

Troubleshoot SecureX with Secure Firewall 7.1 and Older Versions

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Troubleshoot](#)

[Detect Connectivity Problems](#)

[Connectivity Problems due to Domain Name Server \(DNS\) Resolution](#)

Introduction

This document describes problems related to SecureX with Cisco Secure Firewall integration - versions 7.1 and older releases.

Prerequisites

Requirements

Cisco recommends knowledge of these topics:

- Firepower Management Center (FMC)
- Cisco Secure Firewall
- Optional Virtualization of images

Components Used

- Cisco Secure Firewall - 6.5
- Firepower Management Center (FMC) - 6.5
- Security Services exchange (SSE)
- SecureX
- Smart License Portal
- Cisco Threat Response (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. If your network is live, ensure that you understand the potential impact of any command.

Troubleshoot

Detect Connectivity Problems

You can detect generic connectivity problems from the `action_queue.log` file. In cases of failures, you can see

such logs present in the file:

```
ActionQueueScrape p1[19094]: [SF::SSE::Enrollment] canConnect: System (/usr/bin/curl -s --connect-timeo
```

In this case, **code 28** means operation timed out and check connectivity to the Internet.

There is also **code 6** which means problems with DNS resolution

Connectivity Problems due to Domain Name Server (DNS) Resolution

Step 1. Check that the connectivity works properly.

```
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'
```

The output shows that the device is unable to resolve the URL [_](https://api-sse.cisco.com/).

In this case, validate that the proper DNS server is configured. It can be validated with a **nslookup** from the expert CLI:

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

The output shows that the configured DNS is not reached. In order to confirm the DNS settings, use the **show network** command:

```
> 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 this example, the wrong DNS server was used. Change the DNS settings with this command:

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

After this, connectivity can be tested again. This time, the connection is successful.

```

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
Cpath: /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;
```

Registration issues to SSE Portal

Both FMC and Cisco Secure Firewall 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:

```
<#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
```

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 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
Cpath: /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; ,;
```

 **Note:** 403 Forbidden message means that the parameters sent from the test are not what SSE expects, but this proves enough to validate connectivity.

Verify SSEConnector state

Verify the connector properties as shown.

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

To check the connectivity between the SSEConnector and the EventHandler, 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_SSEConnecto
```

In the example of an established connection, verify 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.sock
```

Verify data sent to the SSE portal and CTR


To send events from the Cisco Secure Firewall device to SSE, 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 Cisco Secure Firewall:

```
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:443
```

In the `connector.log` logs:

```
time="2020-04-13T14:34:02.88472046-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connect] failed to connect to SSE portal: dial tcp 100.25.93.234:443: connect: connection refused"
time="2020-04-13T14:38:18.244707779-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connect] failed to connect to SSE portal: dial tcp 100.25.93.234:443: connect: connection refused"
time="2020-04-13T14:42:42.564695622-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connect] failed to connect to SSE portal: dial tcp 100.25.93.234:443: connect: connection refused"
time="2020-04-13T14:47:48.484762429-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connect] failed to connect to SSE portal: dial tcp 100.25.93.234:443: connect: connection refused"
time="2020-04-13T14:52:38.404700083-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connect] failed to connect to SSE portal: dial tcp 100.25.93.234:443: connect: connection refused"
```

 **Note:** Notice that the IP addresses displayed x.x.x.246 and 1x.x.x.246 belong to <https://eventing-ingest.sse.itd.cisco.com> possibly change. 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 Cisco Secure Firewall 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 x.x.x.200:56495->ec2-35-172-147-246.compute-1.amazonaws.com:443
```