IPS 6.X und höher/IDSM2: Inline-Schnittstellenpaarmodus - IDM-Konfigurationsbeispiel

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Zugehörige Produkte Konventionen Konfiguration von Inline-Schnittstellenpaaren CLI-Konfiguration IDM-Konfiguration IDM-Konfiguration Konfigurieren des Switches für IDSM-2 im Inline-Modus Fehlerbehebung Problem Lösung Zugehörige Informationen

Einführung

Bei Betrieb im Inline-Schnittstellenpaarmodus wird das Intrusion Prevention System (IPS) direkt in den Datenverkehrsfluss integriert und beeinflusst die Paketweiterleitungsraten, was diese bei Hinzufügen von Latenz verlangsamt. So kann der Sensor Angriffe stoppen, sodass schädlicher Datenverkehr verworfen wird, bevor er das gewünschte Ziel erreicht, und so einen Schutzdienst bereitstellt. Die Informationen zur Inline-Geräteverarbeitung werden nicht nur auf Layer 3 und 4 analysiert, sondern auch Inhalt und Nutzlast der Pakete für komplexere, eingebettete Angriffe (Layer 3 bis 7). Diese tiefer gehende Analyse ermöglicht dem System, Angriffe zu identifizieren und zu stoppen bzw. zu blockieren, die normalerweise über ein herkömmliches Firewall-Gerät erfolgen.

Im Inline-Schnittstellenpaarmodus wird ein Paket über die erste Schnittstelle des Paars auf dem Sensor und über die zweite Schnittstelle des Paars empfangen. Das Paket wird an die zweite Schnittstelle des Paars gesendet, es sei denn, das Paket wird abgelehnt oder durch eine Signatur geändert.

Hinweis: Sie können AIM-IPS und AIP-SSM für den Betrieb inline konfigurieren, obwohl diese Module nur eine Sensorschnittstelle haben.

Hinweis: Wenn die gepaarten Schnittstellen mit demselben Switch verbunden sind, sollten Sie sie auf dem Switch als Access-Ports mit unterschiedlichen Zugriffs-VLANs für die beiden Ports

konfigurieren. Andernfalls fließt der Datenverkehr nicht über die Inline-Schnittstelle.

<u>Voraussetzungen</u>

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco IPS Sensor, der die Befehlszeilenschnittstelle 6.0 und den Intrusion Prevention System Device Manager (IDM) 6.0 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 von Inline-Schnittstellenpaaren

Verwenden Sie den Befehl inline-interface name im Dienstschnittstellenuntermodus, um Inline-Schnittstellenpaare zu erstellen.

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.

Hinweis: AIP-SSM ist für den Inline-Schnittstellenmodus von der Cisco ASA-CLI und nicht von der Cisco IPS-CLI konfiguriert.

Diese Optionen gelten für:

 Name der Inline-Schnittstellen - Name des logischen Inline-SchnittstellenpaarsHinweis: An allen Backplane Sensing Interfaces auf allen Modulen (IDSM-2 NM-CIDS und AIP-SSM) ist admin-state aktiviert und geschützt (die Einstellung kann nicht geändert werden). Der Admin-Status 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
- interface1 interface_name Die erste Schnittstelle im Inline-Schnittstellenpaar
- interface2 interface_name Die zweite Schnittstelle im Inline-Schnittstellenpaar
- no Entfernt eine Eingabe- oder Auswahleinstellung
- Admin-State {enabled, | disabled} Der Status der administrativen Verbindung der Schnittstelle, unabhängig davon, ob die Schnittstelle aktiviert oder deaktiviert ist.

