Configurar o vSphere para enviar o tráfego leste/oeste para o FlowSensor

Contents

Introdução

Este documento descreve como configurar o vSphere para que o tráfego leste/oeste possa ser enviado ao sensor de fluxo de análise de rede segura

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- VMware vSphere
- Análise de rede segura (SNA)

Componentes Utilizados

VMware vSphere versão 7.0.3

Secure Network Analytics versão 7.4.2.

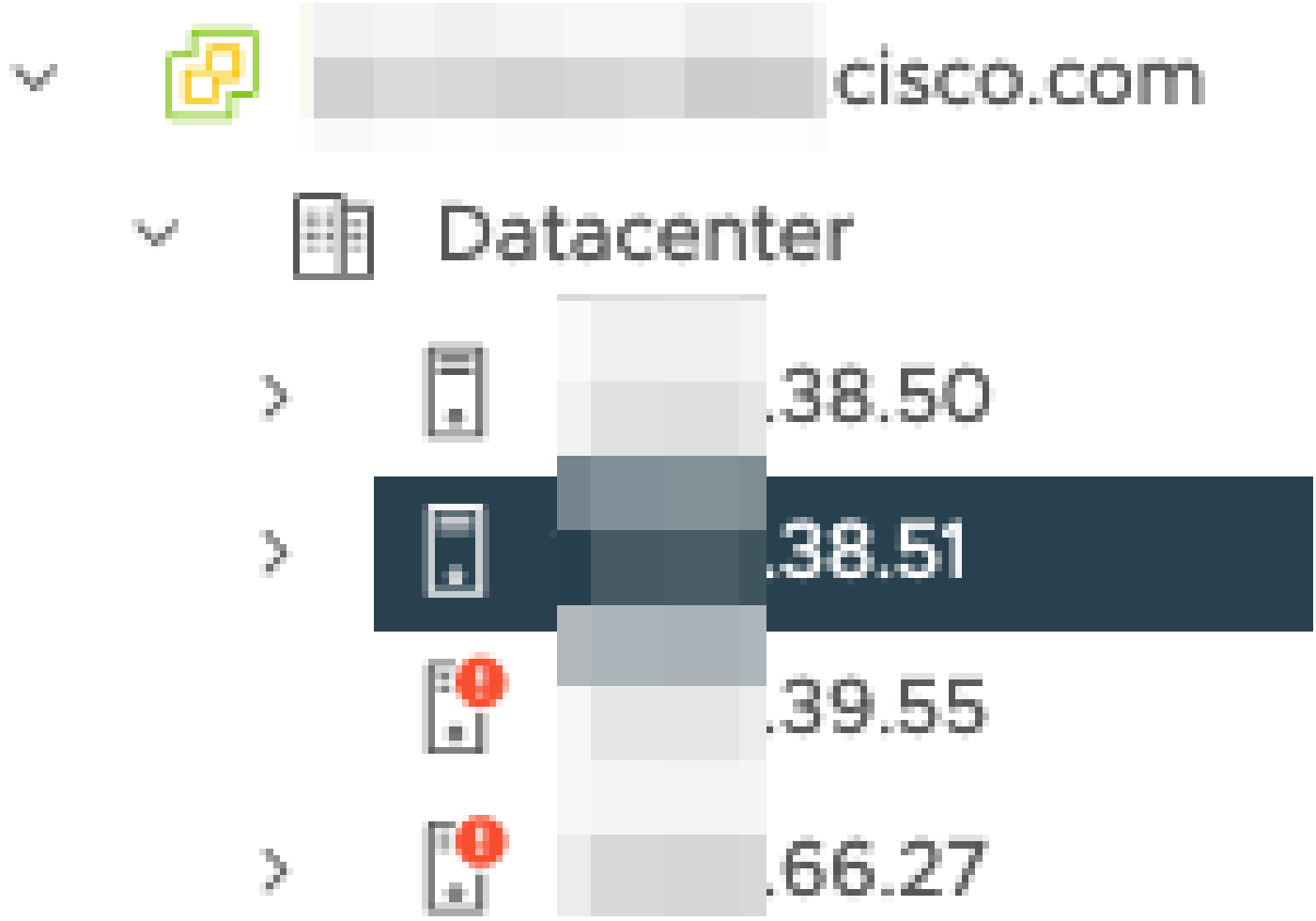
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer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

Configurar

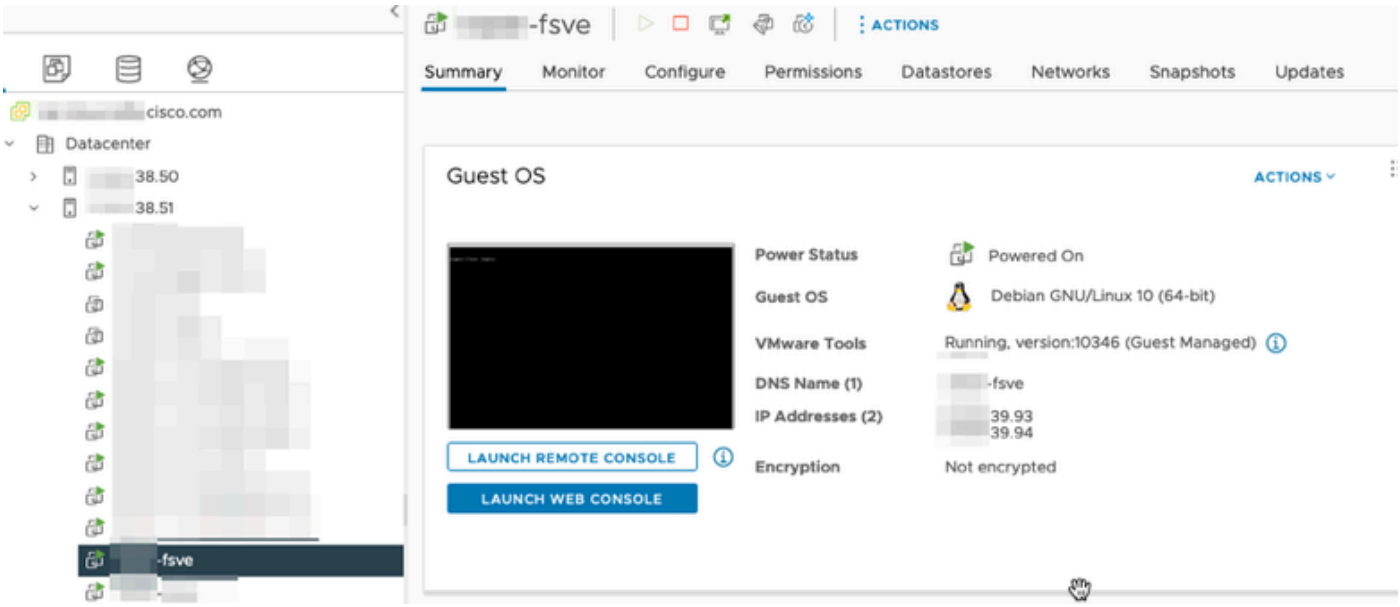
No vSphere, analise o data center quanto ao número de hosts ESXi e determine de quais hosts você deseja coletar o tráfego leste/oeste.

