# CSPM에서 Cisco Secure IDS Sensor 구성

### 목차

소개 <u>사전 요구 사항</u> <u>요구 사항</u> <u>사용되는 구성 요소</u> <u>표기 규칙</u> 구성 <u>CSPM 호스트가 상주하는 네트워크 정의</u> <u>CSPM 호스트 추가</u> <u>센서 장치 추가</u> <u>센서 구성</u> <u>관련 정보</u>

### <u>소개</u>

이 문서에서는 Cisco CSPM(Secure Policy Manager)에서 Cisco IDS(Secure Intrusion Detection System) 센서를 구성하는 데 사용되는 절차에 대해 설명합니다. 이 문서에서는 컴퓨터에 CSPM 버 전 2.3.I를 설치한 것으로 가정합니다. 버전 "I"를 사용하면 Cisco Catalyst® 6000 스위치에서 IDS 장 치(어플라이언스 센서, Cisco IOS<sup>®</sup> 라우터 또는 IDS 블레이드)를 관리할 수 있습니다. 이 문서에서 는 IDS 우체국 매개변수가 올바르게 정의되었다고 가정합니다. 여기에는 HOSTID, ORGID, 호스트 이름 및 ORGNAME이 포함됩니다. CSPM 호스트가 센서와 통신하려면 ORGID 및 ORGNAME이 센서에 정의된 것과 일치해야 합니다.

### <u>사전 요구 사항</u>

### <u>요구 사항</u>

이 문서에 대한 특정 요건이 없습니다.

#### <u>사용되는 구성 요소</u>

이 문서의 정보는 CSPM 2.3.I 이상을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

#### <u>표기 규칙</u>

문서 규칙에 대한 자세한 내용은 <u>Cisco 기술 팁 표기 규칙</u>을 참조하십시오.

## <u>구성</u>

이 섹션에서는 CSPM에서 IDS 센서를 구성하는 데 사용되는 프로세스에 대해 설명합니다.

CSPM을 시작하고 로그인합니다. 네트워크를 정의할 수 있는 빈 템플릿(초기 시작)이 나타납니다.



이 세 가지 정의는 IDS용 CSPM 토폴로지에 필요합니다.

- 1. 센서의 제어 인터페이스가 상주하는 네트워크와 CSPM 호스트가 상주하는 네트워크를 정의 합니다. 동일한 서브넷에 있는 경우 하나의 네트워크만 정의해야 합니다. 먼저 이 네트워크를 정의하십시오.
- 2. 네트워크에서 CSPM 호스트를 정의합니다. CSPM 호스트 정의가 없으면 센서를 관리할 수 없 습니다.
- 3. 네트워크에서 센서를 정의합니다.

<u>CSPM 호스트가 상주하는 네트워크 정의</u>

다음 단계를 완료하십시오.

1. 토폴로지에서 **인터넷** 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **New > Network를** 선택하여 새 네트워크를 생성합니다

🕌 Cisc	o Secure	Policy	Manage	7			
<u>F</u> ile <u>E</u> d	lit <u>V</u> iew	<u>T</u> ools	<u>W</u> izards	<u>H</u> elp			
🔚 Save	🔛 Update	🖍 Undo	<b>Qu</b> Redo	<b>⟨</b> ₽ Back	<b>→</b> Forward	ී Lock	Tearoff
	-*S, Netw 📥 Netw	vork Poli vork Top	cy ology		Gener	al ] Interfa	aces   Perim
156		nternet	New	Þ	Netwo	rk	
	- 🍂 Took - 🎒 Benr	s and 5 orte	Policy	•	Cloud	Network	
	- 📆 Admi	nistrativ	Iree	•	DI DI	niect Tune	Internet
** **	~		<u>H</u> enama <u>D</u> elete <u>F</u> ind	à	En	forcement Policy	: No
			Tear <u>O</u> ff <u>P</u> ropertie Wizards	View es ►			
			Help		]		

네트워크 패널의 오른쪽에 새 네트워크 이름, 네트워크 주소 및 사용할 넷마스크를 추가합니
 다

ave Update Undor Rodo Back	🔿 🖄 😨 🚧 🌆 🤗 🗙	🤗 🚜 Vext Start
** Network Policy     Network Topology     Network 1     Not and Services     Reports     Administrative Accounts	General       Internet         Internet       Interter         Intern	Insert New Permee Interface Network Permee Interface Network PAddress Edit Network Selection Name Network 1 Network Address 172 18 124 0 Network Address 172 18 124 0 Network Mask 255 255 0 Unnumbered Organize the gateway's internal perimeters, including associated interfaces (IP adapters) and networks. You can perform these actions with controls, diag and drop, or right-click popup menu operations. See Help for more details.

