Troubleshoot Secure Firewall Integration with Security Services Exchange

Contents

Introduction

This document describes how to troubleshoot Cisco Secure Firewall integration with Security Services Exchange (SSX).

Prerequisites

Requirements

Cisco recommends knowledge of these topics:

- Secure Firewall Management Center (FMC)
- Cisco Secure Firewall

Components Used

- Cisco Secure Firewall - 7.6.0
- Secure Firewall Management Center (FMC) - 7.6.0
- Security Services eXchange (SSX)

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.

Troubleshooting

Connectivity

The major requirement is to allow HTTPS traffic toward these addresses from the registering device:

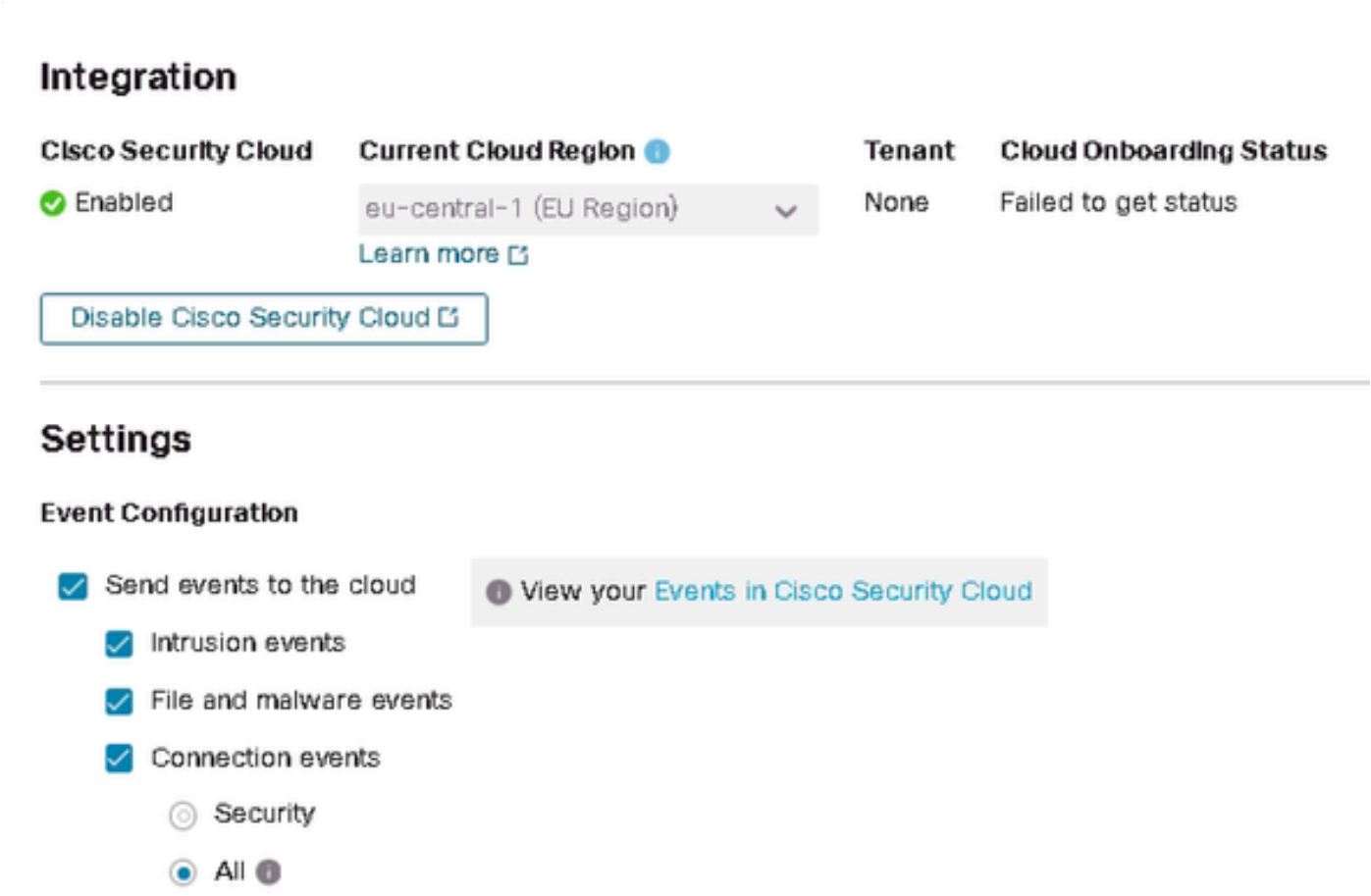
- US region:
  - api-sse.cisco.com
  - mx*.sse.itd.cisco.com
  - dex.sse.itd.cisco.com
  - eventing-ingest.sse.itd.cisco.com
  - registration.us.sse.itd.cisco.com
  - defenseorchestrator.com
  - edge.us.cdo.cisco.com
- EU region:
  - api.eu.sse.itd.cisco.com
  - mx*.eu.sse.itd.cisco.com
  - dex.eu.sse.itd.cisco.com
  - eventing-ingest.eu.sse.itd.cisco.com
  - registration.eu.sse.itd.cisco.com
  - defenseorchestrator.eu
  - edge.eu.cdo.cisco.com
- Asia (APJC) region:
  - api.apj.sse.itd.cisco.com
  - mx*.apj.sse.itd.cisco.com
  - dex.apj.sse.itd.cisco.com
  - eventing-ingest.apj.sse.itd.cisco.com
  - registration.apj.sse.itd.cisco.com
  - apj.cdo.cisco.com
  - edge.apj.cdo.cisco.com
- Australia region:
  - api.aus.sse.itd.cisco.com
  - mx*.aus.sse.itd.cisco.com
  - dex.au.sse.itd.cisco.com
  - eventing-ingest.aus.sse.itd.cisco.com

