Konfigurieren eines Cisco Secure IDS Sensors in CSPM

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Konfiguration Definieren des Netzwerks, auf dem sich der CSPM-Host befindet Hinzufügen des CSPM-Hosts Hinzufügen des Sensorgeräts Konfigurieren des Sensors Zugehörige Informationen

Einführung

In diesem Dokument wird das Verfahren zur Konfiguration eines Cisco Secure Intrusion Detection System (IDS)-Sensors im Cisco Secure Policy Manager (CSPM) beschrieben. In diesem Dokument wird davon ausgegangen, dass Sie CSPM Version 2.3.1 auf Ihrem Computer installiert haben. Version "I" ermöglicht die Verwaltung von IDS-Geräten (Appliance-Sensoren, Cisco IOS[®]-Router oder IDS-Blades) in einem Cisco Catalyst[®] Switch der Serie 6000. In diesem Dokument wird auch davon ausgegangen, dass die IDS-Parameter korrekt definiert sind. Dazu gehören HOSTID, ORGID, HOSTNAME und ORGNAME. Beachten Sie, dass die ORGID und der ORGNAME für die Kommunikation zwischen dem CSPM-Host und einem Sensor den auf dem Sensor definierten Werten entsprechen müssen.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf CSPM 2.3.1 und höher.

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.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den <u>Cisco Technical Tips</u> <u>Conventions</u>.

Konfiguration

In diesen Abschnitten wird der Prozess zum Konfigurieren eines IDS-Sensors in CSPM erläutert.

Starten Sie CSPM, und melden Sie sich an. Es wird eine leere Vorlage (Erststart) angezeigt, mit der Sie Ihr Netzwerk definieren können.



Diese drei Definitionen sind in der CSPM-Topologie für IDS erforderlich.

- 1. Definieren Sie das Netzwerk, in dem sich die Steuerungsschnittstelle des Sensors befindet, und das Netzwerk, in dem sich der CSPM-Host befindet. Wenn sie sich im gleichen Subnetz befinden, muss nur ein Netzwerk definiert werden. Definieren Sie dieses Netzwerk zuerst.
- 2. Definieren Sie den CSPM-Host in seinem Netzwerk. Ohne die CSPM-Hostdefinition kann der Sensor nicht verwaltet werden.
- 3. Definieren Sie den Sensor im Netzwerk.

Definieren des Netzwerks, auf dem sich der CSPM-Host befindet

Gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf das **Internet-**Symbol in der Topologie, und wählen Sie **New > Network** aus, um ein neues Netzwerk zu



2. Fügen Sie auf der rechten Seite der Netzwerkleiste den Namen des neuen Netzwerks, die Netzwerkadresse und die Netzmaske hinzu, die verwendet werden soll.

Elle Edit View Iools Wisards Help	Reso Secure Policy Manager		_ [] ×
	Eile Edit View Iools Wisands Help		
Save Update Under Richt Back, Foreinic Lock, Tearoff Find Check, Help Context, Start	Save Update Unit: First: Back F	🐡 🖄 📆 🚧 🌇 🤗 紀 🚜 Formano Lock Tearoff Find Check Help Context Start	
Image: Second Services Image: Second Servic	Administrative Accounts	General Interfaces Perimeters Internet Intetwork Internet	

- 3. Klicken Sie auf die Schaltfläche **IP-Adresse**, und geben Sie die IP-Adresse für Ihr Netzwerk ein, mit der es das Internet erreicht.Normalerweise ist es das Standard-Gateway für das Netzwerk.**Hinweis:** Wenn Sie Sensoren verwalten, muss die Gateway-Adresse nicht unbedingt korrekt sein, da der Sensor diese Standard-Gateway-Informationen nicht sendet. Sie sollte bereits im Sensor definiert sein.
- 4. Klicken Sie auf **OK**. Das Netzwerk wird der Topologieübersicht ohne Fehler hinzugefügt.

E 18. Network Policy	General Interfaces Perimeters	
	3 loternet	Insert New
Administrative Accounts	Internet Perimeter Internet Perimeter Interlace 1 Interlace 1	Permeter Interface Network
		Edit Network Selection Name Network 1 Network Address 172 .18 .124 .0 Network Mask 255 .255 .0
		You can perform these actions with controls, diag and drop, or right-click popup menu operations. See Help for more details.

Hinzufügen des CSPM-Hosts

Verwenden Sie diese Prozedur, um den CSPM-Host hinzuzufügen.

