IPS 5.X und höher/IDSM2: Inline-VLAN-Paarmodus mit CLI- und IDM-Konfigurationsbeispiel

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Zugehörige Produkte Konventionen Konfiguration der VACL-Erfassung Konfiguration des Inline-VLAN-Paarmodus CLI-Konfiguration IDM-Konfiguration Fehlerbehebung Zugehörige Informationen

Einführung

Die Zuordnung von VLANs in Paaren an einer physischen Schnittstelle wird als Inline-VLAN-Paarmodus bezeichnet. Pakete, die in einem der paarweise verbundenen VLANs empfangen werden, werden analysiert und an das andere VLAN im Paar weitergeleitet. Inline-VLAN-Paare werden auf allen Sensoren unterstützt, die mit Intrusion Prevention System (IPS) 5.1 kompatibel sind, mit Ausnahme von NM-CIDS, AIP-SSM-10 und AIP-SSM-20.

Der Inline-VLAN-Paarmodus ist ein aktiver Sensormodus, bei dem eine Sensorschnittstelle als 802.1q-Trunk-Port fungiert und der Sensor VLAN-Bridging zwischen VLAN-Paaren auf dem Trunk durchführt. Das bedeutet, dass sich der an die Sensorschnittstelle angeschlossene Switch im Trunk-Modus befinden muss.

Der Sensor prüft den Datenverkehr, den er in jedem VLAN in jedem Paar empfängt, und kann die Pakete entweder im anderen VLAN des Paars weiterleiten oder das Paket verwerfen, wenn ein Eindringungsversuch erkannt wird. Sie können einen IPS-Sensor so konfigurieren, dass auf jeder Sensorschnittstelle gleichzeitig bis zu 255 VLAN-Paare überbrückt werden. Der Sensor ersetzt das VLAN-ID-Feld im 802.1q-Header jedes empfangenen Pakets durch die ID des Ausgangs-VLAN, auf dem der Sensor das Paket weiterleitet. Der Sensor verwirft alle Pakete, die auf VLANs empfangen werden, die nicht Inline-VLAN-Paaren zugewiesen sind.

Hinweis: Für IPS-4260 wird eine Fail-Open-Hardware-Umgehung nicht auf Inline-VLAN-Paaren unterstützt. Weitere Informationen finden Sie unter <u>Einschränkungen für die Hardware-Umgehung</u>.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dem Cisco Intrusion Prevention System Sensor, der die Version 5.1 und höher verwendet.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Zugehörige Produkte

Die Informationen in diesem Dokument gelten auch für das Intrusion Detection System (IDSM-2) Services Module.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

Konfiguration der VACL-Erfassung

Informationen zum Senden von Datenverkehr an das IDSM auf dem Switch finden Sie im Abschnitt Configuring VACL Capture (VACL-Erfassung konfigurieren) IDSM-2.

Konfiguration des Inline-VLAN-Paarmodus

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das <u>Command Lookup Tool</u> (nur <u>registrierte</u> Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Verwenden Sie den Befehl **interface_name für physische Schnittstellen** im Dienstschnittstellenuntermodus, um Inline-VLAN-Paare mithilfe der CLI zu konfigurieren. Der Schnittstellenname ist FastEthernet oder GigabitEthernet.

Diese Optionen gelten für:

 Admin-State {enabled, | disabled} - Der Status der administrativen Verbindung der Schnittstelle, unabhängig davon, ob die Schnittstelle aktiviert oder deaktiviert ist. Hinweis: An allen Backplane Sensing Interfaces auf allen Modulen (IDSM-2 NM-CIDS und AIP-SSM) ist der Admin-State aktiviert und geschützt (Sie können die Einstellung nicht ändern). Der Admin-Zustand hat keine Auswirkungen (und ist geschützt) auf die Command-and-Control-Schnittstelle. Es betrifft nur Sensorschnittstellen. Die Command-and-Control-Schnittstelle muss nicht aktiviert werden, da sie nicht überwacht werden kann.

