Secure Event Connectorを介したSecurity Cloud Controlとのセキュアなイベント統合の設定

内容

はじめに

このドキュメントでは、Secure Event Connector(SEC)を使用してセキュリティイベント(SCC)をセキュリティクラウド制御(SCC)に送信するようにCisco Secure FTD(SFTD)を設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Secure Firewall Threat Defense(FTD)
- Linuxコマンドラインインターフェイス(CLI)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

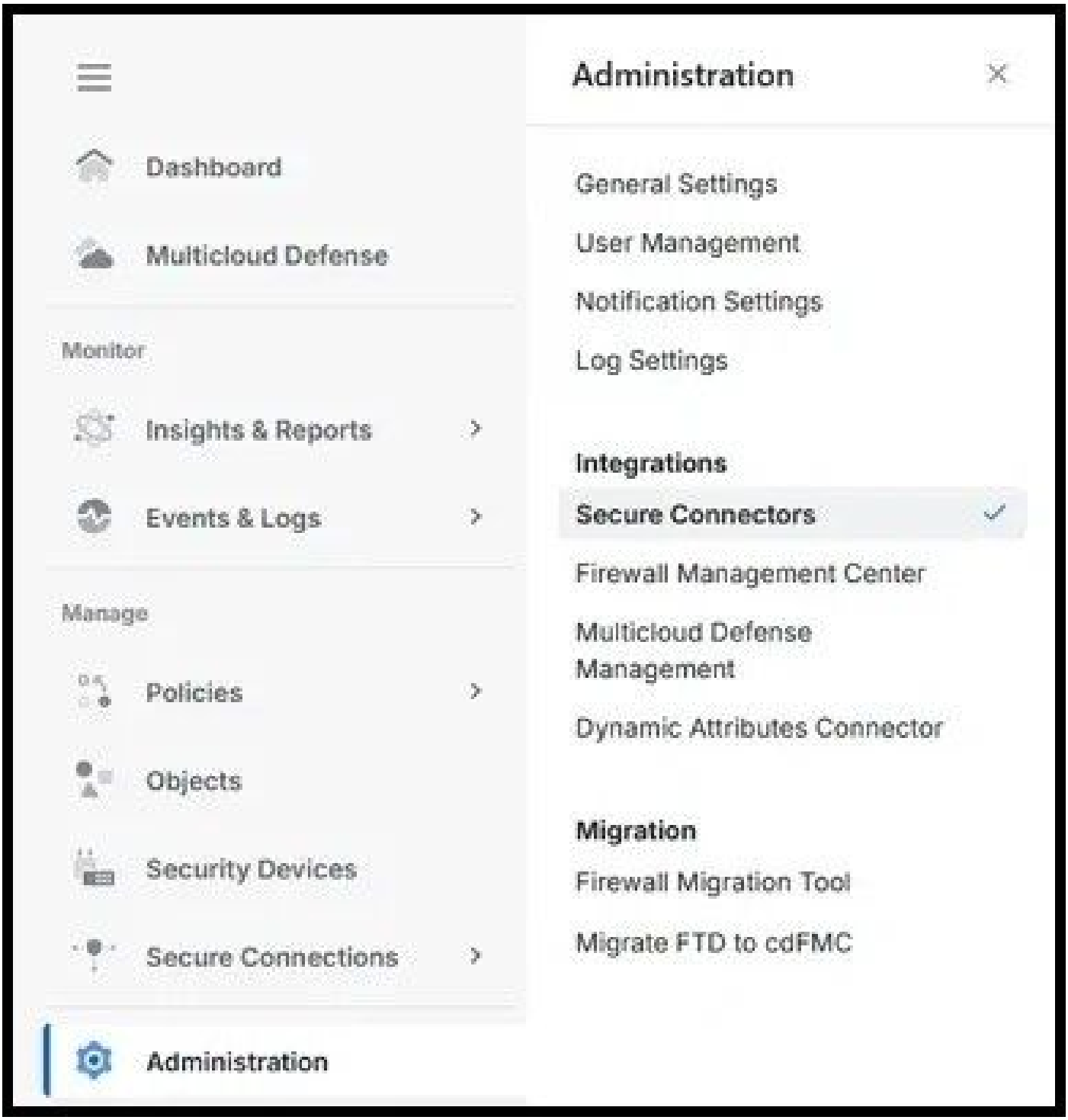
- Cisco Secure FTD 7.6
- Ubuntu Serverバージョン24.04

