Prácticas recomendadas para gestionar cortafuegos con Panorama

10.0 (EoL)

techDOCS paloalto NETWORKS

Contact Information

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

About the Documentation

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

Copyright

Last Revised

December 3, 2020

Table of Contents

Prácticas recomendadas para añadir cortafuegos a Panorama

El servidor de gestión de Panorama™ es la solución de gestión de seguridad de red de Palo Alto Networks para la gestión centralizada y la visibilidad de sus cortafuegos de última generación. Este documento cubre las prácticas recomendadas para incorporar nuevos cortafuegos o migrar cortafuegos existentes a Panorama, para simplificar y agilizar esta operación.

> Caso de uso: Incorporación de nuevos cortafuegos de última generación a Panorama
> Caso de uso: Migración de sus cortafuegos de última generación a Panorama

Caso de uso: Incorporación de nuevos cortafuegos de última generación a Panorama

El primer caso de uso para comenzar con el servidor de gestión de Panorama™ es añadir un cortafuegos recién implementado como un dispositivo gestionado a Panorama.

STEP 1 | **Associate Devices (Asociar dispositivos)** o **Import (Importar)** varios cortafuegos para agilizar el proceso de incorporación.

- Asocie los cortafuegos a un grupo de dispositivos, pila de plantillas, Grupo de recopiladores y Recopilador de logs a medida que los añade a Panorama desde una ubicación en lugar de asociar manualmente los cortafuegos después de que se hayan añadido correctamente a Panorama.
- Si añade un gran número de cortafuegos, importe todos sus cortafuegos nuevos a Panorama en un archivo CSV. Este archivo CSV le permite asociar todos sus cortafuegos a un grupo de dispositivos, una pila de plantillas, un grupo de recopiladores y un recopilador de logs en lugar de asociarlos manualmente. Esta opción es especialmente ventajosa cuando se añade un gran número de cortafuegos donde la asociación manual de cortafuegos llevaría mucho tiempo en completarse.

STEP 2 | Habilite **Auto Push on 1st Connect (Enviar automáticamente al conectar por primera vez)** y configure **To SW Version (A versión de software)** para enviar automáticamente el grupo de dispositivos y las configuraciones de la pila de plantillas a sus cortafuegos gestionados cuando se conecten con éxito por primera vez a Panorama, y actualice sus cortafuegos gestionados a una versión de PAN-OS específica de su elección. Esto incluye la instalación automática de todas las actualizaciones de contenido necesarias para cada versión de PAN-OS en la ruta de actualización de PAN-OS.

- Si va a importar todos sus nuevos cortafuegos a Panorama en un archivo CSV, habilite **Auto Push on 1st Connect (Enviar automáticamente al conectar por primera vez)** y configure **To SW Version (A versión de software)** en el archivo CSV para agilizar el proceso de importación.
- Al implementar el control de acceso basado en funciones, utilice administradores de grupos de dispositivos y plantillas para añadir cortafuegos a grupos de dispositivos y plantillas dentro de su dominio de acceso, en lugar de habilitar privilegios de superusuario para todos los administradores de Panorama.

STEP 3 | Después de añadir correctamente sus cortafuegos a Panorama, cree y aplique etiquetas para que sea más fácil buscar y filtrar en sus cortafuegos gestionados. Esto le ayudará a mantener organizados sus cortafuegos gestionados a medida que crece el número de cortafuegos que gestiona con Panorama.

STEP 4 | Si planifica implementar cortafuegos en sitios remotos con poco o ningún personal de TI, debe utilizar la Configuración de Zero Touch Provisioning (ZTP) para agilizar la implementación inicial del cortafuegos automatizando la incorporación de un nuevo cortafuegos gestionado sin la necesidad de administradores de red o TI en el sitio remoto.

Caso de uso: Migración de sus cortafuegos de última generación a Panorama

El segundo caso de uso para comenzar con el servidor de gestión de Panorama™ es la Transición de cortafuegos existentes a Panorama. Si es posible, trabaje con su ingeniero de ventas o ingeniero de servicios profesionales de Palo Alto Networks durante la migración para asegurarse de que las configuraciones de su cortafuegos se migren correctamente a Panorama.