CLI-Konfiguration

Gehen Sie wie folgt vor, um die Einstellungen für das Inline-VLAN-Paar auf dem Sensor zu konfigurieren:

- 1. Melden Sie sich bei der CLI mit einem Konto an, das über Administratorrechte verfügt.
- 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 lesen, wenn keine Inline-Schnittstellen konfiguriert wurden:

```
sensor(config-int)#show settings
 physical-interfaces (min: 0, max: 9999999999, 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. Nennen Sie das Inline-Paar: sensor(config-int)#inline-interfaces PAIR1

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. Konfigurieren Sie zwei Schnittstellen in einem Paar: sensor(config-int)#interface1 GigabitEthernet0/0

sensor(config-int-inl)#interface2 GigabitEthernet0/1

Sie müssen die Schnittstelle einem virtuellen Sensor zuweisen und aktivieren, bevor sie den Datenverkehr überwachen kann. Weitere Informationen finden Sie in Schritt 10.

- 7. Fügen Sie eine Beschreibung dieser Schnittstelle hinzu: sensor(config-int-phy)#description PAIR1 Gig0/0 and Gig0/1
- 8. Wiederholen Sie die Schritte 4 bis 7 für alle anderen Schnittstellen, die Sie für Inline-Schnittstellenpaare konfigurieren möchten.
- 9. Überprüfen Sie die Einstellungen: sensor(config-int-inl)#show settings

```
name: PAIR1
description: PAIR1 Gig0/0 & Gig0/1 default:
    interface1: GigabitEthernet0/0
    interface2: GigabitEthernet0/1
```

10. Aktivieren Sie die Schnittstellen, die dem Schnittstellenpaar zugewiesen sind:

```
sensor(config-int)#exit
sensor(config-int)#physical-interfaces GigabitEthernet0/0
sensor(config-int-phy)#admin-state enabled
sensor(config-int-phy)#exit
sensor(config-int)#physical-interfaces GigabitEthernet0/1
```

