vSphere configureren om verkeer oost/west naar FlowSensor te sturen

Inhoud

Inleiding

Dit document beschrijft hoe u vSphere kunt configureren zodat verkeer naar het oosten/westen kan worden verzonden naar Secure Network Analytics Flow Sensor

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- VMware vSphere
- Secure Network Analytics (SNA)

Gebruikte componenten

VMware vSphere release 7.0.3.1

Secure Network Analytics-release 7.4.2.

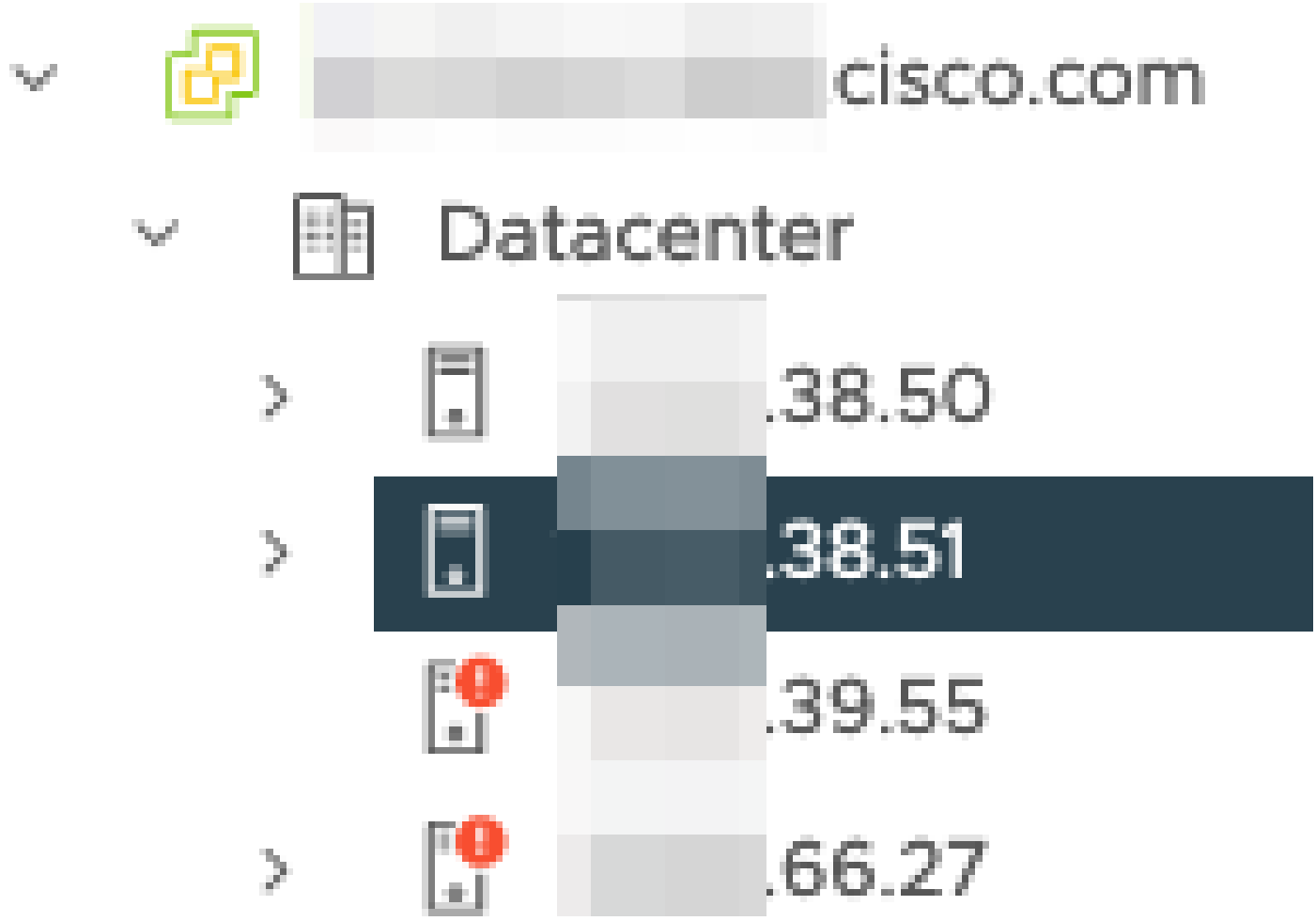
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