- default: Setzt den Wert auf die Standardeinstellung des Systems zurück.
- description Ihre Beschreibung des Inline-Schnittstellenpaars.
- duplex: Die Duplexeinstellung der Schnittstelle.auto Legt die Schnittstelle f
 ür die automatische Aushandlung von Duplex fest.full (Vollst
 ändig): Stellt die Schnittstelle auf Vollduplex ein.half (halb): Legt die Schnittstelle auf Halbduplex fest.Hinweis: Die Duplexoption ist auf allen Modulen gesch
 ützt.
- no Entfernt eine Eingabe- oder Auswahleinstellung.
- speed (Geschwindigkeit): Die Geschwindigkeitseinstellung der Schnittstelle.auto (Automatisch): Stellt die Schnittstelle so ein, dass die Geschwindigkeit automatisch ausgehandelt wird.10 - Legt die Schnittstelle auf 10 MB fest (nur für TX-Schnittstellen).100 (100): Legt die Schnittstelle auf 100 MB fest (nur für TX-Schnittstellen).1000 - Legt die Schnittstelle auf 1 GB fest (für Gigabit-Schnittstellen)Hinweis: Die Geschwindigkeitsoption ist auf allen Modulen geschützt.
- subinterface-type: Gibt an, dass es sich bei der Schnittstelle um eine Subschnittstelle handelt und welcher Subschnittstellentyp definiert ist.inline-vlan-pair - Ermöglicht es Ihnen, die Subschnittstelle als Inline-VLAN-Paar zu definieren.none: Keine Subschnittstellen definiert.
- subinterface Definiert die Subschnittstelle als Inline-VLAN-Paar.vlan1: Das erste VLAN im Inline-VLAN-Paar.vlan2: Das zweite VLAN im Inline-VLAN-Paar.

CLI-Konfiguration

Gehen Sie wie folgt vor, um die Inline-VLAN-Paareinstellungen auf dem Sensor über die CLI zu konfigurieren:

- 1. Melden Sie sich mit einem Konto mit Administratorrechten bei der CLI an.
- 2. Wechseln Sie in den Schnittstellenuntermodus:
- sensor#configure terminal
 sensor(config)#service interface
 sensor(config-int)#
- 3. Überprüfen Sie, ob Inline-Schnittstellen vorhanden sind (der Subschnittstellentyp sollte "none" lauten, wenn keine Inline-Schnittstellen konfiguriert wurden): 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. Entfernen Sie alle Inline-Schnittstellen, die diese physische Schnittstelle verwenden: sensor(config-int)#no inline-interfaces interface_name

5. Anzeigen der Liste der verfügbaren Schnittstellen:

```
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. Angeben einer Schnittstelle:

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

7. Aktivieren Sie den Admin-Status der Schnittstelle: sensor(config-int-phy)#admin-state enabled

Die Schnittstelle muss dem virtuellen Sensor zugewiesen und aktiviert sein, um den Datenverkehr zu überwachen.

8. Fügen Sie eine Beschreibung dieser Schnittstelle hinzu:

sensor(config-int-phy)#description INT1

9. Konfigurieren Sie die Duplexeinstellungen: sensor(config-int-phy)#duplex full

Diese Option ist für Module nicht verfügbar.

10. Konfigurieren Sie die Geschwindigkeit: sensor(config-int-phy)#speed 1000

Diese Option ist für Module nicht verfügbar.

```
11. Einrichten des Inline-VLAN-Paars:
    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. Fügen Sie eine Beschreibung für das Inline-VLAN-Paar hinzu: sensor(config-int-phy-inl-sub)#description pairs vlans 52 and 53
- 13. Überprüfen Sie die Einstellungen für das Inline-VLAN-Paar:

- 14. Beenden Sie den Schnittstellenuntermodus: 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. Drücken Sie **die Eingabetaste**, um die Änderungen anzuwenden, oder geben Sie **no** ein, um sie zu verwerfen.
- 16. Wechseln Sie in den Konfigurationsmodus für virtuelle Sensoren: sensor(config)#service analysis-engine sensor(config-ana)#virtual-sensor vs0
- 17. Fügen Sie die Schnittstelle dem virtuellen Sensor hinzu: sensor(config-ana-vir)#physical-interface GigabitEthernet0/2 subinterface-number 1
- 18. Beenden Sie den Virtual-Sensor-Submodus:

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

19. Drücken Sie **die Eingabetaste**, um die Änderungen anzuwenden, oder geben Sie **no** ein, um sie zu verwerfen.

IDM-Konfiguration

Gehen Sie wie folgt vor, um die Inline-VLAN-Paareinstellungen auf dem Sensor mithilfe des IDS Device Manager (IDM) zu konfigurieren:

- 1. Öffnen Sie Ihren Browser, und geben Sie https://<Management_IP_Address_of_IPS> ein, um auf das IDM auf dem IPS zuzugreifen.
- 2. Klicken Sie auf **IDM Launcher herunterladen und IDM starten**, um das Installationsprogramm für die Anwendung herunterzuladen.
- 3. Rufen Sie die Startseite auf, um Geräteinformationen wie Hostname, IP-Adresse, Version und Modell usw.



 Gehen Sie zu Konfiguration > Sensor Setup, und klicken Sie auf Netzwerk. Hier können Sie den Hostnamen, die IP-Adresse und die Standardroute angeben.

