

Secure Firewall 7.1以前のバージョンでのSecureXのトラブルシューティング

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[トラブルシューティング](#)

[接続の問題の検出](#)

[ドメインネームサーバ\(DNS\)解決による接続の問題](#)

はじめに

このドキュメントでは、SecureXとCisco Secure Firewallの統合（バージョン7.1以前のリリース）に関連する問題について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Firepower Management Center (FMC)
- Cisco Secureファイアウォール
- イメージの仮想化（オプション）

使用するコンポーネント

- Cisco Secureファイアウォール – 6.5
- Firepower Management Center(FMC)- 6.5
- セキュリティサービス交換(SSE)
- SecureX
- スマートライセンスポータル
- Cisco Threat Response (CTR)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

トラブルシューティング

接続の問題の検出

一般的な接続の問題は、`action_queue.log` ファイルから検出できます。障害が発生した場合は、次のようなログがファイルに存在することを確認できます。

```
ActionQueueScrape pl[19094]: [SF::SSE::Enrollment] canConnect: System (/usr/bin/curl -s --connect-timeout 10 -m 20 -L --max-redirs 5 --max-filesize 1000000000)
```

この場合、コード28は「動作タイムアウト」を意味し、インターネットへの接続をチェックします。

コード6も存在しますが、これはDNS解決の問題を意味します

ドメインネームサーバ(DNS)解決による接続の問題

ステップ 1: 接続が正しく動作していることを確認します。

```
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'
```

この出力は、デバイスがURL ([ASAのIPアドレス](https://api-sse.cisco.com/)) を解決できないことを示しています。

この場合は、適切なDNSサーバが設定されていることを確認します。これは、エキスパートCLIから `nslookup` を使用して検証できます。

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

この出力は、設定されたDNSに到達していないことを示しています。DNS設定を確認するには、`show network` コマンドを使用します。

```
> 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

この例では、誤ったDNSサーバが使用されています。次のコマンドを使用して、DNS設定を変更します。

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

その後、接続を再度テストできます。今回は、接続が成功します。

```
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;
```

SSEポータルへの登録の問題

FMCと Cisco Secure Firewall はどちらも、管理インターフェイスでSSE URLに接続する必要があります。

接続をテストするには、ルートアクセス権を持つ Firepower CLI で次のコマンドを入力します。

<#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
```

次のコマンドを使用すると、証明書チェックをバイパスできます。

```
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; ;
```

 **注: 403 Forbidden** メッセージは、テストから送信されるパラメータがSSEで想定されるものではないことを意味しますが、これは接続を検証するのに十分であることを証明します。

図のように、コネクタのプロパティを確認します。

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

SSEConnectorとEventHandlerの間の接続を確認するには、次のコマンドを使用します。次に、接続が正しくない例を示します。

```
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
```

確立された接続の例では、ストリームのステータスがconnectedであることを確認します。

```
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
```

SSEポータルとCTRに送信されるデータの検証


Cisco Secure FirewallデバイスからSSEにイベントを送信するには、<https://eventing-ingest.sse.itd.cisco.com>でTCP接続を確立する必要があります。

次に、SSEポータルとCisco Secure Firewall間に確立されていない接続の例を示します。

```
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)
```

□ **connector.log** グループ内 :

```
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: g
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: g
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: g
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: g
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: g
```

 注：表示されているx.x.x.246および1x.x.x.246のIPアドレスは、<https://eventing-ingest.sse.itd.cisco.com>に属しており、変更される可能性があることに注意してください。IPアドレスではなく、URLに基づいてSSEポータルへのトラフィックを許可することを推奨します。

この接続が確立されない場合、イベントはSSEポータルに送信されません。これは、Cisco Secure FirewallとSSEポータル間の確立された接続の例です。

```
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)
```

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。