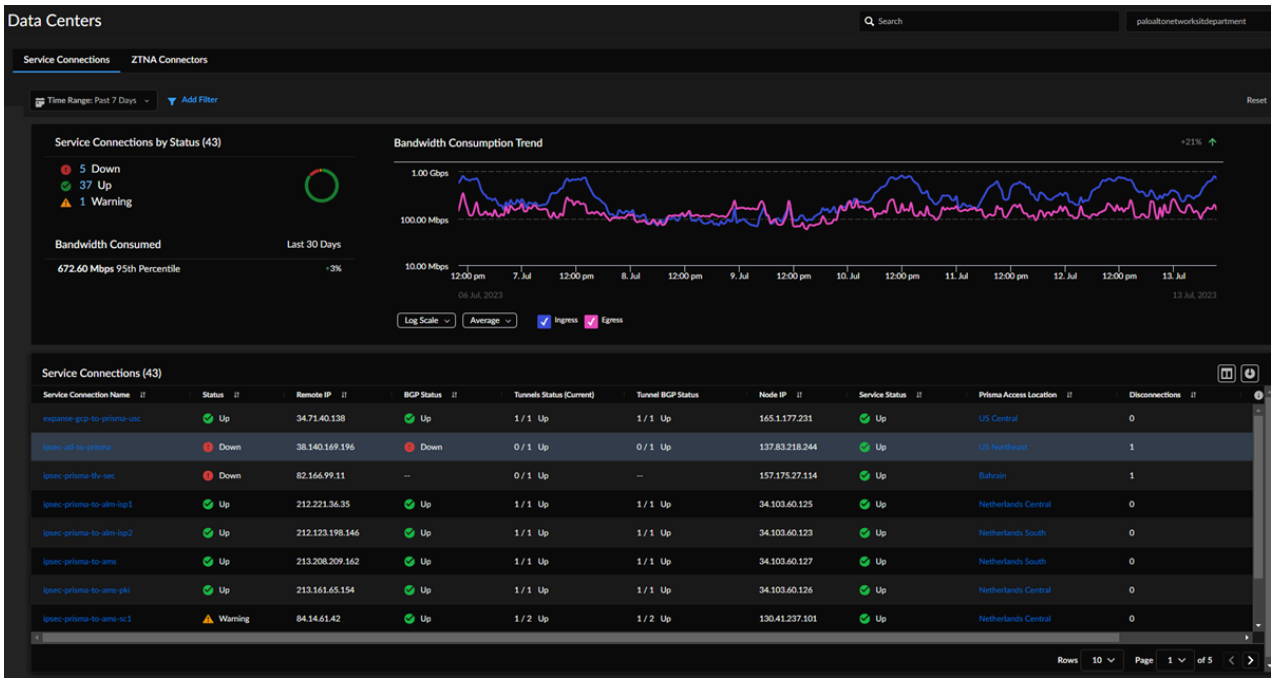
Supervise el rendimiento de las conexiones de servicio, los conectores ZTNA y la conectividad del sitio en los centros de datos y Prisma SD-WAN. Seleccione la pestaña **Monitor (Supervisar)** > **Prisma Access** > **Data Centers (Centros de datos)** > **Service Connections (Conexiones de servicio)** o **ZTNA Connectors (Conectores ZTNA)** para ver el estado de las conexiones de servicio y los conectores en Prisma Access.

Para cada centro de datos Prisma SD-WAN, seleccione **Monitor (Supervisar)** > **Data Centers (Centros de datos)** > **Prisma SD-WAN** para ver la información de conectividad del sitio y el estado de las conexiones VPN superpuestas.

- Conexiones de servicio
- Conectores ZTNA
- Prisma SD-WAN

Conexiones de servicio

Seleccione **Monitor (Supervisar)** > **Data Centers (Centros de datos)** > **Service Connections (Conexiones de servicio)** para comenzar.



Vea los datos agregados de conexiones de servicio, así como información sobre conexiones de servicio individuales. Las conexiones de servicio permiten tanto a los usuarios móviles como a las redes remotas. Más allá de proporcionar acceso a los recursos corporativos, las conexiones de servicio permiten a sus usuarios móviles llegar a las sucursales. Para obtener una descripción detallada de estos widgets, consulte Ver y supervisar centros de datos en la *Guía de gestión de Prisma Access*.

- Seleccione un intervalo de tiempo para ver las conexiones de servicio por estado y su tendencia de consumo de ancho de banda.
- Vea el estado de salud de todas sus conexiones de servicio.
- Vea la tendencia de consumo de ancho de banda para todas sus conexiones de servicio.
- Vea datos sobre sus conexiones de servicio, como el estado, la dirección IP remota, el estado BGP, el estado actual del túnel y otros datos. Seleccione cualquier conexión de servicio para ver sus detalles.

Conectores ZTNA

Seleccione **Monitor (Supervisar)** > **Data Centers (Centros de datos)** > **ZTNA Connectors (Conectores ZTNA)** para empezar.

El conector de acceso a la red de confianza cero (ZTNA) simplifica el acceso privado a aplicaciones para todas sus aplicaciones. La máquina virtual de ZTNA Connector en su entorno forma automáticamente túneles entre sus aplicaciones privadas y Prisma Access. Vea un resumen de todos los conectores ZTNA configurados, incluido los **Application Targets (Destinos de la aplicación)** asociados con el conector, su ancho de banda promedio y medio, y el **Status (Estado)** (Activo, Parcialmente activo o Desactivado). Para obtener una descripción detallada de estos widgets, consulte Ver y supervisar centros de datos en la *Guía de gestión de Prisma Access*.

Usted puede:

- Vea el estado y la salud de un grupo de conectores ZTNA.

- Vea el estado y la salud de los conectores ZTNA individuales.

Centros de datos (Prisma SD-WAN)

Los sitios SD-WAN de Prisma incluyen: centros de datos que desea tener en su red de área amplia. Puede alojar aplicaciones y servicios empresariales en un centro de datos. Como parte de la creación de un centro de datos, puede seleccionar un dominio y un conjunto de políticas predeterminados, configurar redes WAN, categorías de circuitos, etiquetas de circuitos y especificaciones de circuitos. El **Centro de datos** SD-WAN de Prisma muestra la lista de centros de datos con el nombre del centro de datos, el dispositivo ION y las alarmas abiertas para el sitio.

En el caso de un centro de datos, verá:

- La pestaña **Configuration (Configuración)** muestra la información de conectividad del sitio, Modos de implementación, Perfiles de grupos de pares de multidifusión WAN, Internet y circuitos WAN privadosy Prefijos IP. También puede configurar un agente de usuario y ver los detalles de la configuración del clúster para el centro de datos.
- La pestaña **Overlay Connections (Conexiones superpuestas)** muestra el estado de todas las conexiones de VPN superpuestas. La conectividad de cada sitio se calcula en función del estado de sus conexiones de superposición de VPN.

Supervisar Servicios de red

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software • Prisma SD-WAN	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN Las otras licencias y requisitos previos necesarios para la visibilidad son: ❑ Observabilidad de ADEM ❑ DEM autónomo para redes remotas ❑ ADEM con tecnología de IA ❑ Informes de claridad de WAN ❑ Un rol que tiene permiso para ver el panel → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Desde la página **Monitor (Supervisar)** > **Network Services (Servicios de red)**, puede ver el rendimiento de los servicios de red comunes que afectan su experiencia del usuario al acceder a las aplicaciones. Seleccione la pestaña **GlobalProtect Authentication (Autenticación de GlobalProtect)** para ver los recuentos de autenticaciones de puerta de enlace de GlobalProtect realizadas correctamente o que han fallado en diferentes ubicaciones. Seleccionar Servicios de red de **: DNS** para ver las solicitudes y respuestas de proxy DNS recibidas entre los inquilinos con respecto al Proxy DNS de Prisma Access.

- Autenticación de GlobalProtect
- DNS:

Autenticación de GlobalProtect

Seleccione **Monitor (Supervisar)** > **Network Services (Servicios de red)** > **GlobalProtect Authentication (Autenticación GlobalProtect)** para comenzar.

Puede ver el rendimiento de los servicios de red comunes que afectan su experiencia del usuario al acceder a las aplicaciones en Insights. Los servicios de red incluyen informar el número de autenticaciones de GlobalProtect realizados correctamente o que fallaron, como una medida de la capacidad de los usuarios móviles para conectarse a Prisma Access. Puede ver:

- detalles sobre los recuentos de autenticación realizada correctamente para GlobalProtect para diferentes ubicaciones.
- recuentos de errores de autenticación para GlobalProtect para diferentes ubicaciones.
- errores de tiempo de espera de autenticación para GlobalProtect para diferentes ubicaciones.

Para obtener una descripción detallada de estos widgets, consulte Ver y supervisar servicios de red.

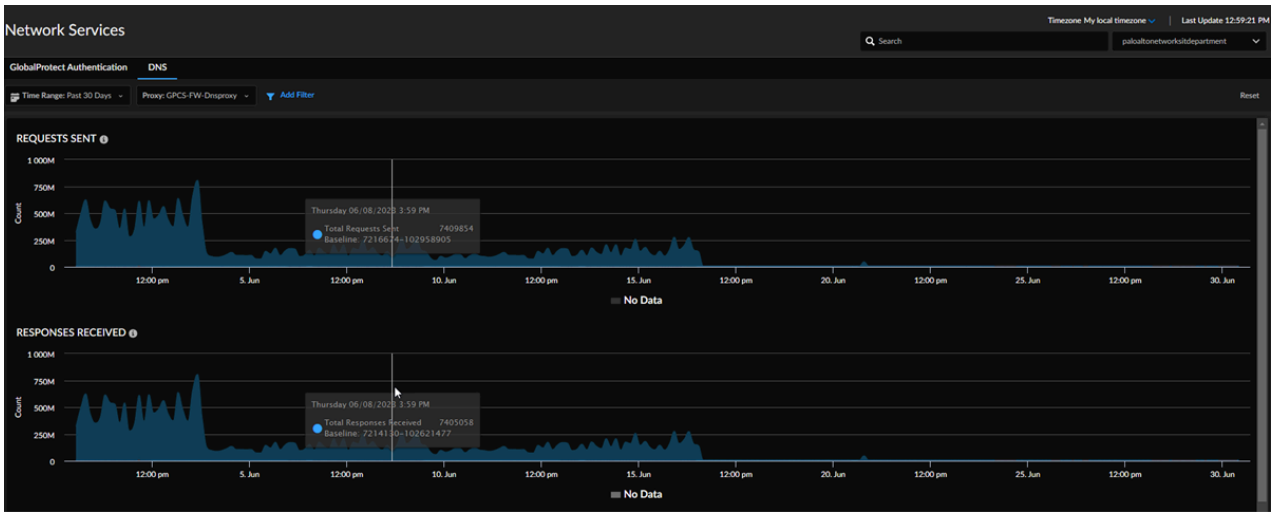
DNS:

Seleccione **Monitor (Supervisar)** > **Network Services (Servicios de red)** > **DNS** para empezar.

Servicios de red: DNS muestra las solicitudes y respuestas de DNS Proxy. Puede utilizar los siguientes filtros:

- **Intervalo de tiempo**
- **Nombres de proxy DNS**

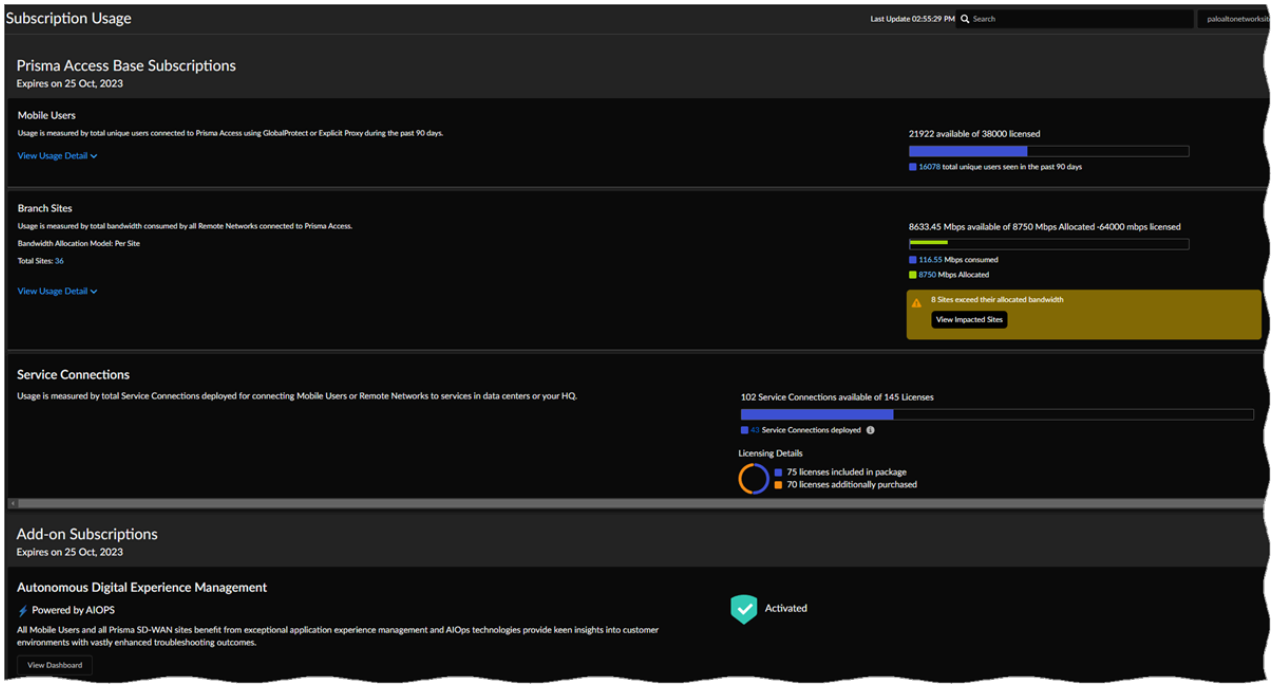
Los valores del filtro de proxy DNS están relacionados con los últimos 30 días y se seleccionan automáticamente al cargar (es decir, si no hay datos de proxy explícito, no hay ningún filtro de proxy explícito). Para obtener información más detallada, consulte Ver y supervisar los servicios de red.



Supervisar Uso de suscripciones

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)*	❑ Licencia de Prisma Access ❑ AI-Powered ADEM para desbloquear ciertas características.

Seleccione **Monitor (Supervisar)** > **Subscription Usage (Uso de suscripciones)** para ver detalles sobre su uso de **Prisma Access Base Subscriptions (Suscripciones básicas a Prisma Access)**, incluido el número total de usuarios únicos conectados, el ancho de banda consumido por los usuarios remotos de la red, el número total de conexiones de servicio implementadas y detalles sobre cualquier suscripción adicional.



- **Mobile Users (Usuarios móviles)**: Vea cuántas licencias únicas de **Mobile Users (Usuarios móviles)** ha consumido hasta ahora. El widget muestra el número total de licencias consumidas por usuarios móviles únicos conectados a Prisma Access en los últimos 90 días, porque las licencias se basan en los últimos 90 días de datos de inicio de sesión de Prisma Access. Un usuario que haya iniciado sesión en Prisma Access al menos una vez en los últimos 90 días contribuye al consumo de una licencia de usuario móvil.
- **Branch Sites (Sucursales)**: Consulte el uso total del ancho de banda consumido por todas las redes remotas conectadas a Prisma Access. Consulte cuánto ancho de banda has asignado y cuánto ha consumido, en Mbps. Puede ver el uso del ancho de banda total consumido por todas las redes remotas conectadas a Prisma Access.
- **Subscriptions Usage (Uso de suscripciones)**: Vea cuántas licencias de **Service Connections (Conexiones de servicio)** ha consumido hasta ahora.

Consulte la sección **Add-on Subscriptions (Suscripciones de complementos)** de esta página para ver las licencias adicionales que ha comprado, como las licencias de **Autonomous Digital Experience Management (Gestión de la experiencia digital autónoma)**para usuarios móviles y redes remotas. Puede ver el número total de licencias compradas, así como el número de licencias no consumidas hasta ahora. Vea **Application Tests for Mobile User Monitoring (Pruebas de aplicación para la supervisión de usuarios móviles)**: el número de pruebas de aplicación que le quedan que puede crear para sus usuarios móviles. Las pruebas de aplicaciones se determinan por el número de usuarios móviles supervisados y se permiten hasta 10 pruebas de aplicaciones por usuarios móviles.

Para obtener más información, consulte Ver y supervisar el uso de la suscripción.

Supervisar Dispositivos ION

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma SD-WAN	❑ Licencia de Prisma SD-WAN

Los Dispositivos ION en Prisma SD-WAN le permiten combinar redes WAN dispares, tales como; MPLS, LTE y enlaces a Internet, en una única red de área amplia (WAN) híbrida de alto rendimiento.

La pantalla **Device List (Lista de dispositivos)** proporciona información sobre la lista de dispositivos de Prisma SD-WAN, incluida la versión de software y el estado del dispositivo ION, donde puede actualizar la versión de software del dispositivo o configurar un dispositivo.

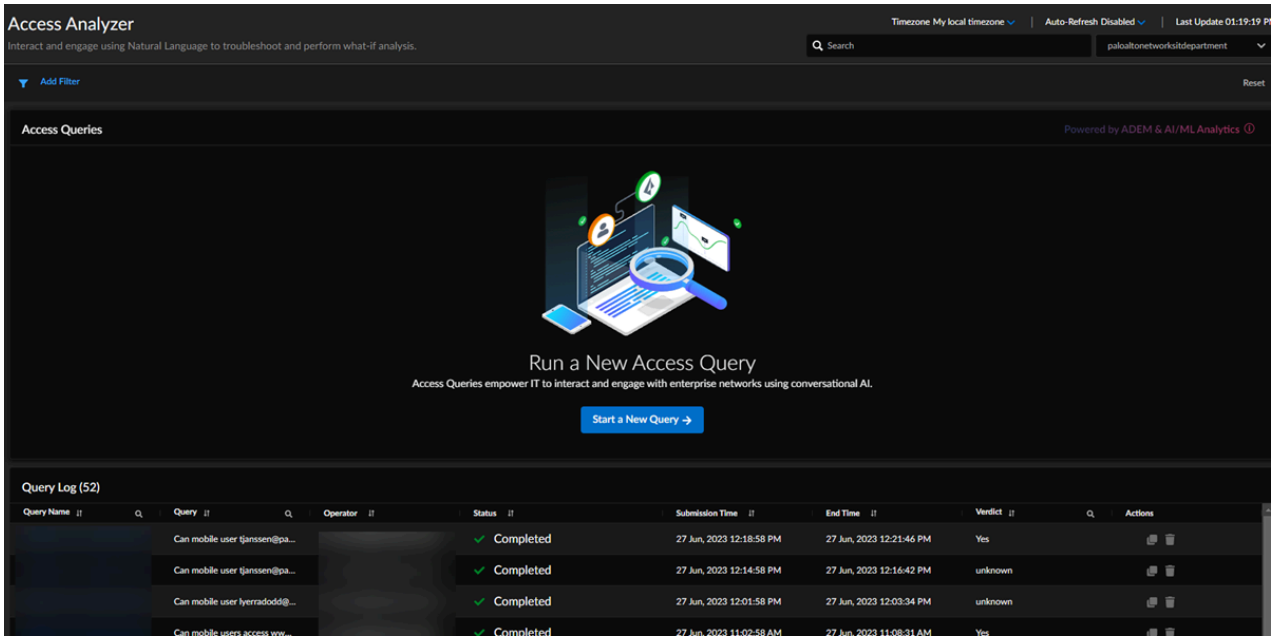
Entidad	Description (Descripción)
Device Name (Nombre del dispositivo)	Muestra el nombre configurado para el dispositivo ION.
Información del dispositivo	Muestra el tipo y el número de serie del dispositivo ION.
Software	Muestra la versión actual del software del dispositivo. Haga clic en **Upgrade (Actualizar)** para cambiar la versión del software del dispositivo.
Última actividad	Muestra información sobre cuándo se configuró y actualizó por última vez el dispositivo ION.
Estatal o regional	Muestra el estado actual del dispositivo ION.
Redundancia	Muestra si el dispositivo ION forma parte de una configuración de alta disponibilidad (HA).
Acciones	Puede elegir configurar el dispositivo ION desde el menú de puntos suspensivos.

La pantalla **Device Activity (Actividad del dispositivo)** muestra varios informes de actividad del dispositivo para un sitio en las últimas 24 horas.

Supervisar Analizador de acceso

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)*	❑ Licencia de Prisma Access ❑ Licencia de AI-Powered ADEM

Seleccione **Monitor (Supervisar)** > **Access Analyzer (Analizador de acceso)** para iniciar una nueva consulta de Analizador de acceso y ver una tabla de consultas existentes.



El analizador de acceso proporciona una supervisión automática de su entorno SASE. Ofrece una herramienta de IA conversacional para la resolución de problemas contextuales y el análisis de y-si para analizar los problemas de acceso y conectividad en su entorno SASE.

Usted puede:

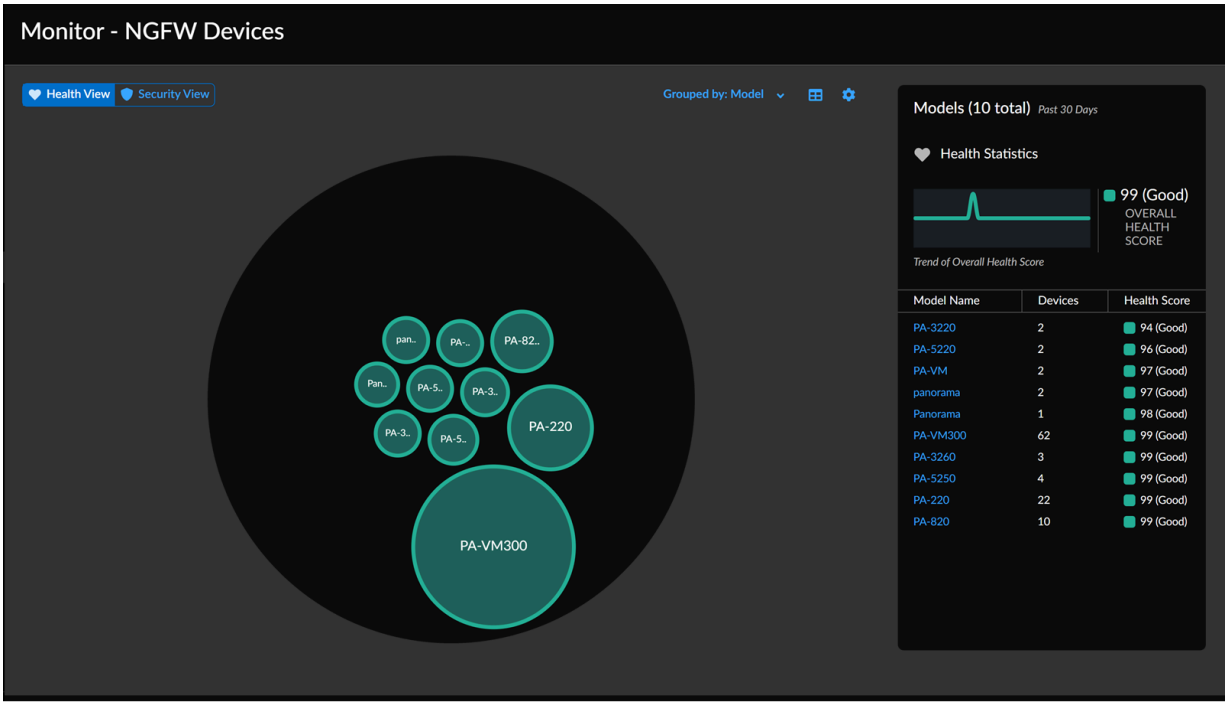
- Aprenda a crear una consulta de lenguaje natural en el Analizador de acceso.
- Inicie una nueva consulta de Analizador de acceso.
- Vea una lista de consultas existentes y seleccione cualquier consulta de la tabla para ver más detalles.

Supervisar Dispositivos NGFW

¿Dónde puedo usar esto?	¿Qué necesito?
• Cortafuegos NGFW *(con gestión de la configuración de Strata Cloud Manager o Panorama)*	❑ AIOps for NGFW Free (use the AIOps for NGFW Free ap o AIOps for NGFW Premium license (use the Strata Cloud ❑ Créditos NGFW de software *(para NGFW de software de VM-Series)*

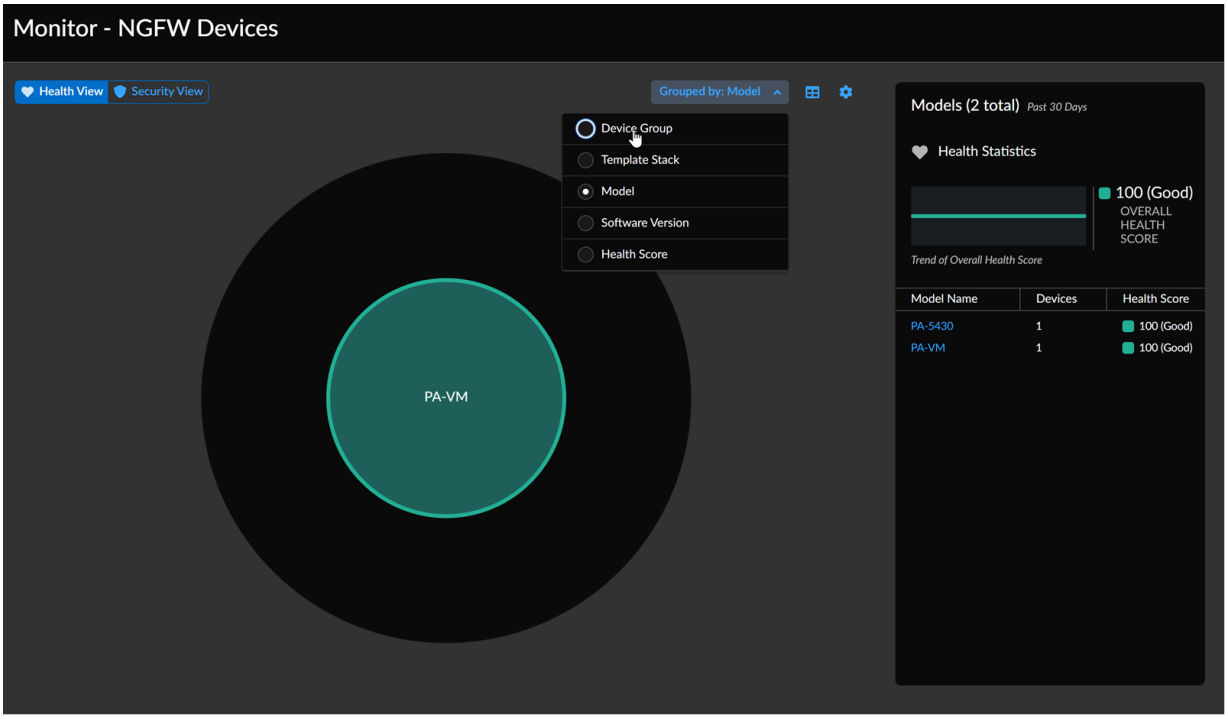
En **Monitor (Supervisar)** > **Dispositivos NGFW**, puede obtener una representación interactiva codificada por colores de los dispositivos de su implementación, para una gestión e investigación sencillas e intuitivas.

STEP 1 | Seleccione **Monitor (Supervisar)** > **NGFW Devices (Dispositivos NGFW)**.



STEP 2 | Seleccione **Health (Estado)** o **Security (Seguridad)**.

STEP 3 | Seleccione por qué atributo desea que la visualización se **Grouped by (Agrupe)**.



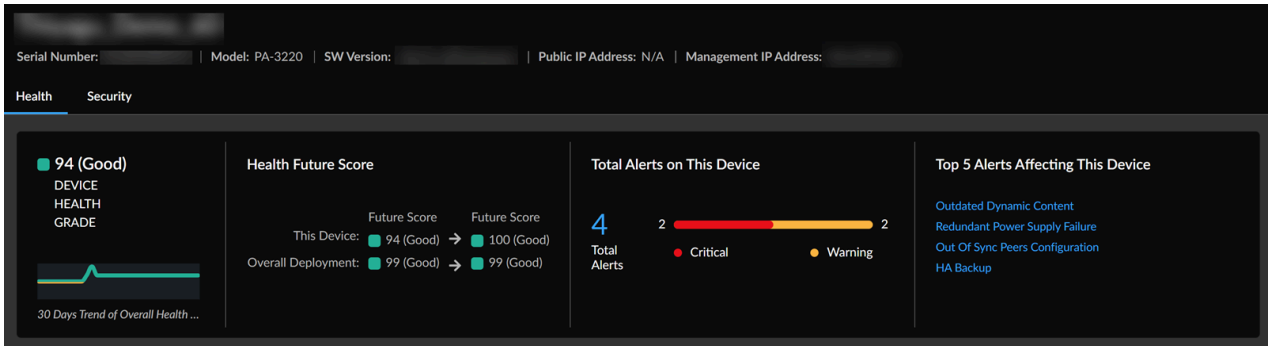
*Las opciones de agrupación **Device Group (Grupo de dispositivos)** y la **Template Stack (Pila de plantillas)** solo están disponibles en implementaciones gestionadas por Panorama en las que Panorama envía telemetría de dispositivos.*

STEP 4 | Seleccione un grupo para ver los dispositivos que contiene y seleccione un dispositivo para ver información general sobre él.

Si desea obtener más información sobre un dispositivo, selecciónelo.

Ver detalles del dispositivo

Al seleccionar un dispositivo de los **NGFW Devices (Dispositivos NGFW)** o siguiendo un enlace desde otra parte de la aplicación, puede ver detalles específicos sobre un cortafuegos o un dispositivo Panorama, como el grado de salud, las métricas, las conexiones, etc.



Grado de estado del dispositivo

El estado de salud actual del dispositivo y un gráfico que muestra su historial durante los últimos 30 días<x>. Las posibles clasificaciones de estado son Bueno, Regular, Deficiente y Crítico.

Grado de estado después de la remediación

El grado de mantenimiento del dispositivo después de haber abordado las alertas abiertas. Este icono también muestra el estado de la implementación general después de cerrar las alertas.

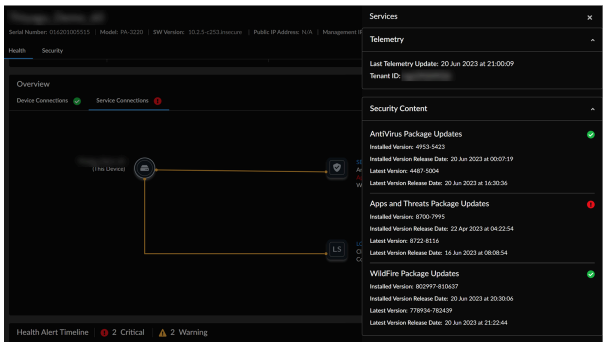
Alertas totales

El número total de alertas abiertas en el dispositivo.

Las 5 alertas principales

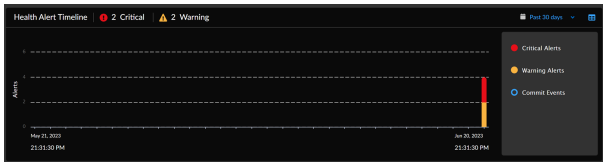
Cinco de las alertas más comunes en este dispositivo en los últimos 30 días.

Descripción general > Conexiones de dispositivos Los otros dispositivos conectados al que está viendo actualmente. Seleccione un dispositivo para ver sus detalles.	
Descripción general > Conexiones de servicio Una descripción general de todos los servicios de seguridad y registro de logs integrados con el dispositivo. Seleccione un servicio para ver sus detalles.	



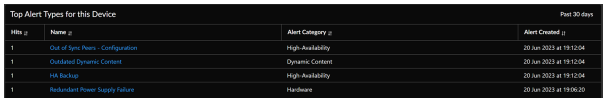
Cronología de alerta

Una línea de tiempo de alertas de dispositivos y eventos de confirmación. Las alertas se clasifican como eventos críticos, de advertencia o de confirmación. Alterne para ver los datos de alerta en formato de tabla.



Principales tipos de alerta para este dispositivo

Las alertas más comunes de los últimos 30 días. Seleccione una alerta para ver sus detalles de la alerta.



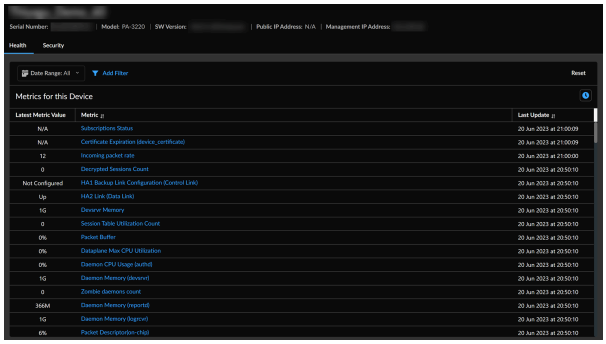
Las 10 aplicaciones que más se utilizan

Las diez aplicaciones que utilizan la mayor cantidad de datos en el cortafuegos.

Métricas para este dispositivo

Una lista de todas las métricas de estado recopiladas para la ejecución de controles de seguridad en el dispositivo, incluidos los datos de enlace de alta disponibilidad.

Seleccione una métrica para ver sus detalles.



Supervisar Analizador de capacidad

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW	❑ AIOps for NGFW Premium o Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

El Analizador de capacidad le permite analizar y supervisar la capacidad de recursos de sus dispositivos realizando un seguimiento del uso de sus métricas en función de sus tipos de modelo. El analizador de capacidad ofrece los siguientes beneficios:

- Una comprensión integral de la utilización de las métricas existentes y la capacidad métrica no utilizada hasta el límite máximo.
- Una visualización de mapa de calor que muestra el uso de métricas con respecto a las plataformas de hardware en una sola vista y ayuda a profundizar en los detalles.
- La capacidad de planificar la actualización a cortafuegos de mayor capacidad según sus necesidades específicas.

*La función **Capacity Analyzer (Analizador de capacidad)** no es compatible con los cortafuegos VM-Series.*

Este es un vídeo que muestra cómo utilizar la función Analizador de capacidad:

El analizador de capacidad se ha mejorado para admitir alertas que le ayuden a anticipar el consumo de recursos cuando se acerca a su capacidad máxima y activar notificaciones de manera oportuna. Las alertas del Analizador de capacidad se generan con 3 meses de anticipación para identificar posibles cuellos de botella de capacidad. Esto le ayuda a planificar la limpieza de la configuración o aumentar el tamaño de las capacidades de NGFW antes de que alcancen el uso máximo y a mantener la estabilidad del sistema. Consulte Alertas de estado premium para obtener la lista de alertas de capacidad admitidas.

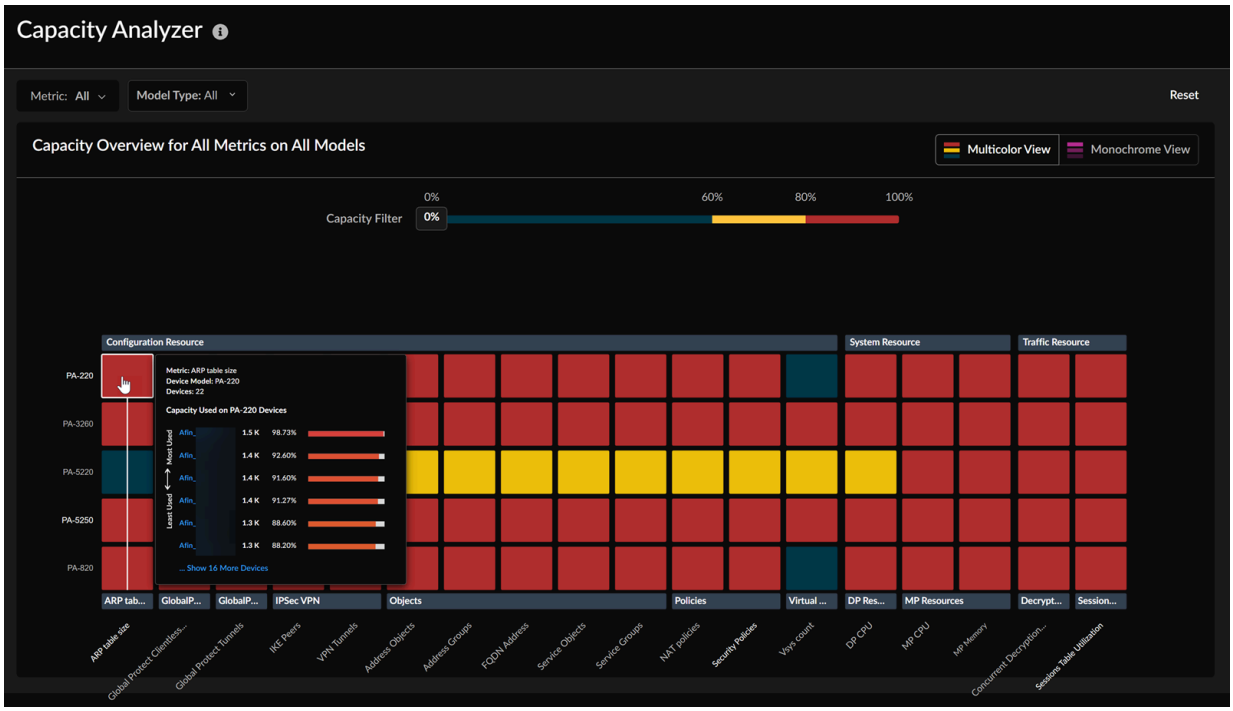
El analizador de capacidad agrupa las métricas según los siguientes tipos:

- Métricas de recursos de configuración, como políticas NAT y objetos de dirección.
- Métricas de recursos operativos del sistema, como CPU, memoria, discos y logs.
- Métricas de recursos de tráfico, como el uso de descifrado y la utilización de la tabla de sesiones.

El mapa de calor muestra el uso de métricas para cada dispositivo. El color más oscuro representa una mayor utilización y el color más claro indica un menor uso. La opción **Multicolor View (Vista Multicolor)**está seleccionada de forma predeterminada. También puede cambiar a la **Monochrome View (Vista monocromática)**.

A continuación se muestran las diferentes formas en las que puede utilizar el mapa de calor del Analizador de capacidad para obtener información sobre el uso de las métricas:

- Coloque el cursor sobre un bloque de métricas de un dispositivo para ver una descripción emergente que proporciona los siguientes detalles:
  - Nombre de la métrica
  - Modelo del dispositivo y lista de dispositivos
  - Rango de capacidad del dispositivo



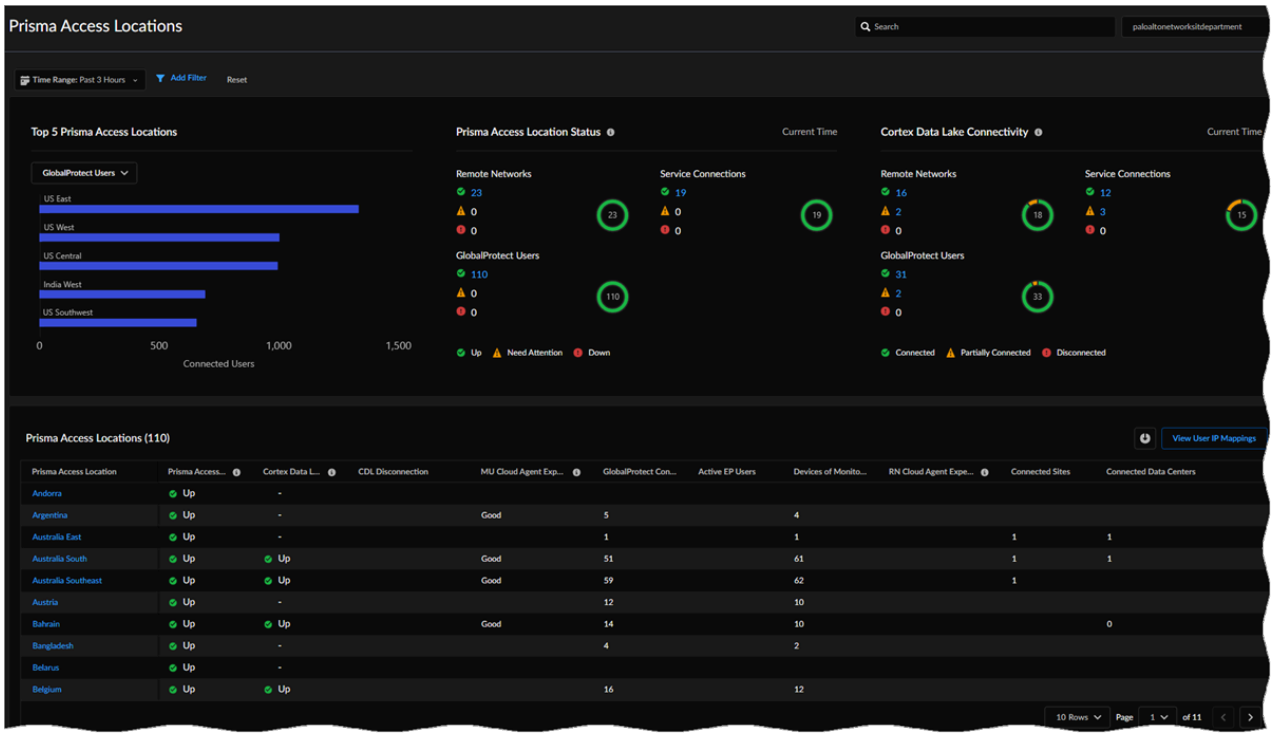
- Filtre datos utilizando los siguientes atributos:
  - **Metric (Métrica)**: seleccione una o más métricas que desee ver o buscar utilizando el nombre de la métrica.
  - **Model (Modelo)**: seleccione uno o más modelos de dispositivos o busque utilizando el nombre del modelo.
  - **Capacity (Capacidad)**: seleccione la capacidad en la escala **Capacity Filter (Filtro de capacidad)**.

Para obtener más información sobre cómo utilizar el mapa de calor del Analizador de capacidad, consulte Analizar la capacidad de las métricas.

Supervisar Ubicaciones de Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)*	❑ Licencia de Prisma Access Esta es una función de Prisma Access Insights.

Seleccione **Monitor (Supervisar)** > **Prisma Access Locations (Ubicaciones de Prisma Access)** para comenzar. Desde aquí, puede ver el estado de todas sus ubicaciones de Prisma Access para sus redes remotas y usuarios móviles. Para obtener una descripción detallada de estos widgets, consulte Ver y supervisar ubicaciones de Prisma Access en la *Guía de gestión de Prisma Access*.

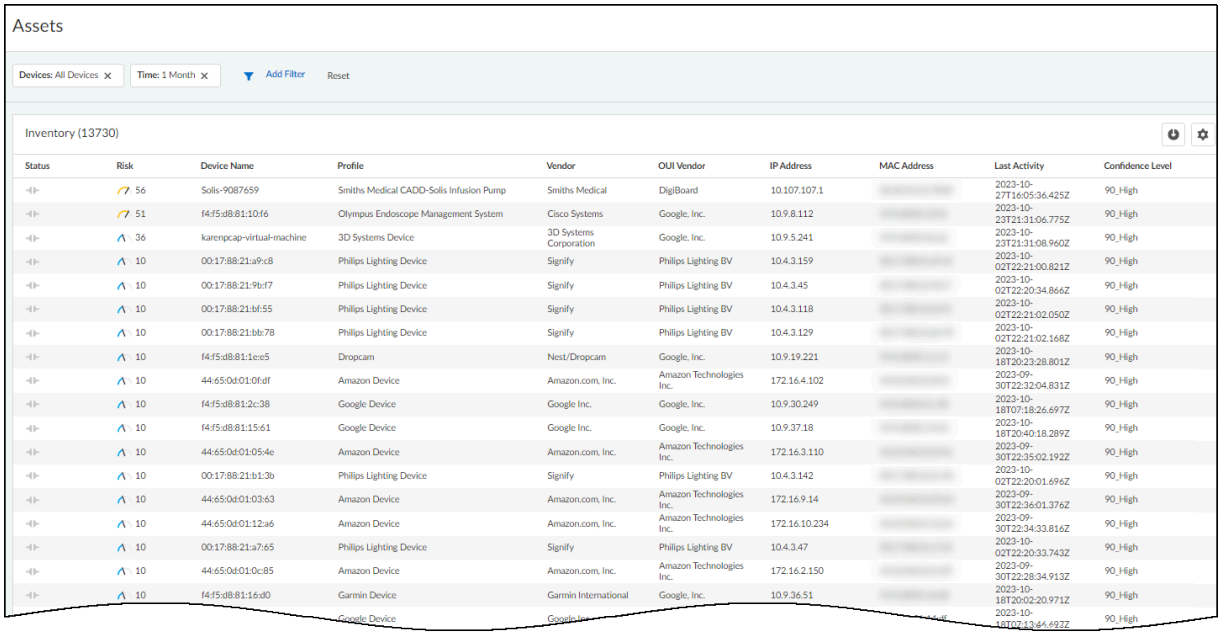


- Consulte las 5 principales ubicaciones de Prisma Access para redes remotas, conexiones de servicio, usuarios móviles de GlobalProtect o usuarios móviles de proxy explícito según el ancho de banda total consumido.
- Vea el estado de sus ubicaciones de Prisma Access.
- Ver conectividad de Strata Logging Service.
- Vea la tabla Ubicaciones de Prisma Access, que enumera todas las ubicaciones de Prisma Access, y seleccione una ubicación de Prisma Access individual por nombre para ver sus detalles.

Supervisar Activos

¿Dónde puedo usar esto?	¿Qué necesito?
• Cortafuegos NGFW *(con gestión de la configuración de Strata Cloud Manager o Panorama)*	❑ Suscripción a IoT Security ❑ Créditos NGFW de software *(para NGFW de software de VM-Series)*

Para comenzar, seleccione **Monitor (Supervisar) > Assests (Activos)**. Desde aquí, puede ver un inventario mantenido dinámicamente de los dispositivos IoT, OT y TI en su red con numerosos atributos para cada uno, como sus direcciones IP y MAC; perfil, proveedor, modelo y sistema operativo; y (para productos de seguridad IoT avanzados) su puntuación de riesgo a nivel de dispositivo.



Utilice los datos de este inventario para obtener más información sobre los activos de su red:

- Vea un inventario generado dinámicamente y actualizado de los dispositivos detectados en su red, incluidos dispositivos IoT, OT y TI.
- Mientras que el Panel de IoT muestra los tipos de dispositivos que tiene en un nivel alto, el inventario de Activos le permite explorar dispositivos individuales para ver más detalles y evaluar su postura de seguridad.
- Filtre los datos que se muestran en el panel por sitio, tipo de dispositivo, período de tiempo y uno o más atributos del dispositivo para ver datos sobre los dispositivos de interés.
- Muestra y oculta columnas para ver los atributos del dispositivo que son importantes para usted. Hay más de 100 columnas de atributos entre las que elegir.

- Descargue los datos que se muestran en la página actualmente activa como un archivo en formato CSV para incluirlos en informes o para referencia futura. El archivo contiene los dispositivos y los atributos de dispositivo que tiene en pantalla en el momento de la descarga.

Incidentes y alertas: Strata Cloud Manager

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software • Prisma SD-WAN	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Prisma SD-WAN ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro Las otras licencias y requisitos previos necesarios para la visibilidad son: ☐ Un rol que tiene permiso para ver el panel → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

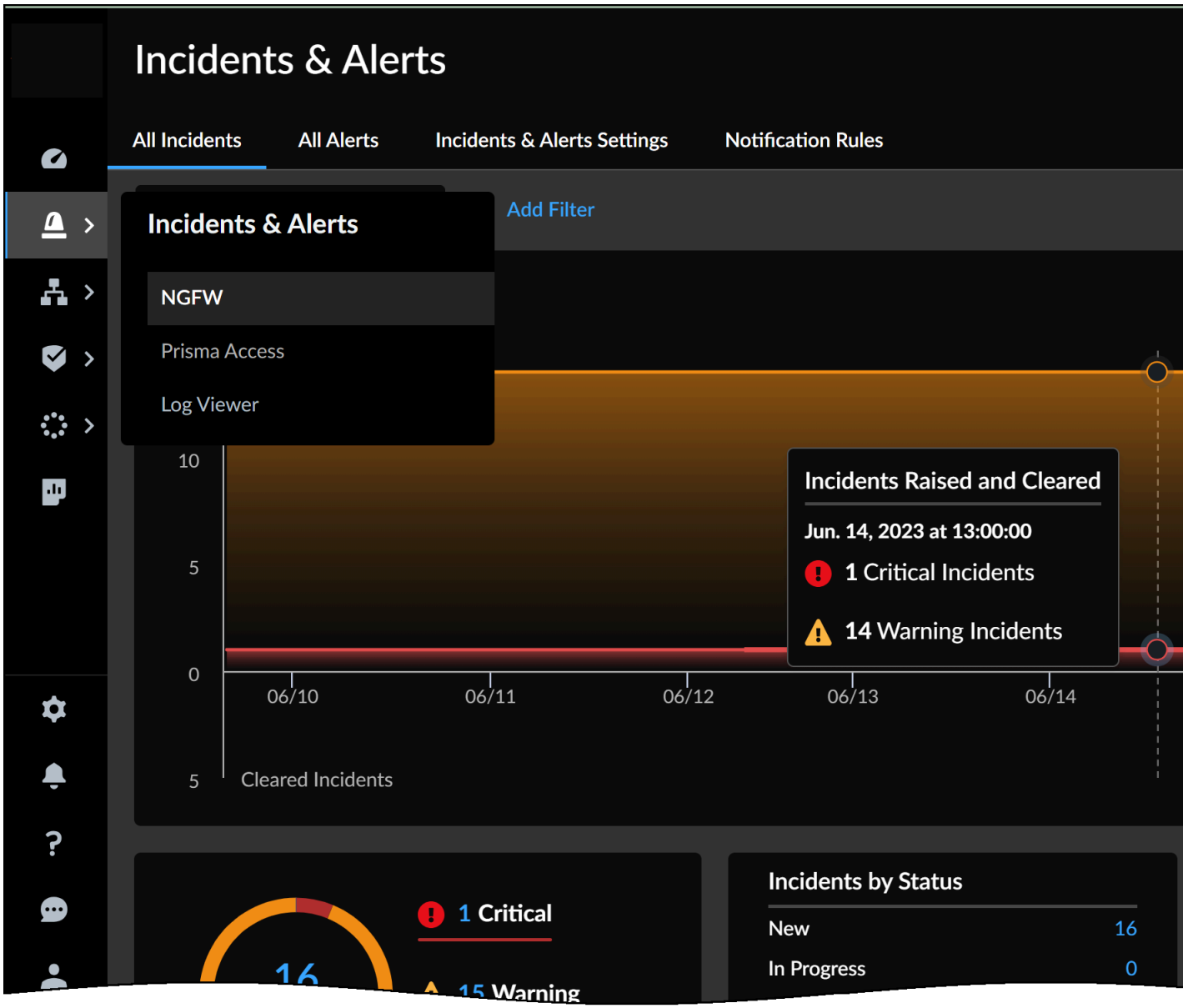
Strata Cloud Manager le ofrece un marco común para interactuar e investigar los incidentes y alertas que los productos y suscripciones de Pala Alto Networks detectan en su empresa:

- Incidentes y alertas: NGFW
- Incidentes y alertas: Prisma Access
- Incidentes y alertas: Prisma SD-WAN

Para ayudarle a mantener el estado continuo de sus dispositivos e implementaciones, y para evitar interrupciones en su negocio, explore cada una de las páginas de incidentes y alertas para:

- Vea incidentes y alertas en toda su red, y profundice para investigar.
- Crear y revisar reglas que activen notificaciones de incidentes y alertas.

Puede moverse entre sus incidentes y alertas y el Incidentes y alertas: Visor de logs para investigar la actividad en su red que está activando o está asociada con incidentes y alertas.



Incidentes y alertas: NGFW

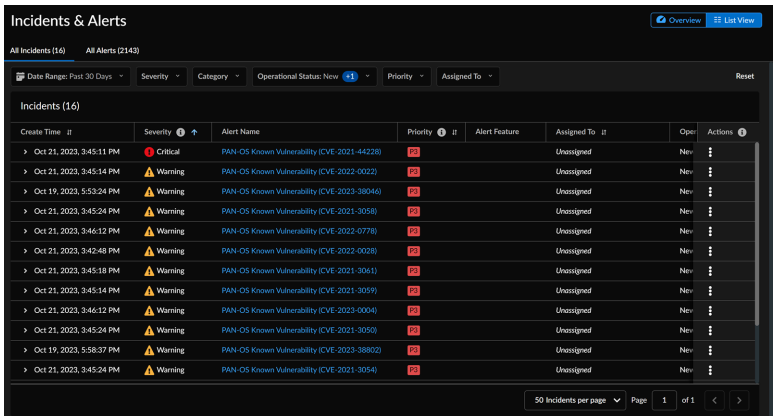
¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW, incluidos los financiados por Créditos de NGFW de software	❑ Una de las siguientes licencias: ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) o AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro

Para ayudarle a mantener el estado continuo de sus dispositivos y evitar incidentes que interrumpan su negocio, sus aplicaciones generan incidentes y alertas basados en uno o más problemas que ha detectado con su implementación del cortafuegos. Con **Incidents & Alerts (Incidentes y alertas)** > **NGFW**, obtiene una vista singular de sus incidentes y alertas en todos los NGFW.

Aquí mostramos cómo ponerse en marcha con **NGFW Incidents & Alerts (Incidentes y alertas de NGFW)**:

- Los incidentes le mantienen informado sobre vulnerabilidades. Puede investigarlos y tomar medidas preventivas si es necesario.

  Vaya a **Incidents & Alerts (Incidentes y Alertas)** > **NGFW** > **All Incidents (Todos los incidentes)** para ver incidentes en toda su red e interactuar con ellos.



- Una alerta indica un problema específico (degradación o pérdida de la funcionalidad del cortafuegos) que debe abordarse. También se pueden generar alertas basadas en la correlación o suma de varios eventos. Esta suma, o agregación, de eventos en una sola alerta ayuda a

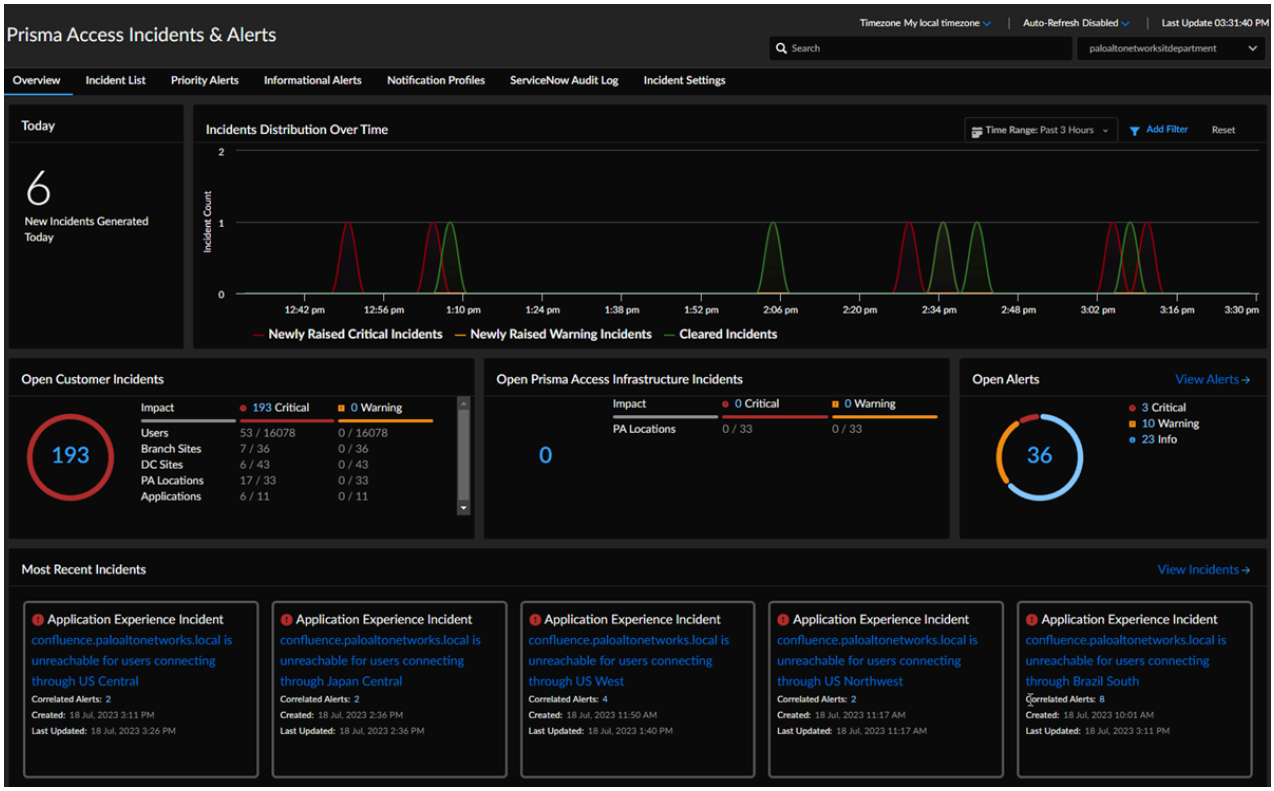
clasificar y agilizar la transferencia de alertas entre equipos, centralizar información crítica y reducir la fatiga de notificaciones.

Vaya a **Incidents & Alerts (Incidentes y Alertas)** > **NGFW** > **All Alerts (Todas las alertas)** para ver alertas en toda su red e interactuar con ellas.

Incidentes y alertas: Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)*	❑ Licencia de AI-Powered ADEM ❑ Licencia de ADEM Observability ❑ Licencia de Prisma Access

Seleccione **Incidents & Alerts (Incidentes y alertas)** > **Prisma Access Incidents & Alerts (Incidentes y alertas de Prisma Access)** para comenzar. Las incidencias y alertas disponibles en su entorno dependen de sus licencias.



Obtenga una descripción general

Consulte una Descripción general de la información sobre incidentes y alertas relacionada con su entorno de Prisma Access. Las incidencias y alertas disponibles en su entorno dependen de sus licencias.

Ver todos los incidentes

Vea la Lista de incidentes, que muestra todos los incidentes en su entorno. Utilice el menú desplegable **Add Filter (Añadir filtro)** para seleccionar Incidencias por las columnas de la tabla (puede filtrar en más de una). Desde dentro de la tabla, seleccione cualquier **Incident (Incidente)** para ver su información detallada.

Ver alertas de prioridad

Consulte Alertas de prioridad, que describen el estado de su entorno de Prisma Access.

Ver alertas informativas

Vea las alertas informativas, que le notifican sobre las próximas actualizaciones de software y el estado de las actualizaciones que están en curso o completadas.

Perfiles de notificación

Desde Perfiles de notificación, puede ver información sobre **Notification Subscriptions (Suscripciones de notificación)** y crear un **Notification Profile (Perfil de notificación)** nuevo o modificar uno existente.

Log de auditoría de ServiceNow

Si usa ServiceNow, puede revisar el Log de auditoría de ServiceNow, que le muestra cada **Incident ID (ID de incidente)** de ServiceNow. También le muestra las operaciones de ServiceNow realizadas en cada incidente, como crear, actualizar y eliminar.

Configuración de incidentes

Desde Configuración de incidentes puede personalizar los incidentes que reciba por categoría de incidente y código de incidente.

Incidentes y alertas por código

Vea incidentes y alertas por sus ID de código, comprenda los problemas y cuestiones que describen y descubra cómo remediarlos. Las incidencias y alertas están clasificadas por licencia:

- Incidentes ADEM basados en IA
- Incidentes de ADEM
- Incidentes de Prisma Access
- Alertas prioritarias
- Alertas informativas

Para obtener información sobre incidentes y alertas, consulte la Guía de referencia de incidentes y alertas.

Para obtener información sobre la integración de ServiceNow, consulte Integrar ServiceNow con Prisma Access en la *Guía de integraciones*.

Incidentes y alertas: Prisma SD-WAN

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma SD-WAN	❑ Licencia de Prisma SD-WAN

Prisma SD-WAN genera incidencias y alertas cuando el sistema alcanza umbrales definidos por el sistema o por el cliente o cuando hay un fallo en el sistema. Utilice estos incidentes y alertas para solucionar problemas del sistema.

Seleccione **Incidents and Alerts (Incidentes y alertas)** > **Prisma SD-WAN** para ver incidentes y alertas en Strata Cloud Manager.

Utilice las siguientes pestañas para navegar por incidentes y alertas en Prisma SD-WAN.

- Descripción general
- Incidentes
- Alertas
- Configuración

Descripción general

Ver incidencias y alertas y sus categorías en Prisma SD-WAN. La pestaña **Overview (Visión general)** es la vista predeterminada.

Vea los principales incidentes y alertas que muestran la siguiente información.

Tipo de incidente	Muestra la categoría del incidente.
Description (Descripción)	Muestra la descripción del incidente.
Gravedad	Muestra la gravedad del incidente.
Prioridad	Muestra la prioridad del incidente.
Alertas correlacionadas	Muestra el número de incidentes sumados a este incidente.
estado	Muestra el estado del incidente.
Creado	Muestra cuando el incidente fue planteado por el sistema.
Actualizado por última vez	Muestra la última vez que el sistema actualizó el incidente.

Incidentes

Un incidente es una indicación de un fallo en el sistema. Los incidentes se plantean y aclaran y varían en gravedad:

- Crítico: toda o parte de una red está caída y requiere una acción inmediata.
- Advertencia: afecta a la red y requiere atención inmediata.
- Informativo: la red está degradada y necesita atención pronto.

Alertas

Una alerta puede ser o no una indicación de un fallo en la red. Se activa una alerta cuando el sistema alcanza umbrales definidos por el sistema o por el cliente.

Configuración

Utilice la pestaña **Settings (Configuración)** para crear políticas de incidencias para gestionar la supresión de código de eventos según las clasificaciones y atributos de acción especificados configurados. Puede utilizar las reglas de políticas de incidentes para suprimir o elevar los incidentes que surjan durante un período de tiempo programado. Además, también puede cambiar la prioridad predeterminada de los incidentes generados por el sistema a un nivel de prioridad que esté más alineado con sus requisitos empresariales.

Incidentes y alertas: Visor de logs

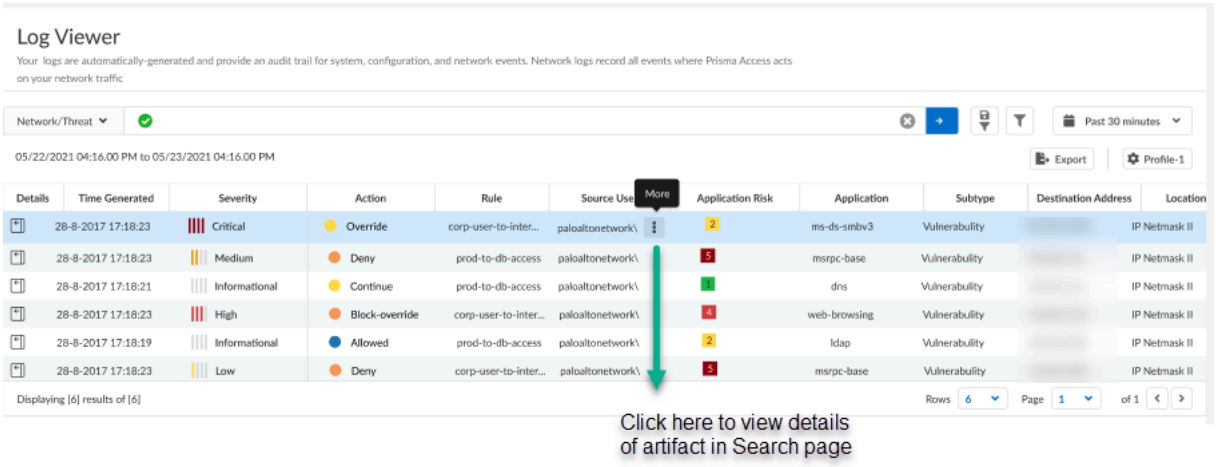
¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)* • NGFW, incluidos los financiados por Créditos de NGFW de software	❑ Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) o AIOps for NGFW Free (use the AIOps for NGFW Free app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Un rol que tiene permiso para ver el panel

Log Viewer (Visor de logs) proporciona las capacidades de Explorar: donde puede ver e interactuar con sus logs almacenados en Strata Logging Service.

Log Viewer (Visor de logs) proporciona una pista de auditoría para eventos del sistema, configuración y red. Salte de un panel a sus logs para obtener detalles e investigar los hallazgos. Un campo de consulta y las preferencias de intervalo de tiempo le ayudan a reducir los logs específicos que le interesan.

- Obtenga más información sobre cómo crear las consultas
- Descubra las nuevas características del Visor de logs en las Notas de la versión de Strata Logging Service.

Log Viewer (Visor de logs) resalta las acciones y la gravedad de los logs para ayudarle a comprender cómo se aplican las sesiones. También puede ver los detalles de los artefactos de seguridad de los logs en la página Search (Buscar).