- registration.au.sse.itd.cisco.com
- aus.cdo.cisco.com

- India region:
  - api.in.sse.itd.cisco.com
  - mx*.in.sse.itd.cisco.com
  - dex.in.sse.itd.cisco.com
  - eventing-ingest.in.sse.itd.cisco.com
  - registration.in.sse.itd.cisco.com
  - in.cdo.cisco.com

Registration

The registration of Secure Firewall to Security Services Exchange is done in Secure Firewall Management Center, in **Integration > Cisco Security Cloud**.



These outputs indicate a successful connection established to Cisco Cloud.

<#root>

```
root@firepower:~#
```

```
netstat -anlp | grep EventHandler_SSEConnector.sock

unix 3 [ ] STREAM CONNECTED 133064 4159/EventHandler /ngfw/var/sf/run/EventHandler_SSEConnector.sock
```

```
<#root>

root@firepower:~#

lsof -i | grep conn

connector 5301 www 6u IPv4 471679686 0t0 TCP firepower:53080->ec2-35-158-61-95.eu-central-1.compute.ama
connector 5301 www 8u IPv6 104710 0t0 TCP *:8989 (LISTEN)
```

Registration logs are stored in **/var/log/connector/**.

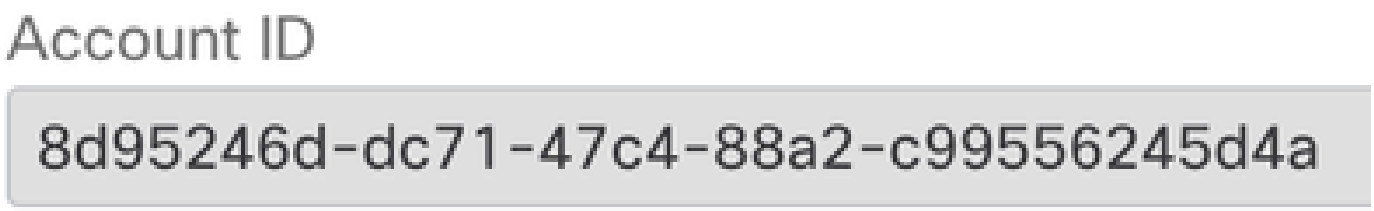
Verifying the registration

Once the registration is successful on the Secure Firewall side, an API call to **localhost:8989/v1/contexts/default/tenant** can be performed to obtain the Security Services Exchange tenant name and ID.

```
<#root>

root@firepower:~#

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

{"registeredTenantInfo":{"companyId":"601143","companyName":"lab","domainName":"tac.cisco.com","id":"56

"Cisco - lab"

,"id":

"8d95246d-dc71-47c4-88a2-c99556245d4a"

,"spId":"AMP-EU"}]}
```

