Troubleshoot the FMC integration with CTR

Contents

Introduction

This document describes the steps to troubleshoot the Security Services Exchange (SSE) Connector process when it becomes disabled on the Firepower Management Center (FMC) or Firepower Threat Defense (FTD) devices for the integration with Cisco Threat Response (CTR).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- FMC
- FTD
- CTR integration

Components Used

The information in this document is based on these software and hardware versions:

- FMC on software version 6.4.0 or above
- FTD on software version 6.4.0 or above
- Cisco Security Services Exchange

- CTR Account

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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

SSEConnector

SSEConnector is a process on the Firepower devices after 6.4.0 which enrolls the devices into the SSE portal. The FMC broadcasts to all the managed FTDs when the Cisco Cloud configuration is set to On or Off. Once the Cisco Cloud is enabled, the SSEConnector service starts the communication between the SSE portal and the Firepower devices. Each FTD requests the FMC for a registration token which allows the devices to be integrated into the SSE portal. After this integration, the SSE context is activated on the devices and the EventHandler is reconfigured to send Intrusion Events to the Cisco Cloud.

CTR

Threat Response is a threat incident response orchestration hub, which supports and automates integrations across multiple Cisco Security products. Threat Response accelerates key security tasks: detection, investigation, and remediation, and is a keystone in our integrated security architecture.

The goal of Threat Response is to help network operations teams and incident responders understand threats on their network by all of the threat intelligence gathered and combined available from Cisco and third parties.

But more than anything else, Threat Response is designed to reduce the complexity of security tools, help identify threats, and speed up incident response.

Threat Response is an integration platform (https://visibility.amp.cisco.com/). The system works via “modules”, which are independent pieces of code that handle communications with different integrated systems (eg Threat Grid, or AMP). These modules handle all 3 of the functions that an integrated system can provide (enrichment, local context, and response).

What can CTR be used for?

- Incident Response
- Investigations
- Threat Hunting
- Incident Management

When you search for an observable, all of your configured modules ask the systems for which they are responsible to search for any record of those observables. They then take the provided responses and pass them back to Threat Response, then it takes the collected results from all modules (in this case the Stealthwatch module), and sorts and organizes the data and display it in a graph.

To integrate CTR with different products are involved two more portals “https://castle.amp.cisco.com/” (Castle) and “https://admin.sse.itd.cisco.com/app/devices”

(Security Services Exchange)

Castle Portal

Here you can manage the Cisco Security Accounts:

A Cisco Security account allows you to manage multiple applications within the Cisco Security portfolio. In accordance on your licensing entitlements, this can include:

- AMP for Endpoints
- Threat Grid
- Threat Response

Security Services Exchange Portal

This portal is an extension of the CTR portal, where you can manage the devices that have been registered in the CTR portal, so here you can create the tokens needed to integrate the products.

Security Services Exchange provides device, service, and event management when you integrate certain Cisco security products with Cisco Threat Response, including these products and features:

- Manage the list of Security Management Appliances that integrate with Cisco Threat Response.
- Collect event data from integrated Cisco Firepower devices, in preparation to forward it (automatically or manually) to Cisco Threat Response.

Troubleshoot

Verify Cloud Services are enabled

On the FMC, first, verify on **System** > **Licenses** > **Smart Licenses** you are not on evaluation mode.

Verify now under **System** > **Integration** on the **Smart Software Satellite** tab that the selected option is **Connect directly to Cisco Smart Software Manager** as this feature is not supported on an air-gapped environment.

Navigate to **System** > **Integration** on the **Cloud Services** tab and check that **Cisco Cloud Event Configuration** option is turned on.

Verify connectivity between FMC/FTD and SSE Portal

These next URLs needs to be whitelisted as IPs can change:

US Region

- api-sse.cisco.com

- est.sco.cisco.com (common across geographies)
- mx*.sse.itd.cisco.com (currently only mx01.sse.itd.cisco.com)
- dex.sse.itd.cisco.com (for customer success)
- eventing-ingest.sse.itd.cisco.com (for CTR and CDO)

EU Region

- api.eu.sse.itd.cisco.com
- est.sco.cisco.com (common across geographies)
- mx*.eu.sse.itd.cisco.com (currently only mx01.eu.sse.itd.cisco.com)
- dex.eu.sse.itd.cisco.com (for customer success)
- eventing-ingest.eu.sse.itd.cisco.com (for CTR and CDO)

APJ Region

- api.apj.sse.itd.cisco.com
- est.sco.cisco.com (common across geographies)
- mx*.apj.sse.itd.cisco.com (currently only mx01.apj.sse.itd.cisco.com)
- dex.apj.sse.itd.cisco.com (for customer success)
- eventing-ingest.apj.sse.itd.cisco.com (for CTR and CDO)

Both FMC and FTD need a connection to the SSE URLs on their management interface, to test the connection, enter these commands on the Firepower CLI with root access:

```
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
```

After each command is run, you must see this line around the end of the connection: **Connection #0 to host "URL" left intact**.

If the connection times out or you don't receive this line on the output, please verify that the management interfaces are allowed access to these URLs and that there are no upstream devices that block or modify the connection between the devices and these URLs.

The certificate check can be bypassed with this command:

```
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;
```

> **Note**: You get the 403 Forbidden message as the parameters sent form the test is not what SSE expects but this proves enough to validate connectivity.

Verify SSEConnector state

You can verify the connector properties as below.

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

In order to check the connectivity between the SSConnector and the EventHandler you can use this command, this is an example of a bad connection:

```
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 the example of an established connection you can see that the stream status is connected:

```
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
```

Verify data sent to the SSE portal and CTR

In order to send events from the FTD device to SEE a TCP connection needs to be established with **https://eventing-ingest.sse.itd.cisco.com** This is an example of a connection not established between the SSE portal and the 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 the connector.log logs:

```
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"
```

> **Note**: Noticed that the IP addresses displayed 18.205.49.246 and 18.205.49.246 belong to **https://eventing-ingest.sse.itd.cisco.com** might change, this is why the recommendation is to allow the traffic to SSE Portal based on URL instead of IP addresses.

If this connection is not established, the events are not sent to the SSE portal, this is an example of an established connection between the FTD and the SSE portal:

```
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)
```

Common Issues

After the upgrade to 6.4 the SSE connector does not communicate with the SSE portal. Connector.log provides errors similar to events:(*Service).Start] Could not connect to ZeroMQ PUSH endpoint: could not dial to \"ipc:///ngfw/var/sf/run/EventHandler_SSEConnector.sock\": dial unix /ngfw/var/sf/run/EventHandler_SSEConnector.sock: connect: no such file or directory\n"

Restart the SSEConnector Service:

1) sudo pmtool disablebyid SSEConnector

2) sudo pmtool enablebyid SSEConnector

3) Restart the device. Upon restart, the device communicates to the cloud.

Important Log File Locations

Debug logs - Shows successful connection or failure messages

`/ngfw/var/log/connector/connector.log`
Configuration Settings

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

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

Related Information

- **https://docs.castle.amp.cisco.com/CiscoSecurityAccountUserGuide.pdf**
- **Technical Support & Documentation - Cisco Systems**