IPS TCP opnieuw instellen met IME

Inhoud

Inleiding

Dit document behandelt de configuratie van het IPS (Inbraakpreventiesysteem) TCP-reset met behulp van IPS Manager Express (IME). IME en IPS Sensors worden gebruikt om een Cisco-router voor TCP-reset te beheren. Denk bij het bekijken van deze configuratie aan deze punten:

- Installeer de sensor en controleer of de sensor goed werkt.
- Maak de gebruikersinterface-span aan de router buiten de interface.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IPS Manager Express 7.0
- Cisco IPS Sensor 7.0(0.88)E3

- Cisco IOS®-router met Cisco IOS-softwarerelease 12.4

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

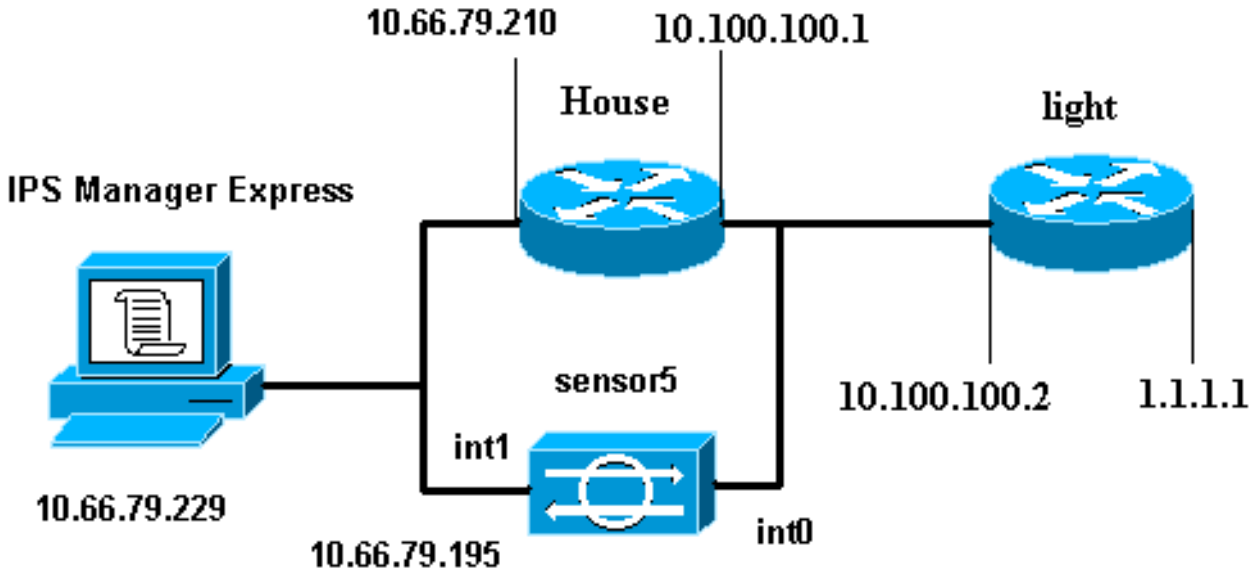
Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Configureren

Netwerkdiagram

Dit document gebruikt de netwerkinstellingen die in dit diagram worden weergegeven.



Configuraties

Dit document gebruikt de configuraties die hier worden weergegeven.

- Routerlicht
- Routerhuis

Routerlicht

```
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
```

Routerhuis

```
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
```

De configuratie van de sensor starten

Volg deze stappen om de configuratie van de Sensor te starten.

1. Als dit de eerste keer is dat u in de Sensor inlogt, moet u **cisco** invoeren als de gebruikersnaam en **cisco** als wachtwoord.
2. Wanneer het systeem u vraagt, wijzigt u uw wachtwoord.**Opmerking:** Cisco123 is een woordenboek en is niet toegestaan in het systeem.
3. **Stel** het type **in** en vul de systeemmelding in om de basisparameters voor de sensoren in te stellen.
4. Voer deze informatie in:

```
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. Bewaar de configuratie.Het kan een paar minuten duren voordat de sensor de configuratie opslaat.

