Een Cisco Secure IDS-sensor in CSPM configureren

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Conventies Configuratie Bepaal het netwerk waarop de CSPM-host verblijft Voeg de CSPM-host toe Het sensor-apparaat toevoegen De sensor configureren Gerelateerde informatie

Inleiding

Dit document legt de procedure uit die wordt gebruikt om een Cisco Secure Inbraakdetectiesysteem (IDS)-sensor (Cisco Secure Policy Manager (CSPM) te configureren. Bij dit document wordt ervan uitgegaan dat u CSPM versie 2.3.1 op uw computer hebt geïnstalleerd. Versie "I" maakt het beheer mogelijk van IDS-apparaten (toevoersensoren, Cisco IOS[®] routers of IDS-blades) in een Cisco Catalyst[®] 6000 switch. Dit document gaat er ook van uit dat de IDSpostoffsparameters correct zijn gedefinieerd. Hieronder vallen HOSTID, ORGID, HOSTNAME en ORGNAME. Let erop dat de CSPM-host voor communicatie met een sensor de ORGID en ORGNAME overeenkomt met wat op de Sensor is gedefinieerd.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op CSPM 2.3.I en later.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg <u>Cisco Technical Tips Conventions</u> (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Configuratie

In deze secties wordt het proces uitgelegd dat wordt gebruikt om een IDS-sensor in CSPM te configureren.

Start CSPM en log in. Er verschijnt een blancosjabloon (eerste lancering) waarmee u uw netwerk kunt definiëren.



Deze drie definities zijn vereist in de CSPM-topologie voor IDS.

- Bepaal het netwerk waarin de controle interface van de Sensor en het netwerk waar de gastheer CSPM verblijft. Als ze op hetzelfde net zijn, hoeft slechts één netwerk te worden gedefinieerd. Defineert eerst dit netwerk.
- 2. Defineert de CSPM-host in het netwerk. Zonder de CSPM host-definitie kan de sensor niet worden beheerd.
- 3. Defineer de sensor in zijn netwerk.

Bepaal het netwerk waarop de CSPM-host verblijft

Voer de volgende stappen uit:

1. Klik met de rechtermuisknop op het pictogram **Internet** in de topologie en selecteer **Nieuw** > **Netwerk** om een nieuw netwerk te



2. Aan de rechterkant van het paneel van het Netwerk, voeg de naam van het nieuwe netwerk, het netwerkadres, en het netwerkmasker toe dat zal worden gebruikt.

L Cisco Secure Policy Manager
Elle Edit View Iools Wizards Help
Save Update Units Ficto Back, Format Lock Tearoff Find Check Help Context Start
Image: Second Services Image: Second Servic

- 3. Klik op de knop IP-adres en voer het IP-adres in voor het netwerk dat wordt gebruikt om het internet te bereiken.Normaal gesproken is het de standaardgateway voor het netwerk.Opmerking: wanneer u sensoren beheert, hoeft het adres van de poort niet noodzakelijkerwijs te zijn correct aangezien de Sensor deze standaard gateway-informatie niet verstuurd heeft. Het zou al in de Sensor moeten worden gedefinieerd.
- 4. Klik op **OK**. Het netwerk wordt zonder enige fouten aan de topologie kaart toegevoegd.

ave Update Undo Rodo Back	Forma Lock Tearolf Find Check Help Cor	vlext Start
A Retwork Topology A Retwork Topology A Retwork Topology A Reports	Internet Internet Perimeter Internet Perimeter Interlace 1	Permiter
	T72 .18 .124 .1	Network IP Address Edit Network Selection Name Network 1
		Network Address 172 18 .124 .0 Network Mask 255 255 255 0 Unnumbered 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 <u>Help</u> for more details.

Voeg de CSPM-host toe

Gebruik deze procedure om de CSPM-host toe te voegen.

 In de Topologie van het Netwerk, klik op het netwerk dat u enkel toevoegde en selecteer Nieuw > Host.CSPM brengt een scherm dat hierop lijkt. Als niet, dan is het netwerk dat u zojuist hebt gedefinieerd niet het netwerk waarin uw CSPM-host zich bevindt. Controleer het IP-adres op uw CSPM-

Cisco Se	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
host.	

- 2. Klik op Ja om de CSPM-host in de topologie te installeren.
- 3. Controleer of de informatie op het Algemene scherm voor de CSPM-host niet geschikt is.
- 4. Klik op OK op het Algemene scherm van de CSPM-host.

Het sensor-apparaat toevoegen

Gebruik deze procedure om het Sensor-apparaat toe te voegen.

