排除安全防火墙与安全服务交换的集成故障

目录

简介

先决条件

- 要求
- 使用的组件

故障排除

- 连接性
- 注册
  - 验证注册
  - 安全服务交换端验证
- 事件
- 对未在安全服务交换中处理的事件的故障排除

简介

本文档介绍如何对思科安全防火墙与安全服务交换(SSX)的集成进行故障排除。

先决条件

要求

建议掌握下列主题的相关知识：

- 安全防火墙管理中心(FMC)
- 思科安全防火墙

使用的组件

- 思科安全防火墙 — 7.6.0
- 安全防火墙管理中心(FMC)- 7.6.0
- 安全服务交换(SSX)

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。

故障排除

连接性

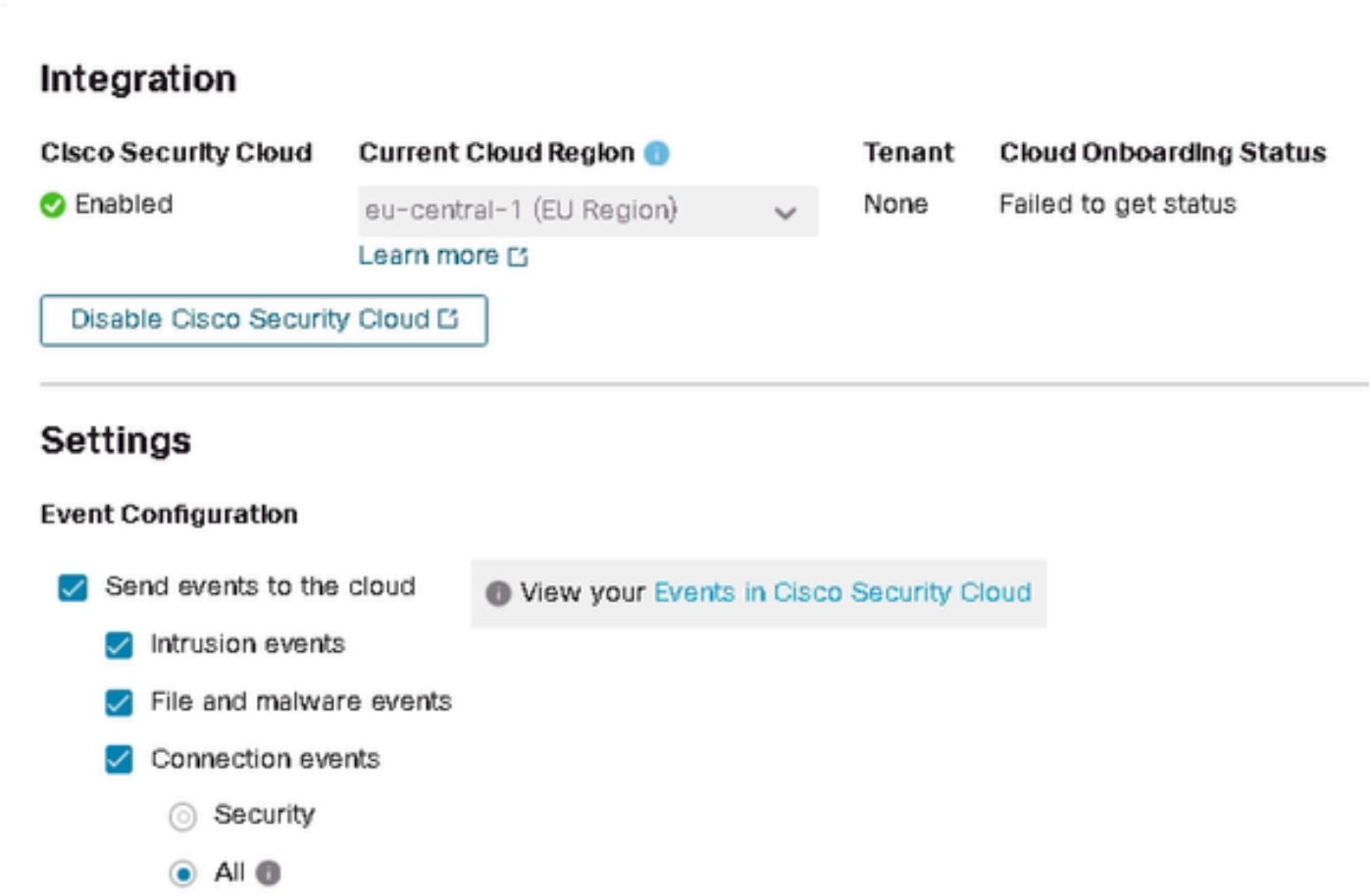
主要要求是允许从注册设备流向这些地址的HTTPS流量：

- 美国地区：
  - api-sse.cisco.com
  - mx*.sse.itd.cisco.com
  - dex.sse.itd.cisco.com
  - eventing-ingest.sse.itd.cisco.com
  - registration.us.ss e.itd.cisco.com
  - defenseorchestrator.com
  - edge.us.cd o.cisco.com
- 欧盟地区：
  - api.eu.ss e.itd.cisco.com
  - mx*.eu.sse.itd.cisco.com
  - dex.eu.ss e.itd.cisco.com
  - eventing-ingest.eu.ss e.itd.cisco.com
  - registration.eu.ss e.itd.cisco.com
  - defenseorchestrator.eu
  - edge.eu.cd o.cisco.com
- 亚洲(APJC)地区：
  - api.apj.sse.itd.cisco.com
  - mx*.apj.sse.itd.cisco.com
  - dex.apj.sse.itd.cisco.com
  - eventing-ingest.apj.sse.itd.cisco.com
  - registration.apj.sse.itd.cisco.com
  - apj.cdo.cisco.com