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

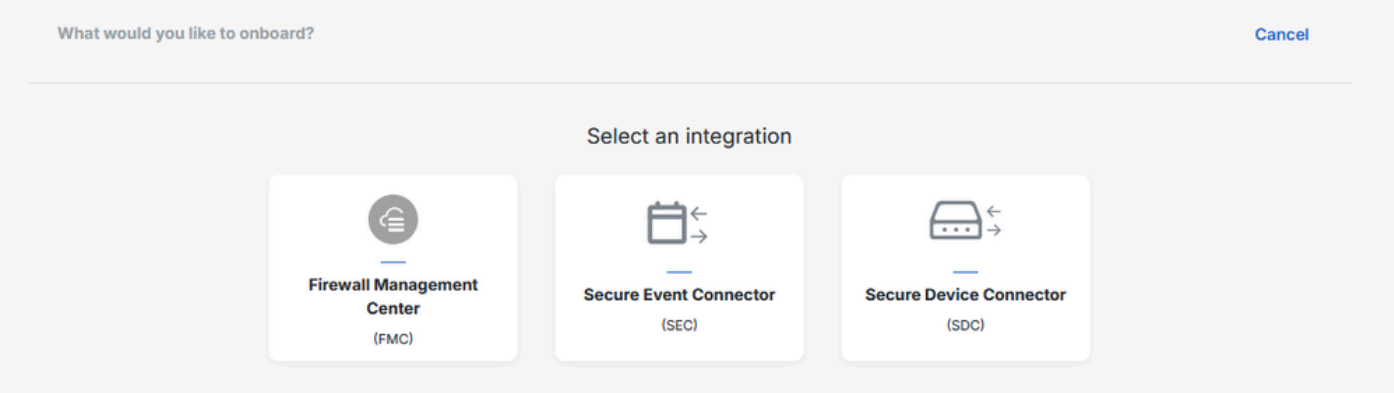
設定

ステップ 1：SCCクラウドポータルにログインします。

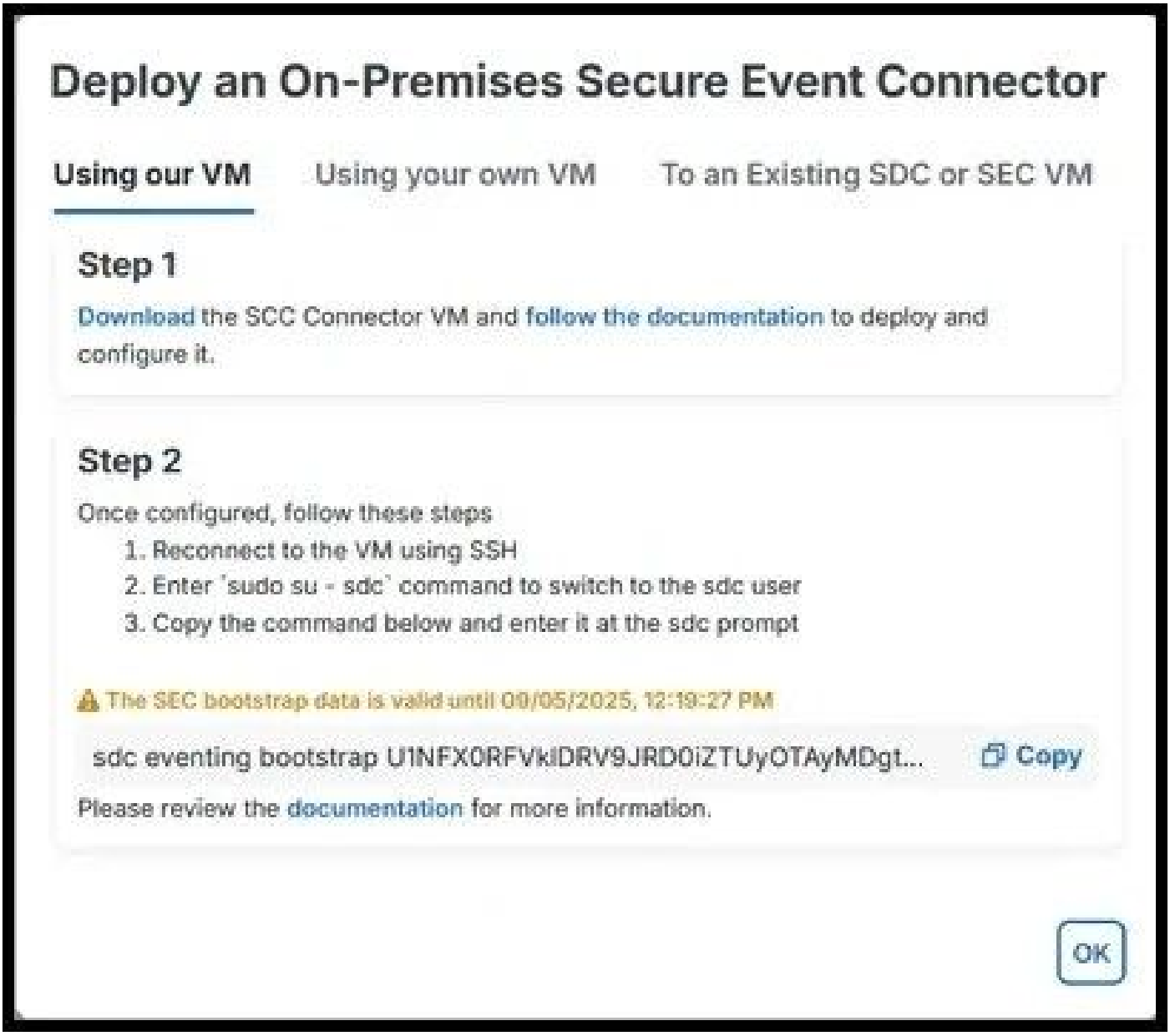
ステップ 2：左側のメニューから、AdministrationおよびSecure Connectorsを選択します。



