IPS 5.X y later/IDSM2: Modo en línea de los pares del VLA N usando el ejemplo de configuración CLI y IDM

Contenido

Introducción prerrequisitos Requisitos Componentes Utilizados Productos Relacionados Convenciones Configuración de la captura VACL Configuración de modo en línea de los pares del VLA N Configuración de CLI Configuración IDM Troubleshooting Información Relacionada

Introducción

La asociación de VLAN por pares en una interfaz física se conoce como modo de pares VLAN en línea. Los paquetes recibidos en uno de los VLAN emparejados se analizan y se reenvían al otro VLAN en la pareja. Los pares en línea del VLA N se soportan en todos los sensores que sean compatibles con el Sistema de prevención de intrusiones (IPS) 5.1, excepto NM-CIDS, AIP-SSM-10, y AIP-SSM-20.

El modo en línea de los pares del VLA N es un modo de detección activo donde una interfaz de detección actúa como puerto de tronco 802.1q, y el sensor realiza el VLAN Bridging entre los pares de VLA N en el trunk. Esto significa que el Switch conectado con la interfaz de detección debe estar en el modo tronco.

El sensor examina el tráfico que recibe en cada VLA N en cada par, y puede adelante los paquetes en el otro VLA N en los pares o caer el paquete si se detecta una tentativa de la intrusión. Usted puede configurar un sensor IPS para interligar simultáneamente hasta 255 pares del VLA N en cada interfaz de detección. El sensor substituye el campo VLAN ID en la encabezado 802.1q de cada paquete recibido por el ID del VLA N de la salida en el cual el sensor adelante el paquete. El sensor cae todos los paquetes recibidos en cualquier VLA N que no se asigne a los pares en línea del VLA N.

Nota: Para el IPS-4260, puente fracaso-abierto del hardware no se soporta en los pares en línea del VLA N. Refiera a las <u>restricciones de configuración de puente del hardware</u> para más información.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en el sensor de Cisco Intrusion Prevention System que utiliza los 5.1 y posterior.

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Productos Relacionados

La información en este documento es también aplicable al Módulo de servicios del sistema de la detección de intrusos (IDSM-2).

Convenciones

Consulte <u>Convenciones de Consejos TécnicosCisco</u> para obtener más información sobre las convenciones del documento.

El VACL captura la configuración

Refiera a la sección de la <u>captura VACL que configura de</u> <u>configurar el IDSM-2</u> para enviar el tráfico al IDSM en el Switch.

Configuración de modo en línea de los pares del VLA N

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta <u>Command Lookup Tool</u> (<u>clientes registrados solamente</u>) para obtener más información sobre los comandos utilizados en esta sección.

Utilice el comando del **interface_name de las interfaces físicas** en el submode de la interfaz del servicio para configurar los pares en línea del VLA N usando el CLI. El nombre de la interfaz es FastEthernet o gigabitethernet.

Estas opciones se aplican:

 Estado del administrador {habilitado | discapacitado} — el estado administrativo del link de la interfaz, si la interfaz está habilitada o inhabilitada.Nota: En todo el backplane que detecta las interfaces en todos los módulos (IDSM-2 NM-CIDS, y AIP-SSM), fijan a habilitado y se protegen al Estado del administrador (usted no puede cambiar la configuración). El Estado del administrador no tiene ningún efecto (y se protege) sobre el comando y la interfaz de control. Afecta solamente a detectar las interfaces. El comando y la interfaz de control no necesita ser habilitado porque no puede ser monitoreada.

- valor por defecto Fija el valor de nuevo a la configuración de valor predeterminado del sistema.
- descripción Su descripción de los pares en línea de la interfaz.
- duplex La configuración dúplex de la interfaz.auto Fija la interfaz al auto negocian el duplex.Conjuntos completos la interfaz por completo - al duplex.medio — Fija la interfaz al half duplex.Nota: La opción dúplex se protege en todos los módulos.
- no Quita una configuración de la entrada o de la selección.
- velocidad La configuración de la velocidad de la interfaz.auto Fija la interfaz al auto negocian la velocidad.10 Fija la interfaz al 10 MB (para las interfaces TX solamente).100 Fija la interfaz al 100 MB (para las interfaces TX solamente).1000 Fija la interfaz a 1 GB (para las interfaces Gigabit)Nota: La opción de la velocidad se protege en todos los módulos.
- subinterfaz-tipo Especifica que la interfaz es una subinterfaz y definen a qué tipo de subinterfaz.en línea-VLAN-pares — Le deja definir la subinterfaz como par en línea del VLA N.ningunos — Ningunas subinterfaces definidas.
- subinterfaz Define la subinterfaz como par en línea del VLA N.vlan1 El primer VLA N en los pares en línea del VLA N.vlan2 — El segundo VLA N en los pares en línea del VLA N.