STEP 1 | La planificación es clave; antes de comenzar la migración, asegúrese de haber entendido lo siguiente:

- Revise la Matriz de compatibilidad de Palo Alto Networks para entender la compatibilidad entre Panorama y los cortafuegos, en los recopiladores de logs, y las versiones de contenido para asegurarse de que no se encuentren errores de compatibilidad durante la migración.
- Planifique la jerarquía de su grupo de dispositivos y de la plantilla de forma que reduzca la redundancia y agilice la gestión de los ajustes que se comparten entre todos los cortafuegos dentro de un conjunto de cortafuegos.
- Prepare un plan de prueba posterior a la migración para verificar el tráfico clave y el tráfico de aplicaciones después de migrar con éxito su cortafuegos a Panorama.

STEP 2 | Cuando migra un cortafuegos a la gestión de Panorama, habilite **Import devices' shared objects into Panorama's shared context (Importar objetos compartidos de los dispositivos en el contexto compartido de Panorama)** para evitar duplicar objetos de configuración idénticos.

STEP 3 | Después de una migración correcta, revise las **Policies (Políticas)** para identificar cualquier regla duplicada. Elimine una de cada regla duplicada antes de **Commit (Confirmar)** en Panorama para evitar errores de confirmación.

STEP 4 | Al **Export or push device config bundle (Exportar o insertar el paquete de configuración del dispositivo)** a sus cortafuegos gestionados debe habilitar **Merge with Candidate Config (Combinar con configuración candidata)**, **Include Device and Network Templates (Incluir dispositivos y plantillas de red)** y **Force Template Values (Forzar valores de plantilla)** para forzar una confirmación para cualquier cambio local pendiente en el cortafuegos; incluya todos los grupos de dispositivos y plantillas en el envío y elimine cualquier configuración local que no esté presente en un grupo de dispositivos o plantilla en Panorama. Esto garantiza que una configuración básica gestionada por Panorama se envíe a todos los cortafuegos migrados a Panorama.

STEP 5 | Realice sus pruebas posteriores a la migración para verificar que la migración se haya realizado correctamente y que todo funcione según lo previsto. A medida que pasa el tiempo, optimice la configuración cuando lo considere necesario. Utilice herramientas de migración como Expedition para evaluar periódicamente el estado de su configuración, eliminando los objetos duplicados o no utilizados, y Policy Optimizer para optimizar su base de reglas de políticas de seguridad.

Prácticas recomendadas para la gestión de la configuración del cortafuegos en Panorama

Los cortafuegos tienen dos tipos de configuraciones: seguridad y red. Panorama utiliza grupos de dispositivos para gestionar las configuraciones de seguridad, como objetos y reglas de políticas, y plantillas y pilas de plantillas para gestionar las configuraciones de red.

- Gestión de las configuraciones de su grupo de dispositivos en Panorama
- Gestión de la configuración de su plantilla y la pila de plantillas en Panorama
- Gestión de las variables de la plantilla y la pila de plantillas en Panorama

Gestión de las configuraciones de su grupo de dispositivos en Panorama

Los grupos de dispositivos proporcionan una forma de organizar y reutilizar sus políticas aplicando el principio de herencia e implementando una jerarquía de grupos de dispositivos bien definida. Si bien Panorama le permite reutilizar la misma configuración de grupo de dispositivos en varios grupos de dispositivos en una jerarquía, también puede personalizar cualquier configuración local para anular cualquier configuración heredada.

- Al diseñar su jerarquía de grupos de dispositivos, tenga en cuenta sus necesidades funcionales o regionales y comprenda la diferencia entre reglas previas y reglas posteriores.

