Determinar el tráfico manejado por una instancia de Snort específica

Contenido

Introducción

Este documento describe cómo determinar el tráfico manejado por una instancia específica de Snort en un entorno Cisco Firepower Threat Defence (FTD).

Prerequisites

Requirements

Cisco recomienda que conozca estos productos:

- FirePOWER Management Center seguro (FMC)
- Firepower Threat Defense (FTD) seguro
- Syslog y SNMP
- API REST

Componentes Utilizados

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se iniciaron con una configuración sin definir (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

1. Uso de comandos CLI

Mediante la interfaz de línea de comandos (CLI) del dispositivo FTD, puede acceder a información detallada sobre las instancias de Snort y el tráfico que gestionan.

- Este comando proporciona los detalles sobre los procesos Snort en ejecución.

show snort instances

Este es un ejemplo del resultado del comando.

> show snort instances

Total number of instances available - 1 +----------+----------+ | INSTANCE | PID | +----------+----------+ | **1** | **4765** | <<< One instance available and its process ID +----------+----------+

- Para obtener información más detallada sobre las estadísticas de tráfico gestionadas por las instancias de Snort, se pueden utilizar estos comandos. Muestra varias estadísticas, incluido el número de paquetes procesados, descartados y las alertas generadas por cada instancia de Snort.

show snort statistics

Este es un ejemplo del resultado del comando.

> show snort statistics Packet Counters: Passed Packets 3791881977 Blocked Packets 707722 Injected Packets 87 **Packets bypassed (Snort Down) 253403701** <<< Packets bypassed **Packets bypassed (Snort Busy) 0** Flow Counters: Fast-Forwarded Flows 294816 Blacklisted Flows 227 Miscellaneous Counters: Start-of-Flow events 0 End-of-Flow events 317032 Denied flow events 14230 Frames forwarded to Snort before drop 0 Inject packets dropped 0 TCP Ack bypass Packets 6412936 TCP Meta-Ack Packets 2729907 Portscan Events 0 Packet decode optimized 21608793 Packet decode legacy 6558642

show asp inspect-dp snort

Este es un ejemplo del resultado del comando.

> show asp inspect-dp snort

SNORT Inspect Instance Status Info Id Pid Cpu-Usage Conns Segs/Pkts Status tot (usr | sys) -- ----- ---------- ---------- ---------- -- -------- 0 16450 8% (7%| 0%) 2.2 K 0 READY 1 16453 9% (8%| 0%) 2.2 K 0 READY 2 16451 6% (5%| 1%) 2.3 K 0 READY 3 16454 5% (5%| 0%) 2.2 K 1 READY 4 16456 6% (6%| 0%) 2.3 K 0 READY 5 16457 6% (6%| 0%) 2.3 K 0 READY 6 16458 6% (5%| 0%) 2.2 K 1 READY 7 16459 4% (4%| 0%) 2.3 K 0 READY 8 16452 9% (8%| 1%) 2.2 K 0 READY **9 16455 100% (100%| 0%) 2.2 K 5 READY** <<<< High CPU utilization 10 16460 7% (6%| 0%) 2.2 K 0 READY -- ----- ---------- ---------- ---------- ---------- Summary 15% (14%| 0%) 24.6 K 7

-

Uso de Firepower Management Center (FMC)

Si está gestionando sus dispositivos FTD a través de FMC, puede obtener información detallada e informes sobre el tráfico y las instancias de

Snort a través de la interfaz web.

