

Configurar Integração de Evento de FTD Seguro com Controle de Nuvem de Segurança via Conector de Evento Seguro

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Verificar](#)

[Troubleshooting](#)

Introdução

Este documento descreve como configurar o Cisco Secure FTD para enviar eventos de segurança ao Security Cloud Control (SCC) usando o Secure Event Connector (SEC).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Defesa contra ameaças (FTD) do Cisco Secure Firewall
- Interface de linha de comando (CLI) do Linux

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Secure FTD 7.6
- Ubuntu Server versão 24.04

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Etapa 1. Fazer login no portal de nuvem do SCC:



The screenshot shows the Cisco Security Cloud Sign On login page. At the top, the Cisco logo is displayed. Below it, the text "CONNECTING TO SECURITY CLOUD CONTROL (US)" is shown. The main heading is "Security Cloud Sign On". There is a label "Email" next to a text input field. Below the input field is a blue button labeled "Continue".

CISCO

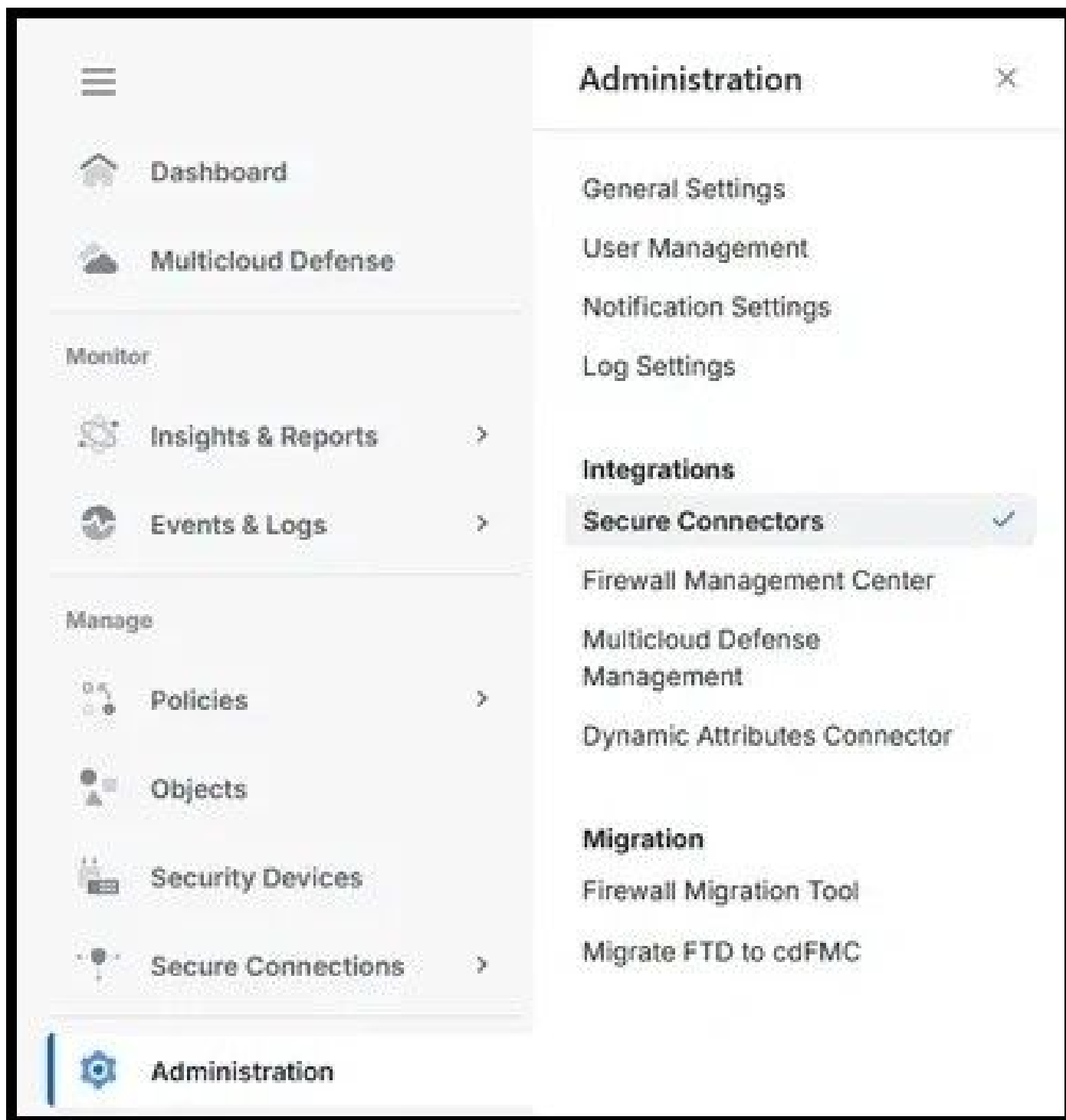
CONNECTING TO SECURITY CLOUD CONTROL (US)

