paloalto
TECHDOCS

Incidentes y alertas de NGFW

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

January 31, 2025

Table of Contents

Alertas

¿Dónde puedo usar esto?	¿Qué necesito?
• , incluidos los financiados por Créditos de NGFW de software	Uno de estos: ❑ o ❑ o

Para ayudarle a mantener la salud de sus dispositivos y evitar incidentes que interrumpan su negocio, AIOps for NGFW genera alertas basadas en uno o más problemas que ha detectado con la implementación de su cortafuegos. Estos problemas, o *eventos*, se desencadenan de una de tres maneras:

- Cuando una métrica cambia significativamente
- Cuando un evento generado anteriormente cambia
- Cuando el usuario o el sistema realiza una acción, como reconocer o cerrar una alerta

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.

Las alertas se dividen en diferentes categorías según la métrica con la que están asociadas. Puede utilizar categorías de alerta para especificar los tipos de alertas para las que recibe notificaciones. Por ejemplo, hardware, límites de configuración, límites de recursos, contenido dinámico y PAN-OS y suscripciones.

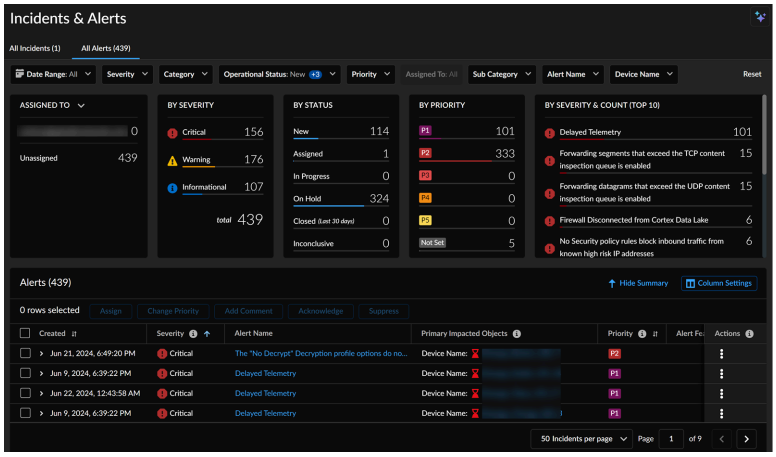
Desde **Incidents & Alerts (Incidentes y alertas)** > **NGFW** > **All Alerts (Todas las alertas)**, puede ver y gestionar todas las alertas generadas para su implementación. En **Notification Rules (Reglas de notificación)**, puede configurar reglas de notificación que especifiquen cuándo y cómo desea recibir notificaciones cuando los eventos activen una alerta.

- Gestionar alertas de NGFW
- Ver detalles de alerta
- Ver causas probables
- Forecasting y detección de anomalías
- Gestionar alertas del analizador de capacidad
- Métricas de uso de la CPU en AIOps para NGFW
- Crear una Regla de notificación
- Integración con ServiceNow

Gestionar alertas de NGFW

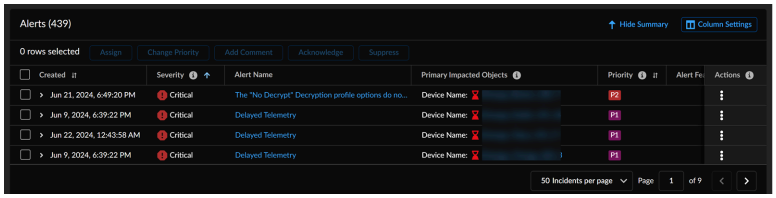
¿Dónde puedo usar esto?	¿Qué necesito?
• , incluidos los financiados por Créditos de NGFW de software	Uno de estos: ❑ o ❑ o

Obtenga una vista panorámica de las alertas de NGFW seleccionando **Incidents & Alerts (Incidentes y alertas)** > **NGFW** > **All Alerts (Todas las alertas)**. Explore la página de alertas para ayudarle a mantener el estado continuo de sus dispositivos e implementaciones, y evitar interrupciones en su negocio. Tiene acceso directo a una lista detallada de alertas junto con resúmenes visuales críticos. También puede **Hide Summary (Ocultar resumen)** para ocultar los widgets y solo ver las alertas en un formato tabular.



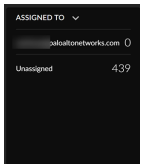
Estos son los datos que se muestran en **All Alerts (Todas las alertas)**.

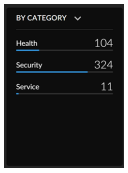
- **Alerts (Alertas)** Muestra todas las alertas.



  En esta tabla puedes realizar las siguientes tareas:

  - **Ocultar Resumen** para ocultar los widgets y solo ver las alertas en un formato tabular.
  - Expandir una alerta para ver su descripción e impacto.
  - En Acciones, puede realizar las siguientes acciones:
    - **Asigne** una alerta a un usuario, usted mismo, o anule la asignación de una alerta.
    - **Cambie la prioridad** de una alerta o seleccione "No establecido" para eliminar la prioridad.
    - **Reconozca** una alerta seleccionando **Sí**, lo que confirma que ha visto la alerta.
    - **Suprimir** establece una alerta en un estado operativo de "En espera" cuando no planifica resolverlo de forma activa.
    - **Añada un comentario** para una alerta.
  - Haga clic en una alerta para ver sus detalles.
  - Utilice la **Configuración de columnas** para ver u ocultar columnas específicas para alertas y reorganizar el orden predeterminado de las columnas. Estos cambios persistirán en sesiones futuras.
- **ASIGNADO A**: Muestra el número de alertas de la persona o entidad que tiene la tarea de resolverlas. En la parte superior se muestra las alertas asignadas al usuario que ha iniciado sesión y las alertas no asignadas. También puede ver el número de alertas **POR CATEGORÍA** seleccionándolas en la lista desplegable.





- **POR GRAVEDAD Y RECUENTO (TOP 10):** Muestra las alertas clasificadas por gravedad, junto con el recuento de alertas en cada categoría. Primero se dan prioridad a las alertas críticas, seguidas de las alertas de advertencia y luego las alertas informativas.

- **POR ESTADO:** Muestra el número total de alertas por estado.
  - Nuevo indica los incidentes que no se han asignado.
  - Asignado indica los incidentes que se han asignado a un usuario.
  - En curso indica que se está trabajando en el incidente.
  - En espera indica que no planifica resolver una alerta o un incidente de forma activa.
  - Cerrado indica las alertas cerradas durante los últimos 30 días.
  - No concluyente indica que no hay solución para estas alertas.

- **POR GRAVEDAD:** Muestra el número total de alertas clasificados como críticos, de advertencia e informativos.

- **POR PRIORIDAD:** Muestra las alertas según su prioridad, siendo P1 la más grave.

Ver detalles de alerta

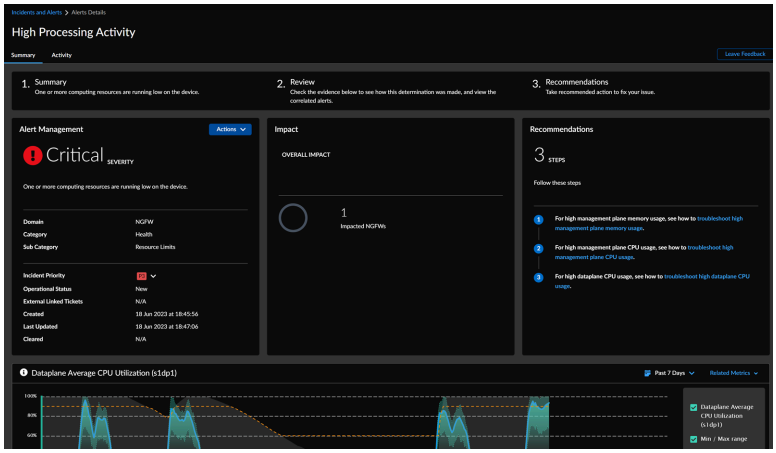
¿Dónde puedo usar esto?	¿Qué necesito?
• , incluidos los financiados por Créditos de NGFW de software	Uno de estos: ❑ o ❑ o

Desde **All Alerts (Todas las alertas)**, puede seleccionar una alerta para abrir una página con detalles al respecto. La pestaña **Summary (Resumen** muestra los siguientes detalles:

1. Resumen de la alerta con detalles. Puede cambiar la prioridad de la alerta o asignarla a un usuario.
2. Impacto causado por la alerta, es decir, el número de cortafuegos NGFW afectados.
3. Recomendaciones y recursos para solucionar su problema.

También puede consultar los gráficos de eventos que contribuyen.

La pestaña **Activity (Actividad)** muestra la actividad registrada para la alerta.



Ver causas probables

¿Dónde puedo usar esto?	¿Qué necesito?
• , incluidos los financiados por Créditos de NGFW de software	❑ o

AIOps utiliza capacidades avanzadas de IA para NGFW para mostrar las causas probables de las alertas y ofrece recomendaciones sobre cómo solucionar el problema subyacente. Esta característica garantiza un rendimiento óptimo de la red al mitigar las interrupciones y maximizar la efectividad de su solución de ciberseguridad.

Estas son las alertas que apoyan el análisis de causa probable:

- Actividad de procesamiento alta
- Aumento de la latencia de tráfico - Búfer de paquetes
- Aumento de la latencia de tráfico - Descriptor de paquetes en el chip
- Amenazas permitidas
- Latencia de tráfico - Descriptores de paquetes (en chip)
- Uso adverso de recursos
- Pares fuera de sincronización - Configuración
- Abuso potencial de robo de credenciales
- Confirmación y envío fallido

El análisis de causa probable se mejora para utilizar los logs de Strata Logging Service y proporcionar metadatos adicionales a la causa probable que condujo a la creación de la alerta o incidente. Esta mejora le permite identificar las políticas, aplicaciones, zonas de origen, URL, IP de origen y regiones que potencialmente generan la alerta.

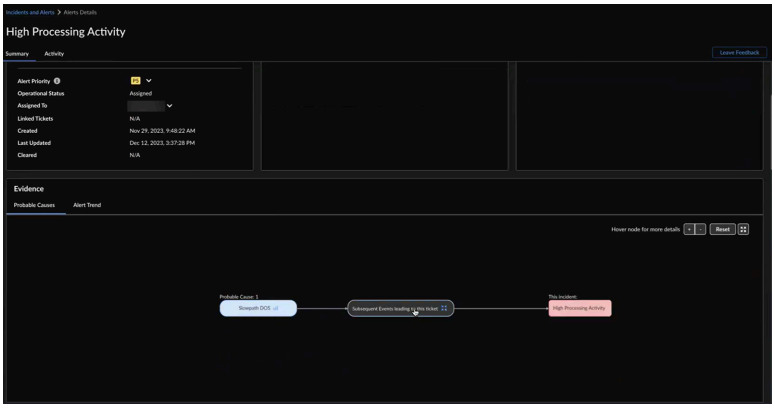
Puede ver las causas probables para los siguientes escenarios:

- **Actividad de procesamiento alta** (alerta de actividad de procesamiento alta): Cuando el uso de la CPU del plano de datos es alto, puede conducir a varios problemas, incluidos inestabilidad en los cortafuegos, cortafuegos que se cuelga o estados de bloqueo, así como problemas de pérdida de paquetes o latencia. Esto puede afectar negativamente sus operaciones comerciales. Si el uso de la CPU del plano de datos es de al menos el 60 % y hay un pico significativo en el uso, AIOps para NGFW mostrará las causas probables en la alerta de alta actividad de procesamiento. Sin embargo, si el uso de la CPU del plano de datos permanece constante a un nivel alto durante un largo período de tiempo sin ninguna variación, la causa será ambigua y no se puede determinar con facilidad, por lo que no se mostrará ninguna causa probable. Por ejemplo, si el uso de la CPU del plano de datos es consistentemente del 70 % durante un período prolongado de tiempo, AIOps para NGFW no mostrará ninguna causa probable.
- Detección y reparación de **una o varias sesiones voraces** (alerta de actividad de procesamiento alta): Un ataque de sesión voraz a un cortafuegos se refiere a un atacante que crea rápidamente numerosas conexiones, explotando los recursos internos del cortafuegos que

pueden conducir a incidentes de agotamiento de recursos y denegación de servicio (DoS). Las AIOps para NGFW pueden detectar estos problemas y mostrar las causas probables de los mismos.

