

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.

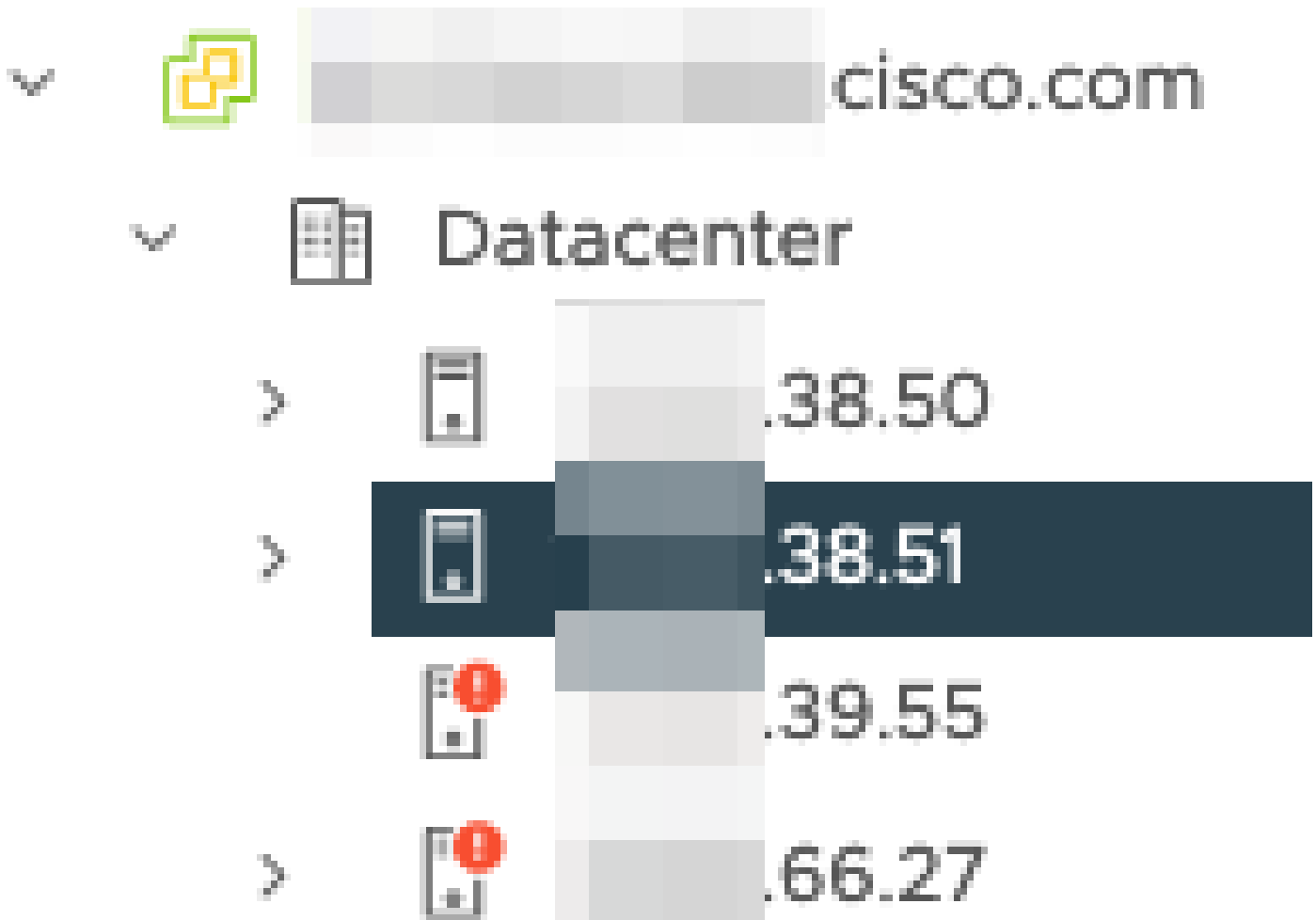
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

