FlowSensor에 East/West 트래픽을 전송하도록 vSphere 구성

목차

소개

이 문서에서는 East/West 트래픽을 Secure Network Analytics Flow Sensor로 전송하도록 vSphere를 구성하는 방법에 대해 설명합니다

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- VMware vSphere
- SNA(보안 네트워크 분석)

사용되는 구성 요소

VMware vSphere 릴리스 7.0.3.

Secure Network Analytics 릴리스 7.4.2.

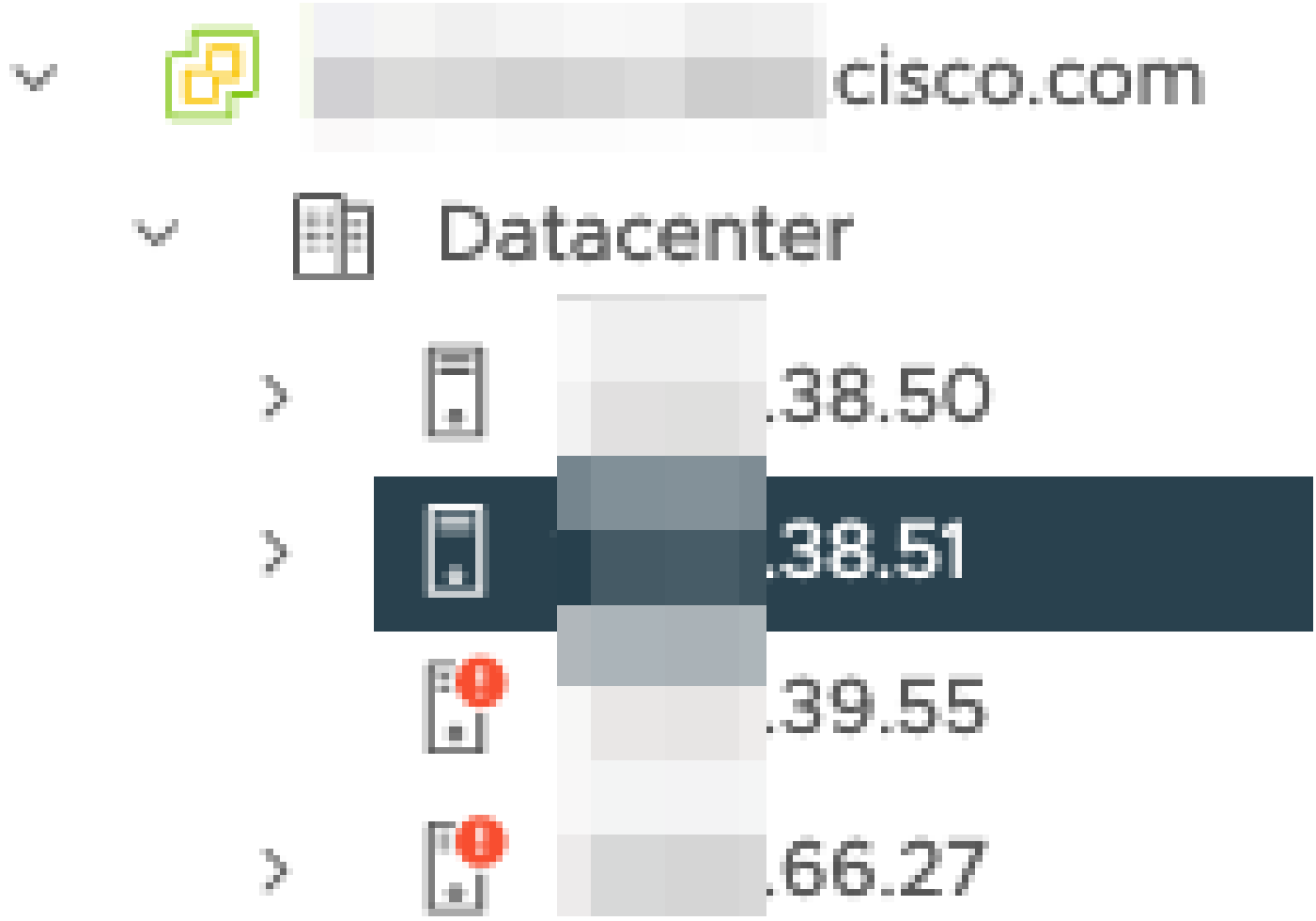
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

