

Cisco XDR integreren en problemen oplossen met Firepower Threat Defence (FTD)

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Licentie](#)

[Koppel uw accounts aan SSE en registreer de apparaten.](#)

[Registreer de apparaten in SSE](#)

Inleiding

Dit document beschrijft de stappen die nodig zijn om Cisco XDR te integreren, te verifiëren en problemen op te lossen met Firepower Threat Defence (FTD).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)
- Optionele virtualisatie van afbeeldingen

Gebruikte componenten

- Firepower Threat Defence (FTD) - 6.5
- Firepower Management Center (FMC) - 6.5
- Security Services exchange (SSE)
- Cisco XDR router
- Smart License Portal

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.

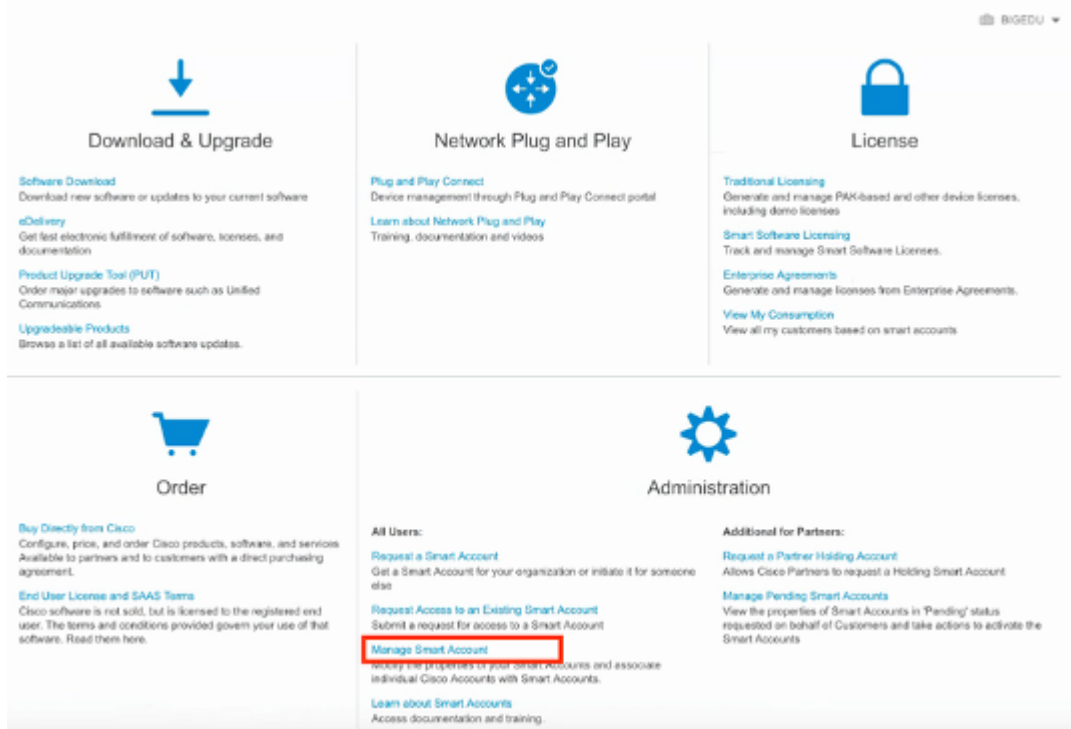
Configureren

Licentie

Virtuele accountrollen:

Alleen de Virtual Account Admin of de Smart Account Admin heeft het voorrecht om de smart account te koppelen aan de SSE-account.

Stap 1. Om de slimme accountrol te valideren, navigeer naar **software.cisco.com** en selecteer in het **menu Beheer** de optie **Slimme account beheren**.



Stap 2. Om de gebruikersrol te valideren, navigeer naar **Gebruikers** en valideer dat onder Rollen de accounts zijn ingesteld op Virtuele accountbeheerder, zoals in het beeld wordt getoond.

Cisco Software Central > Manage Smart Account > Users

Account Properties | Virtual Accounts | **Users** | Custom Tags | Requests | Account Agreements | Event Log

Users

Users		User Groups				
<input type="checkbox"/>	User ↑	Email	Organization	Account Access	Role	User
<input type="checkbox"/>	danieber					
<input type="checkbox"/>	Daniel Benitez danieben	danieben@cisco.com	Cisco Systems, Inc.	All Virtual Accounts Mex-AMP TAC	Smart Account Administrator Virtual Account Administrator	- -

Stap 3. Zorg ervoor dat de virtuele account die is geselecteerd om op SSE te koppelen, de licentie voor de beveiligingsapparaten bevat als een account dat de beveiligingslicentie niet bevat, is gekoppeld aan SSE, de beveiligingsapparaten en de gebeurtenis niet op het SSE-portal wordt weergegeven.

