

Beveiligde FTD-gebeurtenisintegratie configureren met Cloud Security Control via Secure Event Connector

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

In dit document wordt beschreven hoe u de Cisco Secure FTD configureert voor het verzenden van beveiligingsgebeurtenissen naar de Security Cloud Control (SCC) met behulp van de Secure Event Connector (SEC).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Secure Firewall Threat Defense (FTD)
- Linux Command Line Interface (CLI)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Secure FTD 7.6
- Ubuntu Server versie 10 .04

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

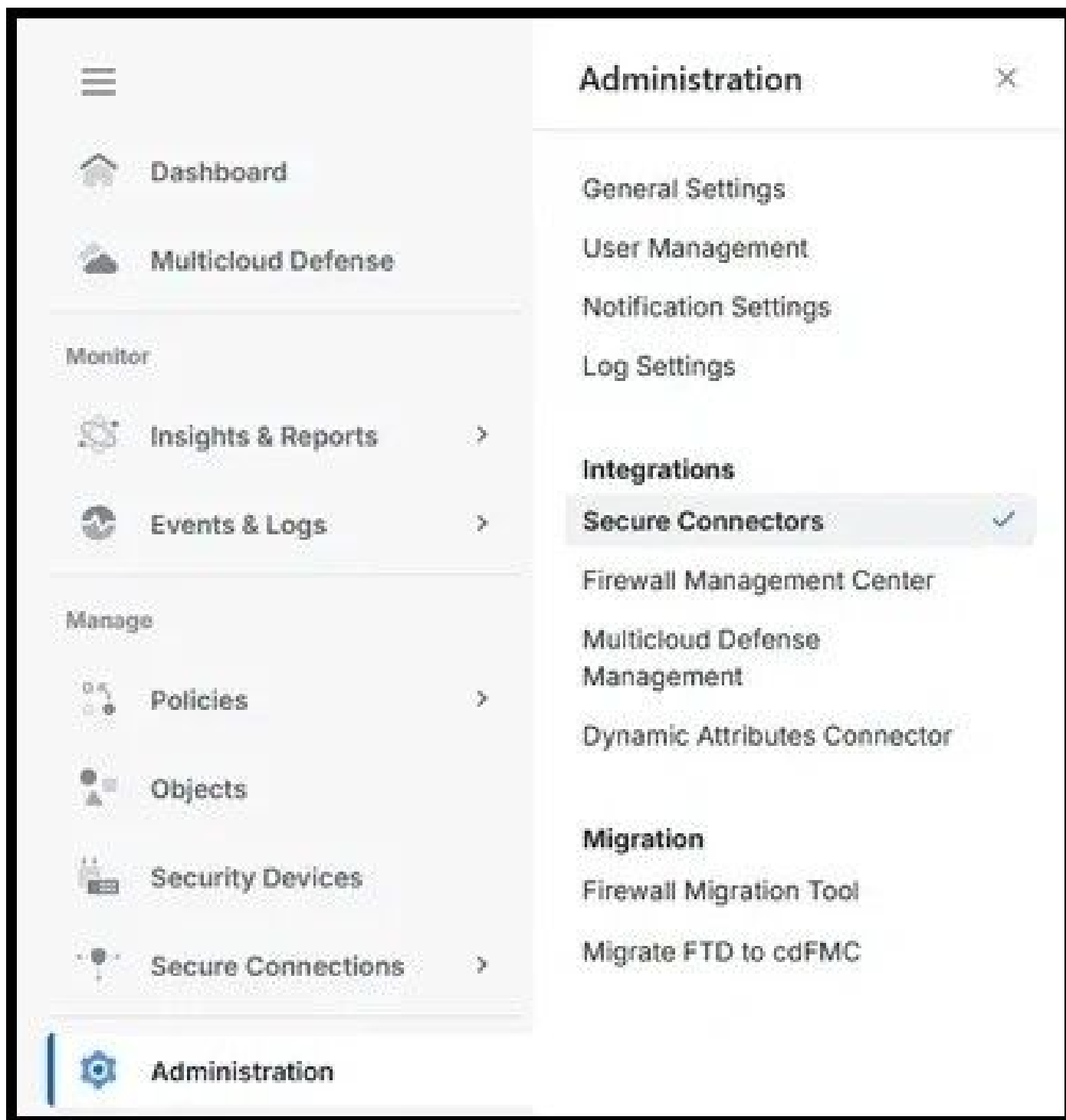
Configureren

Stap 1. Meld u aan bij het SCC cloud portal:

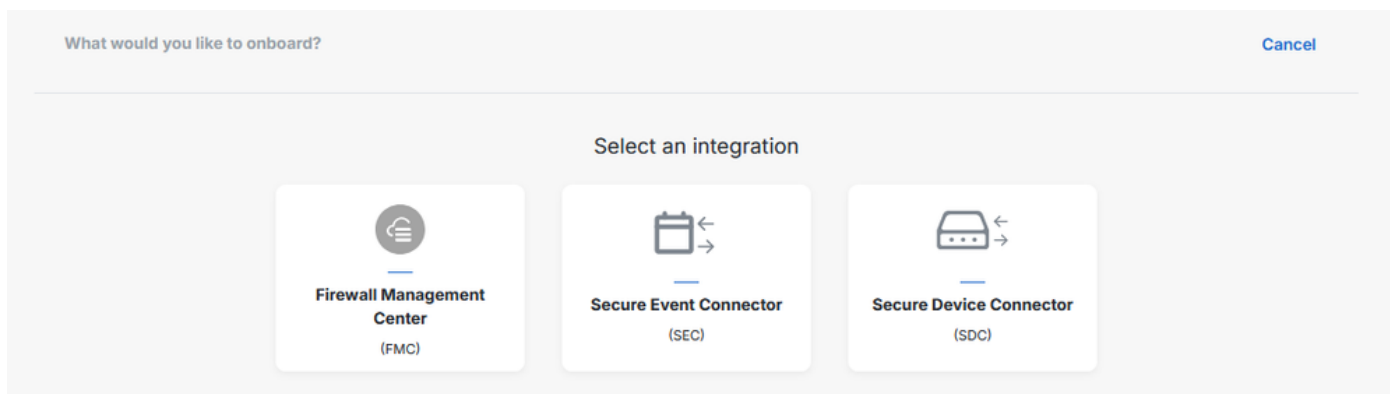


The screenshot shows the Cisco Security Cloud Sign On portal. At the top is the Cisco logo. Below it, the text "CONNECTING TO SECURITY CLOUD CONTROL (US)" is displayed. The main heading is "Security Cloud Sign On". Underneath, there is a label "Email" followed by a text input field. At the bottom of the form is a blue button labeled "Continue".

Stap 2. Kies in het menu aan de linkerkant de optie Beheer en Beveiligde connectors:



Stap 3. Klik rechtsboven op het plus-pictogram om een nieuwe connector aan boord te nemen en kies Secure Event Connector:



Stap 4. Gebruik de stappen om de connector te installeren en op te starten, afhankelijk van de gewenste optie tussen 'Onze VM gebruiken', 'Uw eigen VM gebruiken' of 'Naar een bestaande SDC- of SEC-VM':

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 09/05/2025, 12:19:27 PM

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

 Copy

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



Stap 5. Een soortgelijk bericht wordt weergegeven wanneer de bootstrap succesvol wordt uitgevoerd:

```
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
sdcl@lcorream-sdc:~$
```

Stap 6. Zodra de connector is geïmplementeerd en opgestart, is de poortinformatie zichtbaar in het SCC-portaal:

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

Stap 7. Navigeer in het Cisco Secure Firewall Management Center (FMC) naar Beleid en vervolgens naar Toegangsbeheer. Kies het beleid dat overeenkomt met de apparaten die aan

boord zijn.

Stap 8. Kies Meer en vervolgens Logboekregistratie:

 **Firewall Management Center**
Policies / Access Control / Policy Editor

OverviewAnalysisPoliciesDevicesObjectsIntegrations

[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

Stap 9. Schakel de optie Verzenden met specifieke syslog-waarschuwing in en voeg een nieuwe syslog-waarschuwing toe. Gebruik het IP-adres (Internet Protocol) en de poortinformatie die u hebt verkregen via de SEC-connector in het SCC-portaal:

Create Syslog Alert Configuration



Name

SEC-Connector

Host

19.0.0.10

Port

10025

Facility

CONSOLE (ALERT)



Severity

ALERT



Tag

Cancel

Save

Stap 10. Terug in het toegangsbeleid wijzigt u de afzonderlijke regels om de gebeurtenissen naar de Syslog-server te verzenden:

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

Stap 11. Implementeer de wijzigingen die in de FTD zijn aangebracht om de firewall in staat te stellen de gebeurtenissen te registreren.

Verifiëren

Om te controleren of de wijzigingen met succes zijn uitgevoerd en of de gebeurtenisregistratie plaatsvindt, gaat u naar Events & Logs en Event Logging in het SCC-portaal en bevestigt u dat de gebeurtenissen zichtbaar zijn:

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

Problemen oplossen

Voer op FTD een pakketopname uit op het apparaat met behulp van de beheerinterface die overeenkomt met het verkeer dat naar de SEC navigeert om het syslog-verkeer vast te leggen:

```
> 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 data 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 data 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

Zorg ervoor dat de virtuele machine vanaf de SEC een internetverbinding heeft. Voer de opdracht `sdc troubleshoot` uit, om een bundel voor probleemoplossing te genereren die kan worden gebruikt om het `lar.log`-bestand te controleren voor verdere diagnose.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.