Konfigurieren der sicheren FTD-Ereignisintegration mit der Cloud-Sicherheitssteuerung über den sicheren Ereignisanschluss

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie Cisco Secure FTD so konfigurieren, dass Sicherheitsereignisse über den Secure Event Connector (SEC) an das Security Cloud Control (SCC) gesendet werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Secure Firewall Threat Defense (FTD)
- Linux-Befehlszeilenschnittstelle (CLI)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Secure FTD 7.6
- Ubuntu Server Version 24.04

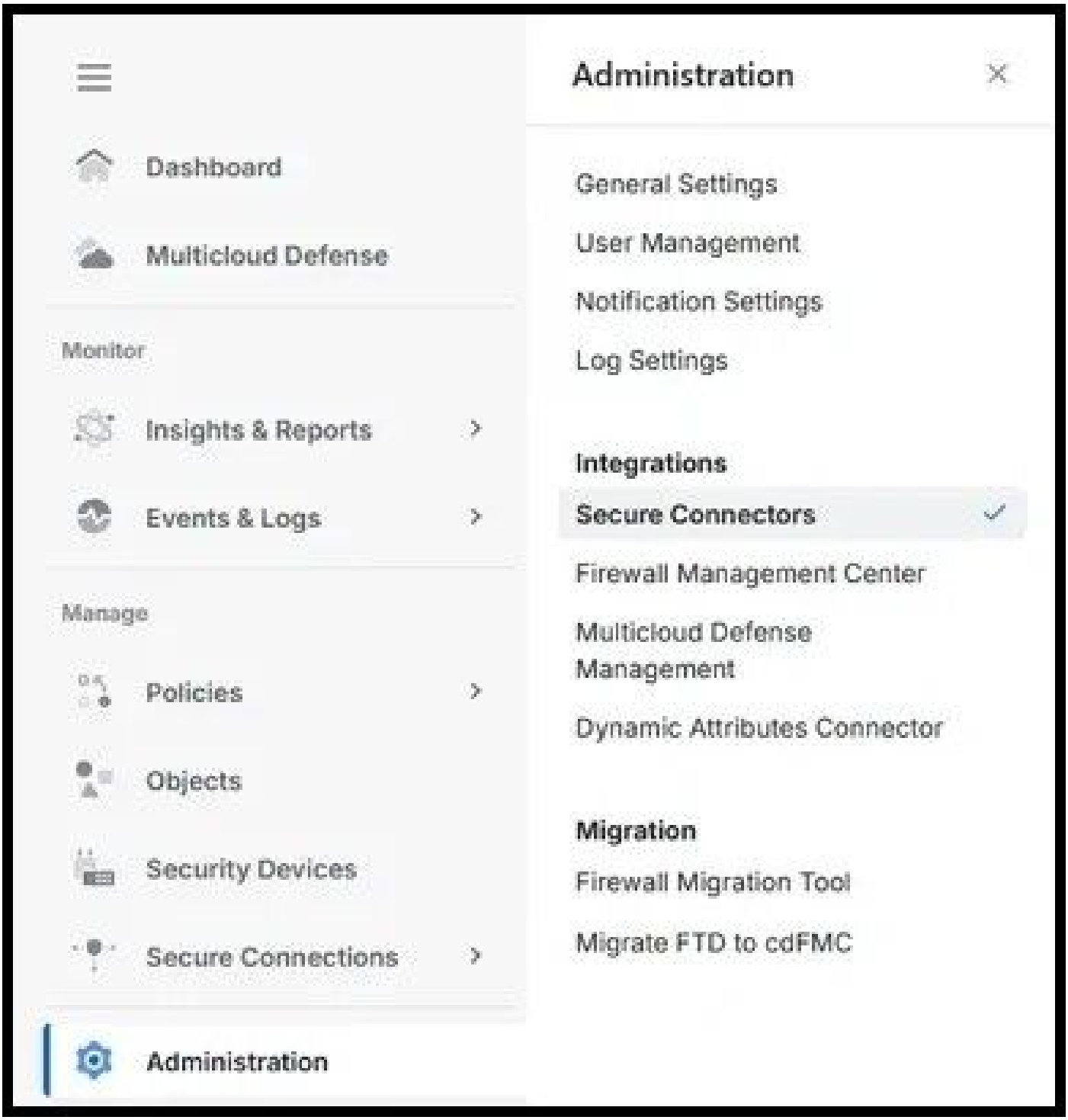
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher,

dass Sie die möglichen Auswirkungen aller Befehle kennen.