  Por ejemplo, cree las reglas previas de seguridad que desea que los cortafuegos gestionados apliquen sin excepción mientras crea reglas posteriores de seguridad para que actúen como limpieza para cualquier tráfico que no coincida con una regla previa de seguridad.
- Evite el uso excesivo del grupo de dispositivos **Shared (Compartido)** para no superar los límites de capacidad de los cortafuegos gestionados más pequeños. La gestión de los objetos de configuración en el nivel de grupo de dispositivos adecuado ayuda a minimizar el número de cortafuegos `sin sincronización` de manera más eficiente porque todos los cortafuegos se vuelven `sin sincronización` si el objeto de una sola configuración compartida se modifica.
- Configure regiones personalizadas mediante el uso de objetos de dirección personalizados para especificar rangos de direcciones o geolocalizaciones.

  Si bien las empresas utilizan el espacio de direcciones RFC 1918, las políticas que gobiernan toda la red 10.0.0x no son útiles. En su lugar, defina regiones personalizadas mediante el uso de objetos de dirección personalizados para especificar rangos de direcciones o geolocalizaciones. Esto le permite crear políticas más pormenorizadas y relevantes para reducir su superficie de ataque.
- Configure el **Master Device (Dispositivo maestro)** para cada grupo de dispositivos para permitir que Panorama recopile asignaciones de grupos de usuarios. Tener un Dispositivo maestro configurado en el grupo de dispositivos hace que los grupos de usuarios estén disponibles al crear reglas de políticas. Además, puede filtrar las pestañas ACC y Monitor (Supervisar) utilizando las asignaciones de grupos de usuarios recopiladas por Panorama.
- Para completar una configuración de seguridad, asocie **Reference Templates (Plantillas de referencia)** para hacer referencia a los objetos de configuración de red incluidos en una plantilla a la que no pertenece el cortafuegos gestionado. Esto le permite aprovechar al máximo los objetos de configuración comunes en los grupos de dispositivos y las plantillas, sin hacer un uso excesivo del grupo de dispositivos **Shared (Compartidos)** o volver a crear objetos de configuración de red idénticos.

Gestión de la configuración de su plantilla y la pila de plantillas en Panorama

Utilice Plantillas y pilas de plantillas para reutilizar su red y los objetos de configuración de cortafuegos en sus cortafuegos gestionados para configuraciones comunes como registro de logs y alta disponibilidad (HA), a la par que le permite configurar plantillas modulares que se pueden combinar según sea necesario para varios cortafuegos gestionados en diferentes pilas de plantillas.

- Cambie a modular mediante la creación de plantillas con agrupaciones lógicas de configuraciones, incluso si la configuración no está completa. Recuerde, la configuración debe estar completa y todas las referencias resueltas en el nivel de pila de plantillas, no en todas las plantillas. Puede reutilizar, hacer referencia y anular objetos de diferentes plantillas para completar la configuración de la pila de plantillas.
- Cree plantillas específicas de modelos (por ejemplo, configuración de la interfaz de red) y plantillas específicas de casos de uso (por ejemplo, administradores, conjuntos de control de acceso basados en funciones). Esto le permite combinar las plantillas adecuadas cuando las añade a una pila de plantillas.
- Configure la pila de plantillas con las configuraciones de red que desea anular en una plantilla o localmente en el cortafuegos gestionado.

Gestión de las variables de la plantilla y la pila de plantillas en Panorama

Cree Variables de plantillas y pilas de plantillas para maximizar el uso compartido de la configuración y la reutilización de los objetos de configuración de red y dispositivos en sus cortafuegos gestionados.

- Utilice variables de plantillas y pilas de plantillas cuando sea apropiado para ayudar a gestionar la configuración de su cortafuegos gestionado con menos plantillas a la par que optimiza su configuración.

  Por ejemplo, las direcciones IP suelen variar de un cortafuegos a otro. Con las variables de plantilla, puede crear la configuración que necesita indicando una variable en lugar de una dirección IP. Cuando la configuración se envía a sus cortafuegos gestionados, Panorama puede completar la dirección IP correcta por cortafuegos en función del valor configurado por cortafuegos gestionado.
- Cree variables con el valor predeterminado **`Ninguno`** para asegurarse de que la configuración incorrecta no se envíe por error al cortafuegos gestionado.

  Una notable excepción a esto es una dirección IP de DNS. En el peor de los casos, el cortafuegos gestionado aún debería poder resolver las consultas de DNS.