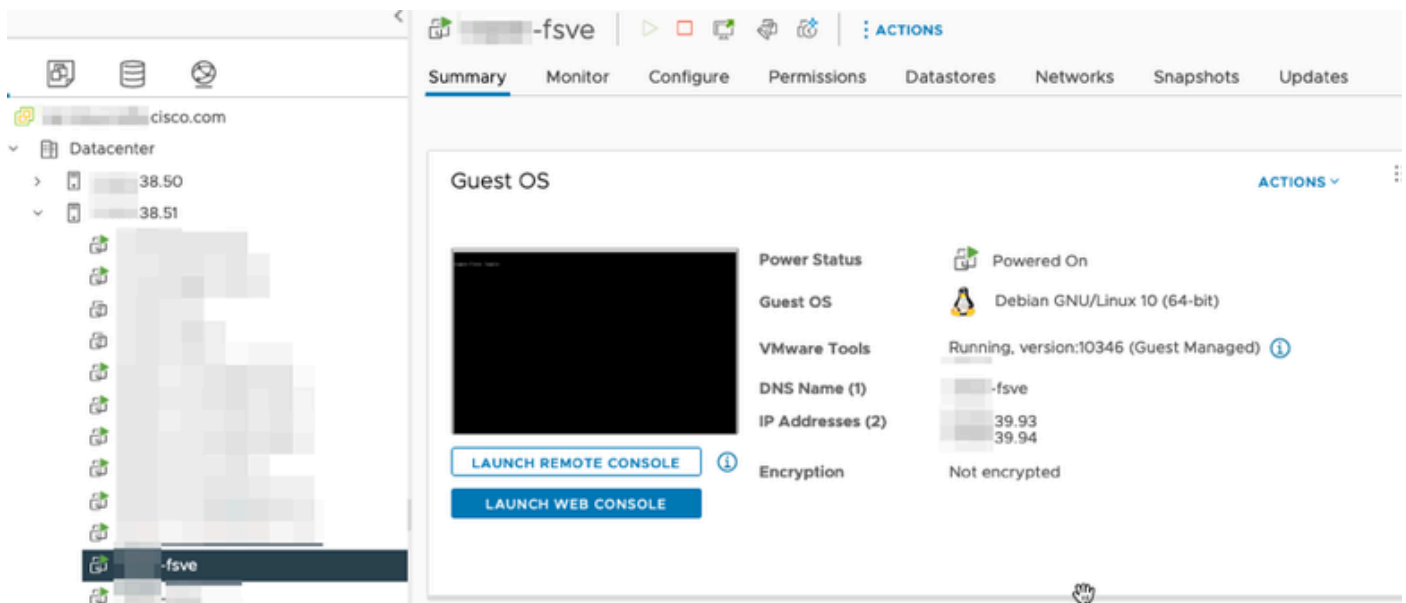
In vSphere bekijk het Datacenter voor het aantal ESXi-hosts en bepaal van welke hosts u Oost/West-verkeer wilt ophalen.

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.

