Konfigurieren von IPS TCP Reset mit IME

Inhalt

Einführung

In diesem Dokument wird die Konfiguration des IPS-TCP-Resets (Intrusion Prevention System) mit IPS Manager Express (IME) erläutert. IME- und IPS-Sensoren werden zur Verwaltung eines Cisco Routers für TCP Reset verwendet. Beachten Sie beim Überprüfen dieser Konfiguration folgende Punkte:

- Installieren Sie den Sensor, und stellen Sie sicher, dass der Sensor ordnungsgemäß funktioniert.
- Stellen Sie die Sniffing-Schnittstelle auf den Router außerhalb der Schnittstelle ein.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco IPS Manager Express 7.0
- Cisco IPS Sensor 7.0(0.88)E3
- Cisco IOS® Router mit Cisco IOS Software, Version 12.4

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

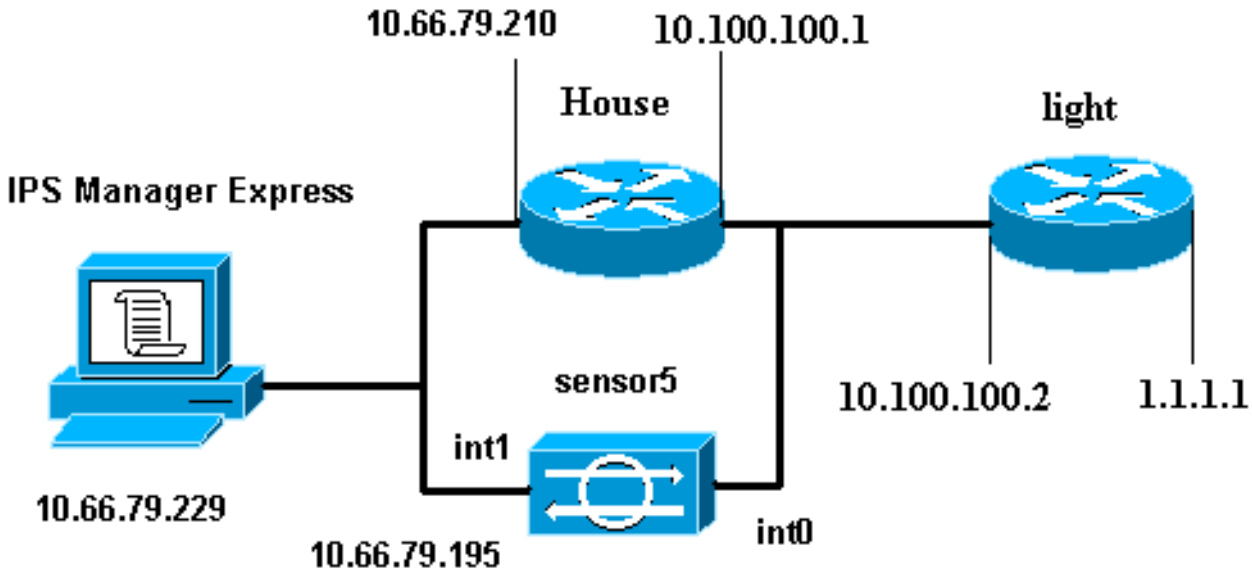
Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Konfigurieren

Netzwerkdiagramm

In diesem Dokument wird die in diesem Diagramm dargestellte Netzwerkeinrichtung verwendet.



Konfigurationen

In diesem Dokument werden die hier gezeigten Konfigurationen verwendet.

- Routerleuchte
- Router-Haus

Routerleuchte

```
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-Haus

```
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
```

Starten der Sensorkonfiguration

Führen Sie diese Schritte aus, um die Konfiguration des Sensors zu starten.

1. Wenn Sie sich zum ersten Mal beim Sensor anmelden, müssen Sie **cisco** als Benutzernamen und **cisco** als Kennwort eingeben.
2. Wenn Sie vom System dazu aufgefordert werden, ändern Sie Ihr Kennwort.**Hinweis:** Cisco123 ist ein Wörterbuch und im System nicht zulässig.
3. Geben Sie **setup ein**, und schließen Sie die Systemaufforderung ab, um die Basisparameter für die Sensoren einzurichten.
4. Geben Sie folgende Informationen ein:

```
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. Speichern Sie die Konfiguration.Es kann einige Minuten dauern, bis der Sensor die Konfiguration gespeichert hat.

```
[0] Go to the command prompt without saving this config.
```

