

Integrar e solucionar problemas do Cisco XDR com o Firepower Threat Defense (FTD)

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Licenciamento](#)

[Vincule suas contas ao SSE e registre os dispositivos.](#)

[Registrar os dispositivos no SSE](#)

Introdução

Este documento descreve as etapas necessárias para integrar, verificar e solucionar problemas do Cisco XDR com o Firepower Threat Defense (FTD).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)
- Virtualização opcional de imagens

Componentes Utilizados

- Firepower Threat Defense (FTD) - 6,5
- Firepower Management Center (FMC) - 6,5
- Troca de serviços de segurança (SSE)
- Cisco XDR
- Portal Smart License

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.

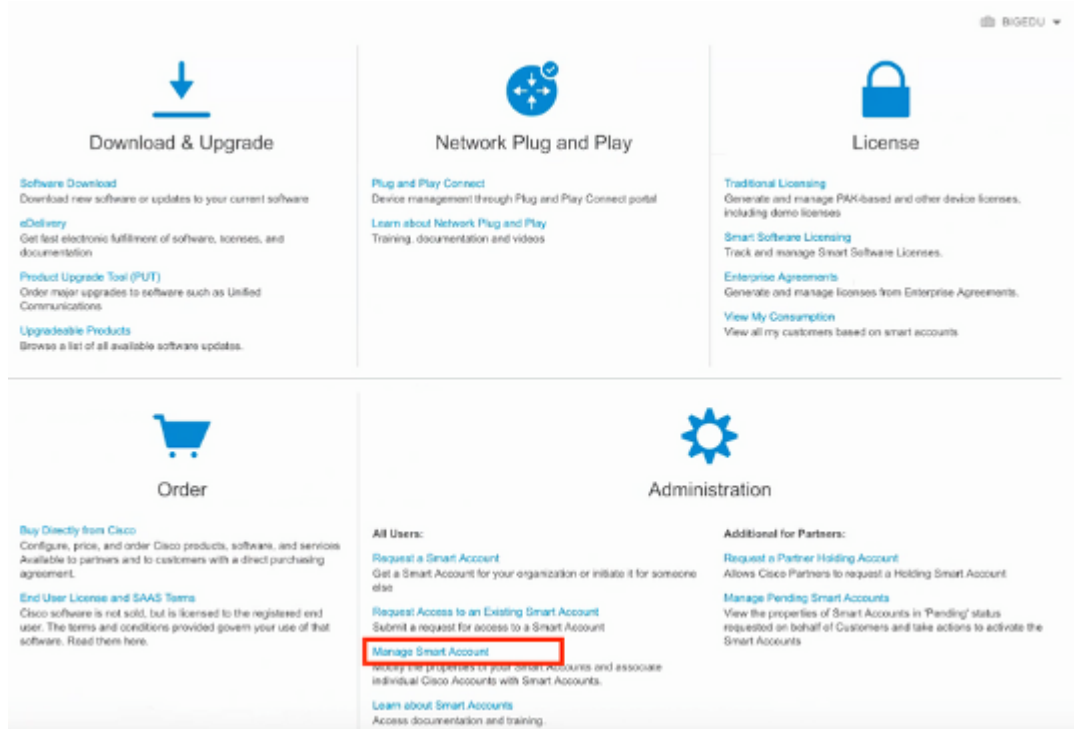
Configurar

Licenciamento

Funções da Virtual Account:

Somente o administrador da Virtual Account ou o administrador da Smart Account têm o privilégio de vincular a Smart Account à conta SSE.

Etapa 1. Para validar a função da Smart Account, navegue até **software.cisco.com** e, no **menu Administração**, selecione **Gerenciar Smart Account**.



Etapa 2. Para validar a função de usuário, navegue até **Usuários** e confirme se, em Funções, as contas estão definidas para ter um Administrador de conta virtual, como mostrado na imagem.