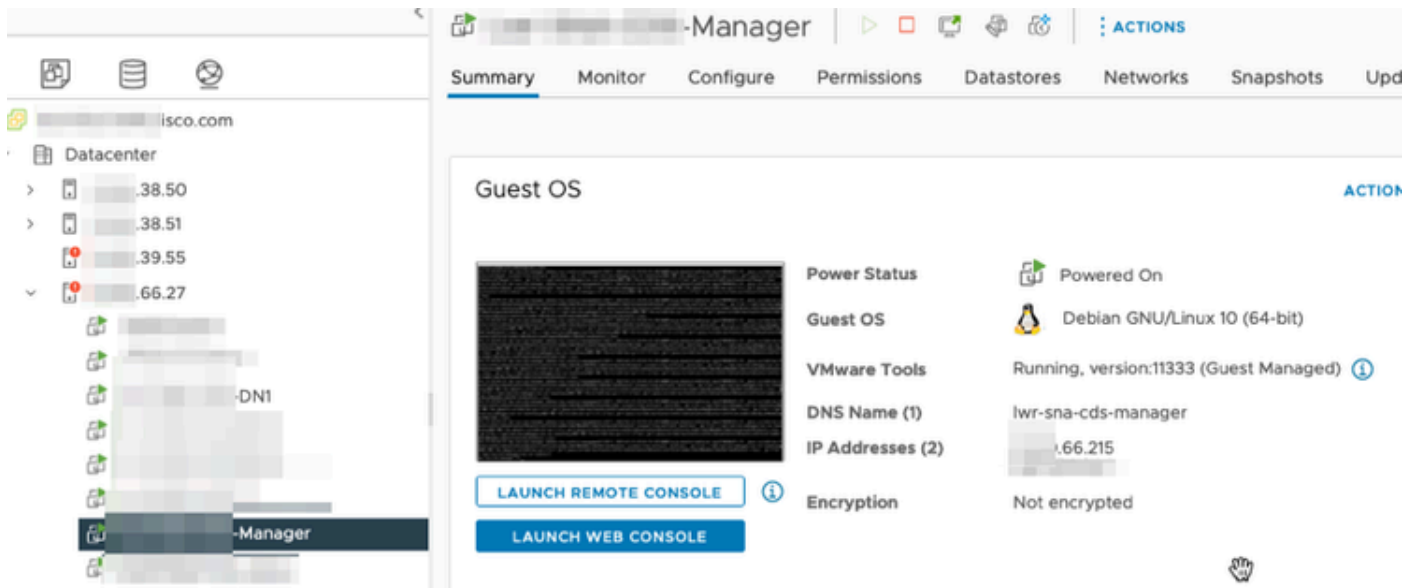
De laatste twee octetten van deze twee hosts zijn 66.215 en 66.217 voor respectievelijk de

Manager en DN1.

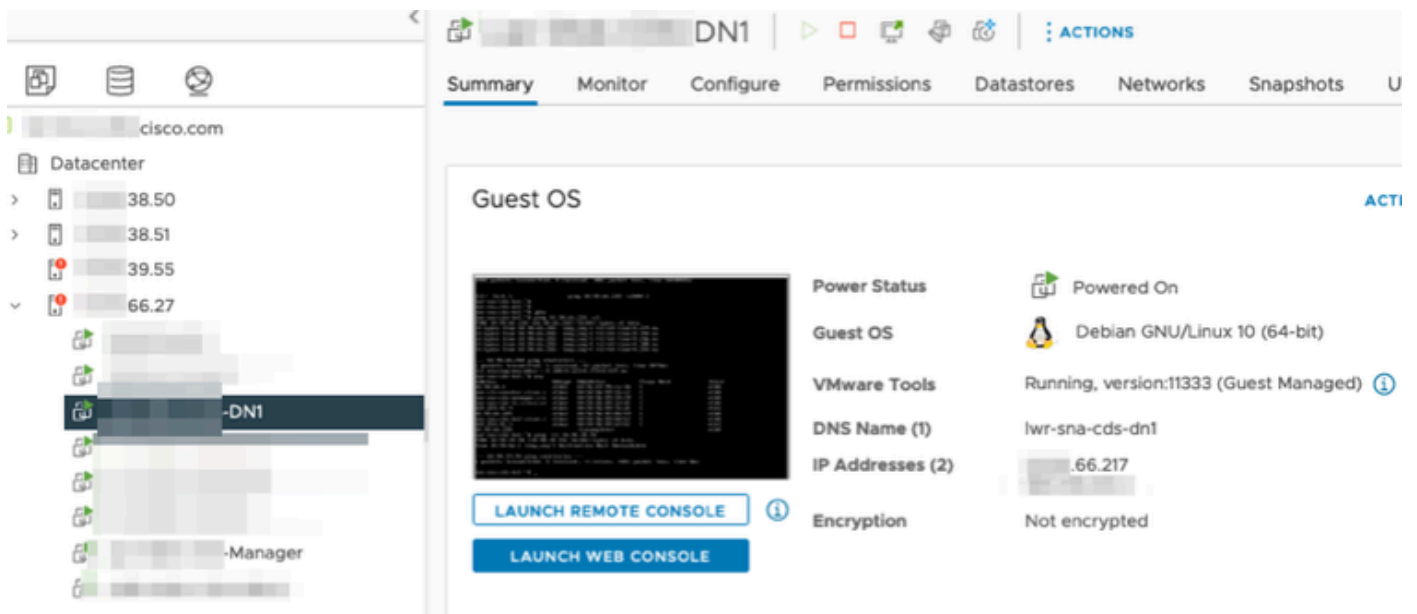
Beide hosts worden geïmplementeerd op de ESXi-host waarvan de laatste twee octetten 66.27 zijn. Dit is een andere ESXi dan de Flow Sensor wordt geïmplementeerd op.

