# Configuración de vSphere para enviar tráfico horizontal a FlowSensor

## Contenido

## Introducción

Este documento describe cómo configurar vSphere para que el tráfico horizontal se pueda enviar al sensor de flujo de Secure Network Analytics

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- VMware vSphere
- Secure Network Analytics (SNA)

#### **Componentes Utilizados**

Versión 7.0.3 de VMware vSphere.

Secure Network Analytics versión 7.4.2.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Configurar

En vSphere, revise el Data Center para ver el número de hosts ESXi y determine de qué hosts desea recopilar tráfico horizontal.

En esta imagen, de los cuatro hosts, solo dos son de discutido cuyos últimos dos octetos son 38.51, y 66.27.

El host ESXi 38.51 ejecuta la versión 7.0.3 y el host ESXi 6.27 ejecuta la versión 6.7.0.



Se ha implementado un sensor de flujo SNA versión 7.4.2 en el host 38.51 ESXi, que se ha configurado con dos direcciones IP con los últimos octetos de 39.93 y 39.94.

<	🗟 🛛 -fsve 🗠 🗆 😭	🖗 🐯 🕴 Аст	TIONS	
ð e 👳	Summary Monitor Configure	Permissions	Datastores Networks Snapshots	Updates
@ cisco.com				
✓  ☐ Datacenter				
> 🕄 38.50	Guest OS			ACTIONS Y
~ 🗓 38.51				
6		Deuros Status		
8	and the second	Power Status	D Powered On	
(D)		Guest OS	Debian GNU/Linux 10 (64-bit)	
80		VMware Tools	Running, version:10346 (Guest Manage	d) (j)
8				
8		DNS Name (1)	-fsve	
8		IP Addresses (2)	39.93 39.94	
8	LAUNCH REMOTE CONSOLE	Encryption	Not encrypted	
8	LAUNCH WEB CONSOLE			
8				
ලි -fsve				
æ			8	

Hay otros dos dispositivos, un Administrador SNA y un Nodo de datos denominados Administrador y DN1 respectivamente.

Los dos últimos octetos de estos dos hosts son 66.215 y 66.217 para el Administrador y DN1

respectivamente.

Ambos hosts están implementados en el host ESXi cuyos dos últimos octetos son 66.27. Se trata de un ESXi diferente del que utiliza el Flow Sensor.

El tráfico entre el administrador y el host DN1 no se ve fuera del switch proxy en el host 66.27 ESXi.

El Administrador SNA:



#### Configuraciones

Cree un switch distribuido de la versión 6.5.0 llamado DSwitch y un grupo de puertos distribuidos llamado DPortGroup.



Las máquinas virtuales y los dos enlaces ascendentes para los hosts de ESXi se agregaron al grupo de puertos distribuidos en el DSwitch.



En DSwitch, configure una sesión de duplicación ERSPAN de tipo II.

DSwitch ACTIONS							
Summary Monitor	Configure Permissions Ports Hosts VMs Networks						
Settings V Properties Topology	Port Mirroring						
LACP Private VLAN NetFlow	Session Name	Ŧ	Port mirroring ses	ssion: ERSPANtypell			
Port Mirroring Health Check Resource Allocation	ERSPANtypell	~	Session name Session type	ERSPANtypell Encapsulated Remote Mirroring (L3) Source ERSPAN Type II			
System traffic Network resource pools Alarm Definitions		Ð	Session ID Status Mirrored packet length Sampling rate	0 Enabled			

Para la sesión de duplicación de puertos, se han seleccionado todos los hosts de los hosts 66.27 ESXi (incluidos el administrador y DN1).

Edit Port Mirroring Session	DSwitc	h					×
Edit properties	All ports	Selected ports (8)					
Select sources	SELECT ALL	CLEAR SELECTION	REMOVE	INGRESS EGRESS	INGRESS/EGRESS		
Select destinations	Port ID	T Hos	t	T Connectee		Traffic Direction	Ŧ
	44		.66.27	<b>a</b>	Manager	⑤ Ingress/Egress	
	45	٦	.66.27	æ -	-DN1	⑤ Ingress/Egress	
	46	Ξ	.66.27	æ		<ol> <li>Ingress/Egress</li> </ol>	
	47		.66.27	æ		<ol> <li>Ingress/Egress</li> </ol>	
	49		.66.27	8		Ingress/Egress	
	50	٦	.66.27	æ		<ol> <li>Ingress/Egress</li> </ol>	
	51	٦	.66.27	8		<ol> <li>Ingress/Egress</li> </ol>	
	52		.66.27	8		<ol> <li>Ingress/E<sup>m</sup>yess</li> </ol>	

Para el destino, establézcalo en la IP de la interfaz eth1 en el Flow Sensor, 39.94.