Security Cloud Sign On

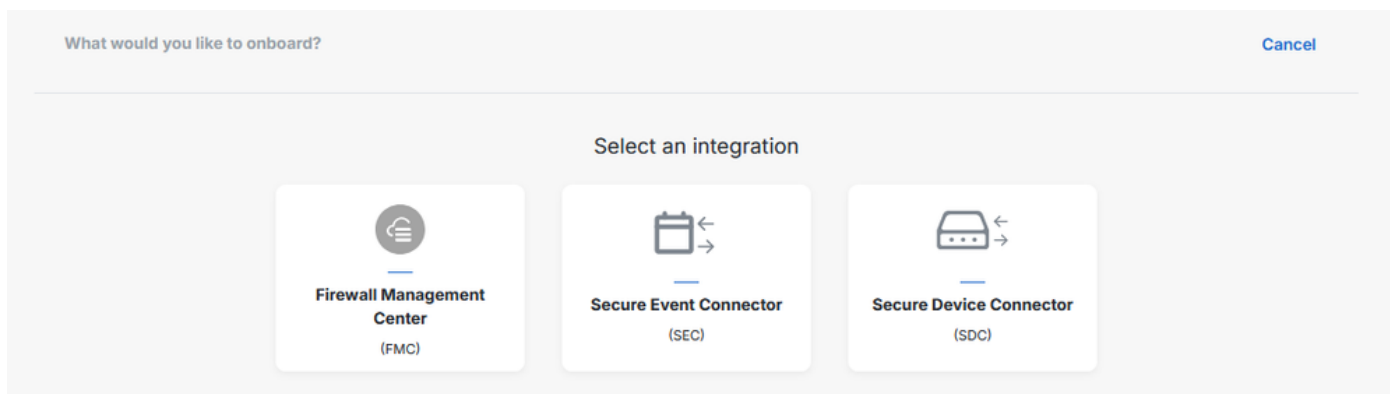
Email

Continue

Etapa 2. No menu do lado esquerdo, escolha Administration e Secure Connectors:



Etapa 3. No lado superior direito, clique no ícone plus para integrar um novo conector e escolha Secure Event Connector:



Etapa 4. Use as etapas para instalar e inicializar o conector, dependendo da opção desejada entre 'Usando nossa VM', 'Usando sua própria VM' ou 'Para um SDC ou VM SEC existente':

Deploy an On-Premises Secure Event Connector

Using our VM Using your own VM To an Existing SDC or SEC VM

Step 1

Download the SCC Connector VM and [follow the documentation](#) to deploy and configure it.

Step 2

Once configured, follow these steps

1. Reconnect to the VM using SSH
2. Enter 'sudo su - sdc' command to switch to the sdc user
3. Copy the command below and enter it at the sdc prompt

 The SEC bootstrap data is valid until 00/05/2025, 12:19:27 PM

```
sdc eventing bootstrap U1NFX0RFVkiDRV9JRD0iZTUyOTAyMDgt...
```

 Copy

Please review the [documentation](#) for more information.