- 3. IP Address(IP 주소) 버튼을 클릭하고 인터넷에 연결하는 데 사용하는 네트워크의 IP 주소를 입력합니다.일반적으로 네트워크의 기본 게이트웨이입니다.참고: 센서를 관리할 때 센서가 이 기본 게이트웨이 정보를 전송하지 않으므로 게이트웨이 주소가 반드시 정확할 필요는 없습니 다. 센서에 이미 정의되어 있어야 합니다.
- 4. 확인을 클릭합니다. 네트워크가 오류 없이 토폴로지 맵에 추가됩니다



#### <u>CSPM 호스트 추가</u>

CSPM 호스트를 추가하려면 이 절차를 사용합니다.

 Network Topology(네트워크 토폴로지)에서 방금 추가한 네트워크를 마우스 오른쪽 버튼으로 클릭하고 New(새로 만들기) > Host(호스트)를 선택합니다.CSPM은 이와 유사한 화면을 표시 합니다. 그렇지 않은 경우 방금 정의한 네트워크는 CSPM 호스트가 있는 네트워크가 아닙니다 . CSPM 호스트의 IP 주소를 다시 확인합니다



- 2. Yes(**예**)를 클릭하여 CSPM 호스트를 토폴로지에 설치합니다.
- 3. CSPM 호스트에 대한 General(일반) 화면의 정보가 정상인지 확인합니다.
- 4. CSPM 호스트의 General(일반) 화면에서 OK(확인)를 클릭합니다.

#### <u>센서 장치 추가</u>

이 절차를 사용하여 센서 장치를 추가합니다.

1. 센서가 있는 네트워크를 마우스 오른쪽 버튼으로 클릭하고 Wizards(마법사) > Add Sensor(센 서 **추가)를** 선택합니다.**참고:** 센서의 CSPM 호스트와 제어 인터페이스가 동일한 네트워크에 있지 않은 경우 센서가 있는 네트워크를 정의합니다



2. 센서에 대한 올바른 우체국 매개변수를 입력합니다

/elcome to the Ac	ld Sensor Wizard. To add a Sen	sor to the topology fill in the following information
Sensor Identifical	tion	
Sensor Name	Sensor1	Host ID 99 Org. ID 1
Organization Nam	e Itp	Policy Enforcement Associated
IP Address	172 . 18 . 124 . 99	Network Cisco Post Uffice
Postoffice Heartbeat Interva	al 5	Port UDP 45000
Comments		
Check here to	o verify the Sensor's address.	Enter the IP Address and the Host
		uou mau enter it manuallu

- 3. 센서 주소 상자를 확인하려면 여기를 클릭하십시오.참고: 이 센서를 처음 설정하는 경우 센서 구성을 캡처하지 않습니다. UNIX 디렉터 또는 다른 CSPM 호스트를 통해 이 센서를 이전에 구 성한 경우 센서 서명에 대한 컨피그레이션을 변경한 경우 센서 컨피그레이션을 캡처합니다.
- 4. Next(다음)를 클릭하여 센서에서 서명 버전을 정의합니다. 또한{\f418 }{\f418 }센서에서{\f418 }이를{\f418 }확인하기{\f418 }위해{\f418 }nervers{\f418 }명령을{\f418 }실행할{\f418 }수{\f418 }있습니다

PSec support. Choose th Distribution Host CSPM (1)	e appropriate Signature Ten Select the host that w device-sp	plate from the drop down lis Cisco Secure Policy Manag vil publish the generated ecific command sets to this (	ts. Jer tevice.
Sensor Version	IPSec	eck here to enable IPSec or oported Sensor versions.	1.
Signature Template Del Template Comment	ault		•
Cisco Systems, Inc. defa	ult Signature Template settir	igs.	
	n the latest signature undat	e (3.0(1)58) that do not appl	u to this

고: CSPM에 센서에서 실행 중인 올바른 센서 버전이 없으면 CSPM 호스트의 서명을 업데이 트합니다. 업데이트는 <u>소프트웨어 다운로드(등록된</u> 고객만 해당)를 참조하십시오.

