Firepowerデバイスでの"；クラウド設定障害"；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、Firepowerシステムがヘルスアラート「Threat Data Updates - Cisco Cloud Configuration - Failure」をトリガーする一般的なシナリオ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。

- Firepowerシステム
- クラウドの統合
- DNS解決とプロキシ接続
- Cisco Threat Response(CTR)の統合

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。

- Firepower Management Center(FMC)バージョン6.4.0以降
- Firepower Threat Defense(FTD)またはFirepower Sensor Module(SFR)バージョン6.4.0以降
- Cisco Secure Services Exchange(SSE)
- Ciscoスマートアカウントポータル

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

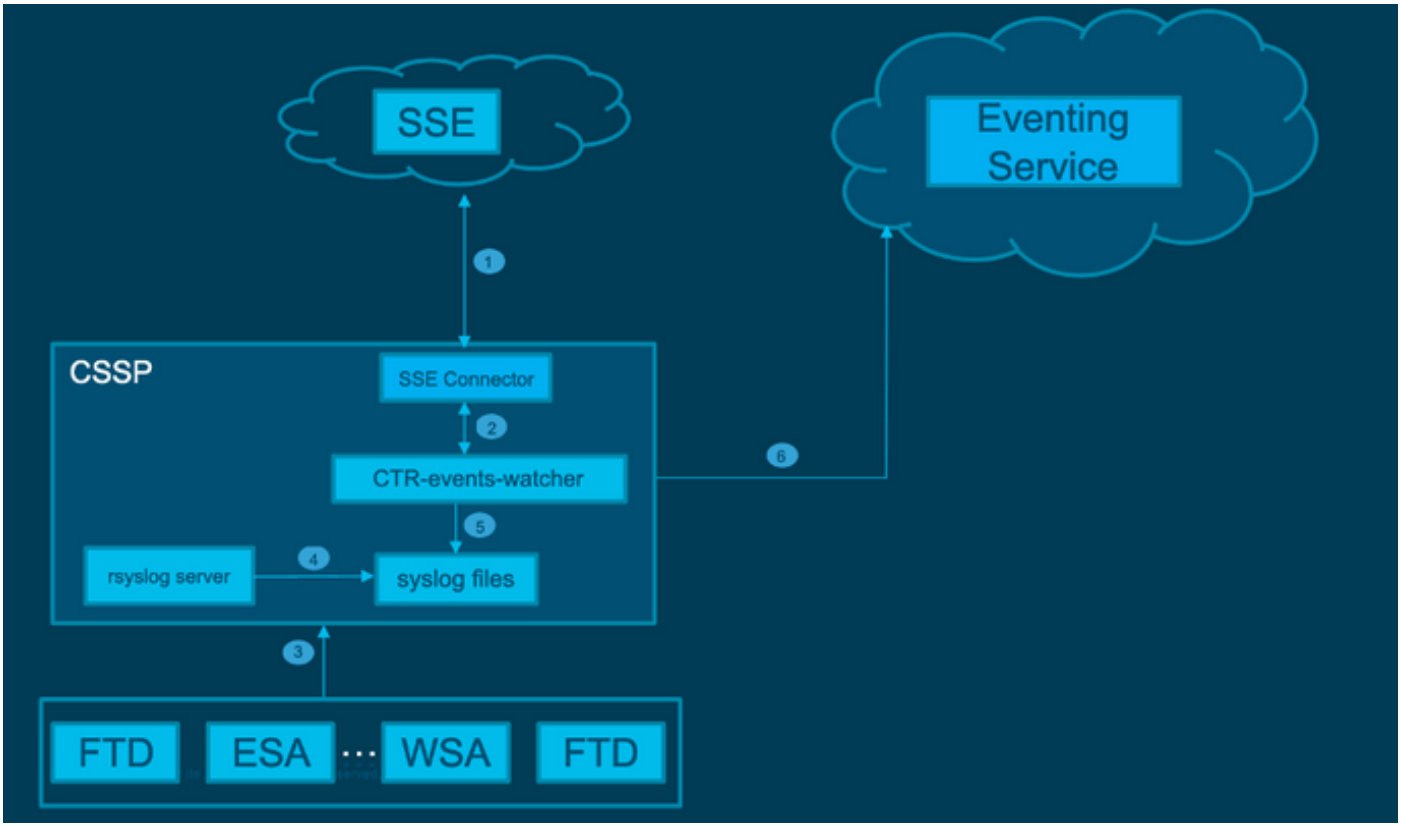
。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

