# Configurazione di un sensore Cisco Secure IDS in CSPM

## Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Configurazione Definizione della rete in cui risiede l'host CSPM Aggiungere l'host CSPM Aggiungi dispositivo sensore Configurazione del sensore Informazioni correlate

## **Introduzione**

Questo documento spiega la procedura utilizzata per configurare un sensore Cisco Secure Intrusion Detection System (IDS) su Cisco Secure Policy Manager (CSPM). in questo documento si presume che CSPM versione 2.3.I sia stato installato nel computer. La versione "I" consente la gestione di dispositivi IDS (sensori di appliance, router Cisco IOS<sup>®</sup> o blade IDS) in uno switch Cisco Catalyst<sup>®</sup> 6000. Nel documento si presume inoltre che i parametri IDS relativi agli uffici postali siano definiti correttamente. Questi includono HOSTID, ORGID, HOSTNAME e ORGNAME. Notare che affinché l'host CSPM comunichi con un sensore, ORGID e ORGNAME devono corrispondere a quanto definito sul sensore.

# **Prerequisiti**

## Requisiti

Nessun requisito specifico previsto per questo documento.

#### Componenti usati

Le informazioni fornite in questo documento si basano su CSPM 2.3.I e versioni 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.

#### **Convenzioni**

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

## **Configurazione**

Nelle sezioni seguenti viene illustrato il processo utilizzato per configurare un sensore IDS in CSPM.

Avviare CSPM e accedere. Viene visualizzato un modello vuoto (avvio iniziale) che consente di definire la rete.



Queste tre definizioni sono richieste nella topologia CSPM per IDS.

- 1. Definire la rete in cui risiede l'interfaccia di controllo del sensore e la rete in cui risiede l'host CSPM. Se si trovano nella stessa subnet, è necessario definire una sola rete. Definire prima questa rete.
- 2. Definire l'host CSPM nella relativa rete. Senza la definizione dell'host CSPM, il sensore non può essere gestito.
- 3. Definire il sensore nella rete.

## Definizione della rete in cui risiede l'host CSPM

Attenersi alla seguente procedura:

1. Fare clic con il pulsante destro del mouse sull'icona **Internet** nella topologia e selezionare **Nuovo > Rete** per creare una nuova



 Sul lato destro del pannello Rete, aggiungere il nome della nuova rete, l'indirizzo di rete e la netmask che verrà utilizzata.

Ele Edit View Look Woards Help	K Cisco Secure Policy Manager		
Save       Update       One       Sake       Save       Check       Help       Context       State         Image: Save       Network Topology       Internet       Internet       Internet       Internet       Internet         Image: Save       Network Topology       Internet       Internet       Internet       Internet         Image: Save       Reports       Internet Perimeter       Internet       Internet       Internet         Image: Save       Cloud Networks       Cloud Networks       Internet       Internet       Internet         Image: Save       Cloud Networks       Cloud Networks       Internet       Internet       Internet         Image: Save       Cloud Networks       Cloud Networks       Internet       Internet       Internet         Image: Save       Cloud Networks       Internet       Internet       Internet       Internet         Image: Save       Cloud Ne	Eile Edit View Iools Wizards Help		
Image: Serveral Policy         Internet	Save Update Unit: Ficht Back	🔿 🛱 📆 🚧 🍾 🏘	🤗 🔐 View Stat
Network Mask       255.255.0         Umnumbered         Organize the gateway's internal perimeters, including associated interfaces (IP adapters) and networks.         You can perimeters diversions with controls, drag and drop, or right-click popup menu operations. See Help for more details.         Output this view       QK         Quest       Lock this view	Administrative Accounts	General       Internet         Internet       Internet Perimeter         Inter       Int	Insert New  Permeter  Interface  Network  Edit Network Selection Name Network 1  Network Address  TZ 18 124 0 Network Address  TZ 18 124 0 Network Mask 255 255 0  Unnumbered  Og Organize the gateway's internal perimeters, including associated interfaces (IP adapters) and networks.  You can perform these actions with controls, diag and drop, or ight-cick popup menu operations. See Help for more details.  Dancel Help