* Puede ver los detalles en Buscar los siguientes tipos de logs y campos de logs:

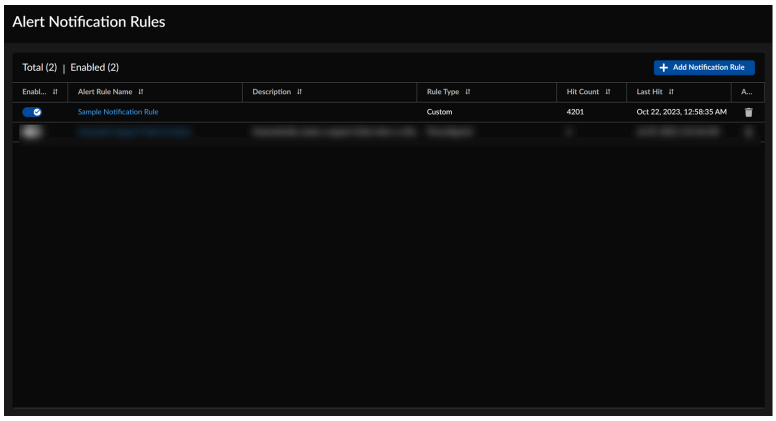
Tipo de log	Nombre de columna
Tráfico, Amenaza, URL, Archivo	• Dirección de origen • Dirección de destino • Fuente NAT • Destino NAT
Amenaza, Archivo	Hash de archivo
URL	• URL • Dominio URL
DNS Security	• Dirección de origen • Dirección de destino • Dominio • FQDN

Configuración de incidentes y alertas

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW, incluidos los financiados por Créditos de NGFW de software	❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) o AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro

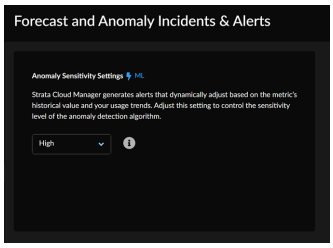
- Para definir preferencias de notificación, como qué alertas activan las notificaciones, cómo recibirlas y con qué frecuencia recibirlas, cree una regla de notificación.

  Vaya a **Incidents & Alerts (Incidentes y alertas)** > **Incident & Alert Settings (Configuración de incidentes y alertas)** > **Notification Rules (Reglas de notificación)** para ver y añadir reglas para activar notificaciones.



- Strata Cloud Manager genera alertas e incidentes que se ajustan dinámicamente en función del valor histórico de la métrica y sus tendencias de uso. Puede ajustar esta configuración para controlar el nivel de sensibilidad del algoritmo de detección de anomalías.

  Vaya a **Incidents & Alerts (Incidentes y alertas)** > **Incident & Alert Settings (Configuración de incidentes y alertas)** > **Anomaly Sensitivity (Sensibilidad a anomalías)** para configurar el nivel de sensibilidad del algoritmo de detección de anomalías.

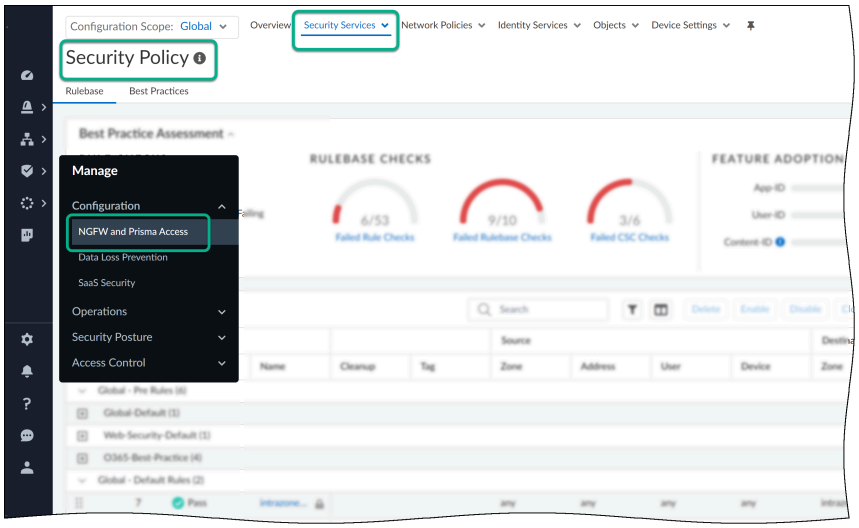


Gestionar: NGFW y Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Strata Cloud Manager le permite configurar una política de seguridad que se comparte entre sus NGFW y Prisma Access. Para empezar:

- ❑ Configure Prisma Access, sus NGFW o ambos con Strata Cloud Manager
- ❑ Configure carpetas para agrupar los NGFW que requieren una configuración similar. Las carpetas de Prisma Access están predefinidas y le permiten orientar la configuración según el tipo de implementación: usuarios móviles, redes remotas, conexiones de servicio.
- ❑ Establezca el Gestionar: Alcance de la configuración en el que desea trabajar. Puede configurar los ajustes que se aplicarán globalmente, tanto en sus NGFW como en el entorno de Prisma Access, y también puede dirigir la configuración a NGFW específicos o implementaciones de Prisma Access en función de carpetas.
- ❑ Use Gestionar: Fragmentos para estandarizar una configuración de base común para un conjunto de dispositivos NGFW o implementaciones. Los fragmentos le permiten incorporar rápidamente nuevos dispositivos, usuarios o ubicaciones con una configuración correcta conocida y reducir el tiempo necesario para incorporar un nuevo dispositivo.
- ❑ Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** para comenzar a crear su política de seguridad y compartirla entre sus NGFW y Prisma Access utilizando las funciones de gestión descritas anteriormente.



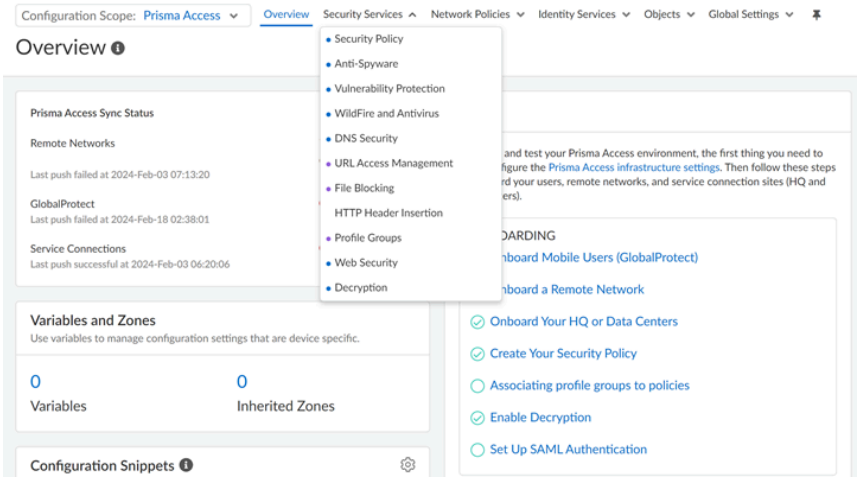
Gestionar: Alcance de la configuración

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Con Strata Cloud Manager, puede aplicar los ajustes de configuración y hacer cumplir la políticas en todo el entorno, o los ajustes y la políticas de destino en determinadas partes de su organización. Al trabajar en la gestión de la configuración de Strata Cloud Manager, el **Configuration Scope (Alcance de configuración)** actual siempre es visible para usted y puede alternar su vista para gestionar una configuración más amplia o más granular.

Puede obtener claridad sobre los elementos de configuración que son aplicables para un ámbito de configuración particular y si son heredados de un ámbito de configuración común o generados por el sistema. Los indicadores de configuración codificados por colores le ayudan a comprender de dónde se heredan las configuraciones y también a distinguir visualmente los tipos de objetos para facilitar el análisis.

- Punto gris indica configuración heredada
- Punto morado indica una configuración predefinida
- Punto azul indica que el objeto está presente en el ámbito de configuración actual



Los ajustes de configuración **globales** le ayudan a gestionar y aplicar fácilmente los requisitos de políticas que se aplican a todo el tráfico de red. Alternativamente, puede orientar los parámetros de políticas y configuración a los tipos de implementaciones donde tengan sentido.

- **Prisma Access**
  - **Contenedor de usuarios móviles**: la configuración se aplica a todos los tipos de conexión de usuario móvil: GlobalProtect y Proxy explícito, o individualmente a cada tipo de conexión.
  - **Redes remotas**: la configuración se aplica a sitios de redes remotas (sucursales, locales minoristas, etc.).
  - **Conexiones de servicio**: la configuración se aplica a los sitios de conexión de servicio (sede central y centros de datos).
- **Todos los cortafuegos**: los ajustes se aplican a todas los NGFW o a carpetas específicas que agrupan NGFW que requieren ajustes de configuración compartidos o específicos o la aplicación de políticas.

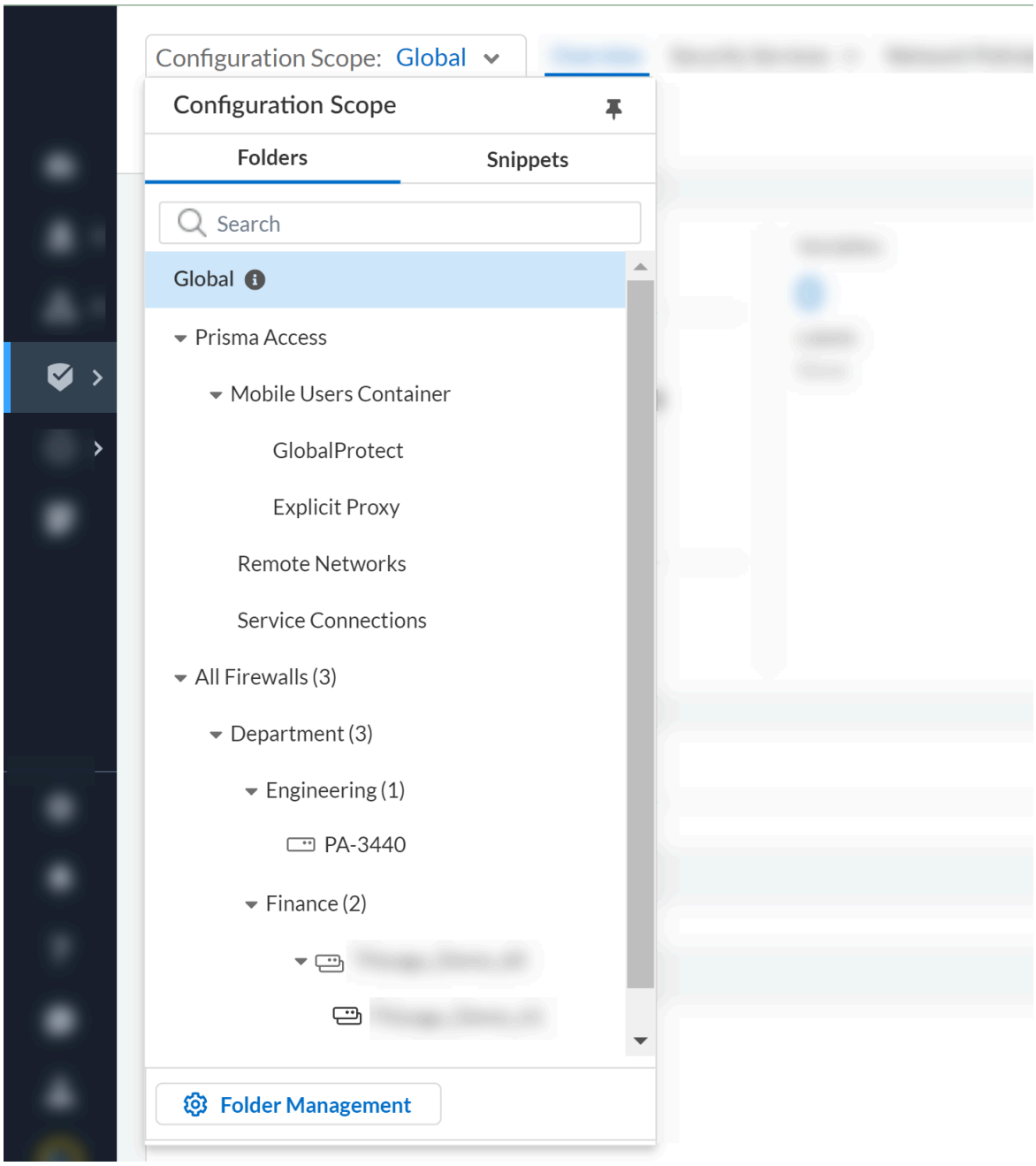
Obtenga más información sobre:

- **Flujos de trabajo: Gestión de carpetas**

  Utilice carpetas para agrupar lógicamente sus dispositivos y tipos de implementación para una gestión de configuración simplificada.
- **Gestionar: Fragmentos**

  Utilice fragmentos de código para agrupar configuraciones que pueda enviar rápidamente a sus cortafuegos o implementaciones.
- **Gestionar: Variables**

  Utilice variables en sus configuraciones para acomodar dispositivos u objetos de configuración específicos de la implementación.



Gestionar: Fragmentos

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ☐ Prisma Access ☐ AIOps for NGFW Premium ☐ Strata Cloud Manager Essentials

¿Dónde puedo usar esto?	¿Qué necesito?
	❑ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

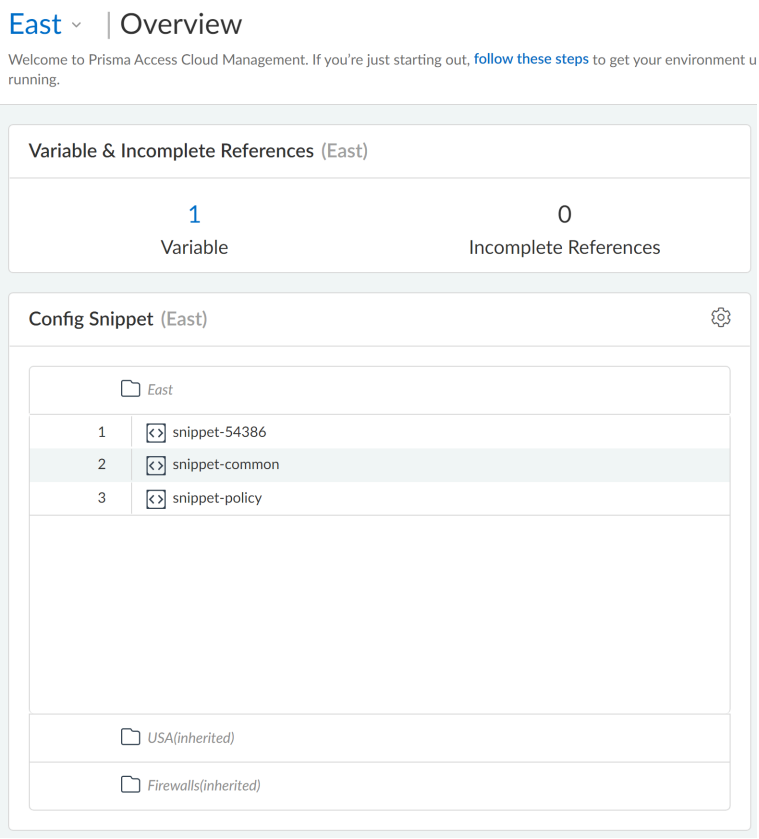
Utilice fragmentos de código para agrupar configuraciones que pueda enviar rápidamente a sus cortafuegos o implementaciones.

Un fragmento es un objeto de configuración, que no puede caber en una jerarquía o agrupación de objetos de configuración, que se puede asociar a una carpeta, implementación o dispositivo. Los fragmentos de código se utilizan para estandarizar una configuración base común para un conjunto de cortafuegos o implementaciones, lo que le permite incorporar rápidamente nuevos dispositivos con una configuración correcta conocida y reducir el tiempo necesario para incorporar un nuevo dispositivo. Por ejemplo, puede incorporar un nuevo cortafuegos en una sucursal remota. Puede asociar un conjunto de fragmentos de código que contengan todas las configuraciones de reglas de red y políticas necesarias con la carpeta a la que pertenece el nuevo cortafuegos. Esto reduce el tiempo necesario para configurar el cortafuegos para proteger la sucursal remota.

Las asociaciones de fragmentos tienen una prioridad descendente en caso de que los valores de los objetos entren en conflicto. No se permiten reglas con nombres duplicados y se produce un error en la validación durante la creación de un fragmento con el mismo nombre en cualquier carpeta o al asociar un fragmento a una carpeta si el fragmento con el mismo nombre ya está asociado.

Esto significa que si el primer y el último fragmento asociado tienen valores diferentes para el mismo objeto, el dispositivo o la implementación heredan el valor del primer fragmento. Además, todas las configuraciones heredadas de un fragmento se pueden anular en el nivel de carpeta secundaria, implementación o dispositivo.

Dentro de una jerarquía de carpetas, es posible que un fragmento solo se asocie una vez dentro de cualquier jerarquía de carpetas. Esto significa que un fragmento no se puede asociar a una carpeta y a la carpeta anidada debajo de ella. Sin embargo, puede asociar el mismo fragmento con diferentes carpetas o carpetas anidadas en diferentes carpetas. Los fragmentos de código que ya están asociados a una carpeta en la jerarquía de carpetas aparecen atenuados para que no se puedan usar más de una vez cuando corresponda.



Referenciabilidad de la configuración transversal de fragmentos

Esta función le permite hacer referencia a cualquier configuración u objeto común adjunto a un ámbito global e insertarlo en los cortafuegos NGFW y Prisma Access. Estos objetos y configuraciones compartidos dentro del ámbito global están disponibles para todos los fragmentos. Un fragmento asociado con el alcance global se considera un fragmento global. Se puede hacer referencia a los objetos definidos dentro de estos fragmentos adjuntos al ámbito global en cualquier fragmento de código de la configuración.

Por ejemplo, puede crear un fragmento denominado Global Variable para consolidar variables y adjuntarlo a un ámbito global. Esto garantiza una fácil referencia y disponibilidad en todos los demás fragmentos de la configuración. Del mismo modo, puede gestionar de forma eficaz categorías de URL personalizadas para reglas de política de acceso, perfiles de prevención de amenazas, zonas, direcciones y otros objetos que representan segmentos de red estándar.

Crear un fragmento

Cree y asocie un fragmento a una carpeta, implementación o dispositivo para aplicar una configuración de referencia común a un grupo de dispositivos. Puede asociar tantos fragmentos a una carpeta, implementación o dispositivo como sea necesario.

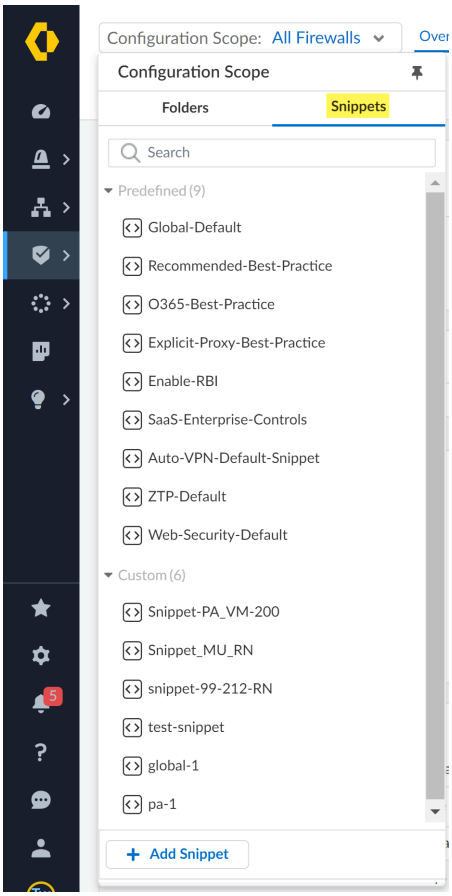
Los fragmentos se pueden modificar y volver a asociar con cualquier carpeta, implementación o dispositivo en cualquier momento después de su creación.

Los fragmentos personalizados que ya no estén en uso se pueden eliminar.

STEP 1 | Inicie sesión en Strata Cloud Manager.

STEP 2 | Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Overview (Visión general)** y expanda el alcance de configuración para ver los **Snippets (Fragmentos)**.

STEP 3 | **Add Snippet (Añadir fragmento)**.

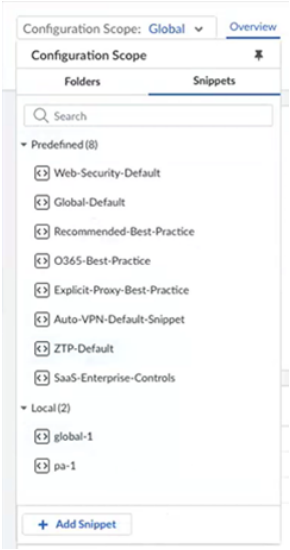


STEP 4 | Crear el fragmento.

1. Dale al fragmento un **Name (Nombre)** descriptivo.
2. (Opcional) Introduzca una **Description (Descripción)** para el fragmento.
3. (Opcional) Asigne uno o más **Labels (Etiquetas)**.

   Puede seleccionar una etiqueta existente o crear una nueva escribiendo la etiqueta que desea crear.
4. **Create (Crear)**.

   Los fragmentos recién creados se enumeran categorizados en Fragmentos **Local (locales)**. Una vez publicados los fragmentos, estos se mueven a Fragmentos publicados.



STEP 5 | Cree la configuración del fragmento.

Ahora se encuentra en el Alcance de configuración del fragmento. Todas las configuraciones que cree en el ámbito del fragmento de código solo se producen para el fragmento de código.

Mientras está en el alcance del fragmento, puede revisar el fragmento **Descripción general** para ver información detallada sobre el fragmento. Esto incluye información como el número de variables, información sobre el fragmento que se creó y se actualizó por última vez, y la lista de todas las carpetas, implementaciones y dispositivos a los que está asociado el fragmento.

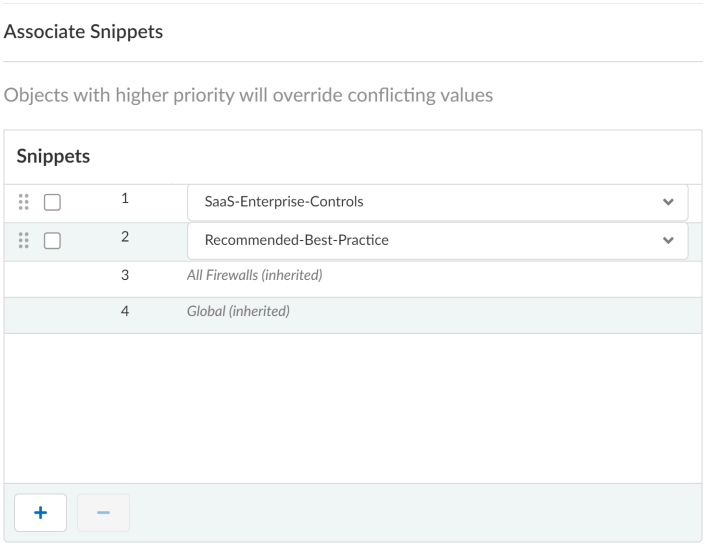
STEP 6 | Asociar un fragmento.

1. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Overview (Visión general)** y expanda el alcance de la configuración para ver el **Config Tree (Árbol de configuración)**.
2. Seleccione la carpeta, la implementación o el dispositivo al que desea asociar el fragmento.
3. Editar el **Config Snippet (Fragmento de configuración)**.
4. Añada los fragmentos que desee asociar y ordénelos según sea necesario.

   Si va a asociar un fragmento de código al ámbito global, se puede hacer referencia a él y estará disponible para todos los demás fragmentos de código de la configuración. Todos

los fragmentos podrán hacer referencia a los objetos que tiene en el fragmento adjunto a la carpeta global.

5. **Cerrar**.



STEP 7 | Seleccione **Push Config (Configuración de envío)** para enviar los cambios de configuración a su red.

Modificar un fragmento

Modifique las configuraciones, los detalles y las asociaciones de los fragmentos.

Los fragmentos personalizados que ya no estén asociados a una carpeta, implementación o dispositivo se pueden eliminar.

STEP 1 | Inicie sesión en Strata Cloud Manager.

STEP 2 | Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Overview (Visión general)** y expanda el alcance de configuración para ver los **Snippets (Fragmentos)**.

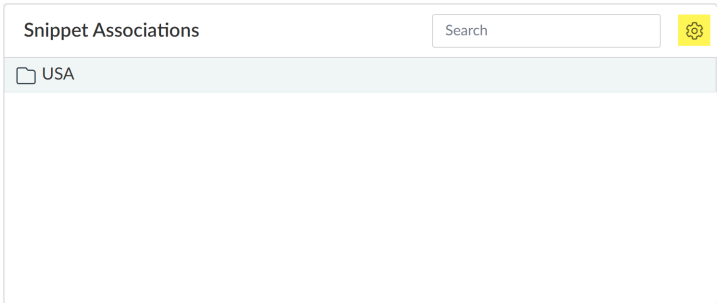
STEP 3 | Seleccione el fragmento que desea modificar.

Después de seleccionar un fragmento, se le redirigirá a la **Overview (Descripción general) del fragmento**.

STEP 4 | (Opcional) Edite el fragmento para modificar el **Name (Nombre)**, **Description (Descripción)**, o para cambiar o asignar **Labels (Etiquetas)**. Habilitar o deshabilitar **Pause Update (Pausar actualización)** para ver las diferencias de configuración y decidir aceptar el cambio.

STEP 5 | Edite las **Snippet Associations (Asociaciones de fragmentos)** para volver a asociar el fragmento con una carpeta, implementación o dispositivo diferente, o para asociar el fragmento con carpetas, implementaciones o dispositivos adicionales.

Salga de la pantalla de reasociación de fragmentos para aplicar los cambios.



STEP 6 | Realice los cambios necesarios en la configuración del fragmento.

STEP 7 | **Push Config (Enviar configuración)**.

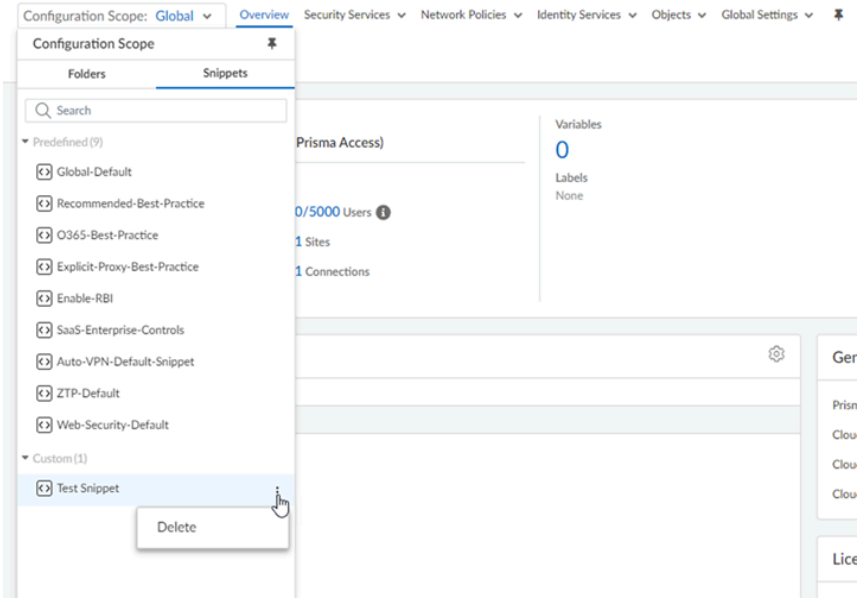
Eliminar un fragmento

Elimine sus fragmentos personalizados para mantener sus configuraciones organizadas. Los fragmentos de código no deben estar asociados a ningún cortafuegos, carpeta o implementación antes de que se puedan eliminar. No se admite la eliminación de fragmentos predefinidos.

STEP 1 | Inicie sesión en Strata Cloud Manager.

STEP 2 | Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Overview (Visión general)** y expanda **Configuration Scope (Alcance de la configuración** para ver los Fragmentos.

STEP 3 | Haga clic en los tres puntos verticales del fragmento personalizado que desea eliminar.



STEP 4 | **Delete (Eliminar)** el fragmento.

> *Los fragmentos asociados actualmente a carpetas, implementaciones o dispositivos no se pueden eliminar. En primer lugar, edite las **Snippet Associations (Asociaciones de fragmentos)** para eliminar todas las asociaciones existentes antes de que se pueda eliminar.*

Duplicar un fragmento

Si desea utilizar un fragmento de código existente como plantilla para un nuevo fragmento, puede duplicarlo fácilmente para no tener que configurar un nuevo objeto.

Los fragmentos duplicados no están asociados a ningún dispositivo, carpeta o implementación; lo que le permite personalizarlos libremente sin tener que desasociarlos antes de comenzar las configuraciones.

STEP 1 | Inicie sesión en Strata Cloud Manager.

STEP 2 | Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Overview (Visión general)** y expanda **Configuration Scope (Alcance de la configuración** para ver los Fragmentos.

STEP 3 | Haga clic en los tres puntos verticales del fragmento personalizado que desea duplicar.

STEP 4 | **Clone (Duplicar)** el fragmento.

1. (Opcional) Asigne un nuevo nombre al fragmento duplicado.

Compartir una configuración de fragmento

Esta característica proporciona un método único y flexible para compartir configuraciones comunes entre cualquier inquilino, incluso en un entorno de varios inquilinos. Puede guardar y gestionar varias configuraciones como fragmentos, compartiéndolas fácilmente entre los inquilinos de una cuenta de cliente. Esta capacidad proporciona una flexibilidad y un control considerables en la gestión de configuraciones compartidas en diferentes entornos de inquilino.

Además, esta característica admite la centralización de la gestión de la configuración para escenarios comunes entre inquilinos y la supervisión de configuraciones globales dentro de una configuración de varias unidades de negocio.

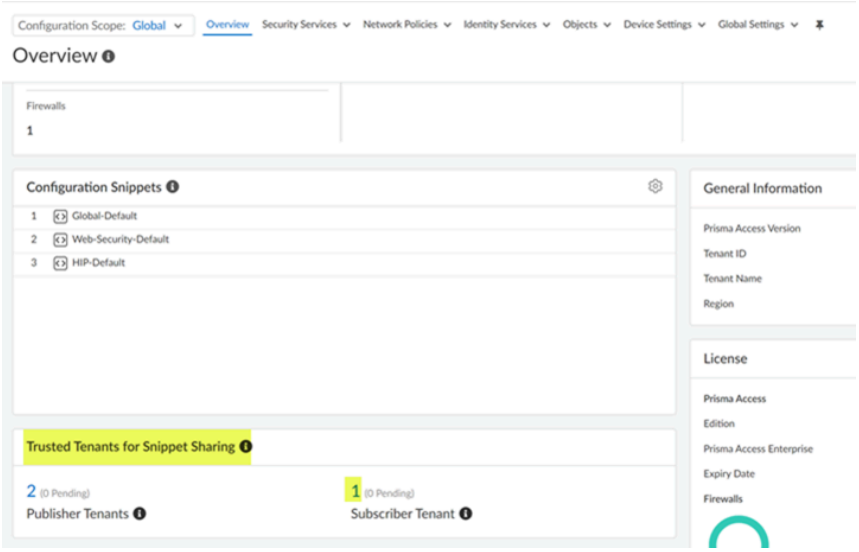
En este marco, el inquilino del editor comparte fragmentos de código con el inquilino del suscriptor, mientras que el inquilino del suscriptor recibe fragmentos del inquilino del editor.

STEP 1 | Inicie sesión en Strata Cloud Manager.

STEP 2 | En el inquilino del editor, seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Overview (Visión general)**, seleccione el alcance de configuración **Global**.

STEP 3 | **Establecer la confianza entre los inquilinos**: Establezca una conexión entre el suscriptor y los inquilinos del editor para permitir el uso compartido de fragmentos.

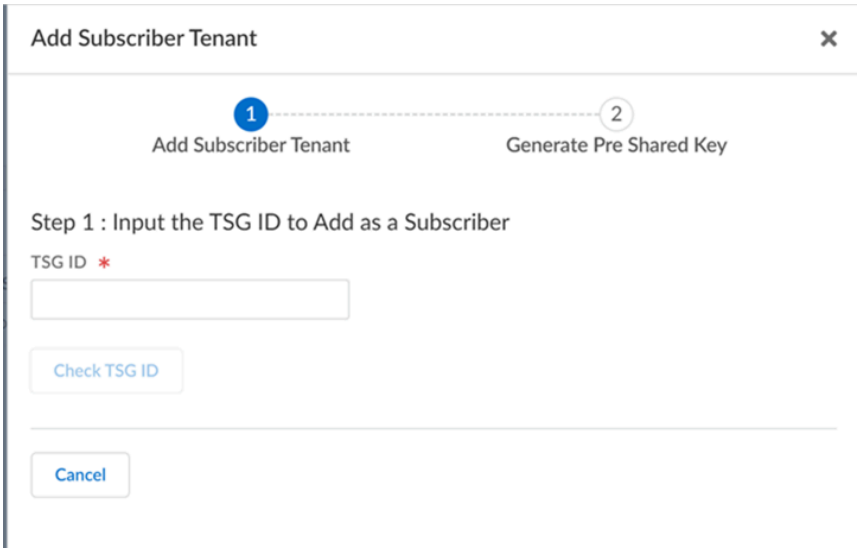
1. Haga clic en **Subscriber Tenant (Inquilino del suscriptor)** en **Trusted Tenants for Snippet Sharing (Inquilinos de confianza para el uso compartido de fragmentos de código)**.



2. **Add Subscriber Tenant (Añadir inquilino de suscriptor)**.

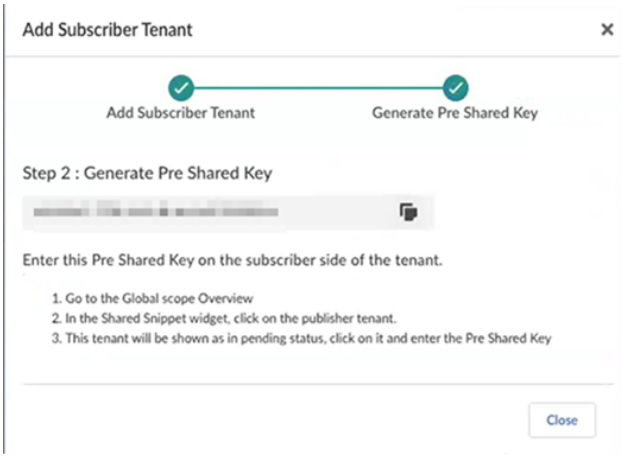
3. Introduzca el archivo **TSG ID** para añadir como inquilino de suscriptor, y **Check TSG ID (Comprobar el ID de TSG)**. Esto garantiza la prevención de ataques TSG generados aleatoriamente o basados en TSG serializados.

   Tras una validación correcta, un mensaje de confirmación indica que se ha verificado el ID de TSD.



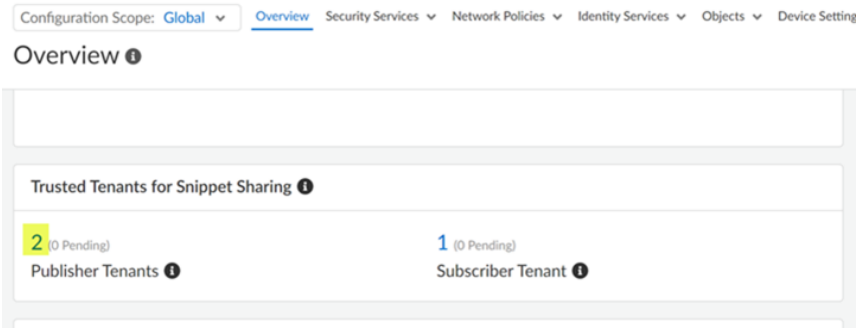
4. **Siguiente: Generar clave precompartida**.

   Copie la PSK generada. Introducirá este PSK al validar el inquilino del editor en el paso 4.



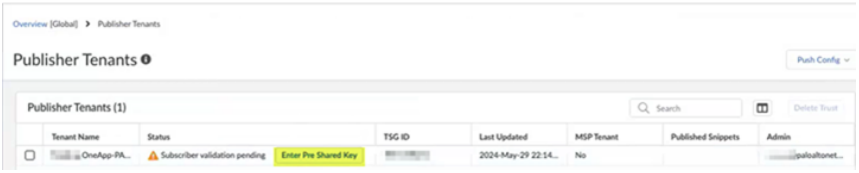
STEP 4 | Vaya al inquilino del suscriptor, seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Overview (Visión general)** y establezca el alcance de configuración en **Global**.

1. El estado **Publisher Tenants (Inquilinos del editor)** en **Trusted Tenants for Snippet Sharing (Inquilinos de confianza para el uso compartido de fragmentos de código)** se muestra como **Pending (Pendiente)**.



2. Haga clic en **Publisher Tenants (Inquilinos de editor)** y **Enter Pre Shared Key (Introducir clave precompartida)** generada en el paso anterior, y luego en **Validate (Validar)** para validar el inquilino del suscriptor.

   Después de una validación correcta, un mensaje confirma que el inquilino es de confianza, lo que establece la confianza entre el suscriptor y los inquilinos del editor.



STEP 5 | Publique un fragmento en un inquilino del suscriptor.

1. Cree y asocie el fragmento con una carpeta.

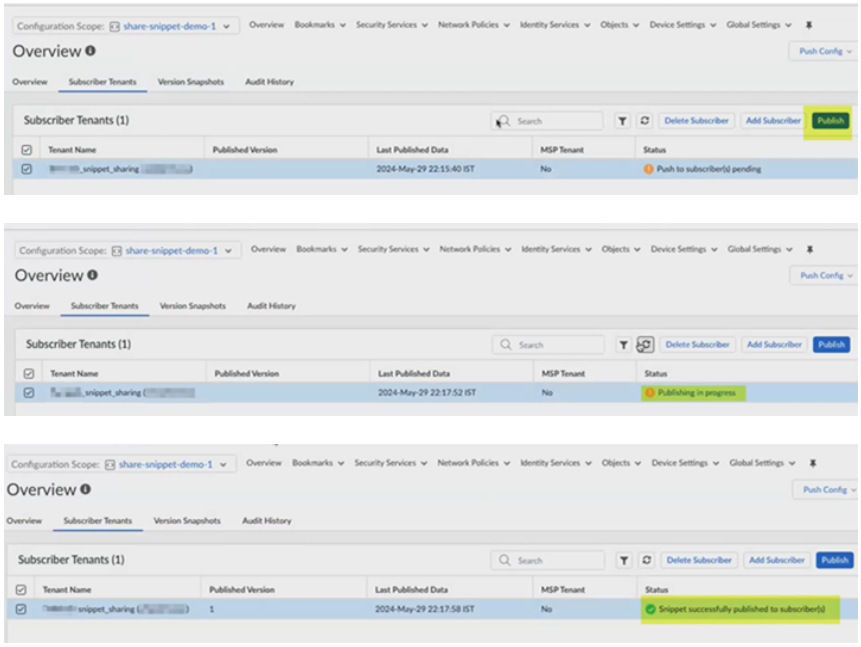
   Los fragmentos recién creados están disponibles en Fragmentos **local (locales)**.

   - La **Overview (Visión general)** muestra los detalles del fragmento, como el nombre, la descripción, la hora de creación (cuando se cargó el fragmento en el lado del suscriptor), la hora de la última actualización y los detalles de las etiquetas.
   - La pestaña **Subscriber Tenants (Inquilinos de suscriptores)** muestra el nombre del inquilino, la versión publicada en el inquilino, la última fecha de publicación y el estado de publicación.
     - Haga clic en **Published Version (Versión publicada)** para revisar los cambios de configuración.
     - Antes de publicar un fragmento de código en un inquilino, deberá **Add Subscriber (Añadir suscriptor)** y **Save (Guardar)**.
   - Las **Version Snapshots (Instantáneas de versión)** proporciona un historial de la configuración de su fragmento. En esta pantalla, puede comparar las instantáneas de configuración con la configuración candidata, y **Save Version Snapshot (Guardar instantánea de versión)** o **Load (Cargar)** una instantánea de configuración anterior como candidato. Haga clic en el botón **Version (Versión)** para ver las diferencias de configuración.
   - El **Audit History (Historial de auditoría)** proporciona una pista de auditoría de todas las acciones iniciadas por el administrador. Registra detalles como el número de versión

publicada, los cambios realizados, el propietario del cambio, la fecha y la hora del cambio y los detalles del cambio.

2. En la pestaña **Subscriber Tenant (Inquilino del suscriptor**, seleccione el nombre del inquilino y **Publish (Publicar)**.

   Esto envía la solicitud de publicación al inquilino del suscriptor. En la columna **Status (Estado)** indica que el fragmento se publicó correctamente para el suscriptor y el fragmento estará disponible en Fragmentos publicados.



STEP 6 | Verificar en el inquilino del suscriptor.

1. Vaya a **Overview (Visión general)** > **Configuration Scope (Alcance de la configuración)** > **Snippets (Fragmentos)**y seleccione el fragmento de código en fragmentos **Subscribed (Subscritos)**.

   Se te redirigirá a la **Overview (Visión general)** de los fragmentos que muestra detalles como el nombre del inquilino del editor, la descripción, el ID de TSG, la hora de creación del fragmento, la hora de la última actualización, las etiquetas y los detalles de la actualización en pausa.

STEP 7 | Eliminar la confianza.

> *Los fragmentos de código suscritos asociados a carpetas o cortafuegos solo se pueden clonar y no se pueden eliminar.*

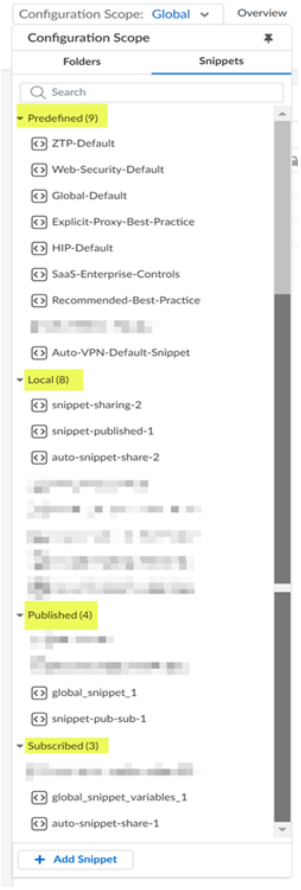
1. Vaya al suscriptor o al inquilino del editor.
2. Haga clic en **Subscriber Tenant (Inquilino del suscriptor)** en **Trusted Tenants for Snippet Sharing (Inquilinos de confianza para el uso compartido de fragmentos de código)**.
3. Seleccione la opción **Tenant Name (Nombre del inquilino)**y **Delete Trust (Eliminar confianza)**.

Después de eliminar la confianza, el fragmento ya no se asociará con el cortafuegos o la carpeta y se convertirá en un fragmento local.

Clasificación de fragmentos

- Predefinido: Todos los usuarios de Strata Cloud Manager pueden acceder a estos fragmentos para configurar rápidamente nuevos cortafuegos e implementaciones con configuraciones de prácticas recomendadas.
- Local: Estos fragmentos de código editables se crean dentro del inquilino y no se pueden compartir con otros inquilinos suscriptores.
- Publicado: Los inquilinos de suscriptores de confianza tienen acceso a estos fragmentos compartidos, que no se pueden duplicar ni editar.

- Subscrito: Estos fragmentos, compartidos por el inquilino del editor, los pueden duplicar los usuarios, pero no se pueden modificar.



Gestionar: Variables

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ☐ Prisma Access ☐ AIOps for NGFW Premium ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Utilice variables en sus configuraciones para acomodar dispositivos u objetos de configuración específicos de la implementación.

Las variables son una herramienta avanzada que le permite estandarizar sus configuraciones, al tiempo que le proporciona la flexibilidad necesaria para acomodar valores de configuración únicos que son específicos del dispositivo o de la implementación. Las variables le permiten reducir el número de fragmentos de código que necesita gestionar, al tiempo que le permiten mantener los valores de configuración específicos del cortafuegos o de la implementación según sea necesario.

Por ejemplo, tiene un fragmento de código para la configuración que desea asociar con varios anidados donde cada carpeta anidada contiene un conjunto de cortafuegos específicos de una ubicación geográfica. En el fragmento, ha configurado reglas de política para restringir el acceso a los sistemas críticos para la empresa solo para rangos de IP específicos. En este escenario, puede crear una variable para cada intervalo de IP específico de cada carpeta anidada y usar esa variable en la configuración del fragmento heredado. Esto le permite gestionar e insertar cambios de configuración mientras usa menos fragmentos para acomodar valores de configuración específicos del dispositivo o de la implementación.

Las variables se pueden crear en el nivel de carpeta, implementación o cortafuegos. Al crear una variable para una carpeta, la variable la heredan todas las carpetas anidadas en la carpeta. En el caso de que haya variables en conflicto en un ámbito de configuración de carpeta, el cortafuegos o la implementación heredan el valor de la variable de la carpeta que contiene las carpetas anidadas. Sin embargo, puede invalidar una variable heredada en el nivel de carpeta anidada, implementación o cortafuegos.

Se admiten los siguientes tipos de variables:

Tipo de variable	Description (Descripción)
AS Number	Número de sistema autónomo que se utilizará en la configuración de BGP.
Count	Número de eventos que deben producirse para desencadenar una acción.
ID de dispositivo	Device-ID que se usará para asignar un evaluador de prioridad de dispositivo en una configuración de alta disponibilidad (HA) activa/activa.
Prioridad del dispositivo	Prioridad del dispositivo para indicar una preferencia sobre qué cortafuegos debe asumir la función activa en una configuración de alta disponibilidad (HA) activa-pasiva.
Máximo de salida	Valor máximo de salida que se utilizará en la configuración del perfil de calidad de servicio (QoS).
FQDN	Nombre de dominio cualificado completo.
ID de grupo	ID de grupo de alta disponibilidad.
Máscara de red IP	IP estática o dirección de red.
Rango de IP	Un rango de IP. Por ejemplo, **`192.168.1.10-192.168.1.20`**

Tipo de variable	Description (Descripción)
Comodín IP	Máscara comodín de IP para permitir o denegar direcciones IP similares. Por ejemplo, `10.0.0.5/255.255.0.255`.
Etiqueta de enlace	Etiqueta de enlace para usar en la configuración de SD-WAN.
Porcentaje	Porcentaje entre **`0`** y **`99`**.
Puerto	Puerto de origen o destino.
Perfil de QoS	Perfil de QoS para su uso en configuraciones de QoS.
Tasa	Tasa para especificar un umbral que desencadena una acción. Por ejemplo, la `Tasa de alarmas` para un perfil de protección DoS.
ID del enrutador	ID de enrutador al configurar el protocolo de puerta de enlace de borde (BGP) para un enrutador lógico.
Temporizador	Temporizador en segundos para configurar un umbral que desencadene una acción.
Zona	Una zona de seguridad.

Crear una variable

También puede crear una variable en línea donde se admita una variable.

STEP 1 | Inicie sesión en Strata Cloud Manager.

STEP 2 | Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Overview (Visión general)** y seleccione el alcance de configuración donde desea crear la variable.

En **Folders (Carpetas)**, seleccione la carpeta o el dispositivo para el que desea crear una variable.

En **Snippets (Fragmentos)**, seleccione el fragmento específico para el que desea crear una variable.

STEP 3 | En la sección Variables, haga clic en el Recuento de variables que se muestra.

STEP 4 | **Add Variable (Añadir variable)**.

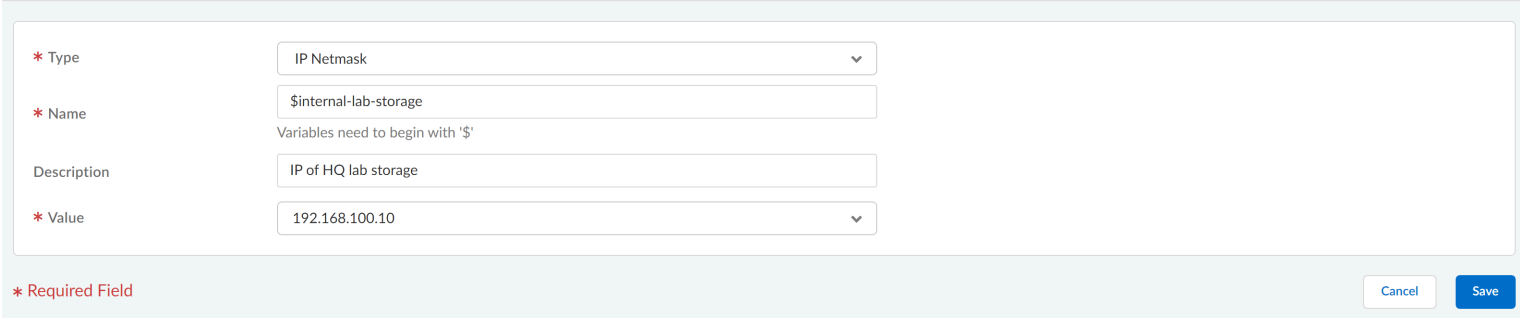
STEP 5 | Cree la variable.

En este ejemplo, se crea una variable de `Máscara de red IP` para su uso como objeto de dirección para un recurso interno crítico.

1. Seleccione el **Type (Tipo)** de variable.
2. Asigne a la variable un **Name (Nombre)** descriptivo.

   Todos los nombres de variables deben comenzar con **$**.
3. (Opcional) Introduzca una **Description (Descripción)** para la variable.
4. Introduzca el **Value (Valor)** de la variable.
5. **Save (Guardar)**.

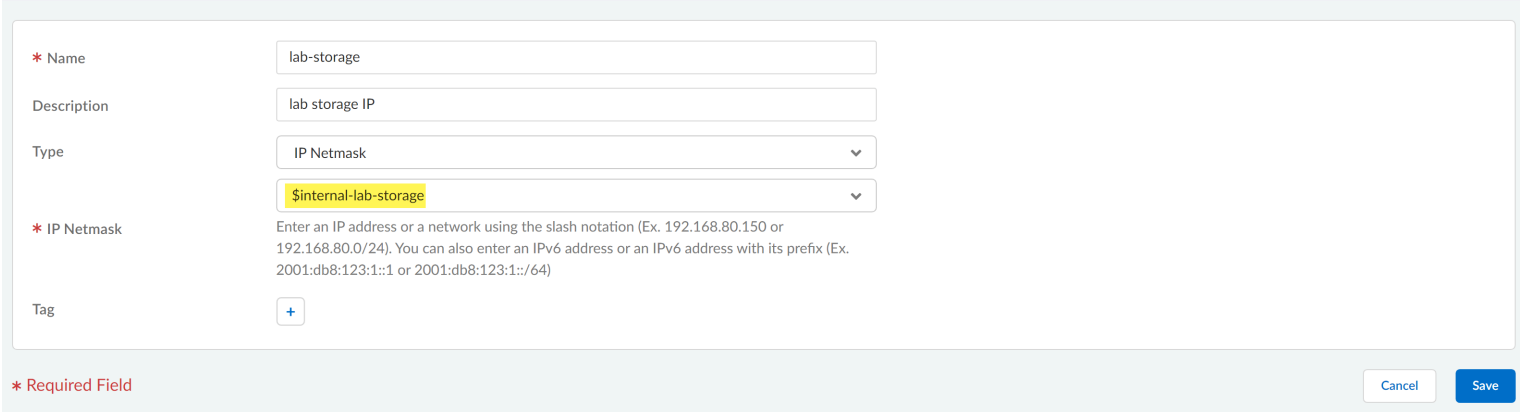
Variables



STEP 6 | Añada la variable a su configuración.

En este ejemplo, la variable `$internal-lab-storage` creada en el paso anterior se agrega a la configuración del objeto dirección.

Addresses



STEP 7 | **Push Config (Enviar configuración)**.

Importar una variable

¿Dónde puedo usar esto?	¿Qué necesito?
• Strata Cloud Manager	❑ Licencia de AIOps for NGFW Premium

¿Dónde puedo usar esto?	¿Qué necesito?
	❑ Licencia de Prisma Access

Importar variables a Strata Cloud Manager mediante un archivo CSV. Las importaciones de variables están diseñadas para sobrescribir varias variables heredadas de la jerarquía de carpetas por el cortafuegos, o ya configuradas en el ámbito de configuración del cortafuegos, con nuevos valores específicos del cortafuegos.

La variable ya debe estar heredada de la jerarquía de carpetas o configurada en el ámbito de configuración del cortafuegos para sobrescribir mediante importaciones de variables. No se admite la importación de variables para crear variables completamente nuevas.

STEP 1 | Inicie sesión en Strata Cloud Manager.

STEP 2 | Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Overview (Visión general)**.

STEP 3 | En la sección Variables, haga clic en el Recuento de variables que se muestra.

STEP 4 | Seleccione **CSV Export/Import (Exportar/importar CSV)** > **Export (Exportar)** para exportar las variables que desea sobrescribir.

Palo Alto Networks recomienda exportar primero las variables que desea sobrescribir. Esto garantiza que el archivo CSV que cargue en Strata Cloud Manager está formateado correctamente. Esto también acelera el proceso de importación al garantizar que la carpeta de destino y las variables del cortafuegos se atribuyan correctamente.

STEP 5 | Modifique las variables en el archivo CSV exportado.

Tenga en cuenta lo siguiente al modificar el archivo CSV para la importación.

- Solo los editores de texto sin formato, como el Bloc de notas, son compatibles para modificar un archivo CSV exportado.
- # significa que la variable se crea en la jerarquía de carpetas y es heredada por el cortafuegos.

  Elimine el # para invalidar el valor de la variable heredada con un valor específico del cortafuegos.

  Strata Cloud Manager ignora un valor de variable anexado con # en la importación, ya que solo se admiten los valores de variable de reemplazo en el ámbito de configuración del cortafuegos.
- `-NA-` significa que la variable no existe en la configuración del cortafuegos. Esto significa que la variable se creó fuera de la jerarquía de carpetas a la que pertenece el cortafuegos.

  Cambiar el valor de una variable a `-NA-` no es compatible. Strata Cloud Manager ignora cualquier valor de variable modificado a `-NA-`.

  La asignación de un valor específico del cortafuegos a una variable con un valor de `-NA-` no es compatible porque la variable no existe en el ámbito de configuración del cortafuegos. La variable debe ser heredada por el cortafuegos de la jerarquía de carpetas, o configurada en

el ámbito de configuración del cortafuegos, para que se reemplace mediante la importación de variables.

- Un valor de variable de `None#` o `None` significa que la variable se creó con la variable **Value (Valor)** como **None (Ninguna)**.

  Puede modificar cualquier valor de variable como `Ninguno` para eliminar el valor pero no eliminar la variable.

- En el caso de una variable creada en el ámbito de configuración del cortafuegos, si se elimina un valor de variable y se deja en blanco, se elimina la variable.

  En el caso de una variable creada en la jerarquía de carpetas y heredada por el cortafuegos, si se elimina un valor de variable y se deja en blanco, se revierte el valor de la variable al heredado de la jerarquía de carpetas.

1. Localice y abra el archivo CSV que has exportado. El formato del archivo CSV exportado, el nombre es:

   `<cloud-management-tenant-name> - Prisma Access_<export-date>_variables`

2. Modifique las variables según sea necesario.

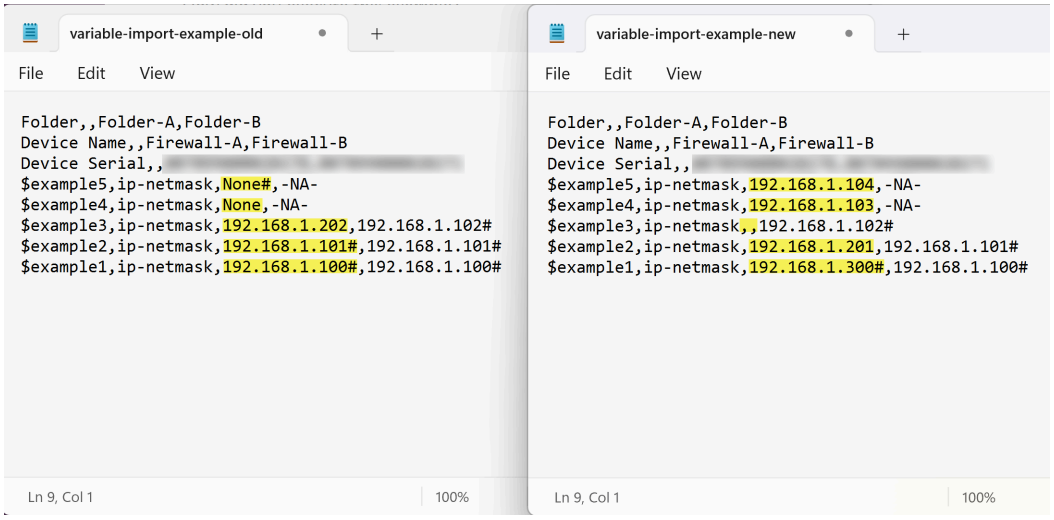
   Palo Alto Networks no recomienda modificar los nombres de las carpetas, los nombres de los dispositivos ni los números de serie de los mismos. Esto podría dar lugar a errores de importación.

   En el siguiente ejemplo, se realizaron los siguientes cambios en los valores de las variables en el ámbito de configuración `Cortafuegos-A` para ilustrar cómo se

pueden usar las importaciones de variables para modificar varias variables con una sola operación.

- `$example 1`: sobrescribe el valor heredado `None#` con un valor específico del cortafuegos.
- `$example 2`: sobrescribe el valor específico `Ninguno` del cortafuegos con un valor específico del cortafuegos.
- `$example 3`: si la variable se creó en el ámbito de configuración del cortafuegos, un valor vacío elimina la variable.

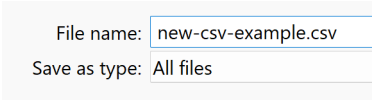
  Si la variable se heredó de la jerarquía de carpetas y se invalidó en el ámbito de configuración del cortafuegos, un valor vacío restaura el valor de la variable heredado de la jerarquía de carpetas.
- `$example 4`: sobrescriba el valor heredado `192.168.1.101` con un valor específico de cortafuegos.
- `$example 5`: ejemplo de un cambio de variable Strata Cloud Manager ignora porque # todavía está adjunto.



STEP 6 | Guarde sus cambios.

Seleccione **File (Archivo)** > **Save (Guardar)** para guardar los cambios realizados en el archivo CSV.

Como alternativa, seleccione **File (Archivo)** > **Save as (Guardar como)** para guardar los cambios en un nuevo archivo CSV. Para crear un nuevo archivo CSV, debe incluir **`.csv`** como la extensión del archivo.



STEP 7 | Importar el archivo CSV a Strata Cloud Manager.

1. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **Overview (Descripción general)**.
2. En la sección Variables, haga clic en el Recuento de variables que se muestra.
3. Seleccione **CSV Export/Import (Exportación/Importación de CSV)** > **Import (Importar)**.
4. **Choose File (Elija archivo)** y seleccione el archivo CSV que contiene las variables que ha modificado.
5. **Importar**.

Exportar variables

Exporte su carpeta y las variables de configuración del cortafuegos en formato CSV a su dispositivo local. La exportación de las variables es útil cuando se sobrescribe un gran número de variables en varios cortafuegos.

No es posible la exportación de variables de interfaz creadas al configurar una interfaz en el nivel de carpeta.

STEP 1 | Inicie sesión en Strata Cloud Manager.

STEP 2 | Seleccione **Manage (Gestionar)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Configuration (Configuración)** > **Overview (Visión general)**.

STEP 3 | En la sección Variables, haga clic en el Recuento de variables que se muestra.

STEP 4 | Seleccione **CSV Export/Import (Exportación/Importación de CSV)** > **Export (Exportar)**.

STEP 5 | Seleccione la carpeta y los cortafuegos con las variables que desea exportar y haga clic en **Next (Siguiente)**.

*Si desea exportar todas las variables creadas en Strata Cloud Managerseleccione **All Firewalls (Todos los cortafuegos)**.*

STEP 6 | Seleccione una o más variables para exportar.

STEP 7 | (Opcional) Deberá **Preview (Realizar una vista previa)** de las variables seleccionadas para ver detalles adicionales.

En la vista previa de variables, puede ver información como el nombre de la variable, el alcance de configuración donde se creó la variable y el valor de la variable.

Haga clic en **Cancel (Cancelar)** y continue con el siguiente paso o **Download CSV (Descargar CSV)** a su dispositivo local.

STEP 8 | Deberá **Export (Exportar)** las variables seleccionadas en formato CSV.

El CSV se exporta y descarga localmente en su dispositivo. El formato del archivo CSV exportado, el nombre es:

```
<cloud-management-tenant-name> - Prisma Access_<export-
date>_variables
```


Gestionar: Descripción general

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Piense en la página Descripción general como su punto de lanzamiento en NGFW y Prisma Access tanto para la configuración por primera vez, como para la gestión de la configuración diaria [**Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Overview (Descripción general)**].

- Global
- Prisma Access
- Strata Cloud Manager

Global

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Licencia de Prisma Access

Si selecciona el alcance de configuración **Global**, puede ver los siguientes detalles:

- Carpetas globales creadas y sus variables
- cortafuegos con conflictos de configuración
- Estado de sincronización del cortafuegos y Estado de conectividad del cortafuegos

- Información general
- Fragmentos de configuración
- Licencia
- Inquilinos de confianza para el uso compartido de fragmentos
- Instantáneas de la versión de configuración

Descripción general de la configuración (Prisma Access)

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licencia de Prisma Access

Si está empezando a usar Prisma Access:

- La lista de comprobación **Basic (Básica)** le muestra cómo ponerse en marcha con Prisma Access; complete las tareas y tutoriales aquí para comenzar con una configuración básica, luego, pruebe su entorno y desarrolle su implementación.
- Así es como funcionan las carpetas de políticas y configuración.
- A continuación, se explica cómo enviar cambios de configuración a Prisma Access.

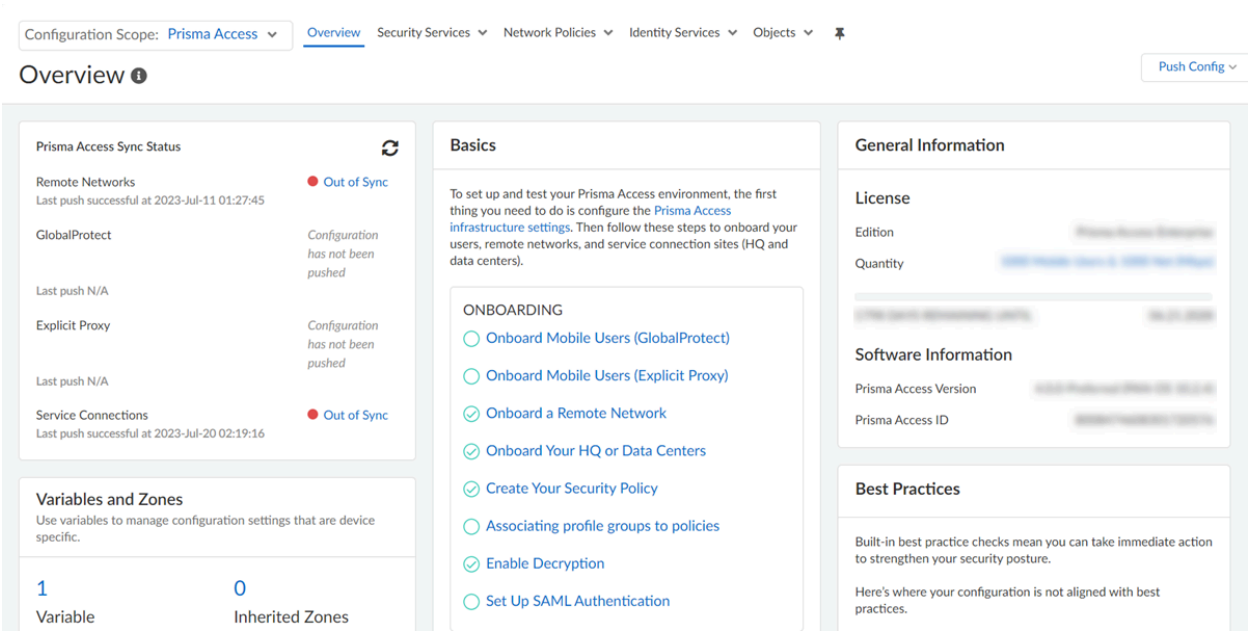
Para obtener más información sobre el entorno de Prisma Access:

- Revise los detalles de la **License (Licencia)** para ver qué incluye su suscripción a Prisma Access.
- El panel **Acerca de** muestra la **Información de software e inquilinos** para su entorno Prisma Access.

