Secure FTD Event Integration with Security Cloud Control via Secure Event Connector 구성

목차

소개

이 문서에서는 SEC(Secure Event Connector)를 사용하여 SCC(Security Cloud Control)에 보안 이벤트를 전송하도록 Cisco Secure FTD를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco FTD(Secure Firewall Threat Defense)
- Linux CLI(Command Line Interface)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

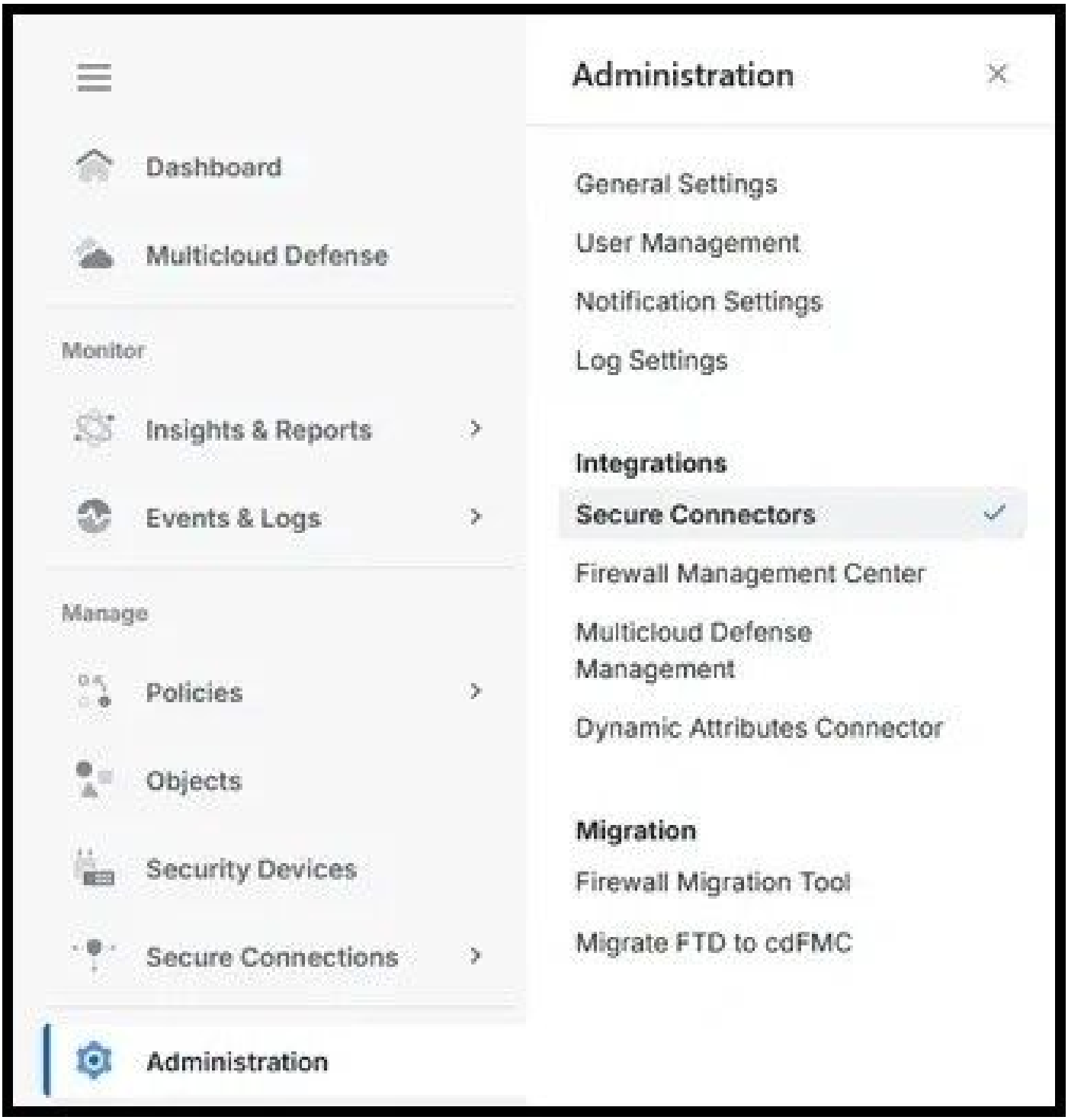
- Cisco Secure FTD 7.6
- Ubuntu Server 버전 24.04