```
[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.
```

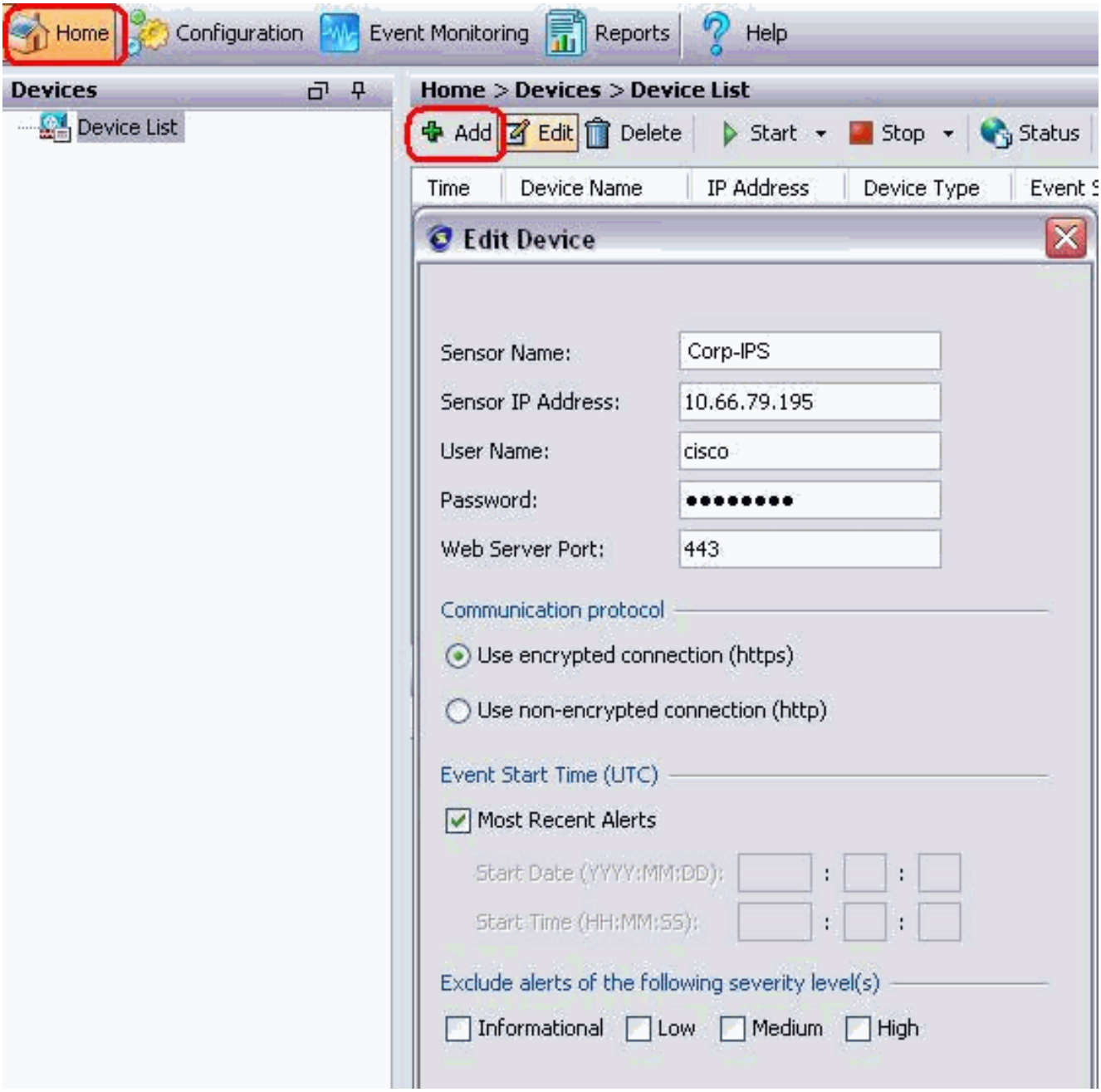
```
Enter your selection[2]: 2
```

Stop de sensor in het IME

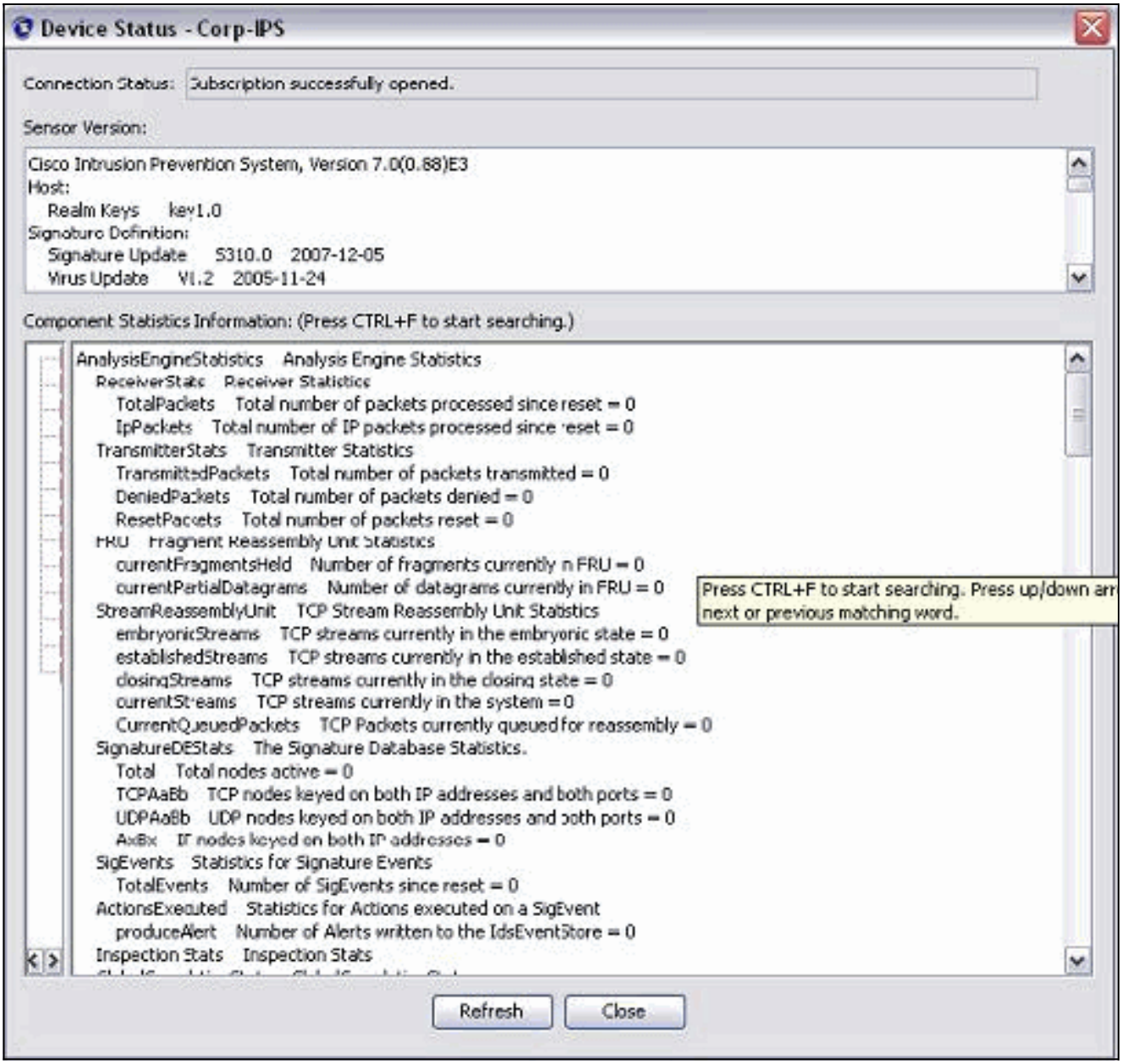
Volg deze stappen om de sensor aan de IME toe te voegen:

1. Ga naar de Windows PC, die de IPS Manager Express heeft geïnstalleerd en open de IPS Manager Express.
2. Kies **startpunt > Toevoegen**

.



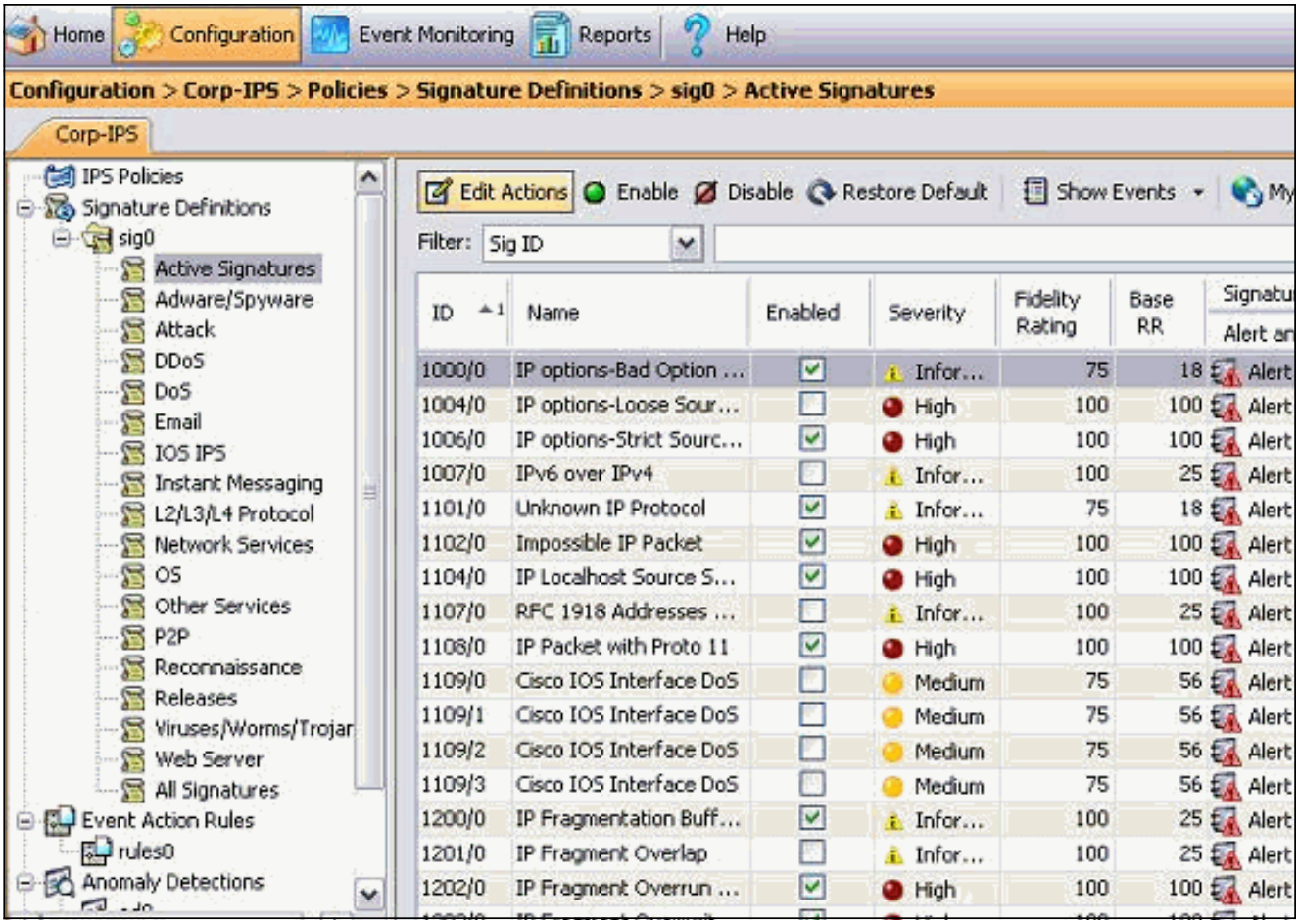
3. Typ deze informatie en klik op **OK** om de configuratie te voltooien.