OK

Etapa 5. Uma mensagem semelhante é vista quando o bootstrap é executado com êxito:

```
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/

5a99d0351c1ae91cd790dcf18ee1d0594d37fcfaf5a1725473eed042342a567
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
sdcc@lcorream-sdc:~$
```

Etapa 6. Depois que o conector for implantado e inicializado, as informações da porta estarão visíveis no portal SCC:

CDO_cisco-lcorream-cdo-us_swz1we-SEC_a3889708-0844-4110-a1e8-641bf17374a6

Details

ID	a3889708-0844-4110-a1e8-641bf17374a6
Tenant ID	77cbf34d-91e0-4b2a-a7a8-2597430ce7ce
Version	202407211709
IP Address	19.0.0.10
TCP Port	10125
UDP Port	10025
NetFlow Port	10425

Etapa 7. No Cisco Secure Firewall Management Center (FMC), navegue para Policies e, em seguida, para Access Control. Escolha a política correspondente aos dispositivos que estão

sendo integrados.

Etapa 8. Escolha Mais e, em seguida, Log:



Firewall Management Center
Policies / Access Control / Policy Editor

Overview

Analysis

Policies

Devices

Objects

Integra

[Return to Access Control Policy Management](#)

FTD-Policy 

 Packets

 →

 Prefilter Rules

 →

 Decryption

 →

 Security Intelligence

 →

 Identity

 →

 Access Control

 |

 More



☐

Name

Action

Source

Zones

Networks

Advanced Settings

HTTP Responses

Inheritance Settings

Logging

Etapa 9. Ative a opção Send using specific syslog alert e adicione um novo Syslog Alert. Use as informações de endereço e porta do Internet Protocol (IP) obtidas do conector SEC no portal SCC:

Create Syslog Alert Configuration



Name

SEC-Connector

Host

19.0.0.10

Port

10025

Facility

CONSOLE (ALERT)



Severity

ALERT



Tag

Cancel

Save

Etapa 10. De volta à Política de controle de acesso, modifique as regras individuais para enviar os eventos ao servidor Syslog:

Logging settings for Rule 12: PC-to-Internet

☒ Log at beginning of connection

☒ Log at end of connection

☒ Log Files

 File Policy

FTDv-Malware/File



Send Connection Events to:

☒ Firewall Management Center

☒ Syslog server

(Using default syslog configuration in Access Control Logging)

[> Show overrides](#)

Discard

Confirm

Etapa 11. Implante as alterações feitas no FTD para permitir que o firewall comece a registrar os eventos.

Verificar

Para verificar se as alterações foram executadas com êxito e se o registro de eventos está ocorrendo, navegue para Eventos e registros e Registro de eventos no portal do SCC e confirme se os eventos estão visíveis:

Clear Time Range After 06/03/2025 11:40:01			
+ Views View 1			
	Date/Time	Device Type	Event Type ⓘ
⊕	Jun 5, 2025, 11:49:17	FTD	Connection
⊕	Jun 5, 2025, 11:49:18	FTD	Connection
⊕	Jun 5, 2025, 11:49:46	FTD	Connection
⊕	Jun 5, 2025, 11:49:46	FTD	Connection
⊕	Jun 5, 2025, 11:49:59	FTD	Connection
⊕	Jun 5, 2025, 11:50:02	FTD	Connection
⊕	Jun 5, 2025, 11:50:10	FTD	Connection
⊕	Jun 5, 2025, 11:50:47	FTD	Connection
⊕	Jun 5, 2025, 11:51:08	FTD	Connection
⊕	Jun 5, 2025, 11:51:15	FTD	Connection
⊕	Jun 5, 2025, 11:51:23	FTD	Connection
⊕	Jun 5, 2025, 11:51:38	FTD	Connection
⊕	Jun 5, 2025, 11:51:40	FTD	Connection

Troubleshooting

No FTD, execute uma captura de pacote no dispositivo usando a interface de gerenciamento que corresponde ao tráfego que navega para o SEC para capturar o tráfego 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 reduce the amount of traffic captured.
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 reduce the amount of traffic captured.
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

Na máquina virtual SEC, verifique se a máquina virtual tem conectividade com a Internet. Execute o comando `sdc troubleshoot`, para gerar um pacote de solução de problemas que pode ser usado para verificar o arquivo `lar.log` para diagnóstico adicional.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.