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

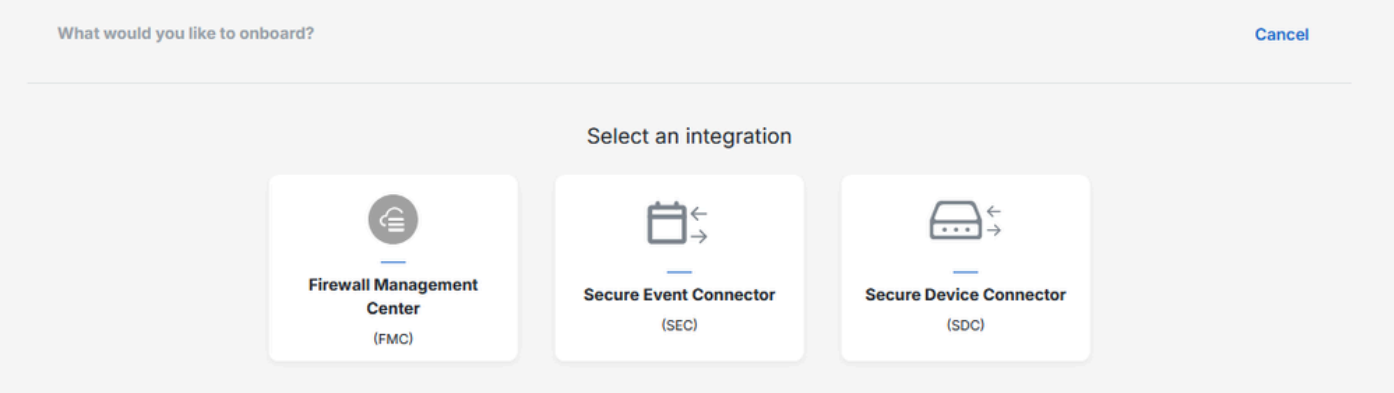
구성

1단계. SCC 클라우드 포털에 로그인합니다.

