Configure vSphere to Send East/West Traffic to FlowSensor

Contents

Introduction

This document describes how to configure vSphere so East/West traffic can be sent to Secure Network Analytics Flow Sensor

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- VMware vSphere
- Secure Network Analytics (SNA)

Components Used

VMware vSphere release 7.0.3.

Secure Network Analytics release 7.4.2.

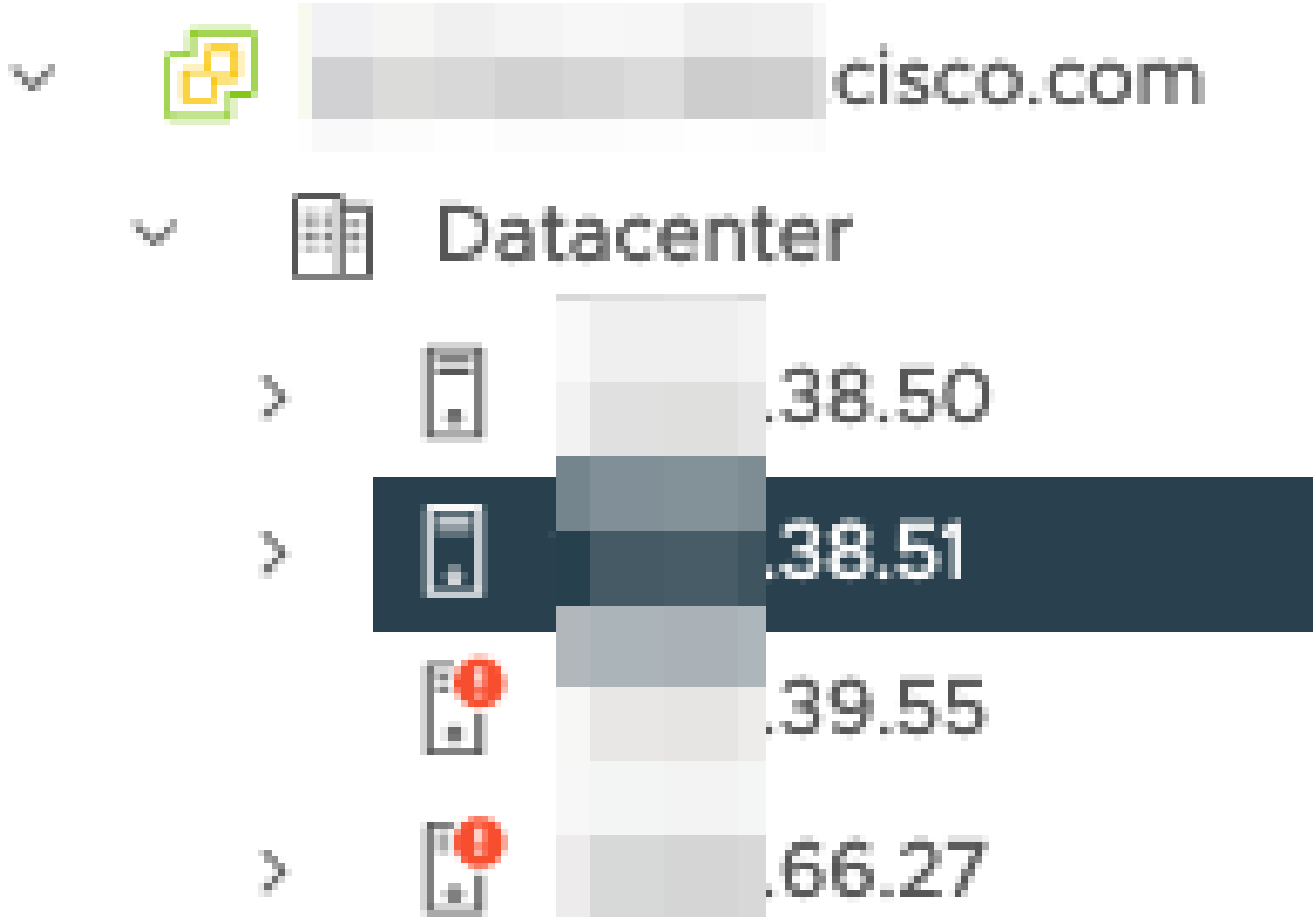
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