Smart Software Licensing

[Feedback](#) [Support](#) [Help](#)[Alerts](#) | [Inventory](#) | [Convert to Smart Licensing](#) | [Reports](#) | [Preferences](#) | [On-Prem Accounts](#) | [Activity](#)Virtual Account: **Mex-AMP TAC** ▼13 Minor | [Hide Alerts](#)

General

Licenses

Product Instances

Event Log

Available Actions ▼

Manage License Tags

License Reservation...



Search by License

By Name

By Tag



<input type="checkbox"/> License	Billing	Purchased	In Use	Balance	Alerts	Actions
<input type="checkbox"/> FPR1010 URL Filtering	Prepaid	10	0	+ 10		Actions ▼
<input type="checkbox"/> FPR4110 Threat Defense Malware Protection	Prepaid	1	0	+ 1		Actions ▼
<input type="checkbox"/> FPR4110 Threat Defense Threat Protection	Prepaid	1	0	+ 1		Actions ▼
<input type="checkbox"/> FPR4110 Threat Defense URL Filtering	Prepaid	1	0	+ 1		Actions ▼
<input type="checkbox"/> HyperFlex Data Platform Enterprise Edition Subscription	Prepaid	2	0	+ 2		Actions ▼
<input type="checkbox"/> ISE Apex Session Licenses	Prepaid	1	0	+ 1		Actions ▼
<input type="checkbox"/> ISE Base Session Licenses	Prepaid	10	0	+ 10		Actions ▼
<input type="checkbox"/> ISE Plus License	Prepaid	10	0	+ 10		Actions ▼
<input type="checkbox"/> Threat Defense Virtual Malware Protection	Prepaid	10	1	+ 9		Actions ▼
<input type="checkbox"/> Threat Defense Virtual Threat Protection	Prepaid	10	1	+ 9		Actions ▼

10 ▼

Showing Page 5 of 7 (86 Records) |◀◀▶▶|

Stap 4. Ga naar **System>Licences>Smart License** om te bevestigen dat het VCC op de juiste virtuele account is geregistreerd:

Smart License Status

[Cisco Smart Software Manager](#)

Usage Authorization: Authorized (Last Synchronized On Jun 10 2020)

Product Registration: Registered (Last Renewed On Jun 10 2020)

Assigned Virtual Account: **Mex-AMP TAC**

Export-Controlled Features: Enabled

Cisco Success Network: [Enabled](#) ⓘCisco Support Diagnostics: [Disabled](#) ⓘ

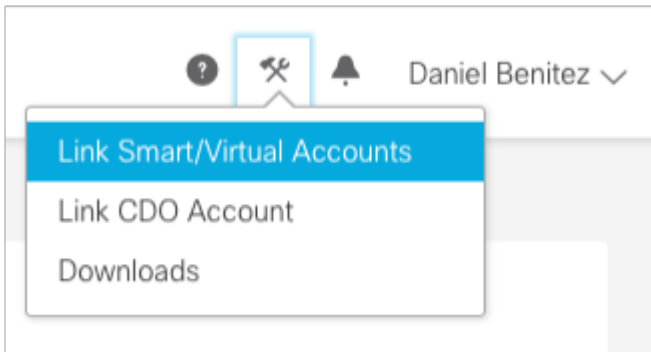
Smart Licenses

License Type/Device Name	License Status
> Firepower Management Center Virtual (1)	
> Base (1)	
> Malware (1)	
> Threat (1)	
> URL Filtering (1)	
> AnyConnect Apex (1)	
> AnyConnect Plus (1)	
AnyConnect VPN Only (0)	

Note: Container Instances of same blade share feature licenses

Koppel uw accounts aan SSE en registreer de apparaten.

Stap 1. Wanneer u zich aanmeldt bij uw SSE-account, moet u uw slimme account koppelen aan uw SSE-account, zodat u op tools-pictogram moet klikken en **Link-accounts** moet selecteren.



Zodra de account is gekoppeld, zie je de Smart Account met alle Virtual Accounts erop.

