對安全防火牆與安全服務交換的整合進行故障排除

目錄

簡介

本檔案介紹如何對思科安全防火牆與安全服務交換(SSX)的整合進行疑難排解。

必要條件

需求

思科建議瞭解以下主題：

- 安全防火牆管理中心(FMC)
- 思科安全防火牆

採用元件

- 思科安全防火牆 — 7.6.0
- 安全防火牆管理中心(FMC)- 7.6.0
- 安全服務交換(SSX)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

疑難排解

連線

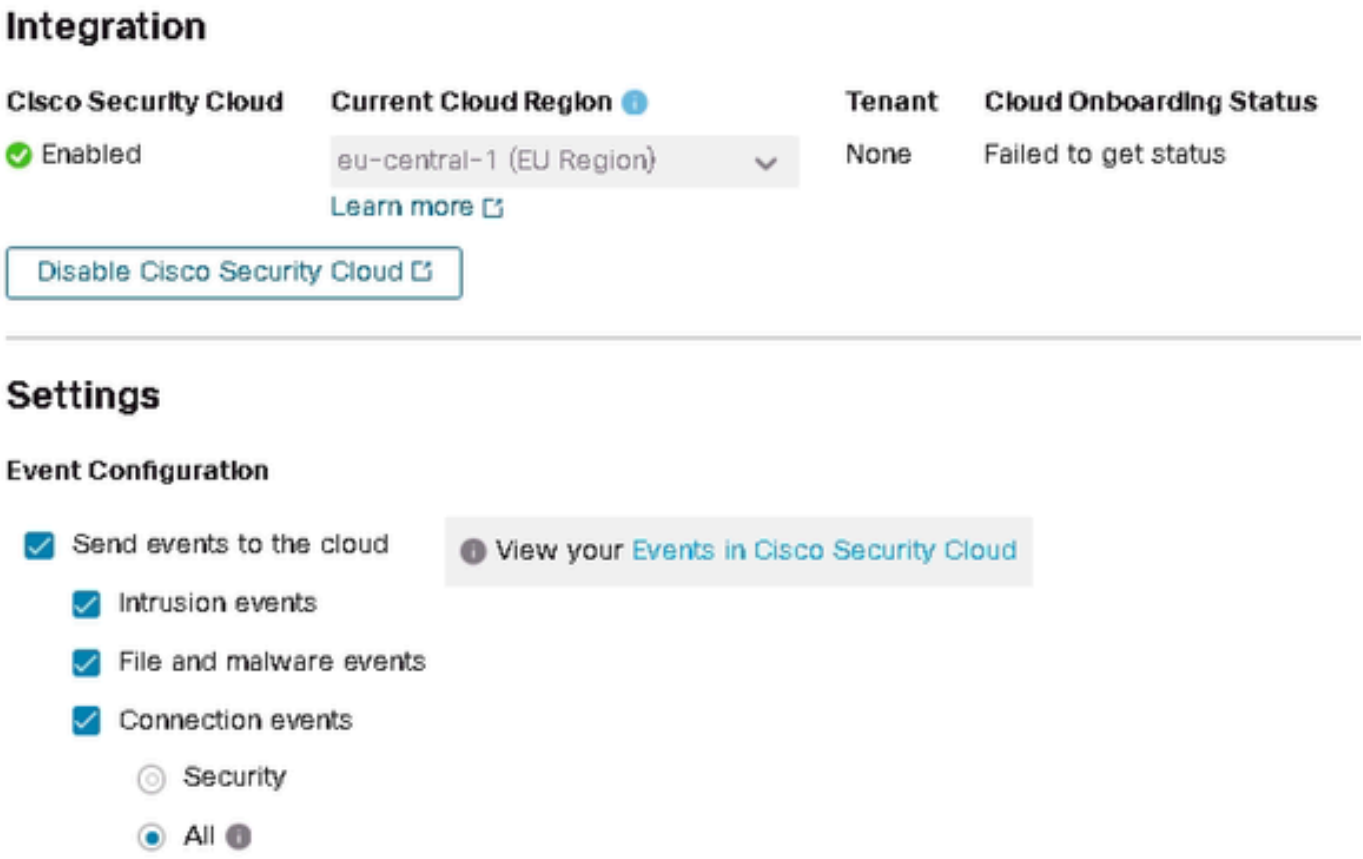
主要要求是允許從註冊裝置流向這些地址的HTTPS流量：

- 美國地區：
  - api-sse.cisco.com
  - mx*.sse.itd.cisco.com
  - dex.sse.itd.cisco.com
  - eventing-ingest.sse.itd.cisco.com
  - registration.us.sse.itd.cisco.com
  - defenseorchestrator.com
  - edge.us.cdo.cisco.com
- 歐盟地區：
  - api.eu.sse.itd.cisco.com
  - mx*.eu.sse.itd.cisco.com
  - dex.eu.sse.itd.cisco.com
  - eventing-ingest.eu.sse.itd.cisco.com
  - registration.eu.sse.itd.cisco.com
  - defenseorchestrator.eu
  - edge.eu.cdo.cisco.com
- 亞洲(APJC)地區：
  - 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
- 澳洲地區：
  - api.aus.sse.itd.cisco.com