Edit Port Mirroring Session	DSwitch				
Edit properties	ADD REMOVE				
Select sources	IP address				
Select destinations	.39.94				

Las interfaces eth0 y eth1 del Flow Sensor se muestran en el DPortGroup asociado con 38.51.





Las interfaces eth0 del Manager y DN1 se muestran en el DPortGroup asociado con 66.27.

DPortGroup			V DSwitch-DVUplinks
VLAN ID:			v m Uplink 1 (2 NIC Adapters)
> VMkernel Ports (2)			vmnic0 38.51 ····
Virtual Machines (20)			vmnic0 66.27 ····
	⊳…		Uplink 10 (0 NIC Adapters)
			Uplink 11 (O NIC Adapters)
	Þ	D	Uplink 12 (0 NIC Adapters)
	Þ	D	Uplink 13 (0 NIC Adapters)
	Þ ····	D	Uplink 14 (0 NIC Adapters)
		D	Uplink 15 (0 NIC Adapters)
		D	Uplink 16 (0 NIC Adapters)
	⊳ …	D	Uplink 2 (0 NIC Adapters)
DNI	⊳…	D-	Uplink 3 (0 NIC Adapters)
	⊳…	D	Uplink 4 (0 NIC Adapters)
	D ····	D	Uplink 5 (0 NIC Adapters)
	> …	D	Uplink 6 (0 NIC Adapters)
-Manager	⊳ …	D	Uplink 7 (0 NIC Adapters)
	> …	D	Uplink 8 (0 NIC Adapters)
	⊳…	D	Uplink 9 (0 NIC Adapters)
	⊳…	D	
	> …	D	
	⊳ …	D	
	⊳ …	D	
	⊳ …	D	
-fsve MAC Astress: 8180-02	⊳…	D	
MAC Address 871d.7d	⊳…	D	



## Verificación

Desde la CLI del Flow Sensor se ejecuta un tcpdump para mostrar que el túnel GRE aparece en la interfaz eth1.

fsve:~# tcpdump -epnni ethl not broadcast and not multicast -c10												
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode												
listening on ethl, link-type EN10MB (Ethernet), capture size 262144 bytes												
17:43:57.080043	>		8f:1d:7d,	ethertype ARP	(0x0806),	length 60	D: Request	who-has	39.94	8f:1d:70	i) tell 0.0.0.0,	length 46
17:43:57.080066	. >		48:16:21,	ethertype ARP	(0x0806),	length 42	2: Reply	39.94	is-at (	8f:1d:7d, ler	igth 28	
17:44:06.728457	>		8f:1d:7d,	ethertype IPv	4 (0x0800),	, length 1	102:	.66.27 >	.39.94:	GREv0, key=0x2000	000, proto TEB	(0x6558), ]
17:44:06.728474	95:ca:4e >		8f:1d:7d,	ethertype IPv	4 (0x0800)	, length 1	102:	66.27 >	.39.94:	GREv0, key=0x2000	0000, proto TEB	(0x6558), ]
17:44:06.728475	95:ca:4e >		8f:1d:7d,	ethertype IPv	4 (0x0800)	, length 1	102:	.66.27 >	.39.94:	GREv0, key=0x0, p	roto TEB (0x655	8), length
and the second se												
17:44:06.728477	95:ca:4e >		8f:1d:7d,	ethertype IPv	4 (0x0800),	, length 1	102:	.66.277 >	.39.94:	GREv0, key=0x0, p	roto TEB (0x655	8), length
and the second se								2				

Se ejecuta una búsqueda de flujo para el administrador y los dispositivos DN1 en el administrador SNA que recibe netflow del Flow Sensor y muestra el tráfico entre el administrador y el host DN1.

Ō	Network Analytics INF • D			Dashboards •	Monitor +	Analyze -	Jobs +	Configure *	Deploy -		
Flow	/ Search Res	ults (3)									
Edi	it Search Subject:	Last 12 Hours (Time Range) 10.90.66.215 Either (Orienta	2,000 (Max Records)								(
	Connection: Peer:	All (Flow Direction) fc-	+ fsve								
0											Mar
	Flow ID		Start	Dur	ration			Subject IP Addr	355	Peer IP Address	
			Ex. 06/09/2017 08:51 AM - 06/1								
•	6234150		Mar 30, 2023 4:07:52 PM (13min 10s ago)	111	nin 2s			10.90.66.215 •		10.90.66.217 •••	
•	6234097		Mar 30, 2023 4:07:46 PM (13min 16s ago)	1 10r	min 48s			10.90.66.215 •		10.90.66.217 •••	

1min 11s

10.90.66.215 •••

10.90.66.217 •••

Mar 30, 2023 4:10:36 PM (10min 26s ago)

6234668

#### Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).