ステップ 3：右上のプラスアイコンをクリックして、新しいコネクタをオンボードし、Secure Event Connectorを選択します。



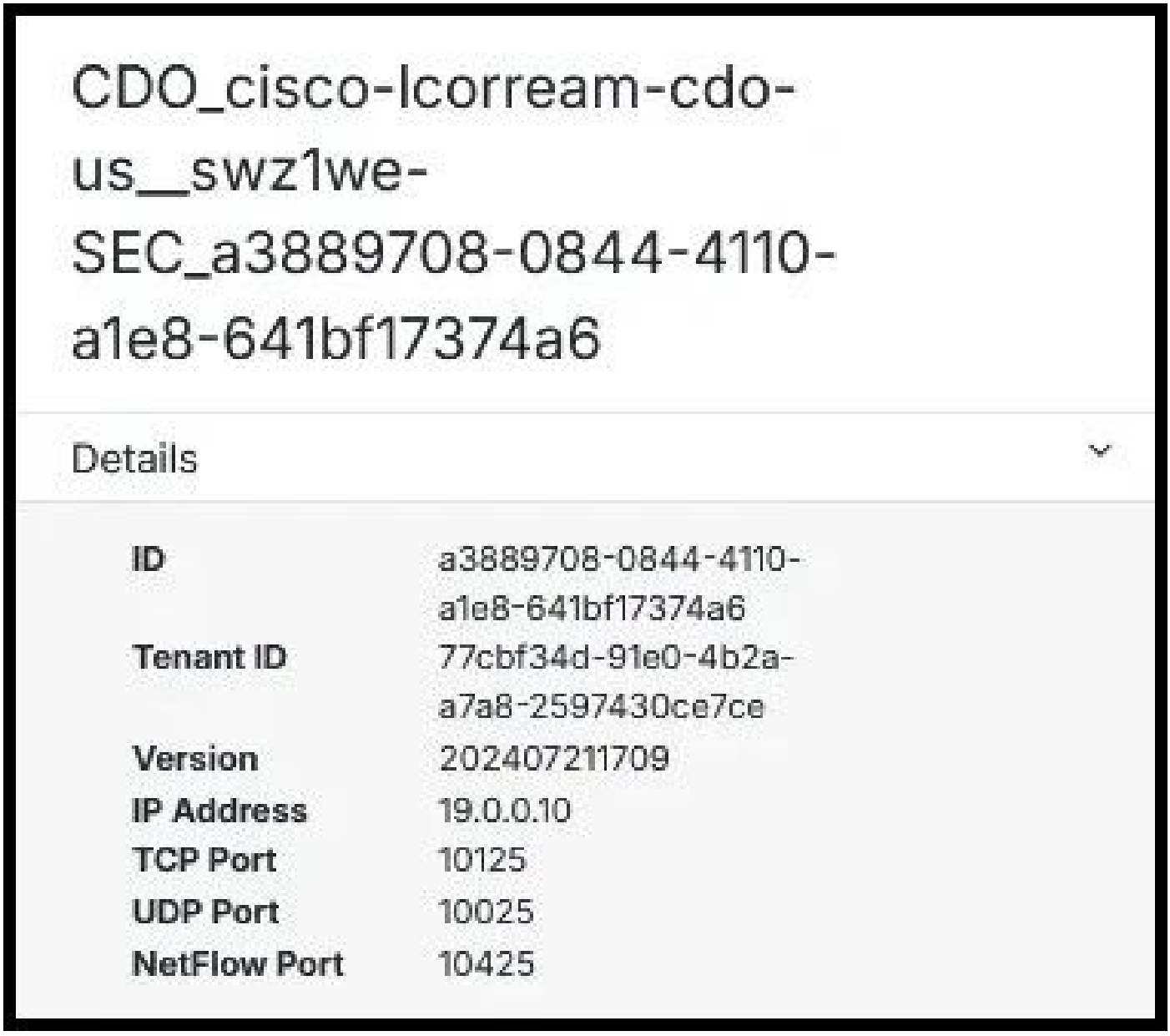
ステップ 4：「VMの使用」、「独自のVMの使用」、「既存のSDCまたはSEC VMへの接続」の希望するオプションに応じて、コネクタのインストールとブートストラップの手順を使用します。



