IME を使用した IPS ブロッキングの設定

目次

概要

この資料は IPS Manager Express （IME）の使用とブロックする侵入防御システム（IPS）の設定を説明します。 IME および IPS センサーがブロックのための Ciscoルータを管理するのに使用されています。 この設定を考慮するときこれらの項目を覚えていて下さい:

- センサーをインストールし、センサー作業をきちんと確かめて下さい。
- スニフィング インターフェイスのスパンを、インターフェイス外部のルータまで及ぶようにします。

前提条件

要件

このドキュメントに関する固有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、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IPS Manager Express 7.0

- Cisco IPS センサー 7.0(0.88)E3
- Cisco IOS ソフトウェア リリース 12.4 の Cisco IOS ® ルータ

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。

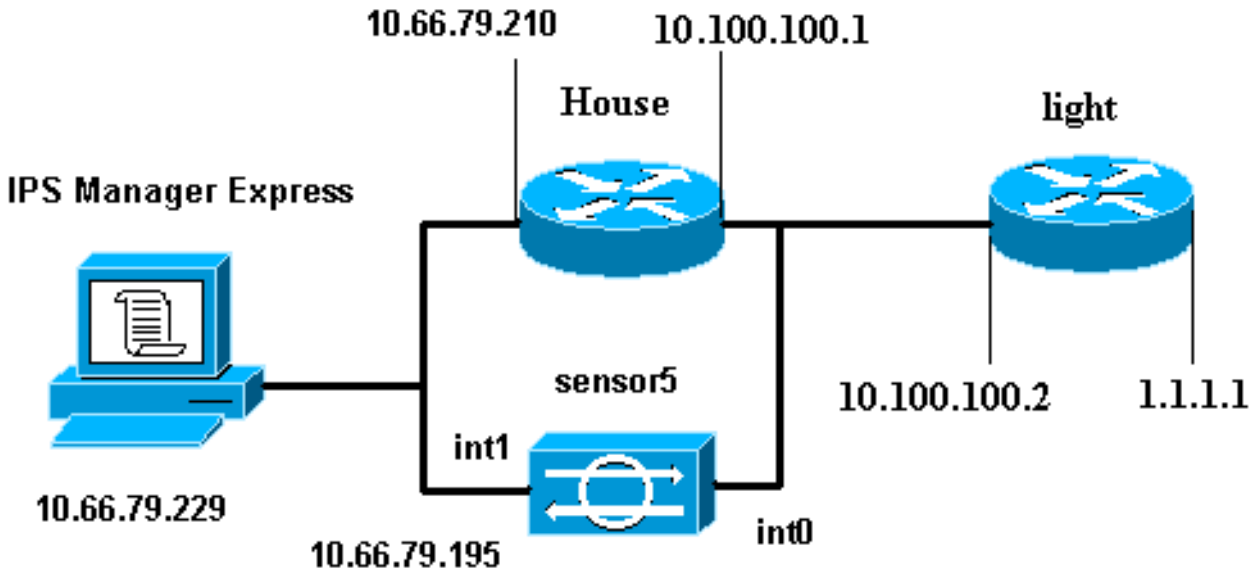
表記法

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。

設定

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



設定

このドキュメントでは、次の設定を使用します。

- Router Light
- Router House

Router Light
Current configuration : 906 bytes ! version 12.4 service timestamps debug uptime service timestamps log uptime no service password-encryption ! **hostname light** ! enable password cisco ! username cisco

```
password 0 cisco ip subnet-zero ! ! ! ip ssh time-out
120 ip ssh authentication-retries 3 ! call rsvp-sync ! !
! fax interface-type modem mta receive maximum-
recipients 0 ! controller E1 2/0 ! ! ! interface
FastEthernet0/0 ip address 10.100.100.2 255.255.255.0
duplex auto speed auto ! interface FastEthernet0/1 ip
address 1.1.1.1 255.255.255.0 duplex auto speed auto !
interface BRI4/0 no ip address shutdown interface BRI4/1
no ip address shutdown ! interface BRI4/2 no ip address
shutdown ! interface BRI4/3 no ip address shutdown ! ip
classless ip route 0.0.0.0 0.0.0.0 10.100.100.1 ip http
server ip pim bidir-enable ! ! dial-peer cor custom ! !
line con 0 line 97 108 line aux 0 line vty 0 4 login !
end
```

Router House

```
Current configuration : 939 bytes
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname house ! logging queue-limit 100 enable password
cisco ! ip subnet-zero ! ! no ip cef no ip domain lookup
! ip audit notify log ip audit po max-events 100 ! ! no
voice hpi capture buffer no voice hpi capture
destination ! ! ! ! interface FastEthernet0/0 ip address
10.66.79.210 255.255.255.224 duplex auto speed auto !
interface FastEthernet0/1 ip address 10.100.100.1
255.255.255.0 ip access-group IDS_FastEthernet0/1_in_0
in !--- After you configure blocking, !--- IDS Sensor
inserts this line. duplex auto speed auto ! interface
ATM1/0 no ip address shutdown no atm ilmi-keepalive ! ip
classless ip route 0.0.0.0 0.0.0.0 10.66.79.193 ip route
1.1.1.0 255.255.255.0 10.100.100.2 no ip http server no
ip http secure-server ! ! ip access-list extended
IDS_FastEthernet0/1_in_0 permit ip host 10.66.79.195 any
permit ip any any !--- After you configure blocking, !--
- IDS Sensor inserts this line. ! call rsvp-sync ! !
mgcp profile default ! ! line con 0 exec-timeout 0 0
line aux 0 line vty 0 4 exec-timeout 0 0 password cisco
login line vty 5 15 login ! ! end
```

センサー設定を開始して下さい

センサーの設定を開始するためにこれらのステップを完了して下さい。

1. センサーに初めてログインする場合は、ユーザ名 cisco、パスワード cisco を入力する必要があります。
2. システムがパスワード変更のプロンプトを表示したら、パスワードを変更します。**注**：Cisco123 は辞書ワードで、システムで許されません。
3. **セットアップを**入力し、センサーのための基本的なパラメータを設定するためにシステムプロンプトに従って下さい。
4. 次の情報を入力します。`sensor5#setup --- System Configuration Dialog --- !--- At any point you may enter a question mark '?' for help. !--- Use ctrl-c to abort the configuration dialog at any prompt. !--- Default settings are in square brackets '[]'. Current time: Thu Oct 22 21:19:51 2009 Setup Configuration last modified: Enter host name[sensor]: Enter IP interface[10.66.79.195/24,10.66.79.193]: Modify current access list?[no]: Current access`

```
list entries: !--- permit the ip address of workstation or network with IME
Permit:10.66.79.0/24 Permit: Modify system clock settings?[no]: Modify summer time
settings?[no]: Use USA SummerTime Defaults?[yes]: Recurring, Date or Disable?[Recurring]:
Start Month[march]: Start Week[second]: Start Day[sunday]: Start Time[02:00:00]: End
Month[november]: End Week[first]: End Day[sunday]: End Time[02:00:00]: DST Zone[]:
Offset[60]: Modify system timezone?[no]: Timezone[UTC]: UTC Offset[0]: Use NTP?[no]: yes
NTP Server IP Address[]: Use NTP Authentication?[no]: yes NTP Key ID[]: 1 NTP Key Value[]:
8675309
```

