Configurer l'intégration sécurisée des événements FTD avec le contrôle cloud de sécurité via le connecteur d'événements sécurisé

Table des matières

Introduction

Ce document décrit comment configurer le Cisco Secure FTD pour envoyer des événements de sécurité au Security Cloud Control (SCC) à l'aide du Secure Event Connector (SEC).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Secure Firewall Threat Defense (FTD)
- Interface de ligne de commande (CLI) Linux

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

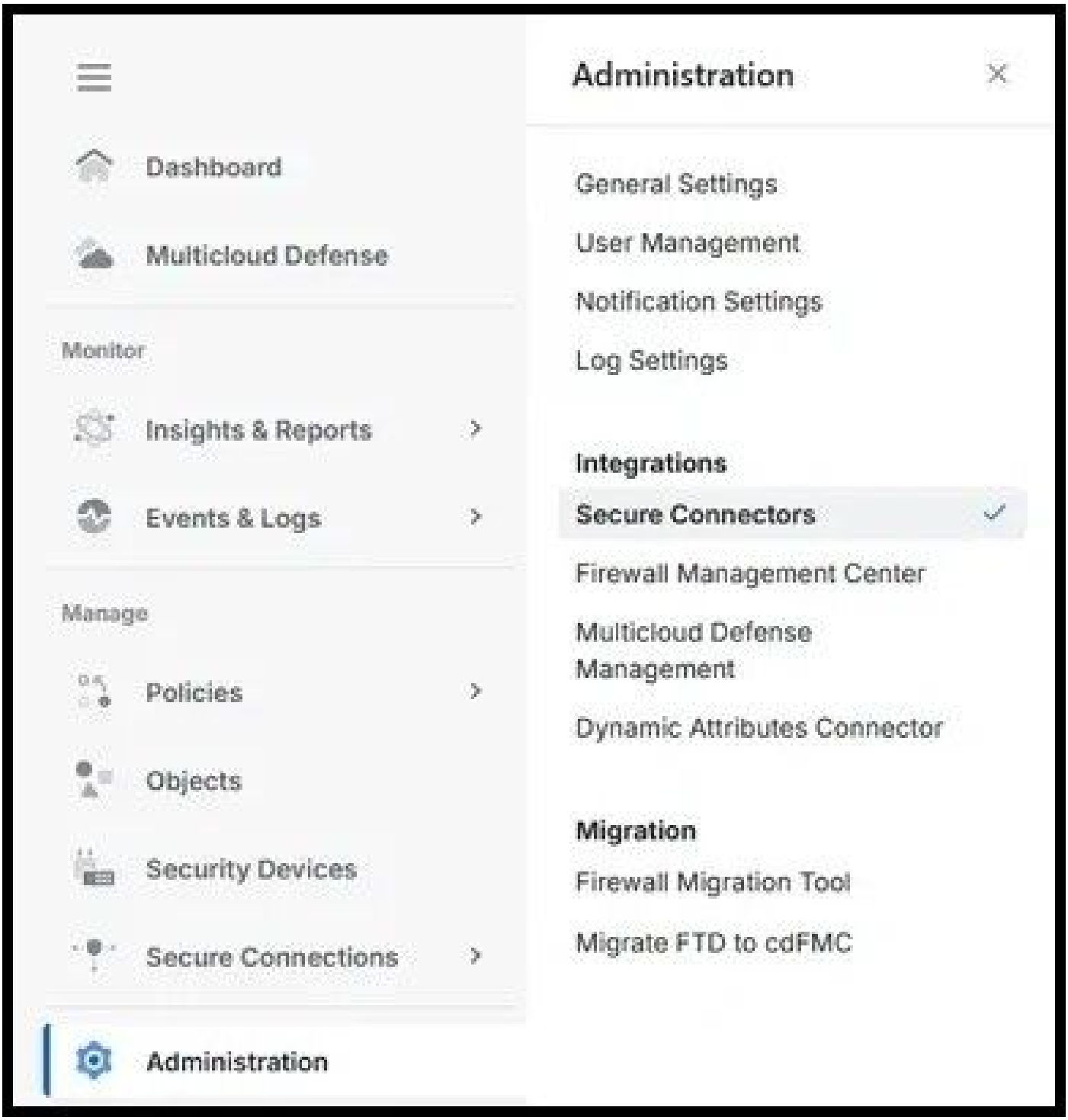
- Cisco Secure FTD 7.6
- Serveur Ubuntu version 24.04