Configuración de CLI

Complete estos pasos para configurar las configuraciones en línea de los pares del VLA N en el sensor usando el CLI:

- 1. Inicie sesión al CLI usando una cuenta con los privilegios de administrador.
- 2. Ingrese el submode de la interfaz: sensor#configure terminal sensor(config)#service interface sensor(config-int)#
- 3. Verifique si existen algunas interfaces en línea (el tipo de la subinterfaz no debe leer "ninguno" si no se ha configurado ningunas interfaces en línea):

```
sensor(config-int)#show settings
 physical-interfaces (min: 0, max: 999999999, current: 2)
 _____
   <protected entry>
   name: GigabitEthernet0/0 <defaulted>
   _____
    media-type: tx <protected>
    description: <defaulted>
    admin-state: disabled <protected>
    duplex: auto <defaulted>
    speed: auto <defaulted>
    alt-tcp-reset-interface
     _____
      none
      _____
      _____
     _____
     subinterface-type
     _____
      none
      _____
```

```
-----
   _____
  _____
<protected entry>
  name: GigabitEthernet0/1 <defaulted>
  _____
   media-type: tx <protected>
   description: <defaulted>
   admin-state: disabled <defaulted>
   duplex: auto <defaulted>
   speed: auto <defaulted>
   alt-tcp-reset-interface
   _____
    none
     -----
     _____
   _____
   subinterface-type
   _____
    none
     _____
     _____
     -----
  _____
  <protected entry>
  name: GigabitEthernet0/2 <defaulted>
  _____
   media-type: tx <protected>
   description: <defaulted>
   admin-state: disabled <defaulted>
   duplex: auto <defaulted>
   speed: auto <defaulted>
   alt-tcp-reset-interface
   _____
    none
     _____
     _____
   -----
   subinterface-type
   _____
    none
     _____
     _____
   _____
  _____
  <protected entry>
  name: GigabitEthernet0/3 <defaulted>
  -----
   media-type: tx <protected>
   description: <defaulted>
   admin-state: disabled <defaulted>
   duplex: auto <defaulted>
   speed: auto <defaulted>
   alt-tcp-reset-interface
   _____
    none
     _____
     _____
     _____
   subinterface-type
   _____
     none
     _____
     _____
```

_____ <protected entry> name: Management0/0 <defaulted> _____ media-type: tx <protected> description: <defaulted> admin-state: disabled <protected> duplex: auto <defaulted> speed: auto <defaulted> alt-tcp-reset-interface _____ none _____ _____ _____ subinterface-type _____ none _____ _____ _____ _____ _____ command-control: Management0/0 <protected> inline-interfaces (min: 0, max: 999999999, current: 0) _____ _____ bypass-mode: auto <defaulted> interface-notifications _____ missed-percentage-threshold: 0 percent <defaulted> notification-interval: 30 seconds <defaulted> idle-interface-delay: 30 seconds <defaulted> _____

sensor(config-int)#

4. Quite cualquier interfaz en línea que utilice esta interfaz física: sensor(config-int)#no inline-interfaces interface_name

5. Visualice la lista de interfaces disponibles:

```
sensor(config-int)#physical-interfaces ?
GigabitEthernet0/0 GigabitEthernet0/0 physical interface.
GigabitEthernet0/1 GigabitEthernet0/1 physical interface.
GigabitEthernet0/2 GigabitEthernet0/2 physical interface.
GigabitEthernet0/3 GigabitEthernet0/3 physical interface.
Management0/0 Management0/0 physical interface.
sensor(config-int)#physical-interfaces
```

6. Especifique una interfaz:

sensor(config-int)#physical-interfaces GigabitEthernet0/2

7. Habilite al Estado del administrador de la interfaz: sensor(config-int-phy)#admin-state enabled

La interfaz se debe asignar al sensor virtual y habilitar para monitorear el tráfico.

