

Fehlerbehebung bei SecureX mit Secure Firewall 7.1 und älteren Versionen

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Fehlerbehebung](#)

[Erkennen von Verbindungsproblemen](#)

[Verbindungsprobleme aufgrund der DNS-Auflösung \(Domain Name Server\)](#)

[Registrierungsprobleme beim SSE-Portal](#)

[Überprüfen des SSEConnector-Status](#)

[Überprüfen der an das SSE-Portal und den CTR gesendeten Daten](#)

Einleitung

In diesem Dokument werden Probleme im Zusammenhang mit SecureX und der Integration von Cisco Secure Firewall - Version 7.1 und älteren Versionen - beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Firepower Management Center (FMC)
- Sichere Cisco Firewall
- Optionale Virtualisierung von Images

Verwendete Komponenten

- Cisco Secure Firewall - 6.5
- FirePOWER Management Center (FMC) - 6.5
- Security Services Exchange (SSE)
- SecureX
- Smart License-Portal
- Cisco Threat Response (CTR)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Fehlerbehebung

Erkennen von Verbindungsproblemen

Sie können generische Verbindungsprobleme aus dem `action_queue.log` Datei. Bei Fehlern werden die Protokolle in der Datei angezeigt:

```
ActionQueueScrape pl[19094]: [SF::SSE::Enrollment] canConnect: System (/usr/bin/curl -s --connect-timeout 10 -m 20 -L --max-redirs 5 --max-filesize 104857600 --capath /ngfw/etc/sf/keys/fireamp/thawte_roots -f https://api.eu.sse.itd.cisco.com/providers/sse/api/v1/regions) Failed, curl returned 28 at /ngfw/usr/local/sf/lib/perl/5.10.1/SF/System.pmline 10477.
```

In diesem Fall bedeutet **Code 28**, dass der Vorgang abgelaufen ist und die Verbindung zum Internet überprüft wird.

Es gibt auch **Code 6**, was Probleme mit der DNS-Auflösung bedeutet

Verbindungsprobleme aufgrund der DNS-Auflösung (Domain Name Server)

Schritt 1: Stellen Sie sicher, dass die Verbindung ordnungsgemäß funktioniert.

```
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'
```

Die Ausgabe zeigt, dass das Gerät die URL nicht auflösen kann.

Überprüfen Sie in diesem Fall, ob der richtige DNS-Server konfiguriert ist. Validierung mithilfe eines `nslookup` über die CLI des Experten:

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

Die Ausgabe zeigt an, dass der konfigurierte DNS nicht erreicht wurde. Um die DNS-Einstellungen zu bestätigen, verwenden Sie den `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 diesem Beispiel wurde der falsche DNS-Server verwendet. Ändern Sie die DNS-Einstellungen mit dem folgenden Befehl:

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

Danach kann die Konnektivität erneut getestet werden. Diesmal ist die Verbindung erfolgreich.

```
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
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 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;
```

Registrierungsprobleme beim SSE-Portal

Sowohl FMC als auch Cisco Secure Firewall benötigen eine Verbindung zu den SSE-URLs auf ihrer Verwaltungsoberfläche.

Um die Verbindung zu testen, geben Sie die folgenden Befehle ein: Firepower CLI mit Root-Zugriff:

```
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
```

Die Zertifikatsüberprüfung kann mit dem folgenden Befehl umgangen werden:

```
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
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 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; , ;
```

Anmerkung: 403 Forbidden -Nachricht bedeutet, dass die vom Test gesendeten Parameter nicht den Erwartungen des SSE entsprechen. Dies reicht jedoch aus, um die Verbindung zu validieren.

Überprüfen des SSEConnector-Status

Überprüfen Sie die Verbindungseigenschaften wie dargestellt.

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

Verwenden Sie diesen Befehl, um die Verbindung zwischen SSEConnector und EventHandler zu überprüfen. Dies ist ein Beispiel für eine fehlerhafte Verbindung:

```
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
```

Überprüfen Sie im Beispiel einer bestehenden Verbindung, ob der Streamstatus verbunden ist:

```
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
```

Überprüfen der an das SSE-Portal und den CTR gesendeten Daten

Um Ereignisse vom Cisco Secure Firewall-Gerät an SSE zu senden, muss eine TCP-Verbindung mit <https://eventing-ingest.sse.itd.cisco.com> hergestellt werden.

Dies ist ein Beispiel für eine nicht hergestellte Verbindung zwischen dem SSE-Portal und der 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:https (SYN_SENT)
```

Im `connector.log` Protokolle:

```
time="2020-04-13T14:34:02.88472046-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp x.x.x.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 x.x.x.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 x.x.x.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 x.x.x.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 x.x.x.234:443: getsockopt: connection timed out"
```

Anmerkung: Beachten Sie, dass die angezeigten IP-Adressen x.x.x.246 und 1x.x.x.246 zu <https://eventing-ingest.sse.itd.cisco.com> gehören, möglicherweise ändern. Es wird empfohlen, den Datenverkehr zum SSE-Portal basierend auf der URL und nicht auf IP-Adressen zuzulassen.

Wenn diese Verbindung nicht hergestellt wird, werden die Ereignisse nicht an das SSE-Portal gesendet. Dies ist ein Beispiel für eine bestehende Verbindung zwischen der Cisco Secure Firewall und dem 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:https (ESTABLISHED)
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.