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

註冊

在安全防火牆管理中心的整合>思科安全雲中完成安全防火牆到安全服務Exchange的註冊。



這些輸出表明已成功建立到思科雲的連線。

<#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.ama
connector 5301 www 8u IPv6 104710 0t0 TCP *:8989 (LISTEN)
```

註冊日誌儲存在/var/log/connector/中。

驗證註冊

在安全防火牆端成功註冊後，可以執行對localhost:8989/v1/contexts/default/tenant 的API呼叫，以獲取安全服務交換租戶名稱和ID。

<#root>

root@firepower:~#

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

{"registeredTenantInfo":{"companyId":"601143","companyName":"lab","domainName":"tac.cisco.com","id":"56

"Cisco - lab"

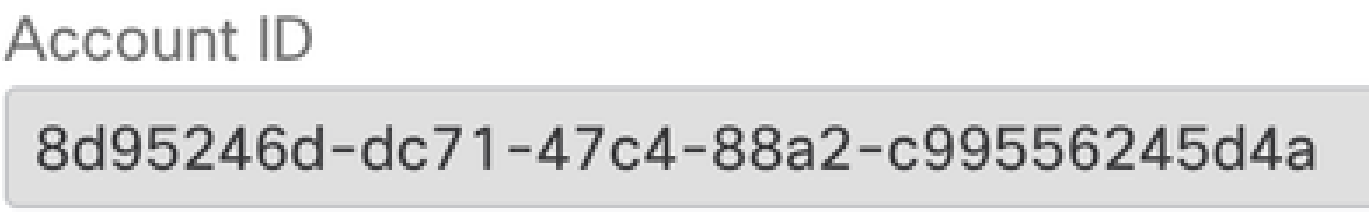
,"id":

"8d95246d-dc71-47c4-88a2-c99556245d4a"

,"spId":"AMP-EU"}]}

安全服務交換端驗證

在Security Services Exchange中，導航到右上角的使用者名稱，然後點選User Profile，確認帳戶ID與之前在安全防火牆中獲取的租戶ID匹配。



在Cloud Services頁籤中，需要啟用Eventing。此外，Cisco XDR交換器必須開啟，才能使用此解決方案。

Devices頁籤包含已註冊裝置的清單。

每個裝置的條目均可擴展，並包含以下資訊：

- 裝置ID — 對於Secure Firewall，可通過查詢curl -s http://localhost:8989/v1/contexts/default找到此ID | grep deviceId

- 登記日期
- IP 位址
- SSX聯結器版本
- 上次修改

活動

通過「事件」頁籤，我們可以對由Secure Firewall傳送並在Security Services Exchange中處理和顯示的資料執行操作。

1. 過濾事件清單並建立和儲存過濾器，
2. 顯示或隱藏其他表列，
3. 檢視從安全防火牆裝置傳送的事件。

在Secure Firewall與Security Services Exchange之間的整合中，支援以下事件型別：

事件型別	支援直接整合的威脅防禦裝置版本	支援用於系統日誌整合的威脅防禦裝置版本
入侵事件	6.4及更高版本	6.3及更高版本
高優先順序連線事件： • 與安全相關的連線事件。 • 與檔案和惡意軟體事件相關的連線事件。 • 與入侵事件相關的連線事件。	6.5及更高版本	不支援
檔案和惡意軟體事件	6.5及更高版本	不支援

對安全服務Exchange中未處理的事件進行故障排除

如果觀察安全防火牆管理中心中的特定事件，可能需要確定事件是否與要在安全服務Exchange中處理和顯示的條件（與入侵、檔案/惡意軟體和連線事件相關的條件）相匹配。

通過查詢localhost:8989/v1/contexts/default確認事件正在傳送到雲，可以確定是否將事件傳送到雲。

<#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中接收的事件數表示適用於傳送到安全防火牆處理的安全服務Exchange的事件。

TotalEventsSent中傳送的事件數表示傳送到Cisco Cloud的事件。

如果在安全防火牆管理中心（而不是安全服務交換）中發現事件，則必須驗證/ngfw/var/sf/detection_engine/<engine>/中可用的事件日志。

基於使用u2dump的時間戳解碼特定事件日誌：

<#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中處理和顯示。確保在已解碼的日誌中，特定事件包含標誌：

<#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
```

- 檔案和惡意軟體事件

根據安全服務Exchange平台要求，僅處理和顯示具有特定事件子型別的事件。

<#root>

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

     {
 “Unified2ID”: 502,

     “SyslogID”: 430005
     }
   }
 }
```

因此，這些解碼日誌中看起來類似：

<#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
```

- 連線事件

關於連線事件，沒有子型別。但是，如果連線事件具有這些欄位中的任一欄位，則將其視為安全情報事件，並在安全服務交換中進一步處理。

· URL_SI_Category

· DNS_SI_Category

· IP_ReputationSI_Category

附註：如果在Secure Firewall Management Center中看到的檔案/惡意軟體或連線事件，在使用u2dump解碼的統一事件日誌中沒有包含提到的子型別或引數，則意味著這些特定事件不會在Security Services Exchange中進行處理和顯示

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。