4. Kies **Apparaten > Corp-IPS** om de status van de sensor te controleren en klik met de rechtermuisknop om de **status van het apparaat** te kiezen.Zorg ervoor dat u `abonnement` kunt zien
`geopend.`



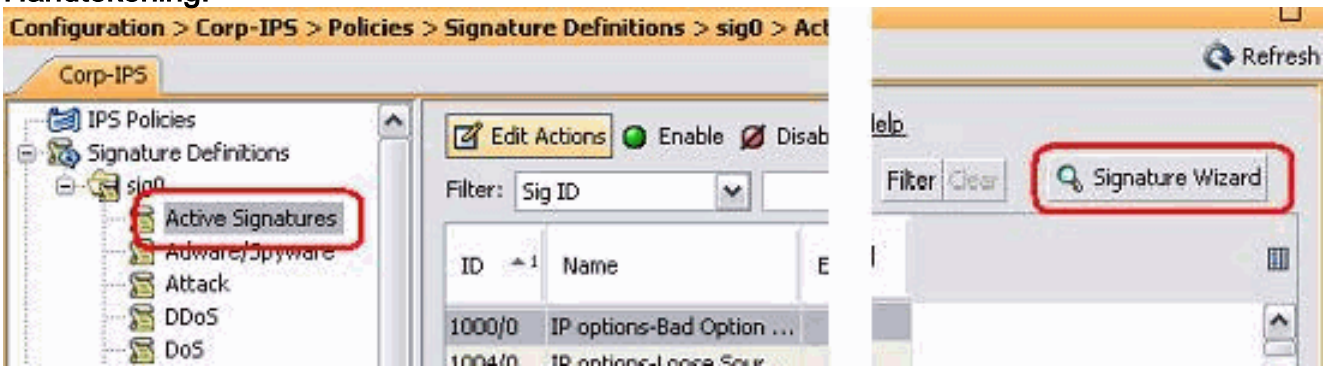
Configureer de TCP-reset voor Cisco IOS-router