- 5. 계속하려면 Next 버튼을 클릭합니다.
- 6. Finish(마침)를 클릭하여 토폴로지에 센서 설치를 완료합니다.
- 7. 기본 CSPM 메뉴에서 File > Save and Update를 선택하여 토폴로지에 입력된 정보를 CSPM으로 컴파일합니다. 이 단계는 CSPM 호스트에서 Postoffice 프로토콜을 시작하는 데 필 요합니다.
- 8. 센서에 네트워크 사용자로 로그인하여 모든 것이 작동하는지 확인합니다.
- 9. nrconns 명령을 실행합니다.

```
>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

>

참고: 센서 및 CSPM 호스트가 통신하지 않으면 다음과 유사한 출력이 대신 나타납니다.

netrangr@gacy:/usr/nr

#### >nrconns

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

netrangr@gacy:/usr/nr

이 경우 스니퍼 추적을 얻어 양측이 UDP 45000 패킷을 전송하는지 확인합니다. UDP 45000은 IDS 디바이스가 서로 통신하는 데 사용하는 디바이스입니다. 센서에서 이를 테스트 하려면 루트로 **이동하고**(있는 센서에 따라) snoop -d iprb**1 포트 45000**(IDS 4210 센서용) 및 snoop -d iprb0 포트 4500(다른 센서 모델용)을 실행합니다.<control-c>를 사용하여 스누프 세 션을 해제합니다.이 출력은 센서와 CSPM 간에 통신이 없는 경우 나타납니다.

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

^C#

위의 출력에서 센서는 UDP 45000 패킷을 전송하지만 수신하지는 않습니다. 올바른 컨피그레 이션은 다음과 유사한 출력을 생성합니다.

#### # 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

위 출력에서 UDP 45000 트래픽은 양방향으로 이동합니다.UDP 45000 패킷이 양방향으로 플 로우되고 센서의 nconn의 출력에서 연결이 설정되어 있지 않다고 계속 말하면 센서 및 CSPM 호스트의 포스트오피스 매개변수가 일치하지 않습니다.CSPM 호스트의 포스트오피스 매개변 수를 수동으로 확인하려면Windows 탐색기를 사용하여 NT 시스템에 CSPM이 설치된 위치로 이동합니다

etc		• 🗈 墙 📶	* BB 🔊 🗙		
Name	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	
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				

쓰기 또는 워드패드로 호스트, 경로 및 조직 파일을 편집합니다(서식이 손상되므로 메모장을 사용하지 않음).이러한 파일이 설치 시 올바른지 확인하십시오. 값이 올바르지 않으면 다음 단 계를 사용하여 값을 편집하고 NT 컴퓨터를 재부팅합니다.네트워크 토폴로지에서 CSPM 아이 콘을 클릭합니다.Policy Distribution(정책 배포) 탭을 클릭하여 우체국 매개변수를 입력합니다 .변경을 저장하고 업데이트합니다.NT 컴퓨터를 재부팅합니다



### <u>센서 구성</u>

컨피그레이션이 CSPM에 저장된 후 센서를 구성합니다. 이렇게 하려면 먼저 센서에서 보이는 경보 를 자체 로그에 기록하도록 설정합니다. 그런 다음 올바른 인터페이스에서 센서를 "sniff"로 설정합 니다.

#### <u>로그에 경보 쓰기</u>

이 절차를 사용하여 로그에 경보를 기록합니다.

1. Generate audit **event log files(감사 이벤트 로그 파일 생성**) 상자를 클릭하여 센서가 경보를 로 컬 로그로 전송하도록 지시합니다.또한 컨피그레이션을 CSPM 상자로 푸시하면 기본적으로 경보를 보냅니다



2. OK(**확인)**를 클릭하여 계속합니다.

#### <u>센서를 "Sniff"로 설정합니다.</u>

이 절차를 사용하여 센서를 "Sniff"로 설정합니다.

- 1. CSPM 토폴로지에서 Sensor를 선택하고 Sensing(센싱) 탭을 클릭합니다.
- 2. 패킷 캡처 디바이스를 정의합니다.iprb0 IDS 4210 센서용spwr0 다른 센서 모델용



- 3. OK(**확인)**를 클릭하여 계속합니다.
- 4. CSPM 메뉴 모음에서 Update(업데이트) 아이콘을 클릭하여 CSPM을 정보로 업데이트합니다 .참고: 모든 작업이 정상적으로 진행되면 이와 유사한 화면이 나타납니다. 빨간색 오류가 없습 니다. 노란색 경고는 일반적으로 정상입니다



5. 네트워크 토폴로지에서 Sensor를 선택하고 Command 탭을 클릭하여 업데이트된 컨피그레이 션을 센서로 보냅니다

Security Policy     Security Policy Enforcement     Ciaco System Folder     System Overrides	Properties Sensing Blocking Fill	ering   Logging   Advani	ed Command Contro Status Processing comple	eted 13 (no errors)
<ul> <li>Trusted Networks</li> <li>Trusted Networks</li> <li>Default Policy</li> <li>IPSec Turnel Groups</li> <li>Network Topology</li> <li>Internet</li> <li>Network 1</li> <li>Network 1</li> <li>Network 1</li> <li>Network 1</li> <li>Security Policy Abstracts</li> <li>Security Policy Abstracts</li> <li>Example Policies</li> <li>System Policies</li> <li>System Policies</li> <li>Network Service Bundles</li> <li>Policy Domains</li> <li>Network Services</li> <li>Sensor Signatures</li> <li>Yelaut</li> <li>Network Object Groups</li> <li>Internet Interface 1: 172.1</li> <li>gacy.Interface 1: 172.18.</li> </ul>	Command Review/Edt  Command Review/Edt  Command Review/Edt  Command Review/Edt  Command Approval  Approve Now  Command Approval  Approve Now  Command Approval  Approve Now  Command Approval  Command Approve Now  Command Ap	Start of Sensor Configure Start of Sensor Configure Do not edit Generated at 10/12/01 moor Name: gacy moor Organization: rtp moor IP Alias: 172 18.122 moor IP Alias: 172 18.122 moor IP Alias: 172 18.122 moor IP Alias: 172 18.122 moor Org ID: 1 writrol Agert Organization mitrol Agert Organizatio mitrol Ag	Policy 3 tion 11:51:16 (Eastern Dayligh 4.106 NE 24.106 File I <u>mpo</u>	Eol

