Configuración de la integración segura de eventos de FTD con control de seguridad en la nube mediante el conector de eventos seguro

Contenido

Introducción

Este documento describe cómo configurar Cisco Secure FTD para enviar eventos de seguridad a Security Cloud Control (SCC) mediante Secure Event Connector (SEC).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Secure Firewall Threat Defence (FTD)
- Interfaz de línea de comandos (CLI) de Linux

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

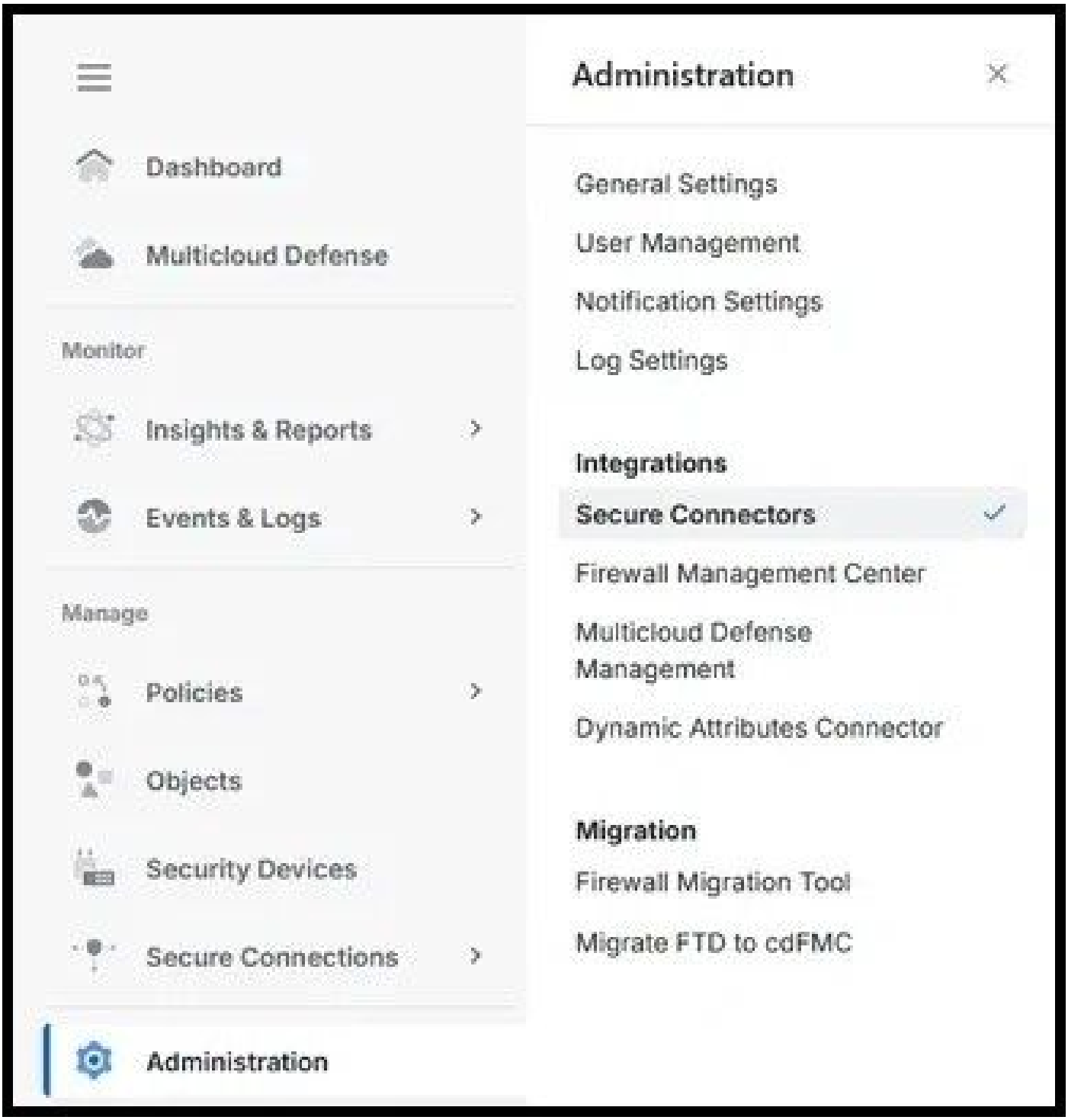
- Cisco Secure FTD 7.6
- Servidor Ubuntu versión 24.04

