Beveiligde FTD-gebeurtenisintegratie configureren met Cloud Security Control via Secure Event Connector

Inhoud

Inleiding

In dit document wordt beschreven hoe u de Cisco Secure FTD configureert voor het verzenden van beveiligingsgebeurtenissen naar de Security Cloud Control (SCC) met behulp van de Secure Event Connector (SEC).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

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

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

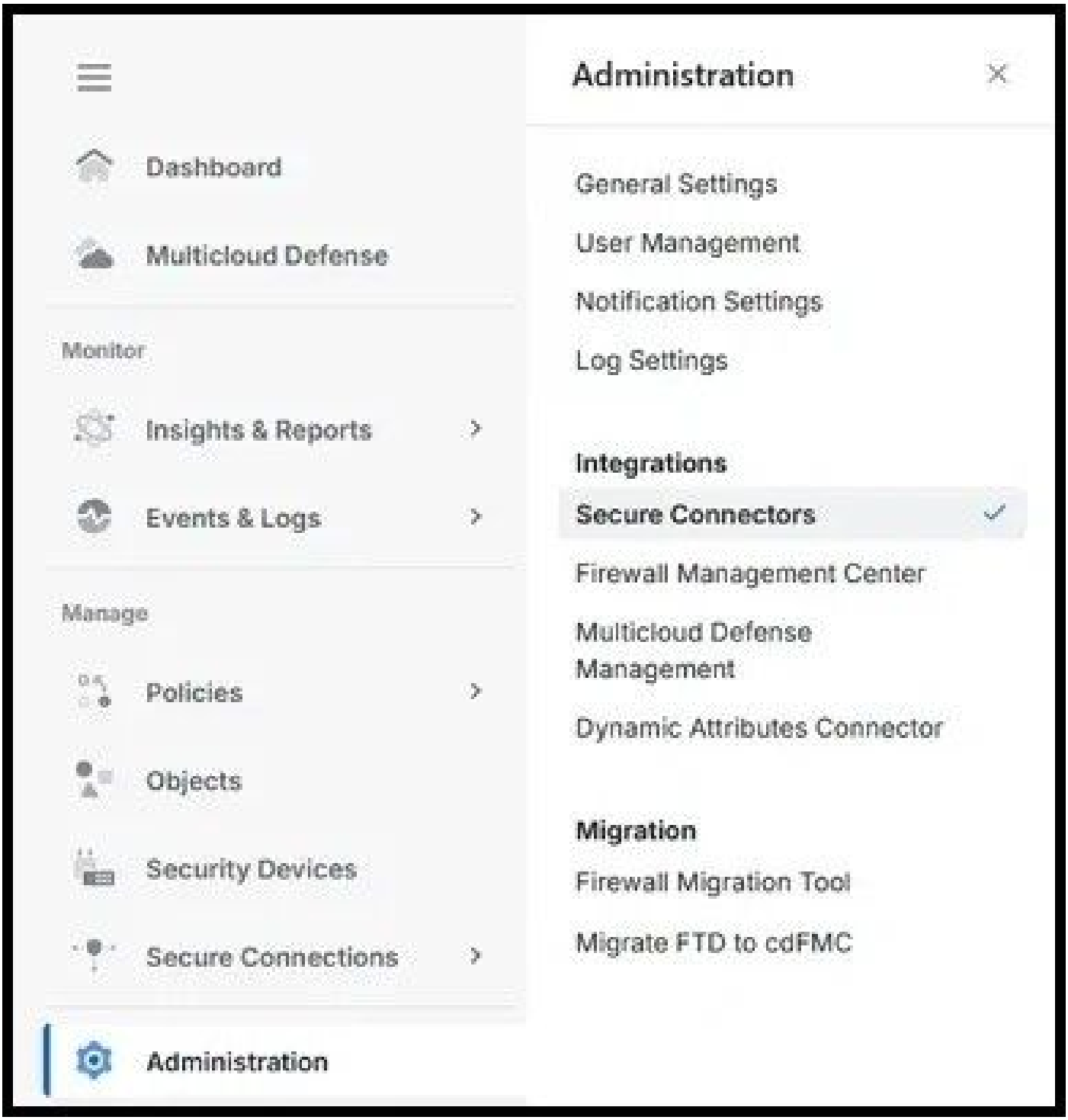
- Cisco Secure FTD 7.6
- Ubuntu Server versie 10 .04