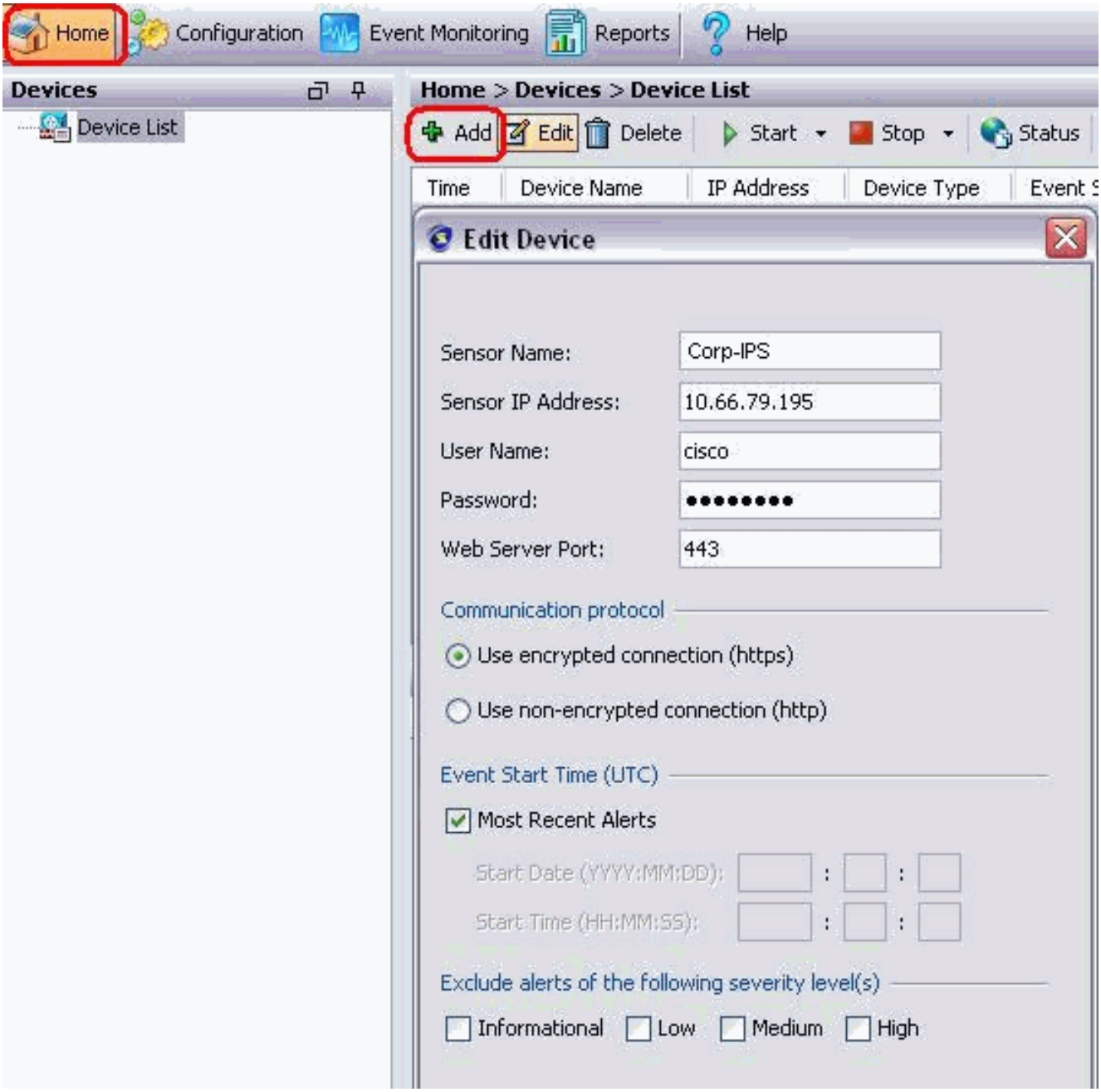
```
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.

Enter your selection[2]: 2
```

Hinzufügen des Sensors zum IME

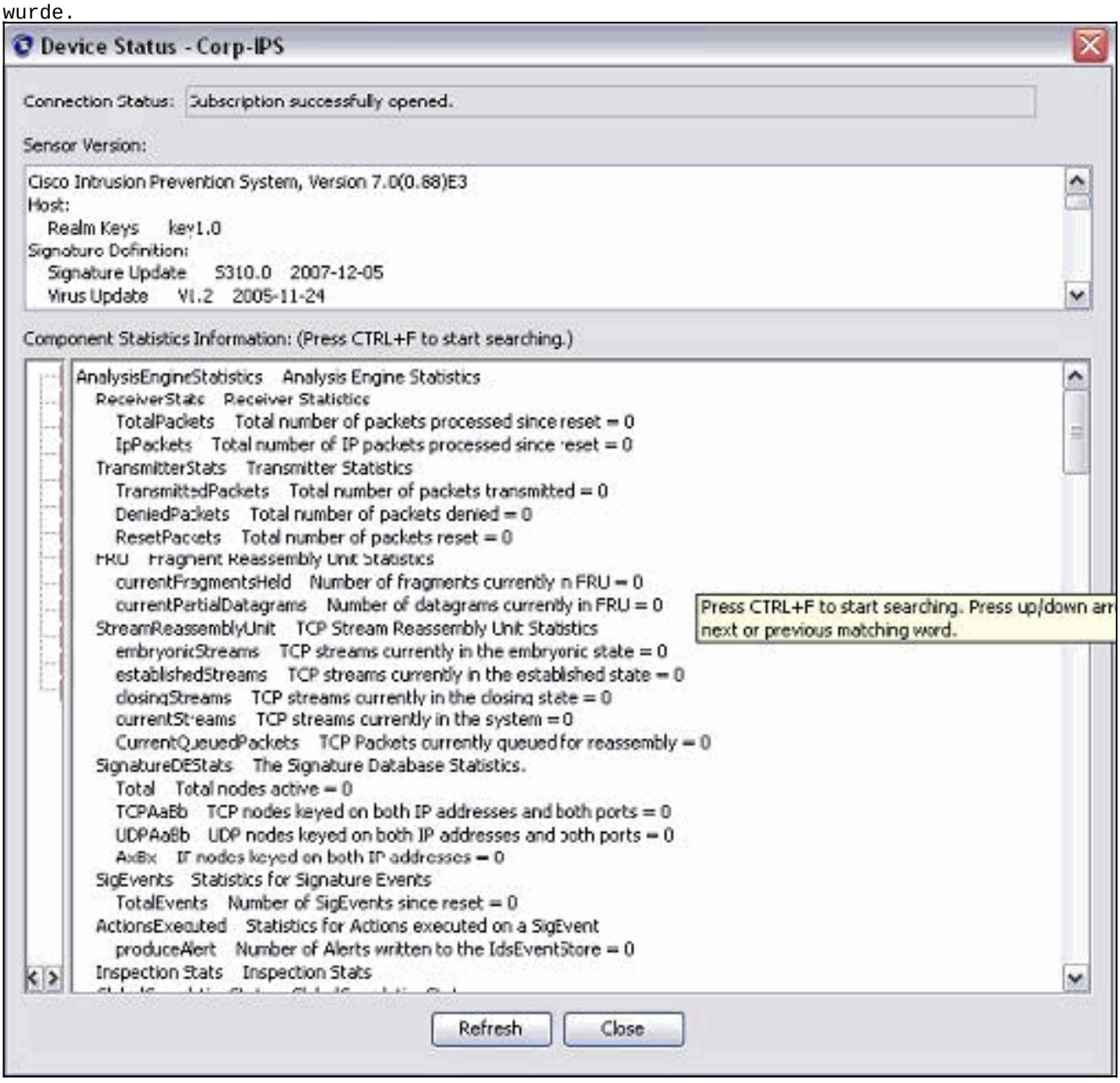
Gehen Sie wie folgt vor, um den Sensor in die IME einzufügen:

1. Öffnen Sie den Windows-PC, auf dem IPS Manager Express installiert wurde, und öffnen Sie den IPS Manager Express.
2. Wählen Sie **Home > Add aus**.



3. Geben Sie diese Informationen ein und klicken Sie auf **OK**, um die Konfiguration abzuschließen.
4. Wählen Sie **Geräte > Corp-IPS**, um den Sensorstatus zu überprüfen, und klicken Sie dann mit der rechten Maustaste, um den **Gerätestatus** auszuwählen.Vergewissern Sie sich, dass das `Abonnement erfolgreich geöffnet`

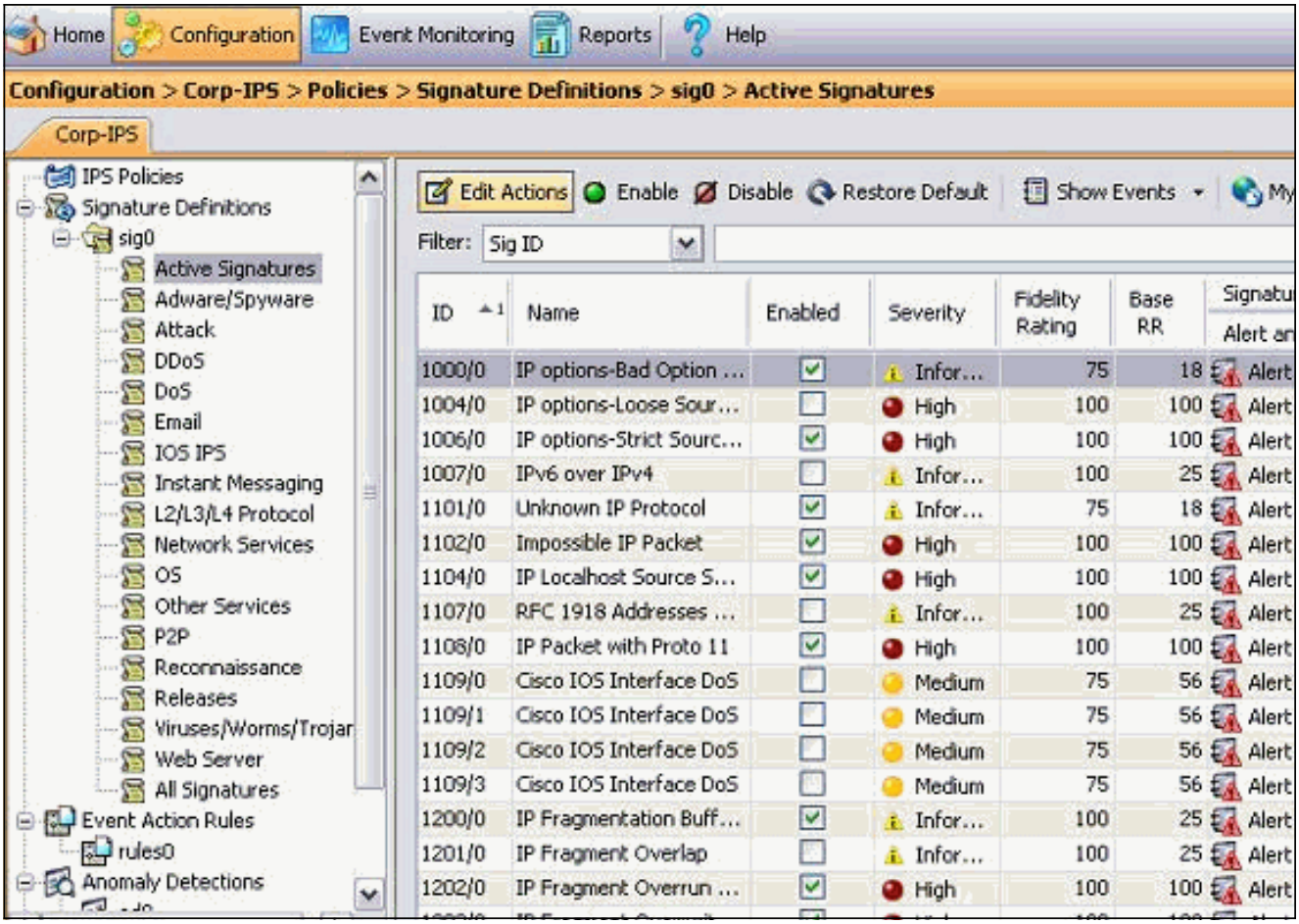
wurde.