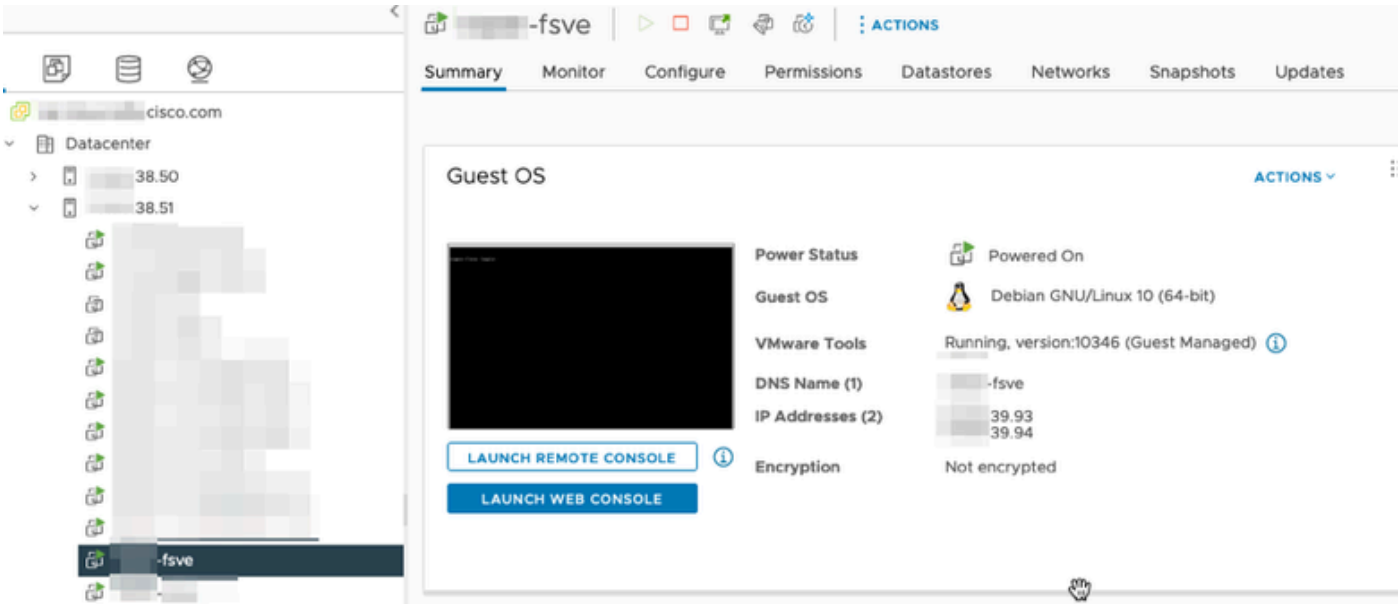
vSphere에서 데이터 센터에서 ESXi 호스트 수를 검토하고 East/West 트래픽을 수집할 호스트를 결정합니다.

이 그림에서는 4개의 호스트 중 마지막 2개의 옥텟이 38.51 및 66.27인 호스트 2개만 논의됩니다.

ESXi 호스트 38.51은 릴리스 7.0.3을 실행하고 ESXi 호스트 66.27은 릴리스 6.7.0을 실행합니다.



SNA Flow Sensor 릴리스 7.4.2는 38.51 ESXi 호스트에 구축되었으며 마지막 옥텟이 39.93 및 39.94인 2개의 IP 주소로 구성되었습니다.



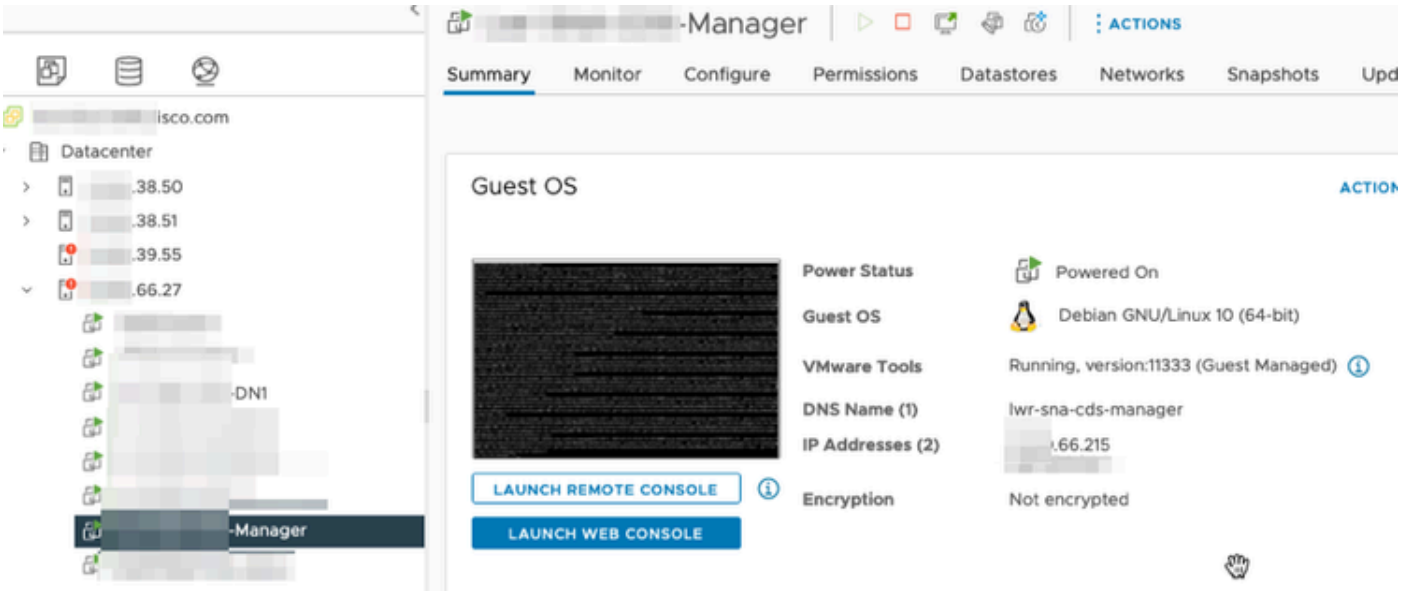
두 개의 다른 디바이스, 즉 각각 Manager 및 DN1이라는 SNA Manager와 Data Node가 있습니다.