Registreer de apparaten in SSE

Stap 1. Zorg ervoor dat deze URL's zijn toegestaan in uw omgeving:

Amerikaanse regio

- api-sse.cisco.com
- eventing-ingest.sse.itd.cisco.com

EU-regio

- api.eu.sse.itd.cisco.com
- eventing-ingest.eu.sse.itd.cisco.com

APJ-regio

- api.apj.sse.itd.cisco.com
- eventing-ingest.apj.sse.itd.cisco.com

Stap 2. Meld u aan bij het SSE-portal met deze URL <https://admin.sse.itd.cisco.com>, navigeer naar **cloudservices** en schakel zowel de opties **Event** en **Cisco XDR bedreigingsrespons in**, zoals in de volgende afbeelding:

Cloud Services for Sourcefire Support

Cisco SecureX threat response

[Cisco SecureX threat response](#) enablement allows you to utilize supported devices in the course of a cybersecurity response. It also allows this platform to send high fidelity security events and observations to Threat Response.

Eventing

Eventing allows you to collect and view events in the cloud.

Stap 3. Log in op het Firepower Management Center en navigeer naar **System>Integration>Cloud Services**, schakel **Cisco Cloud Event Configuration in** en selecteer de gebeurtenissen die u naar de cloud wilt verzenden:

The screenshot shows the Cisco Firepower Management Center configuration interface. The top navigation bar includes Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. Below this, there are tabs for Configuration, Users, and Domains. The main content area has a sub-navigation bar with Cloud Services, Realms, Identity Sources, eStreamer, Host Input Client, and Smart Software Satellite. The Cloud Services section is active, showing four configuration panels:

- URL Filtering:** Includes a toggle for 'Enable Automatic Updates' (checked), 'Query Cisco Cloud for Unknown URLs' (checked), a dropdown for 'Cached URLs Expire' set to 'Never', and a checkbox for 'Dispute URL categories and reputations' (checked). A 'Save' button is at the bottom.
- AMP for Networks:** Includes a toggle for 'Enable Automatic Local Malware Detection Updates' (checked), 'Share URI from Malware Events with Cisco' (checked), and 'Use Legacy Port 32137 for AMP for Networks' (unchecked). A 'Save' button is at the bottom.
- Cisco Cloud Region:** Features a dropdown menu for 'Region' set to 'us-east-1 (US Region)'. A note below states: 'This setting determines where events are sent to, if configured to send to the cloud, as well as data generated by the Cisco Success Network and Cisco Support Diagnostics tools.' A 'Save' button is at the bottom.
- Cisco Cloud Event Configuration:** Includes three toggles: 'Send high priority Connection Events to the cloud' (checked), 'Send File and Malware Events to the cloud' (checked), and 'Send Intrusion Events to the cloud' (checked). Links for 'Click here to view your Cisco Cloud configuration' and 'Click here to view your events in Cisco Threat Response' are provided. A 'Save' button is at the bottom.

Stap 4. U kunt teruggaan naar het SSE-portal en bevestigen dat u nu de apparaten kunt zien die zijn ingeschreven op SSE:

Security Services Exchange | Devices | Cloud Services | Events | Audit Log

Devices for Sourcefire Support

0 Rows Selected

	W	#	Name	Type	Version
<input type="checkbox"/>		1	firepower	Cisco Firepower Threat Defense for VMWare	6.5.0
			IP269d7f3	IP Address: 10.10.10.27	
			Created 2020-08-10 19:51:46 UTC		
<input type="checkbox"/>		2	MEX-AMP-FMC	Cisco Firepower Management Center for VMW...	6.5.0
			IP6577b12	IP Address: 10.10.10.24	
			Created 2020-08-10 20:17:37 UTC		

Page Size: 25 | Total Entries: 2

De Evenementen worden verzonden door de FTD apparaten, navigeer naar de **Evenementen** op het portaal SSE om de gebeurtenissen te verifiëren die door de apparaten naar SSE, zoals getoond in het beeld worden verzonden:

Security Services Exchange | Devices | Cloud Services | Events | Audit Log

Event Stream for Sourcefire Support

0 Rows Selected

08/04/2020, 18:50 - 08/05/2020, 18:50

	Talos Disposition	Incident	Destination IP	Event Time	Ingest Time	Message	Protocol	Repo
<input type="checkbox"/>	Neutral	No	10.10.10.252	2020-08-05 18:48:50 UTC	2020-08-05 18:48:51 UTC		tcp	
<input type="checkbox"/>	Neutral	No	10.10.10.145	2020-08-05 18:47:38 UTC	2020-08-05 18:47:38 UTC		tcp	
<input type="checkbox"/>	Unknown	No	10.10.10.100	2020-08-05 18:47:30 UTC	2020-08-05 18:47:30 UTC		tcp	
<input type="checkbox"/>	Neutral	No	10.10.10.252	2020-08-05 18:46:50 UTC	2020-08-05 18:46:50 UTC		tcp	