Prácticas recomendadas para la gestión de cambios de configuración

Gestione los cambios de configuración que sus administradores pueden realizar aprovechando el control de acceso basado en funciones (RBAC) y segmentando el acceso a cortafuegos gestionados, utilizando estructuras dinámicas, como Listas dinámicas externas (EDL) y Grupos de usuarios dinámicos (DAG), para mantener las reglas de políticas actualizadas, y aprovechando el control granular sobre los cambios de configuración que los administradores pueden realizar y enviar a los cortafuegos gestionados.

- Gestión de funciones de administrador y acceso a dominios desde Panorama
- Simplifique las reglas de seguridad gestionadas por Panorama
- Gestión de cambios de configuración para equipos grandes
- Confirmación de sus cambios de configuración de Panorama
- Envíe los cambios de configuración de Panorama

Gestión de funciones de administrador y acceso a dominios desde Panorama

Una clave para la gestión correcta de la configuración en un entorno dinámico es poder asignar los privilegios adecuados a los miembros de su equipo. Panorama proporciona un amplio control de acceso basado en funciones (RBAC) que permite una definición detallada de las funciones. RBAC se puede combinar con dominios de acceso para facilitar el acceso segmentado a los cortafuegos gestionados. Esto ayuda a reducir su superficie de ataque y a evitar el uso indebido accidental o malintencionado de los privilegios de administrador.

Consulte las Prácticas recomendadas para el acceso administrativo de seguridad para obtener información más detallada sobre cómo controlar correctamente el acceso a su Panorama y las configuraciones de cortafuegos gestionados.

- Defina las funciones administrativas para ayudar a los administradores a gestionar con éxito los cortafuegos sin sobre aprovisionar su acceso.
- Cree dominios de acceso para sus administradores de Panorama, si tiene varios subconjuntos de cortafuegos con diferentes propósitos. Por ejemplo, si los cortafuegos de su centro de datos, cortafuegos perimetrales y cortafuegos de sucursales son gestionados por diferentes administradores de Panorama, configure y asigne dominios de acceso que restrinjan el acceso solo a los cortafuegos que administran.
- Cree administradores de plantillas y grupos de dispositivos para controlar mejor el acceso administrativo a los cortafuegos gestionados dentro de un dominio de acceso y una función de administrador. Esto ofrece el acceso más granular posible que permite a su equipo hacer su trabajo sin causar problemas operativos.

Simplifique las reglas de seguridad gestionadas por Panorama

La gestión de su política de seguridad es una de las tareas más importantes al gestionar su base de reglas de políticas.

- Haga que su base de reglas sea sensible a las aplicaciones mediante una combinación de Policy Optimizer y la utilización de las reglas de la política para realizar la transición a reglas de política de seguridad basadas en App-ID y User-ID.

  Cree Grupos de eso en sus reglas de política de seguridad para hacerlas más efectivas y legibles. Además, puede aprovechar las herramientas Expedition y Best Practice Asessment (BPA) para ayudar a repetir el proceso a través de las revisiones de su base de reglas, para fortalecer su estrategia de seguridad.
- Utilice Búsqueda global cuando evalúe su base de reglas de políticas para identificar objetos o reglas existentes. Esto ayudará a reducir el desorden innecesario en su configuración que generalmente ralentizará las confirmaciones en Panorama.
- Solucione los problemas de las reglas de su política para probar si un cambio de configuración de la regla de política propuesto ya ha sido gestionado por una regla existente que solo necesita modificación. Esto le permite reducir las reglas de políticas duplicadas y evitar que su base de reglas de políticas crezca demasiado.
- Utilice grupos de reglas basados en etiquetas para identificar el propósito, la función, el ciclo de vida u otras características de las reglas para ordenar y agrupar rápidamente reglas similares. Los grupos de reglas basados en etiquetas le permiten distinguir visualmente entre conjuntos de reglas dentro de una base de reglas, donde es posible gestionarlas como un grupo o modificarlas de forma individual.
- Aplique los comentarios de auditoría para la creación y modificación de reglas de política compatibles con la función operativa crítica de respaldar las auditorías de seguridad. Una regla con una serie bien documentada de comentarios de auditoría facilita la respuesta a una solicitud de auditoría en lugar de depender de descripciones de reglas o herramientas externas. Además, puede complementar los comentarios de auditoría introduciendo una descripción cuando confirma cambios de configuración en Panorama.
- Utilice construcciones dinámicas como Listas dinámicas externas, Grupos de direcciones dinámicas y Grupos de usuarios dinámicos para optimizar su configuración y simplificar el mantenimiento de su base de reglas de políticas de seguridad. A medida que cambia su entorno, puede modificarlas según sea necesario sin la necesidad de confirmar.
- Al crear su regla de política de seguridad, evite seleccionar uno o más cortafuegos gestionados en la pestaña **Target (Destino)**, ya que hace que el estado de sincronización de la configuración del cortafuegos gestionado no sea fiable.

