通过安全事件连接器配置安全FTD事件与安全云控制集成

目录

简介

本文档介绍如何配置思科安全FTD，以使用安全事件连接器(SEC)将安全事件发送到安全云控制(SCC)。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科安全防火墙威胁防御(FTD)
- Linux命令行界面(CLI)

使用的组件

本文档中的信息基于以下软件和硬件版本：

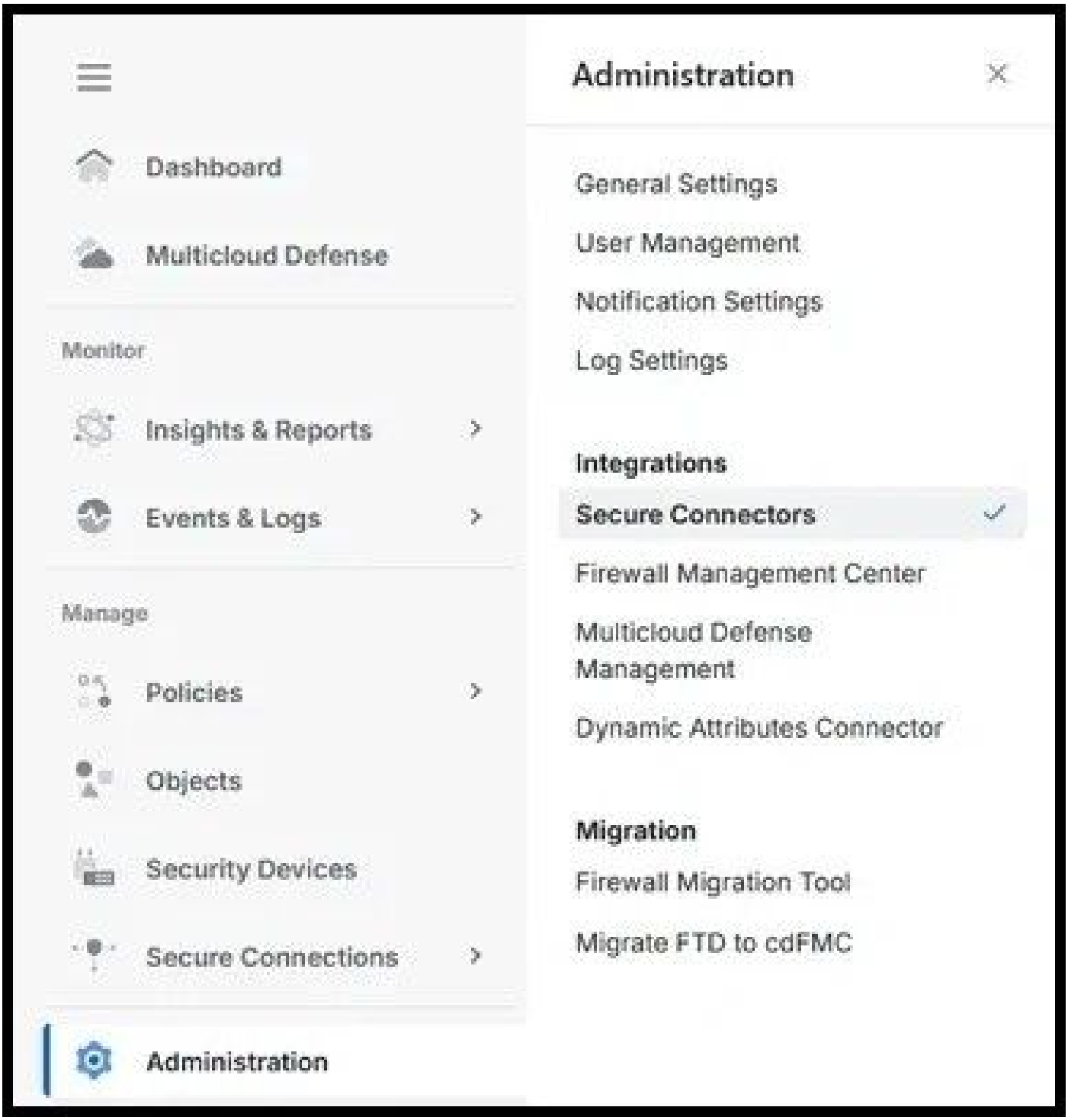