Nessa imagem, dos quatro hosts, apenas dois são discutidos cujos últimos dois octetos são 38.51 e 66.27.

O host ESXi 38.51 executa a versão 7.0.3 e o host ESXi 66.27 executa a versão 6.7.0.



Um SNA Flow Sensor versão 7.4.2 foi implantado no host ESXi 38.51; ele foi configurado com dois endereços IP com os últimos octetos 39.93 e 39.94.



Há dois outros dispositivos, um Gerenciador SNA e um Nó de Dados chamados Gerenciador e DN1, respectivamente.

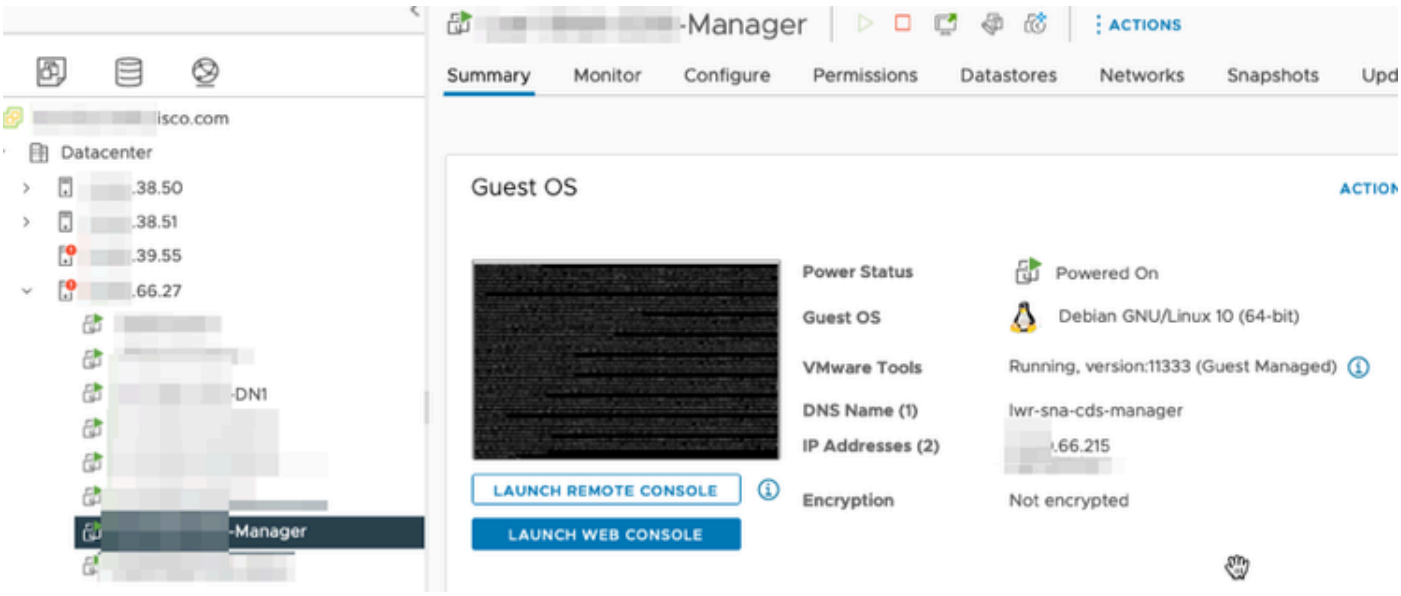
Os dois últimos octetos desses dois hosts são 66.215 e 66.217 para o Gerenciador e DN1,

respectivamente.