5. 設定を保存します。設定を保存するためにセンサーのための数分かかる場合があります。

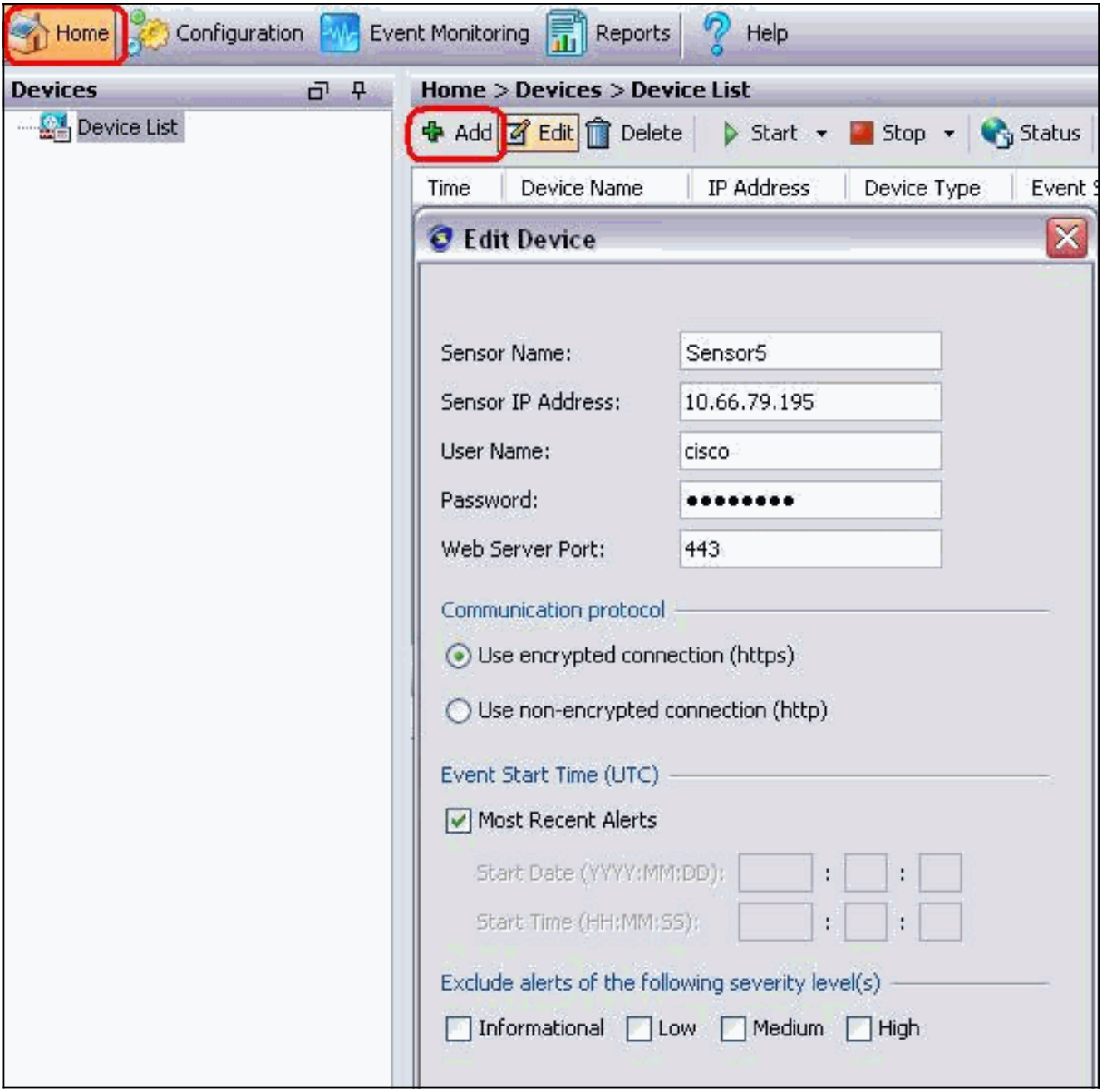
```
[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.

Enter your selection[2]: 2
```

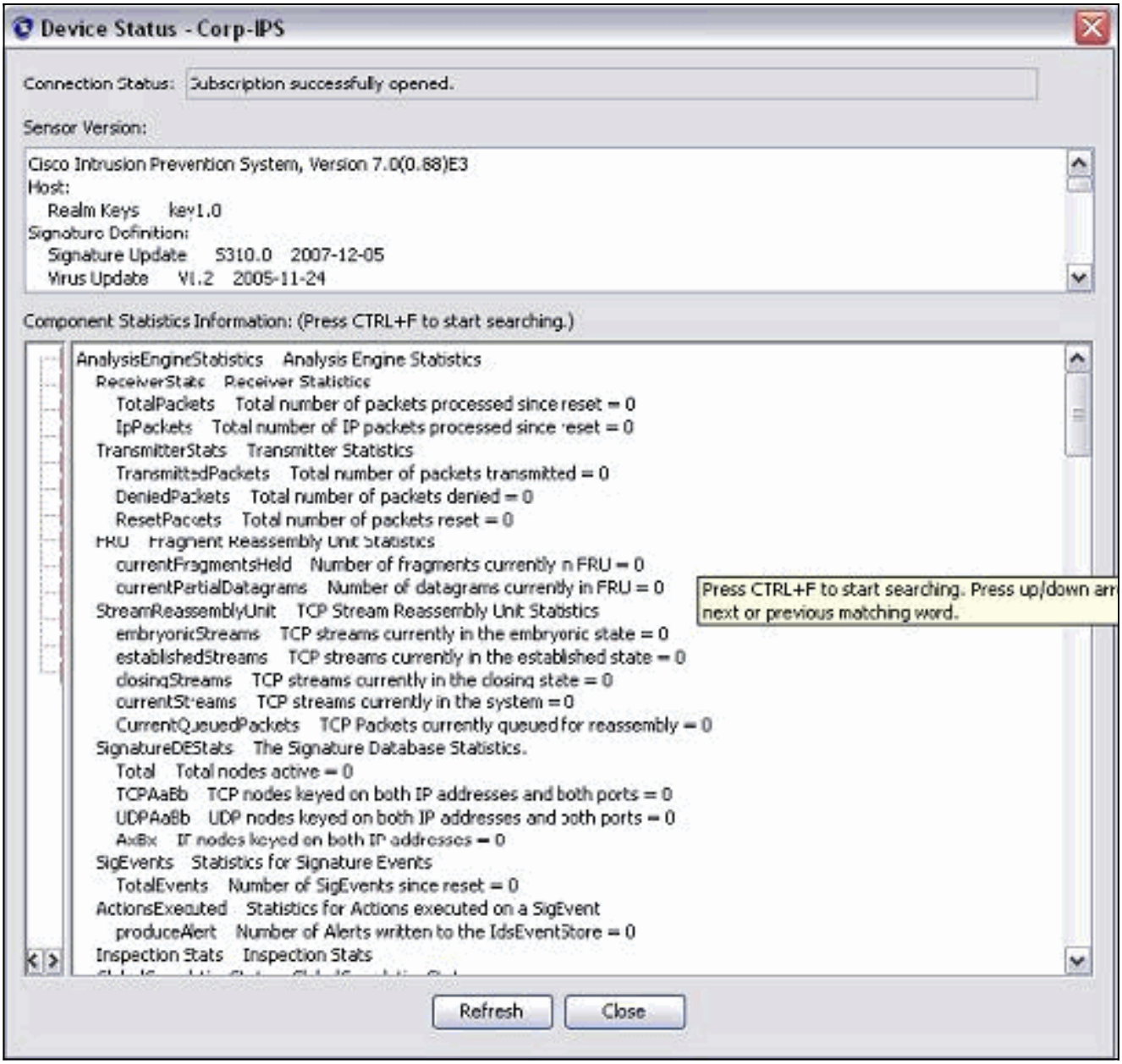
IME にセンサーを追加して下さい

IME にセンサーを追加するためにこれらのステップを完了して下さい。

1. IPS Manager Express をインストールし、**IPS Manager Express を**開く Windows PC に行って下さい。
2. **> Add を**『Home』 を選択 して下さい。
3. この情報を入力し、設定を終了するために『OK』 をクリック して下さい。