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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

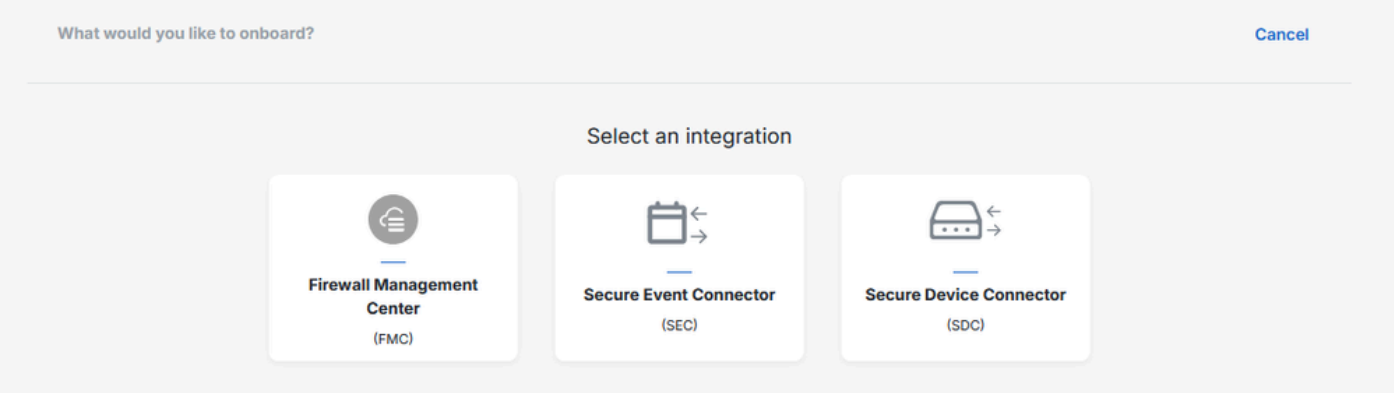
Configureren

Stap 1. Meld u aan bij het SCC cloud portal:

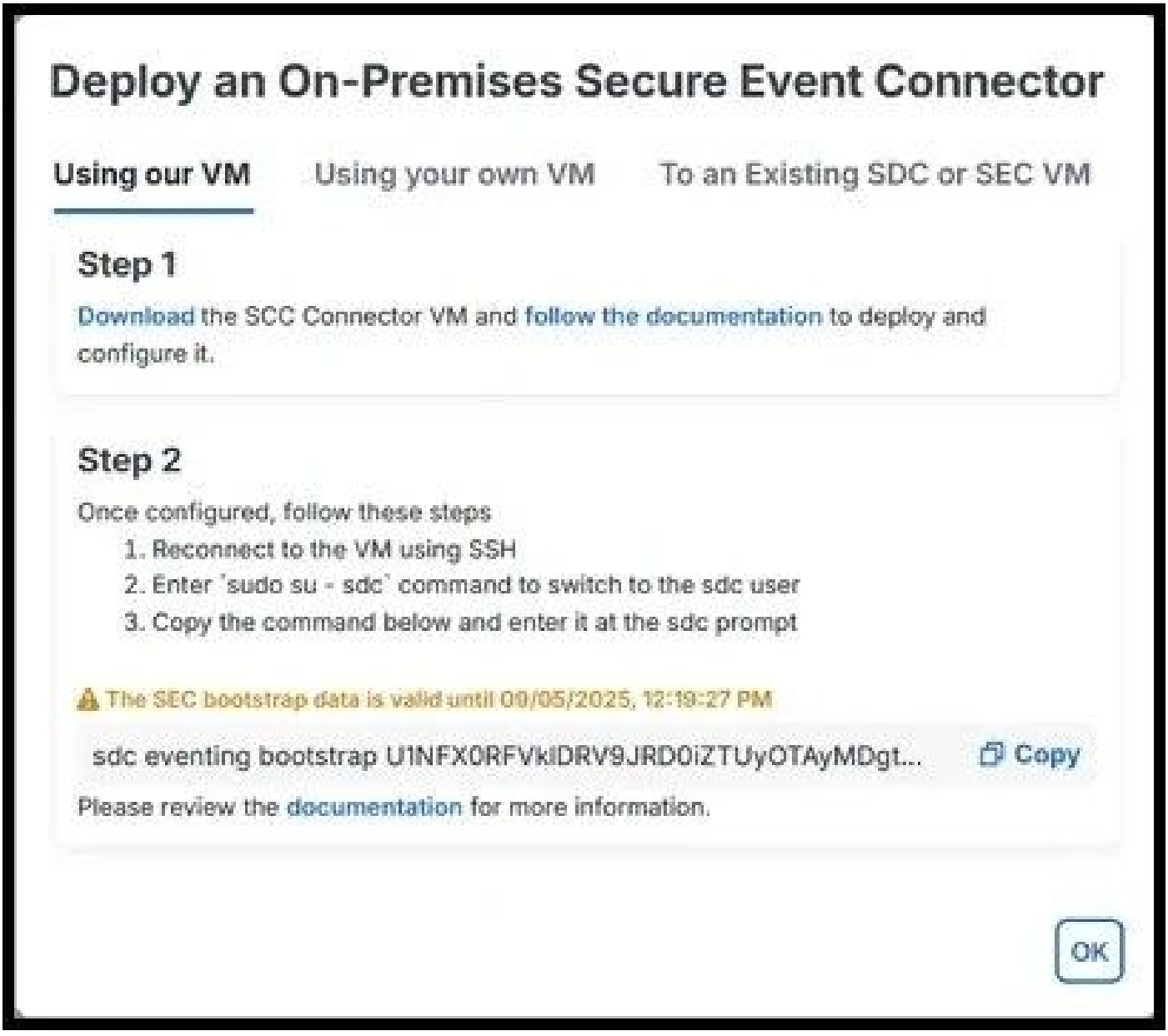
Stap 2. Kies in het menu aan de linkerkant de optie Beheer en Beveiligde connectors:



Stap 3. Klik rechtsboven op het plus-pictogram om een nieuwe connector aan boord te nemen en kies Secure Event Connector:



Stap 4. Gebruik de stappen om de connector te installeren en op te starten, afhankelijk van de gewenste optie tussen 'Onze VM gebruiken', 'Uw eigen VM gebruiken' of 'Naar een bestaande SDC- of SEC-VM':



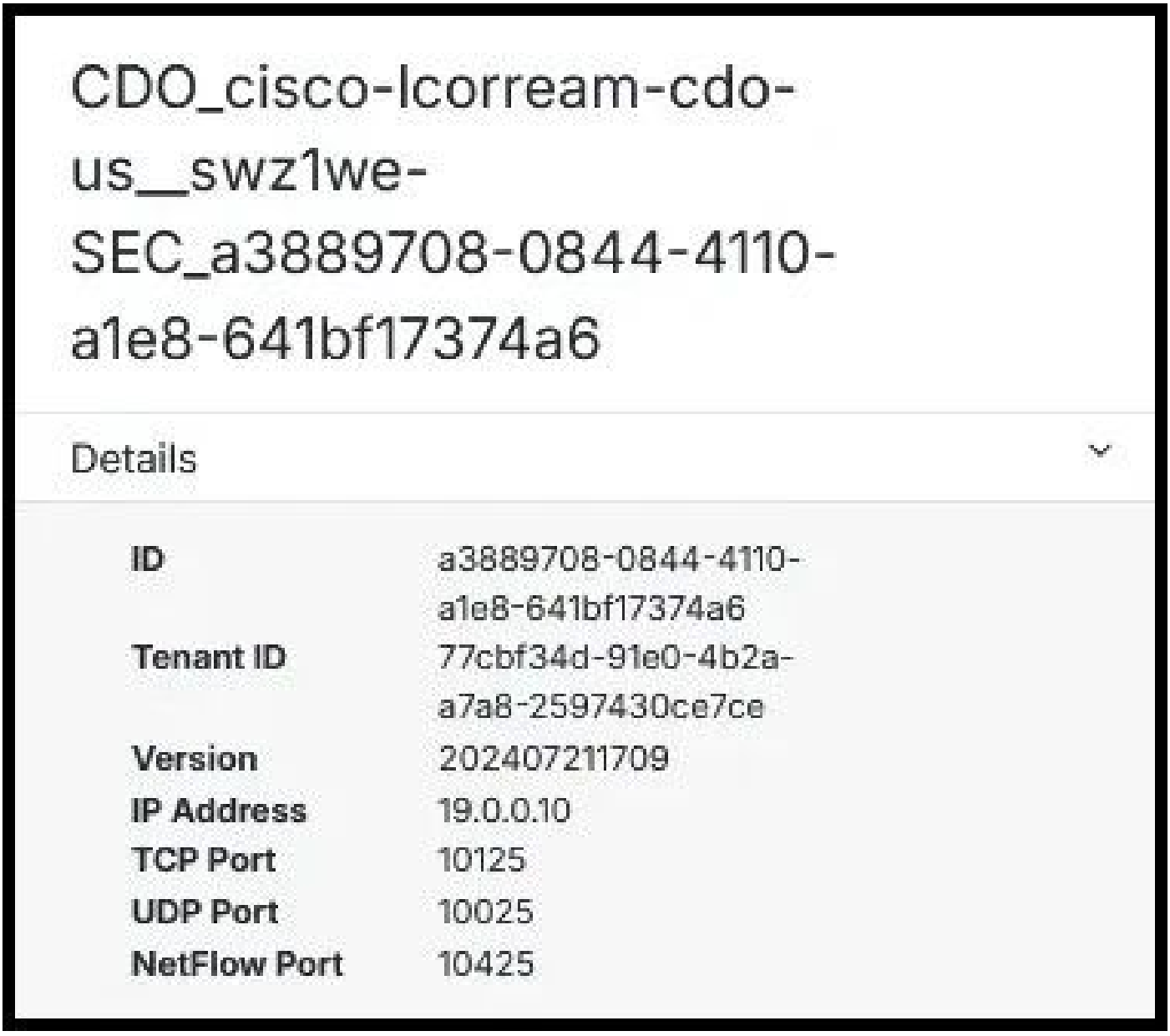
Stap 5. Een soortgelijk bericht wordt weergegeven wanneer de bootstrap succesvol wordt uitgevoerd:

```
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:~$
```