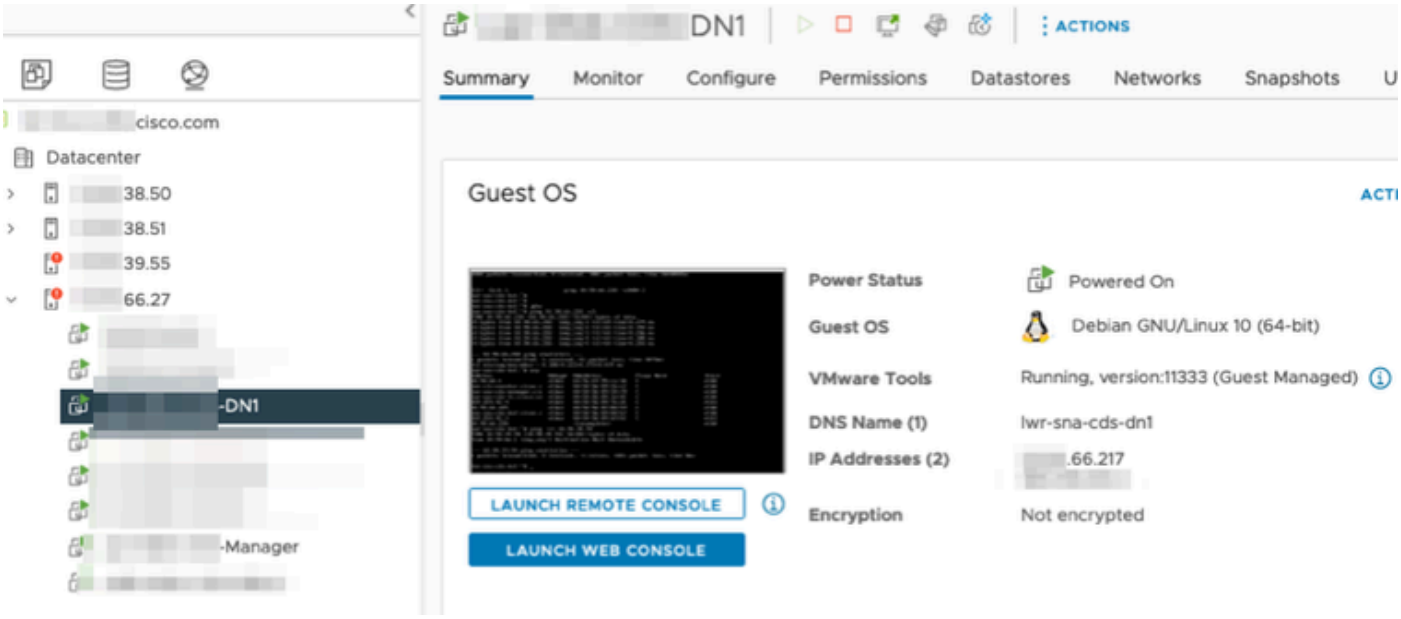
Esses dois hosts são implantados no host ESXi, cujos dois últimos octetos são 66.27. Esse é um ESXi diferente daquele no qual o Flow Sensor é implantado.

O tráfego entre o gerenciador e o host DN1 não é visto fora do switch proxy no host ESXi 66.27.

O Gerenciador SNA:

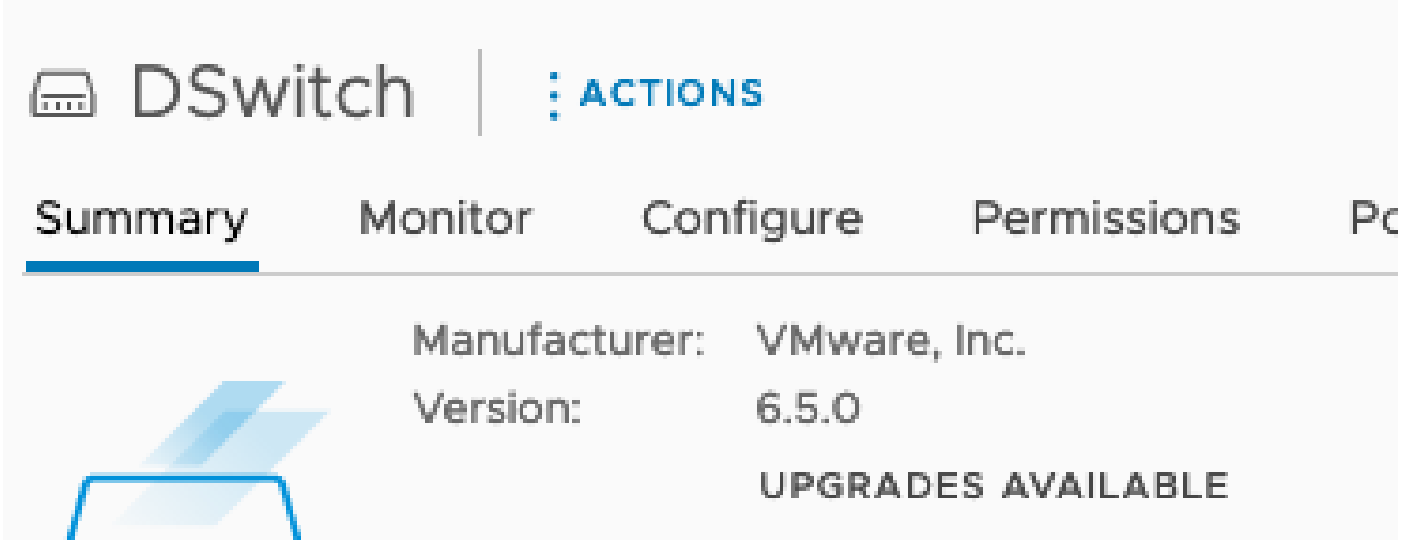


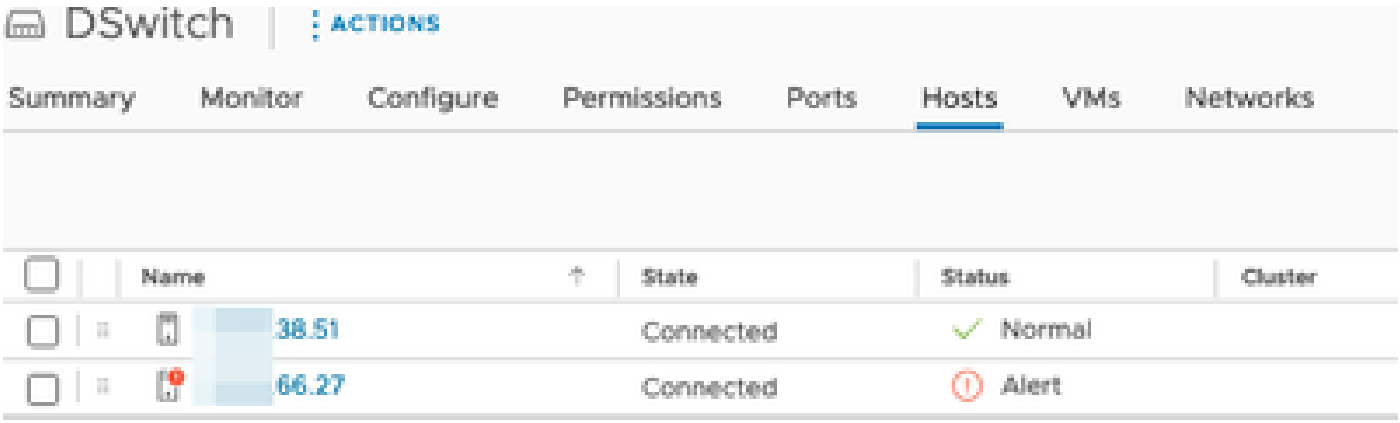
O DN1 SNA:



Configurações

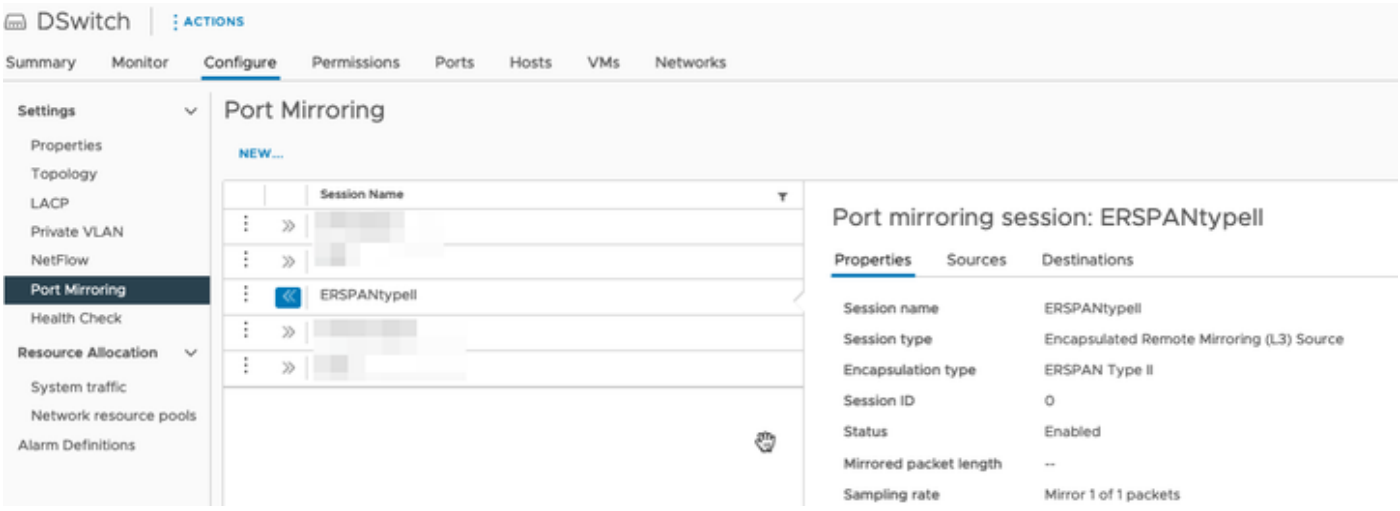
Crie um switch distribuído versão 6.5.0 chamado DSwitch e um grupo de portas distribuído chamado DPortGroup.



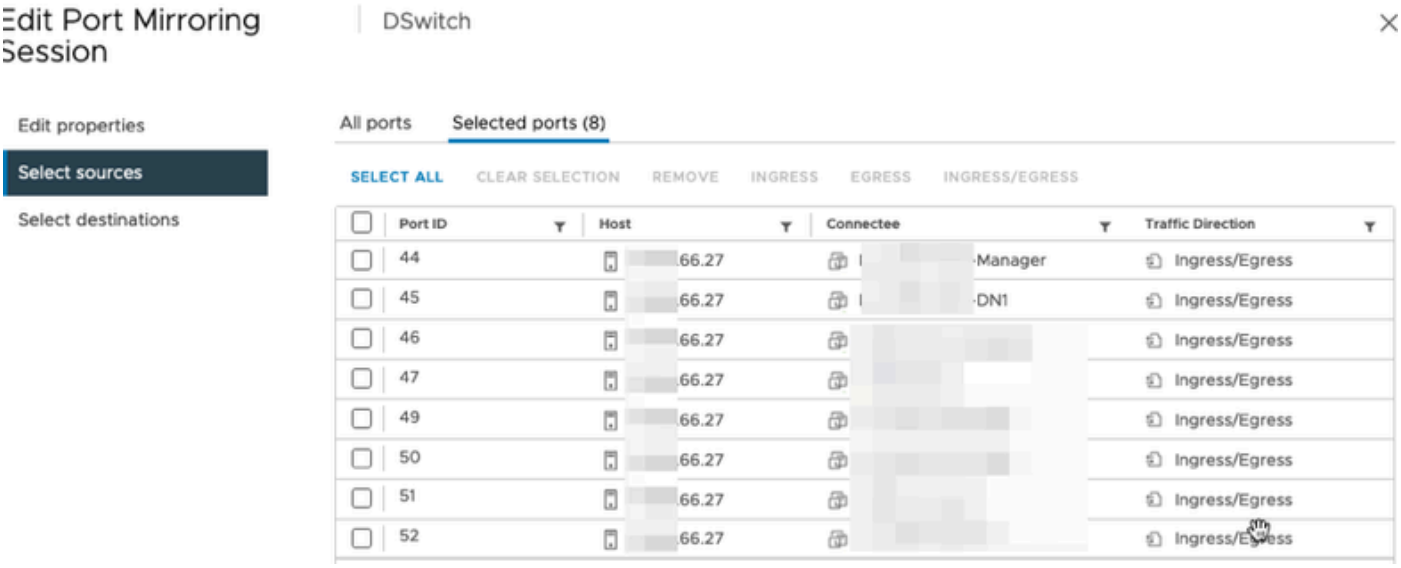


As máquinas virtuais e os dois uplinks para os hosts ESXi foram adicionados ao grupo de portas distribuídas no DSwitch.