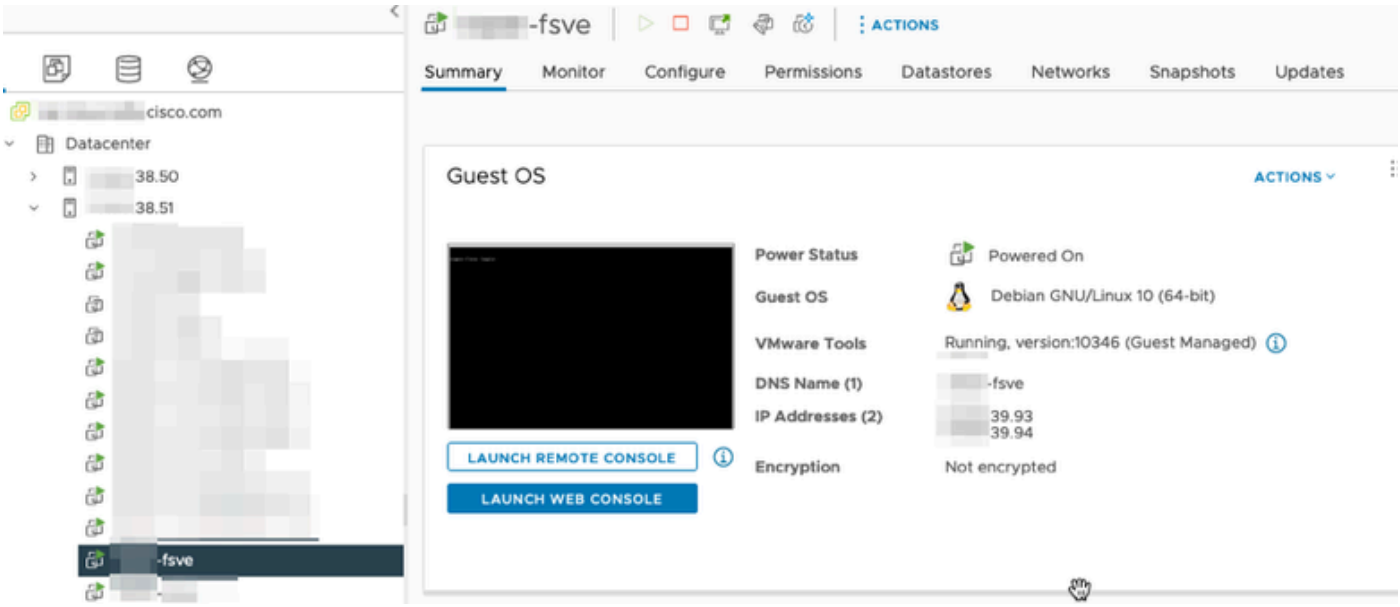
In vSphere bekijk het Datacenter voor het aantal ESXi-hosts en bepaal van welke hosts u Oost/West-verkeer wilt ophalen.

In deze afbeelding, van de vier hosts, zijn slechts twee van besproken waarvan de laatste twee octetten 38.51 en 66.27 zijn.

De ESXi-host 38.51 draait release 7.0.3 en de ESXi-host 66.27 voert release 6.7.0 uit.



Een SNA Flow Sensor release 7.4.2 is geïmplementeerd op de 38.51 ESXi-host. Deze is geconfigureerd met twee IP-adressen met de laatste octetten van 39.93 en 39.94.



Er zijn twee andere apparaten, een SNA Manager en een Data Node genaamd Manager en DN1 respectievelijk.

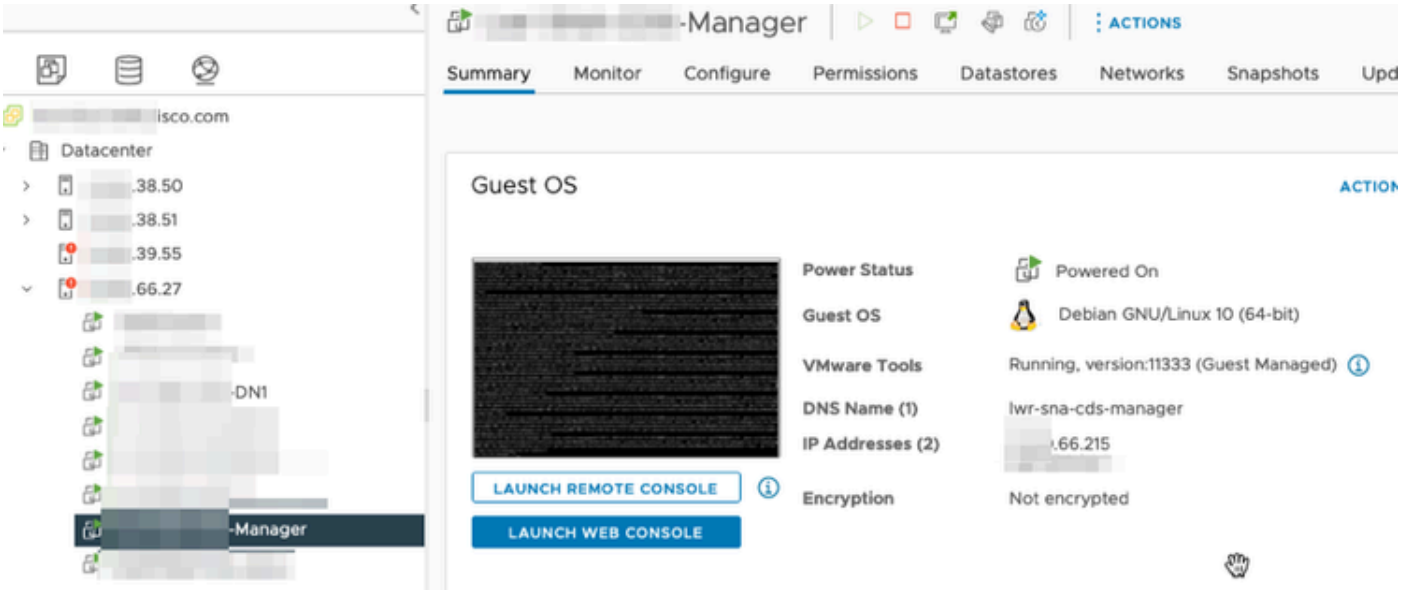
De laatste twee octetten van deze twee hosts zijn 66.215 en 66.217 voor respectievelijk de

Manager en DN1.

