

Secure Firewall Integration with Security Services Exchangeのトラブルシューティング

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[トラブルシューティング](#)

[接続](#)

[登録](#)

[登録の確認](#)

[Security Services Exchange側の検証](#)

[イベント](#)

[Security Services Exchangeで処理されないイベントのトラブルシューティング](#)

はじめに

このドキュメントでは、Cisco Secure Firewall integration with Security Services Exchange(SSX)のトラブルシューティング方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- セキュアファイアウォール管理センター(FMC)
- Cisco Secureファイアウォール

使用するコンポーネント

- Cisco Secureファイアウォール – 7.6.0
- セキュアファイアウォール管理センター(FMC) - 7.6.0
- セキュリティサービス交換(SSX)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

トラブルシューティング

接続

主な要件は、登録デバイスから次のアドレスへのHTTPSトラフィックを許可することです。

- 米国地域：
 - 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
- EU地域：
 - 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 (米国)
 - edge.eu.cdo.cisco.com
- アジア(APJC)地域：
 - 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
- オーストラリア地域 :
 - 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
- インド地域 :
 - 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

登録

Security Services Exchangeへのセキュアファイアウォールの登録は、Secure Firewall Management CenterのIntegration > Cisco Security Cloudで行います。

Integration

Cisco Security Cloud

✔ Enabled

Current Cloud Region ⓘ

eu-central-1 (EU Region) ▼

[Learn more](#) ↗

Tenant

None

Cloud Onboarding Status

Failed to get status

[Disable Cisco Security Cloud](#) ↗

Settings

Event Configuration

Send events to the cloud

📘 View your [Events in Cisco Security Cloud](#)

Intrusion events

File and malware events

Connection events

Security

All ⓘ

これらの出力は、シスコクラウドへの接続が正常に確立されたことを示しています。

<#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)
```

登録ログは/var/log/connector/に保存されています。

登録の確認

セキュアファイアウォール側の登録が成功すると、localhost:8989/v1/contexts/default/tenant へのAPIコールを実行してSecurity Services Exchangeのテナント名とIDを取得できます。

```
<#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"}]}
```

Security Services Exchange側の検証

Security Services Exchangeで、右上隅にあるユーザ名に移動し、User Profileをクリックして、アカウントIDがセキュアファイアウォールで取得したテナントIDと一致することを確認します。

Account ID

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

Cloud Servicesタブでは、Eventingを有効にしておく必要があります。また、このソリューションを使用する場合は、Cisco XDRスイッチをオンにする必要があります。

<p>Cisco XDR</p> <p>Cisco XDR enablement allows you to utilize supported devices in the course of a cybersecurity investigation. It also allows this platform to send high fidelity security events and observations to Threat Response.</p> <p><input checked="" type="checkbox"/> ⚙️</p>
<p>Eventing</p> <p>Eventing allows you to collect and view events in the cloud.</p> <p><input checked="" type="checkbox"/> ⚙️</p>

Devicesタブには、登録済みアプライアンスのリストが表示されます。

各デバイスのエントリは拡張可能で、次の情報が含まれています。

- デバイスID：セキュアファイアウォールの場合、このIDはcurl -s <http://localhost:8989/v1/contexts/default> | grep deviceId

- 登録年月日
- IP アドレス
- SSXコネクタバージョン
- 最終変更

イベント

イベントタブでは、セキュアファイアウォールによって送信され、処理されてSecurity Services Exchangeに表示されるデータに対してアクションを実行できます。

1. イベントのリストをフィルタリングし、フィルタを作成して保存します。
2. 追加のテーブル列の表示と非表示を切り替える
3. セキュアファイアウォールデバイスから送信されたイベントを確認します。

Secure FirewallとSecurity Services Exchange間の統合では、次のイベントタイプがサポートされています。

イベント タイプ	直接統合用にサポートされている脅威対策デバイスバージョン	syslog統合でサポートされる脅威対策デバイスバージョン
侵入イベント	6.4 以降	6.3 以降
高優先順位接続イベント： <ul style="list-style-type: none"> • セキュリティ関連の接続イベント • ファイルイベントとマルウェアイベントに関連する接続イベント。 • 侵入イベントに関連する接続イベント。 	6.5 以降	非サポート
ファイルおよびマルウェアイベント	6.5 以降	非サポート

Security Services Exchangeで処理されないイベントのトラブルシューティング

Secure Firewall Management Centerで特定のイベントを監視する場合、イベントがSecurity Services Exchangeで処理および表示される条件（侵入、ファイル/マルウェア、および接続イベントに関連する条件）と一致するかどうかを判断する必要があります。

localhost:8989/v1/contexts/default のクエリーを実行してイベントがクラウドに送信されていること
の確認 (イベントがクラウドに送信されているかどうかを確認できる)

```
<#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で受信したイベントの数は、セキュアファイアウォールによって処理される Security Services Exchangeへの送信に適用できるイベントを意味します。

TotalEventsSentで送信されたイベントの数は、シスコクラウドに送信されたイベントを意味します。

Secure Firewall Management Center(FMC)でイベントが見られるが、Security Services Exchangeでは見られない場合、/ngfw/var/sf/detection_engines/<engine>/で使用可能なイベントログを確認する必要があります。

u2dumpを使用したタイムスタンプデコード固有のイベントログに基づきます。

```
<#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
```

- 侵入イベント

すべての侵入イベントが処理され、SSXおよびXDRに表示されます。デコードされたログで、特定のイベントにフラグが含まれていることを確認します。

```
<#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
```

- ファイルおよびマルウェアイベント

Security Services Exchangeプラットフォームの要件に基づき、特定のイベントサブタイプを持つイベントのみが処理および表示されます。

```
<#root>
```

```
"FileEvent":
{
  "Subtypes":
  {
    "FileLog":
    {
      "Unified2ID": 500,
      "SyslogID": 430004
    },
    "FileMalware":
    {
      "Unified2ID": 502,
      "SyslogID": 430005
    }
  }
}
```



```
}  
}
```

したがって、デコードされた次のログのようになります。

```
<#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
```

- 接続イベント

接続イベントには、サブタイプはありません。ただし、接続イベントにこれらのフィールドのいずれかが含まれている場合、その接続イベントはセキュリティインテリジェンスイベントと見なされ、Security Services Exchangeでさらに処理されます。

- URL_SI_Category
- DNS_SI_Category
- IP_ReputationSI_Category

 注:Secure Firewall Management Centerで見られるファイル/マルウェアまたは接続イベントに、u2dumpでデコードされた統合イベントログに前述のサブタイプやパラメータが含まれていない場合、これらの特定のイベントは処理されず、Security Services Exchangeに表示されないことを意味します

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。