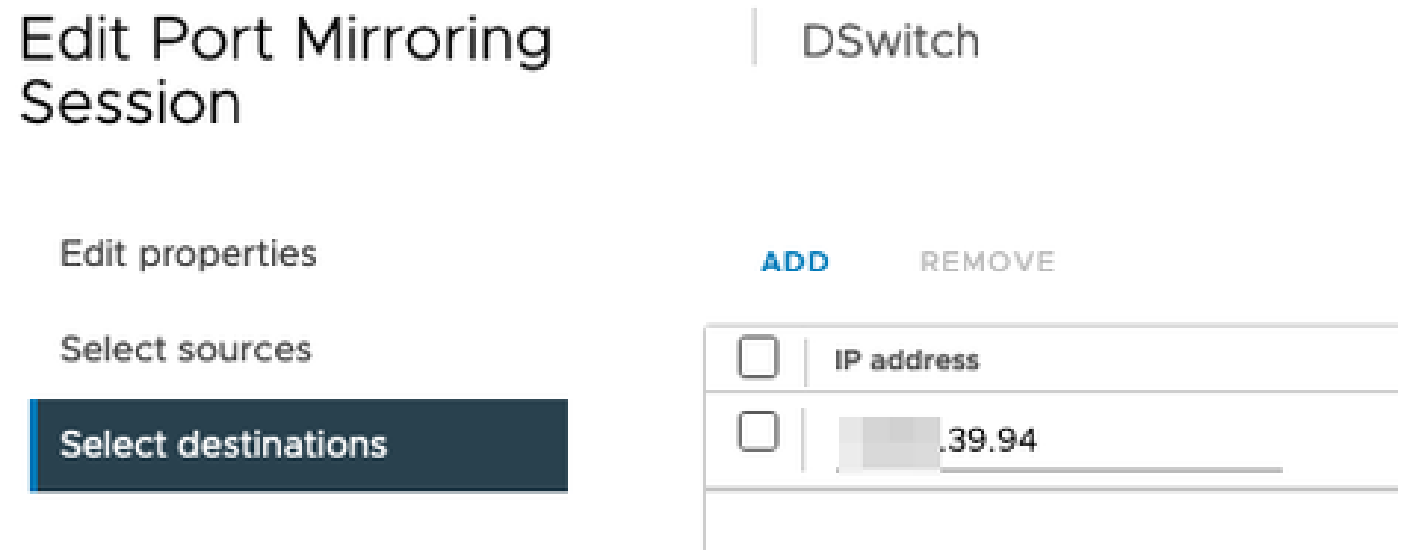
No DSwitch, configure uma sessão de espelhamento ERSPAN Tipo II.



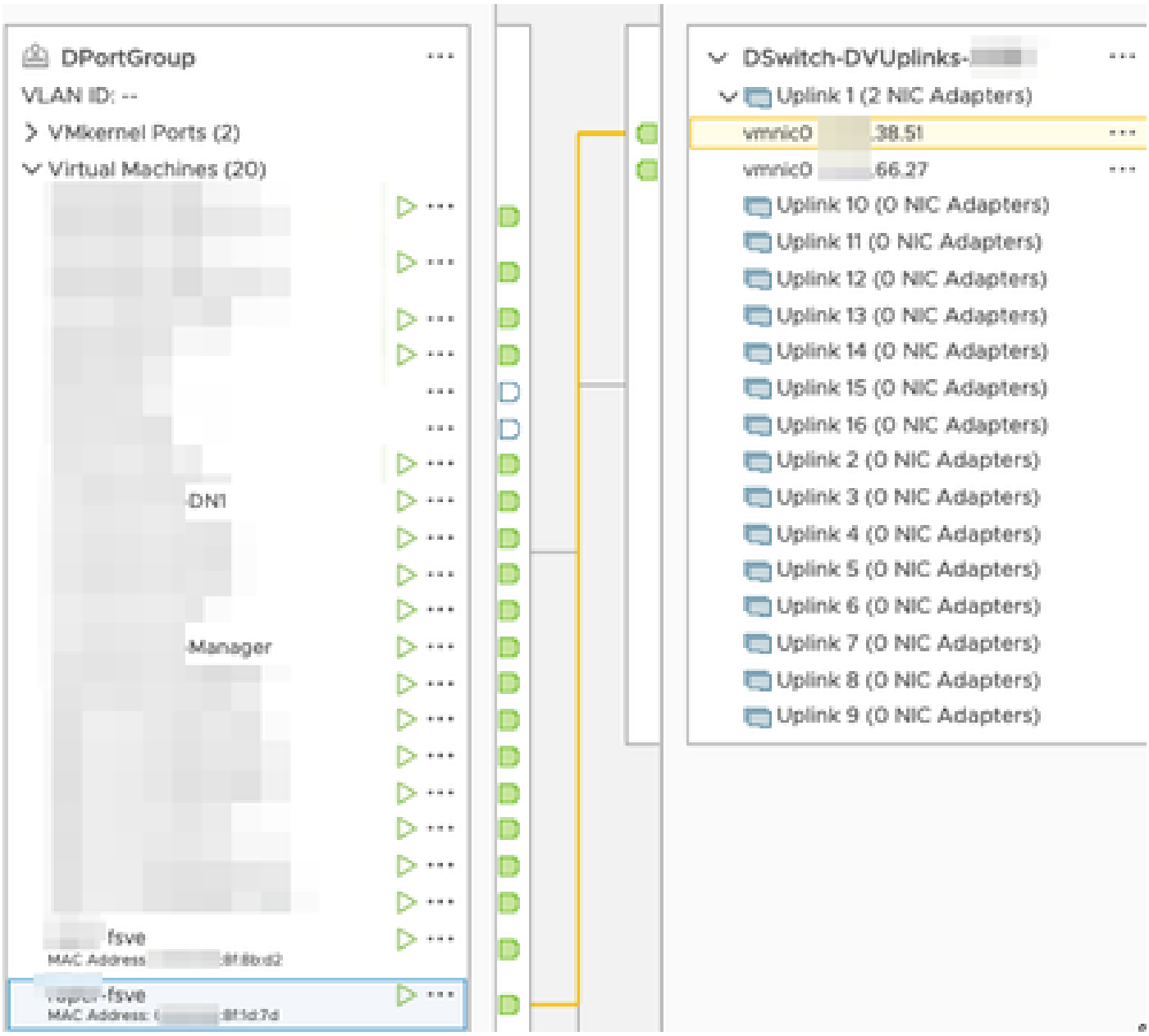
Para a sessão de espelhamento de porta, todos os hosts nos hosts ESXi 66.27 (incluindo o Gerenciador e o DN1) foram selecionados.