Para la gestión diaria de la configuración:

- Obtenga el estado de la configuración en un vistazo
- Estandarice una configuración base común para un conjunto de implementaciones de Prisma Access mediante el uso fragmentos de configuración
- Buscar instantáneas de configuración: comparar versiones de configuración y restaurar (o cargar) una versión anterior para recuperarse de un envío de configuración con un efecto no deseado en el flujo de tráfico o la seguridad
- Optimice su configuración limpiando los objetos y las reglas que no se utilizan, y endureciendo las reglas que introducen brechas de seguridad a través de aplicaciones con permisos que no se utilizan
- Identifique las áreas en las que puede realizar cambios de configuración que Fortalezcan su postura de seguridad

- También puede encontrar detalles sobre su Licencia de Prisma Access y qué incluye

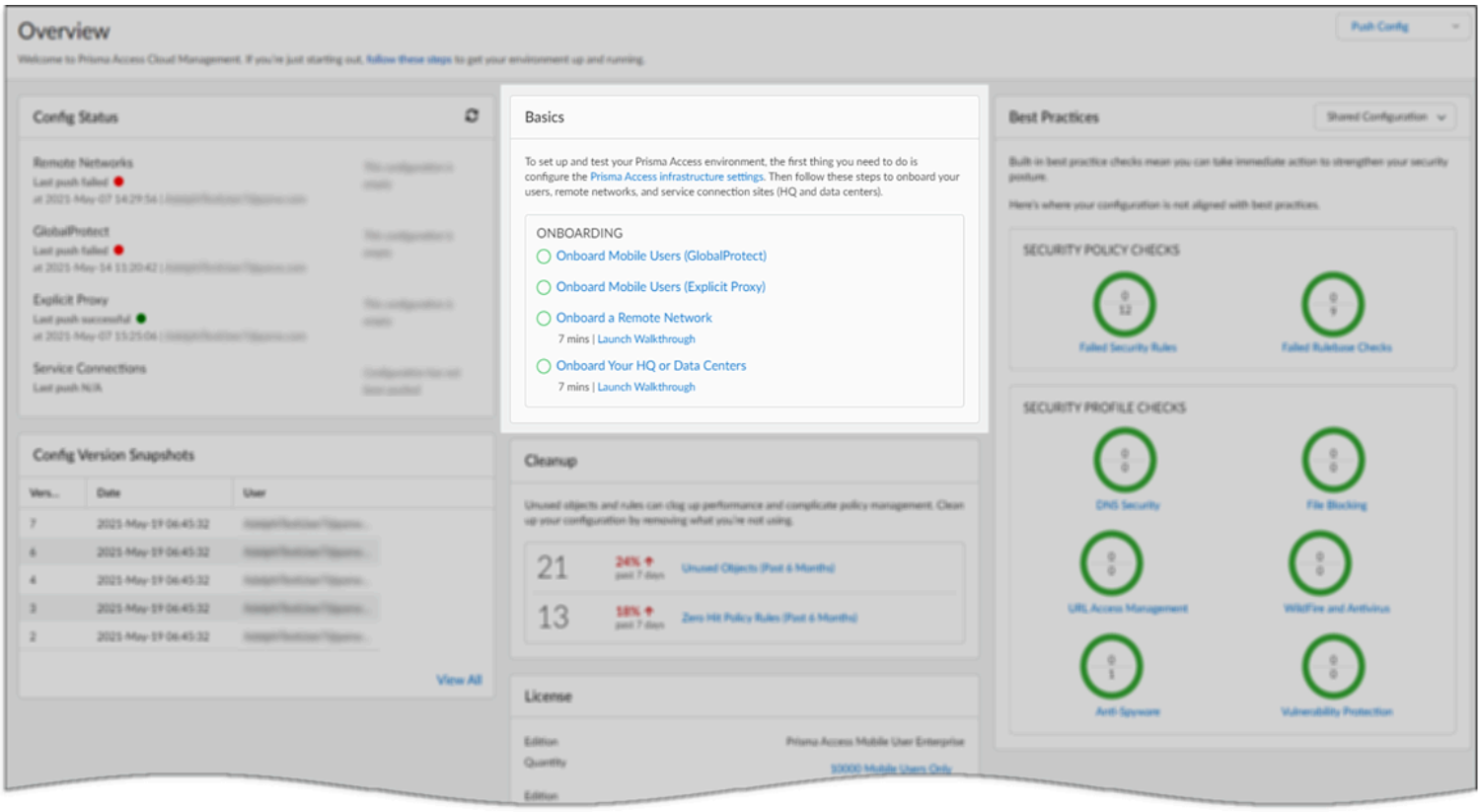


Después de completar la configuración básica, puede comenzar a probar su entorno y crear su implementación.

Básicas

Los **Fundamentos básicos** de la configuración de Prisma Access le guían para comenzar a trabajar con Prisma Access. Complete las tareas que se indican aquí para empezar con una configuración básica, que luego puede usar para probar el entorno y crear la implementación.

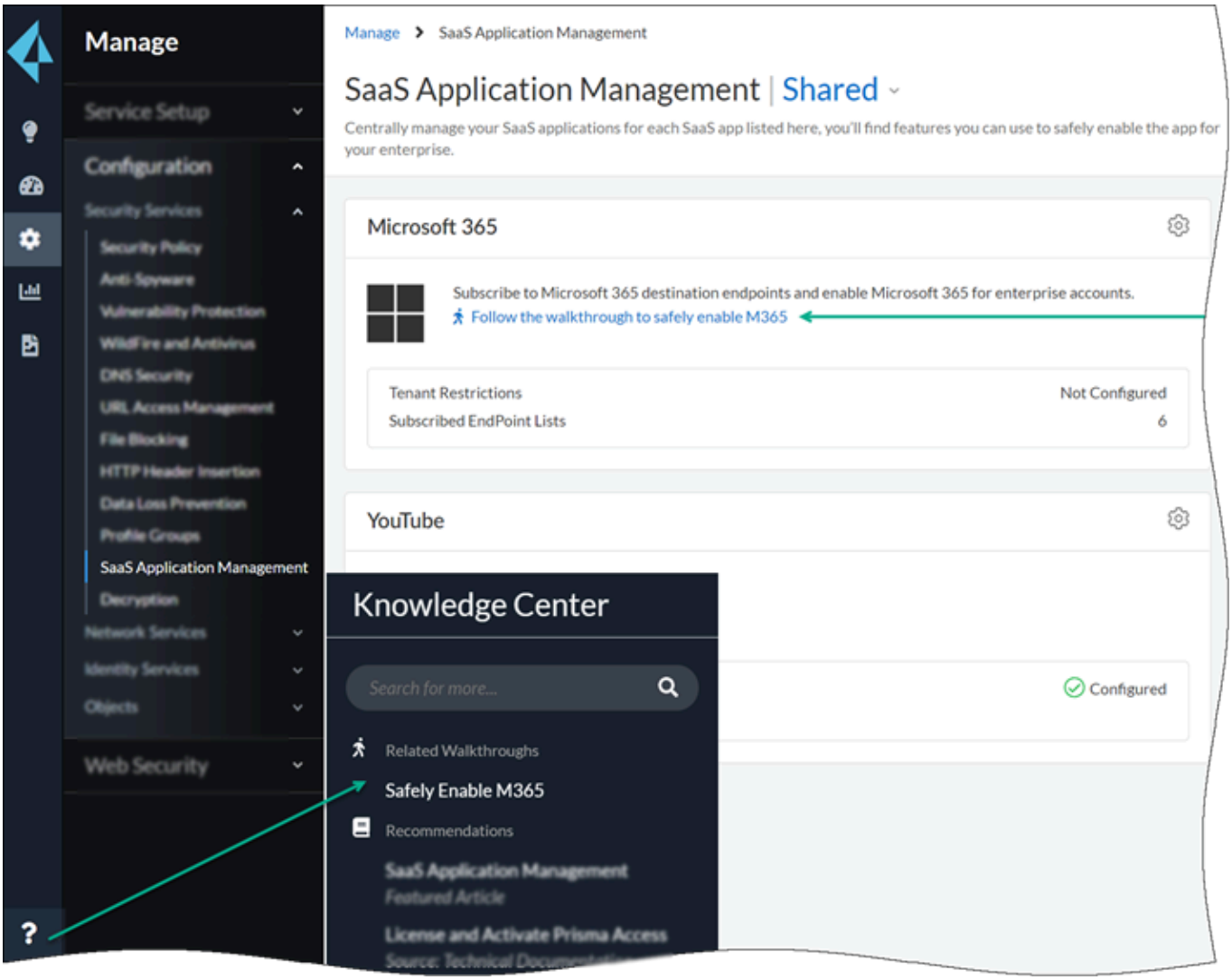
Cada tarea le vincula a la página en la que puede configurar la configuración asociada; cuando haya terminado, las tareas de esta lista se mostrarán como completadas. Por lo tanto, puede realizar fácilmente un seguimiento de su progreso de un vistazo, lo que es especialmente útil si está en la fase de incorporación.

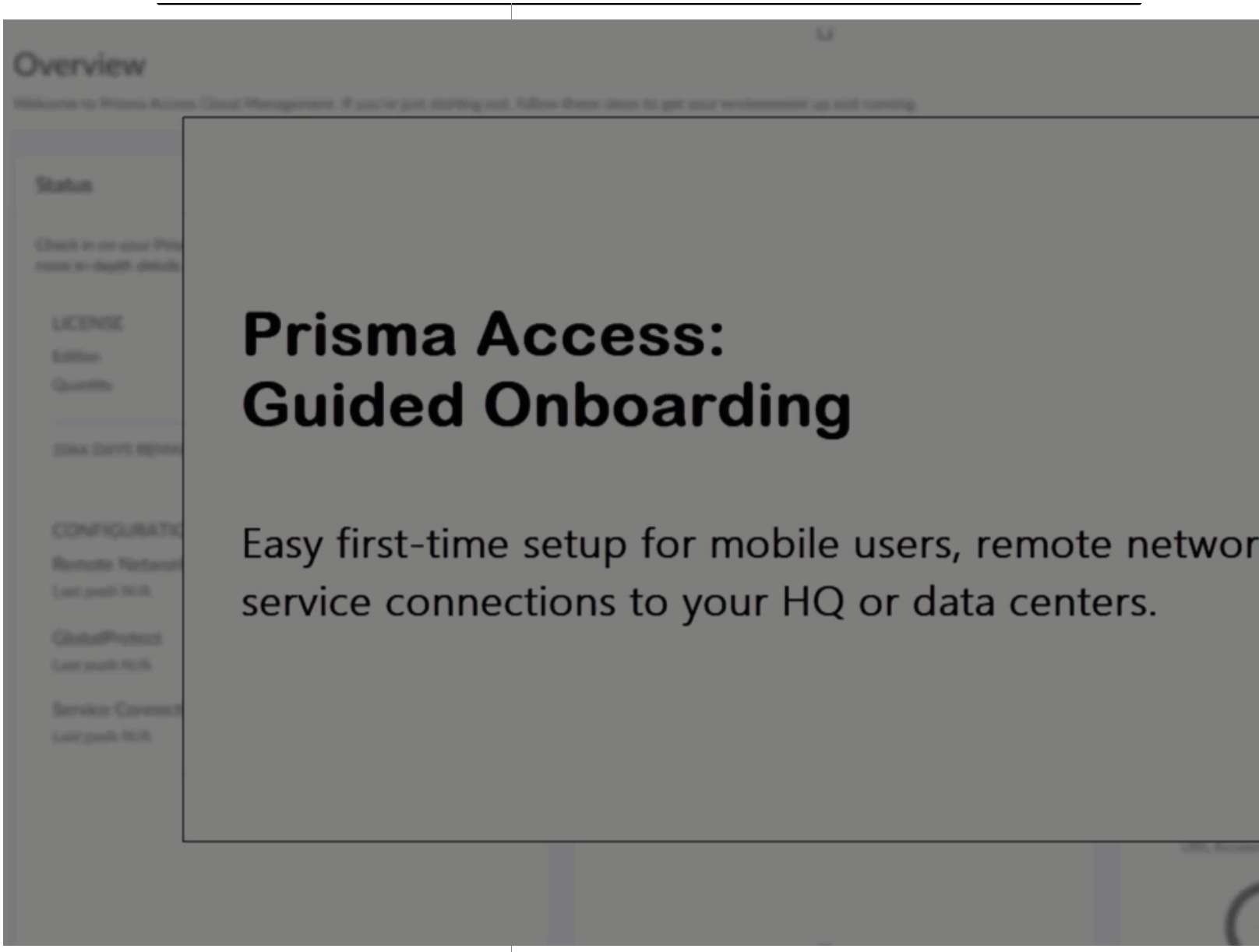


Tutoriales

Algunas tareas pendientes también incluyen tutoriales que le guiarán a través de los pasos básicos necesarios para poner en marcha su entorno.

Los tutoriales de incorporación están disponibles en el panel**Overview (Descripción general)**. Puede hacer clic en la ayuda para ver si hay tutoriales disponibles para la página en la que se encuentra, y estar atento a los tutoriales que puede iniciar directamente en la página:





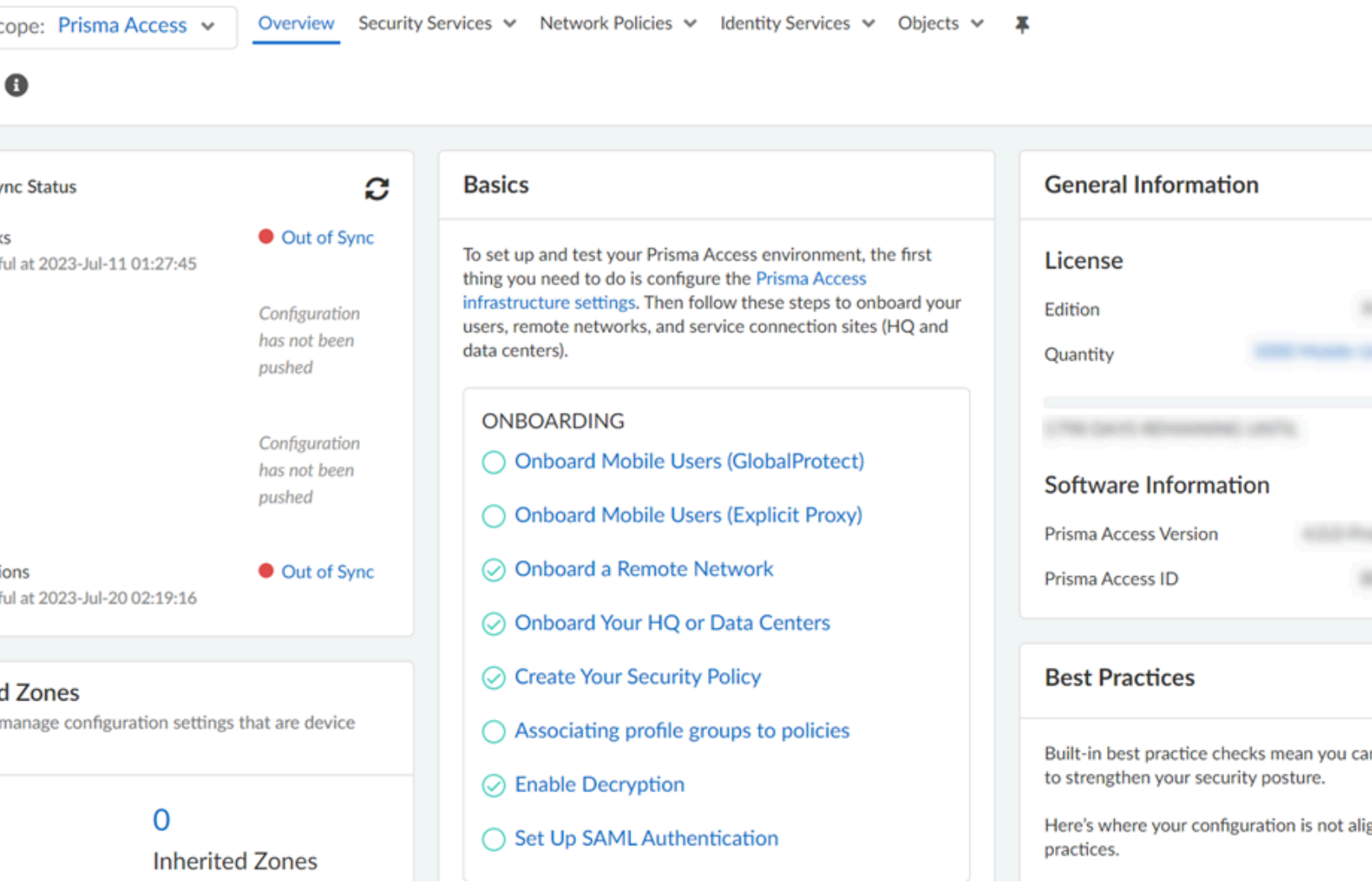
Estado de sincronización de Prisma Access

En la página **Overview (Descripción general)** puede verificar rápidamente el estado de sus configuraciones de Prisma Access. Si ve algo imprevisto, profundice para identificar la configuración afectada. Estos son los estados que puede ver:

- **La configuración no se ha enviado**: por ahora no se ha enviado ninguna configuración a Prisma Access.
- **Esta configuración está vacía**: un usuario envió una configuración en blanco en Prisma Access. En este caso, previamente se había establecido una configuración, por lo que el envío a Prisma Access podría haber sido eliminar la configuración. Vaya a**Push Config (Configuración de envío)** > **Jobs (Tareas)** para revisar los cambios recientes.

- **Desincronizado**: un usuario ha enviado una configuración a Prisma Access, pero hay un error o una advertencia relacionada con el envío. Esto podría ser un problema de configuración o podría ser un problema relacionado con el envío a Prisma Access.
- **En sincronización**: el último envío de configuración a Prisma Access se realizó correctamente y no hay errores.

Si ve algo inesperado, haga clic en el estado para abrir una vista de mapa que muestra las ubicaciones en las que tiene usuarios móviles (GlobalProtect o conexiones proxy explícitas), redes remotas o conexiones de servicio. A continuación, puede identificar la configuración que requiere revisión o en la que es posible que deba realizar una actualización.

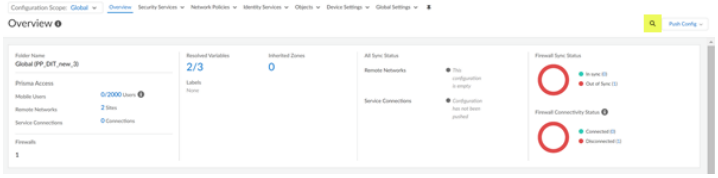


Búsqueda global mediante la Búsqueda de configuración

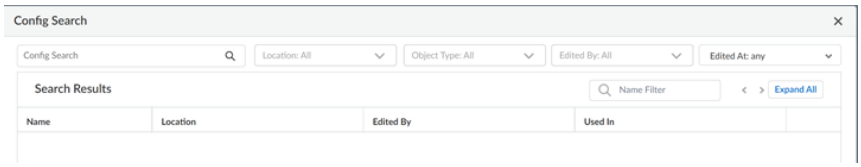
La búsqueda de configuración le permite encontrar objetos de configuración y configuraciones específicos para una cadena en particular, como direcciones IP, nombre de objeto, objetos referenciados, objetos duplicados, nombres de políticas, reglas de políticas, políticas cubiertas para CVE específicos, UUID de reglas, fragmentos predefinidos o nombre de aplicación y obtener la lista de todas las referencias donde se usa el objeto.

1. Para iniciar **Config Search (Búsqueda de configuración)**, haga clic en el icono

   al lado de **Push Config (Configuración de envío)** en la parte superior derecha de la interfaz web. **Config Search (Búsqueda de configuración)** está disponible en todas las páginas en **Manage (Gestionar)**.



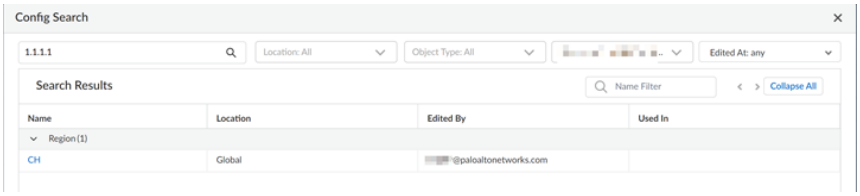
2. En la pantalla **Config Search (Configurar búsqueda)**, puede buscar utilizando los campos **Config String (Configurar cadena)**, **Location (Ubicación)**, **Object Type (Tipo de objeto)**, **Edited By (Editado por)** o **Edited At (Editado en)**.



   Sugerencias de búsqueda:

   - Para encontrar una frase exacta, indíquela entre comillas.
   - Los espacios de los términos de búsqueda se tratan como operaciones AND. Por ejemplo, si busca en política corporativa, los resultados de la búsqueda incluirán casos en los que tanto la palabra política como la palabra corporativa existen en la configuración.
   - Para volver a ejecutar una búsqueda anterior, haga clic en el icono **Config Search (Búsqueda de configuración)**, que muestra las últimas 50 búsquedas. Haga clic en cualquier elemento de la lista para volver a ejecutar dicha búsqueda. La lista del historial de búsqueda es exclusiva para cada cuenta de administrador.
   - La búsqueda de configuración está disponible para cada campo en el que se pueden realizar búsquedas. Por ejemplo, puede buscar una política de seguridad en los siguientes tipos de objetos: Etiquetas, Zona, Dirección, Usuario, Perfil HIP, Aplicación, UUID y Servicio.
   - La ubicación se agrupa por Carpetas y Fragmentos. Puede seleccionar más de una ubicación para buscar. Si no selecciona ninguna ubicación, **All (Todas)** las ubicaciones se seleccionarán de forma predeterminada.
   - Si no se selecciona el tipo de objeto, **All (Todos)** será seleccionado.

3. Los resultados de la búsqueda se categorizan y se proporcionan enlaces a la ubicación de configuración en Strata Cloud Manager, lo que le permite encontrar fácilmente todas las ocurrencias y referencias de la cadena buscada.



Descripción general de la configuración (Strata Cloud Manager)

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)

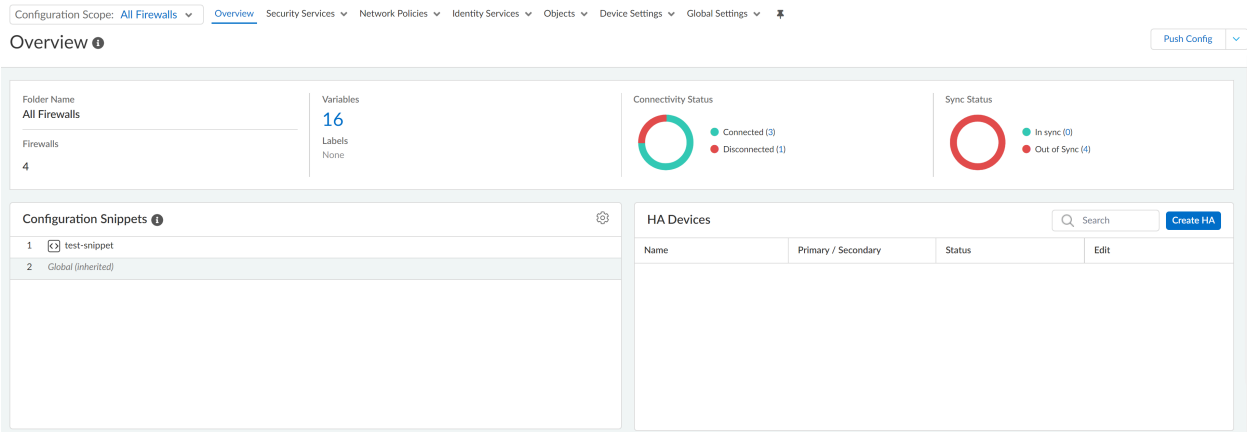
Si recién está empezando con Gestión de la nube de NGFW:

- Así es como funcionan las carpetas de políticas y configuración.
- Aquí le mostramos cómo introducir cambios de configuración en los cortafuegos.

Para la gestión diaria de la configuración:

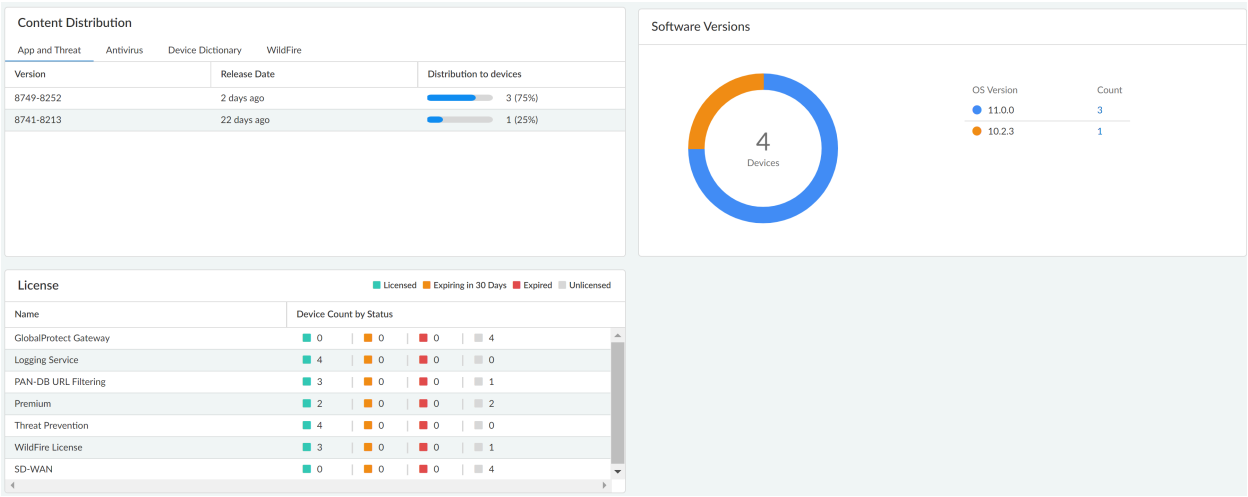
- Obtenga un resumen de un vistazo del nombre de la carpeta actual, el número de cortafuegos agregados a la carpeta, el número de variables creadas para la carpeta.
- Obtenga visibilidad y control sobre las configuraciones de cortafuegos locales sin necesidad de cambiar entre la gestión central y cortafuegos individuales para gestionar configuraciones locales.
  - **Firewalls with config conflicts (Cortafuegos con conflictos de configuración)** muestra el número de cortafuegos con conflictos. Haga clic en el número para ver los conflictos de los cortafuegos junto con sus ubicaciones. Haga clic en cualquier cortafuegos para ver conflictos a nivel de dispositivo.
  - **Objects with config conflicts (Objetos con conflictos de configuración)** muestra el número de conflictos por cortafuegos. Haga clic en el número para ver los objetos en conflicto y sus tipos para un cortafuegos específico. Al hacer clic en el objeto se proporcionan detalles pormenorizados sobre el conflicto.
- Estandarizar una configuración base común para un conjunto de cortafuegos gestionados mediante fragmentos de configuración.
- Configure cortafuegos gestionados en una configuración de alta disponibilidad (HA) para proporcionar redundancia y garantizar la continuidad del negocio.
- Revise el **Connectivity Status (Estado de conectividad)** de cortafuegos gestionados con Strata Cloud Manager.

- Revise el **Sync Status (Estado de sincronización)** de la configuración entre Strata Cloud Manager y la configuración actual en ejecución en los cortafuegos gestionados.



Para obtener más información sobre los cortafuegos gestionados:

- Revise los detalles de **distribución de contenido** y **Software Versions (Versiones de software)** para ver qué actualizaciones de contenido dinámico y versiones de software de PAN-OS se están ejecutando en sus cortafuegos gestionados.
- Revise los detalles de la **License (Licencia)** para ver qué licencias se activan en los cortafuegos gestionados.



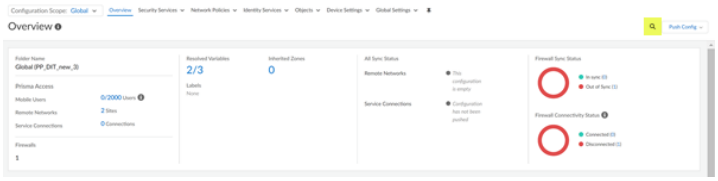
Búsqueda global mediante la Búsqueda de configuración

La búsqueda de configuración le permite buscar objetos de configuración y configuraciones específicos para una cadena en particular, como direcciones IP, nombre de objeto, objetos referenciados, objetos duplicados, nombres de políticas, reglas de políticas, políticas cubiertas para CVE específicos, UUID de reglas, fragmentos predefinidos o nombre de aplicación y obtener la lista de todas las referencias donde se usa el objeto.

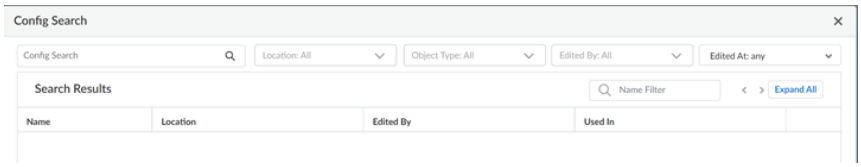
1. Para iniciar **Config Search (Búsqueda de configuración)**, haga clic en el icono

   al lado de **Push Config (Configuración de envío)** en la parte superior derecha de la interfaz web. **Config Search (Búsqueda de configuración)** está disponible en todas las páginas en **Manage (Gestionar)**.

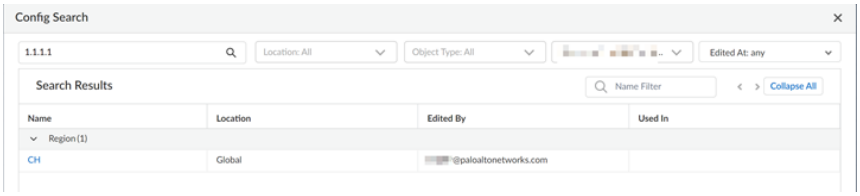
2. En la pantalla **Config Search (Configurar búsqueda)**, puede buscar utilizando los campos **Config String (Configurar cadena)**, **Location (Ubicación)**, **Object Type (Tipo de objeto)**, **Edited By (Editado por)** o **Edited At (Editado en)**.

   Sugerencias de búsqueda:

   - Para encontrar una frase exacta, indíquela entre comillas.
   - Los espacios de los términos de búsqueda se tratan como operaciones AND. Por ejemplo, si busca en política corporativa, los resultados de la búsqueda incluirán casos en los que tanto la palabra política como la palabra corporativa existen en la configuración.
   - Para volver a ejecutar una búsqueda anterior, haga clic en el icono de Búsqueda de configuración, que muestra las últimas 50 búsquedas. Haga clic en cualquier elemento de la lista para volver a ejecutar dicha búsqueda. La lista del historial de búsqueda es exclusiva para cada cuenta de administrador.
   - La búsqueda de configuración está disponible para cada campo en el que se pueden realizar búsquedas. Por ejemplo, puede buscar una política de seguridad en los siguientes tipos de objetos: Etiquetas, Zona, Dirección, Usuario, Perfil HIP, Aplicación, UUID y Servicio.
   - La ubicación está agrupada por carpetas y fragmentos. Puede seleccionar más de una ubicación para buscar. Si no selecciona ninguna ubicación, **All (Todas)** las ubicaciones se seleccionarán de forma predeterminada.
   - Si no se selecciona el tipo de objeto, **All (Todos)** será seleccionado.

3. Los resultados de la búsqueda se categorizan y se proporcionan enlaces a la ubicación de configuración en Strata Cloud Manager, lo que le permite encontrar fácilmente todas las ocurrencias y referencias de la cadena buscada.

Gestionar: Servicios de seguridad

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Gestione sus servicios de seguridad y proteja su red, sistemas y usuarios.

Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Security Services (Servicios de seguridad)**.

Con los servicios de seguridad, puede:

- Defina cómo desea aplicar el tráfico de Prisma Access con Gestionar: Política de seguridad.
- Detenga las amenazas ocultas en el tráfico cifrado con Gestionar: descifrado.

Gestionar: Política de seguridad

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Su Política de seguridad es donde se define cómo se desea aplicar el tráfico en las implementaciones de Prisma Access y NGFW. Todo el tráfico que pasa a través de su entorno de

Strata Cloud Manager se evalúa en función de la política de seguridad y las reglas se aplican de arriba hacia abajo.

Para configurar su política de seguridad, vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Security Services (Servicios de seguridad)** > **Security Policy (Política de seguridad)**.

Introducción a la política de seguridad

Estas son algunas cosas que puede hacer ahora para que la política de seguridad funcione para usted.

- Creación de una regla de política de seguridad: las políticas de seguridad le permiten hacer cumplir reglas y tomar medidas, y pueden ser tan generales o específicas como sea necesario.
- Seguimiento de reglas dentro de una base de reglas: cada regla dentro de una base de reglas se numera automáticamente; al mover o reordenar las reglas, los números cambian en función del nuevo orden.
- Aplicación de las prácticas recomendadas de reglas de política: cuando cree o modifique reglas de las políticas, puede exigir que se introduzcan una descripción, etiquetas, observaciones de auditoría, etc. para garantizar que la base se organiza y se agrupa correctamente, así como para conservar el importante historial de las reglas con fines de auditoría.
- Probar reglas de la política: utilice el Analizador de políticas para comprobar las reglas de la política.
- Activar un perfil de seguridad: se aplica un perfil de seguridad para explorar el tráfico después de que la política de seguridad permita la aplicación o categoría.
- Crear un grupo de perfiles de seguridad: un grupo de perfiles de seguridad es un conjunto de perfiles de seguridad que se pueden tratar como una unidad y luego se pueden añadir fácilmente a las políticas de seguridad.
- Configurar el bloqueo de archivos: Identifique tipos de archivos específicos que desea bloquear o supervisar.
- Crear un perfil de filtrado de datos: evite que la información confidencial salga de su red.
- Gestionar seguridad web: controle el acceso (navegación general) a internet y a las aplicaciones SaaS.

Gestionar: descifrado

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud

¿Dónde puedo usar esto?	¿Qué necesito?
	Manager depende de qué licencia(s) esté usando.

Habilite el descifrado para detener las amenazas ocultas en el tráfico cifrado. Todo lo que tiene que hacer para empezar es importar sus certificados de descifrado: para todo lo demás, hemos incorporado una configuración de prácticas recomendadas que puede utilizar para ponerse en marcha.

Obtenga más información sobre cómo descifrar el tráfico aquí.

Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Security Services (Servicios de seguridad)** > **Decryption (Descifrado)**.

Descripción general del descifrado

Los protocolos de descifrado de Capa de sockets seguros (Secure Sockets Layer, SSL) y Shell seguro (Secure Shell, SSH) aseguran el tráfico entre dos entidades, como un servidor web y un cliente. El SSL y el SSH encapsulan el tráfico y cifran los datos de modo que sean ininteligibles para todas las entidades, excepto para el cliente y el servidor que cuentan con los certificados para garantizar la confianza entre los dispositivos y las claves para decodificar los datos. Descifre el tráfico de SSL y SSH para:

- Evite que el malware camuflado como tráfico cifrado se introduzca en su red. Por ejemplo, un atacante pone en riesgo un sitio web que usa el cifrado SSL. Los empleados visitan ese sitio web y descargan un exploit o malware sin darse cuenta. El malware usa el endpoint del empleado infectado para moverse lateralmente por la red y poner en riego otros sistemas.
- Evite que la información confidencial salga de la red.
- Asegúrese de que las aplicaciones correctas se ejecuten en una red segura.
- Descifre el tráfico de manera selectiva. Por ejemplo, cree una política y un perfil de descifrado para excluir del descifrado el tráfico de los sitios financieros o médicos.

El descifrado de proxy SSH no es compatible con Strata Cloud Manager.

Políticas de descifrado

Strata Cloud Manager proporciona dos tipos de reglas de políticas de descifrado: Proxy SSL de reenvío para controlar el tráfico SSL saliente e Inspección de entrada SSL para controlar el tráfico SSL entrante.

Proxy SSL de reenvío

Cuando configura el cortafuegos para descifrar tráfico SSL que se dirige a sitios externos, funciona como un proxy SSL de reenvío. Utilice una política de descifrado del proxy SSL de reenvío para descifrar y examinar el tráfico SSL/TLS de usuarios internos a Internet. El descifrado de proxy SSL de reenvío evita que el malware oculto como tráfico cifrado SSL entre en su red corporativa mediante el descifrado del tráfico, de modo que el cortafuegos pueda aplicar perfiles de descifrado y perfiles y políticas de seguridad en el tráfico.

Inspección de entrada SSL

Use la Inspección de entrada SSL para descifrar y examinar el tráfico SSL/TLS entrante de un cliente a un servidor de red objetivo (cualquier servidor para el que tenga el certificado y pueda importarlo en el cortafuegos) y bloquee las sesiones sospechosas. Por ejemplo, supongamos que un actor malintencionado quiere explotar una vulnerabilidad conocida en su servidor web. El descifrado SSL/TLS entrante proporciona visibilidad del tráfico, lo que permite que el cortafuegos responda a la amenaza de forma proactiva.

Perfiles de descifrado

Puede adjuntar un perfil de descifrado a una regla de política para aplicar la configuración de acceso detallada al tráfico, como comprobaciones para los certificados de servidores, modos no compatibles y fallos.

Perfiles de proxy SSL de reenvío

El perfil de descifrado de proxy de reenvío SSL controla la verificación del servidor, las comprobaciones de modo de sesión y las comprobaciones de errores para el tráfico SSL/TLS saliente definido en las políticas de descifrado de proxy de reenvío al que se adjunta el perfil.

Perfiles de inspección de entrada SSL

El perfil de descifrado de inspección de entrada SSL controla las comprobaciones de modo de sesión y las comprobaciones de errores para el tráfico SSL/TLS entrante definido en las políticas de descifrado de inspección de entrada a las que se adjunta el perfil.

Perfil para configuración sin cifrado

Los perfiles de descifrado realizan comprobaciones de verificación del servidor para el tráfico que usted decide no descifrar. Adjunte un perfil de configuración sin cifrado a una política de descifrado que defina el tráfico que se excluirá del descifrado. (No utilice la política para excluir el tráfico que no pueda descifrar porque un sitio rompa el descifrado por motivos técnicos como un certificado fijado o una autenticación mutua. En cambio, añada el nombre de host a la Lista de exclusión de descifrado).

Sugerencias de descifrado

- **Utilice las reglas de políticas de prácticas recomendadas como punto de partida para crear su política de descifrado**

  Estas reglas (una que descifra el tráfico y otra que excluye el contenido confidencial del descifrado) se crean basándose en categorías de URL.

- **Excluya contenido confidencial del descifrado**

  Excluya el contenido confidencial del descifrado por motivos comerciales, legales o normativos.

  - Exclusiones de descifrado predefinidas: Palo Alto Networks mantiene esta lista de exclusiones y la actualiza periódicamente. Esta lista se aplica globalmente y de forma

predeterminada a todo el tráfico que especifique para el descifrado. Puede deshabilitar las entradas de la lista si eso se ajusta a las necesidades de su negocio.

- Exclusiones personalizadas: excluya globalmente sitios o aplicaciones del descifrado.
- Exclusiones basadas en políticas: utilice categorías de URL y listas dinámicas externas para crear reglas de descifrado específicas y basadas en políticas. Establezca una acción de regla de políticas de descifrado en **no-decrypt** para excluir el tráfico coincidente del descifrado.

Coloque siempre las exclusiones de descifrado en la parte superior de las reglas de su política, para que se apliquen primero.

- **Tenga en cuenta que puede aplicar algunas configuraciones de descifrado globalmente y dirigir otras a ubicaciones específicas**
  - La política de descifrado de su Strata Cloud Manager se aplica globalmente a todos los NGFW y ubicaciones de Prisma Access.

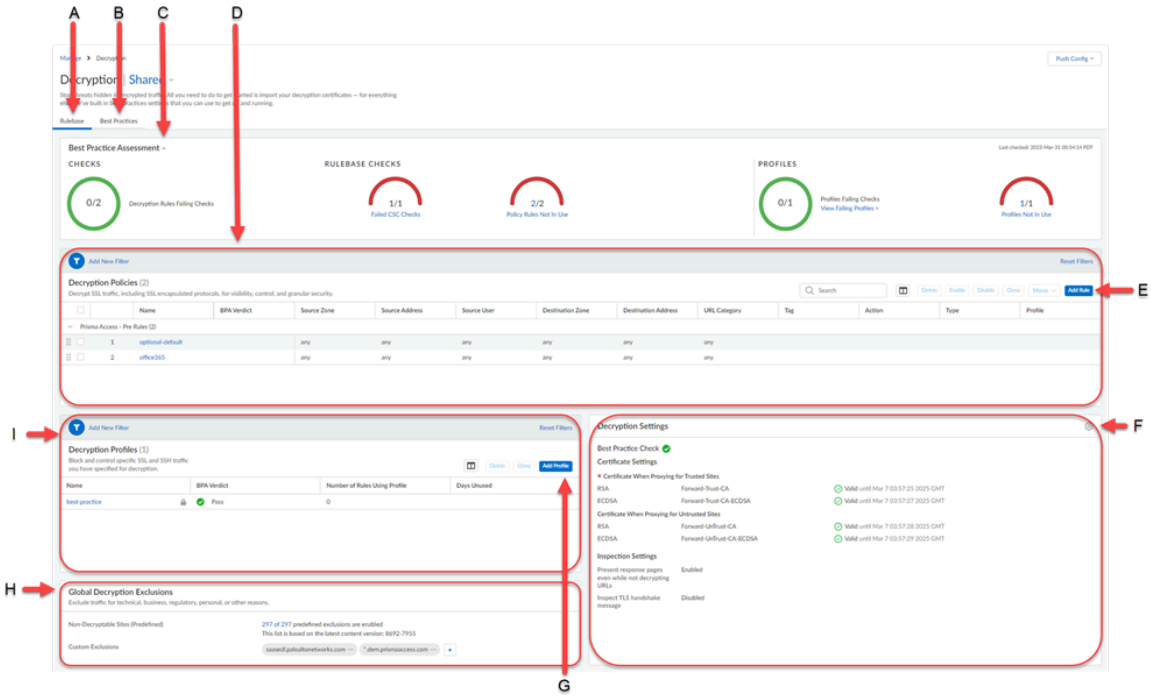
    Gestionar > **Configuración** > **NGFW y Prisma Access** > **Servicios de seguridad** > **descifrado**
  - Vaya a la política de descifrado de cada tipo para crear reglas de políticas destinadas a cortafuegos específicos, ubicaciones de usuarios móviles, sitios de red remotos o conexiones de servicio

    Gestionar > **Configuración** > **NGFW y Prisma Access** > **Alcance de la configuración** > **Global / Cortafuegos / Usuarios móviles / Redes remotas / Conexiones de servicio**
- **El orden de las reglas es importante**

  Las reglas de la política de descifrado se aplican de arriba hacia abajo. Coloque las reglas que desea aplicar primero en la parte superior de la lista de reglas de política de descifrado. Las reglas globales (reglas previas) se aplican primero y siempre se enumeran antes de las reglas específicas de los usuarios móviles, las redes remotas y las conexiones de servicio.

Descifrado de un vistazo

La pantalla de descifrado es el lugar para configurar las políticas y los perfiles de descifrado y ver las Evaluaciones de prácticas recomendadas.



A) Base de reglas: las comprobaciones de la base de reglas analizan cómo se organiza y gestiona la política de seguridad, incluidos los ajustes de configuración que se aplican a muchas reglas.

B) Prácticas recomendadas: aquí puede obtener una vista completa de cómo la implementación de la función se alinea con las prácticas recomendadas. Examine los controles que han fallado para ver dónde puede realizar mejoras (también puede revisar los controles aprobados).

C) Evaluación de las prácticas recomendadas: las puntuaciones de las prácticas recomendadas se muestran en el panel de descifrado. Estas puntuaciones le dan una visión rápida de su progreso con las prácticas recomendadas. De un vistazo, puede identificar las áreas que requieren una investigación más profunda o en las que desea tomar medidas para mejorar su posición de seguridad.

d) Políticas de descifrado: lista de políticas de descifrado incorporadas. Revise la configuración de la políticas, el tipo de políticas (*Proxy de reenvío SSL*, *Inspección de entrada SSL*o *SSH Proxy*), la acción de política (*descifrar* o *no descifrar*), y el veredicto de BPA.

E) Añadir regla: añada y configure nuevas políticas de descifrado.

f) Configuración de descifrado: certificado de acceso y configuración de descifrado. Importe y exporte certificados.

g) Añadir perfil: añada y configure nuevos perfiles de descifrado.

h) Exclusiones de descifrado global: aplicaciones excluidas del descifrado.

i) Perfiles de descifrado: lista de perfiles de descifrado incorporados. Revise la configuración del perfil, las políticas que usan el perfil y el veredicto de la BPA.

Gestionar: Políticas de red

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Puede crear varios tipos de políticas de red para proteger su red de amenazas e interrupciones. Le ayuda a optimizar la asignación de recursos de red y a gestionar sus políticas de red para priorizar el tráfico y configurar las clasificaciones de aplicaciones.

Las reglas se evalúan de arriba abajo y cuando el tráfico coincide con los criterios de reglas definidos, no se evalúan las reglas posteriores. Deberá ordenar reglas de política más específicas por encima de las más genéricas para hacer cumplir los mejores criterios de coincidencia posibles. Se genera un registro para el tráfico que coincide con una regla de políticas cuando el registro está habilitado para la regla. Las opciones de registro son configurables para cada regla.

Las reglas de políticas de prácticas recomendadas están disponibles para la mayoría de los tipos de políticas y le ayudan a comenzar de forma rápida y segura. Si bien estas reglas no se pueden editar para garantizar que siempre tenga un nivel mínimo de seguridad disponible, puede duplicarlas si desea usarlas como base para personalizar su políticas.

Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Network Policies (Políticas de red)**.

Con las políticas de red, puede:

- Priorice el tráfico que más importa a sus operaciones con Gestionar: QoS.
- Gestione cómo Prisma Access clasifica sus aplicaciones con Gestionar: Cancelación de aplicación.

Gestionar: QoS

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	Uno de estos: ❑ Licencia de Prisma Access ❑ Strata Cloud Manager Pro

¿Dónde puedo usar esto?	¿Qué necesito?
	→ Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Con Calidad de servicio (QoS), puede priorizar el tráfico crítico del negocio y las aplicaciones que requieren baja latencia (como VoIP y aplicaciones de vídeo). Para añadir o editar una regla de políticas de QoS, vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Network Policies (Políticas de red)** > **QoS**.

Reglas de políticas QoS

Reglas de política de Calidad de servicio (QoS) para identificar el tráfico que requiere un trato preferencial o limitación de ancho de banda. Las reglas de QoS le permiten ejecutar aplicaciones y tráfico de alta prioridad de forma fiable bajo una capacidad de red limitada. Puede configurar el tratamiento de QoS de tráfico utilizando los puntos de código de servicios diferenciados (DSCP). Estos puntos de código son valores de encabezado de paquete que se pueden utilizar para solicitar (por ejemplo) entrega de alta prioridad o mejor esfuerzo para el tráfico. Prisma Access impone valores DSCP para el tráfico entrante y marca una sesión con un valor DSCP a medida que el tráfico de sesión sale del cortafuegos. Esto significa que todo el tráfico entrante y saliente de una sesión está recibiendo un tratamiento continuo de QoS. Puede configurar el tratamiento de QoS de tráfico mediante los siguientes puntos de código:

- **Expedited Forwarding (EF)**: se usa para solicitar pérdida baja, latencia baja y ancho de banda garantizado para el tráfico.

  Los paquetes con valores de puntos de código EF suelen tener garantizado el envío de máxima prioridad.
- **Assured Forwarding (AF)**: se puede usar para ofrecer entregas fiables a las aplicaciones.

  Los paquetes con puntos de código AF indican una solicitud para que el tráfico reciba un tratamiento de prioridad más alta que el que proporciona el servicio de mejor esfuerzo. Los paquetes con punto de código EF tienen prioridad sobre los paquetes con punto de código AF.
- **Selector de clase (CS)**: se puede usar para ofrecer compatibilidad con dispositivos de red más antiguos que usan el campo Prioridad de IP para marcar el tráfico prioritario.
- **Precedencia de IP (ToS)**: las direcciones IP de red heredadas las utilizan para marcar el tráfico prioritario.
- **Punto de código personalizado**: cree un punto de código personalizado para que coincida con el tráfico introduciendo un Nombre de punto de código y un Valor binario.

  Por ejemplo, puede crear una regla de políticas de QoS para priorizar las comunicaciones de voz, como la voz sobre IP (VOIP), para garantizar una transmisión coherente de paquetes. Esto garantiza que la comunicación de voz sea coherente.

Gestionar: Cancelación de aplicación

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Cree una política de anulación de aplicaciones para designar aplicaciones que se procesarán mediante la inspección de Capa 4 de ruta rápida, en lugar de utilizar la inspección de App-ID para Capa 7. Esto obliga al nodo de aplicación de seguridad a gestionar la sesión como una inspección de estado regular y ahorra tiempos de procesamiento de aplicaciones. Puede crear una regla de políticas de anulación de aplicaciones cuando no desee inspeccionar el tráfico para aplicaciones personalizadas entre direcciones IP conocidas. Por ejemplo, si tiene una aplicación personalizada en un puerto no estándar que sabe que los usuarios que acceden a la aplicación están autorizados y ambos están en la zona de confianza, puede anular los requisitos de inspección de la aplicación para los usuarios de confianza que acceden a la aplicación personalizada.

Para cambiar la forma en que Prisma Access clasifica las aplicaciones, vaya a **Manage (Gestionar)** > **Configuration (configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Network Policies (Políticas de red)** > **Application Override (Cancelación de aplicación)** y, a continuación, cree la regla de políticas de anulación de aplicaciones.

Sugerencias de anulación de aplicaciones

Tenga en cuenta que cuando crea una regla de políticas de anulación de aplicación, está impidiendo que App-ID clasifique el tráfico de su implementación y realice una inspección de amenazas basada en esa identificación de aplicación. Para admitir aplicaciones propietarias internas, vale la pena pensar en crear una aplicación personalizada (en lugar de una regla de anulación de aplicación) que incluya la firma de la aplicación para que Strata Cloud Manager realice la inspección de Capa 7 y analice el tráfico de la aplicación en busca de amenazas. Para crear una aplicación personalizada, vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Objects (Objetos)** > **Applications (aplicaciones)**.

Políticas de anulación de aplicaciones

Utilice las siguientes secciones para configurar una regla de anulación de aplicaciones.

- **Origen**
  - **Zonas**—**Añadir** zonas de origen.
  - **Direcciones**—**Añadir** direcciones de origen, grupos de direcciones o regiones y especifique la configuración.
- **Destino**
  - **Zonas**—**Añadir** para elegir zonas de destino.
  - **Direcciones**—**Añadir** direcciones de origen, grupos de direcciones o regiones y especifique la configuración.
- **Aplicación**
  - **Aplicación**—Seleccionar la aplicación de anulación de los flujos de tráfico que coincidan con los criterios de la regla anterior. Cuando se antepone una aplicación personalizada, no se realizará una inspección de amenazas. La excepción es si anula y se va a una aplicación predefinida que admite la inspección de amenazas.

    Para definir nuevas aplicaciones, vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Objects (Objetos)** > **Applications (Aplicaciones)**.
- **Protocolo**
  - **Protocolo**—Seleccionar el protocolo (**TCP** o **UDP**) para el cual permitir una anulación de la aplicación.
  - **Puerto**—Introduzca el número de puerto (0 a 65535) o el intervalo de números de puerto (puerto1-puerto2) de las direcciones de destino especificadas. Si especifica varios puertos o intervalos, deben estar separados por comas.

Gestionar: Reenvío basado en políticas

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Las reglas de reenvío basadas en políticas permiten al tráfico tomar una ruta alternativa desde el siguiente salto especificado en la tabla de enrutamiento, y se suelen usar para especificar una interfaz de salida por razones de seguridad o rendimiento.

Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Network Policies (Políticas de red)** > **Policy Based Forwarding (Reenvío basado en políticas)**.

Utilice una regla de reenvío basado en políticas para dirigir el tráfico a una interfaz de salida específica y anular la ruta predeterminada para el tráfico. Antes de crear una regla de Reenvío basado en políticas, asegúrese de comprender que el conjunto de direcciones IPv4 se trata como un subconjunto del conjunto de direcciones IPv6.

Utilice las siguientes secciones para configurar una regla de reenvío basada en políticas:

- **Origen**
  - **Zonas**—**Añadir** zonas de origen.
  - **Interfaz: añadir** interfaces de origen

    .
  - **Direcciones**:**añadir** direcciones de origen, grupos de direcciones o regiones y especifique la configuración.
  - **Usuarios**: **Añadir** los usuarios y grupos de usuarios a los que se aplica la política.
- **Destino**
  - **Direcciones**: **Añadir** direcciones, grupos de direcciones o regiones de origen y especificar la configuración.
- **Aplicación y servicios**
  - **Entidades de aplicaciones**: seleccione las aplicaciones que desea enrutar a través de rutas alternativas.

    Una regla de reenvío basada en políticas se puede aplicar antes de que el cortafuegos tenga suficiente información para determinar la aplicación. Por lo tanto, no se recomienda usar las reglas específicas de aplicación con el Reenvío basado en políticas. Siempre que sea posible, utilice un objeto de servicio.

    No puede utilizar aplicaciones personalizadas, filtros de aplicaciones o grupos de aplicaciones en las reglas de Reenvío basado en políticas.
  - **Entidades de servicio**: seleccione los servicios y grupos de servicios que desea enrutar a través de rutas alternativas

    .

- **Reenvío**
  - **Acción**: puede establecer la acción que debe realizar al hacer coincidir un paquete eligiendo entre:
    - **Reenviar**: dirige el paquete a la interfaz especificada en **Interfaz de salida**.
    - **Descartar**: descarta el paquete.
    - **Sin PBF**: excluye los paquetes que coinciden con los criterios de origen, destino, aplicación o servicio definidos en la regla. Los paquetes coincidentes utilizan la tabla de rutas en lugar de PBF.
  - **Interfaz de salida**: seleccione la información de red a la que desea reenviar el tráfico que coincida con su regla de reenvío basado en políticas.
  - **Siguiente salto**
    - **Dirección IP**: introduzca una dirección IP o seleccione un objeto de dirección del tipo máscara de red IP al que reenviar los paquetes coincidentes.
    - **FQDN**: introduzca un FQDN (o bien seleccione o cree un objeto de dirección del tipo FQDN) al que reenviar los paquetes coincidentes.
    - **Ninguno**: significa que se usa la dirección IP de destino del paquete como siguiente salto. El reenvío falla si la dirección IP de destino no está en la misma subred que la interfaz de salida.
  - **Supervisar**: habilite la supervisión para verificar la conectividad a una dirección IP de destino o, si no se especifica ninguna, a la dirección IP de Siguiente salto.

Gestionar: NAT

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

El NAT le permite traducir la direcciones IPv4 privadas y no enrutables a una o más direcciones IPv4 globalmente enrutables, con lo cual se conservan las direcciones IP enrutables de la organización. El NAT también le permite no tener que divulgar las direcciones IP reales de los hosts que deben acceder a direcciones públicas y gestionar el tráfico al realizar el reenvío de puertos. Puede usar NAT para resolver dificultades de diseño de la red y permitir que las redes con subredes IP idénticas se comuniquen entre sí.

Puede configurar una regla de políticas NAT que coincida con una zona de origen del paquete y una zona de destino, como mínimo. Además de las zonas, puede configurar criterios equivalentes basados en la interfaz de destino del paquete, la dirección de origen y destino y servicio. Puede configurar múltiples reglas NAT.

Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Network Services (Servicios de red)** > **NAT**.

Troubleshoot (Resolver) *problemas de conectividad: obtenga una vista agregada de sus estados de enrutamiento y túnel, y explique los detalles para encontrar anomalías y configuraciones problemáticas.*

Gestionar: SD-WAN

¿Dónde puedo usar esto?	¿Qué necesito?
• SD-WAN	❑ Licencia SD-WAN

Una regla de políticas de SD-WAN especifica las aplicaciones o servicios y un perfil de distribución de tráfico para determinar cómo el cortafuegos selecciona la ruta preferida para un paquete entrante que no pertenece a una sesión existente y que coincide con todos los demás criterios, como las zonas de origen y destino, las direcciones IP de origen y destino y el usuario de origen. La regla de políticas de SD-WAN también especifica un perfil de calidad de ruta de umbrales para latencia, fluctuación de fase y pérdida de paquetes. Cuando se excede uno de los umbrales, el cortafuegos selecciona una nueva ruta para las aplicaciones o servicios.

Para configurar una política SD-WAN, seleccione**Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Network Policies (Políticas de red)** > **SD-WAN**.

Reglas

Puede definir las reglas previas o posteriores en un contexto compartido como políticas compartidas para todos los cortafuegos gestionados o, en un grupo de dispositivos, como específicas para un grupo de dispositivos concreto.

- **Reglas previas**: reglas añadidas a la parte superior del orden de las reglas y que se evalúan en primer lugar. Puede utilizar las reglas previas para aplicar la política de uso aceptable de una organización. Por ejemplo, puede bloquear el acceso a categorías URL concretas o permitir el tráfico DNS para todos los usuarios.
- **Reglas posteriores**: reglas que se añaden al final del orden de reglas y que se evalúan después de las reglas previas y de las reglas definidas localmente en el cortafuegos. Las reglas posteriores suelen incluir reglas para impedir el acceso al tráfico basado en **App-ID™**, **User-ID™** o **Servicio**.

Perfiles

Cree perfiles que aplicar a conjuntos de aplicaciones y servicios especificados en las reglas de políticas de SD-WAN.

Calidad del camino

SD-WAN le permite crear un perfil de calidad de ruta para cada conjunto de aplicaciones, filtros de aplicaciones, grupos de aplicaciones, servicios, objetos de servicio y objetos de grupo de servicios que tienen requisitos de calidad de red únicos y, después, hacer referencia a ese perfil en una regla de políticas de SD-WAN. En el perfil, establezca umbrales máximos para tres parámetros: latencia, jitter y pérdida de paquetes. Cuando un enlace de SD-WAN exceda cualquiera de los umbrales, el cortafuegos seleccionará una nueva mejor ruta para los paquetes que coincidan con la regla de SD-WAN donde aplique este perfil.

Calidad SaaS

SD-WAN le permite crear perfiles de calidad de software como servicio (SaaS, Software-as-a-Service) para medir la calidad del estado de la ruta entre el cortafuegos de la central o de la sucursal y las aplicaciones SaaS del lado del servidor para supervisar con precisión la fiabilidad de la aplicación SaaS e intercambiar rutas si la calidad de la ruta disminuye. Esto permite que el cortafuegos determine con precisión cuándo realizar la conmutación por error a un enlace de acceso directo a Internet (DIA, Direct Internet Access) diferente.

El perfil de calidad de SaaS le permite especificar la aplicación SaaS que supervisar mediante un algoritmo de aprendizaje adaptativo que supervisa la actividad de la aplicación, o mediante la especificación de una aplicación SaaS mediante la dirección IP de la aplicación, FQDN o URL.

Distribución de tráfico

Para este perfil de distribución de tráfico, seleccione el método que usa el cortafuegos para distribuir sesiones y conmutar por error a una mejor ruta cuando la calidad de la ruta se deteriora. Añada las etiquetas de enlace que considera el cortafuegos al determinar el enlace por el que reenvía el tráfico de SD-WAN. Aplique un perfil de distribución de tráfico a cada regla de política de SD-WAN que cree.

Corrección de errores

Si su tráfico SD-WAN incluye una aplicación que es sensible a la pérdida o daño de paquetes, como audio, VoIP o videoconferencia, puede aplicar la corrección de errores de reenvío (FEC, Forward Error Correction) o la duplicación de paquetes como medio de corrección de errores. Con FEC, el cortafuegos receptor (descodificador) puede recuperar paquetes perdidos o dañados mediante bits de paridad que el codificador incrusta en un flujo de aplicación. La duplicación de paquetes es un método alternativo de corrección de errores, en el que una sesión de aplicación se duplica de un túnel a un segundo túnel. Para emplear uno de estos métodos, cree un perfil de corrección de errores y haga referencia a él en una regla de política de SD-WAN para aplicaciones específicas.

(También debe especificar qué interfaces están disponibles para que el cortafuegos seleccione para la corrección de errores indicando en un perfil de interfaz SD-WAN que las interfaces son elegibles para la selección de la interfaz del perfil de corrección de errores).

Interfaz de SD-WAN

Cree un perfil de interfaz de SD-WAN para definir las características de las conexiones ISP y para especificar la velocidad de los enlaces y con qué frecuencia el cortafuegos supervisa el enlace, y especifique una etiqueta de enlace para el enlace. Cuando especifique la misma etiqueta de enlace en varios enlaces, agrupa (empaqueta) esos enlaces físicos en un paquete de enlaces o una tubería gruesa. Debe configurar un perfil de interfaz de SD-WAN y especificarlo para una interfaz Ethernet compatible con SD-WAN para poder guardar la interfaz Ethernet.

Etiquetas de enlace

Cree una etiqueta de enlace para identificar uno o más enlaces físicos que desee que las aplicaciones y servicios utilicen en un orden específico durante la distribución del tráfico de SD-WAN y la protección contra conmutación por error. La agrupación de varios enlaces físicos le permite maximizar la calidad de la aplicación y el servicio si el estado del enlace físico se deteriora.

Cuando planifique cómo agrupar sus enlaces, considere el uso o el fin de los enlaces y agrúpelos en consecuencia. Por ejemplo, si está configurando enlaces destinados a tráfico de bajo coste o no crítico para la empresa, cree una etiqueta de enlace y agrupe estas interfaces para garantizar que el tráfico previsto fluya principalmente en esos enlaces y no en enlaces más caros que puedan impactar en aplicaciones o servicios críticos para la empresa.

Gestionar: Servicios de identidad

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Aprenda a gestionar sus servicios de identidad y confirme que solo ciertos usuarios puedan acceder a los datos correctos en su red.

Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Identity Services (Servicios de identidad)**.

Con los servicios de identidad, usted puede:

- Permita que solo usuarios legítimos accedan a su red conectando Prisma Access a su proveedor de identidad (IdP) y eligiendo el método de autenticación que desea utilizar. Gestionar: Autenticación.
- Otorgue a Prisma Access acceso de solo lectura a su información de Active Directory con el Gestionar: Motor de identidad en la nube.
- Aplique su política de seguridad de manera coherente y comparta datos de identidad con dispositivos locales en sitios de red remotos o sitios de conexión de servicio (sede central y centros de datos) con Gestionar: Redistribución de identidades.

Gestionar: Autenticación

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro

¿Dónde puedo usar esto?	¿Qué necesito?
	→ Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Para garantizar que solo los usuarios legítimos tengan acceso a sus recursos más protegidos, Prisma Access admite varios tipos de autenticación, incluida la compatibilidad con SAML, TACACS +, RADIUS, LDAP, Kerberos, MFA, autenticación de bases de datos locales y SSO.

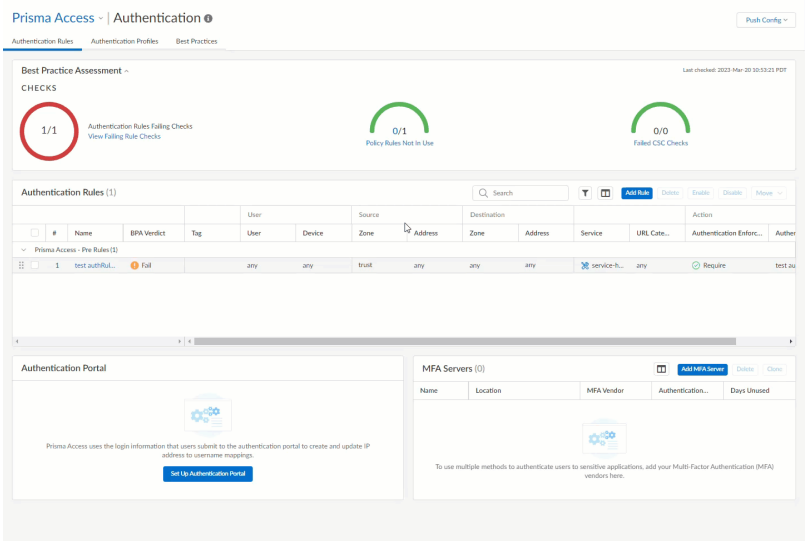
Para configurar las políticas de autenticación, vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Identity Services (Servicios de identidad)** > **Authentication (Autenticación)**.

Estos son los servicios con los que se integra Prisma Access para proporcionar autenticación, y las características a tener en cuenta cuando está planificando la configuración de su autenticación:

Soporte de autenticación

SAML	Si sus usuarios acceden a los servicios y aplicaciones externos a su red, puede utilizar SAML para integrar Prisma Access con un proveedor de identidad (IdP) que controla el acceso a los servicios y aplicaciones externos e internos. El inicio de sesión único (SSO) de SAML permite un inicio de sesión para acceder a varias aplicaciones y es útil en entornos donde cada usuario accede a varias aplicaciones y la autenticación de cada uno impediría la producción de usuario. En este caso, el inicio de sesión único (SSO) de SAML permite que un inicio de sesión acceda a varias aplicaciones. De igual modo, el cierre de sesión único (single logout, SLO) de SAML le permite a un usuario finalizar sesiones de varias aplicaciones cerrando la sesión de una sola sesión. SSO funciona para usuarios móviles que acceden a aplicaciones a través de la aplicación GlobalProtect o usuarios en redes remotas que acceden a aplicaciones a través del Portal de autenticación. SLO está disponible para los usuarios de la aplicación GlobalProtect. *No puede utilizar los perfiles de autenticación de SAML en las secuencias de autenticación.*
TACACS+	El sistema de control de acceso del controlador de acceso a terminales (Terminal Access Controller Access-Control System Plus, TACACS+) es una familia de protocolos que permiten la autenticación y la autorización mediante un servidor centralizado. TACACS+ cifra nombres de usuario y contraseñas, lo que lo convierte en una opción más segura que RADIUS, que solo cifra contraseñas. TACACS+ es más fiable dado que utiliza TCP, mientras que RADIUS utiliza UDP.