- 3. Fare clic sul pulsante **Indirizzo IP** e immettere l'indirizzo IP della rete utilizzato per raggiungere Internet.In genere si tratta del gateway predefinito per la rete.**Nota:** quando si gestiscono i sensori, l'indirizzo del gateway non deve essere necessariamente corretto, in quanto al sensore non vengono inviate le informazioni sul gateway predefinito. Dovrebbe già essere definita nel Sensore.
- 4. Fare clic su **OK**. La rete viene aggiunta alla mappa della topologia senza errori.

eve Update Undo Hr07 Back	General Interfaces Petimeters	ntext Start
A Internet	a Internet	Insert New
Tools and Services     Peparts     Administrative Accounts	Internet Perimeter     Internet Perimete	Permeter Interface Network IP Address Edit Network Selection Name Network 1 Network Address 172 18 124 0 Network Mask 255 255 255 0
	Delete Move Up Move Dawn	Organize the gateway's internal perimeters, including associated interfaces (IP adapters) and networks.           You can perform these actions with controls, drag and drop, or right-click popup menu operations. See Help for more details.           Cancel         Help

## Aggiungere l'host CSPM

Utilizzare questa procedura per aggiungere l'host CSPM.

 Nella Topologia di rete, fare clic con il pulsante destro del mouse sulla rete appena aggiunta e selezionare Nuovo > Host.CSPM visualizza una schermata simile a questa. In caso contrario, la rete appena definita non è quella in cui si trova l'host CSPM. Controllare nuovamente l'indirizzo IP sull'host

Cisco S	ecure Policy Manager 🛛 🕅
?	A network object of the specified type has been detected in the Policy Database, and the external address of the object is consistent with the parent network address.
	The name of this object is "CSPM "
	Is this the object you wish to insert into the Network Topology? If so click 'Yes', otherwise 'No'.
	Yes No

- 2. Fare clic su Sì per installare l'host CSPM nella topologia.
- 3. Verificare che le informazioni nella schermata Generale per l'host CSPM siano corrette.
- 4. Fare clic su **OK** nella schermata Generale dell'host CSPM.

#### Aggiungi dispositivo sensore

Utilizzare questa procedura per aggiungere la periferica sensore.

 Fare clic con il pulsante destro del mouse sulla rete in cui risiede il sensore e selezionare Procedure guidate > Aggiungi sensore.Nota: se l'host CSPM e l'interfaccia di controllo del sensore non si trovano nella stessa rete, definire la rete in cui risiede il sensore.



2. Immettere i parametri corretti per il sensore.

elcome to the Ad d press Next.	dd Sensor Wizard. To add a S	ensor to the topology fill in the following information
Sensor Identifica	tion	
iensor Name	Sensor1	Host ID 99 Org. ID 1
)rganization Nam	ne <mark>Itp</mark>	Policy Enforcement Associated
IP Address	172 . 18 . 124 . 99	Network Cisco Post Office     Service
Postoffice Heartbeat Interv	al 5	Port UDP 45000
Comments		
Check here t	o verify the Sensor's address.	Enter the IP Address and the Host
		ID will populate automatically. Ur

- 3. Fare clic su Controlla qui per verificare l'indirizzo del sensore nella casella.Nota: se è la prima volta che si configura questo sensore, non si desidera acquisire la configurazione del sensore. Se il sensore è stato precedentemente configurato in un'altra posizione tramite un director UNIX o un altro host CSPM e sono state apportate modifiche alla configurazione delle firme dei sensori, acquisire la configurazione del sensore.
- 4. Fare clic su **Avanti** per definire le versioni della firma sul sensore. Per verificare questa condizione sul sensore, è possibile anche usare il comando **nrvers**.