```
sensor(config-int-phy)#admin-state enabled
 sensor(config-int-phy)#exit
 sensor(config-int)#
11. Überprüfen Sie, ob die Schnittstellen aktiviert sind:
  sensor(config-int)#show settings
   physical-interfaces (min: 0, max: 999999999, current: 5)
    _____
     <protected entry>
     name: GigabitEthernet0/0
     _____
      media-type: tx <protected>
      description: <defaulted>
      admin-state: enabled default: disabled
      duplex: auto <defaulted>
      speed: auto <defaulted>
      default-vlan: 0 <defaulted>
      alt-tcp-reset-interface
      -----
        none
        -----
        _____
      _____
      subinterface-type
       -----
        none
          _____
        _____
       _____
     _____
     <protected entry>
     name: GigabitEthernet0/1
     -----
      media-type: tx <protected>
      description: <defaulted>
      admin-state: enabled default: disabled
      duplex: auto <defaulted>
      speed: auto <defaulted>
      default-vlan: 0 <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>
      default-vlan: 0 <defaulted>
      alt-tcp-reset-interface
      _____
```

none



12. Geben Sie diesen Befehl ein, um ein Inline-Schnittstellenpaar zu löschen und die Schnittstellen in den Promiscuous-Modus zurückzugeben: sensor(config-int)#no inline-interfaces PAIR1

Sie müssen auch das Inline-Schnittstellenpaar aus dem virtuellen Sensor löschen, dem es zugewiesen ist.

13. Überprüfen Sie, ob das Inline-Schnittstellenpaar gelöscht wurde:

sensor(config-int)#show settings

- 14. Exit Interface Configuration-Submodus: 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.

IDM-Konfiguration

Gehen Sie wie folgt vor, um die Inline-VLAN-Paareinstellungen auf dem Sensor mithilfe des 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.
- Rufen Sie die Startseite auf, um Geräteinformationen wie Hostname, IP-Adresse, Version und Modell anzuzeigen.

Cisco IDM 6.0	0 - 10.10.1	0.11								6	
ile Help											
Home	Configuration	Monitoring	Back	Forward	@ Refresh	🢡 Help				CIS	
Device Informa	tion				Interfac	e Status					
Host Name:	ips	IP Address:	10.10.10.11		Interfa	ice	Link	Enabled	Speed	Mode	0.1
IPS Version:	6.0(4a)E1	Device Type:	IDS-4215-K9	1	FastEth	ernet2/2	🔵 Down	Yes	N/A	Unpaired	~
IDM Version	6.0.202.35	Total Memory:	479 MB		FastEth	ernet2/1	Down	Yes	N/A	Unpaired	
Bypass Mode:	Auto_off	Total Data Storage:	166.8 MB		FastEth	ernet2/0	🙆 Down	Yes	N/A	Unpaired	11
Missed Packets		Total Sensing			FastEth	ernet0/1	Down	Yes	N/A	Unpaired	
Percentage:	0	Interface:	5		FastEth	ernet2/3	Down	Yes	N/A	Unpaired	~
					Select a	n interface	to view recei	ived and tr	ansmitted	packets count.	

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

					Rental fea
Montoring	Back	O Forward	@ Retresh	? Help	cisco
Specify the net	work and co	mmunication p	arameters for	r the sensor.	
Hostname:	IPS				
IP Address:	10.10.10.1	1			
Network Mask:	255.0.0.0				
Default Route:	10,10.10.1	0			
FTP Timeout	300				seconds
Allow Passy	word Recov	ery			
Web Server S	ettings		Remote	Access	1
Enable TLS	S/SSL		Telnet is disabled	not a secure access service and is by default.	
Web server po	ort: 443		🗌 Enat	ble Teinet	
			Apply	Reset	
	Montoring Network Specify the network Hostneme: IP Address: Network Mask: Default Route: FTP Timeout: Vieb Server S Vieb Server po	Montoring Back	Montoring Back Forward Network Specify the network and communication p Hostname: IPS IP Address: 10.10.10.11 Network Mask: 255.0.0.0 Default Route: 10.10.10.10 FTP Timeout: 300 ✓ Allow Password Recovery Web Server Settings ✓ Enable TLS/SSL Web server port: 443	Monitoring Back Forward Refresh Network Specify the network and communication parameters for Hostneme: IPS IP Address: 10.10.10.11 Network Mask: 255.0.0.0 Default Route: 10.10.10.10 FTP Timeout: 300 IV Allow Password Recovery Web Server Settings IV Enable TLS/SSL Teinet is disabled Web server port: 443	Montoring Book Forward Retiresh Help Montoring Book Forward Retiresh Help Network Specify the network and communication parameters for the sensor. Hostname: PS P Address: 10.10.10.11 Network Mask: 255.0.0.0 Default Route: 10.10.10.10 FTP Timeout: 300 FTP Timeout: 300 Allow Password Recovery Web Server Settings Finable TLSISSL Web server port: 443 Finable Teinet