RADIUS	El servicio de autenticación remota telefónica de usuario (RADIUS) es un protocolo de red ampliamente admitido que brinda autenticación y autorización centralizadas. También puede añadir un servidor RADIUS a Prisma Access para implementar la autenticación multifactor.
LDAP:	El protocolo ligero de acceso a directorios (LDAP) es un protocolo estándar para acceder a directorios de información. Puede utilizar LDAP para autenticar a los usuarios que accedan a aplicaciones o servicios a través del Portal de autenticación.
Kerberos	Kerberos es un protocolo de autenticación que permite un intercambio seguro de información entre las partes utilizando claves únicas (denominadas vales) para identificar a las partes. Con Kerberos, puede autenticar a los usuarios que acceden a las aplicaciones a través del Portal de autenticación. Si el SSO de Kerberos está habilitado, el usuario solo debe iniciar sesión durante el acceso inicial a su red (como iniciar sesión en Microsoft Windows). Tras este inicio de sesión inicial, el usuario podrá acceder a cualquier servicio basado en el explorador de la red sin tener que iniciar sesión de nuevo hasta que venza la sesión con SSO. Para usar Kerberos, primero necesita una cuenta de Kerberos para Prisma Access que autenticará a los usuarios. Se requiere una cuenta para crear un keytab de Kerberos, que es un archivo que contiene el nombre principal y una contraseña con hash del cortafuegos o Panorama. El proceso de SSO requiere un keytab. El SSO de Kerberos se encuentra disponible solo para los servicios y las aplicaciones internas de su entorno de Kerberos. Para habilitar el SSO para los servicios y las aplicaciones externas, utilice SAML.
Motor de identidad en la nube	Cloud Identity Engine (CIE) proporciona tanto identificación de usuario como autenticación de usuario para usuarios móviles en una implementación de Prisma Access-Proxy explicito. Cloud Identity Engine se integra con el Servicio de caché de la autenticación (ACS) de proxy explícito y utiliza proveedores de identidad SAML (IdP) para proporcionar autenticación a los usuarios móviles del proxy explícito.
MFA	La autenticación multifactor (MFA) le ofrece una forma de implementar múltiples desafíos de autenticación de diferentes tipos (estos se llaman *factores*) para proteger sus servicios y aplicaciones más sensibles. Por ejemplo, es posible que desee una autenticación más sólida para los documentos financieros clave que para los motores de búsqueda.

	Prisma Access tiene una lista integrada de proveedores de MFA compatibles que se actualiza automáticamente a medida que se añaden nuevos proveedores: 
Autenticación de base de datos local	Cree una base de datos que se ejecute localmente en Prisma Access y contenga cuentas de usuario (nombres de usuario y contraseñas o contraseñas hash). Este tipo de autenticación es útil para la creación de cuentas de usuario que reutilizan las credenciales de las cuentas Unix existentes en casos donde solo conoce las contraseñas con hash, no las contraseñas en texto normal. En el caso de las cuentas que utilizan contraseñas en texto normal, también puede realizar el paso Defina la complejidad de la contraseña y la configuración del vencimiento. Este método de autenticación está disponible para los usuarios que acceden a servicios y aplicaciones a través del Portal de autenticación o la aplicación GlobalProtect.

Aspectos destacados de la característica de autenticación

SSO	Si utiliza SAML o Kerberos, puede implementar el inicio de sesión único (SSO), que permite a los usuarios autenticarse solo una vez para acceder a varios servicios y aplicaciones. SAML y Kerberos admiten el SSO.
Portal de autenticación	Redirige las solicitudes web que coincidan con una regla de autenticación a una página de inicio de sesión de Prisma Access donde se les solicita la autentificación. Prisma Access utiliza la información que el usuario envía a este portal de autenticación para crear o actualizar la dirección IP a las asignaciones de nombres de usuario.

	Esto es especialmente útil para las redes remotas, de modo que continúe supervisando y haciendo cumplir el tráfico basado en un usuario (o grupo). Cuando un usuario inicia un tráfico web (HTTP o HTTPS) que coincide con una regla de autenticación, Prisma Access solicita al usuario que se autentique con el portal de autenticación. Prisma Access crea o actualiza la dirección IP a la asignación de nombres de usuario en función de la información que el usuario envía al portal. Esto garantiza que conozca exactamente quién accede a sus aplicaciones y datos más delicados desde un sitio de red remoto.
Secuencia de autenticación	Si utiliza varios tipos de autenticación para diferentes propósitos, puede establecer una secuencia de autenticación para clasificar sus perfiles. Prisma Access verifica cada perfil en función de su clasificación hasta que uno autentique con éxito al usuario.

Cómo funciona la autenticación

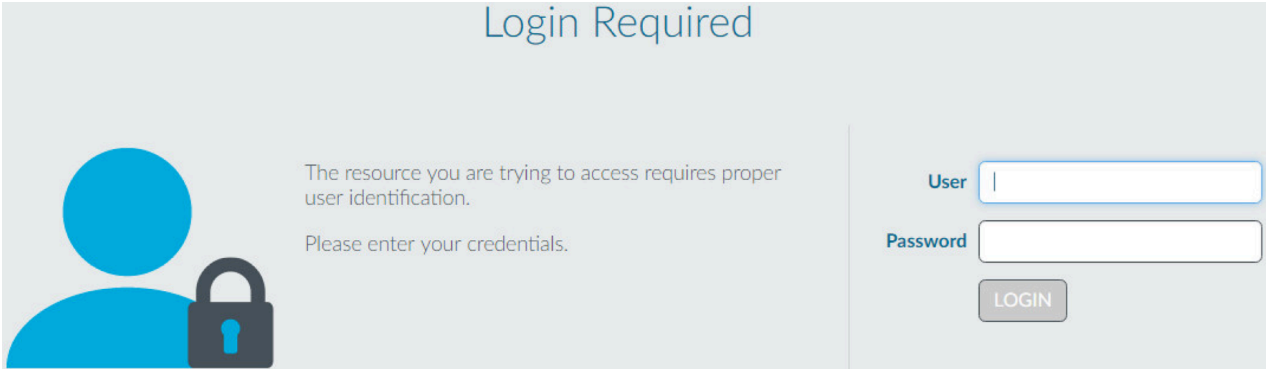
Después de añadir los servicios de autenticación de su organización a Prisma Access (aquí se muestra cómo), Prisma Access autentica usuarios en varios puntos:

- **Cuando se conectan a Prisma Access**

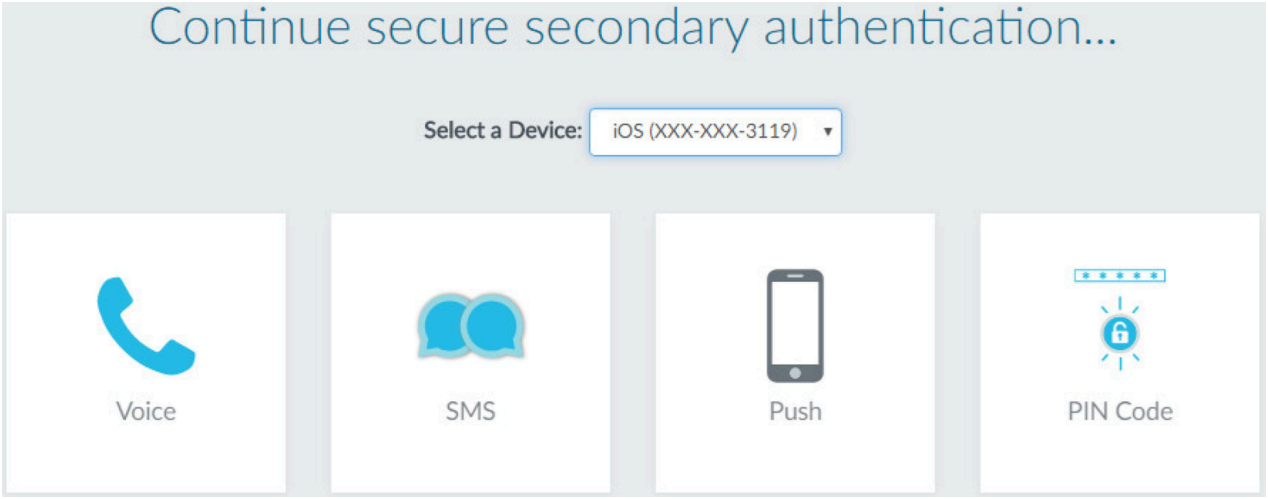
  Aquí te mostramos cómo definir cómo te gustaría que los usuarios móviles se autentiquen en Prisma Access. No es necesario definir la configuración de autenticación para que los usuarios de redes remotas se conecten a Prisma Access, ya que el tráfico de red remoto se enruta a través de túneles VPN seguros.
- **Cuando el tráfico de usuarios cumple con sus requisitos de autenticación adicional**

  A continuación se muestra cómo exigir a los usuarios que se autentiquen (mediante uno o varios métodos) para acceder a las aplicaciones de empresa y los recursos de red protegidos.

Cuando los usuarios generan tráfico web que coincide con sus requisitos de autenticación, Prisma Access comprueba que los usuarios son legítimos indicándoles que se autentiquen mediante uno o más métodos (factores), como la autenticación de inicio de sesión y contraseña, voz, SMS, notificaciones push (envíos) o contraseña única (OTP). Todos los factores que utiliza Prisma Access se basan en el servicio de autenticación y en la configuración que especifique en sus *perfiles de autenticación*. Para el primer factor (inicio de sesión y contraseña), los usuarios se autentican a través del portal de autenticación.



Para los demás factores, los usuarios se autentican a través de una página de inicio de sesión de autenticación multifactor.



Después de autenticar a los usuarios, Prisma Access evalúa sus reglas de seguridad para determinar si permite el acceso a la aplicación. Prisma Access registra toda la actividad en la que los usuarios intentan acceder a aplicaciones, servicios o recursos que ha designado para un acceso seguro.

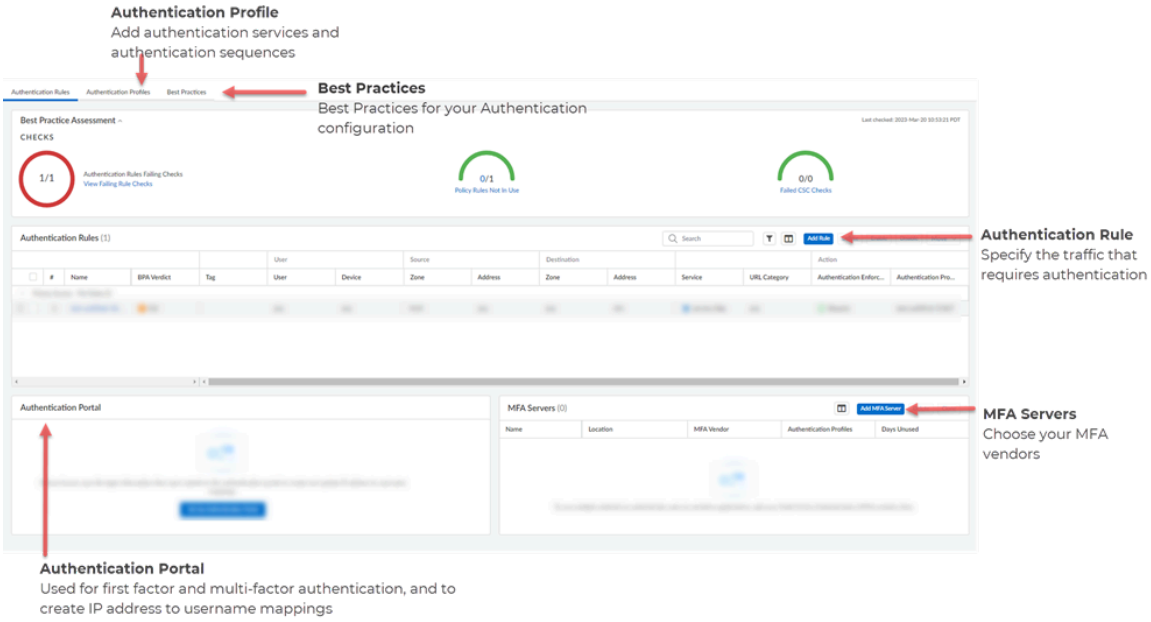
Gestionar: Configuración de autenticación

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	Uno de estos: ☐ Licencia de Prisma Access ☐ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Para configurar la autenticación con Prisma Access en Strata Cloud Manager, primero añada sus servicios de autenticación a Prisma Access. A continuación, especifique el tráfico para el que

desea requerir autenticación. Desarrolle en base a estos ajustes para añadir más funciones de autenticación, como MFA, secuencias de autenticación o habilite Prisma Access para crear y actualizar la dirección IP a las asignaciones de nombres de usuario.

Así es cómo empezar: todos los ajustes que necesita para habilitar la autenticación con Prisma Access están en un único lugar: **Manage (Gestionar)** > **Identity Services (Servicios de identidad)** > **Authentication (Autenticación)**.

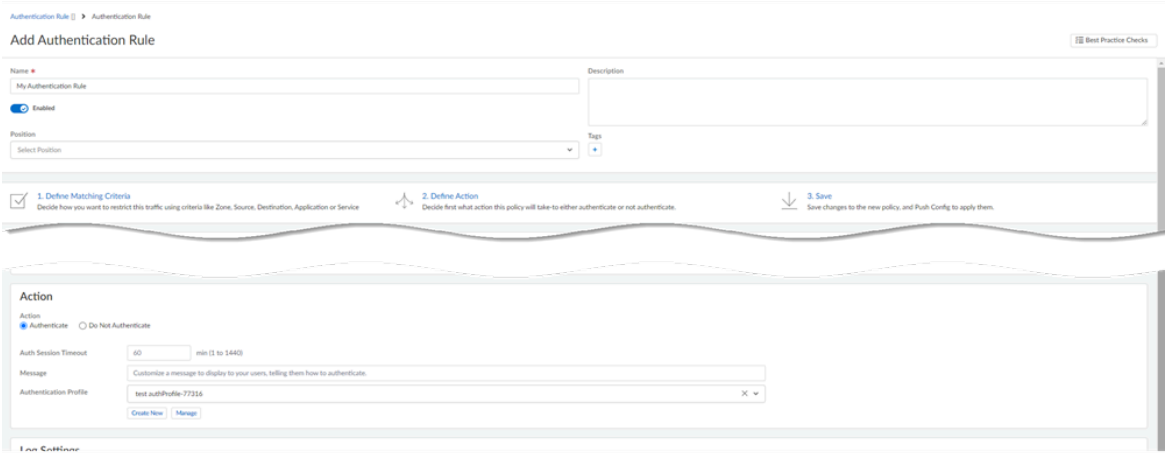


- **Reglas de autenticación** Aquí es donde especifica el tráfico para el que desea requerir autenticación

  Parte de la configuración de una regla de autenticación incluye añadir un perfil de autenticación a la regla. Cuando Prisma Access detecta tráfico que coincide con una regla de autenticación, aplica los métodos y configuraciones de autenticación definidos en el perfil de autenticación al tráfico coincidente. El perfil es lo que define cómo se requerirá que los usuarios se autentiquen.

  1. Vaya a **Manage (Gestionar)** > **Identity and Access Services (Servicios de identidad y acceso)** > **Authentication (Autenticación)** > **Authentication Rule (Regla de autenticación)** y **Add Authentication Rule (Añadir regla de autenticación)**.
  2. Defina los usuarios, servicios y categorías de URL que requieren autenticación.

3. Establezca la acción de regla en **Authenticate (Autenticación)** y elija el **Profile (Perfil)** que define el método de autenticación que desea utilizar para el tráfico que coincida con esta regla.



- **Perfil de autenticación** Añada sus servicios de autenticación aquí y defina la configuración de autenticación

  Conecte Prisma Access a los servicios que desea utilizar para autenticar usuarios (SAML, TACACS+, RADIUS, LDAP o Kerberos) y defina la configuración de autenticación (por ejemplo, establezca un límite para los intentos fallidos de inicio de sesión).

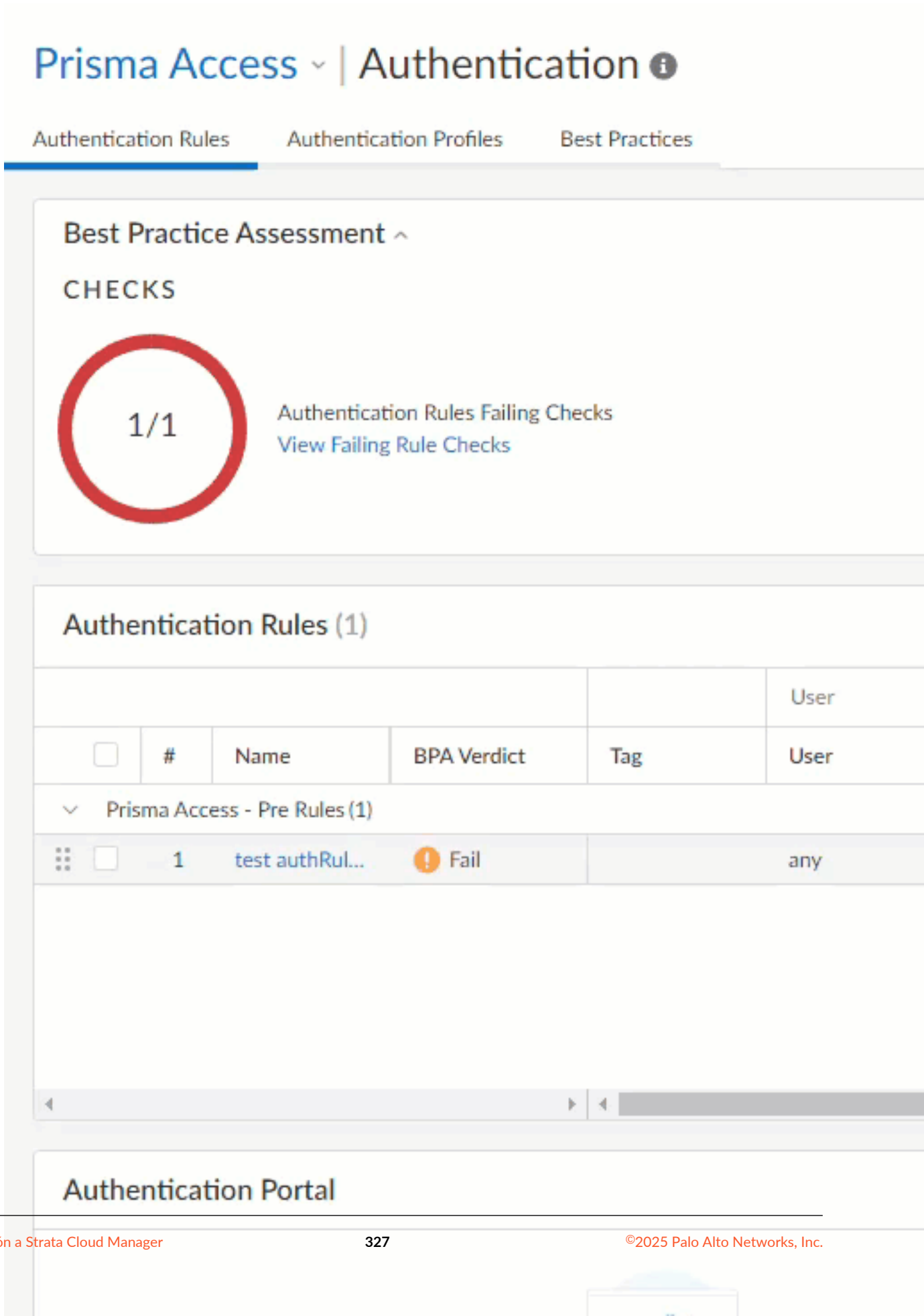
  Si está utilizando un servicio de autenticación local, primero debe crear una conexión de servicio para conectar el servicio de autenticación local a Prisma Access. Luego, regrese aquí para configurar su perfil de autenticación.

  Vaya a **Manage (Gestionar)** > **Identity and Access Services (Servicios de identidad y acceso)** > **Authentication (Autenticación)** > **Authentication Profile (Perfil de autenticación)** > **Add Profile (Añadir perfil)** y comience por establecer el **Auth Type (Tipo de autenticación)** del perfil:

  Se le pedirá que añada detalles sobre el servicio de autenticación que seleccionó para permitir que Prisma Access se conecte al servicio y lea las credenciales de usuario y los permisos de rol. En el perfil se proporcionan ajustes adicionales para personalizar la autenticación, que pueden variar según el tipo de autenticación que esté configurando.

- **Servidores MFA** Especifique el proveedor de MFA que está utilizando

  Para utilizar varios métodos para autenticar a los usuarios en aplicaciones sensibles, comience añadiendo los proveedores de MFA que desea utilizar (**Add MFA Server (Añadir servidor MFA**). Prisma Access proporciona una lista de proveedores de MFA para que pueda elegir.

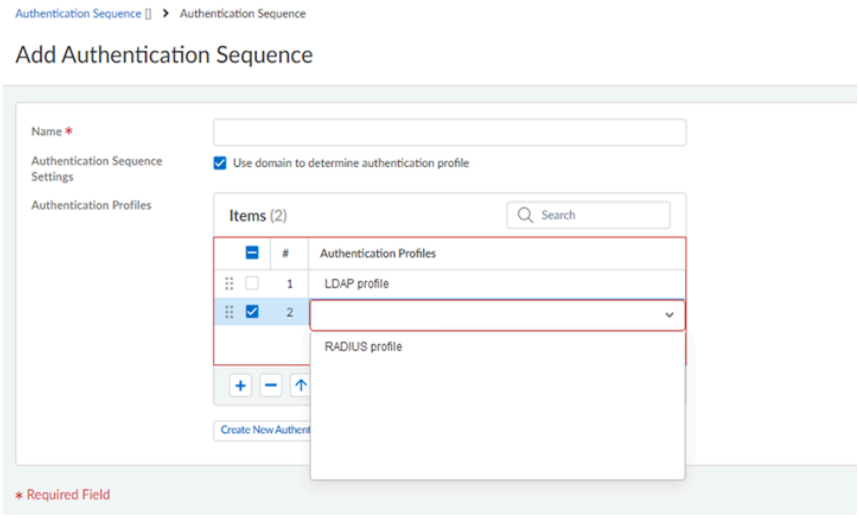


- **Portal de autenticación**: configure el portal de autenticación (también conocido como *Portal cautivo*) para usuarios en sitios de red remotos y habilite Prisma Access para crear asignaciones de direcciones IP a nombres de usuario

  Para la autenticación de un único factor (login y contraseña), los usuarios en sitios de red remotos deben autenticarse a través del portal de autenticación. Si la autenticación se realiza correctamente, Prisma Access muestra una página de inicio de sesión MFA para cada factor de autenticación adicional que se requiera. Prisma Access utiliza las credenciales que los usuarios envían para crear y actualizar asignaciones de direcciones IP a nombres de usuario. Esto significa que siempre sabrá quién en un sitio de red remoto está accediendo a contenido web y aplicaciones empresariales.

- **Secuencia de autenticación** Clasifique los perfiles de autenticación en el orden en que desee que Prisma Access los pruebe

  Seleccione **Manage (Gestionar)** > **Identity and Access Services (Servicios de identidad y acceso)** > **Authentication (Autenticación)** > **Authentication Profile (Perfil de autenticación)** y **Add Authentication Sequence (Añadir secuencia de autenticación)** para clasificar sus perfiles de autenticación. Prisma Access comprueba cada uno de ellos en secuencia hasta que uno autentica correctamente al usuario.



Gestionar: Perfiles de autenticación

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	Uno de estos: ☐ Licencia de Prisma Access ☐ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud

¿Dónde puedo usar esto?	¿Qué necesito?
	Manager depende de qué licencia(s) esté usando.

Un perfil de autenticación define el servicio de autenticación que valida las credenciales de inicio de sesión de los administradores que acceden a la interfaz web del cortafuegos y a los usuarios finales que acceden a las aplicaciones a través del portal cautivo o GlobalProtect. El perfil de autenticación también define las opciones como el inicio de sesión único (SSO).

- Kerberos
- Motor de identidad en la nube

Motor de identidad en la nube

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licencia de Prisma Access

Cloud Identity Engine (CIE) proporciona tanto identificación de usuario como autenticación de usuario para usuarios móviles en una implementación de Prisma Access-Proxy explicito. Cloud Identity Engine se integra con el Servicio de caché de la autenticación (ACS) de proxy explícito y utiliza proveedores de identidad SAML (IdP) para proporcionar autenticación a los usuarios móviles del proxy explícito.

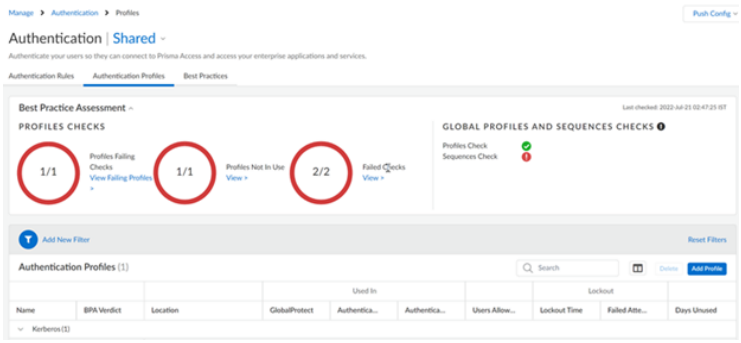
Configure un perfil de autenticación para autenticar usuarios con Cloud Identity Engine.

El método de autenticación SAML/CIE solo se muestra si el servicio de autenticación en la nube (CAS) está habilitado. Si la autenticación CIE o CAS no es compatible con su inquilino de Prisma Access, entonces muestra solo el método de autenticación SAML.

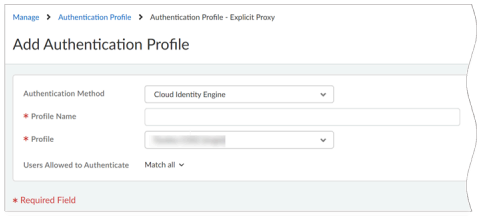
Antes de comenzar:

- Revise las Directrices de proxy explícito.
- Configure un perfil de autenticación en Cloud Identity Engine.

STEP 1 | Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **Identity Services (Servicios de identidad)** > **Authentication (Autenticación)**, establezca el ámbito de configuración en **Explicit Proxy (Proxy explícito)** y **Add Profile (Añadir perfil)** en **Authentication Profiles (Perfiles de autenticación)**.



STEP 2 | Seleccione el **Authentication Method (Método de autenticación)**. **Cloud Identity Engine**.



STEP 3 | Introduzca un **Profile Name (Nombre de perfil)** único.

STEP 4 | Seleccione el **Profile (Perfil)** de autenticación de Cloud Identity Engine que configuró en Cloud Identity Engine.

STEP 5 | Haga clic en **Save (Guardar)** para guardar sus cambios.

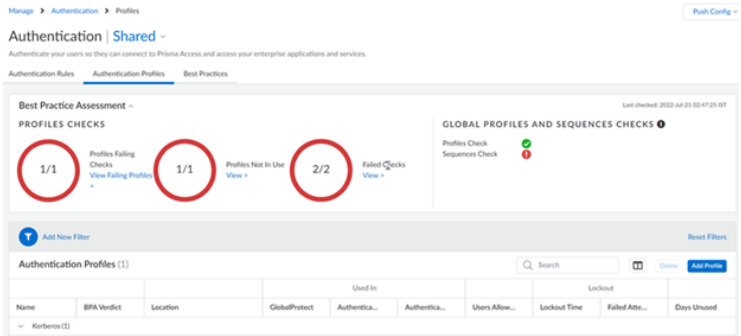
Kerberos

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licencia de Prisma Access

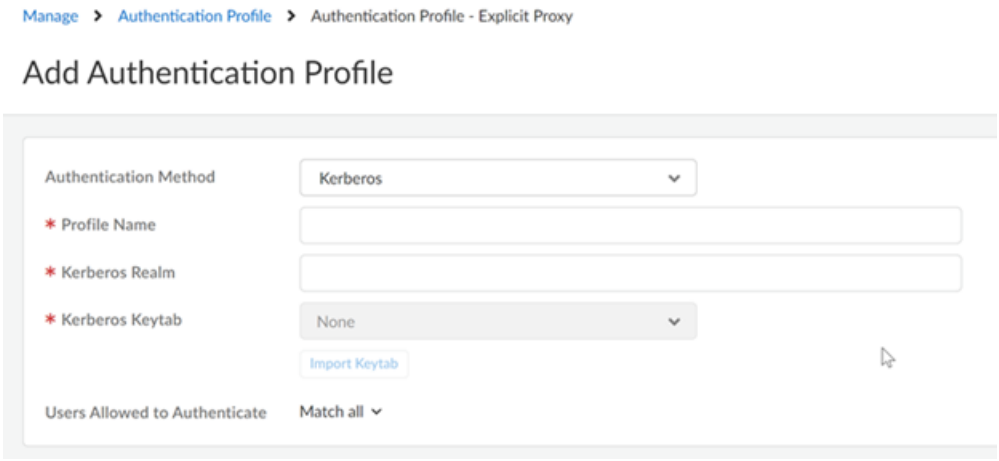
Kerberos es un protocolo de autenticación de red informática que usa vales para permitir que los nodos se comuniquen a través de una red no segura para demostrar su identidad entre sí de forma segura.

El perfil de autenticación especifica el perfil de servidor que debe utilizar el portal o las puertas de enlace cuando autentican a los usuarios. Siga estos pasos para configurar el perfil de autenticación de Kerberos para que los usuarios móviles de Proxy explícito se conecten a Prisma Access.

STEP 1 | Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **Identity Services (Servicios de identidad)** > **Authentication (Autenticación)** > **Authentication Profiles (Perfiles de autenticación)** y **Add Profile (Añadir perfil)**.



STEP 2 | Seleccione el **Authentication Method (Método de autenticación). Kerberos**.



STEP 3 | Introduzca el **Profile Name (Nombre del perfil)** para identificar el perfil del servidor. El perfil de autenticación especifica el perfil de servidor que debe utilizar el portal o las puertas de enlace cuando autentican a los usuarios.

STEP 4 | Introduzca el **Kerberos Realm (Dominio Kerberos)** (hasta 127 caracteres) para especificar la parte del nombre de host del nombre de inicio de sesión del usuario. Por ejemplo, en el nombre de cuenta de usuario usuario@EJEMPLO.LOCAL, el dominio es EJEMPLO.LOCAL.

STEP 5 | **Import (importar)** un archivo **Keytab Kerberos** que contenga la información de la cuenta Kerberos. Cuando se le solicite, busque el archivo de keytab y, luego, haga clic en **Save (Guardar)**. Durante la autenticación, el endpoint primero intenta establecer el SSO con el keytab.

STEP 6 | Seleccione el **Kerberos Keytab (Archivo keytab de Kerberos)**.

STEP 7 | Haga clic en **Save (Guardar)**.

Gestionar: Motor de identidad en la nube

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ☐ Prisma Access ☐ AIOps for NGFW Premium ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Cloud Identity Engine (Directory Sync) le proporciona a Prisma Access acceso de solo lectura a su información de Active Directory, para que pueda configurar y gestionar fácilmente políticas de seguridad y descifrado para usuarios y grupos.

Cloud Identity Engine funciona tanto con Active Directory local como con Azure Active Directory.

Para configurar el Motor de identidad en la nube con Prisma Access, comience por ir al hub para activarlo y añadirlo a Prisma Access. Luego, vaya a Prisma Access para validar que Prisma Access pueda acceder a los datos del directorio.

STEP 1 | Activar Cloud Identity Engine

Cloud Identity Engine puede compartir información de Active Directory con cualquier aplicación compatible en el hub. Es gratis y no requiere un código de autorización para comenzar. La configuración de Cloud Identity Engine incluye la activación de la aplicación Cloud Identity Engine en el hub, la configuración del agente de Cloud Identity Engine para recopilar asignaciones de Active Directory y la configuración de la autenticación mutua entre Cloud Identity y el agente.

Asegúrese de implementar la instancia de Cloud Identity Engine en la misma región en la que implementó Prisma Access y Strata Logging Service.

STEP 2 | Habilitar Cloud Identity Engine para Prisma Access.

Puede asociar Prisma Access con Cloud Identity Engine cuando active Prisma Access por primera vez o en cualquier momento posterior:

- **Mientras activa Prisma Access:** Cuando activa por primera vez Prisma Access gestionado en la nube, puede elegir una instancia de Cloud Identity Engine para que Prisma Access la utilice. Asegúrese de seleccionar una instancia que esté implementada en la misma región que Prisma Access.
- **Después de haber activado Prisma Access:** Para habilitar Cloud Identity Engine para una instancia de Prisma Access existente, inicie sesión en el hub. Desde el menú desplegable de configuración del hub (ver el engranaje en la barra de menú superior), seleccione **Manage Apps (Gestionar aplicaciones)**. Busque la instancia de Prisma Access que desea actualizar y seleccione la instancia de Cloud Identity Engine que desea que Prisma Access utilice.

STEP 3 | Confirme que Prisma Access esté conectado a Cloud Identity Engine y que Cloud Identity Engine esté compartiendo información de directorio con Prisma Access.

- Compruebe que pueda ver sus directorios en Prisma Access.

  Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **Identity Services (Servicios de identidad)** > **Cloud Identity Engine**:

- Verifique que pueda añadir usuarios y grupos a una regla de política.

  Seleccione **Manage (Gestionar)** > **Security Services (Servicios de seguridad)** > **Security (Seguridad)** o **Decryption (Descifrado)**. En una regla de política de seguridad o descifrado, verifique que el menú desplegable **Usuarios** muestre las entradas de usuarios y grupos de

Active Directory. Ahora puede comenzar a añadir estos usuarios y grupos a sus reglas de política de seguridad y descifrado.

Troubleshoot (Resolución los problemas) *de tráfico que no se ejecuta como se espera: verifique el estado de cortafuegos específicos para comprender si hay una discrepancia entre las políticas previstas (según la configuración) y las políticas aplicadas.*

Gestionar: Redistribución de identidades

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Utilice Strata Cloud Manager para configurar y gestionar la redistribución de identidades para NGFW y Prisma Access.

- Prisma Access
- NGFW

Redistribución de identidades (Prisma Access)

Para que pueda aplicar su política de seguridad de forma coherente, Prisma Access comparte los datos de identidad que GlobalProtect descubre localmente en todo su entorno de Prisma Access. Prisma Access también puede compartir datos de identidad con dispositivos locales en sitios de red remotos o sitios de conexión de servicios (sedes centrales y centros de datos).

Para Prisma Access Cloud Management, hemos habilitado parte de la redistribución de datos de identidad de forma predeterminada y, para lo que queda, hemos simplificado mucho la configuración para habilitar la redistribución (simplemente seleccione una casilla de verificación para seleccionar qué datos desea compartir).

Desde el panel de control Distribución de identidades, puede ver cómo se comparten los datos de identidad y gestionar la redistribución de datos (**Manage (Gestionar)** > **Configuration (Configuración)** > **Identity Services (Servicios de identidad)** > **Identity Redistribution (Redistribución de identidades)**.

Entre los datos de identidad que se pueden redistribuir se incluyen:

- Datos de HIP

- Asignaciones de direcciones IP a etiquetas
- Asignaciones de dirección IP a usuario
- Asignaciones de usuario a etiqueta
- Dispositivos en cuarentena

Introducción a la redistribución de identidades:

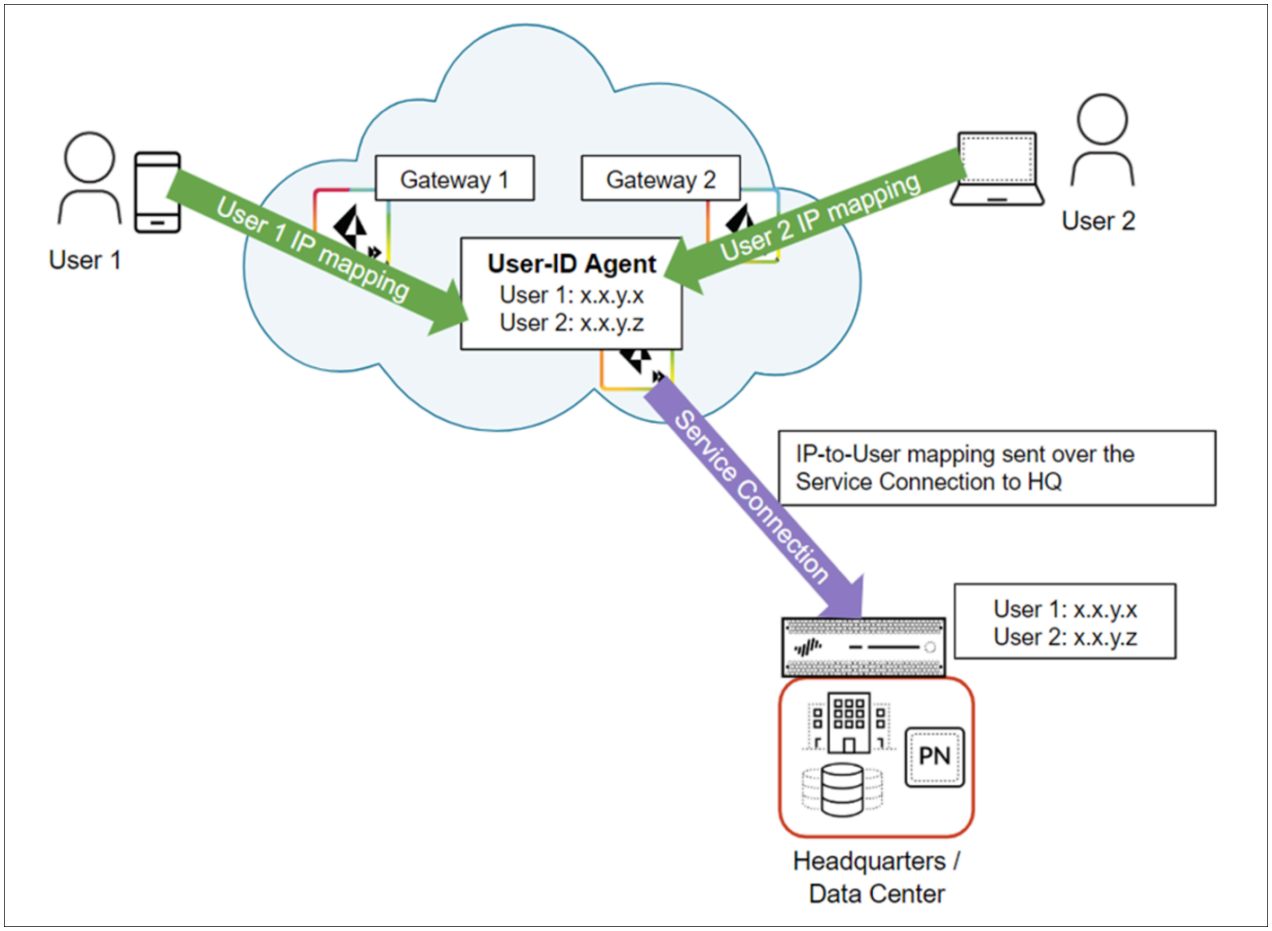
Cómo funciona la redistribución de identidades

Para que los usuarios móviles accedan a un recurso en una ubicación de red remota o en una sede o centro de datos protegido por un dispositivo con políticas basadas en el usuario, debe redistribuir los datos de identidad de los usuarios móviles de Prisma Access y los usuarios de redes remotas a ese dispositivo local.

Cuando los usuarios se conectan a Prisma Access, Prisma Access recopila los datos de identidad del usuario y los almacena.

En el siguiente ejemplo, se muestran dos usuarios móviles que tienen una asignación de dirección IP a nombre de usuario existente en Prisma Access. A continuación, Prisma Access redistribuye esta asignación a través de una conexión de servicio a los dispositivos locales que protegen la sede central o el centro de datos.

Prisma Access Cloud Management habilita automáticamente las conexiones de servicio para que funcionen como agentes de redistribución de identidad (también llamados agentes de User-ID).



Configurar la redistribución de identidades

- Confirme la configuración de la conexión de servicio

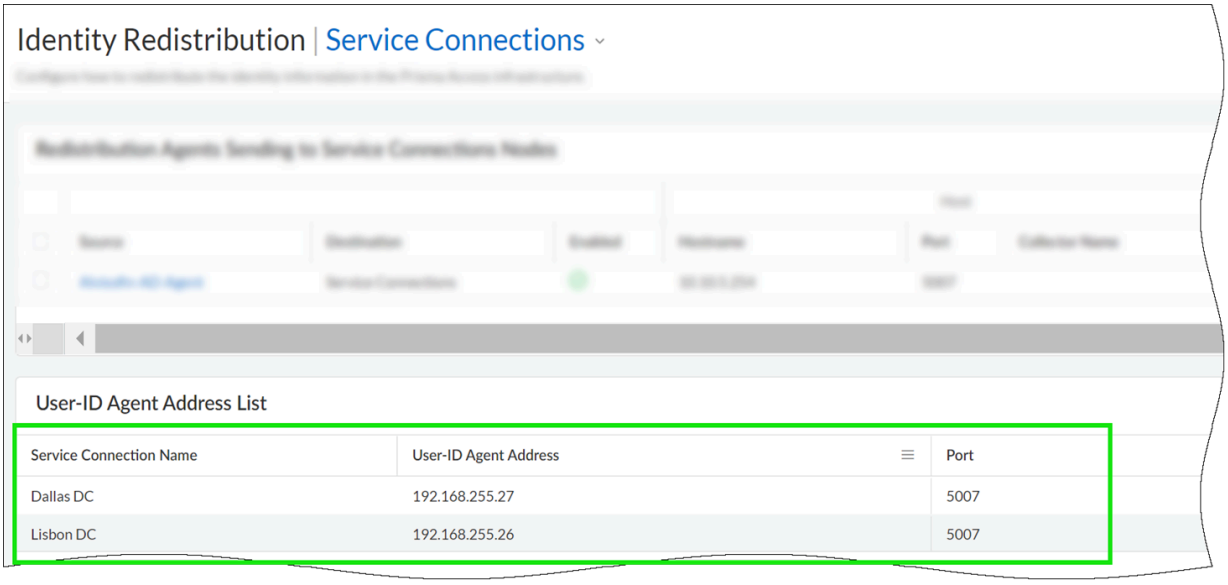
  Si aún no ha configurado una conexión de servicio para su sede central o centros de datos, comience por Configurar una conexión de servicio. Se requiere una conexión de servicio para que Prisma Access comparta datos de identidad en todo su entorno; Prisma Access permite automáticamente que las conexiones de servicio funcionen como agentes de redistribución. Una conexión de servicio recién creado estará listo para usarse como agente de redistribución cuando vea que se le ha asignado una dirección de agente de User-ID (Prisma Access hace esto automáticamente, y esto puede tardar unos pocos minutos). Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **Identity Services (Servicios de identidad)** > **Identity Redistribution (Redistribución de identidades)** y establezca el parámetro Alcance de la configuración en **Service Connections (Conexiones de servicio)** para verificar los detalles del agente de User-ID de la conexión de servicio.

- Envíe datos de identidad desde Prisma Access a dispositivos locales

  La información del agente de ID de usuario de la conexión de servicio es todo lo que necesita para configurar Prisma Access para distribuir datos de identidad a dispositivos locales.

  Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **Identity Services (Servicios de identidad)** > **Identity Redistribution (Redistribución de identidades)** y establezca el parámetro Alcance de la configuración en **Service Connections (Conexiones de servicio)** para obtener los detalles del agente de User-ID de la conexión de servicio.

  Utilice estos detalles para configurar Prisma Access como agente de redistribución de datos en Panorama o en un cortafuegos de nueva generación.

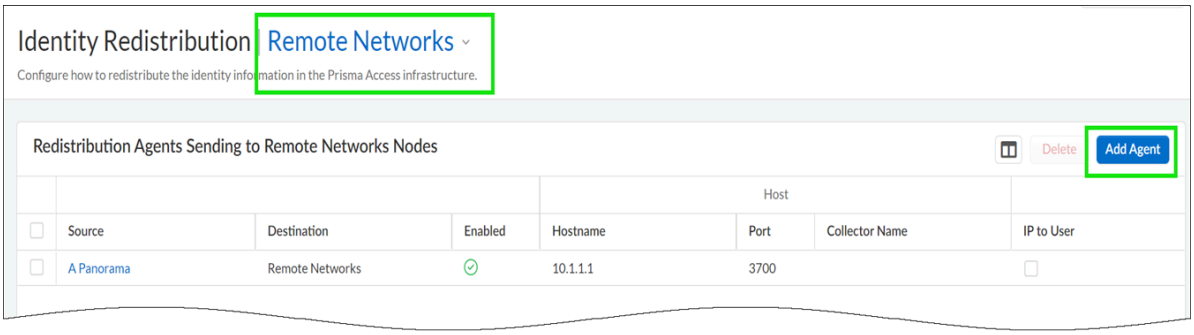


- Envíe datos de identidad desde dispositivos locales a Prisma Access

  Añada dispositivos locales a Prisma Access como agentes de redistribución; los dispositivos que añada podrán distribuir datos de identidad a Prisma Access.

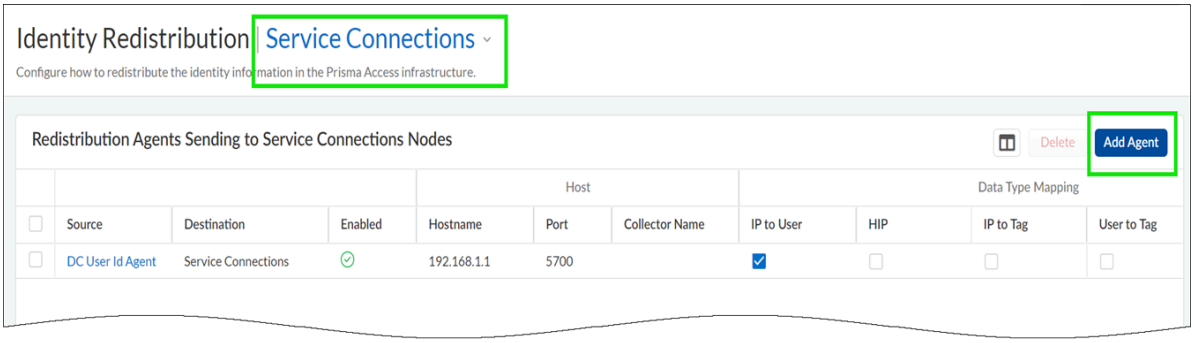
  - **Desde dispositivos en sitios de red remotos:**

    Vaya al panel **Identity Redistribution (Redistribución de identidades)**, establezca el Configuration Scope (Alcance de la configuración) para **Remote Networks (Redes remotas)**y **Add Agent (Añadir agente)**. Además de especificar los detalles del host, seleccione el tipo de datos que el dispositivo comparte con Prisma Access. La configuración opcional incluye el nombre y una clave previamente compartida para el dispositivo.



  - **Desde dispositivos en sitios de conexión de servicio:**

    Vaya al panel **Identity Redistribution (Redistribución de identidades)**, establezca el Configuration Scope (Alcance de la configuración) para **Service Connections (Conexiones de servicio)**y **Add Agent (Añadir agente)**. Además de especificar los detalles del host, seleccione el tipo de datos que el dispositivo comparte con Prisma Access. La configuración opcional incluye el nombre y una clave previamente compartida para el dispositivo.



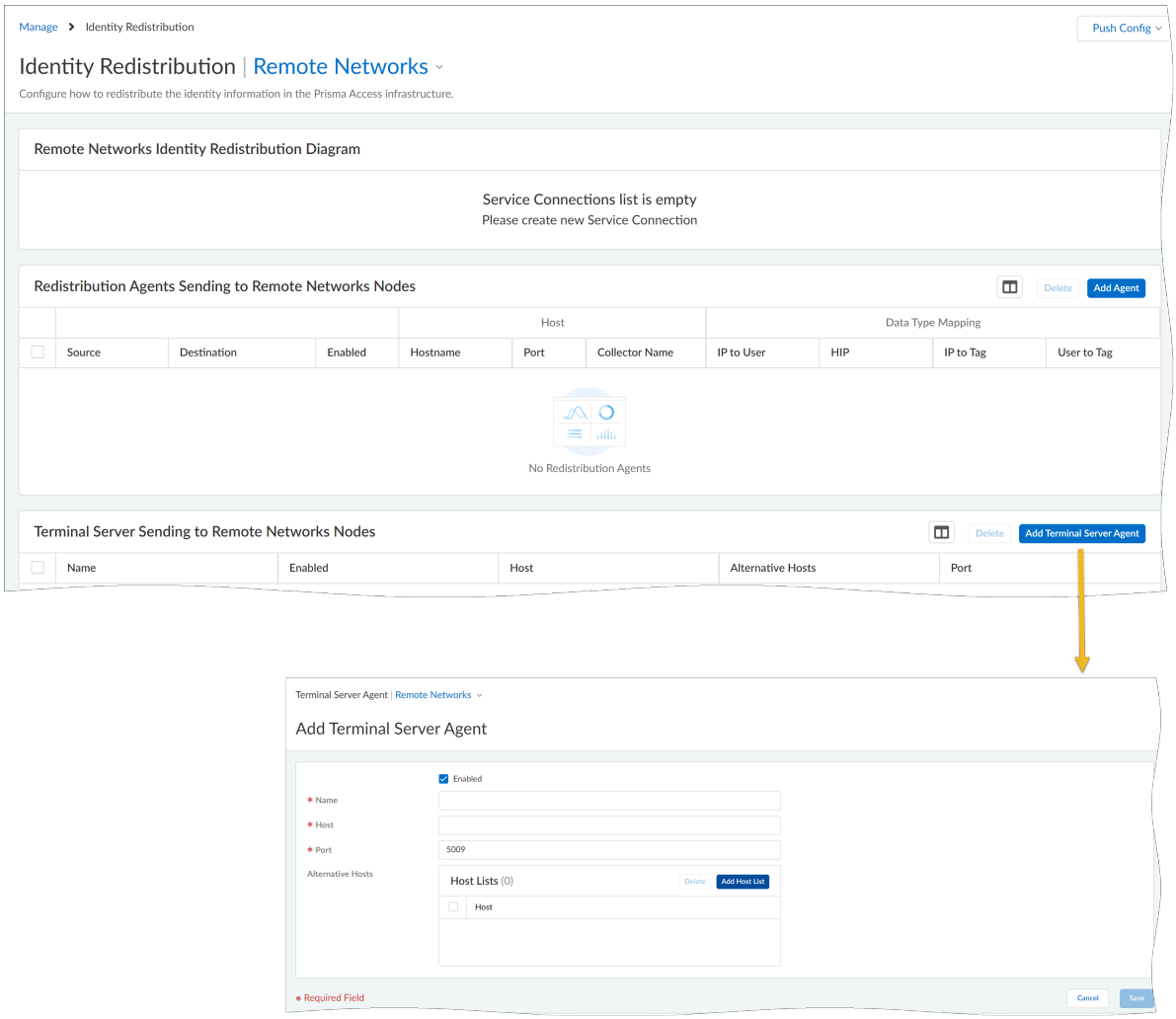
- Configure el Agente de Terminal Server para la asignación de usuarios

  El agente de Terminal Server (TS) asigna un intervalo de puertos a cada usuario para identificar a usuarios específicos en servidores de terminal basados en Windows. El agente TS notifica a Prisma Access los rangos de puertos asignados, de modo que Prisma Access pueda aplicar la política basada en usuarios y grupos de usuarios.

  En el panel **Identity Redistribution (Redistribución de identidades)**, establezca el Configuration Scope (Alcance de la configuración) para **Remote Networks (Redes remotas)** y **Add Terminal**

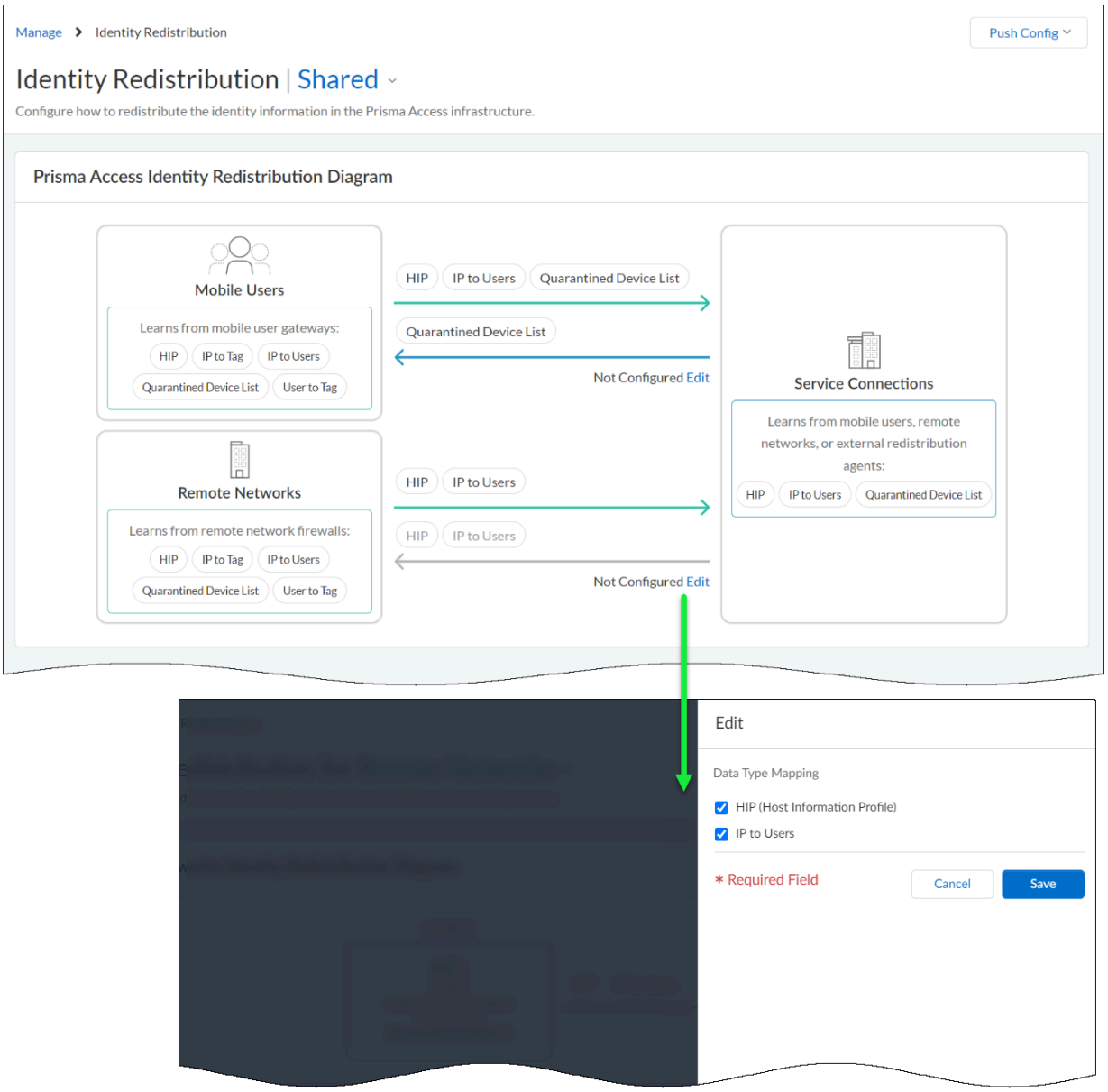
Server Agent (Añadir agente de Terminal Server) en **Terminal Server Sending to Remote Networks Nodes (Envío de Terminal Server a nodos de redes remotas)**.

- De forma predeterminada, la configuración está **Enabled (Habilitada)**.
- Introduzca un **Name (Nombre)** para el Agente TS.
- Introduzca la dirección IP del **Host** de Windows en el que está instalado el agente TS.
- Introduzca el número de **Port (Puerto)** en el que el agente escucha solicitudes de asignación de usuarios. El puerto está establecido en 5009 de forma predeterminada.
- Haga clic en **Save (Guardar)** para guardar sus cambios.



- Distribuya los datos de identidad en su entorno de Prisma Access

  En el panel **Identity Redistribution (Redistribución de identidades)**, debe **Edit (Editar)** el diagrama para especificar los datos de identidad que desea recopilar de cada origen y compartir a través de Prisma Access.



- Para activar los cambios, envíe la configuración a Prisma Access.

Redistribución de identidades (NGFW)

En una red a gran escala, en lugar de configurar todos sus cortafuegos para consultar directamente la asignación de fuentes de información, puede dinamizar el uso de recursos configurando algunos cortafuegos para recopilar la información de asignación a través de la redistribución. La redistribución de datos también proporciona granularidad, lo que le permite redistribuir solo los tipos de información que especifique solo a los dispositivos que seleccione.

También puede filtrar las asignaciones de usuarios de IP o las asignaciones de etiquetas de IP mediante subredes e intervalos para garantizar que los cortafuegos recopilen solo las asignaciones que necesitan para hacer cumplir las reglas de la política.

Para redistribuir los datos, puede utilizar los siguientes tipos de arquitectura:

- **Hub and spoke architecture for a single region (Arquitectura de hubs y radios para una sola región):**

  Para redistribuir datos entre cortafuegos, utilice una arquitectura de hub y radio como práctica recomendada. En esta configuración, un servidor de seguridad central recopila los datos de orígenes como agentes de User-ID de Windows, servidores Syslog, controladores de dominio u otros servidores de seguridad. Configure los cortafuegos del cliente de redistribución para recopilar los datos del cortafuegos del hub.
- **Arquitectura de radios y hubs múltiples para varias regiones:**

  Si tiene cortafuegos implementados en varias regiones y desea distribuir los datos a los cortafuegos en todas estas regiones para hacer cumplir las reglas de políticas de forma coherente, independientemente de dónde inicie sesión el usuario, puede utilizar una arquitectura radial y de varios hubs para varias regiones.
- **Hierarchical architecture (Arquitectura jerárquica):**

  Para redistribuir datos, también puede utilizar una arquitectura jerárquica. Por ejemplo, para redistribuir datos como la información de identificación de usuario, organice la secuencia de redistribución en capas, donde cada capa tiene uno o más cortafuegos. En la capa inferior, los agentes de User-ID integrados a PAN-OS que se ejecutan en cortafuegos y agentes de User-ID basados en Windows que se ejecutan en servidores de Windows realizan la asignación de direcciones IP a nombres de usuario. Cada capa superior tiene cortafuegos que reciben la información de asignación y marcas de tiempo de autenticación de hasta 100 puntos de redistribución en la capa inmediatamente inferior. Los cortafuegos de capas superiores agregan la información de asignación y las marcas de tiempo de todas las capas. Esta implementación ofrece la opción de configurar reglas de políticas para todos los usuarios en los cortafuegos de capa superior y reglas de políticas específicas de la región o de la función para un subconjunto de usuarios en los dominios correspondientes en los cortafuegos de capa inferior.

Cuando el tráfico no se ejecuta según lo previsto, utilice **Troubleshooting (Resolución de problemas)** *para verificar el estado del plano de datos de cortafuegos específicos para comprender si hay una discrepancia entre las políticas esperadas (según la configuración) y las políticas aplicadas.*

STEP 1 | Inicie sesión en Strata Cloud Manager.

STEP 2 | Asegúrese de que su implementación de Strata Cloud Manager cumple los requisitos para configurar la redistribución de identidad.

1. Configure y active Cloud Identity Engine (CIE) para su inquilino de Strata Cloud Manager.

   Esto es necesario para utilizar la redistribución de identidad.

   1. Activar Cloud Identity Engine.
   2. Configurar Cloud Identity Engine.
2. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Objects (Objetos)** > **Address Groups (Grupos de**

direcciones) y **Add (Añadir)** un grupo de direcciones dinámicas con las asignaciones de direcciones IP a etiquetas requeridas.

Para el tipo de grupo de direcciones, seleccione **Dynamic (Dinámico)**. Configure el grupo de direcciones dinámicas según sea necesario y dele a **Save (Guardar)**.

3. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Objects (Objetos)** > **Dynamic User Groups (Grupos de usuarios dinámicos)** y **Add (añadir)** un grupo de usuarios dinámicos con las asignaciones de nombre de usuario a etiqueta requeridas.

   Configure el grupo de usuarios dinámico según sea necesario y seleccione **Save (Guardar)**.

STEP 3 | Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW y** > **redistribución de identidad** > **Identity Services** y seleccione el alcance de configuración donde desea configurar la redistribución de identidad.

Puede seleccionar una carpeta o cortafuegos de sus **Folders (Carpetas)** o seleccionar **Snippets (Fragmentos)** para configurar la redistribución de identidad en un fragmento.

STEP 4 | **Añadir agente**.

STEP 5 | Introduzca un **Name (Nombre)** descriptivo para el agente.

STEP 6 | Introduzca la dirección IP del **host**.

STEP 7 | Introduzca el **Port (Puerto)** (el rango es 1-65535).

STEP 8 | Seleccione la **Data Type Mapping (Asignación de tipo de datos)**.

- **IP a usuario**: asignaciones de direcciones IP a nombres de usuario para User-ID.
- **Perfil de información de host (HIP):**asignaciones de direcciones IP a etiquetas para grupos de direcciones dinámicas.
- **IP a etiqueta**: asignaciones de nombre de usuario a etiqueta para grupos de usuarios dinámicos.
- **HIP**: datos de HIP de GlobalProtect que incluye objetos y perfiles de HIP.
- **Quarantine Device List (Lista de dispositivos en cuarentena)**: dispositivos que GlobalProtect identifica como en cuarentena.

STEP 9 | **Save (Guardar)**.

STEP 10 | (Gestión en la nube de NGFW únicamente) Habilite la redistribución de identidad para cortafuegos.

1. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Device Settings (Configuración de dispositivos)**

> **Device Setup (Configuración de dispositivo)** > **Management (Gestión)** y seleccione **Customize (Personalizar)** para configurar una ruta de servicio para el servicio **uid-agent** .

Seleccione el Alcance de configuración donde desea crear la ruta de servicio. Puede seleccionar una carpeta o cortafuegos de sus **Folders (Carpetas)** o seleccionar **Snippets (Fragmentos)** para configurar la ruta de servicio en un fragmento.

2. Permita que el cortafuegos responda cuando otros cortafuegos consulten los datos que redistribuir.
   1. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Device Settings (Configuración de dispositivos)** > **Device Setup (Configuración de dispositivo)** > **Management (Gestión)** y habilite el servicio de red **User-ID** .
   2. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Device Settings (Configuración de dispositivos)** > **Interfaces** para crear o seleccionar una interfaz de Capa 3.

      Expandir la **Advanced Settings (Configuración avanzada)**. En **Other (Otros)**, cree o edite el Perfil de gestión para habilitar **User-ID**.

   - Seleccione

STEP 11 | Push Config (Enviar configuración).

Gestionar: Usuarios y grupos locales

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, incluidos los financiados por Créditos de NGFW de software	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ☐ Prisma Access ☐ AIOps for NGFW Premium ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Almacene localmente información de autenticación para administradores y usuarios finales. Puede almacenar información de autenticación de administradores y usuarios finales que se autentican mediante GlobalProtect o el portal de autenticación.

Para configurar la autenticación de base de datos local, cree una base de datos que se ejecute localmente en el cortafuegos y que contenga cuentas de usuario (nombres de usuario y contraseñas o contraseñas en hash). Puede configurar una base de datos de usuarios que sea local en el cortafuegos para autenticar a los administradores que acceder a la interfaz web del cortafuegos y para autenticar a los usuarios finales que acceden a las aplicaciones mediante el portal de autenticación o GlobalProtect.

La autenticación de base de datos local se puede asociar con un perfil de autenticación para que pueda adaptarse a implementaciones donde diferentes conjuntos de usuarios requieren diferentes configuraciones de autenticación, como el inicio de sesión único (SSO) de Kerberos o la autenticación multifactor (MFA). Para las cuentas de administrador que utilizan un perfil de autenticación, no se aplica la complejidad de la contraseña ni la configuración de caducidad. Este método de autenticación se encuentra disponible para los administradores que acceden al cortafuegos y para los usuarios finales que acceden a servicios y aplicaciones mediante el portal de autenticación o GlobalProtect.

Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Identity Services (Servicios de identificación)** > **Local Users & Groups (Usuarios y grupos locales)** para comenzar a recopilar datos de autenticación.

Crear un usuario local

STEP 1 | Inicie sesión en Strata Cloud Manager.

STEP 2 | Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW y Prisma Access** > **Identity Services** > **Usuarios locales y grupos** > **Usuarios locales** y seleccione el alcance de configuración donde desea crear un usuario local.

Puede seleccionar una carpeta o cortafuegos de sus **Folders (Carpetas)** o seleccionar **Snippets (Fragmentos)** para configurar un usuario local en un fragmento.

STEP 3 | **Añadir usuario local**

STEP 4 | Introduzca el **Name (Nombre)**de usuario.