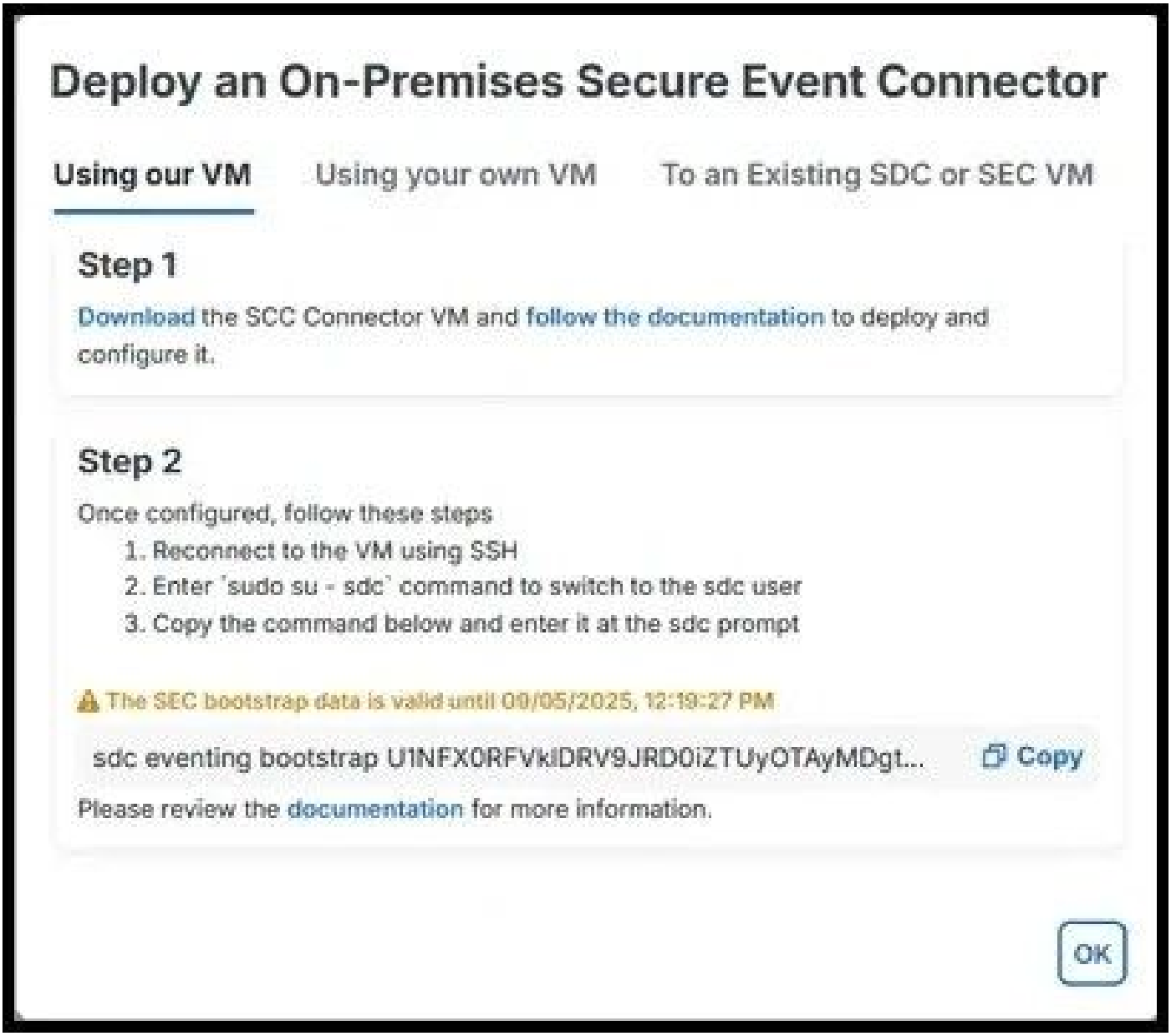
2단계. 왼쪽 메뉴에서 Administration(관리) 및 Secure Connectors(보안 커넥터)를 선택합니다.



3단계. 새 커넥터를 온보딩하려면 오른쪽 상단에서 더하기 아이콘을 클릭하고 Secure Event Connector(보안 이벤트 커넥터)를 선택합니다.