- **Agotamiento de sesión con pérdida de conectividad** (alerta de alta actividad de procesamiento): Cuando un cortafuegos recibe tráfico, este establece una sesión para que ese tráfico rastree su estado y realice las inspecciones de seguridad necesarias. Cada sesión consume recursos del sistema, incluyendo ciclos de memoria y CPU. Si el cortafuegos alcanza su capacidad máxima para sesiones simultáneas, provocará el agotamiento de la sesión. Este problema puede ocurrir debido a varias razones, incluido un alto volumen de tráfico, políticas de seguridad mal configuradas y ajustes de tiempo de espera de sesión incorrectos. AIOps para NGFW utiliza capacidades avanzadas de IA para detectar de forma proactiva problemas de agotamiento de sesión en dispositivos de red. Esto permite una asignación de recursos optimizada, eleva el rendimiento de la red y mitiga los problemas de conectividad para garantizar la disponibilidad ininterrumpida del servicio.
- **Alta utilización del búfer de paquetes debido a una Única aplicación** (Aumento de la latencia de tráfico - Búfer de paquetes): AIOps para NGFW detecta la causa raíz probable de la alta utilización del búfer de paquetes debido a que una única aplicación monopoliza el búfer de paquetes. AIOps para NGFW aprovecha las capacidades avanzadas de IA para garantizar un rendimiento óptimo de la red, alertando oportunamente sobre la asignación subóptima de recursos y evitando la degradación del rendimiento.
- **Uso alto del descriptor de paquetes en el chip debido a una única aplicación** (Aumento de la latencia de tráfico - Descriptor de paquetes en el chip): AIOps para NGFW detecta la causa raíz probable de la alta utilización de descriptores de paquetes en chip. Esto ayuda a la identificación proactiva y la resolución de la congestión de red causada por una única aplicación que monopoliza el descriptor de paquetes en chip.
- **Sugerencia de detección y remediación del ataque DoS de actividad baja y lenta** (alerta de actividad de procesamiento alta): AIOps para NGFW detecta ataques DoS de actividad lenta con tecnología impulsada por IA, lo que garantiza la seguridad de la red y la disponibilidad ininterrumpida del servicio. Realiza alertas de alta actividad de procesamiento de plano de datos, análisis de causa raíz de actividad de denegación de política alta y sugerencias de remediación basadas en el análisis de causalidad.
- **Detección y remediación de alta actividad de búsqueda de caché de URL** (alerta de actividad de procesamiento alta): AIOps para NGFW detecta y aborda la alta actividad de búsqueda de caché de URL, optimizando la eficiencia de procesamiento y manteniendo la estabilidad del sistema. Esta característica correlaciona la actividad de búsqueda de caché de URL con la utilización de la CPU del DP, identifica el alto uso de CPU y proporciona sugerencias de remediación para evitar escenarios de casi saturación.
- **Detección y remediación de alta actividad de procesamiento de contenido** (alerta de actividad de procesamiento alta): La función AIOps para NGFW detecta alta actividad de procesamiento de contenido. Esta característica analiza las correlaciones entre las diversas etapas de procesamiento de contenido y la utilización de CPU de plano de datos, identifica instancias de alto uso de CPU o condiciones de casi saturación y proporciona sugerencias de remediación procesables para mejorar la estabilidad del sistema.
- **Informe de RCA de certificado demasiado largo** (alerta de confirmación y envío fallido): AIOps para NGFW detecta un fallo de confirmación y describe las posibles causas de fallos de confirmación, especialmente cuando la longitud del certificado supera el tamaño del búfer.

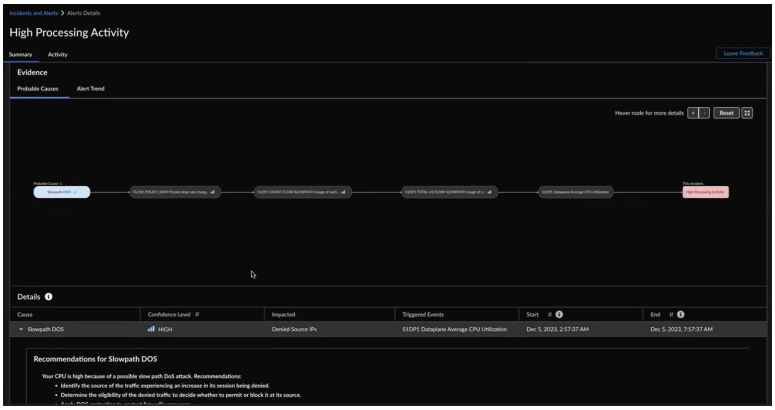
STEP 1 | Desde **Incidents & Alerts (Incidentes y alertas)** > **Alerts (Alertas)**, seleccione una alerta para abrir una página con detalles sobre la alerta.



El diagrama de flujo indica:

- eventos que activaron la alerta de alta actividad de procesamiento
- Causa probable de la activación del evento

También puede pasar el cursor sobre los nodos para ver más detalles, como la causa probable, el nivel de confianza, el evento desencadenado y la duración del impacto. Podrá hacer clic y expandir los eventos para ver los detalles siempre que haya tres o más nodos de eventos.



AIOps para NFGW también muestra la misma información en un formato tabular. Puede pasar el cursor por encima de una causa probable en la tabla para ver los nodos y la ruta resaltados en el diagrama de flujo. También puede hacer clic en una causa probable en el diagrama de flujo para ver sus detalles en formato tabular.

El **Confidence Level (Nivel de confianza)** indica cómo determinados AIOp para NGFW identifican las causas de la alerta de actividad de procesamiento elevada. Las causas probables se clasifican en orden descendente del nivel de confianza. Puede empezar por comprobar las causas con un alto nivel de confianza.

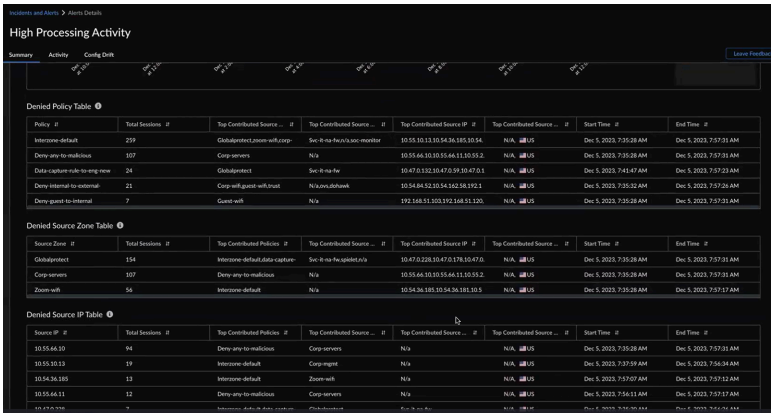
STEP 2 | Expanda una causa probable en la tabla para ver los gráficos y las métricas afectadas que desea investigar tras la activación de la alerta.

STEP 3 | Utilice herramientas de gráficos para inspeccionar los gráficos.

El período de causalidad le permite visualizar la relación de causa y efecto entre la **Cause (Causa)** de la alerta y el **Triggered Event (Evento desencadenado)** a lo largo del tiempo.

En el gráfico puede ver 6 horas, 24 horas o 48 horas antes y después del impacto.

El análisis de causa probable se mejora para utilizar los registros SLS y proporcionar metadatos adicionales a la causa probable que condujo a la creación de una alerta o incidente. Esta mejora le permite identificar las políticas, aplicaciones, zonas de origen, URL, IP de origen y regiones que potencialmente generan la alerta. Por ejemplo, cuando el uso elevado de CPU en el plano de datos activa una alerta de **High Processing Activity (Actividad de procesamiento alta)**, puede utilizar el análisis de causa probable para identificar los contribuyentes principales a la alerta y seguir las recomendaciones de corrección sugeridas.



Forecasting y detección de anomalías

¿Dónde puedo usar esto?	¿Qué necesito?
• , incluidos los financiados por Créditos de NGFW de software	Uno de estos: ❑ o ❑ o

Normalmente, AIOps for NGFW detecta problemas aplicando reglas fijas a las métricas de su implementación. Por ejemplo, si el uso de la CPU en el plano de gestión supera el 85 %, la métrica entra en un estado crítico.

Sin embargo, para alertarle de eventos que las reglas fijas podrían perder, AIOps for NGFW puede utilizar el aprendizaje automático para comprender su implementación y ofrecerle alertas e incidentes adicionales adaptados a sus tendencias de uso.

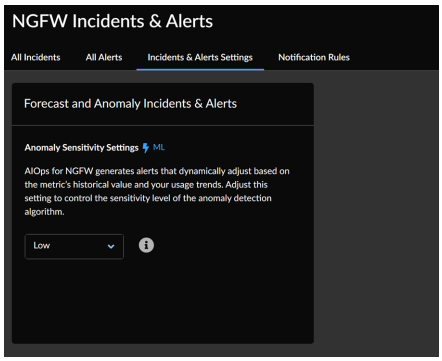
- Las **Forecast-Based Alerts (Alertas basadas en pronósticos)** le ayudan a anticipar problemas al predecir cómo puede cambiar una métrica del dispositivo y alertarle en consecuencia.
- Las **Anomaly-Based Alerts (Alertas basadas en anomalías)** establecen un comportamiento de referencia para una métrica de dispositivo y le avisan cuando esa métrica cruza la **Anomaly Sensitivity Settings (Configuración de sensibilidad de anomalía)** que usted especifique.

Los beneficios del forecasting y de la detección de anomalías son los siguientes:

- Gestión proactiva: Al predecir problemas potenciales e identificar anomalías a tiempo, los administradores pueden tomar medidas proactivas para prevenir problemas, reducir el tiempo de inactividad y mejorar el rendimiento general de la red.
- Seguridad mejorada: La detección de patrones y comportamientos inusuales puede ayudar a identificar amenazas y vulnerabilidades de seguridad, lo que permite una intervención y mitigación oportunas.
- Recursos optimizados: El forecasting contribuye a una mejor planificación y asignación de los recursos, garantizando que la infraestructura de la red esté adecuadamente preparada para gestionar las demandas futuras.

Vaya a **Incidents & Alerts (Incidentes y alertas)** > **Incident & Alert Settings (Configuración de incidentes y alertas)** > **Forecast and Anomaly Incidents & Alerts (Pronóstico e incidencias y alertas de anomalías)**.

AIOps for NGFW genera alertas e incidentes que se ajustan dinámicamente en función del valor histórico de la métrica y sus tendencias de uso. Las desviaciones de la banda de normalidad pueden indicar problemas potenciales. Puede ajustar esta configuración para controlar el nivel de sensibilidad del algoritmo de detección de anomalías.



Gestionar alertas del analizador de capacidad

¿Dónde puedo usar esto?	¿Qué necesito?
•	❑ o

El Analizador de capacidad utiliza modelos de aprendizaje automático para anticipar cuando el consumo de recursos se acerca a su capacidad máxima y generar alertas. Las alertas del analizador de capacidad se generan con antelación identificando posibles cuellos de botella de capacidad.

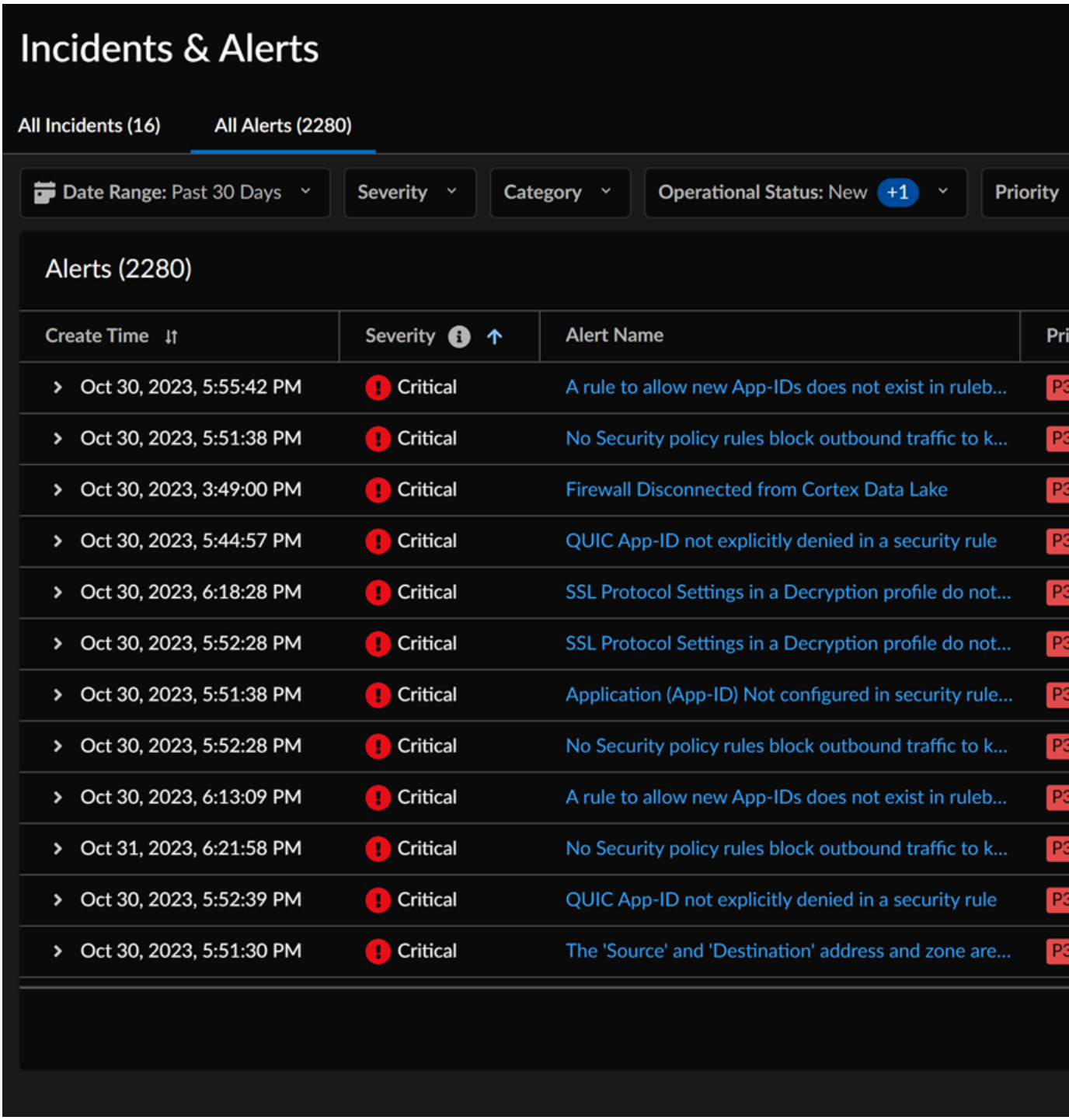
También puede crear una regla de notificación para activar notificaciones para las alertas del analizador de capacidad.

STEP 1 | Vaya a **Incidents & Alerts (Incidentes y alertas)** > **NGFW** > **All Alerts (Todas las alertas)** y haga clic en **List View (Vista de lista)**.

STEP 2 | En **Alert Name (Nombre de alerta)**, busque **approaching max alerts (aproximándose al número máximo de alertas)**.

