使用IME配置IPS TCP重置

目錄

簡介
必要條件
需求
採用元件
慣例
設定
網路圖表
組態
啟動感測器配置
將感測器新增到IME
為Cisco IOS路由器配置TCP重置
驗證
發動攻擊並重置TCP
疑難排解
提示
相關資訊

簡介

本檔案將討論使用IPS Manager Express(IME)設定入侵防禦系統(IPS)TCP重設。IME和IPS感測器用於管理用於TCP重置的Cisco路由器。檢視此設定時，請記住以下專案：

- 安裝感測器並確保感測器正常工作。
- 使監聽介面跨距介面以外的路由器。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco IPS管理員Express版本7.0
- Cisco IPS感應器7.0(0.88)E3
- 採用Cisco IOS軟體版本12.4的Cisco IOS®路由器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

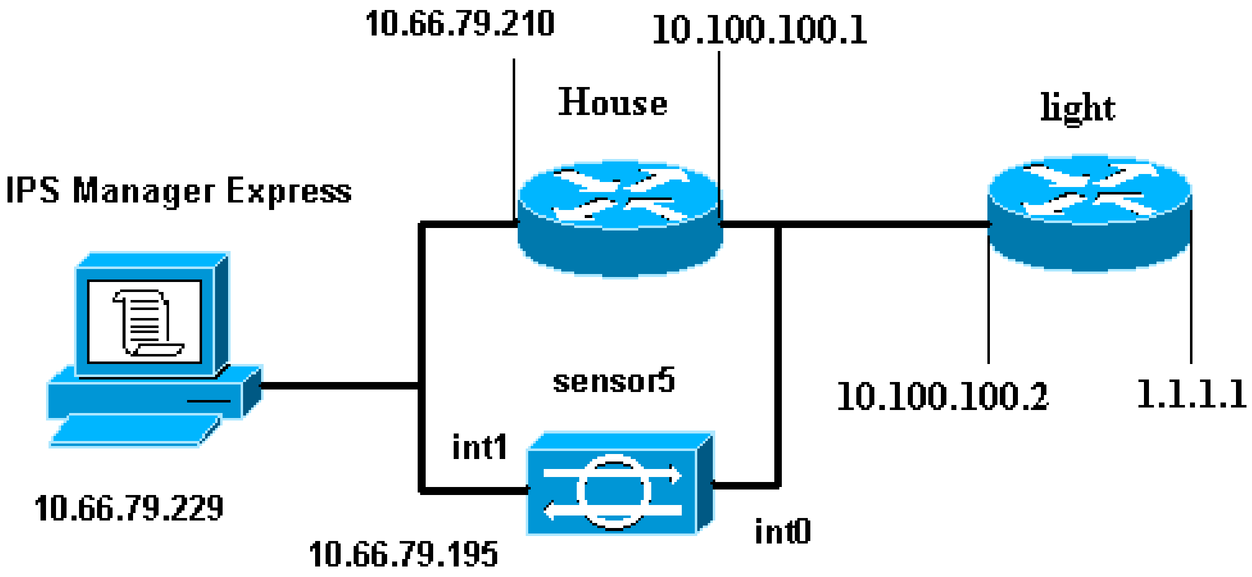
慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

設定

網路圖表

本檔案會使用下圖中所示的網路設定。



組態

本文檔使用此處顯示的配置。

- 路由器指示燈
- 路由器外殼

路由器指示燈

```
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
```

路由器外殼

```
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
 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
!
!
!
!
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
```

啟動感測器配置

完成以下步驟以開始配置感測器。

1. 如果這是您首次登入感測器，則必須輸入**cisco**作為使用者名稱，**cisco**作為密碼。
2. 系統提示時，請更改密碼。**注意：**Cisco123是一個詞典，系統不允許使用。
3. 鍵入**setup**並完成系統提示，以便為感測器設定基本引數。
4. 輸入以下資訊：

   ```
   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 Configuration:

   networkParams
   ipAddress 10.66.79.195
   netmask 255.255.255.224
   defaultGateway 10.66.79.193
   hostname Corp-IPS
   telnetOption enabled
   !--- Permit the IP address of workstation or network with IME accessList ipAddress
   10.66.79.0 netmask 255.255.255.0
   exit
   timeParams
   summerTimeParams
   active-selection none
   exit
   exit
   service webServer
   general
   ports 443
   exit
   exit
   ```
5. 儲存組態。感測器儲存配置可能需要幾分鐘時間。

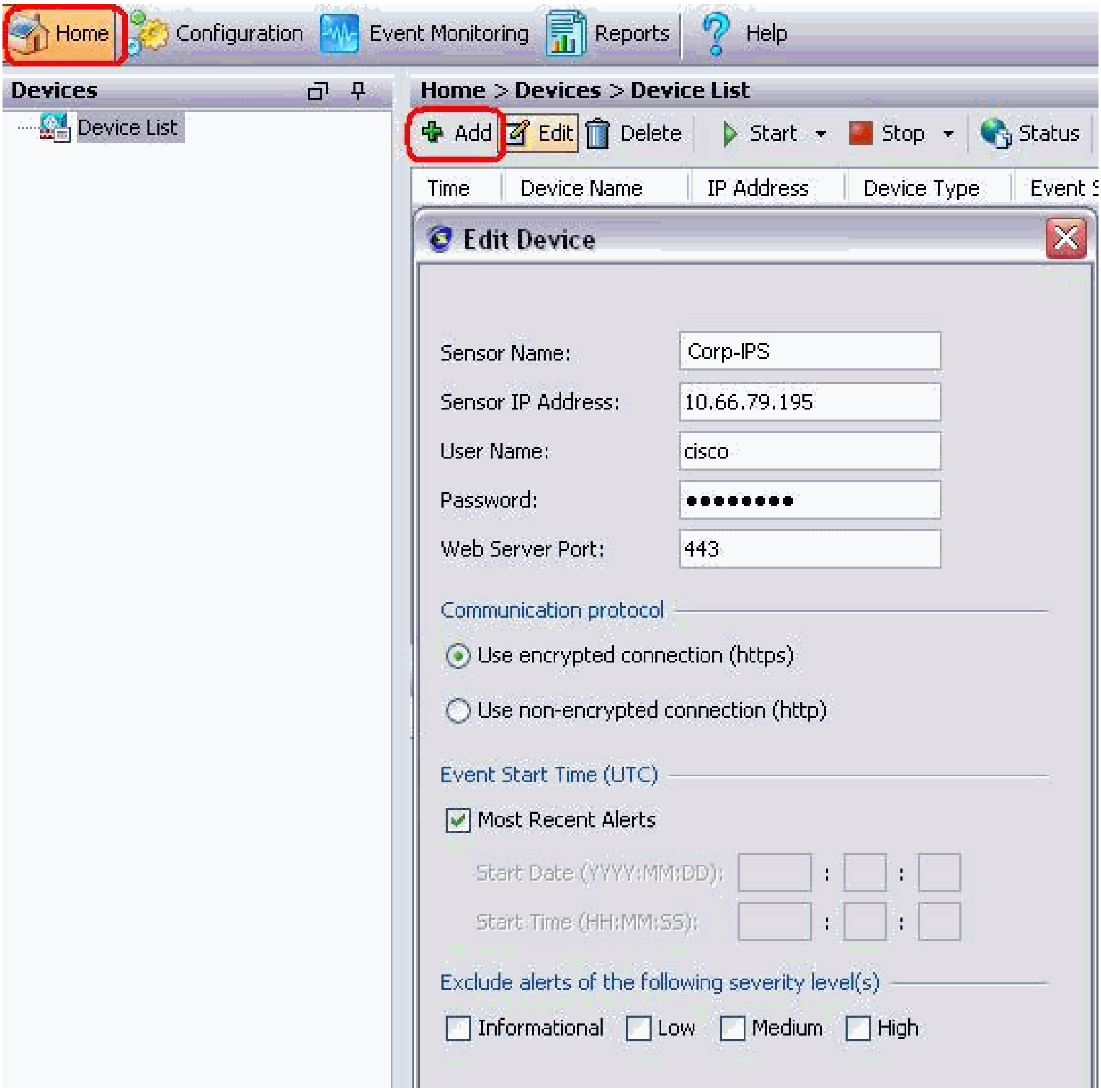
   ```
   [0] Go to the command prompt without saving this config.
   [1] Return back to the setup without saving this config.
   [2] Save this configuration and exit setup.

   Enter your selection[2]: 2
   ```