- 8. Agregue una descripción de esta interfaz: sensor(config-int-phy)#description INT1
- 9. Configure las configuraciones dúplex: sensor(config-int-phy)#duplex full

Esta opción no está disponible en los módulos.

10. Configure la velocidad:

sensor(config-int-phy)#speed 1000

Esta opción no está disponible en los módulos.

11. Configure los pares en línea del VLA N:

```
sensor(config-int-phy)#subinterface-type inline-vlan-pair
sensor(config-int-phy-inl)#subinterface 1
sensor(config-int-phy-inl-sub)#vlan1 52
sensor(config-int-phy-inl-sub)#vlan2 53
```

- 12. Agregue una descripción para los pares en línea del VLA N: sensor(config-int-phy-inl-sub)#description pairs vlans 52 and 53
- 13. Verifique las configuraciones en línea de los pares del VLA N:

```
sensor(config-int-phy-inl-sub)#show settings
subinterface-number: 1
```

```
description: VLANpair1 default:
vlan1: 52
vlan2: 53
```

sensor(config-int-phy-inl-sub)#

- 14. Salga el submode de la interfaz: sensor(config-int-phy-inl-sub)#exit sensor(config-int-phy-inl)#exit sensor(config-int-phy)#exit sensor(config-int)#exit Apply Changes:?[yes]:
- 15. Presione ENTER para aplicar los cambios, o ingresar no para desecharlos.
- 16. Ingrese el modo virtual de la Configuración del sensor:

```
sensor(config)#service analysis-engine
    sensor(config-ana)#virtual-sensor vs0
```

17. Agregue la interfaz al virtual-sensor:

sensor(config-ana-vir)#physical-interface GigabitEthernet0/2
subinterface-number 1

18. Salga el submode del virtual-sensor:

```
sensor(config-ana-vir)#exit
    sensor(config-ana)#exit
    Apply Changes:?[yes]:
```

19. Presione ENTER para aplicar los cambios, o ingresar no para desecharlos.

Configuración IDM

Complete estos pasos para configurar las configuraciones en línea de los pares del VLA N en el sensor usando el IDS Device Manager (IDM):

- 1. Abra su hojeador y ingrese el <Management_IP_Address_of_IPS> de https:// para acceder el IDM en el IPS.
- 2. Haga clic el **lanzador de la descarga IDM y comience el IDM** para descargar el instalador para la aplicación.

3. Van al Home Page para ver la información del dispositivo tal como nombre del host, la dirección IP, la versión, y el modelo., los



4. Vaya a la **configuración > a la configuración del sensor** y haga clic la **red**. Aquí usted puede especificar el nombre de host, la dirección IP y la ruta predeterminado.

🅵 Cisco IDM 6.0 - 10.77.241.1	42								
File Help									
Home Configuration	Monitoring	Back	Forward	@ Refresh	? Help	 CI			
Sensor Setup	Network Specify the net	work and c	ommunication (parameters for	the sensor.				
B-Q SSH	Hostname:	Hostname: sensor							
Sensor Key	P Address:	10.77.24	1.142						
Trusted Hosts	Network Mask: 255.255.255.192								
	Default Route:	10.77.24	1.129						
 Interface Configuration Summary 	FTP Timeout	300				second			
Interfaces Interface Pairs VLAN Pairs	Alow Pass	word Reco	very						
VLAN Groups Bypass Traffic Flow Notificati	Web Server S	ettings /SSL		Remote . Teinet is i disabled l	Access not a secure access service and is by default.				
Analysis Engine Virtual Sensors Global Variables	Web server po	rt: 443		🗹 Enab	ie Teinet				

5. Vaya a la **configuración > a la configuración de la interfaz** y haga clic el **resumen**.Esta página muestra el resumen de la configuración de la interfaz de detección.