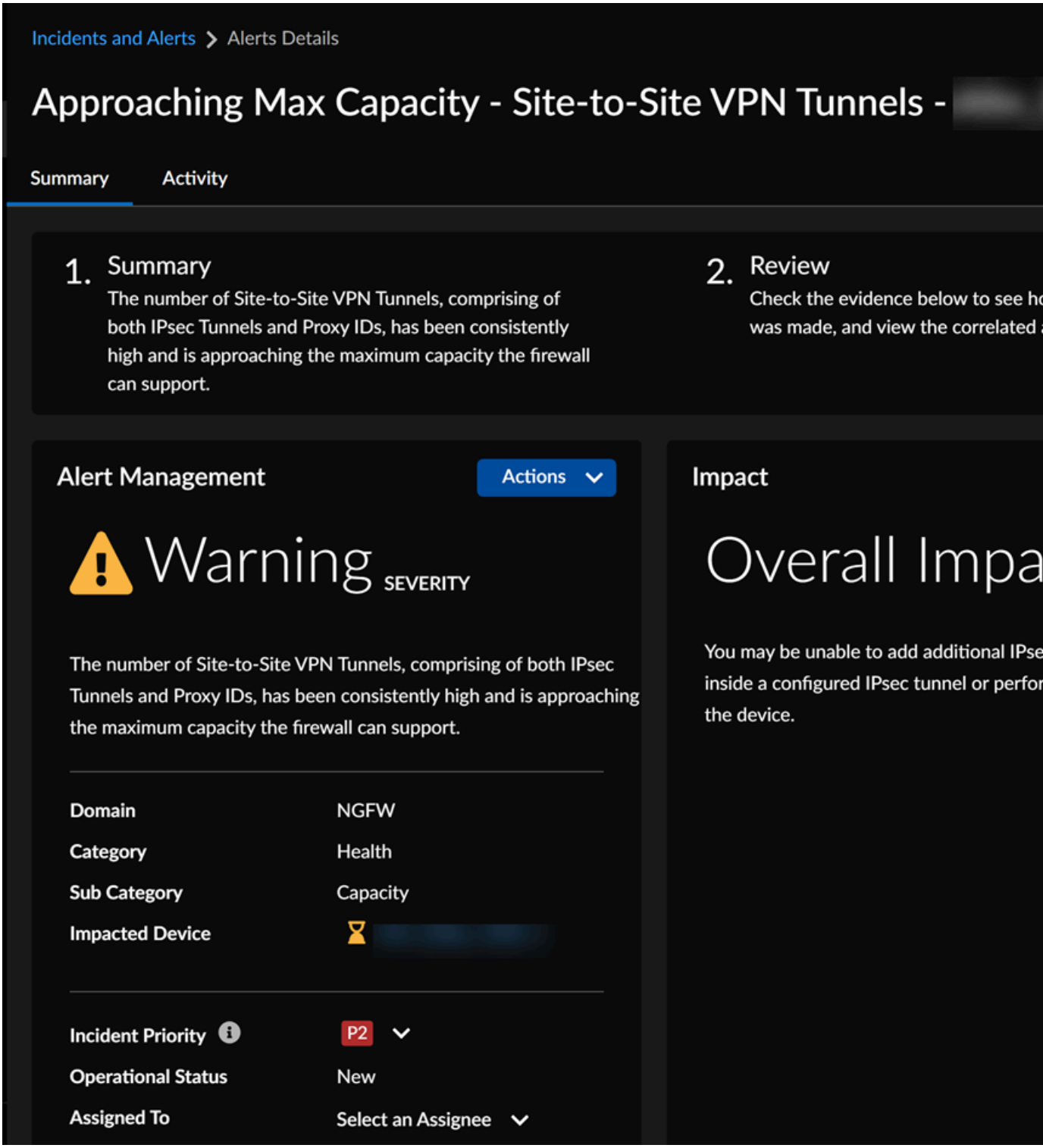
Las alertas generadas para la función de analizador de capacidad se nombran como:

Aproximándose a la capacidad máxima - *<Metric-Name>*.



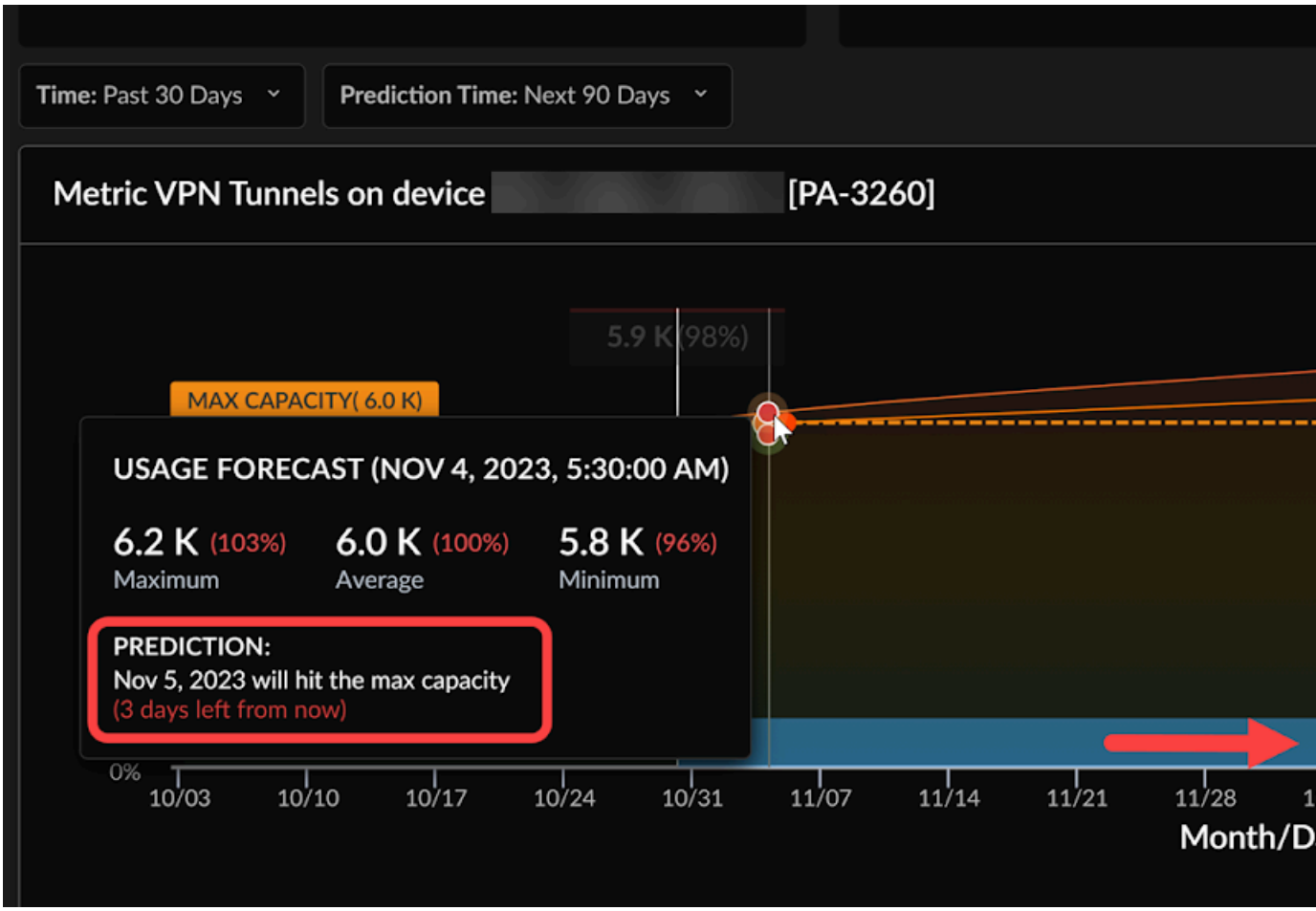
STEP 3 | Seleccione una de las alertas para ver sus detalles que incluyen:

- Resumen de la alerta con detalles.
- Impacto causado por la alerta.
- Acción recomendada para solucionar el problema.

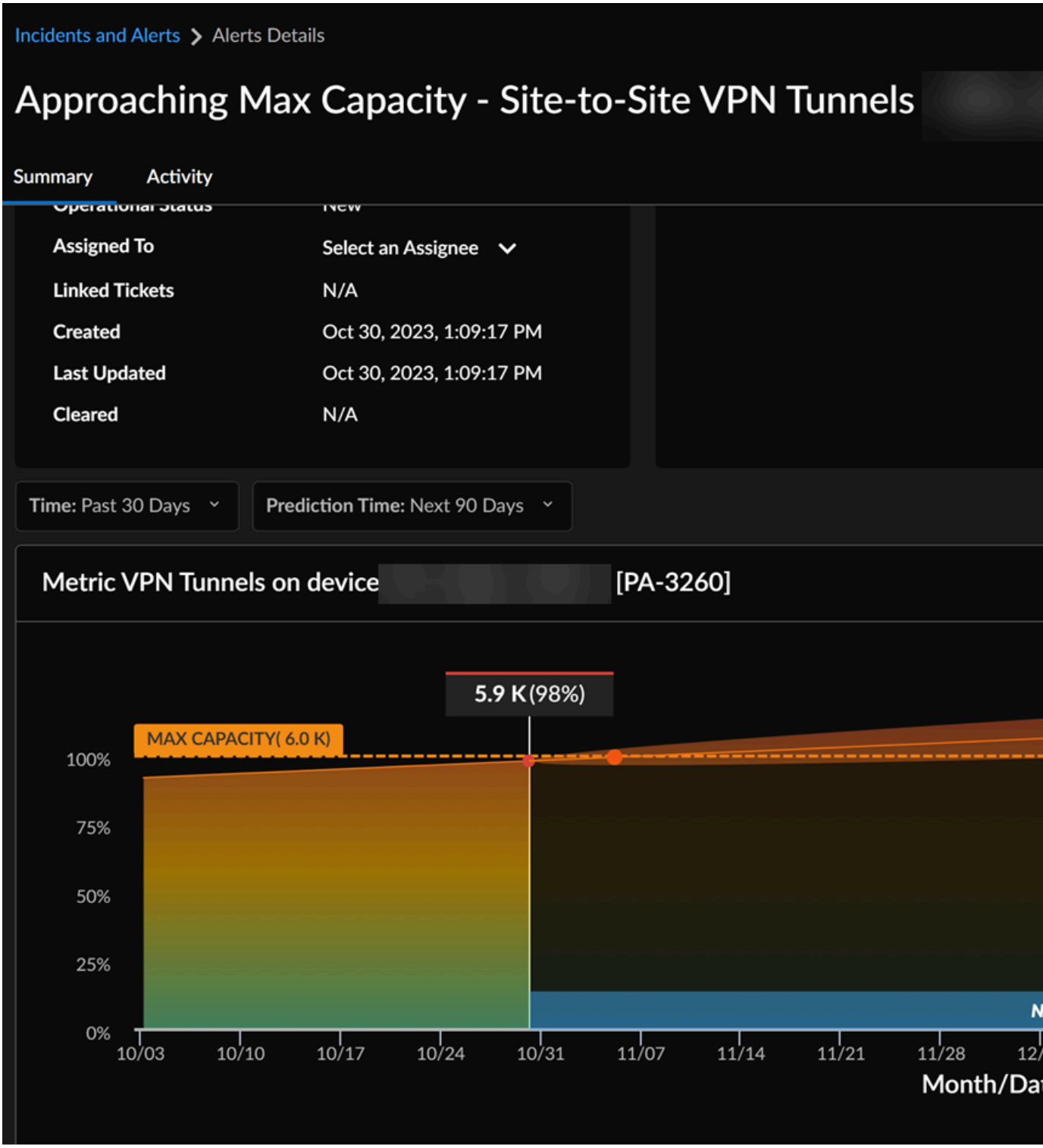


En los detalles de la alerta, también puede ver un gráfico que muestra la tendencia de la métrica. Strata Cloud Manager pronostica la fecha en que la métrica alcanzará la capacidad máxima. Puede pasar el cursor sobre el gráfico para comprobar la capacidad de la métrica en cualquier momento. Puede seleccionar un **Prediction Time (Tiempo de predicción)** para los próximos 30 días o 90 días.

En este ejemplo, puede ver que la métrica de túneles VPN en el dispositivo alcanzará la capacidad máxima el **5 de noviembre de 2023**.



STEP 4 | Desde la página **Alerts (Alertas)**, puede **Go to Capacity Analyzer Page (Ir a Página del analizador de capacidad)** para ver el mapa de calor del analizador de capacidad.



Para obtener información sobre cómo utilizar el mapa de calor del analizador de capacidad y comprobar las alertas de capacidad, consulte Analizar capacidad de la métrica.

Métricas de uso de la CPU en AIOps para NGFW

¿Dónde puedo usar esto?	¿Qué necesito?
• , incluidos los financiados por Créditos de NGFW de software	Uno de estos: ❑ o ❑ o

El uso de la CPU se rastrea en un AIOps para NGFW usando las siguientes métricas:

- **mp_system_resources.mp_cpu**: Indica el uso total de la CPU.
- **mp_system_resources_daemon.cpu_usage_sum**: Indica el uso de la CPU resultante de las tareas del Plano de gestión que se ejecutan en la CPU del plano de gestión (MP-CPU). Esta métrica es equivalente al uso de CPU encontrado en SNMP.
- **mp_system_resources_daemon.pan_task_cpu_usage**: Indica el uso de la CPU resultante de las tareas de PAN que se ejecutan en la MP-CPU que realiza operaciones de tipo Plano de datos. Estos datos no forman parte de la métrica SNMP y **mp_system_resources_daemon.pan_task_cpu_usage**.

El uso total de CPU se calcula como:

mp_system_resources.mp_cpu = **mp_system_resources_daemon.cpu_usage_sum** + **mp_system_resources_daemon.pan_task_cpu_usage**

Crear una Regla de notificación

¿Dónde puedo usar esto?	¿Qué necesito?
• , incluidos los financiados por Créditos de NGFW de software	Uno de estos: ❑ o ❑ o

La integración de Strata Cloud Manager en sus operaciones existentes implica configurar alertas proactivas que le permitan detectar y gestionar posibles problemas antes de que se conviertan en complicaciones graves. Estas alertas se pueden adaptar para que coincidan con el protocolo de gestión de casos de su equipo de operaciones, como los comúnmente utilizados P1 o P2.