將感測器新增到IME

完成以下步驟，將感測器新增到IME:

1. 轉到安裝了IPS Manager Express的Windows PC，然後開啟IPS Manager Express。
2. 選擇**Home > Add**。



Sensor Name: Corp-IPS

Sensor IP Address: 10.66.79.195

User Name: cisco

Password: ●●●●●●●●●

Web Server Port: 443

Communication protocol

● Use encrypted connection (https)

○ Use non-encrypted connection (http)

Event Start Time (UTC)

☑ Most Recent Alerts

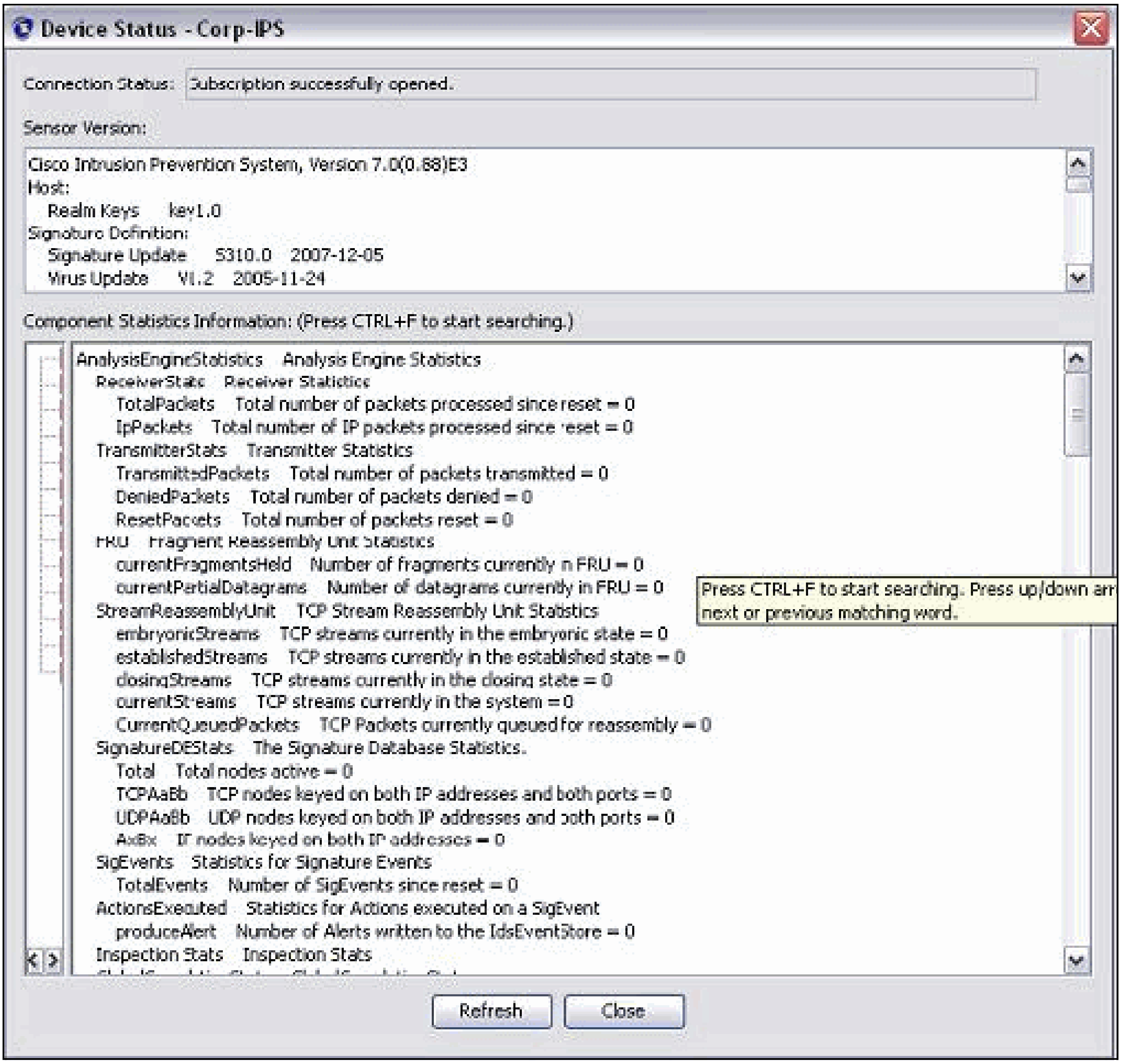
Start Date (YYYY:MM:DD): : :

Start Time (HH:MM:SS): : :

Exclude alerts of the following severity level(s)

□ Informational □ Low □ Medium □ High

3. 鍵入此資訊並按一下**OK**以完成配置。
4. 選擇**Devices > Corp-IPS**以驗證感測器狀態，然後按一下右鍵以選擇**Device Status**。確保可以看到已成功打



Connection Status: Subscription successfully opened.