 Klik met de rechtermuisknop op het netwerk waar uw sensor staat en selecteer Wizard > Sensor toevoegen.Opmerking: Als de CSPM-host en de regelinterface van uw sensor niet in hetzelfde netwerk zijn, specificeert u het netwerk waarin de sensor



2. Voer de juiste postoffparameters in voor de sensor.

nd press Next.	ia sensor wizala. To ada a ser	sor to the topology in in the following information
Sensor Name	Sensor1	Host ID 99 Org. ID 1
Organization Nam	e rtp	Policy Enforcement Associated
IP Address Postoffice Heartbeat Interva	172 . 18 . 124 . 99 1 5	Port UDP 45000
Comments		
	a ucifu tha Canaci'a address	Enter the IP Address and the Host

- 3. Klik hier op Controleer om het adres van de sensor te controleren.N.B.: Als dit de eerste keer is dat u deze Sensor instelt, dan wilt u niet de configuratie van de Sensor opnemen. Als u deze Sensor eerder elders hebt geconfigureerd, via een UNIX-directeur of een andere CSPM-host en u wijzigingen hebt aangebracht in de configuratie van de Sensorshandtekeningen, dan wilt u de configuratie van de Sensor opnemen.
- Klik op Next om de kenmerkende versies op de sensor te definiëren. U kunt ook de opdracht vers geven om dit op de sensor te controleren.

Host CSPM (1)	Select the Cisco Secure Policy Manager host that will publish the generated
Sensor Version	IPSec
Signature Template Defa Template Comment	ault
Cisco Systems, Inc. defau	It Signature Template settings.
	the latest circuit as undate (2 0(1)CD) that do not each to this

erking: Als CSPM niet de juiste versie van de Sensor heeft die u op uw sensor gebruikt, update de handtekeningen op uw CSPM-host. Zie <u>Software Download</u> (<u>alleen geregistreerde</u> klanten) voor updates.

