# IPS トラフィックのインスペクションとシグニチャ アラートの確認方法

## 目次



## 概要

このドキュメントでは、実稼働環境の侵入防御システム（IPS）センサーおよびシグニチャ テスト オプションの動作を検証する手順を説明します。

## 前提条件

### 要件

このドキュメントに関しては個別の要件はありません。

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づくものです。

- Intrusion Prevention System Release 6.2(x)E4
- Intrusion Prevention System Release 7.0(x)E4
- Intrusion Prevention System Release 7.1(x)E4

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。

## 内部通信、外部通信、および管理通信

次の手順を実行して、IPS 管理アクセスと準備状態を検証します。

- IPS のコンソールにアクセスします。 モジュールの問題である場合、以下を入力します。適応型セキュリティ アプライアンス（ASA）5500 および 5585 シリーズの**セッション 1**、5500x の**セッション ips**、ネットワーク モジュール強化（NME）モジュールの **service-module ids-sensor slot/port セッション**、CatOS の **sessionslot_number** 、侵入検知システム（IDSM）および IDSM-2（第二世代）モジュールの IOS 内の**セッション スロット module_number プロセッサ 1**
- 初期設定で設定したたユーザ名とパスワードでログインします。 デフォルトのユーザ名とパスワードは「Cisco」です。 リリースごとの詳細については、『設定ガイド』を参照してください。
- 設定がすでに完了している場合、IPS 管理への IP 接続のテストに進みます。
- **show statistics host** コマンドを入力し、ping を実行して IPS 管理の IP アドレスに対するセキュア シェル（SSH）アクセスを取得します。 これが成功した場合、次のステップに進みます。 そうでない場合は、適切なリリースの「設定ガイド」を使用して、接続問題のトラブルシューティングを実行します。
- **show version** コマンドを入力します。 ソフトウェア バージョンが最新であること、ライセンスがインストールされていること、シグニチャ バージョンが最新であること、すべてのエンジンが動作可能であること、ホストの証明書が有効であることを検証します。
- 前の手順すべてを確認したら、IPS の管理アドレスに HTTPS 経由でアクセスし、IDM を起動します。 Java 6 をインストールする必要があります。 Java 6 を使用できない場合は、IPS Web ページから IPS Manager Express（IME）をインストールします。**注:** 現時点で Java 7 は IPS Device Manager（IDM）を起動したり、Adaptive Security Device Manager（ASDM）内の IPS オプションにアクセスすることはできません。
- 接続に成功したら、IDM で、[Configuration] > [Sensor Management] > [Licensing and Update License from Cisco.com] に移動します。 有効なライセンスがある場合、インターネットへの接続を確認します。
- 成功したら、[Configuration] > [Policies] > [Global Correlation] > [Inspection/Reputation] に移動し、[Test Global Correlation] をクリックして DNS が作動することを確認します。 これを確認するには、[Monitoring] > [Events] に移動し、[Warning, Error and Fatal] のみを選択して、[Global Correlation] のアップデートが失敗するか確認します。**注:** グローバル 小リレーションは、IPS リリース 7.0 以前の IPS ソフトウェアでは使用できません。

## トラフィック インスペクションの検証

IPS を通じて通信を検証したら、次の手順によりトラフィックのインスペクションを検証できます。

- センサー センシング インターフェイスのリンク ステータスが **UP**であり、トラフィックを受信していることを検証します。 センサー インターフェイスにログインし、次のコマンドを入力します。