ステップ 5：ブートストラップが正常に実行されると、同様のメッセージが表示されます。

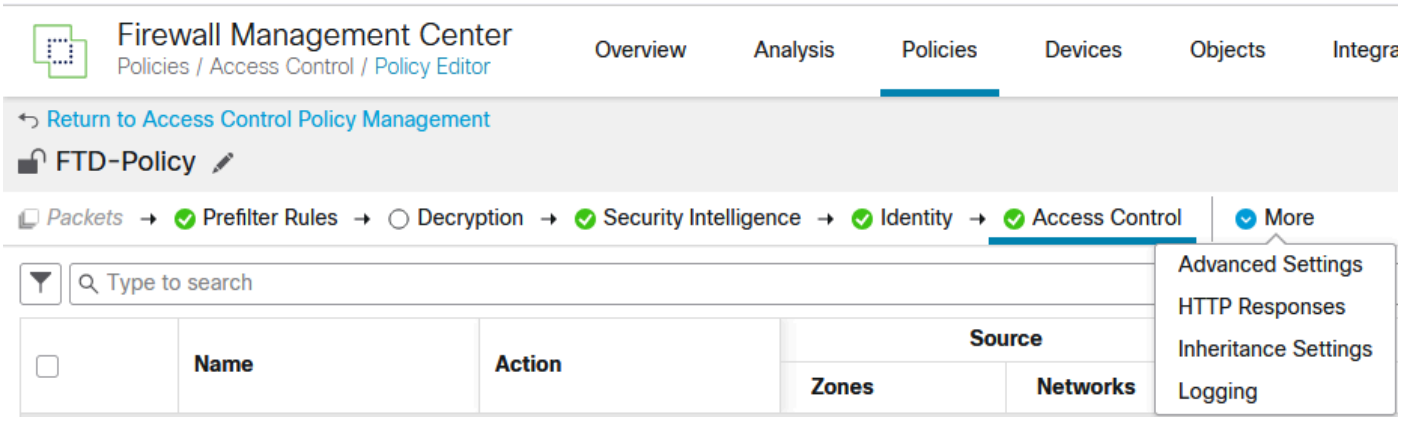
```
2025-06-09 05:41:56 [INFO] Bootstrap package processed successfully
2025-06-09 05:41:56 [INFO] Default AWS Region is us-west-2
2025-06-09 05:42:00 [INFO] Scanning for next available TCP port starting with 10125
2025-06-09 05:42:00 [INFO] TCP port found and set to 10125