STEP 5 | Verifique que el usuario local esté **Enabled (Habilitado)**.

En lugar de eliminar un usuario local de la base de datos del cortafuegos local para su autenticación, puede desmarcar (deshabilitar) para que el usuario ya no esté habilitado para la autenticación.

STEP 6 | Introduzca una **Password** y seleccione **Confirm Password**.

STEP 7 | **Save (Guardar)**.

STEP 8 | **Push Config (Enviar configuración)**.

Crear un grupo de usuarios local

Agrupe varios usuarios locales en un solo grupo local para añadir información del grupo a la base de datos del cortafuegos local. Puede crear un grupo de usuarios local para gestionar varios usuarios locales que tengan los mismos requisitos de autenticación.

STEP 1 | Inicie sesión en Strata Cloud Manager.

STEP 2 | Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW y Prisma Access** > **Identity Services** > **Usuarios y grupos locales** > **Grupos de usuarios locales** y seleccione el alcance de configuración donde desea crear un grupo de usuarios local.

Puede seleccionar una carpeta o cortafuegos de sus **Folders (Carpetas)** o seleccionar **Snippets (Fragmentos)** para configurar un grupo de usuarios local en un fragmento.

STEP 3 | **Add Local User Group (Añadir grupo de usuarios local)**.

STEP 4 | Introduzca un **Name (Nombre)**de grupo de usuarios local.

STEP 5 | Añada los **Local Users (Usuarios locales)** que creó en el paso anterior.

STEP 6 | **Save (Guardar)**.

STEP 7 | **Push Config (Enviar configuración)**.

Gestionar: Configuración de dispositivo

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW, incluidos los financiados por Créditos de NGFW de software	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium o Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Desde **Device Settings (Configuración del dispositivo)**, puede configurar la siguiente configuración para los cortafuegos gestionados en la nube:

setting	Description (Descripción)
Interfaces	Configure interfaces para permitir que su cortafuegos funcione en varias implementaciones a la vez. En la pestaña **Ethernet**, utilice la **pestaña Mostrar configuraciones** de dispositivos locales para ver las diversas configuraciones presentes en el cortafuegos local y Strata Cloud Manager.
Enrutamiento	Configure perfiles de enrutamiento, un enrutador lógico y una ruta estática para sus cortafuegos.
Túneles IPSec	Configure túneles IPSec para autenticar y cifrar paquetes IP a medida que atraviesan el túnel.
DHCP	Configure DHCP para proporcionar los parámetros de configuración de capa de enlace y TCP/IP, y proporcionar direcciones de red con hosts configurados dinámicamente en la red TCP/IP.
Zonas	Configure zonas para segmentar su red en zonas funcionales y organizativas para reducir su superficie de ataque.
Proxy Dns	Configure un proxy DNS para configurar el cortafuegos para que actúe como intermediario entre los clientes DNS y los servidores.
Configuración de dispositivo	Configure sus dispositivos para configurar las rutas de servicio, los ajustes de conexión, los servicios permitidos

setting	Description (Descripción)
	y los ajustes de acceso administrativo para las interfaces auxiliares y de administración de los cortafuegos.
Proxy	Configure un proxy web para consolidar la funcionalidad de proxy y cortafuegos en un dispositivo. *El proxy web para Strata Cloud Manager requiere la pila de enrutadores heredada. Si desea que esta opción esté habilitada, póngase en contacto con su equipo de cuentas.*
Virtual Wire	Configure un cable virtual para integrar una interfaz de cortafuegos en una topología de modo que las dos interfaces conectadas en el cortafuegos no necesiten realizar ninguna conmutación o enrutamiento.
GlobalProtect	Habilite sus NGFW gestionados en la nube como portales y puertas de enlace GlobalProtect, para proporcionar acceso remoto flexible y seguro a los usuarios de todo el mundo.

Gestionar: Configuración global

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	Uno de estos: ☐ Licencia de Prisma Access ☐ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Revise y configure la configuración global en Strata Cloud Manager **[Manage (Gestionar) > Configuration (Configuración) > NGFW and Prisma Access (NGFW y Prisma Access) > Global Settings (Configuración global)]**

Objeto	Description (Descripción)
Gestión de aplicaciones SaaS	Gestione de forma centralizada sus aplicaciones SaaS para cada una de sus aplicaciones SaaS. La Gestión de aplicaciones SaaS le permite encontrar funciones que puede usar para habilitar aplicaciones de forma segura para su empresa.
Plantilla de notificación de formación de usuarios	Gestione centralmente las plantillas de notificación del usuario final para alertar a los usuarios a través de AI-Powered ADEM si el usuario genera un incidente de Enterprise Data Loss Prevention (E-DLP) cuando se inspecciona y bloquea el tráfico que contiene datos confidenciales.
VPN automática	Configurar dispositivos de red y establecer túneles VPN manualmente es un proceso tedioso y propenso a configuraciones erróneas. Auto VPN crea el túnel VPN entre los dispositivos de red automáticamente. Auto VPN le permite crear un clúster VPN para conectar varias redes de área local (LAN). SD-WAN con VPN automática facilita la implementación y gestión de las implementaciones de SD-WAN.

Plantilla de notificación de formación de usuarios

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Versión 6.3 o posterior de GlobalProtect app ❑ Licencia de Enterprise Data Loss Prevention (E-DLP) ❑ Licencia de usuarios móviles de Prisma Access ❑ Licencia de Prisma Access O cualquiera de las siguientes licencias que incluyen la licencia de Enterprise DLP ❑ Licencia CASB de Prisma Access ❑ Licencia de Next-Generation CASB for Prisma Access and NGFW (CASB-X)

La plantilla de notificación de entrenamiento de usuario final le permite configurar la notificación que se muestra a sus usuarios en la interfaz de usuario (UI) Access Experience cuando generan un incidente de Enterprise Data Loss Prevention (E-DLP). Se genera un incidente de Enterprise DLP cuando se descarga o carga un archivo que contiene datos confidenciales, o si el tráfico no basado en archivos que contiene datos confidenciales se publica en un formulario web.

Para determinar qué se considera información confidencial, añada una o más **Inline DLP Rules (Reglas DLP en línea)**. Reglas DLP que contienen los criterios de coincidencia de tráfico que define lo que se considera datos sensibles. La regla DLP se deriva del perfil de datos de Enterprise DLP del mismo nombre. Además, puede configurar mensajes personalizados para cuando se genere un incidente de Enterprise DLP **File Based (Basado en archivos)** o **Non-File Based (No basado en archivos)**. Después de generar un incidente de Enterprise DLP, el usuario que generó el incidente puede ver la notificación de seguridad de datos para obtener más información sobre los datos confidenciales cargados, descargados o publicados.

Solo se muestra una notificación por incidente en un período de 30 segundos, independientemente de cuántas veces el usuario genere el mismo incidente. Por ejemplo, un usuario intenta cargar un archivo que contiene datos confidenciales en la aplicación Box Web y Enterprise Data Loss Prevention (E-DLP) bloquea la carga. El usuario inmediatamente intenta cargar el mismo archivo 5 veces más, pero se bloquea cada vez. En este caso, solo se genera una alerta de Experiencia de acceso, aunque se haya bloqueado al usuario para que cargue un archivo que contenga una fecha sensible en la aplicación Box Web 6 veces en total.

STEP 1 | Comuníquese con su representante de Palo Alto Networks para habilitar el Coaching de usuario final en su inquilino.

STEP 2 | Instale la versión 6 6.3 o posterior de GlobalProtect app en Windows o macOS.

STEP 3 | Inicie sesión en Strata Cloud Manager.

STEP 4 | Habilitación Autonomous DEM.

En Strata Cloud Manager, seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **GlobalProtect** > **GlobalProtect App (Aplicación de GlobalProtect)** y **Add App Settings (Añadir configuración de aplicación)**. Debe configurar estos ajustes necesarios para mostrar notificaciones a sus usuarios en la IU de Access Experience cuando generen un incidente de DLP.

- Habilitar **Autonomous DEM y la recopilación de logs de GlobalProtect para solucionar problemas**
- **DEM for Prisma Access (Windows and Mac Only) [DEM para Prisma Access (solo Windows y Mac)]**: seleccione **Install and User Cannot Enable or Disable DEM (Instalar y usuario no puede habilitar o deshabilitar DEM)**
- **DEM for Prisma Access version 6.3 and above (Windows and Mac Only) [DEM para Prisma Access versión 6.3 y superior (solo Windows y Mac]**: seleccione **Install the Agent (Instalar el agente)**

STEP 5 | (Solo macOS) En la interfaz de usuario de Access Experience, seleccione **Settings (Configuración)** > **Notifications (Notificaciones)** y habilite **Allow notifications (Permitir notificaciones)**.

Esta configuración debe estar habilitada en la interfaz de usuario de Access Experience para cada usuario y es necesaria para mostrar notificaciones en el escritorio del usuario. Configure el resto de los ajustes de notificaciones de Access Experience según sea necesario.

STEP 6 | Configurar Enterprise DLP.

1. Cree un perfil de descifrado y una regla de políticas.

   Esto es necesario para que Enterprise DLP descifre e inspeccione el tráfico en busca de datos confidenciales.
2. Cree patrones de datos personalizados para definir los criterios de coincidencia.

   Alternativamente, puede usar los patrones de datos predefinidos en lugar de crear patrones de datos personalizados.
3. Cree un perfil y añada sus patrones de datos.

   Solo son compatibles los perfiles de datos personalizados. De forma predeterminada, las **Actions (Acciones)** de todas las reglas DLP predefinidas se establecen en **Alert (Alerta)**. Si debe duplicar el perfil de datos predefinido para editar la **Action (Acción)** de regla DLP.
4. Modificar la regla DLP.
   - Al modificar la regla DLP, debe establecer la **Action (Acción)** en **Block (Bloquear)**. Esto es necesario para generar alertas en la IU de Access Experience. No se muestran alertas si la **Action (Acción)** está configurada en **Alert (Alerta)**.
   - Añada la regla DLP a un grupo de perfiles y adjunte el grupo de perfiles a una regla de políticas de seguridad. Esto es necesario para que Enterprise DLP genere un incidente de DLP que luego genere una notificación en la IU de Access Experience.

STEP 7 | Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Global Settings (Configuración global)** > **User Coaching Notification Template (Plantilla de notificación de entrenamiento de usuario)** y **Add Notification Template (Añadir plantilla de notificación)**.

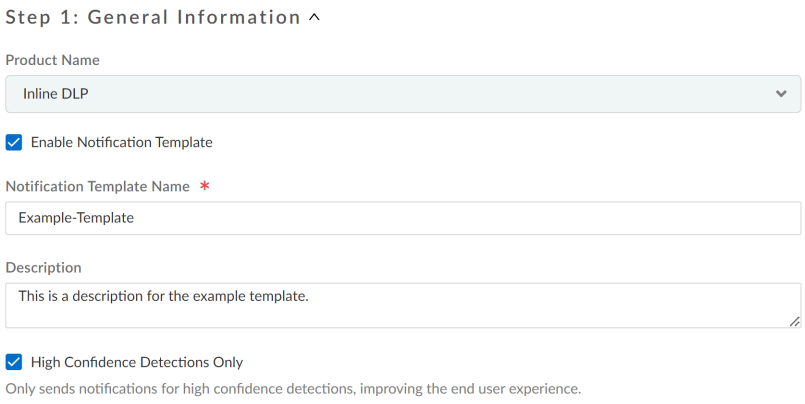
STEP 8 | Configure la **General Information (Información general)**.

1. Compruebe que el **Product Name (Nombre del producto)** es **Inline DLP (DPL en línea)**.

   Esta es la configuración predeterminada y no se puede cambiar
2. Seleccione **Enable Notification Template (Habilitar plantilla de notificación)** para habilitar la plantilla después de guardar.

   Esta configuración está habilitada de forma predeterminada.
3. Introduzca un **Notification Template Name (Nombre de plantilla de notificación)** descriptivo.
4. (Opcional) Introduzca una **Description (Descripción)** para la plantilla de notificación.
5. (Opcional) Seleccione **High Confidence Detections Only (Solo detecciones de alta confianza)** para generar solo alertas de Access Experience para coincidencias de tráfico de alta confianza.

   Las coincidencias de alta confianza reflejan la confianza que tiene Enterprise DLP al detectar tráfico coincidente. Para patrones de expresión regular (regex), esto se basa en la distancia de los caracteres a las palabras clave de proximidad configuradas. Para los patrones de aprendizaje automático (ML), este nivel de confianza se calcula mediante los modelos de ML.

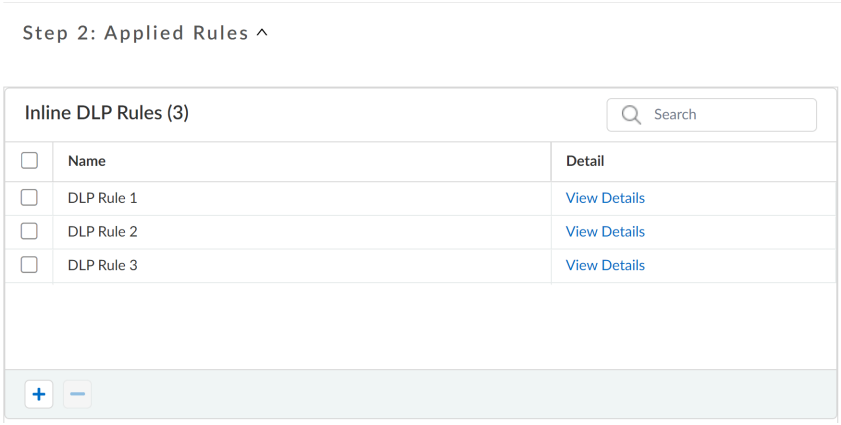


STEP 9 | Añada una o más **reglas aplicadas** a la plantilla de notificación.

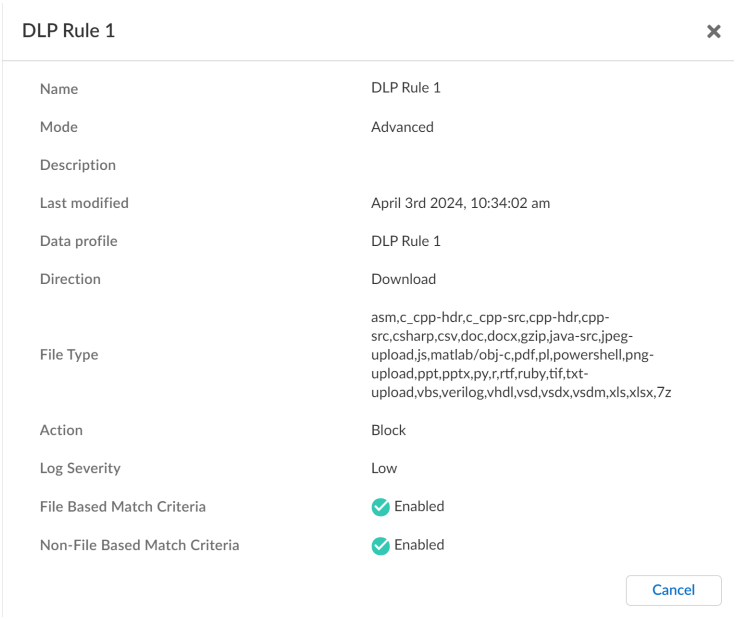
Las reglas DLP deben tener la regla **Action (Acción)** establecida en **Block (Bloquear)** y se deben añadir a un grupo de perfiles que se adjunta a una regla de políticas de seguridad para generar una notificación de experiencia de acceso. Solo añada las reglas DLP añadidas a un grupo de perfiles asociado con una regla de políticas de seguridad. Esto es necesario para que Enterprise DLP genere un incidente de DLP que luego genere una notificación en la IU de

Access Experience. Se puede añadir una sola regla DLP a varias plantillas de notificación de formación de usuario.

Todas las reglas DLP añadidas a la plantilla de notificación generan el mismo **Notification Message (Mensaje de notificación)** cuando Enterprise DLP bloquea datos confidenciales que coinciden con los perfiles de datos asociados con la regla DLP.



Puede **View Details (Ver detalles)** de cada regla DLP que añade para revisar los detalles específicos de la inspección. Esto incluye la **Direction (Dirección)** de inspección de tráfico, el **File Type (Tipo de archivo)** aplicable, la **Action (Acción)** y si la regla DLP está inspeccionando los **File Based Match Criteria (Criterios de coincidencia basados en archivos)**, los **Non-File Based Match Criteria (Criterios de coincidencia no basados en archivos)** o ambos.



STEP 10 | Defina el **Notification Message (Mensaje de notificación)** que reciben los usuarios cuando Enterprise DLP bloquea datos confidenciales que coinciden con los perfiles de datos asociados con la regla DLP.

Las plantillas de mensaje son las notificaciones toast de Access Experience que reciben los usuarios cuando Enterprise DLP bloquea datos confidenciales. Puede utilizar las siguientes variables en sus plantillas de mensajes. Debe incluir los corchetes para cada variable.

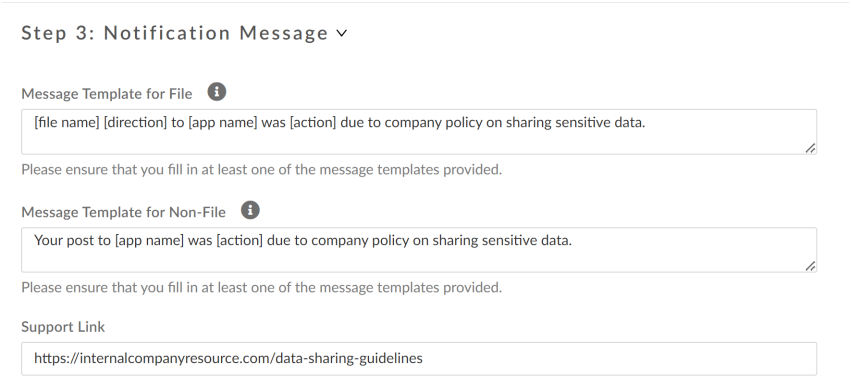
- **`[nombre de archivo]`**: nombre de archivo y extensión que contiene datos confidenciales bloqueados por Enterprise DLP.
- (Solo basado en archivos) **`[dirección]`**: especifica si Enterprise DLP bloqueó una carga o descarga de archivos.
- **`[nombre de aplicación]`**: el usuario de la aplicación intentó cargar, descargar o publicar contenido no basado en archivos.
- **`[action]`**—Acción que Enterprise DLP tomó cuando se detectaron datos sensibles. Este valor siempre está `Bloqueado`.

1. Defina las detecciones basadas en la **Message Template for File (Plantilla de mensajes para archivos)**.

   Omita este paso si la regla DLP no está configurada para detecciones basadas en archivos.
2. Defina las detecciones basadas en la **Message Template for Non-File (Plantilla de mensajes para archivos no archivos)**.

   Omita este paso si la regla DLP no está configurada para detecciones no basadas en archivos.
3. Añadir un **Support Link (Enlace de asistencia)**.

   Puede añadir enlaces directamente a la notificación emergente de Access Experience que describen la política de su empresa para compartir o descargar datos confidenciales.



STEP 11 | **Save (Guardar)**.

STEP 12 | El usuario que generó el incidente de Enterprise DLP puede ver la notificación de seguridad de datos para ver un fragmento de los datos confidenciales que se cargaron, descargaron o publicaron.

Gestionar: Operaciones

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by Panorama or Strata Cloud Manager) • Incluyendo VM-Series	❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) → Las características y capacidades disponibles para usted en Strata Cloud Manager dependen de qué licencia(s) está utilizando.

Solución de problemas

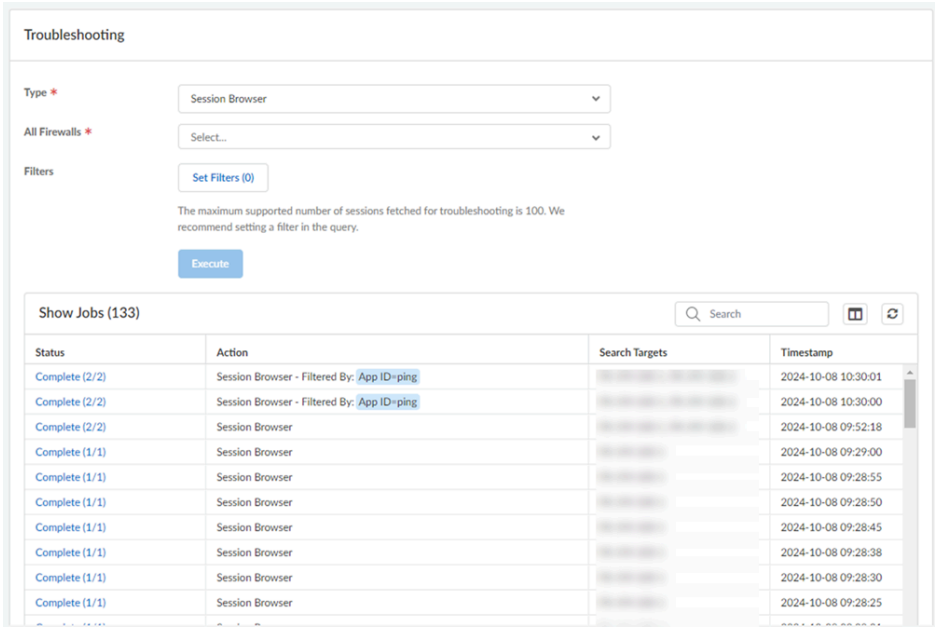
Resuelva los problemas de sus cortafuegos NGFW desde Strata Cloud Manager sin tener que moverse entre varias interfaces de cortafuegos.

Para obtener más información sobre la solución de problemas, haga clic aquí.

El panel de control de resolución de problemas le permite solucionar problemas de red, identidad y políticas para sus NGFW gestionados por Strata Cloud. Con el panel de resolución de problemas, puede localizar anomalías y configuraciones problemáticas para las siguientes áreas:

- ❑ Proxy DNS
- ❑ NAT
- ❑ Grupos de usuarios
- ❑ Grupos de direcciones dinámicas
- ❑ Grupos de usuarios dinámicos
- ❑ ID de usuario
- ❑ Explorador de sesión

Para empezar, vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Operations (Operaciones)** > > **Troubleshooting (Resolución de problemas)** > **Session Browser (Navegador de sesión)**.



Gestionar: Recomendación de política de IoT:

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)* • Cortafuegos NGFW *(con gestión de la configuración de Strata Cloud Manager o Panorama)*	❑ Al menos una de estas licencias es necesaria para gestionar su configuración con Strata Cloud Manager; para la gestión unificada de NGFW y Prisma Access, necesitará ambas: ❑ licencia de Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ La suscripción de IoT Security para un producto de IoT Security avanzado (Enterprise IoT Security Plus, Industrial IoT Security o Medical IoT Security)

IoT Security proporciona Strata Cloud Manager con recomendaciones de reglas de política de seguridad generadas automáticamente y organizadas por perfil de dispositivo. Hay una recomendación por aplicación por perfil. Elija un perfil, seleccione las recomendaciones de reglas que desea utilizar y, a continuación, los cortafuegos de nuevas generación o tipos de implementación de Prisma Access en los que desee aplicarlos.

Comenzar

Seleccione Recomendaciones de reglas de políticas de seguridad y aplíquelas a los cortafuegos de nueva generación o Prisma Access.

STEP 1 | Cree carpetas o fragmentos de código para cortafuegos de nueva generación.

Omita este paso si desea utilizar carpetas predefinidas, o carpetas o fragmentos creados anteriormente. Las carpetas de Prisma Access son predefinidas.

Carpetas son básicamente contenedores que contienen varios tipos de reglas, configuraciones de seguridad y objetos. Para importar las recomendaciones de reglas de políticas que IoT SecurityIoT Security ha generado, las carpetas deberán contener cortafuegos de nueva generación o implementaciones de Prisma Access.

Fragmentos también son un tipo de contenedor que se puede asociar a varias carpetas. Con carpetas y fragmentos, puede importar reglas de políticas en los grupos de cortafuegos o implementaciones que desee.

Por ejemplo, puede crear una carpeta denominada California y colocar 60 cortafuegos en ella y, a continuación, crear otra carpeta llamada Hawaii y colocar 15 cortafuegos en ella. A continuación, cree un fragmento de código denominado CA-HI y aplíquelo a las carpetas California y Hawái. Si desea importar recomendaciones de reglas solo a cortafuegos en California, establezca el ámbito como **Folder (Carpeta)** y seleccione la carpeta California. Si desea importar las recomendaciones de reglas tanto a California como a Hawái, establezca el alcance como **Snippet (Fragmento)** y seleccione el fragmento de CA-HI.

Dependiendo de la jerarquía de la estructura de carpetas, es posible que tengamos una carpeta principal como Oeste de EE.UU por encima de California y Hawái. A continuación, si importa recomendaciones de reglas mientras el ámbito está establecido como **Folder (Carpeta)** con **US-West (Oeste de EE. UU.)** seleccionadas, las dos carpetas secundarias California y Hawái heredarán las reglas importadas. Sin embargo, esto no funcionaría si solo quisiera importar reglas a California y Hawái si tuvieran carpetas del mismo nivel como Oregón, Alaska, Washington y Arizona en la carpeta Oeste de EE. UU. Entonces tendría que usar el fragmento de CA-HI.

STEP 2 | Cree Reglas de política de seguridad.

1. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **IoT Policy Recommendation (Recomendación de política de IoT)**.
2. Seleccione un nombre de perfil.

   IoT Security utiliza el aprendizaje automático para generar automáticamente recomendaciones de reglas de política de seguridad basadas en los comportamientos de red normales y aceptables de los dispositivos IoT en el mismo perfil de dispositivo.

Strata Cloud Manager muestra una lista de estas recomendaciones organizadas por aplicación. Para cada comportamiento, puede ver lo siguiente:

Componente de comportamiento	Explicación
Riesgo de la aplicación	Este es el nivel de riesgo inherente a una aplicación, determinado por varios factores, en una escala de riesgo creciente del 1 al 5.
Política de seguridad creada	Cuando aparecen aquí uno o varios nombres de carpetas o fragmentos, este indica que se creó previamente una regla de políticas de seguridad para este comportamiento. Al hacer clic en uno de ellos, se abre un panel lateral con los nombres del perfil, la aplicación y la carpeta o fragmento de código, así como la acción de la regla de políticas. Cuando **No** aparece aquí, indica que aún no se ha creado una regla.
Ubicación descubierta	**Internal (Interno)** Indica que el destino está en la red local. **External (Externo)** indica que el destino está fuera de la red local.
Observado localmente	**Yes (Sí)** indica que se observó el comportamiento en el entorno de inquilino de seguridad de IoT. **No** indica que se observó en varios entornos de inquilino de IoT Security, pero no en el suyo.
Uso de la aplicación	**Common (Común)** indica que se ha detectado una aplicación en varios entornos de inquilino de IoT Security. **Unique (Único)** Indica que se ha observado en su entorno pero no en el de otros inquilinos que también tienen dispositivos en el mismo perfil.
Dirección de destino y FQDN	Este es el destino de una regla de políticas recomendada. Puede ser Cualquiera, una dirección IP o un FQDN.
Perfil de destino	Se muestra un perfil cuando el destino es interno y se identifica el perfil de dispositivo del destino.
Last Seen	En el caso de los comportamientos observados localmente, esta es la marca de tiempo en la que se observó por última vez. En el caso de comportamientos comunes que

Componente de comportamiento	Explicación
	no se observan localmente, se muestra un guión.

3. Seleccione uno o más comportamientos y, a continuación, **Create Security Policy (Crear política de seguridad)**.
4. Revise las reglas de políticas de seguridad que se crearán y, a continuación, seleccione el alcance de configuración para donde Strata Cloud Manager los aplicará.

   Para aplicar las reglas a uno o más cortafuegos de nueva generación o implementaciones de Prisma Access en una carpeta, seleccione **Folders (Carpetas)** y, a continuación, elija la carpeta de Selección de ámbito.

   Para aplicar las reglas a uno o más cortafuegos de nueva generación o implementaciones de Prisma Access en un segmento, seleccione **Snippets (Segmentos)** y, a continuación, elija el segmento de Selección de ámbito.
5. **Crear políticas de seguridad**.

STEP 3 | Traslade la configuración a los cortafuegos de nueva generación y a las implementaciones de Prisma Access.

1. Seleccione **Manage (Gestionar)** > **Operations (Operaciones)** > **Push Config (Configuración de envío)**.
2. Seleccione las carpetas con los cambios de configuración, **Push Config (Enviar configuración)**, **Push (Enviar)** y entonces **Push (Enviar)** otra vez.

   Strata Cloud Manager muestra un número de ID en la columna ID de trabajo para las carpetas seleccionadas y el estado de la inserción de configuración en la columna Estado de inserción.

   Cuando el estado de inserción cambia de **Pending (Pendiente)** a **Success (Correcto)**, sabe que la configuración enviada ha comenzado a ejecutarse.
3. Para ver el estado de un trabajo de envío, seleccione **Manage (Gestionar)** > **Operations (Operaciones)** > **Push Status (Estado de envío)**. Allí puede ver el estado del trabajo principal y también el estado de las tareas secundarios, uno para cada cortafuegos o implementación.

Gestionar: DLP empresarial

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)* • Cortafuegos NGFW *(con gestión de la configuración de Strata Cloud Manager o Panorama)*	• Licencia de Enterprise Data Loss Prevention (E-DLP) • **NGFW (Managed by Panorama)**—soporte y licencias de gestión de dispositivos de Panorama • Licencia de **Prisma Access (Managed by Strata Cloud Manager)**—Prisma Access • Licencia de **SaaS Security**—SaaS Security • **NGFW (Managed by Strata Cloud Manager)**—Soporte y licencias de AIOps for NGFW Premium O cualquiera de las siguientes licencias que incluyen la licencia de Enterprise DLP • Licencia CASB de Prisma Access • Licencia de Next-Generation CASB for Prisma Access and NGFW (CASB-X) • Licencia de Data Security

Enterprise Data Loss Prevention (E-DLP) protege la información confidencial contra el acceso no autorizado, el mal uso, la extracción o el uso compartido. Enterprise DLP en Strata Cloud Manager le permite hacer cumplir los estándares de seguridad de datos de su organización y evitar la pérdida de datos confidenciales en sus NGFW y sus usuarios móviles y redes remotas de Prisma Access.

Características destacadas

- **Panel de prevención de pérdida de datos empresariales (E-DLP)**

  Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **Data Loss Prevention (Prevención de pérdida de datos)** para configurar y gestionar Enterprise DLP.

  Su configuración de Enterprise DLP se comparte entre los productos donde está utilizando Enterprise DLP. Es posible que vea aquí configuraciones que se configuraron en otro lugar, y algunas configuraciones que puede configurar aquí también se pueden aprovechar en otros productos.

- **Configuración Predefinida + Personalizada de Enterprise DLP**

  Enterprise DLP incluye configuraciones integradas que puede usar para comenzar a proteger rápidamente su contenido más confidencial:

  - El patrón de datos basados en ML y la expresión regular predefinida especifican tipos comunes de información confidencial (como tarjetas de crédito y números de seguridad social) que es posible que desee escanear y proteger.
  - Los perfiles de datos predefinidos agrupan patrones de datos que comúnmente requieren el mismo tipo de aplicación.

  También puede crear patrones y perfiles de datos personalizados directamente en Strata Cloud Manager.

- **Investigación para incidentes DLP**

  Un incidente de DLP se genera cuando el tráfico coincide con un perfil de datos de DLP adjunto a una regla de política de seguridad en Strata Cloud Manager. En el Panel de incidentes de DLP puede ver detalles del tráfico que desencadenó el incidente, como patrones de datos coincidentes, el origen y el destino del tráfico, el archivo y el tipo de archivo.

- **Búsqueda de imágenes en formatos de archivo compatibles**

  Fortalezca su postura de seguridad para prevenir aún más el uso indebido, la pérdida o el robo accidental de datos con el reconocimiento óptico de caracteres (OCR). El OCR permite que el servicio en la nube DLP analice los tipos de archivos compatibles con imágenes que contienen información confidencial que coincide con sus perfiles de filtrado de Enterprise DLP.

- **Coincidencia exacta de datos (EDM)**

  EDM es una herramienta de detección avanzada para supervisar y proteger datos confidenciales contra la exfiltración. Utilice EDM para detectar información confidencial y de identificación personal (PII), como números de seguro social, números de historiales médicos, números de cuentas bancarias y números de tarjetas de crédito, en una fuente de datos estructurada, como bases de datos, servidores de directorio o archivos de datos estructurados (CSV y TSV), con alta precisión.

- **Tipos de documentos personalizados**

  Suba sus documentos personalizados que contengan propiedad intelectual o información confidencial a Enterprise Data Loss Prevention (E-DLP) para crear tipos de documentos personalizados. Los tipos de documentos personalizados se utilizan como criterios de coincidencia en el perfil de datos avanzado para detectar y prevenir la exfiltración.

- **Email DLP**

  DLP de correo electrónico evita la exfiltración de correos electrónicos que contienen información confidencial mediante detecciones de datos impulsadas por IA y ML. Por ejemplo, Enterprise DLP puede evitar la exfiltración de datos confidenciales a través de un correo electrónico saliente enviado por un vendedor dentro de su organización a su correo electrónico personal.

- **Acceso basado en roles para Enterprise DLP**

  Puede habilitar el acceso basado en roles a controles de Enterprise DLP en el interior de Strata Cloud Manager. Esto le permite controlar qué usuarios tienen privilegios de acceso de lectura y escritura a diferentes partes de Enterprise DLP.

Comenzar

STEP 1 | Habilitar Enterprise DLP en Strata Cloud Manager.

Para configurar Enterprise DLP, debe crear un perfil de descifrado para permitir que el servicio en la nube DLP inspeccione el tráfico. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **Security Services (Servicios de seguridad)** > **Decryption (Descifrado)** y:

1. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Security Services (Servicios de seguridad)** > **Decryption (Descifrado)** y **Add Rule (Añadir regla)**.

   La configuración del perfil de descifrado predefinido permite a Enterprise DLP inspeccionar el tráfico. No es necesario modificar la configuración del perfil de descifrado predefinido a menos que necesite habilitar **Strip ALPN (Eliminar ALPN)** [**Advanced Settings (Configuración avanzada)** > **SSL Forward Proxy (Proxy de reenvío SSL)**].
2. Añada el perfil de descifrado a una regla de descifrado de **SSL Forward Proxy (Proxy de reenvío SSL)** .

- A continuación se explica cómo habilitar Enterprise DLP

STEP 2 | (Opcional) Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **Data Loss Prevention (Prevención de pérdida de datos)** > **Detection Methods (Métodos de detección)** y cree un patrón de datos

Puedes crear diseños personalizados de patrones de datos de Enterprise DLP para especificar qué contenido es sensible y necesita protección: este es el contenido que está filtrando. Puede crear un patrón de datos personalizado basado en expresiones regulares o un patrón de datos basado en propiedades de archivo.

- Aquí se explica cómo crear un patrón de datos

STEP 3 | Crear un perfil de datos

Patrones de datos de grupo que deben aplicarse de la misma manera en un perfil de datos. También puede utilizar perfiles de datos para especificar criterios de coincidencia adicionales y niveles de confianza para la coincidencia.

- Aquí se explica cómo crear un perfil de datos

STEP 4 | Crear una regla DLP

Especifique el tráfico y los tipos de archivos que desea que Enterprise DLP proteja. Establezca la acción que debe tomar Enterprise DLP cuando detecte un incidente de DLP.

- A continuación se explica cómo crear una regla DLP

Gestionar: SaaS Security:

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)*	❑ Licencia de Prisma Access

Identifique las amenazas basadas en la nube y la actividad de riesgo de los usuarios en aplicaciones autorizadas y no autorizadas con SaaS Security Inline.

SaaS Security Inline está integrada en Cloud Managed Prisma Access para brindarle una visión centralizada de la seguridad de la red y CASB. Ofrece visibilidad SaaS, que incluye análisis avanzados e informes, para que su organización tenga la información necesaria para comprender los riesgos de seguridad de los datos del uso de aplicaciones SaaS autorizadas y no autorizadas en su red.

El paquete Cloud Access Security Broker (CASB) incluye Saas Security Inline, Prevención de pérdida de datos empresariales (DLP) en línea, API de SaaS Security, API de Prevención de pérdida de datos (DLP) y Gestión de la estrategia de seguridad de SaaS (SSPM).

La licencia de Agente de seguridad de acceso a la nube de nueva generación (CASB-X) contiene todos los componentes de CASB, como SaaS Security Inline, API de SaaS Security, Gestión de la estrategia de seguridad de SaaS (SSPM) y Enterprise DLP. Se puede aplicar en dispositivos de Prisma Access gestionados en la nube, Prisma Access gestionados por Panorama y cortafuegos de nueva generación gestionados por Panorama (NGFW) en un solo entorno de inquilino.

Esto es todo lo que necesita saber *para usar SaaS Security en Strata Cloud Manager.*

Comenzar

Te mostramos cómo ponerte en marcha con SaaS Security Inline en Prisma Access Cloud Management:

- Confirme que la licencia adicional de SaaS Security se incluye con su suscripción de Prisma Access.

  Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **Overview (Descripción general)** para comprobar lo que está disponible con su licencia.

- Si aún no lo ha hecho, active la aplicación SaaS Security Inline en el hub.

  Después de la activación, SaaS Security Inline descubre automáticamente todas las aplicaciones y usuarios de SaaS y analiza la actividad de SaaS de los usuarios y los datos de uso de sus logs de Prisma Access almacenados en Strata Logging Service.

- Revise y gestione roles de administrador y acceso.

  Vaya a **Settings (Configuración)** > **Identity and Access (Identidad y acceso)** para proporcionar acceso basado en roles a los controles de SaaS Security en Prisma Access Cloud Management.

  > *Para gestionar de manera integral SaaS Security, los usuarios también deben ser administradores de la aplicación SaaS Security Inline. Salte directamente del panel de control de Prisma Access Cloud Management a la **SaaS Security Console (Consola de SaaS Security)** para Add (añadir) administradores de SaaS Security Inline.*

- Explore el panel de **SaaS Security** en Prisma Access Cloud Management.

  Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **Security Services (Servicios de seguridad)** > **SaaS Security**.

  Todas las vistas del panel son compatibles directamente con Prisma Access Cloud Management. Examine estas vistas para identificar aplicaciones y usuarios peligrosos de SaaS y la Gestión de la postura de seguridad de SaaS. SaaS Security Posture Management (SSPM) ayuda a detectar y remediar ajustes mal configurados en aplicaciones SaaS autorizadas a través de una supervisión continua.

- Revise y comparta el informe de Seguridad SaaS.

  SaaS Security Inline incluye un informe de seguridad SaaS que proporciona una instantánea del uso de la aplicación con datos y vistas agregados avanzados. Este informe sirve como herramienta de comunicación entre su equipo de seguridad SaaS y la gestión ejecutiva. Puede compartir este informe en PDF a petición con su equipo de seguridad de SaaS para una comprobación periódica, o enviarlo por correo electrónico a sus ejecutivos para resaltar las aplicaciones de SaaS en uso en su organización y los riesgos de seguridad que representan.

  - Aquí encontrará más sobre el informe de seguridad SaaS
  - Te mostramos cómo generar el informe de SaaS Security en la aplicación SaaS Security Inline

- Vea qué más puede hacer con SaaS Security y Prisma Access Cloud Management.

Recomendación de política de SaaS

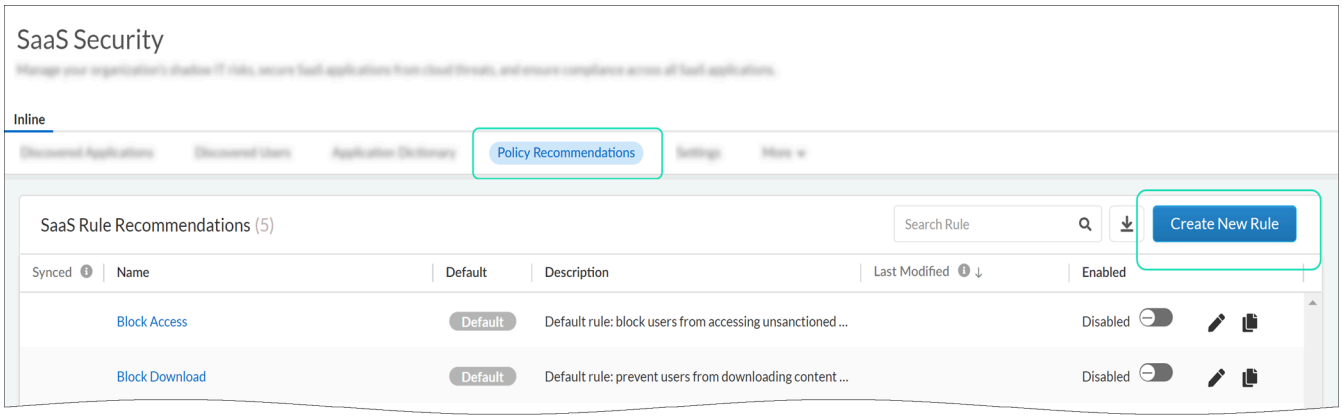
Para obtener visibilidad y control de las aplicaciones SaaS, los administradores de SaaS Security crean recomendaciones de reglas SaaS con identificadores de aplicaciones SaaS específicos proporcionados por el motor de nube de identificadores de aplicaciones (ACE).

En Prisma Access Cloud Management, ahora puede revisar y elegir aceptar las reglas que recomiendan los administradores de SaaS Security. Las recomendaciones de reglas SaaS se añaden a su políticas de acceso web: debe tener habilitada la seguridad web para aprovechar las recomendaciones de reglas SaaS.

Así es como puede comenzar: revise el flujo de trabajo para revisar y aceptar las recomendaciones de políticas de SaaS aquí:

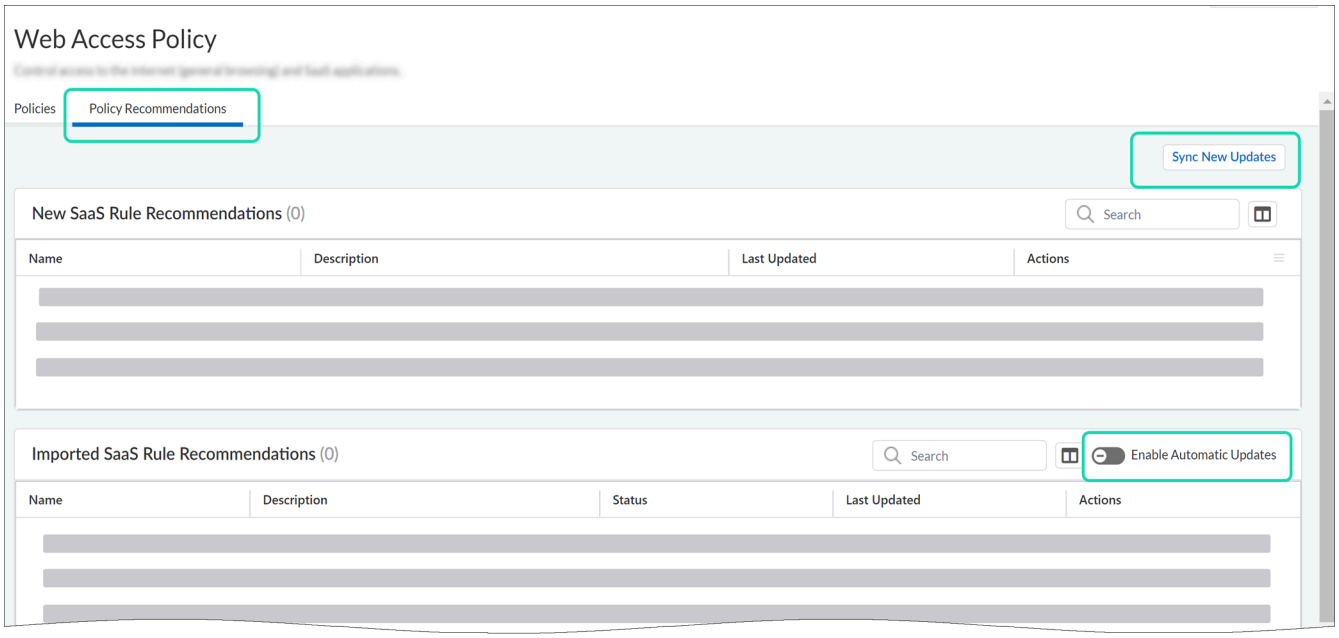
1. Los administradores de SaaS Security crean recomendaciones de reglas SaaS en la aplicación SaaS Security Inline o directamente en Prisma Access Cloud Management.

   # En Gestión en la nube de Prisma Access, vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **Security Services (Servicios de seguridad)** > **SaaS Security (Seguridad SaaS)**

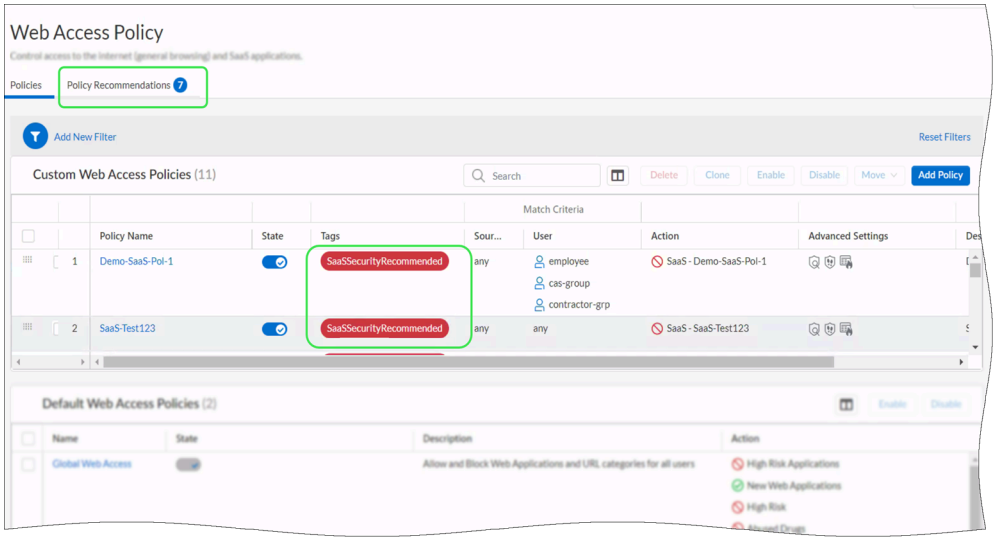


2. Puede revisar e importar las recomendaciones de reglas SaaS.

   # Vaya a **Manage (Gestionar)** > **Web Security (Seguridad web)** > **Web Access Policy (Política de acceso web)**



3. Las recomendaciones de reglas SaaS que ha importado están etiquetadas para que pueda identificarlas fácilmente.



Gestionar: Prisma SD-WAN

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma SD-WAN	❑ Licencia Prisma SD-WAN

Prisma SD-WAN proporciona una solución de red de área extensa (SD-WAN) definida por software que transforma las redes de área extensa (WAN) heredadas en un tejido de aplicaciones (AppFabric) radicalmente simplificado y seguro, virtualizando los transportes subyacentes heterogéneos en una WAN híbrida unificada. En el núcleo del sistema está el motor de rendimiento de la aplicación.

Puede ver análisis granulares basados en aplicaciones, crear una política sólida y gestionar el tráfico basado en el rendimiento de la WAN. A través de los dispositivos Instant-On Network (ION), Prisma SD-WAN simplifica la forma en que se diseñan, construyen y gestionan las WAN, ampliando de forma segura la seguridad de clase del centro de datos al perímetro de la red.

Prisma SD-WAN admite políticas apiladas para operaciones de reenvío de flujo. Utilizando políticas definidas de forma centralizada, cada dispositivo ION realiza acciones como la selección automática de rutas, la configuración de tráfico o el equilibrio de carga activo-activo entre enlaces, mientras que el controlador Prisma SD-WAN proporciona una visibilidad completa del rendimiento de la aplicación y los tiempos de respuesta en todos los enlaces WAN.

Prisma SD-WAN controla el rendimiento de la aplicación de red basándose en acuerdos de nivel de servicio (SLA) de rendimiento de la aplicación y prioridades de negocio. Puede configurar políticas, recursos, CloudBlades y ajustes del sistema para Prisma SD-WAN mediante Strata Cloud Manager.

Seleccione **Manage (Gestionar)** > **Prisma SD-WAN**para gestionar configuraciones para:

- Policies (Políticas)
- Resources (Recursos)
- CloudBlades
- System (Sistema)

Gestionar: Políticas de Prisma SD-WAN

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma SD-WAN	❑ Licencia de Prisma SD-WAN

Prisma SD-WAN admite políticas apiladas y originales. Utilizando políticas definidas de forma centralizada, cada dispositivo ION realiza acciones como la selección automática de rutas, la configuración de tráfico o el equilibrio de carga activo-activo entre enlaces, mientras que el controlador de Prisma SD-WAN proporciona una visibilidad completa del rendimiento de la aplicación y los tiempos de respuesta en todos los enlaces WAN.

Configurar políticas en Prisma SD-WAN mediante Strata Cloud Manager.

STEP 1 | Seleccione **Manage (Gestionar)** > **Prisma SD-WAN** > **Policies (Políticas)**.

Puede configurar los siguientes tipos de políticas en Prisma SD-WAN:

- Path

  Configure políticas de ruta apiladas para operaciones de reenvío de flujo y conformación de tráfico.
- Rendimiento

  Configure políticas de rendimiento para medir el rendimiento de las aplicaciones y los SLA de las aplicaciones.
- QoS

  Configure políticas de QoS apiladas para especificar prioridades de negocio.
- Seguridad

  Configure políticas de seguridad apiladas para definir reglas que determinan el acceso a la aplicación dentro de una sucursal.
- NAT

  Configure políticas NAT apiladas para garantizar la privacidad de las redes internas conectadas a redes públicas o privadas.
- Seguridad (original)

  Estas son políticas de seguridad heredadas. Si es un usuario nuevo a partir de la versión 6.0.1 del software del dispositivo ION, solo puede configurar políticas de seguridad apiladas. Si ha configurado políticas originales o heredadas, tiene que convertir estas políticas heredadas en políticas apiladas antes de poder actualizar su dispositivo a la versión 6.0.1.
- Red (Original)

  Estas son políticas de red heredadas. Si es un usuario nuevo a partir de la versión 6.0.1 del software del dispositivo ION, solo puede configurar políticas de red apiladas. Si ha configurado políticas originales o heredadas, tiene que convertir estas políticas heredadas en políticas apiladas antes de poder actualizar su dispositivo a la versión 6.0.1.

STEP 2 | Seleccione **Bindings (Enlaces)** para vincular pilas de políticas a un sitio.

Para que las reglas de políticas en las pilas de Rutas, QoS, Seguridad y NAT sean eficaces, debe vincular las pilas de políticas a un sitio. Puede vincular solo una única ruta, pila de QoS, Seguridad y NAT a un sitio a la vez.

Gestionar: Tipos de recursos para Prisma SD-WAN

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma SD-WAN	❑ Licencia de Prisma SD-WAN

Puede gestionar diferentes tipos de recursos en Prisma SD-WAN.

Gestionar recursos en Prisma SD-WAN usando Strata Cloud Manager.

Seleccione **Manage (Gestionar)** > **Prisma SD-WAN** > **Resources (Recursos)**.

Puede gestionar los siguientes tipos de recursos en Prisma SD-WAN:

- Aplicaciones

  Las aplicaciones son el núcleo de la solución Prisma SD-WAN. Los dispositivos ION implementados en la red analizan activamente todos los flujos de las aplicaciones para garantizar que se mantengan las políticas de rendimiento, cumplimiento y seguridad, y que se utilicen conexiones de red óptimas para cada flujo. El dispositivo ION utiliza definiciones de aplicaciones y tecnologías de toma de huellas dactilares para la selección de rutas, calidad de servicio y políticas de cortafuegos.

  Las aplicaciones del sistema están disponibles de forma predeterminada, aunque usted puede configurar aplicaciones personalizadas según los requisitos de su empresa.

- Categorías de circuitos

  Las categorías de circuitos son una agrupación lógica de varios tipos de circuitos y conectividades que pueden estar presentes en la red. Esta agrupación permite reglas de políticas de red simplificadas y reutilizables para toda la red. Por ejemplo, banda ancha de Internet por cable, conexiones a Internet LTE con medición, conexiones a Internet por satélite, Internet DSL o conexiones MPLS privadas.

- Contextos de red

  El contexto de red segmenta el tráfico de red con el fin de aplicar diferentes reglas de política de red para la misma aplicación. Una regla con un contexto de red siempre tiene prioridad sobre una regla sin un contexto de red. Puede crear uno o más contextos de red, pero una red LAN individual solo puede pertenecer a un contexto de red. Debe adjuntar los contextos de red a los segmentos LAN apropiados para que sean efectivos.

- Grupos de servicios y de CD

  Utilice grupos de servicios y controladores de dominio para asignar endpoints de terceros a grupos y así permitir flexibilidad al crear reglas de políticas de red para tener en cuenta la singularidad entre sitios. La intención es que las reglas de la política sigan siendo las mismas independientemente de la ubicación del sitio.

- Zonas de seguridad

  Las zonas de seguridad especifican límites de aplicación donde el tráfico está sujeto a inspección y filtrado. Cada zona de seguridad se asigna a redes conectadas a interfaces físicas, interfaces lógicas o subinterfaces de un dispositivo. Estas interfaces a nivel de zona

sirven como proxy para circuitos físicos y circuitos virtuales, como VLAN, VPN de Capa 3 y circuitos VPN de Capa 2.

- Plantillas de sitios

  La plantilla de configuración del sitio le ayuda a crear plantillas de sitio personalizadas que se adaptan a sus requisitos de implementación, lo que le permite implementar de manera eficiente sucursales y centros de datos a escala con facilidad. Con esta plantilla, puedes implementar varios sitios. Puede utilizar una plantilla existente, editar una existente o crear una nueva plantilla para implementar múltiples sitios.

- Filtros de prefijo

  Un prefijo es un grupo de una o más direcciones IP individuales o subredes de direcciones IP. Los prefijos se utilizan con políticas de conjunto de rutas y políticas de prioridad. Pueden tener alcance global o local.

- **Configuration Profiles (Perfiles de configuración)**

  Utilice perfiles de configuración para configurar ajustes para diferentes tipos de recursos.

  - IPsec

    Cree un perfil IPsec para configurar conexiones VPN IPsec entre los dispositivos de sucursal y los endpoints del servicio de seguridad en la nube.

  - IPFIX

    Un perfil IPFIX es un objeto de configuración IPFIX global que identifica la configuración del recopilador, la configuración del filtro, la plantilla para exportar elementos de información de flujo y la configuración del comprobador de flujo.

  - APN

    Cree un perfil de nombre de punto de acceso (APN) para definir la ruta de red para la conectividad de datos celulares. Se requiere información de APN para conectarse a una red móvil.

  - DNS

    Configure un perfil del Sistema de nombres de dominio (DNS) para especificar los parámetros de configuración para el servicio DNS. Los parámetros comúnmente configurados incluyen servidores DNS, asignación de dominio a dirección, configuración

de caché y configuración de DNSSEC. Una vez creado el perfil del servicio DNS, se vincula a un dispositivo.

- Plantillas NTP

  Utilice las plantillas de configuración del Protocolo de tiempo de red (NTP) para añadir o editar servidores NTP.

- Multidifusión

  Cree un perfil de configuración de multidifusión WAN y asócielo con una sucursal para habilitar el enrutamiento de multidifusión WAN para la sucursal.

- VRF

  Cree y asocie el perfil de tablas de enrutamiento y reenvío virtuales (VRF) globales (predeterminados) y asígnelo a todas las sucursales y centros de datos.

- Descubrimiento de IoT

  Utilice la visibilidad del dispositivo IoT para identificar dispositivos en su red. Los dispositivos Prisma SD-WAN branch ION inspeccionan paquetes, extraen información y generan mensajes para enviar al Strata Logging Service en un formato específico.

Gestionar: CloudBlades para Prisma SD-WAN

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma SD-WAN	❑ Licencia de Prisma SD-WAN ❑ Licencia CloudBlade para el CloudBlade respectivo

Utilice la plataforma CloudBlades de Prisma SD-WAN para acceder de forma segura a los dispositivos ION y automatizar los flujos de trabajo de la interfaz web con plantillas personalizadas para reducir la complejidad operativa.

Configure CloudBlades en Prisma SD-WAN mediante Strata Cloud Manager.

Seleccione **Manage (Gestionar)** > **Prisma SD-WAN** > **CloudBlades**.

Podrá ver los CloudBlades a los que se ha suscrito en Prisma SD-WAN. Utilice los pasos en la guía de integración de CloudBlade correspondiente para configurar su CloudBlade.

Gestionar: Recursos del sistema para Prisma SD-WAN

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma SD-WAN	❑ Licencia de Prisma SD-WAN

Gestione y supervise los usuarios y permisos en Prisma SD-WAN utilizando los recursos disponibles en la pestaña **System (Sistema)**.

Seleccione **Manage (Gestionar)** > **Prisma SD-WAN** > **System (Sistema)**.

Puede configurar los siguientes tipos de recursos del sistema en Prisma SD-WAN:

- Gestión de licencia

  Utilice la gestión de licencia para generar tokens de autorización para ION virtual. Esto proporciona un conjunto de controles para evitar la adición no autorizada de dispositivos virtuales a un entorno.

- Logs de auditoría

  Utilice los logs de auditoría para ver los registros de cambios de configuración en un sistema. Puede utilizar estos logs para fines de cumplimiento y resolución de problemas. Los logs de auditoría proporcionan información como los cambios realizados, el propietario del cambio, el momento del cambio y el alcance del cambio en un sitio, sistema o subconjunto de sitios.

- Prefijos de empresa

  Utilice Prefijos de empresa para permitir que los sitios del centro de datos de Prisma SD-WAN anuncien fácilmente las rutas y la accesibilidad a las sucursales.

- **Access Management (Gestión de acceso)**
  - Acceso de usuario
    - Gestión de usuario

      Añada un nuevo usuario con un rol en el sistema según los requisitos de su empresa. Los roles del sistema son un conjunto predefinido de permisos para cada rol. Estos roles incluyen una colección de uno o más permisos del sistema. Los roles de sistema disponibles incluyen Raíz, Super administrador, Administrador de IAM, Administrador de red, Administrador de seguridad y Usuario de solo vista.

    - Roles personalizados

      Puede crear roles personalizados combinando los roles y permisos existentes del sistema de diferentes maneras. Puede crearlos ensamblando un conjunto de permisos del sistema o añadiendo o quitando permisos de roles del sistema.

- Requisitos de contraseña

  Establezca el carácter y los requisitos de seguridad de las contraseñas. También puede establecer la frecuencia para reutilizar contraseñas antiguas y actualizar contraseñas.

- Acceso a dispositivo
  - Acceso de usuario al kit de herramientas de dispositivo
  - Política de acceso al dispositivo
- Acceso de inquilino
  - Tokens de autenticación

    Configure los token de autenticación para acceder a las API de Prisma SD-WAN. Una vez que se genera un token para un usuario, este se puede utilizar para realizar llamadas repetidas a la API y eliminar inicios de sesión innecesarios para acceder a las API.

    Un usuario con acceso a un token de autenticación puede acceder a todos los permisos asignados al token.

    Seleccione **Manage (Gestionar)** > **System (Sistema)** > **Tenant Access (Acceso de inquilino)** > **Auth Tokens (Tokens de autenticación)** > **Create Auth Token (Crear token de autenticación)** para crear una ficha de autenticación.
- Gestión de la identidad
  - Cloud Identity Engine

Gestionar: Prisma Access Browser

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licencia de Prisma Access

Desde Strata Cloud Manager, seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **Prisma Access Browser**.

Prisma Access Secure Enterprise Browser (Prisma Access Browser) es la única solución que protege los dispositivos gestionados y no gestionados, a través de un navegador empresarial integrado de forma nativa que extiende la protección a los dispositivos no gestionados. Consulte ¿Qué es Prisma Access Browser?

Inicio

Inicio es la página de destino cuando accede Prisma Access Browser de Strata Cloud Manager. Desde la página de inicio, puede utilizar los paneles de control de Prisma Access Browser para obtener información significativa del análisis del comportamiento del usuario y de los datos de navegación. Hay una variedad de paneles para casos de uso específicos que quizás desee supervisar, como el comportamiento del usuario, la prevención de fugas de datos, la seguridad web y las políticas. Cada panel contiene una colección de widgets y algunos de ellos aparecen en varios paneles.

Análisis

La pantalla de Eventos de Prisma Access Browser es la herramienta de visibilidad clave para investigar cada actividad dentro de su implementación de Enterprise Browser para verificar que las políticas y reglas funcionen como deberían. Aquí es donde se investigan los eventos de Prisma Access Browser.

Directory

- El directorio de usuarios sirve como ubicación central para obtener información sobre los usuarios y sus dispositivos conectados a Prisma Access Browser, afiliación en grupos de usuarios y reglas de políticas relacionadas. Gestionar usuarios de Prisma Access Browser
- El directorio de dispositivos proporciona una lista de sus dispositivos y grupos de dispositivos de Prisma Access Browser. Gestione dispositivos con Prisma Access Browser
- Prisma Access Browser viene equipado con una lista preexistente de aplicaciones Verificadas. La lista de aplicaciones verificadas hace referencia al catálogo de aplicaciones App-ID™ de Palo Alto Networks y se sincroniza periódicamente con la base de datos en la nube. También puedes crear aplicaciones personalizadas y privadas. Gestionar aplicaciones de Prisma Access Browser
- Prisma Access Browser mantiene un directorio de extensiones que incluye extensiones instaladas por los usuarios finales en el navegador. Esta información le permite mantener una adecuada gestión de políticas corporativas, gestionar la visibilidad y el análisis de riesgos.Gestionar extensiones de Prisma Access Browser

Política

- Puede utilizar reglas para especificar los usuarios, grupos de usuarios y grupos de dispositivos que se verán afectados por las distintas políticas. Estas reglas rigen el acceso a las aplicaciones web, las políticas de seguridad y las opciones de personalización. Al utilizar reglas, puede controlar con precisión el acceso de los usuarios a las herramientas y los componentes de la organización.Gestionar las reglas de políticas de Prisma Access Browser
- Los controles para las reglas de Prisma Access Browser se pueden configurar dentro del cuerpo de la regla individual. Los perfiles (controles externos) se pueden usar cuando desea guardar perfiles reutilizables (heredados) y añadirlos a las reglas más adelante. Gestionar los perfiles de políticas de Prisma Access Browser
- Utilice reglas de inicio de sesión para determinar qué usuarios y dispositivos tienen acceso a Prisma Access Browser. Gestionar las reglas de inicio de sesión de Prisma Access Browser
- Después de definir las condiciones de omisión dentro de las reglas de política, cuando los usuarios intentan realizar una acción o visitar un sitio bloqueado por la regla correspondiente, pueden enviar una solicitud de omisión. Para establecer condiciones de omisión, configure la acción de solicitud para habilitar las solicitudes de permiso. Gestionar las solicitudes de Prisma Access Browser para omitir las reglas de políticas.

Gestión

Gestione integraciones para obtener funcionalidad adicional con lo siguiente:

- Microsoft 365
- Protección de la información de Microsoft
- Google Workspace
- Votiro
- CrowdStrike Falcon Intelligence
- OPSWAT MetaDefender
- YazamTech SelectorIT
- Symantec DLP

Gestionar: Operaciones

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)* • NGFW, incluidos los financiados por Créditos de NGFW de software	❑ Al menos una de estas licencias es necesaria para gestionar su configuración con Strata Cloud Manager; para la gestión unificada de los NGFW y Prisma Access, necesitará ambas: ❑ Prisma Access: licencia ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager dependen de la(s) licencia(s) que esté usando.

Utilice las operaciones de Strata Cloud Manager para insertar cambios de configuración, revisar envíos de configuración anteriores y gestionar las instantáneas de las versiones de configuración para cargarlas o cambiarlas a una versión de configuración anterior.

- Envíe sus cambios de configuración
- Revise el estado de un envío de configuración
- Vea cómo puede limpiar su configuración

Gestionar: Enviar configuración

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)* • NGFW, incluidos los financiados por Créditos de NGFW de software	❑ Al menos una de estas licencias es necesaria para gestionar su configuración con Strata Cloud Manager; para la gestión unificada de los NGFW y Prisma Access, necesitará ambas: ❑ Prisma Access: licencia ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager dependen de la(s) licencia(s) que esté usando.

Una vez que haya realizado cambios en la configuración y esté listo para activarlos, debe enviar los cambios a los cortafuegos. Tiene la opción de enviar todos los cambios de configuración o seleccionar administradores específicos para incluirlos en el envío. Es necesario enviar cambios a todos los administradores para el primer envío de configuración. Puede elegir qué cambios de configuración desea enviar a Prisma Access:

- **Seguridad Web**

  Envíe actualizaciones de Seguridad Web a Prisma Access.
- **Usuarios móviles — GlobalProtect**

  Enviar actualizaciones de Global Protect a Prisma Access.
- **Usuarios móviles: Proxy explícito**

  Envíe actualizaciones de Proxy explícito a Prisma Access.
- **Redes remotas**

  Envíe actualizaciones de Redes remotas a Prisma Access.
- **Conexiones de servicio**

  Enviar actualizaciones de conexión de servicio a Prisma Access.

