CTRとのFMC統合のトラブルシューティング

内容

概要

このドキュメントでは、Cisco Threat Response(CTR)との統合のためにFirepower Management Center(FMC)またはFirepower Threat Defense(FTD)デバイスでセキュリティサービス交換(SSE)コネクタプロセスが無効になった場合のトラブルシューティング手順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。

- FMC
- FTD
- CTR統合

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ソフトウェアバージョン6.4.0以降のFMC
- ソフトウェアバージョン6.4.0以降のFTD

- Cisco Security Services Exchange
- CTRアカウント

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、初期（デフォルト）設定の状態から起動しています。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。

背景説明

SSEConnector

SSEConnectorは、6.4.0以降のFirepowerデバイスでデバイスをSSEポータルに登録するプロセスです。FMCは、Cisco Cloudの設定が[On]または[Off]に設定されている場合、すべての管理対象FTDにブロードキャストします。Cisco Cloudが有効になると、SSEConnectorサービスはSSEポータルとFirepowerデバイス間の通信を開始します。各FTDは、デバイスをSSEポータルに統合できる登録トークンをFMCに要求します。この統合の後、SSEコンテキストがデバイスでアクティブになり、侵入イベントをCisco Cloudに送信するようにEventHandlerが再設定されます。

CTR

Threat Responseは、複数のシスコセキュリティ製品間の統合をサポートおよび自動化する、脅威インシデント対応オーケストレーションハブです。脅威への対応により、主なセキュリティタスクを迅速化：検出、調査、および修復は、統合セキュリティアーキテクチャの重要な要素です。

脅威への対応の目的は、シスコとサードパーティが収集および統合したすべての脅威インテリジェンスによって、ネットワーク運用チームとインシデント対応担当者がネットワーク上の脅威を理解できるようにすることです。

しかし、Threat Responseは、セキュリティツールの複雑さを軽減し、脅威の特定を支援し、インシデント対応を迅速化するように設計されています。

Threat Responseは統合プラットフォームです(https://visibility.amp.cisco.com/)。 このシステムは、「モジュール」を介して動作します。これは、異なる統合システム（Threat Grid、AMPなど）との通信を処理する独立したコードです。 これらのモジュールは、統合システムが提供できる3つの機能（エンリッチメント、ローカルコンテキスト、および応答）すべてを処理します。

CTRは何に使用できますか。

- インシデント対応
- 調査
- 脅威追跡
- インシデント管理

監視可能なデータを検索する際には、すべての設定済みモジュールが、その観測量の記録を検索する責任があるシステムに問い合わせます。次に、指定された応答を取得して脅威応答に渡し、すべてのモジュール（この場合はStealthwatchモジュール）から収集された結果を取得し、データをソートしてグラフに表示します。

異なる製品とCTRを統合するには、2つのポータル「https://castle.amp.cisco.com/」(Castle)と「https://admin.sse.itd.cisco.com/app/devices」(Security Services Exchange)が必要です

キャッスルポータル

ここでは、シスコセキュリティアカウントを管理できます。

シスコセキュリティアカウントを使用すると、シスコセキュリティポートフォリオ内の複数のアプリケーションを管理できます。ライセンス付与に応じて、次の内容を含めることができます。

- AMP for Endpoints
- Threat Grid
- 脅威への対応

セキュリティサービス交換ポータル

このポータルはCTRポータルの拡張であり、CTRポータルに登録されているデバイスを管理できるため、製品の統合に必要なトークンを作成できます。

Security Services Exchangeは、特定のシスコセキュリティ製品をCisco Threat Responseに統合する際に、次の製品や機能を含むデバイス、サービス、およびイベント管理を提供します。

- Cisco Threat Responseと統合されるセキュリティ管理アプライアンスのリストを管理します。
- 統合されたCisco Firepowerデバイスからイベントデータを収集し、それを（自動的または手動で）Cisco Threat Responseに転送する準備をします。

トラブルシュート

クラウドサービスが有効になっていることを確認する

FMCで、まず、[System] > [Licenses] > [Smart Licenses]で評価モードになっていないことを確認します。

[スマートソフトウェアサテライト]タブの[システム] > [統合] で、選択したオプションが[Cisco Smart Software Managerに直接接続する] であることを確認します。この機能は工アギャップ環境ではサポートされていません。