  Esto se conoce comúnmente como focalización de políticas. La focalización de políticas se evalúa en el cortafuegos y no en Panorama. Como consecuencia, los cortafuegos gestionados a los que no se envía una regla de política pueden mostrarse erróneamente como `No sincronizados`. Diseñe su jerarquía de grupos de dispositivos para minimizar o evitar la necesidad de establecer políticas de destino.

Gestión de cambios de configuración para equipos grandes

Los errores de configuración se producen cuando un equipo grande aprovecha Panorama para la gestión de configuración centralizada. Panorama permite la manipulación pormenorizada utilizando las operaciones de configuración revertir, importar, exportar, cargar, fusionar y reemplazar. Estas operaciones se realizan a nivel de plantilla o grupo de dispositivos.

- Cuando intente revertir rápidamente la configuración de Panorama a un estado previamente conocido, considere revertir solo el grupo de dispositivos o la plantilla afectados en lugar de la configuración completa de Panorama.

  Esto ayuda a preservar los cambios de otros administradores que no realizaron ningún cambio de configuración en la plantilla o grupo de dispositivos afectados. Además, puede exportar la configuración para modificarla sin conexión y luego volver a importarla a Panorama cuando esté lista.
- Exporte los cambios de configuración en curso del grupo de dispositivos y la plantilla para enviar cualquier cambio de configuración de emergencia a los cortafuegos gestionados. Después de la exportación, revierte la configuración de Panorama para realizar los cambios de emergencia. Cuando los cambios se envían correctamente a los cortafuegos gestionados, puede importar la configuración de Panorama que incluía los cambios de configuración en curso.
- Si está consolidando múltiples configuraciones de Panorama, fusione de forma táctica su grupo de dispositivos y configuraciones de plantilla para consolidar la configuración en un único Panorama.

Confirmación de sus cambios de configuración de Panorama

Panorama ofrece muchas formas de controlar el proceso de confirmación. Vale la pena comprender qué son y adoptarlos en sus operaciones diarias.

- Cuando confirma los cambios de configuración de Panorama, seleccione **Commit Changes Made by (Confirmar los cambios realizados por)** para confirmar solo sus propios cambios y no confirmar los cambios de configuración realizados por otros administradores. Esto garantiza que otros cambios de configuración que están en curso o que aún no se han aprobado no se envíen por error a Panorama.
- Cuando solicita cambios de configuración, solicite a los administradores que realicen una **Preview Changes (Vista previa de los cambios)** y revisen el resumen de cambios. Una verificación visual de los cambios de configuración a menudo ayuda a detectar errores y ahorra tiempo en el mantenimiento operativo posterior.

Envíe los cambios de configuración de Panorama

Panorama proporciona muchas formas de controlar el envío de cambios de configuración a los cortafuegos gestionados. Vale la pena comprender qué son y adoptarlos en sus operaciones diarias.

- Antes de que los administradores envíen cambios de configuración a los cortafuegos gestionados, solicíteles que revisen la selección del ámbito de envío [**Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)** > **Edit Selections (Editar selecciones)**] para comprobar que la lista de cortafuegos de destino sea la correcta.