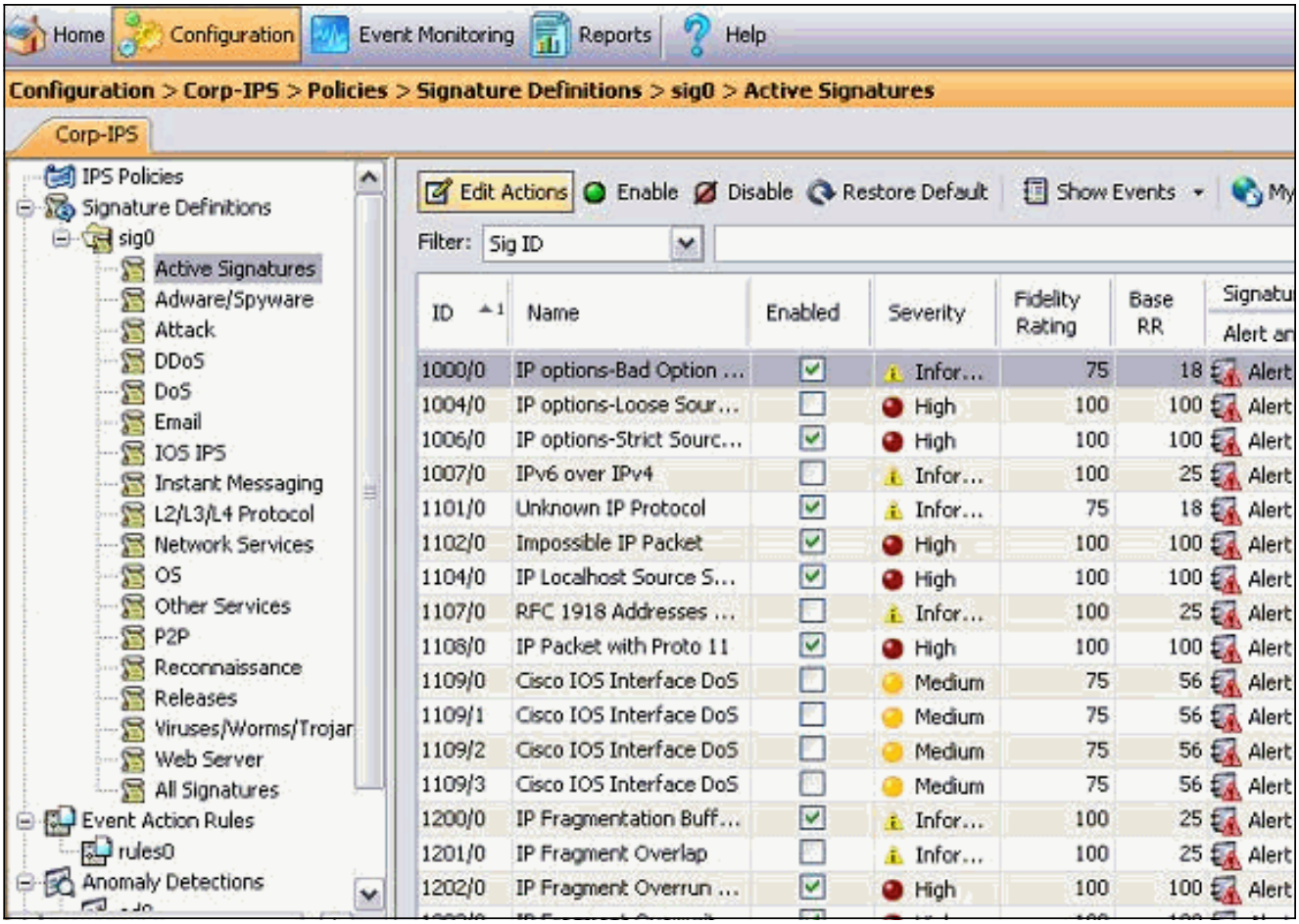
4. センサー ステータスを確認し、次に『Status』 を選択 するために右クリックするために Devices > sensor5 の順に選択 して下さい。うまく*開く*サブスクリプションを表示できることを確かめて下さい。 メッセージに応答します。



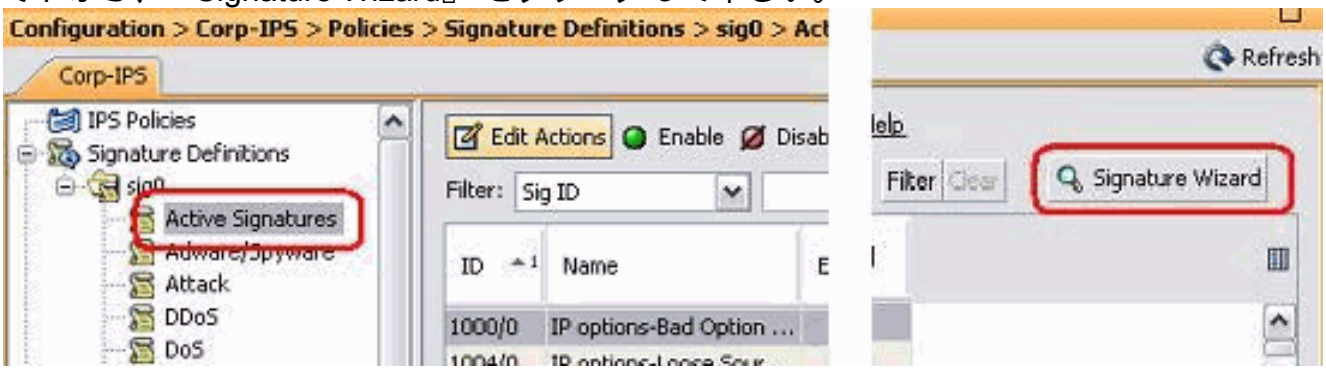
Cisco IOS ルータのための設定 ブロッキング

Cisco IOS ルートのためのブロッキングを設定するためにこれらのステップを完了して下さい:。

1. IME PC から、Webブラウザを開き、**https://10.66.79.195** に行って下さい。
2. センサーからダウンロードされる HTTPS 認証を受け入れるために『OK』 をクリック して下さい。
3. Login ウィンドウで、ユーザ名に cisco、パスワードに 123cisco123 を入力します。この IME マネージメントインターフェイスは現われます
:

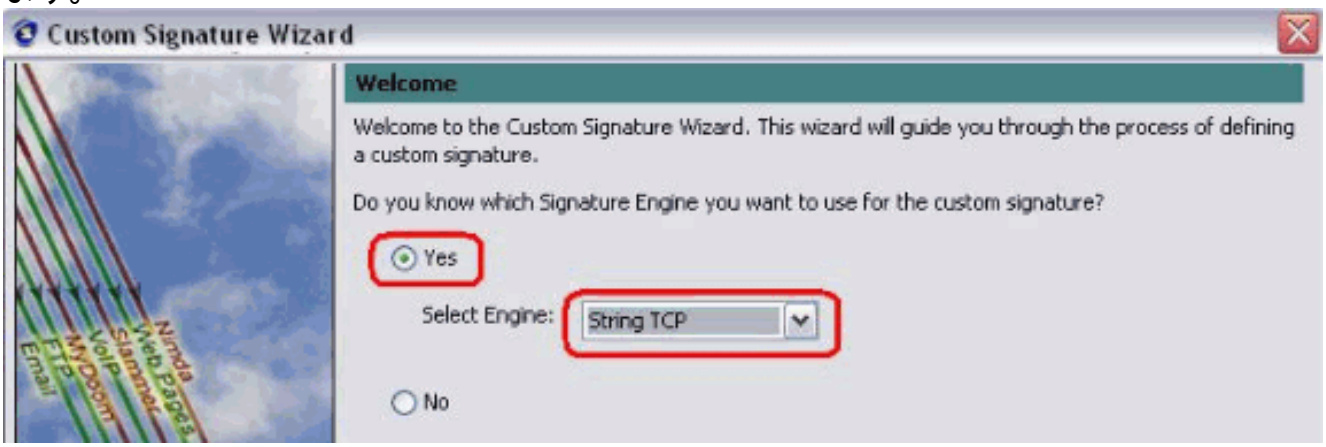


4. Configuration タブから、**アクティブなシグニチャを**クリックして下さい。
5. それから、『Signature Wizard』 をクリック して下さい。

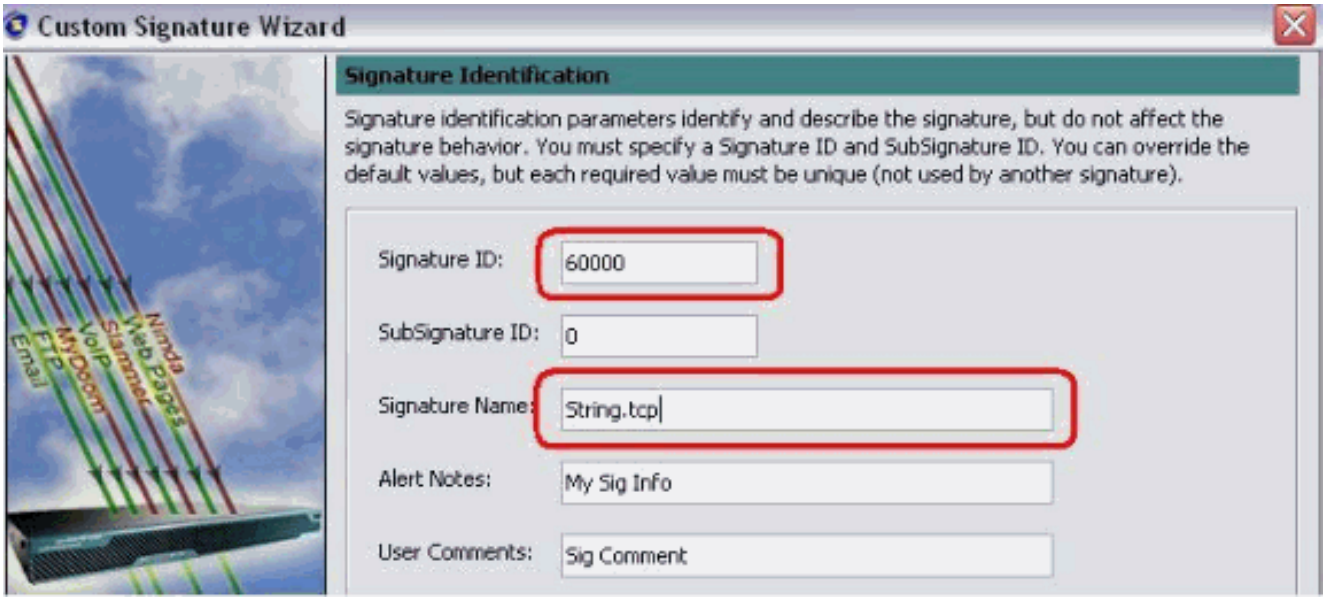


注: 前のスクリーン ショットはスペース制限が理由で 2 人の部に切られました。

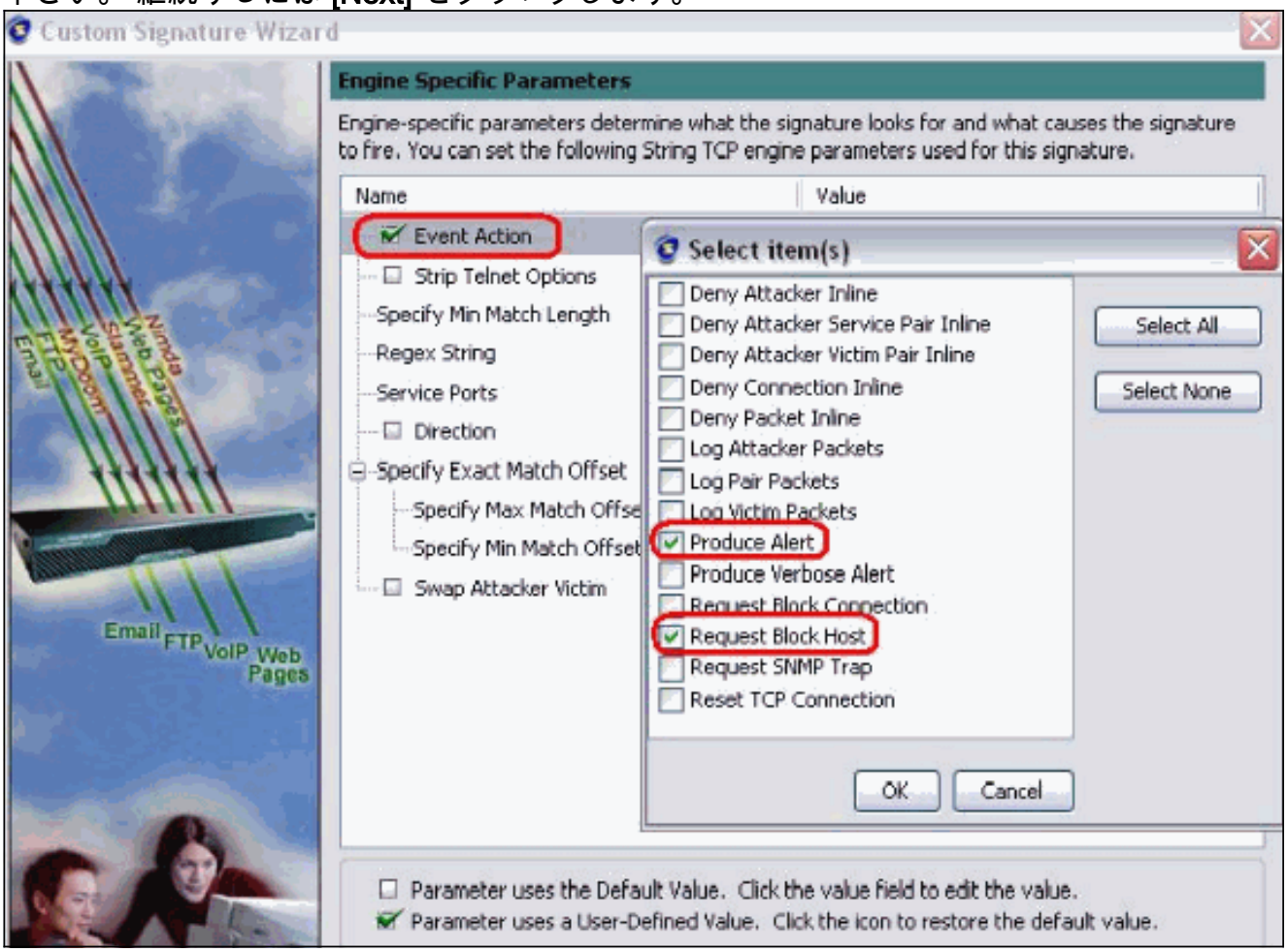
6. シグニチャ エンジンとして**ストリング TCP** 『Yes』 を選択 すれば。 [Next] をクリックします。