FTDがapi-sse.cisco.com(FirepowerデバイスがSecureXおよびクラウドサービスと統合するために到達する必要があるサイト)と通信できないため、クラウド設定エラーが発生します。

このアラートは、Rapid Threat Containment(RTC)機能の一部です。RTCは新しいFirepowerバージョンではデフォルトで有効になっており、FTDはインターネット上でapi-sse.cisco.comと通信できる必要があります。この通信が利用できない場合、FTDのヘルスモニタモジュールは次のエラーメッセージを表示します。

ネットワーク図



問題

Cisco Bug ID CSCvr46845の機能拡張で、Firepowerシステムがヘルスアラート「Cisco Cloud Configuration - Failure」をトリガーするタイミングについて説明されているように、ほとんどの場合、問題はFTDとapi-sse.cisco.com間の接続に関連しています。ただし、このアラートは非常に汎用的であり、接続に関する問題が依然として存在する場合でも、必要なトラブルシューティングに焦点を当てることは大きな助けにはなりませんが、状況が異なります。

次の2つの主要なシナリオが考えられます。

シナリオ 1.クラウド統合が有効になっていません。クラウド統合が存在する場合は、このアラートを受け取ることが完全に期待されます。クラウドポータルへの接続が許可されていないため。

シナリオ 2.クラウド統合が有効になっています。この場合、接続障害を含むさまざまな状況を除外するために、より詳細な分析を実行する必要があります。

次の図に、Health Failure Alertの例を示します。

ヘルス障害アラートの例

トラブルシュート

シナリオ1の解決策。FTDがhttps://api-sse.cisco.com/と通信できないため、クラウド設定エラーが発生します

[Cisco Cloud Configuration-Failure]アラートを無効にするには、[System] > [Health] > [Policy] > [Edit policy] > [Threat Data Updates on Devices] > [Choose Enabled (Off)] > [Save Policy and Exit] に移動します。インライン設定のリファレンスガイドラインを次に示します。

シナリオ2の解決策。クラウド統合を有効にする必要がある場合。

トラブルシューティングに役立つ主なコマンド：

```
curl -v -k https://api-sse.cisco.com <-- To verify connection with the external site
nslookup api-sse.cisco.com <-- To dicard any DNS error
/ngfw/etc/sf/connector.properties <-- To verify is configure properly the FQDN settings
lsof -i | grep conn <-- To verify the outbound connection to the cloud on port 8989/tcp is ESTABLISHED
```

オプション 1DNS設定なし

ステップ 1：FTDでDNSサーバが設定されていることを確認します。DNS設定がない場合は、次の手順を実行できます。

```
> show network
```

ステップ 2：次のコマンドを使用してDNSサーバを追加します。

```
> configure network dns servers dns_ip_addresses
```

DNSの設定後、ヘルスアラートは固定され、デバイスは正常として表示されます。変更を反映して適切なDNSサーバを設定するには、しばらく時間がかかります。

オプション 2お客様のDNSがhttps://api-sse.cisco.comを解決できませんでした。

curl コマンドを使用してテストします。デバイスがクラウドサイトに到達できない場合は、次の例のような出力が表示されます。

```
FTD01:/home/ldap/abbac# curl -v -k https://api-sse.cisco.com
* Rebuilt URL to: https://api-sse.cisco.com/
* getaddrinfo(3) failed for api-sse.cisco.com:443
* Couldn't resolve host 'api-sse.cisco.com'
* Closing connection 0
curl: (6) Couldn't resolve host 'api-sse.cisco.com'
```

ヒント：オプション1と同じ方法でトラブルシューティングを開始します。まず、DNS設定が正しく設定されていることを確認します。curlコマンドを実行した後でDNSの問題に気づくことがあります。

