

Determinar o tráfego tratado por uma instância específica do Snort

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Usando comandos CLI](#)

[Uso do Firepower Management Center \(FMC\)](#)

[Usando Syslog e SNMP](#)

Introdução

Este documento descreve como determinar o tráfego tratado por uma instância específica do Snort em um ambiente de Defesa contra ameaças (FTD) do Cisco Firepower.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento sobre estes produtos:

- Secure Firepower Management Center (FMC)
- Defesa contra ameaças (FTD) Secure Firepower
- Syslog e SNMP
- API REST

Componentes Utilizados

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos usados neste documento começaram com uma configuração limpa (padrão). Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

1. Usando comandos CLI

Usando a Interface de linha de comando (CLI) no dispositivo FTD, você pode acessar informações detalhadas sobre as instâncias do Snort e o tráfego que elas manipulam.

- Esse comando fornece os detalhes sobre a execução dos processos do Snort.

```
show snort instances
```

Aqui está um exemplo para a saída do comando.

```
> show snort instances
```

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

- Para obter informações mais detalhadas sobre as estatísticas de tráfego tratadas pelas instâncias do Snort, esses comandos podem ser usados. Isso exibe várias estatísticas, incluindo o número de pacotes processados, descartados e os alertas gerados por cada instância do Snort.

```
show snort statistics
```