- 思科安全FTD 7.6
- Ubuntu服务器版本24.04

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

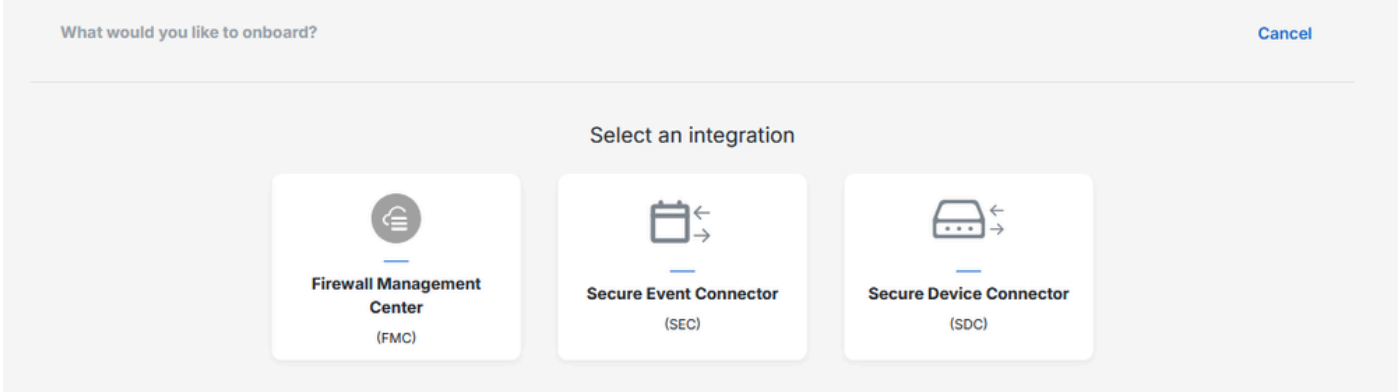
配置

步骤1.登录SCC云门户：

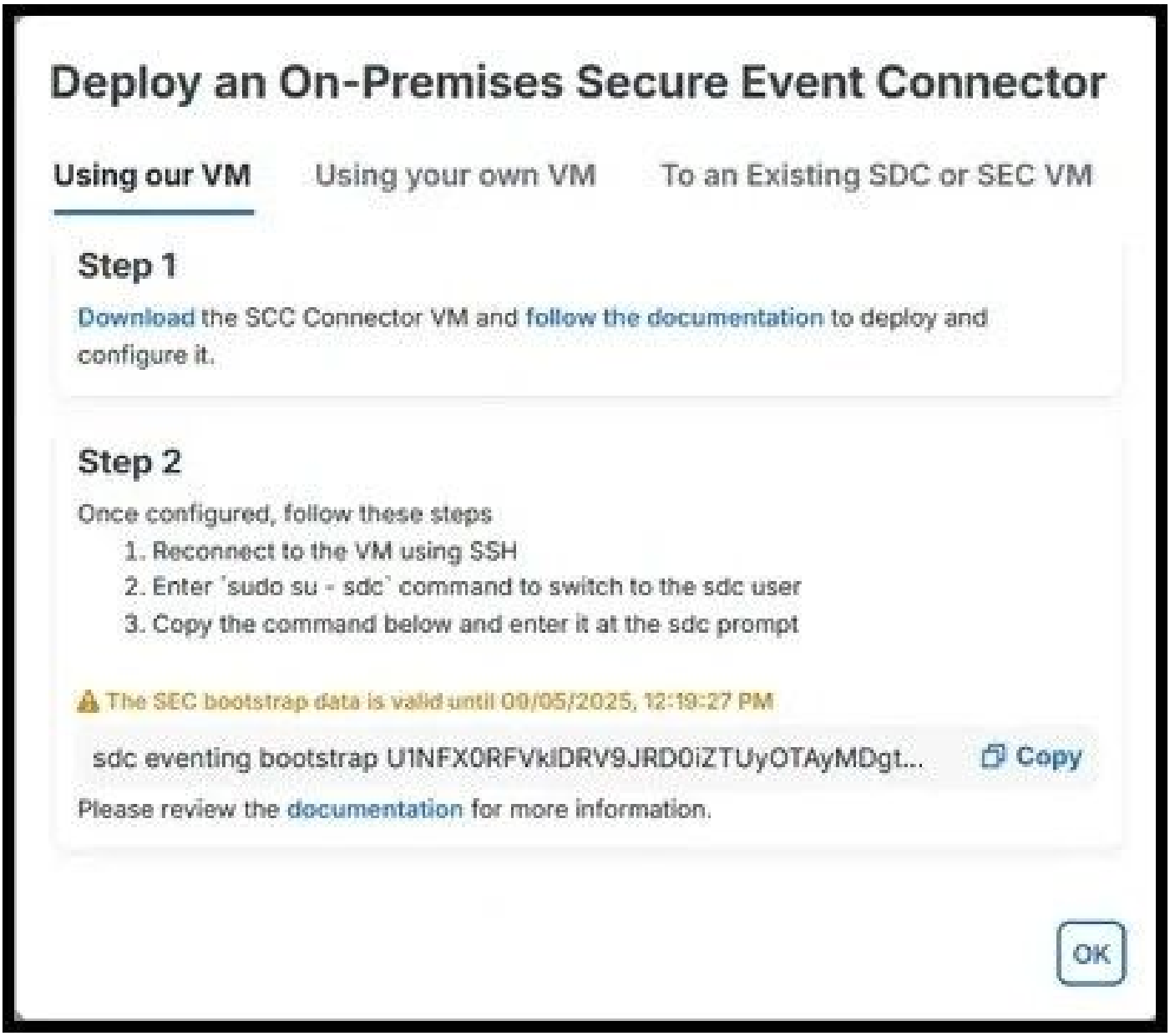
步骤2.从左侧菜单中选择Administration和Secure Connectors:



步骤3.在右上角，单击加号图标以加入新的连接器，然后选择Secure Event Connector:



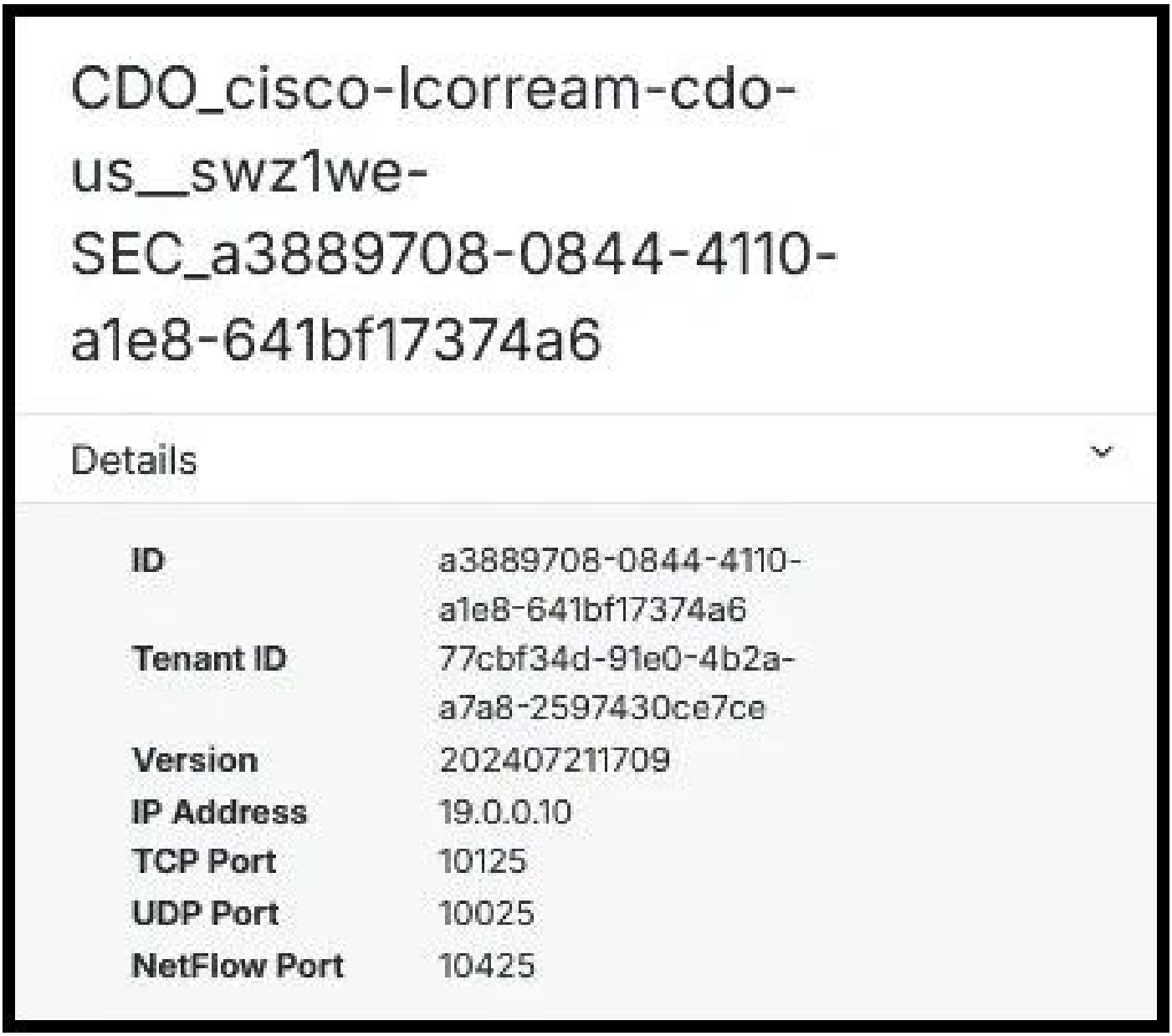
步骤4.根据在“使用我们的VM”、“使用您自己的VM”或“到现有的SDC或SEC VM”之间的所需选项，使用步骤安装和引导连接器：