Sensor Version:

```
Cisco Intrusion Prevention System, Version 7.0(0.88)E3
Host:
    Realm Keys      key1.0
Signature Definition:
    Signature Update      S310.0    2007-12-05
    Virus Update      V1.2    2005-11-24
```

Component Statistics Information: (Press CTRL+F to start searching.)

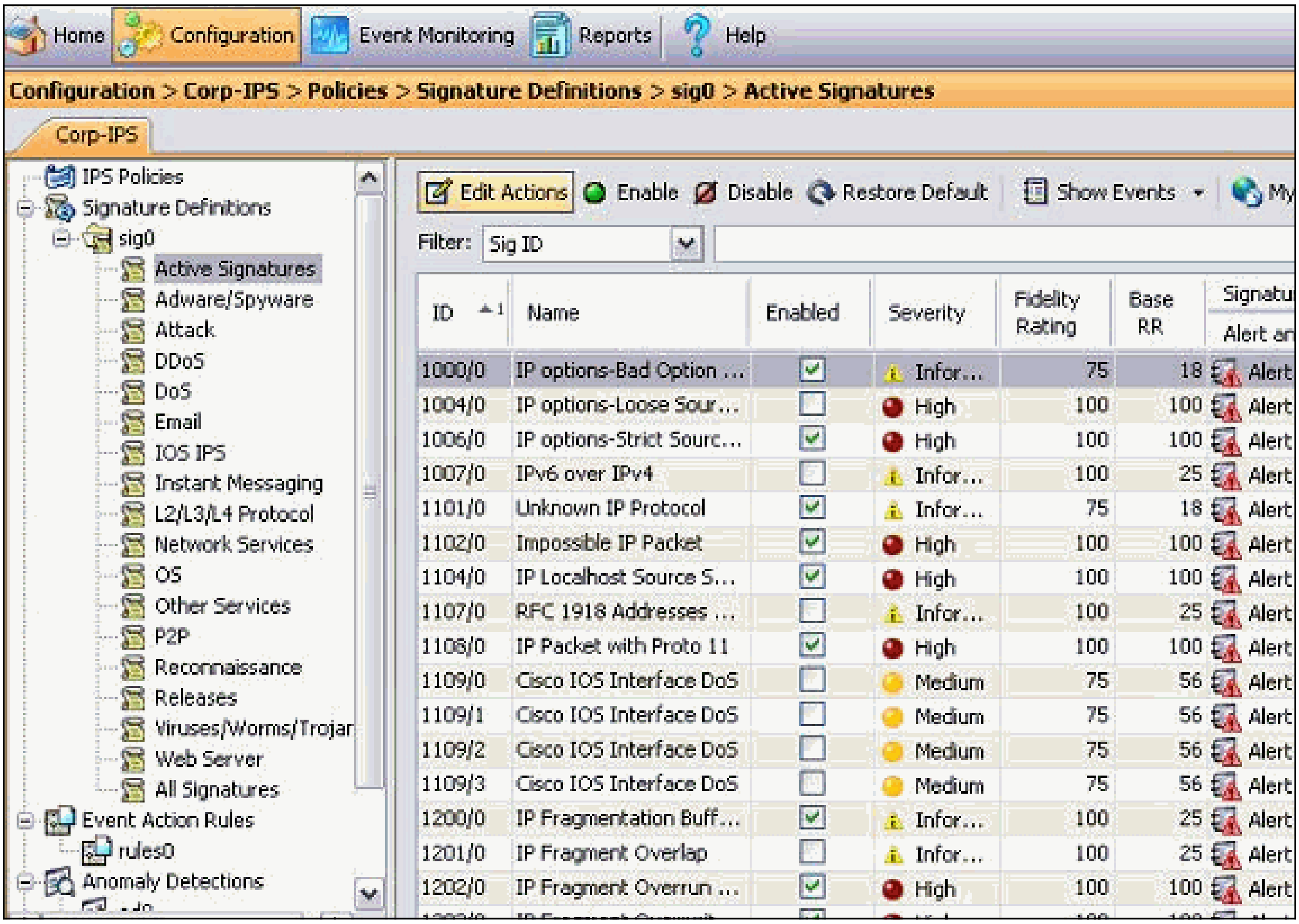
```
AnalysisEngineStatistics    Analysis Engine Statistics
   ReceiverStats    Receiver Statistics
      TotalPackets    Total number of packets processed since reset = 0
      IpPackets    Total number of IP packets processed since reset = 0
   TransmitterStats    Transmitter Statistics
      TransmittedPackets    Total number of packets transmitted = 0
      DeniedPackets    Total number of packets denied = 0
      ResetPackets    Total number of packets reset = 0
   FRU    Fragment Reassembly Unit Statistics
      currentFragmentsHeld    Number of fragments currently in FRU = 0
      currentPartialDatagrams    Number of datagrams currently in FRU = 0
   StreamReassemblyUnit    TCP Stream Reassembly Unit Statistics
      embryonicStreams    TCP streams currently in the embryonic state = 0
      establishedStreams    TCP streams currently in the established state = 0
      closingStreams    TCP streams currently in the closing state = 0
      currentStreams    TCP streams currently in the system = 0
      CurrentQueuedPackets    TCP Packets currently queued for reassembly = 0
   SignatureDEStats    The Signature Database Statistics.
      Total    Total nodes active = 0
      TCPAaBb    TCP nodes keyed on both IP addresses and both ports = 0
      UDPAaBb    UDP nodes keyed on both IP addresses and both ports = 0
      AxBx    IP nodes keyed on both IP addresses = 0
   SigEvents    Statistics for Signature Events
      TotalEvents    Number of SigEvents since reset = 0
   ActionsExecuted    Statistics for Actions executed on a SigEvent
      produceAlert    Number of Alerts written to the IdsEventStore = 0
   Inspection Stats    Inspection Stats
```

Press CTRL+F to start searching. Press up/down arr
next or previous matching word.