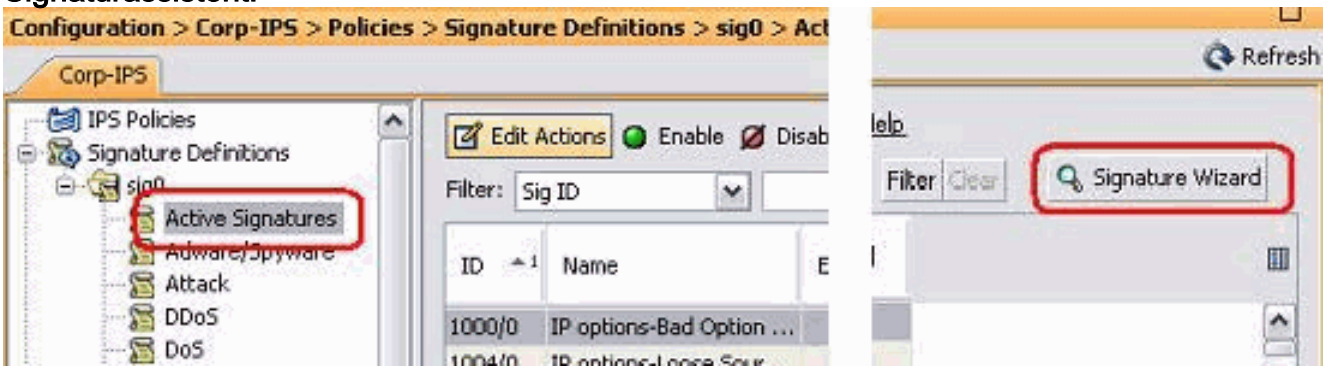
Konfigurieren des TCP-Resets für den Cisco IOS-Router

Gehen Sie wie folgt vor, um das TCP Reset für den Cisco IOS-Router zu konfigurieren:

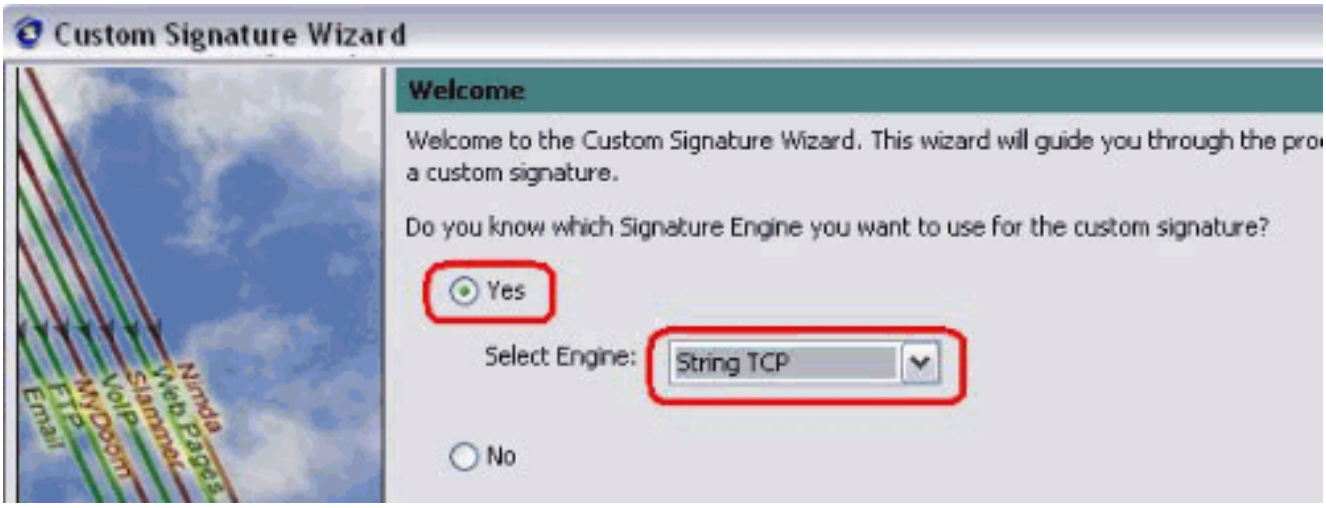
1. Öffnen Sie auf dem IME-PC Ihren Webbrowser, und gehen Sie zu **https://10.66.79.195**.
2. Klicken Sie auf **OK**, um das vom Sensor heruntergeladene HTTPS-Zertifikat zu akzeptieren.
3. Geben Sie im Anmeldefenster **cisco** als Benutzernamen und **123cisco123** als Kennwort ein.Diese IME-Verwaltungsschnittstelle wird angezeigt:



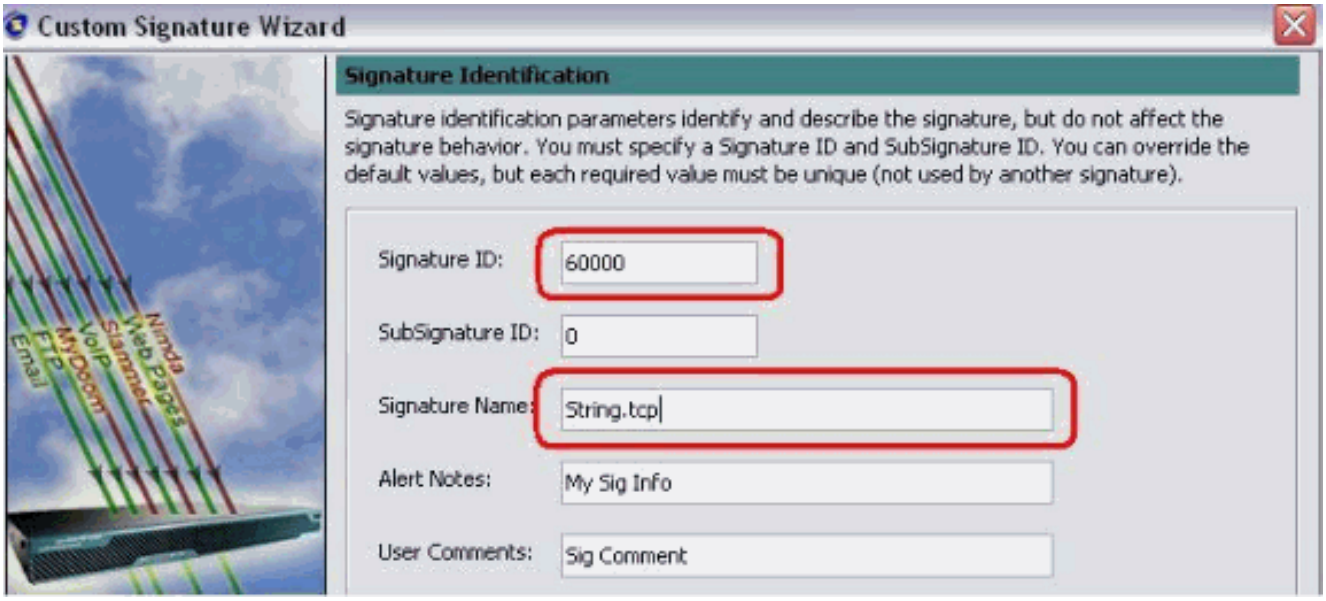
4. Klicken Sie auf der Registerkarte Konfiguration auf **Aktive Signaturen**.
5. Klicken Sie anschließend auf **Signaturassistent.**



