# Solución de problemas de integración de FMC con CTR

## Contenido



## Introducción

Este documento describe los pasos para resolver problemas del proceso del conector de Security Services Exchange (SSE) cuando se inhabilita en los dispositivos Firepower Management Center (FMC) o Firepower Threat Defense (FTD) para la integración con Cisco Threat Response (CTR).

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- FMC
- FTD
- integración CTR

### Componentes Utilizados

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

- FMC en la versión de software 6.4.0 o posterior
- FTD en la versión de software 6.4.0 o posterior
- Intercambio de servicios de seguridad de Cisco
- Cuenta CTR

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

# Antecedentes

## SSEConnector

SSEConnector es un proceso en los dispositivos FirePOWER después de 6.4.0 que inscribe los dispositivos en el portal SSE. FMC transmite a todos los FTD administrados cuando la configuración de Cisco Cloud está activada o desactivada. Una vez habilitada la nube de Cisco, el servicio SSEConnector inicia la comunicación entre el portal SSE y los dispositivos Firepower. Cada FTD solicita al FMC un token de registro que permita integrar los dispositivos en el portal SSE. Después de esta integración, el contexto SSE se activa en los dispositivos y EventHandler se reconfigura para enviar eventos de intrusión a la nube de Cisco.

## CTR

Threat Response es un centro de orquestación de respuesta ante incidentes de amenazas que admite y automatiza las integraciones en varios productos de seguridad de Cisco. Threat Response acelera las tareas clave de seguridad: detección, investigación y remediación, y es una piedra angular de nuestra arquitectura de seguridad integrada.

El objetivo de Threat Response es ayudar a los equipos de operaciones de red y a los responsables de responder ante incidentes a comprender las amenazas en su red por toda la inteligencia de amenazas recopilada y combinada disponible de Cisco y de terceros.

Pero más que nada, Threat Response se ha diseñado para reducir la complejidad de las herramientas de seguridad, ayudar a identificar las amenazas y acelerar la respuesta ante incidentes.

Threat Response es una plataforma de integración (https://visibility.amp.cisco.com/). El sistema funciona a través de "módulos", que son piezas independientes de código que controlan las comunicaciones con diferentes sistemas integrados (por ejemplo, Threat Grid o AMP). Estos módulos se ocupan de las 3 funciones que puede proporcionar un sistema integrado (enriquecimiento, contexto local y respuesta).

¿Para qué se puede utilizar CTR?

- Respuesta ante incidentes
- Investigaciones
- Búsqueda de amenazas
- Manejo de incidentes

Cuando busca un observable, todos los módulos configurados le piden a los sistemas de los que son responsables que busquen cualquier registro de esos observables. Luego toman las respuestas proporcionadas y las envían de vuelta a Threat Response, luego toman los resultados

recopilados de todos los módulos (en este caso, el módulo Stealthwatch), ordenan y organizan los datos y los muestran en un gráfico.

Para integrar CTR con diferentes productos, se incluyen dos portales más "https://castle.amp.cisco.com/" (Castle) y "https://admin.sse.itd.cisco.com/app/devices" (Security Services Exchange)

### Portal del castillo

Aquí puede gestionar las cuentas de seguridad de Cisco:

Una cuenta de seguridad de Cisco le permite administrar varias aplicaciones dentro de la cartera de seguridad de Cisco. De acuerdo con sus derechos de licencia, esto puede incluir:

- AMP para terminales
- Threat Grid
- Respuesta ante amenazas

### Portal de intercambio de servicios de seguridad

Este portal es una extensión del portal CTR, donde puede administrar los dispositivos que se han registrado en el portal CTR, de modo que aquí puede crear los tokens necesarios para integrar los productos.

Security Services Exchange proporciona gestión de dispositivos, servicios y eventos al integrar determinados productos de seguridad de Cisco con Cisco Threat Response, incluidos estos productos y funciones:

- Gestione la lista de dispositivos de administración de seguridad que se integran con Cisco Threat Response.
- Recopile datos de eventos de los dispositivos Cisco Firepower integrados, como preparación para reenviarlos (automática o manualmente) a Cisco Threat Response.

## Troubleshoot

### Verifique que los servicios en la nube estén habilitados

En el FMC, primero, verifique en **System > Licenses > Smart Licenses** que no está en el modo de evaluación.

Verifique ahora bajo **System > Integration** en la pestaña **Smart Software Satellite** que la opción seleccionada es **Connect directamente a Cisco Smart Software Manager** ya que esta función no se soporta en un entorno de Air-Gap.