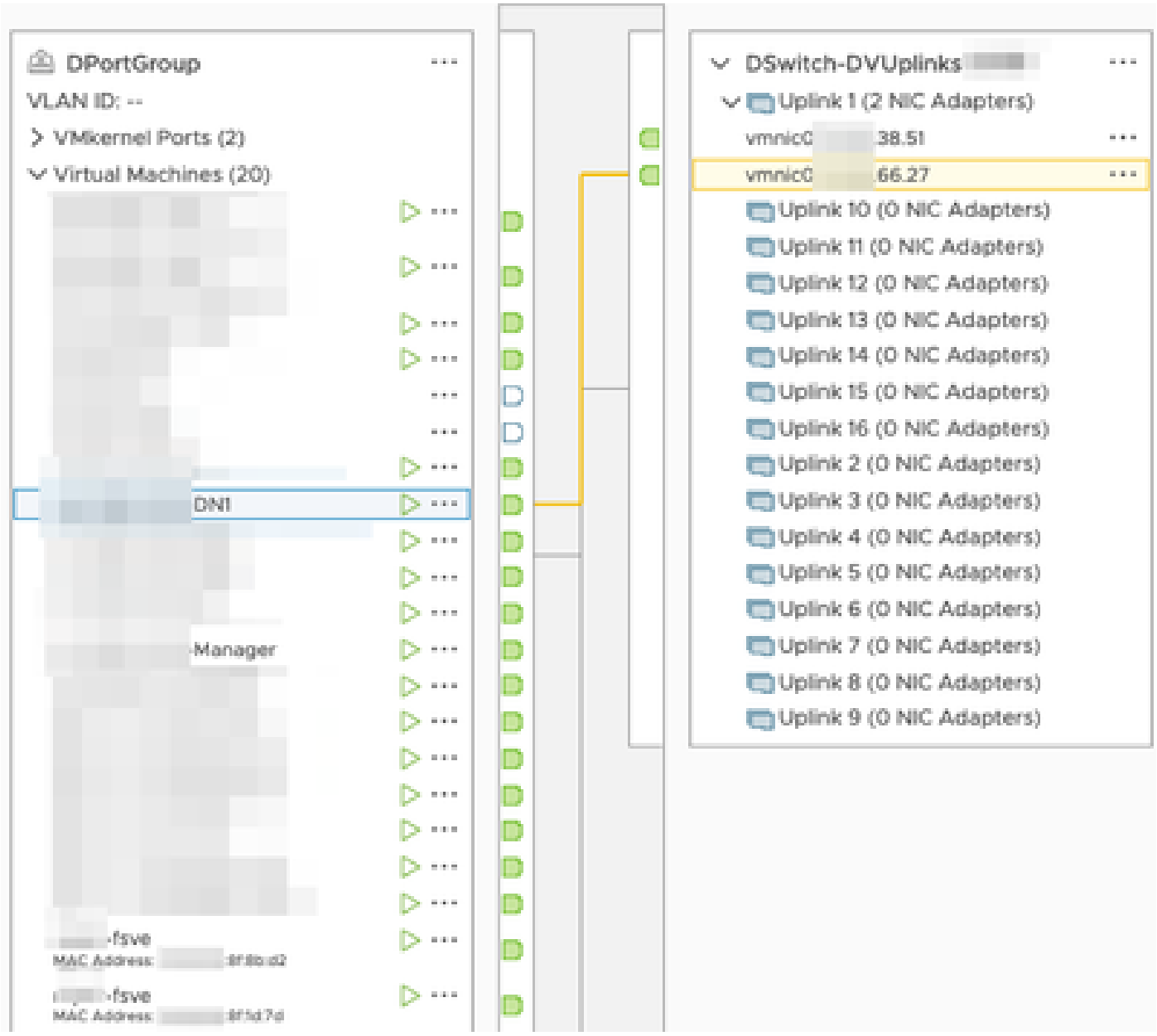
Para o destino, defina-o como o IP da interface eth1 no Flow Sensor, 39.94.

