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.

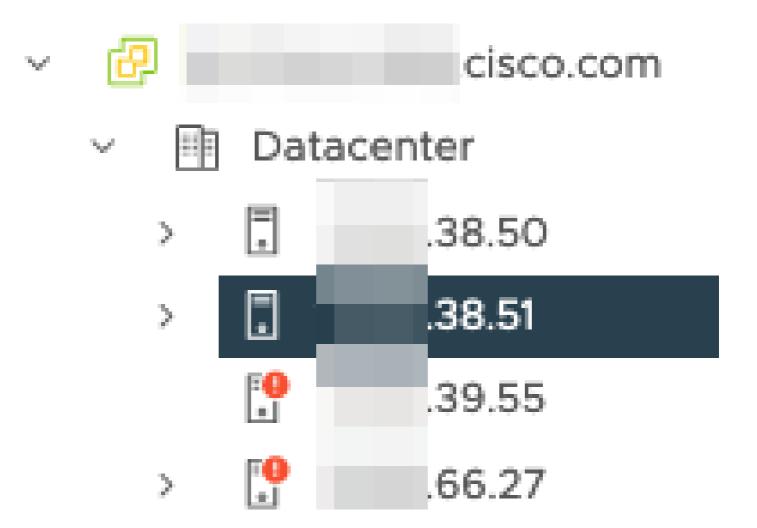
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

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.

<	al -fsve 🛛 🖓 🖬	🗇 🐯 🔜	CTIONS	
ð e Q	Summary Monitor Configure	Permissions	Datastores Networks Snapshot	ts Updates
@ cisco.com				
✓				
> 38.50	Guest OS			ACTIONS
~ 🕄 38.51				
6		Power Status	Powered On	
8	ages from the second	Power Status		
(J)		Guest OS	Debian GNU/Linux 10 (64-bit)	
æ		VMware Tools	Running, version:10346 (Guest Mana	ged) 🕦
3		DNS Name (1)	-fsve	
8				
8		IP Addresses (2)	39.93 39.94	
8	LAUNCH REMOTE CONSOLE	Encryption	Not encrypted	
8	LAUNCH WEB CONSOLE			
8				
යි -fsve				
<i>ä</i>			8	

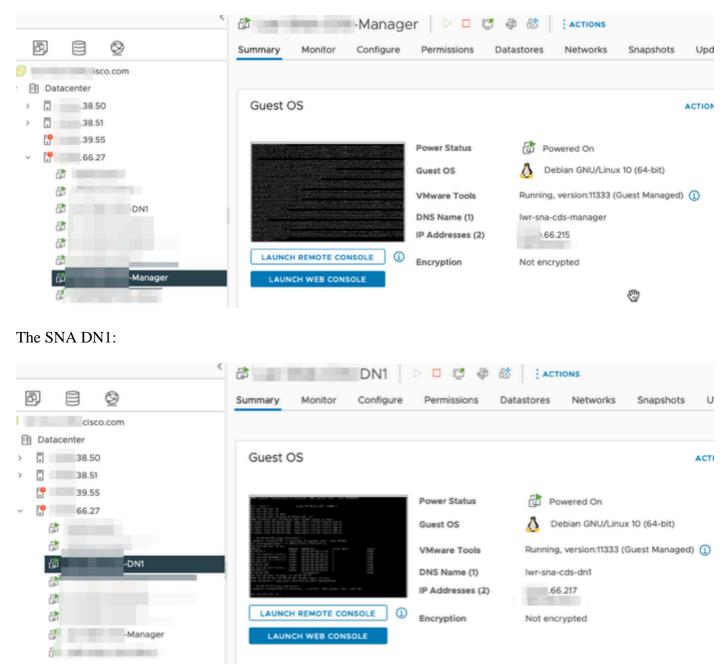
There are two other devices, an SNA Manager and Data Node called Manager and DN1 respectively. The last two octets of these two hosts are 66.215 and 66.217 for the Manager and DN1 respectively.

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.