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

File Help					
Home Configuration	Montoring Bac	ck Forward Retresh	🦞 Help		cisco
Sensor Setup	Summary The following is the co promiscuous, inline inte	ntiguration summary of the sensin erface pair, or inline VLAN pair mo	g interfaces. You car de, but no combination	n configure any single physical n of these modes is allowed.	interface for
Known Host Keys	Name	Details		Assigned Virtual Sensor	Descriptio
- Q. Certificates	FastEthernet0/1	Promiscuous Interface		None	
Trusted Hosts	FastEthernet2/0	Promiscuous Interface		None	
Server Certificate	FastEthernet2/1	Promiscuous Interface		None	
B Time	FastEthernet2/2	Promiscuous Interface		None	
🖓 Users 🗧	FastEthernet2/3	Promiscuous Interface		None	
Distances Sector ration Summary Distances Distances Number VLAN Pairs VLAN Groups Distances Dist					

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	6.0 - 10.10.10	11							
File Help									
Home	Configuration	Montoring	Back	Forward	🔞 🤗 Refresh Hel	p			cisco
Sensor Seti M Network Allowed SSH M Aut	up	Interfaces A sensing inter can enable/dis	srface must sable the av	be enabled and allable sensing in	assigned to a virtual : iterfaces by selecting	sensor before ti g the row(s) an	he sensor will m d clicking Enable Speed	onitor that int or Disable. Default	erface. You Select All
S Sen	sor Key	TREET DE E 140	into	Linderos	mount the	Dober	Shood	VLAN	
- Q Certifica	tes	FastEthernet	0/1	Yes	TX (copper)	Auto	Auto	1	Edit
🔁 Tru	sted Hosts	FastEthernet	2/0	Yes	TX (copper)	Auto	Auto		-
Ser Ser	ver Certificate	FastEthernet	2/1	Yes	TX (copper)	Auto	Auto		Enable
Time		FastEthernet2/2		Yes					
S Users		FastEthernet	2/3	Edit In	terface				
Analysis En Analysis En Analysis En Analysis En Analysis En Virtual S Bolicies Bolicies Company Signatu Signatu Company Company Signatu Signat	es Pairs airs aroups Flow Notificatic gine Bensors Aariables re Definitions ction Rules s0 y Detections			Interface I Enabled: Media Typ Duplex: Speed: Default VI Cluse A Select Descriptio	Name: FastEtherr Name: TX (coppe Auto Auto LAN: 0 Nernate TCP Reset in Priorface: FastEther In:	et2.0 No r) v terface net0/1 (v)			
Blocking	Properties	hand			ОК	Can	cel]	Help	

7. Gehen Sie zu **Konfiguration > Schnittstellenkonfiguration > Schnittstellenkombinationen,** und klicken Sie auf **Hinzufügen**, um das Inline-Paar zu

erstellen.

🕲 Cisco ID <i>N</i> File Helo	16.0 - 10.10.10.	11				
Home	Configuration	Monitoring Back	Forward Refres	? h Help		cisco
Sensor Set	up 📩	Interface Pairs You can create logical in pair(s) by selecting the r	iterface pair(s) for the avai ow(s) and clicking Edit or D	lable sensing interfaces. Y elete.	ou can edit/delete the exi	isting interface
Aut	horized Keys	Interface Pair Name	Paired Interfaces		Description	Select All
Ser	nsor Key ates					Add
Ser Ser	sted Hosts ver Certificate		🗇 Add Interface Pa	ir		Edt
B Users	Ξ		Interface Pair Name:	INLINE		Delete
Interface C Summa D Interface VLANC	e Pairs		Select two interfaces:	FastEthernet0/1 FastEthernet2/0 FastEthernet2/1		
Bypass Traffic Analysis Er Vitual	: Flow Notificatic Igine Sensors		6	FastEthernet2/2 FastEthernet2/3		
B Globel V Policies Signatu	Variables re Definitions		Description			
S rule	Action Rules ISD		ок	Cancel	Help	
ad0)	<				
Blocking	g Properties 🗸		Appl	Reset		

8. Zeigen Sie die Zusammenfassung der Inline-Paarkonfiguration an, und wenden Sie sie an.

Cisco IDM	6.0 - 10.10.10	.11						
ile Help								
Home	Configuration	Monitoring	Back	Forward	Refresh	🤗 Help		cisco
Sensor Set Networ Allowed C SSH	up 📤	Interface Pairs You can cre pair(s) by s	aate logical inter electing the row	face pair(s) fi r(s) and clickir	or the available ig Edit or Delet	e sensing interfac le.	es. You can edit/delete the ex	disting interface
Aut	horized Keys	Interface I	Pair Name	Paired In	terfaces		Description	Select All