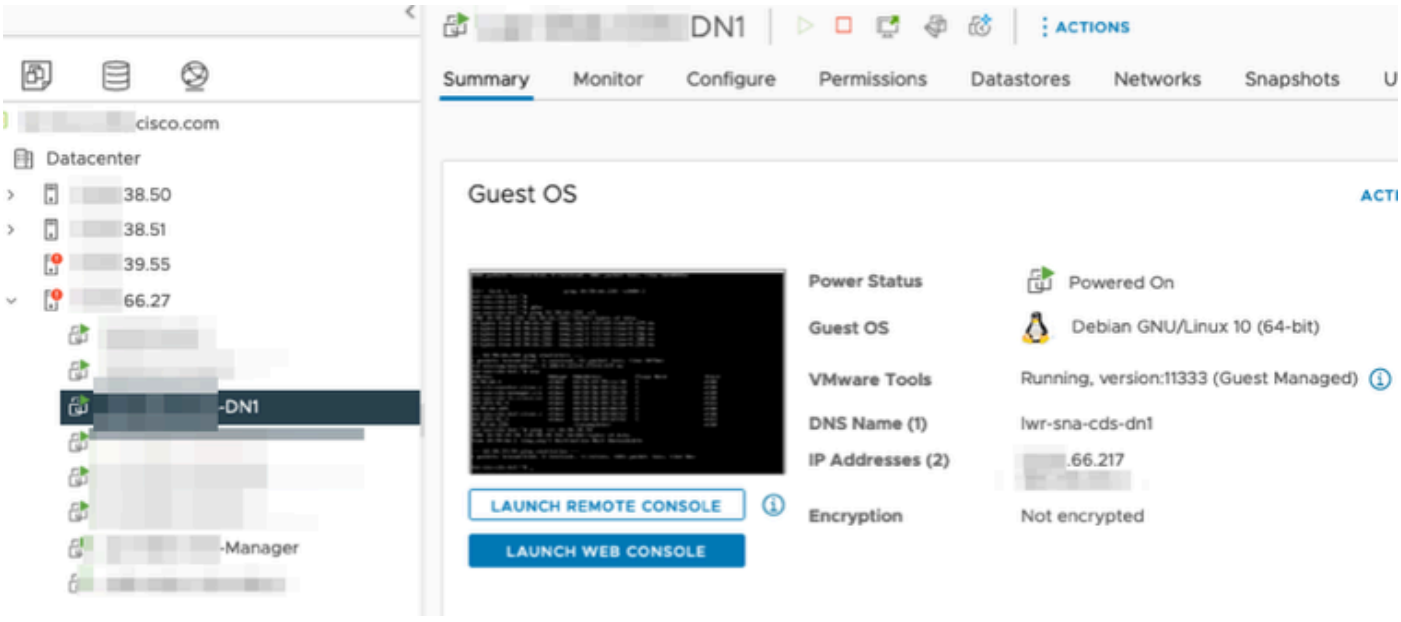
Beide hosts worden geïmplementeerd op de ESXi-host waarvan de laatste twee octetten 66.27 zijn. Dit is een andere ESXi dan de Flow Sensor wordt geïmplementeerd op.

Het verkeer tussen de Manager en de DN1-host is niet zichtbaar buiten de proxy-switch op de 66.27 ESXi-host.

SNA-beheer:

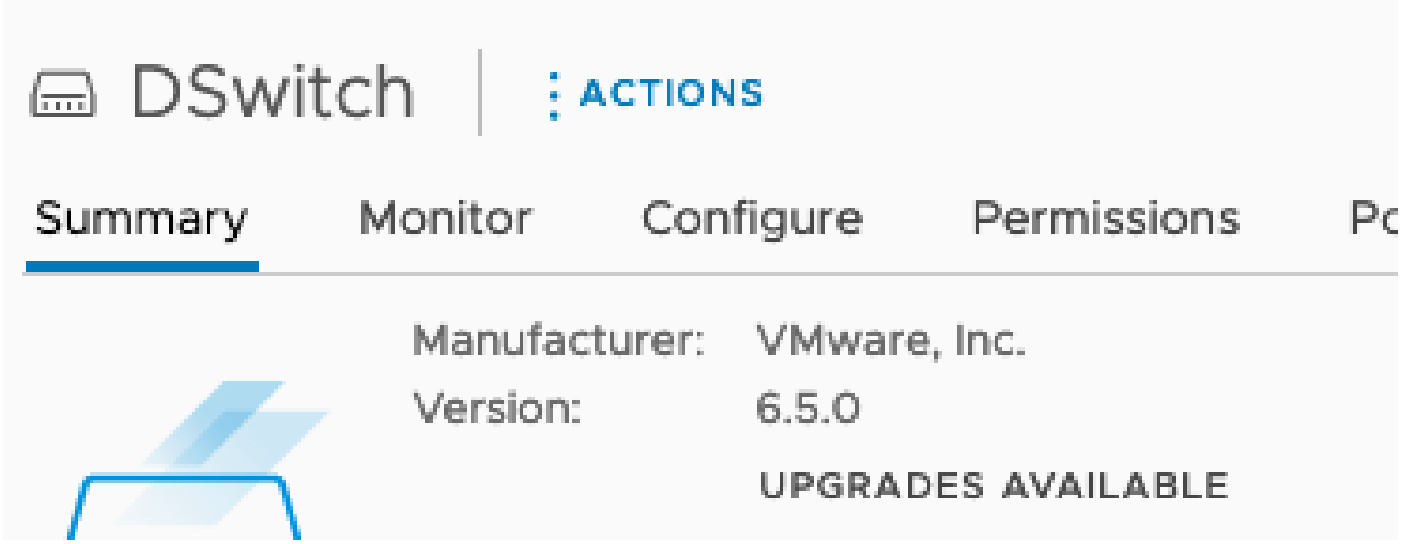


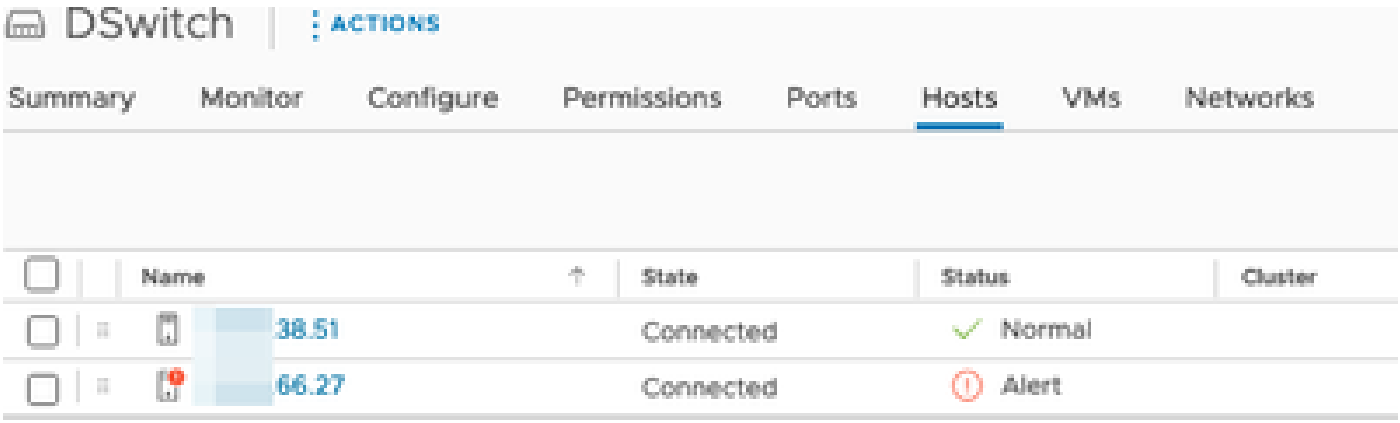
SNA DN1:



Configuraties

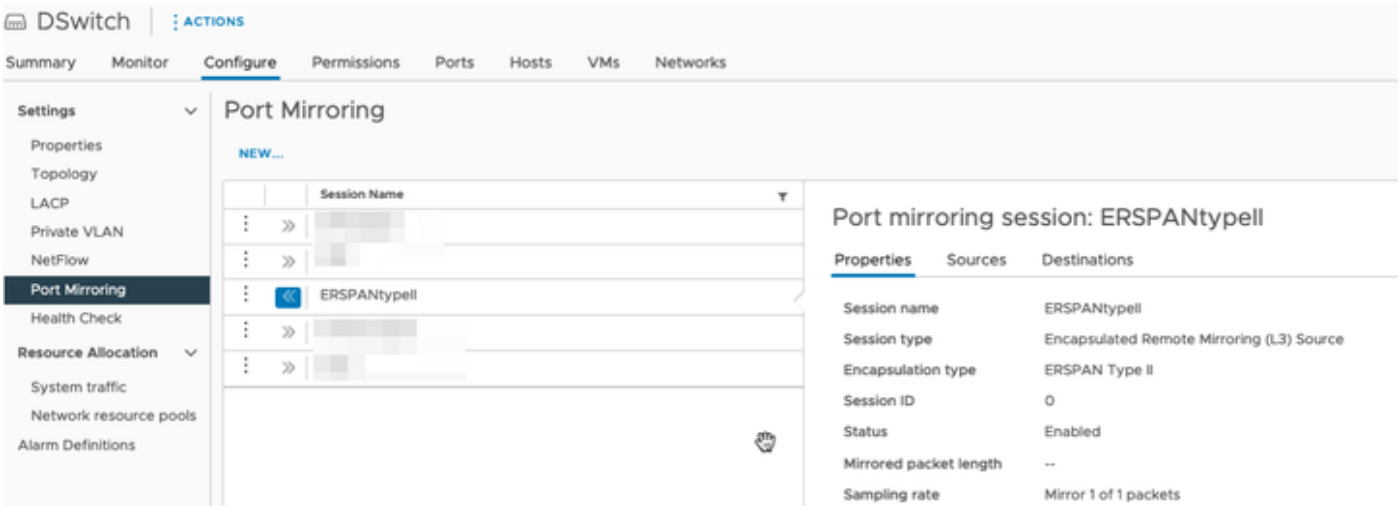
Maak een gedistribueerde versie 6.5.0-Switch met de naam DS-Switch en een gedistribueerde poortgroep met de naam DPortGroup.