Vaya a **System > Integration** en la pestaña **Cloud Services** y verifique que la opción **Cisco Cloud Event Configuration** esté activada.

### Verifique la conectividad entre FMC/FTD y el portal SSE

Es necesario permitir estas siguientes URL, ya que las IP pueden cambiar:

Región de EE. UU.

- api-sse.cisco.com
- est.sco.cisco.com (común en todas las zonas geográficas)
- mx*.sse.itd.cisco.com (actualmente sólo mx01.sse.itd.cisco.com)
- dex.sse.itd.cisco.com (para el éxito del cliente)
- eventing-ingest.sse.itd.cisco.com (para CTR y CDO)

Región de la UE

- api.eu.sse.itd.cisco.com
- est.sco.cisco.com (común en todas las zonas geográficas)
- mx*.eu.sse.itd.cisco.com (actualmente sólo mx01.eu.sse.itd.cisco.com)
- dex.eu.sse.itd.cisco.com (para el éxito del cliente)
- eventing-ingest.eu.sse.itd.cisco.com (para CTR y CDO)

Región APJ

- api.apj.sse.itd.cisco.com
- est.sco.cisco.com (común en todas las zonas geográficas)
- mx*.apj.sse.itd.cisco.com (actualmente sólo mx01.apj.sse.itd.cisco.com)
- dex.apj.sse.itd.cisco.com (para el éxito del cliente)
- eventing-ingest.apj.sse.itd.cisco.com (para CTR y CDO)

Tanto FMC como FTD necesitan una conexión a las URL SSE en su interfaz de administración, para probar la conexión, ingrese estos comandos en la CLI de Firepower con acceso raíz:

```
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
```

Después de ejecutar cada comando, debe ver esta línea alrededor del final de la conexión: **Conexión #0 para alojar "URL" dejado intacto**.

Si la conexión se agota o no recibe esta línea en el resultado, verifique que las interfaces de administración tengan permiso para acceder a estas URL y que no haya dispositivos ascendentes que bloqueen o modifiquen la conexión entre los dispositivos y estas URL.

La verificación del certificado se puede omitir con este comando:

```
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;
```

**Nota:** Recibe el mensaje 403 Forbidden, ya que los parámetros enviados desde la prueba no son lo que espera SSE, pero esto demuestra lo suficiente para validar la conectividad.

## Verificación del estado SSEConnector

Puede verificar las propiedades del conector como se muestra a continuación.

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

Para verificar la conectividad entre el SSConnector y el EventHandler puede utilizar este comando, este es un ejemplo de una conexión incorrecta:

```
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
```

En el ejemplo de una conexión establecida, puede ver que el estado de la secuencia está conectado:

```
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
```

## Verificar los datos enviados al portal SSE y al CTR

Para enviar eventos desde el dispositivo FTD a SEE se necesita establecer una conexión TCP con https://eventing-ingest.sse.itd.cisco.com Este es un ejemplo de una conexión no establecida entre el portal SSE y el 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)
```

En los registros 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"
```

> **Nota:** Notando que las direcciones IP mostradas 18.205.49.246 y 18.205.49.246 pertenecen a https://eventing-ingest.sse.itd.cisco.com pueden cambiar, por esta razón la recomendación es permitir el tráfico al portal SSE basado en URL en lugar de direcciones IP.

Si no se establece esta conexión, los eventos no se envían al portal SSE, este es un ejemplo de una conexión establecida entre el FTD y el portal SSE:

```
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)
```

## Problemas comunes

Después de la actualización a 6.4, el conector SSE no se comunica con el portal SSE. Connector.log proporciona errores similares a los eventos:(*Service).Start] No se pudo conectar al extremo PUSH ZeroMQ: no se pudo marcar a \"ipc:///ngfw/var/sf/run/EventHandler_SSEConnector.sock\": dial unix /ngfw/var/sf/run/EventHandler_SSEConnector.sock: conectar: no tal archivo o directorio\n"

Reinicie el servicio SSEConnector:

1) sudo pmtool disablebyid SSEConnector

2) sudo pmtool habilidoySSEConnector

3) Reinicie el dispositivo. Al reiniciar, el dispositivo se comunica con la nube.

### Ubicaciones importantes del archivo de registro

Registros de depuración: muestra mensajes de conexión o fallo correctos

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

Configuración

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

Configuración

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

## Información Relacionada

- https://docs.castle.amp.cisco.com/CiscoSecurityAccountUserGuide.pdf
- Soporte Técnico y Documentación - Cisco Systems