Puede enviar una configuración mientras se está llevando a cabo otro envío de configuración. Prisma Access aplica los cambios de configuración en el orden en que los envía.

En caso de que una configuración se envíe por error, o un cambio provoque interrupciones en la red o la seguridad, puede revertir la configuración de Prisma Access a la configuración de Prisma Access en ejecución más reciente. Esto le permite revertir la configuración de Prisma Access a una configuración que sepa que funciona y que no compromete la seguridad de su red. No tiene

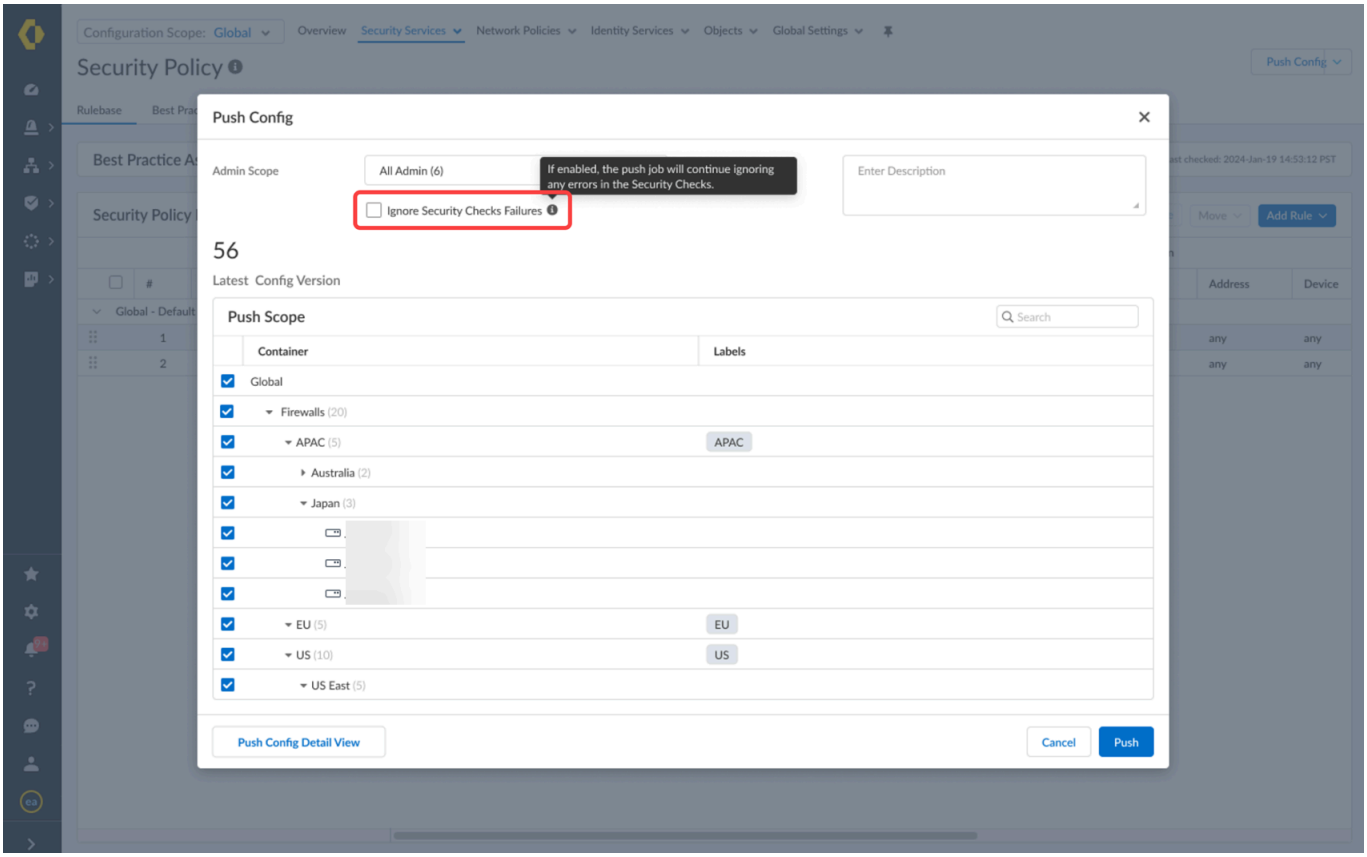
la opción de seleccionar una configuración de ejecución específica. Prisma Access selecciona automáticamente la última configuración en ejecución conocida y vuelve a ella.

STEP 1 | Inicie sesión en Strata Cloud Manager.

STEP 2 | Realice los cambios de configuración necesarios.

STEP 3 | **Push Config (Configuración de envío** y **Push (Enviar)** sus cambios en la configuración.

*Alternativamente, puede seleccionar **Manage (Gestionar)** > **Operations (Operaciones)** > **Push Config To Devices (Enviar configuración a dispositivos)**.*



En el cuadro de diálogo **Push Config (Configuración de envío)** puede **Ignore Security Check Failures (Ignorar errores de comprobación de seguridad)**. Esta función le permite continuar con las operaciones de inserción incluso cuando ciertas comprobaciones bloquearían el proceso. Si deja la casilla de verificación sin marcar (la configuración predeterminada) y se produce un error en una comprobación de prácticas recomendadas con una acción de "bloqueo", Strata Cloud Manager detiene el envío.

STEP 4 | (Opcional) **Add New Filter (Añadir nuevo filtro)**.

Puede filtrar los dispositivos que se muestran en el ámbito de envío mediante la aplicación de filtros. La aplicación de filtros solo afecta a los cortafuegos o implementaciones de Prisma Access que se muestran en el ámbito de inserción y no tiene ningún impacto en los dispositivos a los que se inserta.

STEP 5 | Edite el alcance del envío.

La edición del alcance de inserción le permite enviar cambios de configuración específicos a algunos o todos sus cortafuegos o implementaciones de Prisma Access.

No se admite la realización de un envío de configuración parcial y debe enviar toda la configuración de Strata Cloud Manager si:

- Configure un nuevo inquilino *y este es su primer envío de configuración.*
- Incorporar un cortafuegos *en Strata Cloud Manager.*
- *Incorpore un Prisma Access para usuarios móviles y remotos.*
- *Cambia el nombre o mueve una* carpeta *para que esté anidado en una carpeta diferente.*
- *Mueva un cortafuegos a una carpeta diferente.*
- *Cambiar el nombre, asociar o desasociar un* fragmento.
- *Cargar una configuración.*
- *Revierta la configuración a la última configuración enviada o a una instantánea de versión de configuración anterior.*

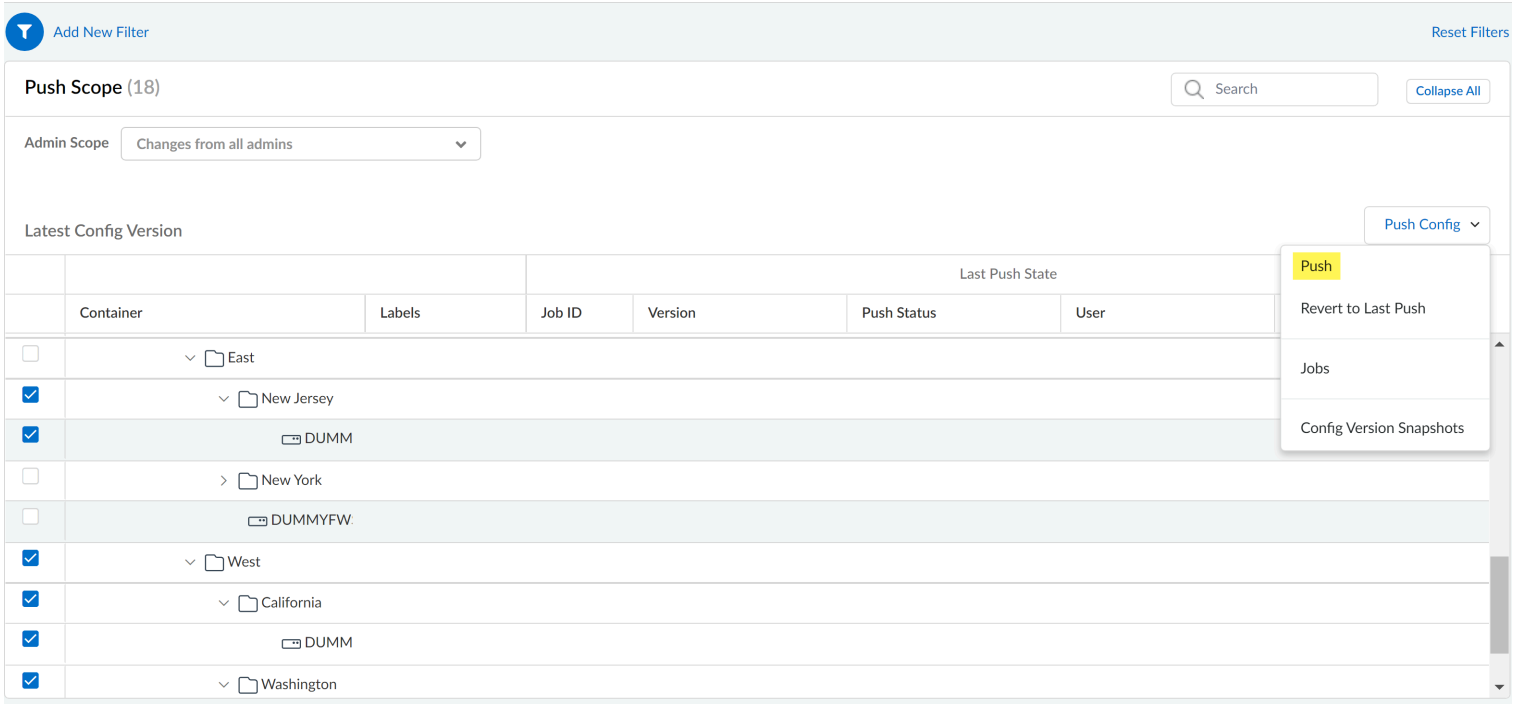
- **Admin Scope (Alcance de gestión)** : seleccione los cambios de configuración del administrador que se incluirán en el envío. De forma predeterminada, el ámbito de gestión selecciona el usuario actual y los cambios realizados por ese usuario se insertan en los cortafuegos seleccionados o en las implementaciones de Prisma Access. La selección de cambios **Changes from all admins (Cambios de todos los administradores)** incluye todos los cambios de configuración realizados por todos los administradores.

  La edición del ámbito de gestión para seleccionar administradores específicos incluye todos los cambios de configuración realizados por los administradores seleccionados. Esta opción no se puede usar al realizar el primer envío de configuración. No se admite la selección de cambios de configuración específicos para incluirlos en el envío.
- **Alcance de envío**: seleccione los tipos de implementación o las carpetas a las que desea enviar. Al seleccionar una implementación o carpeta, los cambios de configuración se insertan en todos los cortafuegos o implementaciones.

  Al seleccionar una carpeta que contiene carpetas secundarias, todas las carpetas secundarias y los cortafuegos asociados o las implementaciones de Prisma Access se incluyen en la inserción. Al seleccionar un cortafuegos específico o una implementación de Prisma Access, se selecciona automáticamente la carpeta a la que está asociado.

STEP 6 | **Push Config (Configuración de envío)** y **Push (Envío)**.

Revise los objetivos de envío y seleccione **Push (Enviar)**.



STEP 7 | Revisión Estado de envío de configuración.

En caso de que una configuración se introduzca por error, o de que un cambio provoque una interrupción de la red o de la seguridad, puede revertir su configuración de Prisma Access.

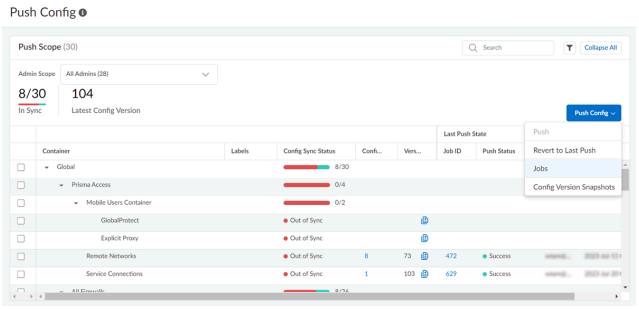
Restaurar, cargar y comparar versiones de configuración

Ver tareas de Prisma Access

Puede ver el historial de **Jobs (Tareas)** en Prisma Access para mostrar detalles sobre las operaciones que iniciaron los administradores, así como actualizaciones automáticas de contenido y licencias. Esto incluye cualquier confirmación, envío y vuelta a una versión anterior de la configuración. Puede usar la vista de tareas para solucionar problemas de operaciones con errores, investigar advertencias asociadas con compilaciones finalizadas o cancelar compilaciones pendientes.

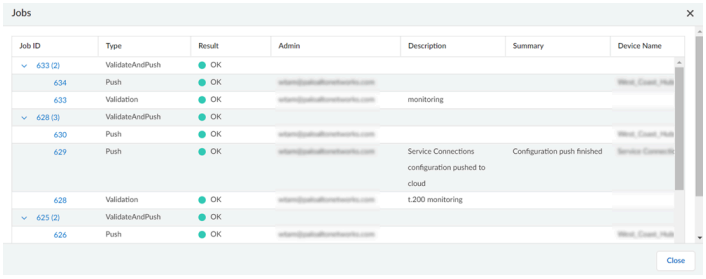
STEP 1 | Iniciar Prisma Access.

STEP 2 | En la barra de menú superior, seleccione **Push Config (Configuración de envío)** y ver los **Jobs (Tareas)** de Prisma Access.



STEP 3 | Realizar cualquiera de las siguientes tareas:

- **Investigación de advertencias o errores**: lea las entradas de la columna Resumen para obtener detalles de advertencia o error.
- **Ver una descripción de confirmación**: si un administrador introdujo una descripción de confirmación, puede consultar la columna Descripción para comprender el objetivo de la confirmación.
- **Comprobar la posición de una operación en la cola**: vea la posición y el estado de la operación para determinar la posición de la operación.



Gestionar: Estado de envío

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)* • NGFW, incluidos los financiados por Créditos de NGFW de software	❑ Al menos una de estas licencias es necesaria para gestionar su configuración con Strata Cloud Manager; para la gestión unificada de los NGFW y Prisma Access, necesitará ambas: ❑ Prisma Access: licencia ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager dependen de la(s) licencia(s) que esté usando.

Revise el estado de inserción de sus configuraciones anteriores en sus cortafuegos para revisar detalles como el resultado de la operación de inserción, el administrador que inició la inserción y los cortafuegos de destino.

STEP 1 | Inicie sesión en Strata Cloud Manager.

STEP 2 | Envíe sus cambios de configuración.

STEP 3 | Seleccione **Manage (Gestionar)** > **Operation (Operación)** > **Push Status (Estado de envío)** y ubique la operación de envío de configuración que desea revisar.

STEP 4 | Expanda el `Job ID (ID de trabajo)` para el envío de la configuración que desea revisar.

Siempre se realiza una tarea de `Validación` de configuración antes de que se envíe cualquier configuración. Cuando se envía a varios cortafuegos, cada envío de configuración tiene un `ID de trabajo` único con detalles del envío.

STEP 5 | Revise los detalles sobre el estado de envío de la configuración.

Por ejemplo, revise el `resultado`del envío push, el `administrador` que inició el envío de configuración, el `resumen`del envío de configuración y la `hora de finalización` y `la hora de inicio` del envío de configuración.

El `resultado` del envío de configuración puede ser `OK` (Aceptar) si el envío se realizó correctamente o `FAIL` (Fallido) si el envío de configuración falló.

STEP 6 | Haga clic en el `Job ID (ID de trabajo)` único para enviar una configuración a un cortafuegos para revisar los detalles del trabajo.

Los detalles del trabajo proporcionan información detallada sobre `Advertencias` y `Errores` encontrados al realizar el envío de la configuración. Por ejemplo, si falla un envío a un cortafuegos, puede revisar los Detalles del trabajo para comprender qué causó el fallo del envío de configuración.

Gestionar: Instantáneas de la versión de configuración

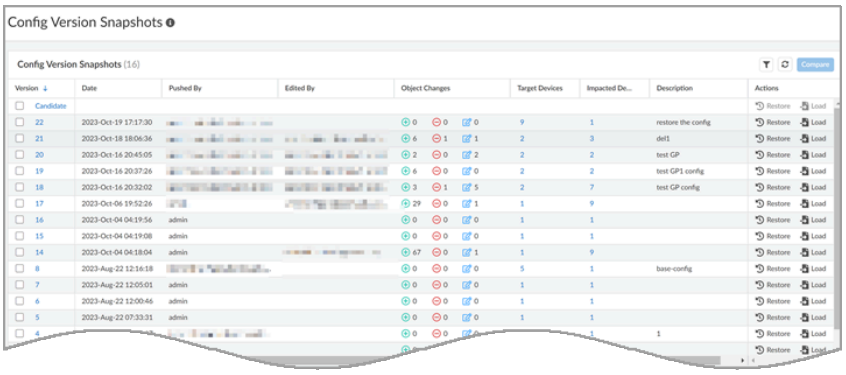
¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)* • NGFW, incluidos los financiados por Créditos de NGFW de software	❑ Al menos una de estas licencias es necesaria para gestionar su configuración con Strata Cloud Manager; para la gestión unificada de los NGFW y Prisma Access, necesitará ambas: ❑ Prisma Access: licencia ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager dependen de la(s) licencia(s) que esté usando.

Las instantáneas de configuración le ofrecen una vista del historial de configuración de su Strata Cloud Manager. Cuando un envío de configuración tiene implicaciones de seguridad no deseadas o un impacto inesperado en el tráfico, vuelva a una versión anterior para recuperarse. También puede comparar configuraciones para ver qué ha cambiado en las versiones.

Descripción general de la instantánea de configuración

La pantalla Instantánea de la versión de configuración es el lugar para revisar configuraciones enviadas, comparar instantáneas de configuración con su candidato de configuración y cargar o restaurar configuraciones anteriores.

Seleccione **Manage (Gestionar)** > **Operations (Operaciones)** > **Config Version Snapshots (Configurar instantáneas de versión)** para encontrar instantáneas de configuración y restaurar, cargar o comparar versiones.



1. **Add New Filter (Añadir filtro nuevo)**: seleccione filtros para ordenar y filtrar las versiones de configuración por columna.

2. **Version (Versión)**: el número de versión de la configuración que se envió.

   El **Candidato** le permite comparar los cambios de configuración actualmente pendientes en Strata Cloud Manager con una versión de configuración anterior.

   El número de versión de configuración es incremental. Por ejemplo, si tiene 10 versiones y restaura la versión de configuración 2, la versión de configuración cambiará de 10 a 11 (no se mostrará como 2).

3. **Date (Fecha)**: fecha y hora en que se envío la configuración.
4. **Pushed by (Enviado por)**: el administrador que envío los cambios.
5. **Edited By (Editado por)**: el administrador que hizo los cambios de configuración antes de que se enviasen.
6. **Object Changes (Cambios de objetos)**: vea cuántos objetos se añadieron, eliminaron o modificaron cuando se envió la configuración.
7. **Target Devices (Dispositivos de destino)**: dispositivos que fueron seleccionados en el ámbito de la instantánea de configuración enviada.

   Al realizar una acción de **restablecimiento**, puede elegir en cuál de los dispositivos realizar la operación.
8. **Impacted Devices (Dispositivos afectados)**: dispositivos que se han modificado desde el envío de configuración anterior. Los dispositivos solo se consideran afectados por el envío de la instantánea de configuración anterior.

   Dispositivos objetivo y afectados

   Si tiene dos dispositivos, A y B, y solo envía el dispositivo A, A se convierte en el dispositivo tanto objetivo como afectado.

   Si de nuevo vuelve a enviar hacia el dispositivo A y B, A y B son los dispositivos objetivo pero solo B es un dispositivo afectado.

   Al realizar una acción de **Carga**, los dispositivos enumerados se verán afectados.

9. **Description (Descripción)**: revise cualquier información proporcionada en el momento en que se envió la configuración.
10. **Refresh (Actualizar)**: actualice la información en la tabla de instantáneas.
11. **Reset Filters (Restablecer filtros)**: borre todos los filtros para mostrar todas las versiones de configuración.
12. **Compare (Comparar)**: vea lo que ha cambiado de versión en versión.

    Puede comparar solo dos versiones a la vez.
13. **Actions (Acciones)**: puede **Restore (Restaurar)** o **Load (Cargar)** una versión de configuración.

    - **Restore (Restaurar)**: restaura una versión de configuración anterior.

      Restaurar una versión de configuración actualiza directamente la configuración en ejecución en las implementaciones dentro del alcance del envío original y no requiere **Enviar la configuración**.

      Restaure todos los dispositivos o implementaciones en el alcance original de la configuración de envío o seleccione dispositivos o implementaciones específicos

para restaurar. No puede expandir la configuración para incluir dispositivos o implementaciones fuera del alcance original.

Restaurar una versión de configuración no elimina ni modifica la configuración candidata. La configuración en curso se guardará. Restaurar una configuración solo actualiza la versión de configuración en ejecución. Las implementaciones pueden parecer desincronizadas cuando se utiliza la acción de restablecimiento.

- **Load (Cargar)**: cargue una versión anterior como configuración candidata en Strata Cloud Manager. Su configuración candidata actual se perderá cuando se cargue una configuración anterior.

  Realice actualizaciones de la nueva configuración candidata o aplique la configuración a nuevos dispositivos e implementaciones fuera de la instantánea de configuración original y, cuando esté listo, **envíe la configuración**.
- **Save (Guardar)**: guarde la configuración candidata como una instantánea con nombre para usarla como configuración conocida. Tener una configuración conocida le permite llevar fácilmente sus implementaciones a un estado conocido y viable. Puede cambiar de un lado a otro entre sus **Named Snapshots (Instantáneas con nombre)** y la configuración registrada automáticamente que se activa en **Version Snapshots (Instantáneas de versión)**.

Strata Cloud Manager guardará hasta 6 meses de instantáneas o 200 instantáneas individuales.

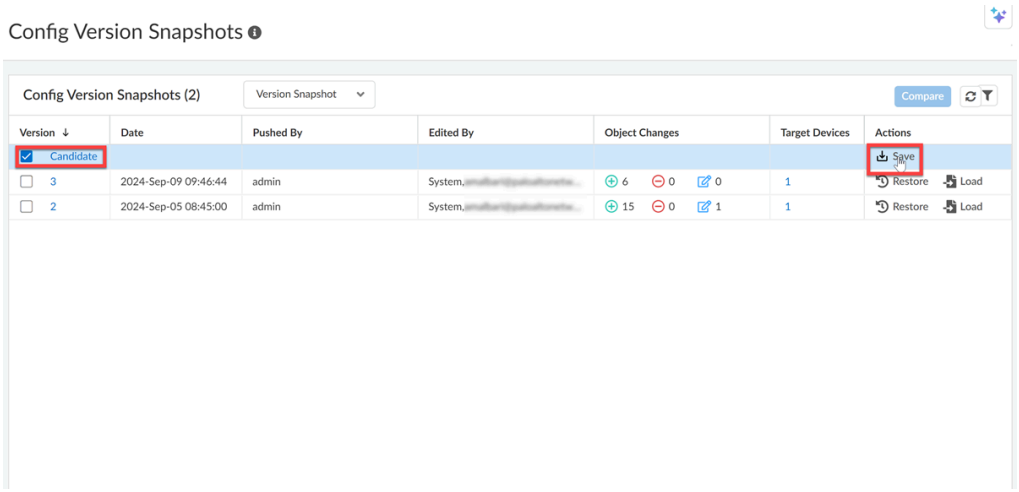
Guardar una instantánea con nombre

Guarde el candidato de configuración actual como una instantánea con nombre. No es posible guardar una configuración parcial como una instantánea con nombre. Guardar una instantánea con nombre le permite cargar un estado de configuración conocido sin tener que realizar un seguimiento de las instantáneas individuales que eventualmente se eliminarán de la tabla Instantáneas de versiones de configuración.

STEP 1 | Inicie sesión en Strata Cloud Manager.

STEP 2 | Seleccione **Manage (Gestionar)** > **Operations (Operaciones)** > **Config Version Snapshots (Configurar instantáneas de versión)**.

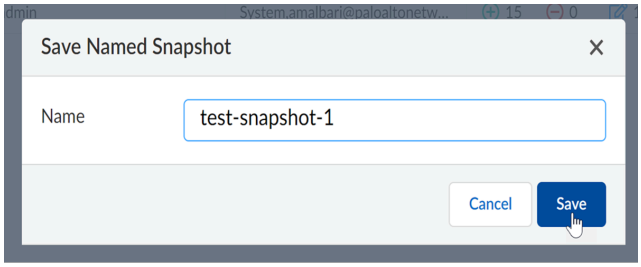
STEP 3 | Seleccione el **Candidate (Candidato)**.



STEP 4 | Haga clic en **Save (Guardar)**.

STEP 5 | Introduzca un **Name (Nombre)** de hasta 64 caracteres.

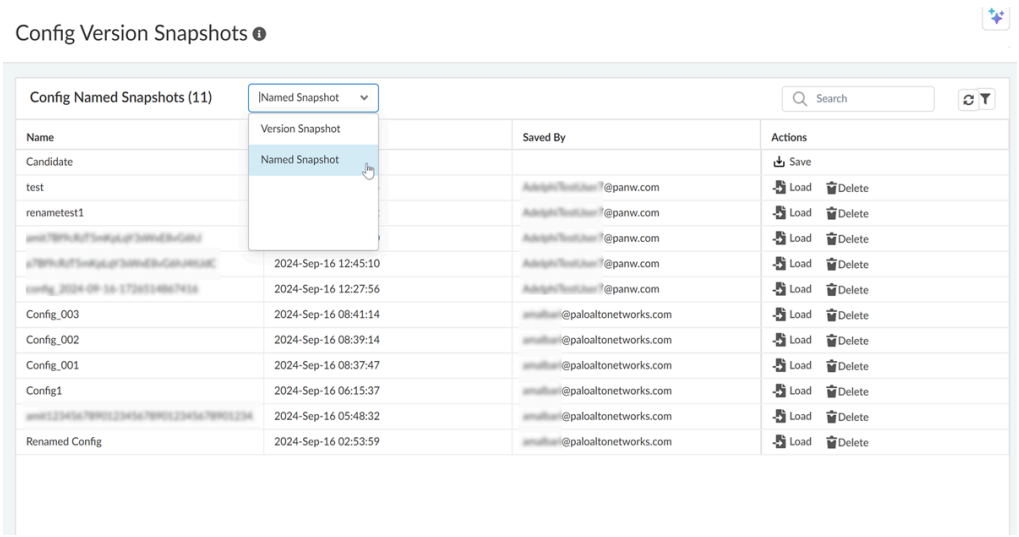
El nombre de la instantánea será **config_year-month-day-timestamp**.



STEP 6 | Deberá **Save (Guardar)** su instantánea.

STEP 7 | (Opcional) Compruebe que la instantánea se guardó navegando hasta las **Named Snapshots (Instantáneas con nombre)** en la tabla Instantáneas de configuración de versión.

> ***Gestionar instantáneas con nombre***
>
> *Los administradores pueden eliminar sus propias instantáneas con nombre. Los superusuarios pueden eliminar todas las instantáneas con nombre.*



Restablecer una instantánea

Restablezca una configuración previamente enviada. Restablecer una configuración anterior actualiza la configuración que se ejecuta en las implementaciones y dispositivos. Estos cambios no se reflejan en Strata Cloud Manager, por lo que las implementaciones y los dispositivos pueden aparecer desincronizados.

Solo los dispositivos configurados que estaban dentro del alcance del envío de configuración original pueden restaurarse a una versión seleccionada.

STEP 1 | Inicie sesión en Strata Cloud Manager.

STEP 2 | Seleccione **Manage (Gestionar)** > **Operations (Operaciones)** > **Config Version Snapshots (Configurar instantáneas de versión)**.

STEP 3 | Seleccione la versión de configuración que desea restaurar.

1. (Opcional) Seleccione el número de versión para revisar los cambios realizados por la instantánea de configuración.

STEP 4 | **Restore (Restablezca)** la versión.

1. (Opcional) Seleccione los dispositivos a los que desea dirigirse con la acción de restablecimiento.
2. **Restore (Restablecer)**.

STEP 5 | (Opcional) Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **Operations (Operaciones)** > **Push Config (Enviar configuración)** para validar la configuración que se restableció.

Cargar una instantánea

Cargue una instantánea de configuración anterior para usarla como configuración candidata.

Una vez que se haya cargado la configuración, puede continuar introduciendo modificaciones antes de presionar.

STEP 1 | Inicie sesión en Strata Cloud Manager.

STEP 2 | Seleccione **Manage (Gestionar)** > **Operations (Operaciones)** > **Config Version Snapshots (Instantáneas de la versión de configuración)**.

STEP 3 | Seleccione la versión de configuración que desea cargar.

1. (Opcional) Seleccione el número de versión para revisar los cambios realizados por la instantánea de configuración.

STEP 4 | Elija **Load (Cargar)** la versión.

STEP 5 | (Opcional) Modifique el candidato de configuración cargado según sea necesario.

STEP 6 | **Push Config (Enviar configuración)**.

Gestionar: Postura de seguridad

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)* • NGFW, incluidos los financiados por Créditos de NGFW de software	❑ Al menos una de estas licencias es necesaria para gestionar su configuración con Strata Cloud Manager; para la gestión unificada de los NGFW y Prisma Access, necesitará ambas: ❑ Prisma Access: licencia ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager dependen de la(s) licencia(s) que esté usando.

Utilice estas herramientas para mejorar su posición de seguridad y compruebe que está protegido contra las amenazas siguiendo Prácticas recomendadas de políticas de seguridad.

- Personalice las comprobaciones de postura de seguridad para su implementación a fin de maximizar las recomendaciones pertinentes en Gestionar: Configuración de la postura de seguridad
- Utilice la Limpieza de la configuración para identificar y eliminar objetos de configuración y reglas de políticas no utilizados.
- Configure las Comprobaciones de cumplimiento para perfeccionar y optimizar las reglas de seguridad excesivamente permisivas de modo que solo permitan aplicaciones que se estén utilizando realmente en su red.
- Cree sus propias Gestionar: Configuración de la postura de seguridad: personalice las comprobaciones de prácticas recomendadas existentes y cree y gestione exenciones especiales para alinearse mejor con los requisitos empresariales de su organización.
- Utilice un Analizador de políticas para asegurarse de que las actualizaciones que realice a sus reglas de Política de seguridad cumplan con sus requisitos y no introduzcan errores o configuraciones incorrectas (como cambios que resulten en reglas duplicadas o conflictivas).

Gestionar: Analizador de políticas

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Gestionado por Panorama) • VM-Series, funded with Software NGFW Credits (gestionado por Panorama) • Prisma Access (Managed by Panorama)	❑ Se necesita al menos una de estas licencias: ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro ❑ Complemento Panorama CloudConnector para implementaciones gestionadas por Panorama

Las actualizaciones de las reglas de su política de seguridad suelen ser urgentes y requieren que usted actúe rápidamente. Sin embargo, desea asegurarse de que cualquier actualización que realice a su base de reglas de política de seguridad cumpla con sus requisitos y no introduzca errores o configuraciones incorrectas (como cambios que resulten en reglas duplicadas o conflictivas).

Para lograr esto, el Analizador de políticas en Strata Cloud Manager permite optimizar el tiempo y los recursos al implementar una solicitud de cambio. El analizador de políticas no solo analiza y proporciona sugerencias para la posible consolidación o eliminación de reglas específicas para cumplir con su intención, sino que también comprueba si hay anomalías, como sombras, redundancias, generalizaciones, correlaciones y consolidaciones en la base de reglas.

Use analizador de políticas para añadir u optimizar la base de reglas de políticas de seguridad.

- **Antes de añadir una nueva regla**: compruebe si es necesario añadir nuevas reglas. El analizador de políticas, Policy Analyzer, recomienda la mejor manera de cambiar las reglas de políticas de seguridad existentes para cumplir con sus requisitos sin añadir otra regla, si es posible.
- **Optimice su base de reglas existente**: vea dónde puede actualizar sus reglas para minimizar la sobrecarga y eliminar conflictos, y también para asegurarse de que la aplicación del tráfico se alinee con la intención de la base de reglas de su política de seguridad.

Analice las reglas de la política de seguridad antes y después de confirmar los cambios.

- **Análisis de políticas previas al cambio**: le permite evaluar el impacto de una nueva regla y analizar la intención de las nuevas reglas con respecto a las reglas que ya existen para recomendar la mejor manera de cumplir con la intención.
- **Análisis de políticas posteriores al cambio**: le permite limpiar la base de reglas existente identificando sombras, redundancias y otras anomalías que se han acumulado a lo largo del tiempo.

Consulte el Analizador de políticas para obtener más información.

Gestionar: Optimizador de políticas

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)* • NGFW, incluidos los financiados por Créditos de NGFW de software	❑ Al menos una de estas licencias es necesaria para gestionar su configuración con Strata Cloud Manager; para la gestión unificada de NGFWs y Prisma Access, necesitará ambas: ❑ Prisma Access: licencia ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager dependen de la(s) licencia(s) que esté usando.

Pruebe Policy Optimizer mientras esté disponible para acceso anticipado. Si está interesado en seguir usando esta función más allá del período de acceso anticipado, póngase en contacto con su equipo de cuentas.

Las reglas que son demasiado generales introducen lagunas de seguridad porque permiten aplicaciones que no están en uso en su red. El optimizador de políticas le permite convertir estas reglas excesivamente permisivas en reglas más específicas y enfocadas que solo permiten a las aplicaciones que está utilizando.

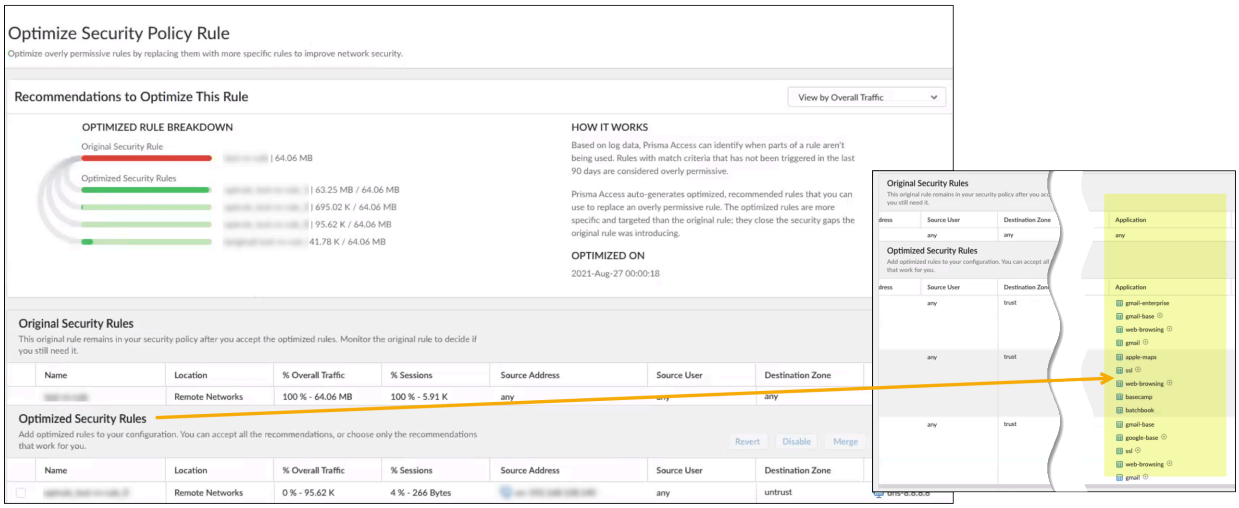
Solo las reglas creadas hace más de 90 días en el pasado se tienen en cuenta para la optimización de políticas.

Cómo funciona

Strata Cloud Manager analiza los datos de los logs y categoriza las reglas como demasiado permisivas cuando permiten **any (cualquier)** tráfico de la aplicación y las reglas deben tener al menos 90 días de antigüedad. Estas reglas pueden introducir lagunas de seguridad, si permiten tráfico que no es necesario para el uso empresarial.

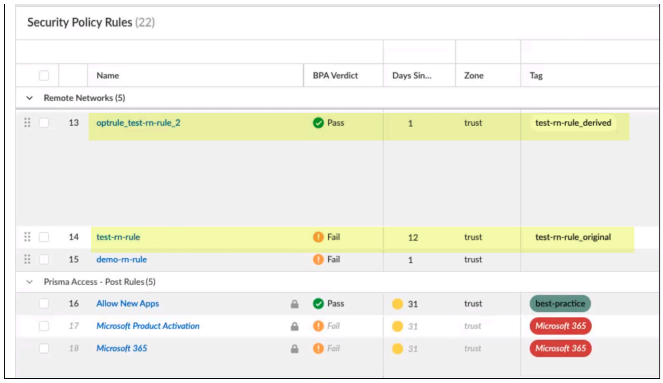
En el caso de las reglas identificadas como demasiado permisivas, Strata Cloud Manager genera automáticamente recomendaciones que puede aceptar para optimizar la regla. Las nuevas reglas recomendadas son más específicas y precisas que la regla original; permiten explícitamente solo las aplicaciones que se han detectado en su red en los últimos 90 días.

Seleccione una regla demasiado permisiva para revisar, ajustar y aceptar recomendaciones de optimización. La sustitución de estas reglas por las reglas recomendadas más específicas refuerza la posición de seguridad.



Al aceptar recomendaciones para optimizar una regla, no se quita la regla original. La regla original permanece en la lista debajo de las nuevas reglas de la política de seguridad; esto es para que pueda supervisar la regla y eliminarla cuando esté seguro de que no es necesaria.

Tanto la regla original como las reglas optimizadas están etiquetadas para que pueda identificarlas fácilmente en su política de seguridad:



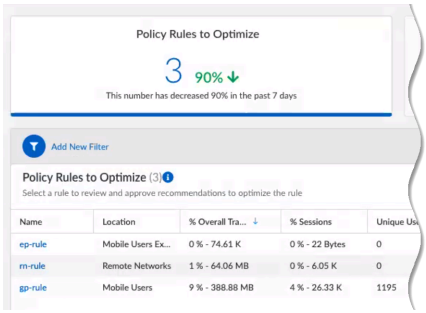
Optimizar una regla

STEP 1 | Visite **Config Cleanup (Limpieza de configuración)** para ver si hay reglas que pueda optimizar.

Vaya a **Manage (Gestionar)** > **Security Posture (Postura de seguridad)** > **Policy Optimizer (Optimizador de políticas)**.

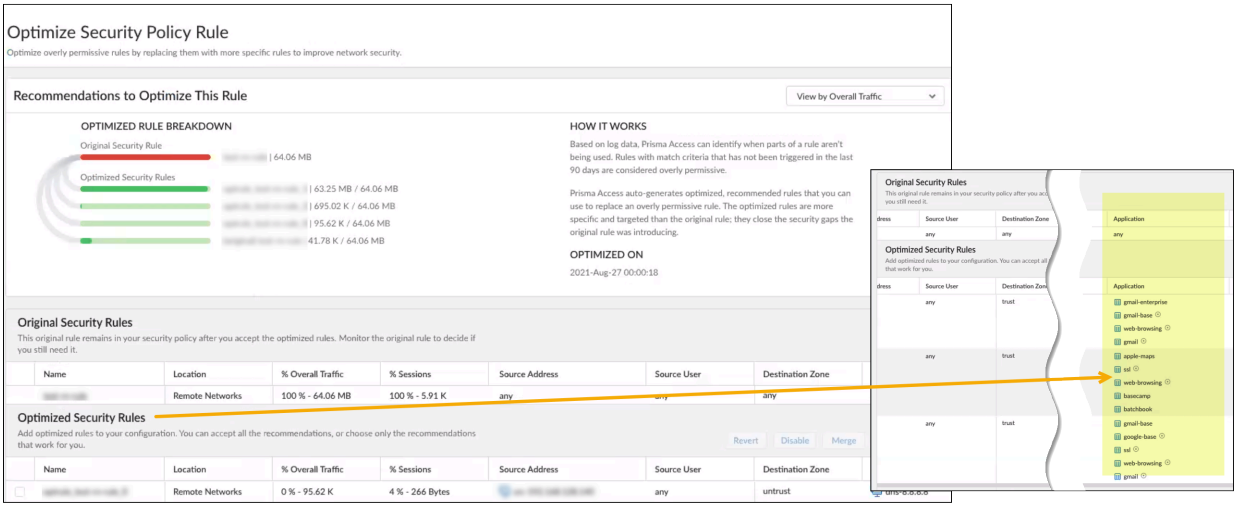
STEP 2 | Revise las reglas demasiado permisivas y elija una regla para ver las recomendaciones de optimización.

Si hay varias reglas demasiado permisivas, concéntrese en optimizar las reglas que afectan más al tráfico; Esto le dará las ganancias más significativas a la hora de fortalecer su postura de seguridad.



STEP 3 | Revise las reglas recomendadas y optimizadas.

Puede ver la cantidad de tráfico de la regla original que cubrirá cada nueva regla. Tenga en cuenta las aplicaciones específicas que aplica cada nueva regla.



STEP 4 | Acepte algunas o todas las recomendaciones de reglas.

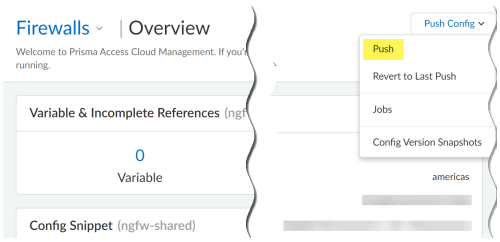
Al aceptar las nuevas reglas optimizadas, estas se añaden a las reglas en la base de reglas. Todavía no estarán activas; que sucederá en el siguiente paso cuando elija **Push Config (Enviar la configuración)** a Prisma Access.

Accept All (Aceptar todo) acepta las reglas recomendadas tal como están. También puede realizar cambios antes de aceptar las reglas optimizadas:

- Eliminar una regla de la optimización. Añada esta regla a una lista de reglas que desee excluir de la optimización (esta vez y en adelante).
- Deshabilitar una regla optimizada. Esto significa que no acepta esta regla y no se añadirá a la base de reglas.
- Revierte los cambios que haya realizado. De este modo, se deshacen las ediciones que haya realizado y se revierten las reglas a las recomendaciones.
- Reglas de combinación. Puede decidir hacer esto si encuentra que algunas de las reglas recomendadas son similar.

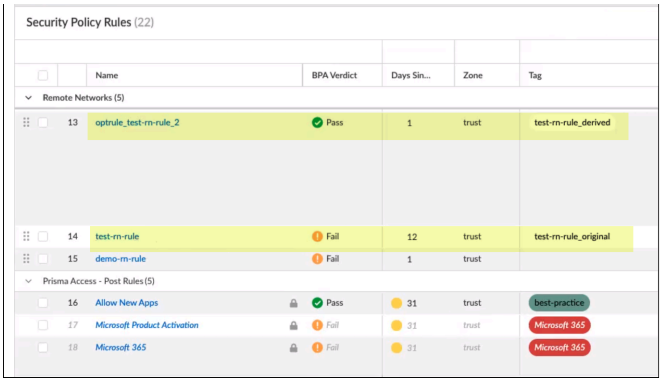
Después de aceptar las reglas optimizadas, se le pedirá que haga lo siguiente: **Update Rulebase (Actualizar la base de reglas)**. Cuando acepta, las reglas optimizadas se añaden a su política de seguridad. Sin embargo, aún no se están aplicando al tráfico.

STEP 5 | Deberá **Push Config (Enviar configuración)** para enviar las actualizaciones de configuración a Prisma Access y comenzar a aplicar las reglas optimizadas.



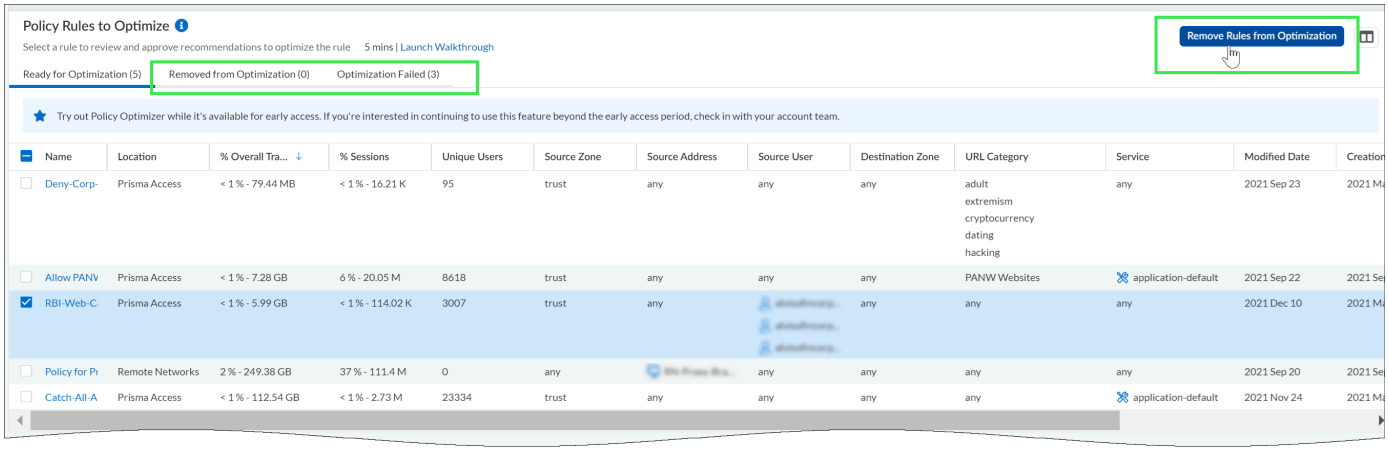
STEP 6 | Supervise la regla original hasta que esté seguro de que no la necesita.

Las reglas originales y excesivamente permisivas permanecen en su política de seguridad; se enumeran debajo de las reglas optimizadas en su base de reglas y están etiquetadas para que pueda identificarlas fácilmente. El nombre de la etiqueta anexa _original al nombre de la regla (por ejemplo, nombre-regla-seguridad_original).



Excluir una regla de la optimización

Traslade una regla a la lista **Excluidas de la optimización** y Prisma Access no la optimizará. La configuración de las reglas permanece tal cual.

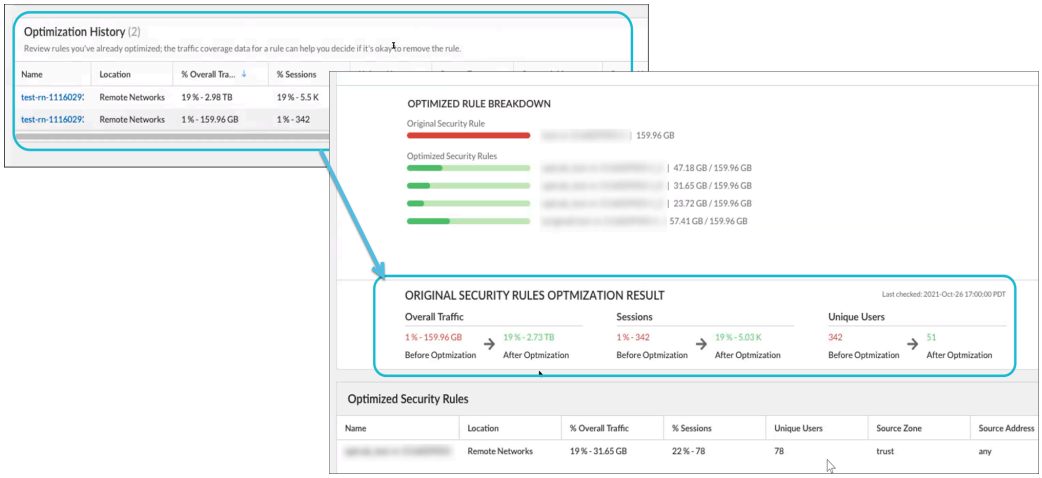


Asegúrese de **Push Config (Enviar configuración)** después de mover una regla a la lista de exclusión; después de enviar la configuración, la regla puede tardar hasta 24 horas en aparecer en la lista. Siempre puede optar por volver a añadir la regla a la lista de optimización más adelante.

Realizar seguimiento de los resultados de optimización

Policy Optimizer muestra un historial de las reglas de seguridad que ha optimizado. Los datos históricos incluyen los resultados de la optimización: compare la cobertura de tráfico de la regla original con las reglas optimizadas.

Los datos que ve para **Policy Optimizer History (Historial del optimizador de políticas)** es de los últimos 30 días. Si una regla original (una regla que usted optimizó) no recibe visitas durante seis meses, se quita del historial del optimizador de políticas y, en su lugar, se clasifica como un Regla de políticas con cero coincidencias.



Gestionar: Limpieza de la configuración

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)* • NGFW, incluidos los financiados por Créditos de NGFW de software	❑ Al menos una de estas licencias es necesaria para gestionar su configuración con Strata Cloud Manager; para la gestión unificada de NGFWs y Prisma Access, necesitará ambas: ❑ Prisma Access: licencia ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager dependen de la(s) licencia(s) que esté usando.

Utilice la Limpieza de la configuración para identificar y eliminar objetos de configuración y reglas de políticas no utilizados de la configuración de Strata Cloud Manager. Eliminar objetos de configuración no utilizados facilita la gestión del cortafuegos al eliminar el desorden y preservar solo los objetos de configuración necesarios para la aplicación de la seguridad.

STEP 1 | Inicie sesión en Strata Cloud Manager.

STEP 2 | Seleccione **Manage (Gestionar)** > **Security Posture (Postura de seguridad)** > **Config Cleanup (Limpieza de la configuración)**.

STEP 3 | Seleccione los objetos y las reglas de políticas no utilizados en toda la configuración de Strata Cloud Manager durante los últimos 6 meses.

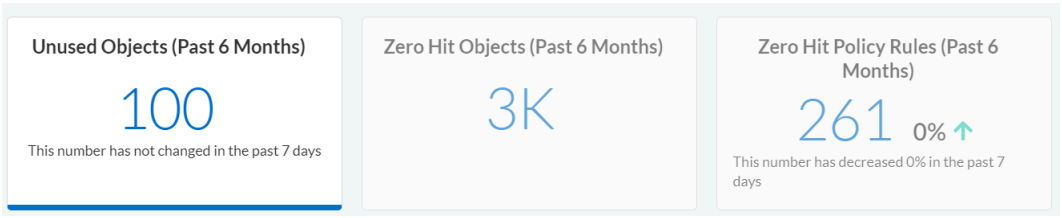
- **Policy Rules to Optimize (Reglas de políticas para optimizar)**: haga clic para revisar las reglas de políticas que son reglas excesivamente permisivas, para convertirlas en reglas más específicas y centradas que solo permitan las aplicaciones que usted está utilizando.
- **Unused Objects (Past 6 Months) [Objetos no utilizados (últimos 6 meses)]**: todos los objetos de configuración que no se utilizaron en ninguna regla de configuración o políticas en los últimos 6 meses.
- **Zero Hit Objects (Past 6 Months) [Objetos con cero coincidencias (últimos 6 meses)]**: reglas de políticas con objetos de configuración donde el objeto de configuración de la regla de políticas recibe cero coincidencias.

  Los objetos de configuración enumerados aquí han recibido cero resultados solo en las reglas de políticas a las que están asociadas. Su uso podría recibir coincidencias en las otras reglas de política en las que se utilizan.
- **Zero Hit Rules (Past 6 Months) [Reglas de cero coincidencias (últimos 6 meses)]**: todas las reglas de política que no han tenido coincidencias de tráfico en los últimos 6 meses.

STEP 4 | Aplique filtros adicionales para orientar objetos y reglas de políticas no utilizados específicos.

Add New Filter (Añadir filtro nuevo) es compatible con **Unused Objects (Past 6 Months [Objetos no utilizados (últimos 6 meses)]** y **Zero Hit Policy Rules (Past 6 Months) [Reglas de la política con cero coincidencias (últimos 6 meses)]**.

- **Unused Objects (Past 6 Months) [Objetos no utilizados (últimos 6 meses)]**: puede filtrar y **Delete (Eliminar)** objetos no utilizados en función de:
  - **Name (Nombre)**: busque y seleccione un nombre de objeto de configuración específico.
  - **Ubicación**: alcance de configuración en el que se creó el nombre del objeto de configuración.
  - **Object Type (Tipo de objeto)**: tipo de objeto de configuración.
  - **Days Unused (Días sin usar)**: el número de días que el objeto de configuración se usó.
    - **< 50**: menos de 50 días sin usar.
    - **>= 50, <=100**: entre 50 y 100 días sin usar.
    - **< 50**: más de 100 días sin usar.
- **Zero Hit Policy Rules (Past 6 Months) [Reglas de políticas con cero coincidencias (últimos 6 meses)]**: puede filtrar y **Enable (Habilitar)**, **Disable (Deshabilitar)** o **Delete (Eliminar)** reglas de políticas con cero coincidencias según el **Name (Nombre)**, los **Days with Zero Hits (Días con cero coincidencias)** o cualquiera de los datos de `origen` y `destino`.



Gestionar: Configuración de la postura de seguridad

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW, incluidos los financiados por Créditos de NGFW de software • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager depende de qué licencia(s) esté usando.

Strata Cloud Manager aprovecha un conjunto de Comprobaciones de prácticas recomendadas predefinidas que se alinean con los controles de ciberseguridad estándar específicos de la industria, como CIS (Centro de Seguridad de Internet) y NIST (Instituto Nacional de Estándares y Tecnología) y las comprobaciones personalizadas que crea en función de las necesidades específicas de su organización. Estas comprobaciones evalúan las configuraciones y los ajustes dentro de la infraestructura de nube, identificando desviaciones de las prácticas recomendadas o requisitos de cumplimiento.

Las comprobaciones de postura de seguridad en Strata Cloud Manager abarcan una serie de dominios de seguridad, incluida la seguridad de la red, la protección de datos y la gestión de identidades y accesos. Estas comprobaciones evalúan las reglas del cortafuegos, el cifrado, los mecanismos de autenticación y la integridad general de las configuraciones.

Cuando su configuración detecta desviaciones, Strata Cloud Manager proporciona información útil y recomendaciones de corrección, e incluso puede automatizar algunas partes del proceso para corregir configuraciones incorrectas y ajustes que no cumplen con normativas para ayudarle a mantener un entorno de nube seguro y en conformidad, con la mínima intervención manual.

La configuración de postura de seguridad reúne la funcionalidad de las páginas de configuración de comprobación de seguridad de AIOps y Strata Cloud Manager.

Seleccione **Manage (Gestionar)** > **Security Posture (Postura de seguridad)** > **Settings (Configuración)** para ver, gestionar y personalizar las comprobaciones de postura de seguridad para su implementación a fin de maximizar las recomendaciones pertinentes.

- **Comprobaciones de seguridad**: lista de las comprobaciones de prácticas recomendadas que se utilizan para evaluar su configuración.

  Su configuración se compara con estas comprobaciones para evaluar la postura de seguridad de sus dispositivos y generar alertas de seguridad. Puede realizar las siguientes acciones para gestionar estas comprobaciones en función de su entorno:

  1. Establecer el nivel de gravedad de sus comprobaciones personalizadas para identificar las comprobaciones más críticas para su implementación.

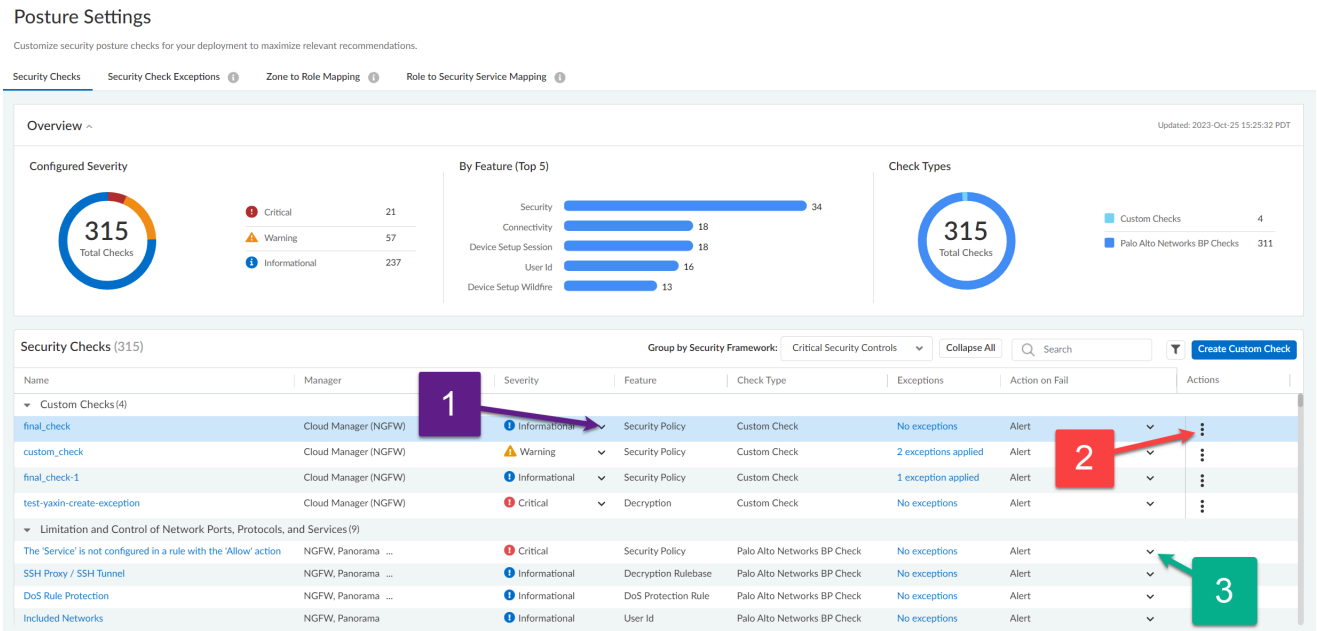
     Puede cambiar el nivel de gravedad de sus comprobaciones personalizadas, pero los niveles de gravedad de las comprobaciones de prácticas recomendadas de Palo Alto Networks son fijos y no se pueden cambiar.

  2. Cree y elimine sus propias comprobaciones personalizadas, duplique y edite las comprobaciones existentes para crear otros nuevos, y haga excepciones especiales para las comprobaciones que no desee que se apliquen a partes de su implementación.

     Como parte de la implementación inicial de estas comprobaciones, puede duplicar las comprobaciones que se encuentran en el marco de comprobación personalizado.

  3. Establezca la respuesta cuando una comprobación falle.
     - **Alerta** (predeterminada): emite una alerta por la comprobación fallida.
     - **Block (Bloquear)**: detenga las posibles configuraciones erróneas antes de que entren en su implementación. Bloquear puede significar cualquiera de los siguientes dependiendo de cómo lo gestione:
       - **Comprobaciones en línea de Strata Cloud Manager**: le impide enviar o impulsar una configuración no conforme, pero no le impide guardar su configuración localmente.
       - **Comprobaciones en línea en tiempo real* de Strata Cloud Manager**: le impide incluso guardar una configuración no conforme.
       - **Gestionado por Panorama****: le impide enviar una configuración no conforme a Panorama, pero no le impide guardarla en la configuración candidata de Panorama.
       - Gestión de interfaz web, API o CLI de PAN-OS: el bloqueo no tiene ningún efecto coercitivo en las configuraciones que no se gestionan en la nube ni en Panorama.

       - **Debido a su complejidad lógica, algunas comprobaciones en línea se realizan de forma asíncrona en un horario fijo pero no en tiempo real. Un fallo de una comprobación en tiempo real en su configuración le impedirá guardar esa configuración, incluso localmente.*
       - ***El Complemento Panorama CloudConnector es necesario para hacer cumplir la acción de confirmación de bloque en Panorama.*



- **Excepciones de comprobación de seguridad**

  Desactive las comprobaciones individuales de dispositivos o grupos de dispositivos que especifique.
- **Asignación de zona a un rol**

  Asigne las zonas en NGFW a roles para obtener recomendaciones personalizadas.
- **Asignación de servicios de rol a seguridad**

  Gestionar los servicios de seguridad necesarios para el tráfico entre zonas y funciones en todos los NGFW.

Crear una comprobación personalizada

Cree su propia comprobación personalizada a partir de una comprobación existente. Alternativamente, vaya al paso n.º 4 para crear una comprobación personalizada desde cero.

STEP 1 | Seleccione **Manage (Gestionar)** > **Security Posture (Postura de seguridad)** > **Settings (Configuración)**.

STEP 2 | Identifica la comprobación que quiere duplicar y proceda a **Clone (Duplicar)**.

STEP 3 | Deberá **Edit (Editar)** la comprobación que duplicó y saltar al paso n-º 5 para realizar sus cambios.

STEP 4 | Vaya a **Manage (Gestionar)** > **Security Posture (Postura de seguridad)** > **Settings (Configuración)** y seleccione **Create Custom Check (Crear comprobación personalizada)**.

STEP 5 | Especifique la **Información general** para su comprobación. Su comprobación personalizada debe tener un **Nombre** y una **Descripción**, pero también debe añadir una **Recomendación** y un **Fundamento** para que su comprobación pueda ayudar a otros a entender la intención y las prácticas recomendadas de su comprobación personalizada.

STEP 6 | Opcional Seleccione un **Tipo de objeto**: la sección de su configuración para la que está creando una comprobación que determina qué **Propiedades de regla** puede elegir al crear su comprobación.

STEP 7 | Utilice el **Generador de lógica** para su comprobación personalizada.

1. **Añadir expresión**: una única línea lógica que describe los criterios de coincidencia para una configuración.

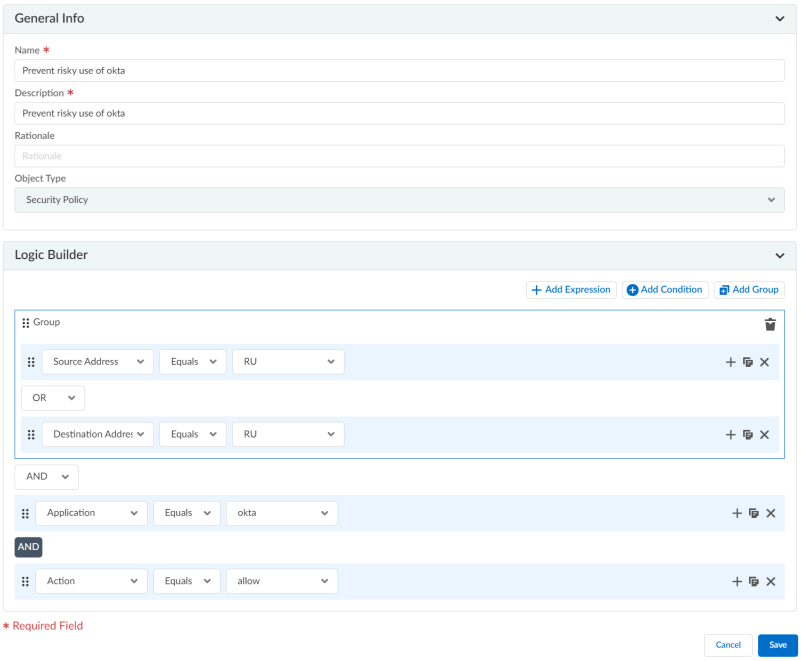
Propiedades de regla para coincidir	Operador de coincidencia	Criterios específicos
• Nombre general, descripción, posición y horario • Fuentes: zonas, direcciones, usuarios • Destinos: zonas y direcciones • Aplicaciones, servicios y URL • Acciones e inspección avanzada	• Es • No es • Está vacío • No está vacío • Comienza con • Termina con • Contiene • Mayor que • dentro • Es igual o mayor que • Es igual o menor que • Menos de • Igual • No es igual • No contiene • Todos • Algunos • Ninguno	[Campo de texto]

2. **Añadir condición**: utilice operadores lógicos (como AND, OR, IF, THEN, ELSE y ELSE IF) para conectar o combinar expresiones, condiciones adicionales y grupos.

3. **Añadir grupo**: cree un conjunto de expresiones, condiciones o ambas. Este grupo, tomado en conjunto, resulta en una condición Verdadera o Falsa.

   - *Añade una nueva expresión o condición*
   - *duplica una expresión o condición*
   - *Elimina una expresión o condición*

   La expresión en este ejemplo emite una advertencia cuando ve reglas de política que permiten el tráfico Okta desde y hacia direcciones IP rusas. El ejemplo simplemente ilustra cómo funciona el constructor de lógica y no pretende ser una recomendación.



STEP 8 | Seleccione **Save (Guardar)** para guardar su comprobación.

Gestione sus comprobaciones

Puede realizar cualquiera de las siguientes **Actions (Acciones)** en sus comprobaciones de seguridad:

- **Duplicar***: crea una copia de un comprobación.
- **Editar****: realice cambios en una comprobación personalizada existente.
- **Eliminar****: elimina una comprobación personalizada que ha creado.

Seleccione las comprobaciones en las que desea tomar medidas y seleccione la acción apropiada.