Aqui está um exemplo para a saída do 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
```

Aqui está um exemplo para a saída do 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 do Firepower Management Center (FMC)

Se você estiver gerenciando seus dispositivos FTD através do FMC, você poderá obter informações e relatórios detalhados sobre o tráfego e as

instâncias do Snort através da interface da Web.

- Monitoramento

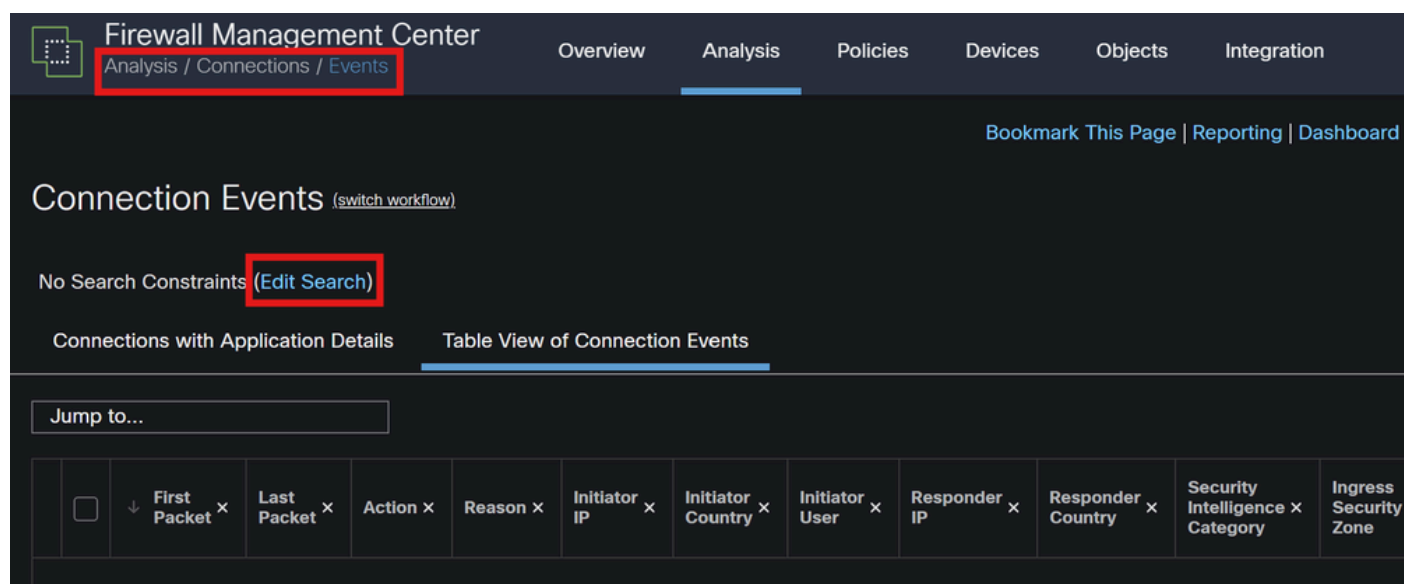
Painel do FMC: navegue até o painel onde você pode ver uma visão geral do status do sistema, incluindo instâncias do Snort.

Monitoramento de integridade: na seção de monitoramento de integridade, você pode obter estatísticas detalhadas sobre processos do Snort, incluindo o tráfego manipulado.

- Análise

Análise: Navegue até **Análise > Eventos de Conexão**.

Filtros: use filtros para restringir os dados à ocorrência ou ao tráfego específico do Snort no qual você está interessado.



Firewall Management Center

Analysis / Connections / Events

Overview Analysis Policies Devices Objects Integration

Bookmark This Page | Reporting | Dashboard

Connection Events (switch workflow)

No Search Constraints **Edit Search**

Connections with Application Details **Table View of Connection Events**

Jump to...

<input type="checkbox"/>	↓ First Packet ×	Last Packet ×	Action ×	Reason ×	Initiator IP ×	Initiator Country ×	Initiator User ×	Responder IP ×	Responder Country ×	Security Intelligence × Category	Ingress Security Zone
--------------------------	------------------	---------------	----------	----------	----------------	---------------------	------------------	----------------	---------------------	----------------------------------	-----------------------

Eventos de conexão