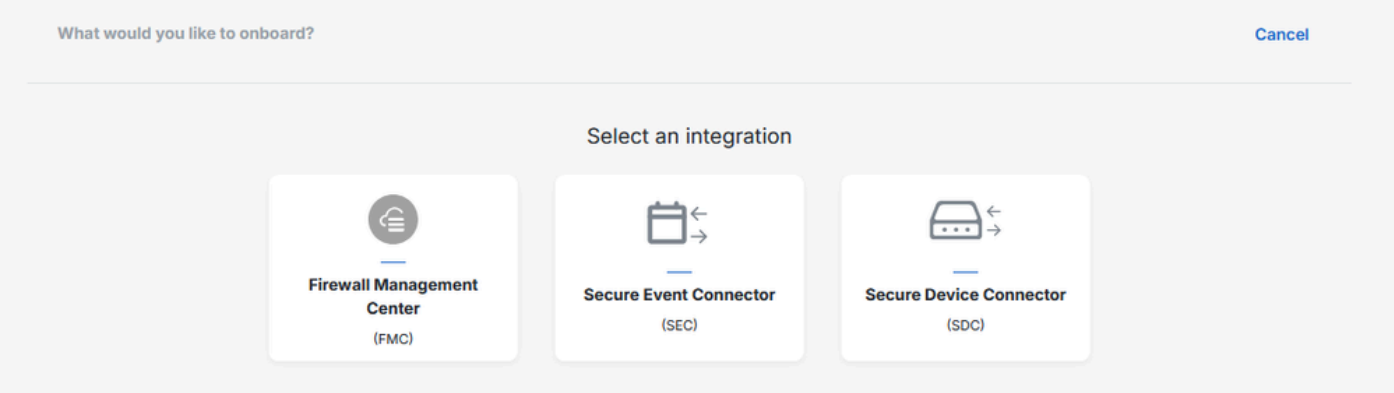
Konfigurieren

Schritt 1: Melden Sie sich beim SCC-Cloud-Portal an:

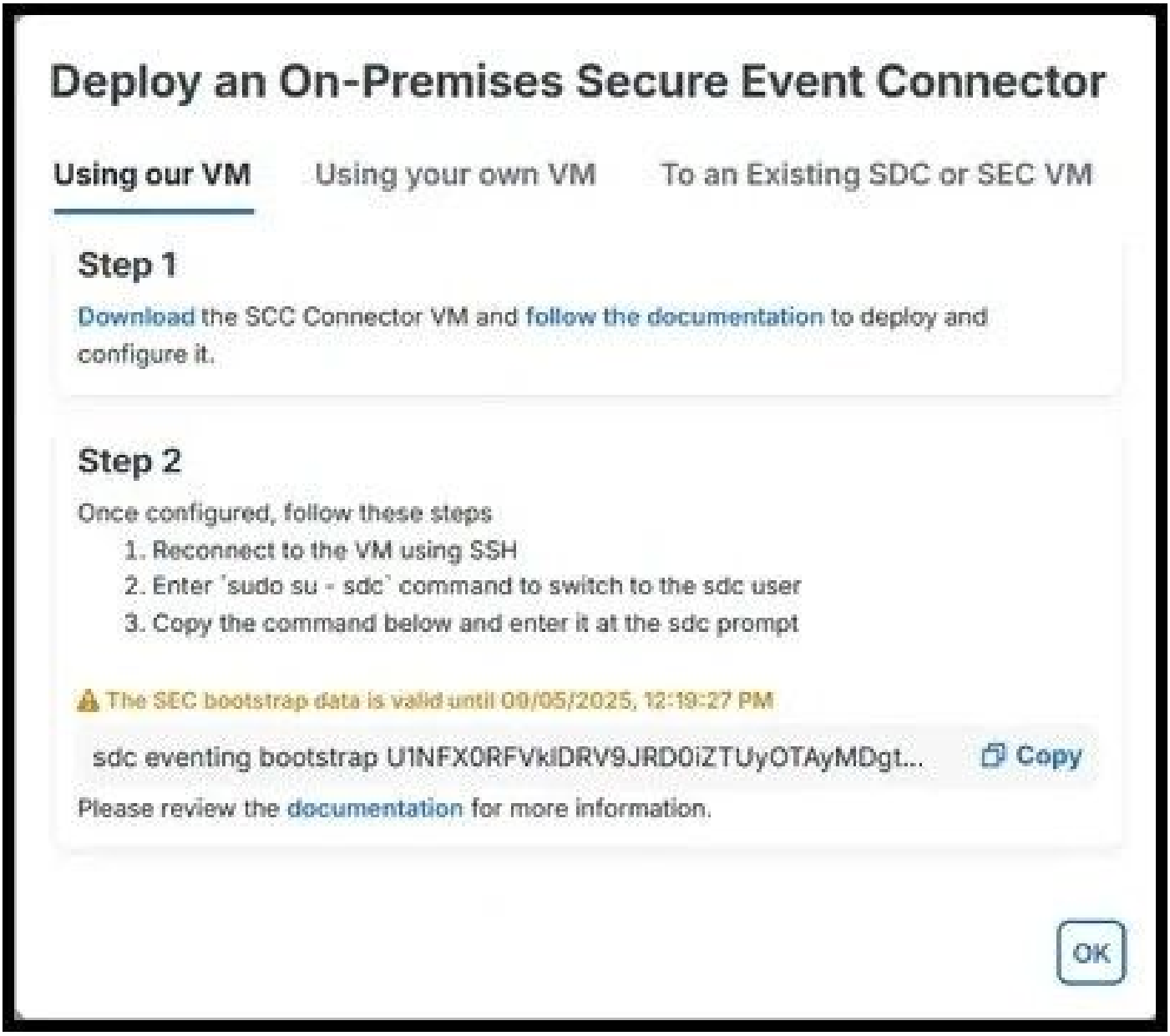
Schritt 2. Wählen Sie im Menü auf der linken Seite Administration and Secure Connectors aus:



Schritt 3. Klicken Sie rechts oben auf das Pluszeichen, um einen neuen Connector zu integrieren, und wählen Sie Secure Event Connector aus:



Schritt 4: Führen Sie die Schritte zum Installieren und Bootstrap des Connectors je nach der gewünschten Option zwischen 'Using our VM', 'Using your own VM' oder 'To an Existent SDC or SEC VM' aus:



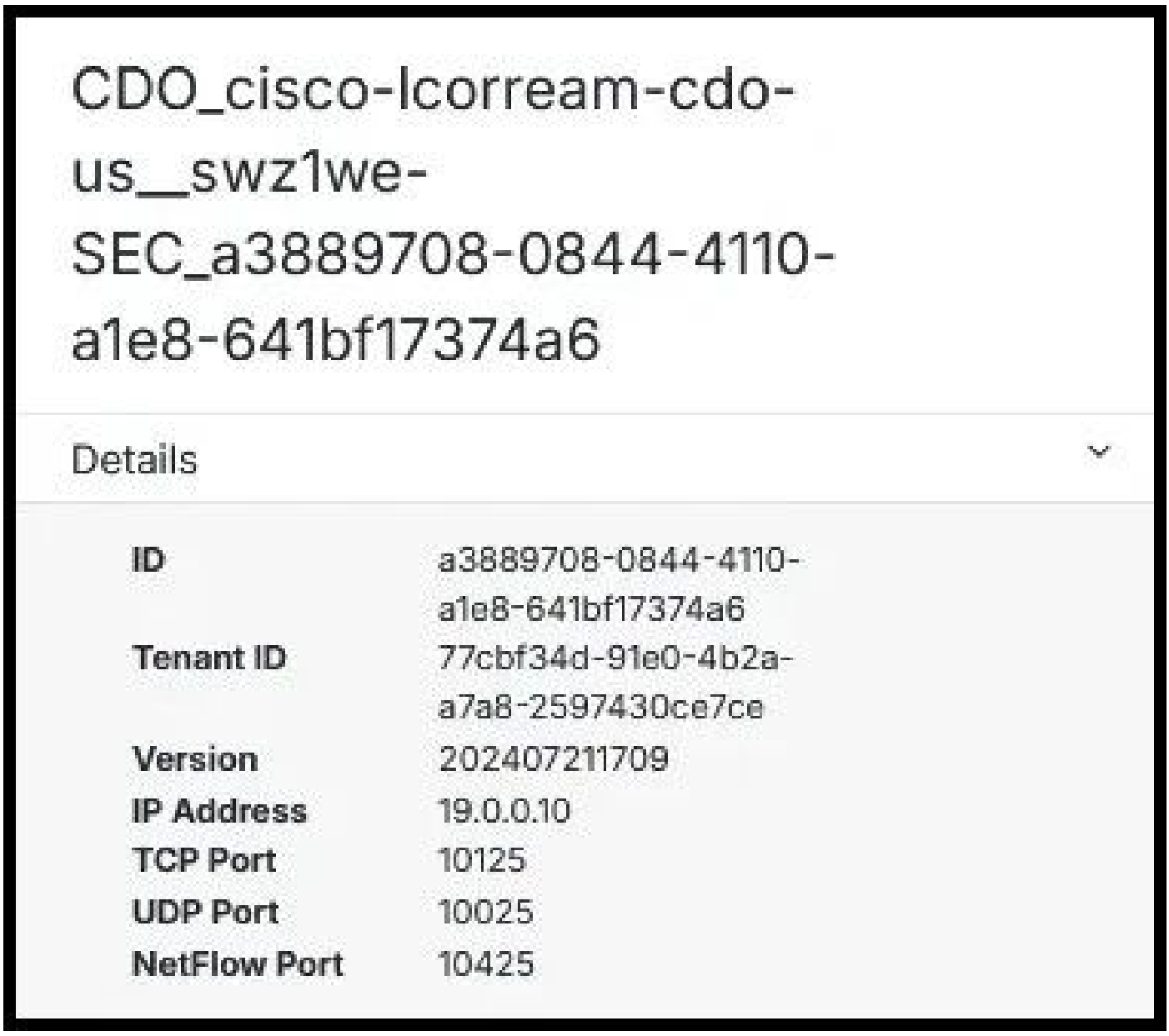
Schritt 5. Eine ähnliche Meldung wird angezeigt, wenn der Bootstrap erfolgreich durchgeführt wird:

```
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:~$
```