Voltooi deze stappen om de TCP-reset voor de Cisco IOS-router te configureren:

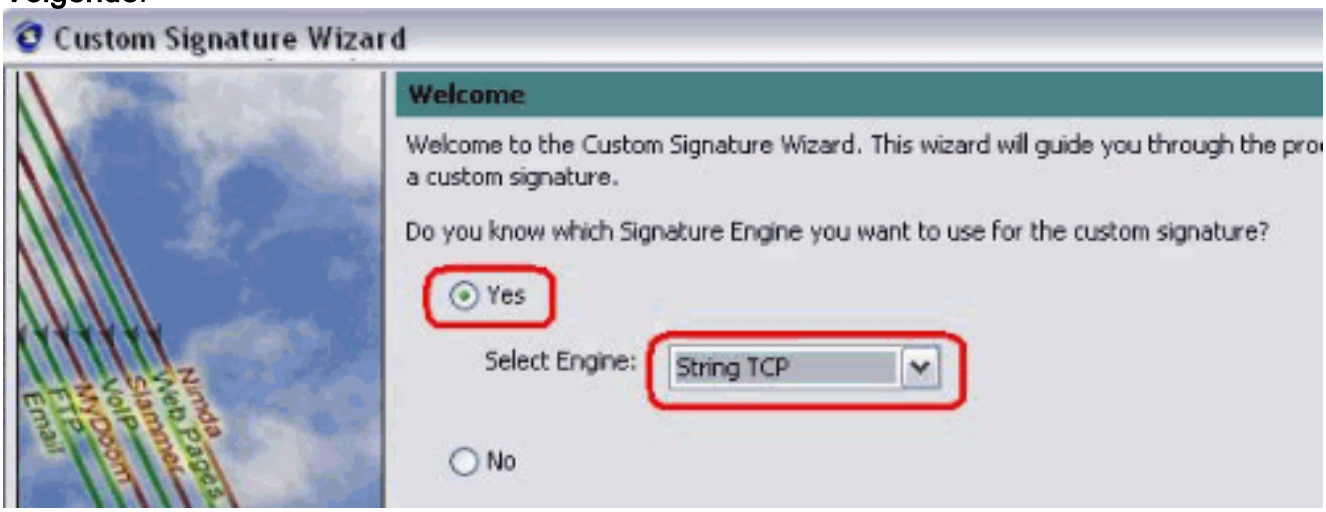
1. Open uw webbrowser vanaf de IME-pc en ga naar **https://10.66.79.195**.
2. Klik op **OK** om het HTTPS-certificaat te aanvaarden dat van de Sensor is gedownload.