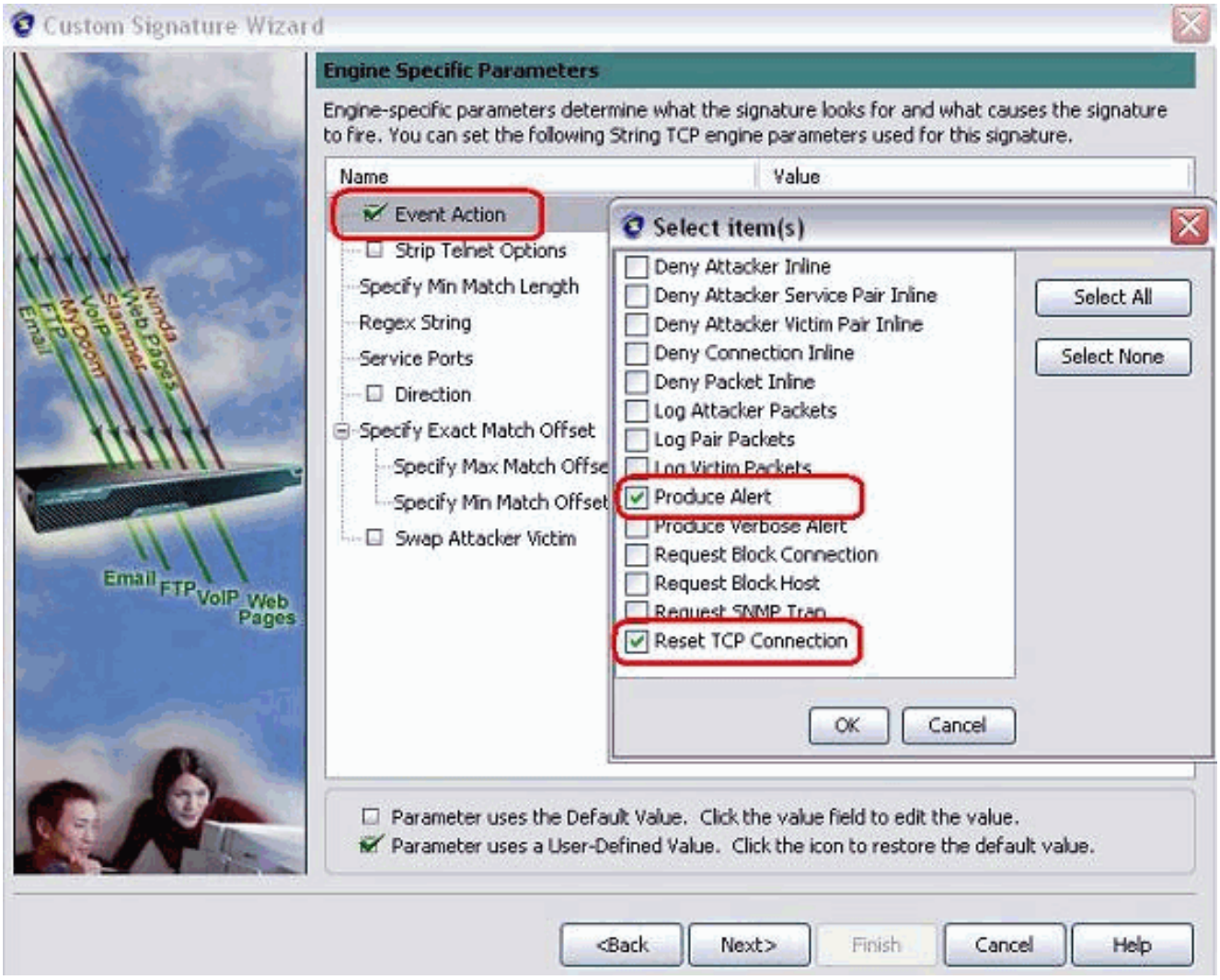
6. Wählen Sie im Assistenten **Yes (Ja)** aus, und wählen Sie **String TCP** als Signature-Engine aus. Klicken Sie auf **Weiter**.