步骤5.成功执行引导程序时，会出现类似消息：

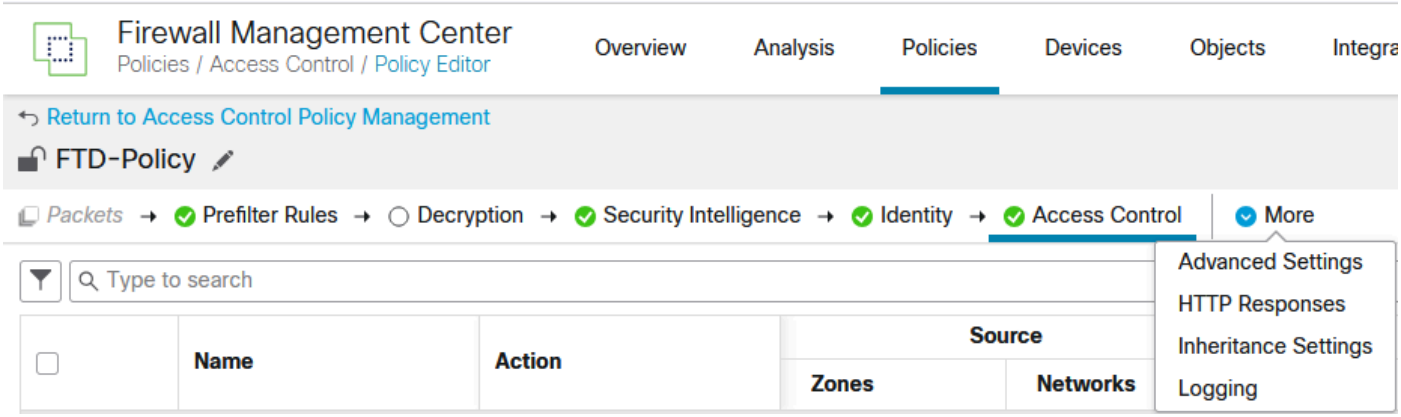
```
2025-06-09 05:41:56 [INFO] Bootstrap package processed successfully
2025-06-09 05:41:56 [INFO] Default AWS Region is us-west-2
2025-06-09 05:42:00 [INFO] Scanning for next available TCP port starting with 10125