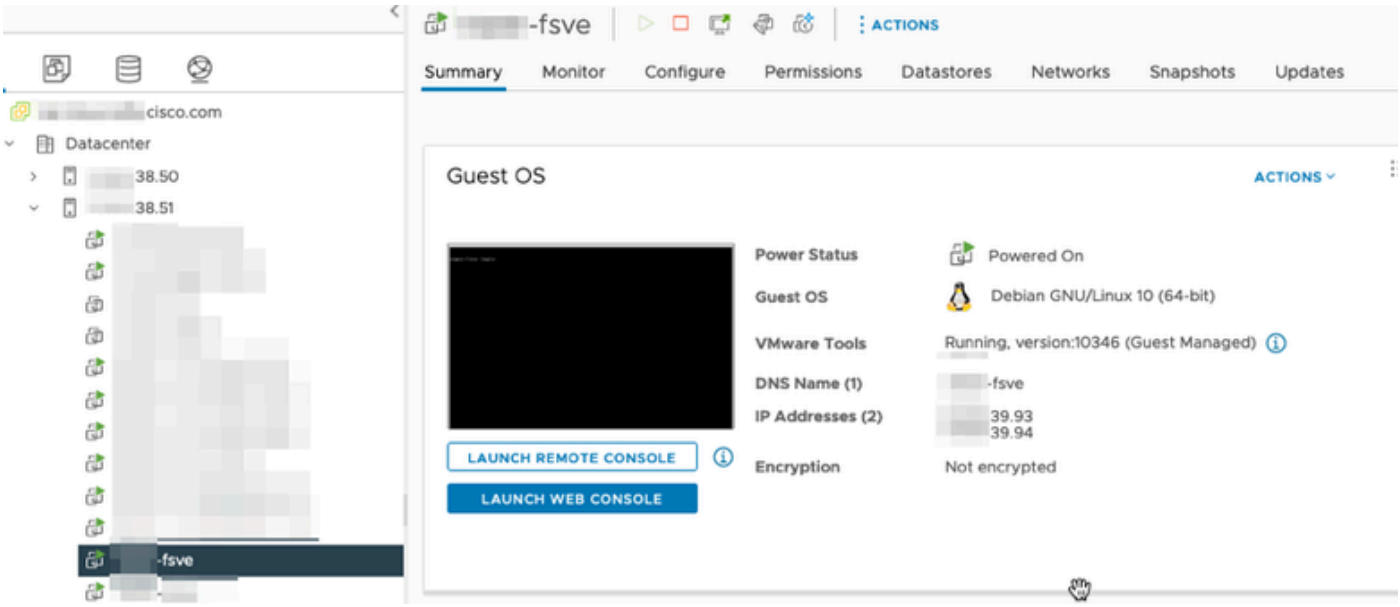
In vSphere review the Datacenter for the number of ESXi hosts and determine which hosts you wish to collect East/West traffic from.

In this image, of the four hosts, only two are of discussed whose last two octets are 38.51, and 66.27.

The ESXi host 38.51 runs release 7.0.3, and the ESXi host 66.27 runs release 6.7.0.



An SNA Flow Sensor release 7.4.2 has been deployed on the 38.51 ESXi host, it has been configured with two IP addresses with the last octets of 39.93 and 39.94.



There are two other devices, an SNA Manager and Data Node called Manager and DN1 respectively.

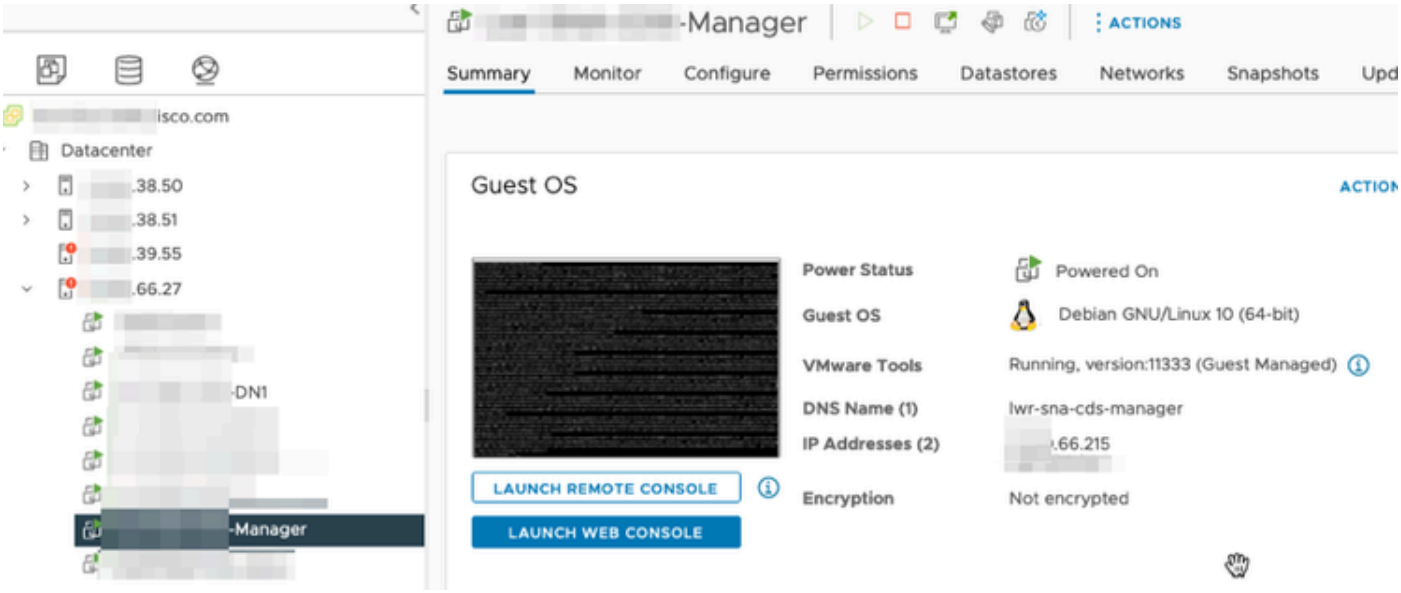
The last two octets of these two hosts are 66.215 and 66.217 for the Manager and DN1 respectively.