Cisco IDM 6	.0 - 10.77.241.14	2						_10
File Help								
Home	Configuration	Monitoring	Back	O Forward	@ Refresh	? Help		cisco
Sensor Setu - Natwork - Natwork - Natwork - Natwork - Natwork - Natwork - Natwork - Natwork - Natwork - Natwork	P A	Summary The following promiscuous	g is the configu , inline interfac	ration summar e pair, or inline	y of the sens YLAN pair m	ng interfaces ade , but no co	You can configure any single phy mbination of these modes is allow	vsical interface for ed.
- N Auth	norized Keys wn Host Keys	N	lame			Details	Assign Virtual Se	ed Descrip
Certifical	tes ted Hosts ver Certificate infiguration s Pains airs roups low Notificati- gine ensors ariables e Definitions ction Rules s0 Detections	U-I gat (telfier	netulu	++omscuous	Interface		-1400	
Blocking Blocking Device	Properties	<[

6. Vaya a la configuración > a la configuración de la interfaz > a las interfaces y seleccione el nombre de la interfaz. Entonces, permiso del tecleo para habilitar la interfaz de detección. También, configure el duplex, la velocidad y la información de VLAN.

🕵 Cisco IDM	6.0 - 10.77.241.14	12						_10
File Help								
				@ ?				սիսի
Home	Configuration	Monitoring Bax	k Forward	Refresh Help				CISCO
Sensor Set Metwor Mowe SH	up k d Hosts	Interfaces A sensing interface ma can enable/disable the	ist be enabled and a available sensing in	assigned to a virtual s terfaces by selecting	ensor before the the row(s) and o	sensor will mor dicking Enable o	ntor that inte r Disable.	rface. You
- Aut - Aut Kno	thorized Keys own Host Keys	Interface Name	Enabled	Media Type	Duplex	Speed	Defat VLAI	Select All
E-Q. Certific	nsor Key	GigabitEthernet0.0	Yes	TX (copper)	Auto	Auto		Edit
Tru	isted Hosts							~
Ser 🖓 Ser	rver Certificate	💕 Edit Interfa	ce				×	Enable
Time Silers								
💠 Interface Co	onfiguration	Interface Nam	e GigabitEthem	et0/0				Disable
Summa		Enabled:	(Yes (no No				
- Dinteriac	a Pars	Media Type:	TX (copper)					
- N VLAN F	Pairs	Durslay:						
	Groups	E-donese	pauro -					
Traffic	Flow Notificati	Speed:	Auto	3				
Analysis Er	ighe Sensors	Default VLAN	p					
	Variables	Use Altern	ste TCP Reset Inter	face				
E- Signatu	ire Definitions 0	Selectineer	toon:					
E-B Event A	Action Rules es0	Description						
È- 😓 Anomai —¶Ω adŭ	ly Detections	च					F	
- Blocking	n Dronerties		ок	Cancel	Help		F	

 Vaya a la configuración > a la configuración de la interfaz > a los pares del VLA N y el tecleo agrega para crear los pares en línea del VLA N.

🕞 Fisco IDM 6.0 - 10.77.241.14		
Home Configuration	Monitoring Back Forward Refresh Help	ahaha cisco
Allowed Hosts	VLAN Peirs You can create inline VLAN pair(s) for the available sensing interfaces. You can edit/delete the existing in by selecting the row(s) and clicking Edit or Delete.	ine VLAN pair(s)
BQ Certificates	Interface Name Subinterface Description	Select Al
Trusted Hosts	VLANA VLANB	Add
Summary		Coloto
- N interfaces	🖬 Add Inline VLAN Pair	overere.
A Mertace Pare	Interface Name: Gigsb/tEthernet0/0	
Byposs Diraffic Flow Notificati	Subinterface Number.	
Policies	YLANA:	
Event Action Rules	YLAN B:	
Anomaly Detections	Description	
Blocking Properties Social Device Login Profiles Blocking Devices	OK Cancel Help	
Router Blocking Devic		1
Cat 6K Blocking Devic	Asply Reset	

8. Ingrese el número de la subinterfaz, el VLA N A y el VLA N B para la interfaz de detección (GigabitEthernet0/0).

r i la companya da serie da s	×
GigabitEthernet0/0	
1	
52	
53	
pairs vlans 52 and 53	
Cancel Help	
	GigabitEthernet0./0 1 52 53 pairs vlans 52 and 53 Cancel Help

ver el resumen de la configuración en línea de los pares del VLA N.