Por ejemplo, puede configurar un sistema de alertas en el que las alertas críticas, que representan los problemas más severos, se envíen instantáneamente a su equipo de seguridad para su atención inmediata. Por otro lado, las alertas de advertencia, que son de menor urgencia pero aun así significativas, se pueden organizar para su revisión diaria. Este tipo de acuerdos garantiza una gestión eficiente de incidentes y al mismo tiempo mantiene el buen funcionamiento de sus operaciones.

Otra opción es enrutar las alertas en función de los equipos; ciertas categorías de alertas, o incluso alertas específicas, pueden enrutarse a los equipos que estén mejor equipados y preparados para gestionarlas. Puede definir preferencias de notificación, como qué alertas activan las notificaciones, cómo recibirlas y con qué frecuencia recibirlas, y luego crear una regla de notificación.

Aquí tenemos un vídeo que muestra cómo crear una regla de notificación.

STEP 1 | Seleccione **Incidents & Alerts (Incidentes y alertas)** > **Incident & Alert Settings (Configuración de incidentes y alertas)** > **Notification Rules (Reglas de notificación)** > **+ Add Notification Rule (+ Añadir regla de notificación)**

STEP 2 | Introduzca un `Name (Nombre)` y una `Description (Descripción)`.

STEP 3 | Deberá **Add New Condition (Añadir nueva condición)** para especificar las `Rule Conditions (Condiciones de la regla)` que activarán la notificación.

Por ejemplo, para crear una notificación para alertas de hardware, seleccione **subCategory (subCategoría)**, **Equals (Igual)** y **Hardware**.

STEP 4 | Elija `Notification Type and Recipients (Tipo de notificación y destinatarios)` de la notificación.

1. Si elige **Email (Correo electrónico)**, seleccione un grupo de correo electrónico, que es el grupo de usuarios que recibirán las notificaciones por correo electrónico, o **Create a New Email Group (Crear un nuevo grupo de correo electrónico)**.

   1. Si va a crear un nuevo grupo de correo electrónico, introduzca un Nombre de grupo de correo electrónico y comience a escribir las direcciones de correo electrónico de aquellos que desea añadir al grupo. Pulse la tecla Intro después de completar cada dirección de correo electrónico.

2. Seleccione **Next (Siguiente)**.
3. Seleccione la frecuencia con la que desea enviar estas notificaciones:

- Inmediatamente
- Agrupadas y enviadas cada 4 horas
- Agrupadas y enviadas una vez al día

2. Si selecciona **ServiceNow**, introduzca la `URL de ServiceNow`, las credenciales del cliente, las credenciales de ServiceNow y la `Versión de la API de ServiceNow`.
   1. Proceda a **Test (Probar)** su conexión para asegurarse de que la integración esté funcionando.
   2. Seleccione **Next (Siguiente)**.

STEP 5 | y **Save Rule (Guardar regla)**.

Integración con ServiceNow

¿Dónde puedo usar esto?	¿Qué necesito?
• , incluidos los financiados por Créditos de NGFW de software	❑ o

Al configurar la integración de ServiceNow en la regla de notificación de AIOps for NGFW, necesita lo siguiente:

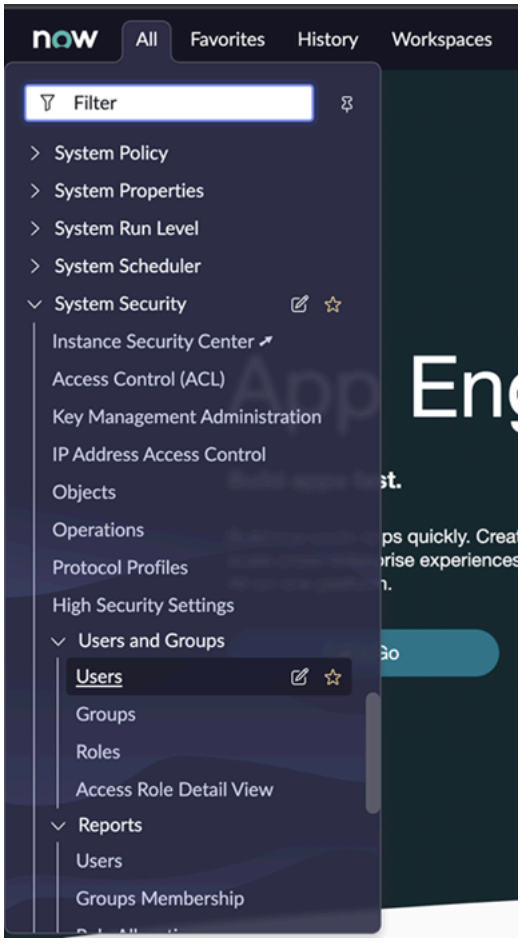
- Instancia de ServiceNow configurada con acceso administrativo
- Nombre de usuario y contraseña de ServiceNow con acceso web y roles específicos para crear incidentes o consultar diversas tablas
- ID de cliente y contraseña creados en el Registro de aplicaciones para autorizar a AIOps a acceder a su instancia de ServiceNow
- URL de su instancia de ServiceNow

Su instancia de ServiceNow también debe tener una tabla de **Incident (incidentes)** para que AIOp envíe alertas y **Assignment Groups (Grupos de asignación)** con **Assignees (Asignados)** para que estas alertas puedan elevarse a personas específicas.

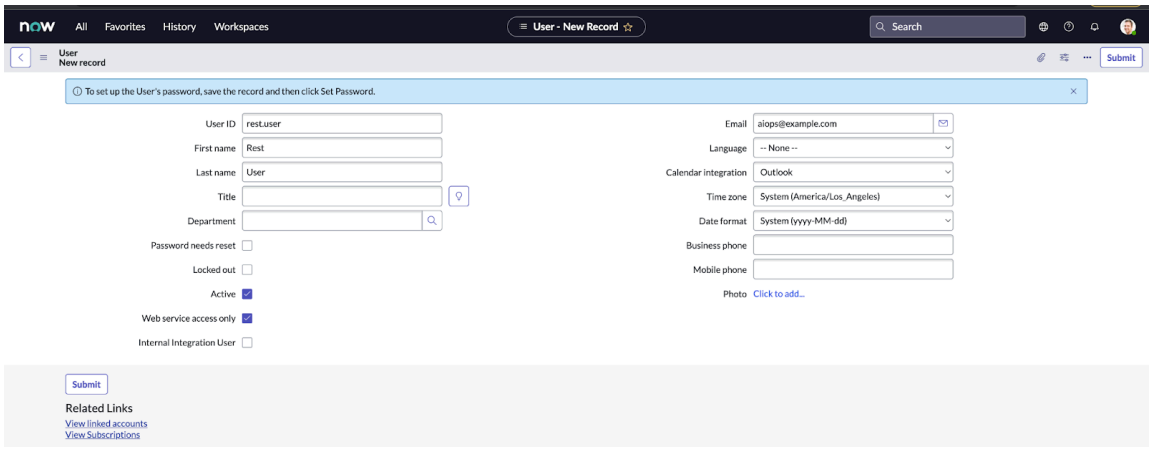
STEP 1 | Crear un usuario Rest de ServiceNow.

Crear un nuevo usuario de ServiceNow con roles específicos para leer y escribir en las diversas tablas necesarias para la integración (Incidente, Grupos de asignación y Asignados).

1. Para crear un usuario en ServiceNow, vaya a **Users (Usuarios)** en **Security (Seguridad) > Users and Groups (Usuarios y grupos)**.

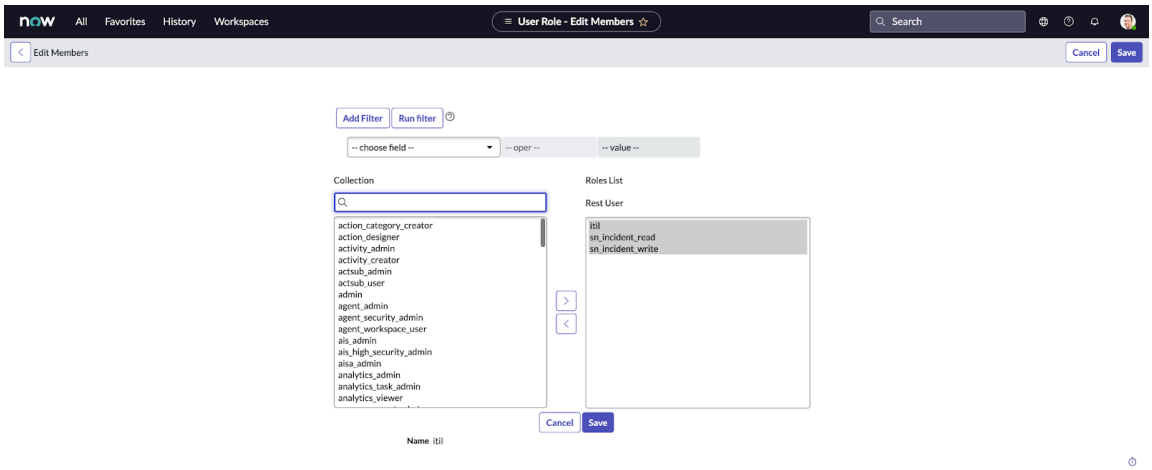


2. Marque la casilla de verificación **Web service access only (Solo acceso web)** y envíe sus cambios.



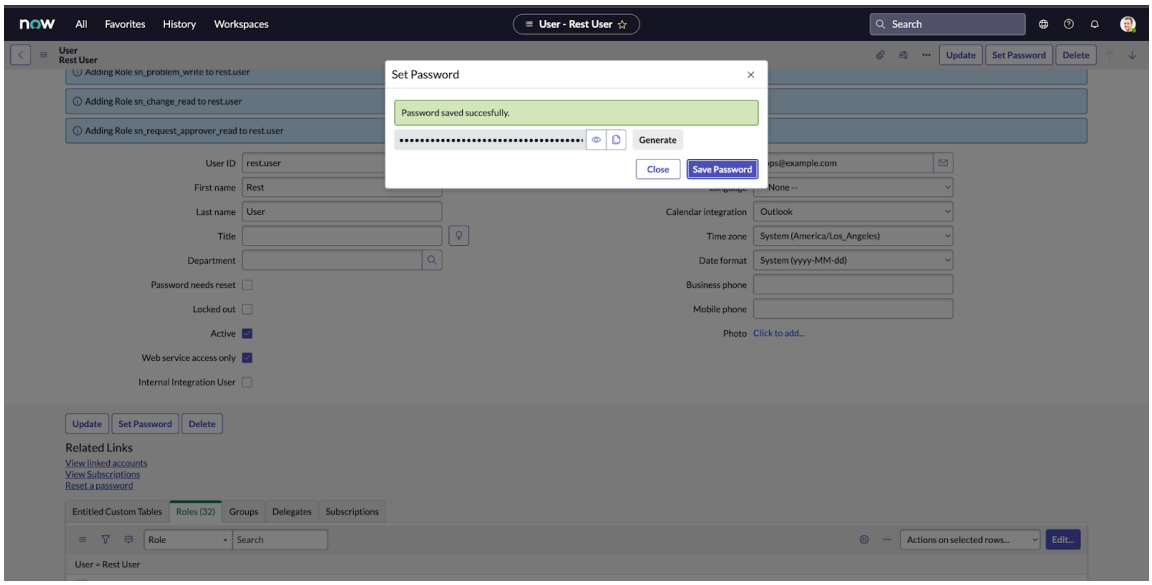
3. Busque el usuario recién creado. Seleccione la pestaña **Roles (Roles)** en la tabla en la parte inferior de la página y haga clic en **Edit (Editar)**. Tendrá que dar permisos al usuario

para los siguientes tres roles: **itil, sn_incident_read** y **sn_incident_write**. Guarde sus cambios.



4. Haga clic en **Set Password (Establecer contraseña)** en la página Usuario. En la ventana emergente, haga clic en **Generate (Generar)** y **Save Password (Guardar contraseña)**. Asegúrese de copiar la contraseña en una ubicación segura junto con el ID de usuario.

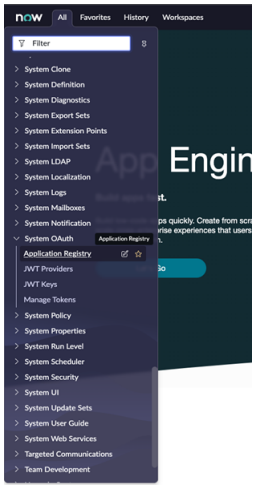
Esta información se utilizará para rellenar las credenciales de **ServiceNow User (Usuario de ServiceNow)** en AIOps for NGFW.



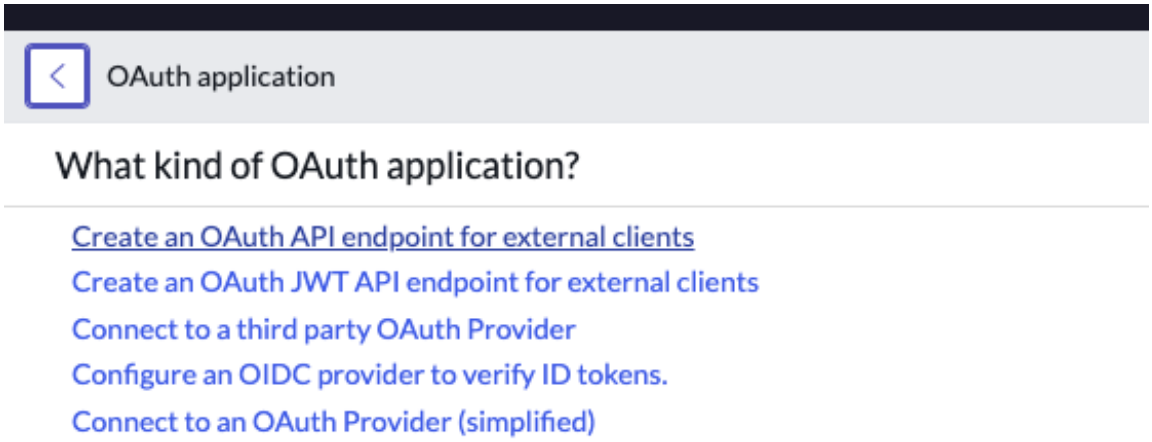
STEP 2 | Crear un cliente Web OAuth.