IPSec support. Choose the app Distribution	propriate Signature Template from the drop down lists. Select the Cisco Secure Policy Manager
(I)	device-specific command sets to this device.
Sensor Version 301158	IPSec     Check here to enable IPSec on     supported Sensor versions.
Signature Template Default Template Comment	
Cisco Systems, Inc. default Si	gnature Template settings.
There are 3 signatures in the	e latest signature update (3.0(1)S8) that do not apply to this

: se CSPM non dispone della versione corretta del sensore in esecuzione sul sensore, aggiornare le firme sull'host CSPM. Per gli aggiornamenti, vedere <u>Download del software</u> (solo utenti <u>registrati</u>).

- 5. Per continuare, fare clic sul pulsante Avanti.
- 6. Fare clic su **Fine** per completare l'installazione del sensore nella topologia.
- Dal menu principale di CSPM, selezionare File > Salva e Aggiorna per compilare in CSPM le informazioni immesse nella topologia. Questo passaggio è necessario per avviare il protocollo dell'ufficio postale sull'host CSPM.
- 8. Verificare che tutto funzioni accedendo al sensore come utente netranger.
- 9. Eseguire il comando **nrconns**.

```
Connection Status for gacy.rtp
```

cspm.rtp Connection 1: 172.18.124.106 45000 1 [Established] sto:0004 with Version 1

netrangr@gacy:/usr/nr

>

**Nota:** se il sensore e l'host CSPM non comunicano, viene visualizzato un output simile a questo:

netrangr@gacy:/usr/nr

#### >nrconns

```
Connection Status for gacy.rtp
insane.rtp Connection 1: 172.18.124.194 45000 1 [SynSent]
sto:5000 syn NOT rcvd!
```

#### netrangr@gacy:/usr/nr

In questo caso, ottenere una traccia dello sniffer per verificare se entrambi i dispositivi inviano pacchetti UDP 4500. UDP 4500 è ciò che i dispositivi IDS utilizzano per comunicare tra loro. Per verificarlo sul sensore, **passare** alla radice e (a seconda del sensore in uso) eseguire **snoop -d iprb1 porta 45000** (per un sensore IDS 4210) e **snoop -d iprb0 porta 45000** (per qualsiasi altro modello di sensore).Utilizzare **<control-c>** per interrompere una sessione snoop.Questo output viene visualizzato se non vi sono comunicazioni tra il sensore e CSPM:

netrangr@gacy:/usr/nr

>su -

Password:

Sun Microsystems Inc. SunOS 5.8 Generic February 2000

# snoop -d spwr0 port 45000

Using device /dev/spwr (promiscuous mode)

172.18.124.100 -> 172.18.124.106 UDP D=45000 S=45000 LEN=52 172.18.124.100 -> 172.18.124.106 UDP D=45000 S=45000 LEN=52 172.18.124.100 -> 172.18.124.106 UDP D=45000 S=45000 LEN=52 172.18.124.100 -> 172.18.124.106 UDP D=45000 S=45000 LEN=52

^C#

Nell'output precedente, il sensore invia pacchetti UDP 4500, ma non ne riceve alcuno. Una configurazione corretta produce un output simile al seguente: # snoop -d spwr0 port 45000

Using device /dev/iprb (promiscuous mode) 172.18.124.106 -> gacy UDP D=45000 S=45000 LEN=56 gacy -> 172.18.124.106 UDP D=45000 S=45000 LEN=56 172.18.124.142 -> gacy UDP D=45000 S=45000 LEN=56

gacy -> 172.18.124.194 UDP D=45000 S=45000 LEN=56

Nell'output precedente, il traffico UDP 4500 va in entrambe le direzioni.Se i pacchetti UDP 4500 vengono trasmessi in entrambe le direzioni e l'output di **nrconns** sul sensore continua a indicare che non è stata stabilita una connessione, i parametri della postazione sul sensore e sull'host CSPM non corrispondono.Per controllare manualmente i parametri di postoffice sull'host CSPM:Utilizzare Esplora risorse per passare alla posizione in cui è installato CSPM nel computer NT.