Verifiëren

Valideren dat de FTD's gebeurtenissen genereren (malware of inbraakaanvallen), voor inbraakgebeurtenissen navigeer naar **Analyse>Bestanden>Malware Events**, voor inbraakgebeurtenissen navigeren naar **Analysis>Inbraakgebeurtenissen>Gebeurtenissen**.

Valideren dat de gebeurtenissen worden geregistreerd op het SSE-portaal zoals vermeld in het **Registreer de apparaten om SSE** sectie stap 4.

Bevestig dat de informatie op het Cisco XDR-dashboard wordt weergegeven of controleer de API-logbestanden zodat u de reden voor een mogelijke API-fout kunt zien.

Problemen oplossen

Connectiviteitsproblemen detecteren

U kunt generische connectiviteitsproblemen detecteren uit het action_Queue.log bestand. In geval van mislukking kunt u dergelijke logboeken zien huidig in het bestand:

```
ActionQueueScrape.pl[19094]: [SF::SSE::Enrollment] canConnect: System (/usr/bin/curl -s --connect-timeout
```

In dit geval betekent afsluitcode 28 uitgeschakelde bediening en moeten we de internetverbinding controleren. Je moet ook exit code 6 zien wat problemen met DNS resolutie betekent

Connectiviteitsproblemen als gevolg van DNS-resolutie

Stap 1. Controleer of de connectiviteit goed werkt.

```
root@ftd01:~# curl -v -k https://api-sse.cisco.com
* Rebuilt URL to: https://api-sse.cisco.com/
* getaddrinfo(3) failed for api-sse.cisco.com:443
* Couldn't resolve host 'api-sse.cisco.com'
* Closing connection 0
curl: (6) Couldn't resolve host 'api-sse.cisco.com'
```

Deze output toont aan dat het apparaat niet in staat is om de URL <https://api-sse.cisco.com> op te lossen, in dit geval, moeten we valideren dat de juiste DNS server is geconfigureerd, het kan worden gevalideerd met een naslookup van de expert CLI:

```
root@ftd01:~# nslookup api-sse.cisco.com
;; connection timed out; no servers could be reached
```

Deze uitvoer toont aan dat de DNS geconfigureerd niet wordt bereikt om de DNS-instellingen te bevestigen. Gebruik hiervoor de opdracht **netwerk tonen**:

```
> show network
===== [ System Information ] =====
Hostname           : ftd01
DNS Servers        : x.x.x.10
Management port    : 8305
IPv4 Default route
Gateway            : x.x.x.1

===== [ eth0 ] =====
State              : Enabled
Link               : Up
Channels           : Management & Events
Mode               : Non-Autonegotiation
MDI/MDIX           : Auto/MDIX
MTU                : 1500
MAC Address        : x:x:x:x:9D:A5
----- [ IPv4 ] -----
Configuration      : Manual
Address            : x.x.x.27
Netmask            : 255.255.255.0
Broadcast          : x.x.x.255
----- [ IPv6 ] -----
Configuration      : Disabled

===== [ Proxy Information ] =====
```

```
State : Disabled
Authentication : Disabled
```

In dit voorbeeld is de verkeerde DNS-server gebruikt, kunt u de DNS-instellingen met deze opdracht wijzigen:

```
> configure network dns x.x.x.11
```

