# IPS 6.X e versioni successive/IDSM2: esempio di configurazione IDM per la modalità Inline Interface Pairs

## Sommario

Introduzione Prerequisiti Requisiti Componenti usati Prodotti correlati Convenzioni Configurazione coppie di interfacce inline Configurazione dalla CLI Configurazione dalla CLI Configurazione IDM Configurazione dello switch per IDSM-2 in modalità inline Risoluzione dei problemi Problema Soluzione Informazioni correlate

## Introduzione

Operando in modalità Inline Interface Pair, il sistema di prevenzione delle intrusioni (IPS) entra direttamente nel flusso del traffico e influisce sulla velocità di inoltro dei pacchetti, che li rallenta quando viene aggiunta la latenza. In questo modo il sensore può arrestare gli attacchi in modo da far cadere il traffico dannoso prima di raggiungere il target previsto, fornendo così un servizio di protezione. Non solo il dispositivo inline elabora le informazioni sui layer 3 e 4, ma analizza anche il contenuto e il payload dei pacchetti per attacchi embedded più sofisticati (layer 3-7). Questa analisi più approfondita consente al sistema di identificare e arrestare e/o bloccare gli attacchi che normalmente passano attraverso un tradizionale dispositivo firewall.

Nella modalità Inline Interface Pair, un pacchetto passa attraverso la prima interfaccia della coppia sul sensore ed esce dalla seconda interfaccia della coppia. Il pacchetto viene inviato alla seconda interfaccia della coppia, a meno che il pacchetto non venga rifiutato o modificato da una firma.

Nota: è possibile configurare AIM-IPS e AIP-SSM in modo che funzionino in linea anche se questi moduli dispongono di una sola interfaccia di rilevamento.

Nota: se le interfacce accoppiate sono connesse allo stesso switch, è necessario configurarle sullo switch come porte di accesso con VLAN di accesso diverse per le due porte. In caso contrario, il traffico non passerà attraverso l'interfaccia inline.

## Prerequisiti

### Requisiti

Nessun requisito specifico previsto per questo documento.

### Componenti usati

Per questo documento, è stato usato un sensore Cisco IPS che usa l'interfaccia della riga di comando 6.0 e IDM (Intrusion Prevention System Device Manager) 6.0.

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 coppie di interfacce inline

Per creare coppie di interfacce inline, usare il comando inline-interfaces name nella modalità secondaria dell'interfaccia del servizio.

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>).

Nota: AIP-SSM è configurato per la modalità interfaccia inline dalla CLI di Cisco ASA e non dalla CLI di Cisco IPS.

Si applicano le seguenti opzioni:

• nome interfacce inline: nome della coppia di interfacce inline logiche

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-state 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
- interface1 interface\_name Prima interfaccia della coppia di interfacce inline
- interface2 interface\_name Seconda interfaccia della coppia di interfacce in linea
- no Rimuove una voce o un'impostazione di selezione
- stato-amministratore {enabled | disabled}: lo stato del collegamento amministrativo dell'interfaccia, sia essa abilitata o disabilitata.

#### Configurazione dalla CLI

Per configurare le impostazioni della coppia di VLAN in linea sul sensore, completare la procedura seguente:

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

```
<#root>
sensor#
configure terminal
sensor(config)#
service interface
```

sensor(config-int)#

```
-
```

3. Verificare se esistono interfacce inline. Il tipo di sottointerfaccia deve leggere none (nessuno) se non sono state configurate interfacce inline:

```
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. Denominare la coppia inline:

<#root>

sensor(config-int)#

```
inline-interfaces PAIR1
```

5. Visualizzare l'elenco delle interfacce disponibili:

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

6. Configurare due interfacce in una coppia:

<#root>

```
sensor(config-int)#
interface1 GigabitEthernet0/0
```

<#root>

sensor(config-int-inl)#

```
interface2 GigabitEthernet0/1
```

È necessario assegnare l'interfaccia a un sensore virtuale e abilitarla prima che possa monitorare il traffico. Per ulteriori informazioni, vedere il passo 10.

7. Aggiungere una descrizione dell'interfaccia:

```
<#root>
sensor(config-int-phy)#
description PAIR1 Gig0/0 and Gig0/1
```

8. Ripetere i passaggi da 4 a 7 per tutte le altre interfacce che si desidera configurare su coppie di interfacce inline.

#### 9. Verificare le impostazioni:

<#root>
sensor(config-int-inl)#
show settings
name: PAIR1
description: PAIR1 Gig0/0 & Gig0/1 default:
interface1: GigabitEthernet0/0
interface2: GigabitEthernet0/1

10. Abilitare le interfacce assegnate alla coppia di interfacce:

```
<#root>
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. Verificare che le interfacce siano abilitate:

#### <#root>

```
sensor(config-int)#
show settings
```

```
physical-interfaces (min: 0, max: 9999999999, 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
    _____
    _____
   _____
   subinterface-type
```



12. Per eliminare una coppia di interfacce inline e ripristinare la modalità promiscua, usare questo comando:

```
<#root>
sensor(config-int)#
no inline-interfaces PAIR1
```

È inoltre necessario eliminare la coppia di interfacce inline dal sensore virtuale a cui è assegnata.