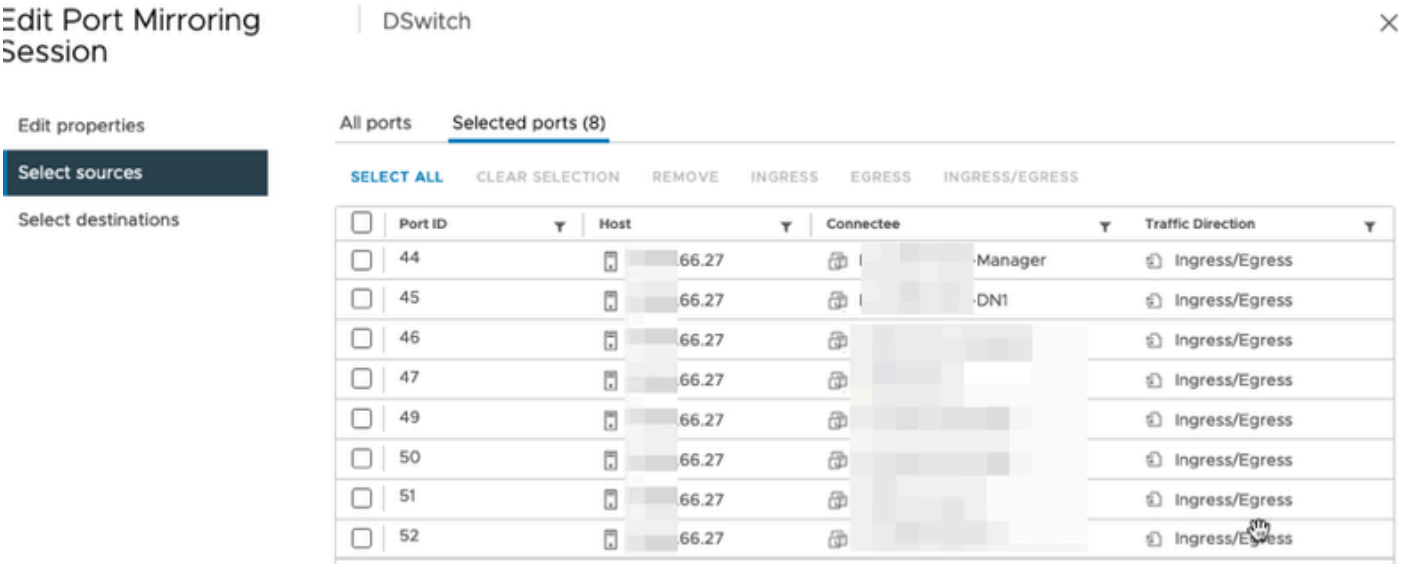


De virtuele machines en de twee uplinks voor de ESXi-hosts zijn toegevoegd aan de gedistribueerde poortgroep op de DS-switch.

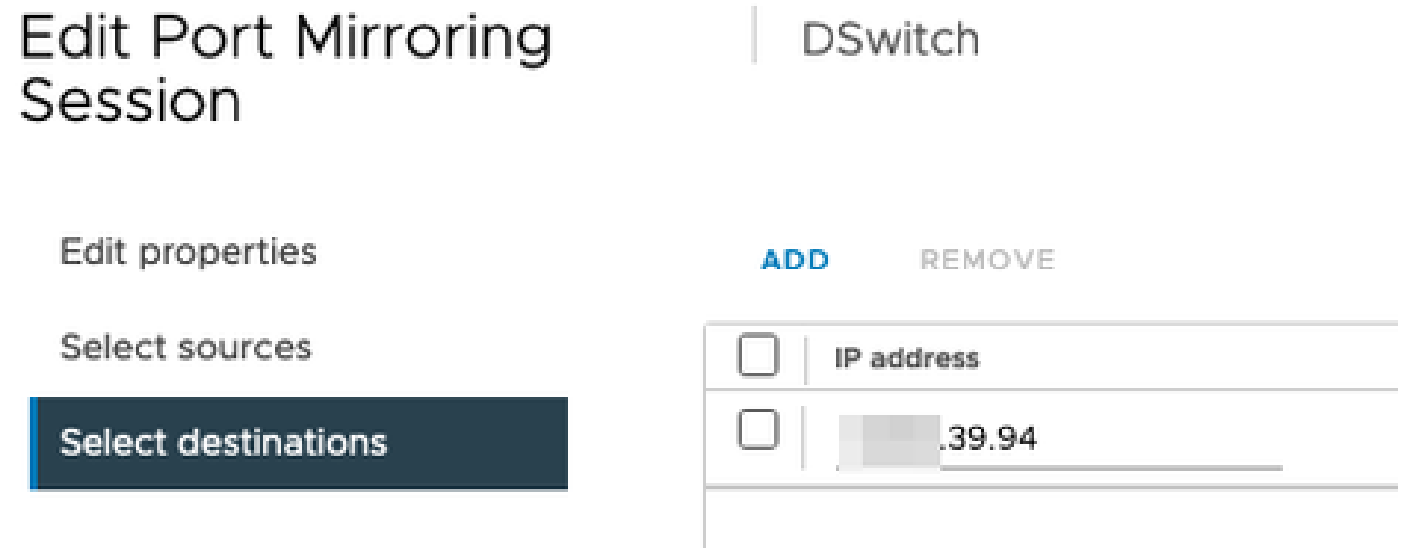
Configureer op de DS-switch een ERSPAN Type II-spiegelsessie.