Both of these hosts are deployed on the ESXi host whose last two octets are 66.27, this is a different ESXi

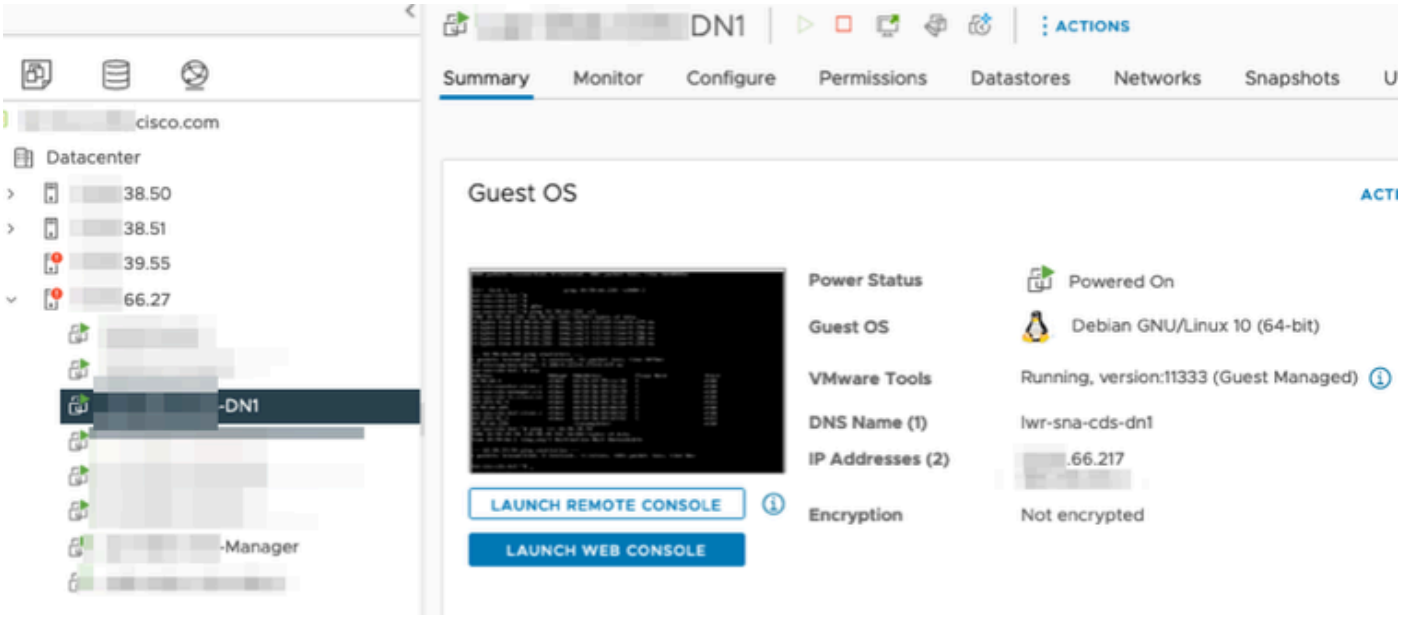
than the Flow Sensor is deployed on.

Traffic between the Manager and DN1 host is not seen outside of the proxy switch on the 66.27 ESXi host.

The SNA Manager:

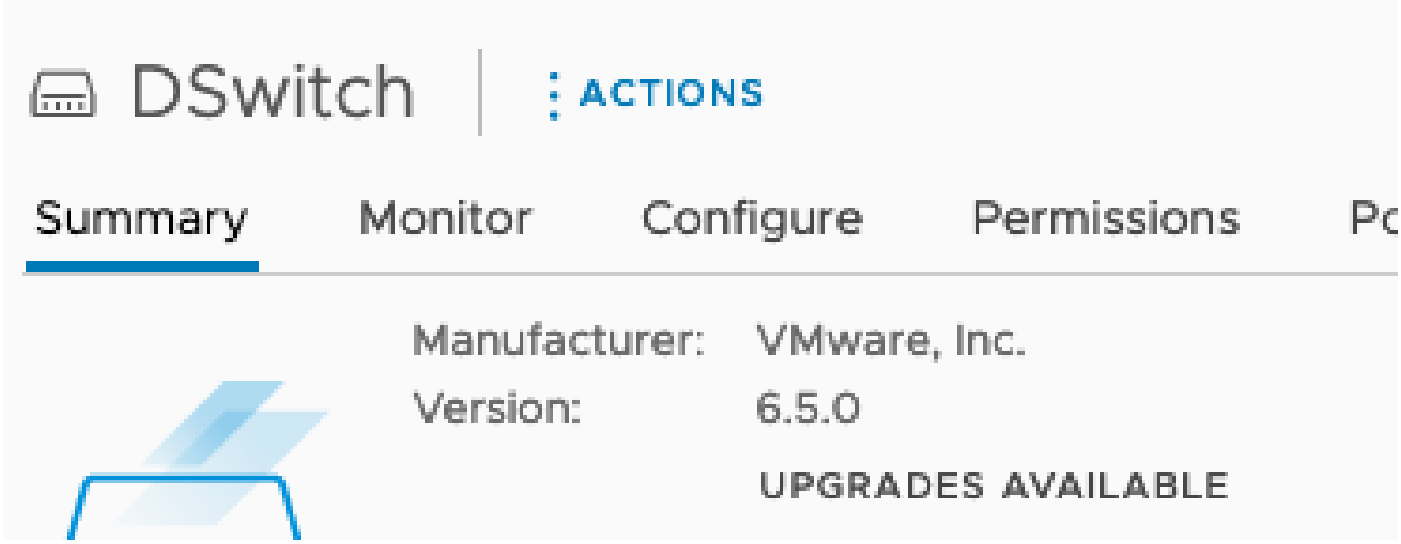


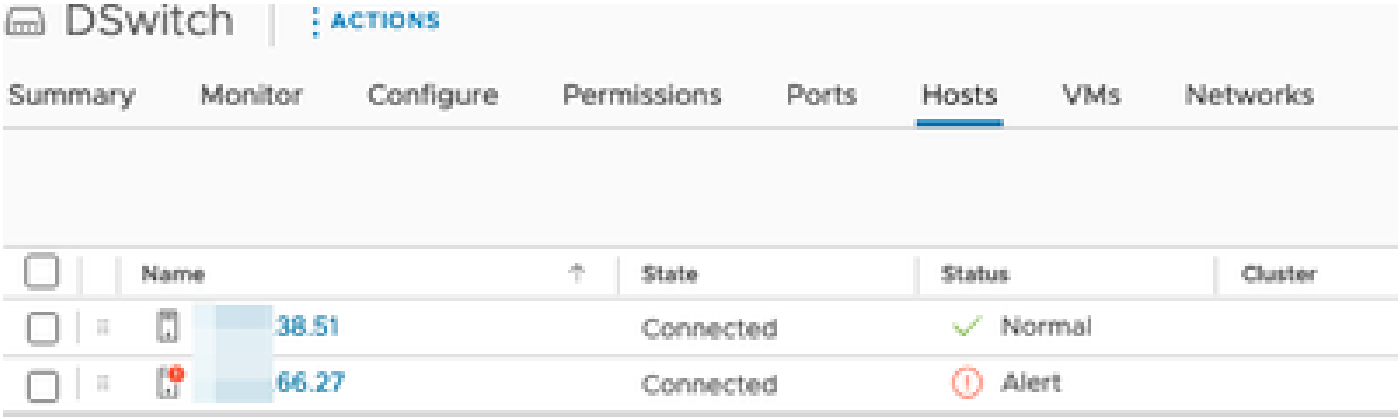
The SNA DN1:



Configurations

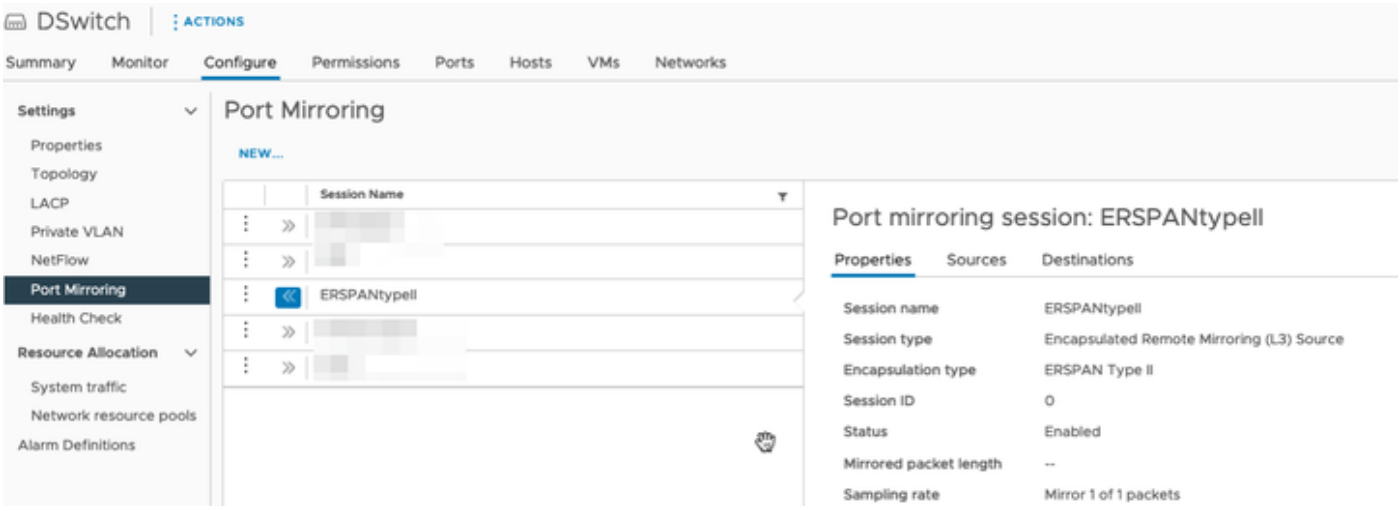
Create a version 6.5.0 Distributed Switch called DSwitch and a Distributed Port Group called DPortGroup.