- **Puede duplicar solo un comprobación a la vez.*
- ***Solo puede editar o eliminar comprobaciones personalizadas.*
- *Es posible que necesite obtener permiso de un administrador para editar una comprobación personalizada.*

Crear una excepción para una comprobación

Cuando sea necesario, puede restringir dónde se aplican las comprobaciones en su implementación.

STEP 1 | Seleccione **Manage (Gestionar)** > **Security Posture (Postura de seguridad)** > **Settings (Configuración)** > **Security Check Exceptions (Excepciones de comprobación de seguridad)** y **Create Security Check Exception (Crear excepción de comprobación de seguridad)**.

De forma alternativa, seleccione **Manage (Gestionar)** > **Security Posture (Postura de seguridad)** > **Settings (Configuración)** e identifique la marca que desea excluir y selecciónela [columna **Exceptions (Excepciones)**].

STEP 2 | Especifique la información necesaria para **Crear regla de excepción** para su comprobación. Proporcione un nombre, una razón y condiciones para su excepción.

*La función **Security Check Exception (Excepción de comprobación de seguridad)** solo es aplicable actualmente a las alertas y a los paneles de **Best Practices (Prácticas recomendadas)** y **Security Posture Insights (Información sobre la postura de seguridad)**.*

STEP 3 | Opcional Añada un **Número de ticket** o una **Descripción** para su excepción para ayudar a otros a entender la intención y la historia detrás de su excepción.

STEP 4 | **Save (Guardar)** su excepción.

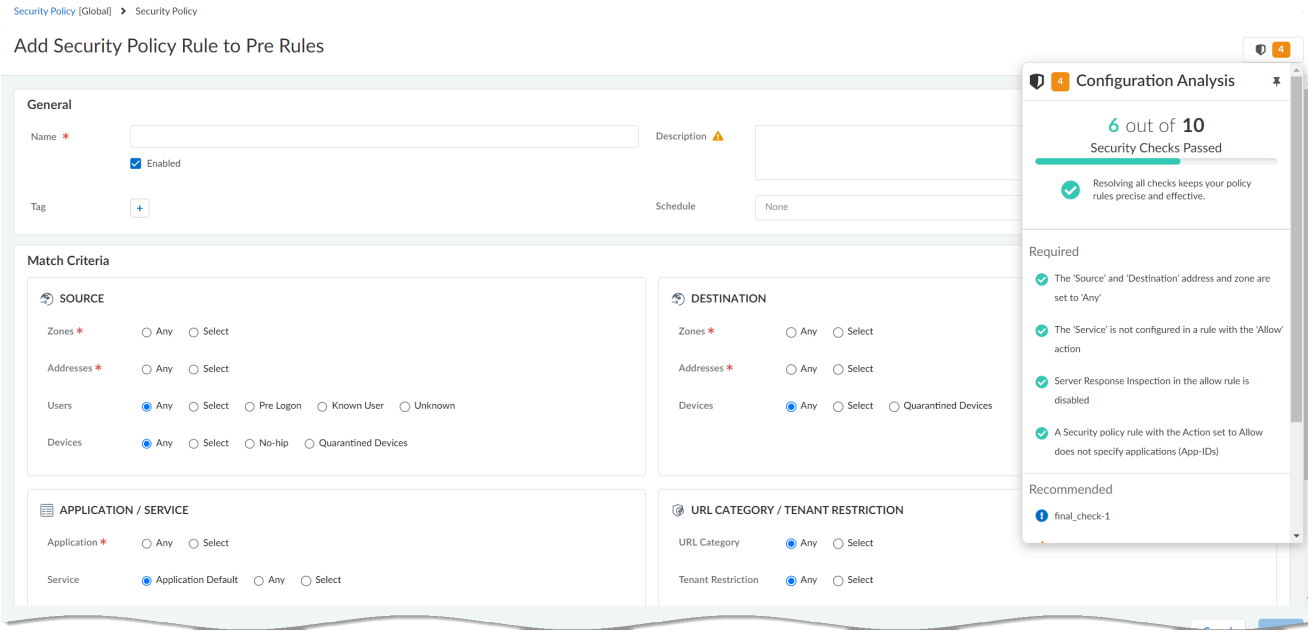
Sus comprobaciones en funcionamiento

Las comprobaciones a nivel de campo le muestran dónde su configuración no se alinea con las prácticas recomendadas o la comprobación personalizada. Los controles proporcionan orientación sobre las prácticas recomendadas en línea, para que pueda tomar medidas inmediatamente.

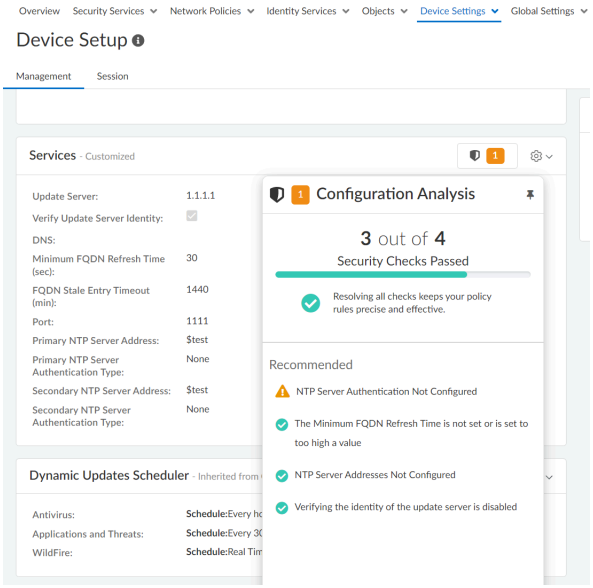
También puede ver y gestionar los controles de seguridad justo donde se encuentra.

- Cree y gestione sus reglas de política: las reglas de política de seguridad le permiten hacer cumplir las reglas y tomar medidas, y pueden ser tan generales o específicas como sea necesario. [**Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access**

(NGFW y Prisma Access) > Security Services (Servicios de seguridad) > Security Policy (Política de seguridad)]



- Dispositivos de seguridad: configure la ruta de servicio, la configuración de conexión, los servicios permitidos y la configuración de acceso administrativo para las interfaces de gestión y auxiliares de sus cortafuegos. [**Manage (Gestionar) > Configuration (Configuración) > NGFW and Prisma Access (NGFW y Prisma Access) > Device Settings (Configuración de dispositivos) > Device Setup (Configuración de dispositivo)**]



Si la configuración que intenta guardar no supera sus criterios para pasar, tendrá la opción de remediar el problema o anular* la advertencia y guardar los cambios de todos modos.

- **El permiso de anulación se rige por los controles de acceso basados en roles (RBAC) y debe estar habilitado para que aparezca esta opción. Las acciones relacionadas con anulaciones, comprobaciones personalizadas y excepciones se registran en los logs de auditoría:* ***Incidents and Alerts (Incidentes y alertas)Log Viewer (Visor de logs)Audit (log type) [Auditoría (tipo de log)]****.*
- *Todo lo que hace con comprobaciones personalizadas, anulaciones y excepciones se registra en Auditoría:* ***Incidents and Alerts (Incidentes y alertas)*** *>* ***Log Viewer (Visor de logs)*** *>* ***Audit (log type) [Auditoría (Tipo de log)]****.*

Gestionar: Control de acceso

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)* • NGFW, incluidos los financiados por Créditos de NGFW de software	❑ Se necesita al menos una de estas licencias para gestionar su configuración con Strata Cloud Manager; para la gestión unificada de NGFW y Prisma Access, necesitará ambos: ❑ Prisma Access licencia ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro ❑ Créditos de NGFW de software *(para cortafuegos NGFW de software VM-Series)* → Las características y capacidades disponibles para usted en Strata Cloud Manager dependiendo de qué licencia(s) está utilizando.

El Control de acceso basado en funciones (Role-based access control, RBAC) le permite definir los privilegios y las responsabilidades correspondientes de los usuarios administrativos (administradores). Cada administrador debe tener una cuenta de usuario que especifique un rol y un método de autenticación. Gestión en la nube de Prisma Access implementa RBAC personalizado para permitirle gestionar roles o permisos específicos y asignar derechos de acceso a usuarios administrativos. Con RBAC, puede gestionar usuarios y su acceso a varios recursos dentro de la Gestión de la nube.

*RBAC no es compatible con SaaS Security Inline y las amenazas de comportamiento. Todas las pestañas en **Discovered Apps (Aplicaciones descubiertas)** y **Behavior Threats (Amenazas de comportamiento)** son visibles para todos los usuarios, independientemente de sus roles asignados.*

MÁS RECURSOS DE RBAC

- ¿Quién puede utilizar los servicios comunes? Identidad y acceso: Gestionado en la nube Prisma Access
- ¿Qué es el Flujo general de servicios comunes? Identidad y acceso
- Acerca de los roles y permisos a través de Servicios comunes

Roles de administrador

Un usuario en Prisma Access es alguien a quien se le han asignado privilegios administrativos, y un rol define el tipo de acceso que el administrador tiene en el servicio. Cuando se asigna un rol, se especifica el grupo de permisos y los grupos de cuentas que el administrador puede gestionar. El hub tiene los siguientes grupos de permisos integrados para los administradores que utilizan Prisma Access.

- **Administrador de aplicaciones**: tiene acceso completo a la aplicación dada, incluidas todas las instancias que se agreguen a la aplicación en el futuro. Los administradores de aplicaciones puede asignar funciones para instancias de aplicaciones y también pueden activar instancias de aplicaciones específicas para dicha aplicación.
- **Administrador de instancias**: tiene acceso completo a la instancia de la aplicación para la que se asigna este rol. El administrador de instancias también puede hacer que otros usuarios sean un administrador de instancia para la instancia de la aplicación. Si la aplicación tiene roles predefinidos o personalizados, el administrador de instancias puede asignar esos roles a otros usuarios.
- **Superlector**: puede ver todos los elementos de configuración, logs y configuraciones. Los superlectores no pueden realizar cambios en otros ajustes.
- **Administrador de auditoría**: solo puede ver y gestionar logs y configuraciones de logs. Los administradores de auditoría no pueden realizar cambios en otras configuraciones.
- **Administrador de cifrado**: puede ver logs y gestionar configuraciones criptográficas como IKE, IPSec, gestión de claves maestras y configuración de certificados. Los administradores de cifrado no pueden ver ni realizar cambios en otras configuraciones.
- **Administrador de seguridad**: puede ver logs y gestionar todas las configuraciones, excepto la configuración criptográfica que está disponible para el rol de administrador de cifrado.
- **Administrador de seguridad web**: solo puede ver los elementos de configuración relacionados con la seguridad web.
- **Administrador de prevención de pérdida de datos**: puede acceder a la configuración de Enterprise DLP, pero no puede enviar cambios de configuración a Prisma Access.
- **Administrador de seguridad de datos**: puede acceder a los controles de seguridad de Enterprise DLP y SaaS, pero no puede enviar cambios de configuración a Prisma Access.
- **Administrador de SaaS**: puede acceder a la configuración de seguridad de SaaS, pero no puede enviar cambios de configuración a Prisma Access.

Control de acceso personalizado basado en roles: configuración

A continuación, se explica cómo usar un rol predefinido o crear un rol personalizado, asignar un rol a un usuario y gestionar el ámbito del usuario cuando accede a la aplicación de Prisma Access.

STEP 1 | Añada un rol personalizado a través de Servicios comunes

Si necesita un control de acceso más granular que los roles predefinidos proporcionan, puede agregar roles personalizados para definir qué permisos se aplican a los usuarios. Al igual que los roles predefinidos, los roles personalizados son un conjunto de permisos y conjuntos de permisos. A diferencia de los roles predefinidos, cada rol personalizado solo se puede asignar a los usuarios de la jerarquía en el Grupo de servicios para inquilinos (TSG) donde se define. Esto evita conflictos de nombres entre roles personalizados con nombres similares definidos por diferentes clientes.

Si añade un rol personalizado en el nivel superior (nivel primario) de la jerarquía, ese rol se asigna a los inquilinos anidados debajo para que el inquilino primario pueda gestionar los inquilinos secundarios.

STEP 2 | Añada acceso de usuario a través de Servicios comunes

Los Servicios comunes: Acceso e identidad le permite añadir acceso de usuario a la plataforma, así como a los inquilinos que ha creado.

STEP 3 | Asigne un rol predefinido a un usuario inquilino o a una cuenta de servicio a través de Servicios comunes

Si ya ha añadido usuarios y desea añadir roles adicionales, también puede asignar un lote de roles predefinidos. Revisar información adicional acerca de los roles y permisos.

STEP 4 | Cree un nuevo ámbito en el archivo Prisma Access Interfaz de usuario de gestión en la nube

Prisma Access Gestión de la nube le permite (como administrador) asignar un ámbito de gestión a un usuario de gestión de la nube (no administrador) para asociar permisos basados en ámbitos, como carpetas y fragmentos de código.

Los permisos son acciones que están permitidas en el sistema. Los permisos representan un conjunto específico de llamadas a la interfaz de programación de aplicaciones (API) que se utilizan para leer, escribir y eliminar objetos dentro de los sistemas. Todos los permisos se agrupan en roles.

Gestionar: Gestión del alcance

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)* • NGFW, incluidos los financiados por Créditos de NGFW de software	❑ Al menos una de estas licencias es necesaria para gestionar su configuración con Strata Cloud Manager; para la gestión unificada de NGFWs y Prisma Access, necesitará ambas: ❑ Prisma Access: licencia ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager dependen de la(s) licencia(s) que esté usando.

Configure la gestión del alcance para aplicar un control de acceso personalizado basado en roles. Esto le permite especificar qué administradores de Strata Cloud Manager pueden acceder y modificar carpetas específicas, cortafuegos, implementaciones de Prisma Access y configuraciones de fragmentos. La definición de la gestión del ámbito para los administradores de la nube garantiza que no estén sobreaprovisionados y define los privilegios de acceso de lectura y escritura para las carpetas, cortafuegos, implementaciones de Prisma Access y configuraciones de fragmentos. Los Servicios comunes de varias plataformas y roles empresariales se utilizan para definir los privilegios de acceso de lectura y escritura para un administrador de Strata Cloud Manager.

La configuración de gestión del ámbito se define en todo el inquilino de Strata Cloud Manager. La gestión del ámbito no se puede definir para una carpeta específica, Prisma Accesso el alcance de configuración del cortafuegos.

Solo un administrador de gestión de la nube o un superusuario puede crear un objeto de alcance. El widget de Gestión de alcance no está disponible para usuarios con otros roles.

STEP 1 | Inicie sesión en Strata Cloud Manager.

STEP 2 | Seleccione **Manage (Gestionar)** > **Access Control (Control de acceso)** > **Scope Management (Gestión del alcance)**.

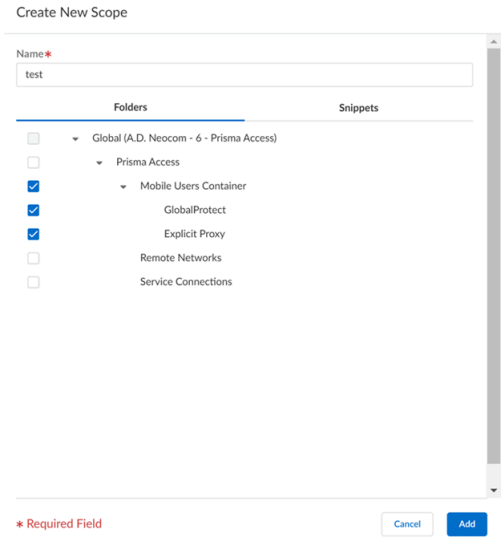
STEP 3 | **Crear nuevo alcance**.

STEP 4 | Defina la configuración de gestión de alcance.

Las configuraciones de gestión de alcance se etiquetan como un `Objeto de alcance`.

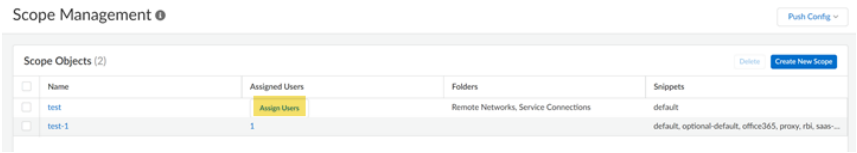
1. Introduzca un **Name (Nombre)** descriptivo.
2. Seleccione **Folders (Carpetas)** y verifique (habilite) las carpetas, cortafuegos e implementaciones de Prisma Access que desee incluir en el ámbito.

   La selección de un cortafuegos también incluye la carpeta a la que está asociado el cortafuegos seleccionado en la configuración de gestión del ámbito. Solo se incluye la carpeta asociada inmediatamente, y no la carpeta principal.
3. Seleccione **Snippets (Fragmentos)** y marque (habilite) los fragmentos que desea incluir.
4. **Add (Añadir)** el objeto de alcance.



STEP 5 | Aplique la configuración de gestión de alcance a los administradores de Strata Cloud Manager.

1. **Assign Users (Asignar usuarios)** al objeto de alcance que creó en el paso anterior.



2. Seleccione un **Role (Rol)** para el admin de Strata Cloud Manager: Por ejemplo, puede seleccionar Superusuario de MSP para un usuario que necesita acceso a todas las funciones de todos los inquilinos.

   El valor predeterminado es `None (Ninguna)`. Para obtener más información sobre los permisos de acceso de lectura y escritura para cada rol disponible, consulte las Distintas plataformas y roles empresariales para servicios comunes

   *Seleccione un administrador específico de Strata Cloud Manager y **Clear Role (Borrar función)** para quitar el rol de Servicios comunes asignado actualmente. Esto aplica de forma predeterminada el rol `Ninguno` al administrador.*

3. Para modificar un alcance existente para editar el nombre y añadir o quitar carpetas, seleccione el objeto del alcance, modifique el alcance según sea necesario y seleccione **Update (Actualizar)** el alcance.
4. Para modificar los usuarios asignados, añadir más usuarios o cambiar los usuarios, haga clic en **Assigned Users (Usuarios asignados)** y modifique según sea necesario, y luego elija **Close (Cerrar)** la ventana.

Gestionar: Restricciones de IP

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)* • NGFW, incluidos los financiados por Créditos de NGFW de software	❑ Al menos una de estas licencias es necesaria para gestionar su configuración con Strata Cloud Manager; para la gestión unificada de NGFWs y Prisma Access, necesitará ambas: ❑ Prisma Access: licencia ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro → Las características y capacidades disponibles para usted en Strata Cloud Manager dependen de la(s) licencia(s) que esté usando.

Especifique direcciones IP de confianza para los administradores de gestión de nube de Prisma Access. Solo los administradores que inician sesión desde estas direcciones IP de origen (y también que se autentican con éxito) pueden acceder a la gestión de la nube de Prisma Access.

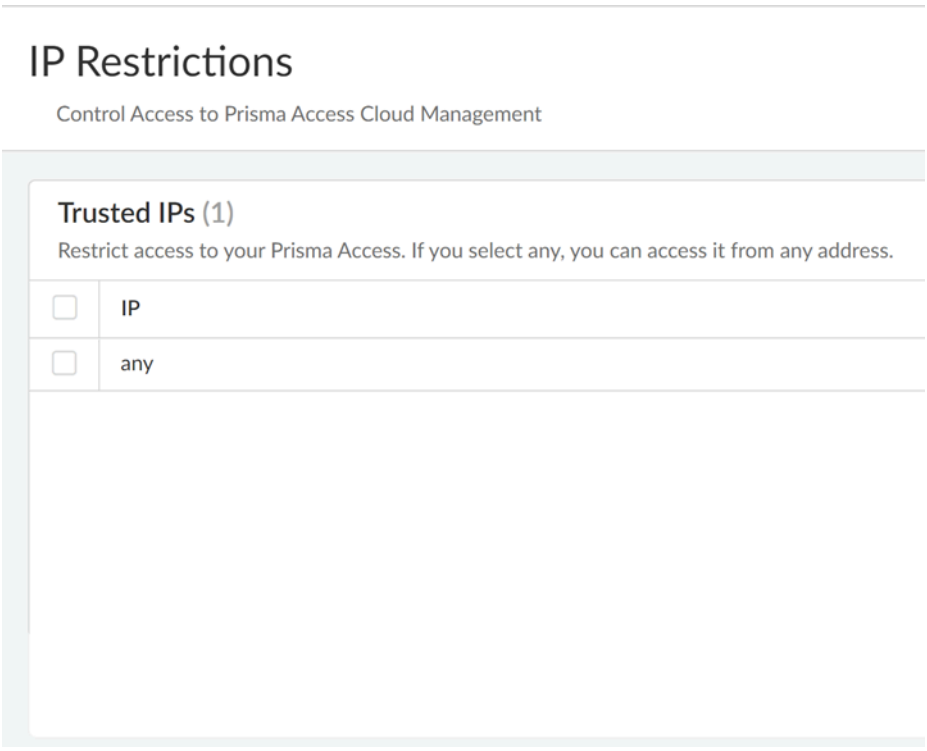
Las direcciones IP deben ser direcciones públicas. De forma predeterminada, no se aplica ninguna dirección de confianza [la lista se establece en **any (cualquiera)**].

Para empezar, vaya a **Manage (Gestionar)** > **Access Control (Control de acceso)** > **IP Restrictions (Restricciones IP)**.

Para restricciones IP, la dirección de subred no es compatible. Solo son compatibles direcciones IP y rango de direcciones IP. No especifique ninguna subred que se solape con las siguientes direcciones IP y subredes, porque Prisma Access reserva esas direcciones IP y subredes para su uso interno:

- 169.254.169.253 y 169.254.169.254
- 100.64.0.0/10
- 169.254.201.0/24
- 169.254.202.0/24

Recomendamos usar un grupo de direcciones IP compatible con RFC 1918 y RFC 6598. Aunque se admite el uso de direcciones IP (públicas) no compatibles con RFC 1918 y RFC 6598, no lo recomendamos debido a posibles conflictos con el espacio de direcciones IP públicas de Internet.



Flujos de trabajo: Strata Cloud Manager

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • NGFW (Managed by Strata Cloud Manager) • Prisma SD-WAN	Una o más de estas licencias, dependiendo del flujo de trabajo: ❑ Licencia de AIOps for NGFW Premium ❑ Licencia de Strata Logging Service, se requiere para el registro de logs ❑ Licencia de Prisma Access ❑ Prisma SD-WAN ❑ Licencia de Aislamiento remoto del navegador

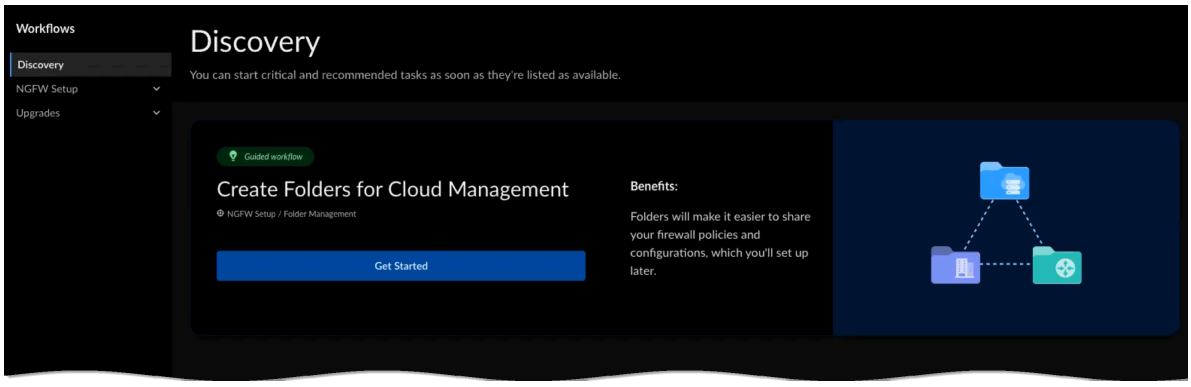
Cuando navegue por primera vez a sus flujos de trabajo, el panel **Descubrimiento** mostrará las acciones críticas y recomendadas que puede realizar para mejorar la postura de seguridad u optimizar la gestión de la configuración, tan pronto como estén disponibles para usted. Continúe aquí para configurar e incorporar usuarios móviles y redes remotas de NGFW y Prisma Access, y planificar actualizaciones de software para NGFW.

- Descubre las tareas de incorporación
- Configurar Prisma Access
- Configurar dispositivos NGFW
- Configurar Prisma SD-WAN
- Actualizaciones de software (NGFW)
- Actualizaciones de software (Prisma Access)

Flujos de trabajo: Descubrimiento

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • NGFW (Managed by Strata Cloud Manager) • Prisma SD-WAN	❑ Licencia de AIOps for NGFW Premium o licencia de Prisma Access

Descubrimiento es donde puede iniciar tareas críticas y recomendadas tan pronto como estén disponibles. Puede haber flujos de trabajo guiados o tareas que pueda completar por su cuenta. En este tema, le mostraremos cómo utilizar el flujo de trabajo guiado para crear su estructura de carpetas y asignarles dispositivos, de manera sencilla e intuitiva.



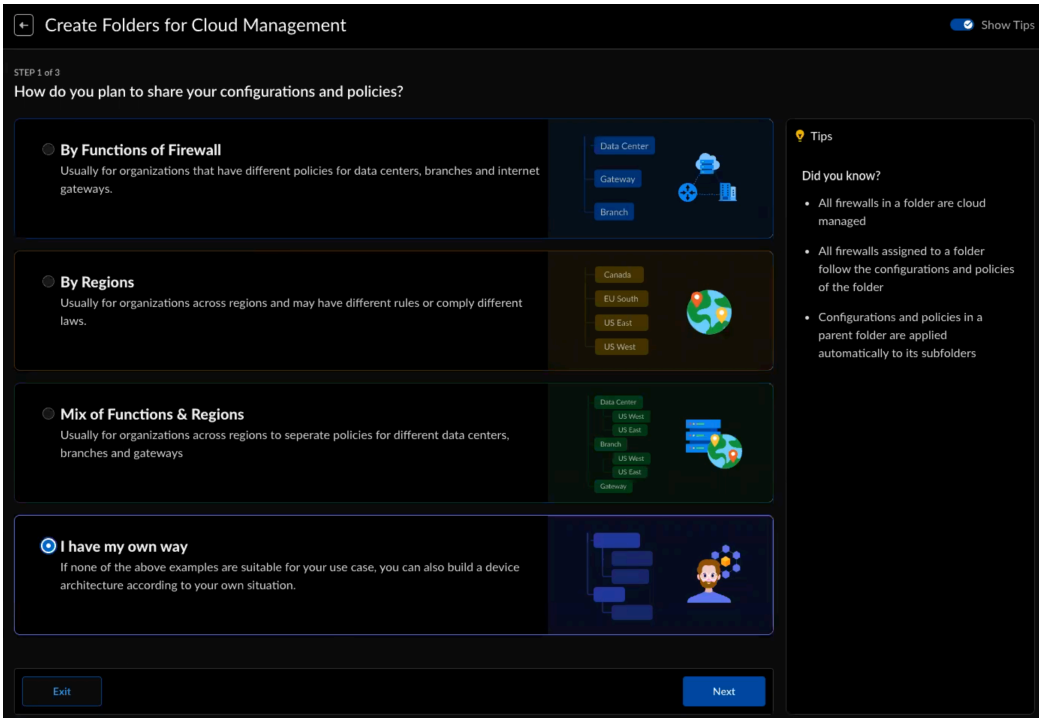
Siga estos pasos para crear carpetas para sus cortafuegos:

STEP 1 | Vaya a **Workflows (Flujos de trabajo)** > **Discovery (Descubrimiento)** y seleccione **Get Started (Empezar)**.

STEP 2 | Elija cómo desea compartir sus reglas y configuraciones de políticas.

- **Según las funciones del cortafuegos**: ¿su organización tiene diferentes políticas para centros de datos, sucursales y puertas de enlace de Internet? Esta podría ser la opción para usted.
- **Por región**: ¿Su organización abarca regiones que tienen reglas diferentes o cumplen con leyes diferentes? Considere esta opción.
- **Combinación de funciones y regiones**: ¿Desea su organización interregional separar políticas para diferentes centros de datos, sucursales y puertas de enlace de Internet? Prueba esta opción.
- **Tengo mi propia manera**: si ninguno de los ejemplos anteriores es adecuado para su caso de uso, también puede crear una arquitectura de dispositivo según su propia situación.

Para este ejemplo, elegiremos la opción **I have my own way (Tengo mi propia manera)**.

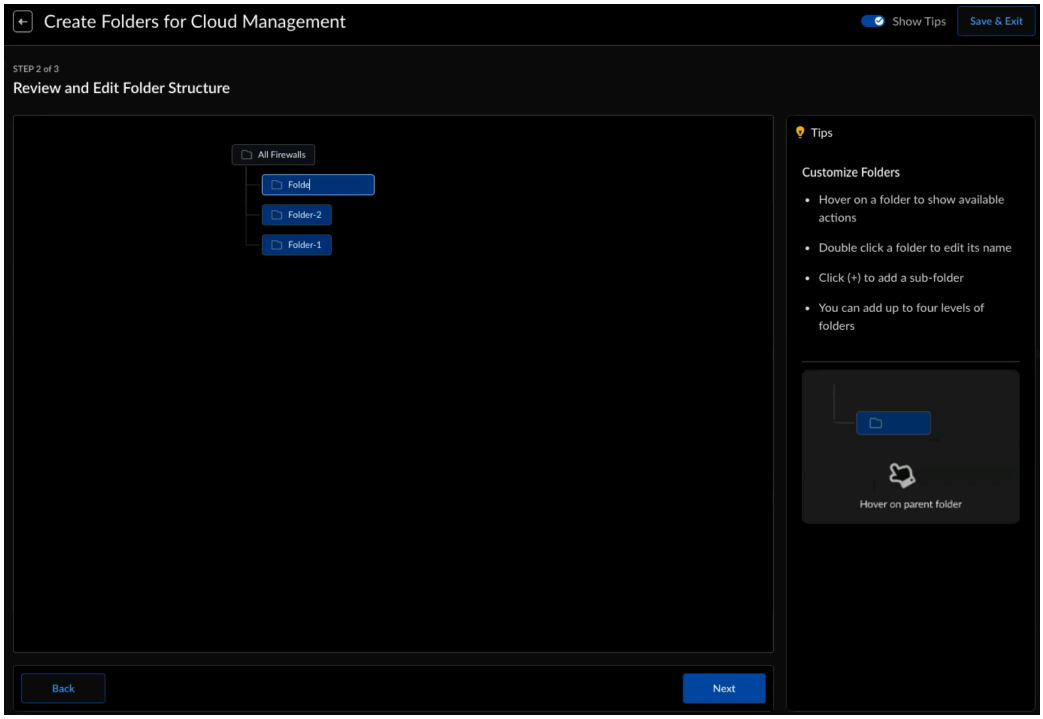


*Active **Mostrar sugerencias** para ver sugerencias de ayuda que le ayudarán a tomar una decisión informada.*

STEP 3 | Seleccione **Next (Siguiente)**para crear su estructura de carpetas.

STEP 4 | Utilice las siguientes acciones para crear su estructura de carpetas según la plantilla que seleccionó en el paso 1. Usted puede:

- **Add a new Folder (Añadir una nueva carpeta)**: pase el cursor sobre una carpeta para mostrar la opción para añadir una nueva carpeta. Haga clic en y luego ponga un nombre a su nueva carpeta.
- **Delete Folder (Eliminar carpeta)**: pase el cursor sobre una carpeta para mostrar la opción para eliminarla. Seleccione para eliminar la carpeta.
- **Rename Folder (Cambiar el nombre de la carpeta)**: haga doble clic en una carpeta para volver a escribir un nuevo nombre. Pulse la tecla Intro o haga clic fuera del campo de texto para que su nuevo nombre surta efecto.
- **Expand or Collapse (Expandir o contraer)** nodos de carpeta que tengan elementos secundarios.

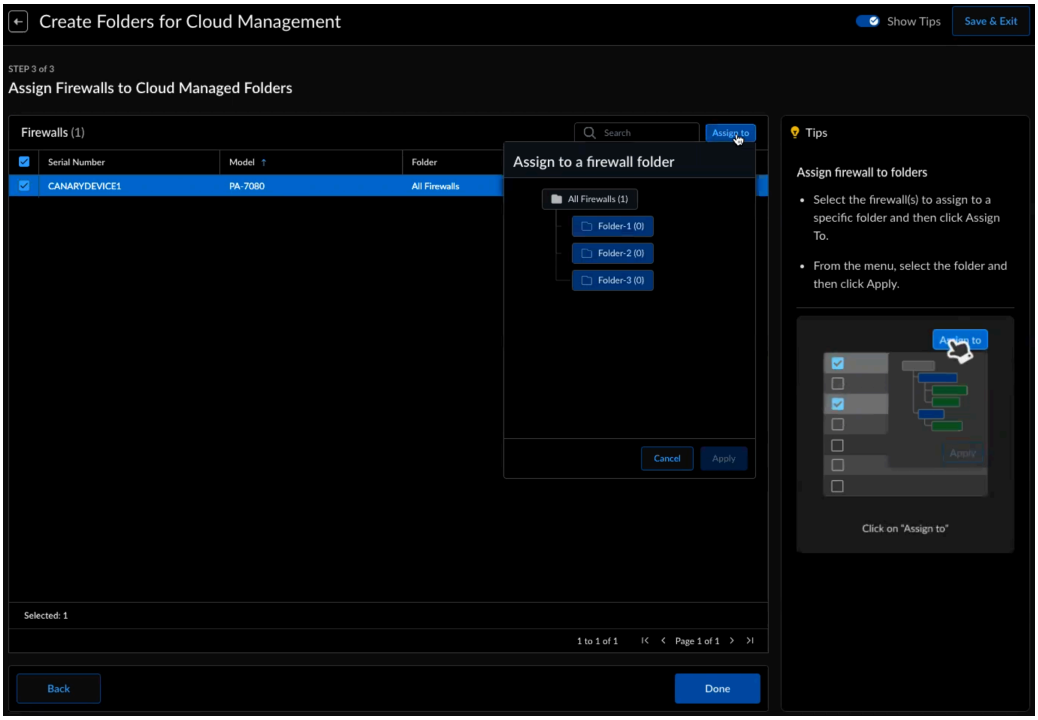


- *Los árboles de carpetas pueden tener un máximo de cuatro niveles.*
- *Las carpetas de nivel superior no se pueden eliminar ni cambiar de nombre.*
- *Consulte las Sugerencias para obtener sugerencias sobre determinadas acciones de carpeta.*
- *Guardaremos tu trabajo, podrá **Salir** en cualquier momento y volver más tarde.*

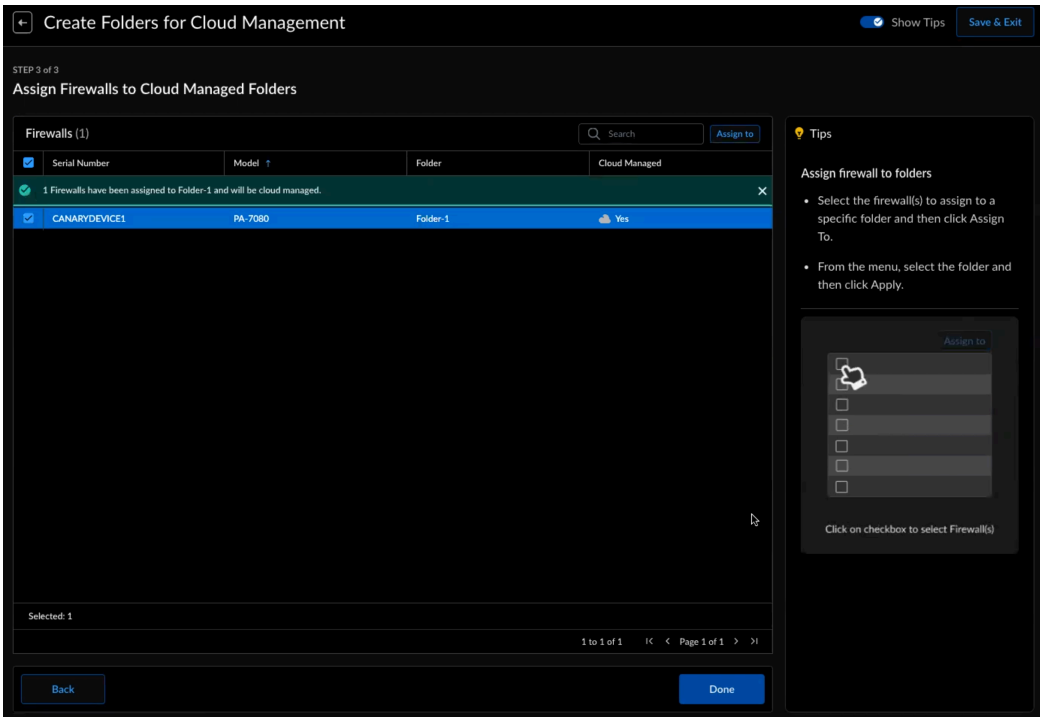
STEP 5 | Seleccione **Next (Siguiente)** para asignar sus cortafuegos a carpetas.

STEP 6 | Seleccione uno o más cortafuegos de esta lista.

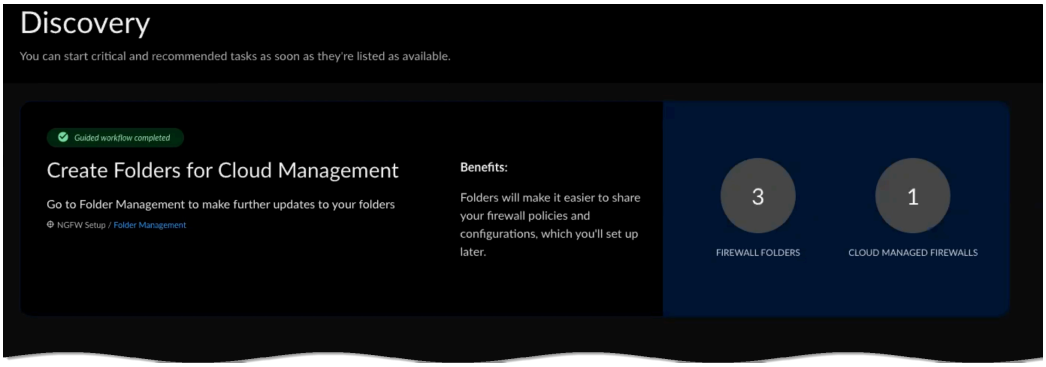
STEP 7 | Seleccione **Assign to (Asignar a)**, elija una carpeta a la que desee asignar sus cortafuegos y luego seleccione **Apply (Aplicar)**. La gestión en la nube está habilitada para los cortafuegos que usted asigna a una carpeta **Cloud Managed (Gestionada en la nube)**.



STEP 8 | Confirme sus asignaciones y seleccione **Done (Listo)**.



Verá las carpetas que creó y los cortafuegos que asignó en la página principal de **Discovery (Descubrimiento)**, así como en la pestaña **NGFW Setup (Configuración de NGFW)** > **Folder Management (Gestión de carpetas)**.



Flujos de trabajo: Configuración de NGFW

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by Strata Cloud Manager)	❑ La licencia AIOps for NGFW Premium se requiere para la gestión en la nube para NGFW ❑ Se requiere licencia de Strata Logging Service para el registro de logs ❑ Si tiene una licencia de Prisma Access, puede usar **Folder Management (Gestión de carpetas)** para ver las carpetas predefinidas y habilitar la Seguridad Web para una carpeta

Como parte de la configuración de sus NGFW para la gestión en la nube, deberá hacer lo siguiente Incorporar sus cortafuegos de nueva generación a Strata Cloud Manager. La incorporación incluye la configuración de carpetas para agrupar cortafuegos que requieren una configuración similar. Obtenga más información sobre Flujos de trabajo: Gestión de carpetas y utilice la página **Device Management (Gestión de dispositivos)** para ver los detalles de todos los dispositivos que se encuentran en la jerarquía de carpetas.

STEP 1 | Active las licencias Strata Logging Service y AIOps para NGFW Premium.

La licencia de Strata Logging Service se requiere para el registro de logs y la licencia AIOps for NGFW Premium se requiere para la gestión en la nube de NGFW.

STEP 2 | Crear una o más carpetas.

Las carpetas se utilizan para agrupar lógicamente los cortafuegos o los tipos de implementación para simplificar la gestión de la configuración.

STEP 3 | Incorporar un cortafuegos en Strata Cloud Manager.

Para incorporar un cortafuegos a Strata Cloud Manager, debe configurar los ajustes de Panorama local en el cortafuegos y asociar el cortafuegos con su arrendatario de Strata Cloud Manager. Una vez incorporado, puede continuar configurando las configuraciones General y de Sesión del cortafuegos .

STEP 4 | (Solo HA) Configure los cortafuegos gestionados en alta disponibilidad (HA) si es necesario.

STEP 5 | Crear uno o más fragmentos.

Los fragmentos de código se utilizan para agrupar objetos de configuración que se aplican a carpetas, implementaciones o cortafuegos individuales. Esto facilita y agiliza el proceso de incorporación al permitirle estandarizar configuraciones básicas comunes que se pueden aplicar e impulsar rápidamente.

STEP 6 | Creación de los objetos de configuración.

Los objetos de configuración son bloques de creación para las configuraciones de reglas de red y políticas.

STEP 7 | Cree y configure la red y la configuración de reglas de políticas.

STEP 8 | Envíe los cambios en la configuración de Strata Cloud Manager a su cortafuegos gestionado.

Flujos de trabajo: Gestión de dispositivos

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by Strata Cloud Manager)	☐ AIOps for NGFW Premium

Un cortafuegos NGFW de Palo Alto Networks gestionado por Strata Cloud Manager se denomina un *Dispositivo gestionado en la nube*. Strata Cloud Manager puede gestionar cortafuegos que ejecutan PAN-OS 10.2.3 o más reciente.

Para obtener más información sobre los requisitos previos para Strata Cloud Manager, haga clic aquí.

Con el panel de **Device Management (Gestión de dispositivos) [Workflows (Flujos de trabajo) > NGFW Setup (Configuración de NGFW) > Device Management (Gestión de dispositivos)]** puede revisar detalles importantes de dispositivos y versiones sobre todos sus dispositivos gestionados y seleccionar qué dispositivos pasar a la gestión en la nube.

Ver todos los detalles de los NGFW gestionados en la nube

La pestaña **Cloud Managed Devices (Dispositivos gestionados en la nube [Workflows (Flujos de trabajo) > NGFW Setup (Configuración de NGFW) > Device Management (Gestión de dispositivos) > Cloud Managed Devices (Dispositivos gestionados en la nube)]** muestra todos los cortafuegos incorporados en el SCM, las carpetas a las que están asignados y detalles importantes sobre ellos.

Información de dispositivo	Description (Descripción)
Nombre	El nombre del dispositivo NGFW y la(s) carpeta(s) bajo las que está organizada.
Etiquetas	Cualquier etiqueta adherida al NGFW.
Estado de sincronización de configuración	El estado de sincronización del NGFW: • Sincronizado • Fuera de sincronización
Estado HA	Estado de la HA del NGFW incorporado:

Información de dispositivo	Description (Descripción)
	• **Active (Activo)**: estado operativo de gestión de tráfico normal. • **Sassive (Pasivo)**: estado de copia de seguridad normal. • **Initiating (Iniciándose)**: el cortafuegos se encuentra en este estado por hasta 60 segundos desde el arranque. • **Non-functional (No funcional)**: estado de error. • **Suspended (Suspendido)**: un administrador deshabilitó el cortafuegos. • **Tentative (Tentativo)**: para una monitorización de enlace o ruta en una configuración activo/activo.
Número de serie	El número de serie del NGFW incorporado.
Modelo	Número de modelo del NGFW incorporado.
Tipo	El tipo del cortafuegos NGFW incorporado: • VM • PA
Dirección	La dirección IP del NGFW incorporado.
Licencia	La información de licencia para el NGFW incorporado • Emparejado • No emparejado
Versión de software | Aplicación y amenaza | Antivirus | Filtrado de URL	Muestra las versiones de software y contenido instaladas actualmente en el cortafuegos. Para obtener más información, consulte Software de cortafuegos y actualizaciones de contenido.
Diccionario de dispositivo	Un archivo para importar cortafuegos. El archivo de diccionario proporciona al administrador de Strata Cloud Manager y del cortafuegos una lista de atributos del dispositivo para seleccionarlos al importar las reglas de políticas de seguridad recomendadas.
Acciones	Las acciones para el cortafuegos incorporado: • Recuperar información de licencia • Reiniciar • Cambiar el modo de enrutamiento • Gestión de configuración local • Forzar arranque

Eliminar un NGFW de los dispositivos gestionados en la nube

La pestaña **Available Devices (Dispositivos disponibles)** muestra todos los NGFW disponibles para incorporar a SCM y los NGFW ya gestionados por Strata Cloud Manager.

Para obtener más información sobre el proceso de incorporación de Strata Cloud Manager, haga clic aquí.

Puede usar la pestaña dispositivos disponibles para mover dispositivos dentro y fuera de Strata Cloud Manager.

STEP 1 | Inicie sesión en Strata Cloud Manager.

STEP 2 | Seleccione **Workflows (Flujos de trabajo)** > **NGFW Setup (Configuración de NGFW)** > **Device Management (Gestión de dispositivos)** > **Available Devices (Dispositivos disponibles)**.

1. Seleccione **Back to Available Devices (Volver a dispositivos disponibles)** para mover un cortafuegos fuera de Strata Cloud Manager.

Restaure la instantánea de versión de configuración local en el cortafuegos

Puede restaurar cualquier versión y descargar los detalles de configuración en formato XML.

STEP 1 | Inicie sesión en Strata Cloud Manager.

STEP 2 | Seleccione **Workflows (Flujos de trabajo)** > **NGFW Setup (Configuración de NGFW)** > **Device Management (Gestión de dispositivos)** y, a continuación, seleccione **Local Configuration Management (Gestión de configuración local)** en **Actions (Acciones)**.

STEP 3 | Deberá **Load (Cargar)** la versión para restaurar la configuración local.

STEP 4 | Haga clic en **Yes (Sí)** para reemplazar la configuración local del cortafuegos por la versión de configuración. Se crea una nueva tarea de envío.

Puede usar la vista de **Tareas** para solucionar problemas de operaciones con errores, investigar advertencias asociadas con compilaciones finalizadas o cancelar compilaciones pendientes.

STEP 5 | Deberá **Download (Descargar)** los detalles de configuración de la vista para la versión seleccionada.

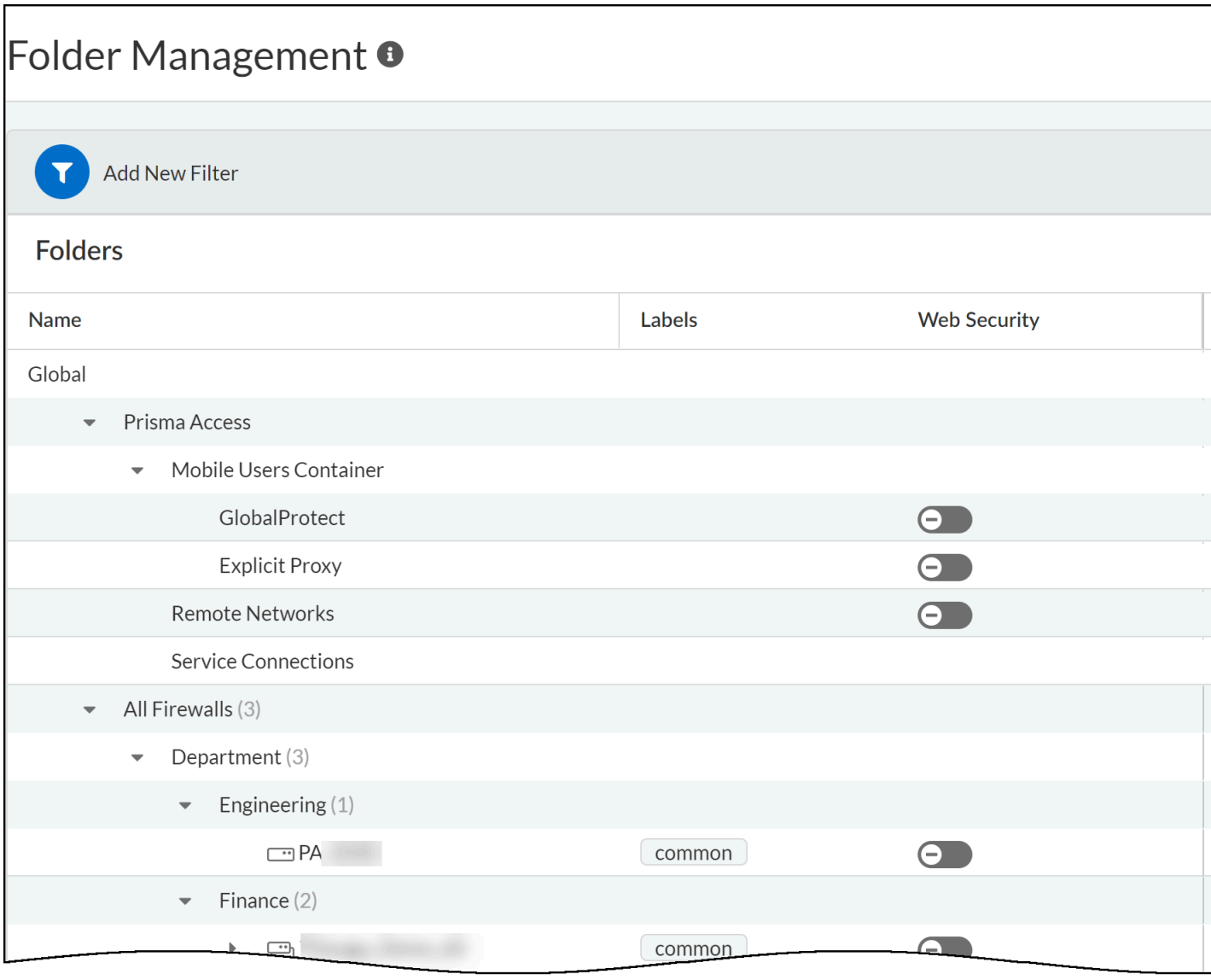
Flujos de trabajo: Gestión de carpetas

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • NGFW (Managed by Strata Cloud Manager)	❑ Licencia de AIOps for NGFW Premium (o) ❑ Licencia de Prisma Access

Las carpetas se utilizan para agrupar lógicamente los cortafuegos o los tipos de implementación (usuarios móviles de Prisma Access, redes remotas o conexiones de servicio) para simplificar la gestión de la configuración. Puede crear una carpeta que contenga varias carpetas anidadas para

agrupar cortafuegos e implementaciones que requieran configuraciones similares. Las carpetas que ya están anidadas también pueden tener varias carpetas anidadas.

Carpetas para Prisma Access y sus NGFW están separados; no es posible agrupar dispositivos NGFW en una carpeta con implementaciones de Prisma Access. Sin embargo, puede aplicar fácilmente la configuración compartida globalmente en todas las carpetas o usar Gestionar: Fragmentos para aplicar fácilmente la configuración estándar y los requisitos de políticas en varias carpetas.

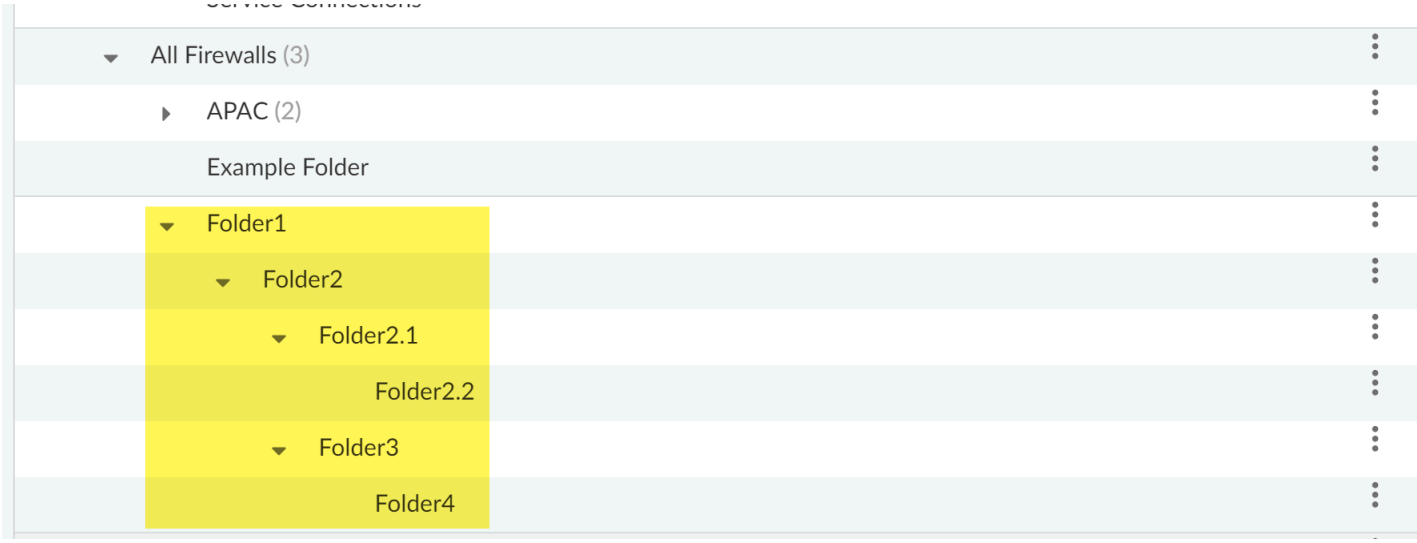


- NGFW
- Prisma Access

Gestión de carpetas (NGFW)

Para ayudar a gestionar carpetas y cortafuegos, puede aplicar etiquetas para filtrar y apuntar a grupos específicos de cortafuegos para cambios de configuración. Además, cada carpeta muestra la versión del software actualmente instalado, las versiones de lanzamiento de contenido dinámico y la versión de la aplicación GlobalProtect de los cortafuegos asociados con la carpeta.

Para las carpetas de cortafuegos, Strata Cloud Manager admite hasta cuatro carpetas anidadas dentro de cualquier jerarquía de carpetas determinada, siendo la carpeta predeterminada `Todos los cortafuegos` siempre el nivel más alto de cualquier jerarquía de carpetas. Por ejemplo, considere lo siguiente al diseñar su jerarquía de carpetas. En el siguiente ejemplo, `Carpeta1`, `Carpeta2`, `Carpeta3`y `Carpeta4` están anidadas bajo la carpeta `Todos los cortafuegos` y no se pueden añadir carpetas adicionales a esta jerarquía de carpetas en particular. Además, `Carpeta2.1` y `Carpeta2.2` están anidadas bajo `Carpeta2` y no puede añadir ninguna carpeta adicional.



Crear una carpeta

Cree una carpeta para agrupar lógicamente sus cortafuegos para una gestión simplificada de la configuración. Puede crear una carpeta en la carpeta predeterminada `Cortafuegos` o en otra carpeta existente.

STEP 1 | Inicie sesión en Strata Cloud Manager.

STEP 2 | Seleccione **Workflows (Flujos de trabajo)** > **NGFW Setup (Configuración de NGFW)** > **Folder Management (Gestión de carpetas)** y **Add Folder (Añadir carpeta)**.

STEP 3 | Dale un **Name (Nombre)**descriptivo a la carpeta.

STEP 4 | (Opcional) Introduzca una **Description (Descripción)** para la carpeta.

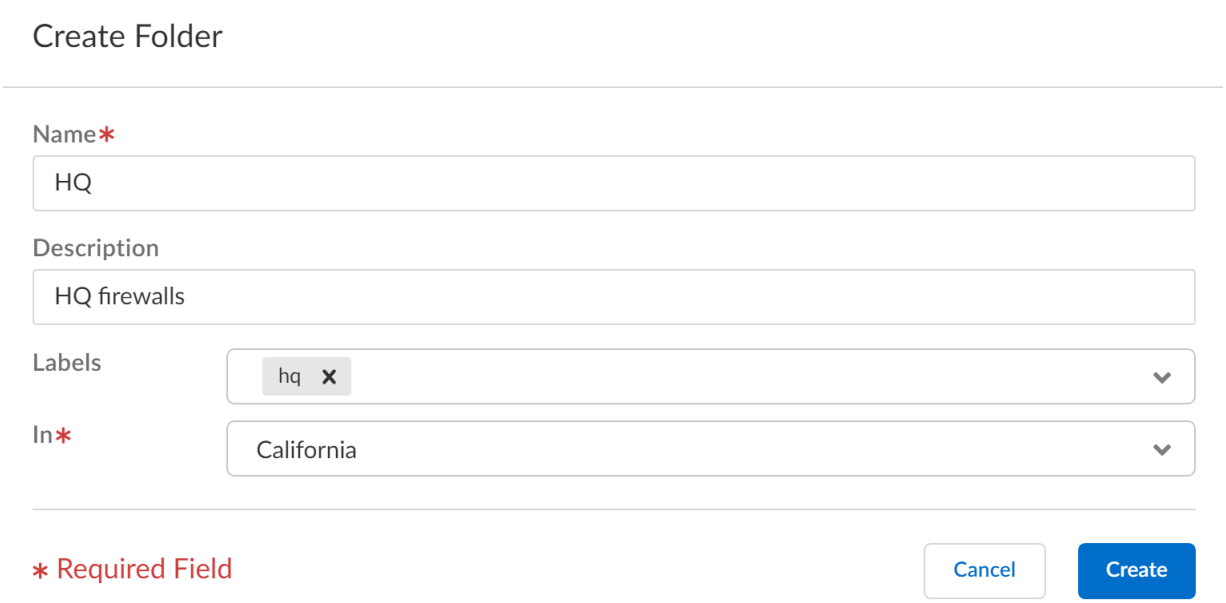
STEP 5 | (Opcional) Asignar una o más **Labels (Etiquetas)**.

Puede seleccionar una etiqueta existente o crear una nueva etiqueta escribiendo la etiqueta que desea crear..

STEP 6 | Especifique dónde crear la carpeta **In (En)**.

Seleccione **All Firewalls (Todos los cortafuegos)** o seleccione una carpeta existente para anidar la carpeta en ella.

STEP 7 | **Cree** la carpeta.

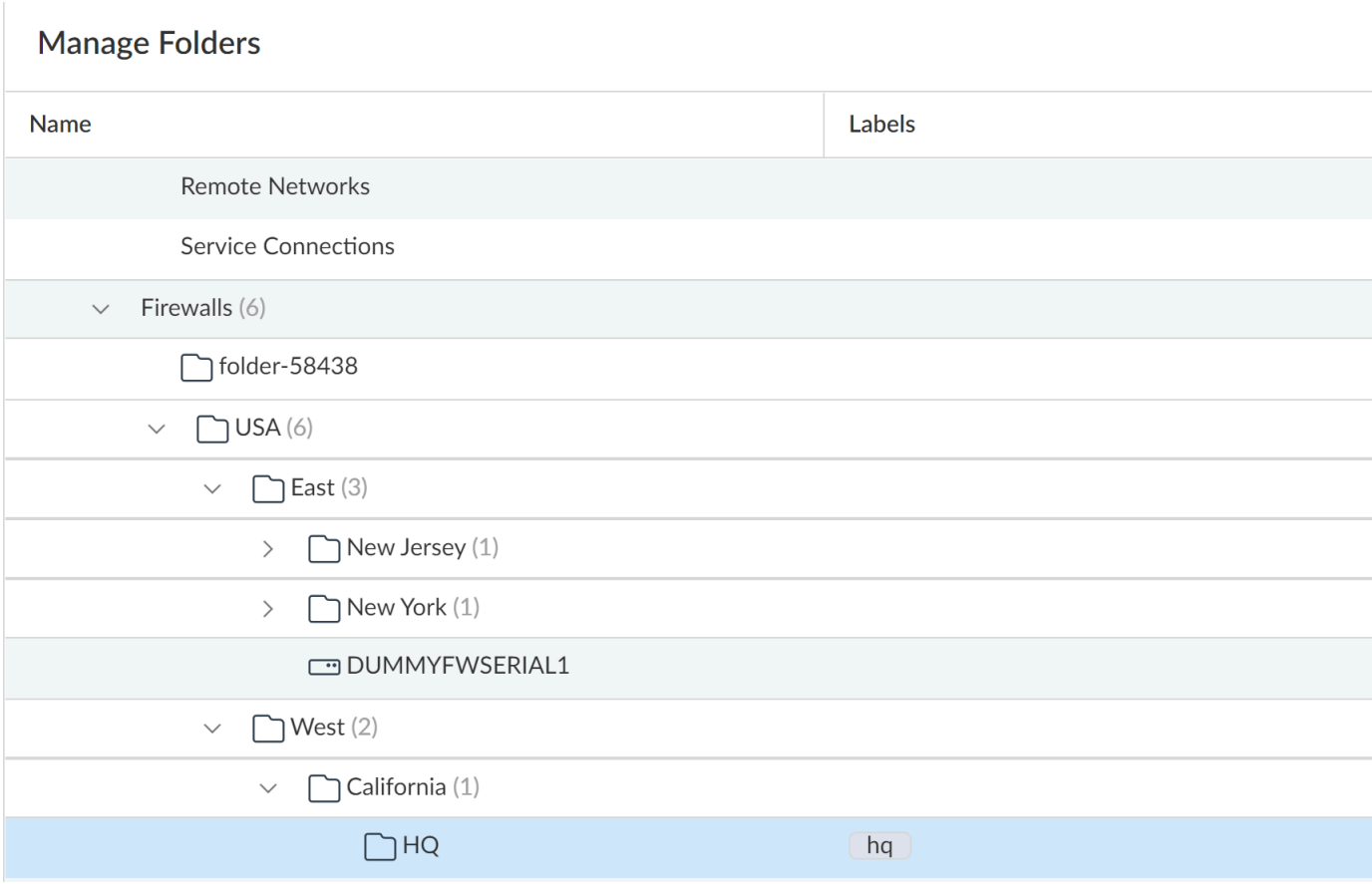


Modificar una carpeta

Modifique una carpeta existente para editar el nombre, la descripción y para añadir o cambiar las etiquetas. Además, puede mover o eliminar la carpeta según sea necesario.

STEP 1 | Inicie sesión en Strata Cloud Manager.

STEP 2 | Seleccione **Workflows (Flujos de trabajo)** > **NGFW Setup (Configuración de NGFW)** > **Folder Management (Gestión de carpetas)** y expanda el menú Acciones.



STEP 3 | Modifique la carpeta según sea necesario.

- **Edit (Editar)** la carpeta
  1. Editar el **Name (Nombre)**de la carpeta.
  2. (Opcional) edite la **Description (Descripción)**de la carpeta.
  3. Seleccionar o crear **Labels (Etiquetas)**.

     Puede asignar etiquetas completamente diferentes a la carpeta o añadir etiquetas adicionales.
  4. **Save (Guardar)**.
- Deberá **Move (Trasladar)** la carpeta y seleccionar el **Destination (Destino)**.

Puede mover una carpeta de las siguientes maneras.

- Puede mover una carpeta para anidarla bajo una carpeta diferente.
- Puede mover una carpeta anidada a la carpeta `Cortafuegos`.
- Puede mover una carpeta anidada de una carpeta a otra.

Move (Trasladar) la carpeta después de seleccionar la carpeta de destino.

- Seleccione **Delete Folder (Eliminar carpeta)** y haga clic en **OK (Aceptar)** para confirmar.

Solo puede eliminar una carpeta que no tenga cortafuegos asociados ni carpetas anidadas debajo de ella.

Gestión de carpetas (Prisma Access)

Las carpetas de Prisma Access están predefinidas; puede usarlas para especificar el alcance de la configuración y asegurarse de que los tipos de implementación de Prisma Access (usuarios móviles, redes remotas y conexiones de servicio) reciban todas las configuraciones globales y, a continuación, las configuraciones necesarias o específicas para cada tipo.

Todas las carpetas anidadas en esa jerarquía de carpetas heredan las configuraciones definidas en una carpeta Por ejemplo, puede configurar los ajustes que son comunes en GlobalProtect, proxy explícito, redes remotas y conexiones de servicio en la carpeta **Prisma Access**. Del mismo modo, puede configurar los ajustes que son comunes en GlobalProtect y Proxy explícita en el **Contenedor de usuarios móviles** y así sucesivamente.

No puede editar la jerarquía de carpetas para Prisma Access.

En el nivel de carpeta, también puede habilitar la seguridad web para la implementación de usuario móvil, red remota o conexión de servicio de Prisma Access.

Flujos de trabajo: Configuración de Prisma SD-WAN

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma SD-WAN	❑ Licencia de Prisma SD-WAN

Puede configurar sitios de sucursales, sitios de centros de datos y dispositivos ION en Prisma SD-WAN mediante Strata Cloud Manager.

Seleccione **Workflows (Flujos de trabajo)** > **Prisma SD-WAN Setup (Configuración)**.

Puede configurar flujos de trabajo para:

- Sucursales

  Configure sucursales en la red mediante la pestaña **Branch Sites (Sucursales)**. Una empresa puede tener una o más sucursales dentro de una red. Al crear una sucursal, puede seleccionar un dominio predeterminado y un conjunto de reglas de política y configurar redes WAN, categorías de circuitos, etiquetas de circuitos y especificaciones de circuitos.