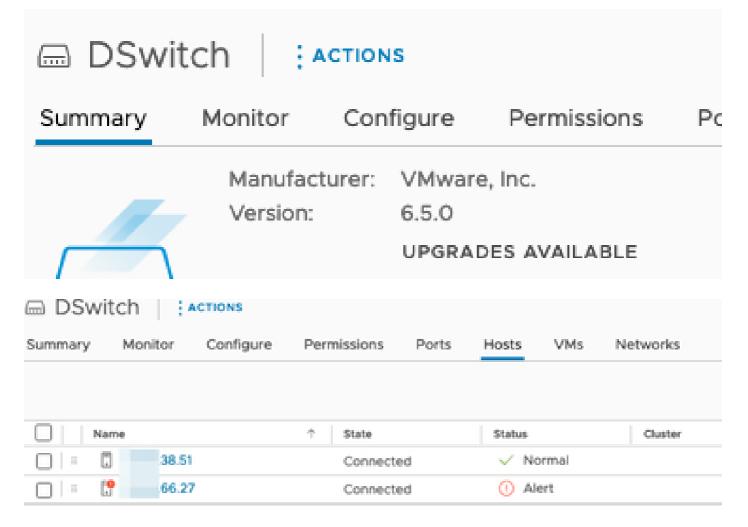
Traffic between the Manager and DN1 host is not seen outside of the proxy switch on the 66.27 ESXi host.





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.

DSwitch EACTIONS								
Summary Monitor	Configure Permissions Ports Hosts VMs Networks							
Settings 🗸	Port Mirroring							
Properties Topology	NEW							
LACP	Session Name	Ŧ	Port mirroring see	ssion: ERSPANtypell				
Private VLAN NetFlow	: »		Properties Sources	Destinations				
Port Mirroring Health Check	ERSPANtypell		Session name	ERSPANtypell				
Resource Allocation \sim	: »		Session type Encapsulation type	Encapsulated Remote Mirroring (L3) Source ERSPAN Type II				
System traffic Network resource pools		_	Session ID	0				
Alarm Definitions		٢	Status Mirrored packet length	Enabled				
			Sampling rate	Mirror 1 of 1 packets				

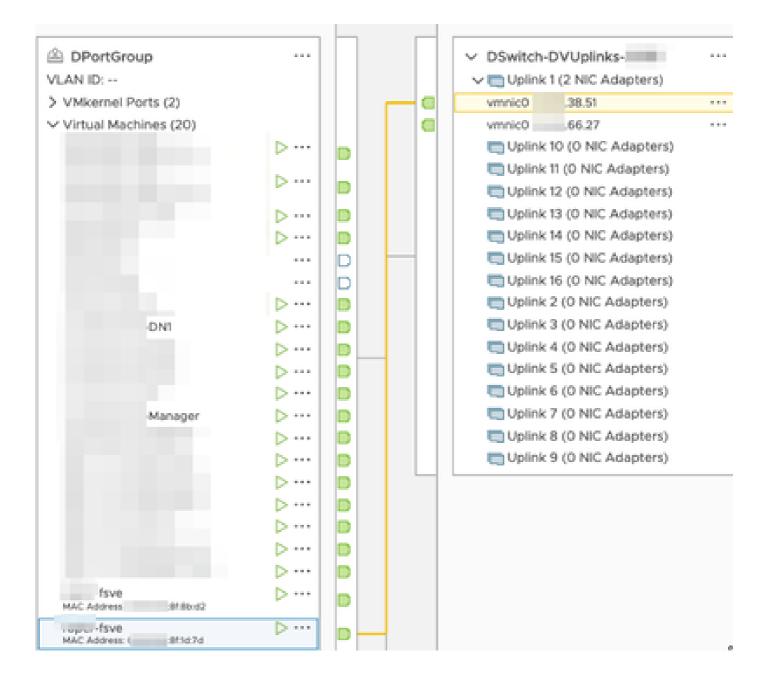
For the Port mirroring session, all hosts on the 66.27 ESXi hosts (including the Manager and DN1) were selected.