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

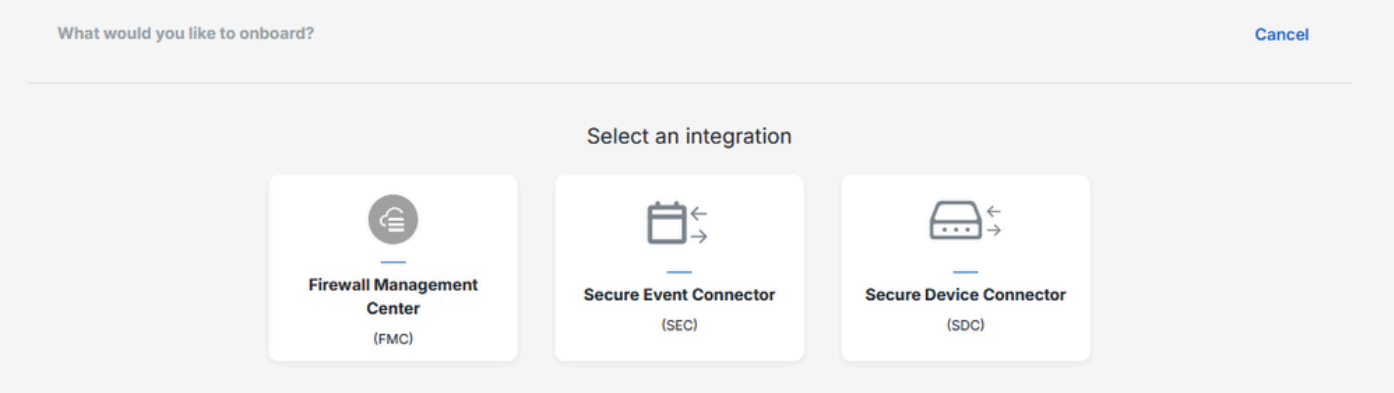
Configurer

Étape 1. Connexion au portail cloud SCC :

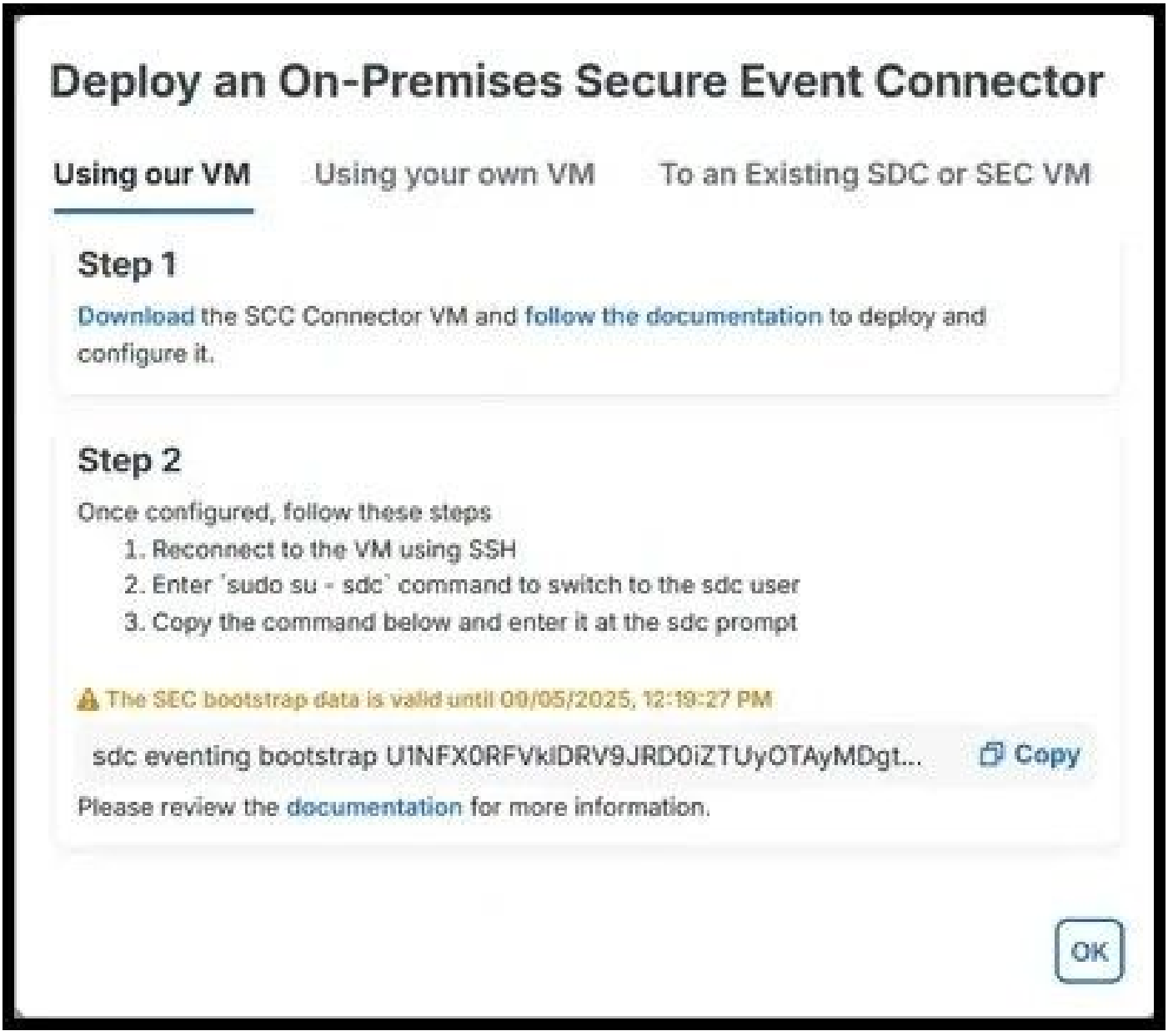
Étape 2. Dans le menu de gauche, sélectionnez Administration and Secure Connecteurs (Administration et connecteurs sécurisés) :



