

Configurar o NetFlow no FMC

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Adicionar coletor no NetFlow](#)

[Adicionar classe de tráfego ao NetFlow](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar o Netflow no Cisco Secure Firewall Management Center executando a versão 7.4 ou superior.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Secure Firewall Management Center (FMC)
- Defesa contra ameaças (FTD) do Cisco Secure Firewall
- Protocolo NetFlow

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- O Secure Firewall Management Center para VMWare é executado na v7.4.1
- Firewall seguro executa v7.4.1

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

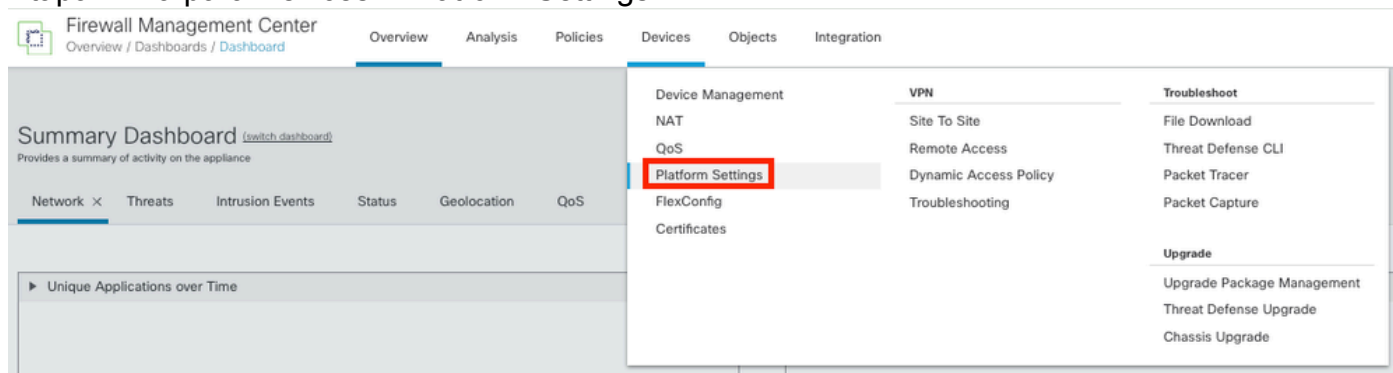
Informações de Apoio

Os requisitos específicos deste documento incluem:

- Cisco Secure Firewall Threat Defense executando a versão 7.4 ou posterior
- Cisco Secure Firewall Management Center executando a versão 7.4 ou posterior

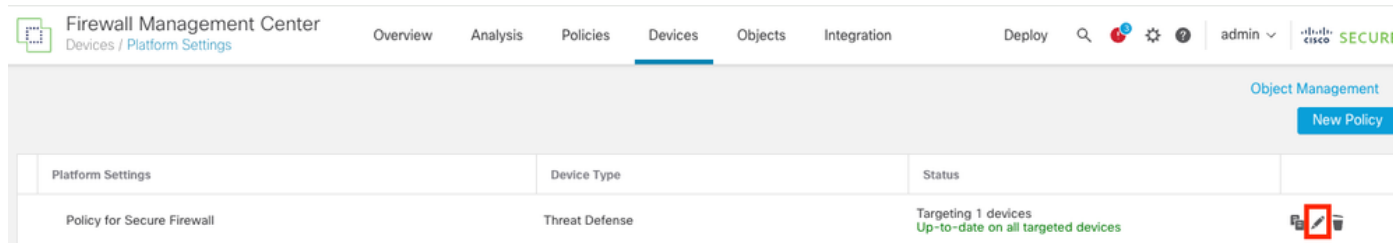
Adicionar coletor no NetFlow

Etapa 1. Vá para Devices > Platform Settings:



Acessando configurações da plataforma

Etapa 2. Edite a Política de Configurações de Plataforma atribuída ao Dispositivo de Monitoramento:



Edição de Política

Etapa 3. Escolha Netflow:



Policy for Secure Firewall

Enter Description

ARP Inspection

Banner

DNS

External Authentication

Fragment Settings

HTTP Access

ICMP Access

NetFlow

SSH Access

SMTP Server

SNMP

SSL

Syslog

Timeouts

Time Synchronization

Time Zone

UCAPL/CC Compliance

Performance Profile

Interface

Inspect Enabled

Acessando as configurações do NetFlow

Etapa 4. Ative a opção Exportação de fluxo para ativar a exportação de dados do NetFlow:

Policy for Secure Firewall

Enter Description

ARP Inspection

Banner

DNS

External Authentication

Fragment Settings

HTTP Access

ICMP Access

NetFlow

SSH Access

SMTP Server

SNMP

SSL

Syslog

Timeouts

Time Synchronization

Time Zone

UCAPL/CC Compliance

Performance Profile

Enable Flow Export

Active Refresh Interval (1-60)

minutes

Delay Flow Create (1-180)

seconds

Template Timeout Rate (1-3600)

minutes

Collector

Traffic Class

Ativando o NetFlow

Etapa 5. Clique em Add Collector:

Policy Assignments (1)

Add Collector

Add Traffic Class

Adicionando coletor

Etapa 6. Escolha o objeto IP do host do coletor de eventos do NetFlow, a porta UDP no coletor para o qual os pacotes do NetFlow devem ser enviados, escolha o grupo de interface através do qual o coletor deve ser alcançado e clique em OK:

Add Collector

Host
Netflow_Collector

Port (1-65535)
2055

Available Interface Groups (1) +

Netflow_Export

Add

Selected Interface Groups (0)

Select at least one interface group.

Cancel OK

Configurações do coletor

Adicionar classe de tráfego ao NetFlow

Etapa 1. Clique em Add Traffic Class:

Enable Flow Export

Active Refresh Interval (1-60)
1 minutes

Delay Flow Create (1-180)
seconds

Template Timeout Rate (1-3600)
30 minutes

| Host | Interface Groups | Port | |
|-------------------|------------------|------|---|
| Netflow_Collector | Netflow_Export | 2055 | <input type="text"/> <input type="text"/> |

Traffic Class

No traffic class records.

Add Traffic Class

Adicionando classe de tráfego

Etapa 2. Insira o campo de nome da classe de tráfego que deve corresponder aos eventos do NetFlow, a ACL para especificar a classe de tráfego que deve corresponder ao tráfego capturado para os eventos do NetFlow, marque as caixas de seleção para os diferentes eventos do NetFlow

que você deseja enviar para os coletores e clique em OK:

Add Traffic Class ?

Name
Netflow_class

Type
 Access List Default

Access List Object
Netflow_ACL

Event Types

| Collector | All | Created | Denied | Updated | Torn Down |
|-------------------|-------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| Netflow_Collector | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Configurações de classe de tráfego

Troubleshooting

Etapa 1. Você pode verificar a configuração na CLI do FTD.

1.1. A partir do FTD CLI, digite para suporte do sistema diagnostic-cli:

```
>system support diagnostic-cli
```

1.2 Verifique a configuração do mapa de políticas:

```
<#root>
```

```
firepower#show running-config policy-map  
!  
policy-map type inspect dns preset_dns_map  
parameters  
message-length maximum client auto  
message-length maximum 512  
no tcp-inspection
```

```
policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP
parameters
eool action allow
nop action allow
router-alert action allow
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect rtsp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect sip
inspect netbios
inspect tftp
inspect icmp
inspect icmp error
inspect ip-options UM_STATIC_IP_OPTIONS_MAP
class class_snmp
inspect snmp

class Netflow_class_Netflow_ACL
```

```
flow-export event-type all destination 192.168.31.1
```

