Firepower Management Center(FMC)でのSecurity Intelligence Feedのアップデート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、セキュリティ インテリジェンス フィードの更新に関する問題をトラブルシュートする方法について説明します。

背景

セキュリティインテリジェンスフィードは、Cisco Talos Security Intelligence and Research Group(Talos)が決定する、レピュテーションの低いIPアドレスの定期的に更新される複数のリストで構成されています。Cisco Firepowerシステムが最新の情報を使用してネットワークトラフィックをフィルタリングできるように、インテリジェンスフィードを定期的に更新しておくことが重要です。

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。

- Cisco Firepower Management Center
- セキュリティ インテリジェンス フィード

使用するコンポーネント

このドキュメントの情報は、ソフトウェアバージョン5.2以降を実行するCisco Firepower Management Center(FMC)に基づくものです。

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。

問題

セキュリティインテリジェンスフィードの更新エラーが発生しました。この障害は、Web GUIまたはCLIを使用して確認できます（以降のセクションで詳しく説明します）。

Web GUIからの問題の確認

セキュリティインテリジェンスフィードの更新が失敗すると、Firepower Management Centerにヘルスアラートが表示されます。

CLIからの問題の確認

セキュリティインテリジェンスフィードによるアップデート障害の根本原因を特定するには、Firepower Management CenterのCLIに次のコマンドを入力します。

```
admin@Sourcefire3D:~$ cat /var/log/messages
```

メッセージで次のいずれかの警告を検索します。

```
Sourcefire3D SF-IMS[2004]: [2011] CloudAgent:IPReputation [WARN] Cannot download
Sourcefire_Intelligence_Feed

Sourcefire3D SF-IMS[24085]: [24090] CloudAgent:IPReputation [WARN] Download
unsucessful: Failure when receiving data from the peer
```

解決方法

この問題のトラブルシューティングを行うには、次の手順を実行します。

1. 次のことを確認します。 **intelligence.sourcefire.com** サイトはアクティブです。ブラウザで https://intelligence.sourcefire.comに移動します。

2. セキュアシェル(SSH)でFirepower Management Center(FMC)のCLIにアクセスします。

3. ping intelligence.sourcefire.com firepower Management Centerから次の操作を実行します。

   ```
   admin@Sourcefire3D:~$ sudo ping intelligence.sourcefire.verifyyou receive an output similar
   to this:

   64 bytes from x (xxx.xxx.xx.x): icmp_req=1 ttl=244 time=4.05 ifyou do not receive a
   response similar to that shown, then you can have an outbound connectivity issue, or you do
   not have a route to intelligence.sourcefire.com.
   ```

4. のホスト名を解決します intelligence.sourcefire.com:

```
admin@Firepower:~$ sudo nslookup intelligence.sourcefire.com
```

次のような応答が表示されることを確認します。

```
Server: 8.8.8.8
Address: 8.8.8.8#53

Name: intelligence.sourcefire.com
Address: xxx.xxx.xx.x
```

注：上記の出力では、例としてGoogleパブリックドメインネームシステム(DNS)サーバを使用しています。この出力は、[System] > [Local] > [Configuration] で設定したDNS設定によって異なります。 **Network** 。次に示すような応答が表示されない場合は、DNS設定が正しいことを確認します。**注意**：サーバは、ロードバランシング、耐障害性、および稼働時間にラウンドロビンIPアドレススキーマを使用します。したがって、IPアドレスは変更される可能性があります。シスコでは、ファイアウォールを **CNAME** IPアドレスの代わりに使用されます。

5. 接続を確認します。 intelligence.sourcefire.com telnetを使用する場合：

```
admin@Firepower:~$ sudo telnet intelligence.sourcefire.com 443
```

次のような出力が表示されることを確認します。

```
Trying xxx.xxx.xx.x...
Connected to intelligence.sourcefire.com.
Escape character is '^]'.
```

注:2番目の手順を正常に完了できても、Telnetで接続できない場合は、 **intelligence.sourcefire.com** ポート443に対して、ポート443の発信をブロックするファイアウォール規則を設定できます。 intelligence.sourcefire.com.