為Cisco IOS路由器配置TCP重置

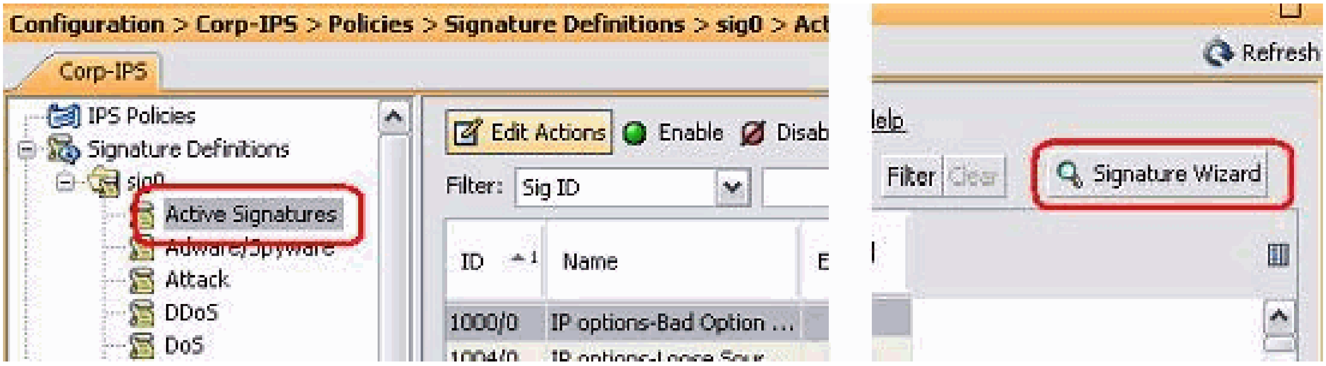
完成以下步驟，以便為Cisco IOS路由器設定TCP重設：

1. 在IME PC上，開啟Web瀏覽器，轉到**https://10.66.79.195**。
2. 按一下「**OK**」以接受從感測器下載的HTTPS證書。
3. 在登入視窗中，輸入**cisco**作為使用者名稱，輸入**123cisco123**作為密碼。出現此IME管理介面：



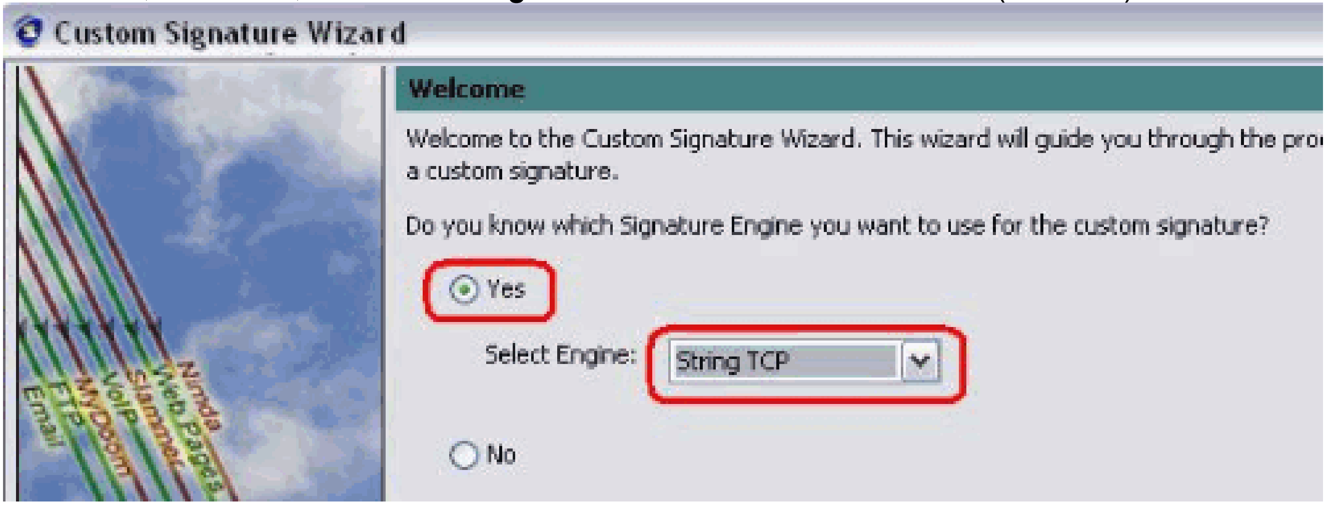
ID	Name	Enabled	Severity	Fidelity Rating	Base RR	Signatu… Alert an…
1000/0	IP options-Bad Option ...	☑	Infor...	75	18	Alert
1004/0	IP options-Loose Sour...	☐	High	100	100	Alert
1006/0	IP options-Strict Sourc...	☑	High	100	100	Alert
1007/0	IPv6 over IPv4	☐	Infor...	100	25	Alert
1101/0	Unknown IP Protocol	☑	Infor...	75	18	Alert
1102/0	Impossible IP Packet	☑	High	100	100	Alert
1104/0	IP Localhost Source S...	☑	High	100	100	Alert
1107/0	RFC 1918 Addresses ...	☐	Infor...	100	25	Alert
1108/0	IP Packet with Proto 11	☑	High	100	100	Alert
1109/0	Cisco IOS Interface DoS	☐	Medium	75	56	Alert
1109/1	Cisco IOS Interface DoS	☐	Medium	75	56	Alert
1109/2	Cisco IOS Interface DoS	☐	Medium	75	56	Alert
1109/3	Cisco IOS Interface DoS	☐	Medium	75	56	Alert
1200/0	IP Fragmentation Buff...	☑	Infor...	100	25	Alert
1201/0	IP Fragment Overlap	☐	Infor...	100	25	Alert
1202/0	IP Fragment Overrun ...	☑	High	100	100	Alert

4. 在「配置」頁籤中，按一下**活動簽名**。
5. 然後按一下**簽名嚮導**。



ID	Name
1000/0	IP options-Bad Option ...

6. 在嚮導中，選擇**Yes**，然後選擇**String TCP**作為簽名引擎。按「**Next**」（下一步）。



Welcome

Welcome to the Custom Signature Wizard. This wizard will guide you through the pro
a custom signature.