 Klicken Sie in der Netzwerktopologie mit der rechten Maustaste auf das Netzwerk, das Sie gerade hinzugefügt haben, und wählen Sie Neu > Host aus.CSPM zeigt einen ähnlichen Bildschirm an. Ist dies nicht der Fall, ist das Netzwerk, das Sie gerade definiert haben, nicht das Netzwerk, in dem sich Ihr CSPM-Host befindet. Überprüfen Sie erneut die IP-Adresse auf Ihrem CSPM-



- 2. Klicken Sie auf Ja, um den CSPM-Host in die Topologie zu installieren.
- 3. Überprüfen Sie, ob die Informationen auf dem Bildschirm "Allgemein" für den CSPM-Host korrekt sind.
- 4. Klicken Sie auf dem Bildschirm "Allgemein" des CSPM-Hosts auf OK.

Hinzufügen des Sensorgeräts

Verwenden Sie dieses Verfahren, um das Sensorgerät hinzuzufügen.

 Klicken Sie mit der rechten Maustaste auf das Netzwerk, in dem sich der Sensor befindet, und wählen Sie Assistenten > Sensor hinzufügen aus.Hinweis: Wenn sich der CSPM-Host und die Steuerungsschnittstelle Ihres Sensors nicht im gleichen Netzwerk befinden, definieren Sie das Netzwerk, in dem sich Ihr Sensor befindet.



2. Geben Sie die korrekten Parameter für die Leistung des Sensors ein.

Velcome to the Add ind press Next.	Sensor Wizard. To add a Sen	sor to the topology fill in the following information
Sensor Identification	n	10. 20. 10. 10. 10. 10.
Sensor Name	Sensor1	Host ID 99 Org. ID 1
Organization Name	Itb	Policy Enforcement Associated
IP Address	172 . 18 . 124 . 99	- Network Uisco Post Uffice Service
Postoffice Heartbeat Interval	5	Port UDP 45000
Comments		
Check here to	varify the Sensor's address	Enter the IP Address and the Host
	venity are bensor a dudress.	ID will populate automatically. Or

- 3. Klicken Sie auf **Hier prüfen, um das** Feld **Adresse des Sensors zu überprüfen.Hinweis:** Wenn Sie diesen Sensor zum ersten Mal einrichten, möchten Sie die Konfiguration des Sensors nicht erfassen. Wenn Sie diesen Sensor zuvor entweder über einen UNIX-Director oder einen anderen CSPM-Host an einem anderen Ort konfiguriert und Konfigurationsänderungen an den Sensorsignaturen vorgenommen haben, dann können Sie die Konfiguration des Sensors erfassen.
- 4. Klicken Sie auf **Weiter**, um die Signaturversionen auf dem Sensor zu definieren. Sie können auch den Befehl **nrvers** ausführen, um dies auf dem Sensor zu überprüfen.

IPSec support. Choose the Distribution	e appropriate Si	gnature Template from the drop down li Select the Cisco Secure Policy Mana bot that will publish the generated	sts. ger
(I)	1	device-specific command sets to this	device.
Sensor Version	8	IPSec Check here to enable IPSec of supported Sensor versions.	n
Signature Template De Template Comment	fault	<u> </u>	•
Cisco Systems, Inc. defa	ult Signature Te	mplate settings.	
There are 3 signatures	in the latest sign	ature update (3.0(1)S8) that do not app	ly to this

eis: Wenn CSPM nicht über die richtige Sensorversion verfügt, die Sie auf Ihrem Sensor ausführen, aktualisieren Sie die Signaturen auf Ihrem CSPM-Host. Informationen zu Aktualisierungen finden Sie unter <u>Software Download</u> (nur <u>registrierte</u> Kunden).

- 5. Klicken Sie auf die Schaltfläche Weiter, um fortzufahren.
- 6. Klicken Sie auf **Fertig stellen**, um die Installation des Sensors in die Topologie abzuschließen.
- 7. Wählen Sie im CSPM-Hauptmenü Datei > Speichern und Aktualisieren aus, um die in die Topologie eingegebenen Informationen in CSPM zu kompilieren. Bitte beachten Sie, dass dieser Schritt erforderlich ist, um das Protokoll "POSTOffice" auf dem CSPM-Host zu starten.
- 8. Stellen Sie sicher, dass alles funktioniert, indem Sie sich beim Sensor als Netzwerkbenutzer anmelden.
- 9. Führen Sie den Befehl **nrconns aus**.

```
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
```

>

Hinweis: Wenn der Sensor und der CSPM-Host nicht miteinander kommunizieren, wird stattdessen eine ähnliche Ausgabe angezeigt:

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

Wenn dies der Fall ist, rufen Sie eine Sniffer-Trace ab, um festzustellen, ob beide Seiten UDP 45000-Pakete senden. Die IDS-Geräte verwenden UDP 45000 für die Kommunikation untereinander. Um dies auf dem Sensor zu testen, **su** zu root und (abhängig von dem Sensor, den Sie haben) führen **snoop -d iprb1 Port 45000** (für einen IDS 4210 Sensor) und **snoop -d iprb0 Port 45000** (für jedes andere Sensormodell) aus.Verwenden Sie **<control-c>**, um eine Snoop-Sitzung zu beenden.Diese Ausgabe wird angezeigt, wenn zwischen dem Sensor und dem CSPM keine Kommunikation besteht:

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#

In der obigen Ausgabe sendet der Sensor UDP 45000-Pakete, empfängt jedoch keine. Eine richtige Konfiguration erzeugt eine ähnliche Ausgabe wie die folgende: # 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

In der obigen Ausgabe verläuft der UDP 4500-Datenverkehr in beide Richtungen.Wenn UDP 45000-Pakete in beide Richtungen fließen und die Ausgabe von **Nrconns** auf dem Sensor immer noch besagt, dass keine Verbindung hergestellt wurde, stimmen die Postoffice-Parameter auf dem Sensor und dem CSPM-Host nicht überein.So überprüfen Sie die Parameter für das POSTLEISTUNGSVERHÄLTNIS auf dem CSPM-Host manuell:Navigieren Sie mit Windows Explorer zu dem Speicherort, auf dem CSPM auf dem NT-System installiert

10	ct	۰.
15	วเ	

y etc					
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	
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	

Bearbeiten Sie die Host-, Route- und Organisationsdateien mit Write oder Wordpad (verwenden Sie nicht Notepad, da die Formatierung beschädigt ist).Stellen Sie sicher, dass diese Dateien für Ihre Installation richtig aussehen. Wenn eine der Werte nicht korrekt ist, bearbeiten Sie sie und starten Sie Ihren NT-Computer wie folgt neu:Klicken Sie in der Netzwerktopologie auf das **CSPM**-Symbol.Klicken Sie auf die Registerkarte "Policy Distribution" (Richtlinienverteilung), um Ihre Postoffice-Parameter einzugeben.**Speichern** und **Aktualisieren** Ihrer ÄnderungenStarten Sie den NT-Computer neu.



Konfigurieren des Sensors

Nachdem die Konfiguration im CSPM gespeichert wurde, konfigurieren Sie den Sensor. Legen Sie dazu zunächst den Sensor fest, um die angezeigten Alarme in das eigene Protokoll zu schreiben. Stellen Sie dann den Sensor auf "schnüffeln" an der richtigen Schnittstelle ein.

Alarme in das Protokoll schreiben

Verwenden Sie diese Prozedur, um Alarme in das Protokoll zu schreiben.

 Klicken Sie auf das Feld Protokolldateien f
ür
Überwachungsereignisse generieren, um dem Sensor mitzuteilen, dass er die Alarme an seine lokalen Protokolle senden soll.Sie sendet ebenfalls standardm
äßig Alarme an das CSPM-Feld, nachdem Sie eine Konfiguration nach unten gepresst haben.



2. Klicken Sie auf OK, um fortzufahren.

Stellen Sie den Sensor auf "Sniff" ein.

Mit diesem Verfahren setzen Sie den Sensor auf "Sniff".

- 1. Wählen Sie den Sensor in der CSPM-Topologie aus, und klicken Sie auf die Registerkarte Sensing (Sensoren).
- 2. Definieren des Paketerfassungsgeräts:iprb0 für einen IDS 4210-Sensorspwr0 für jedes andere

Sensormodell



- 3. Klicken Sie auf **OK**, um fortzufahren.
- 4. Klicken Sie in der CSPM-Menüleiste auf das Symbol Update (Aktualisieren), um CSPM die Informationen zu aktualisieren. Hinweis: Wenn alles gut geht, wird ein ähnlich gelagerter Bildschirm angezeigt. Beachten Sie, dass keine roten Fehler vorliegen. Gelbe Warnungen sind in der Regel in Ordnung.



5. Wählen Sie den Sensor in der Netzwerktopologie aus, und klicken Sie auf die Registerkarte Command (Befehle), um die aktualisierte Konfiguration an den Sensor zu senden

Update 1735 Head Black Porward ********************************	Properties Sensing Blocking Filtering	Logging Advance	ed Command Control	1
R. System Overrides NSANE Trusted Networks Networks	Enmond Visiver	ls/Messages	Processing comple Policy 3	ted 13 (no errors)
Network Topology Invernet Network 1 Network 1 Network 1 Network 2 Security Policy Abstracts Network Service Bundles Policy Domains Network Services Policy Domains Network Services Security Policy Abstracts Internet Internet Interface 1 Internet Interface 1 Internet Interface 1 Security Policy Interface 1: 172.18.	Generated Commands Generated Command	of Sensor Configural at edit! Name: gacy Organization: rtp IP: 172.18.124.122 IP: Afas: 172.18.124 Host ID: 122 Org ID: 1 Agent Vorganization: Agent IP: 172.18.12 Agent Vorganization: Agent IP: 172.18.12 Agent Host ID: 10 ce Port: 45000 Eind	ion 1:51:16 (Eastern Dayligh 105 IE Rp 4.106 File I <u>mpo</u>	t Time)