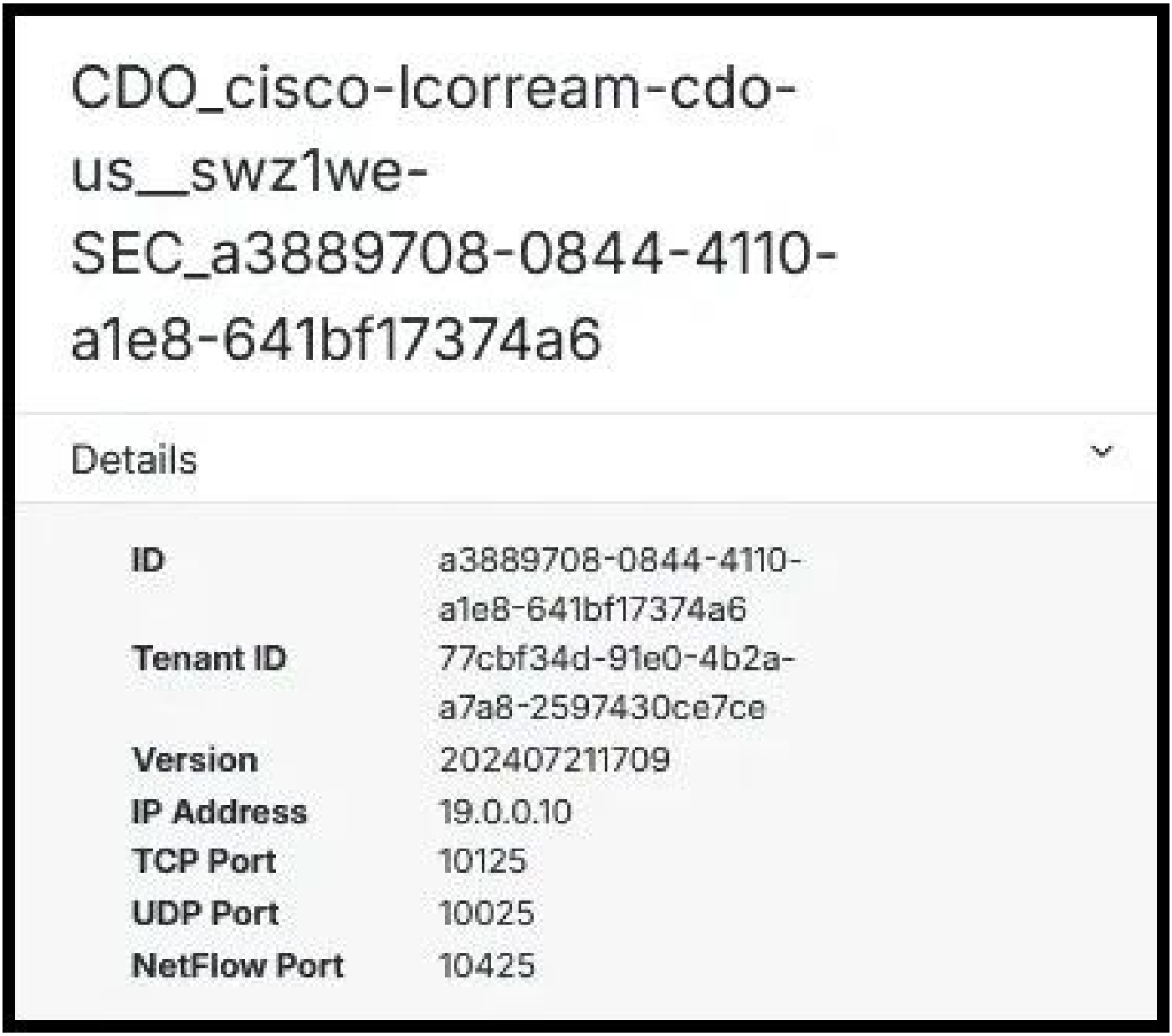
4단계. 'Using our VM', 'Using your own VM' 또는 'To an Existing SDC or SEC VM' 중에서 원하는 옵션에 따라 커넥터를 설치하고 부트스트랩하려면 다음 단계를 사용합니다.



5단계. 부트스트랩이 성공적으로 수행된 경우에도 유사한 메시지가 표시됩니다.