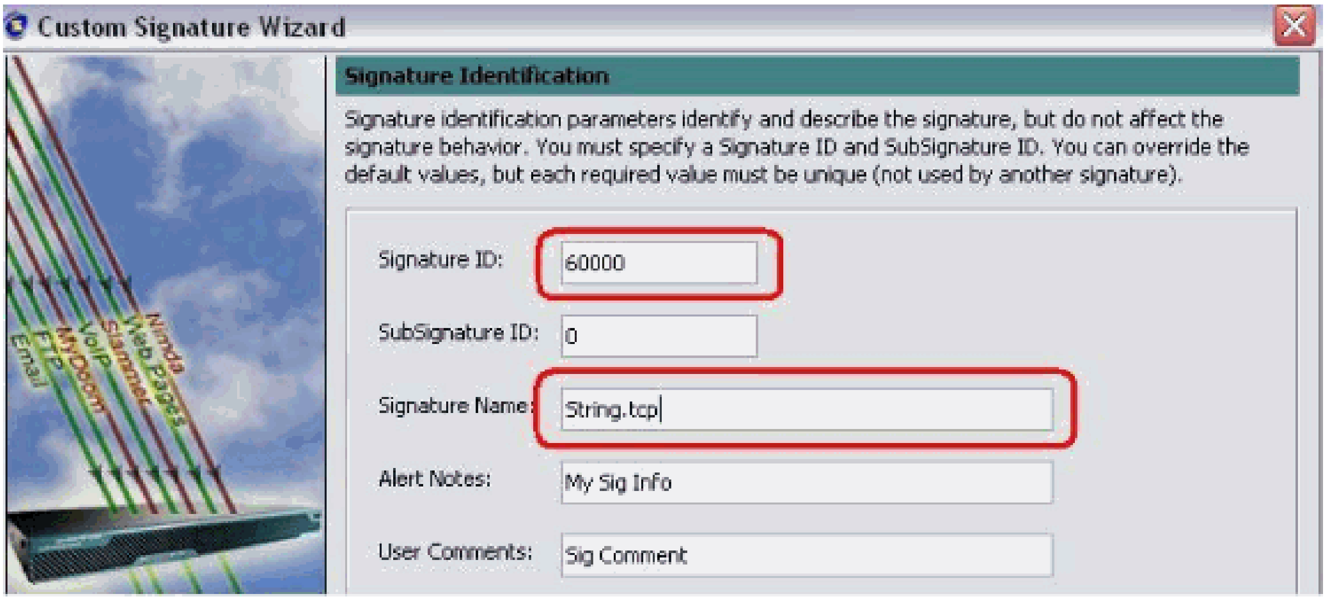
Do you know which Signature Engine you want to use for the custom signature?

● Yes

Select Engine: String TCP

○ No

7. 您可以將此資訊保留為預設值，或輸入自己的簽名ID、簽名名稱和使用者註釋。按「**Next**」（下一步）。



Custom Signature Wizard

Signature Identification

Signature identification parameters identify and describe the signature, but do not affect the signature behavior. You must specify a Signature ID and SubSignature ID. You can override the default values, but each required value must be unique (not used by another signature).

Signature ID: 60000

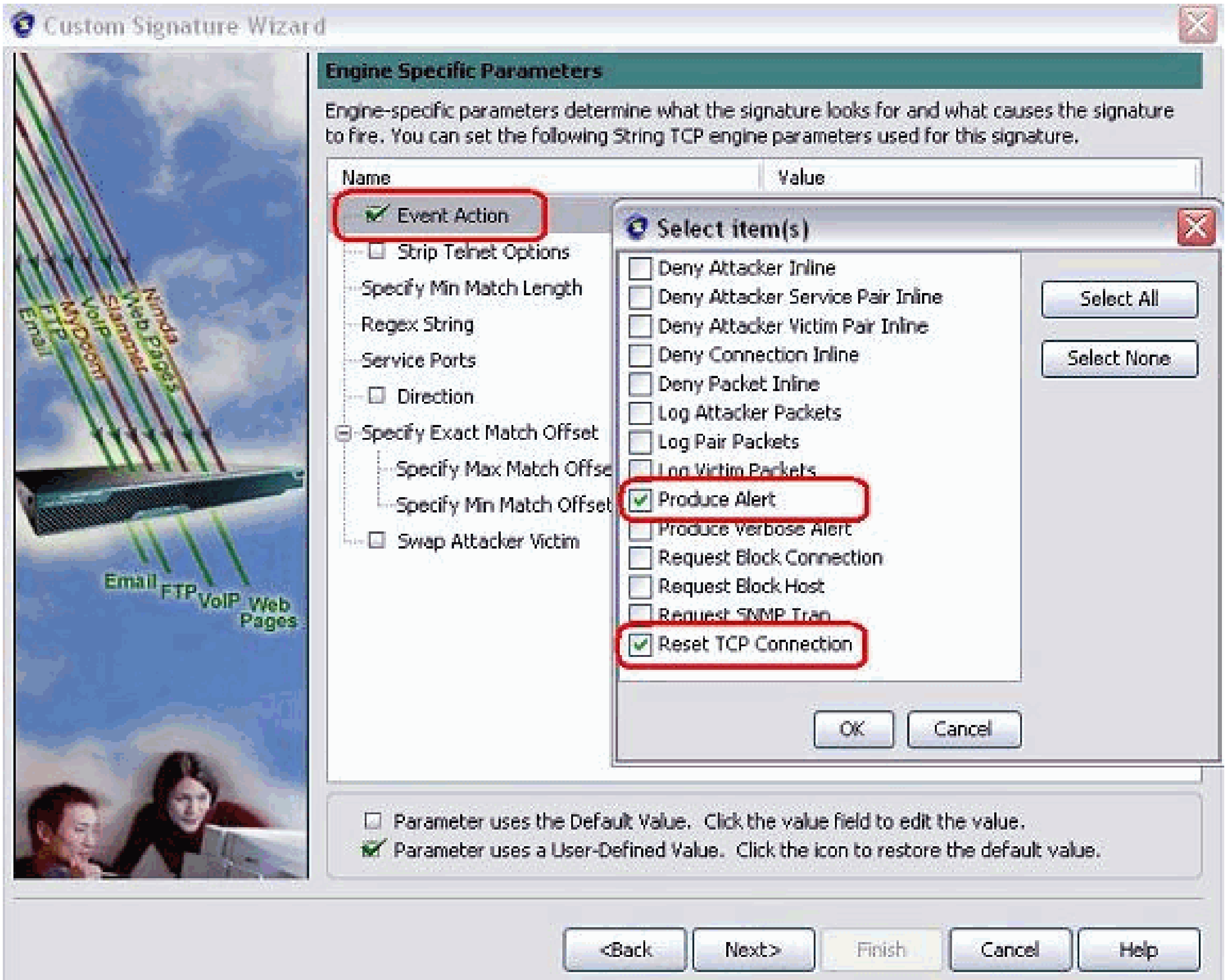
SubSignature ID: 0

Signature Name: String.tcp

Alert Notes: My Sig Info

User Comments: Sig Comment

8. 選擇**Event Action**，然後選擇**Produce Alert**和**Reset TCP Connection**。按一下「**OK**」，然後「**Next**」以繼續。



Custom Signature Wizard

Engine Specific Parameters

Engine-specific parameters determine what the signature looks for and what causes the signature to fire. You can set the following String TCP engine parameters used for this signature.