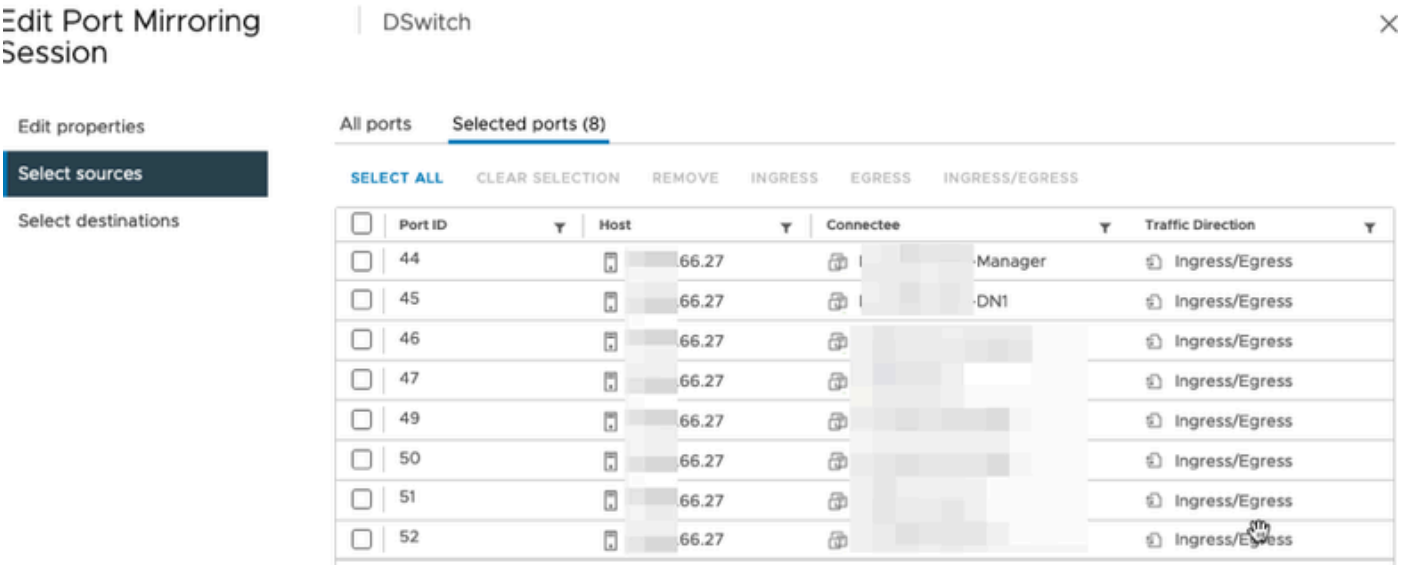


The virtual machines, and the two Uplinks for the ESXi hosts were added to the Distributed Port Group on the DSwitch.

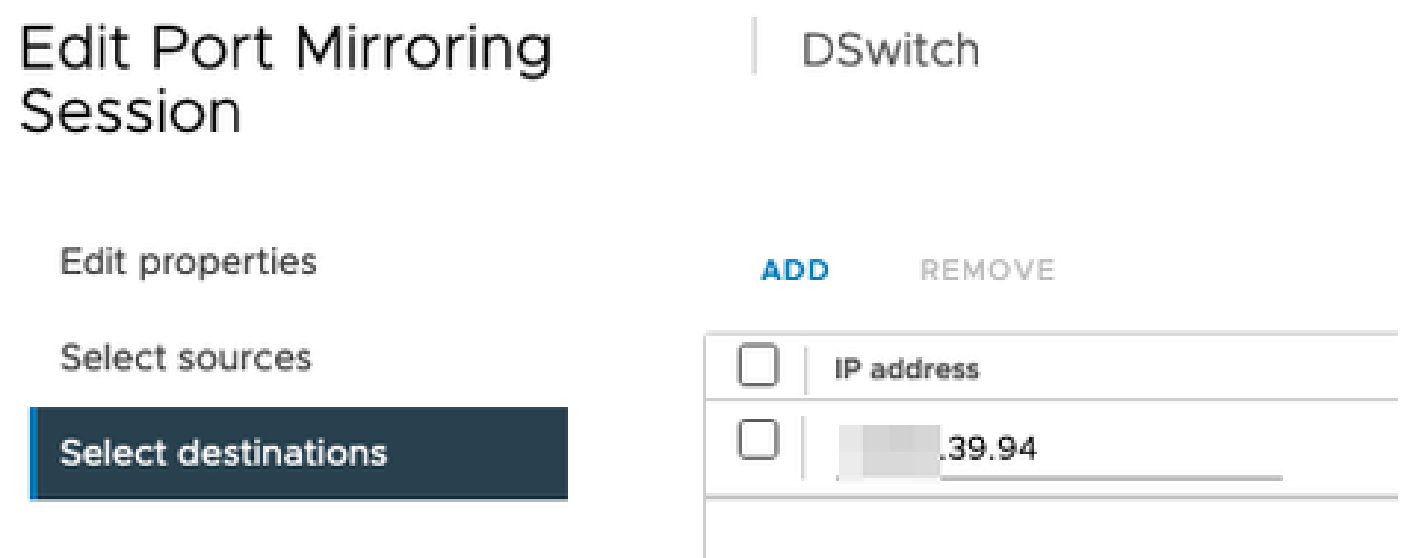
On the DSwitch, configure an ERSPAN Type II mirroring session.