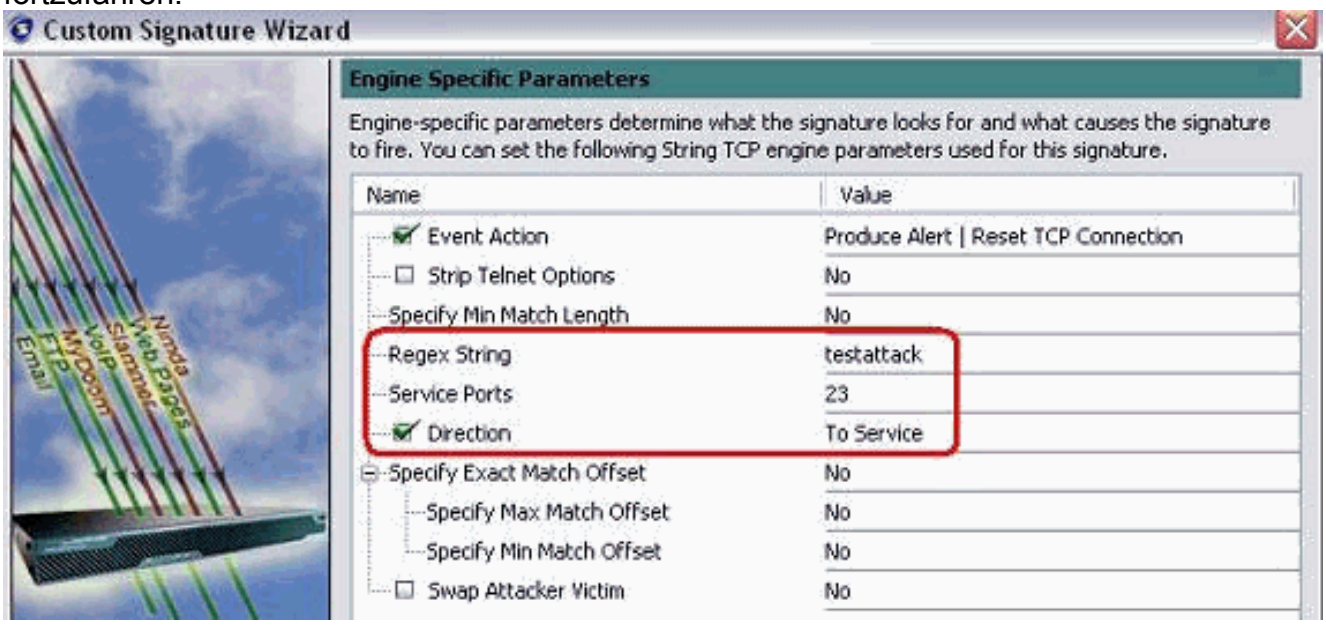
7. Sie können diese Informationen als Voreinstellung belassen oder Ihre eigene Signature-ID, Signaturname und Benutzerhinweise eingeben. Klicken Sie auf **Weiter**.



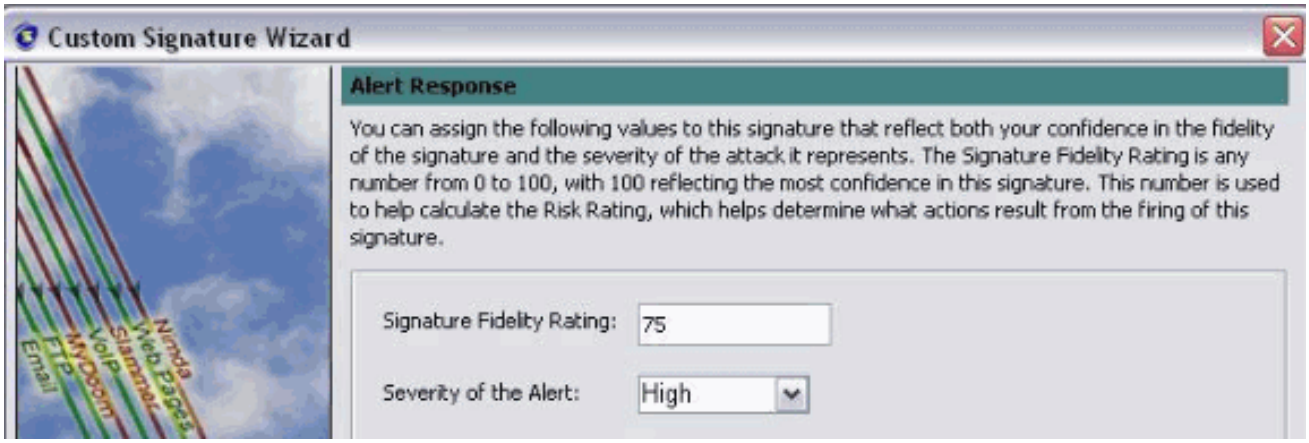
8. Wählen Sie **Event Action** (Ereignisaktion) **aus**, und wählen Sie **Produce Alert** and **Reset TCP Connection aus**. Klicken Sie auf **OK** und dann auf **Weiter**, um fortzufahren.