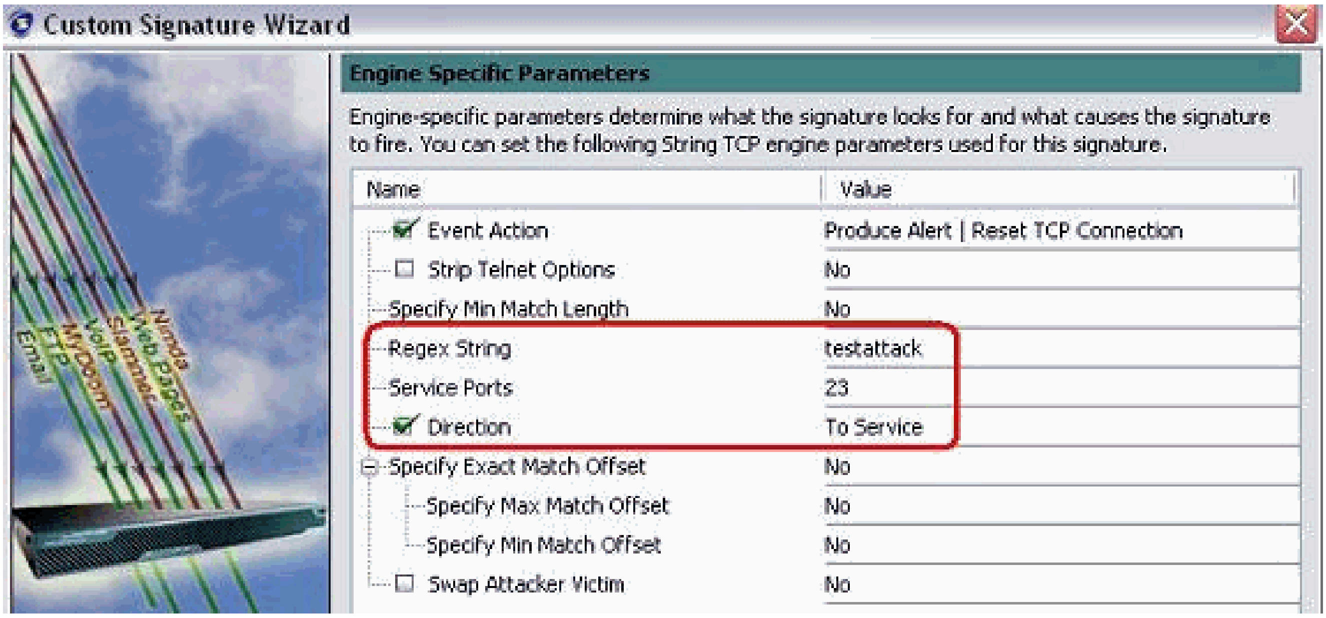
Name	Value
✓ Event Action	
□ Strip Telnet Options	
Specify Min Match Length	
Regex String	
Service Ports	
□ Direction	
⊟ Specify Exact Match Offset	
Specify Max Match Offse	
Specify Min Match Offset	
□ Swap Attacker Victim	

Select item(s)

□ Deny Attacker Inline
□ Deny Attacker Service Pair Inline
□ Deny Attacker Victim Pair Inline
□ Deny Connection Inline
□ Deny Packet Inline
□ Log Attacker Packets
□ Log Pair Packets
□ Log Victim Packets
☑ Produce Alert
□ Produce Verbose Alert
□ Request Block Connection
□ Request Block Host
□ Request SNMP Trap
☑ Reset TCP Connection

□ Parameter uses the Default Value. Click the value field to edit the value.
✓ Parameter uses a User-Defined Value. Click the icon to restore the default value.

9. 輸入正規表示式，本示例中使用`testattack`。輸入**23**作為Service Ports，選擇**To Service**作為Direction，然後按一下**Next**以繼續。



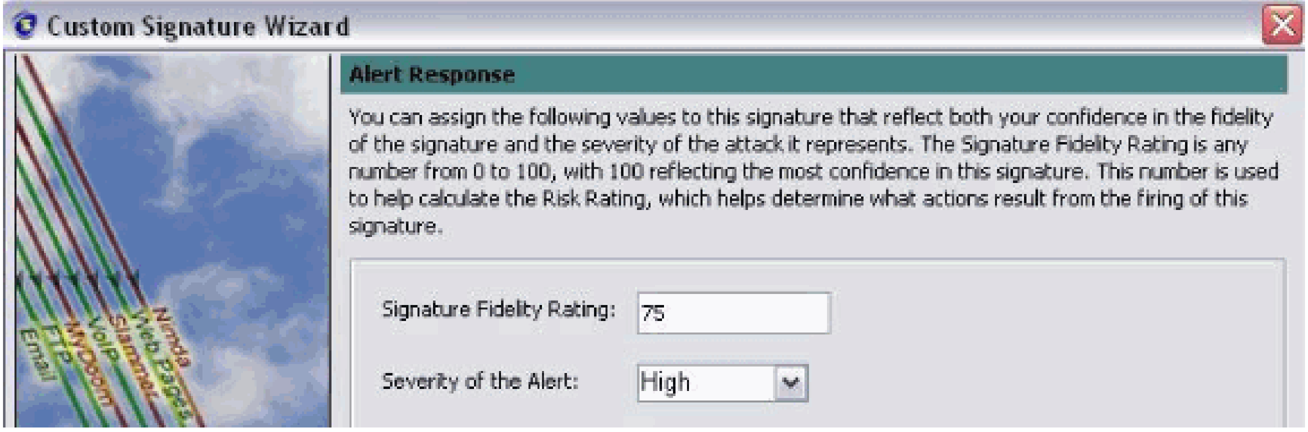
Custom Signature Wizard

Engine Specific Parameters

Engine-specific parameters determine what the signature looks for and what causes the signature to fire. You can set the following String TCP engine parameters used for this signature.

Name	Value
☑ Event Action	Produce Alert | Reset TCP Connection
□ Strip Telnet Options	No
Specify Min Match Length	No
Regex String	testattack
Service Ports	23
☑ Direction	To Service
Specify Exact Match Offset	No
Specify Max Match Offset	No
Specify Min Match Offset	No
□ Swap Attacker Victim	No