🅵 Cisco IDM 6	5.0 - 10.77.241.14	2						_1
File Help								
Home	Configuration	Monitoring	Back	Forward	Refresh P	? Ielp		cisco
Allowed	Hosts	VLAN Pairs You can create in by selecting the re	nine VLAN ow(s) and	pair(s) for the s clicking Edit or D	vailable sensing velete.	interfaces. Yo LAN Pair	u can edit/delete the existin	g inline VLAN pair(s
	nes sted Hosts	Interface N	lame	Subinterfac	9 YLAN A	VLAN B	Description	
Time Time Time Dusers Interface Co Dinterface Ninterface VLANG VLANG VLANG VLANG Poloies Signatur Poloies Poloies	ver Certificate Infiguration Y ss Pairs Pairs Pow Notificati gine Ction Rules s0 / Detections					32	oo juaris vans oo arnu oo	Delete
Blocking Blocking Cat 6K E Master I	Devices Blocking Devic Blocking Devic Blocking Sens	•			Apply	Res	et	I

9. Va al **motor de la configuración > del análisis > el sensor virtual** y el tecleo **edita** para crear el nuevo sensor virtual.

🕵 Cisco IDM 6.0 - 10.77.241.1	12						
File Help							
Home Configuration	Monitoring	Back Forward	Refresh	? Help			cisco
Certificates	Virtual Sensors The sensor mor create a new v clicking Edit or 0	nitors traffic that bravers intual sensor by clicking belete.	ses interfaces, in Add. You can er	ferface pairs, dit or delete an	or VLAN pairs assigned t existing virtual sensor by	o a virtual se / selecting th	nsor. You can e row(s) and
Interface Configuration	Name	Assigned int	erfaces (or Pairs	e)	Sig Definition Policy	Event /	Select All
Summary Summary Interfaces Interfaces	vs0				sig0		Add
							Edit
- Dypass Dypass Dypass							Delete
Analysis Engine							
Policies E-To Signature Definitions							
Event Action Rules							
Anomaly Detections							
Blocking							
Device Login Profiles							
Cat 6K Blocking Devic	-						
SNMP			Apply		Reset		

10. Asigne los pares en línea 52 y 53 del VLA N al sensor virtual vs0.

🎼 Edit Virtual Sensor			
Virtual Sensor Name:	vs0		
Signature Definition Policy:	sig0 💌		
Event Action Rules Policy:	rules0 💌		
Anomaly Detection Policy:	ad0 💌		
AD Operational Mode:	Detect 💌		
Inline TCP Session Tracking Mode:	Virtual Sensor		
Description	default virtual sensor		
Available Interfaces			
Name	Details	Assigned	Select All
GigabitEthernet0/0.1	Inline VLAN Pair: 52<->53	Yes	
			Assign
			Remove
	OK Cancel Help		

Vea el resumen de la información virtual asignada del sensor.

Cisco IDM 6.0	- 10.77.241.1	42							_1
Home (Configuration	Monitoring	Back	Forward	@ Refresh	? Help			cisco
Certificates	r Key 3 d Hosts Certificate	Virtual Sensors The sensor m create a new clicking Edit o	nonitors traffic virtual senso r Delete.	that traverse: r by clicking A	s interfaces, in dd. You can ei	terface pai dit or delete	rs, or VLAN pairs as an existing virtual s	signed to a virtual se ensor by selecting th	nsor. You can e row(s) and
🛶 interface Config 🖗 Interface Config	guration	Name	Ass	igned Interfact	es (or Pairs)		Sig Definition Policy	Event Action R	Select All
- Summary - Sinterfaces		vs0	GigabitEthern	et0.0.1 (Inline	VLAN Pair: 52	«->53)	sig0	rules0	Add
	airs s								Edit
- SVLAN Grou	.ps								Lincat
- Dypass Traffic Flow	v Notificati								Delete
Analysis Engine	e sors								
	ables								
Signature D	Definitions								
	n Rules								
rules0 🖓 — J Anomaly De	etections								
L-S ad0									
Blocking Blocking Pri Blocking Pri	operties								
Device Log	in Profiles								
	evices cking Devic								
Cat 6K Bloc	king Devic	4							
Master Blot	cking Sens					1			
🚯 General Co	ntiguration				Apply		Reset		
4									

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- <u>Cisco ASA 5500 Series Adaptive Security Appliances</u>
- <u>Cisco Intrusion Prevention System</u>
- Sensores Cisco IPS de la serie 4200
- Soporte Técnico y Documentación Cisco Systems