[Cloud Services]タブで[System] > [Integration]に移動し、[Cisco Cloud Event Configuration]オプションがオンになっていることを確認します。

FMC/FTDとSSEポータルの間の接続を確認する

次のURLは、IPが変更される可能性があるため許可する必要があります。

米国地域

- api-sse.cisco.com
- est.sco.cisco.com（地域間で共通）
- mx*.sse.itd.cisco.com（現在はmx01.sse.itd.cisco.comのみ）
- dex.sse.itd.cisco.com（顧客成功用）

- eventing-ingest.sse.itd.cisco.com（CTRおよびCDO用）

EU地域

- api.eu.ss e.itd.cisco.com
- est.sco.cisco.com（地域間で共通）
- mx*.eu.sse.itd.cisco.com(現在はmx01.eu.sse.itd.cisco.comのみ)
- dex.eu.sse.itd.cisco.com（お客様の成功のために）
- eventing-ingest.eu.sse.itd.cisco.com（CTRおよびCDO用）

APJ地域

- api.apj.sse.itd.cisco.com
- est.sco.cisco.com（地域間で共通）
- mx*.apj.sse.itd.cisco.com（現在はmx01.apj.sse.itd.cisco.comのみ）
- dex.apj.sse.itd.cisco.com（顧客成功用）
- eventing-ingest.apj.sse.itd.cisco.com（CTRおよびCDO用）

FMCとFTDの両方で、管理インターフェイスのSSE URLへの接続が必要です。接続をテストするには、Firepower CLIでrootアクセスで次のコマンドを入力します。

```
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
```

各コマンドを実行した後、接続の最後に次の行が表示される必要があります。**Connection #0 to host "URL"はそのまま残ります。**

接続がタイムアウトしたり、出力にこの行が表示されない場合は、管理インターフェイスがこれらのURLへのアクセスを許可されていることと、デバイスとURL間の接続をブロックまたは変更するアップストリームデバイスがないことを確認してください。

証明書チェックは、次のコマンドでバイパスできます。

```
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：403 Forbiddenメッセージが表示されます。これは、テストから送信されたパラメータがSSEが期待するものではなく、接続を検証するのに十分であることを証明するためです。

SSEConnectorの状態の確認

コネクタのプロパティは次のように確認できます。

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

SSConnectorとEventHandlerの間の接続を確認するには、次のコマンドを使用できます。これは接続が正しくない例です。

```
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
```

確立された接続の例では、ストリームのステータスがconnectedであることがわかります。

```
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
```

SSEポータルおよびCTRに送信されるデータを確認します

FTDデバイスからイベントを送信してTCP接続を確立するには、https://eventing-ingest.sse.itd.cisco.comを使用する必要があります。これは、SSEポータルとFTD間に確立されていない接続の例です。

```
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)
```

connector.logログ：

```
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**：18.205.49.246と18.205.49.246が表示されるIPアドレスはhttps://eventing-ingest.sse.itd.cisco.comに属する可能性があることに気付き、IPアドレスではなくURLに基づいてSSEポータルへのトラフィックを許可することを推奨します。

この接続が確立されていない場合、イベントはSSEポータルに送信されません。これは、FTDとSSEポータル間で確立された接続の例です。

```
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)
```

一般的な問題

6.4へのアップグレード後、SSEコネクタはSSEポータルと通信しません。Connector.logはイベント(*Service).Start] Could not connect to ZeroMQ PUSH endpoint:\"ipc:///ngfw/var/sf/run/EventHandler_SSEConnector.sock\"にダイヤルできませんでした：dial unix /ngfw/var/sf/run/EventHandler_SSEConnector.sock:connect:no such file or directory\n"

SSEConnectorサービスを再起動します。

1)sudo pmtool disablebyid SSEConnector

2) sudo pmtool enablebyid SSEConnector

3)デバイスを再起動します。再起動すると、デバイスはクラウドと通信します。

重要なログファイルの場所

デバッグログ：正常な接続または失敗メッセージを表示します

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

コンフィギュレーション設定

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

コンフィギュレーション設定

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

関連情報

- https://docs.castle.amp.cisco.com/CiscoSecurityAccountUserGuide.pdf
- テクニカル サポートとドキュメント – Cisco Systems