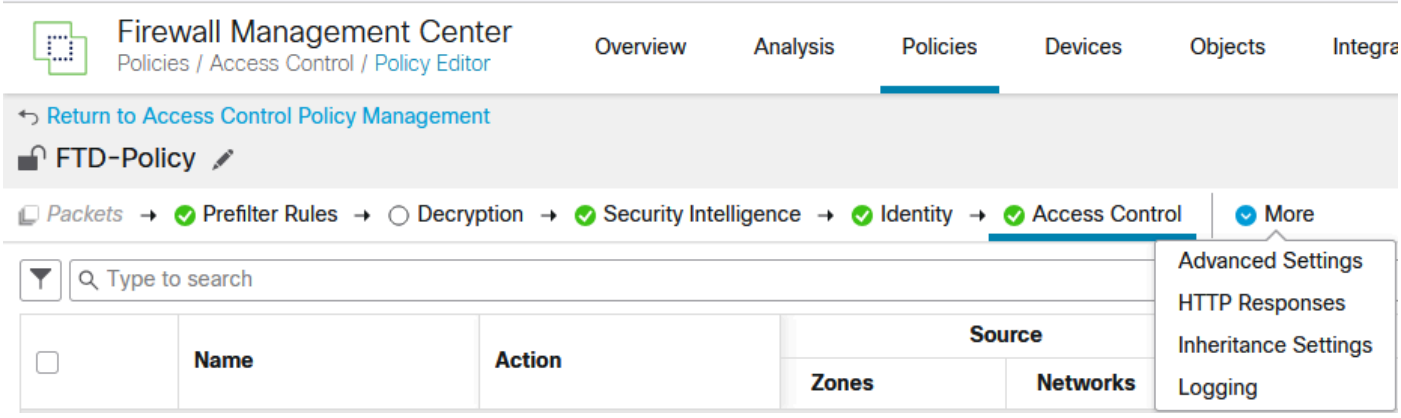
```
2025-06-09 05:41:56 [INFO] Bootstrap package processed successfully
2025-06-09 05:41:56 [INFO] Default AWS Region is us-west-2
2025-06-09 05:42:00 [INFO] Scanning for next available TCP port starting with 10125
2025-06-09 05:42:00 [INFO] TCP port found and set to 10125
2025-06-09 05:42:00 [INFO] Scanning for next available UDP port starting with 10025
2025-06-09 05:42:00 [INFO] UDP port found and set to 10025
2025-06-09 05:42:00 [INFO] Scanning for next available Netflow port starting with 10425
2025-06-09 05:42:00 [INFO] Netflow port found and set to 10425

WARNING! Your credentials are stored unencrypted in '/var/lib/sdc/.docker/config.json'.
Configure a credential helper to remove this warning. See
https://docs.docker.com/go/credential-store/

5a99d0351c1ae91cd790dcf18ee1d0594d37fcfaf5a1725473eeed042342a567
2025-06-09 05:42:06 [INFO] The SEC is up and running - You should be all set to go
2025-06-09 05:42:08 [INFO] Your SEC has been successfully bootstrapped! Please verify that everything is working within
the SCC UI, and thank you for being a customer
sdc@lcorream-sdc:~$
```

6단계. 커넥터가 구축되고 부트스트랩되면 포트 정보가 SCC 포털에 표시됩니다.

