

Solucionar problemas do SecureX com Secure Firewall 7.1 e versões mais antigas

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Troubleshooting](#)

[Detectar problemas de conectividade](#)

[Problemas de conectividade devido à resolução do Servidor de Nomes de Domínio \(DNS\)](#)

Introdução

Este documento descreve problemas relacionados ao SecureX com a integração do Cisco Secure Firewall - versões 7.1 e versões mais antigas.

Pré-requisitos

Requisitos

A Cisco recomenda o conhecimento destes tópicos:

- Firepower Management Center (FMC)
- Firewall seguro da Cisco
- Virtualização opcional de imagens

Componentes Utilizados

- Cisco Secure Firewall - 6,5
- Firepower Management Center (FMC) - 6,5
- Troca de serviços de segurança (SSE)
- SecureX
- Portal Smart License
- Cisco Threat Response (CTR)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Troubleshooting

Detectar problemas de conectividade

Você pode detectar problemas de conectividade genéricos a partir do **action_queue.log** arquivo. Em caso de falhas, você pode ver esses logs presentes no arquivo:

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

Nesse caso, o **código 28** significa que a operação atingiu o tempo limite e verifica a conectividade com a Internet.

Há também o **código 6**, que significa problemas com a resolução DNS

Problemas de conectividade devido à resolução do Servidor de Nomes de Domínio (DNS)

Etapa 1. Verifique se a conectividade funciona corretamente.

```
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'
```

A saída mostra que o dispositivo não pode resolver a URL <https://api-sse.cisco.com/>

Nesse caso, valide se o servidor DNS apropriado está configurado. Ele pode ser validado com um **nslookup** da CLI do especialista:

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

A saída mostra que o DNS configurado não foi alcançado. Para confirmar as configurações DNS, use o **show network** comando:

```
> 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: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

Neste exemplo, foi usado o servidor DNS errado. Altere as configurações DNS com este comando:

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

Depois disso, a conectividade pode ser testada novamente. Desta vez, a conexão é bem-sucedida.

```
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;
```

Problemas de registro no portal SSE

Tanto o FMC como o **Cisco Secure Firewall** precisam de uma ligação aos URLs SSE na sua interface de gestão.

Para testar a conexão, digite estes comandos no **Firepower CLI** com acesso raiz:

```
<#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
```

A verificação do certificado pode ser ignorada com este comando:

```
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; ;
```

 **Observação: 403 Forbidden** mensagem significa que os parâmetros enviados do teste não são o que o SSE espera, mas isso prova o suficiente para validar a conectividade.

Verificar o estado do SSEConnector

Verifique as propriedades do conector conforme mostrado.

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

Para verificar a conectividade entre o SSEConnector e o EventHandler, use esse comando. Este é um exemplo de conexão ruim:

```
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
```

No exemplo de uma conexão estabelecida, verifique se o status do fluxo está conectado:

```
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
```

Verificar os dados enviados ao portal SSE e ao CTR

Para enviar eventos do dispositivo Cisco Secure Firewall para o SSE, uma conexão TCP precisa ser estabelecida com <https://eventing-ingest.sse.itd.cisco.com>

Este é um exemplo de uma conexão não estabelecida entre o portal SSE e o 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)
```

Nos **connector.log** registros:

```
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
```



Observação: observe que os endereços IP exibidos x.x.x.246 e 1x.x.x.246 pertencem a <https://eventing-ingest.sse.itd.cisco.com> possivelmente mudam. A recomendação é permitir o tráfego para o Portal SSE com base na URL em vez de endereços IP.

Se essa conexão não for estabelecida, os eventos não serão enviados ao portal SSE. Este é um exemplo de uma conexão estabelecida entre o Cisco Secure Firewall e o portal 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)
```

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.