- Control

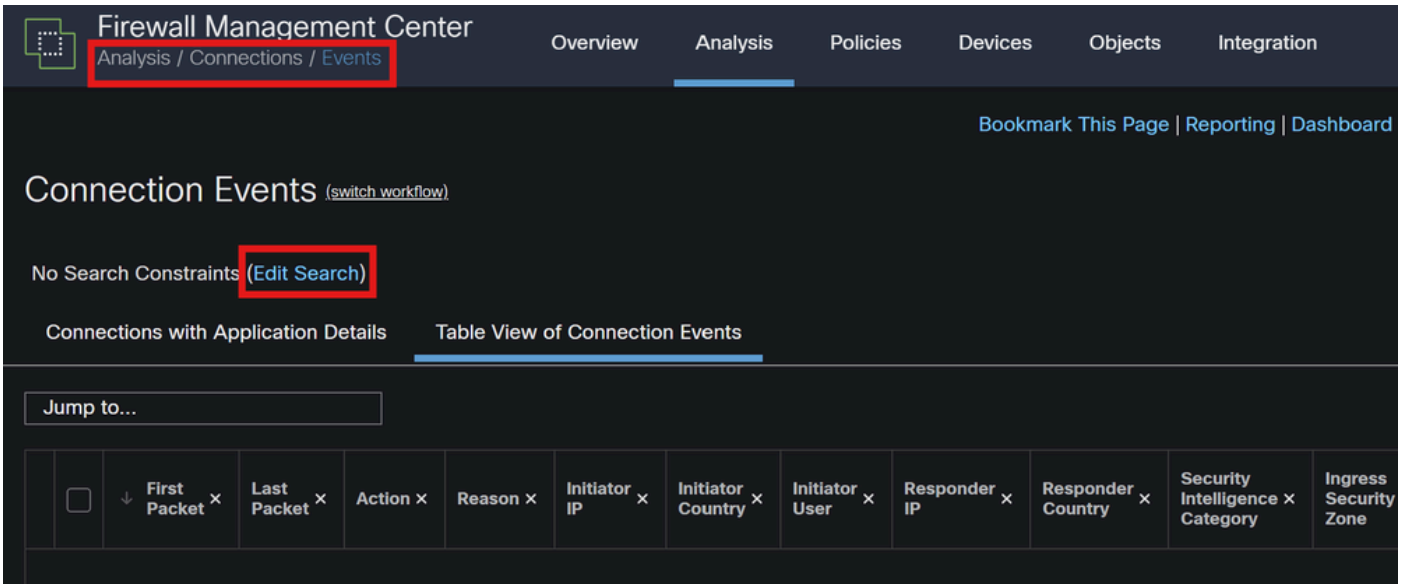
Panel de control de FMC: acceda al panel de control, donde podrá ver una descripción general del estado del sistema, incluidas las instancias de Snort.

Supervisión de estado: en la sección Supervisión de estado, puede obtener estadísticas detalladas sobre los procesos de Snort, incluido el tráfico gestionado.

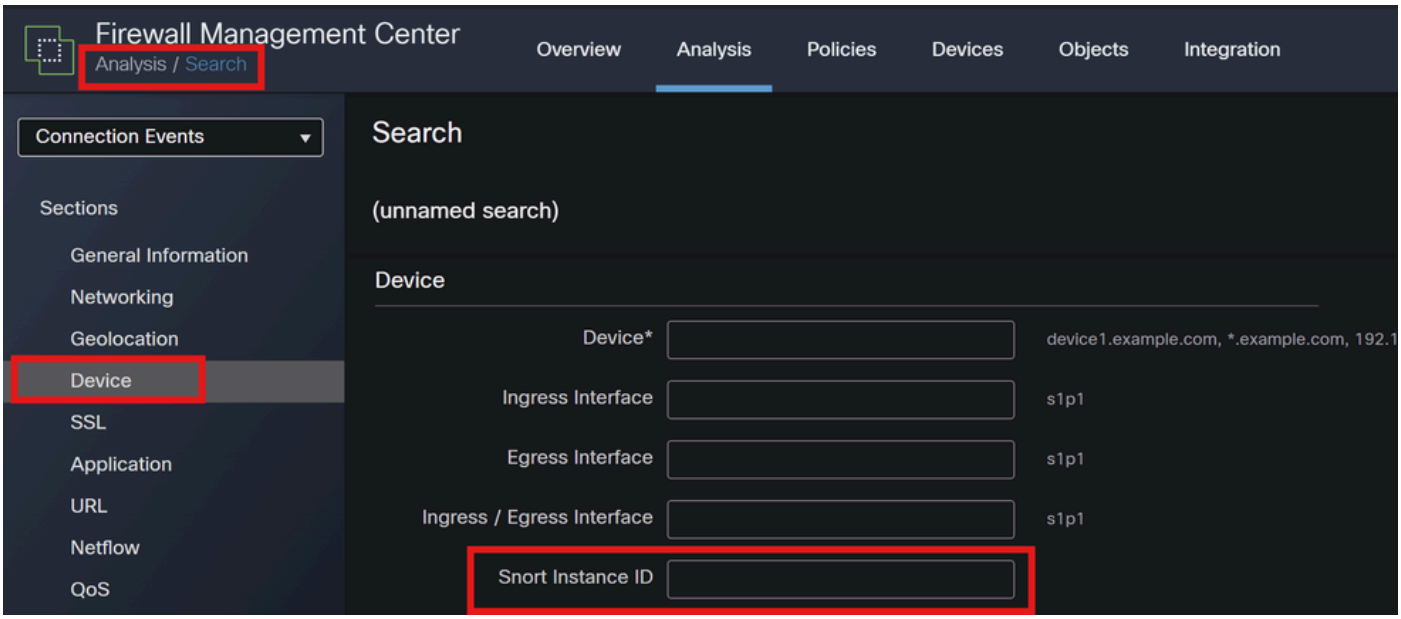
- Análisis

Análisis: Vaya a **Análisis > Eventos de Conexión**.