Nadat deze connectiviteit opnieuw kan worden getest en deze keer, is de verbinding succesvol.

```
root@ftd01:~# curl -v -k https://api-sse.cisco.com
* Rebuilt URL to: https://api-sse.cisco.com/
* Trying x.x.x.66...
* Connected to api-sse.cisco.com (x.x.x.66) port 443 (#0)
* ALPN, offering http/1.1
* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH
* successfully set certificate verify locations:
* CAfile: none
CApath: /etc/ssl/certs
* TLSv1.2 (OUT), TLS header, Certificate Status (22):
* TLSv1.2 (OUT), TLS handshake, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (IN), TLS handshake, Server key exchange (12):
* TLSv1.2 (IN), TLS handshake, Request CERT (13):
* TLSv1.2 (IN), TLS handshake, Server finished (14):
* TLSv1.2 (OUT), TLS handshake, Certificate (11):
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.2 (OUT), TLS change cipher, Client hello (1):
* TLSv1.2 (OUT), TLS handshake, Finished (20):
* TLSv1.2 (IN), TLS change cipher, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.2 / ECDHE-RSA-AES128-GCM-SHA256
* ALPN, server accepted to use http/1.1
* Server certificate:
* subject: C=US; ST=California; L=San Jose; O=Cisco Systems, Inc.; CN=api -sse.cisco.com
* start date: 2019-12-03 20:57:56 GMT
* expire date: 2021-12-03 21:07:00 GMT
* issuer: C=US; O=HydrantID (Avalanche Cloud Corporation); CN=HydrantID S SL ICA G2
* SSL certificate verify result: self signed certificate in certificate chain (19), continuing anyway.
> GET / HTTP/1.1
> Host: api-sse.cisco.com
> User-Agent: curl/7.44.0
> Accept: */*
>
< HTTP/1.1 403 Forbidden
< Date: Wed, 08 Apr 2020 01:27:55 GMT
< Content-Type: text/plain; charset=utf-8
< Content-Length: 9
< Connection: keep-alive
< Keep-Alive: timeout=5
< ETag: "5e17b3f8-9"
< Cache-Control: no-store
< Pragma: no-cache
```



```
< Content-Security-Policy: default-src 'self'  
< X-Content-Type-Options: nosniff  
< X-XSS-Protection: 1; mode=block  
< Strict-Transport-Security: max-age=31536000; includeSubdomains;
```

Registratieproblemen voor SSE Portal

Zowel FMC als FTD hebben een verbinding met de SSE URL's op hun beheerinterface nodig om de verbinding te testen. Voer deze opdrachten in op de Firepower CLI met root access:

```
<#root>
```

```
curl -v https://api-sse.cisco.com/providers/sse/services/registration/api/v2/clients --cacert /ngfw/etc/
```

```
curl -v https://est.sco.cisco.com --cacert /ngfw/etc/ssl/connectorCA.pem
```

```
curl -v https://eventing-ingest.sse.itd.cisco.com --cacert /ngfw/etc/ssl/connectorCA.pem
```

```
curl -v https://mx01.sse.itd.cisco.com --cacert /ngfw/etc/ssl/connectorCA.pem
```

De certificaatcontrole kan met deze opdracht worden overgeslagen:

```
root@ftd01:~# curl -v -k https://api-sse.cisco.com  
* Rebuilt URL to: https://api-sse.cisco.com/  
* Trying x.x.x.66...  
* Connected to api-sse.cisco.com (x.x.x.66) port 443 (#0)  
* ALPN, offering http/1.1  
* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH  
* successfully set certificate verify locations:  
* CAfile: none  
CApath: /etc/ssl/certs  
* TLSv1.2 (OUT), TLS header, Certificate Status (22):  
* TLSv1.2 (OUT), TLS handshake, Client hello (1):  
* TLSv1.2 (IN), TLS handshake, Server hello (2):  
* TLSv1.2 (IN), TLS handshake, Certificate (11):  
* TLSv1.2 (IN), TLS handshake, Server key exchange (12):  
* TLSv1.2 (IN), TLS handshake, Request CERT (13):  
* TLSv1.2 (IN), TLS handshake, Server finished (14):  
* TLSv1.2 (OUT), TLS handshake, Certificate (11):  
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):  
* TLSv1.2 (OUT), TLS change cipher, Client hello (1):  
* TLSv1.2 (OUT), TLS handshake, Finished (20):  
* TLSv1.2 (IN), TLS change cipher, Client hello (1):  
* TLSv1.2 (IN), TLS handshake, Finished (20):  
* SSL connection using TLSv1.2 / ECDHE-RSA-AES128-GCM-SHA256  
* ALPN, server accepted to use http/1.1  
* Server certificate:  
* subject: C=US; ST=California; L=San Jose; O=Cisco Systems, Inc.; CN=api -sse.cisco.com
```

```
* start date: 2019-12-03 20:57:56 GMT
* expire date: 2021-12-03 21:07:00 GMT
* issuer: C=US; O=HydrantID (Avalanche Cloud Corporation); CN=HydrantID S SL ICA G2
* SSL certificate verify result: self signed certificate in certificate chain (19), continuing anyway.
> GET / HTTP/1.1
> Host: api-sse.cisco.com
> User-Agent: curl/7.44.0
> Accept: */*
>
< HTTP/1.1 403 Forbidden
< Date: Wed, 08 Apr 2020 01:27:55 GMT
< Content-Type: text/plain; charset=utf-8
< Content-Length: 9
< Connection: keep-alive
< Keep-Alive: timeout=5
< ETag: "5e17b3f8-9"
< Cache-Control: no-store
< Pragma: no-cache
< Content-Security-Policy: default-src 'self'
< X-Content-Type-Options: nosniff
< X-XSS-Protection: 1; mode=block
< Strict-Transport-Security: max-age=31536000; includeSubdomains;
```