Étape 3. En haut à droite, cliquez sur l’icône plus pour intégrer un nouveau connecteur et choisir Secure Event Connector :



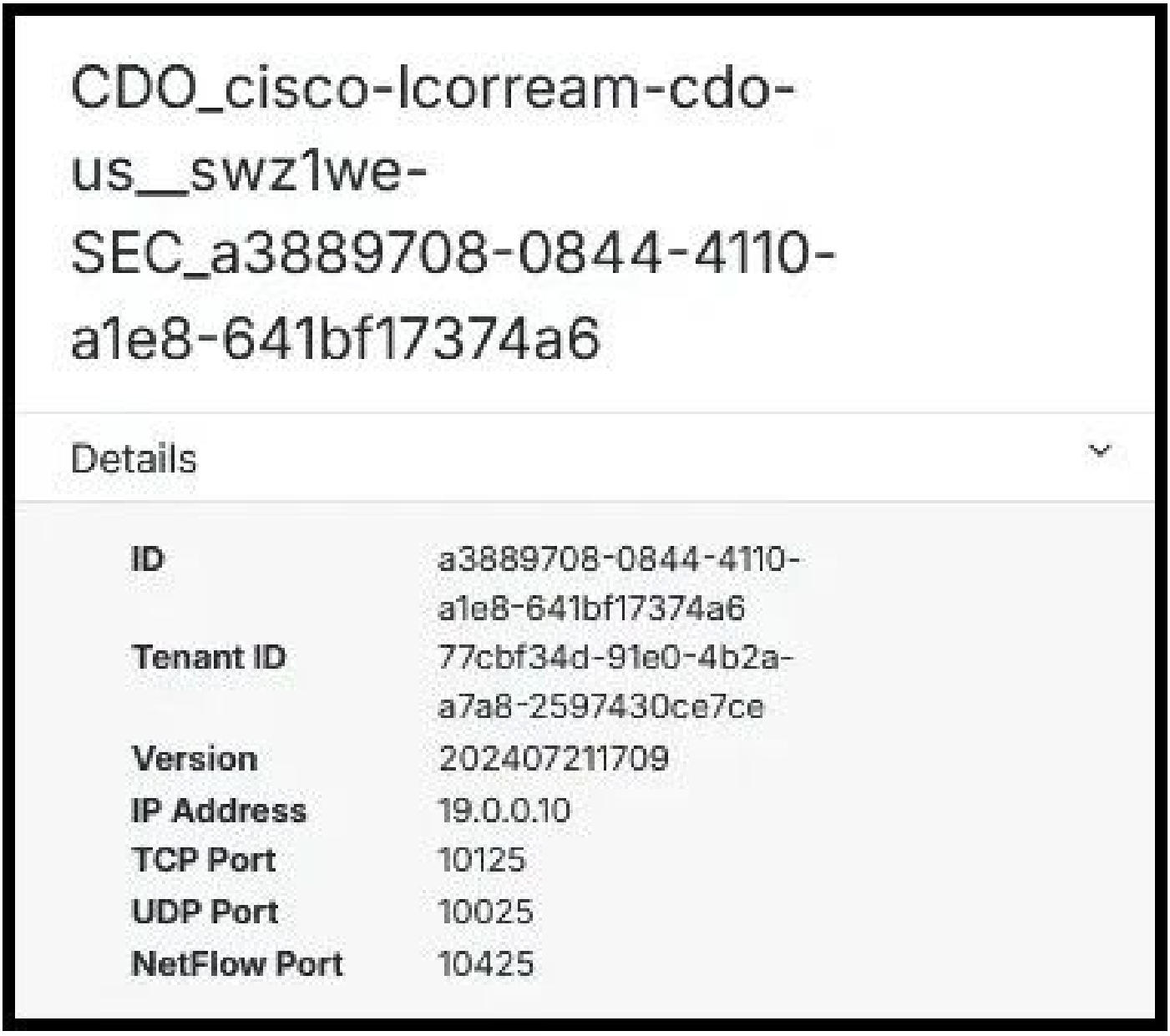
Étape 4. Suivez les étapes d'installation et d'amorçage du connecteur selon l'option souhaitée entre « Utilisation de votre machine virtuelle », « Utilisation de votre propre machine virtuelle » ou « Vers un SDC existant ou une machine virtuelle de sécurité » :