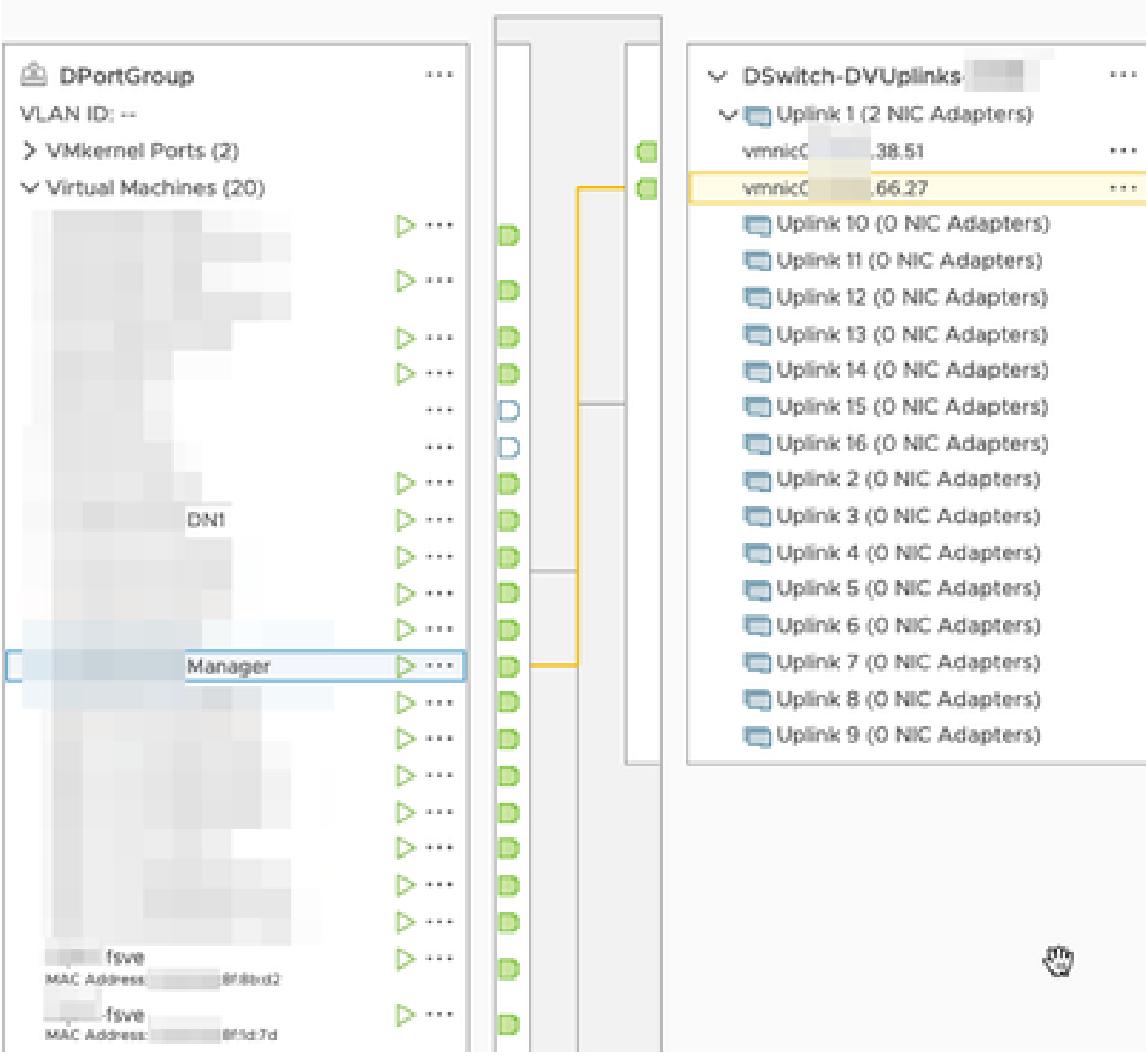


As interfaces eth0 e eth1 do Flow Sensor são exibidas no DPortGroup associado a 38.51.


DPortGroup
VLAN ID: --
VMkernel Ports (2)
Virtual Machines (20)
DN1
Manager
fsve
MAC Address
-fsve
MAC Address:
DSwitch-DVUplinks-
Uplink 1 (2 NIC Adapters)
vmnic0 38.51
vmnic0 66.27
Uplink 10 (0 NIC Adapters)
Uplink 11 (0 NIC Adapters)
Uplink 12 (0 NIC Adapters)
Uplink 13 (0 NIC Adapters)
Uplink 14 (0 NIC Adapters)
Uplink 15 (0 NIC Adapters)
Uplink 16 (0 NIC Adapters)
Uplink 2 (0 NIC Adapters)
Uplink 3 (0 NIC Adapters)
Uplink 4 (0 NIC Adapters)
Uplink 5 (0 NIC Adapters)
Uplink 6 (0 NIC Adapters)
Uplink 7 (0 NIC Adapters)
Uplink 8 (0 NIC Adapters)
Uplink 9 (0 NIC Adapters)

As interfaces eth0 do Manager e DN1 são mostradas no DPortGroup associado a 66.27.


DPortGroup
VLAN ID: --
VMkernel Ports (2)
Virtual Machines (20)
DN1
Manager
-fsve
MAC Address:
-fsve
MAC Address:
DSwitch-DVUplinks
Uplink 1 (2 NIC Adapters)
vmnic0 38.51
vmnic0 66.27
Uplink 10 (0 NIC Adapters)
Uplink 11 (0 NIC Adapters)
Uplink 12 (0 NIC Adapters)
Uplink 13 (0 NIC Adapters)
Uplink 14 (0 NIC Adapters)
Uplink 15 (0 NIC Adapters)
Uplink 16 (0 NIC Adapters)
Uplink 2 (0 NIC Adapters)
Uplink 3 (0 NIC Adapters)
Uplink 4 (0 NIC Adapters)
Uplink 5 (0 NIC Adapters)
Uplink 6 (0 NIC Adapters)
Uplink 7 (0 NIC Adapters)
Uplink 8 (0 NIC Adapters)
Uplink 9 (0 NIC Adapters)



Verificar

A partir do CLI do Flow Sensor, um tcpdump é executado para mostrar que o túnel GRE é ativado na interface eth1.