6. 지금 승인 단추를 클릭하여 컨피그레이션을 센서로 전송합니다

							- 🗆 🗵
I 🕤 k Tearoff I	M Kon Tind Check	🤗 Help	<b>№?</b> Context	) Start			
Sensing Block	ing Filtering	Logging	Advance	d Comm	iand Conti	rol	
010				Status			
n-210					Transfering	files to sensor	
	Command	. //		Policy 0		<u>P</u> oll	
Review/Edit-	Commanu:	s/imessay	es				
	# Start of	Sensor C	onfiguratio	n			
<u>R</u> efresh	#	124	-				
	H Do not	edit!					
ig Commands	# Genera	ted at 01/	18/01 10:	59:55 (Ce	ntral Standa	ard Time)	

상태 창에 "업로드 <#> 완료" 메시지가 표시됩니다. 이는 유효하고 완전한 전송 프로세스를 나 타냅니다. 센서가 업데이트되어 이제 정상적으로 실행됩니다.센서가 정상적으로 실행되고 있 지 않으면 Sensor로 돌아가 nconns 명령의 출력을 확인하여 CSPM 호스트와 센서 간의 연결 이 설정되었는지 확인합니다

			<u> ×</u>
l 💽 🖬	d Check Help Conte	, <mark>⊎0</mark> ext Start	
Sensing Blocking	] Filtering   Logging   Advar	nced Command	Control
n-2111		Status Upload	1 completed (no errors)
	Commands/Messages	Policy 1	Eol
Review/Edit	# # Start of Sensor Configure #	ation	*

이 작업이 완료되면 센서가 이벤트 뷰어의 CSPM 호스트에 전송하는 경보를 찾을 수 있습니다 . 이벤트 뷰어를 보려면 CSPM 주 메뉴에서 **도구 > 센서 이벤트 보기 > 데이터베이스를** 선택합

Vie	Database Events
Г	/pe
	CSIDS Alarms
T	me
	Start
	At <u>E</u> arliest Event
	C At Time: 10/10/01
	Now 5.59:46 PM
	Stop
	C At Time: 10/10/01
	Now 5:59:46 PM
	Don't Stop
니다	OKCancel 
· · ······· 이스 창을	표시합니다. 화면이 표시되는 경보에 따라 달라집니다

iod	<b>-</b> -							
wof attack								
INT GLOBAS	. 🕯 II							
nreachable	10.32,10.10	172.18.124.154	<none></none>	OUT	OUT	0	Low	ıtp
ents overlap	i 💉 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>	200 C					
acket	" 🐮 (I)							
	ireachable ients overlap ep-echo ce Initial Notification iown! ip ck.et	Iteachable 10.32:10.10 Initial Notification (none) Iteo Initial Notifica	Iteachable 10.32:10.10 172:18:124:154 Interference overlap Interference	Iteachable 10.32.10.10 172.18.124.154 <none> Itents overlap  ep-echo  ce Initial Notification <none> <none> postolficed initial notification msg fownl  cnone&gt; <none> + lp  chat +</none></none></none></none>	Inteachable         10.32:10:10         172:18:124:154         Conne>         DUT           rents overlap         +         +         -	Inteachable     10.32.10.10     172.18.124.154 <none>     OUT     OUT     OUT       ents overlap     +     +     +     +     +       ep-echo     +     +     +     +     +       cc Initial Notification     <none> <none>     +     +       rownl     <none> <none>     +       iownl     <none>     +     +       iownl     <none>     +       iownl     <none>     +       iownl     <none>     +</none></none></none></none></none></none></none></none></none>	Inteachable         10.32:10.10         172:18:124:154 <none>         OUT         OUT</none>	Inteachable     10.32:10:10     172:18:124:154 <none>     OUT     OUT     OUT     OUT     OUT     OUT       rents overlap     +</none>

## <u>관련 정보</u>

• <u>기술 지원 및 문서 - Cisco Systems</u>