🕵 Cisco IDM 6.0 - 10.77.241.1	12					
File Help						
Home Configuration	Monitoring	Back	Forward	@ Refresh	? Help	il Cl
Sensor Setup Allowed Hosts	Network Specify the netv	vork and c	ommunication (parameters for	the sensor.	
-Q SSH	Hostname:	sensor				
Sensor Key	P Address:	10.77.24	1.142			
Trusted Hosts	Network Mask:	255.255.2	255.192			
	Default Route:	10.77.241	1.129			
Interface Configuration Summary	FTP Timeout	300				second
- A Interfaces	Alow Passv	word Recov	very			
- D VLAN Pairs - D VLAN Groups - D Bypass - D Traffic Flow Notificati	-Web Server Si	ettings /SSL		Remote Teinet is disabled	Access not a secure access service and is by default.	
Analysis Engine N Virtual Sensors Global Variables	Web server po	rt: 443		🔽 Enat	vie Teinet	

5. Gehen Sie zu Konfiguration > Schnittstellenkonfiguration, und klicken Sie auf Zusammenfassung.Diese Seite zeigt die Konfigurationsübersicht der Sensorschnittstelle.

Cisco IDM 6	.0 - 10.77.241.14	2							
File Help									
e Home	Configuration	Monitoring	Back	Forward	@ Refresh	💡 Help			cisco
Sensor Setu Matwork Alowed SSH	p A	Summary The followin promiscuous	g is the configu s, inline interfac	aration summar se pair, or inline	y of the sensi YLAN pair m	ng interfaces ade, but no c	s. You can configu combination of the	re any single physical se modes is allowed.	interface for
- Autr	horized Keys wh Host Keys	ŀ	eme			Details		Assigned Virtual Sensor	Descrip
E-Q Cartificat	sorney	GigabitEther	met0/0	Promscuous	Interface			None	
 Service Stervice Summary Summary	ver Certificate Infiguration Ses Pairs airs roups Tow Notification ine iensors ariables e Definitions ction Rules s0 potections								
Blocking	Descettor								
Bocking Device	properties	<u></u>							
4	J J								

6. Gehen Sie zu Konfiguration > Schnittstellenkonfiguration > Schnittstellen, und wählen Sie den Schnittstellennamen aus.Klicken Sie anschließend auf Aktivieren, um die Sensorschnittstelle zu aktivieren. Konfigurieren Sie außerdem die Informationen zu Duplex, Geschwindigkeit und VLAN.

🕵 Cisco IDM I	6.0 - 10.77.241.14	12						
File Help								
Home	Configuration	Monitoring B	ack Forward	💽 💡 Refresh Help	, ÷			cisco
Sensor Setu - Network - Network	up 🔺	Interfaces A sensing interface r can enable/disable th	nust be enabled and e available sensing i	assigned to a virtual s iterfaces by selecting	ensor before the the row(s) and o	sensor will mor dicking Enable o	ntor that inte r Disable	rface. You
	horized Keys own Host Keys	Interface Name	Enabled	Media Type	Duplex	Speed	Defai VLAJ	Select All
E-Q Certifica	nsor Key ates	GigabitEthernet0.0	Yes	TX (copper)	Auto	Auto		Edit
Ser Time	sted Hosts ver Certificate	🕵 Edit Inter	face				× (Enable
- 🖗 Users	onfiguration	Interface Na	me GigabitEthen	net0/0				Disable
Summar Interfac		Enabled:	• Yes	C No				
por interriso	e Pars	Media Type:	TX (copper)					
	ars Groups	Duplex:	Auto 💌					
Traffic I	Flow Notificati	Speed:	Auto	-				
Analysis En	gine Sensors	Default VLA	Nt 0					
Policies	variables	Use Alte	mate TCP Reset Inter	face				
E Signatu	re Definitions	Select int	ertoce: 💌					
Event A	ction Rules Is0	Description						
E-Sa Anomal adu	y Detections	at						
Blocking	n Pronerties		ок	Cancel	Help			

7. Gehen Sie zu **Konfiguration > Schnittstellenkonfiguration > VLAN-Paare,** und klicken Sie auf **Hinzufügen**, um Inline-VLAN-Paare zu erstellen.