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.



DSwitch

ACTIONS

Summary

Monitor

Configure

Permissions

Ports



Manufacturer: VMware, Inc.

Version: 6.5.0

UPGRADES AVAILABLE



DSwitch

ACTIONS

Summary

Monitor

Configure

Permissions

Ports

Hosts

VMs

Networks

<input type="checkbox"/>	Name	State	Status	Cluster
<input type="checkbox"/>	38.51	Connected	✓ Normal	
<input type="checkbox"/>	66.27	Connected	⚠ Alert	

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.

DSwitch | ACTIONS

Summary Monitor **Configure** Permissions Ports Hosts VMs Networks

Settings

- Properties
- Topology
- LACP
- Private VLAN
- NetFlow
- Port Mirroring**
- Health Check
- Resource Allocation
 - System traffic
 - Network resource pools
 - Alarm Definitions

Port Mirroring

NEW...

Session Name
ERSPANTypell

Port mirroring session: ERSPANtypell

Properties	Sources	Destinations
Session name	ERSPANTypell	
Session type	Encapsulated Remote Mirroring (L3) Source	
Encapsulation type	ERSPAN Type II	
Session ID	0	
Status	Enabled	
Mirrored packet length	--	
Sampling rate	Mirror 1 of 1 packets	

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

Edit Port Mirroring Session

DSwitch

Edit properties

Select sources

Select destinations

All ports **Selected ports (8)**

SELECT ALL CLEAR SELECTION REMOVE INGRESS EGRESS INGRESS/EGRESS

<input type="checkbox"/>	Port ID	Host	Connectee	Traffic Direction
<input type="checkbox"/>	44	66.27	Manager	Ingress/Egress
<input type="checkbox"/>	45	66.27	DN1	Ingress/Egress
<input type="checkbox"/>	46	66.27		Ingress/Egress
<input type="checkbox"/>	47	66.27		Ingress/Egress
<input type="checkbox"/>	49	66.27		Ingress/Egress
<input type="checkbox"/>	50	66.27		Ingress/Egress
<input type="checkbox"/>	51	66.27		Ingress/Egress
<input type="checkbox"/>	52	66.27		Ingress/Egress