2025-06-09 05:42:00 [INFO] TCP port found and set to 10125
2025-06-09 05:42:00 [INFO]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

步骤6.一旦部署了连接器并启动连接器，端口信息在SCC门户中可见：



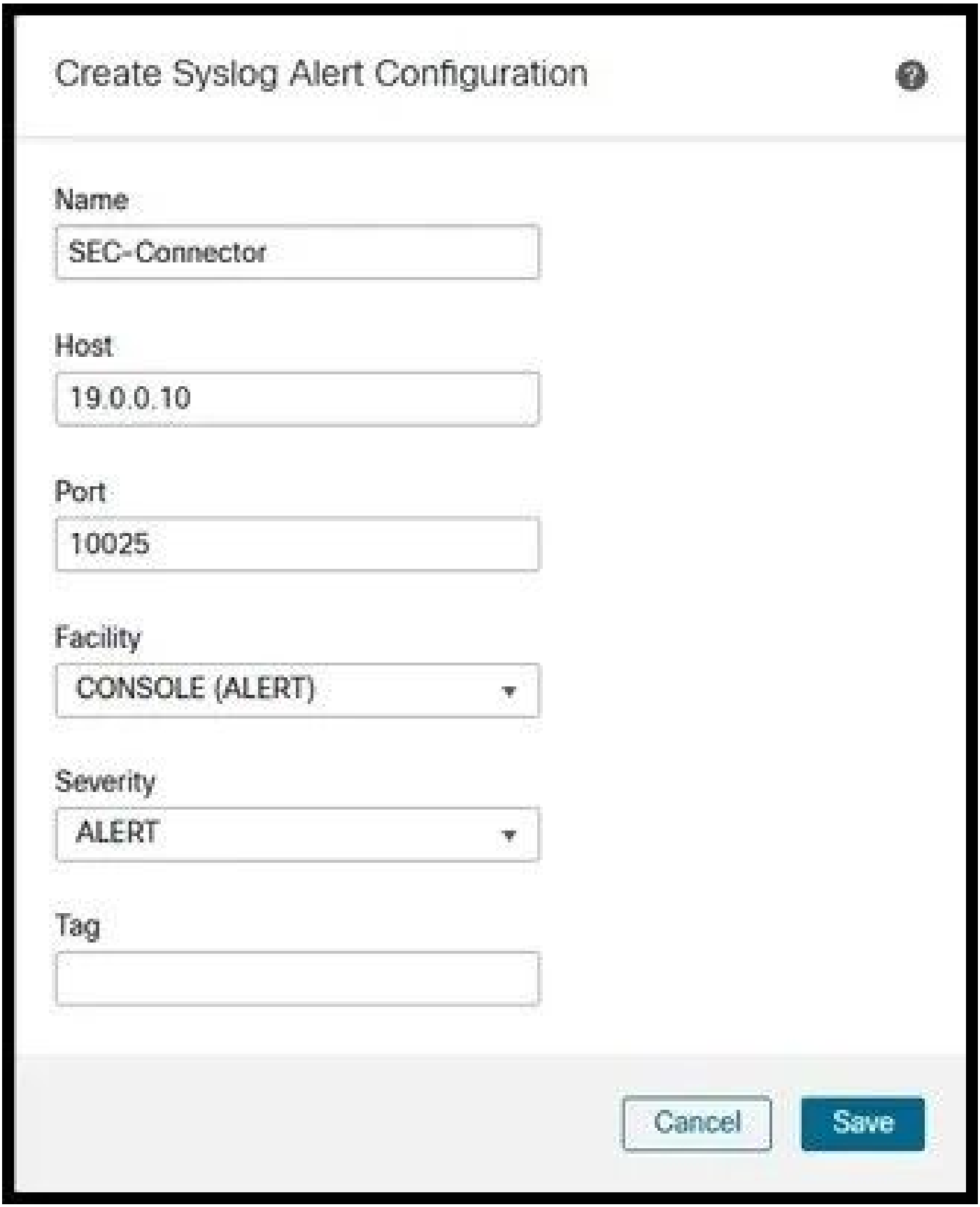
步骤7.在思科安全防火墙管理中心(FMC)上，依次导航到策略和访问控制。选择与要登录的设备对应的策略。

步骤8.依次选择More和Logging:

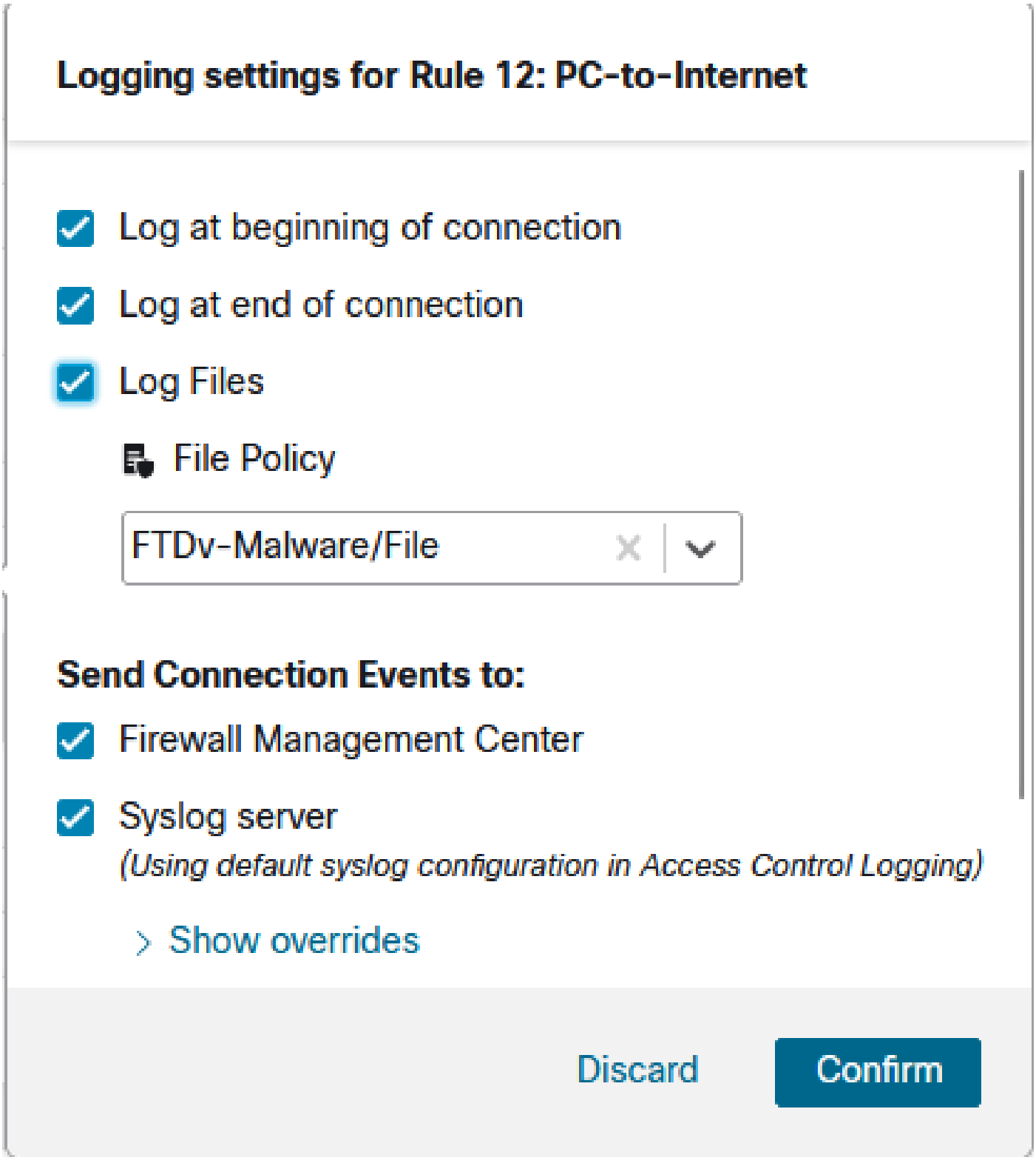


步骤9.启用Send using specific syslog alert选项并添加新的Syslog Alert。使用从SCC门户中的

SEC连接器获取的Internet协议(IP)地址和端口信息：



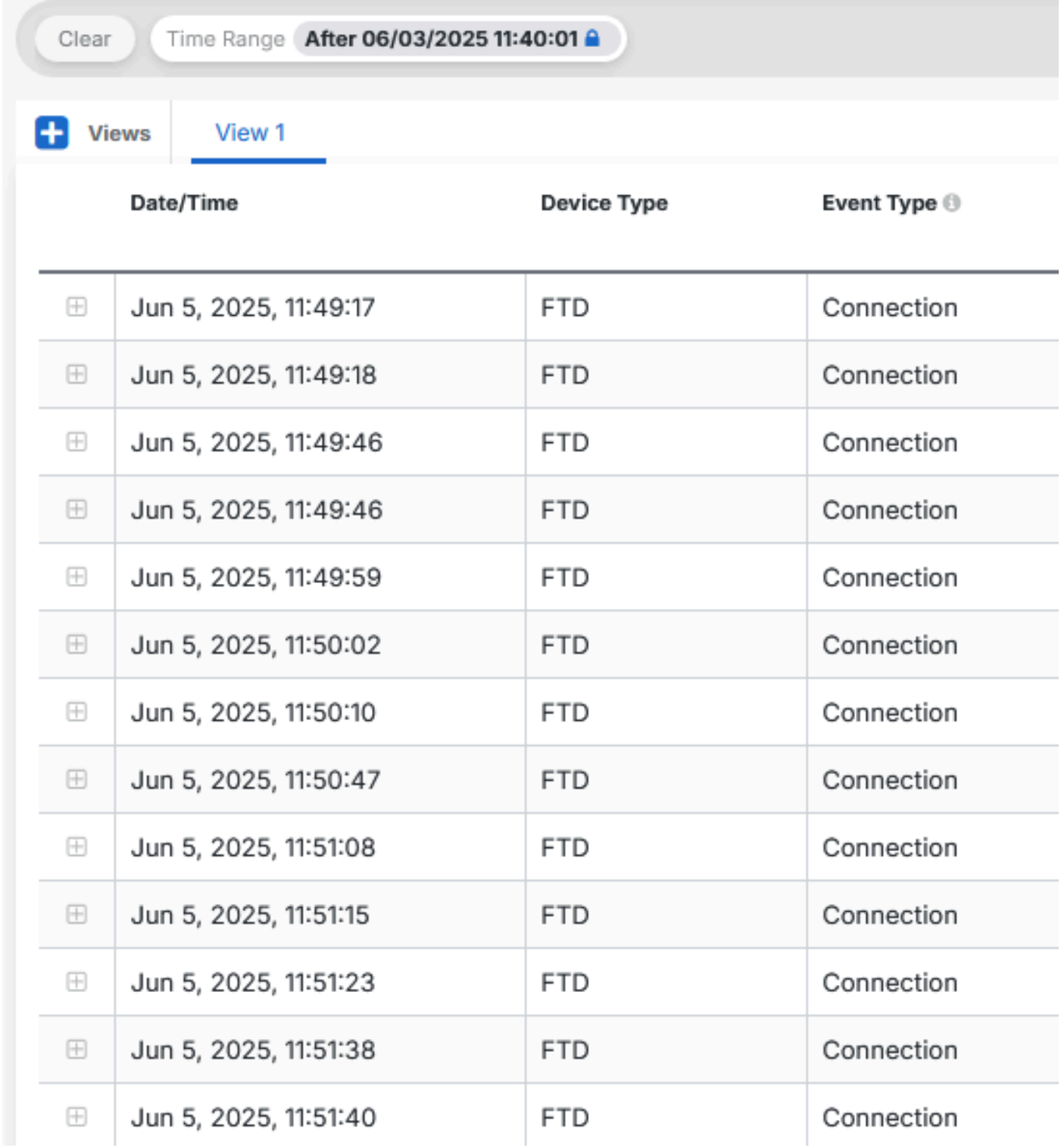
步骤10.返回访问控制策略，修改各个规则以将事件发送到系统日志服务器：



步骤11.部署对FTD所做的更改，以允许防火墙开始记录事件。

验证

要验证更改是否成功执行且事件日志记录是否发生，请导航到SCC门户中的事件与日志和事件记录，并确认事件是否可见：



故障排除

在FTD上，使用与导航到SEC的流量匹配的管理接口在设备上运行数据包捕获，以捕获系统日志流量：

```
> 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
```

从SEC虚拟机，确保虚拟机具有Internet连接。运行命令sdc troubleshooting，以生成可用于检查lar.log文件以进一步诊断的故障排除套件。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。