IPS 5.X e versioni successive/IDSM2: Modalità inline per coppie VLAN con esempio di configurazione CLI e IDM

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Prodotti correlati Convenzioni Configurazione acquisizione VACL Configurazione in linea della modalità coppia VLAN Configurazione CLI Configurazione IDM Risoluzione dei problemi Informazioni correlate

Introduzione

L'associazione delle VLAN a coppie su un'interfaccia fisica è nota come modalità di coppia di VLAN in linea. I pacchetti ricevuti su una delle VLAN accoppiate vengono analizzati e inoltrati all'altra VLAN della coppia. Le coppie di VLAN in linea sono supportate su tutti i sensori compatibili con Intrusion Prevention System (IPS) 5.1, ad eccezione di NM-CIDS, AIP-SSM-10 e AIP-SSM-20.

La modalità inline di coppia di VLAN è una modalità di rilevamento attivo in cui un'interfaccia di rilevamento opera come porta trunk 802.1q e il sensore esegue il bridging VLAN tra coppie di VLAN sul trunk. Ciò significa che lo switch collegato all'interfaccia di rilevamento deve essere in modalità trunk.

Il sensore controlla il traffico che riceve su ciascuna VLAN in ciascuna coppia e può inoltrare i pacchetti sull'altra VLAN nella coppia o scartare il pacchetto se viene rilevato un tentativo di intrusione. È possibile configurare un sensore IPS in modo da collegare simultaneamente fino a 255 coppie di VLAN su ciascuna interfaccia di rilevamento. Il sensore sostituisce il campo VLAN ID nell'intestazione 802.1q di ciascun pacchetto ricevuto con l'ID della VLAN in uscita su cui il sensore inoltra il pacchetto. Il sensore scarta tutti i pacchetti ricevuti sulle VLAN che non sono assegnate a coppie di VLAN in linea.

Nota: per IPS-4260, il bypass hardware fail-open non è supportato sulle coppie di VLAN in linea. Per ulteriori informazioni, fare riferimento a <u>Limitazioni della configurazione di bypass hardware</u>.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sul sensore Cisco Intrusion Prevention System che usa la versione 5.1 e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Le informazioni discusse in questo documento si applicano anche al modulo Servizi del sistema di rilevamento delle intrusioni (IDSM-2).

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento <u>Cisco sulle convenzioni</u> <u>nei suggerimenti tecnici</u>.

Configurazione acquisizione VACL

Per inviare il traffico a IDSM sullo switch, consultare la sezione <u>Configurazione</u> dell'<u>acquisizione</u> <u>VACL</u> in <u>Configurazione di IDSM-2</u>.

Configurazione in linea della modalità coppia VLAN

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo <u>strumento di</u> <u>ricerca</u> dei comandi (solo utenti <u>registrati</u>).

Usare il comando **physical-interfaces interface_name** nella modalità secondaria dell'interfaccia del servizio per configurare le coppie di VLAN inline con la CLI. Il nome dell'interfaccia è FastEthernet o Gigabit Ethernet.

Si applicano le seguenti opzioni:

 stato-amministratore {enabled | disabled}: lo stato del collegamento amministrativo dell'interfaccia, sia essa abilitata o disabilitata.Nota: su tutte le interfacce di rilevamento backplane su tutti i moduli (IDSM-2 NM-CIDS e AIP-SSM), admin-state è impostato su enabled ed è protetto (non è possibile modificare l'impostazione). Lo stato admin non ha alcun effetto (ed è protetto) sull'interfaccia di comando e controllo. Influisce solo sulle interfacce di rilevamento. Non è necessario abilitare l'interfaccia di comando e controllo perché non può essere monitorata.

