Probleemoplossing voor de FMC-integratie met CTR

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Achtergrondinformatie](#)
[SSEC-connector](#)
[CTR](#)
[Castle-portal](#)
[Security Services exchange-portal](#)
[Problemen oplossen](#)
[Controleer of de cloudservices zijn ingeschakeld](#)
[Controleer de connectiviteit tussen FMC/FTD en SSE Portal](#)
[Controleer de SSECconnector-status](#)
[Controleer gegevens die naar het SSE-portaal en de CTR zijn verzonden](#)
[Veelvoorkomende problemen](#)
[Belangrijke bestandslocaties](#)
[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft de stappen om problemen op te lossen met het installatieproces van de Security Services Exchange (SSE) wanneer het wordt uitgeschakeld op de Firepower Management Center (FMC) of Firepower Threat Defense (FTD) apparaten voor de integratie met Cisco Threat Response (CTR).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- FMC
- FTD
- CTR-integratie

Gebruikte componenten

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

- FMC op softwareversie 6.4.0 of hoger
- FTD op softwareversie 6.4.0 of hoger
- Cisco Security Services exchange
- CTR-account

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 levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

SSEC-connector

SSECconnector is een proces op de FirePOWER-apparaten na 6.4.0 dat de apparaten in het SSE-portaal invoert. Het FMC zendt uit naar alle beheerde FTD's wanneer de Cisco Cloud-configuratie is ingesteld op Aan of Uit. Als de Cisco Cloud is ingeschakeld, start de SSECconnectorservice de communicatie tussen het SSE-portal en de FirePOWER-apparaten. Elke FTD vraagt het VCC om een registratietok waarmee de apparaten in het SSE-portaal kunnen worden geïntegreerd. Na deze integratie wordt de SSE-context op de apparaten geactiveerd en de EventHandler wordt opnieuw geconfigureerd om inbraakgebeurtenissen naar de Cisco Cloud te sturen.

CTR

Threat Response is een hub van reacties op bedreigingsincidenten, die integraties tussen meerdere Cisco Security producten ondersteunt en automatisert. Threat Response versnelt belangrijke beveiligingstaken: detectie, onderzoek en herstel, en is een hoeksteen in onze geïntegreerde security architectuur.

Het doel van de Reactie van de Bedreiging is om de teams van de netwerkoperaties en de hulpverleners van het incident te helpen bedreigingen op hun netwerk door alle bedreigingen begrijpen die van de bedreigingsintelligentie verzameld en gecombineerd beschikbaar zijn van Cisco en derden.

Maar bovenal is de Threat Response ontworpen om de complexiteit van security tools te verminderen, bedreigingen te identificeren en de respons op incidenten te versnellen.

Threat Response is een integratieplatform (https://visibility.amp.cisco.com/). Het systeem werkt via "modules", die onafhankelijke codestukken zijn die communicatie met verschillende geïntegreerde systemen (bijvoorbeeld Threat Grid of AMP) afhandelen. Deze modules behandelen alle drie de functies die een geïntegreerd systeem kan bieden (verrijking, lokale context en respons).

Wanneer kan CTR worden voorgeschreven?

- Incidentrespons
- Onderzoek
- Threat Hunting
- Incidentbeheer

Wanneer u op zoek bent naar een waarneembaar document, vragen al uw geconfigureerde modules de systemen waarvoor zij verantwoordelijk zijn om naar een register van die

waarneembare waarden te zoeken. Ze nemen de geboden reacties en geven ze terug aan Threat Response, dan neemt ze de verzamelde resultaten van alle modules (in dit geval de Stealthwatch-module), sorteert en organiseert ze de gegevens en tonen ze in een grafiek.

Om CTR met verschillende producten te integreren zijn nog twee portals "https://castle.amp.cisco.com/" (Castle) en "https://admin.sse.itd.cisco.com/app/devices" (Security Services Exchange) betrokken

Castle-portal

Hier kunt u de Cisco-beveiligingsrekeningen beheren:

Een Cisco Security-account stelt u in staat meerdere toepassingen te beheren in de Cisco Security-portefeuille. Overeenkomstig uw vergunningsrechten kan dit het volgende omvatten:

- Advanced Malware Protection voor endpoints
- Threat Grid
- Threat Response

Security Services exchange-portal

Dit portaal is een uitbreiding van het CTR-portaal, waar je de apparaten kunt beheren die geregistreerd zijn in het CTR-portaal, zodat je de penningen kunt maken die nodig zijn om de producten te integreren.

Security Services Exchange biedt apparaat, service en eventbeheer wanneer u bepaalde Cisco security producten met Cisco Threat Response integreert, inclusief deze producten en functies:

- Beheer van de lijst met security beheerapplicaties die integreren met Cisco Threat Response.
- Verzamel eventgegevens van geïntegreerde Cisco Firepower apparaten, ter voorbereiding om dit (automatisch of handmatig) naar Cisco Threat Response te verzenden.

Problemen oplossen

Controleer of de cloudservices zijn ingeschakeld

Controleer eerst op FMC op **System > Licenties > Smart Licenties** die u niet in de evaluatiemodus hebt.

Controleer nu onder **System > Integration** op het tabblad **Smart Software Satellite** dat de geselecteerde optie **rechtstreeks** wordt **aangesloten op Cisco Smart Software Manager** omdat deze functie niet wordt ondersteund in een lucht-getinte omgeving.

navigeren naar **Systeem > Integratie** in het tabblad **Cloudservices** en controleer of **Cisco Cloud Event Configuration** optie is ingeschakeld.