- Centros de datos

  Configure los sitios de los centros de datos en su red mediante la pestaña **Data Centers (Centros de datos)**. Los sitios del centro de datos están conectados a las sucursales y usted puede alojar aplicaciones y servicios empresariales en un centro de datos.

- Dispositivos

  Configure los dispositivos ION en su red mediante la pestaña **Devices (Dispositivos)**. Los dispositivos ION se pueden implementar en una sucursal o en un centro de datos. Estas están disponibles en formato de hardware y software para satisfacer las necesidades de cualquier ubicación y cualquier escenario de implementación. Tiene que conectar, reclamar, asignar y configurar los dispositivos ION para los sitios de sus sucursales y centros de datos.

Flujos de trabajo: Configuración de Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	Licencia de Prisma Access

Seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configurar)** para comenzar a configurar su Prisma Access.

- Configure la infraestructura de servicios para habilitar la comunicación entre las ubicaciones de red remotas, los usuarios móviles y la sede o los centros de datos que planifica conectar a Prisma Access a través de conexiones de servicio. Una conexión de servicio proporciona conectividad al centro de datos.
- Incorpore usuarios móviles y determine cómo los está conectando a Prisma Access.
- Incorpore redes remotas para proteger ubicaciones de redes remotas, como sucursales, y usuarios en esas sucursales. En el sitio remoto se requiere un cortafuegos de nueva generación o un dispositivo de terceros compatible con IPSec, incluida SD-WAN, que pueda establecer un túnel IPSec al servicio.
- Añada las conexiones de servicio para permitir que tanto los usuarios móviles como los usuarios de las redes de sucursales accedan a los recursos de la sede central (HQ) o del centro de datos (DC). Más allá de proporcionar acceso a los recursos corporativos, las conexiones de servicio permiten a sus usuarios móviles llegar a las sucursales.

Flujos de trabajo: Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	Licencia de Prisma Access

Antes de utilizar Prisma Access para proteger sus redes remotas y usuarios móviles, debe configurar una subred de infraestructura.

Prisma Access utiliza la subred para crear la red troncal de red para la comunicación entre las redes de sucursales, los usuarios móviles y la infraestructura de seguridad de Prisma Access, así como con las redes de la sede central y del centro de datos que planea conectar a Prisma Access a través de conexiones de servicio. Si utiliza enrutamiento dinámico para sus redes remotas o conexiones de servicio, también debe configurar un número AS privado de BGP compatible con RFC 6696.

Utilice las siguientes recomendaciones y requisitos cuando añada una subred de infraestructura para Prisma Access.

- Utilice una subred compatible con RFC 1918. Aunque Prisma Access admite el uso de direcciones IP (públicas) no compatibles con RFC 1918, no se recomienda debido a posibles conflictos con el espacio de direcciones IP públicas de Internet.

- No especifique ninguna subred que se solape con 169.254.169.253, 169.254.169.254 y el rango de subredes 100.64.0.0/10, porque Prisma Access reserva esas direcciones IP y subredes para su uso interno. Esta subred es una extensión de la red existente y, por lo tanto, no puede solaparse con ninguna subred IP que utilice dentro de su red corporativa o con los grupos de direcciones IP que asigne a Prisma Access para usuarios o Prisma Access para redes. Debido a que la infraestructura de servicios requiere un gran número de direcciones IP, debe designar una subred /24 (por ejemplo, 172.16.55.0/24).
- Introduzca una subred de infraestructura que Prisma Access pueda utilizar para habilitar la comunicación entre las ubicaciones de red remotas, los usuarios móviles y la sede o los centros de datos que planifica conectar a Prisma Access a través de conexiones de servicio. Utilice una subred compatible con RFC 1918 para la subred de infraestructura.

Consulte Prisma Access Configuración para obtener más información.

Configurar el DNS para la infraestructura

Prisma Access le permite especificar servidores del Sistema de Nombres de Dominio (DNS) para resolver tanto los dominios que son internos de su organización como los dominios externos. Prisma Access realiza una conexión proxy de la solicitud DNS basándose en la configuración de sus servidores DNS.

La configuración de la infraestructura DNS proporcionará acceso a servicios en su red corporativa, como servidores LDAP y DNS, especialmente si planea configurar conexiones de servicio para proporcionar acceso a este tipo de recursos en la sede o en los centros de datos. Las consultas DNS para los dominios de la Lista interna de dominios se envían a los servidores DNS locales para asegurarse de que los recursos estén disponibles para los usuarios de red remotos de Prisma Access y los usuarios móviles.

Esto establecerá listas internas de dominios que se aplican a todo el tráfico. Si lo prefiere, puede consultar la Guía del administrador para ver cómo crear listas internas de dominios que se aplican solo a implementaciones de usuarios móviles específicas o sitios de red remotos.

Los beneficios de configurar los DNS para la infraestructura son:

- Habilite Prisma Access para resolver sus dominios internos
- Configurar DNS para resolver dominios internos y externos
- Utilice un comodín (*) antes de los dominios de la lista de dominios, por ejemplo, *.acme.local o *.acme.com

Consulte DNS para Prisma Accesspara obtener más información.

Flujos de trabajo: Usuarios móviles

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licencia de Prisma Access ❑ Licencia de Strata Logging Service

Antes de configurar los usuarios móviles, asegúrese de tener las licencias necesarias (licencia de Prisma Access para usuarios móviles y una licencia de Strata Logging Service con espacio de almacenamiento de cortafuegos adecuado). Si los usuarios de dispositivos móviles se conectan

a otras redes conectadas, necesitará la licencia Zero Trust Network Access (ZTNA) o Prisma Access Enterprise Edition que proporcionará el nodo de acceso corporativo (CAN) necesario para conectarse.

Primero elegirá su tipo de conexión, o puede usar GlobalProtect, proxy explícito o ambos. Para ambos tipos de conexión, solo hay unos pocos ajustes requeridos que debe completar inicialmente para permitir a Prisma Access aprovisionar el entorno de sus usuarios móviles.

1. Conectar a Prisma Access.

   Determine cómo deben conectarse a Prisma Access los usuarios móviles de la ubicación que está configurando. Puede dividir su licencia de usuario móvil entre GlobalProtect y conexiones proxy explícitas; algunos usuarios pueden conectarse a través de GlobalProtect y otros a través de proxy explícito.

   La aplicación GlobalProtect instalada en los dispositivos móviles de los usuarios envía tráfico a Prisma Access.
2. Establecer la infraestructura.

   Establezca la configuración básica de la infraestructura y, a continuación, configure los ajustes de la infraestructura específica de su tipo de conexión (GlobalProtect o Proxy explícito).

   Un archivo de configuración automática de proxy (PAC) en dispositivos de usuario móviles redirige el tráfico del navegador a Prisma Access.
3. Seleccione la ubicación de Prisma Access.

   El mapa muestra las regiones globales donde puede implementar Prisma Access para los usuarios: América del Norte, América del Sur, Europa, África, Oriente Medio, Asia, Japón y ANZ (Australia y Nueva Zelanda). Además, Prisma Access proporciona múltiples ubicaciones dentro de cada región para garantizar que sus usuarios puedan conectarse a una ubicación que proporcione una experiencia de usuario adaptada a la configuración regional de los usuarios. Para obtener el mejor rendimiento, seleccione Todo. Alternativamente, seleccione las ubicaciones específicas dentro de cada región seleccionada donde sus usuarios necesitarán acceso. Al limitar su implementación a una sola región, puede tener un control más granular sobre sus regiones implementadas y excluir las regiones requeridas por su política o regulaciones de la industria.
4. Añadir las ubicaciones de Prisma Access.

   Configure la configuración para añadir las ubicaciones de Prisma Access que desea admitir a sus usuarios.
5. Autenticar usuarios móviles.

   Configure la autenticación de usuario para que solo los usuarios legítimos tengan acceso a sus servicios y aplicaciones. Para probar la configuración, puede añadir usuarios que Prisma Access autentique localmente o puede ir directamente a configurar la autenticación a nivel empresarial.

Una vez que haya enviado su configuración inicial a Prisma Access, Prisma Access comenzará a aprovisionar su entorno de usuario móvil. Esto puede tardar hasta 15 minutos. Cuando sus ubicaciones de usuario móvil estén en funcionamiento, podrá verificarlas en la página de configuración de usuarios móviles, la página Resumen general y en Insights de Prisma Access.

Consulte Usuarios móviles de Prisma Access para obtener más información.

Flujos de trabajo: Redes remotas

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	Licencia de Prisma Access

A medida que se prepara para conectar redes remotas a Prisma Access, necesitará saber cuántos sitios incorporará. Esta información le ayudará a determinar los requisitos de conectividad, como cómo enrutar el tráfico a través de Prisma Access. Mientras planifica su implementación de red remota, necesitará saber qué aplicaciones pasarán por Prisma Access para configurar adecuadamente las mejores reglas de política de seguridad. Igualmente importante es establecer la configuración de su perfil de amenazas. Además, debe considerar la posibilidad de aplicar un análisis coherente de amenazas, URL y WildFire a todas las reglas para una estrategia coherente de mitigación de amenazas.

Para obtener más información, consulte Prisma AccessRedes remotas.

Flujos de trabajo: Conexiones de servicio

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	Licencia de Prisma Access

Las conexiones de servicio permiten que tanto los usuarios móviles como los usuarios de las redes de sucursales accedan a los recursos de la sede central (HQ) o del centro de datos (DC). Más allá de proporcionar acceso a los recursos corporativos, las conexiones de servicio permiten a sus usuarios móviles llegar a las sucursales.

Seleccione **Workflows (Flujos de trabajo)** > **Setup (Configuración de) Prisma Access** > **Service Connections (Conexiones de servicios)** para añadir una conexión de servicio.

El primer túnel que se crea es el túnel principal para la conexión de servicio. Repita este flujo de trabajo para, opcionalmente, configurar un túnel secundario. Cuando ambos túneles están activos, el túnel primario tiene prioridad sobre el túnel secundario. Si el túnel de conexión del servicio primario cae, la conexión cae de nuevo al túnel secundario hasta que el túnel primario regrese. Basado en el dispositivo IPSec que utiliza para establecer el túnel, Prisma Access proporciona configuraciones de seguridad IKE e IPSec integradas y recomendadas. Puede usar los ajustes recomendados para comenzar o personalizarlos según sea necesario para su entorno.

Para obtener más información, consulte Prisma Access Conexiones de servicio.

Flujos de trabajo: Aislamiento remoto del navegador

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	Prisma Access 5.0 Innovation

¿Dónde puedo usar esto?	¿Qué necesito?
	❑ Licencia Prisma Access con la suscripción de licencia de Usuarios móviles o Redes remotas ❑ Licencia de aislamiento del navegador remoto

Remote Browser Isolation (RBI) de Palo Alto Networks es una solución que aísla y transfiere toda la actividad de navegación lejos de los dispositivos gestionados y redes corporativas de su usuario a una entidad externa como Prisma Access, que asegura y aísla código y contenido potencialmente malicioso dentro de su plataforma.

Integrado de forma nativa con Prisma Access, RBI le permite aplicar perfiles de aislamiento fácilmente a las políticas de seguridad existentes. Todo el tráfico en aislamiento se somete a análisis y prevención de amenazas proporcionados por los servicios de seguridad en la nube (CDSS), como Advanced Threat Prevention, Advanced WildFire, Advanced URL Filtering, DNS Security, and SaaS Security.

A medida que se prepara para incorporar a sus usuarios a RBI, considere qué categorías de URL desea habilitar para la navegación aislada de sus usuarios. Piense qué acciones del navegador quiere impedir que realicen sus usuarios, por ejemplo copiar y pegar funciones, entradas de teclado y opciones para compartir como cargar, descargar e imprimir archivos.

Para obtener más información, consulte Aislamiento remoto del navegador.

Flujos de trabajo: Actualizaciones de software

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • NGFW (Managed by Strata Cloud Manager)	• Al menos una de estas licencias es necesaria para gestionar su configuración con Strata Cloud Manager; para la gestión unificada de NGFW y Prisma Access, necesitará licencias NGFW y Prisma Access: ❑ licencia de Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro

Utilice Strata Cloud Manager para planificar y gestionar sus actualizaciones de software para NGFW y Prisma Access. Estos son los flujos de trabajo que puede realizar:

- Recomendaciones de actualización Cree recomendaciones de actualización para determinar la mejor versión de software para los dispositivos que se pueden actualizar. Recomendaciones de actualización de software analiza las características habilitadas en cortafuegos y proporciona una recomendación personalizada.
- Panel de control de actualización de Prisma Access Elija una ventana de tiempo preferida para ciertas actualizaciones de Prisma Access.
- NGFW - Programador: Programe una actualización de software de PAN-OS para actualizar o degradar sus cortafuegos a una versión de PAN-OS objetivo en la fecha y hora que elija.
- NGFW
- Prisma Access

Actualizaciones de software (NGFW)

Seleccione **Workflows (Flujos de trabajo)** > **Software Upgrades (Actualizaciones de software)** > **Upgrade Recommendations (Recomendaciones de actualización)** para planificar la actualización de sus dispositivos analizándolos y creando recomendaciones de actualización.

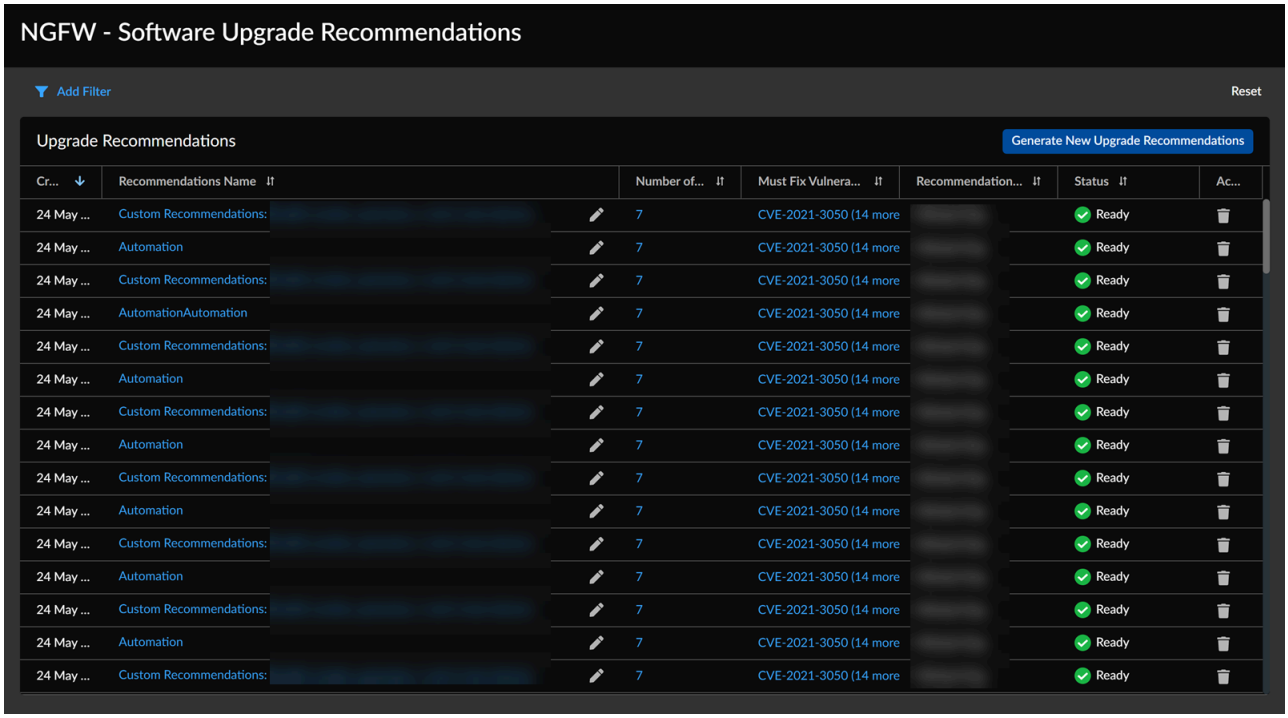
Recomendaciones de actualización

En **Workflows (Flujos de trabajo)** > **Software Upgrades (Actualizaciones de software)** > **Upgrade Recommendations (Recomendaciones de actualizaciones)**, puede crear recomendaciones para determinar las mejores versiones de software para sus dispositivos que se pueden actualizar. Recomendaciones de actualización de software analiza las características habilitadas en cortafuegos y proporciona una recomendación personalizada que incluye:

- La mejor versión de software para los dispositivos que se pueden actualizar.
- Información sobre nuevas características, cambios en el comportamiento, vulnerabilidades y problemas de software en cada versión de software recomendada.

Los tipos de recomendaciones de actualización son:

- Recomendaciones generadas por el sistema que se generan cada semana y contienen las opciones de actualización sugeridas.
- Recomendaciones personalizadas generadas por el usuario que se generan en función de los dispositivos seleccionados para CVE específicos en el Resumen de aviso de seguridad.
- Recomendaciones generadas por el usuario que se generan en función de la carga de un archivo de asistencia técnica (TSF) de un cortafuegos.



Para cada plan de **Upgrade Recommendations (Recomendaciones de actualización)**, puede:

- ver el número de dispositivos que requieren una actualización y la vulnerabilidades que se deben corregir.
- editar el nombre de un informe de recomendación para diferenciar los informes personalizados.
- filtrar los informes de recomendaciones por Fecha de creación, Nombre del plan y Recomendaciones generadas por.
- borrar una recomendación de actualización que no se cumpla o ya no sea necesaria.

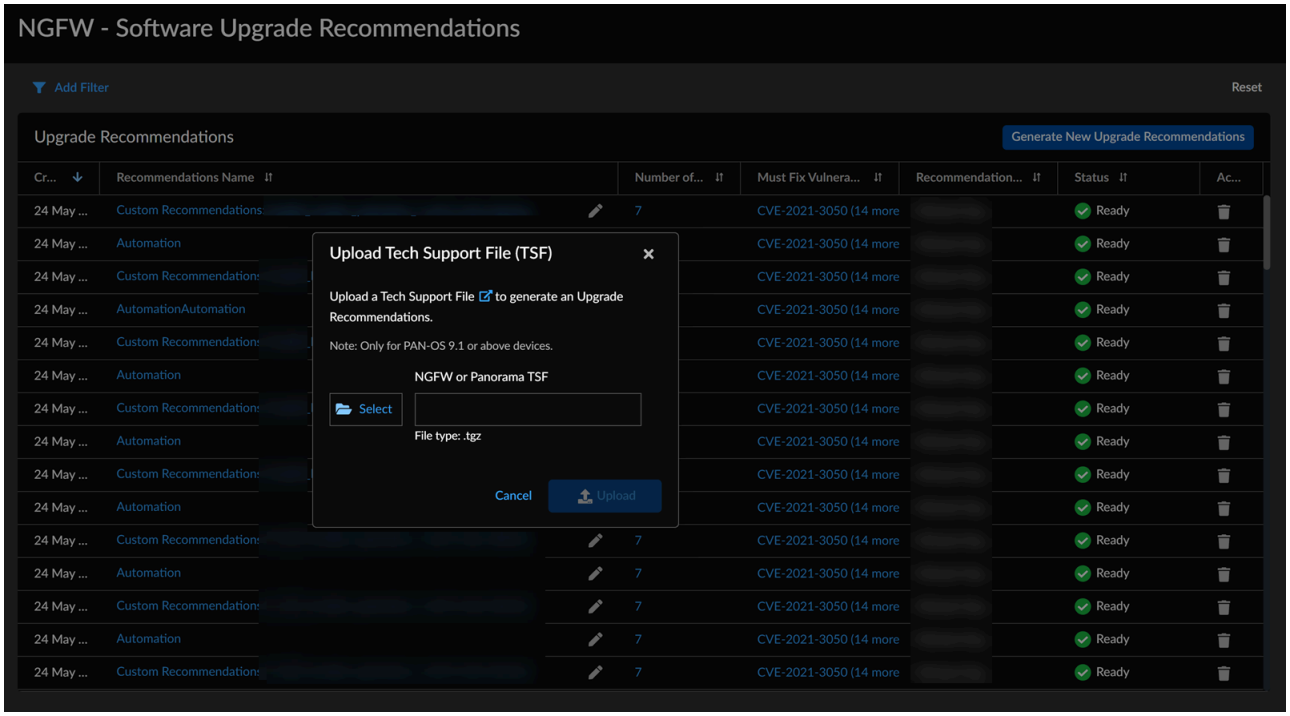
Haga clic en un informe de recomendación para ver el informe detallado con las opciones de actualización de los dispositivos. Seleccione una opción de actualización para ver más detalles sobre **New Features (Nuevas características)**, **PAN-OS Known Vulnerabilities (Vulnerabilidades conocidas de PAN-OS)**, **Changes of Behavior (Cambios de comportamiento)** y **PAN-OS Known Issues (Problemas conocidos de PAN-OS)**. Para un problema conocido en **PAN-OS Known Issues (Problemas conocidos de PAN-OS)**, el valor en **Associated Case Count (Recuento de casos asociados)** se obtiene por el número de clientes que han informado de este problema.

Haga clic en **Export (Exportar)** para descargar este informe en formato CSV.

Generar recomendaciones de actualización de software bajo demanda

1. Vaya a **Workflows > Software Upgrades > Upgrade Recommendations (Flujos de trabajo > Actualizaciones de software > Recomendaciones de actualización)**.
2. **Generate New Upgrade Recommendations (Generar nuevas recomendaciones de actualización**.
3. Deberá **Select (Seleccionar)** y **Upload (Cargar)** un archivo de asistencia técnica (TSF).

   - *Puede cargar el TSF de un solo dispositivo a la vez y debe ser un TSF en formato de archivo .tgz.*
   - *Recomendaciones de actualización de software admite TSF desde dispositivos con la versión 9.1 de PAN-OS o superior para la generación de informes.*



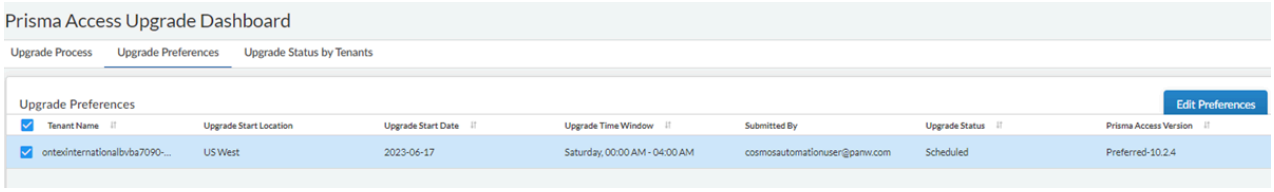
4. Vea las recomendaciones de actualización de software después de que el estado se muestre como **Ready (Listo)**. También puede comprobar la columna **Status (Estado)** para ver si hay algún error relacionado con la carga, el formato de archivo o el procesamiento del archivo TSF.

Actualizaciones de software (Prisma Access)

Seleccione **Workflows (Flujos de trabajo)** > **Software Upgrades (Actualizaciones de software)** > **Prisma Access** para ver información sobre el proceso de actualización del plano de datos de Prisma Access.

Usted puede:

- Comprenda el proceso de actualización del plano de datos de Prisma Access.
- Elija sus preferencias de actualización:



Seleccione un nombre de inquilino para elegir sus preferencias de actualización. Para obtener más información, consulte Seleccionar una ventana preferida para ciertas actualizaciones de Prisma Access.

Flujos de trabajo: Prisma Access Browser

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licencia de paquete de Prisma Access con Prisma Access Browser ❑ Superusuario o rol de Prisma Access Browser

Seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración)** > **Prisma Access Browser** para comenzar a incorporar su Prisma Access Browser.

Prisma Access Secure Enterprise Browser (Prisma Access Browser) es la única solución que protege los dispositivos gestionados y no gestionados, a través de un navegador empresarial integrado de forma nativa que extiende la protección a los dispositivos no gestionados. Consulte ¿Qué es Prisma Access Browser?

La incorporación consta de una serie de pasos en los que configurará los siguientes elementos:

- Autenticación de usuarios y grupos
- Integración de Prisma Access
- Enrutamiento
- Aplicar aplicaciones de SSO
- Descargar y distribuir
- Política del navegador

Incorporar Prisma Access Browser en Strata Cloud Manager.

Informes: Strata Cloud Manager

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)* • Cortafuegos NGFW *(con gestión de la configuración de Strata Cloud Manager o Panorama)* • Prisma SD-WAN	❑ Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN ❑ Créditos NGFW de software *(para NGFW de software de VM-Series)* ❑ Licencia de WAN Clarity Report ❑ Un rol que tiene permiso para descargar, compartir y programar informes.

Obtenga informes sobre los patrones de tráfico de red, la utilización del ancho de banda y los datos de suscripción de seguridad en Strata Cloud Manager. Los informes proporcionan información práctica sobre su red que puede utilizar para planificar y supervisar. Se admiten informes en ciertos paneles de Prisma Access y NGFW, Activity Insights y Prisma SD-WAN. Los usuarios de Prisma Access y NGFW que tienen acceso completo a usar el panel de control pueden descargar datos del panel en formato PDF, compartir el informe dentro de su organización y programar informes para que se entreguen a su bandeja de entrada de correo electrónico a intervalos regulares. Los informes son un servicio de suscripción con licencia en Prisma SD-WAN. Puede descargar y ver informes de controladores, en todos los sitios y circuitos en Prisma SD-WAN.

Ver estos informes en Strata Cloud Manager:

- Prisma Access y NGFW: puede generar informes desde los paneles de Prisma Access y NGFW y desde Activity Insights. Estos iconos  en la parte superior derecha del panel indican que los informes son compatibles con este panel. También puede generar, descargar, compartir y programar informes directamente desde el menú **Reports (Informes)**.
- Prisma SD-WAN: vea los siguientes informes de WAN Clarity:
  - Informes de sucursal de WAN Clarity
  - Informes de centros de datos de WAN Clarity
  - Informes de Uso de ancho de banda agregado
- Prisma Access y NGFW
- Prisma SD-WAN

Informes (Prisma Access y NGFW)

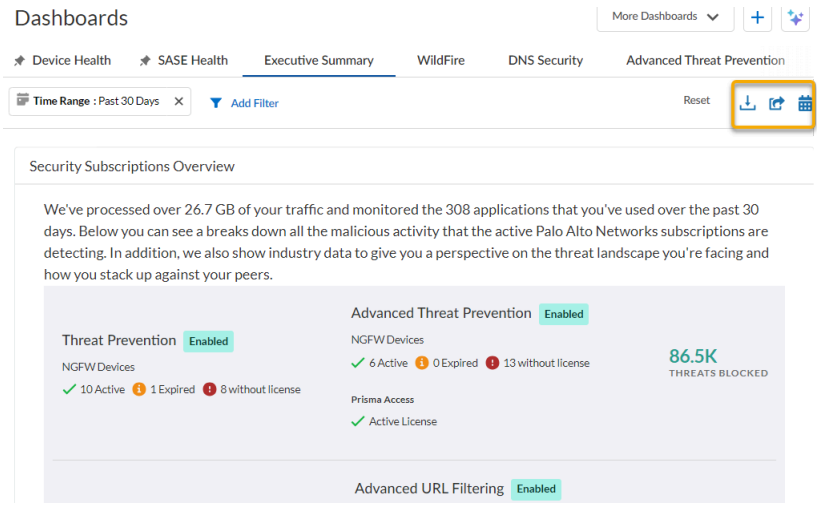
Los paneles y el resumen de información de actividad se pueden compartir dentro de su organización como informes en PDF, y también puede programar informes para que se envíen a su bandeja de entrada de correo electrónico (y a las bandejas de entrada de sus compañeros) a intervalos regulares (diarios, semanales o mensuales).

Para que pueda compartir informes fácilmente con personas de su organización, configure Cloud Identity Engine (sincronización de directorios) para esta aplicación. Cloud Identity Engine brinda a las aplicaciones acceso de solo lectura a su información de Active Directory. Una vez configurado Cloud Identity Engine, puede añadir fácilmente destinatarios a un informe programado. Los destinatarios de su informe se comparan con Cloud Identity Engine y, si no encuentra una coincidencia, realiza un paso de validación adicional al comparar el dominio de la dirección de correo electrónico con los dominios de direcciones de correo electrónico asociados con su cuenta de asistencia. Estas comprobaciones garantizan que los informes no se envíen fuera de la organización.

Puede descargar, compartir o programar informes directamente desde el menú **Reports (Informes)** o desde la página **Dashboard (Panel)** individual y la página **Insights (Información) > > Activity Insights (Información de actividad)** > **Overview (Descripción general)**. Los informes se comparten y descargan como archivos PDF.

Para descargar, compartir o programar un informe:

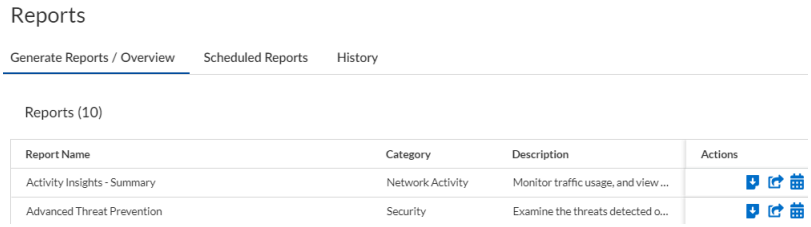
STEP 1 | Haga clic en cualquiera de estos iconos, en la página **Dashboard (Panel)** o desde la página **Insights > > Activity Insights** > **Overview (Descripción general)**.



O

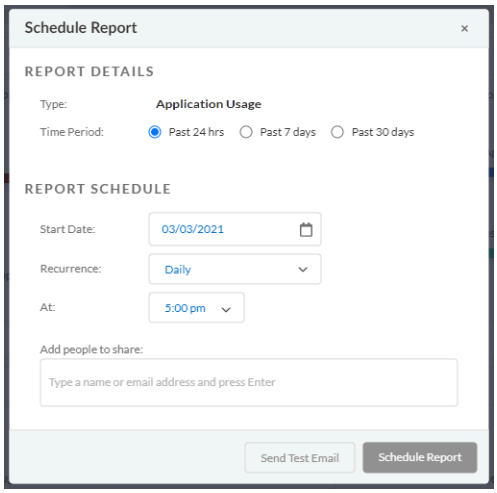
Haga clic en**Strata Cloud Manager** > **Reports (Informes)** > **Generate Reports/Overview (Generar informes/descripción general)** y seleccione cualquiera de estos iconos de la lista de formatos de informe. De forma predeterminada, los informes se generan con los datos de las últimas 24 horas o 30 días según el tipo de panel para el que esté generando el informe.

Puede personalizar el período de tiempo durante el cual desea recopilar datos en el informe al programar el informe.

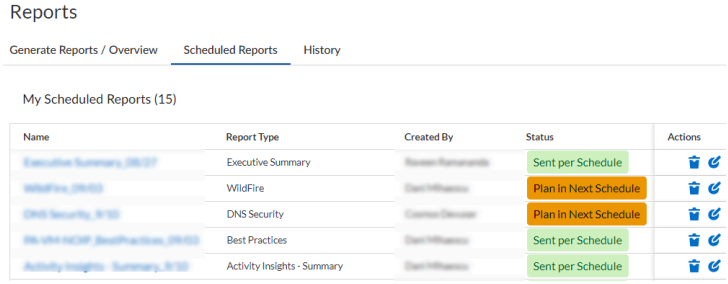


STEP 2 | Si está programando un informe, deberá continuar definiendo los parámetros del informe, incluidos:

- El **Time Period (Período de tiempo)** durante el cual se recopilarán los datos
- La **Recurrence (Periodicidad)**, que es la frecuencia con la que desea que se entregue el informe (diario, semanal o mensual)



Puede ver, editar o eliminar todos los informes programados desde la pestaña **Strata Cloud Manager** > **Reports (Informes)** > **Scheduled Reports (Informes programados)**.



El **History (Historial)** muestra todos los informes descargados en los últimos 30 días.

Informes (Prisma SD-WAN)

Los informes de WAN Clarity de Prisma SD-WAN proporcionan una vista agregada de la distribución del tráfico y la utilización del ancho de banda en su red. Puede descargar todo el paquete de informes o ver los informes desde el controlador de Prisma SD-WAN, lo que permite comparaciones de tendencias semana tras semana, así como comparaciones entre sitios y circuitos.

Los informes están disponibles para su uso inmediato como un servicio de suscripción con licencia. Comuníquese con el equipo de ventas de Prisma SD-WAN para habilitar la suscripción.

Los informes de WAN Clarity de Prisma SD-WAN incluyen:

- Informes de sucursal de WAN Clarity
- Informes de centros de datos de WAN Clarity
- Informes de Uso de ancho de banda agregado

Para ver los informes:

STEP 1 | Seleccione **Reports (Informes)** > **Prisma SD-WAN**.

STEP 2 | Haga clic en **View Reports (Ver informes)** en **WAN Clarity Reports (Informes de WAN Clarity)**.

STEP 3 | Seleccione un **Time Range (Intervalo de tiempo** y seleccione cualquiera de los siguientes en el campo **Report for (Informe para)**.

- **Sucursal**
- **Centro de datos**
- **Uso de ancho de banda agregado**

Favoritos: Strata Cloud Manager

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)* • Cortafuegos NGFW *(con gestión de la configuración de Strata Cloud Manager o Panorama)*	❑ Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Cualquier Inquilino o Grupos de servicios para inquilinos (TSG) es compatible con la aplicación ❑ Un rol dependiendo de sus necesidades

La función Favoritos le permite guardar elementos de interés y luego acceder rápidamente a ellos cuando los necesite desde cualquier ubicación en Strata Cloud Manager. Puede personalizar los nombres de sus elementos de menú favoritos en su propia lista privada organizando, editando y eliminando el contenido de su lista.

Administre sus favoritos de la siguiente manera:

- Añadir favoritos
- Ver favoritos
- Editar favoritos
- Eliminar favoritos

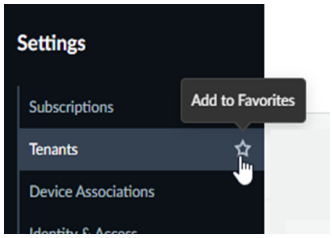
Añadir favoritos

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)* • Cortafuegos NGFW *(con gestión de la configuración de Strata Cloud Manager o Panorama)*	❑ Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Cualquier Inquilino o Grupos de servicios para inquilinos (TSG) es compatible con la aplicación ❑ Un rol dependiendo de sus necesidades

Si tiene elementos de menú o páginas en Strata Cloud Manager donde necesita ir repetidamente, pero ya no quiere buscarlos ni navegar hasta ellos, puede guardar estos elementos en una lista de favoritos.

STEP 1 | Vaya al elemento del menú o a la página que desea guardar.

STEP 2 | Pase el cursor sobre el elemento para ver el icono de estrella.



STEP 3 | Selecciona la estrella para añadir este artículo a sus **Favoritos**.

Los elementos del menú de nivel superior no se pueden añadir como favoritos. Sólo se pueden añadir submenús como favoritos.

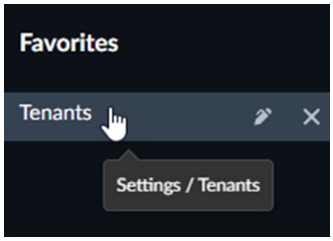
Ver favoritos

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)* • Cortafuegos NGFW *(con gestión de la configuración de Strata Cloud Manager o Panorama)*	❑ Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Cualquier Inquilino o Grupos de servicios para inquilinos (TSG) es compatible con la aplicación ❑ Un rol dependiendo de sus necesidades

Después de añadir favoritos, puede ver sus favoritos y sus ubicaciones originales.

STEP 1 | Seleccione **Favorites (Favoritos)**.

STEP 2 | Coloque el cursor sobre el elemento para ver el icono de ubicación.



STEP 3 | Se muestra la ruta a la ubicación real y el nombre del menú.

Al hacer clic en el elemento de la lista de favoritos, se accede a su ubicación original.

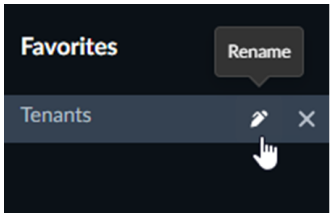
Editar favoritos

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)* • Cortafuegos NGFW *(con gestión de la configuración de Strata Cloud Manager o Panorama)*	❑ Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Cualquier Inquilino o Grupos de servicios para inquilinos (TSG) es compatible con la aplicación ❑ Un rol dependiendo de sus necesidades

Después de añadir favoritos, puede editarlos para personalizarlos.

STEP 1 | Seleccione **Favorites (Favoritos)**.

STEP 2 | Pase el cursor sobre el elemento para ver el icono de edición.



STEP 3 | Cambie el nombre del elemento.

Cambiar el nombre del elemento en su lista de favoritos no cambia el nombre original del elemento en su ubicación original.

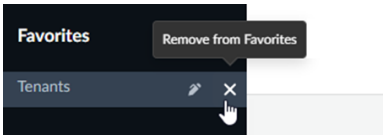
Eliminar favoritos

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access *(con gestión de la configuración de Strata Cloud Manager o Panorama)* • Cortafuegos NGFW *(con gestión de la configuración de Strata Cloud Manager o Panorama)*	❑ Cada una de estas licencias incluye acceso a Strata Cloud Manager: ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Cualquier Inquilino o Grupos de servicios para inquilinos (TSG) es compatible con la aplicación ❑ Un rol dependiendo de sus necesidades

Después de añadir favoritos, puede eliminar favoritos de su lista.

STEP 1 | Seleccione **Favorites (Favoritos)**.

STEP 2 | Coloque el cursor sobre el elemento para ver el icono de eliminación.



STEP 3 | Haga clic en el icono para eliminar el favorito de la lista.

Al eliminar el elemento de la lista de favoritos, no se elimina el elemento original de su ubicación original.

Configuración: Strata Cloud Manager

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	☑ Cualquier Inquilino o Grupos de servicios para inquilinos (TSG) es compatible con la aplicación ☐ Un rol dependiendo de sus necesidades ☐ Strata Logging Service para gestionar logs

De **Settings (Configuración)**, puede gestionar los procesos que pertenecen a todos los servicios ofrecidos en Strata Cloud Manager. Estos procesos incluyen:

Suscripciones

Vea las suscripciones aprobadas para su producto.

Gestionar suscripciones.

Device Associations

Se utiliza con mayor frecuencia en la incorporación de dispositivos y aplicaciones, **Device Associations** le permite:

- Asociar nuevos dispositivos a un inquilino
- Asociar aplicaciones con sus dispositivos
- Gestionar asociaciones de dispositivos y aplicaciones

Introducción a Asociaciones de dispositivos.

Productos

Si tiene un entorno de un solo inquilino, vea, inicie y gestione sus productos:

- Obtener información del producto
- Cambiar el nombre de la instancia
- Gestionar el uso compartido
- Añadir un inquilino

Introducción a Gestión de productos.

Inquilinos

Si es un proveedor de servicios de seguridad gestionados (MSSP) o una empresa distribuida, puede crear y gestionar su jerarquía de organizaciones y unidades empresariales, representadas por inquilinos. De **Tenants (Inquilinos)**, puede:

- Añadir un inquilino
- Editar un inquilino
- Gestionar licencias de inquilino
- Eliminar un inquilino
- Transición de una implementación de un solo inquilino a una implementación de varios inquilinos

Introducción a la gestión de inquilinos.

Identidad y acceso

Controle la autenticación y autorización de roles de usuario y permisos para todas las aplicaciones y el acceso basado en API. A través de Identidad y acceso, puede gestionar:

- Acceso del usuario
- Cuentas de servicio
- Roles (Roles)
- Integración de proveedores de identidad de terceros

Introducción a Identidad y acceso.

Logs de auditoría

Ver logs de todas las acciones iniciadas por los usuarios de Strata Cloud Manager

Ver logs de auditoría.

Gestión de licencias ION

Genere tokens de autorización para dispositivos ION virtuales. Esto proporciona un conjunto de controles para evitar la adición no autorizada de dispositivos virtuales a un entorno.

Gestionar licencias ION.

Preferencias del usuario

Personalice sus preferencias para que se adapten a sus necesidades. Por ejemplo, elija el modo de visualización.

Configurar las preferencias del usuario.

Lista de IP de confianza

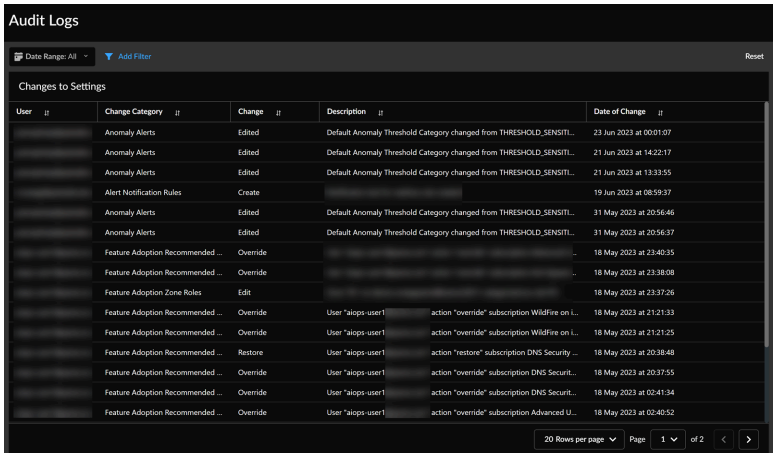
Use las listas de direcciones IP de confianza para restringir el acceso a las aplicaciones especificando las direcciones IP permitidas por inquilino.

Configurar una lista de IP de confianza.

Configuración: Logs de auditoría

¿Dónde puedo usar esto?	¿Qué necesito?
• Strata Cloud Manager	❑ Uno de estos: • aplicación AIOps for NGFW Free • AIOps for NGFW Premium (utilice la aplicación Strata Cloud Manager) • Strata Cloud Manager Essentials • Strata Cloud Manager Pro ❑ Cualquiera de los siguientes roles predefinidos: Auditor, Administrador empresarial, Administrador de seguridad de datos, Administrador de implementación, Administrador de IAM, Administrador de IAM multiinquilino, Usuario administrador multiinquilino, Usuario de supervisión multiinquilino, Superusuario multiinquilino, Administrador de red, Administrador de seguridad, Analista de SOC, Superusuario, Asistencia técnica de nivel 1, Asistencia técnica de nivel 2, Administrador de solo visualización

En **Settings > Audit Logs (Configuración > Logs de auditoría)**, puede ver una lista de acciones iniciadas por los usuarios de Strata Cloud Manager. Proporciona logs de los cambios realizados, el propietario del cambio, la fecha y hora del cambio y la descripción del cambio. Puede utilizar estos logs para fines de cumplimiento y resolución de problemas. Puede filtrar los logs de auditoría por rango de fechas con la capacidad, por un usuario, categoría y tipo de cambio.



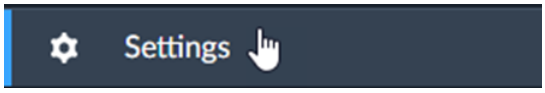
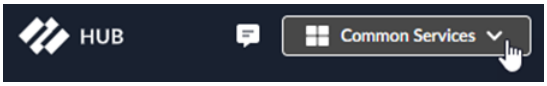
Configuración: Lista de IP de confianza

¿Dónde puedo usar esto?	¿Qué necesito?
• Strata Cloud Manager	❑ Rol de IAM de Superusuario, Superusuario multiinquilino, Administrador IAM multiinquilino o cualquier rol personalizado con el conjunto de permisos "Lista de IP de confianza"

Las aplicaciones en la nube ofrecen la comodidad de la accesibilidad desde cualquier parte del mundo. Sin embargo, esto permite la exposición a riesgos como el acceso con credenciales robadas, ataques de diccionario y otras formas de ataques de fuerza bruta para obtener acceso a las aplicaciones.

Si bien la Gestión de identidad y acceso mitiga parte de este riesgo, puede usar Listas de IP fiables (Trusted IP Lists) para restringir aún más el acceso a sus aplicaciones especificando las direcciones IP permitidas por inquilino.

De forma predeterminada, durante la creación de un nuevo inquilino, se permite el acceso tanto a la interfaz web como a la API desde cualquier dirección IP. La Lista de IP de confianza es una lista de direcciones IP de confianza que pueden acceder a un inquilino. Puede usar una lista de direcciones IP de confianza para limitar el acceso a un solo inquilino, o puede usarla para limitar el acceso a un inquilino primario y sus secundarios en una jerarquía de múltiples inquilinos. En una jerarquía de varios inquilinos, se añade la lista de direcciones IP de confianza en el inquilino principal, la lista se hereda del inquilino principal a sus inquilinos secundarios y se aplica de arriba hacia abajo.

Cómo gestionar una lista de IP de confianza desde Strata Cloud Manager	Cómo gestionar una lista de IP de confianza desde el hub
Para gestionar una lista de IP de confianza desde Strata Cloud Manager, seleccione **Settings (Configuración)** > **Trusted IP List (Lista de direcciones IP de confianza)**.  Puede gestionar listas de IP de confianza desde Strata Cloud Manager y la interfaz web de Strata Cloud Manager y la API permitirá el acceso solo a esas IP fiables.	Para gestionar una Lista de IP de confianza desde el hub, seleccione la **tenant view of the hub (vista de inquilino del hub** > **Common Services (Servicios Comunes)** > **Trusted IP List (Lista de IP de confianza)**.  Puede gestionar listas de IP de confianza desde el hub, pero el hub está exento de la aplicación de IP de confianza, por lo que su acceso al hub no está limitado a las IP de confianza. Si su dirección IP se bloquea a partir de un inquilino en Strata Cloud Manager al que debería poder acceder, puede ir al hub y desbloquear su acceso si tiene los permisos enumerados.

Añadir direcciones IP de confianza

¿Dónde puedo usar esto?	¿Qué necesito?
• Strata Cloud Manager	❑ Rol de IAM de Superusuario, Superusuario multiinquilino, Administrador IAM multiinquilino o cualquier rol personalizado con el conjunto de permisos "Lista de IP de confianza"

Después de activar su licencia, crear los inquilinos y gestionar el acceso de los usuarios a Strata Cloud Manager, podrá restringir aún más el acceso a sus inquilinos añadiendo direcciones IP de confianza a una lista de direcciones IP de confianza. De forma predeterminada, se permite el acceso a cualquier dirección IP.

Agregue direcciones IP de confianza mediante Strata Cloud Manager.

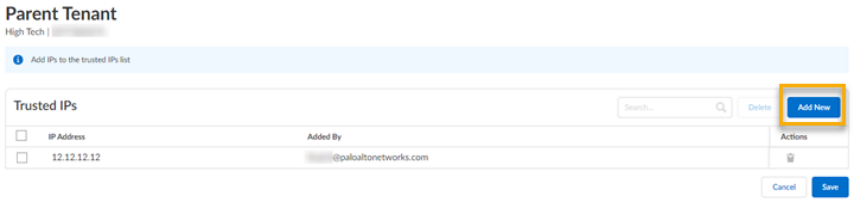
STEP 1 | Seleccione **Settings (Configuración)** > **Trusted IP List (Lista de direcciones IP de confianza)**.

STEP 2 | Busque o desplácese para buscar y seleccionar su inquilino.

STEP 3 | Seleccione **Add new (Añadir nuevo)**.

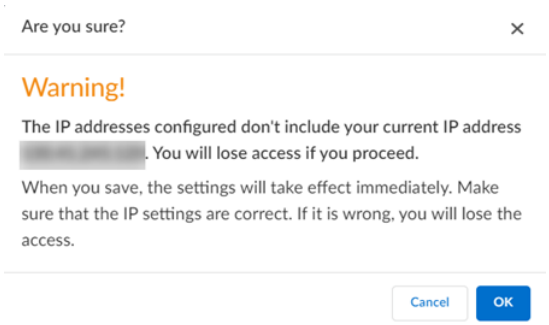
STEP 4 | Introduzca un **IP Address (Dirección IP)** que puede acceder a este inquilino.

- El campo es compatible con la notación CIDR. Solo se permiten direcciones IPv4.
- Puede usar una sola dirección IP o puede usar un intervalo con una máscara de subred como 12.12.12.1/30.
- La IP y el rango se validan, por lo que se muestran los errores de los elementos no compatibles.
- El campo **Added By (Añadido por)** se rellena automáticamente.



STEP 5 | **Save (Guardar).**

El cambio surte efecto inmediatamente, así que asegúrese de que su dirección IP sea correcta o puede perder el acceso al inquilino.



STEP 6 | Después de añadir una lista de direcciones IP de confianza en el inquilino principal, la lista se hereda del inquilino principal a sus inquilinos secundarios y se aplica de arriba hacia abajo. Un inquilino secundario también puede añadir su propia lista de direcciones IP de confianza.

Eliminar direcciones IP de confianza

¿Dónde puedo usar esto?	¿Qué necesito?
• Strata Cloud Manager	❑ Rol de IAM de Superusuario, Superusuario multiinquilino, Administrador IAM multiinquilino o cualquier rol personalizado con el conjunto de permisos "Lista de IP de confianza"

Después de que usted añada direcciones IP de confianza a una lista de direcciones IP de confianza para el inquilino, puede volver al acceso sin restricciones eliminando las direcciones IP de confianza.

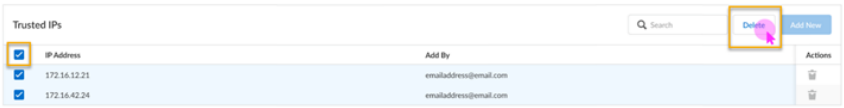
Elimine direcciones IP de confianza utilizando Strata Cloud Manager.

STEP 1 | Seleccione **Settings (Configuración)** > **Trusted IP List (Lista de direcciones IP de confianza)**.

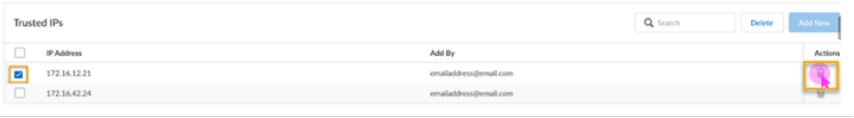
STEP 2 | Busque o desplácese para buscar y seleccionar su inquilino.

STEP 3 | Utilice una de las siguientes opciones:

- Eliminar varias direcciones IP: seleccione la opción **IP Address (Dirección IP)** para resaltar todas las direcciones IP al mismo tiempo y, a continuación, seleccione el botón **Delete (Eliminar)**.



- Eliminar una sola IP: seleccione la casilla de verificación individual de la IP y, a continuación, elimine de **Actions (Acciones)** > **Delete (Eliminar)**.



Si heredó una lista de direcciones IP de confianza de un inquilino primario, no es posible eliminarla de un inquilino secundario porque es heredada. Solo puede eliminar una lista de direcciones IP de confianza de un inquilino secundario si la añadió directamente en el nivel secundario.

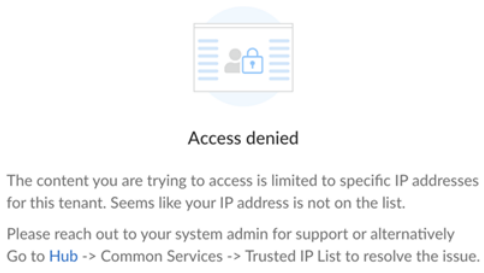
STEP 4 | Seleccione **OK (Aceptar)** en la solicitud.

El cambio entra en vigor inmediatamente. Si elimina todas las direcciones IP de confianza, el acceso a las direcciones IP vuelve a **Any (Cualquiera)**.

Desbloquear acceso

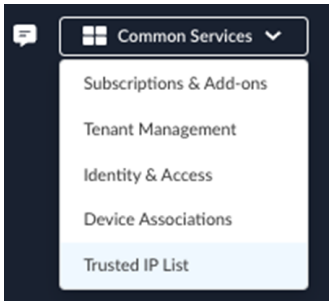
¿Dónde puedo usar esto?	¿Qué necesito?
• Strata Cloud Manager	☐ Rol de IAM de Superusuario, Superusuario multiinquilino, Administrador IAM multiinquilino o cualquier rol personalizado con el conjunto de permisos "Lista de IP de confianza"

Después de añadir direcciones IP de confianza a una lista de IP de confianza para su inquilino, Strata Cloud Manager se encarga de hacer cumplir ese acceso. Si su dirección IP no está en la lista de direcciones IP de confianza del inquilino, verá un mensaje de acceso denegado si intenta acceder a ella.

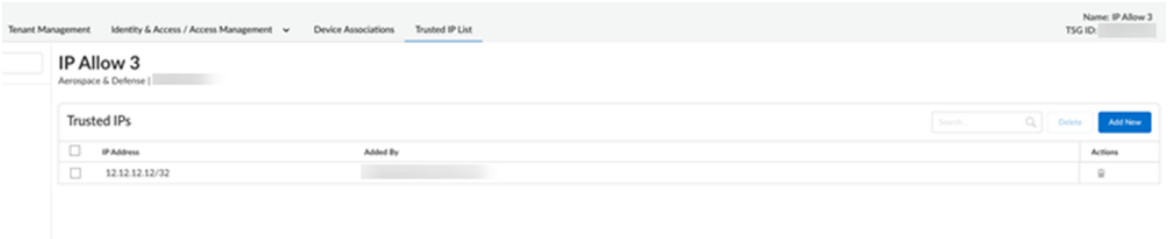


Si su dirección IP es bloqueada por un inquilino al que debería tener acceso, puede ir al hub para desbloquearse si tiene los permisos enumerados.

STEP 1 | En el hub, seleccione **tenant view of the hub (vista de inquilino del hub** > **Common Services (Servicios comunes)** > **Trusted IP List (Lista de IP de confianza)**.



STEP 2 | Añada su dirección IP a la lista de direcciones IP de confianza.



Configuración: Preferencias del usuario

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Strata Cloud Manager	Uno de estas: ❑ Licencia de AIOps for NGFW Free o AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro

En **Configuración > Preferencias de usuario**, puede personalizar Strata Cloud Manager para adaptarse a sus necesidades específicas modificando las `Preferencias de usuario`. Esta configuración incluye lo siguiente:

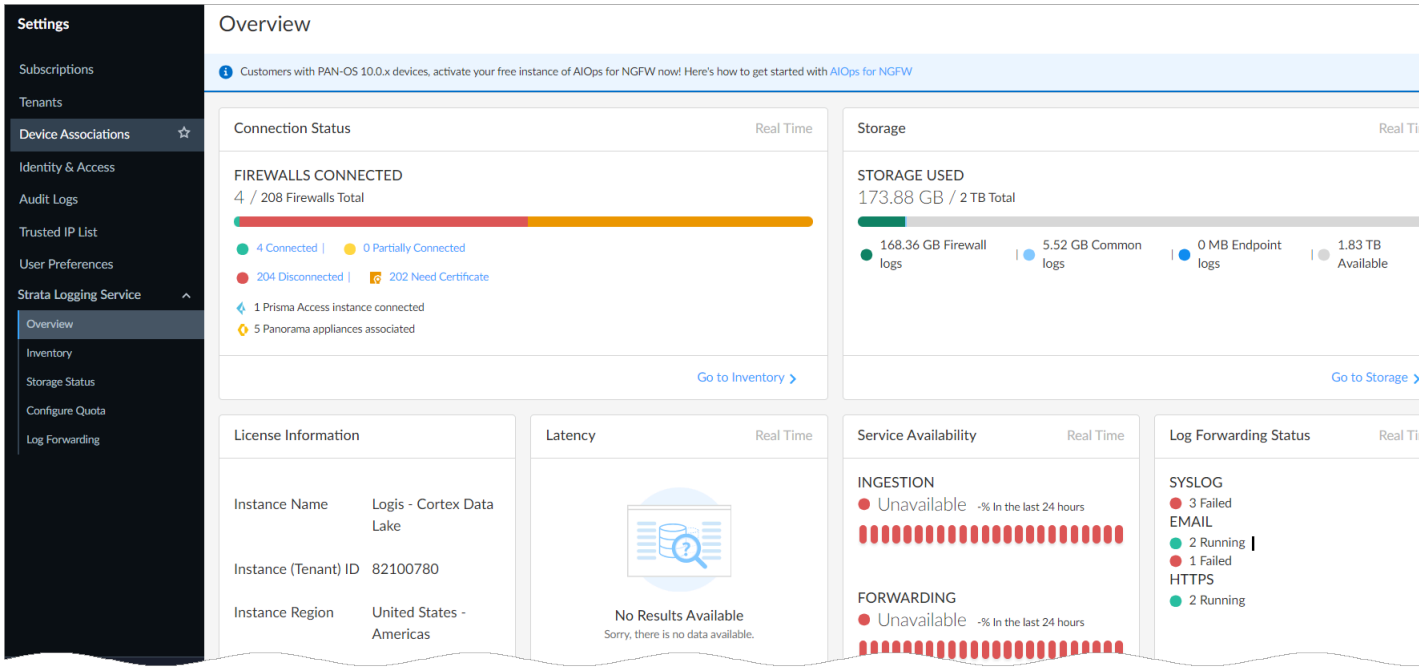
- **Light/Dark/System Mode (Modo claro/oscuro/sistema)**: elija entre los modos de visualización oscuro y claro o elija seguir su propia configuración del sistema.

Configuración: Strata Logging Service

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by PAN-OS or Panorama) • NGFW (Managed by Strata Cloud Manager)	❑ Strata Logging Service

Strata Logging Service (anteriormente Cortex Data Lake) es un sistema de registro de logs basado en la nube que almacena logs de red mejorados y ricos en contexto generados por nuestros productos de seguridad, incluidos nuestros NGFW, Prisma Access y Cloud NGFW para AWS. Con Strata Logging Service, puede recopilar volúmenes de datos en constante expansión sin necesidad de planificar los procesos y el almacenamiento locales, y está listo para escalar desde el principio. Aprenda cómo activar e implementar Strata Logging Service en su producto.

Además, también puede acceder y gestionar logs con la aplicación de Strata Logging Service disponible en el hub. Los datos de registro de logs son los mismos en la aplicación deStrata Logging Service y Strata Cloud Manager, a excepción de su diferencias en la interfaz web.



Use Strata Logging Service para:

- Comprobar el estado de una instancia de Strata Logging Service: haga clic en **Strata Logging Service** > **Overview (Visión general)**
- Vea e incorpore cortafuegos, Cloud NGFW, Prisma Access o dispositivos Panorama: haga clic en **Strata Logging Service** > **Inventory (Inventario)**
- Vea la cuota de almacenamiento de logs asignada, el espacio de almacenamiento disponible y el número de días que se conservan los logs en función de la tasa de logs entrantes: haga clic en **Strata Logging Service** > **Storage Status (Estado de almacenamiento)**
- Configure la cuota de almacenamiento de logs: haga clic en **Strata Logging Service** > **Configure Quota (Configurar cuota)**
- Busque, filtre y exporte datos de logs: haga clic en **Incidents & Alerts (Incidentes y alertas)** > **Log Viewer (Visor de logs)**. El visor de logs tiene las mismas características que Explore en la aplicación de Strata Logging Service.
- Reenviar datos de logs a servidores externos para almacenamiento a largo plazo, SOC o auditoría interna: haga clic en **Strata Logging Service** > **Log Forwarding (Reenvío de logs)**

Experiencia de aplicación

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	Cualquiera de estas licencias: ❑ licencia de Prisma Access ❑ licencia de ADEM Observability o licencia de AI-Powered ADEM

Utilice la página **Application Experience (Experiencia de aplicación)** para gestionar sus usuarios de Autonomous DEM y sitios remotos. Consulte los logs de auditoría para ver qué administradores se han autenticado en Prisma Access durante el **intervalo de tiempo** seleccionado.

Consulte la sección Gestionar actualizaciones del agente de Autonomous DEM para obtener información sobre las **Upgrade Options. (Opciones de actualización).**

Gestión de agentes de endpoints

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	Cualquiera de estas licencias: ❑ licencia de Prisma Access ❑ licencia de ADEM Observability o licencia de AI-Powered ADEM

Utilice esta pestaña para obtener detalles sobre todos los usuarios de ADEM registrados, como si el usuario está en línea (el dispositivo de usuario está enviando mensajes de mantenimiento activo al servicio ADEM) o sin conexión (el servicio ADEM no ha recibido un mensaje de mantenimiento activo del dispositivo de usuario en los últimos diez minutos), cuándo se vio por última vez el dispositivo de usuario, el nombre de usuario, el tipo de dispositivo y el nombre de host del usuario ADEM, y qué versión del agente ADEM está ejecutando.

Cada fila de la tabla de esta ficha representa un usuario único en una fila separada. Cada combinación usuario/dispositivo se considera como un usuario único. Por ejemplo, si 2 usuarios han iniciado sesión en 3 dispositivos cada uno, el número de usuarios únicos será 6. Por lo tanto, un nombre de usuario podría duplicarse en varias filas dependiendo del número de dispositivos en los que se haya iniciado sesión.

En el título de la tabla de este widget, el número de **Total Endpoint Agents (Agentes totales de endpoint)** indica el número total de dispositivos supervisados. El número de **Users (Usuarios)** es el total de usuarios independientemente del número de dispositivos en los que hayan iniciado sesión. Esto se debe a que el consumo de licencia se basa en el número total de usuarios, independientemente de cuántos dispositivos haya iniciado sesión cada usuario.

Utilice las casillas de verificación a la izquierda del **Last logged in User (Último usuario conectado)** para realizar una configuración masiva seleccionando la fila para los endpoints. Eliminar una entrada seleccionándola de la tabla Gestión de agentes de endpoint liberará la entrada de licencia.

Nombre de columna	Description (Descripción)
Último usuario conectado	Un dispositivo puede tener varios usuarios iniciando sesión en él. Esta columna muestra el ID de usuario del usuario más reciente que ha iniciado sesión en GlobalProtect con este dispositivo.
Dispositivo	El sistema operativo que se ejecuta en este dispositivo.
Nombre de host	El nombre del host del dispositivo.
Last Seen	El último mensaje enviado desde el dispositivo al servidor DEM.
First Seen	El primer mensaje recibido de este dispositivo por el servidor DEM.
Estado del usuario	Estado de conexión del usuario actual.
Estado de supervisión	Si las pruebas de la aplicación se ejecutan en el dispositivo.
Versión del agente de endpoint	La versión del agente ADEM instalado en el dispositivo.

Gestión de agentes de sitio remoto

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	Cualquiera de estas licencias: ❑ licencia de Prisma Access ❑ licencia de ADEM Observability o licencia de AI-Powered ADEM

Esta pestaña le da detalles sobre los dispositivos Prisma SD-WAN ION de sucursal que están habilitados para la gestión de experiencias digitales. Utilice esta pestaña para obtener detalles sobre todos sus sitios remotos ADEM registrados, como el modelo del dispositivo, el nombre del host, el estado del sitio, el estado de supervisión (si la supervisión está habilitada para el sitio), el nombre del host del servidor de alta disponibilidad (si lo hay) y la versión del agente del sitio remoto.

Nombre de columna	Description (Descripción)
Nombre del sitio remoto	Sucursal de Pisma SD-WAN.
Modelo de dispositivo	Número de modelo del dispositivo Prisma SD-WAN ION.
Nombre de host	Nombre de host del dispositivo ION.
Nombre de host del par de alta disponibilidad	Si se ha configurado un dispositivo ION de reserva de alta disponibilidad en ese sitio.
Last Seen	El último mensaje enviado desde el dispositivo ION al servidor DEM.
First Seen	El primer mensaje recibido por el servidor DEM del dispositivo ION.
Estado del sitio	Estado de conectividad del dispositivo ION del sitio con el agente DEM.
Estado de supervisión	Si el sitio está configurado para ejecutar pruebas de aplicaciones.
Versión del agente de sitio remoto	La versión del agente ADEM instalado en el dispositivo ION.

Perfiles de puntuación de estado

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	Cualquiera de estas licencias: ❑ licencia de Prisma Access ❑ licencia de ADEM Observability o licencia de AI-Powered ADEM

Consulte los detalles de la puntuación de estado del dominio en esta pestaña.

Nombre de columna	Description (Descripción)
Nombre de la métrica de puntuación de estado del dominio	Enumera los dominios para los que se calculan las métricas de puntuación de estado. Haga clic en un nombre de dominio en esta columna para ver sus métricas, como los umbrales inferior y superior, y el impacto (porcentaje de la puntuación total de la experiencia) que tiene en la puntuación total cuando los

Nombre de columna	Description (Descripción)
	números cruzan el umbral. Actualmente, estas métricas son de solo lectura según lo establecido por el administrador. No se pueden modificar.
Tipo	Tipo de dominio
Caso de uso asociado	El panel o widget en el que se muestra la puntuación de experiencia calculada.

Logs de auditoría ADEM

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	Cualquiera de estas licencias: ❑ licencia de Prisma Access ❑ licencia de ADEM Observability o licencia de AI-Powered ADEM

Vea los logs de auditoría de todos los eventos que se activan debido a las llamadas a la API.

Nombre de columna	Description (Descripción)
Hora del evento	El momento en que se desencadenó el evento que hizo que se creara el log.
Correo electrónico	Dirección de correo electrónico de la persona que fue notificada cuando se creó el log.
Description (Descripción)	La llamada a la API que provocó que el evento se activara creando así el registro.