- default Ripristina l'impostazione di default del sistema.
- description: descrizione della coppia di interfacce inline.
- duplex Impostazione del duplex dell'interfaccia.auto: imposta l'interfaccia per la negoziazione automatica del duplex.full - Imposta l'interfaccia su full duplex.half - Imposta l'interfaccia su half-duplex.Nota: l'opzione duplex è protetta su tutti i moduli.
- no Rimuove una voce o un'impostazione di selezione.
- speed Impostazione della velocità dell'interfaccia.auto Imposta la velocità di negoziazione automatica per l'interfaccia.10 - Imposta l'interfaccia su 10 MB (solo per interfacce TX).100 -Imposta l'interfaccia su 100 MB (solo per interfacce TX).1000 - Imposta l'interfaccia su 1 GB (per interfacce Gigabit)Nota: l'opzione speed è protetta su tutti i moduli.
- tipo sottointerfaccia (subinterface-type) Specifica che l'interfaccia è una sottointerfaccia e il tipo di sottointerfaccia definito.inline-vlan-pair: consente di definire la sottointerfaccia come coppia di VLAN in linea.none - Nessuna sottointerfaccia definita.
- subinterface Definisce la sottointerfaccia come coppia di VLAN in linea.vlan1: la prima VLAN nella coppia di VLAN in linea.vlan2: la seconda VLAN nella coppia di VLAN in linea.

Configurazione CLI

Completare questa procedura per configurare le impostazioni della coppia di VLAN in linea sul sensore con CLI:

- 1. Accedere alla CLI utilizzando un account con privilegi di amministratore.
- 2. Accedere alla modalità secondaria dell'interfaccia:

```
sensor#configure terminal
sensor(config)#service interface
sensor(config-int)#
```

3. Verificare se esistono interfacce inline (il tipo di sottointerfaccia deve essere "none" se non sono state configurate interfacce inline):

```
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. Rimuovere le interfacce inline che utilizzano questa interfaccia fisica: sensor(config-int)#no inline-interfaces interface_name

5. Visualizzare l'elenco delle interfacce disponibili:

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. Specificare un'interfaccia:

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

7. Abilitare lo stato admin-state dell'interfaccia: sensor(config-int-phy)#admin-state enabled

Per monitorare il traffico, l'interfaccia deve essere assegnata al sensore virtuale e abilitata.

- 8. Aggiungere una descrizione dell'interfaccia: sensor(config-int-phy)#description INT1
- 9. Configurare le impostazioni duplex: sensor(config-int-phy)#duplex full

Questa opzione non è disponibile sui moduli.

10. Configurare la velocità:

sensor(config-int-phy)#speed 1000

Questa opzione non è disponibile sui moduli.

11. Configurare la coppia di VLAN in linea:

```
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. Aggiungere una descrizione per la coppia di VLAN inline: sensor(config-int-phy-inl-sub)#description pairs vlans 52 and 53
- 13. Verificare le impostazioni della coppia di VLAN in linea:

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

14. Uscire dalla modalità secondaria dell'interfaccia: 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. Premere Invio per applicare le modifiche o immettere no per ignorarle.
- 16. Accedere alla modalità di configurazione del sensore virtuale:

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

- 17. Aggiungere l'interfaccia al sensore virtuale: sensor(config-ana-vir)#physical-interface GigabitEthernet0/2 subinterface-number 1
- 18. Uscire dalla modalità secondaria del sensore virtuale:

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

19. Premere Invio per applicare le modifiche o immettere no per ignorarle.

Configurazione IDM

Completare questa procedura per configurare le impostazioni della coppia di VLAN in linea sul sensore con IDS Device Manager (IDM):

- Aprire il browser e immettere https://<Management_IP_Address_of_IPS> per accedere a IDM su IPS.
- 2. Fate clic su **Download IDM Launcher e Avvia IDM** per scaricare il programma di installazione dell'applicazione.

3. Andare alla home page per visualizzare le informazioni sul dispositivo, quali il nome host, l'indirizzo IP, la versione e il modello,



 Selezionare Configurazione > Impostazione sensore e fare clic su Rete. Qui è possibile specificare il nome host, l'indirizzo IP e il percorso predefinito.