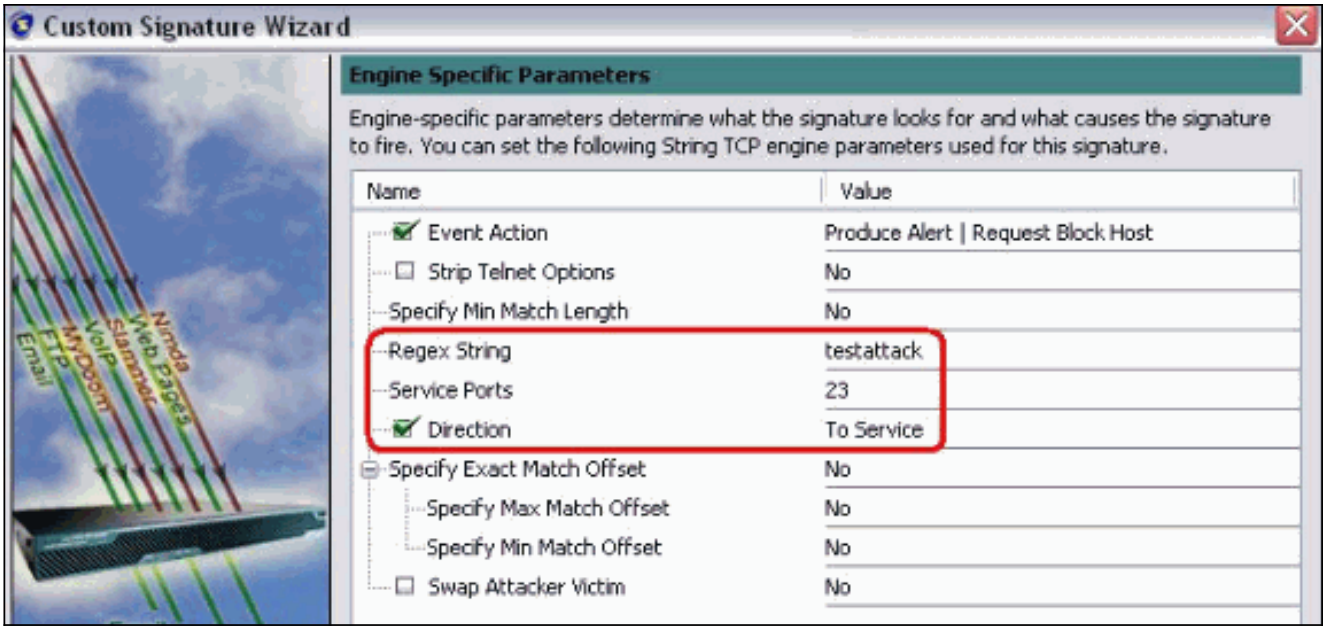
7. デフォルトとしてこの情報を残すか、またはあなた自身のシグニチャ ID、シグニチャ名前 およびユーザ メモを入力することができます。 [Next] をクリックします。



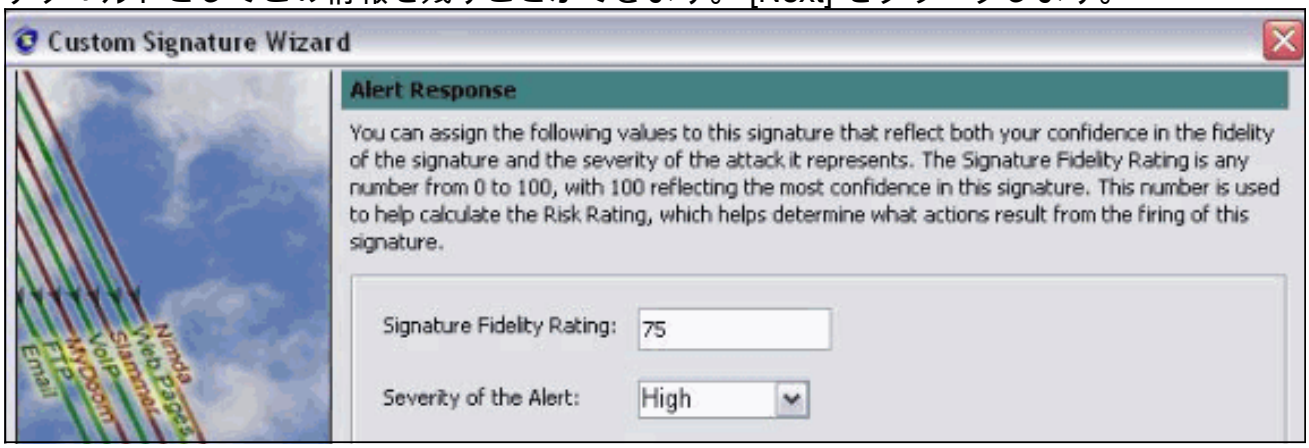
8. **検知時のアクションを**選択し、**生成 します アラート**および**要求ブロック ホストを**選択して下さい。 継続するには **[Next]** をクリックします。