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

Edit Port Mirroring Session

DSwitch

Edit properties

Select sources

Select destinations

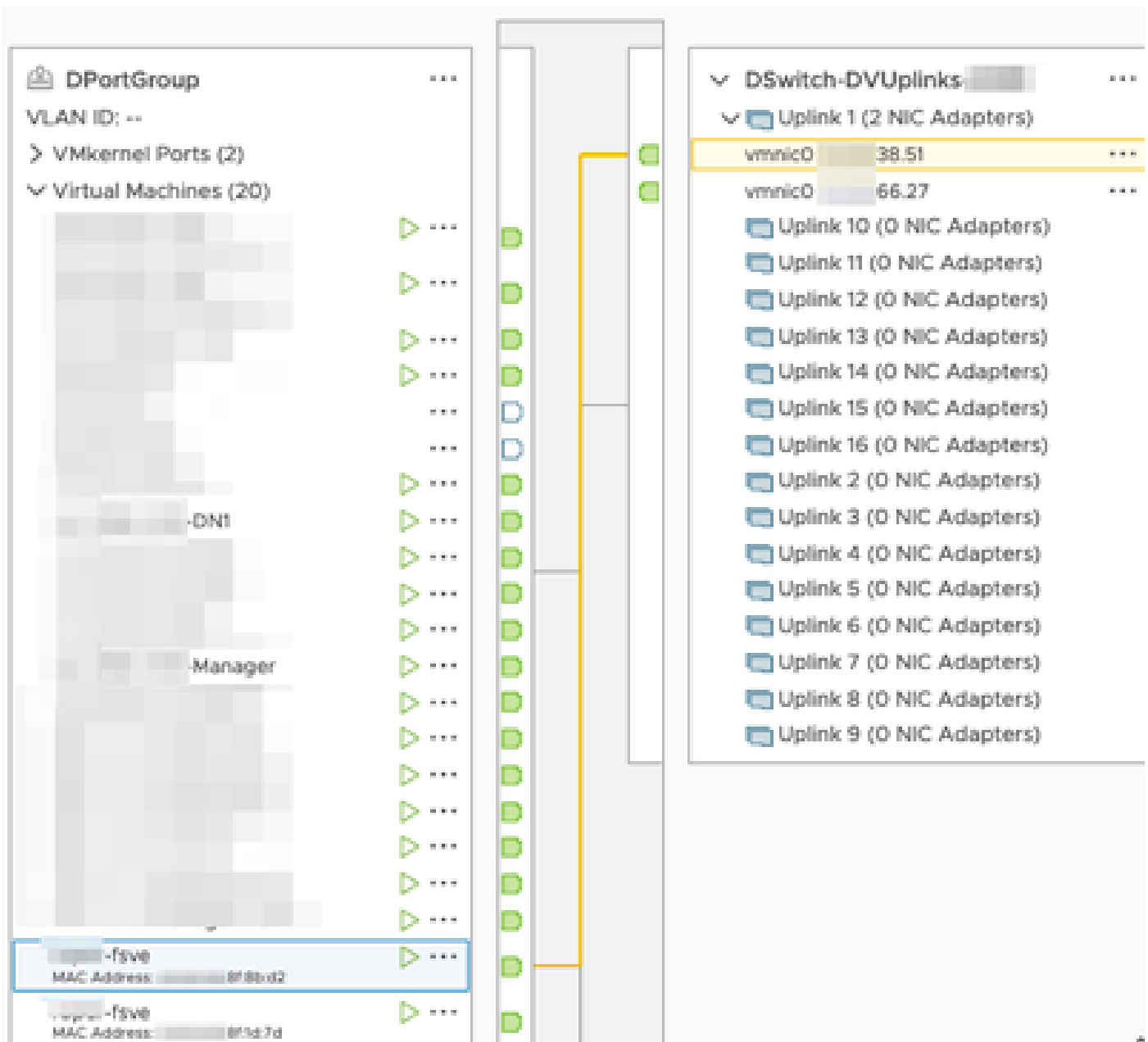
ADD REMOVE