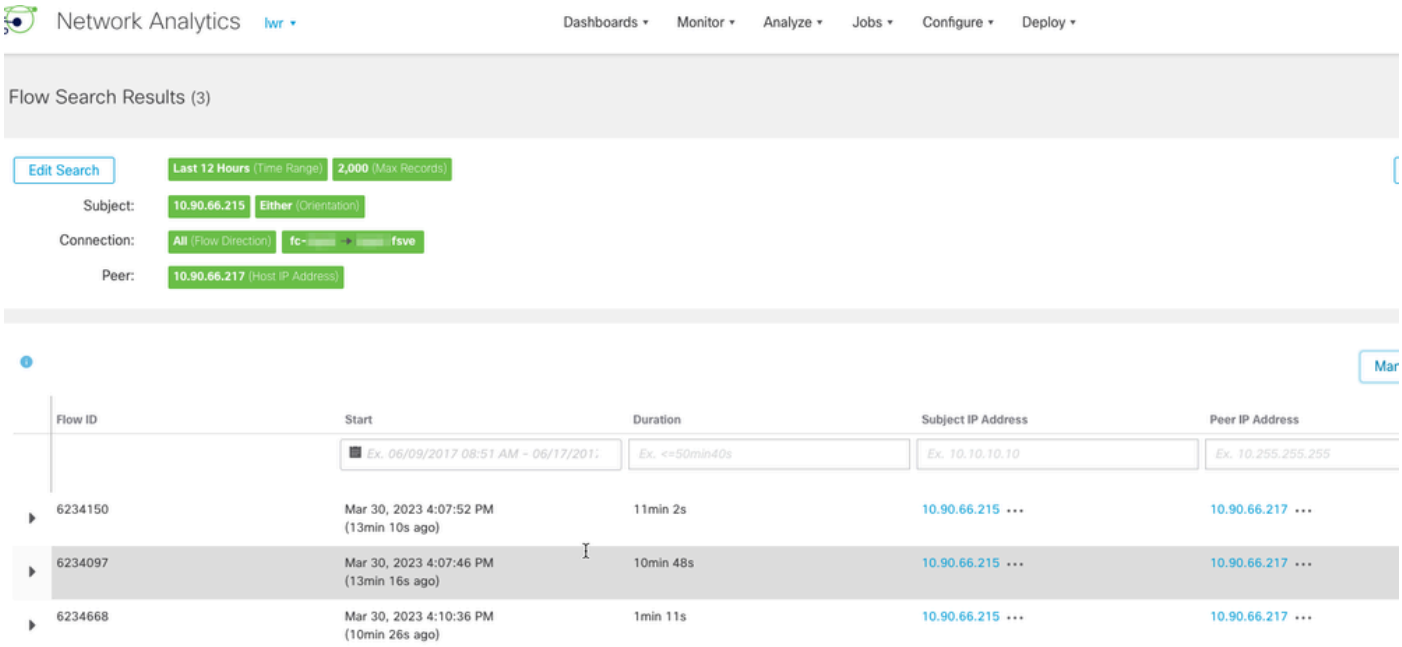
```
fsve:~# tcpdump -epnni eth1 not broadcast and not multicast -c10
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
17:43:57.080043                 > 8f:1d:7d, ethertype ARP (0x0806), length 60: Request who-has  39.94  8f:1d:7d) tell 0.0.0.0, length 46
17:43:57.080066                 > 48:16:21, ethertype ARP (0x0806), length 42: Reply  39.94 is-at  8f:1d:7d, length 28
17:44:06.728457                 > 8f:1d:7d, ethertype IPv4 (0x0800), length 102:  .66.27 >  .39.94: GREv0, key=0x2000000, proto TEB (0x6558),

17:44:06.728474       95:ca:4e > 8f:1d:7d, ethertype IPv4 (0x0800), length 102:  66.27 >  .39.94: GREv0, key=0x2000000, proto TEB (0x6558),

17:44:06.728475       95:ca:4e > 8f:1d:7d, ethertype IPv4 (0x0800), length 102:  .66.27 >  .39.94: GREv0, key=0x0, proto TEB (0x6558), length

17:44:06.728477       95:ca:4e > 8f:1d:7d, ethertype IPv4 (0x0800), length 102:  .66.27 >  .39.94: GREv0, key=0x0, proto TEB (0x6558), length
```

Uma pesquisa de fluxo para os dispositivos do Gerenciador e DN1 é executada no Gerenciador SNA que recebe o netflow do Sensor de fluxo mostra o tráfego entre o Gerenciador e o host DN1.


Network Analytics
lwr
Dashboards
Monitor
Analyze
Jobs
Configure
Deploy
Flow Search Results (3)
Edit Search
Last 12 Hours (Time Range)
2,000 (Max Records)
Subject:
10.90.66.215
Either (Orientation)
Connection:
All (Flow Direction)
fc-
fsve
Peer:
10.90.66.217 (Host IP Address)
Mar
Flow ID
Start
Duration
Subject IP Address
Peer IP Address
Ex. 06/09/2017 08:51 AM - 06/17/201
Ex. <=50min40s
Ex. 10.10.10.10
Ex. 10.255.255.255
6234150
Mar 30, 2023 4:07:52 PM
(13min 10s ago)
11min 2s
10.90.66.215
10.90.66.217
6234097
Mar 30, 2023 4:07:46 PM
(13min 16s ago)
10min 48s
10.90.66.215
10.90.66.217
6234668
Mar 30, 2023 4:10:36 PM
(10min 26s ago)
1min 11s
10.90.66.215
10.90.66.217

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.