Cisco IPS 自動シグニチャ アップデートの機能の動作の説明

目次

概要

このドキュメントでは、Cisco Intrusion Prevention System（IPS）自動更新機能とその動作の概要を説明します。

IPS 自動更新機能は IPS バージョン 6.1 で導入されました。管理者はこの機能を使用して、予定された定期的な間隔で IPS シグネチャの更新を簡単に行うことができます。

前提条件

要件

次の項目に関する知識が推奨されます。

- シグネチャの更新には Cisco Services for IPS の有効なサブスクリプションおよびライセンス キーが必要です。 http://www.cisco.com/go/license にアクセスし、[IPS Signature Subscription Service] をクリックして、ライセンス キーを申し込みます。

- アクティブな Cisco Services for IPS サブスクリプションに関連付けられている Cisco.com（CCO）ユーザ アカウント。

- 暗号化ソフトウェアをダウンロードする権限。 次のように行って下さい。 http://tools.cisco.com/legal/k9/controller/do/k9Check.x?eind=Y こちらで権限があるかどうかを確認できます。

使用するコンポーネント

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

- Cisco IPS バージョン 6.1 以降

- Cisco IPS バージョン 7.2(1)、7.3(1) 以降の固有機能

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。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

ネットワーク要件

1. IPS のコマンドおよび制御インターフェイスには、HTTPS（TCP 443）および HTTPS（TCP 80）によるインターネットへの直接アクセスが必要です。

2. IPS のインターネット接続を許可するには、ルータやファイアウォールなどのエッジ デバイスに、ネットワーク アドレス変換（NAT）およびアクセス コントロール リスト（ACL）を設定する必要があります。

3. すべてのコンテンツ フィルタとネットワーク トラフィック シェーパーからコマンドおよび制御インターフェイスの IP アドレスを除外します。

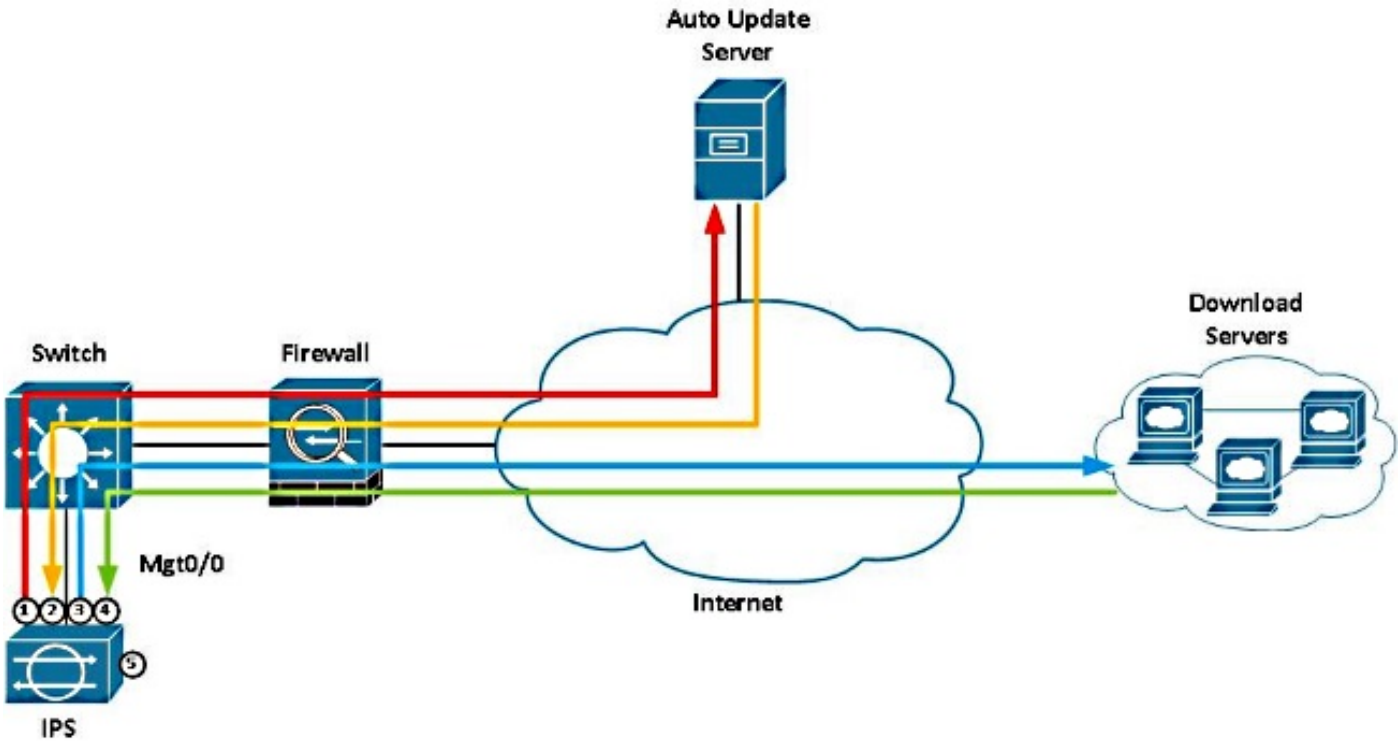
4. 自動更新機能は、7.2(1) FIPS/CC 認定リリースのプロキシ サーバをサポートします。 他の 6.x および 7.x ソフトウェア リリースはすべて、現時点でプロキシ サーバ経由の自動更新をサポートしていません。 7.2(1) リリースにはデフォルトの Secure Shell（SSH）および HTTPS 設定に対する多くの変更が含まれています。 7.2(1) にアップグレードする前に、『Cisco Intrusion Prevention System 7.2(1)E4 のリリース ノート』を参照してください。