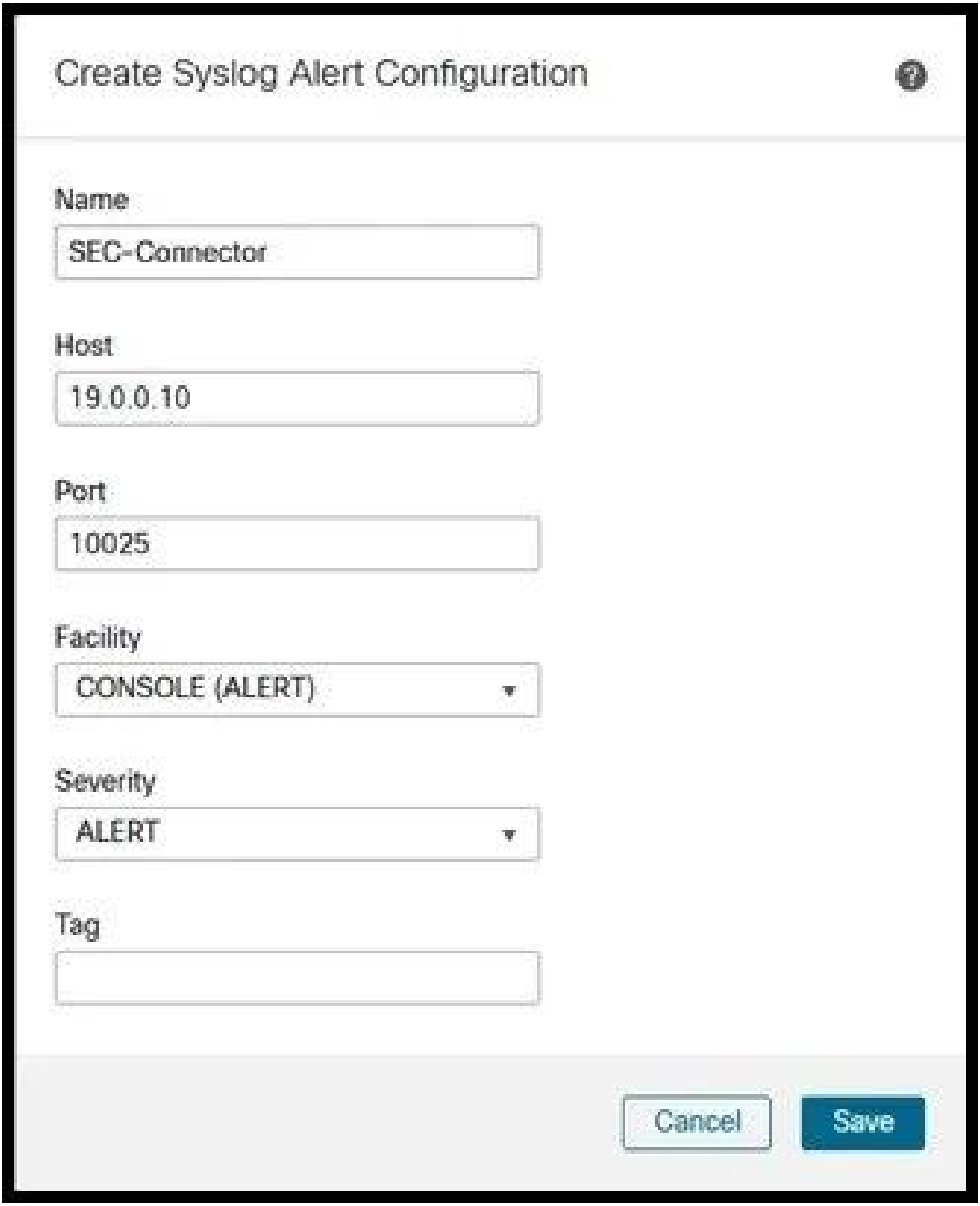


7단계. Cisco FMC(Secure Firewall Management Center)에서 Policies(정책)로 이동한 다음 Access Control(액세스 제어)로 이동합니다. 온보딩 중인 디바이스에 해당하는 정책을 선택합니다.

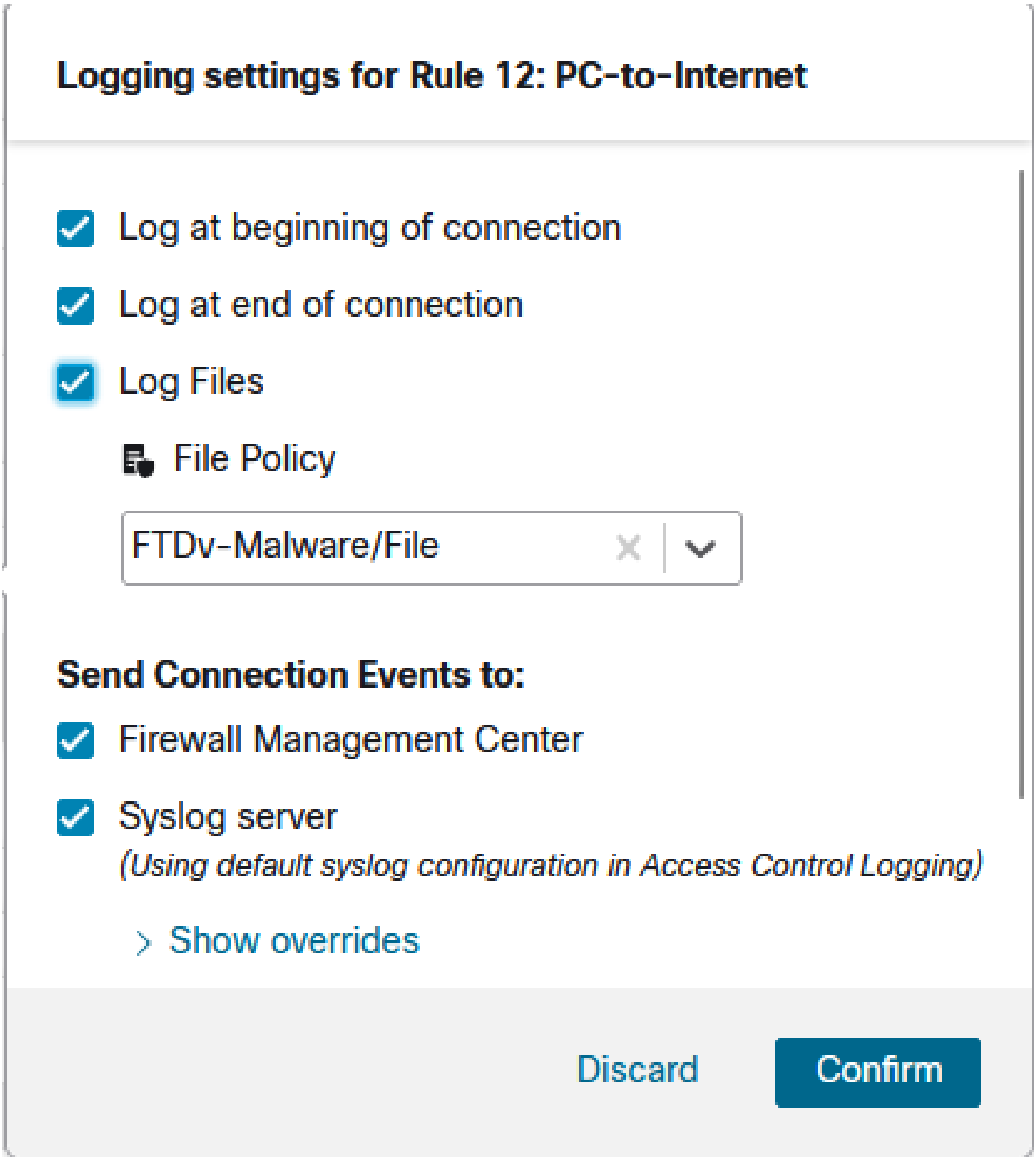
8단계. More(추가)를 선택한 다음 Logging(로깅)을 선택합니다.