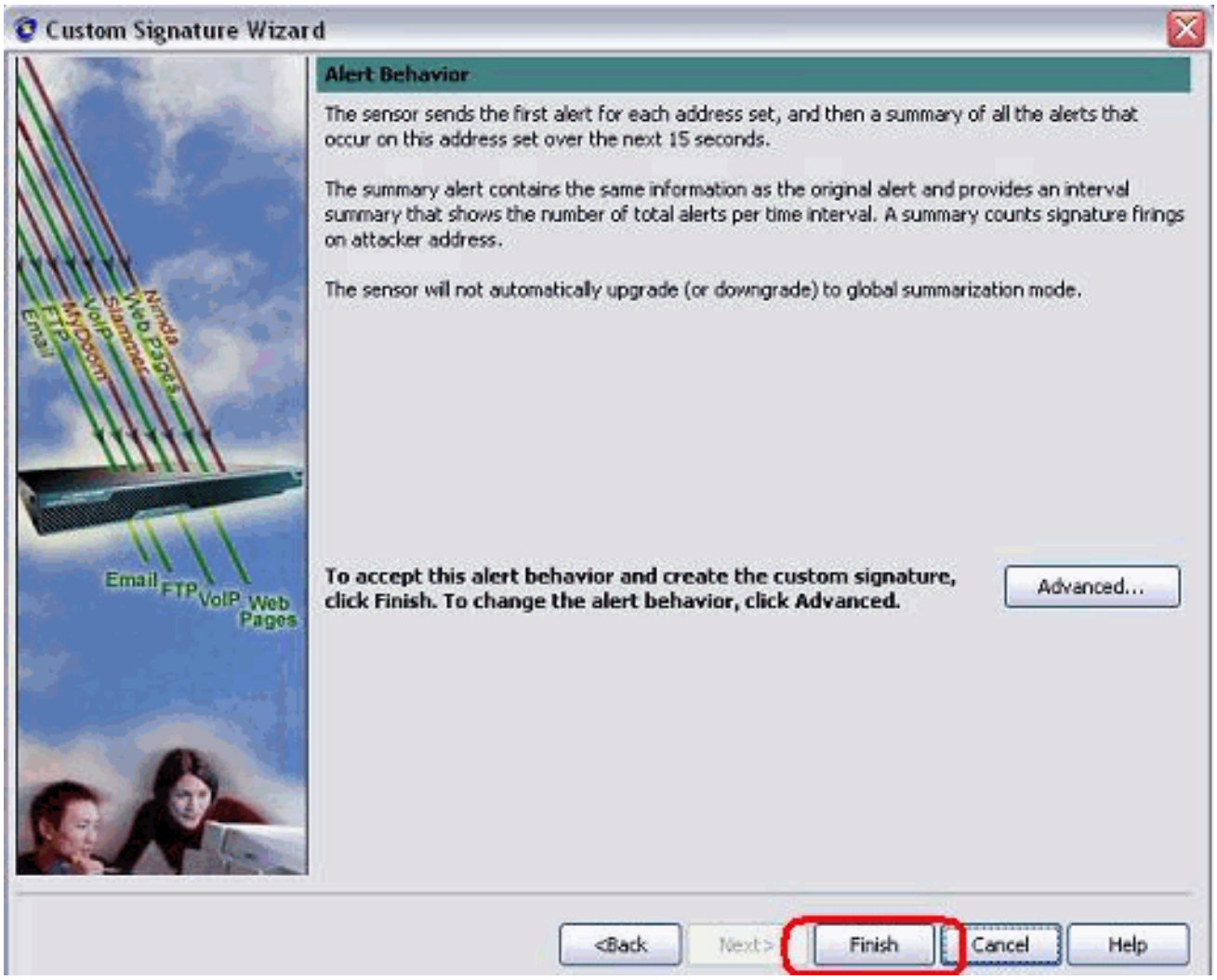
9. Geben Sie einen regulären Ausdruck ein, und in diesem Beispiel wird Tetack verwendet. Geben Sie **23** für Service-Ports ein, wählen Sie **Service** für die Richtung aus, und klicken Sie auf **Weiter**, um fortzufahren.



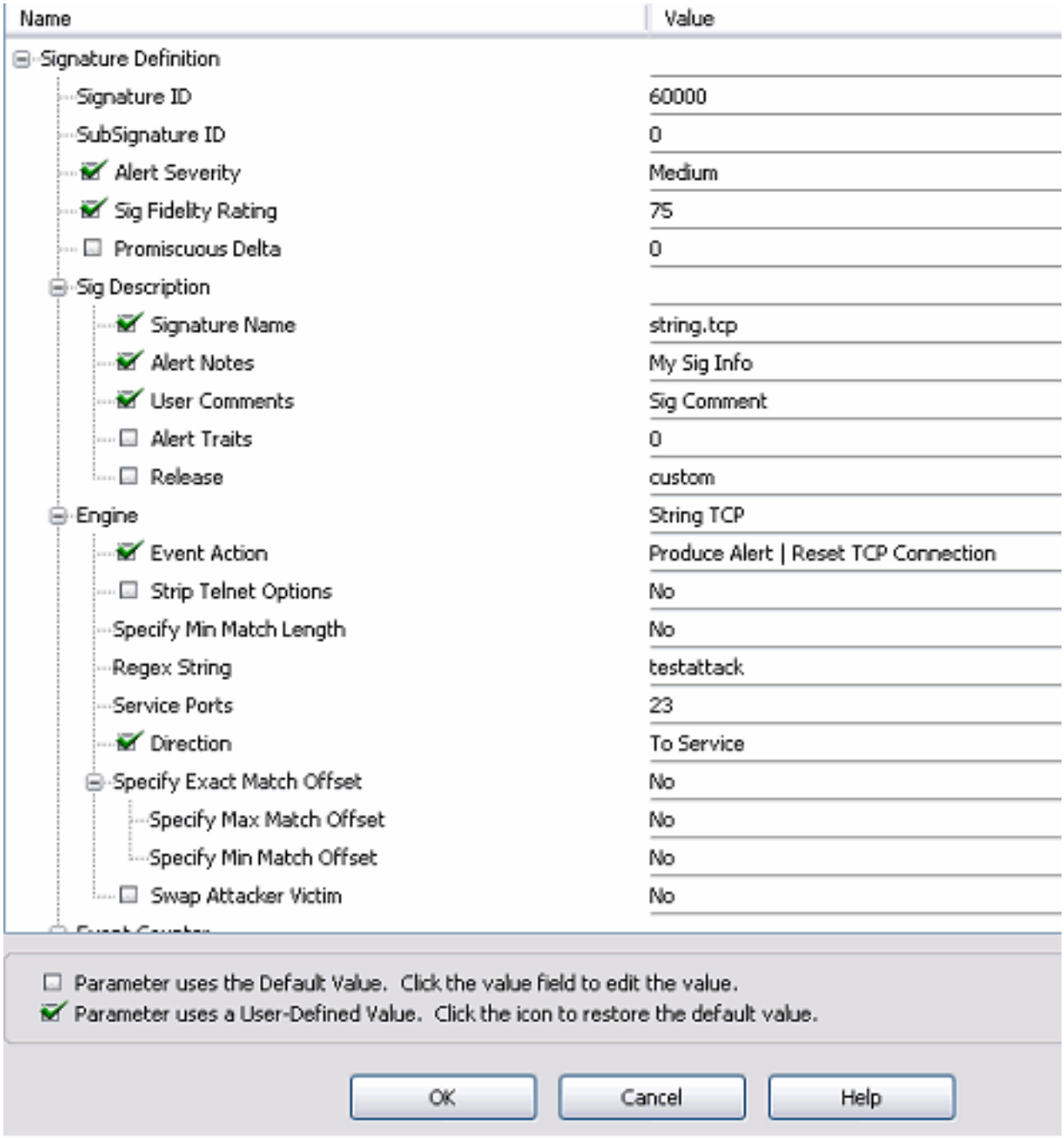
10. Sie können diese Informationen als Standard belassen. Klicken Sie auf **Weiter**.