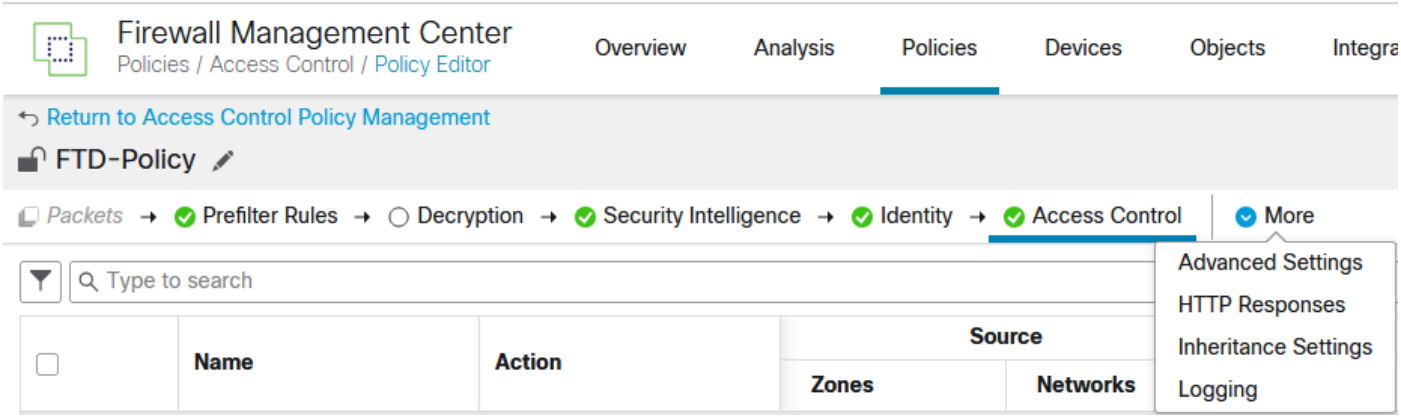
Stap 6. Zodra de connector is geïmplementeerd en opgestart, is de poortinformatie zichtbaar in het SCC-portaal:



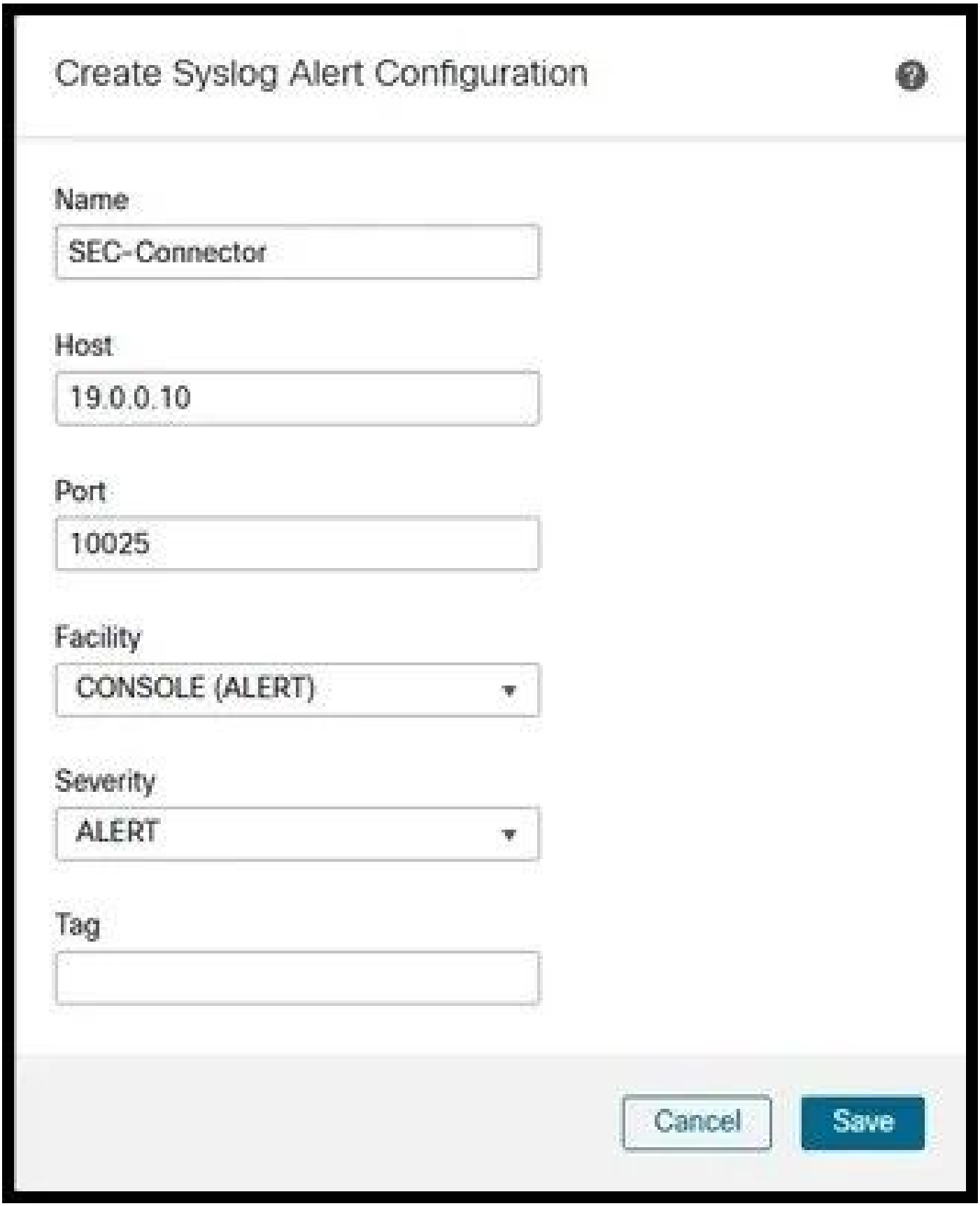
Stap 7. Navigeer in het Cisco Secure Firewall Management Center (FMC) naar Beleid en vervolgens naar Toegangsbeheer. Kies het beleid dat overeenkomt met de apparaten die aan

boord zijn.