이 두 호스트의 마지막 8진수는 각각 Manager 및 DN1의 경우 66.215 및 66.217입니다.

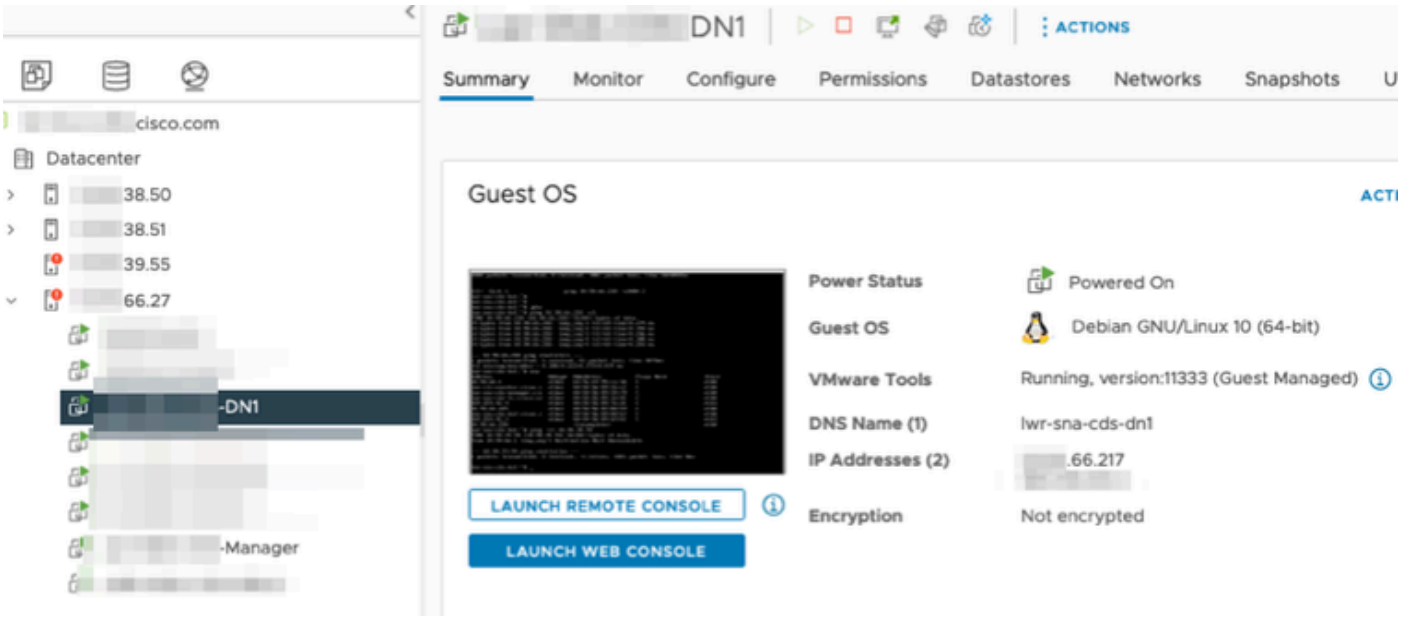
두 호스트 모두 마지막 두 옥텟이 66.27인 ESXi 호스트에 구축됩니다. 이는 Flow Sensor가 구축된 것과는 다른 ESXi입니다.

Manager와 DN1 호스트 간의 트래픽은 66.27 ESXi 호스트의 프록시 스위치 외부에서 보이지 않습니다.

SNA 관리자:

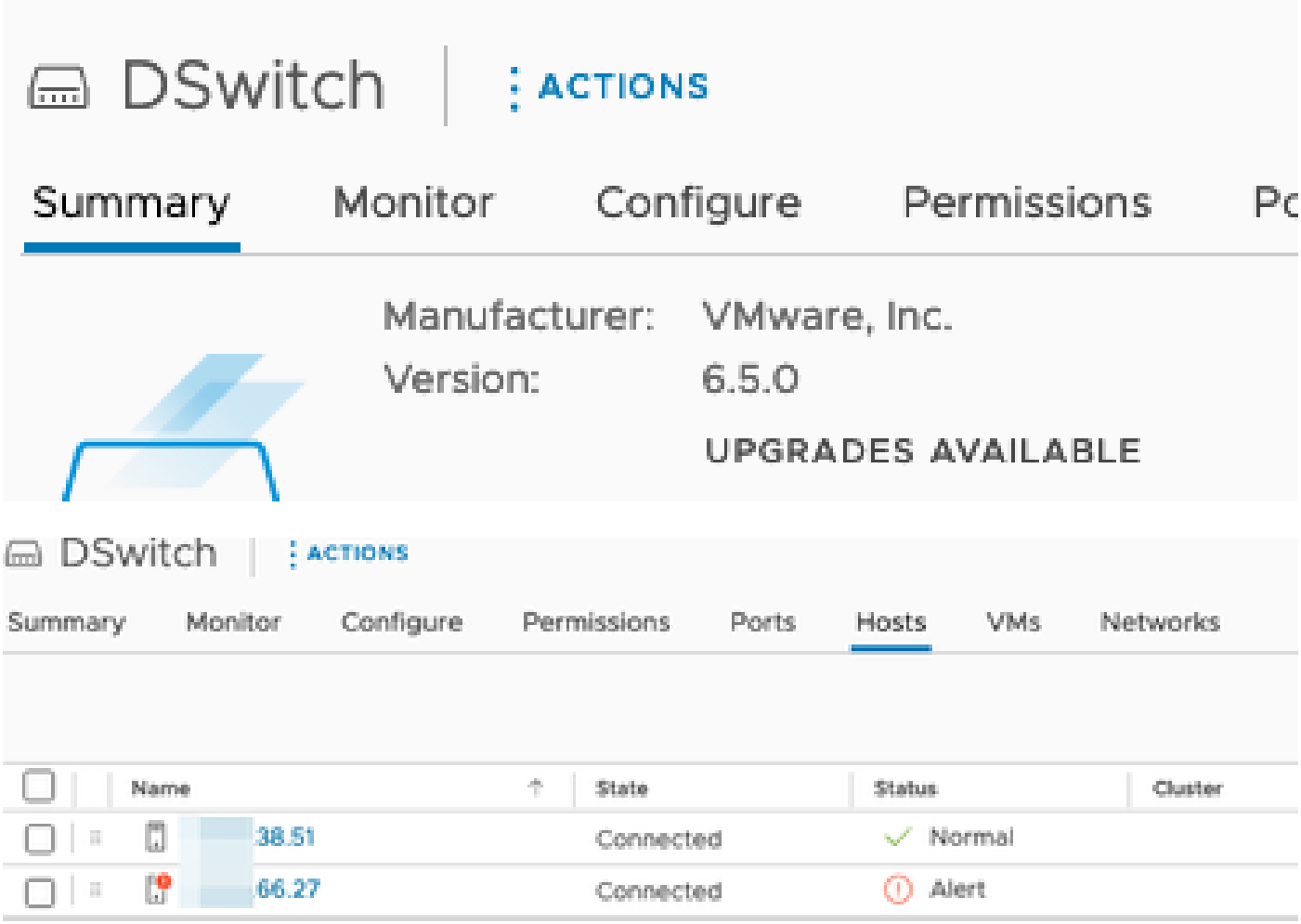


SNA DN1:



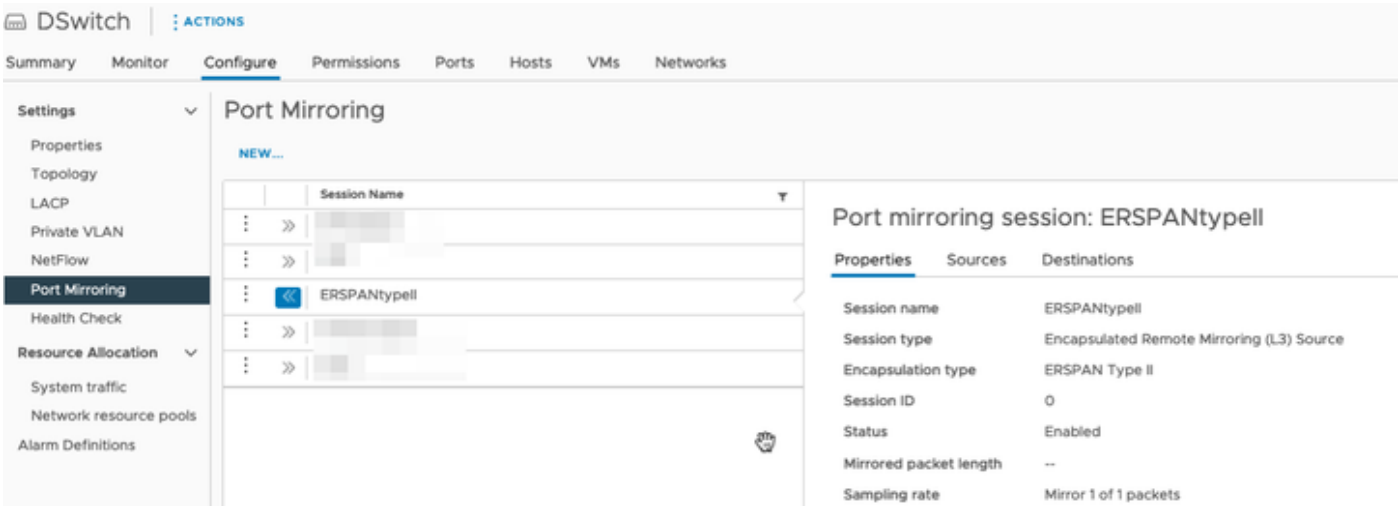
설정

DSwitch라는 버전 6.5.0 분산 스위치와 DPortGroup이라는 분산 포트 그룹을 만듭니다.