9단계. Send using specific syslog alert(특정 syslog 알림을 사용하여 보내기) 옵션을 활성화하고 새 Syslog 알림을 추가합니다. SCC 포털의 SEC 커넥터에서 얻은 인터넷 프로토콜(IP) 주소 및 포트 정보를 사용합니다.



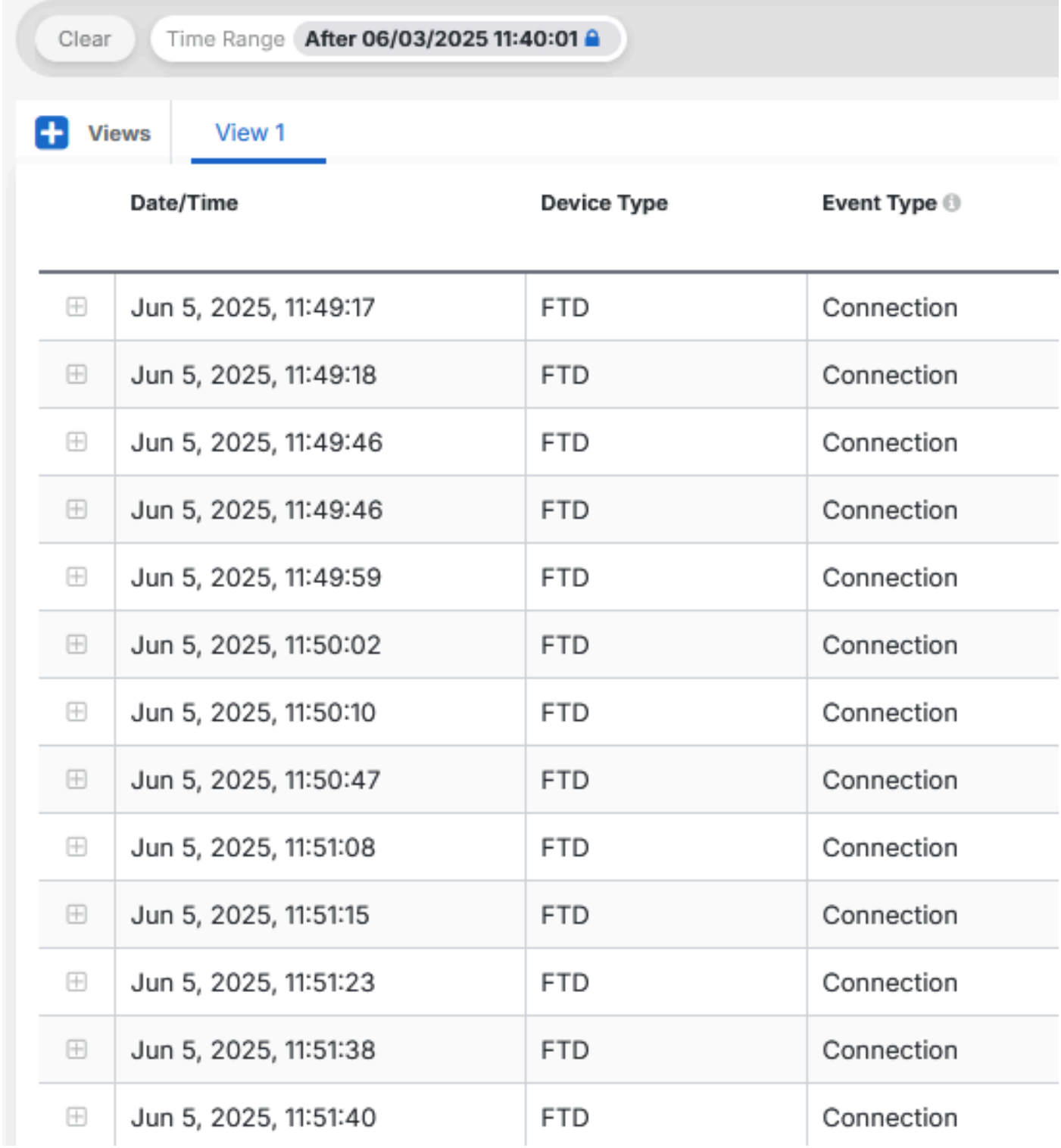
10단계. 액세스 제어 정책으로 돌아가서 개별 규칙을 수정하여 Syslog 서버에 이벤트를 전송합니다
.