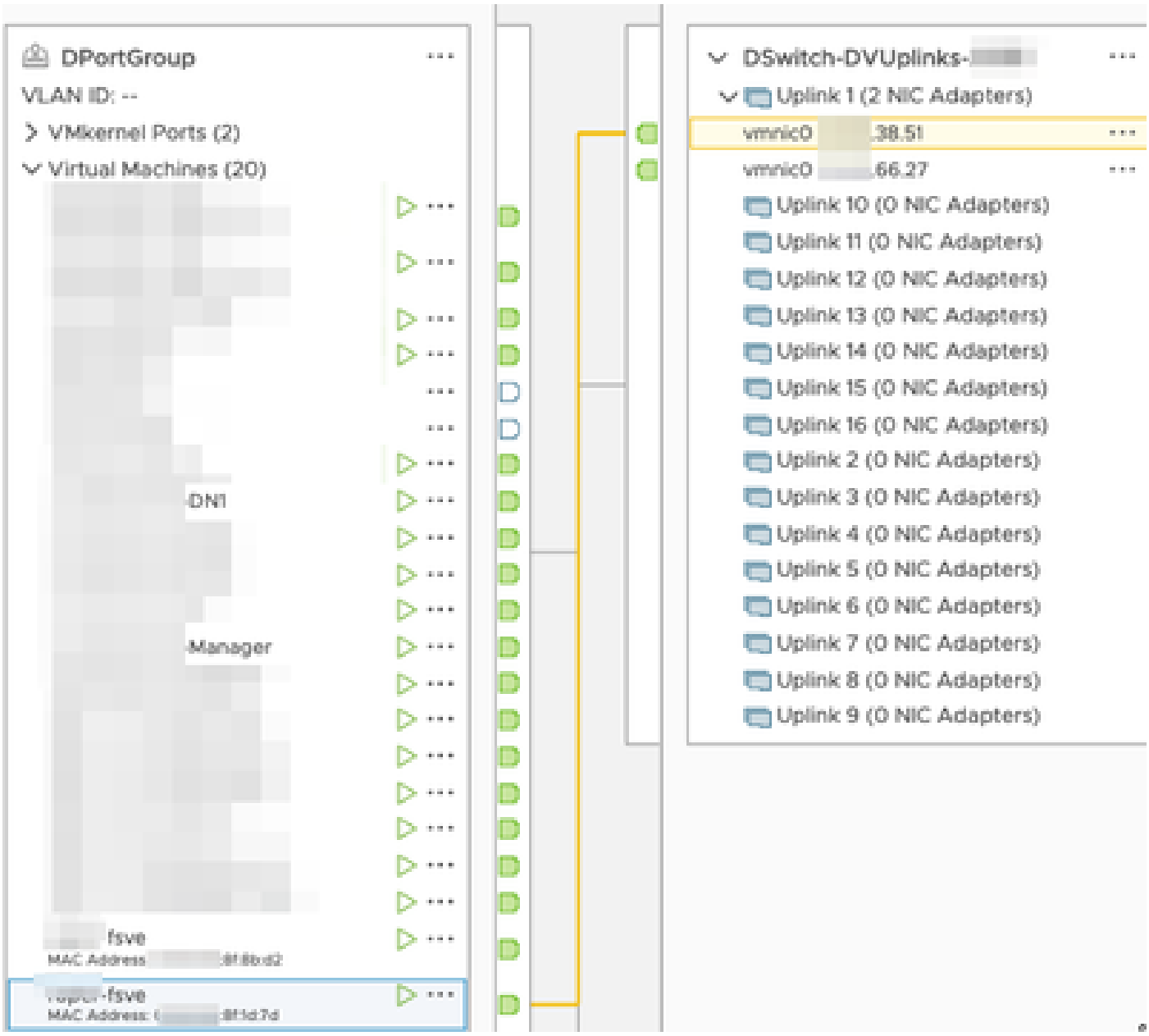
For the Port mirroring session, all hosts on the 66.27 ESXi hosts (including the Manager and DN1) were selected.