Étape 5. Un message similaire s’affiche lorsque le bootstrap est exécuté avec succès :

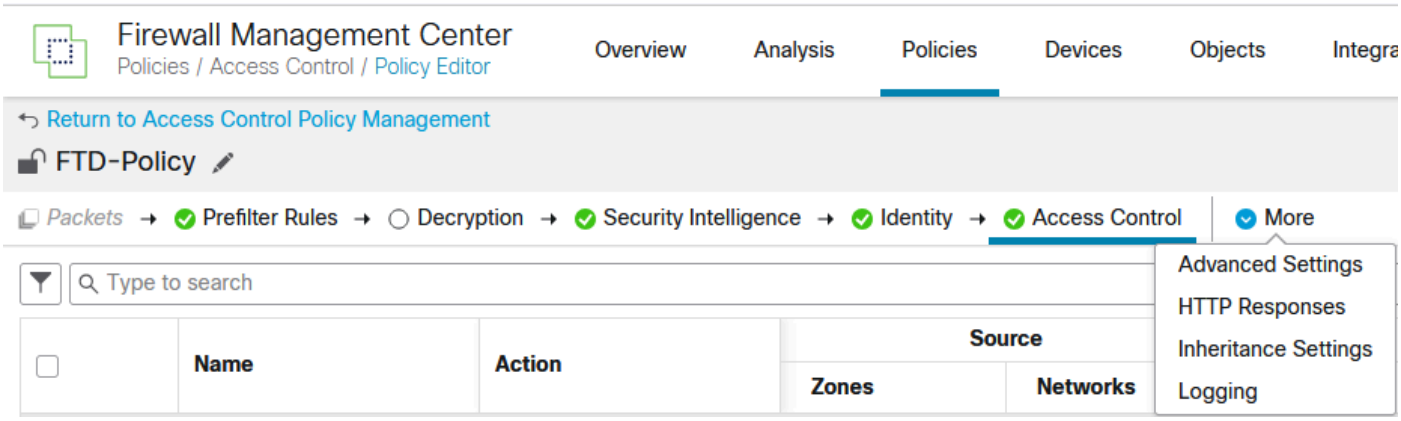
```
2025-06-09 05:41:56 [INFO] Bootstrap package processed successfully
2025-06-09 05:41:56 [INFO] Default AWS Region is us-west-2
2025-06-09 05:42:00 [INFO] Scanning for next available TCP port starting with 10125
2025-06-09 05:42:00 [INFO] TCP port found and set to 10125
2025-06-09 05:42:00 [INFO]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

Étape 6. Une fois le connecteur déployé et amorcé, les informations de port sont visibles dans le portail SCC :