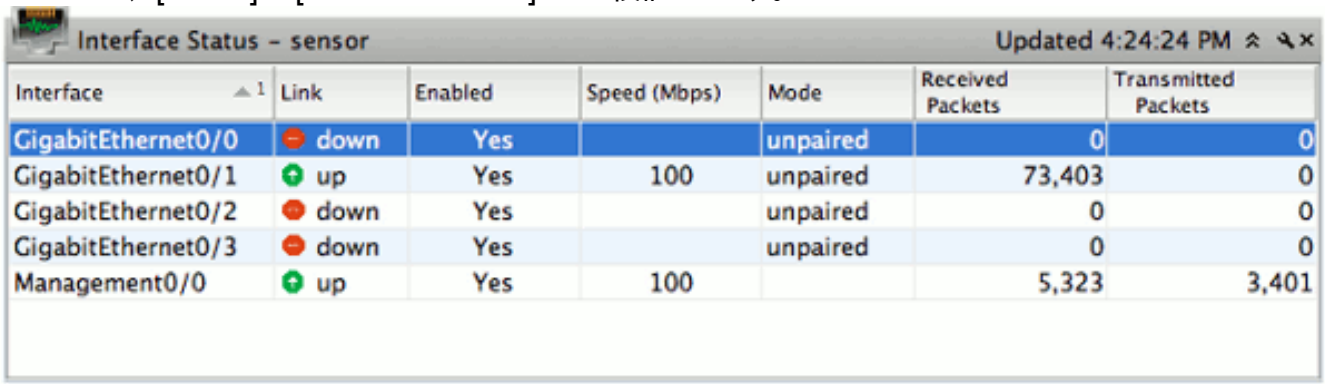
```
sensor# show interface

!! In the output, find the applicable section for the sensing interface(s) in !! question and
```

*confirm that the Link Status value is "Up". If so, note the !! value shown for the Total Packets Received counter. After a few seconds, !! run the command again and compare the current value to the previous. !! If the value has increased, the sensing interface(s) in-question is Up !! and receiving traffic. Example:* sensor# **show interface**
MAC statistics from interface GigabitEthernet0/0
Interface function = Sensing interface
Link Status = Up
Total Packets Received = 100

sensor# **show interface**
MAC statistics from interface GigabitEthernet0/0
Interface function = Sensing interface
Link Status = Up
Total Packets Received = 150

*!! If a sensing interface's Link Status value is expected to be "Up", but is !! not, verify that it is properly and physically connected to a switchport or !! other network device. If so, verify that the switchport or other network !! device is configured properly and the remote interface (the switchport or !! NIC on the other network device) is not administratively-disabled !! ("shutdown"). If needed, try to swap cables with another that is known !! to be good. !! If a sensing interface's Total Packets Received counter does not increment, !! check the configuration of the switchport or other network device to which !! the sensing interface is connected. If the sensing interface is supposed to !! be the destination of a SPAN/monitor session, verify the SPAN/monitor !! configuration on the switch the sensing interface is connected.*

- 別の方法として、IDM のすべてのモニタリング インターフェイスが示すリンク値が **up** であることを、[Home] > [Interface Status] から検証します。




| Interface | Link | Enabled | Speed (Mbps) | Mode | Received Packets | Transmitted Packets |
|---|---|---|---|---|---|---|
| GigabitEthernet0/0 | down | Yes | | unpaired | 0 | 0 |
| GigabitEthernet0/1 | up | Yes | 100 | unpaired | 73,403 | 0 |
| GigabitEthernet0/2 | down | Yes | | unpaired | 0 | 0 |
| GigabitEthernet0/3 | down | Yes | | unpaired | 0 | 0 |
| Management0/0 | up | Yes | 100 | | 5,323 | 3,401 |

- センサーの仮想センサーに少なくとも 1 つのセンシング インターフェイスが割り当てられていて、トラフィックを検査していることを検証します。 センサーにログインし、次のコマンドを入力します。