- 5. Klik op de knop Volgende om verder te gaan
- 6. Klik op Voltooien om de installatie van de sensor in de topologie te voltooien.
- Selecteer in het hoofdmenu CSPM de optie Bestand > Opslaan en bijwerken om de in de topologie ingevoerde informatie in CSPM te compileren. Let erop dat deze stap nodig is om het postprotocol op de CSPM-host te starten.
- 8. Controleer dat alles werkt door in uw sensor te loggen als de netwerkgebruiker.
- 9. Voer de **nrconns** opdracht uit.

```
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

>

Opmerking: Als de Sensor en de CSPM-host niet communiceren, wordt er in plaats daarvan een soortgelijke uitvoer weergegeven:

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

Als dit probleem zich voordoet, kunt u een snuffelspoor bekijken om te zien of beide kanten UDP 45000-pakketten verzenden. UDP 45000 is wat IDS-apparaten gebruiken om met elkaar te communiceren. Om dit op de Sensor te testen, **moet u** roken en (afhankelijk van welke Sensor u heeft) **snoop -d iprb1 poort 45000** (voor een IDS 4210-sensor) en **snoop -d iprb0 poort 45000** (voor elk ander model van Sensor) uitvoeren).Gebruik **<control-c>** om uit een sneeuwsessie te breken.Deze output verschijnt als er geen communicatie is tussen de Sensor en 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#

In de bovenstaande uitvoer stuurt de Sensor UDP 45000 pakketten, maar ontvangt deze niet. Een correcte configuratie produceert uitvoer gelijkend op dit: # 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 de bovenstaande uitvoer gaat UDP 45000-verkeer in beide richtingen. Als UDP 45000 pakketten in beide richtingen stromen en de uitvoer van **nBn** op de Sensor nog steeds zegt dat er geen verbinding is vastgesteld, komen de postoffparameters op de Sensor en de CSPM host niet overeen. U kunt de postoffsparameters als volgt handmatig op de CSPM-host controleren: Gebruik Windows Verkenner om naar de locatie te navigeren waar CSPM op de NT-machine is geïnstalleerd.

🧃 etc		• 🗈 🚈	3 B B 🖍 🗠 🗙		
Name	Size	Туре	Modified	Attributes	
auths 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	
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				

Bewerk de host-, route- en organisatiebestanden met Schrijf- of Word-pad (gebruik geen Kladblok omdat de opmaak beschadigd zal zijn).Zorg ervoor dat deze bestanden op de juiste manier voor uw installatie lijken. Als een van de waarden niet correct is, bewerk ze en start de NT-computer opnieuw met behulp van deze stappen:Klik op het pictogram **CSPM** in de netwerktopologie.Klik op het tabblad Beleidsdistributie om de posteringsparameters in te voeren.**Sla** uw wijzigingen **op** en **update** ze.Herstart de NT-computer.



De sensor configureren

Nadat de configuratie in CSPM is opgeslagen, moet u de sensor configureren. Om dit te doen, stelt u eerst de Sensor in om de alarmen te schrijven die hij op zijn eigen blog ziet. Stel de sensor vervolgens in op "sniff" op de juiste interface.

Schrijf alarmen in het logboek

Gebruik deze procedure om alarmen aan het logbestand te schrijven.

 Klik op het vak Logbestanden van audit genereren om de sensor te vertellen om de alarm naar zijn lokale logbestanden te sturen. Het stuurt ook een alarmsignaal naar de CSPM-doos, nadat je er een configuratie naar beneden duwt.



2. Klik op **OK** om verder te gaan.

Stel de sensor in op "Sniff"

Gebruik deze procedure om de sensor in te stellen op "Sniff".

- 1. Selecteer de sensor in uw topologie van CSPM en klik op het tabblad Sensing.
- Defineert het Packet Capture apparaat:iprb0 voor een IDS 4210 sensorSPW0 voor elk ander Sensormodel



- 3. Klik op **OK** om verder te gaan.
- 4. Klik het pictogram **Update** op de menubalk van CSPM om CSPM met de informatie bij te werken.**Opmerking:** als alles goed gaat, verschijnt er een vergelijkbaar scherm. Merk op dat er geen rode fouten zijn. Gele waarschuwingen zijn doorgaans in orde.



5. Selecteer de sensor in de netwerktopologie en klik op het tabblad Opdracht om de bijgewerkte configuratie naar de sensor te verzenden

e Update Indo Redo Back Forward	Lock Tearoff Find Check Help Context	Start
Network Topology Network 1	Properties Sensing Blacking Filtering Logang	Advanced Command Control Status Processing completed 13 (no errors) Policy 3 Eol Configuration
INSANE INSANE INSANE Security Policy Abstracts Example Policies System Policies INSANE Default Policies Network Service Bundles Policy Domains Network Services Sensor Signatures	Generated Commands Generated Commands Generated Commands Generated at 10 Generated at 10 Generated Sensor Name, gac Generation Status Generatio	/12/01 11:51:16 (Eastern Daylight Time) 9' 9' 124.122 12.124.105 122 10: INSANE anizabion: rtp 72:18.124.106 ID: 10 ID: 10 000
Default Default Network Object Groups Interfaces Internet.Interface 1 Internet.Interface 1: 172.1	Crear current personne T	File Import File Export

6. Klik op de knop Nu goedkeuren om de configuratie naar de sensor te

stur	en.								
								_	
l :k	Tearoff	🀴 Find	Кон Check	🥏 Help	№? Context	Start			
Sen	ising Blo	cking I	Filtering l	.ogging	Advance	d Command	Control		
n-2	10					Status			
						Trai	nsfering files	s to sensor	
		ſ	Commands	/Messar	16%	Policy 0		<u>P</u> oll	
Rev	view/Edit-		#						
Г	Datrack		#Start of (#	Gensor C	onfiguratio	n			
_ (<u>–</u> enesr		≓ #Donote	edit!					
_			#						
ig Li	ommands		# Generati	ed at 01,	/18/01 10:	59:55 (Centra	l Standard 1	[ime]	

et Statusvenster geeft het bericht "Upload <#> Klaar" weer. Dit duidt op een geldig en volledig overdrachtproces. De sensor wordt nu bijgewerkt en werkt nu normaal.Als de sensor niet normaal werkt, ga dan terug naar de Sensor en controleer de uitvoer van de opdrachtregel om er zeker van te zijn dat de verbinding tussen de CSPM-host en de sensor is ingesteld

ing								<u>.</u>	. .
k	Tearoff	M Find	Check	🤗 Help	№? Context	, 20. Start			
Sei	neing Blo	cking I	Filtering L	.ogging	Advance	d Comm	and Contr	rol	
1-2	וורי					Status Up	load 1 com	pleted (no errors)	
		ſ	Summanuls	/Messau	PX	Policy 1		Eoll	
He	view/Edit- <u>B</u> efrest		# # Start of S #	Gensor C	onfiguratio	<u>ממממממממים</u> ז		000000000000000000000000000000000000000	*

adat dit is voltooid, kunt u op zoek gaan naar alarmen die de Sensor naar de CSPM host in de eventviewer stuurt. Om de evenementenviewer te bekijken, selecteert u in het hoofdmenu van CSPM **Gereedschappen > Sensor gebeurtenissen >**

Vi	ew Database Eve	nts	×	
F	Туре			
	CSIDS Alarms	-		
	Time	12		
	Start			
	• At <u>E</u> arliest E	vent		
	C At Time:	10/10/01	v	
	Now	5.59.46 PM		
	Stop			
	C <u>A</u> t Time:	10/10/01	<u>v</u>	
	Now	5:59:46 PM		
	Don't Stop			
		Cancel	. 1	
aseverbouding				Klik on OK

het venster van de events-database weer te geven. Uw scherm zal variëren afhankelijk van de alarmen die u krijat

	ALC: A LA COMPANY	Source Address	Dest Address	Details	Source Loc	Dest Loc	SubSig ID	Severity	Org Name
	MP flood								
5 10	MP smurf attack	· · ·							
6 10	MP unreachable	10.32.10.10	172.18.124.154	<none></none>	OUT	OUT	0	Low	ιtp
40 IP	fragments overlap	i 🐮 🔟							
38 Ne	et sweep-echo	+							
4 Po	stOffice Initial Notification	<none></none>	<none></none>	postofficed initial notification msg	OUT	OUT	0	Low	rtp
24 Ro	oute Down!	<none></none>	<none></none>	+					
29 Ro	oute Up	<none></none>	<none></none>	300					
7 UD	0P Packet	i 🐮 (i)							

Gerelateerde informatie

• Technische ondersteuning en documentatie – Cisco Systems