Se necesita un cliente de OAuth para que AIOps for NGFW se autentique en su instancia de ServiceNow.

1. Vaya a **System OAuth > Application Registry (OAuth del sistema > Registro de aplicaciones)**.

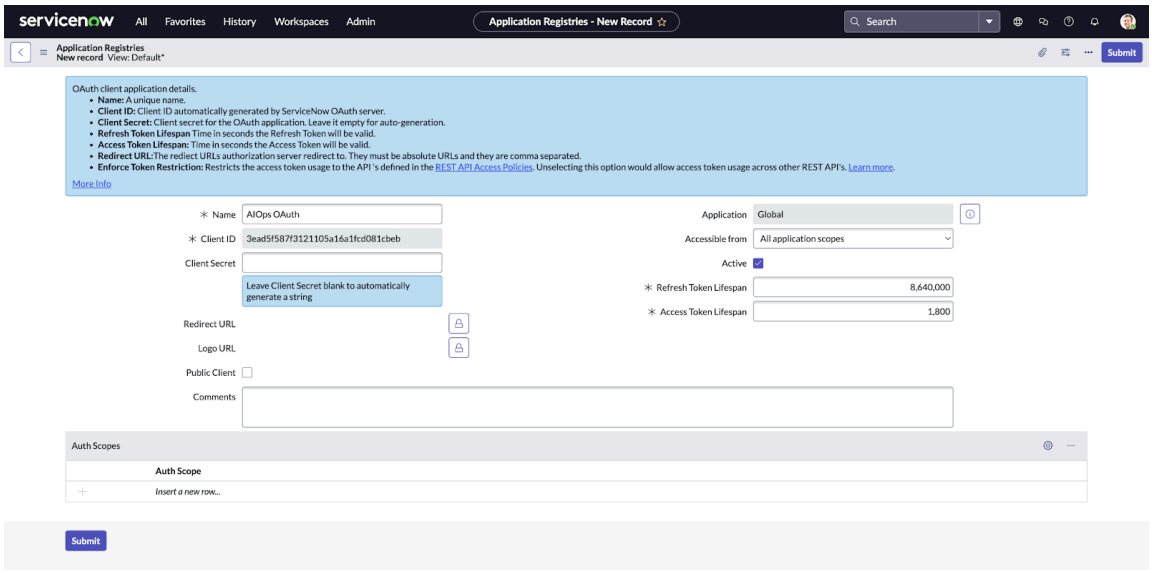


2. Cree una nueva entrada y seleccione **Create an OAuth API endpoint for external clients (Crear un endpoint API OAuth para clientes externos)** en la página siguiente.



3. Añada un nombre para OAuth y cree un **Client Secret (Secreto de cliente)**. El **Client Secret (Secreto de cliente)** también se puede dejar en blanco si se desea un secreto generado de forma automática. Haga clic en **Submit (Enviar)** y, a continuación, vuelva a navegar hasta la entrada Registro de aplicaciones y guarde el **Client ID (ID del cliente)** y

el **Client Secret (Secreto de cliente)** en un lugar seguro. Esta información se utilizará en los formularios de **Client credential (Credencial del cliente)** en AIOps for NGFW.



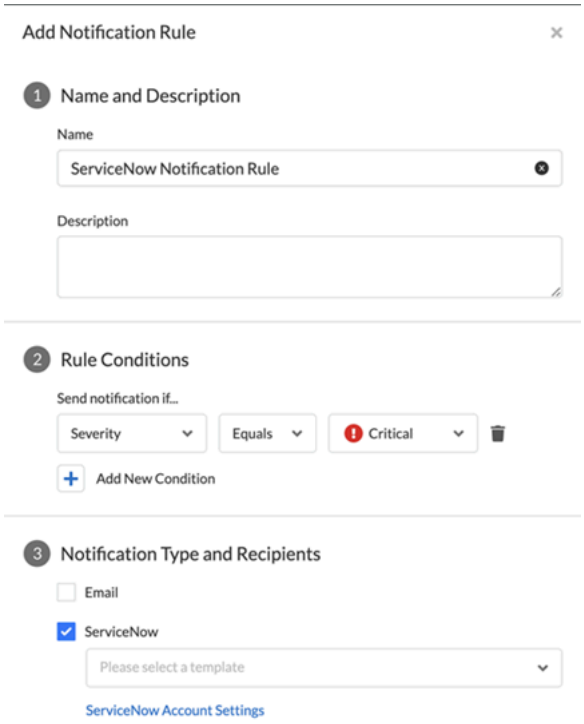
STEP 3 | Añadir la información de la Configuración de cuenta de ServiceNow en AIOps for NGFW.

Añada la información de los pasos anteriores en AIOps for NGFW para completar la integración entre ServiceNow y AIOps for NGFW.

Necesitará lo siguiente:

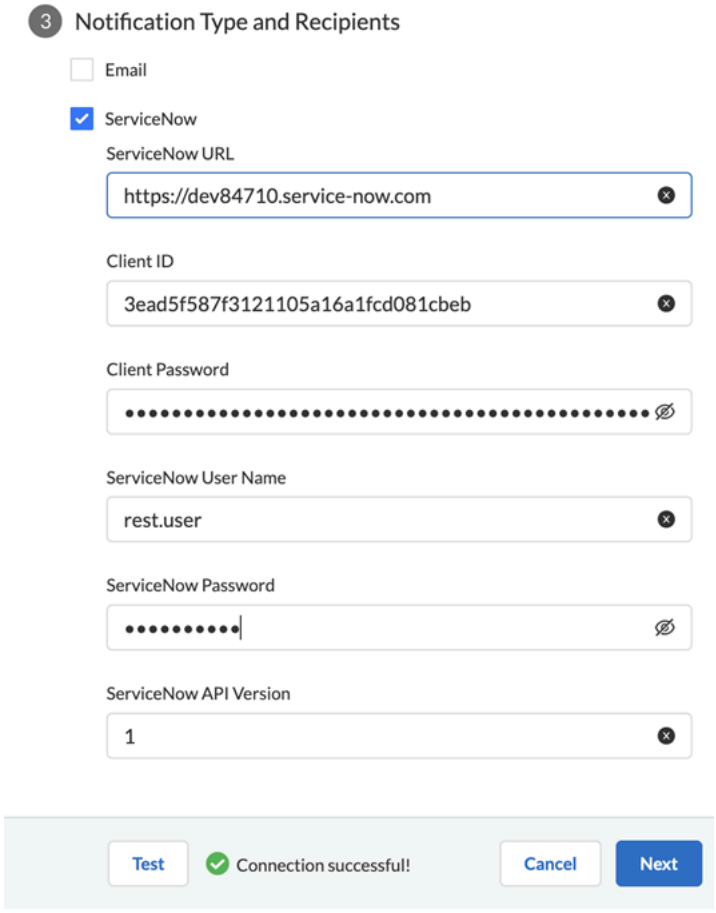
- Tu **URL de instancia de ServiceNow**
- **Usuario de ServiceNow** y **contraseña** desde el paso 1
- **ID de cliente** y **Secreto de cliente** del paso 2

1. En AIOps for NGFW, vaya a **Reglas de notificación de alertas** y haga clic en **Añadir regla de notificación**.

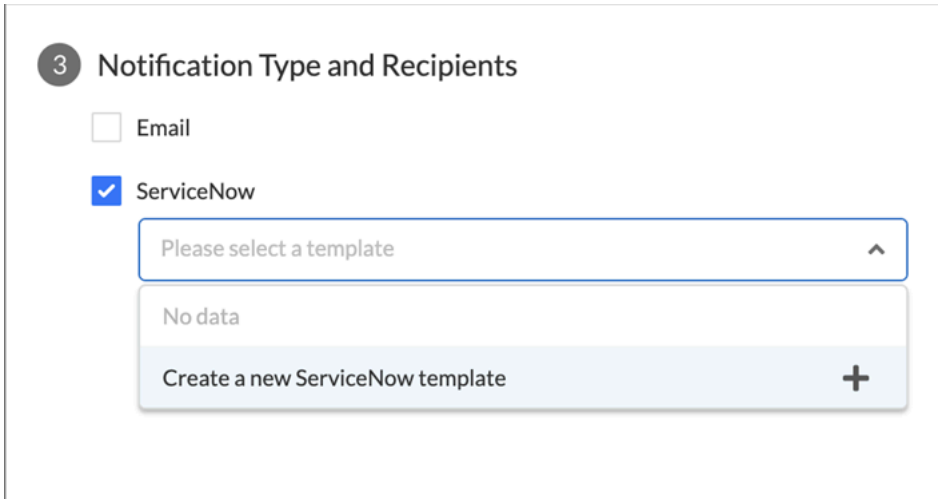


2. Rellene campos como **Rule Name (Nombre de regla)** y **Alert Condition (Condición de alerta)** y, a continuación, haga clic en la casilla de verificación de **ServiceNow** en **Tipo de notificación y destinatarios**.
3. Haga clic en **Configuración de cuenta de ServiceNow** en la parte inferior de la barra lateral. Rellene el siguiente formulario con la información que se guardó anteriormente. **Usuario de ServiceNow** y **Contraseña de ServiceNow** del Paso 1, donde configura el Usuario de Rest. **ID de cliente** y **Secreto de cliente** desde el Paso 2, donde configuró el Registro de aplicaciones. Deje la versión tal cual. Haga clic en **Probar** para guardar la

configuración y publicar un incidente de prueba en su instancia de ServiceNow. Esto debe realizarse correctamente para proceder. Haga clic en **Next (Siguiente)**.



4. Expanda el menú desplegable **Seleccione una plantilla** y haga clic en **Crear una nueva plantilla de ServiceNow**.

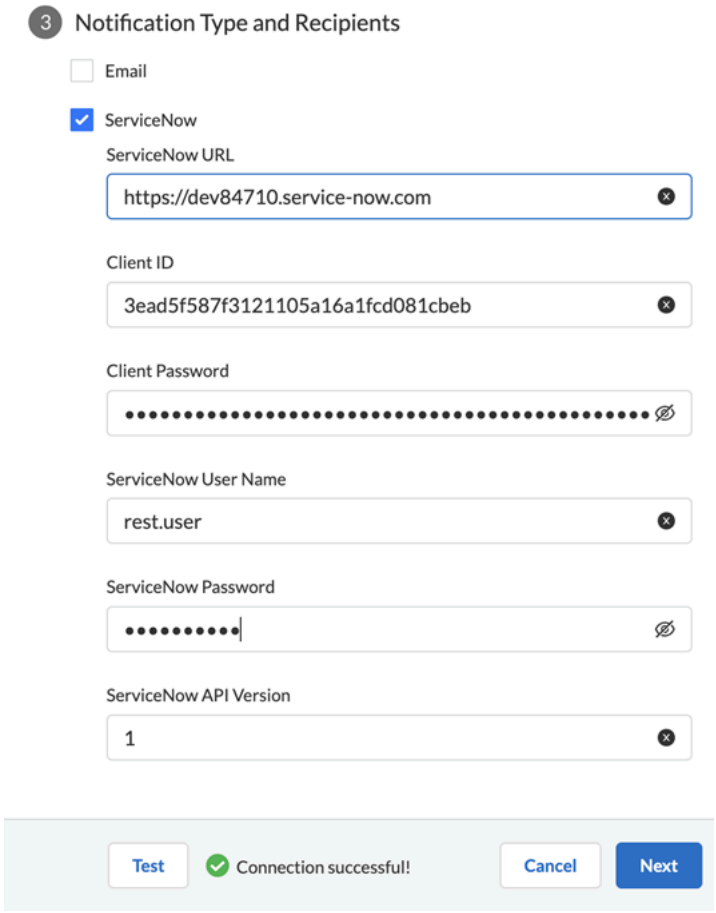


5. Introduzca el **Nombre de plantilla de ServiceNow** y, a continuación, elija un grupo de la lista desplegable **Grupo de asignación**. Elija un asignado en la lista desplegable **Asignado**.

Tenga en cuenta que estas listas desplegables se rellenan llamando a las siguientes tablas desde su instancia de ServiceNow:

- **Seguridad del sistema > Usuarios y grupos > Usuarios**
- **Seguridad del sistema > Usuarios y grupos > Grupos**

Si no hay grupos definidos, la lista desplegable **Assignment Group (Grupo de asignación)** no se rellenará. Si no hay usuarios asignados a un grupo específico, la lista desplegable **Assignees (Asignados)** no se rellenará. Haga clic en **Next (Siguiente)** y luego en **Save Rule (Guardar regla)**.



Referencia de alertas de AIOps for NGFW

Bienvenido a la referencia de alertas de AIOps for NGFW. Las alertas de estado supervisan activamente el estado y el rendimiento de su plataforma en tiempo real. Este enfoque ayuda a identificar problemas, predecir problemas potenciales e implementar acciones de corrección para garantizar que sus dispositivos funcionen de manera óptima. Estos son algunos aspectos clave:

- Métricas de supervisión: Supervisar continuamente varias métricas de los NGFW, incluida la utilización de CPU, el uso de memoria, el espacio en disco, el rendimiento de red y otros indicadores de rendimiento relevantes. Esta supervisión constante garantiza que cualquier desviación del rendimiento normal se identifique rápidamente.
- Detección de anomalías: Genere alertas que se ajusten dinámicamente en función del valor histórico de la métrica y sus tendencias de uso. El sistema aprovecha los datos históricos para poder detectar anomalías que podrían indicar problemas potenciales, lo que permite una gestión proactiva.
- Análisis predictivo: Predecir cuándo ciertos umbrales exceden o cuándo se producen eventos específicos analizando datos y patrones históricos. Esto ayuda a pronosticar problemas potenciales antes de que vayan a más.