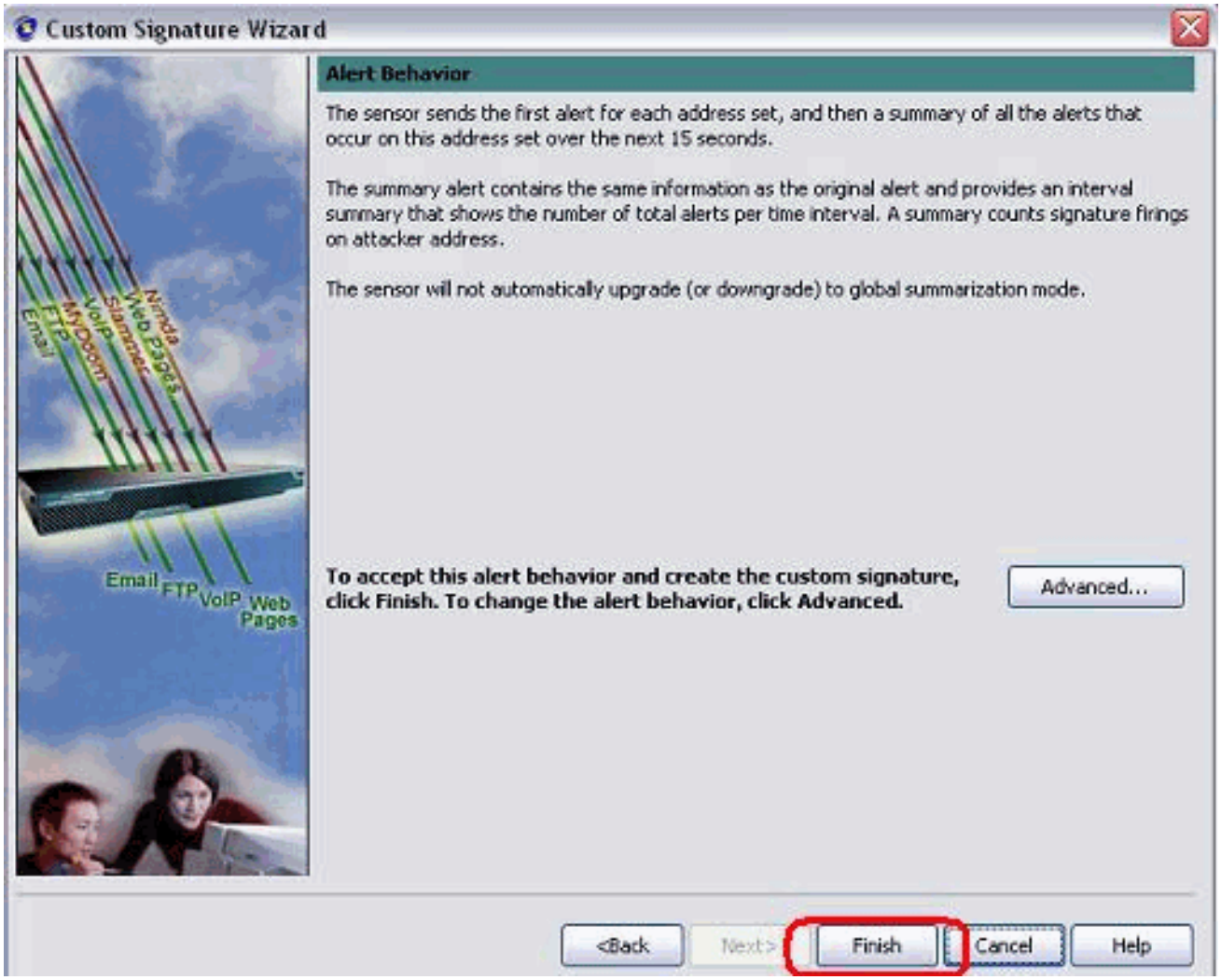
9. この例の *testattack* である正規表現を入力しサービス ポートのための **23 を**、方向のために**保守することを**選択し続くために『Next』 をクリック します入力して下さい。



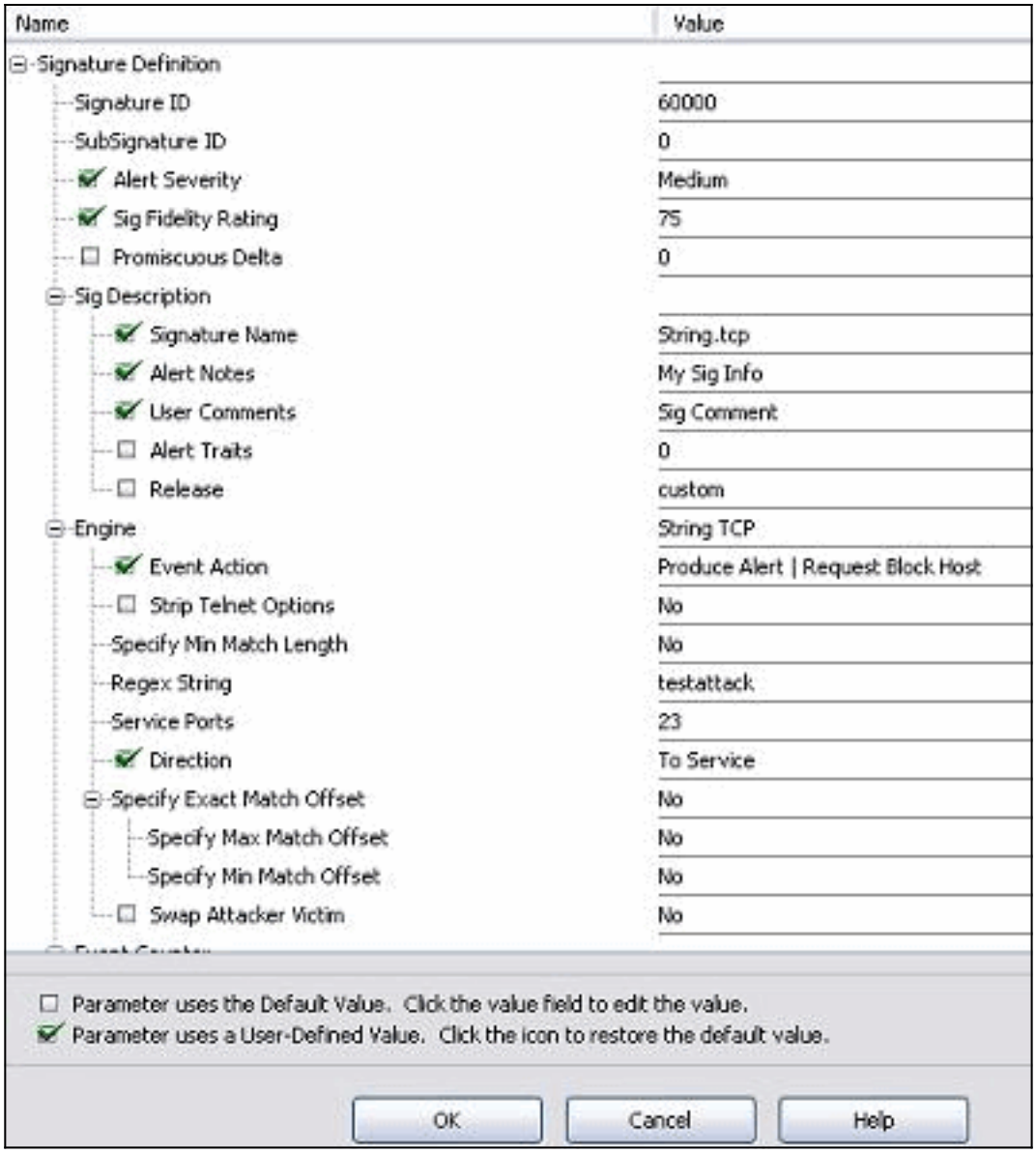
10. デフォルトとしてこの情報を残すことができます。 [Next] をクリックします。