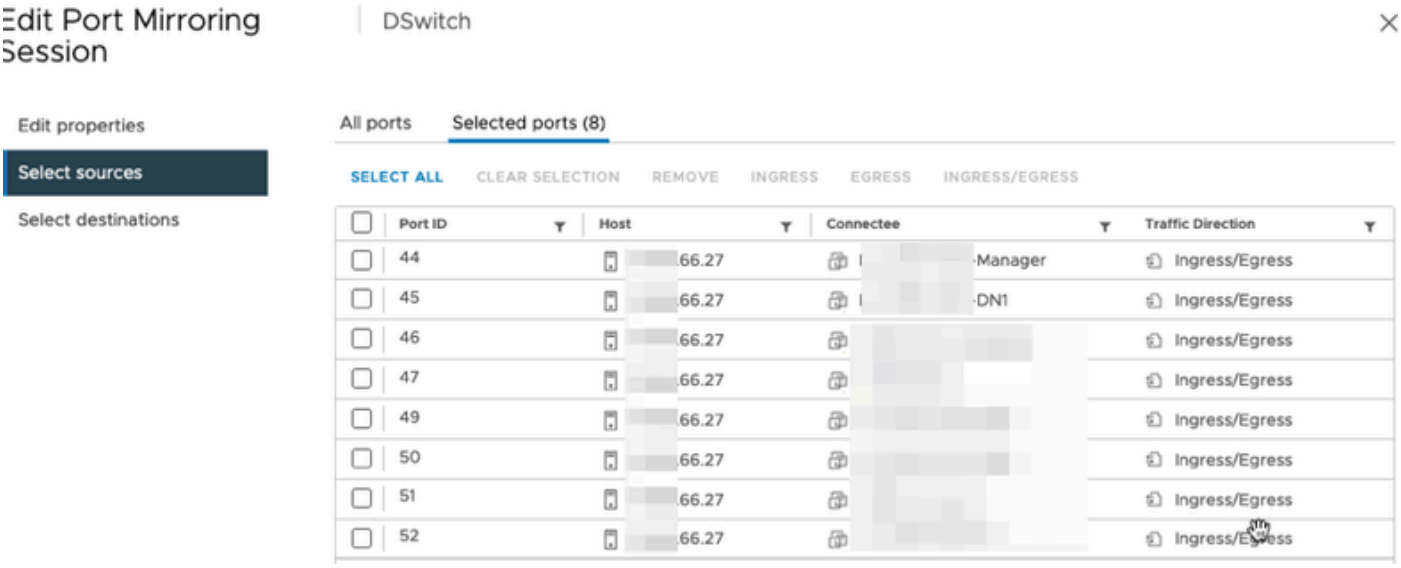


가상 머신 및 ESXi 호스트용 업링크 2개가 DSwitch의 분산 포트 그룹에 추가되었습니다.

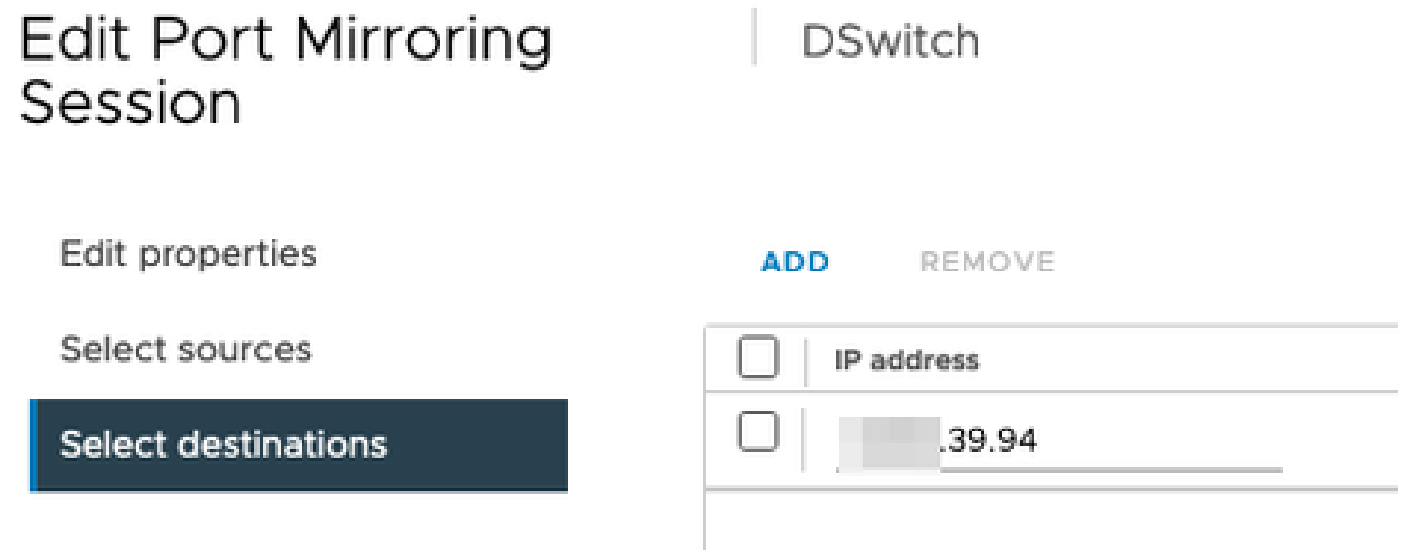
DSwitch에서 ERSPAN Type II 미러링 세션을 구성합니다.