13. Verificare che la coppia di interfacce inline sia stata eliminata:

14. Uscire dalla modalità secondaria di configurazione interfaccia:

```
<#root>
sensor(config-int)#
exit
Apply Changes:?[yes]:
```

15. 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 l'IDM:

- 1. 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.



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

ie Help					
Home Configuration	Montoring	Back Forward	Refresh Help		cisco
Sensor Setue Network SSH Authorized Keys Sensor Key Certificates Sensor Key Certificates Trusted Hosts Server Certificate Time Users Interface Pairs Victual Sensors Victual Sensors Victual Sensors Clobal Variables Potoles Signature Definitions Sign Event Action Rules Sign Event Action Rules Anomaly Detections Sad0 Blocking Potoles	Network Specify the netw Hostname: IP Address: Network Mask: Default Route: FTP Timeout IV Allow Passw Web Server So Web server po	vork and communicatio IPS 10.10.10.11 255.0.0.0 10.10.10.10 300 vord Recovery ttings /SSL rt: 443	Remote Access Teinet is not a secu disabled by default	re access service and is	seconds

5. Selezionare Configurazione > Configurazione interfaccia, quindi fare clic su Riepilogo.

Questa pagina mostra il riepilogo di configurazione dell'interfaccia di rilevamento:

File Help	000							
Home	Configuration	Montoring	Back	Forward	(C) Retresh	🦞 Help		cisco
Sensor Set Network Alower	up k i Hosts	Summery The following is promiscuous, in	the contig line interfa	uration summar ce pair, or inline	y of the sensi VLAN pair m	ng Interfaces. You ca ode, but no combinatio	n configure any single physics on of these modes is allowed.	l interface for
Authorized Keys		Name		Details		Assigned Virtual Sensor	Descriptio	
- Q. Certifics	- Q Cortificates		1	Promiscuous	Interface		None	
True True	sted Hosts	FastEthernet2/0 Promiscu			Interface		None	
Ser Ser	ver Certificate	FastEthernet2/1		Promiscuous	Interface		None	
Time Time		FastEthernet2/2	2	Promiscuous	Interface		None	
- 🛱 Users	8	FastEthernet2/3	3	Promiscuous	Interface		None	
Dinterfac VLANP VLANP DVLANG Bypass	e Pairs eirs eirs iroups							

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



7. Per creare la coppia inline, selezionare Configurazione > Configurazione interfaccia > Coppie di interfacce e fare clic su Aggiungi.

Cisco IDM ile Helo	6.0 - 10.10.10.	.11				
Home	Configuration	Monitoring Back	Forward Refres	🢡 h Help		cisco
Sensor Setu Network Allowed	i Hosts	Interface Pairs You can create logical in pair(s) by selecting the r	nterface pair(s) for the avai row(s) and clicking Edit or D	lable sensing interfaces. Yo elete.	u can edit/delete the exis	ting interface
Aut	horized Keys	Interface Pair Name	Paired Interfaces		Description	Select All
Certifica D True S Serv	ates sted Hosts ver Certificate		Add Interface Pa	ir		Add Edt
B Time Users Interface Co Summar	≡ Infiguration Y		Interface Pair Name:	INLINE		Delete
Dinteriace	e Pairs		Select two interfaces:	FastEthernet0/1 FastEthernet2/0 FastEthernet2/1		
D Bypass Traffic F Analysis En	Tow Notificatic gine Sensors		0	FastEthernet2/2 FastEthernet2/3		
A Global V Policies Signatur Signatur	/ariables re Definitions		Description			
Event A Prules Anomaly adD	ction Rules s0 y Detections	<	ок	Cancel	Help	
Blocking Blocking	Properties 🗸		Appl	Reset		