Voor de Port-mirroring-sessie werden alle hosts op de 66.27 ESXi-hosts (inclusief de Manager en DN1) geselecteerd.

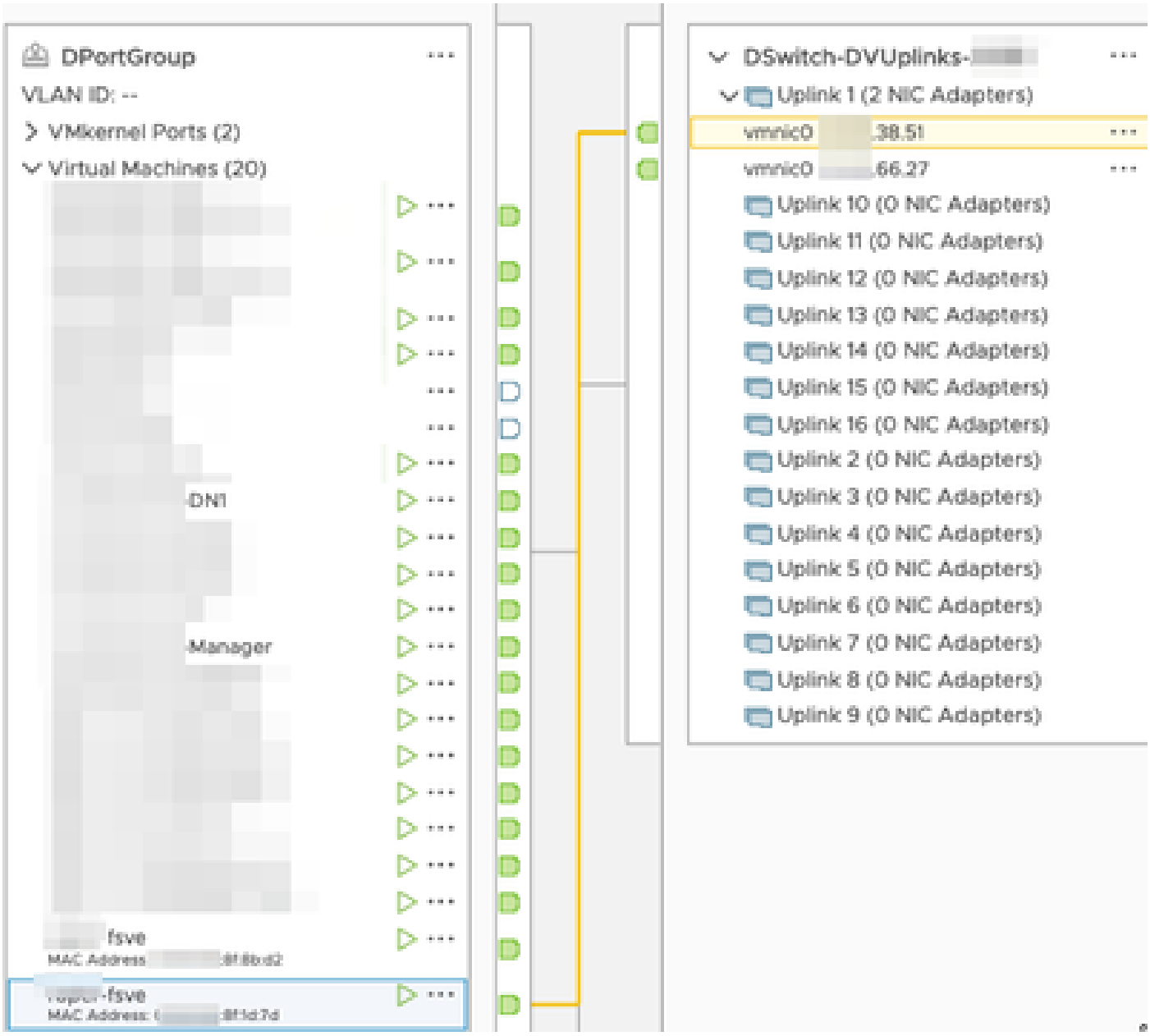


Stel voor de bestemming het in op het IP van de eth1-interface op de Flow Sensor, 39.94.