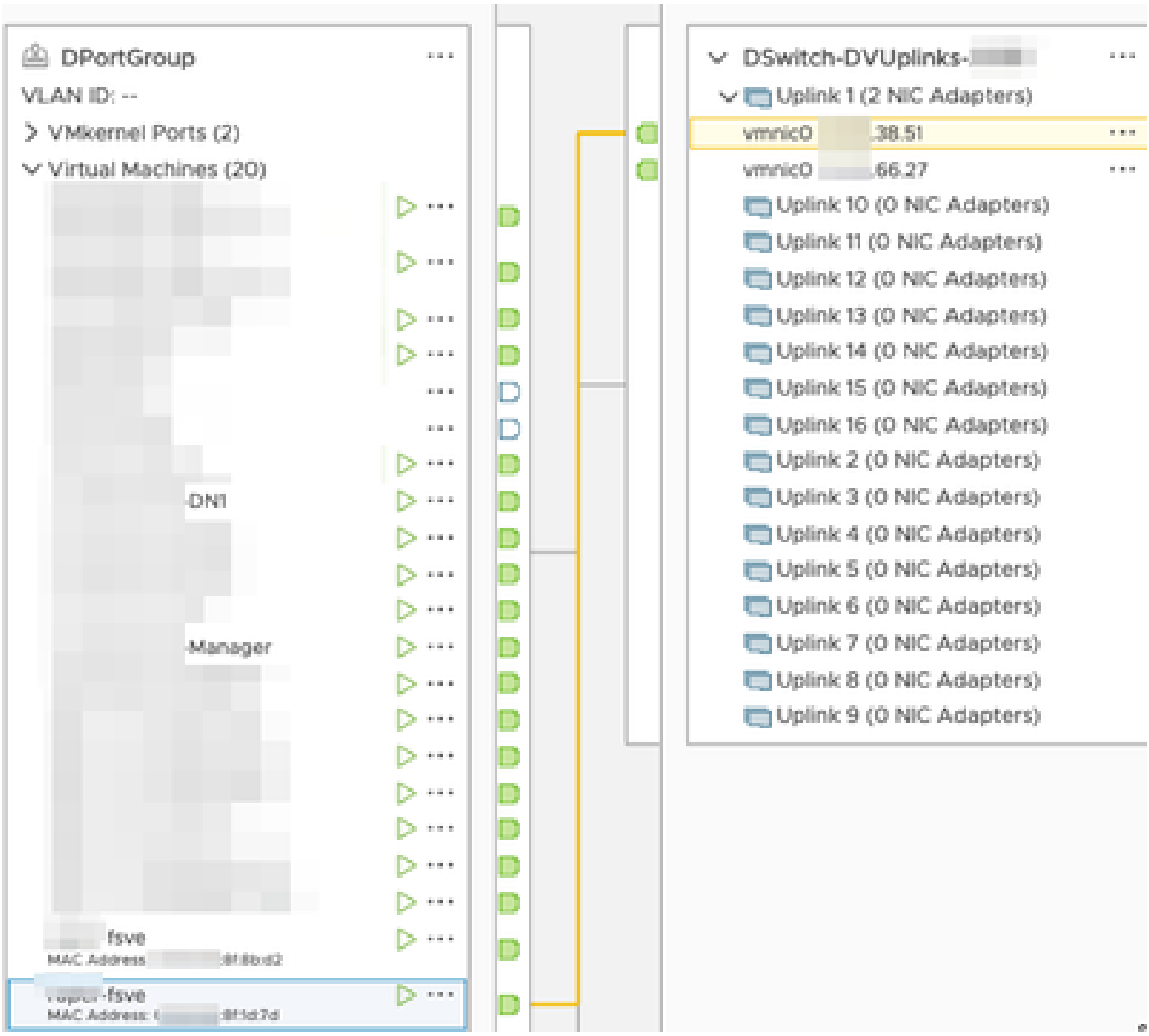
포트 미러링 세션에서는 66.27 ESXi 호스트(Manager 및 DN1 포함)의 모든 호스트가 선택되었습니다.