En las páginas siguientes se identifican las alertas que AIOps for NGFW puede generar.

- Alertas de estado premium: Vea las alertas premium que Strata Cloud Manager puede generar y que están relacionadas con el estado de su plataforma.
- Alertas de estado gratuitas: Vea las alertas gratuitas que AIOps for NGFW puede generar y que están relacionadas con el estado de su plataforma.
- Alertas de servicio: Vea las alertas que AIOps for NGFW puede generar en relación con los servicios conectados a ella.
- Alertas generadas por el aprendizaje automático: Vea las alertas que Strata Cloud Manager puede generar mediante el uso del aprendizaje automático.

Para obtener información acerca de las comprobaciones de la postura de seguridad que AIOps for NGFW puede generar, vaya a la tabla **Manage (gestionar) > Security Posture (Postura de seguridad) > Settings (Configuración) > Security Checks (Comprobaciones de seguridad)** para ver las comprobaciones.

Alertas de estado premium

En la tabla siguiente se identifican las alertas premium que Strata Cloud Manager puede generar y que están relacionadas con el estado de su plataforma.

Se requiere la licencia premium de Strata Cloud Manager para que AIOps for NGFW pueda generar estas alertas.

Alerta	Description (Descripción)
Fallo de consulta de ACC (Alerta premium)	Esta alerta detecta si la consulta del Centro de comandos de aplicaciones (ACC) ha fallado. Clase: Salud Categoría: Generación de informes Ticket de asistencia en la aplicación: No
Uso de recursos de tráfico cifrados adversos (Alerta premium)	Los recursos de tráfico cifrados se están agotando. Clase: Salud Categoría: Uso de recursos Ticket de asistencia en la aplicación: No
Uso adverso de recursos (Alerta premium)	El cortafuegos tiene valores anómalos para conexiones por segundo (CPS), rendimiento o número de sesiones. Clase: Salud Categoría: Uso de recursos Ticket de asistencia en la aplicación: No
Aproximándose a la capacidad máxima - Tabla de ARP (Alerta premium)	El análisis del forecasting de datos muestra que las entradas de la tabla ARP van a alcanzar la capacidad máxima del cortafuegos pronto. Clase: Salud Categoría: Capacidad Ticket de asistencia en la aplicación: No
Aproximándose a la capacidad máxima - Grupos de direcciones (Alerta premium)	El número de objetos del grupo de direcciones ha sido sistemáticamente alto y se está acercando a la capacidad máxima que el cortafuegos puede soportar. Clase: Salud Categoría: Capacidad Ticket de asistencia en la aplicación: No

Alerta	Description (Descripción)
Aproximándose a la capacidad máxima - Objetos de direcciones (Alerta premium)	El número de objetos de dirección ha sido sistemáticamente alto y se está acercando a la capacidad máxima que el cortafuegos puede soportar. Clase: Salud Categoría: Capacidad Ticket de asistencia en la aplicación: No
Aproximándose a la capacidad máxima - CPU de plano de datos (Alerta premium)	El uso de la CPU del plano de datos (DP) ha sido sistemáticamente alto a lo largo del tiempo y se está acercando a la capacidad máxima que el dispositivo puede soportar. Clase: Salud Categoría: Capacidad Ticket de asistencia en la aplicación: No
Aproximándose a la capacidad máxima - Uso de descifrado (Alerta premium)	El análisis del forecasting de datos muestra que las sesiones de descifrado SSL van a alcanzar la capacidad máxima del cortafuegos pronto. Clase: Salud Categoría: Capacidad Ticket de asistencia en la aplicación: No
Aproximándose a la capacidad máxima - Direcciones FQDN (Alerta premium)	El número de objetos de dirección FQDN ha sido sistemáticamente alto y se está acercando a la capacidad máxima que el cortafuegos puede soportar. Clase: Salud Categoría: Capacidad Ticket de asistencia en la aplicación: No
Aproximándose a la capacidad máxima - Túneles de GlobalProtect (sin cliente) (Alerta premium)	El número de túneles VPN sin cliente de GlobalProtect se está acercando a la capacidad máxima que puede soportar el cortafuegos. Clase: Salud Categoría: Capacidad Ticket de asistencia en la aplicación: No
Aproximándose a la capacidad máxima - Pares de IKE (Alerta premium)	El número de pares de IKE ha sido sistemáticamente alto y se está acercando a la capacidad máxima que el cortafuegos puede soportar. Clase: Salud

Alerta	Description (Descripción)
	Categoría: Capacidad Ticket de asistencia en la aplicación: No
Aproximándose a la capacidad máxima - CPU de plano de gestión (Alerta premium)	El uso de la CPU del plano de gestión (MP) ha sido sistemáticamente alto y se está acercando a la capacidad máxima que el dispositivo puede soportar. Clase: Salud Categoría: Capacidad Ticket de asistencia en la aplicación: No
Aproximándose a la capacidad máxima - Memoria del plano de gestión (Alerta premium)	El uso de la memoria del plano de gestión (MP) ha sido sistemáticamente alto y se está acercando a la capacidad máxima que el dispositivo puede soportar. Clase: Salud Categoría: Capacidad Ticket de asistencia en la aplicación: No
Aproximándose a la capacidad máxima - Políticas de NAT (Alerta premium)	El número de reglas de política NAT ha sido sistemáticamente alto a lo largo del tiempo y se está acercando a la capacidad máxima que el cortafuegos puede soportar. Clase: Salud Categoría: Capacidad Ticket de asistencia en la aplicación: No
Aproximándose a la capacidad máxima - Políticas de seguridad (Alerta premium)	El número de reglas de la política de seguridad ha sido sistemáticamente alto y se está acercando a la capacidad máxima que puede soportar el cortafuegos. Clase: Salud Categoría: Capacidad Ticket de asistencia en la aplicación: No
Aproximándose a la capacidad máxima - Grupos de servicio (Alerta premium)	El número de objetos del grupo de servicios ha sido sistemáticamente alto y se está acercando a la capacidad máxima que el cortafuegos puede soportar. Clase: Salud Categoría: Capacidad Ticket de asistencia en la aplicación: No

Alerta	Description (Descripción)
Aproximándose a la capacidad máxima - Objetos de servicio (Alerta premium)	El número de objetos de servicios ha sido sistemáticamente alto y se está acercando a la capacidad máxima que el cortafuegos puede soportar. Clase: Salud Categoría: Capacidad Ticket de asistencia en la aplicación: No
Aproximándose a la capacidad máxima - Utilización de la tabla de sesiones (Alerta premium)	El uso de la Tabla de sesiones (%) ha sido sistemáticamente alto a lo largo del tiempo y se está acercando a la capacidad máxima que puede soportar el cortafuegos o la licencia de VM. Clase: Salud Categoría: Capacidad Ticket de asistencia en la aplicación: No
Aproximándose a la capacidad máxima - Túneles VPN de sitio a sitio (Alerta premium)	El número de túneles VPN de sitio a sitio, que comprenden tanto túneles IPsec como identificadores proxy, ha sido sistemáticamente alto y se está acercando a la capacidad máxima que puede soportar el cortafuegos. Clase: Salud Categoría: Capacidad Ticket de asistencia en la aplicación: No
Aproximándose a la capacidad máxima - Direcciones IP o URL dentro de las EDL (Alerta premium)	El número de direcciones IP, URL o dominios dentro de la(s) EDL configurada(s) utilizada(s) en la política de este cortafuegos se está acercando a la capacidad máxima que el cortafuegos puede soportar. Clase: Salud Categoría: Uso de recursos Ticket de asistencia en la aplicación: No
Aproximándose a la capacidad máxima - Sistemas virtuales (Alerta premium)	El análisis del forecasting de datos muestra que la configuración de Virtual Systems va a alcanzar la capacidad máxima admitida por la licencia del cortafuegos. Clase: Salud Categoría: Capacidad Ticket de asistencia en la aplicación: No
Aproximándose a los límites máximos de configuración	Los objetos de cortafuegos como reglas, grupos y perfiles de seguridad se acercan a los límites del dispositivo.

Alerta	Description (Descripción)
(Alerta premium)	Clase: Salud Categoría: Límites de configuración Ticket de asistencia en la aplicación: No
Vencimiento del certificado (Alerta premium)	Uno o más certificados en el cortafuegos se han revocado o están a punto de caducar. Clase: Salud Categoría: Certificado Ticket de asistencia en la aplicación: No
Confirmación y envío fallido (Alerta premium)	El envío de configuración ha fallado. Clase: Salud Categoría: Configuración Ticket de asistencia en la aplicación: No
Uso de la memoria de configuración acercándose a los límites máximos (Alerta premium)	La configuración del cortafuegos se está acercando a su límite máximo de uso de memoria. Durante las confirmaciones, la memoria de configuración total del cortafuegos debe admitir dos copias: la configuración actual 'en uso' y la nueva configuración 'a usar'. Si la memoria asignada por configuración supera el 50 %, el cortafuegos alcanza su capacidad, lo que resulta en un fallo de confirmación. Clase: Salud Categoría: Uso de recursos Ticket de asistencia en la aplicación: No
Descarte de paquete de DP (Alerta premium)	La Alerta detecta descartes de paquetes inusuales por diferentes motivos Clase: Salud Categoría: Rendimiento Ticket de asistencia en la aplicación: No
Estado de los enlaces de HA (Alerta premium)	El estado de un enlace que está conectado al cortafuegos. El cortafuegos está conectado a varios sistemas para varios servicios. Esta alerta proporciona el estado de estas conexiones. Clase: Salud Categoría: Alta disponibilidad Ticket de asistencia en la aplicación: No

Alerta	Description (Descripción)
Tasa alta de ingesta de logs (Alerta premium)	Un Recopilador de logs se está acercando a su tasa de ingesta máxima soportada. Clase: Salud Categoría: de creación de logs Ticket de asistencia en la aplicación: No
Alta actividad de consulta de logs (Alerta premium)	El recopilador de logs está cerca de su capacidad de trabajos de consulta o informes. Clase: Salud Categoría: de creación de logs Ticket de asistencia en la aplicación: No
Aumento de la latencia de tráfico - Búfer de paquetes (Alerta premium)	Los recursos del Búfer de paquetes se están agotando en el dispositivo. Clase: Salud Categoría: Uso de recursos Ticket de asistencia en la aplicación: Sí
Aumento de la latencia de tráfico - Descriptor de paquetes (Alerta premium)	Los recursos de Packet Descriptor se están agotando en el dispositivo. Clase: Salud Categoría: Uso de recursos Ticket de asistencia en la aplicación: Sí
Aumento de la latencia de tráfico - TCP o UDP (Alerta premium)	El cortafuegos ha recibido una gran cantidad de tráfico de una aplicación que se cataloga como unknown-tcp o unknown-udp. Clase: Salud Categoría: Uso de recursos Ticket de asistencia en la aplicación: No
Perdió la conexión con el destino de reenvío de logs (Alerta premium)	El dispositivo no puede conectarse a su destino de reenvío de logs. Clase: Salud Categoría: de creación de logs Ticket de asistencia en la aplicación: No

Alerta	Description (Descripción)
Período mínimo de retención de logs superado (Alerta premium)	El recopilador de logs contiene logs que son más antiguos que el período de retención mínimo definido. Clase: Salud Categoría: de creación de logs Ticket de asistencia en la aplicación: No
Fallo de asignación de NAT (Alerta premium)	Al menos una regla NAT no puede asignar suficientes recursos para la traducción. Clase: Salud Categoría: Recurso de grupo de NAT Ticket de asistencia en la aplicación: Sí
Uso de grupo NAT (Alerta premium)	Una o más reglas NAT tienen un alto uso de recursos. Clase: Salud Categoría: Recurso de grupo de NAT Ticket de asistencia en la aplicación: No
Alerta de rendimiento de aplicaciones SD-WAN de NGFW (Alerta premium)	Indica la lista de aplicaciones que se ve afectada por un mal rendimiento del enlace. Clase: Salud Categoría: Rendimiento de SD-WAN Ticket de asistencia en la aplicación: No
Alerta de rendimiento de enlaces SD-WAN de NGFW (Alerta premium)	Indica lo que está causando un rendimiento degradado en sus aplicaciones y servicios o enlaces. Clase: Salud Categoría: Rendimiento de SD-WAN Ticket de asistencia en la aplicación: No
Nivel de registro de logs no predeterminado (Alerta premium)	Esta alerta se activa cuando el nivel de registro de logs de un servicio no se establece en su configuración predeterminada. Esta alerta garantiza que los servicios mantengan de forma constante la configuración de registro de logs designada. Clase: Salud Categoría: Uso de recursos Ticket de asistencia en la aplicación: No

Alerta	Description (Descripción)
Servidor supervisado por el agente de User-ID integrado de PAN-OS desconectado (Alerta premium)	Esta alerta se activa cuando el servidor, supervisado por el agente de User-ID integrado de PAN-OS (User-ID sin agente), pierde la conexión con el cortafuegos. Este servidor supervisado es un componente crítico para asignar identidades de usuario a actividades de red. Clase: Salud Categoría: Ticket de asistencia en la aplicación: No
El uso de memoria de configuración de políticas está acercándose a los límites máximos (Alerta premium)	Esta alerta detecta si el uso de la memoria de configuración de las políticas supera un umbral crítico. Clase: Salud Categoría: Uso de recursos Ticket de asistencia en la aplicación: No
Latencia de tráfico - Descriptores de paquetes (en chip) (Alerta premium)	Los recursos de Packet Descriptor (en chip) se están agotando en el dispositivo. Clase: Salud Categoría: Inundación/DoS Ticket de asistencia en la aplicación: No
Túnel caído (Alerta premium)	Uno o más túneles VPN de sitio a sitio están caídos. Clase: Salud Categoría: VPN de sitio a sitio Ticket de asistencia en la aplicación: Sí
Perfil de protección de zonas - Detección de inundaciones (Alerta premium)	Las conexiones establecidas en la zona o la tasa de paquetes entrantes son excesivas o anormales. Clase: Salud Categoría: Inundación/DoS Ticket de asistencia en la aplicación: Sí
Perfil de protección de zona - Recomendación de umbral (Alerta premium)	A una zona le falta un perfil de protección de zona o es necesario ajustar los valores umbral de un perfil de protección de zona. Clase: Salud Categoría: Inundación/DoS Ticket de asistencia en la aplicación: No

Alertas de estado gratuitas

En la tabla siguiente se identifican las alertas gratuitas que AIOps for NGFW puede generar y que están relacionadas con el estado de su plataforma.