Opmerking: Je krijgt het 403 Verboden bericht omdat de parameters die worden verzonden van de test niet is wat SSE verwacht, maar dit bewijst genoeg om connectiviteit te valideren.

Controleer de SSEConnectorstatus

U kunt de eigenschappen van de connector verifiëren zoals aangegeven op de afbeelding.

```
# more /ngfw/etc/sf/connector.properties
registration_interval=180
connector_port=8989
connector_fqdn=api-sse.cisco.com
```

Om de connectiviteit tussen de SSConnector en de EventHandler te controleren kunt u deze opdracht gebruiken, is dit een voorbeeld van een slechte verbinding:

```
root@firepower:/etc/sf# netstat -anlp | grep EventHandler_SSEConnector.sock
unix 2 [ ACC ] STREAM LISTENING 3022791165 11204/EventHandler /ngfw/var/sf/run/EventHandler_SSEConnector.sock
```

In het voorbeeld van een bestaande verbinding kunt u zien dat de status van de stream verbonden is:

```
root@firepower:/etc/sf# netstat -anlp | grep EventHandler_SSEConnector.sock
unix 2 [ ACC ] STREAM LISTENING 382276 7741/EventHandler /ngfw/var/sf/run/EventHandler_SSEConnector.sock
unix 3 [ ] STREAM CONNECTED 378537 7741/EventHandler /ngfw/var/sf/run/EventHandler_SSEConnector.sock
```

Controleer de naar het SSE-portal en de CTR verzonden gegevens

Om gebeurtenissen van het FTD-apparaat naar SSE te sturen moet een TCP-verbinding tot stand worden gebracht met <https://eventing-ingest.sse.itd.cisco.com>. Dit is een voorbeeld van een verbinding die niet tot stand is gebracht tussen het SSE-portaal en het FTD:

```
root@firepower:/ngfw/var/log/connector# lsof -i | grep conn
connector 60815 www 10u IPv4 3022789647 0t0 TCP localhost:8989 (LISTEN)
connector 60815 www 12u IPv4 110237499 0t0 TCP firepower.cisco.com:53426->ec2-100-25-93-234.compute-1.amazonaws.com
```

In de logboeken van connector.log:

```
time="2020-04-13T14:34:02.88472046-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connector] error: dial tcp 100.25.93.234:53426: connect: connection refused"
time="2020-04-13T14:38:18.244707779-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connector] error: dial tcp 100.25.93.234:53426: connect: connection refused"
time="2020-04-13T14:42:42.564695622-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connector] error: dial tcp 100.25.93.234:53426: connect: connection refused"
time="2020-04-13T14:47:48.484762429-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connector] error: dial tcp 100.25.93.234:53426: connect: connection refused"
time="2020-04-13T14:52:38.404700083-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connector] error: dial tcp 100.25.93.234:53426: connect: connection refused"
```

Opmerking: De IP-adressen die worden weergegeven op x.x.x.246 en 1x.x.x.246 behoren tot <https://eventing-ingest.sse.itd.cisco.com> moeten worden gewijzigd. Daarom wordt aanbevolen het verkeer toe te staan naar SSE Portal op basis van URL in plaats van IP-adressen.

Als deze verbinding niet tot stand is gebracht, worden de gebeurtenissen niet naar de SSE-portal verzonden. Dit is een voorbeeld van een bestaande verbinding tussen het FTD- en het SSE-portaal:

```
root@firepower:# lsof -i | grep conn
connector 13277 www 10u IPv4 26077573 0t0 TCP localhost:8989 (LISTEN)
connector 13277 www 19u IPv4 26077679 0t0 TCP x.x.x.200:56495->ec2-35-172-147-246.compute-1.amazonaws.com
```

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.