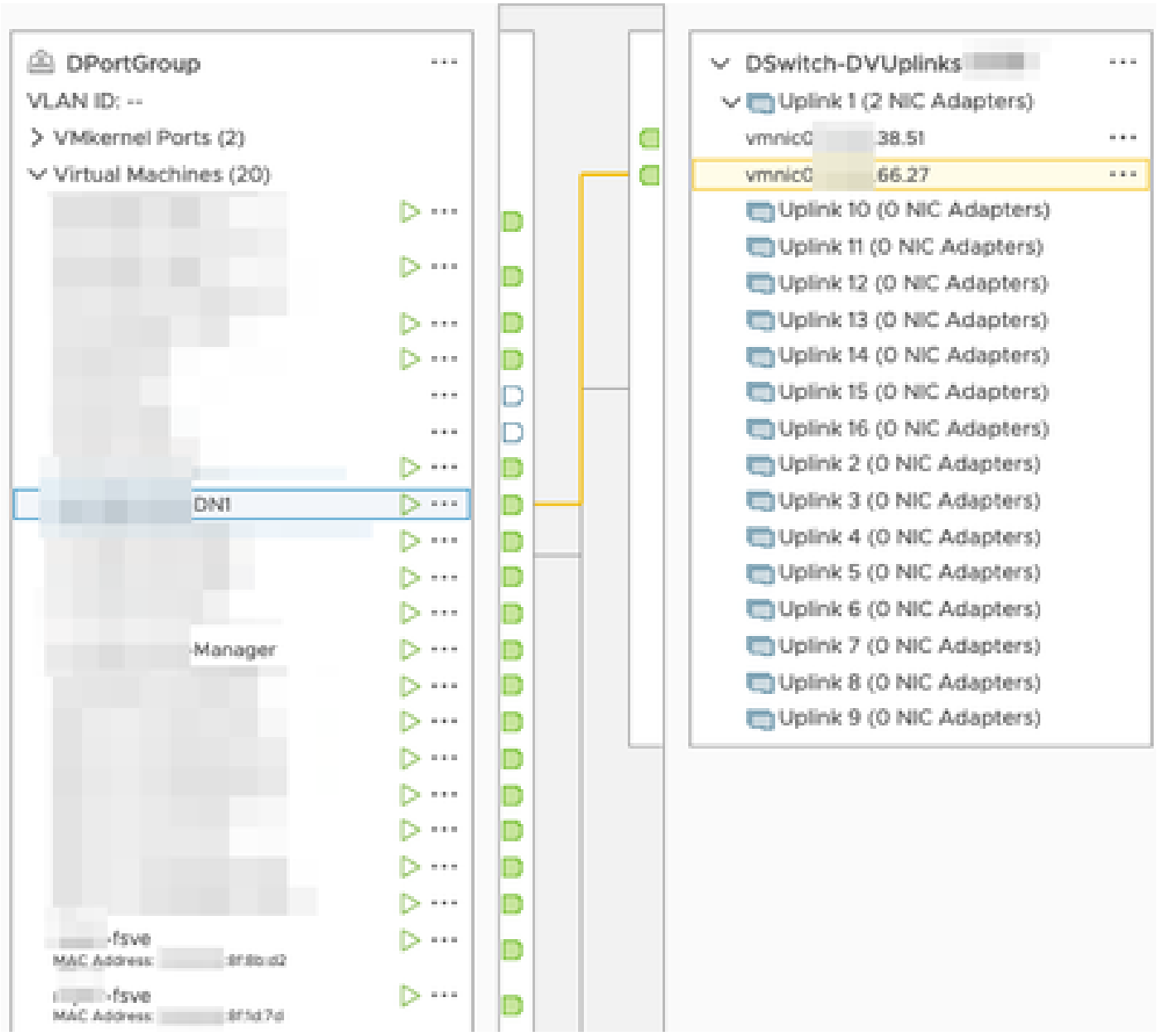


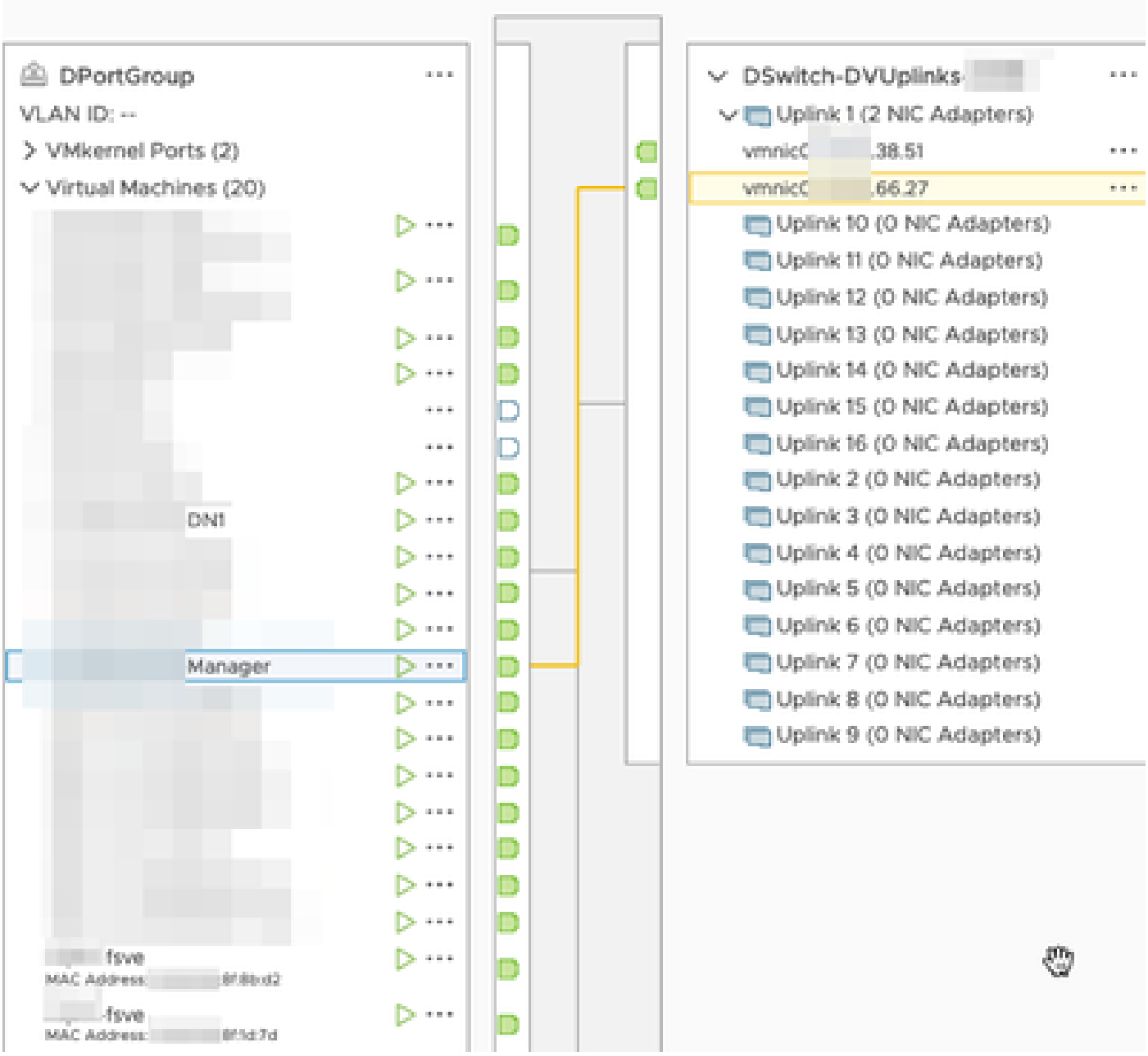
De interfaces eth0 en eth1 van de Flow Sensor worden getoond in DPortGroup geassocieerd met