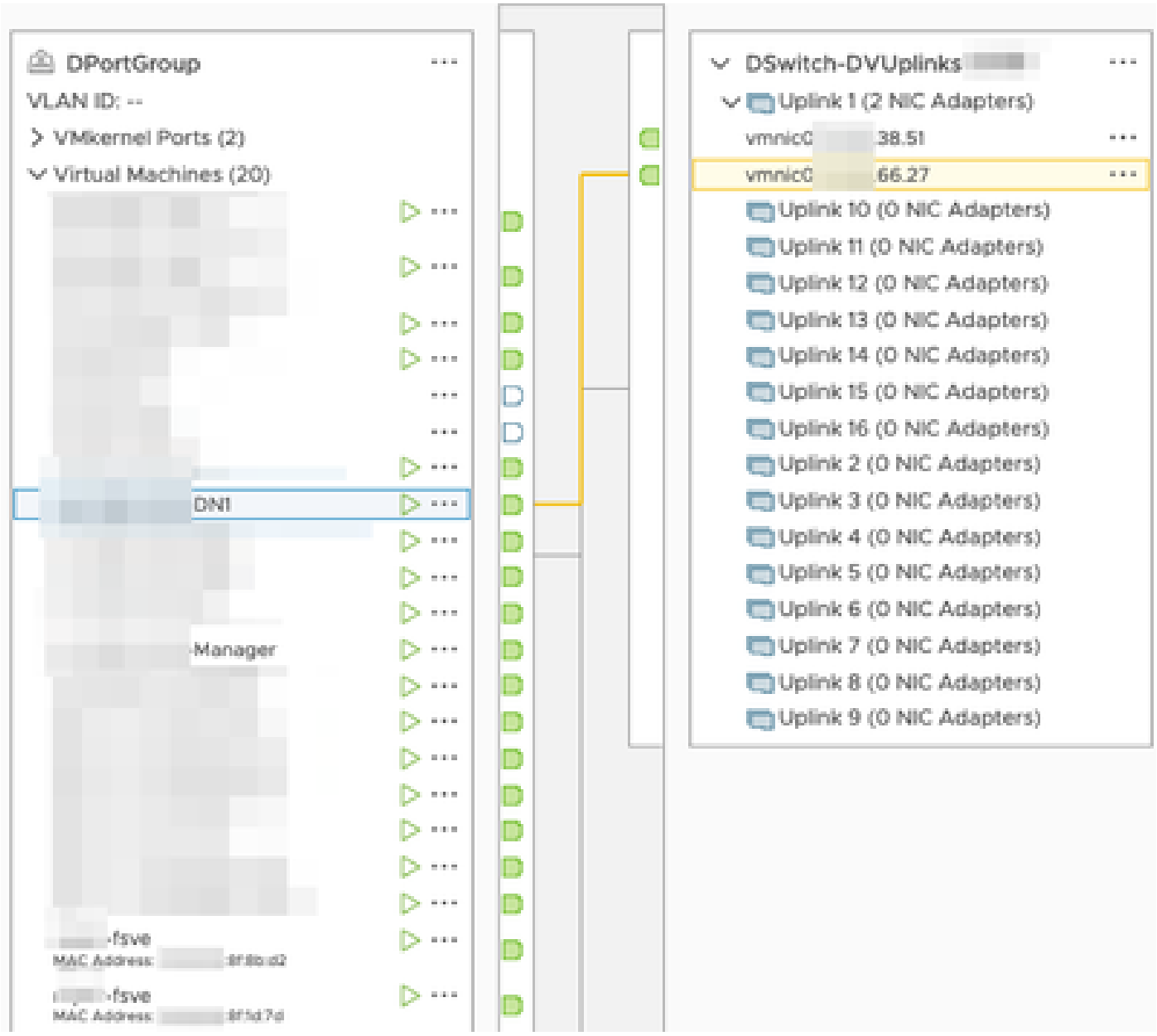
대상의 경우 Flow Sensor의 eth1 인터페이스 IP(39.94)로 설정합니다.