🕻 Cisco IDM 6.0 - 10.77.241.1	12						
File Help							
Home Configuration	Monitoring	Back	Forward	@ Refresh	? Нер	il Cl	
Sensor Setup Allowed Hosts	Network Specify the netv	work and c	ommunication (parameters for	the sensor.		
B-Q. SSH	Hostname:	sensor					
Sensor Key	P Address:	ress: 10.77.241.142					
Trusted Hosts	Network Mask: 255.255.255.192						
B Time	Default Route:	10.77.241.129					
P Interface Configuration	FTP Timeout	300				second	
VLAN Pairs	Alow Passv	word Recor	very				
- D VLAN Groups - D Bypass D Traffic Flow Notificati	-Web Server S	ettings XSSL		Remote . Teinet is i disabled l	Access not a secure access service and is by default.		
Analysis Engine	Web server po	art: 443		🗹 Enab	ie Teinet		

5. Selezionare **Configurazione > Configurazione interfaccia**, quindi fare clic su **Riepilogo**.Questa pagina mostra il riepilogo della configurazione dell'interfaccia di rilevamento.

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	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	<[

 Selezionare Configurazione > Configurazione interfaccia > Interfacce, quindi selezionare il nome dell'interfaccia. Per abilitare l'interfaccia di rilevamento, fare clic su Abilita. Inoltre, configurare le informazioni duplex, velocità e VLAN.

🕵 Eisco IDM	6.0 - 10.77.241.14	12				na a a		_1
File Help								
Home	Configuration	Monitoring Bac	k Forward	Refresh Help				cisco
Sensor Sel Minetwo Malowe	tup rk d Hosts	Interfaces A sensing interface mu can enable/disable the	st be enabled and a available sensing int	ssigned to a virtual s erfaces by selecting	ensor before the the row(s) and (sensor will mor dicking Enable o	ntor that inte r Disable.	rface. You
	thorized Keys own Host Keys	Interface Name	Enabled	Media Type	Duplex	Speed	Defai VLAJ	Select All
E-Q Certific	nsor key vates	GigabitEthernet0/0	Yes	TX (copper)	Auto	Auto		Edit
True True	usted Hosts							
	rver certificate	🕵 Edit Interfa	ce				×	Enable
L-S Users		Interface Name	e GigabitEtherne	±0/0				Disable
Summa Summa	ontiguration ry	Enabled:	· Yes	No				
- painterie	e Pars	Media Type:	TX (copper)					
	Pairs Groups	Duplex:	Auto -					
- B Bypas:	s Flow Notificati	Speed.	Auto *	1				
Analysis Ei	ngine Sensors	Default VLAN	0	-				
Global	Variables	Use Altern	ate TCP Reset Inter1	ace				
E-Co Signatu	ure Definitions	Select inter	1005: 💌					
E-Event /	Action Rules es0	Description						
E-😓 Anoma	ly Detections							
Blocking	0	<u> </u>	ок	Cancel	Help		•	
	a Properties				1 Charles and the			

 Per creare le coppie di VLAN in linea, selezionare Configuration > Interface Configuration > VLAN Pairs e fare clic su Add (Aggiungi).

🕼 Cisco IDM 6.0 - 10.77.241.142						_10
File Help						
Home Configuration	Monitoring Back	Forward Refr	esh Help			cisco
Allowed Hosts	LAN Pairs You can create inline VLAN by selecting the row(s) and	pain(s) for the availa clicking Edit or Delete	ble sensing intre	erfaces. You can	edit/delete the existing i	nine VLAN pair(s)
B-Q. Certificates	Interface Name	Subinterface	VLA	N Par	Description	Select Al
Trusted Hosts						Edit
Summery	The Add Inline VI.4	N Pair			×I	Oelete
A mentaces	Interface Name:	GigabitEthen	iet0/0 💌			
Byposs Traffic Flow Notificati	Subinterface Nur	nber:				
Paicies	YLAN A:					
Sig0	YLAN B:					
E-R Anomaly Detections	Description:					
Blocking Blocking Properties Social Device Login Profiles Blocking Devices Router Blocking Device	<u> </u>	к	ancel	Help		٤
Cat 6K Blocking David		Ag	the last the	Reset		

8. Immettere il numero della sottointerfaccia, la VLAN A e la VLAN B per l'interfaccia di rilevamento (Gigabit

Interface Name:	GigabitEthernet0/0
Subinterface Number:	1
VLAN A:	52
VLAN B:	53
Description:	pairs vlans 52 and 53
OK	Concel Holm

Ethernet0/0).

ossibile visualizzare il riepilogo della configurazione della coppia di VLAN in linea.