  Incluso si la jerarquía de grupos de dispositivos está diseñada correctamente y los cambios de configuración están bien planificados, puede haber escenarios en los que no haga falta enviar los cambios de configuración a todos los cortafuegos en un momento dado debido a los diferentes periodos de mantenimiento. Siempre es una práctica recomendada revisar la lista de cortafuegos de destino para asegurarse de que los cambios de configuración se envíen solo a los cortafuegos gestionados previstos.
- Utilice el ajuste **Force Template Values (Forzar valores de plantilla)** [**Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)** > **Edit Selections (Editar selecciones)**] con moderación. Un envío con este ajuste habilitado sobrescribe toda la configuración del cortafuegos gestionado, incluida cualquier configuración de cortafuegos local.

Prácticas recomendadas para la supervisión y la visibilidad en Panorama

Diseñe su infraestructura de registro de logs para una ingesta y un almacenamiento de logs óptimos según los requisitos de su organización. Luego, aproveche el Centro de control de aplicaciones (ACC), los informes de resumen en PDF y los informes personalizados para identificar la actividad de la red y las amenazas que deben investigarse y resolverse.

- Diseñe su infraestructura de registro
- Supervisión del Centro de comando de aplicaciones (ACC) y logs en Panorama
- Generación de informes estándar y personalizados en Panorama

Diseñe su infraestructura de registro

Es una buena práctica planificar y diseñar su infraestructura de registro antes de implementar nuevos cortafuegos gestionados. El servidor de gestión de Panorama proporciona múltiples modos para la gestión de dispositivos y la recopilación de logs. El modo Panorama le permite gestionar la configuración de su cortafuegos, e ingerir y almacenar logs. Si desea que su Panorama tenga una sola función, el modo de recopilación de logs, Log Collector, está diseñado únicamente para la ingestión y el almacenamiento de logs, mientras que el modo de solo gestión, Management Only, está diseñado únicamente para la gestión de la configuración del cortafuegos.

- Utilice la Guía de diseño y tamaño de Panorama para calcular la tasa de registro y determinar sus requisitos de almacenamiento de logs. Esto es importante a la hora de decidir la capacidad de almacenamiento de logs de sus recopiladores de registros y puede basarse en numerosos factores, como los requisitos normativos.

  Consulte a su ingeniero de ventas (SE) a la hora de medir su infraestructura de registro de logs. Ellos le proporcionarán la experiencia técnica necesaria para interpretar y personalizar su implementación para satisfacer sus necesidades.
- No utilice el modo heredado si está implementando un dispositivo virtual de Panorama, debido a las muchas limitaciones y restricciones de registro asociadas con este modo. Si bien es adecuado para un laboratorio o un entorno de demostración, evite utilizar un panorama en modo heredado en su entorno de producción.
- Utilice una interfaz independiente para la recopilación de logs en sus cortafuegos gestionados. Esto le ayuda a mantener el rendimiento de su interfaz de gestión que se comunica con Panorama. Como práctica recomendada de seguridad sólida, configure una lista de IP permitidas para todas las interfaces.

Supervisión del Centro de comando de aplicaciones (ACC) y logs en Panorama

El Centro de control de aplicaciones (ACC) es una herramienta de visualización interactiva diseñada para ayudarle a comprender rápidamente los eventos en su red. El ACC contextualiza los registros de su cortafuegos gestionado para permitirle obtener información sobre los patrones de tráfico e información procesable sobre amenazas que puede utilizar en sus investigaciones.

- Aprenda a utilizar todas las interacciones de datos disponibles en el ACC.
  - Utilice filtros ACC para analizar a fondo en busca de información específica, como direcciones o usuarios.
  - Aplique filtros globales para desplazarse en la pantalla del ACC en torno a los detalles que más le interesan y excluir la información no relacionada.
  - Si utiliza GlobalProtect, vea el widget **GlobalProtect Activity (Actividad de GlobalProtect)** para ver los informes HIP basados en logs de coincidencia HIP para comprender el estado de seguridad de los dispositivos finales que acceden a su red.
  - Una vez que haya delimitado la información que le interesa, deberá **Export (Exportar)** sus datos de ACC a formato CSV o widgets a formato PDF para compartirlos con su equipo para realizar más investigaciones o correcciones.
- Personalice el ACC para asegurarse de que se adapte a la actividad de red específica que le interesa supervisar.