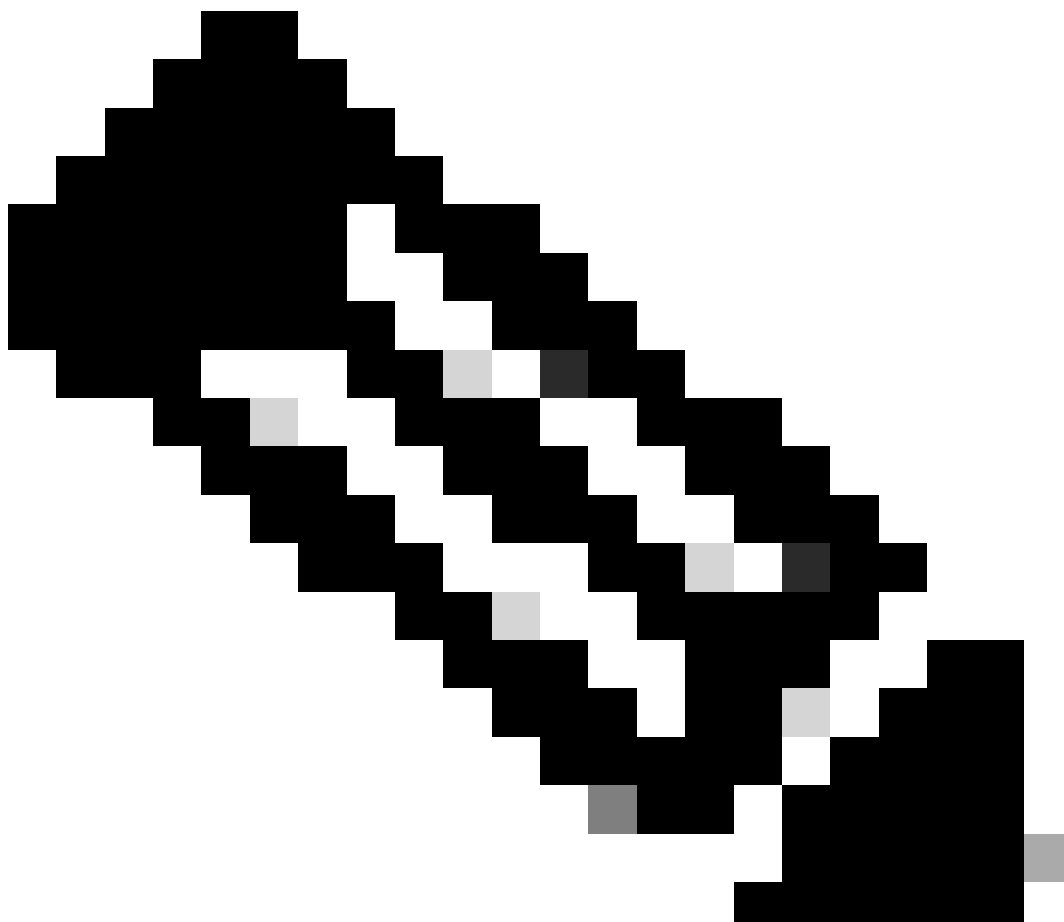
```
class class-default
set connection advanced-options UM_STATIC_TCP_MAP
!
```

1.3. Verifique a configuração de exportação de fluxo:

```
<#root>
```

```
firepower#show running-config flow-export
```

```
flow-export destination Inside 192.168.31.1 2055
```



Observação: neste exemplo, "Inside" é o nome da interface configurada no grupo de interface chamado Netflow_Export

Etapa 2. Verifique a contagem de ocorrências da ACL:

```
<#root>
```

```
firepower#show access-list Netflow_ACL
access-list Netflow_ACL; 1 elements; name hash: 0xbad5d4bf
access-list Netflow_ACL line 1 extended permit ip object Inside_Network any (
hitcnt=44
) 0xb704fc5b
access-list Netflow_ACL line 1 extended permit ip 10.1.2.0 255.255.255.0 any (
hitcnt=44
) 0xb704fc5b
```


Etapa 3. Verifique os contadores do Netflow:

```
<#root>
```

```
firepower#show flow-export counters
```

```
destination: Inside 192.168.31.1 2055
```

```
Statistics:
```

```
packets sent 101
```

```
Errors:
```

```
block allocation failure 0
```

```
invalid interface 0
```

```
template send failure 0
```

```
no route to collector 0
```

```
failed to get lock on block 0
```

```
source port allocation failure 0
```

Informações Relacionadas

- [Guia de configuração de dispositivos do Cisco Secure Firewall Management Center, 7.4](#)

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.