排除FMC与CTR集成故障

目录

简介

本文档介绍当安全服务交换(SSE)连接器进程在Firepower管理中心(FMC)或Firepower威胁防御(FTD)设备上为与思科威胁响应(CTR)集成而禁用时对其进行故障排除的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- FMC
- FTD
- 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：

- 软件版本6.4.0或更高版本上的FMC
- 软件版本6.4.0或更高版本上的FTD
- 思科安全服务交换
- CTR帐户

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

SSEConnector

SSEConnector是在6.4.0之后在Firepower设备上将设备注册到SSE门户的过程。当思科云配置设置为“打开”或“关闭”时，FMC会广播到所有受管FTD。启用思科云后，SSEConnector服务将启动SSE门户和Firepower设备之间的通信。每个FTD都向FMC请求注册令牌，该令牌允许设备集成到SSE门户。此集成后，SSE环境在设备上激活，并重新配置EventHandler以将入侵事件发送到思科云。

CTR

威胁响应是一个威胁事件响应协调中心，支持并自动集成多个思科安全产品。威胁响应可加快关键安全任务：检测、调查和补救，是我们集成安全架构的重点。

威胁响应的目标是帮助网络运营团队和事件响应人员通过从思科和第三方收集并组合的所有威胁情报，了解其网络中的威胁。

但是，威胁响应最能降低安全工具的复杂性，帮助识别威胁并加快事件响应速度。

威胁响应是一个集成平台(https://visibility.amp.cisco.com/)。 系统通过“模块”工作，这些模块是独立的代码片段，处理与不同集成系统（如Threat Grid或AMP）的通信。 这些模块处理集成系统可提供的全部3项功能（丰富、本地情景和响应）。

CTR可用于什么？

- 事件响应
- 调查
- 威胁搜索
- Incident Management

搜索可观察信息时，所有配置的模块都要求负责搜索这些可观察信息记录的系统。然后，他们获取提供的响应并将其传回威胁响应，然后从所有模块（本例中为Stealthwatch模块）获取收集的结果，对数据进行分类和组织，并以图形形式显示。

要将CTR与不同产品集成，还需要另外两个门户“https://castle.amp.cisco.com/”(Castle)和“https://admin.sse.itd.cisco.com/app/devices”（安全服务交换）

城堡门户

您可以在此处管理思科安全帐户：

思科安全帐户允许您管理思科安全产品组合中的多个应用。根据您的许可授权，这包括：

- 面向终端的 AMP
- Threat Grid
- 威胁响应

安全服务交换门户

此门户是CTR门户的扩展，在该门户中，您可以管理已在CTR门户中注册的设备，因此，您可以在此处创建集成产品所需的令牌。

当您将某些思科安全产品与思科威胁响应集成时，安全服务交换可提供设备、服务和事件管理，包括以下产品和功能：

- 管理与思科威胁响应集成的安全管理设备列表。
- 从集成的Cisco Firepower设备收集事件数据，以便（自动或手动）将其转发到思科威胁响应。

故障排除

验证是否已启用云服务

在FMC上，首先在系统>许**可证>智能许**可证上验证您未处于评估模式。

现在，在**智能软件卫星**选项卡上的**系统> 集成**下验证所选选项是否为**直接连接到Cisco智能软件管理器**，因为气隙环境不支持此功能。

导航至Cloud Services选**项卡**上的System > Integration，并检查Cisco Cloud Event Configuration选项是否已打开。

验证FMC/FTD和SSE门户之间的连接

由于IP可以更改，因此需要允许以下下一个URL:

美国地区

- api-sse.cisco.com
- est.sco.cisco.com（跨地域通用）
- mx*.sse.itd.cisco.com（目前仅mx01.sse.itd.cisco.com）
- dex.sse.itd.cisco.com（为了客户成功）
- eventing-ingest.sse.itd.cisco.com（用于CTR和CDO）

欧盟地区

- api.eu.ss e.itd.cisco.com
- est.sco.cisco.com（跨地域通用）
- mx*.eu.sse.itd.cisco.com(目前仅mx01.eu.sse.itd.cisco.com)
- dex.eu.sse.itd.cisco.com（为了客户成功）
- eventing-ingest.eu.sse.itd.cisco.com（用于CTR和CDO）