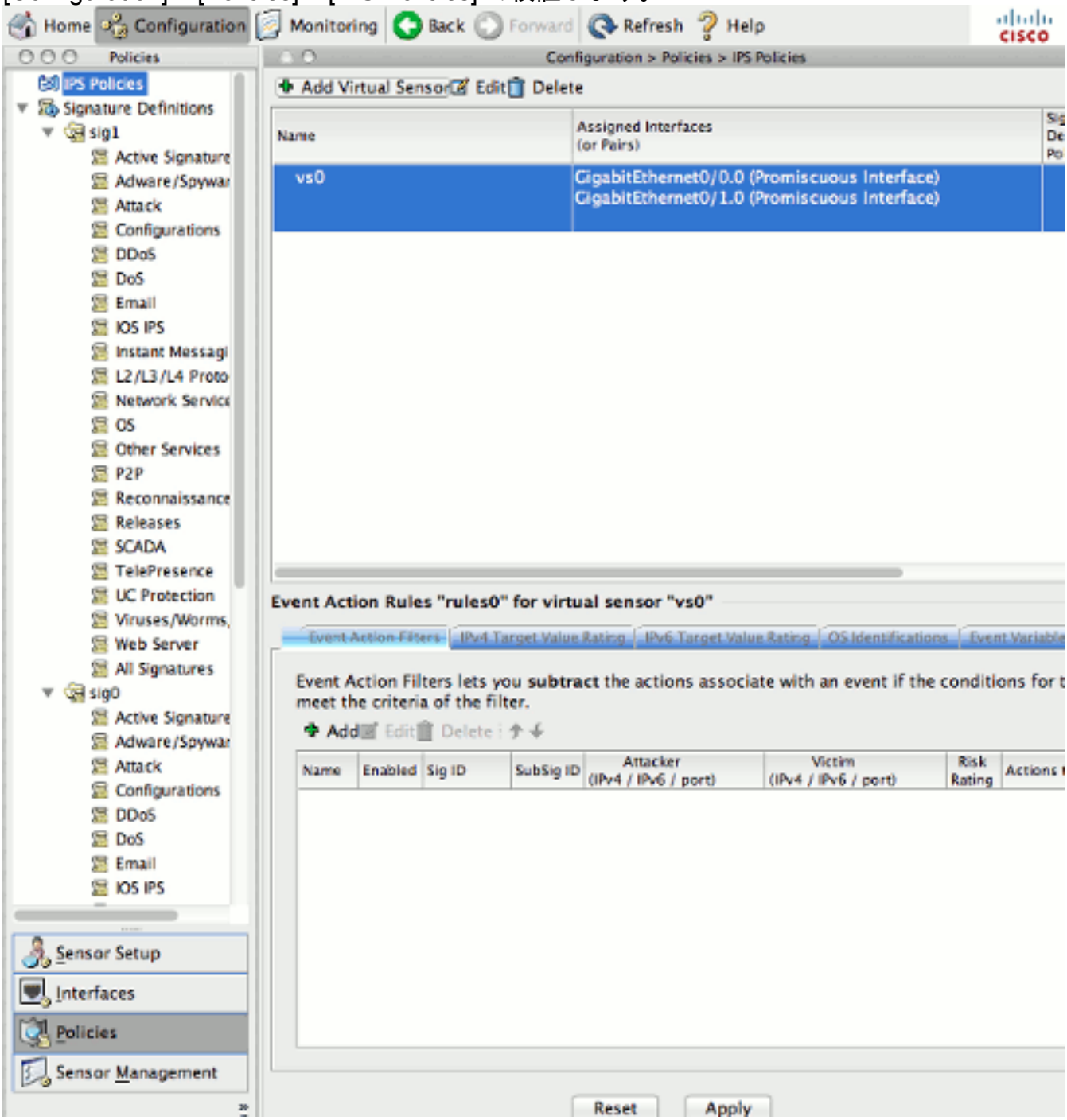
sensor# **show stat virtual**

*!! In the output, find the List of interfaces monitored by this virtual !! sensor line and confirm that at least one (1) sensing interface(s) is !! listed. Additionally, find the Total packets processed since reset !! line/counter and confirm its value is greater-than (>) zero (0). !! Example:* sensor# **show stat virtual**
Statistics for Virtual Sensor vs0
List of interfaces monitored by this virtual sensor = GigabitEthernet0/0
General Statistics for this Virtual Sensor
Total packets processed since reset = 200