6. Klicken Sie auf die Schaltfläche Jetzt genehmigen, um die Konfiguration an den Sensor zu

senden.			
			-o×
I 🕤	йн ^иок 🤗 Find Check Help (№ <u>№</u> Context Start	
Sensing Block	king Filtering Logging A	Advanced Command Cont	irol
- 910		_ Status	
n-210		Transfering	files to sensor
	Commands/Messages	Policy 0	<u>P</u> oll
Review/Edit-			
	# # Start of Sensor Con	figuration	-
Befresh	#	ingaradori	
	📕 🛱 Do not edit!		
	#		
ig Lommands	# Generated at 01/18	3/01 10:59:55 (Central Standa	ard I imej 🛛 🔤 Im

Statusbereich wird die Meldung "Hochladen <#> abgeschlossen" angezeigt. Dies bedeutet einen gültigen und vollständigen Transfer-Prozess. Der Sensor ist jetzt aktualisiert und sollte nun normal ausgeführt werden.Wenn der Sensor nicht normal ausgeführt wird, kehren Sie zum Sensor zurück, und überprüfen Sie die Ausgabe des Befehls **nrconns**, um sicherzustellen, dass die Verbindung zwischen dem CSPM-Host und dem Sensor hergestellt wird.

k Te	aroff Fin	d Check	🤣 Help	№? Context	,⊉ Start	
Sensing) Blocking	Filtering l	_ogging	Advance	d Command	Control
i-2111					Upload 1	completed (no errors)
					Policy 1	Eol

ach Abschluss dieses Vorgangs können Sie in der Ereignisanzeige nach Alarmen suchen, die der Sensor an den CSPM-Host sendet. Um die Ereignisanzeige anzuzeigen, wählen Sie im CSPM-Hauptmenü **Extras > Sensorereignisse anzeigen > Datenbank**

Time			
- I ime Start			
At Earliest E	Event		
C At <u>T</u> ime:	10/10/01	7	
Now	5.59:46 PM		
Stop			
C <u>A</u> t Time:	10/10/01	7	
Now	5:59:46 PM		
Don't Stop			

Datenbankfenster Ereignisse anzuzeigen. Ihr Bildschirm hängt von den Alarmen ab, die Sie möglicherweise

erhalten.

sho request iod	· · · · · ·							
od	- •							
much attacks								
HUIT OTTOCK	. • U.							
nreachable	10.32,10.10	172.18.124.154	<none></none>	OUT	OUT	0	Low	rtp
ents overlap	l # 11							
ep-echo	•							
ce Initial Notification	<none></none>	<none></none>	postofficed initial notification msg	OUT	OUT	0	Low	rtp.
owni	<none></none>	<none></none>	+					
lp	(none)	<none></none>	3 9 3					
ecket	1 🐮 (II)							
	rreachable ents overlap ep-echo ce Initial Notification own! p cket	reachable 10.32,10,10 ents overlap + ep-echo + ce Initial Notification <none> own! <none> p <none> cket +</none></none></none>	reachable 10.32.10.10 172.18.124.154 ents overlap + ep-echo + ce Initial Notification <none> <none> own! <none> <none> p <none> <none> <none> cket +</none></none></none></none></none></none></none>	Ineachable 10.32,10.10 172,18,124,154 <none> ents overlap + - <td< td=""><td>IIII accurate 10.32.10.10 172.18.124.154 <none> DUT ents overlap + -</none></td><td>IIII 32:10:10 172:18:124:154 <none> DUT OUT ents overlap + - ce Initial Notification - - - - - - - - -</none></td><td>Iteachable 10.32.10.10 172.18.124.154 (none> OUT OUT</td><td>Iteachable 10.32.10.10 172.18.124.154 (none> OUT OUT OUT 0 Low ents overlap + -</td></td<></none>	IIII accurate 10.32.10.10 172.18.124.154 <none> DUT ents overlap + -</none>	IIII 32:10:10 172:18:124:154 <none> DUT OUT ents overlap + - ce Initial Notification - - - - - - - - -</none>	Iteachable 10.32.10.10 172.18.124.154 (none> OUT OUT	Iteachable 10.32.10.10 172.18.124.154 (none> OUT OUT OUT 0 Low ents overlap + -

Zugehörige Informationen

• Technischer Support und Dokumentation - Cisco Systems