  - edge.apj.cdo.cisco.com
- 澳大利亚地区：
  - api.aus.sse.itd.cisco.com
  - mx*.aus.sse.itd.cisco.com

    - dex.au.ss e.itd.cisco.com
    - eventing-ingest.aus.sse.itd.cisco.com
    - registration.au.ss e.itd.cisco.com
    - aus.cdo.cisco.com
- 印度地区：
    - api.in.ss e.itd.cisco.com
    - mx*.in.sse.itd.cisco.com
    - dex.in.ss e.itd.cisco.com
    - eventing-ingest.in.ss e.itd.cisco.com
    - registration.in.ss e.itd.cisco.com
    - in.cdo.cisco.com

注册

在安全防火墙管理中心的集成>思科安全云中完成安全防火墙到安全服务Exchange的注册。



这些输出表明已成功建立到思科云的连接。

<#root>

```
root@firepower:~#
netstat -anlp | grep EventHandler_SSEConnector.sock

unix 3 [ ] STREAM CONNECTED 133064 4159/EventHandler /ngfw/var/sf/run/EventHandler_SSEConnector.sock
```

<#root>

```
root@firepower:~#
lsof -i | grep conn

connector 5301 www 6u IPv4 471679686 0t0 TCP firepower:53080->ec2-35-158-61-95.eu-central-1.compute.amaz
connector 5301 www 8u IPv6 104710 0t0 TCP *:8989 (LISTEN)
```

注册日志存储在/var/log/connector/中。

验证注册

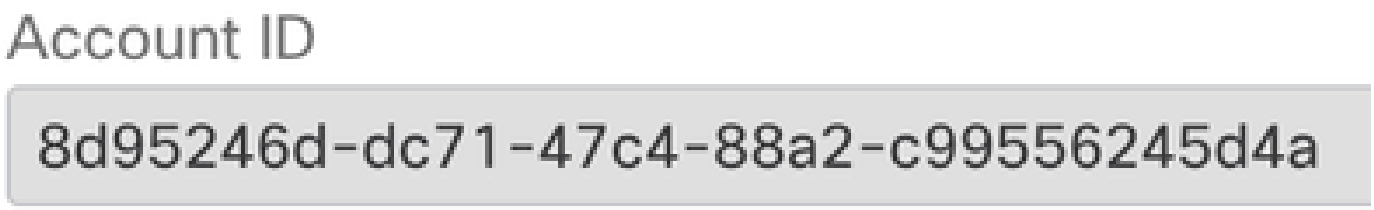
在安全防火墙端成功注册后，可以执行对localhost:8989/v1/contexts/default/tenant的API调用，以获取安全服务交换租户名称和ID。