etc		• 🗈 墙 🔚	8 B C ×		
lame	Size	Туре	Modified	Attributes	
auths	1KB	File	10/10/01 12:53 PM	A	
auths.bak	1KB	BAK File	10/10/01 12:38 PM	A	
daemons	1KB	File	9/27/01 10:45 AM	A	
destinations	1KB	File	10/8/01 5:37 PM	A	
destinations.bak	1KB	BAK File	9/27/01 10:45 AM	A	
A hosts	1KB	File	10/10/01 12:53 PM	A	
hosts.bak	1KB	BAK File	10/10/01 12:38 PM	A	
organizations	1KB	File	9/27/01 10:45 AM	A	
postofficed.conf	1KB	CONF File	10/8/01 5:37 PM	A	
postofficed.conf.tmp	1KB	TMP File	10/10/01 12:05 PM	A	
routes	1KB	File	10/10/01 12:53 PM	A	
routes.bak	1KB	BAK File	10/10/01 12:38 PM	A	
sapd.conf	3KB	CONF File	8/8/01 11:26 PM	A	
services	2KB	File	8/8/01 11:26 PM	A	
signatures	10KB	File	8/8/01 11:26 PM	A	
smid.conf	1KB	CONF File	10/8/01 5:37 PM	A	
smid.conf.bak	1KB	BAK File	9/27/01 10:45 AM	A	
7 object(s)	18.4KB	(			

Modificare i file dell'host, della route e dell'organizzazione con Write o Wordpad (non utilizzare il Blocco note perché la formattazione risulterà danneggiata).Verificare che i file siano corretti per l'installazione. Se uno dei valori non è corretto, modificarlo e riavviare il computer NT attenendosi alla seguente procedura:Fare clic sull'icona **CSPM** nella topologia di rete.Fare clic sulla scheda Distribuzione dei criteri per immettere i parametri relativi all'ufficio postale.**Salvare** e **aggiornare** le modifiche.Riavviare il computer NT.



#### Configurazione del sensore

Dopo aver salvato la configurazione in CSPM, configurare il sensore. A tale scopo, impostare il sensore in modo che scriva gli allarmi rilevati sul proprio registro. Quindi impostare il sensore su "sniff" sull'interfaccia corretta.

#### Scrivi avvisi nel registro

Utilizzare questa procedura per scrivere gli allarmi nel registro.

1. Fare clic sulla casella **Genera file registro eventi di controllo** per indicare al sensore di inviare gli allarmi ai registri locali.Per impostazione predefinita, invia inoltre allarmi al modulo CSPM dopo aver eseguito il push di una configurazione.



2. Fare clic su OK per continuare.

#### Impostare il sensore su "Sniffa"

Utilizzare questa procedura per impostare il sensore su "Sniffing".

- 1. Selezionare il sensore nella topologia CSPM e fare clic sulla scheda Rilevamento.
- Definire il dispositivo di acquisizione pacchetti:iprb0 per sensore IDS 4210spwr0 per qualsiasi altro modello di sensore



- 3. Fare clic su **OK** per continuare.
- 4. Fare clic sull'icona Aggiorna nella barra dei menu di CSPM per aggiornare CSPM con le informazioni.Nota: se tutto va bene, appare una schermata simile a questa. Si noti che non sono presenti errori rossi. Le avvertenze gialle sono in genere corrette.



5. Selezionare il sensore nella topologia di rete e fare clic sulla scheda Comando per inviare la configurazione aggiornata al

Vew Iools Wizards Help	이 5년 4월 Kon 4 19 2	1
III ⊨⊃ Cu	Lock Tearoft Find Check Help Context St	
Network Policy     Security Policy Enforcement     Case System Folder     Case System Folder     System Ovenides     INSANE     Trusted Networks     Default Policy     InFarmet     Network Topology     Internet     Network Topology     Internet     Security Policy Abstracts     System Policies     System Policies     System Policies     Network Services     Service Bundles     Policy Domains     Network Services     Service Signatures     Default     Network Services     Service Signatures     Default     Network Service Bundles     Policy Domains     Network Service I 172.1     Security Police Groups     Internet Interface 1: 172.1     Gacy Interface 1     Case 1     Gacy Interface 1     Security Police 1: 172.18	Properties Sensing Blocking Filtering Logging Adva gacy Command Review/Edt Generated Commands Control devices/Edt Generated at 10/12/0 # Sensor IP Alas: 172 18 Sensor IP Alas: 172 18 Sensor IP Alas: 172 18 Control Agert Name: INS Control Agert Name: INS Control Agert Most ID: 1 Control Agert Most ID	nced Command Control   Status Processing completed 13 (no errors) Policy 3 Eol aration 111:51:16 (Eastern Daylight Time) 22 22:24:106 SANE Ser Ap 1:24:106 06 File Import. File Export.