Controleer de connectiviteit tussen FMC/FTD en SSE Portal

Deze volgende URL's moeten worden toegestaan naarmate IP's kunnen wijzigen:

Amerikaanse regio

- api-sse.cisco.com
- est.sco.cisco.com (overal gelijk)
- mx*.sse.itd.cisco.com (momenteel alleen mx01.sse.itd.cisco.com)
- dex.sse.itd.cisco.com (voor succes van klanten)
- eventing-ingest.sse.itd.cisco.com (voor CTR en CDO)

EU-regio

- api.eu.sse.itd.cisco.com
- est.sco.cisco.com (overal gelijk)
- mx*.eu.sse.itd.cisco.com (momenteel alleen mx01.eu.sse.itd.cisco.com)
- dex.eu.sse.itd.cisco.com (voor succes van klanten)
- eventing-ingest.eu.sse.itd.cisco.com (voor CTR en CDO)

APJ-regio

- api.apj.sse.itd.cisco.com
- est.sco.cisco.com (overal gelijk)
- mx*.apj.sse.itd.cisco.com (momenteel alleen mx01.apj.sse.itd.cisco.com)
- dex.apj.sse.itd.cisco.com (voor succes van klanten)
- eventing-ingest.apj.sse.itd.cisco.com (voor CTR en CDO)

Zowel FMC als FTD hebben een verbinding nodig met de SSE URL's op hun beheerinterface om de verbinding te testen, om deze opdrachten in te voeren in de Firepower CLI met worteltoegang:

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

Nadat elke opdracht uitgevoerd is, moet u deze regel rond het einde van de verbinding zien: **verbinding #0 om "URL" intact te laten**.

Als de verbindingstijden uit zijn of u deze regel niet in de uitvoer ontvangt, controleer dan of de beheerinterfaces toegang tot deze URL's hebben en of er geen upstream apparaten zijn die de verbinding tussen de apparaten en deze URL's blokkeren of wijzigen.

De certificaatcontrole kan met deze opdracht worden omzeild:

```
root@ftd01:~# curl -v -k https://api-sse.cisco.com
* Rebuilt URL to: https://api-sse.cisco.com/
* Trying 52.4.85.66...
* Connected to api-sse.cisco.com (52.4.85.66) 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 c hain (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 uit de test worden verstuurd niet zijn wat SSE verwacht, maar dit bewijst genoeg om connectiviteit te valideren.

Controleer de SSECconnector-status

U kunt de eigenschappen van de connector zoals hieronder controleren.

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

Om de connectiviteit tussen de SSCconnector 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 gevestigde verbinding kunt u zien dat de stream status 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.soc
```

Controleer gegevens die naar het SSE-portaal en de CTR zijn verzonden

Om gebeurtenissen van het FTD-apparaat naar SEE te kunnen versturen 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 de 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:https (SYN_SENT)
```

In de blog connector.log:

```
time="2020-04-13T14:34:02.88472046-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp 18.205.49.246:443: getsockopt: connection timed out"
time="2020-04-13T14:38:18.244707779-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp 100.25.93.234:443: getsockopt: connection timed out"
time="2020-04-13T14:42:42.564695622-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp 18.205.49.246:443: getsockopt: connection timed out"
time="2020-04-13T14:47:48.484762429-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp 100.25.93.234:443: getsockopt: connection timed out"
time="2020-04-13T14:52:38.404700083-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp 100.25.93.234:443: getsockopt: connection timed out"
```

> **Opmerking:** Merkte op dat de IP-adressen die op 18.205.49.246 en 18.205.49.246 zijn weergegeven, tot https://eventing-ingest.sse.itd.cisco.com behoren, wat de reden is dat de aanbeveling het verkeer naar SSE Portal op basis van URL in plaats van IP-adressen toestaat.

Als deze verbinding niet tot stand is gebracht, worden de gebeurtenissen niet naar het SSE-portaal verzonden, dit is een voorbeeld van een gevestigde 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 192.168.1.200:56495->ec2-35-172-147-
246.compute-1.amazonaws.com:https (ESTABLISHED)
```

Veelvoorkomende problemen

Na de upgrade naar 6.4 communiceert de SSE-connector niet met het SSE-portaal. Connector.log biedt fouten vergelijkbaar met gebeurtenissen: (*Service).Start] kon geen verbinding maken met ZeroMQ PUSH-eindpunt: kon niet bellen naar \"ipc:///ngfw/var/sf/run/EventHandler_SSEConnector.sock\": Kies universum /ngfw/var/sf/run/EventHandler_SSEConnector.sock: verbinden: geen dergelijk bestand of folder\n"

Start de SSEC-verbindingsservice:

1) sudogereedschap dat de SSEC-connector verstoort

2) sudogereedschap waarmee SSEC-connector kan worden

3) Start het apparaat opnieuw. Na het opnieuw opstarten communiceert het apparaat met de cloud.

Belangrijke bestandslocaties

Debug-bestanden - toont succesvolle communicatie of foutmeldingen

```
/ngfw/var/log/connector/connector.log
```

Instellingen configuratie

```
/ngfw/etc/sf/connector.properties
```

Instellingen configuratie

```
curl localhost:8989/v1/contexts/default
```

Gerelateerde informatie

- https://docs.castle.amp.cisco.com/CiscoSecurityAccountUserGuide.pdf
- Technische ondersteuning en documentatie – Cisco Systems