2025-06-09 05:42:00 [INFO]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

手順 6：コネクタが導入され、ブートストラップされると、ポート情報がSCCポータルに表示されます。

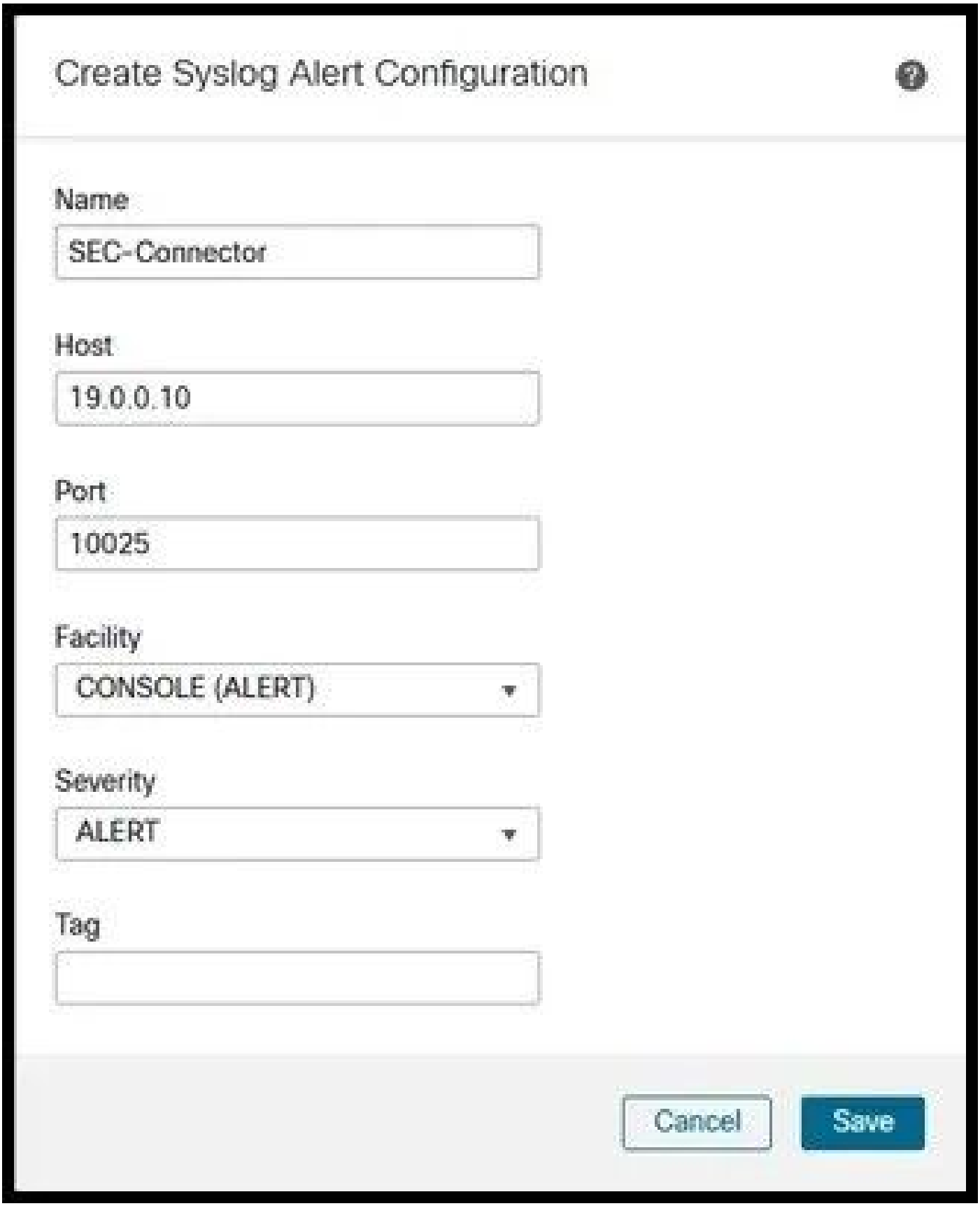


手順 7：Cisco Secure Firewall Management Center(FMC)で、Policiesに移動してから、Access Controlに移動します。オンボーディングするデバイスに対応するポリシーを選択します。

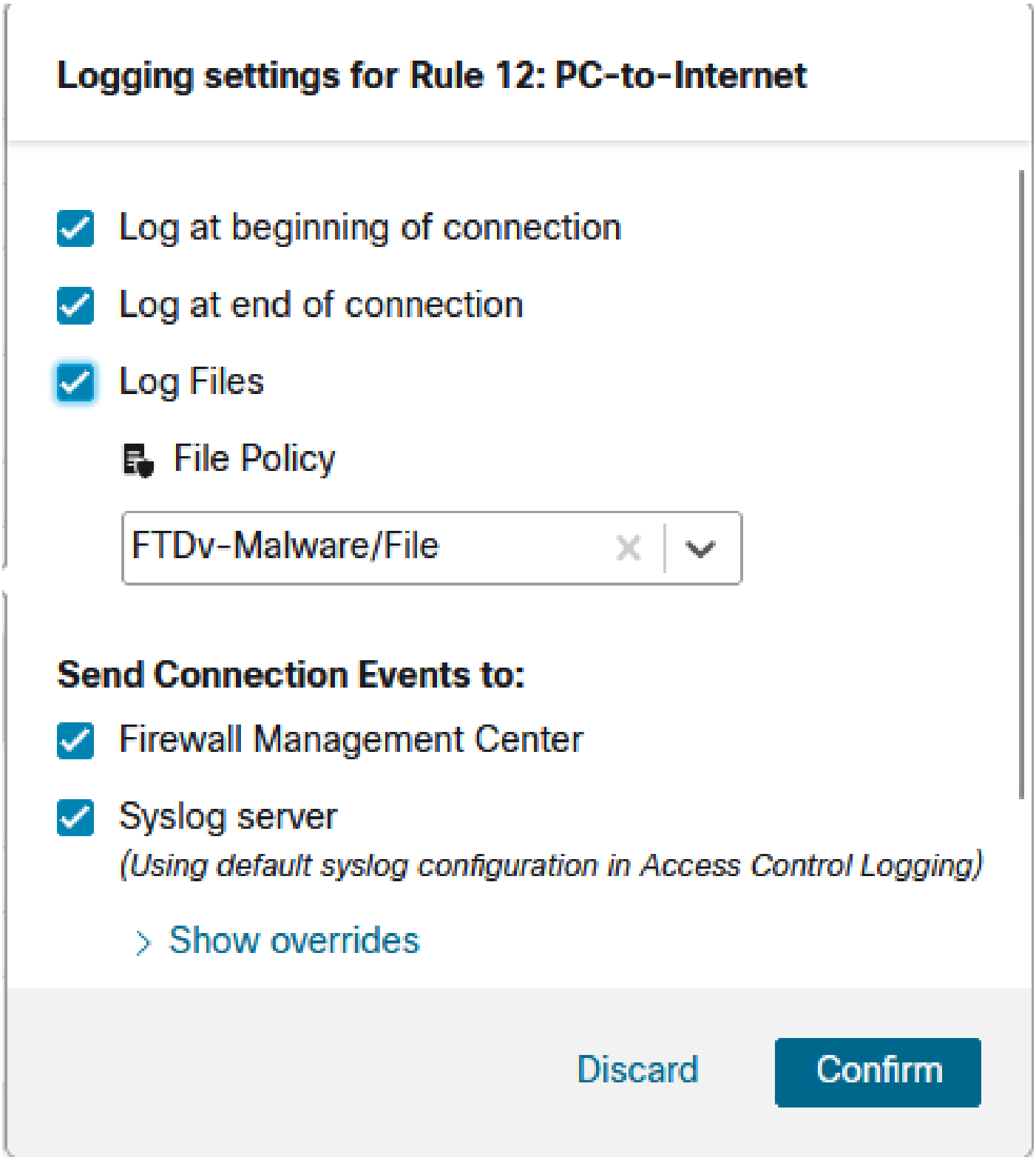
ステップ 8：More、Loggingの順に選択します。