*!! If there are no sensing interface(s) listed (or, if additional sensing !! interfaces need to be assigned), login to the sensor using an !! administrative account and issue the following commands !!* (**NOTE**: In the example provided, the GigabitEthernet0/0 sensing interface !! is assigned to virtual-sensor vs0. Replace that particular configuration !! line accordingly with the actual sensing interface you wish to assign to !! the virtual-sensor. If you need to assign multiple sensing interfaces, !! repeat that line (one per sensing interface)):

```
sensor# conf t
sensor(config) # service analysis-engine
sensor(config-ana) # virtual-sensor vs0
sensor(config-ana-vir)# physical-interface GigabitEthernet0/0
sensor(config-ana-vir)# exit
sensor(config-ana)# exit
Apply Changes?[yes]: yes

!! NOTE: The above example assigns a Promiscuous sensing interface to the vs0 !! virtual-
sensor. Inline sensing interfaces must first be "paired" together !! and then the logical
pair assigned to a virtual-sensor. Details can be !! found in the official product
configuration guide's Configuring !! Interfaces section.
```

- 別の方法として、インターフェイスが IDM で**vs0** に割り当てられていることを、[Configuration] > [Policies] > [IPS Policies] で検証します。

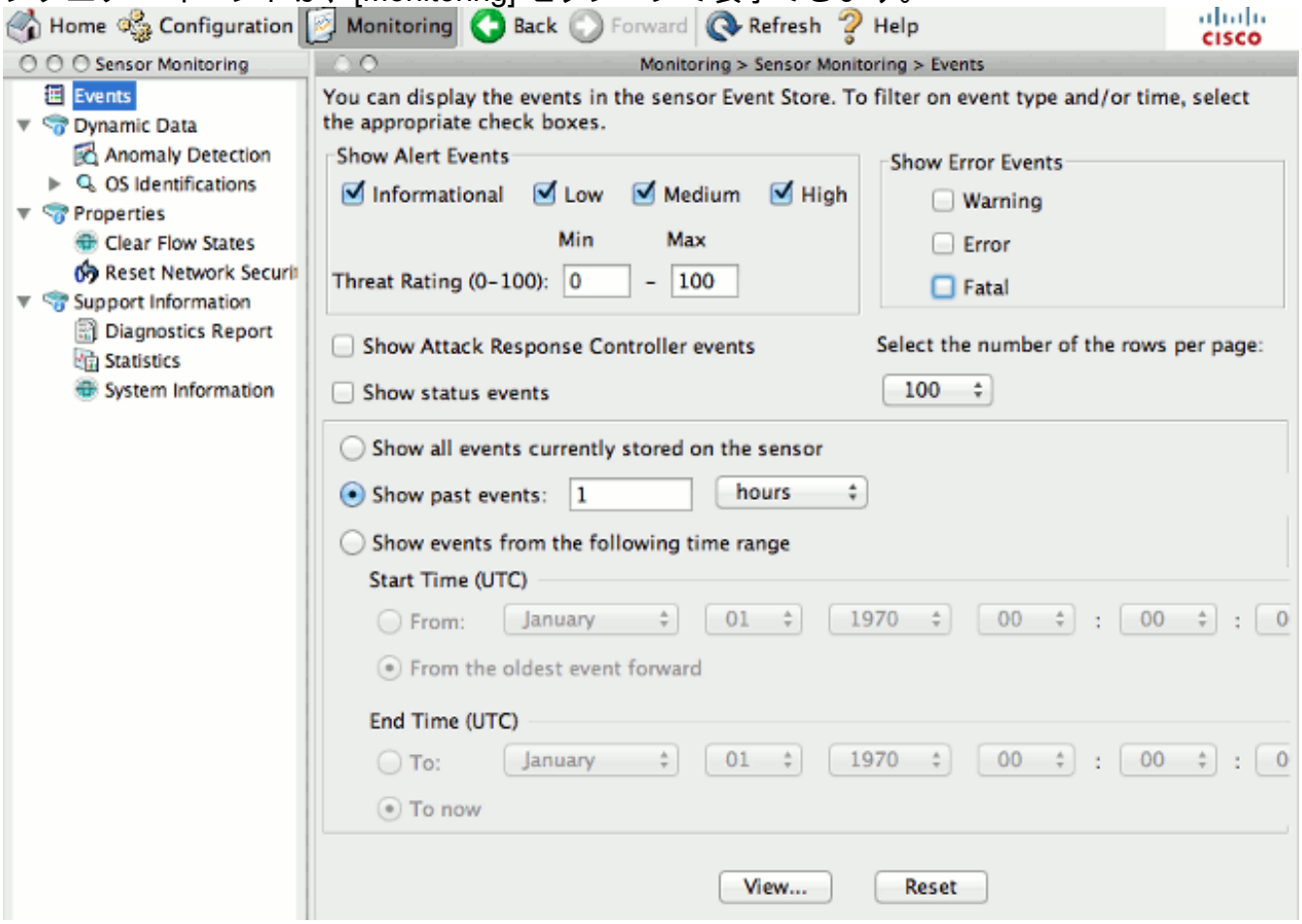



- SSH を IPS に入力し、**packet display interface slot/port** コマンドを入力して、インターフェイス上にトラフィックが表示されることを検証します。**注:** ***expression*** キーワードでは、使用された表現に一致するトラフィックのみを表示させるため、**tcpdump** 表現を使用することができます。