10. 可以將此資訊保留為預設值。按「**Next**」（下一步）。



Custom Signature Wizard

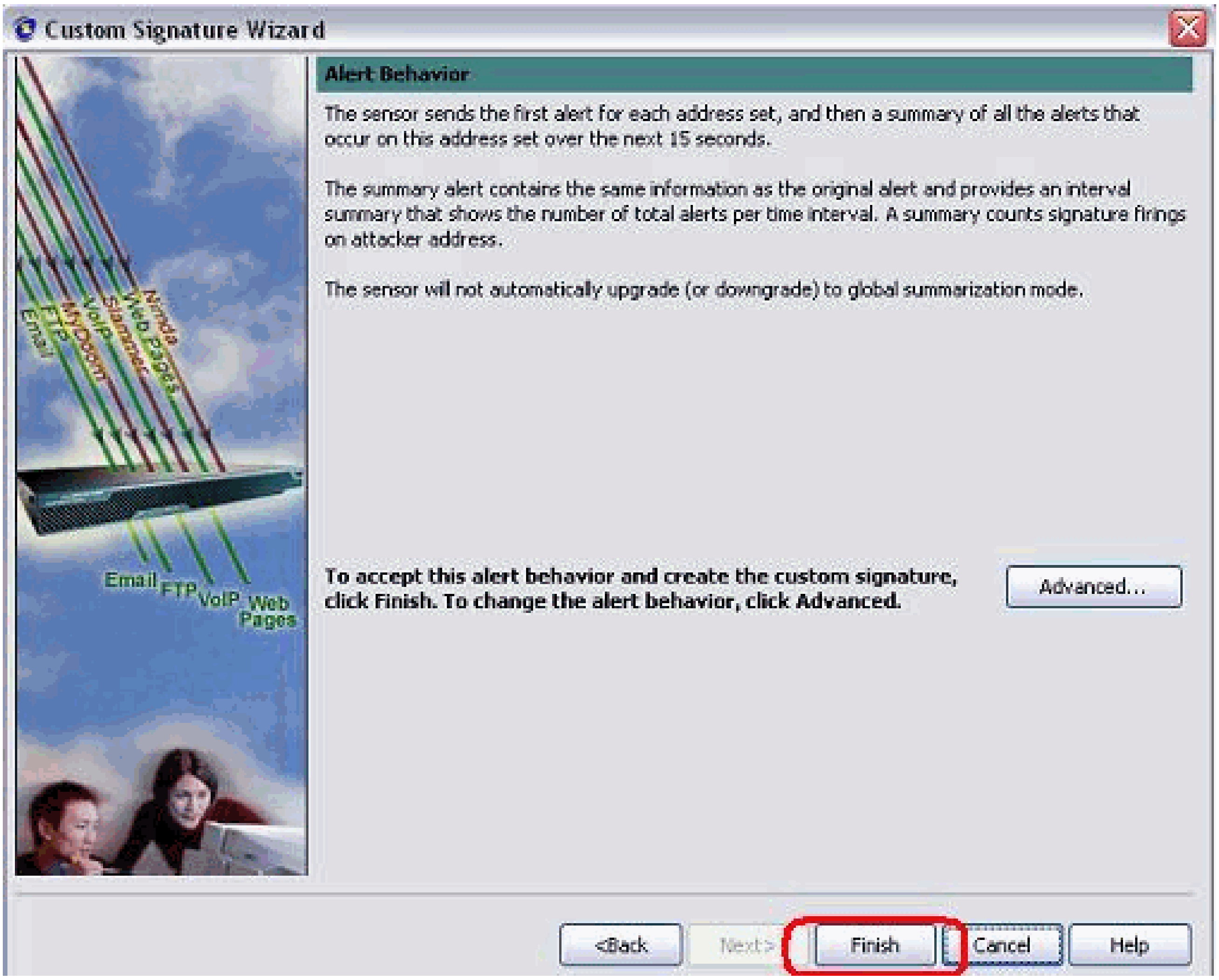
Alert Response

You can assign the following values to this signature that reflect both your confidence in the fidelity of the signature and the severity of the attack it represents. The Signature Fidelity Rating is any number from 0 to 100, with 100 reflecting the most confidence in this signature. This number is used to help calculate the Risk Rating, which helps determine what actions result from the firing of this signature.

Signature Fidelity Rating: 75

Severity of the Alert: High

11. 按一下**完成**以完成嚮導。



Alert Behavior

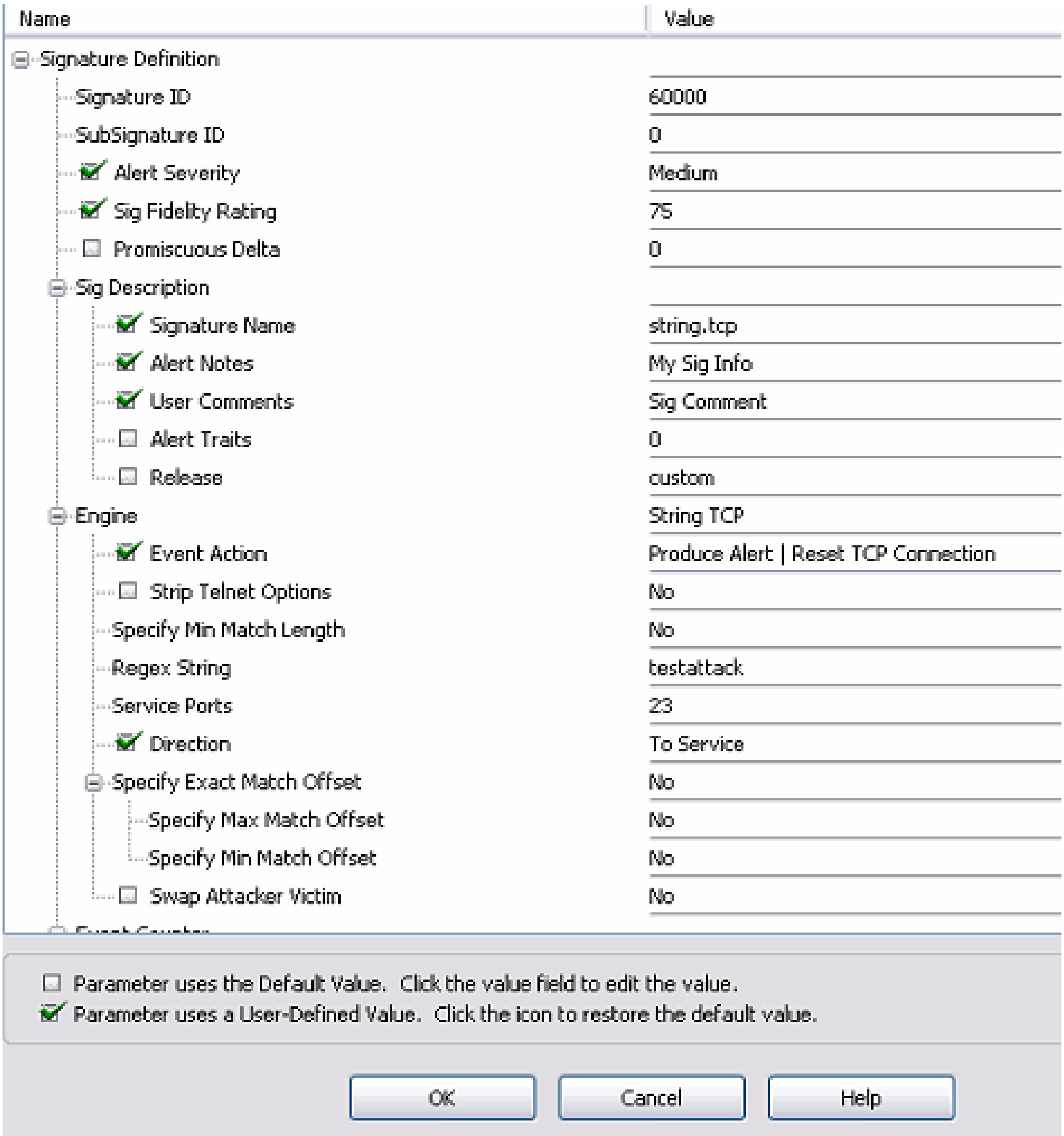
The sensor sends the first alert for each address set, and then a summary of all the alerts that occur on this address set over the next 15 seconds.