The screenshot shows the Firewall Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'Analysis / Search' tab is active. On the left, a sidebar lists sections: 'Connection Events', 'General Information', 'Networking', 'Geolocation', 'Device' (highlighted with a red box), 'SSL', 'Application', 'URL', 'Netflow', and 'QoS'. The main area is titled 'Search (unnamed search)' and contains a 'Device' section with several input fields: 'Device*' (with a dropdown menu), 'Ingress Interface', 'Egress Interface', 'Ingress / Egress Interface', and 'Snort Instance ID' (highlighted with a red box). The 'Device*' field shows a dropdown menu with the selected item 'device1.example.com, *.example.com, 192.1'.

ID da instância do Snort

-

Usando Syslog e SNMP

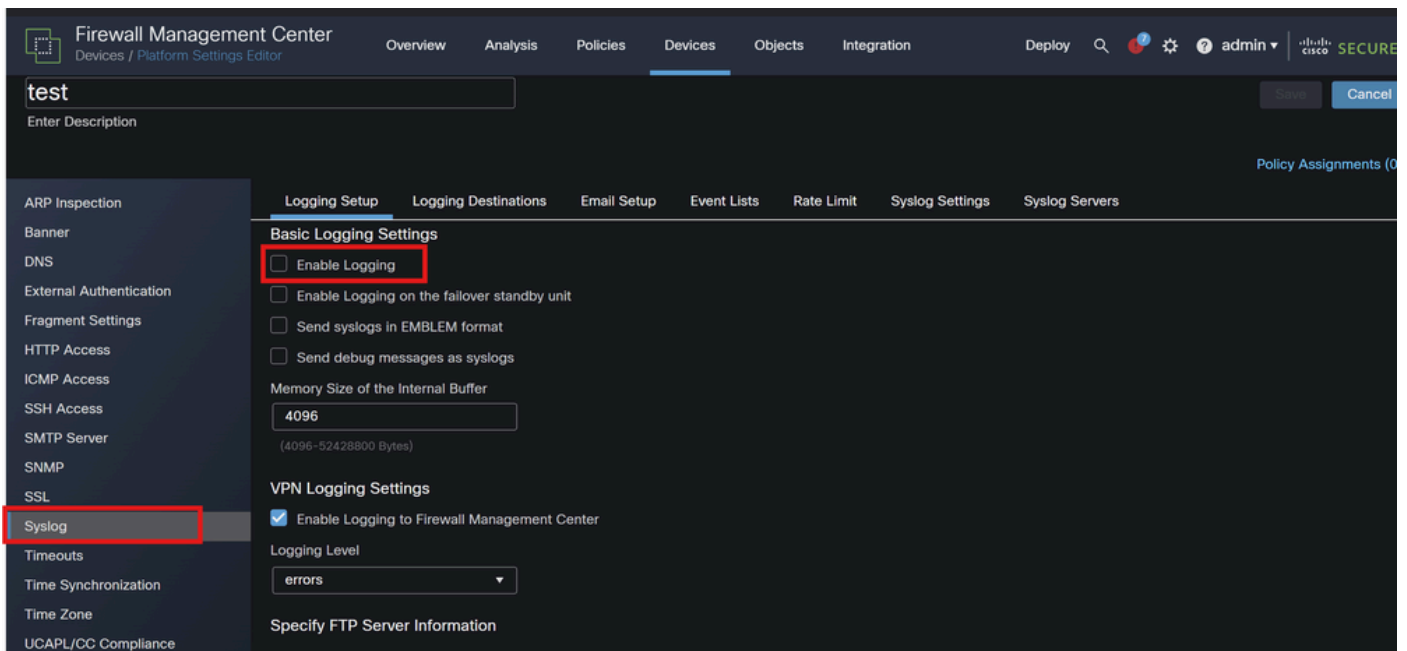
Você pode configurar o FTD para enviar mensagens de syslog ou interceptações SNMP (traps) para um sistema de monitoramento externo, onde é possível analisar os dados de tráfego.

- Configuração de Syslog

Dispositivos: no FMC, navegue até **Dispositivos > Configurações da plataforma**.

Criar ou Editar uma Política: Escolha a política de definições de plataforma apropriada.

Syslog: defina as configurações de syslog para incluir estatísticas e alertas do Snort.

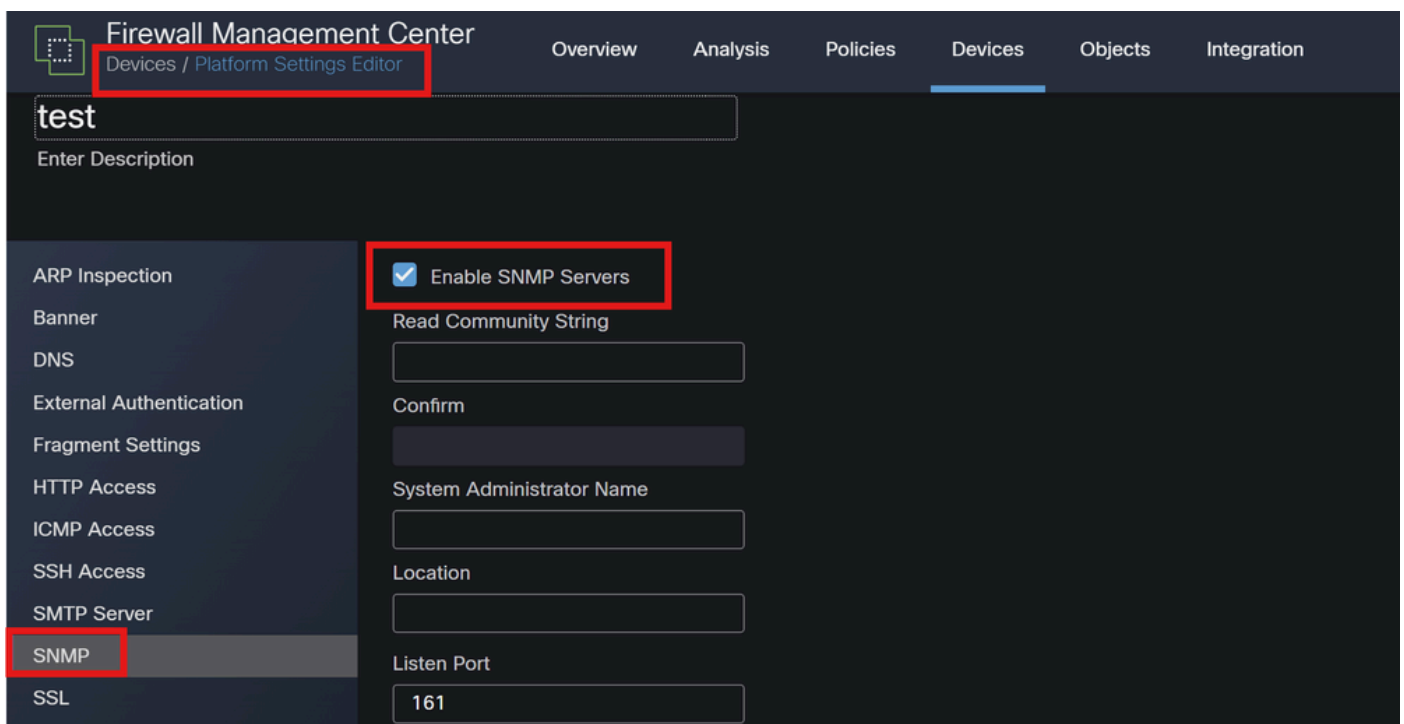


Configuração de Syslog

- Configuração de SNMP

Configurações SNMP: semelhantes ao syslog, defina as configurações SNMP em **Devices > Platform Settings**.

Traps: certifique-se de que os traps SNMP necessários estejam ativados para estatísticas de instância do Snort.



Configuração de SNMP

4. Usando os Scripts Personalizados

Para usuários avançados, você pode criar scripts personalizados que usam a API REST FTD para coletar estatísticas sobre instâncias do Snort. Essa abordagem requer familiaridade com o uso de scripts e API.

- API REST

Acesso à API: verifique se o acesso à API está habilitado no FMC.

Chamadas de API: use as chamadas de API apropriadas para buscar estatísticas de Snort e dados de tráfego.

Isso retorna dados JSON que você pode analisar e analisar para determinar o tráfego tratado por instâncias específicas do Snort.

Combinando esses métodos, você pode obter uma compreensão abrangente do tráfego tratado por cada instância do Snort em sua implantação do Cisco FTD.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.