  Esto le ayudará a mejorar su eficiencia a medida que investiga a un usuario o host en particular. Esto le permite tener información contextual completa sin tener que cambiar de pestaña o desplazarse demasiado.

  - Añada un nuevo widget al ACC y seleccione **Content Activity (Actividad de contenido)**.
  - Añada un nuevo widget al ACC y seleccione **URL Filtering (Filtrado de URL)**.
  - De forma predeterminada, se muestra el widget **Threat Activity (Actividad de amenazas)**. Si no se muestra, añada un nuevo widget y seleccione **Threat Activity (Actividad de amenazas)**.
- Seleccione **Objects (Objetos)** > **Regions (Regiones)** y cree regiones personalizadas con rangos de direcciones IP para usar en sus reglas de política de seguridad. El uso de regiones personalizadas hace que los eventos de red correlacionados en el ACC sean más relevantes.

  Por ejemplo, ha configurado regiones personalizadas para sus sucursales y ha notado que ciertas direcciones IP son responsables de una cantidad de tráfico sospechosamente grande. Al aprovechar las regiones personalizadas, puede correlacionar esta actividad de red sospechosa con una sucursal específica y tomar medidas para investigar y realizar acciones correctivas.

Generación de informes estándar y personalizados en Panorama

El servidor de gestión de Panorama™ le proporciona una forma de centralizar y agregar toda la información en la implementación de su cortafuegos para generar informes PDF y crear informes personalizados.

- Identifique y clasifique todas las aplicaciones SaaS que utiliza su organización como **Sanctioned (Sancionadas)** o **Unsanctioned (No sancionadas)**.

  Panorama y los cortafuegos gestionados consideran que cualquier aplicación sin la etiqueta de sanción no está autorizada para su uso en la red. Las aplicaciones SaaS no autorizadas pueden suponer una exposición a amenazas y la pérdida de datos privados y confidenciales. Es importante clasificar sus aplicaciones SaaS para investigar mejor la actividad de la red.

  1. Seleccione **Objects (Objetos)** > **Applications (Aplicaciones)**.
  2. Cree una aplicación SaaS personalizada según sea necesario.
  3. Seleccione una o más de sus aplicaciones SaaS y seleccione **Edit Tags (Editar etiquetas)**.
  4. En el menú desplegable Añadir etiquetas, seleccione **Sanctioned (Sancionado)** o **Unsanctioned (No sancionado)**.
  5. Repita los pasos 1 a 4 hasta que sus aplicaciones SaaS estén etiquetadas según sea necesario.
  6. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** y seleccione **Commit and Push (Confirmar y enviar)** sus cambios en la configuración.
- Configure el informe de actividad del usuario y el informe de uso de aplicación SaaS en base a los grupos de usuarios para lograr un mayor nivel de pormenorización en sus informes.

  Por ejemplo, su departamento de finanzas almacena una gran cantidad de datos en GitHub. El uso de los grupos de usuarios en su actividad de usuario y los informes de uso de la aplicación SaaS le permiten identificar más fácilmente este comportamiento anómalo. De lo contrario, este comportamiento anómalo puede haber pasado desapercibido si el informe se ejecuta para toda la organización.
- Configure informes personalizados específicos y con un objetivo, y limite el número de columnas según sea necesario.

  Los parámetros de informe concisos le permiten identificar más fácilmente la actividad de la red que necesita investigación.

  Cuando cree un informe personalizado, utilice el Generador de consultas cuando sea posible para acotar rápidamente los resultados.

  Por ejemplo, un informe específico para la ubicación de una oficina es mucho más eficiente y procesable que un informe para todas las ubicaciones de oficinas. Si necesita un informe que abarque varias oficinas, es mejor ejecutar algunos informes diferentes con consultas específicas para cada oficina.