<input type="checkbox"/>	IP address
<input type="checkbox"/>	.39.94

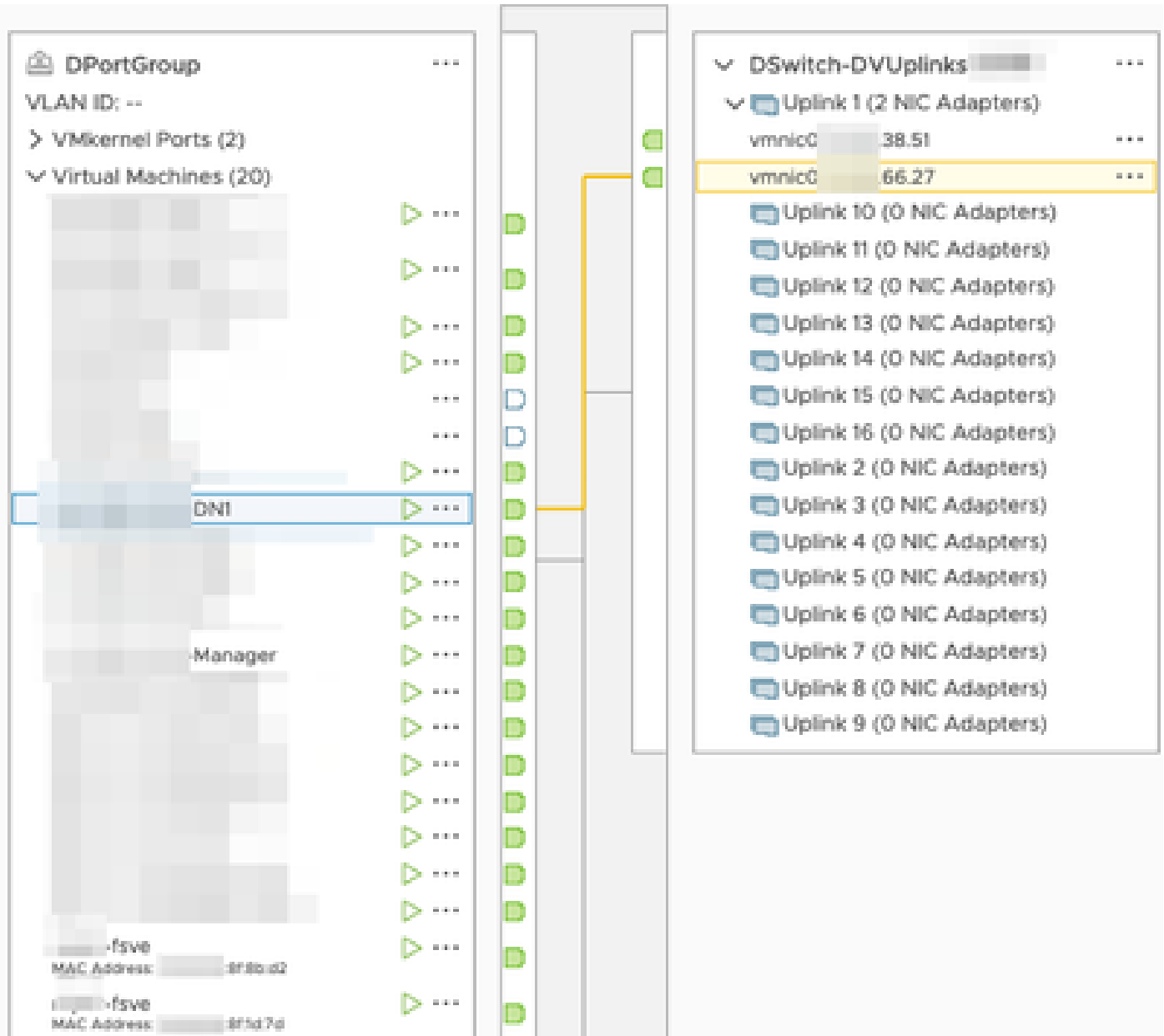
De interfaces eth0 en eth1 van de Flow Sensor worden getoond in DPortGroup geassocieerd met