Cisco Software Central > Manage Smart Account > Users

Account Properties | Virtual Accounts | **Users** | Custom Tags | Requests | Account Agreements | Event Log

Users

Users		User Groups			
User	Email	Organization	Account Access	Role	
<input type="checkbox"/>	danieber				
<input type="checkbox"/>	Daniel Benitez danieben	danieben@cisco.com	Cisco Systems, Inc.	All Virtual Accounts Mex-AMP TAC	Smart Account Administrator Virtual Account Administrator

Etapa 3. Verifique se a Virtual Account selecionada para vincular no SSE contém a licença para os dispositivos de segurança se uma conta que não contém a licença de segurança estiver vinculada no SSE, se os dispositivos de segurança e o evento não aparecerem no portal do SSE.

Smart Software Licensing

[Feedback](#) [Support](#) [Help](#)[Alerts](#) | [Inventory](#) | [Convert to Smart Licensing](#) | [Reports](#) | [Preferences](#) | [On-Prem Accounts](#) | [Activity](#)Virtual Account: **Mex-AMP TAC** ▼13 Minor | [Hide Alerts](#)

General

Licenses

Product Instances

Event Log

Available Actions ▼

Manage License Tags

License Reservation...



Search by License

By Name

By Tag

<input type="checkbox"/> License	Billing	Purchased	In Use	Balance	Alerts	Actions
<input type="checkbox"/> FPR1010 URL Filtering	Prepaid	10	0	+ 10		Actions ▼
<input type="checkbox"/> FPR4110 Threat Defense Malware Protection	Prepaid	1	0	+ 1		Actions ▼
<input type="checkbox"/> FPR4110 Threat Defense Threat Protection	Prepaid	1	0	+ 1		Actions ▼
<input type="checkbox"/> FPR4110 Threat Defense URL Filtering	Prepaid	1	0	+ 1		Actions ▼
<input type="checkbox"/> HyperFlex Data Platform Enterprise Edition Subscription	Prepaid	2	0	+ 2		Actions ▼
<input type="checkbox"/> ISE Apex Session Licenses	Prepaid	1	0	+ 1		Actions ▼
<input type="checkbox"/> ISE Base Session Licenses	Prepaid	10	0	+ 10		Actions ▼
<input type="checkbox"/> ISE Plus License	Prepaid	10	0	+ 10		Actions ▼
<input type="checkbox"/> Threat Defense Virtual Malware Protection	Prepaid	10	1	+ 9		Actions ▼
<input type="checkbox"/> Threat Defense Virtual Threat Protection	Prepaid	10	1	+ 9		Actions ▼

10 ▼

Showing Page 5 of 7 (86 Records) |◀◀▶▶|

Etapa 4. Para confirmar que o FMC foi registrado na Virtual Account correta, navegue até **System>Licenses>Smart License**:

Smart License Status

[Cisco Smart Software Manager](#)

Usage Authorization: Authorized (Last Synchronized On Jun 10 2020)

Product Registration: Registered (Last Renewed On Jun 10 2020)

Assigned Virtual Account: **Mex-AMP TAC**

Export-Controlled Features: Enabled

Cisco Success Network: [Enabled](#) ⓘCisco Support Diagnostics: [Disabled](#) ⓘ

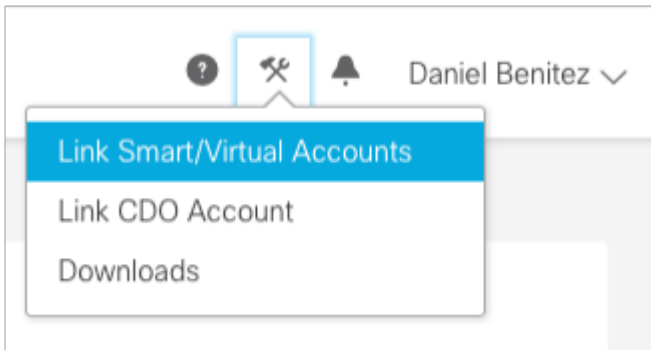
Smart Licenses

License Type/Device Name	License Status
> Firepower Management Center Virtual (1)	
> Base (1)	
> Malware (1)	
> Threat (1)	
> URL Filtering (1)	
> AnyConnect Apex (1)	
> AnyConnect Plus (1)	
AnyConnect VPN Only (0)	

Note: Container Instances of same blade share feature licenses

Vincule suas contas ao SSE e registre os dispositivos.

