

# Dépannage de SecureX avec Secure Firewall 7.1 et versions antérieures

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Dépannage](#)

[Détecter les problèmes de connectivité](#)

[Problèmes de connectivité dus à la résolution DNS \(Domain Name Server\)](#)

---

## Introduction

Ce document décrit les problèmes liés à l'intégration de SecureX avec Cisco Secure Firewall - versions 7.1 et antérieures.

## Conditions préalables

### Exigences

Cisco recommande de connaître les sujets suivants :

- Firepower Management Center (FMC)
- Pare-feu sécurisé Cisco
- Virtualisation facultative des images

### Composants utilisés

- Pare-feu sécurisé Cisco - 6.5
- Centre de gestion Firepower (FMC) - 6,5
- Échange de services de sécurité (SSE)
- SecureX
- Portail de licences Smart
- 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Dépannage



State : Enabled  
Link : Up  
Channels : Management & Events  
Mode : Non-Autonegotiation  
MDI/MDIX : Auto/MDIX  
MTU : 1500  
MAC Address : 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

Dans cet exemple, un serveur DNS incorrect a été utilisé. Modifiez les paramètres DNS à l'aide de cette commande :

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

Ensuite, la connectivité peut être testée à nouveau. Cette fois, la connexion est établie.

```
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;
```

Problèmes d'inscription au portail SSE

FMC et **Cisco Secure Firewall** ont besoin d'une connexion aux URL SSE sur leur interface de gestion.

Pour tester la connexion, entrez les commandes suivantes sur le **Firepower CLI** avec accès racine :

<#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
```

La vérification du certificat peut être contournée avec cette commande :

```
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; ,;
```

---

 **Remarque** : le **403 Forbidden** message signifie que les paramètres envoyés à partir du test ne correspondent pas aux attentes de SSE, mais cela s'avère suffisant pour valider la connectivité.

---

## Vérifier l'état SSEConnector

Vérifiez les propriétés du connecteur comme indiqué.

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

Pour vérifier la connectivité entre le SSEConnector et le EventHandler, utilisez cette commande. Voici un exemple de connexion incorrecte :

```
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
```

Dans l'exemple d'une connexion établie, vérifiez que l'état du flux est connecté :

```
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
```

## Vérifier les données envoyées au portail SSE et CTR

Pour envoyer des événements du périphérique Cisco Secure Firewall à SSE, une connexion TCP doit être établie avec <https://eventing-ingest.sse.itd.cisco.com>


Voici un exemple de connexion non établie entre le portail SSE et le pare-feu sécurisé Cisco :

```
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)
```

Dans les **connector.log** journaux :

```
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
```

---

 **Remarque** : notez que les adresses IP affichées x.x.x.246 et 1x.x.x.246 appartiennent à <https://eventing-ingest.sse.itd.cisco.com> et peuvent être modifiées. Il est recommandé d'autoriser le trafic vers le portail SSE en fonction de l'URL et non des adresses IP.

---

Si cette connexion n'est pas établie, les événements ne sont pas envoyés au portail SSE. Voici un exemple de connexion établie entre le pare-feu sécurisé Cisco et le portail SSE :

```
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)
```

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.