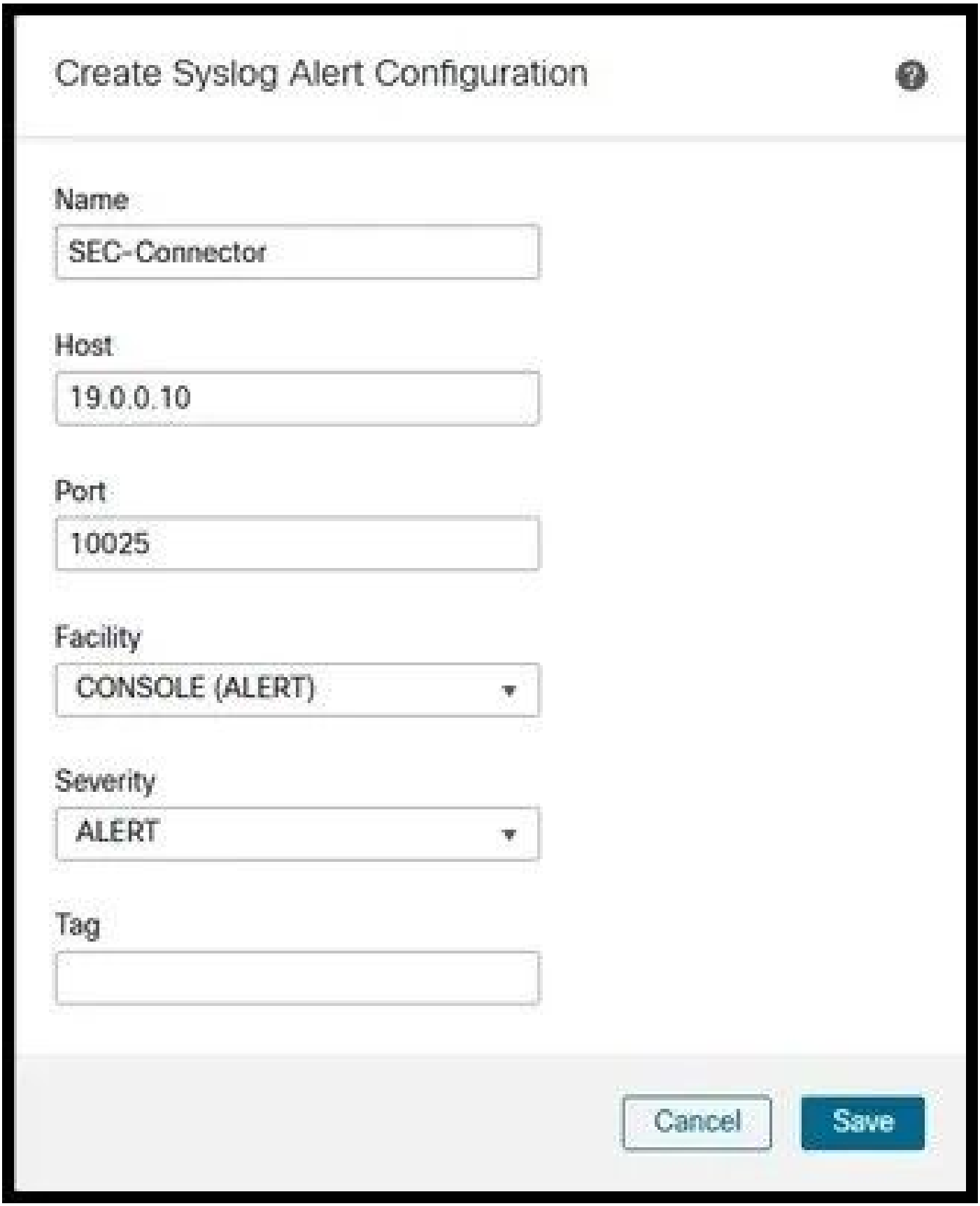


Étape 7. Sur le Cisco Secure Firewall Management Center (FMC), accédez à Policies, puis à Access Control. Sélectionnez la politique correspondant au(x) périphérique(s) à intégrer.

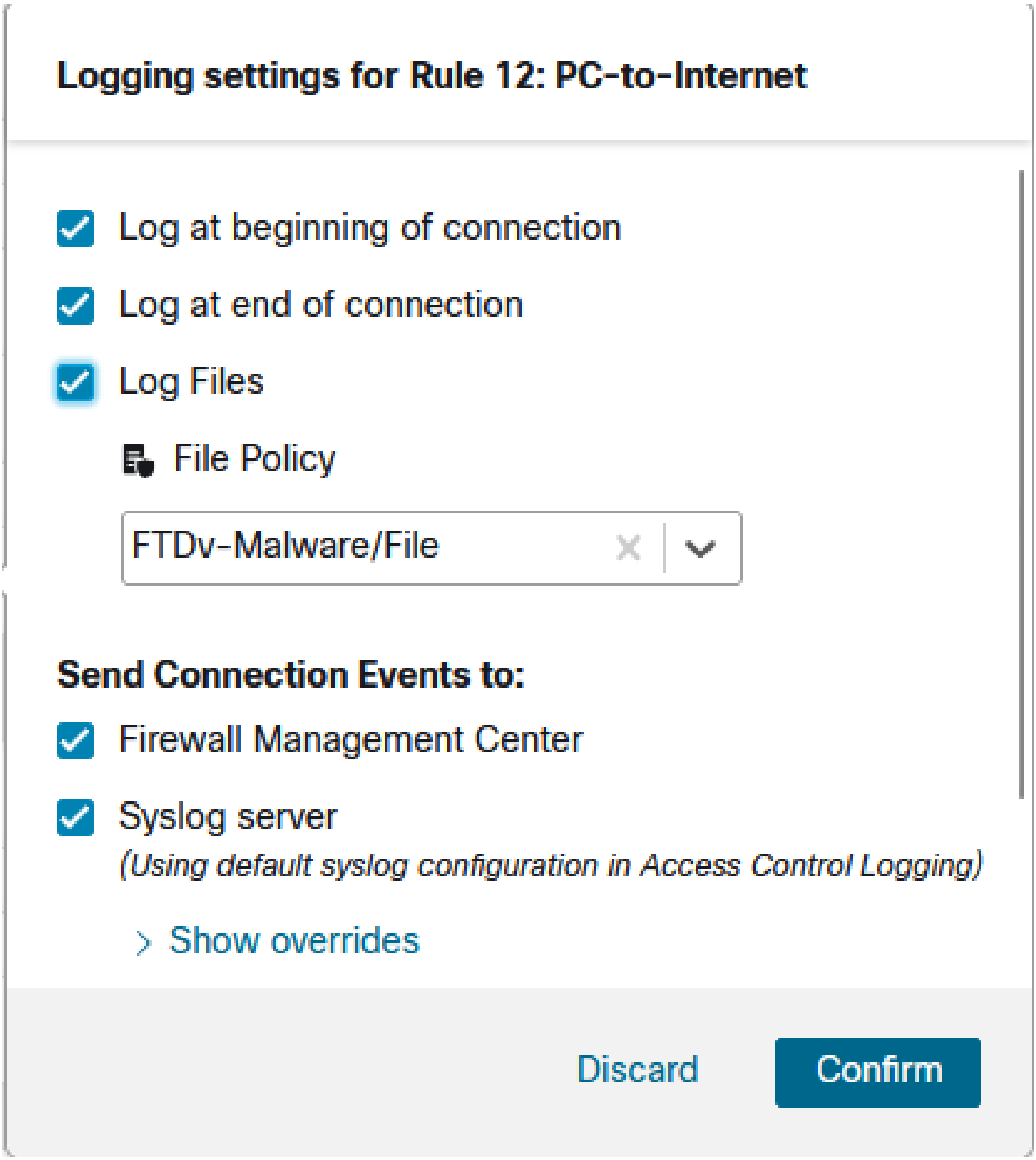
Étape 8. Choisissez More, puis Logging :



Étape 9. Activez l'option Send using specific syslog alert et ajoutez une nouvelle alerte Syslog. Utilisez l'adresse IP (Internet Protocol) et les informations de port obtenues à partir du connecteur SEC dans le portail SCC :