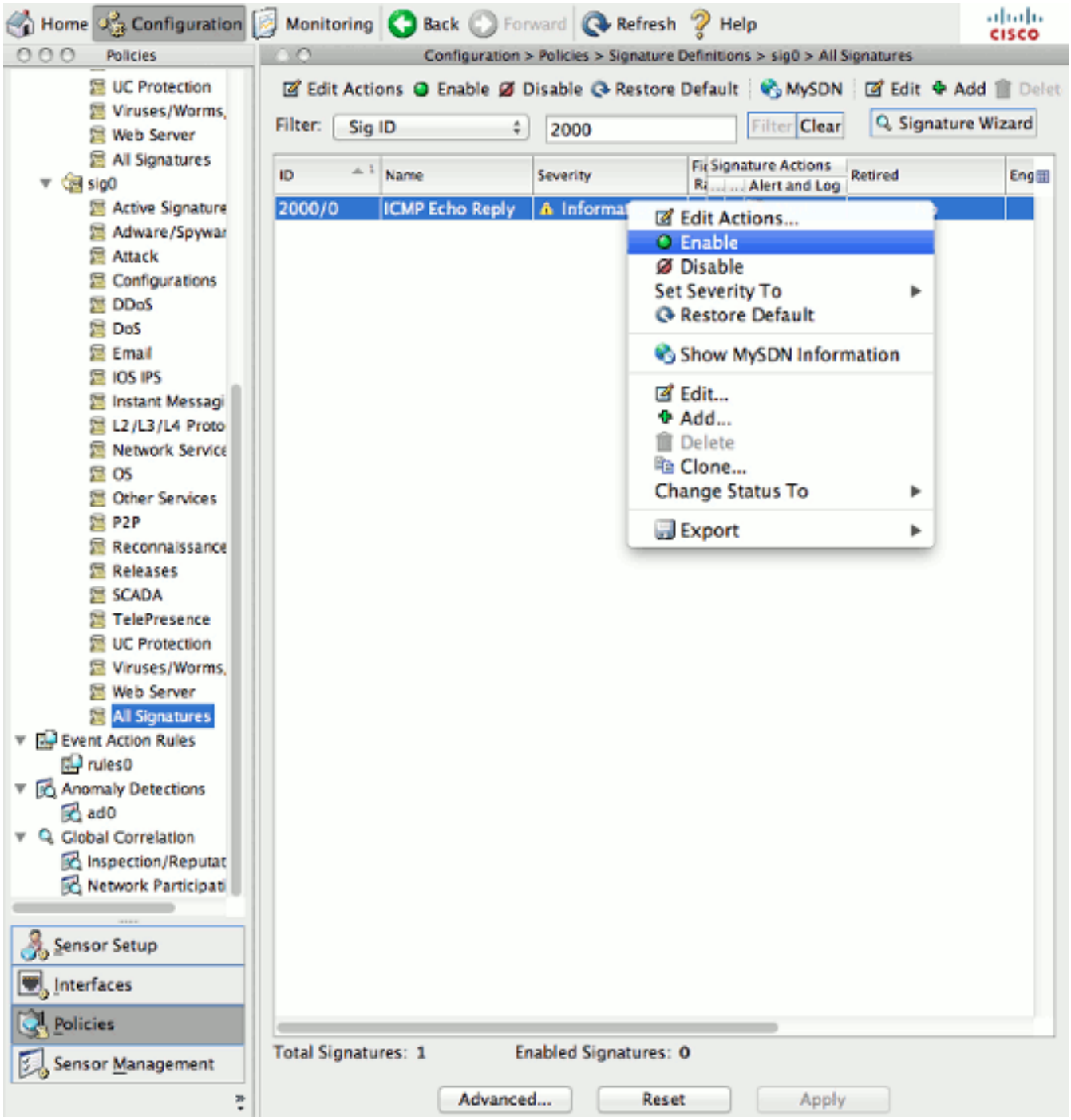
```
sensor# packet display gigabitEthernet0/1 expression ip host 198.51.100.1
Warning: This command will cause significant performance degradation
tcpdump: WARNING: ge0_1: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge0_1, link-type EN10MB (Ethernet), capture size 65535 bytes
18:32:24.247864 IP 198.51.100.1.2000 > 192.0.2.1.2000: UDP, length 172
18:32:24.247868 IP 198.51.100.1.2000 > 192.0.2.1.2000: UDP, length 172
18:32:24.257249 IP 198.51.100.1.2000 > 192.0.2.1.16384: UDP, length 172

 !! Alternatively, in the case of VLAN tagging: sensor# packet display gigabitEthernet0/1
expression vlan 20 and
    ip host 192.51.100.1
```

