

IPS Manager Express を使用した Cisco IOS Intrusion Prevention System で生成されたイベントのモニタ

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[機能](#)

[設定](#)

[ルータの設定](#)

[IME の設定](#)

[関連情報](#)

概要

このドキュメントでは、IPS Manager Express (IME) を使用して Cisco IOS 侵入防御システム (IOS-IPS) によって生成されたモニタ イベントを使用する方法について説明します。

Cisco IOS IPS は効果的にネットワーク攻撃の広範囲を軽減するソフトウェアベースの強度のパケットインスペクション機能です。

Cisco IME は簡単な、GUI ベース IPS 管理 ソフトウェアです。

前提条件

要件

このドキュメントの読者は次のトピックについて理解する必要があります。

- Cisco IOS 侵入防御システム (IPS)
- [IPS Manager Express](#)

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 IPS Manager Express を使用して IOS 侵入防御システム (IPS) on Cisco 基づいています。

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。

機能

要件：

IOS IPS をサポートする IME に関してはルータは Cisco IOS ソフトウェア リリース 12.3(14)T7 および 12.4(15)T2 またはより新しいを実行する必要があります。IME は 10 までのデバイスをサポートできます。

注: IME は IOS IPS のためのイベントモニタリングだけをサポートします。設定はサポートされません。

設定

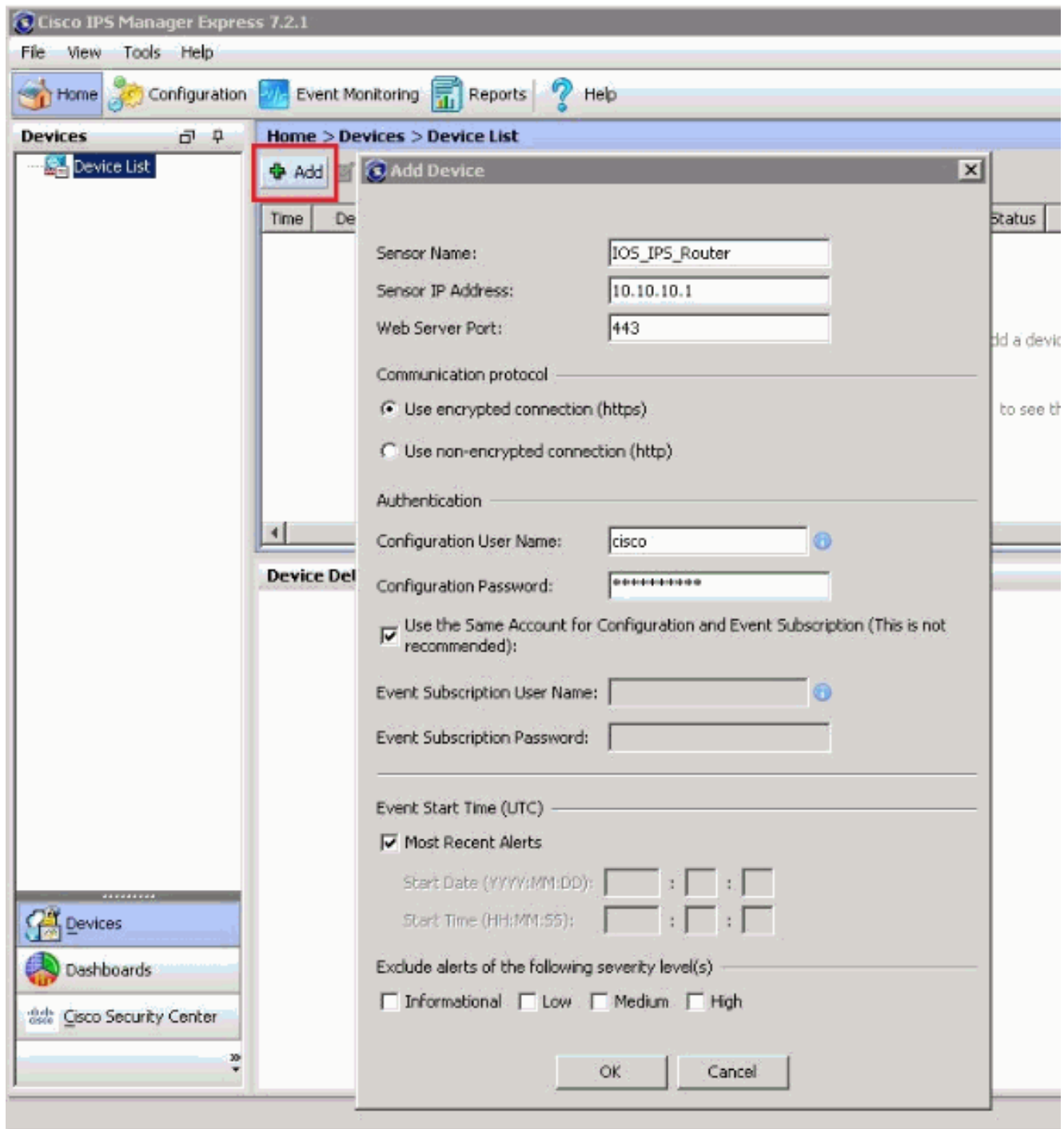
IME は IOS IPS からイベントを得るのに SDEE を使用します。SDEE 通知はデフォルトでディセーブルにされ、手動で有効になる必要があります。SDEE を使用するために、ルータの Webサーバは有効にする必要があります。デフォルトで、IME は HTTPS (443) TCP を使用してルータに信頼できる接続を確立することを試みます。これはデジタル認証がルータで設定されるように要求します。任意で、IME は HTTP (80) TCP を使用して安全でない接続をサポートするために設定することができます。