11단계. 방화벽이 이벤트 로깅을 시작할 수 있도록 FTD에 대한 변경 사항을 구축합니다.

다음을 확인합니다.

변경 사항이 성공적으로 실행되었고 이벤트 로깅이 수행되고 있는지 확인하려면 SCC 포털에서 Events & Logs and Event Logging으로 이동하여 이벤트가 표시되는지 확인합니다.



문제 해결

FTD에서, syslog 트래픽을 캡처하기 위해 SEC로 이동하는 트래픽과 일치하는 관리 인터페이스를 사용하여 디바이스에서 패킷 캡처를 실행합니다.

```
> capture-traffic

Please choose domain to capture traffic from:
  0 - eth0
```

```
  1 - Global

Selection? 0

Warning: Blanket capture may cause high CPU usage and reduced throughput, use selective filtering to re
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: host 19.0.0.10 port 10025
Starting traffic capture, press ctrl + c to exit (Maximum 1,000,000 packets will be captured)
HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: can't parse filter expression: syntax error
Exiting.

> capture-traffic

Please choose domain to capture traffic from:
  0 - eth0
  1 - Global

Selection? 0

Warning: Blanket capture may cause high CPU usage and reduced throughput, use selective filtering to re
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: host 19.0.0.10 and port 10025
Starting traffic capture, press ctrl + c to exit (Maximum 1,000,000 packets will be captured)
HS_PACKET_BUFFER_SIZE is set to 4.
10:43:00.191655 IP firepower.56533 > 19.0.0.10.10025: UDP, length 876
10:43:01.195318 IP firepower.56533 > 19.0.0.10.10025: UDP, length 1192
10:43:03.206738 IP firepower.56533 > 19.0.0.10.10025: UDP, length 809
10:43:08.242948 IP firepower.56533 > 19.0.0.10.10025: UDP, length 1170
```

SEC 가상 머신에서 가상 머신이 인터넷에 연결되어 있는지 확인합니다. 추가 진단을 위해 lar.log 파일을 확인하는 데 사용할 수 있는 문제 해결 번들을 생성하려면 sdc troubleshoot 명령을 실행합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.