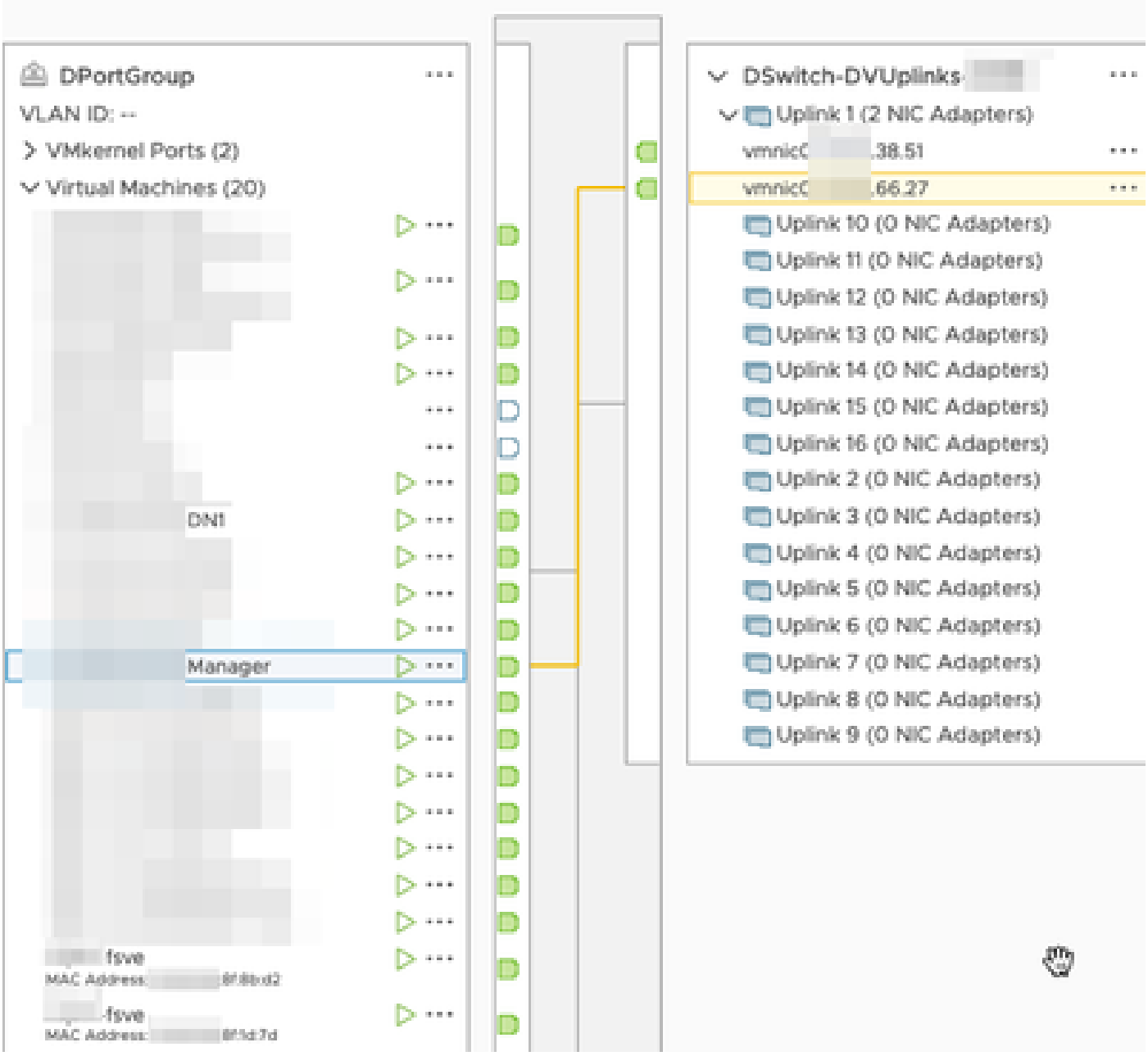


Flow Sensor의 eth0 및 eth1 인터페이스는 38.51과 연결된 DPortGroup에 표시됩니다.


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)

관리자 및 DN1의 eth0 인터페이스는 66.27과 연결된 DPortGroup에 표시됩니다.


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)



다음을 확인합니다.

플로우 센서의 CLI에서 tcpdump가 실행되어 eth1 인터페이스에 GRE 터널이 작동함을 보여줍니다.

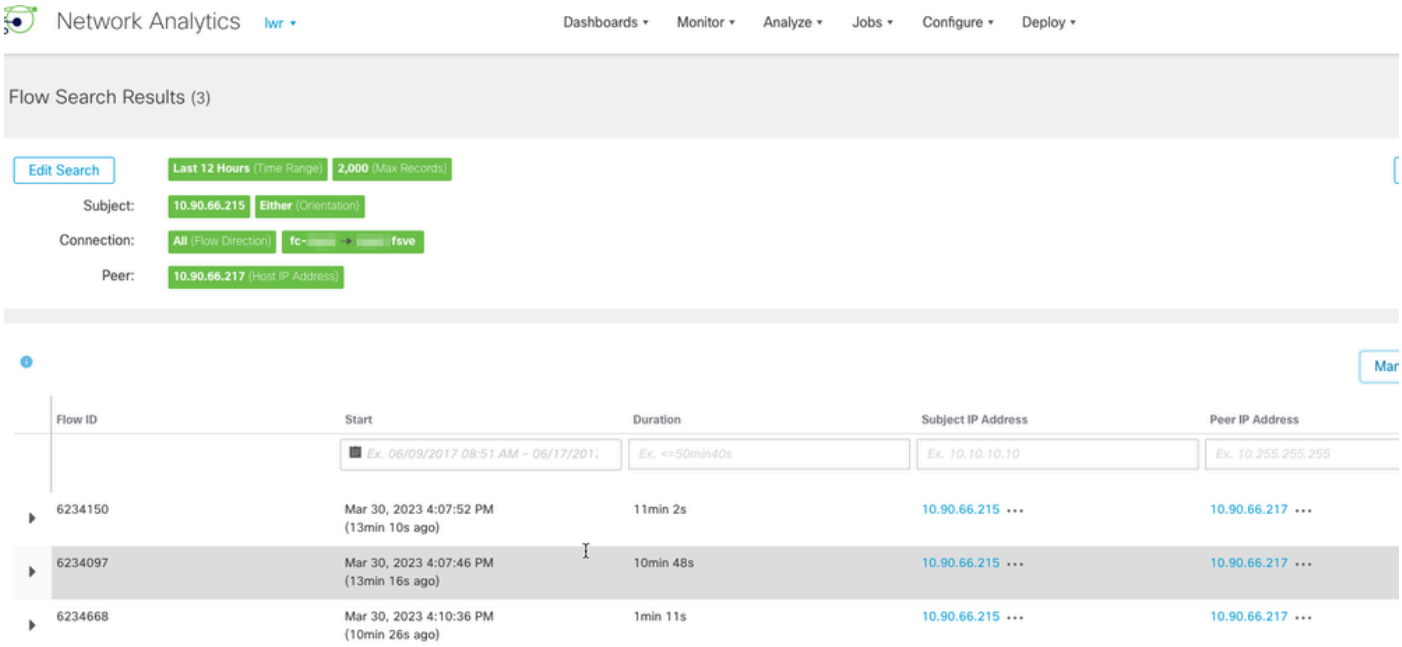
```
fsve:~# tcpdump -epnni eth1 not broadcast and not multicast -c10
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
17:43:57.080043                 >          8f:1d:7d, ethertype ARP (0x0806), length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

Manager 및 DN1 디바이스에 대한 플로우 검색은 SNA Manager에서 실행되며, 이 SNA Manager는 Flow Sensor에서 netflow를 수신하여 Manager와 DN1 호스트 간의 트래픽을 표시합니다.


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

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.