<#root>

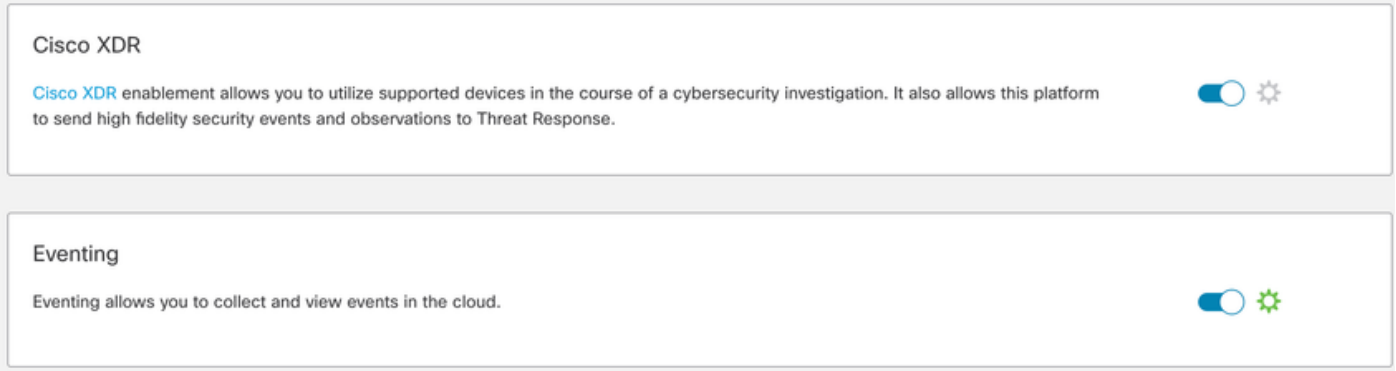
```
root@firepower:~#
curl localhost:8989/v1/contexts/default/tenant

{"registeredTenantInfo":{"companyId":"601143","companyName":"lab","domainName":"tac.cisco.com","id":"56
"Cisco - lab"
,"id":
"8d95246d-dc71-47c4-88a2-c99556245d4a"
,"spId":"AMP-EU"}]}
```

安全服务交换端验证

在安全服务交换中，导航到右上角的用户名，然后点击用户配置文件(User Profile)，确认帐户ID与之前在安全防火墙中获取的租户ID匹配。



在Cloud Services选项卡中，需要启用Eventing。此外，Cisco XDR交换机必须打开，才能使用此解决方案。



Devices选项卡包含已注册设备的列表。

每个设备的条目均可展开并包含以下信息：

- 设备ID — 对于安全防火墙，可通过查询curl -s http://localhost:8989/v1/contexts/default找到此ID | grep deviceId
- 注册日期
- IP Address
- SSX连接器版本
- 上次修改

事件

“事件”选项卡允许我们对安全防火墙发送的数据以及安全服务Exchange中处理和显示的数据执行操作。

1. 过滤事件列表并创建和保存过滤器，
2. 显示或隐藏其他表列，
3. 检查从安全防火墙设备发送的事件。

在安全防火墙和安全服务Exchange之间的集成中，支持以下事件类型：

事件类型	支持的直接集成的威胁防御设备版本	系统日志集成支持的威胁防御设备版本
入侵事件	6.4及更高版本	6.3及更高版本

事件类型	支持的直接集成的威胁防御设备版本	系统日志集成支持的威胁防御设备版本
高优先级连接事件： • 与安全相关的连接事件。 • 与文件和恶意软件事件相关的连接事件。 • 与入侵事件相关的连接事件。	6.5及更高版本	Not Supported
文件和恶意软件事件	6.5及更高版本	Not Supported

对未在安全服务交换中处理的事件的故障排除

如果观察安全防火墙管理中心中的特定事件，可能需要确定事件是否与要在安全服务交换中处理和显示的条件（与入侵、文件/恶意软件和连接事件相关的条件）匹配。

通过查询localhost:8989/v1/contexts/default确认事件正在发送到云，可以确定是否将事件发送到云。

<#root>

```
root@firepower:~#

curl localhost:8989/v1/contexts/default



...

"statistics": {
 "client": [
  {
   "type": "Events",
   "statistics": {
   "ZmqStat": {
   "LastCloudConnectSuccess": "2025-01-21T10:03:13.779677978Z",
   "LastCloudConnectFailure": "2025-01-20T10:54:43.552112185Z",
   "LastCloudDisconnect": "2025-01-20T11:35:44.606352271Z",

   "TotalEventsReceived": 11464,



   "TotalEventsSent": 11463

...
```