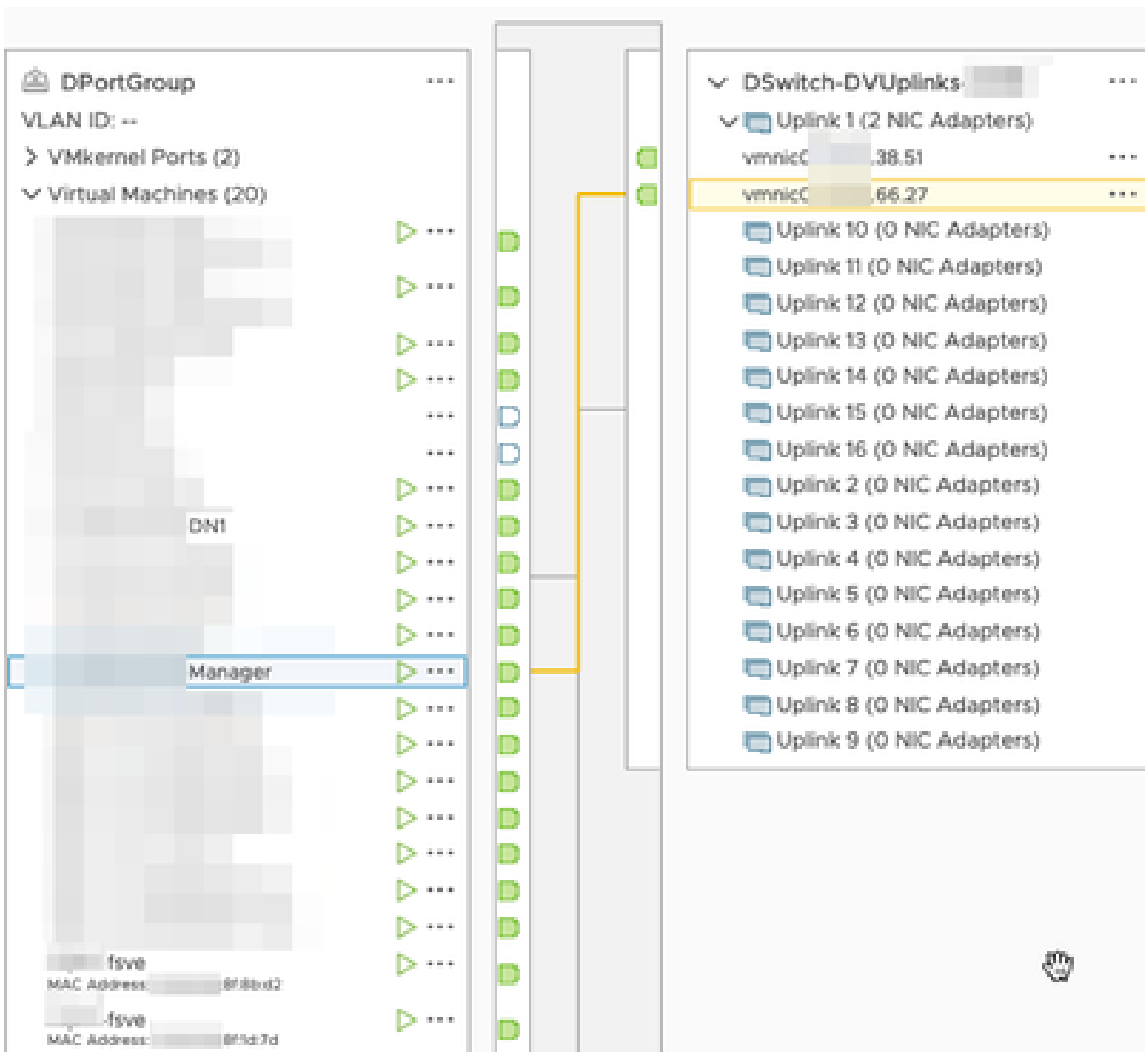
38.51.

The image shows a network management interface with two main panels. The left panel is titled "DPortGroup" and shows a configuration for "VLAN ID: --". It lists "VMkernel Ports (2)" and "Virtual Machines (20)". A list of virtual machines is shown, including "fsv0" (MAC Address: :818bd2) and "vmapr-fsv0" (MAC Address: :815d7d). The right panel is titled "DSwitch-DVUplinks-" and shows a configuration for "Uplink 1 (2 NIC Adapters)". It lists two vmnic0 interfaces: "vmnic0 .38.51" (highlighted in yellow) and "vmnic0 .66.27". Below these are 16 uplink slots, each labeled "Uplink X (0 NIC Adapters)" for X from 10 to 16 and 2 to 9. A yellow line connects the highlighted vmnic0 interface to the first uplink slot in the right panel.



De eth0 interfaces van de Manager en DN1 worden getoond in DPortGroup geassocieerd met 66.27.





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.

```

fsvs:~# 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), l
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), l
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.

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)

Flow ID	Start	Duration	Subject IP Address	Peer IP Address
	<i>Ex. 06/09/2017 08:51 AM - 06/17/2017</i>	<i>Ex. <=50min40s</i>	<i>Ex. 10.10.10.10</i>	<i>Ex. 10.255.255.255</i>
▶ 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.