ステップ 9：Send using specific syslog alertオプションを有効にし、新しいSyslog Alertを追加します。SCCポータルで、SECコネクタから取得したインターネットプロトコル(IP)アドレスとポート情報を使用します。



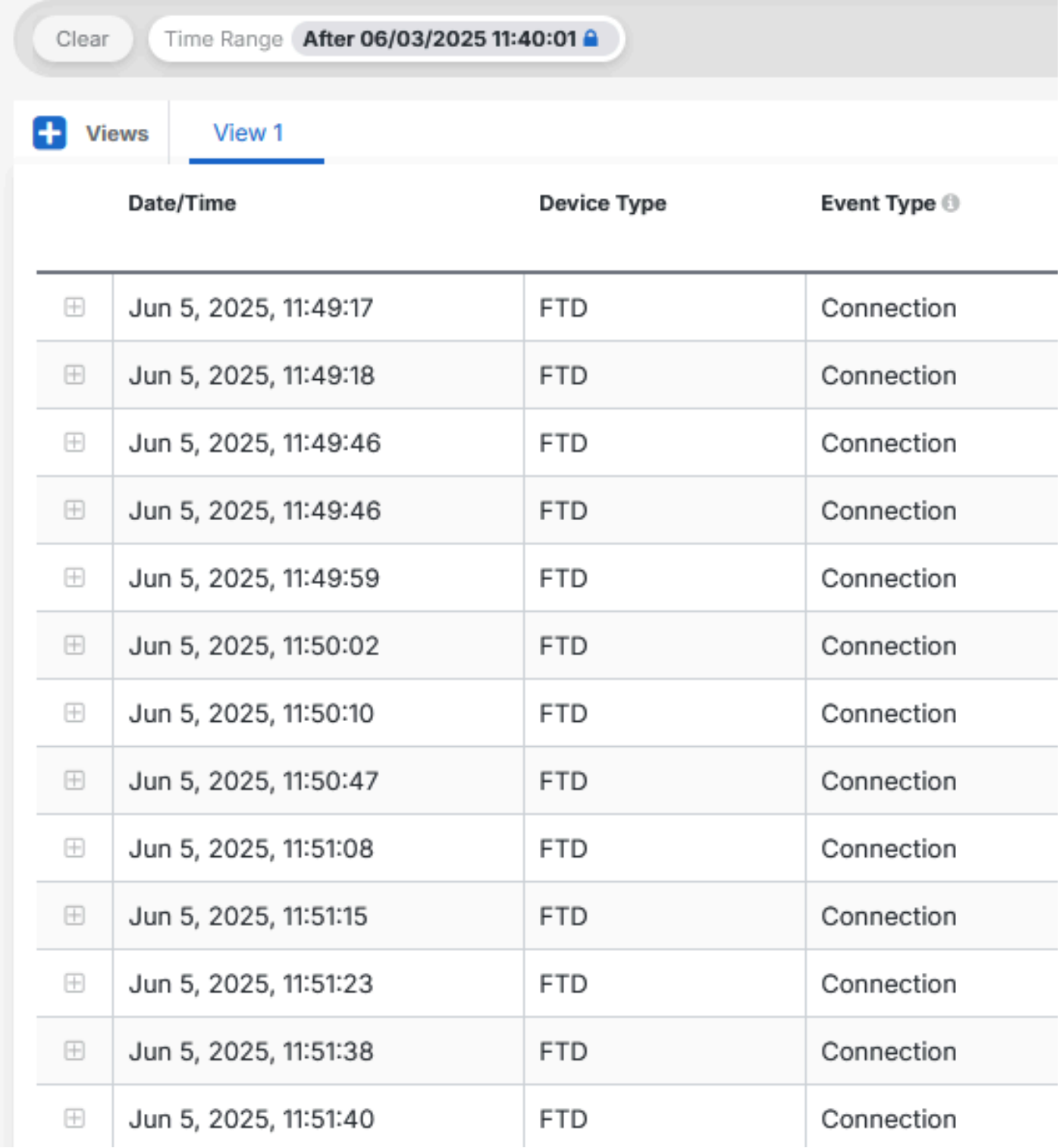
ステップ 10：Access Control Policyに戻り、Syslogサーバにイベントを送信するために個々のルールを変更します。



ステップ 11ファイアウォールがイベントのロギングを開始できるように、FTDに加えられた変更を展開します。

確認

変更が正常に実行され、イベントロギングが行われていることを確認するには、SCCポータルでEvents & LogsおよびEvent Loggingに移動し、イベントが表示されていることを確認します。



トラブルシュート

FTDで、SECに移動するトラフィックと一致する管理インターフェイスを使用してデバイス上でパケットキャプチャを実行し、syslogトラフィックをキャプチャします。

```
> 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仮想マシンから、仮想マシンがインターネットに接続できることを確認します。sdc troubleshootコマンドを実行して、トラブルシューティングバンドルを生成します。このバンドルを使用して、lar.logファイルの詳細診断を確認できます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。