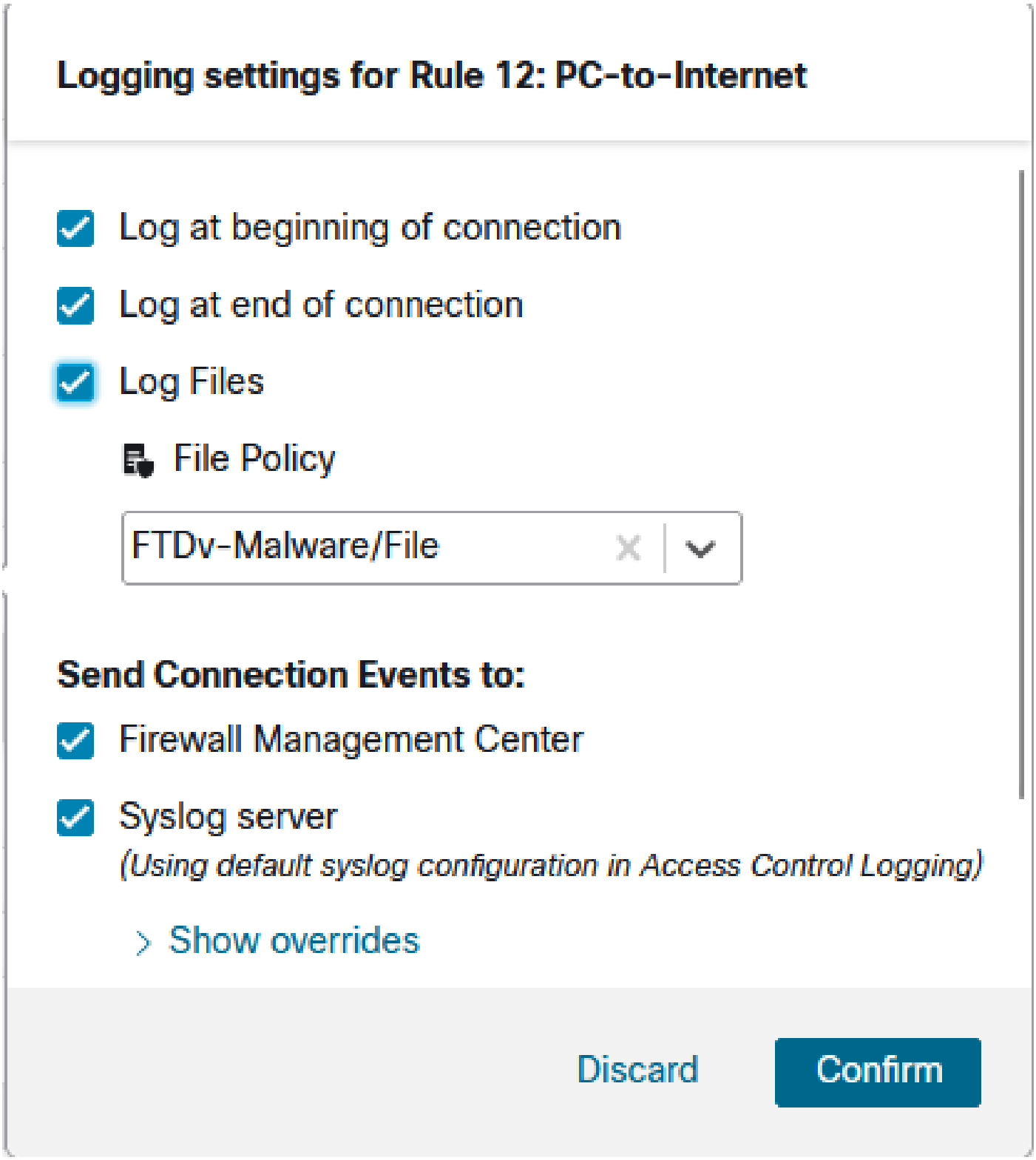
Stap 8. Kies Meer en vervolgens Logboekregistratie:



Stap 9. Schakel de optie Verzenden met specifieke syslog-waarschuwing in en voeg een nieuwe syslog-waarschuwing toe. Gebruik het IP-adres (Internet Protocol) en de poortinformatie die u hebt verkregen via de SEC-connector in het SCC-portaal:



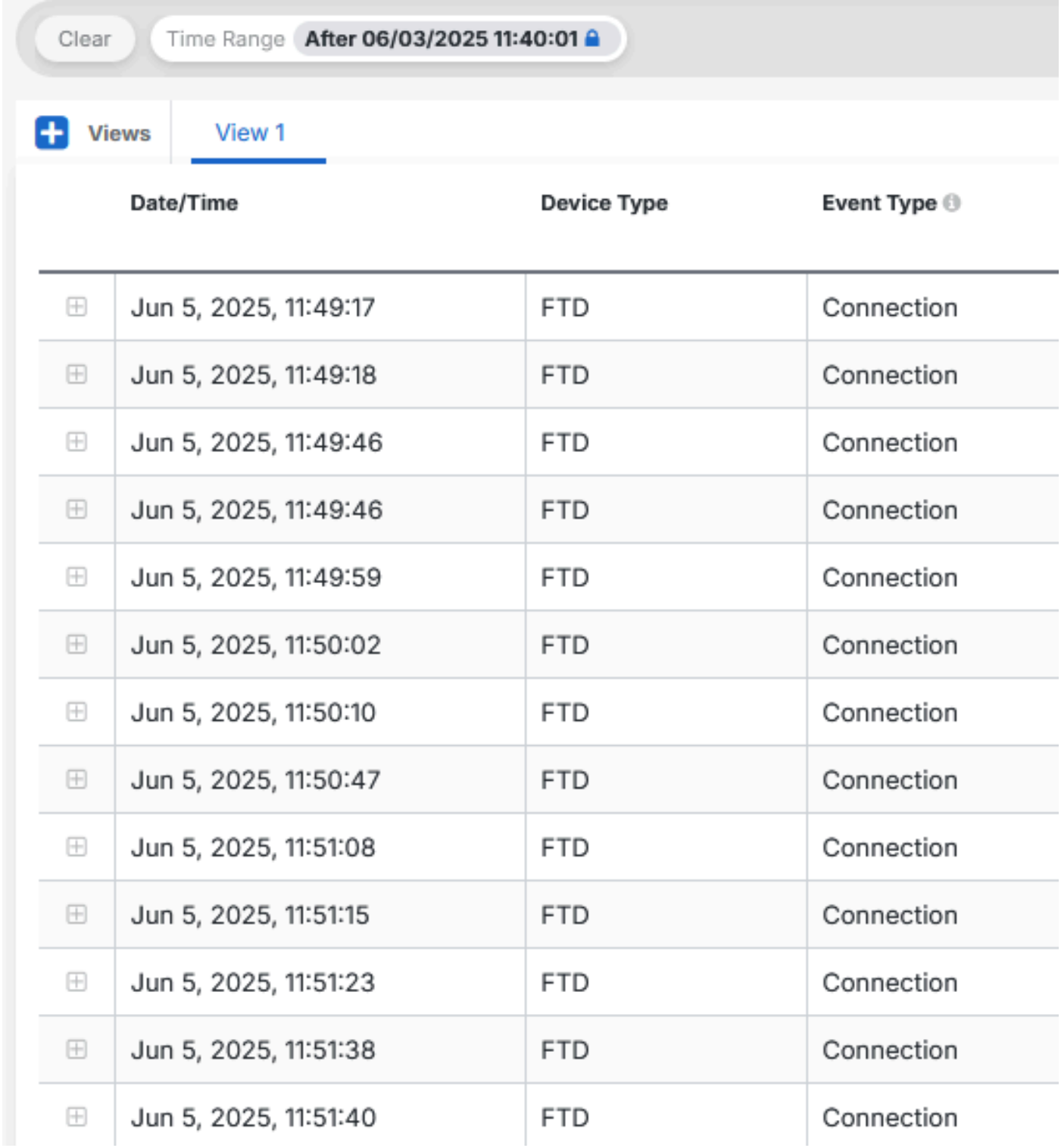
Stap 10. Terug in het toegangsbeleid wijzigt u de afzonderlijke regels om de gebeurtenissen naar de Syslog-server te verzenden:



Stap 11. Implementeer de wijzigingen die in de FTD zijn aangebracht om de firewall in staat te stellen de gebeurtenissen te registreren.

Verifiëren

Om te controleren of de wijzigingen met succes zijn uitgevoerd en of de gebeurtenisregistratie plaatsvindt, gaat u naar Events & Logs en Event Logging in het SCC-portaal en bevestigt u dat de gebeurtenissen zichtbaar zijn:



Problemen oplossen

Voer op FTD een pakketopname uit op het apparaat met behulp van de beheerinterface die overeenkomt met het verkeer dat naar de SEC navigeert om het syslog-verkeer vast te leggen:

```
> 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
```

Zorg ervoor dat de virtuele machine vanaf de SEC een internetverbinding heeft. Voer de opdracht sdc troubleshoot uit, om een bundel voor probleemoplossing te genereren die kan worden gebruikt om het lar.log-bestand te controleren voor verdere diagnose.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.