# 排除Firepower设备上的云配置故障

## 目录


简介

先决条件

- 要求
- 使用的组件

背景信息

- 网络图

问题

故障排除

- 选项1.缺少DNS配置
- 选项2. DNS无法解析https://api-sse.cisco.com
- 更多故障排除选项
- 已知问题

[视频] Firepower — 将FMC注册到SSE


## 简介

本文档介绍Firepower系统触发运行状况警报的常见场景：威胁数据更新思科云配置失败。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- 云集成
- Firepower传感器模块
- Firepower威胁防御
- Firepower 管理中心
- DNS解析和代理连接
- 思科威胁响应(CTR)集成

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科智能帐户门户
- 思科安全服务交换(SSE)
- Firepower管理中心(FMC)版本6.4.0或更高版本
- Firepower威胁防御(FTD)或Firepower传感器模块(SFR)版本6.4.0或更高版本

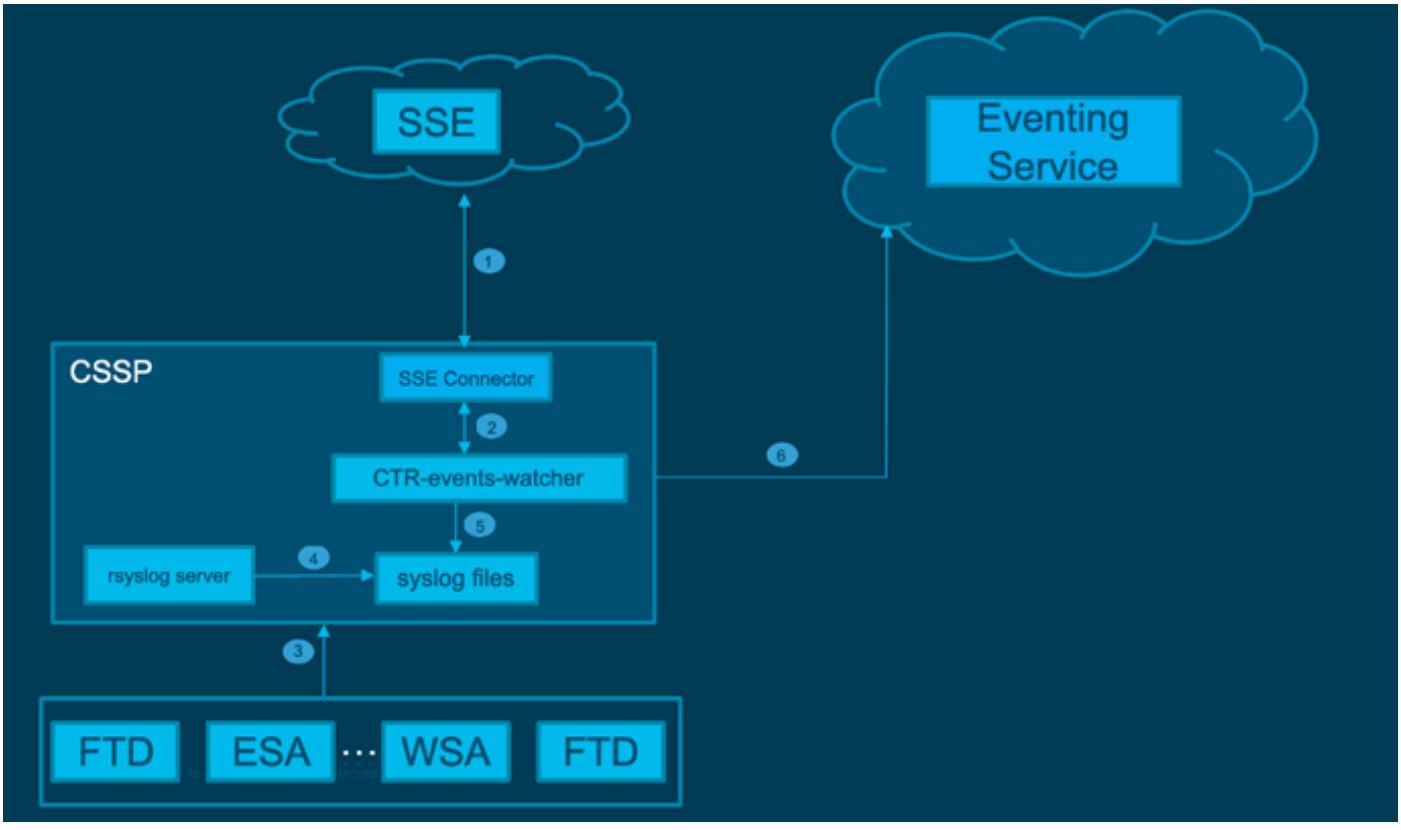
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