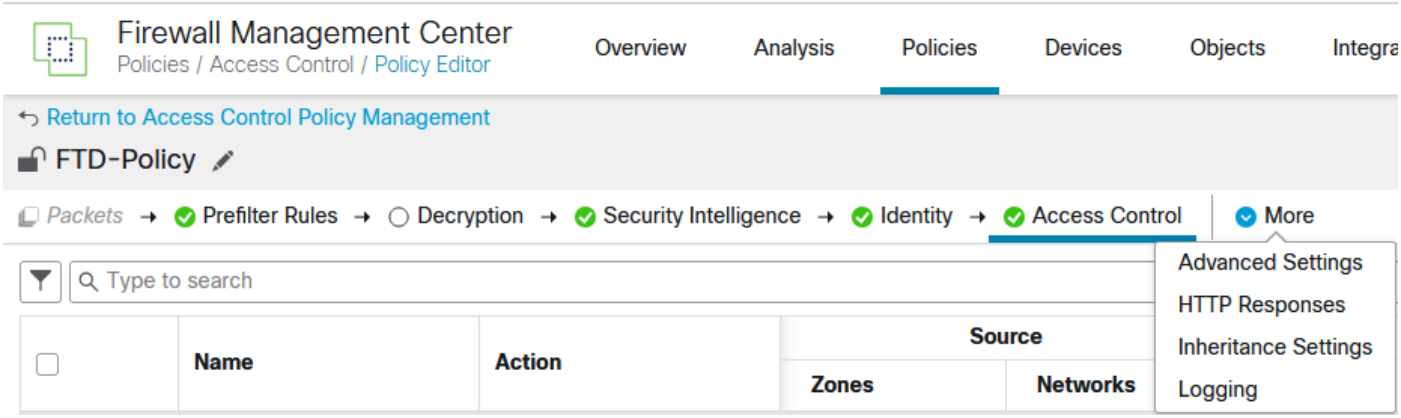
Schritt 6: Nach der Bereitstellung des Connectors und dem Bootstrapping werden die Port-Informationen im SCC-Portal angezeigt:



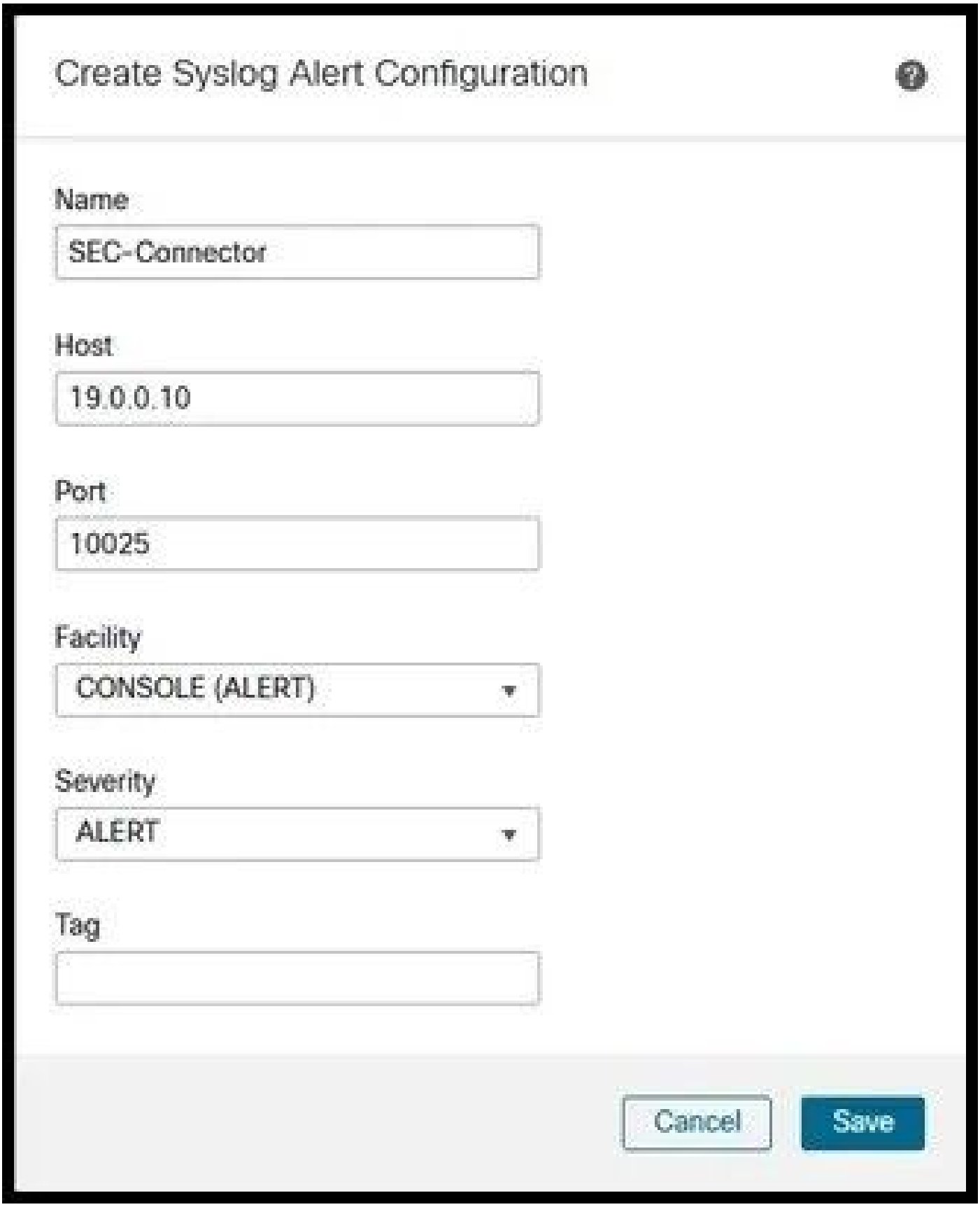
Schritt 7: Navigieren Sie im Cisco Secure Firewall Management Center (FMC) zu Richtlinien und dann zu Zugriffskontrolle. Wählen Sie die Richtlinie aus, die zu den Geräten gehört, die integriert

werden sollen.