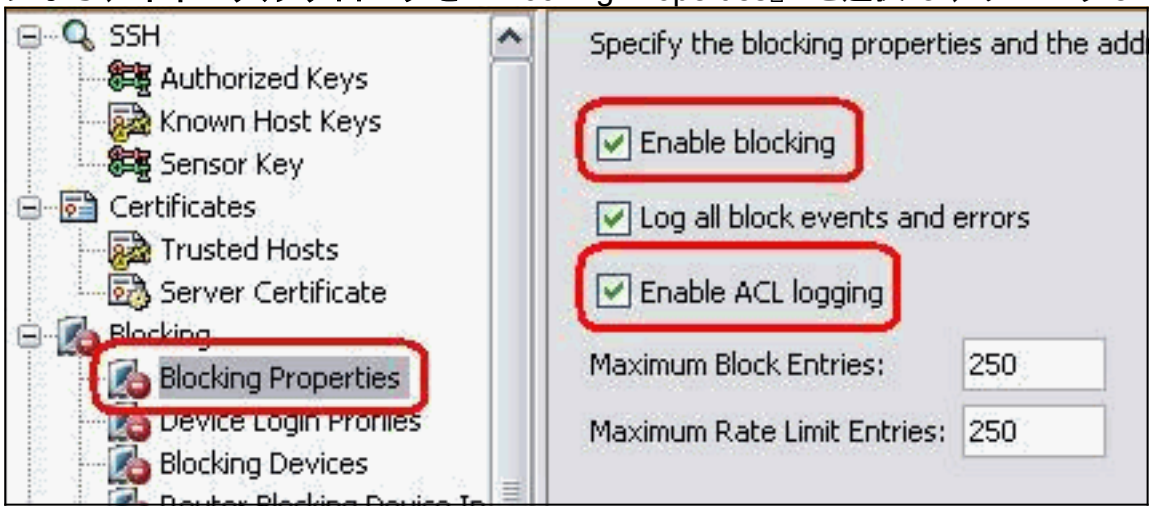
11. ウィザードを終えるために『Finish』 をクリック して下さい。



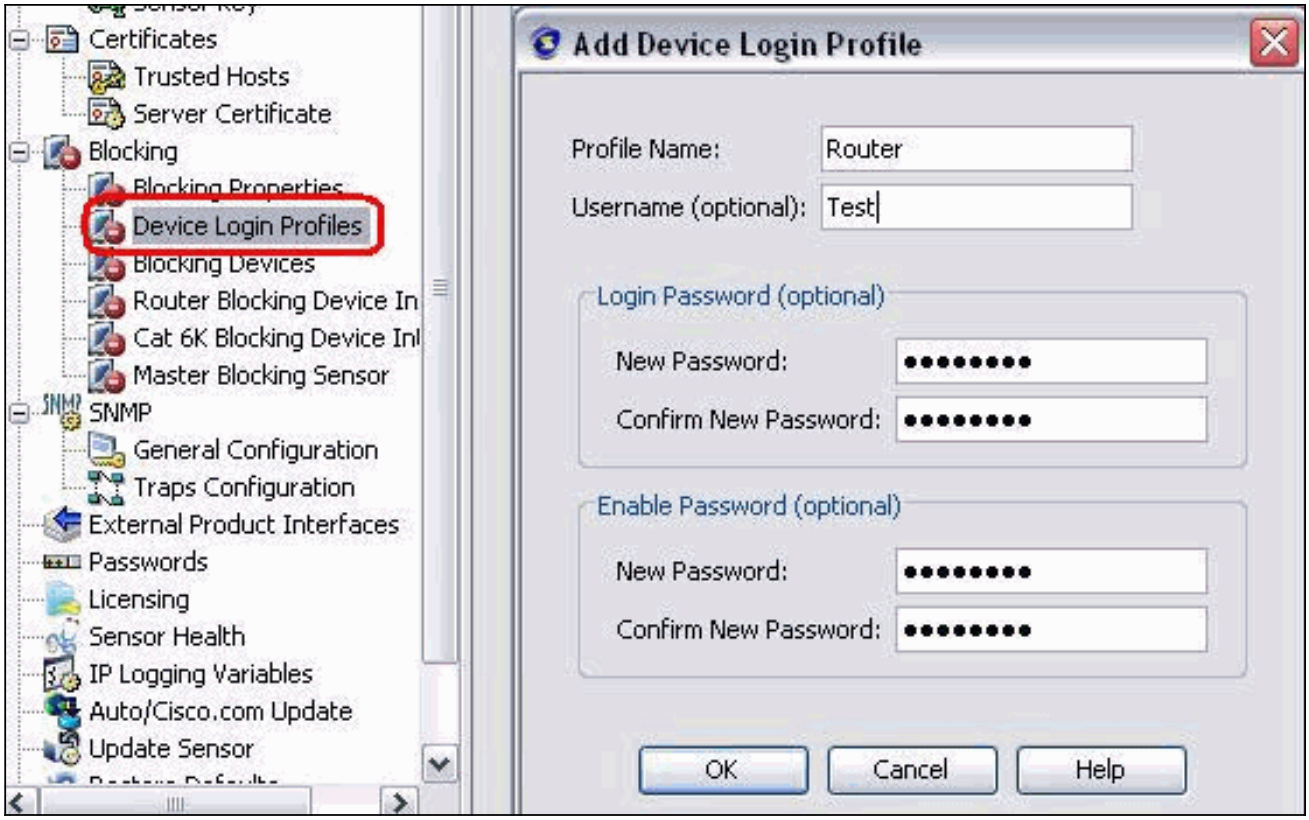
12. **> sig0 >** 順序で**アクティブなシグニチャ**見つけます **SIG ID** か **SIG 名前**によって新しく作成されたシグニチャを『Configuration』 を選択 して下さい。 シグニチャを表示するために『Edit』 をクリック して下さい。



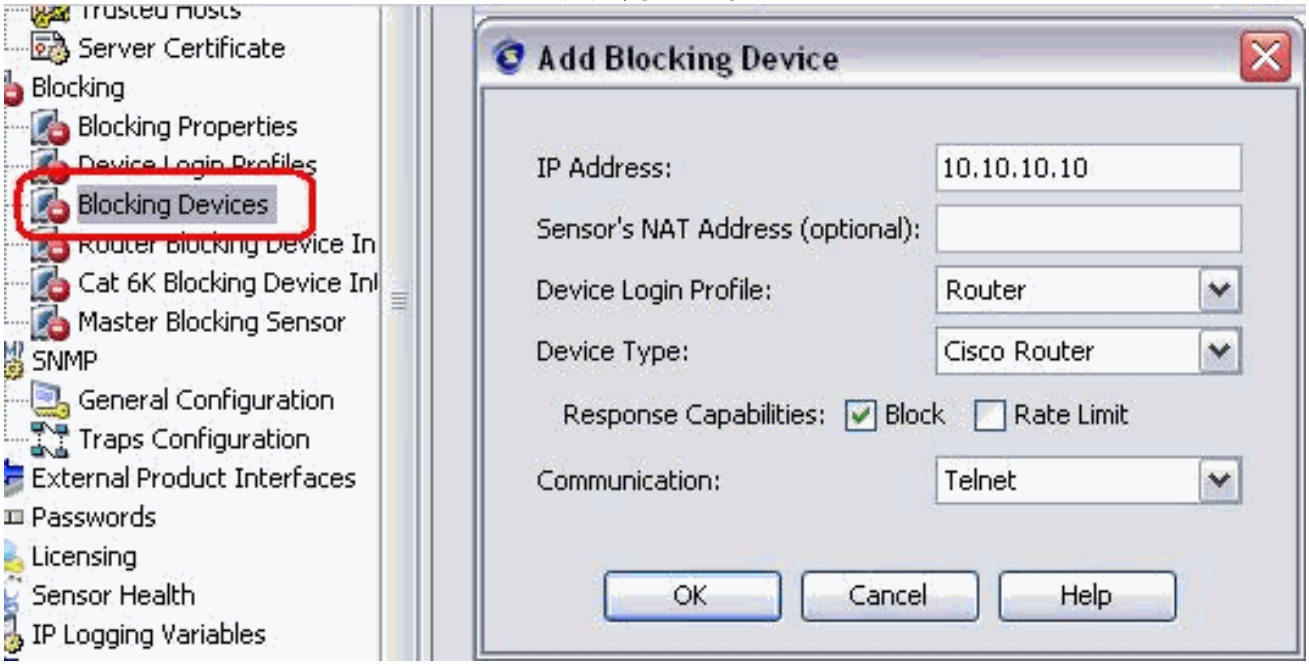
13. センサーにシグニチャを加えるために **Apply ボタンを**確認した、クリックする後『OK』をクリック して下さい。
14. センサー管理の下の Configuration タブから、『Blocking』 をクリック して下さい。 左ペインから、**イネーブル ブロックを**『Blocking Properties』 を選択 し、チェックして下さい。