# 背景信息

由于FTD无法与api-sse.cisco通信，因此观察到Cloud Configuration错误。com。这是Firepower设备与SecureX和云服务集成所需的站点。

此警报是快速威胁遏制(RTC)功能的一部分。默认情况下，在新的Firepower版本上启用此功能，其中FTD必须与Internet上的api-sse.cisco.com通信。如果此通信不可用，FTD运行状况监控模块将显示以下错误消息：威胁数据更新 — 思科云配置 — 故障。

## 网络图



# 问题

Cisco bug ID CSCvr46845说明了Firepower系统何时触发Health Alert Cisco Cloud Configuration - Failure。此问题通常与FTD和api-sse.cisco之间的连接有关。com。但是，警报是通用的，可以指向各种问题，即使与连接有关，但位于不同的环境中。

有两种主要可能的方案：

场景1.在未启用云集成的情况下，由于不允许连接到云门户，因此预期出现此警报。

场景2：在启用云集成的情况下，需要进行更详细的分析，以消除涉及连接故障的情况。

下一个映像中的运行状况故障警报示例：




运行状况故障警报示例

# 故障排除

方案1的解决方案。由于FTD无法与https://通信，因此观察到云配置错误api-sse.cisco.com/。要禁用Cisco Cloud Configuration-Failure警报，请导航到System > Health > Policy > Edit policy > Threat Data Updates on Devices。选择Enabled(Off)> Save Policy > Exit。有关内联配置，请参阅Firepower威胁防御的内联集和被动接口指南。

方案2的解决方案。必须启用云集成时：

用于故障排除的有用命令：

<#root>

```
curl -v -k https://api-sse.cisco.com
```

```
 <-- To verify connection with the external site
```

```
nslookup api-sse.cisco.com

 <-- To dicard any DNS error

/ngfw/etc/sf/connector.properties

 <-- To verify is configure properly the FQDN settings

netstat -na | grep 8989

<-- To verify the outbound connection to the cloud on port 8989/tcp is ESTABLISHED

netstat -na | grep 443

<-- To verify the outbound connection to the cloud on port 443/tcp is ESTABLISHED
```

## 选项1.缺少DNS配置

步骤1.检验FTD上是否配置了DNS。如果没有DNS配置，请按照以下步骤操作：

```
> show network
```

步骤2.通过运行以下命令添加DNS:

```
> configure network dns servers dns_ip_addresses
```

配置DNS后，运行状况警报会得到解决，设备将显示为运行正常。反映更改并配置适当的DNS服务器之前会短暂经过一段时间。

## 选项2. DNS无法解析https://api-sse.cisco.com

运行curl命令。如果设备无法到达云站点，则显示与本示例类似的输出。

```
<#root>
FTD01:/home/ldap/abbac#

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'**

---



注意：运行curl命令后可能会出现DNS问题。如果是，则使用选项1中的相同方法进行故障排除。验证DNS配置是否已正确设置。

---

正确的curl输出必须是：

<#root>