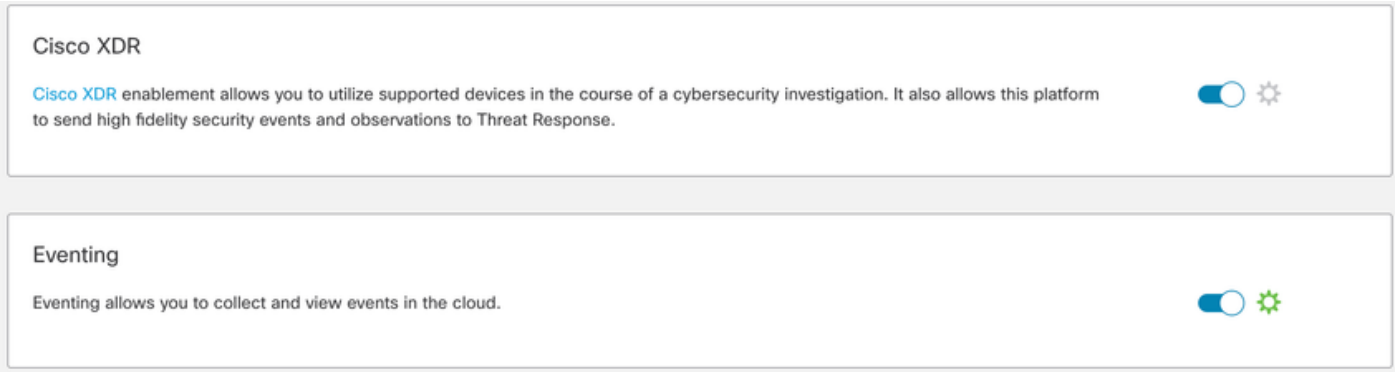
Verification on the Security Services Exchange side

In Security Services Exchange navigate to the username in the top right corner and click User Profile to confirm that the Account ID matches the tenant ID obtained before in Secure Firewall.



In the **Cloud Services** tab, it is required to have **Eventing** enabled. Also, **Cisco XDR** switch must be turned

on in case of utilizing this solution.



The **Devices** tab contains a list of registered appliances.

An entry for each device is expandable and contains these information:

- Device ID - in the case of Secure Firewall this ID can be found by querying **curl -s http://localhost:8989/v1/contexts/default | grep deviceId**
- Date of registration
- IP Address
- SSX connector version
- Last modification

Events

The events tab allows us to perform the actions on the data that was sent by Secure Firewall and that is processed and displayed in Security Services Exchange.

1. Filter the list of events and create and save filters,
2. Show or hide additional table columns,
3. Review the events sent from Secure Firewall devices.

In integration between Secure Firewall and Security Services Exchange these Event Types are supported:

Event Type	Supported Threat Defense Device Version for Direct Integration	Supported Threat Defense Device Version for Syslog Integration
Intrusion events	6.4 and later	6.3 and later
High-priority connection events: • Security-related connection events. • Connection events related to file and malware events. • Connection events related	6.5 and later	Not supported

Event Type	Supported Threat Defense Device Version for Direct Integration	Supported Threat Defense Device Version for Syslog Integration
to intrusion events.		
File and malware events	6.5 and later	Not supported

Troubleshoot events not processed in the Security Services Exchange

In the case of observing specific events in the Secure Firewall Management Center, it can be required to determine whether events match the conditions (those related to Intrusion, File/Malware and Connection events) to be processed and displayed in the Security Services Exchange.

Confirmation that events are being sent to the cloud by querying **localhost:8989/v1/contexts/default** it can be determined whether events are being sent to the cloud.