Filtros: utilice filtros para restringir los datos a la instancia o tráfico de Snort específico en el que esté interesado.



Eventos de conexión



ID de instancia de Snort

-

Uso de Syslog y SNMP

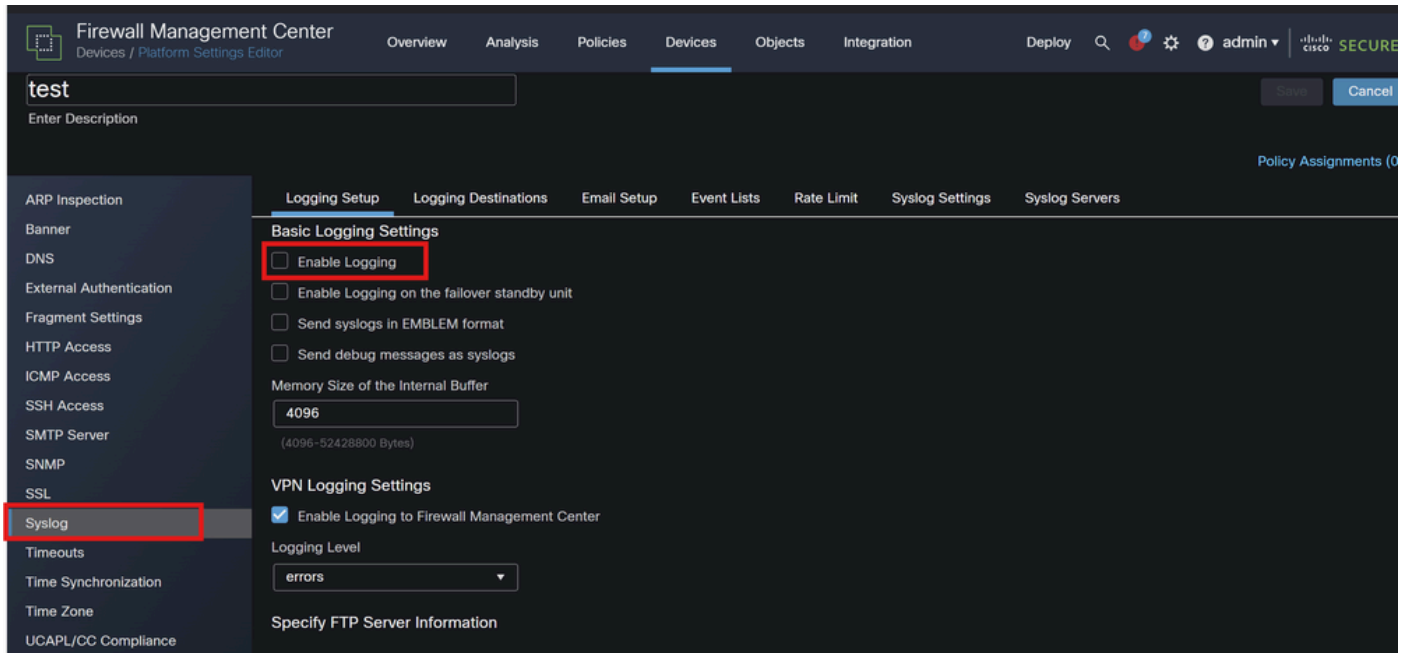
Puede configurar su FTD para enviar mensajes de syslog o trampas SNMP a un sistema de monitoreo externo donde puede analizar los datos de tráfico.

- Configuración de Syslog

Dispositivos: en FMC, vaya a **Dispositivos > Configuración de plataforma**.

Crear o editar una política: elija la política de configuración de plataforma adecuada.

Syslog: configure los parámetros de syslog para incluir alertas y estadísticas de Snort.