```
root@fp:/home/admin# curl -v -k https://api-sse.cisco.com
* Rebuilt URL to: https://api-sse.cisco.com/
* Trying 10.6.187.110...
* Connected to api-sse.cisco.com (10.6.187.110) 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, Server finished (14):
* 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 SSL 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, 30 Dec 2020 21:41:15 GMT
< Content-Type: text/plain; charset=utf-8
< Content-Length: 9
```

```
< Connection: keep-alive
< Keep-Alive: timeout=5
< ETag: "5fb40950-9"
< Cache-Control: no-store
< Pragma: no-cache
< Content-Security-Policy: default-src https: ;
< X-Content-Type-Options: nosniff
< X-XSS-Protection: 1; mode=block
< X-Frame-Options: SAMEORIGIN
< Strict-Transport-Security: max-age=31536000; includeSubDomains
<

* Connection #0 to host api-sse.cisco.com left intact


Forbidden
```

卷曲到服务器主机名：

<#root>

#

**curl -v -k**

```
 https://cloud-sa.amp.cisco.com
*   Trying 10.21.117.50...
* TCP_NODELAY set
* Connected to cloud-sa.amp.cisco.com (10.21.117.50) port 443 (#0)
* ALPN, offering http/1.1
* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH
* successfully set certificate verify locations:
*   CAfile: /etc/ssl/certs/ca-certificates.crt
  CApath: none
* TLSv1.2 (OUT), TLS header, Certificate Status (22):
* TLSv1.2 (OUT), TLS handshake, Client hello (1):
```

使用nslookup、telnet和ping命令等基本连接工具验证思科云站点的正确DNS解析。

---

注意：Firepower云服务必须在端口8989/tcp上拥有到云的出站连接。

---

将nslookup应用于服务器主机名。

```
# nslookup cloud-sa.amp.sourcefire.com
# nslookup cloud-sa.amp.cisco.com
# nslookup api.amp.sourcefire.com
# nslookup panacea.threatgrid.com
```

<#root>

```
root@fp:/home/admin#

nslookup api-sse.cisco.com

Server: 10.25.0.1
Address: 10.25.0.1#53

Non-authoritative answer:
api-sse.cisco.com canonical name = api-sse.cisco.com.akadns.net.
Name: api-sse.cisco.com.akadns.net
Address: 10.6.187.110
Name: api-sse.cisco.com.akadns.net
Address: 10.234.20.16
```

与AMP Cloud的连接问题可能是由于DNS解析。验证DNS设置或从FMC运行nslookup。

```
nslookup api.amp.sourcefire.com
```

Telnet

<#root>

```
root@fp:/home/admin#

telnet api-sse.cisco.com 8989

root@fp:/home/admin#

telnet api-sse.cisco.com 443

root@fp:/home/admin#

telnet cloud-sa.amp.cisco.com 443
```

ping

<#root>

```
root@fp:/home/admin#

ping api-sse.cisco.com
```

## 更多故障排除选项

验证/ngfw/etc/sf/connector.properties下的连接器属性。您必须使用正确的连接器端口(8989)和connector_fqdn以及正确的URL看到此输出。

<#root>

root@Firepower-module1:sf#

**cat /ngfw/etc/sf/connector.properties**

registration_interval=180

**connector_port=8989**

region_discovery_endpoint=https://api-sse.cisco.com/providers/sse/api/v1/regions

**connector_fqdn=api-sse.cisco.com**

有关详细信息，请参阅Firepower配置指南。

## 已知问题

Cisco Bug ID CSCvs05084 FTD Cisco Cloud Configuration Failure due to proxy。

Cisco Bug ID CSCvp56922使用update-context sse-connector API更新设备主机名和版本。

Cisco Bug ID CSCvu02123 DOC Bug:在CTR配置指南中从Firepower设备可访问URL更新为SSE。

Cisco Bug ID CSCvr46845 ENH:运行状况消息Cisco Cloud Configuration - Failure needs improvement。

# [视频] Firepower — 将FMC注册到SSE

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。