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

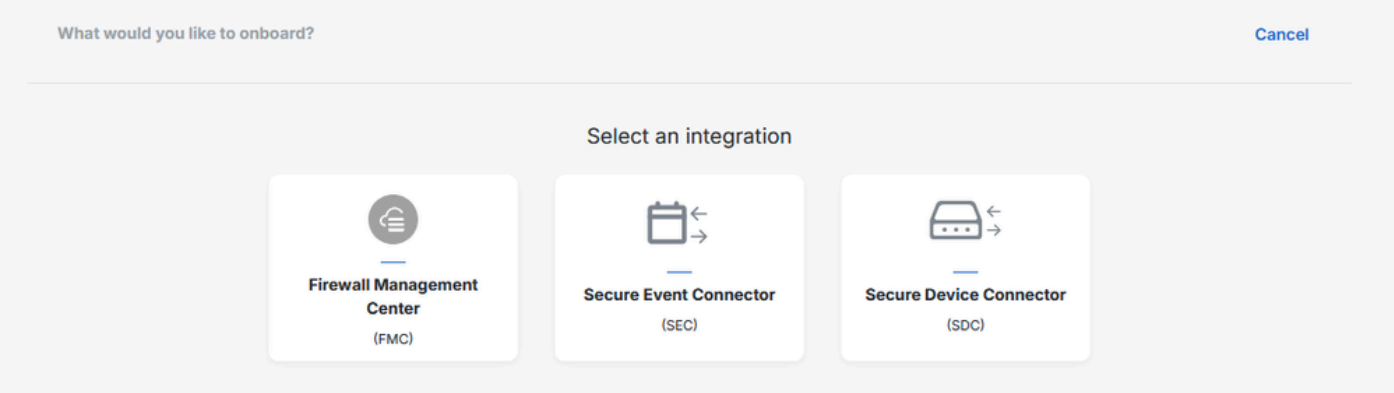
Configurar

Paso 1. Inicie sesión en el portal de nube de SCC:

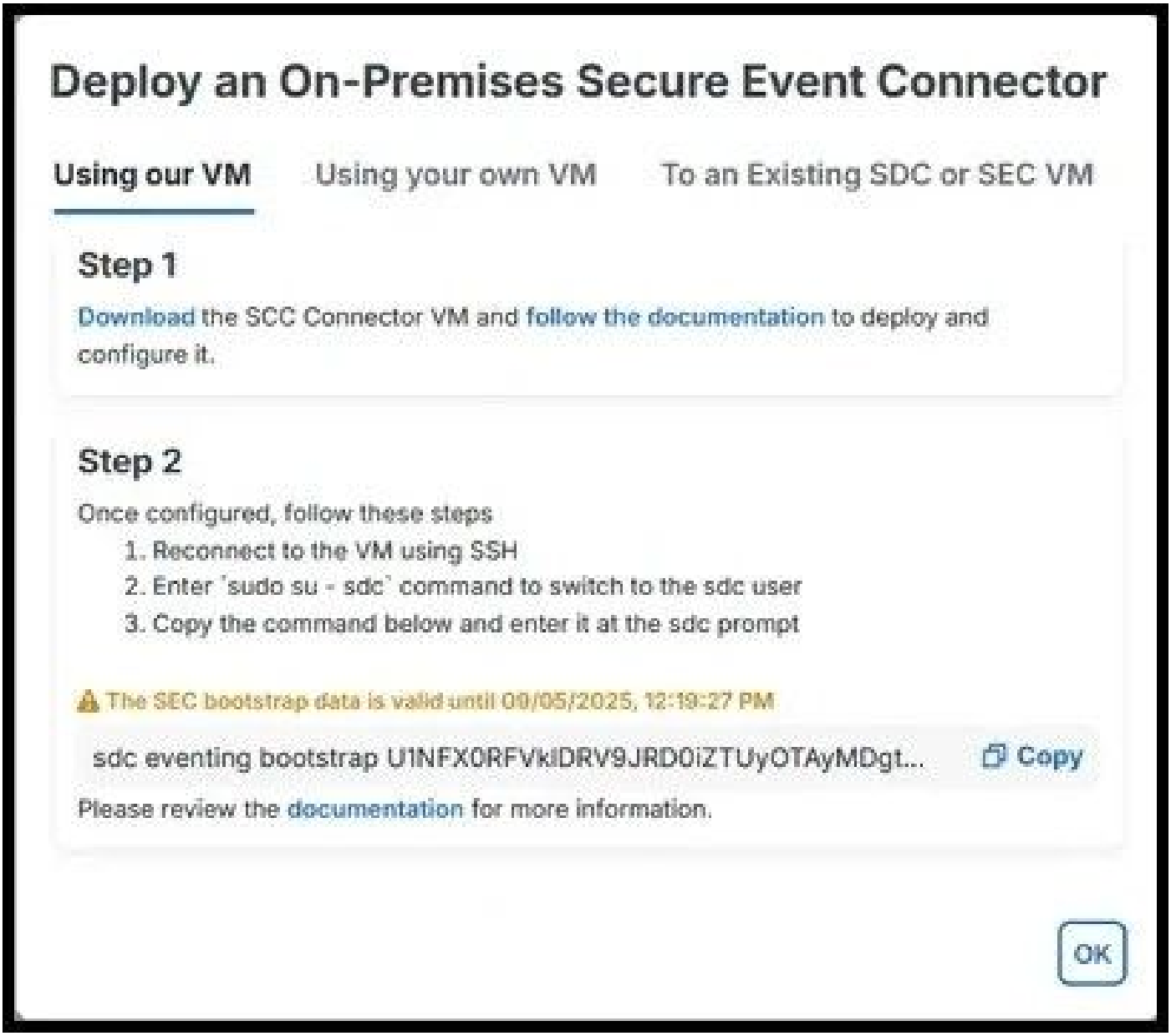
Paso 2. En el menú de la izquierda, elija Administration y Secure Connectors:



Paso 3. En el lado superior derecho, haga clic en el icono más para incorporar un nuevo conector y elegir Secure Event Connector:



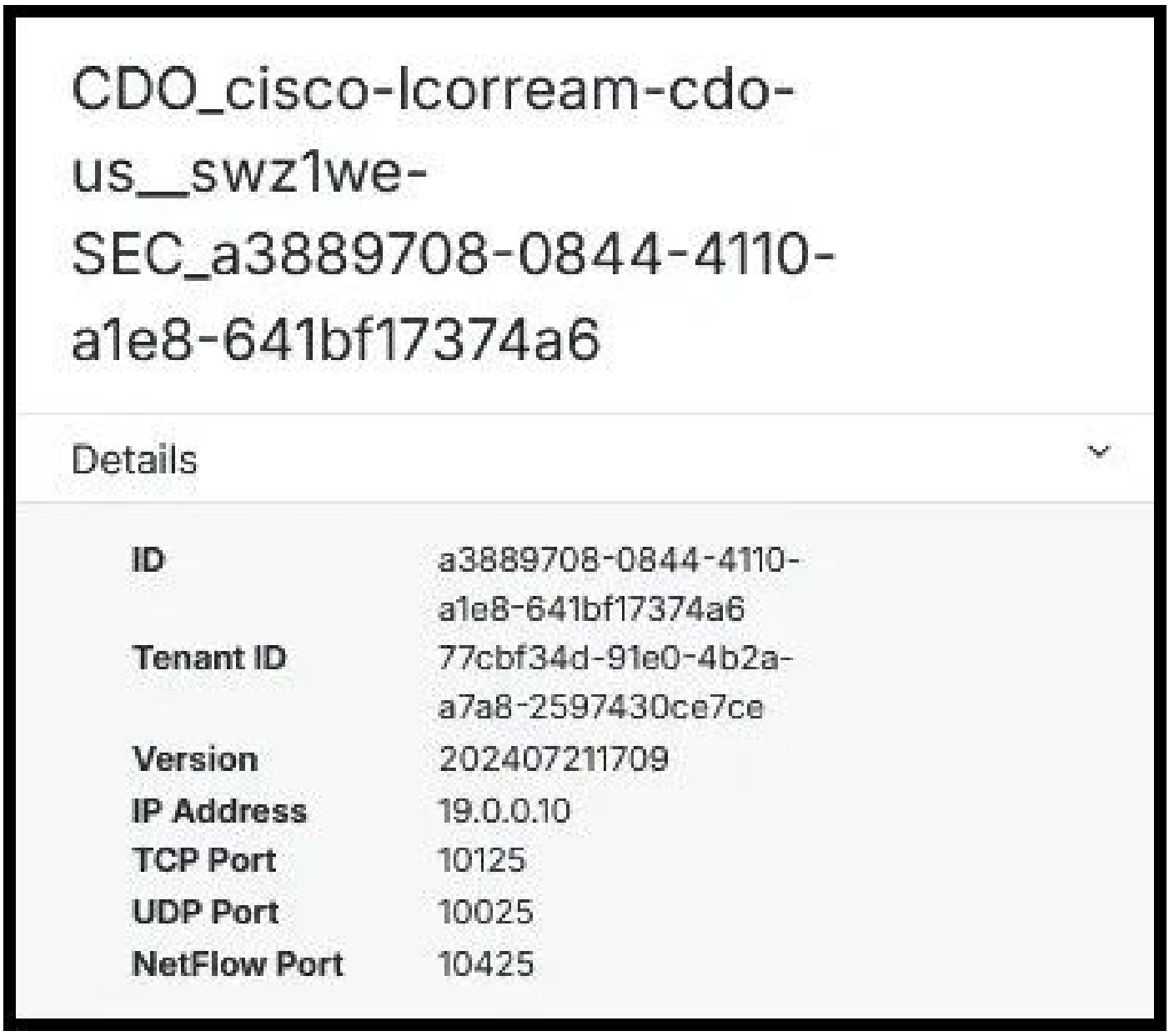
Paso 4. Use los pasos para instalar y arrancar el conector según la opción deseada entre 'Uso de la VM', 'Uso de su propia VM' o 'A una SDC o SEC VM existente':