正しく正しいcurl出力は、次のようになります。

```
root@fp:/home/admin# curl -v -k https://api-sse.cisco.com
* Rebuilt URL to: https://api-sse.cisco.com/
* Trying 10.6.187.110...
* Connected to api-sse.cisco.com (10.6.187.110) 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, Server finished (14):
* 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 SSL ICA G2
* SSL certificate verify result: self signed certificate in certificate chain (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, 30 Dec 2020 21:41:15 GMT
<Content-Type: text/plain; charset=utf-8
<Content-Length: 9
<Connection: keep-alive
<Keep-Alive: timeout=5
<ETag: "5fb40950-9"
<Cache-Control: no-store
<Pragma: no-cache
<Content-Security-Policy: default-src https: ;
<X-Content-Type-Options: nosniff
<X-XSS-Protection: 1; mode=block
<X-Frame-Options: SAMEORIGIN
```

```
<Strict-Transport-Security: max-age=31536000; includeSubDomains
<
* Connection #0 to host api-sse.cisco.com left intact
Forbidden
```

サーバのホスト名までカールします。

```
# curl -v -k https://cloud-sa.amp.cisco.com
*   Trying 10.21.117.50...
* TCP_NODELAY set
* Connected to cloud-sa.amp.cisco.com (10.21.117.50) port 443 (#0)
* ALPN, offering http/1.1
* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH
* successfully set certificate verify locations:
*   CAfile: /etc/ssl/certs/ca-certificates.crt
 CApath: none
* TLSv1.2 (OUT), TLS header, Certificate Status (22):
* TLSv1.2 (OUT), TLS handshake, Client hello (1):
```

nslookup、**telnet**、および **ping**コマンドなどの基本的な接続ツールを使用して、Ciscoクラウドサイトの正しいDNS解決を確認します。

> **注**:Firepowerクラウドサービスには、ポート8989/tcpでクラウドへのアウトバウンド接続が必要です。

nslookupをサーバのホスト名に適用します。

```
# nslookup cloud-sa.amp.sourcefire.com
# nslookup cloud-sa.amp.cisco.com
# nslookup api.amp.sourcefire.com
# nslookup panacea.threatgrid.com

root@fp:/home/admin# nslookup api-sse.cisco.com
Server: 10.25.0.1
Address: 10.25.0.1#53

Non-authoritative answer:
api-sse.cisco.com canonical name = api-sse.cisco.com.akadns.net.
Name: api-sse.cisco.com.akadns.net
Address: 10.6.187.110
Name: api-sse.cisco.com.akadns.net
Address: 10.234.20.16
```

AMPクラウドへの接続の問題は、DNS解決が原因である可能性があります。DNS設定を確認するか、FMCからnslookupを実行します。

```
nslookup api.amp.sourcefire.com
```

Telnet

```
root@fp:/home/admin# telnet api-sse.cisco.com 8989
root@fp:/home/admin# telnet api-sse.cisco.com 443
root@fp:/home/admin# telnet cloud-sa.amp.cisco.com 443
```

ping

```
root@fp:/home/admin# ping api-sse.cisco.com
```

その他のトラブルシューティングオプション

/ngfw/etc/sf/connector.propertiesでコネクタのプロパティを確認します。正しいコネクタポート(8989)とconnector_fqdnに正しいURLが設定された次の出力が表示されます。

```
root@Firepower-module1:sf# cat /ngfw/etc/sf/connector.properties
registration_interval=180
connector_port=8989
region_discovery_endpoint=https://api-sse.cisco.com/providers/sse/api/v1/regions
connector_fqdn=api-sse.cisco.com
```

詳細については、『Firepower設定ガイド』を参照してください。

既知の問題

Cisco Bug ID CSCvs05084 FTD：プロキシが原因のCiscoクラウド設定の失敗

Cisco Bug ID CSCvp56922:update-context sse-connector APIを使用したデバイスのホスト名とバージョンの更新

Cisco Bug ID CSCvu02123 DOC Bug:CTR設定ガイドのFirepowerデバイスからSSEに到達可能なURLの更新

Cisco Bug ID CSCvr46845 ENH：ヘルスメッセージ「Cisco Cloud Configuration - Failure」の改善が必要

[ビデオ] Firepower - SSEへのFMCの登録

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。