No se requiere una licencia Premium para que AIOps for NGFW pueda generar estas alertas.

Alerta	Description (Descripción)
Fallo de la alimentación de la tarjeta (Alerta gratuita)	Se ha detectado un fallo en la tarjeta, lo que sugiere un posible problema con la tarjeta o su colocación dentro del bastidor. Clase: Salud Categoría: Hardware Ticket de asistencia en la aplicación: No
El tamaño de la configuración está alcanzando el límite de capacidad del dispositivo (Alerta gratuita)	El tamaño de la configuración de este dispositivo ha alcanzado su límite de capacidad. Clase: Salud Categoría: Configuración Ticket de asistencia en la aplicación: No
Unidad del sistema degradada (Alerta gratuita)	Se ha identificado una unidad del sistema degradada mediante la supervisión de los valores de sus atributos. Clase: Salud Categoría: Hardware Ticket de asistencia en la aplicación: No
Telemetría diferida (Alerta gratuita)	Los motores de análisis no tienen telemetría nueva de este NGFW/Panorama. Clase: Salud Categoría: Telemetría Ticket de asistencia en la aplicación: Sí
Fallo FE100 (Alerta gratuita)	Se ha detectado un error de calibración en el chip FE100 en el cortafuegos. Este problema suele indicar un error de hardware. Clase: Salud Categoría: Hardware Ticket de asistencia en la aplicación: No
Problemas con los ventiladores	Un ventilador o una bandeja de ventiladores activó una alarma en el dispositivo.

Alerta	Description (Descripción)
(Alerta gratuita)	Clase: Salud Categoría: Hardware Ticket de asistencia en la aplicación: No
Fallo Error de comprobación de máquina (Alerta gratuita)	Se ha detectado un error de comprobación de máquina. Este problema generalmente indica un fallo de hardware en la CPU. Clase: Salud Categoría: Hardware Ticket de asistencia en la aplicación: No
Cortafuegos desconectado de Cortex Data Lake (Alerta gratuita)	Se ha perdido la conexión entre el FW y Strata Logging Service. Clase: Salud Categoría: Conectividad SLS Ticket de asistencia en la aplicación: No
Cortafuegos desconectado de Panorama (Alerta gratuita)	Se ha perdido la conexión entre el cortafuegos y Panorama. Clase: Salud Categoría: Fallo de conexión Ticket de asistencia en la aplicación: No
Copia de seguridad de HA (Alerta gratuita)	Los enlaces de copia de seguridad de HA no están configurados actualmente. Clase: Salud Categoría: Alta disponibilidad Ticket de asistencia en la aplicación: No
Estado de conexión entre pares de HA (Alerta gratuita)	Uno de los cortafuegos en el par de HA está en un estado no saludable. Clase: Salud Categoría: Alta disponibilidad Ticket de asistencia en la aplicación: Sí
Uso de espacio en disco alto - Partición Pancfg (Alerta gratuita)	La partición del disco duro está cerca o a su capacidad. Clase: Salud Categoría: Uso de recursos Ticket de asistencia en la aplicación: Sí

Alerta	Description (Descripción)
Uso de espacio en disco alto: partición panlogs (Alerta gratuita)	La partición del disco duro está cerca o a su capacidad. Clase: Salud Categoría: Uso de recursos Ticket de asistencia en la aplicación: Sí
Alto uso de espacio en disco: partición raíz (Alerta gratuita)	La partición del disco duro está cerca o a su capacidad. Clase: Salud Categoría: Uso de recursos Ticket de asistencia en la aplicación: Sí
Actividad de procesamiento alta (Alerta gratuita)	Uno o más recursos informáticos se están agotando en el dispositivo. Clase: Salud Categoría: Uso de recursos Ticket de asistencia en la aplicación: No
Error de IPQ (Alerta gratuita)	Se ha detectado un error IPQ (cola de paquetes de entrada) en uno de los chips FE100 del cortafuegos. Este error suele indicar que es necesario una recolocación o que hay un error de hardware. Clase: Salud Categoría: Hardware Ticket de asistencia en la aplicación: No
Alimentación de entrada irregular (Alerta gratuita)	Los niveles de potencia del dispositivo están fuera del rango normal. Clase: Salud Categoría: Hardware Ticket de asistencia en la aplicación: No
Caducidad de la licencia (Alerta gratuita)	Una o más de sus licencias están a punto de o ya han caducado. Clase: Salud Categoría: PanOS y suscripción Ticket de asistencia en la aplicación: No
Fallo de la unidad de registro	Se ha identificado una unidad de registro de logs que falla a través de la supervisión del estado del disco del cortafuegos. Clase: Salud

Alerta	Description (Descripción)
(Alerta gratuita)	Categoría: Hardware Ticket de asistencia en la aplicación: No
Tarjeta MPC - Fallo del CPLD (Alerta gratuita)	La tarjeta de procesador de gestión (MPC) es un componente esencial para el PA-5450, ya que proporciona funciones de gestión, registro de logs y alta disponibilidad. La tarjeta MPC ha experimentado un error debido a un problema con su componente, el dispositivo lógico programable complejo (CPLD). Clase: Salud Categoría: Hardware Ticket de asistencia en la aplicación: No
Caducidad del certificado de gestión de NGFW/ Panorama (Alerta gratuita)	Esta alerta detecta la caducidad del certificado de gestión NGFW/ Panorama. Clase: Salud Categoría: Certificado Ticket de asistencia en la aplicación: No
Tarjeta NPC - Fallo FE100 (Alerta gratuita)	Las tarjetas de procesamiento de red (NPC) proporcionan conectividad de red y son esenciales para el procesamiento del tráfico de red. Una tarjeta NPC ha experimentado un problema con su componente FE100, lo que ha provocado su fallo. Clase: Salud Categoría: Hardware Ticket de asistencia en la aplicación: No
Pares fuera de sincronización - Configuración (Alerta gratuita)	Las configuraciones del sistema en los pares de alta disponibilidad no coinciden. Clase: Salud Categoría: Alta disponibilidad Ticket de asistencia en la aplicación: No
Pares fuera de sincronización - Contenido dinámico (Alerta gratuita)	El contenido dinámico, como antivirus o aplicaciones y amenazas, no coincide entre los compañeros de alta disponibilidad. Clase: Salud Categoría: Alta disponibilidad Ticket de asistencia en la aplicación: No
Pares fuera de sincronización - Sesiones	Las sesiones no coinciden ni están actualizadas entre los pares de alta disponibilidad.

Alerta	Description (Descripción)
(Alerta gratuita)	Clase: Salud Categoría: Alta disponibilidad Ticket de asistencia en la aplicación: No
Pares fuera de sincronización - Software (Alerta gratuita)	Las versiones de software de PAN-OS en los pares de alta disponibilidad no coinciden. Clase: Salud Categoría: Alta disponibilidad Ticket de asistencia en la aplicación: No
Contenido dinámico obsoleto (Alerta gratuita)	El contenido dinámico instalado en el dispositivo es obsoleto en comparación con el contenido disponible en el servidor de actualizaciones. Clase: Salud Categoría: Contenido dinámico Ticket de asistencia en la aplicación: No
Vida útil de PAN-OS (Alerta gratuita)	Su versión actual de PAN-OS ya no es compatible. Clase: Salud Categoría: PanOS y suscripción Ticket de asistencia en la aplicación: No
Vulnerabilidad conocida de PAN-OS (Alerta gratuita)	Su versión actual de PAN-OS tiene vulnerabilidades conocidas. Clase: Salud Categoría: Contenido dinámico Ticket de asistencia en la aplicación: No
Caducidad del certificado raíz y predeterminado de PAN-OS: escenario 1 (Alerta gratuita)	El certificado raíz y el certificado predeterminado del cortafuegos han caducado. Clase: Salud Categoría: Certificado Ticket de asistencia en la aplicación: No
Error de PCI (Alerta gratuita)	Una interconexión de componentes periféricos (PCI) es responsable de conectar el plano de gestión (MP) al plano de control (CP). Un determinado error relacionado con este componente indica un fallo en su funcionalidad. Clase: Salud

Alerta	Description (Descripción)
	Categoría: Hardware Ticket de asistencia en la aplicación: No
Error de supervisión de ruta - Tarjeta (Alerta gratuita)	Se ha detectado un error de supervisión de ruta en una tarjeta ubicada dentro de las ranuras del cortafuegos. Clase: Salud Categoría: Hardware Ticket de asistencia en la aplicación: No
Fallo de puerto (Alerta gratuita)	Se ha detectado un fallo relacionado con el puerto físico de gestión o uno de los puertos físicos de alta disponibilidad. Clase: Salud Categoría: Hardware Ticket de asistencia en la aplicación: No
Agotamiento de la memoria de proceso - Configd (Alerta gratuita)	Los procesos del plano de gestión del dispositivo están agotando su memoria disponible. Clase: Salud Categoría: Uso de recursos Ticket de asistencia en la aplicación: Sí
Agotamiento de la memoria de proceso - Servidor de dispositivo (Alerta gratuita)	Los procesos del plano de gestión del dispositivo están agotando su memoria disponible. Clase: Salud Categoría: Uso de recursos Ticket de asistencia en la aplicación: Sí
Agotamiento de la memoria de proceso - Receptor de logs (Alerta gratuita)	Los procesos del plano de gestión del dispositivo están agotando su memoria disponible. Clase: Salud Categoría: Uso de recursos Ticket de asistencia en la aplicación: Sí
Agotamiento de la memoria de procesos - Servidor de gestión (Alerta gratuita)	Los procesos del plano de gestión del dispositivo están agotando su memoria disponible. Clase: Salud Categoría: Uso de recursos Ticket de asistencia en la aplicación: Sí

Alerta	Description (Descripción)
Agotamiento de la memoria de proceso - Id de usuario (Alerta gratuita)	Los procesos del plano de gestión del dispositivo están agotando su memoria disponible. Clase: Salud Categoría: Uso de recursos Ticket de asistencia en la aplicación: Sí
Fallo redundante de la fuente de alimentación (Alerta gratuita)	La redundancia de la fuente de alimentación no se logra porque no se ha insertado, la fuente de alimentación no ha funcionado correctamente o no se ha logrado la redundancia completa. Clase: Salud Categoría: Hardware Ticket de asistencia en la aplicación: Sí
Latencia de reenvío de logs del Strata Logging Service (Alerta gratuita)	La latencia de reenvío en Strata Logging Service va más allá de un valor aceptable. Clase: Salud Categoría: Estado de SLS Ticket de asistencia en la aplicación: No
Reenvío de logs sin conexión de Strata Logging Service (Alerta gratuita)	El servicio de reenvío de logs de Strata Logging Service no funciona Clase: Salud Categoría: Estado de SLS Ticket de asistencia en la aplicación: No
Latencia de ingesta de logs de Strata Logging Service (Alerta gratuita)	La latencia de ingesta en Strata Logging Service va más allá de un valor aceptable. Clase: Salud Categoría: Estado de SLS Ticket de asistencia en la aplicación: No
Ingesta de logs sin conexión de Strata Logging Service (Alerta gratuita)	El servicio de ingesta de Strata Logging Service no funciona. Clase: Salud Categoría: Estado de SLS Ticket de asistencia en la aplicación: No

Alerta	Description (Descripción)
El almacenamiento de logs de Strata Logging Service está alcanzando el límite (Alerta gratuita)	Los tipos de log se aproximan al límite máximo de almacenamiento configurado. Clase: Salud Categoría: de creación de logs Ticket de asistencia en la aplicación: No
Problemas térmicos (Alerta gratuita)	La temperatura del dispositivo está fuera del rango normal. Clase: Salud Categoría: Hardware Ticket de asistencia en la aplicación: No

Alertas de servicio

En la siguiente tabla se identifican las alertas que AIOps for NGFW puede generar en relación con los servicios que tiene conectados a él.

Alerta	Description (Descripción)
Cortafuegos desconectado del Strata Logging Service (Alerta gratuita)	La conexión entre el cortafuegos (FW) y SLS se ha perdido durante más de 5 minutos. Categoría: Conectividad SLS Ticket de asistencia en la aplicación: No
Ingesta de logs sin conexión de Strata Logging Service (Alerta gratuita)	El servicio de ingesta de SLS lleva sin funcionar más de 5 minutos. Categoría: Estado de SLS Ticket de asistencia en la aplicación: No
Reenvío de logs sin conexión de Strata Logging Service (Alerta gratuita)	El servicio de reenvío de registros de SLS lleva sin funcionar más de 5 minutos. Categoría: Estado de SLS Ticket de asistencia en la aplicación: No
Latencia de ingesta de logs de Strata Logging Service (Alerta gratuita)	La latencia de ingesta de SLS supera los 10 minutos en los últimos 15 minutos. Categoría: Estado de SLS Ticket de asistencia en la aplicación: No
Latencia de reenvío de logs del Strata Logging Service (Alerta gratuita)	La latencia de reenvío en SLS supera los 10 minutos en los últimos 15 minutos. Categoría: Estado de SLS Ticket de asistencia en la aplicación: No
El almacenamiento de logs de Strata Logging Service está alcanzando el límite (Alerta gratuita)	Los tipos de log se aproximan al límite máximo de almacenamiento configurado. Categoría: de creación de logs Ticket de asistencia en la aplicación: No

Alertas generadas mediante el uso del aprendizaje automático

En la siguiente tabla se identifican las alertas que AIOps for NGFW puede generar mediante el aprovechamiento del aprendizaje automático.