Edit Port Mirroring Session	DSwitch						
Edit properties	All ports	selected ports (8)					
Select sources	SELECT ALL	CLEAR SELECTION	REMOVE	INGRESS EGRESS	INGRESS/EGRESS		
Select destinations	Port ID	¥ Host		T Connectee		Traffic Direction	т
	44		.66.27	a I	Manager	⑤ Ingress/Egres	is
	45		.66.27	a 1	-DN1) Ingress/Egres	is
	46	5	.66.27	æ		인 Ingress/Egres	is
	47		.66.27	æ		Ingress/Egres	is
	49		66.27	æ		티 Ingress/Egres	is
	50		66.27	æ		Ingress/Egres	is
	51		.66.27	æ		된 Ingress/Egres	s
	52	J	.66.27	æ		 Ingress/Egges 	is

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

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

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





The eth0 interfaces of the Manager and DN1 are shown in the DPortGroup associated with 66.27.

DPortGroup					V DSwitch	-DVUplinks	
VLAN ID:					V 📺 Uplink	1 (2 NIC Adapters)	
> VMkernel Ports (2)					vmnicC	.38.51	
Virtual Machines (20)					vmnic0	66.27	
	⊳…				C Uplink	10 (0 NIC Adapters)	
	D				C Uplink	11 (O NIC Adapters)	
	P				C Uplink	12 (0 NIC Adapters)	
	Þ	D			C Uplink	: 13 (0 NIC Adapters)	
	⊳…	D			C Uplink	: 14 (0 NIC Adapters)	
		D			C Uplink	15 (0 NIC Adapters)	
		D			C Uplink	16 (0 NIC Adapters)	
	⊳…	D			C Uplink	2 (0 NIC Adapters)	
DNI	⊳…		_		C Uplink	3 (0 NIC Adapters)	
	⊳…	D			C Uplink	4 (0 NIC Adapters)	
	⊳…	D			C Uplink	5 (0 NIC Adapters)	
	⊳…	D			C Uplink	6 (0 NIC Adapters)	
-Manager	⊳…	D			C Uplink	7 (0 NIC Adapters)	
	⊳…	D			C Uplink	8 (0 NIC Adapters)	
	⊳…	D			C Uplink	9 (0 NIC Adapters)	
	⊳…	D		·			
	⊳…	D					
	⊳…	D					
	⊳…	D					
	⊳…	D					
-fsve MAC Address - 8780.02	⊳…	D					
-fsve MAC ASSess 875474	⊳…						



Verify

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

fave:~# tondu	mp -epppi ethl not broadc	sast and not multicast -cl0							
	fsve:~≢ tcpdump -epnni ethl not broadcast and not multicast -cl0 tcpdump: verbose output suppressed, use -v or -vv for full protocol decode								
listening on ethl,	link-type EN10MB (Etherne	t), capture size 262144 bytes							
17:43:57.080043	>	8f:ld:7d, ethertype ARP (0x0806), length 60: Request who-has 39.94 8f:ld:7d) tell 0.0.0.0, leng	gth 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:ld:7d, ethertype IPv4 (0x0800), length 102: .66.27 > .39.94: GREv0, key=0x2000000, proto TEB (0x65	558), 1						
17:44:06.728474	95:ca:4e >	8f:ld:7d, ethertype IPv4 (0x0800), length 102: 66.27 > .39.94: GREv0, key=0x2000000, proto TEB (0x65	558), 1						
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), 1	length						
		The second se							
17:44:06.728477	95:ca:4e >		length						
		8f:1d:7d, ethertype IPv4 (0x0800), length 102: .66.3 .39.94: GREv0, key=0x0, proto TEB (0x6558), 1							

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.

Ţ	Network Analytics Iwr -	Dashb	oards • Monitor •	Analyze - Jobs	 Configure • 	Deploy •		
Flow	Search Results (3)							
	Search Last 12 Hours (Time Range) Subject: 10.90.66.215 Connection: All (Flow Direction) Peer: 10.90.66.217 (Host IP Address)							(
0								Mar
	Flow ID	Start	Duration		Subject IP Addr	255	Peer IP Address	
		Ex. 06/09/2017 08:51 AM - 06/17/201;						
•	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 •••	

1min 11s

10.90.66.215 •••

10.90.66.217 •••

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

6234668