警告： Cisco IPS バージョン 7.0(8)E4 では、自動更新 URL 設定でシスコのサーバの IP アドレスのデフォルト値が 198.133.219.25 から 72.163.4.161 に変更されています。 センサーが自動更新用に設定されている場合は、センサーが新しい IP アドレスに接続できるように、ファイアウォール ルールを更新する必要があります。 Cisco IPS バージョン 7.2 以降では、ハードコードされた自動更新サーバの IP アドレスが、名前付き完全修飾ドメイン名（FQDN）およびドメイン ネーム システム（DNS）ルックアップに置き換えられています。 詳細については、このドキュメントの「設定」セクションを参照してください。

警告の回避

一部のシグネチャの更新では、正規表現テーブルの再コンパイルが必要です。IPS はその間、ソフトウェア バイパス モードに入ります。 インライン センサのバイパス モードが [Auto] に設定されている場合、分析エンジンはバイパスされ、トラフィックは検査されることなく、インライン インターフェイスおよびインライン VLAN ペアを通過できます。 バイパス モードを [Off] にすると、インライン センサーは更新の適用中のトラフィックの通過を停止します。

シグネチャの自動更新プロセス



1. IPS は HTTPS（TCP 443）を使用して 72.163.4.161 に自動更新サーバを認証します。

2. IPS は自動更新サーバにクライアント マニフェストを送信しますが、これには、Cisco IPS センサーの信頼性を検証するためにサーバが使用するプラットフォーム ID と暗号化された共有秘密が含まれています。

3. 認証されると、更新サーバはプラットフォーム ID に関連付けられたダウンロード ファイル オプションのリストが含まれたサーバ マニフェストで応答します。 ここに含まれるデータには更新バージョン、ダウンロードの場所、およびサポートされるファイル転送プロトコル

に関する情報が含まれています。 このデータに基づいて、IPS 自動更新ロジックはいずれかのダウンロード オプションが有効かどうかを判定し、ダウンロードに最適な更新プログラム パッケージ選択します。 ダウンロードの準備で、サーバは更新ファイルの復号化に使用するキーのセットを IPS に提供します。

4. IPS は、サーバ マニフェストで特定されたダウンロード サーバへの新しい接続を確立します。 ダウンロード サーバの IP アドレスは、場所に応じて異なります。 IPS は、サーバ マニフェストに指定されたファイル ダウンロード データ URL で定義されたファイル転送プロトコルを使用します（現在は HTTP（TCP 80）を使用）。

5. IPS は以前にダウンロードしたキーを使用して更新プログラム パッケージを復号化し、シグネチャ ファイルをセンサーに適用します。

設定

基本的なシグネチャ自動更新設定

自動更新機能は IPS Device Manager（IDM）または IPS Manager Express（IME）から設定できます。 次の手順を実行します。

1. IDM/IME から [Configuration] > [Sensor Management] > [Auto/Cisco.com Update] を選択します。