6. [System] > [Local] > [Configuration] に移動し、 **Manual Proxy** 設定の下に **Network** 。
注：このプロキシがSecure Sockets Layer(SSL)インスペクションを実行する場合は、プロキシをバイパスするバイパスルールを設定する必要があります。 **intelligence.sourcefire.com**.
7. 次の操作を実行できるかどうかをテストします。 HTTP GET ~ に対する要求 intelligence.sourcefire.com:

```
admin@Firepower:~sudo curl -vvk https://intelligence.sourcefire.com
* About to connect() to intelligence.sourcefire.com port 443 (#0)
* Trying 198.148.79.58...
* Adding handle: conn: 0xec5630
* Adding handle: send: 0
* Adding handle: recv: 0
* Curl_addHandleToPipeline: length: 1
* - Conn 0 (0xec5630) send_pipe: 1, recv_pipe: 0
* Connected to intelligence.sourcefire.com (198.148.79.58) port 443 (#0)
* SSLv3, TLS handshake, Client hello (1):
* SSLv3, TLS handshake, Server hello (2):
* SSLv3, TLS handshake, CERT (11):
* SSLv3, TLS handshake, Server key exchange (12):
* SSLv3, TLS handshake, Server finished (14):
* SSLv3, TLS handshake, Client key exchange (16):
* SSLv3, TLS change cipher, Client hello (1):
```

```
* SSLv3, TLS handshake, Finished (20):
* SSLv3, TLS change cipher, Client hello (1):
* SSLv3, TLS handshake, Finished (20):
* SSL connection using DHE-RSA-AES256-SHA
* Server certificate:
* subject: O=Sourcefire Inc.; OU=VRT Department of Intelligence;
emailAddress=vrt-systems@sourcefire.com; L=Columbia; ST=MD; C=US;
CN=intelligence.sourcefire.com
* start date: 2016-02-29 22:50:29 GMT
* expire date: 2019-02-28 22:50:29 GMT
* issuer: O=Sourcefire Inc.; OU=VRT Department of Intelligence;
emailAddress=vrt-systems@sourcefire.com; L=Columbia; ST=MD; C=US;
CN=intelligence.sourcefire.com; nsCaRevocationUrl=
https://intelligence.sourcefire.com/vrtca.crl
* SSL certificate verify result: unable to get local issuer certificate
(20), continuing anyway.
>GET / HTTP/1.1
>User-Agent: curl/7.31.0
>Host: intelligence.sourcefire.com
>Accept: */*
>
<HTTP/1.1 200 OK
<Date: Tue, 01 Mar 2016 13:06:16 GMT
* Server Apache is not blacklisted
<Server: Apache
<Last-Modified: Tue, 09 Dec 2014 20:08:06 GMT
<ETag: "9da27-3-509ce19e67580"
<Accept-Ranges: bytes
<Content-Length: 3
<Content-Type: text/html
<
:)
* Connection #0 to host intelligence.sourcefire.com left intact
```

注: curl コマンド出力は、接続が正常に行われたことを示します。**注**：プロキシを使用する場合、 curl コマンドにはユーザ名が必要です。コマンドは**curl -U <user> -vvk** https://intelligence.sourcefire.comです。また、コマンドを入力すると、プロキシパスワードの入力を求めるプロンプトが表示されます。

8. セキュリティインテリジェンスフィードをダウンロードするために使用されるHTTPSトラフィックがSSLデクリプタを通過しないことを確認します。SSL復号化が発生していないことを確認するには、ステップ6の出力でサーバ証明書情報を検証します。サーバ証明書が次の例に示す内容と一致しない場合は、証明書を再署名するSSL復号化機能を使用できます。トラフィックがSSLデクリプタを通過する場合は、宛先のすべてのトラフィックをバイパスする必要があります intelligence.sourcefire.com.

```
admin@Firepower:~$ sudo curl -vvk https://intelligence.sourcefire.com
* About to connect() to intelligence.sourcefire.com port 443 (#0)
* Trying 198.148.79.58...
* Adding handle: conn: 0xec5630
* Adding handle: send: 0
* Adding handle: recv: 0
* Curl_addHandleToPipeline: length: 1
* - Conn 0 (0xec5630) send_pipe: 1, recv_pipe: 0
* Connected to intelligence.sourcefire.com (198.148.79.58) port 443 (#0)
* SSLv3, TLS handshake, Client hello (1):
* SSLv3, TLS handshake, Server hello (2):
* SSLv3, TLS handshake, CERT (11):
* SSLv3, TLS handshake, Server key exchange (12):
* SSLv3, TLS handshake, Server finished (14):
* SSLv3, TLS handshake, Client key exchange (16):
```

```
* SSLv3, TLS change cipher, Client hello (1):
* SSLv3, TLS handshake, Finished (20):
* SSLv3, TLS change cipher, Client hello (1):
* SSLv3, TLS handshake, Finished (20):
* SSL connection using DHE-RSA-AES256-SHA
* Server certificate:
* subject: O=Sourcefire Inc.; OU=VRT Department of Intelligence;
emailAddress=vrt-systems@sourcefire.com; L=Columbia; ST=MD; C=US;
CN=intelligence.sourcefire.com
* start date: 2016-02-29 22:50:29 GMT
* expire date: 2019-02-28 22:50:29 GMT
* issuer: O=Sourcefire Inc.; OU=VRT Department of Intelligence;
emailAddress=vrt-systems@sourcefire.com; L=Columbia; ST=MD; C=US;
CN=intelligence.sourcefire.com; nsCaRevocationUrl=
https://intelligence.sourcefire.com/vrtca.crl
*  SSL certificate verify result: unable to get local issuer certificate
(20), continuing anyway.
>GET / HTTP/1.1
>User-Agent: curl/7.31.0
>Host: intelligence.sourcefire.com
>Accept: */*
>
<HTTP/1.1 200 OK
<Date: Tue, 01 Mar 2016 13:06:16 GMT
* Server Apache is not blacklisted
<Server: Apache
<Last-Modified: Tue, 09 Dec 2014 20:08:06 GMT
<ETag: "9da27-3-509ce19e67580"
<Accept-Ranges: bytes
<Content-Length: 3
<Content-Type: text/html
<
:)
* Connection #0 to host intelligence.sourcefire.com left intact
```

注:SSL復号化はSecurity Intelligence Feedに対してバイパスする必要があります。これは、SSL復号化ツールがSSLハンドシェイクでFirepower Management Centerに不明な証明書を送信するためです。Firepower Management Center(FMC)に送信される証明書はSourcefireの信頼できるCAによって署名されていないため、接続は信頼されません。

関連情報

- 自動マチック Firepower Management Center(FMC)でのアップデート障害のダウンロード
- 高度なマルウェア防御(AMP)運用に必要なサーバアドレス
- Firepowerシステムの動作に必要な通信ポート
- テクニカル サポートとドキュメント – Cisco Systems

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。