ルータの設定

1. イネーブル SDEE 通知:Router(config)# ip ips notify sdee
2. イネーブル HTTPS:Router(config)#ip http secure-server
3. イネーブル HTTP (オプションの):Router(config)# ip http server

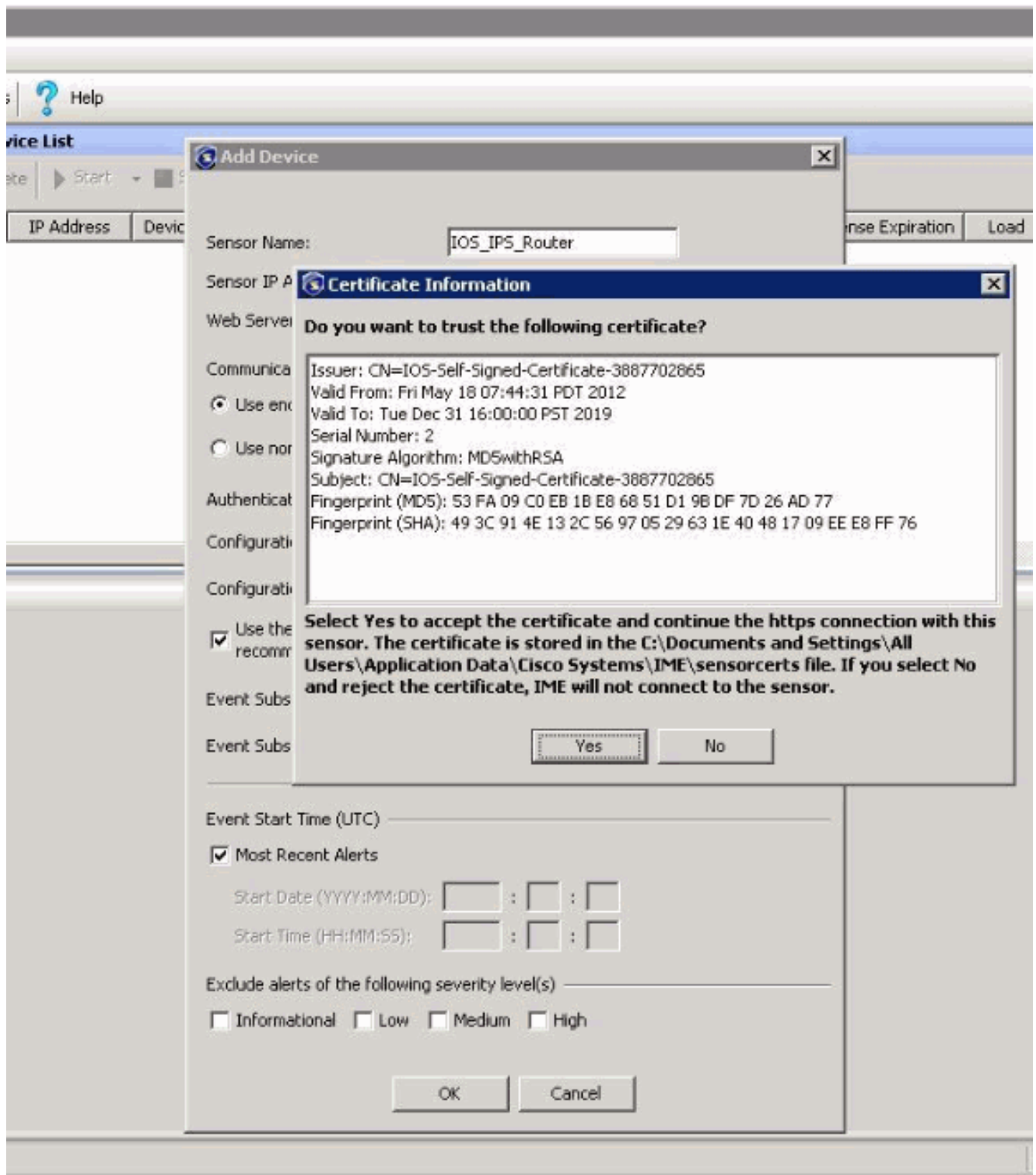
IME の設定

1. ダウンロードおよびインストール IME。IME を実行して下さい。次に、[Add] をクリックします。ダウンロード
IME:<http://www.cisco.com/cisco/software/navigator.html?mdfid=278875433&flowid=4460>



注: デフォルト設定はルータに接続するのに HTTPS およびポート 443 を使用します。また HTTP だけを使用して接続することを選択でき 80 にポートを変更します。

2. HTTPS を使用している場合ルータからの自己署名証明書を受け入れるために、画面が表示されます。[Yes] をクリックします。



正しく追加されて、次が表示されます

:

The screenshot shows the Cisco IPS Manager Express 7.2.1 interface. The top navigation bar includes Home, Configuration, Event Monitoring, Reports, and Help. The main content area is divided into two sections: 'Device List' and 'Device Details - IOS_IPS_Router'.

Device List Table:

Time	Device Name	IP...	Device Type	Event Status	Sensor Health	Global Correlation Status	Version	Lic...
	IOS_IPS_Router	1...	2801	Connected	Not Supp...	Not Supported	12.4(24)T5,	

The 'Event Status' column for the first row is highlighted with a red box.

Device Details - IOS_IPS_Router:

The 'Device Details' section has several tabs: Sensor Health, Sensor Information, CPU, Memory, & Load, Licensing, Interface Status, and Global Correlation Health. The 'Sensor Health' and 'Network Security Health' tabs are active, each displaying a circular gauge with a needle pointing to 'Unknown'. Below each gauge is a 'Details' link.