TotalEventsReceived中接收的事件数表示适用于发送到安全防火墙处理的安全服务Exchange的事件。

TotalEventsSent中发送的事件数表示发送到思科云的事件。

如果在安全防火墙管理中心发现事件，但在安全服务交换中未发现事件，则必须验证/ngfw/var/sf/detection_engines/<engine>/中可用的事件日志。

基于使用u2dump的时间戳解码特定事件日志：

<#root>

```
root@firepower:/ngfw/var/sf/detection_engines/4ca2e696-0996-11ed-be66-77bcdf78a081/instance-1#
u2dump unified_events-1.log.1736964974 > ../fulldump.txt

root@firepower:/ngfw/var/sf/detection_engines/4ca2e696-0996-11ed-be66-77bcdf78a081/instance-1#
cd ../instance-2

root@firepower:/ngfw/var/sf/detection_engines/4ca2e696-0996-11ed-be66-77bcdf78a081/instance-2#
ls -alh | grep unified_events-1.log.1736

-rw-r--r-- 1 root root 8.3K Jan 5 08:19 unified_events-1.log.1736064964
-rw-r--r-- 1 root root 5.0K Jan 7 23:23 unified_events-1.log.1736292107
-rw-r--r-- 1 root root 16K Jan 10 03:17 unified_events-1.log.1736393796
-rw-r--r-- 1 root root 4.7K Jan 12 16:02 unified_events-1.log.1736630477
-rw-r--r-- 1 root root 4.8K Jan 13 11:10 unified_events-1.log.1736766628
-rw-r--r-- 1 root root 5.5K Jan 14 22:41 unified_events-1.log.1736865732
-rw-r--r-- 1 root root 5.5K Jan 15 18:27 unified_events-1.log.1736964964
root@firepower:/ngfw/var/sf/detection_engines/4ca2e696-0996-11ed-be66-77bcdf78a081/instance-2#
u2dump unified_events-1.log.1736964964 >> ../fulldump.txt
```

- 入侵事件

所有入侵事件都在SSX和XDR中处理和显示。确保在解码日志中，特定事件包含标志：

<#root>

```
root@firepower:/ngfw/var/sf/detection_engines/4ca2e696-0996-11ed-be66-77bcdf78a081#
grep -i "ips event count: 1" fulldump.txt

IPS Event Count: 1
```

- 文件和恶意软件事件

根据安全服务Exchange平台要求，仅处理和显示具有特定事件子类型的事件。

<#root>

```
"FileEvent":
 {
   “Subtypes”:
   {
     “FileLog”:
     {
     “Unified2ID”: 500,
     “SyslogID”: 430004
     },

     “FileMalware”:


     {

     “Unified2ID”: 502,


     “SyslogID”: 430005
     }
   }
 }
```

因此，这些已解码日志中看起来类似：

<#root>

```
root@firepower:/ngfw/var/sf/detection_engines/4ca2e696-0996-11ed-be66-77bcdf78a081#

cat fulldump.txt | grep -A 11 "Type: 502"



Type: 502(0x000001f6)


Timestamp: 0
Length: 502 bytes
Unified 2 file log event Unified2FileLogEvent
FilePolicy UUID: f19fb202-ac9e-11ef-b94a-c9dafad481cf
Sensor ID : 0
Connection Instance : 1
Connection Counter : 5930
Connection Time : 1736964963
File Event Timestamp : 1736964964
Initiator IP : 192.168.100.10
Responder IP : 198.51.100.10
```

- 连接事件

关于连接事件，没有子类型。但是，如果连接事件具有上述任何字段，则将其视为安全情报事件，并在安全服务交换中进行进一步处理。

· URL_SI_Category

· DNS_SI_Category

· IP_ReputationSI_Category

注意：如果在安全防火墙管理中心发现文件/恶意软件或连接事件，在使用u2dump解码的统一事件日志中不包含提到的子类型或参数，这意味着这些特定事件不会在安全服务交换中进行处理和显示

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）。