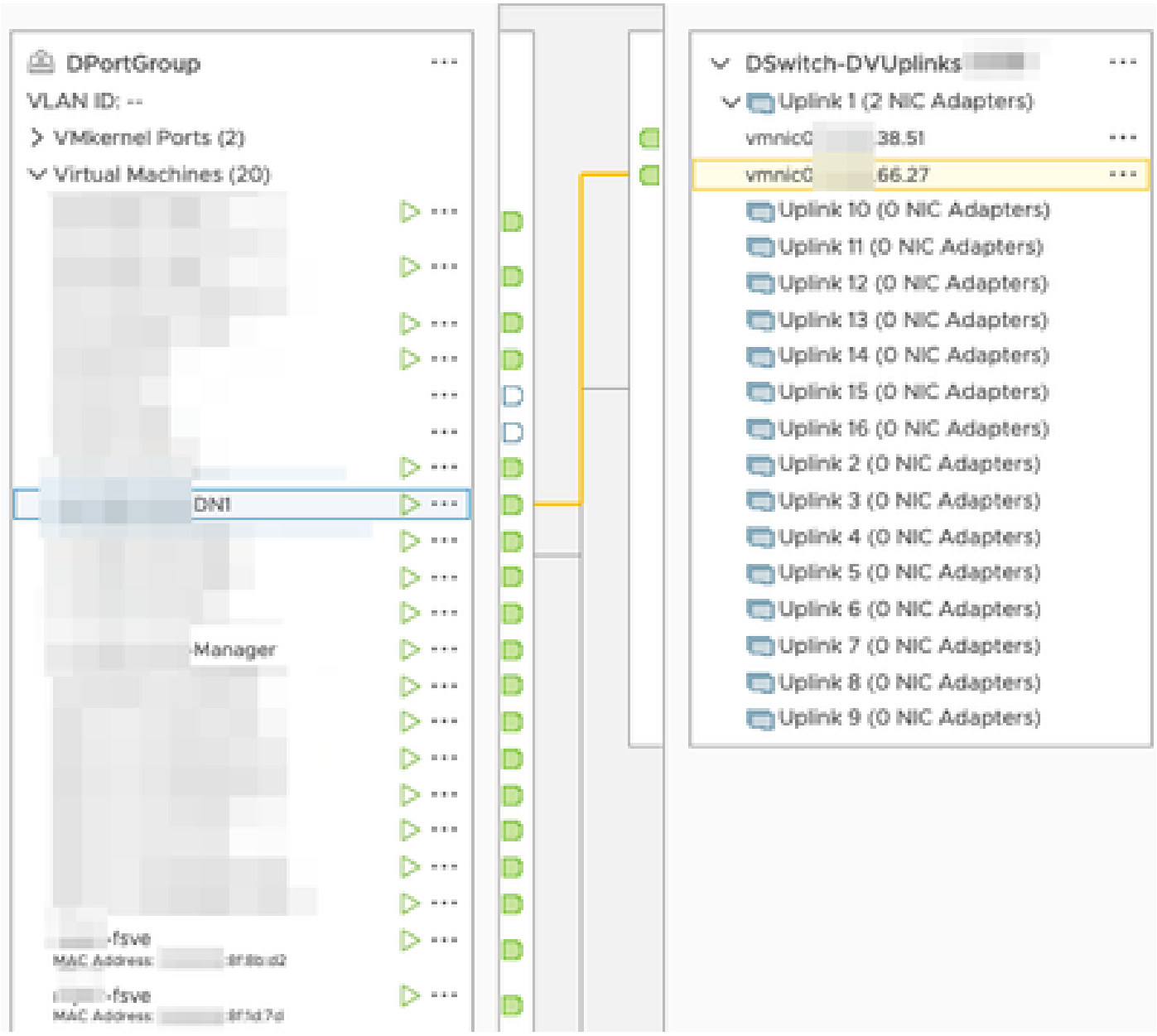
For the destination, set it to the IP of the eth1 interface on the Flow Sensor, 39.94.