Paso 5. Un mensaje similar se ve cuando el bootstrap se realiza con éxito:

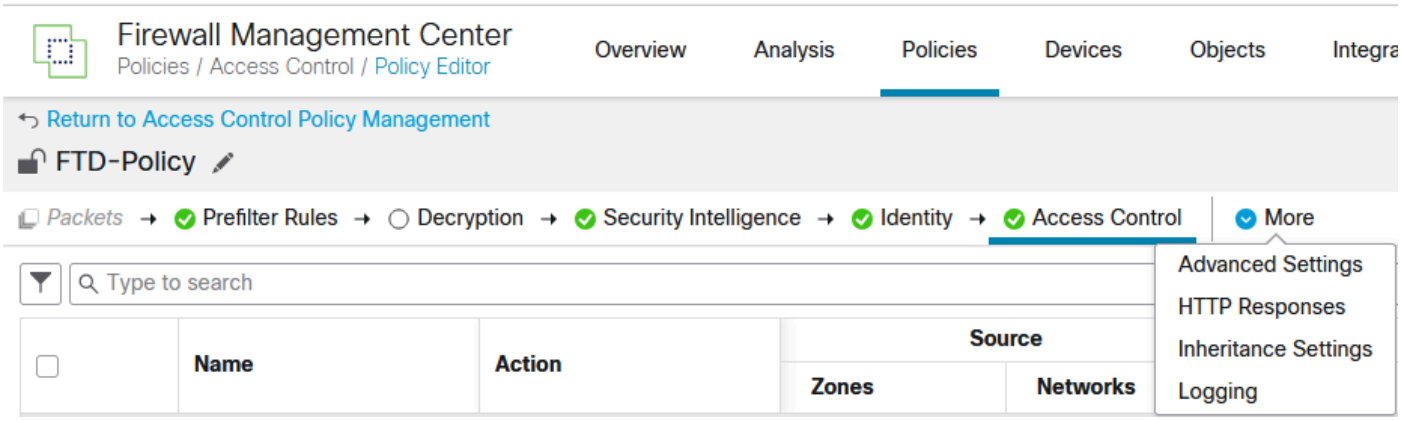
```
2025-06-09 05:41:56 [INFO] Bootstrap package processed successfully
2025-06-09 05:41:56 [INFO] Default AWS Region is us-west-2
2025-06-09 05:42:00 [INFO] Scanning for next available TCP port starting with 10125
2025-06-09 05:42:00 [INFO] TCP port found and set to 10125
2025-06-09 05:42:00 [INFO]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

Paso 6. Una vez que se implementa y se inicia el conector, la información del puerto es visible en el portal SCC:

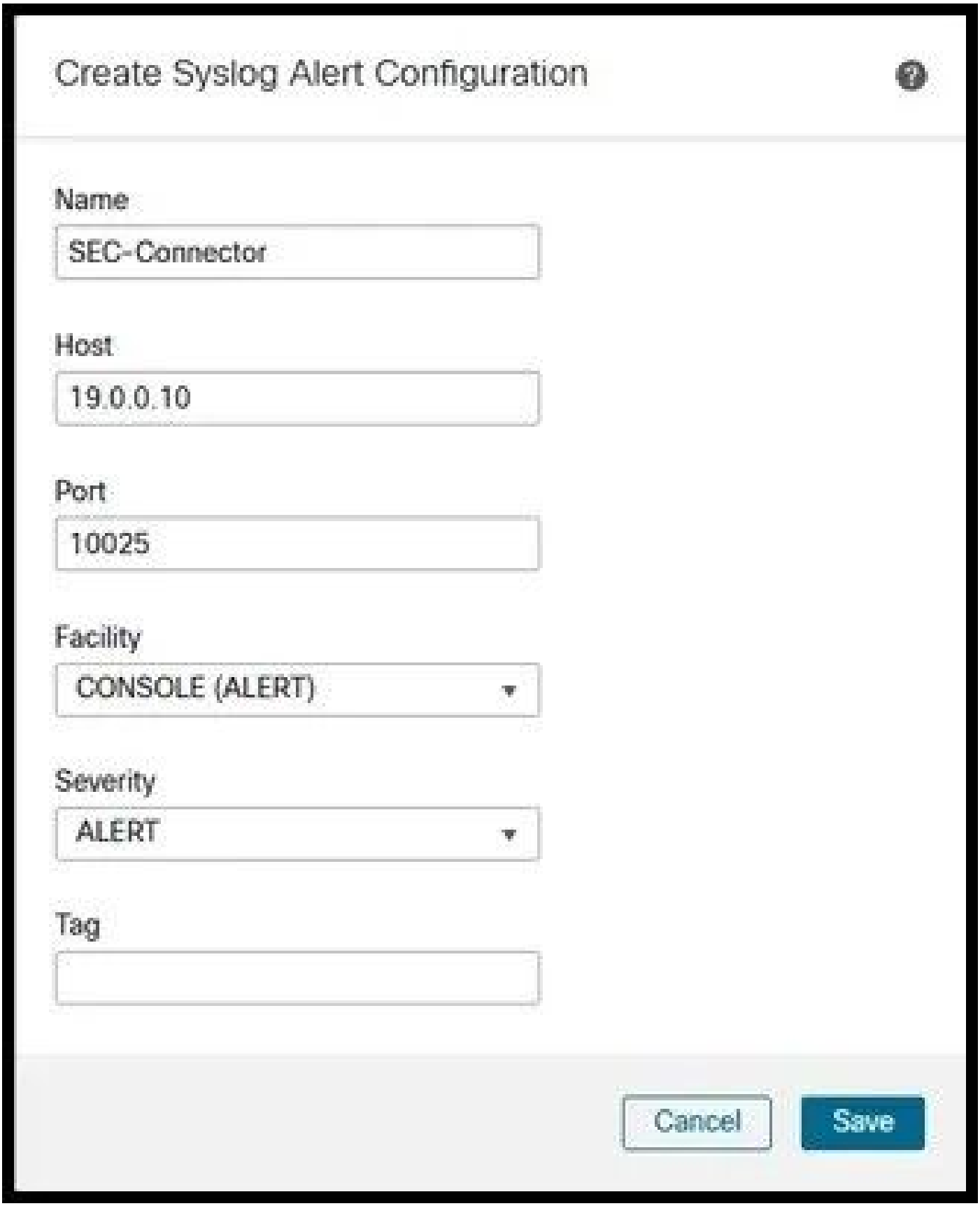


Paso 7. En Cisco Secure Firewall Management Center (FMC), vaya a Políticas y, a continuación, a Control de acceso. Elija la política correspondiente a los dispositivos que se van a incorporar.

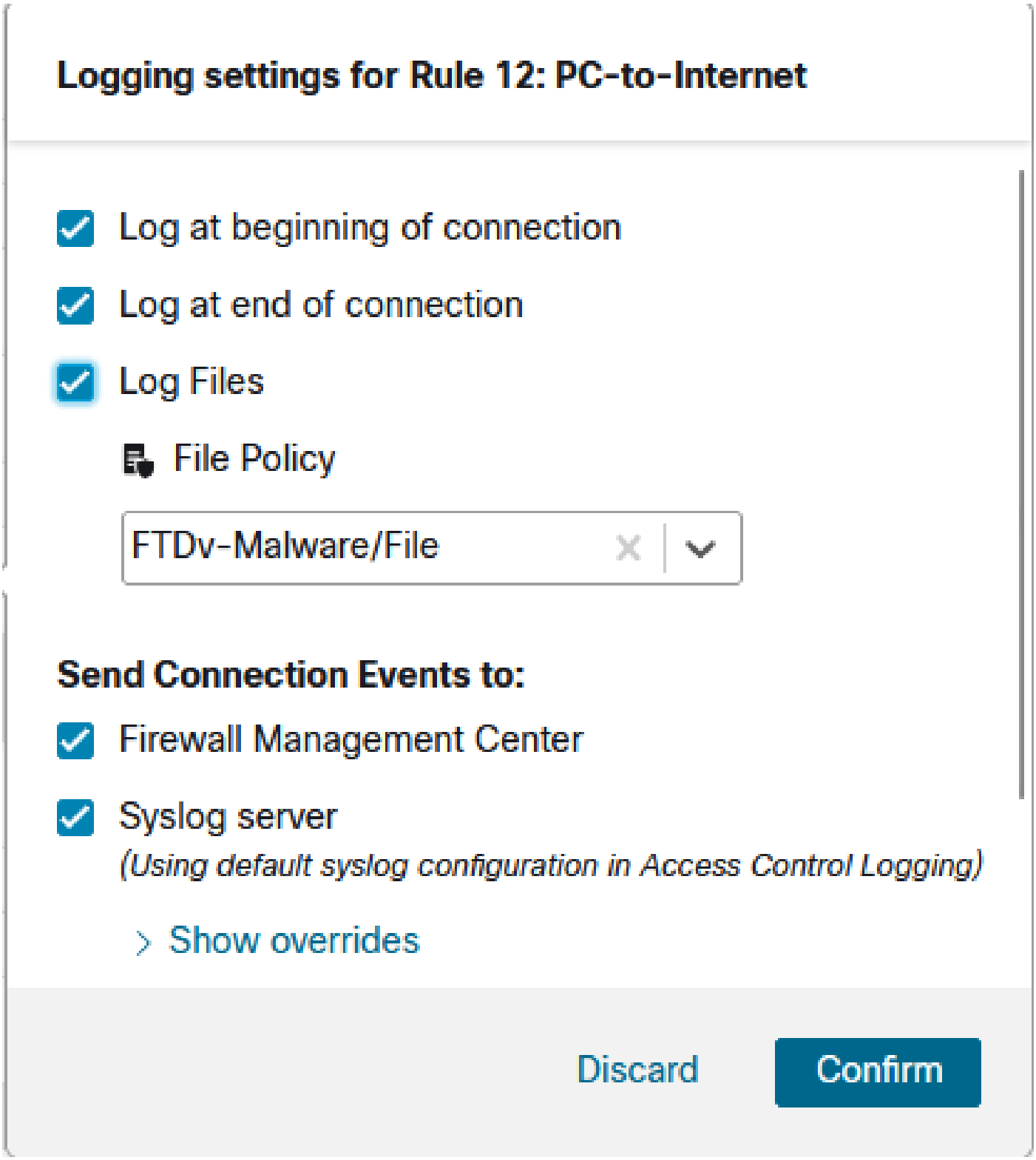
Paso 8. Elija Más y luego Registro:



Paso 9. Habilite la opción de alerta Send using specific syslog y agregue una nueva alerta Syslog. Utilice la información de puerto y dirección del protocolo de Internet (IP) obtenida del conector SEC en el portal SCC:



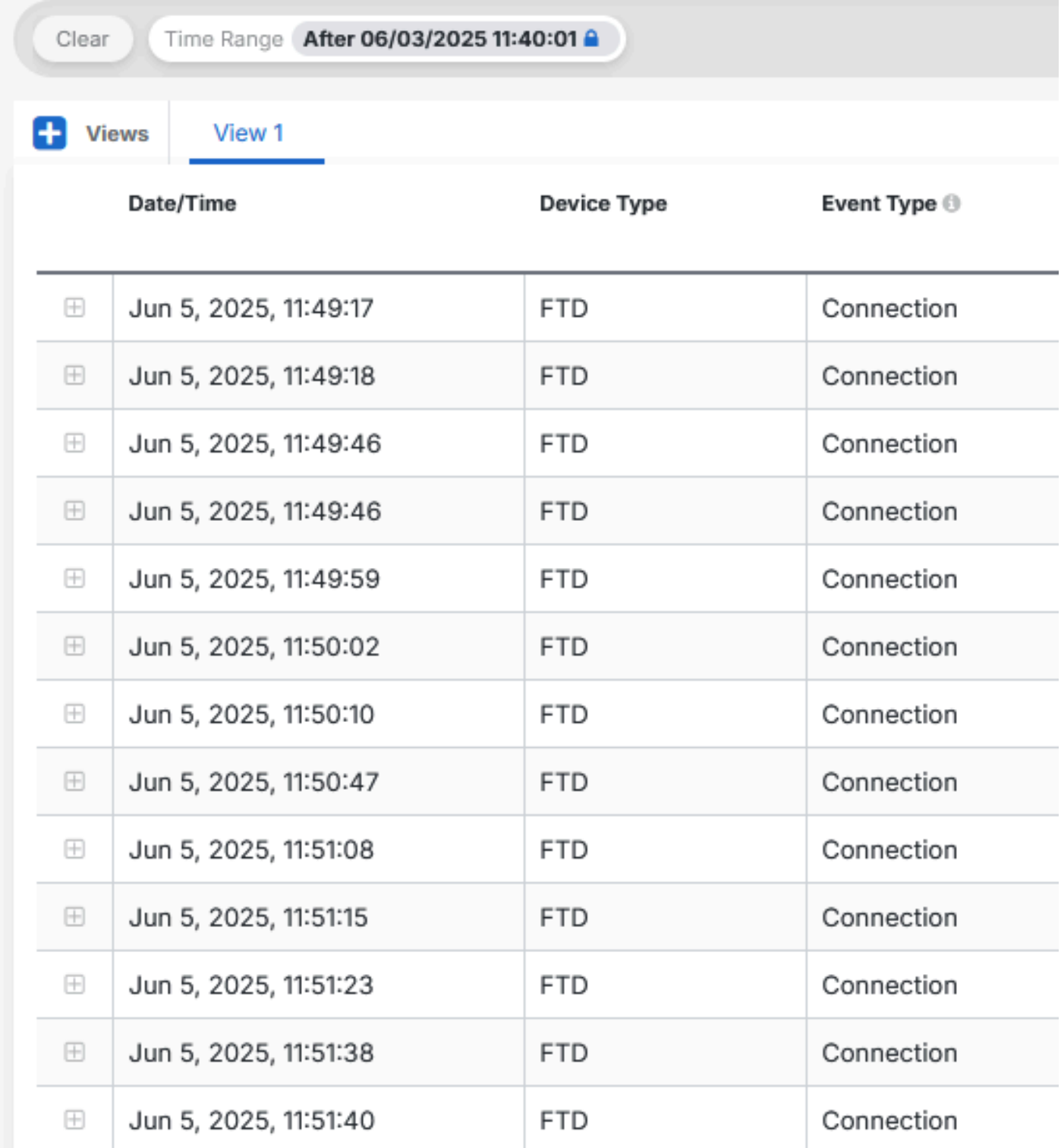
Paso 10. Vuelva a la política de control de acceso, modifique las reglas individuales para enviar los eventos al servidor Syslog:



Paso 11. Implemente los cambios realizados en el FTD para permitir que el firewall comience a registrar los eventos.

Verificación

Para verificar que los cambios se ejecutaron correctamente y que el registro de eventos se está llevando a cabo, navegue hasta Eventos y registros y Registro de eventos en el portal de SCC y confirme que los eventos son visibles:



Troubleshoot

En FTD, ejecute una captura de paquetes en el dispositivo usando la interfaz de administración que coincida con el tráfico que navega a SEC para capturar el tráfico de 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
```

Desde la máquina virtual SEC, asegúrese de que la máquina virtual tenga conectividad a Internet. Ejecute el comando sdc troubleshoot, para generar un paquete de troubleshooting que se puede utilizar para verificar el archivo lar.log para obtener un diagnóstico adicional.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).