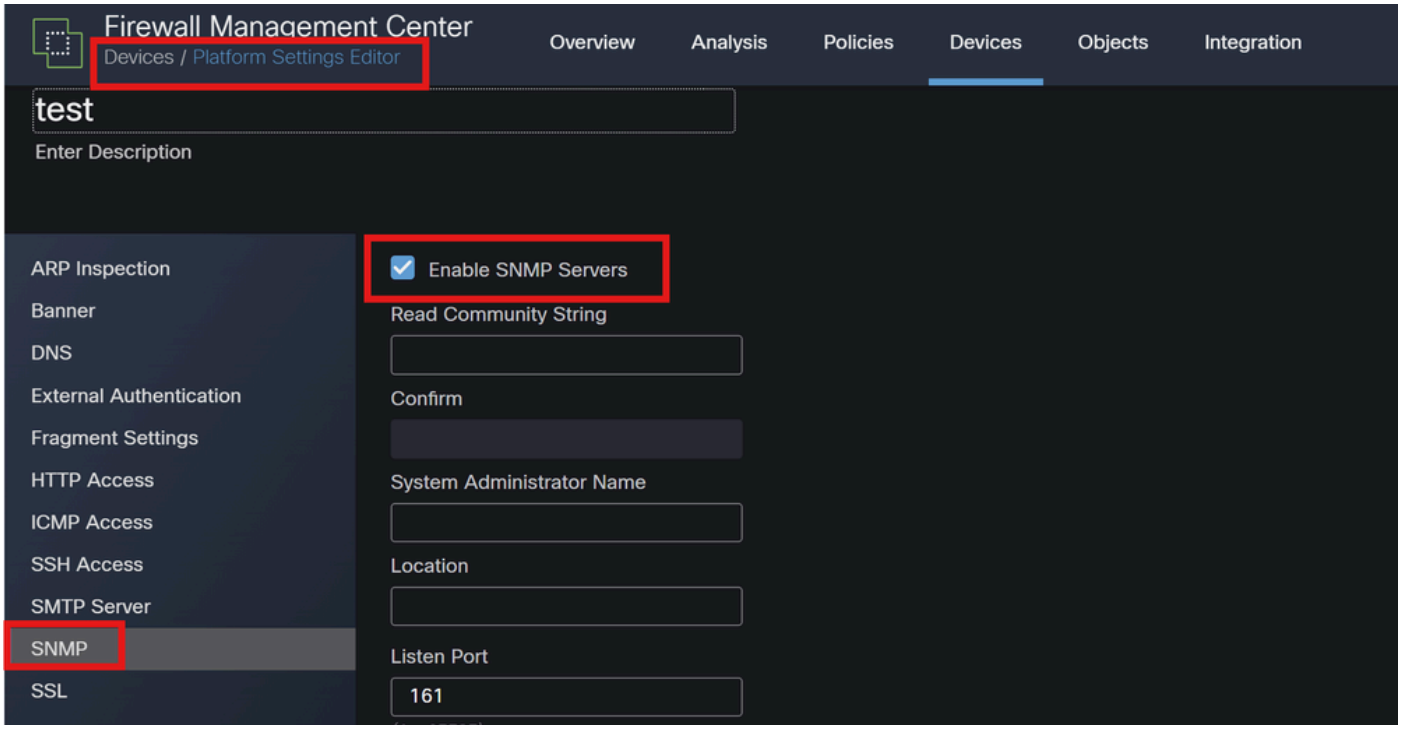


Configuración de Syslog

- Configuración de SNMP

Configuración de SNMP: de forma similar a syslog, configure los ajustes de SNMP en **Dispositivos > Configuración de la plataforma**.

Traps: asegúrese de que las trampas SNMP necesarias están habilitadas para las estadísticas de instancia de Snort.



Configuración de SNMP

4. Uso de las secuencias de comandos personalizadas

Para los usuarios avanzados, puede escribir scripts personalizados que utilicen la API REST de FTD para recopilar estadísticas sobre las instancias de Snort. Este enfoque requiere estar familiarizado con el uso de scripts y API.

- API REST

Acceso API: asegúrese de que el acceso API esté activado en el FMC.

Llamadas API: utilice las llamadas API adecuadas para obtener estadísticas de Snort y datos de tráfico.

Esto devuelve datos JSON que puede analizar y analizar para determinar el tráfico manejado por instancias específicas de Snort.

Al combinar estos métodos, puede obtener una comprensión completa del tráfico gestionado por cada instancia de Snort en su implementación de Cisco FTD.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).