亚太及日本地区

- api.apj.sse.itd.cisco.com
- est.sco.cisco.com（跨地域通用）
- mx*.apj.sse.itd.cisco.com（目前仅mx01.apj.sse.itd.cisco.com）
- dex.apj.sse.itd.cisco.com（为了客户成功）

- eventing-ingest.apj.sse.itd.cisco.com（用于CTR和CDO）

FMC和FTD都需要连接到其管理界面上的SSE URL，以测试连接，请在具有根访问权限的Firepower CLI上输入以下命令：

```
curl -v https://api-sse.cisco.com/providers/sse/services/registration/api/v2/clients --cacert
/ngfw/etc/ssl/connectorCA.pem
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
```

运行每个命令后，您必须在连接结束时看到以下行：**Connection #0 to host "URL"（连接到主机“URL”）保持原状。**

如果连接超时或您未在输出中收到此行，请验证管理接口是否允许访问这些URL，以及没有阻止或修改设备与这些URL之间连接的上游设备。

可使用以下命令绕过证书检查：

```
root@ftd01:~# curl -v -k https://api-sse.cisco.com
* Rebuilt URL to: https://api-sse.cisco.com/
* Trying 52.4.85.66...
* Connected to api-sse.cisco.com (52.4.85.66) 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 c hain (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;
```

> **注意**：您会收到403 Forbidden消息，因为从测试发送的参数不是SSE期望的，但这足以验证连接。

验证SSEConnector状态

您可以按如下所示验证连接器属性。

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

为了检查SSConnector和EventHandler之间的连接，您可以使用此命令，以下是连接错误的示例：

```
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
```

在已建立连接的示例中，您可以看到流状态已连接：

```
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.soc
```

验证发送到SSE门户和CTR的数据

要从FTD设备发送事件以查看TCP连接，需要与https://eventing-ingest.sse.itd.cisco.com建立TCP连接。以下是SSE门户和FTD之间未建立连接的示例：

```
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)
```

在connector.log日志中：

```
time="2020-04-13T14:34:02.88472046-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp 18.205.49.246:443: getsockopt: connection timed out"
time="2020-04-13T14:38:18.244707779-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp 100.25.93.234:443: getsockopt: connection timed out"
time="2020-04-13T14:42:42.564695622-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp 18.205.49.246:443: getsockopt: connection timed out"
time="2020-04-13T14:47:48.484762429-05:00" level=error msg="[firepower.cisco.com][events.go:90
```

```
events:connectWebSocket] dial tcp 100.25.93.234:443: getsockopt: connection timed out"
time="2020-04-13T14:52:38.404700083-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp 100.25.93.234:443: getsockopt: connection timed out"
```

> **注意**：注意显示18.205.49.246和18.205.49.246的IP地址属于https://eventing-ingest.sse.itd.cisco.com，这就是建议根据URL而不是IP地址允许流量到SSE门户的原因。

如果未建立此连接，则事件不会发送到SSE门户，这是FTD和SSE门户之间已建立连接的示例：

```
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 192.168.1.200:56495->ec2-35-172-147-
246.compute-1.amazonaws.com:https (ESTABLISHED)
```

常见问题

升级到6.4后，SSE连接器不与SSE门户通信。Connector.log提供与事件类似的错误：(*Service)。Start] Could not connect to ZeroMQ PUSH endpoint:无法拨号到 \"ipc:///ngfw/var/sf/run/EventHandler_SSEConnector.sock\"拨号unix /ngfw/var/sf/run/EventHandler_SSEConnector.sock:连接:没有此类文件或目录\n

重新启动SSEConnector服务：

1)sudo pmtool disablebyid SSEConnector

2)sudo pmtool enablebyid SSEConnector

3)重新启动设备。重新启动后，设备与云通信。

重要日志文件位置

调试日志 — 显示成功连接或失败消息

```
/ngfw/var/log/connector/connector.log
```

配置设置

```
/ngfw/etc/sf/connector.properties
```

配置设置

```
curl localhost:8989/v1/contexts/default
```

相关信息

- https://docs.castle.amp.cisco.com/CiscoSecurityAccountUserGuide.pdf
- 技术支持和文档 - Cisco Systems