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 FireSIGHT 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あることが推奨されます。

- 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

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この文書に記載されている情報は Cisco FireSIGHT Management Center に基づいています。

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、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

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する。

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:

メッセージのこれらの警告のどちらかを捜して下さい:

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:

   これと同じような出力が表示される必要があります:

   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:

   これと同じような応答を受け取る必要があります:

   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:

   これと同じような出力が表示される必要があります:

   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 で接続することができない場合 *intelligence.sourcefire.com* のためのポート 443 発信

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、インポートに *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:

   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. HTTPS トラフィックが安全保障局供給をダウンロードするために使用するパススルー 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するそれを一致する、認証を辞職する SSL 復号化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。

   注 SSL 復号化は安全保障局供給のために SSL 復号化が FireSIGHT Management Center を SSL ハンドシェイクの未知認証 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 認証は 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 の自動ダウンロード アップデート失敗
- 高度 Malware 保護 (AMP) オペレーションのための必須サーバ アドレス
- FireSIGHT システムオペレーションのための必須 COM ポート
- テクニカルサポートとドキュメント - Cisco Systems