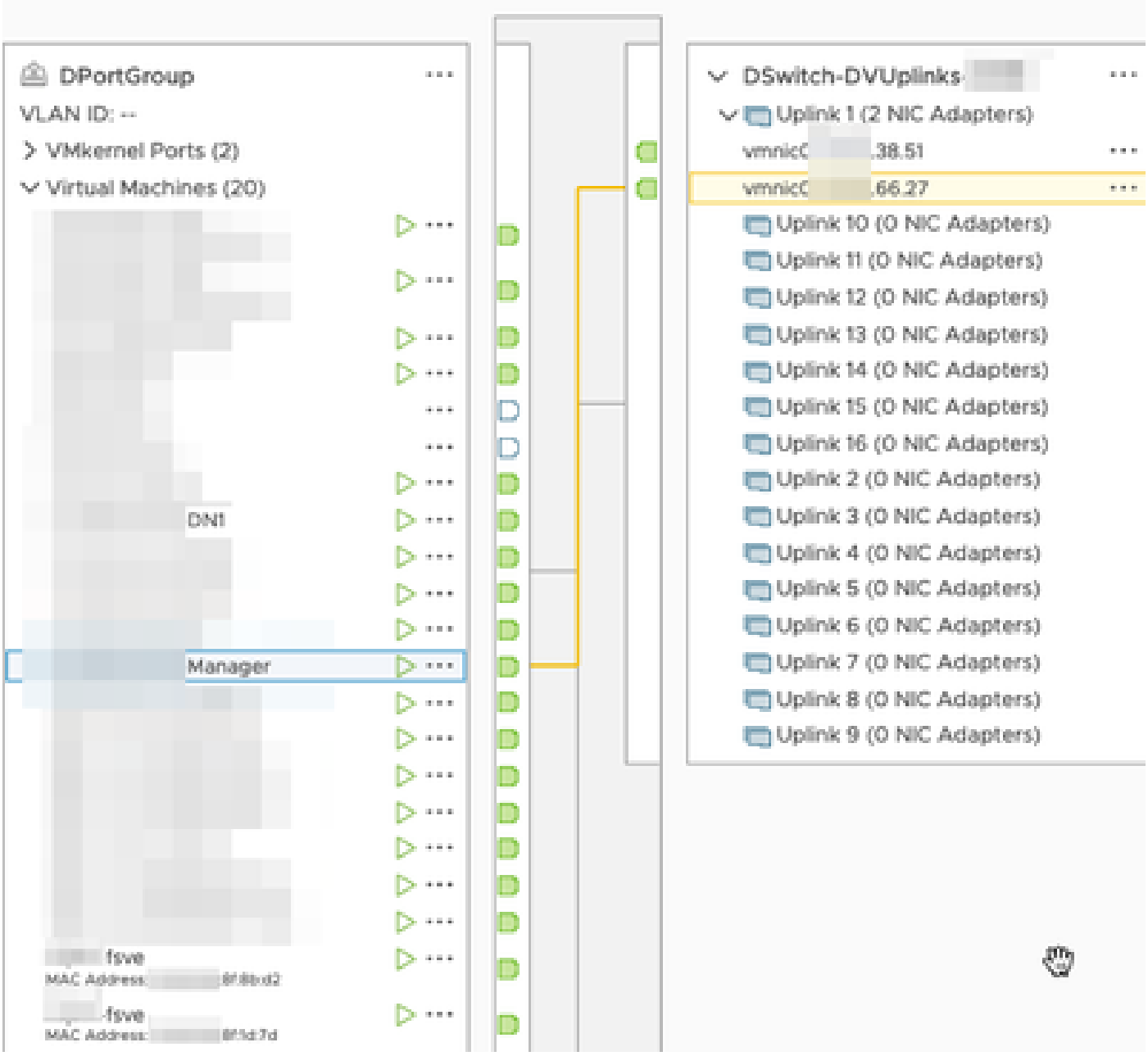


The eth0 and eth1 interfaces of the Flow Sensor is shown in the DPortGroup associated with 38.51.


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)

The eth0 interfaces of the Manager and DN1 are shown in the DPortGroup associated with 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)



Verify

From the CLI of the Flow Sensor a tcpdump is ran to show that the GRE tunnel comes up on the eth1 interface.

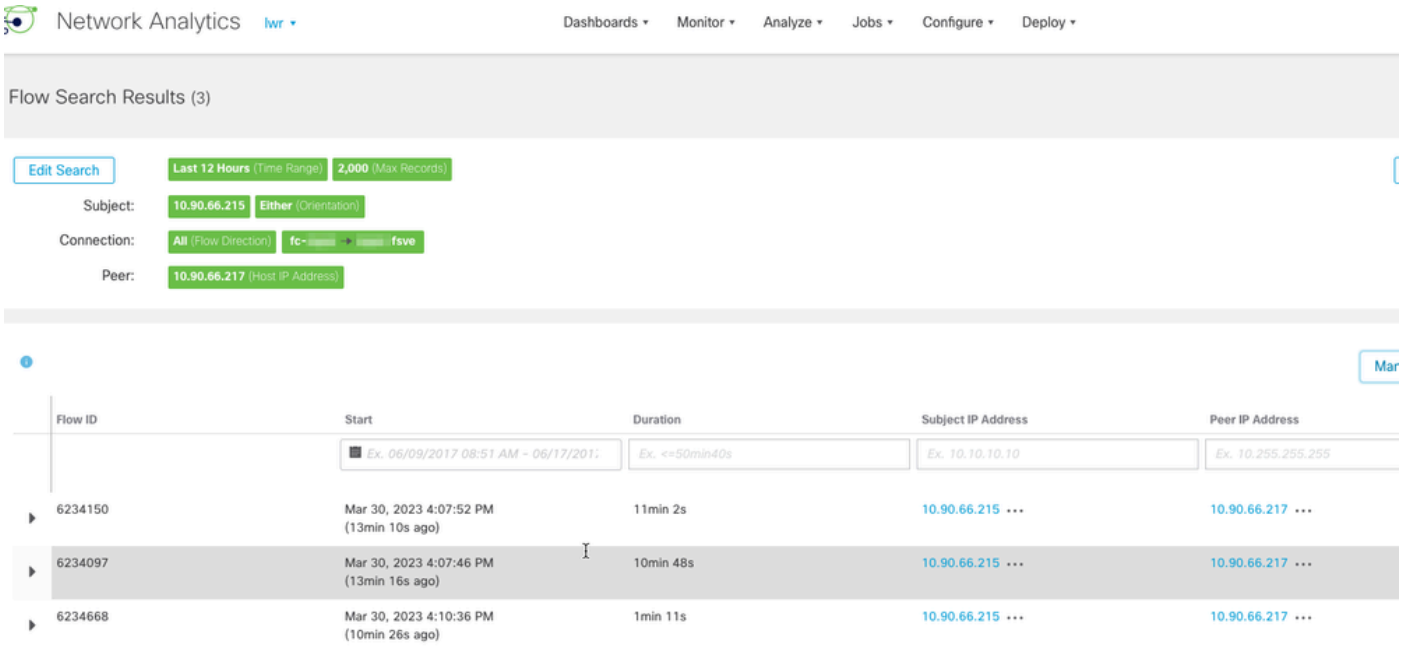
```
fsve:~# tcpdump -epnni eth1 not broadcast and not multicast -c10
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
17:43:57.080043                 >          8f:1d:7d, ethertype ARP (0x0806), length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

A flow search for the Manager and DN1 devices are ran on the SNA Manager that receives netflow from the Flow Sensor shows traffic between the Manager and 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