Etapa 1. Ao fazer login em sua conta SSE, você precisa vincular sua Smart Account à sua conta SSE, para isso, você precisa clicar no ícone de ferramentas e selecionar **Vincular Contas**.



Quando a conta estiver vinculada, você verá a Smart Account com todas as Virtual Accounts nela.

Registrar os dispositivos no SSE

Etapa 1. Verifique se estes URLs são permitidos em seu ambiente:

Região dos EUA

- api-sse.cisco.com
- eventing-ingest.sse.itd.cisco.com

Região da UE

- api.eu.sse.itd.cisco.com
- eventing-ingest.eu.sse.itd.cisco.com

Região APJ

- api.apj.sse.itd.cisco.com
- eventing-ingest.apj.sse.itd.cisco.com

Etapa 2. Faça login no portal SSE com este URL <https://admin.sse.itd.cisco.com>. Navegue até **Cloud Services** e habilite ambas as opções **Eventing** e **Cisco XDR threat response**, como mostrado na imagem a seguir:

Cloud Services for Sourcefire Support

Cisco SecureX threat response

Cisco SecureX threat response enablement allows you to utilize supported devices in the course of a cybersecurity response. It also allows this platform to send high fidelity security events and observations to Threat Response.

Eventing

Eventing allows you to collect and view events in the cloud.

Etapa 3. Faça login no Firepower Management Center e navegue até **System>Integration>Cloud Services**, habilite **Cisco Cloud Event Configuration** e selecione os eventos que deseja enviar para a nuvem:

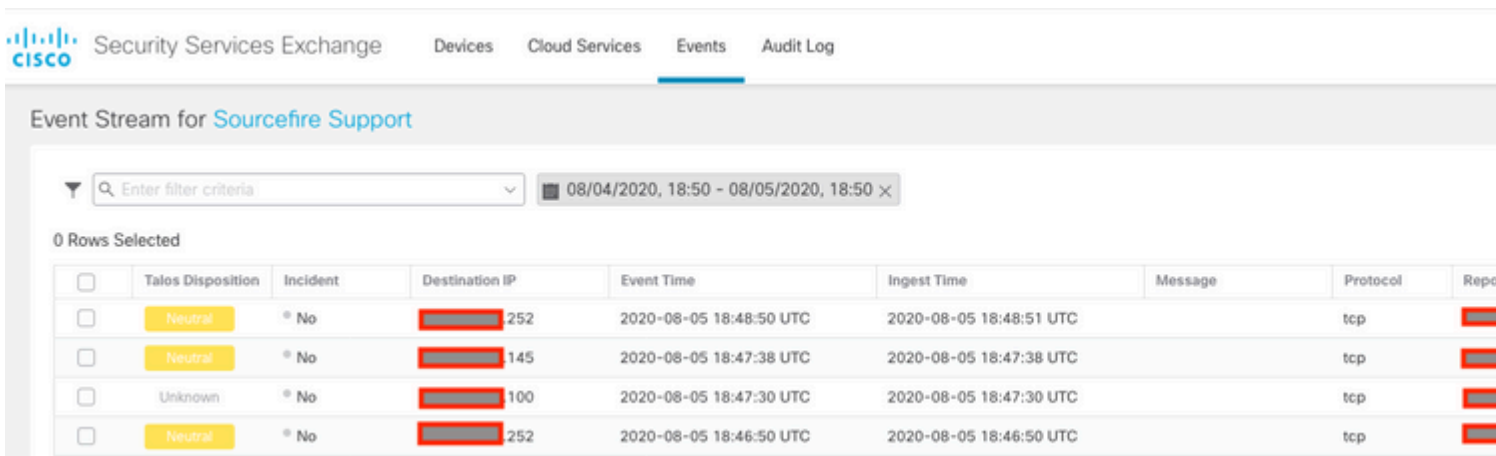
The screenshot displays the Cisco Firepower Management Center configuration interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. Below this, there are tabs for 'Cloud Services', 'Realms', 'Identity Sources', 'eStreamer', 'Host Input Client', and 'Smart Software Satellite'. The main content area is divided into four configuration panels:

- URL Filtering:** Features a toggle switch that is turned on. Below it, there are options to 'Enable Automatic Updates' (checked), 'Query Cisco Cloud for Unknown URLs' (checked), and a dropdown menu for 'Cached URLs Expire' set to 'Never'. A link for 'Dispute URL categories and reputations' is also present.
- AMP for Networks:** Features a toggle switch that is turned on. Below it, there are options to 'Enable Automatic Local Malware Detection Updates' (checked), 'Share URI from Malware Events with Cisco' (checked), and 'Use Legacy Port 32137 for AMP for Networks' (unchecked).
- Cisco Cloud Region:** Features a dropdown menu for 'Region' set to 'us-east-1 (US Region)'. A note below explains that this setting determines where events are sent to the cloud.
- Cisco Cloud Event Configuration:** Features three toggle switches, all of which are turned on: 'Send high priority Connection Events to the cloud', 'Send File and Malware Events to the cloud', and 'Send Intrusion Events to the cloud'. There are also links to view the Cisco Cloud configuration and events in Cisco Threat Response.

Etapa 4. Você pode voltar ao portal SSE e confirmar que agora pode ver os dispositivos inscritos no SSE:



Os eventos são enviados pelos dispositivos de FTD, navegue até os **Eventos** no portal SSE para verificar os eventos enviados pelos dispositivos para o SSE, como mostrado na imagem:



Verificar

Valide se os FTDs geram eventos (malware ou intrusão), para que os eventos de intrusão naveguem até **Análise>Arquivos>Eventos de malware**, para eventos de intrusão, navegue para **Análise>Invasão>Eventos**.

Valide se os eventos estão registrados no portal SSE conforme mencionado na seção **Registrar os dispositivos no SSE** etapa 4.

Verifique se as informações são exibidas no painel do Cisco XDR ou verifique os logs de API para que você possa ver o motivo de uma possível falha de API.

Troubleshooting

Detectar problemas de conectividade

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

```
ActionQueueScrape.pl[19094]: [SF::SSE::Enrollment] canConnect: System (/usr/bin/curl -s --connect-timeout
```

Nesse caso, o código de saída 28 significa que a operação atingiu o tempo limite e precisamos verificar a conectividade com a Internet. Você também deve ver o código de saída 6, que significa problemas com a resolução DNS

Problemas de conectividade devido à resolução 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'
```

Esta saída mostra que o dispositivo não pode resolver o URL <https://api-sse.cisco.com>; neste caso, precisamos validar 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
```

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

```
> 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
```

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

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

Depois que essa conectividade puder ser testada novamente e dessa vez, a conexão será 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

O FMC e o FTD precisam de uma conexão com os URLs SSE em sua interface de gerenciamento. Para testar a conexão, insira estes comandos na CLI do Firepower 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; includeSubdomains;
```

Observação: você recebe a mensagem 403 Forbidden, pois 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

Você pode verificar 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, você pode usar esse comando, este é um exemplo de conexão inválida:

```
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, você pode ver que 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 FTD para SEE, 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 FTD:

```
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
```

Nos logs connector.log:

```
time="2020-04-13T14:34:02.88472046-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connect] failed to connect to https://eventing-ingest.sse.itd.cisco.com:53426"
time="2020-04-13T14:38:18.244707779-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connect] failed to connect to https://eventing-ingest.sse.itd.cisco.com:53426"
time="2020-04-13T14:42:42.564695622-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connect] failed to connect to https://eventing-ingest.sse.itd.cisco.com:53426"
time="2020-04-13T14:47:48.484762429-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connect] failed to connect to https://eventing-ingest.sse.itd.cisco.com:53426"
time="2020-04-13T14:52:38.404700083-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connect] failed to connect to https://eventing-ingest.sse.itd.cisco.com:53426"
```

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> devem ser alterados, por isso a recomendação é permitir o tráfego para o Portal SSE com base na URL em vez de nos 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 FTD 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
```

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.