🔂 Cisco IDM 6.0 - 10.77.241.142		_10
File Help		
Home Configuration	Annitoring Back Forward Refresh Help	cisco
Allowed Hosts	AN Pairs /ou can create inline VLAN pair(s) for the available sensing interfaces. You can edit/delete the existin y selecting the row(s) and clicking Edit or Delete. Interface Name Subinterface VLAN A VLAN B Description	ginins VLAN par(s)
Server Certificate Server Certificate Server Certificate Surver Server Certificate Surver Server Se		Edit
A refaces A refaces A reface Parc A VLAN Pars A VLAN Crotos	Interface Name: GigsbitEthernet0/0 V	Detete
Traffic Flow Notificati Analysis Engine Policies	VLAN A:	
Sig0 ■ Event Action Rules Sign rules0	YLAN B:	
Anomaly Detections	Description:	
Blocking Properties Blocking Properties Blocking Devices Blocking Devices Router Blocking Devic St SK Blocking Devic	OK Cancel Help	L
Master Blocking Sens *	Asply Reset	

8. Geben Sie die Subschnittstellennummer, VLAN A und VLAN B für die Sensorschnittstelle (GigabitEthernet0/0)

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

Sie können

die Zusammenfassung der Inline-VLAN-Paarkonfiguration anzeigen.

🎼 Cisco IDM 6.0 - 1	0.77.241.142	2						_10
File Help								
Home Co	nfiguration	Monitoring	Back	Forward Refr	esh Help			cisco
Allowed Host:	s s d Keys ost Keys øy	VLAN Pairs You can creat by selecting the	te inline VLAM he row(s) and ce Name	I pair(s) for the availa I clicking Edit or Delete Subinterface	ole sensing inte VLAN	erfaces. You car	edit/delete the existing Description	hine VLAN pair(s
Trusted H	osts				YLAN A	VLAN B		
Time Users Interface Configur Summary Interface Configur Interface Configur Interface Pairs Interface Pairs VLAN Groups Bypass Dirteffic Flow N Analysis Engine Policies Policies Policies Policies Event Action F VLAN Groups Policies Policies Policies Policies Bocking Biocking Prop Device Login I Biocking Devik Router Biocking	ation s s lobificatio ntions tules ctions erties Profiles ces ig Devic	*						Delete
Cat 6K Blockin	ng Devic			At	piy	Reset		

9. Gehen Sie zu **Configuration > Analysis Engine > Virtual Sensor**, und klicken Sie auf **Edit**, um den neuen virtuellen Sensor zu erstellen.

🕵 Cisco IDM 6.0 - 10.77.241.1	42						
File Help							
Home Configuration	Monitoring	Back Forward	(C) Refresh	? Help			cisco
Certificates	Virtual Sensors The sensor mo create a new v clicking Edit or I	nitors traffic that traverse irtual sensor by clicking A Delete.	s interfaces, inte udd. You can edit	rface pairs, o or delete an i	r VLAN pairs assigned t existing virtual sensor by	o a virtual se r selecting th	nsor. You can e row(s) and
Interface Configuration	Name	Assigned inte	rfaces (or Pairs)		Sig Definition Policy	Event /	Select All
D Interfaces	vs0				Sigil		Add
- N Interface Pairs							Edit
Bypass Traffic Flow Notificati							Delete
Analysis Engine							
Policies E							
Event Action Rules							
E-Anomaly Detections							
Blocking							
Device Login Profiles							
Router Blocking Devic							
Cat 6K Blocking Devic	4					•	
SNMP		Γ	Apply		Reset		

10. Weisen Sie dem virtuellen Sensor das Inline-VLAN-Paar 52 und 53 zu 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		
Nome	Details	Assigned Select All
GigabitEthernet0/0.1	Inline VLAN Pair: 52<->53	Yes
		Remove
		. 1
	Cancel Hel	<u></u>

Zeigen Sie die Zusammenfassung der zugewiesenen Informationen für virtuelle Sensoren an.

Cisco IDM 6.0 - 10.77.241.142	2			_
Home Configuration	Monitoring	Back Forward Refresh Her	þ	cisco
Certificates	Virtual Sensors The sensor n create a new clicking Edit o	noritors traffic that traverses interfaces, interface v virtual sensor by clicking Add. You can edit or de or Delete.	e pairs, or VLAN pairs as elete an existing virtual se	signed to a virtual sensor. You ca moor by selecting the row(s) and
Interface Configuration	Name	Assigned Interfaces (or Pairs)	Sig Definition Policy	Event Action R Select Al
Summary Interfaces	vs0	GigabitBhemet0/0.1 (Inline YLAN Pair: 52«->53)	sigl	rules0 Add
VLAN Pairs				Edit
- Traffic Flow Notificati				Delete
Virtual Sensors				
Policies				
- @ Signature Definitions				
Event Action Rules				
Anomaly Detections				
Elocking				
Blocking Properties				
Blocking Devices				
Router Blocking Devic Strengthere Devic				
Master Blocking Sens	-			<u>></u>
SNMP		Apply	Reset	

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- <u>Cisco Adaptive Security Appliances der Serie ASA 5500</u>
- <u>Cisco Intrusion Prevention System</u>
- <u>Cisco Sensoren der Serie IPS 4200</u>
- <u>Technischer Support und Dokumentation Cisco Systems</u>