<#root>

```
root@firepower:~#

curl localhost:8989/v1/contexts/default



...

"statistics": {
 "client": [
  {
   "type": "Events",
   "statistics": {
   "ZmqStat": {
   "LastCloudConnectSuccess": "2025-01-21T10:03:13.779677978Z",
   "LastCloudConnectFailure": "2025-01-20T10:54:43.552112185Z",
   "LastCloudDisconnect": "2025-01-20T11:35:44.606352271Z",

   "TotalEventsReceived": 11464,



   "TotalEventsSent": 11463

...
```

The number of events received in **TotalEventsReceived** means events applicable for sending to the Security Services Exchange processed by Secure Firewall.

The number of events sent in **TotalEventsSent** means events sent to Cisco Cloud.

In case of events seen in the Secure Firewall Management Center, but not in the Security Services Exchange, event logs available in **/ngfw/var/sf/detection_engines/<engine>/** must be verified.

Based on a timestamp decode specific event log using u2dump:

<#root>

```
root@firepower:/ngfw/var/sf/detection_engines/4ca2e696-0996-11ed-be66-77bcdf78a081/instance-1#
u2dump unified_events-1.log.1736964974 > ../fulldump.txt

root@firepower:/ngfw/var/sf/detection_engines/4ca2e696-0996-11ed-be66-77bcdf78a081/instance-1#
cd ../instance-2

root@firepower:/ngfw/var/sf/detection_engines/4ca2e696-0996-11ed-be66-77bcdf78a081/instance-2#
ls -alh | grep unified_events-1.log.1736

-rw-r--r-- 1 root root 8.3K Jan 5 08:19 unified_events-1.log.1736064964
-rw-r--r-- 1 root root 5.0K Jan 7 23:23 unified_events-1.log.1736292107
-rw-r--r-- 1 root root 16K Jan 10 03:17 unified_events-1.log.1736393796
-rw-r--r-- 1 root root 4.7K Jan 12 16:02 unified_events-1.log.1736630477
-rw-r--r-- 1 root root 4.8K Jan 13 11:10 unified_events-1.log.1736766628
-rw-r--r-- 1 root root 5.5K Jan 14 22:41 unified_events-1.log.1736865732
-rw-r--r-- 1 root root 5.5K Jan 15 18:27 unified_events-1.log.1736964964
root@firepower:/ngfw/var/sf/detection_engines/4ca2e696-0996-11ed-be66-77bcdf78a081/instance-2#
u2dump unified_events-1.log.1736964964 >> ../fulldump.txt
```

- **Intrusion events**

All intrusion events are processed and displayed in SSX and XDR. Ensure that in decoded logs that specific event contains a flag:

<#root>

```
root@firepower:/ngfw/var/sf/detection_engines/4ca2e696-0996-11ed-be66-77bcdf78a081#
grep -i "ips event count: 1" fulldump.txt

IPS Event Count: 1
```

- **File and Malware events**

Based on Security Services Exchange platform requirements only events with specific Event Subtype are being processed and displayed.

<#root>

```
"FileEvent":
 {
   “Subtypes”:
   {
     “FileLog”:
     {
     “Unified2ID”: 500,
     “SyslogID”: 430004
```

```
    },
    "FileMalware":

    {
    "Unified2ID": 502,

    "SyslogID": 430005
    }
  }
}
```

Therefore, it looks like in these decoded logs:

<#root>

```
root@firepower:/ngfw/var/sf/detection_engines/4ca2e696-0996-11ed-be66-77bcdf78a081#
cat fulldump.txt | grep -A 11 "Type: 502"

Type: 502(0x000001f6)

Timestamp: 0
Length: 502 bytes
Unified 2 file log event Unified2FileLogEvent
FilePolicy UUID: f19fb202-ac9e-11ef-b94a-c9dafad481cf
Sensor ID : 0
Connection Instance : 1
Connection Counter : 5930
Connection Time : 1736964963
File Event Timestamp : 1736964964
Initiator IP : 192.168.100.10
Responder IP : 198.51.100.10
```

- **Connection events**

Regarding Connection Events, there are no subtypes. However, if a connection event has any of these fields, it is considered a Security Intelligence event and it is processed further in the Security Services Exchange.

• URL_SI_Category

• DNS_SI_Category

• IP_ReputationSI_Category

Note: If File/Malware or Connection events seen in Secure Firewall Management Center, do not contain mentioned subtypes or parameters in the unified events logs decoded with u2dump, this means these specific events are not being processed and displayed in Security Services Exchange

---