6. Fare clic sul pulsante Approva ora per inviare la configurazione al

sensore.				
				-O×
I 🕤 :k Tearoff	M Kon Find Check	🤣 😽 Help Conte	ext Start	
Sensing Bloc	sking   Filtering   L	.ogging   Adva	nced Command Conti	rol]
n-210			Transfering	files to sensor
	Commands/	/Messages	Policy 0	Poll
Review/Edit-	# # Stort of S	iensor Configur	ation	4
<u> </u>	L # # Do not e	dit!	2.011	
ig Commands	# # Generate	ed at 01/18/01	10:59:55 (Central Standa	rd Time) N

el riquadro di stato viene visualizzato il messaggio "Caricamento <#> completato". Indica un processo di trasferimento valido e completo. Il sensore è stato aggiornato e ora dovrebbe funzionare normalmente.Se il sensore non funziona normalmente, tornare al sensore e controllare l'output del comando **nrconns** per verificare che la connessione tra l'host CSPM e il sensore sia stata

stabilita.

\¶∐ k Tearoff	Find Chec	.k Help C	<b>№</b> .Щ ontext Start		
Sensing   Bloc	king   Filtering	Logging   A	dvanced Cor	nmand Contro	a ]
i-2111				> Upload 1 comp	leted (no errors)
			http://www.angle.com/angle.com/angle.com/angle.com/angle.com/angle.com/angle.com/angle.com/angle.com/angle.com/		/

termine, è possibile cercare gli allarmi inviati dal sensore all'host CSPM nel visualizzatore eventi. Per visualizzare il Visualizzatore eventi, dal menu principale di CSPM selezionare **Strumenti > Visualizza eventi sensore >** 

ant		9	
10/10/01	7		
5.59.46 PM			
		8	
10/10/01	7		
5:59:46 PM	<u></u>		
	ent 10/10/01 5.59:46 PM 10/10/01 5:59:46 PM	ent 10/10/01 5.59.46 PM 10/10/01 5:59:46 PM 5:59:46 PM	ent 10/10/01 ▼ 5:59:46 PM 10/10/01 ▼ 5:59:46 PM 5:59:46 PM

#### Database.

visualizzare la finestra del database degli eventi. Lo schermo varia a seconda degli allarmi che si

#### ricevono

* 10.32.10.10	172.18.124.154						
10.32.10.10	172.18.124.154						
10.32.10.10	172.18.124.154	Conservation -					
• • ii		<rione></rione>	OUT	OUT	0	Low	rtp
+							
<none></none>	<none></none>	postofficed initial notification msg	OUT	OUT	0	Low	rtp
(none)	<none></none>	+					
(none)	<none></none>	1993 - Carlo Ca					
' <b>₩</b> (1)							
	(none) (none) (none) +	<pre><none> <none> <none> <none> +</none></none></none></none></pre>	<pre><none> <none> postofficed initial notification msg <none> + <none> <none> + </none></none></none></none></none></pre>	<pre><none> <none> postofficed initial notification msg OUT <none> + <none> + + +</none></none></none></none></pre>	<pre><none> <none> postofficed initial notification msg_OUT OUT (none&gt; <none> +</none></none></none></pre>	<pre><none> <none> postofficed initial notification msg OUT OUT 0 <none> <hood line=""> + </hood></none></none></none></pre>	<pre><none> <none> postofficed initial notification msg_OUT OUT O Low (none&gt; <none> +</none></none></none></pre>

# Informazioni correlate

Documentazione e supporto tecnico – Cisco Systems