## シグネチャ ファイアの検証

- シグニチャ イベントは、[Monitoring] セクションで表示できます。

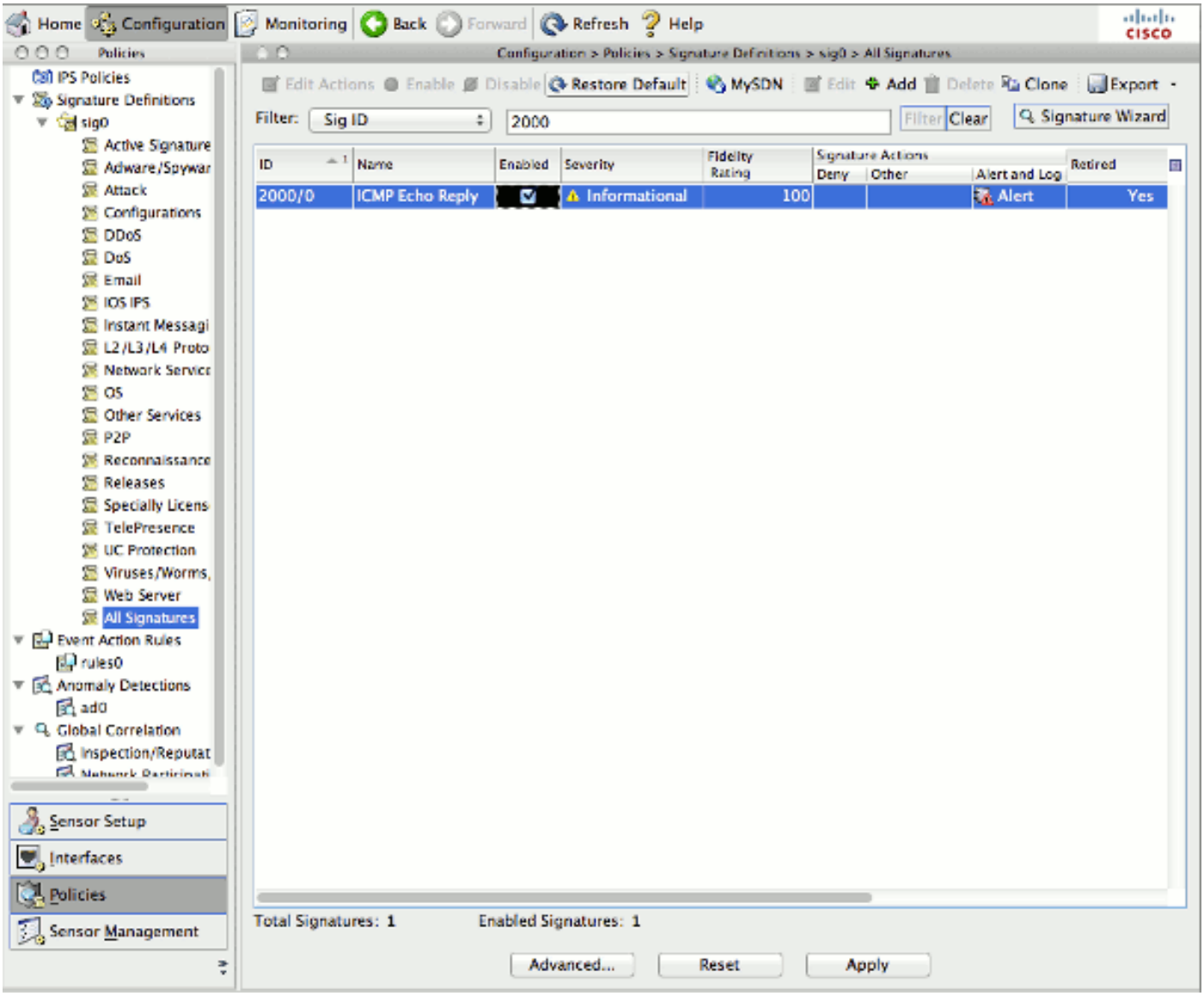



- シグニチャは、[Configuration] > [All Signatures] で変更できます。




- Signature 2000/0 および 2004/0（Internet Control Message Protocol（ICMP）エコー応答および ICMP エコー要求）を有効にし、 センサーから ping を開始して、[Monitoring] タブでイベント ログを確認します。ICMP がブロックされている場合：1107/0 の場合、RFC1918 - アドレスを表示。このシグニチャをトリガーするには、このシグネチャで [retire] を [false] に、[enable] を [true] に設定し、RFC 1918 範囲の IP がシグネチャをトリガすることを確認します。これらのアドレスは、10.0.0.0/8、172.16.0.0-172.31.255.255、192.168.0.0/16 です。シグニチャがリタイアされていないことが必要なため、これは SSC-5 では見られません。3409/0 の場合、ポート 80 に Telnet 接続します。Web サーバを設定すると、ポート 80 が開き、Telnet 接続に成功します。 Telnet が成功したら、IPS でイベントが始動します。TCP 3 ウェイ ハンドシェイクは、センサーが有効な TCP 接続を追跡するために必要です。 非対称ルーティングや部分的なパケット キャプチャのリプレイでは、トラフィックはシグニチャを始動させません。

テストが完了したら、変更したシグニチャをデフォルトに復元します。




# 関連情報

- 5500x IPS モジュールの IPS 管理設定シナリオ
- Cisco Intrusion Prevention System Sensor CLI コンフィギュレーション ガイド for IPS 7.0
- Cisco Intrusion Prevention System Sensor CLI コンフィギュレーション ガイド for IPS 7.1
- IPS Manager Express
- セキュア シェル ( SSH )
- テクニカル サポートとドキュメント – Cisco Systems