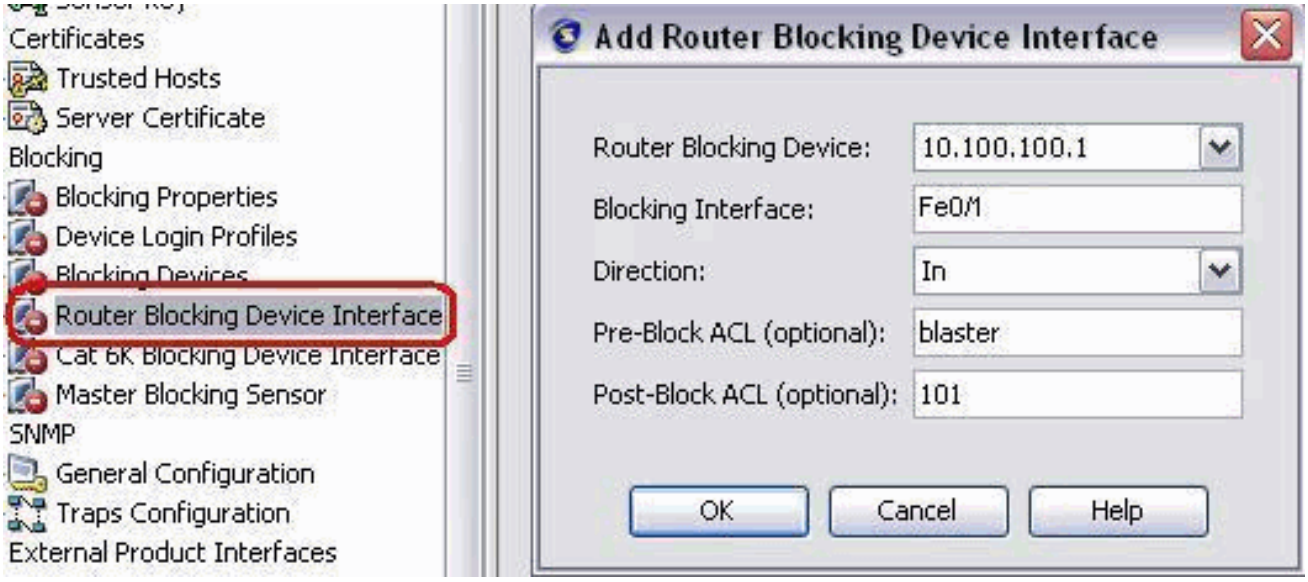
15. この場合左ペインから、**デバイス ログイン プロファイル**に行って下さい。 新しいプロファイルを作成するために、『Add』 をクリック して下さい。 作成される『OK』 をクリック し、センサーを**加え、**続けて下さい。



16. 次 の ステップはブロック デバイスでルータを設定することです。 左ペインから、**デバイスを**、この情報を追加するために『Add』 をクリック します 『Blocking』 を選択 して下さい。 それから『OK』 をクリック し、**適用して下さい。**



17. この場合左ペインからブロック デバイス インターフェイスを設定して下さい。 情報を追加し、『OK』 をクリック し、**適用して下さい。**



確認

攻撃およびブロッキングを起動させて下さい

攻撃およびブロッキングを起動させるためにこれらのステップを完了して下さい:

1. 攻撃を開始する前に、行き、**イベントモニタリングを > 廃棄された不正侵入ビューは** IME に選択し、右のセンサーを選択します。
2. ルータ House に Telnet で接続し、これらのコマンドでサーバからの通信を確認して下さい。`house#show user Line User Host(s) Idle Location * 0 con 0 idle 00:00:00 226 vty 0 idle 00:00:17 10.66.79.195 house#show access-list Extended IP access list IDS_FastEthernet0/1_in_0 permit ip host 10.66.79.195 any permit ip any any (12 matches) house#`
3. Router Light から Router House に Telnet し、testattack と入力します。Telnetセッションを再設定するために **<space>** か **<enter>** を見つけて下さい。`light#telnet 10.100.100.1 Trying 10.100.100.1 ... Open User Access Verification Password: house>en Password: house#testattack [Connection to 10.100.100.1 lost] !--- Host 10.100.100.2 has been blocked due to the !--- signature "testattack" triggered.`
4. ルータ House に Telnet で接続し、ここに示されているように **show access-list コマンドを**使用して下さい。`house#show access-list Extended IP access list IDS_FastEthernet0/1_in_0 10 permit ip host 10.66.79.195 any 20 deny ip host 10.100.100.2 any (71 matches) 30 permit ip any any`
5. IDS Event Viewer のダッシュボードから、赤い警告灯は攻撃が開始すれば現われます。

Date	Time	Sig. Name	Sig. ID
Device: Corp-IPS (188 items)			
Severity: high (188 items)			
10/23/2009	09:59:13	String.tcp	60000/0
10/23/2009	09:59:02	ZOTOB Worm Activity	5570/0
10/23/2009	09:58:57	Anig Worm File Tran...	5599/0
10/23/2009	09:59:00	Anig Worm File Tran...	5599/0
10/23/2009	09:58:58	Anig Worm File Tran...	5599/0
10/23/2009	09:59:17	Nachi Worm ICMP E...	2158/0

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

ヒント

これらのトラブルシューティング に 役立つ ヒントを使用して下さい:

- センサーから出力される **show statistics ネットワーク アクセスを**検知 し、"アクティブであることを確かめて下さい。 コンソールか SSH からセンサーへの、この情報は表示されます:

```
sensor5#show statistics network-access Current Configuration AllowSensorShun = false
ShunMaxEntries = 100 NetDevice Type = Cisco IP = 10.66.79.210 NATAddr = 0.0.0.0
Communications = telnet ShunInterface InterfaceName = FastEthernet0/1 InterfaceDirection =
in State ShunEnable = true NetDevice IP = 10.66.79.210 AclSupport = uses Named ACLs State =
Active ShunnedAddr Host IP = 10.100.100.2 ShunMinutes = 15 MinutesRemaining = 12 sensor5#
```

- 正しいプロトコルがトリプル DES と Telnet か SSH のような使用されることを通信パラメータが示すことを確かめて下さい。 手動 SSH を試みることができますまたはユーザ名 およびパスワード 資格情報をチェックするために PC の SSH/Telnet クライアントから Telnet で接続するために正しくであって下さい。 続いて、センサー自体からルータへ Telnet または SSH を試行して、ルータに正しくログインできるかどうかを確認します。

関連情報

- Cisco Secure Intrusion Prevention のサポート ページ
- テクニカルサポートとドキュメント - Cisco Systems