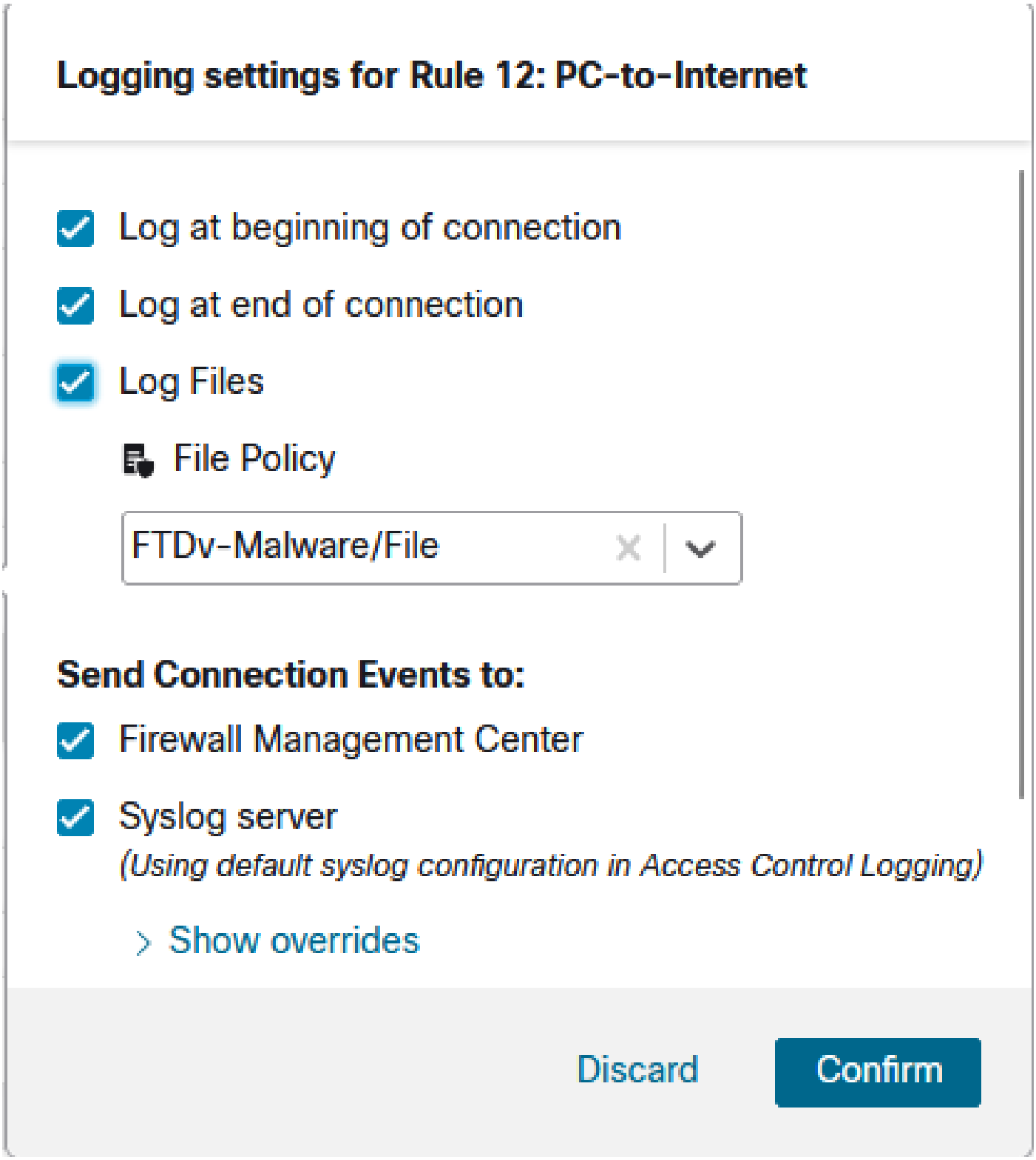
Schritt 8. Wählen Sie Mehr und dann Protokollierung:



Schritt 9: Aktivieren Sie die Option Send using specific syslog alert, und fügen Sie eine neue Syslog-Warnung hinzu. Verwenden Sie die IP-Adresse (Internet Protocol) und die vom SEC-Anschluss im SCC-Portal erhaltenen Port-Informationen:



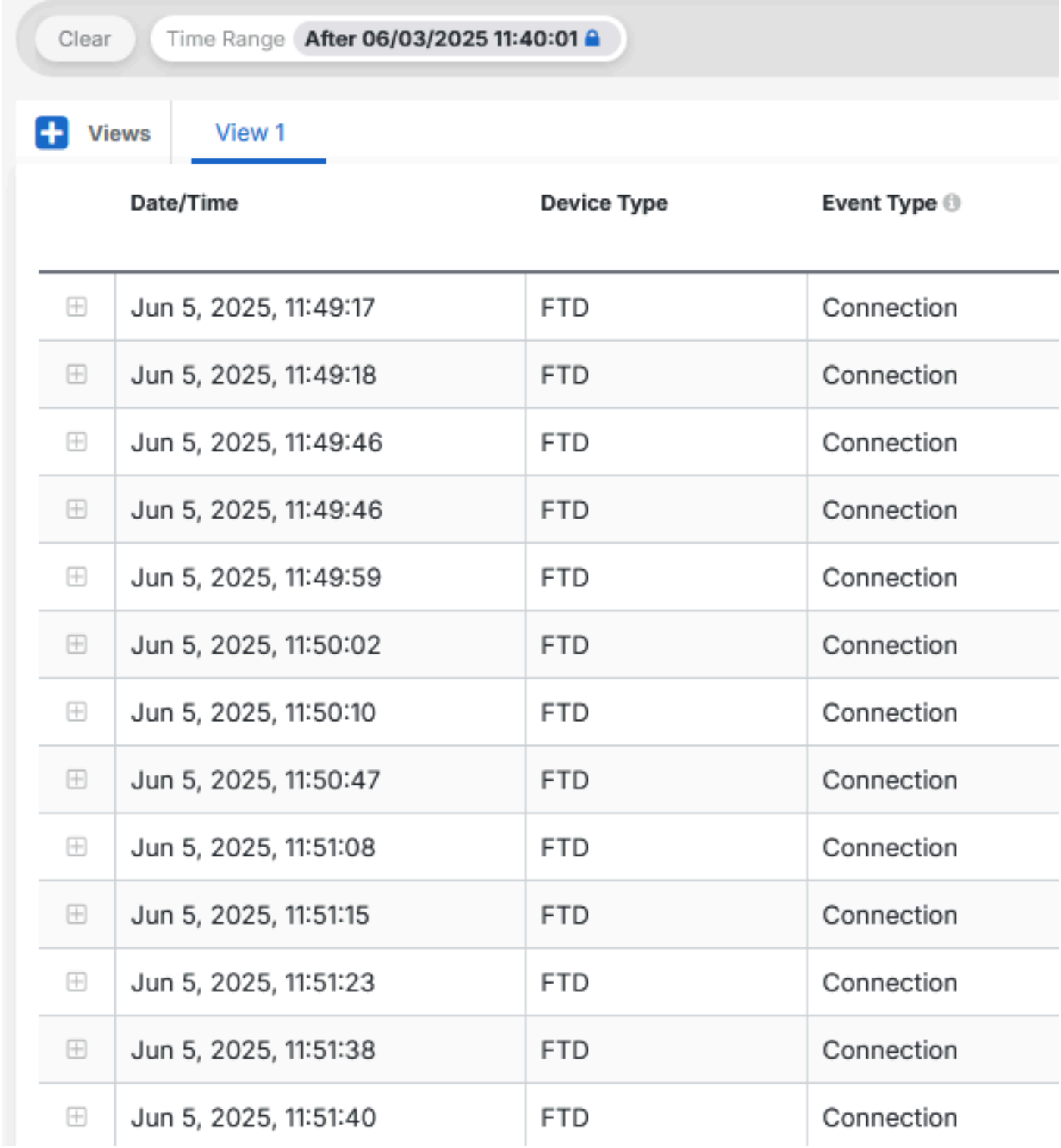
Schritt 10: Ändern Sie in der Zugriffskontrollrichtlinie die einzelnen Regeln, um die Ereignisse an den Syslog-Server zu senden:



Schritt 11: Stellen Sie die Änderungen am FTD bereit, damit die Firewall die Ereignisse protokollieren kann.

Überprüfung

Um sicherzustellen, dass die Änderungen erfolgreich durchgeführt wurden und die Ereignisprotokollierung stattfindet, navigieren Sie zu Events & Logs and Event Logging im SCC-Portal, und bestätigen Sie, dass die Ereignisse sichtbar sind:



Fehlerbehebung

Führen Sie auf FTD eine Paketerfassung auf dem Gerät mithilfe der Verwaltungsschnittstelle durch, die mit dem Verkehr übereinstimmt, der zur SEC navigiert, um den Syslog-Verkehr zu erfassen:

```
> 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
```

Stellen Sie über das virtuelle SEC-System sicher, dass das virtuelle System über eine Internetverbindung verfügt. Führen Sie den Befehl sdc troubleshoot aus, um ein Fehlerbehebungspaket zu generieren, mit dem die Datei lar.log für eine weitere Diagnose überprüft werden kann.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.