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)

De eth0 interfaces van de Manager en DN1 worden getoond in DPortGroup geassocieerd met 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)



Verifiëren

Vanuit de CLI van de Flow Sensor wordt een tcpdump uitgevoerd om aan te tonen dat de GRE-tunnel op de eth1-interface komt.

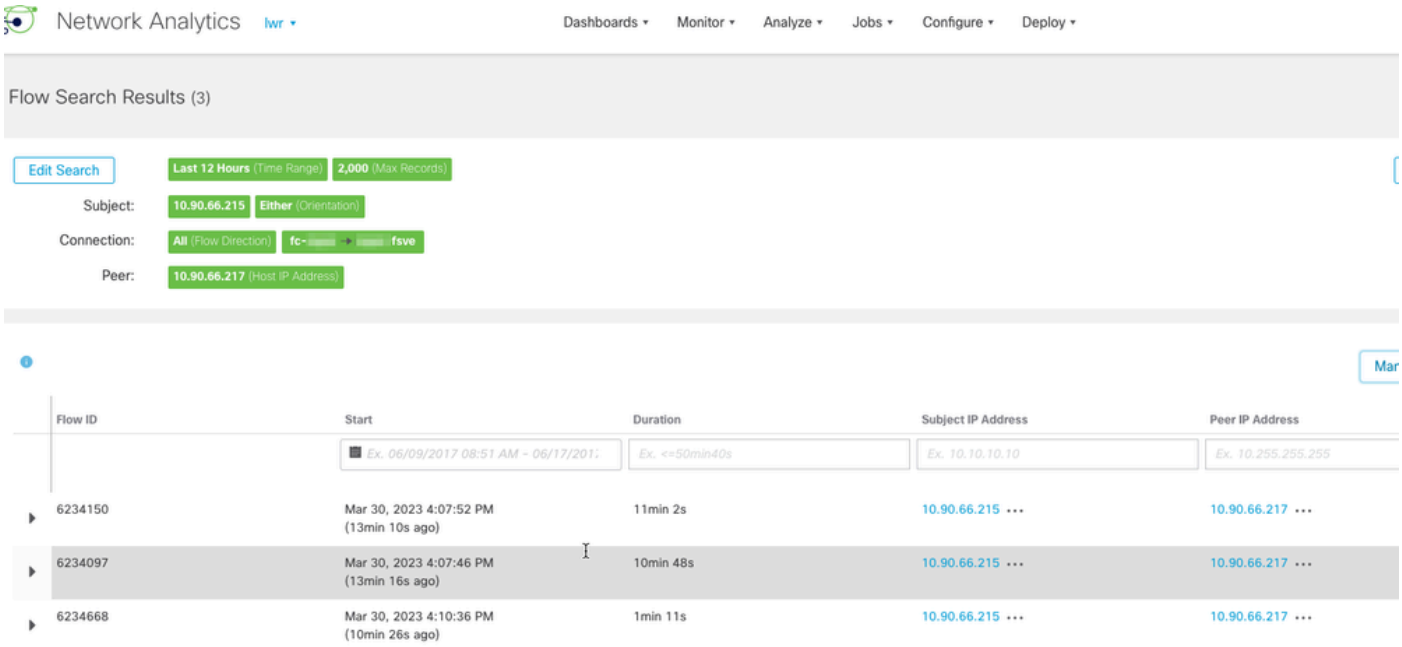
```
fsve:~# tcpdump -epnni eth1 not broadcast and not multicast -c10
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
17:43:57.080043                 >          8f:1d:7d, ethertype ARP (0x0806), length 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
```

Een flowzoekactie naar de Manager en DN1 apparaten wordt uitgevoerd op de SNA Manager die netflow ontvangt van de Flow Sensor toont verkeer tussen de Manager en DN1 host.


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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.