Certifics Certifics Ser Users Interface Ci Summa Interface Ci Summa Interface VLANF	Isor Key stes sted Hosts ver Certificate ⊐ onfiguration ry es e Pains ains kroups	INLINE		FestEther	net2/0«->Fast	Ethernet24		Add Edt Delete
Analysis Er Analysis Er Oktober Policies Of Signatu Signatu	Flow Notificatic ligite Sensors /ariables re Definitions) .ction Rules a0							
Anomal S adu	y Detections	<						>
Blocking	Properties				Apply		teset	
ne license kev	on the sensor has a	expired on 4/7/0	7 12:00 AM UT	0			cisco adm	inistrator

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

: Help									
Home	Configuration	Monitoring	Back	Forward	Refresh	? Help			cisco
Sensor Setu Network Allowed G SSH	ip (I Hosts hortzed Keys	Virtual Sensor The sensor create a ne clicking Edit	nonitors traffi w virtual sense or Delete.	c that traverse or by clicking A	is interfaces, in Add. You can e	nterface pairs dit or delete s	;, or VLAN pairs assign an existing virtual sense	ied to a virtual sen: or by selecting the	or. You con row(s) and
Sen	wn Host Keys sor Key	Name	Assigned In	terfaces (or P	airs)		Sig Definition Policy	Event Act Poli	Select All
Certifica	ites sted Hosts	vsD					sigD		Add
Anomal	Y es e Pairs airs iroups flow Notificatic gne ionsors instales e Definitions ction Rules s0 y Detections					đ			Delete
ad0		<		.0,	-		The second s	>	
Blocking Blocking	Properties 🔽				Apply		Reset		

10. Weisen Sie das Inline-Paar **INLINE** dem virtuellen Sensor vs0 zu.

-0				
Home Config	juration Monitorina B	C C Refresh Help		CISCO
ensor Setup	🔯 Edit Virtual Sensor			
Network	Virtual Sensor Name:	vs0		
Authorized Ke	Signature Definition Policy:	sig0 💌		
Certificates	Event Action Rules Policy:	rules0 💌		
B Trusted Hosts	Anomaly Detection Policy:	ad0 w		
D Time D Users	AD Operational Mode.	Detect		
terface Configuratio Summary	Inline TCP Session Tracking M	lode: Virtual Sensor		
Dinterfaces	Description:	default virtual sensor		
以 VLAN Pairs 以 VLAN Groups	-Available interfaces			
Bypass	Name	Details	Assigned	Select All
palusis Engine	FastEthernet0/1	Promiscuous Interface	No	-
Virtual Sensors	FastEthernet2/2	Promiscuous Interface	No	Assign
Global Variables	FastEthernet2/3	Promiscuous Interface	No	\leq
olicies Signature Definitio Sign Event Action Rule	PLINE	Inline Interface Pair: FastEthernet2/0<>FastEthernet2/1	Yes	Remove
- Prules0	4	11	5	
Anomaly Detection				
Blocking Propertie		OK Cancel Help		

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

Home Configuration	Montoring	Back	Forward	@ Retresh	🤗 Help			cisco
Sensor Setup Network Allowed Hosts G SSH Authorized Keys	Virtual Senso The senso create a ne clicking Edi	r monitors trattic ew virtual senso t or Delete.	that traverses r by clicking A	interfaces, in dd. You can ei	terface pairs, o dit or delete an	or VLAN pairs assign existing virtual sense	ed to a virtual ser or by selecting the	nsor. You can e row(s) and
Sensor Key	Name	Assigned Int	ertaces (or Pa	rs)		Sig Definition Policy	Event Act Poli	Select All
Sectificates	vs0	INLINE.0 (Inir	e Interface Pai	: FastEtherne	12/0<->FastEth	sig0	1	Add
Anternace Configuration Summary Interfaces Interface Pairs VLAN Pairs VLAN Groups Bypass Traffic Flow Notification Policies Signature Definitions Signature Definitions Signature Definitions								Delete

Konfigurieren des Switches für IDSM-2 im Inline-Modus

Im Abschnitt <u>Konfiguration des Catalyst Switch der Serie 6500 für IDSM-2 im Inline-Modus</u> unter <u>Konfigurieren von IDSM-2</u> können Sie den Switch für den Inline-Modus IDSM-2 konfigurieren.

Fehlerbehebung

Problem

Wenn das IPS ausfällt und inline konfiguriert wird, können die Schnittstellen nicht geöffnet (Datenverkehr geht weiter über) oder geschlossen (Datenverkehr wird verworfen) werden.

Lösung

Sie können IPS im Fail-Open-Zustand konfigurieren. Wenn das IPS ausfällt, wird der Datenverkehr weiterhin weitergeleitet, der Datenverkehr wird jedoch nicht überwacht.

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>
- Technischer Support und Dokumentation Cisco Systems