Alerta	Description (Descripción)
Uso de recursos de tráfico cifrados adversos (Alerta premium)	Los recursos de tráfico cifrados se están agotando. Clase: Salud Categoría: Uso de recursos Ticket de asistencia en la aplicación: No Tipo de detección: Anomalía
Uso adverso de recursos (Alerta premium)	El cortafuegos tiene valores anómalos para conexiones por segundo (CPS), rendimiento o número de sesiones. Clase: Salud Categoría: Uso de recursos Ticket de asistencia en la aplicación: No Tipo de detección: Anomalía
Aproximándose a los límites máximos de configuración (Alerta premium)	Los objetos de cortafuegos como reglas, grupos y perfiles de seguridad se acercan a los límites del dispositivo. Clase: Salud Categoría: Límites de configuración Ticket de asistencia en la aplicación: No Tipo de detección: Anomalía
Actividad de procesamiento alta (Alerta gratuita)	Uno o más recursos informáticos se están agotando en el dispositivo. Clase: Salud Categoría: Uso de recursos Ticket de asistencia en la aplicación: No
Aumento de la latencia de tráfico - Búfer de paquetes (Alerta premium)	Los recursos del Búfer de paquetes se están agotando en el dispositivo. Clase: Salud Categoría: Uso de recursos

Alerta	Description (Descripción)
	Ticket de asistencia en la aplicación: Sí Tipo de detección: Anomalía
Aumento de la latencia de tráfico - Descriptor de paquetes (Alerta premium)	Los recursos de Packet Descriptor se están agotando en el dispositivo. Clase: Salud Categoría: Uso de recursos Ticket de asistencia en la aplicación: Sí Tipo de detección: Anomalía
Latencia de tráfico - Descriptores de paquetes (en chip) (Alerta premium)	Los recursos de Packet Descriptor (en chip) se están agotando en el dispositivo. Clase: Salud Categoría: Inundación/DoS Ticket de asistencia en la aplicación: No Tipo de detección: Anomalía
Aproximándose a la capacidad máxima - Tabla de ARP (Alerta premium)	El análisis del forecasting de datos muestra que las entradas de la tabla ARP van a alcanzar la capacidad máxima del cortafuegos pronto. Clase: Salud Categoría: Capacidad Ticket de asistencia en la aplicación: No
Aproximándose a la capacidad máxima - Grupos de direcciones (Alerta premium)	El número de objetos del grupo de direcciones ha sido sistemáticamente alto y se está acercando a la capacidad máxima que el cortafuegos puede soportar. Clase: Salud Categoría: Capacidad Ticket de asistencia en la aplicación: No
Aproximándose a la capacidad máxima - Objetos de direcciones (Alerta premium)	El número de objetos de dirección ha sido sistemáticamente alto y se está acercando a la capacidad máxima que el cortafuegos puede soportar. Clase: Salud Categoría: Capacidad Ticket de asistencia en la aplicación: No

Alerta	Description (Descripción)
Aproximándose a la capacidad máxima - CPU de plano de datos (Alerta premium)	El uso de la CPU del plano de datos (DP) ha sido sistemáticamente alto a lo largo del tiempo y se está acercando a la capacidad máxima que el dispositivo puede soportar. Clase: Salud Categoría: Capacidad Ticket de asistencia en la aplicación: No
Aproximándose a la capacidad máxima - Uso de descifrado (Alerta premium)	El análisis del forecasting de datos muestra que las sesiones de descifrado SSL van a alcanzar la capacidad máxima del cortafuegos pronto. Clase: Salud Categoría: Capacidad Ticket de asistencia en la aplicación: No
Aproximándose a la capacidad máxima - Direcciones FQDN (Alerta premium)	El número de objetos de dirección FQDN ha sido sistemáticamente alto y se está acercando a la capacidad máxima que el cortafuegos puede soportar. Clase: Salud Categoría: Capacidad Ticket de asistencia en la aplicación: No
Aproximándose a la capacidad máxima - Túneles de GlobalProtect (sin cliente) (Alerta premium)	El número de túneles VPN sin cliente de GlobalProtect se está acercando a la capacidad máxima que puede soportar el cortafuegos. Clase: Salud Categoría: Capacidad Ticket de asistencia en la aplicación: No
Aproximándose a la capacidad máxima - Pares de IKE (Alerta premium)	El número de pares de IKE ha sido sistemáticamente alto y se está acercando a la capacidad máxima que el cortafuegos puede soportar. Clase: Salud Categoría: Capacidad Ticket de asistencia en la aplicación: No
Aproximándose a la capacidad máxima - CPU de plano de gestión (Alerta premium)	El uso de la CPU del plano de gestión (MP) ha sido sistemáticamente alto y se está acercando a la capacidad máxima que el dispositivo puede soportar. Clase: Salud

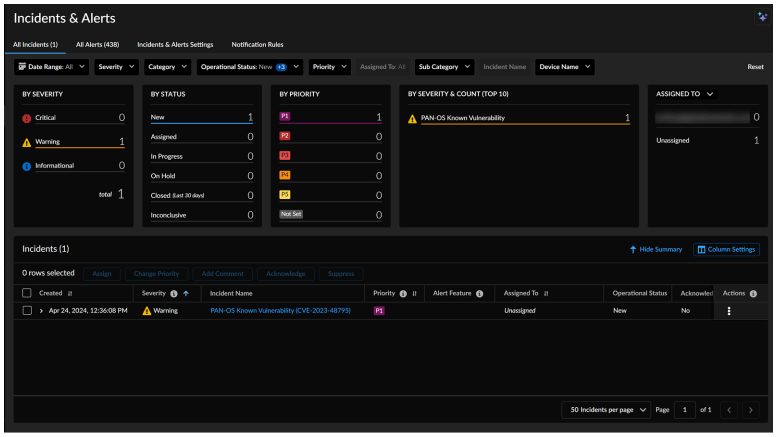
Alerta	Description (Descripción)
	Categoría: Capacidad Ticket de asistencia en la aplicación: No
Aproximándose a la capacidad máxima - Memoria del plano de gestión (Alerta premium)	El uso de la memoria del plano de gestión (MP) ha sido sistemáticamente alto y se está acercando a la capacidad máxima que el dispositivo puede soportar. Clase: Salud Categoría: Capacidad Ticket de asistencia en la aplicación: No
Aproximándose a la capacidad máxima - Políticas de NAT (Alerta premium)	El número de reglas de política NAT ha sido sistemáticamente alto a lo largo del tiempo y se está acercando a la capacidad máxima que el cortafuegos puede soportar. Clase: Salud Categoría: Capacidad Ticket de asistencia en la aplicación: No
Aproximándose a la capacidad máxima - Políticas de seguridad (Alerta premium)	El número de reglas de la política de seguridad ha sido sistemáticamente alto y se está acercando a la capacidad máxima que puede soportar el cortafuegos. Clase: Salud Categoría: Capacidad Ticket de asistencia en la aplicación: No
Aproximándose a la capacidad máxima - Grupos de servicio (Alerta premium)	El número de objetos del grupo de servicios ha sido sistemáticamente alto y se está acercando a la capacidad máxima que el cortafuegos puede soportar. Clase: Salud Categoría: Capacidad Ticket de asistencia en la aplicación: No
Aproximándose a la capacidad máxima - Objetos de servicio (Alerta premium)	El número de objetos de servicios ha sido sistemáticamente alto y se está acercando a la capacidad máxima que el cortafuegos puede soportar. Clase: Salud Categoría: Capacidad Ticket de asistencia en la aplicación: No

Alerta	Description (Descripción)
Aproximándose a la capacidad máxima - Utilización de la tabla de sesiones (Alerta premium)	El uso de la Tabla de sesiones (%) ha sido sistemáticamente alto a lo largo del tiempo y se está acercando a la capacidad máxima que puede soportar el cortafuegos o la licencia de VM. Clase: Salud Categoría: Capacidad Ticket de asistencia en la aplicación: No
Aproximándose a la capacidad máxima - Sistemas virtuales (Alerta premium)	El análisis del forecasting de datos muestra que la configuración de Virtual Systems va a alcanzar la capacidad máxima admitida por la licencia del cortafuegos. Clase: Salud Categoría: Capacidad Ticket de asistencia en la aplicación: No
Aproximándose a la capacidad máxima - Túneles VPN de sitio a sitio (Alerta premium)	El número de túneles VPN de sitio a sitio, que comprenden tanto túneles IPsec como identificadores proxy, ha sido sistemáticamente alto y se está acercando a la capacidad máxima que puede soportar el cortafuegos. Clase: Salud Categoría: Capacidad Ticket de asistencia en la aplicación: No
Alerta de rendimiento de aplicaciones SD-WAN de NGFW (Alerta premium)	Indica la lista de aplicaciones que se ve afectada por un mal rendimiento del enlace. Clase: Salud Categoría: Rendimiento de SD-WAN Ticket de asistencia en la aplicación: No Tipo de detección: Anomalía
Alerta de rendimiento de enlaces SD-WAN de NGFW (Alerta premium)	Indica lo que está causando un rendimiento degradado en sus aplicaciones y servicios o enlaces. Clase: Salud Categoría: Rendimiento de SD-WAN Ticket de asistencia en la aplicación: No Tipo de detección: Anomalía

Gestionar incidentes de NGFW

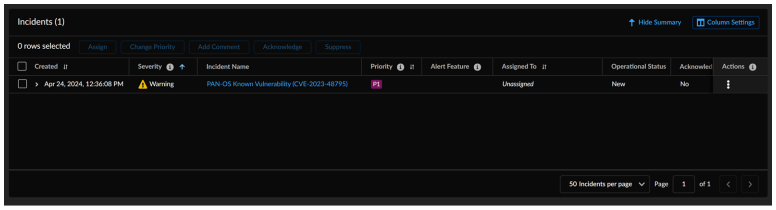
¿Dónde puedo usar esto?	¿Qué necesito?
• , incluidos los financiados por Créditos de NGFW de software	Uno de estos: ❑ o ❑ o

Obtenga una vista panorámica de los incidentes de NGFW seleccionando **Incidents & Alerts (Incidentes y alertas)** > **NGFW** > **All Incidents (Todos los incidentes)**. Explore la página de incidentes para mantenerse informado sobre los cambios en su implementación para que pueda investigarlos y tomar acciones preventivas si es necesario. Tiene acceso directo a una lista detallada de incidentes junto con resúmenes visuales críticos. También puede **Hide Summary (Ocultar resumen)** para ocultar los widgets y solo ver los incidentes en formato tabular.



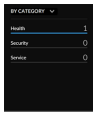
Estos son los datos que se muestran en **All Incidents (Todos los incidentes)**.

- **Incidents (Incidentes)**: Muestra todos los incidentes.



  En esta tabla puedes realizar las siguientes tareas:

  - **Ocultar resumen** para ocultar los widgets y solo ver los incidentes en formato tabular.
  - Expanda un incidente para ver su descripción e impacto.
  - En Acciones, puede realizar las siguientes acciones:
    - **Asignar** un incidente a un usuario, a usted mismo, o anular la asignación de un incidente.
    - **Cambiar prioridad** de un incidente o seleccionar No establecido para eliminar la prioridad.
    - **Reconocer** un incidente seleccionando **Sí**, para confirmar que ha visto el incidente.
    - **Suprimir** establece un incidente en un estado operativo de "En espera" cuando no planifica resolverlo de forma activa.
    - **Añadir comentario** para un incidente.
  - Haga clic en un incidente para ver sus detalles.
  - Utilice **Configuración de columnas** para ver u ocultar columnas específicas para incidentes y reorganizar el orden predeterminado de las columnas. Estos cambios persistirán en sesiones futuras.
- **ASIGNADO A**: Muestra el número de incidentes de la persona o entidad que tiene la tarea de resolverlas. En la parte superior se muestran los incidentes asignados al usuario conectado actual y los incidentes no asignados. También puede ver el número de incidentes **POR CATEGORÍA** seleccionándola en la lista desplegable.



- **POR GRAVEDAD Y RECUENTO (TOP 10):** Muestra los incidentes clasificados por gravedad, junto con el recuento de incidentes en cada categoría. Los incidentes críticos se priorizan primero, seguidos de los incidentes de advertencia y luego los incidentes informativos.

- **POR ESTADO:** Muestra el número total de incidentes por estado.
  - Nuevo indica los incidentes que no se han asignado.
  - Asignado indica los incidentes que se han asignado a un usuario.
  - En curso indica que se está trabajando en el incidente.
  - En espera indica que no planifica resolver un incidente o una incidencia de forma activa.
  - Cerrado indica los incidentes cerrados durante los últimos 30 días.
  - No concluyente indica que no hay solución para estos incidentes.

- **POR GRAVEDAD:** Muestra el número total de incidentes clasificados como críticos, de advertencia e informativos.

- **POR PRIORIDAD:** Muestra los incidentes según su prioridad, siendo P1 el más grave.

Ver detalles del incidente

¿Dónde puedo usar esto?	¿Qué necesito?
• , incluidos los financiados por Créditos de NGFW de software	Uno de estos: ❑ o ❑ o

Desde **All Incidents (Todos los incidentes)**, puede seleccionar un incidente para abrir una página con detalles sobre el mismo. La pestaña **Summary (Resumen** muestra los siguientes detalles:

1. Resumen del incidente con detalles. Puede cambiar la prioridad del incidente o asignarla a un usuario.
2. Impacto causado por el incidente, es decir, el número de cortafuegos NGFW afectados.
3. Acción recomendada para solucionar el problema.

También puede hacer clic en CVE para ver sus detalles en Avisos de seguridad de Palo Alto Networks y vulnerabilidades en la versión PAN-OS.

La pestaña **Correlated Alerts & Activity (Actividades y alertas correlacionadas)** muestra los siguientes detalles:

- Las alertas correlacionadas para el incidente seleccionado
- Actividad registrada del incidente