The summary alert contains the same information as the original alert and provides an interval summary that shows the number of total alerts per time interval. A summary counts signature firings on attacker address.

The sensor will not automatically upgrade (or downgrade) to global summarization mode.

To accept this alert behavior and create the custom signature, click Finish. To change the alert behavior, click Advanced.

12. 選擇**Configuration > sig0 > Active Signatures**，以便通過簽名ID或**簽名**找到新建立的**簽名。**按一下**Edit**以檢視簽名。



Name	Value
⊟ Signature Definition	
Signature ID	60000
SubSignature ID	0
✓ Alert Severity	Medium
✓ Sig Fidelity Rating	75
□ Promiscuous Delta	0
⊟ Sig Description	
✓ Signature Name	string.tcp
✓ Alert Notes	My Sig Info
✓ User Comments	Sig Comment
□ Alert Traits	0
□ Release	custom
⊟ Engine	String TCP
✓ Event Action	Produce Alert | Reset TCP Connection
□ Strip Telnet Options	No
Specify Min Match Length	No
Regex String	testattack
Service Ports	23
✓ Direction	To Service
⊟ Specify Exact Match Offset	No
Specify Max Match Offset	No
Specify Min Match Offset	No
□ Swap Attacker Victim	No

□ Parameter uses the Default Value. Click the value field to edit the value.

✓ Parameter uses a User-Defined Value. Click the icon to restore the default value.

13. 確認後按一下**OK**，然後按一下**Apply**按鈕將特徵碼應用到感測器。

驗證

發動攻擊並重置TCP

完成以下步驟，即可啟動攻擊和TCP重設：

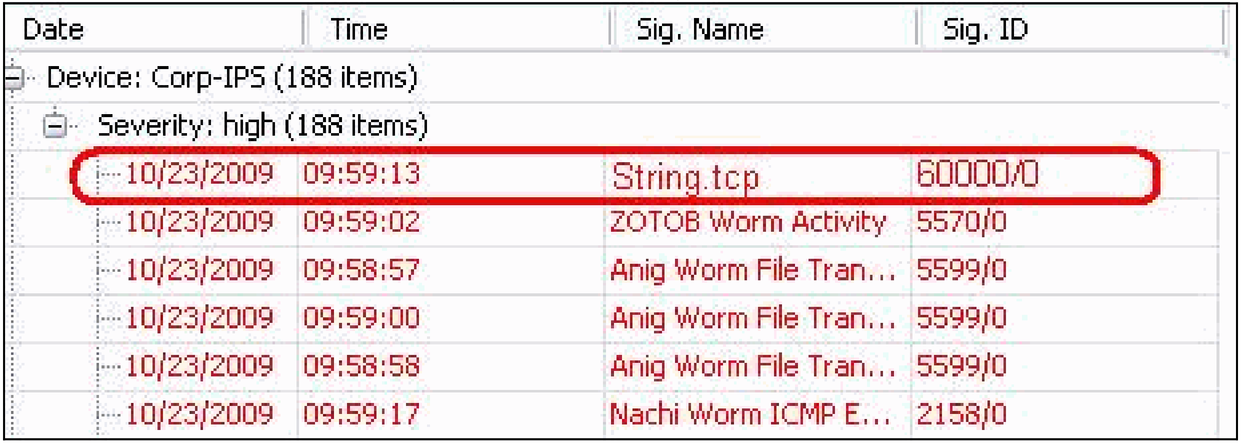
1. 發起攻擊之前，請轉到IME，選擇**Event Monitoring > Dropped Attacks View**，然後選擇右側的感測器。
2. 從Router Light（路由器指示燈），Telnet至Router House並進入**testattack**。按一下**<space>**或**<enter>**可重設Telnet作業階段。

```
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 closed by foreign host]
!--- Telnet session has been reset due to the !--- signature "String.tcp" triggered.
```

3. 在IPS事件檢視器的控制面板中，一旦發起攻擊，就會出現紅色警報。



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

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

提示

使用以下故障排除提示：

- 回撥功能不使用命令和控制埠來重新程式設計路由器訪問控制清單(ACL)。 TCP重置從感測器的**監聽接**口傳送。在交換器上設定span時，請使用**set span <src_mod/src_port><dest_mod/dest_port>**命令，並啟用兩個傳入封包，如下所示。

```
banana (enable)set span 2/12 3/6 both inpkts enable
Overwrote Port 3/6 to monitor transmit/receive traffic of Port 2/12
Incoming Packets enabled. Learning enabled. Multicast enabled.
banana (enable)
banana (enable)
banana (enable)show span

Destination     : Port 3/6
!--- connect to sniffing interface of the sensor
Admin Source    : Port 2/12
!--- connect to FastEthernet0/0 of Router House
Oper Source     : Port 2/12
Direction       : transmit/receive
Incoming Packets: enabled
Multicast       : enabled
```

- 如果TCP重置正常工作，請檢查是否觸發了操作型別TCP重置的警報。如果出現警報，請檢查簽名型別是否設定為TCP重置。使用服務帳戶su登入root並發出此命令。此命令假設感應介面設定為eth0。

```
[root@sensor1 root]#tcpdump -i eth0 -n
```

注意：向受害者/目標傳送一百個tcp重置，然後向攻擊者/客戶端傳送一百個tcp重置。以下是輸出範例：

```
03:06:00.598777 64.104.209.205.1409 >
 10.66.79.38.telnet: R 107:107(0) ack 72 win 0
03:06:00.598794 64.104.209.205.1409 >
 10.66.79.38.telnet: R 108:108(0) ack 72 win 0
```

```
03:06:00.599360 10.66.79.38.telnet >
 64.104.209.205.1409: R 72:72(0) ack 46 win 0
03:06:00.599377 10.66.79.38.telnet >
 64.104.209.205.1409: R 73:73(0) ack 46 win 0
```

相關資訊

- 思科安全入侵防禦支援頁面
- 思科安全入侵防禦系統文檔
- 技術支援與文件 - Cisco Systems