🅵 Cisco IDM 6	5.0 - 10.77.241.14	2						_10
File Help								
Home	Configuration	Monitoring	Back	Forward Ref	s 🦻			cisco
Allowed	Hosts	VLAN Pairs You can crea by selecting b	de inline VLAN he row(s) and ce Name	pair(s) for the avails clicking Edit or Delet	ble sensing inte e. VLAI	erfaces. You car N Pair	edit/delete the existing	inine VLAN pair(s
True	sted Hosts	110110		Caternorisco	YLAN A	VLAN B	o o con paos	
Time Time Users Time Users Interface Co Summar Summar Sunterface VLAN G Synass Traffic F Analysis En Sign Policies Signatur Synatur Signatur Sonado Bocking Bocking Bocking Bocking Bocking Bocking Bocking Router E Router E Sonado	nfiguration Y se Pairs Town Notifications roups Town Notifications properties so Properties Login Profiles Devices Stocking Device	-			4			Delete
Master 8	Blocking Sens			A	pply	Reset		

 Per creare il nuovo sensore virtuale, selezionare Configurazione > Analysis Engine > Virtual Sensor e fare clic su Modifica.

🎼 Cisco IDM 6.0 - 10.77.241.14	12						
File Help							
Home Configuration	Monitoring	Back Forwa	rd Refresh	? Help			cisco
Certificates	Virtual Sensors The sensor mor create a new vi clicking Edit or D	itors traffic that brave rtual sensor by clicki belete.	erses interfaces, i ng Add. You can e	nterface pairs, o dt or delete an	or VLAN pairs assigned t existing virtual sensor by	io a virtual se y selecting th	nsor. You can e row(s) and
Interface Configuration	Name	Assigned	Interfaces (or Pair	8)	Sig Definition Policy	Event /	Select All
Summary Summary Interfaces Interface Doire	vs0				sigO		Add
VLAN Poirs							Edit
Bypass							Delete
Analysis Engine							
Policies E-To Signature Definitions L-S sign							
Event Action Rules							
Anomaly Detections							
Blocking							
Blocking Devices							
Cat 6K Blocking Devic	-					•	
SNMP	Jaidanaa		Apply		Reset		

10. Assegnare la coppia di VLAN inline 52 e 53 al sensore virtuale 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		

Visualizza il riepilogo delle informazioni sul sensore virtuale assegnato.

🕼 Cisco IDM 6.0 - 10.77.241.1	42							
Home Configuration	Monitoring	Back	Forward	@ Refresh	? Help			dhah cisco
Certificates	- Virtual Sensors The sensor n create a new clicking Edit o	nonitors treffic r virtual senso r Delete.	: that traverse ir by clicking A	s interfaces, in dd. You can e	terface pa dit or delet	irs, or VLAN pairs as an existing virtual s	signed to a virtual se ensor by selecting th	nsor. You can e row(s) and
→ SA Users	Name	Ass	igned Interfact	es (or Pairs)		Sig Definition	Event Action R	Select All
Summary Minterfaces	vs0	GigabilEthern	et0/0.1 (Inline	VLAN Pair: 52	«->53)	sig0	rules0	Add
VLAN Pairs								Edit
- Analysis Engine								Delete
Virtual Sensors								
Policies								
E-W Signature Definitions								
Event Action Rules								
E-S Anomaly Detections								
Blocking								
Blocking Properties Device Login Profiles								
Blocking Devices								
Cat 6K Blocking Devic	-							
SIMP			Г		1 1		_	
S General Configuration			L	Apply		Reset		

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- <u>Cisco ASA serie 5500 Adaptive Security Appliance</u>
- <u>Cisco Intrusion Prevention System</u>
- <u>Cisco IPS serie 4200 Sensori</u>
- Documentazione e supporto tecnico Cisco Systems