8. Visualizzare il riepilogo della configurazione della coppia inline e applicarlo.

ie Help								
Home	Configuration	Monitoring B	D ack F	orward Re	🚱 fresh	🤗 Help		cisco
Sensor Setu Network Allowed	p A	Interface Pairs You can create logic pair(s) by selecting t	al interface ne row(s)	e pair(s) for the and clicking Edit	available or Delet	sensing interfac e.	es. You can edit/delete the	existing interface
Aut)	iorized Keys	Interface Pair Name	- 1	Paired Interfac	es		Description	Select All
Sec.	ear Key	INLINE		FastEthernet2.0	->Fasti	Ethernet2/1		
True Service Construction Time Users Interface Construction Summar Interface VLAN P VLAN P VL	ted Hosts ver Certificate antiguration y ss a Pairs airs roups low Notificatic gine ensors ariables e Detinitions ction Rules s0 potections	٤					eset	Edt Delete
				-	-	-		

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

le Help								
Home Configuration	Monitoring	Back	Forward	Refresh	? Help			cisco
Sensor Setup Network Allowed Hosts C SSH Authorized Keys	Virtual Sensor The sensor create a ne clicking Edit	nonitors traffi w virtual sense or Delete.	c that traverse or by clicking A	s interfaces, in dd. You can e	derface pairs dit or delete s	s, or VLAN pairs assign an existing virtual sense	ed to a virtual sen or by selecting the	sor. You can row(s) and
Sensor Key	Name	Assigned In	terfaces (or Pa	irs)		Sig Definition Policy	Event Act Poli	Select All
Trusted Hosts	vs0	<u></u>				sigD		Add
Interface Configuration	4		U.		ð			Delete

10. Assegnare la coppia Inline INLINE al sensore virtuale vs0.

Help									
Home Confi	guration	Monitoring	Back	Forward	Refresh	💡 Help			CISC
Sensor Setup	🕼 Edit	Virtual Sens	or						
Network Allowed Hosts SSH Authorized K Sensor Key Certificates Trusted Host Server Certifi Server Certifi Server Certifi Users Interface Configuratio Summary Interface Pairs VLAN Pairs	Virtual Signatu Event - s Anoma AD Op Inline T Descrit - Avail	Sensor Name: are Definition Poli Action Rules Poli by Detection Poli erational Mode: CP Session Trac otion: able Interfaces -	cy: :y: king Mode:	vs0 sig0 v rules0 v ad0 v Detect v Virtual Sensor default virtual	sensor				
Bypass	Na	me		Details				Assigned	Select Al
Traffic Flow Notif	i Fas	Elhernet0/1		Promiscuous I	nterface			No	
Nalysis Engine	Fas	Ethernet2/2		Promiscuous I	nterface			No	Assign
Ginhal Variables	Fas	Ethernet2/3		Promiscuous I	nterface			No	-
olicies Signature Definiti Sign Sign Levent Action Rule	nLI -	NE		Inline Interface	Pair. FastEthe	met2/0<>Fas	1Ethernet271	Yes	Remove
- Prules0	<			_	18	_		3	1
Anomaly Detectio									51.
Blocking Propertie			(	ок	C	ancel	Help		

11. Visualizza il riepilogo delle informazioni sul sensore virtuale assegnato.

e Help								
Home Configuration	Montoring	Back	Forward	@ Refresh	🤗 Help			cisco
Sensor Setup Network Allowed Hosts G SSH Authorized Keys	Virtual Senso The sensor create a ne clicking Edit	rs montors trattic w virtual senso t or Delete.	that traverse r by clicking A	s interfaces, in dd. You can e	terface pairs, dit or delete an	or VLAN pairs assign existing virtual sense	ed to a virtual sen or by selecting the	isor. You can row(s) and
Sensor Key	Name	Assigned Int	ertaces (or Pa	irs)		Sig Definition Policy	Event Act Poli	Select All
Trusted Hosts	vs0	INLINE.0 (Inin	e Interface Pai	r: FastEtherne	12/0<->FastEth	sig0		Add
A Interfaces Interface Pairs VLAN Pairs VLAN Groups Bypass Traffic Flow Notificatic Aphrois Engine Concol Voltanes Policies Signature Definitions Signature Definitions Sign	٤.			Apriv		Reset	2	
A.			6	C494-0		11121		

## Configurazione dello switch per IDSM-2 in modalità inline

Per configurare lo switch per la modalità in linea IDSM-2, consultare la sezione <u>Configurazione</u> <u>dello switch Catalyst serie 6500</u> per <u>IDSM-2 in modalità in linea</u> di <u>Configurazione di IDSM-2</u>.

## Risoluzione dei problemi

### Problema

Se l'IPS ha esito negativo e viene configurato in linea, le interfacce non saranno aperte (il traffico continuerà a passare) o chiuse (il traffico verrà interrotto).

### Soluzione

È possibile configurare IPS in stato fail-open. Pertanto, se l'IPS si guasta, continuerà a trasmettere il traffico, ma non lo monitorerà.

## 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

#### Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).