At the bottom of the page, there is a message: **Not Supported. This feature requires at least IPS Sensor v6.1.**

注: HTTPS がルータに接続すればのに使用されている場合ルータの認証へのどの変更でもデバイスが IME に再発見されるように要求します。IME の認証をリフレッシュするために、デバイス リストの下でルータをダブルクリックして下さい。それから、新しい認証を得るために IME がルータに接続することを確かめるために『OK』をクリックして下さい。更新済認証を受け入れるために『Yes』をクリックして下さい。

3. イベントの表示: クリック イベント **モニタリング**。「センサー名前」の下でルータを選択するために確かめて下さい。注: デフォルトで、「脅威の評価する」フィールドを評価する「脅威の下のビュー」設定で値は " ≥ 70 " に設定されます。この値は 70 におよび等号上で評価する脅威が付いているだけ結果ディスプレイ シグニチャを作ります。すべての重大度 シグニチャを表示するために「脅威を」フィールドは空白を評価させ続けて下さい。

Version 7.2.1

Event Monitoring | Reports | Help

Event Monitoring > Event Monitoring > Event Views > Basic View

View Settings

Filter | Group By | Color Rules | Fields | General

Filter Name: Basic View Filter

Packet Parameters

Attacker IP:

Victim IP:

Signature Name/ID:

Victim Port:

Rating and Action Parameters

Severity: High Medium Low Info

Risk Rating: Reputation:

Threat Rating:

Action(s) Taken:

Other Parameters

Sensor Name(s): IOS_IPS_Router

Virtual Sensor:

Status: All

Vict. Locality:

Time: Real Time Last: 10 hour Start Time: Fri, 18 May 2012 00:00:00 End Time: Fri, 18 May 2012 00:00:00 Apply

Event | Show All Details | Filter | Edit Signature | Create Rule | Stop Attacker | Tools | Other

Severity	Date	Time	Device	Sig. Name	Sig. ID	Attacker IP	Victim IP	Actions	Victim Port	Threat	Risk Rel.	Reputa...
Info...	05/18/...	08:54:22	IOS_IPS...	RFC 1918 Addresses Seen								
Info...	05/18/...	08:54:25	IOS_IPS...	RFC 1918 Addresses Seen								
Info...	05/18/...	08:54:34	IOS_IPS...	RFC 1918 Addresses Seen								
Info...	05/18/...	08:54:40	IOS_IPS...	RFC 1918 Addresses Seen								
Info...	05/18/...	08:54:47	IOS_IPS...	RFC 1918 Addresses Seen								
Info...	05/18/...	08:54:55	IOS_IPS...	RFC 1918 Addresses Seen								
Info...	05/18/...	08:55:06	IOS_IPS...	RFC 1918 Addresses Seen								
Info...	05/18/...	08:55:15	IOS_IPS...	RFC 1918 Addresses Seen								
Info...	05/18/...	08:14:43	IOS_IPS...	ICMP Echo Request								
Info...	05/18/...	08:14:46	IOS_IPS...	ICMP Echo Request								
Info...	05/18/...	08:16:56	IOS_IPS...	ICMP Echo Request								
Info...	05/18/...	08:16:57	IOS_IPS...	ICMP Echo Request								
Info...	05/18/...	08:16:58	IOS_IPS...	ICMP Echo Request								
Info...	05/18/...	08:16:59	IOS_IPS...	ICMP Echo Request								
low	05/18/...	08:15:55	IOS_IPS...	IGMP Invalid Packet DoS								
low	05/18/...	08:17:52	IOS_IPS...	IGMP Invalid Packet DoS								
low	05/18/...	08:23:50	IOS_IPS...	IGMP Invalid Packet DoS								

Event Details (Event ID - 13373565153745)

Print | Copy

Event Time: 05/18/2012 08:55:15

Sensor Local Time: 05/18/2012 15:55:15

Signature ID: 1107

Signature Sub-ID: 0

Signature Name: RFC 1918 Addresses Seen

Signature Version: 5592

Signature Details: My Sig Info

Interface Group:

VLAN ID:

Interface: Fa0/0

Attacker IP: 192.168.50.1

Protocol: udp

Attacker Port: 63240

Attacker Locality:

Target IP: 255.255.255.255

Target Port: 60

You can copy selected or all rows into clipboard or print the entire contents.

Total EP

関連情報

- [Cisco IOS 侵入防御システム \(IPS\)](#)
- [IOS IPS との開始-詳細なガイド](#)
- [Cisco IPS Manager Express](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)