FireSIGHT Management Center でのセキュリティ インテリジェンス フィード アップデート障害のトラブルシューティング

目次

概要

この資料に安全保障局供給更新で問題を解決する方法を記述されています。 安全保障局供給は悪い評判がある IP アドレスの複数の定期的にアップデートされたリストで Cisco Talos 安全保障局および研究 グループ (Talos) 判別されるように、構成されます。 ネットワークトラフィックをフィルタリングするために Cisco SireSIGHT システムが最新情報を使用できるように知性供給を定期的にアップデートされて保存することは重要です。

前提条件

要件

次の項目に関する知識が推奨されます。

- Cisco FireSIGHT 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 文書に記載されている 情報はソフトウェア バージョン 5.2 またはそれ以降を実行する Cisco FireSIGHT Management Center に基づいています。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 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。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

問題

安全保障局供給アップデート失敗は発生します。 Web GUI か CLI によって失敗をできます（続く）セクションで更に説明される確認。

Web GUI からの問題を確認して下さい

安全保障局供給アップデート失敗が発生するとき、FireSIGHT Management Center は健全性アラートを表示します。

CLI からの問題を確認して下さい

安全保障局供給を持つアップデート失敗の根本的な原因を判別するために、FireSIGHT Management Center の CLI にこのコマンドを入力して下さい:

```
admin@Sourcefire3D:~$

cat /var/log/messages
```

メッセージのこれらの警告のどちらかを捜して下さい:

```
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
```

解決策

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. *intelligence.sourcefire.com* サイトがアクティブであることを確認して下さい。 https://intelligence.sourcefire.comin へのナビゲート ブラウザ。 サイトはライブであることを示すにこやかなフェイスを受け取る必要があります。

2. セキュア シェル（SSH）によって FireSIGHT Management Center の CLI にアクセスして下さい。

3. FireSIGHT Management Center から *intelligence.sourcefire.com* を ping して下さい:

   ```
   admin@Sourcefire3D:~$

   sudo ping intelligence.sourcefire.com
   ```

   これと同じような出力が表示される必要があります:

   ```
   64 bytes from x (xxx.xxx.xx.x): icmp_req=1 ttl=244 time=4.05 ms
   ```

   示されているそれと同じような応答を受け取らない場合送信接続上の問題があるかもしれませんまたは *intelligence.sourcefire.com* にルートがありません。

4. *intelligence.sourcefire.com* のためのホスト名を解決して下さい:

```
admin@Firepower:~$

sudo

nslookup intelligence.sourcefire.com
```

これと同じような応答を受け取る必要があります:

```
Server: 8.8.8.8
Address: 8.8.8.8#53

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

注: 前述出力は一例として Google パブリック・ドメイン名前システム（DNS）サーバを使用します。 出力は**システム > ローカル > 設定**で行われる DNS 設定によって*ネットワーク* セクションの下で決まります。 示されているそれと同じような応答を受け取らない場合 DNS 設定が正しいことを確認して下さい。**注意**： サーバはロード バランシング、フォールト トレランスおよび稼働時間のためにラウンドロビン IP アドレス スキーマを使用します。従って、IP アドレスは変更されるかもしれないしファイアウォールが IP アドレスの代りに *CNAME* で設定されることを Cisco は推奨します。

5. Telnet の使用と *intelligence.sourcefire.com* への接続をチェックして下さい:

```
admin@Firepower:~$

 sudo telnet intelligence.sourcefire.com 443
```

これと同じような出力が表示される必要があります:

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

注: 第2ステップを正常に完了できればが、ポート 443 上の *intelligence.sourcefire.com* に Telnet にない場合、*intelligence.sourcefire.com* のために送信ポート 443 をブロックするファイアウォール ルールがあるかもしれません。

6. **システム > ローカル > 設定**にナビゲート し、*ネットワーク* セクションの下で *手動プロキシ設定*のプロキシ 設定を確認して下さい。
注: このプロキシが Secure Sockets Layer（SSL）インスペクションをする場合、場所に *intelligence.sourcefire.com* のためのプロキシをバイパスするバイパス ルールを入れて下さい。
7. *intelligence.sourcefire.com* に対して *HTTP GET* 要求を行うことができるかどうかテストして下さい:

```
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: *カール* コマンド 出力の端ににこやかなフェイスは接続の成功を示します。**注:** プロキシを使用する場合、*カール* コマンドはユーザ名を必要とします。 コマンドはです**カール- U <user> - vvk** https://intelligence.sourcefire.com。 コマンドを入力した後さらに、入力しますプロキシ パスワードをプロンプト表示されます。

8. 安全保障局供給をダウンロードするために使用する HTTPS トラフィックがパススルー SSL 復号化ことを確認して下さい。 SSL 復号化が発生しないことを確認するために、ステップ

6.からの出力のサーバ証明情報を検証して下さい。 サーバ証明が続く例で表示されるそれと一致しなければ、証明書を辞職する SSL decryptor があるかもしれません。 トラフィックが SSL 復号化を通る場合、*intelligence.sourcefire.com* に行くトラフィックすべてをバイパスして下さい。

```
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 復号化は安全保障局供給のために SSL decryptor が FireSIGHT Management Center を SSL ハンドシェイクの未知証明書 送信 するのでバイパスする必要があります。FireSIGHT Management Center に送信 される 証明書は Sourcefire 信頼された CA、従って接続によって信頼できないです署名しません。

関連情報

- FireSIGHT Management Center での自動ダウンロード更新の失敗
- Advanced Malware Protection（アンペア）オペレーションのための必須サーバ アドレス
- FireSIGHT 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