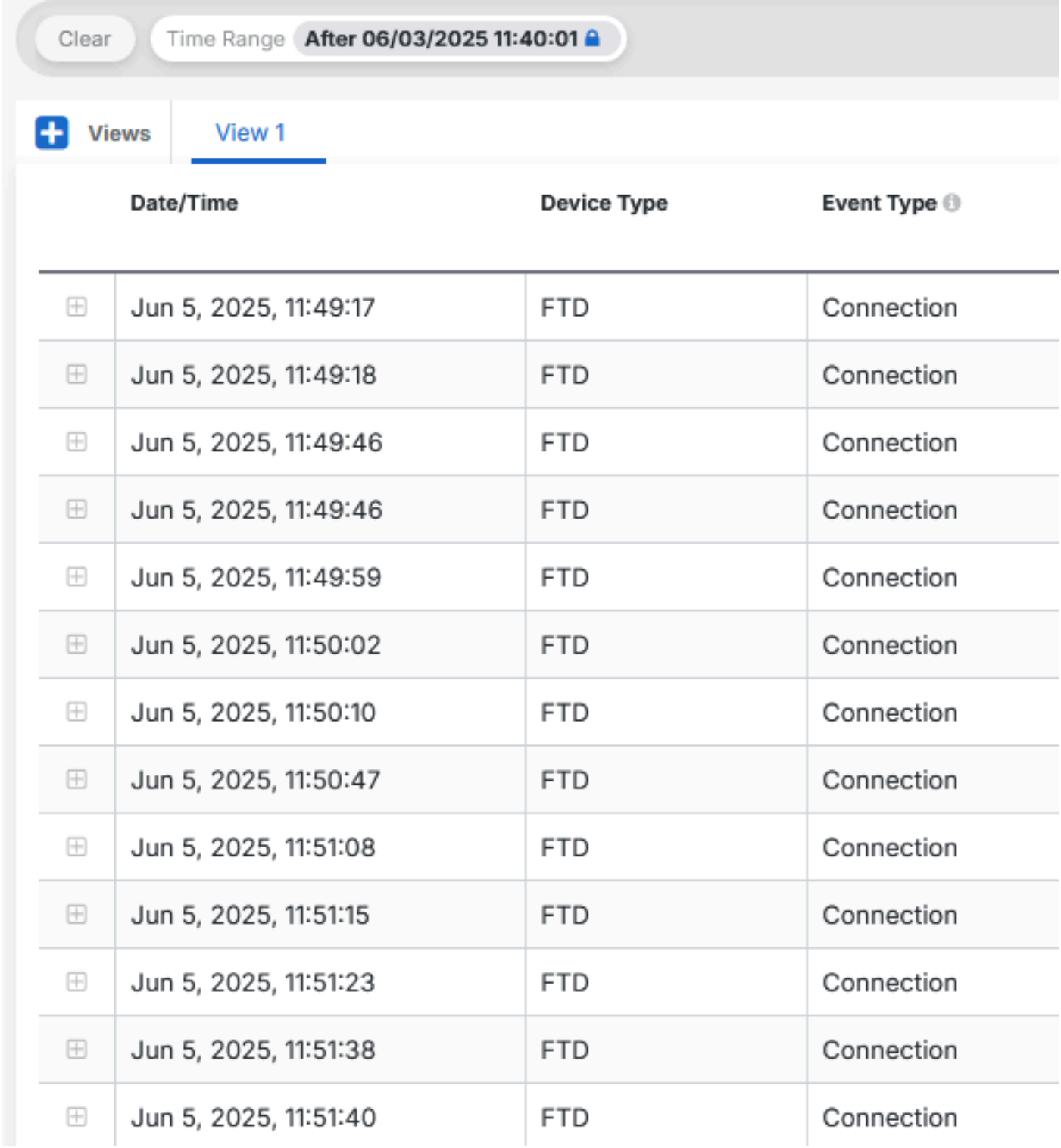
Étape 10. Revenez à la politique de contrôle d'accès, modifiez les règles individuelles afin d'envoyer les événements au serveur Syslog :



Étape 11. Déployez les modifications apportées au FTD afin de permettre au pare-feu de commencer à consigner les événements.

Vérifier

Afin de vérifier que les modifications ont été exécutées avec succès et que la journalisation des événements a lieu, accédez à Events & Logs et Event Logging dans le portail SCC et vérifiez que les événements sont visibles :



Dépannage

Sur FTD, exécutez une capture de paquets sur le périphérique à l'aide de l'interface de gestion correspondant au trafic naviguant vers la SEC afin de capturer le trafic syslog :

```
> 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
```

À partir de l'ordinateur virtuel SEC, assurez-vous que l'ordinateur virtuel dispose d'une connectivité Internet. Exécutez la commande sdc troubleshoot, afin de générer un bundle de dépannage qui peut être utilisé pour vérifier le fichier lar.log pour un diagnostic plus approfondi.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.