11. Klicken Sie auf **Fertig stellen**, um den Assistenten zu beenden.



12. Wählen Sie **Configuration > sig0 > Active Signatures (Konfiguration > sig0 > aktive Signaturen)**, um die neu erstellte Signatur mithilfe der **Signature-ID** oder des **Signaturnamens** zu suchen. Klicken Sie auf **Bearbeiten**, um die Signatur anzuzeigen.



13. Klicken Sie nach der Bestätigung auf **OK** und anschließend auf die Schaltfläche **Übernehmen**, um die Signatur auf den Sensor anzuwenden.

Überprüfen

Starten des Angriffs und des TCP-Resets

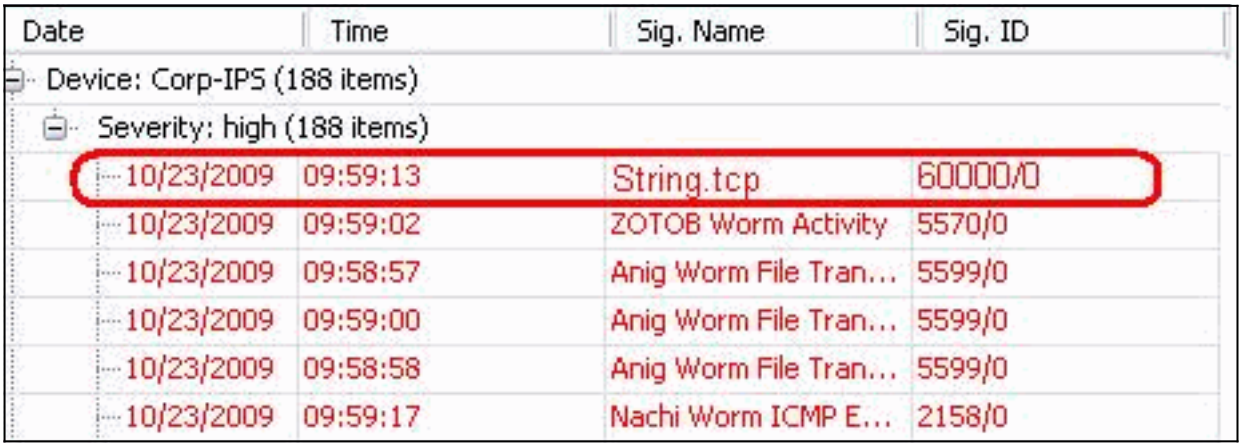
Gehen Sie wie folgt vor, um den Angriff und den TCP-Reset zu starten:

1. Bevor Sie den Angriff starten, gehen Sie zum **IME**, wählen Sie **Event Monitoring > Dropped Attacks View** und wählen Sie den Sensor rechts aus.
2. Geben Sie von der Router Light, Telnet zu Router House ein, und geben Sie **testattack ein**.Drücken Sie entweder **<Leerzeichen>** oder **<Eingabe>**, um Ihre Telnet-Sitzung zurückzusetzen.

```
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. Im Dashboard der IPS Event Viewer wird der rote Alarm angezeigt, sobald der Angriff gestartet
   wurde.



Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Tipps

Tipps zur Fehlerbehebung:

- Das Abschalten erfolgt über den Command-and-Control-Port, um die Zugriffskontrolllisten (ACLs) des Routers neu zu programmieren. Die TCP-Resets werden von der **Sniffing-Schnittstelle** des Sensors gesendet. Wenn Sie **span** im Switch **festlegen**, verwenden Sie den Befehl **set span <src_mod/src_port><dest_mod/dest_port>**, wobei beide eingehenden Pakete wie hier gezeigt aktiviert sind.

```
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
```

- Wenn die TCP-Resets funktionieren, überprüfen Sie, ob der Alarm für den Aktionstyp TCP Reset ausgelöst wird. Wenn der Alarm angezeigt wird, überprüfen Sie, ob der Signaturtyp auf TCP reset eingestellt ist.Melden Sie sich mit dem Dienstkonto su an, um den Root-Befehl

auszuführen. Dieser Befehl geht davon aus, dass die Sensorschnittstelle auf eth0 festgelegt ist.

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

Hinweis: Einhundert tcp-Resets werden an das Opfer/Ziel gesendet und dann hundert an den Angreifer/Client gesendet.Dies ist die Beispielausgabe:

```
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
```

Zugehörige Informationen

- Support-Seite für Cisco Secure Intrusion Prevention
- Dokumentation für das Cisco Secure Intrusion Prevention System
- Technischer Support und Dokumentation - Cisco Systems