3. Voer in het inlogvenster **cisco** in voor de gebruikersnaam en **123cisco123** voor het wachtwoord.Deze IME-beheerinterface verschijnt:



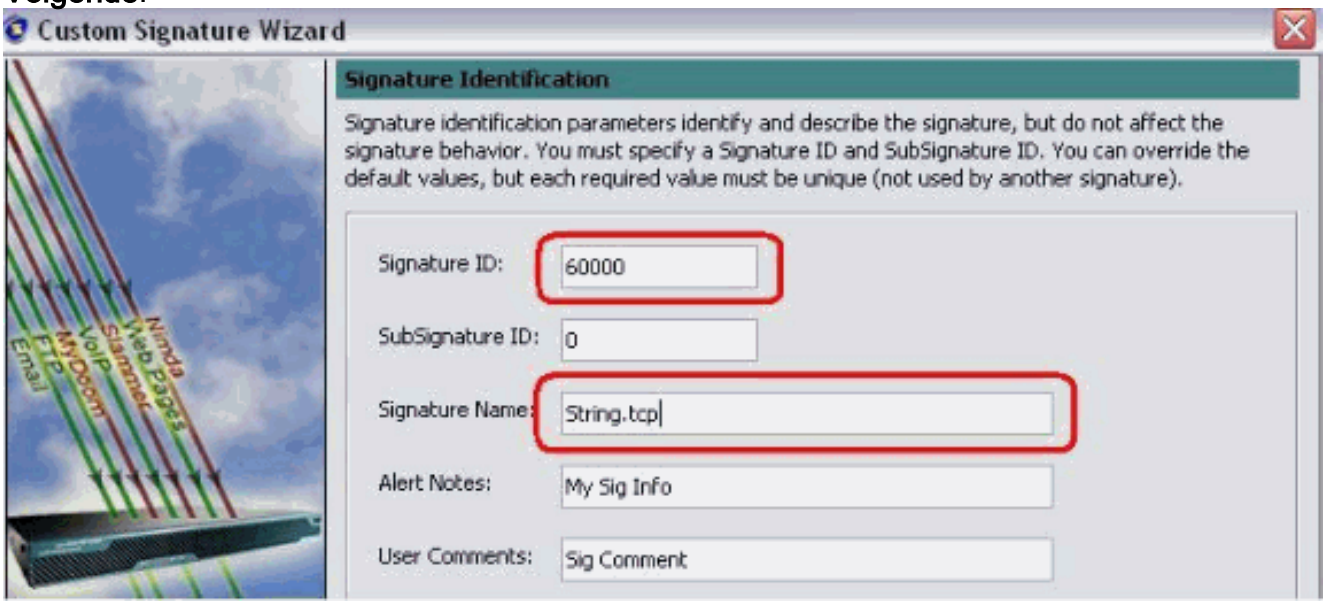
4. Klik in het tabblad Configuration op **actieve handtekeningen**.
5. Klik vervolgens op **Wizard Handtekening.**



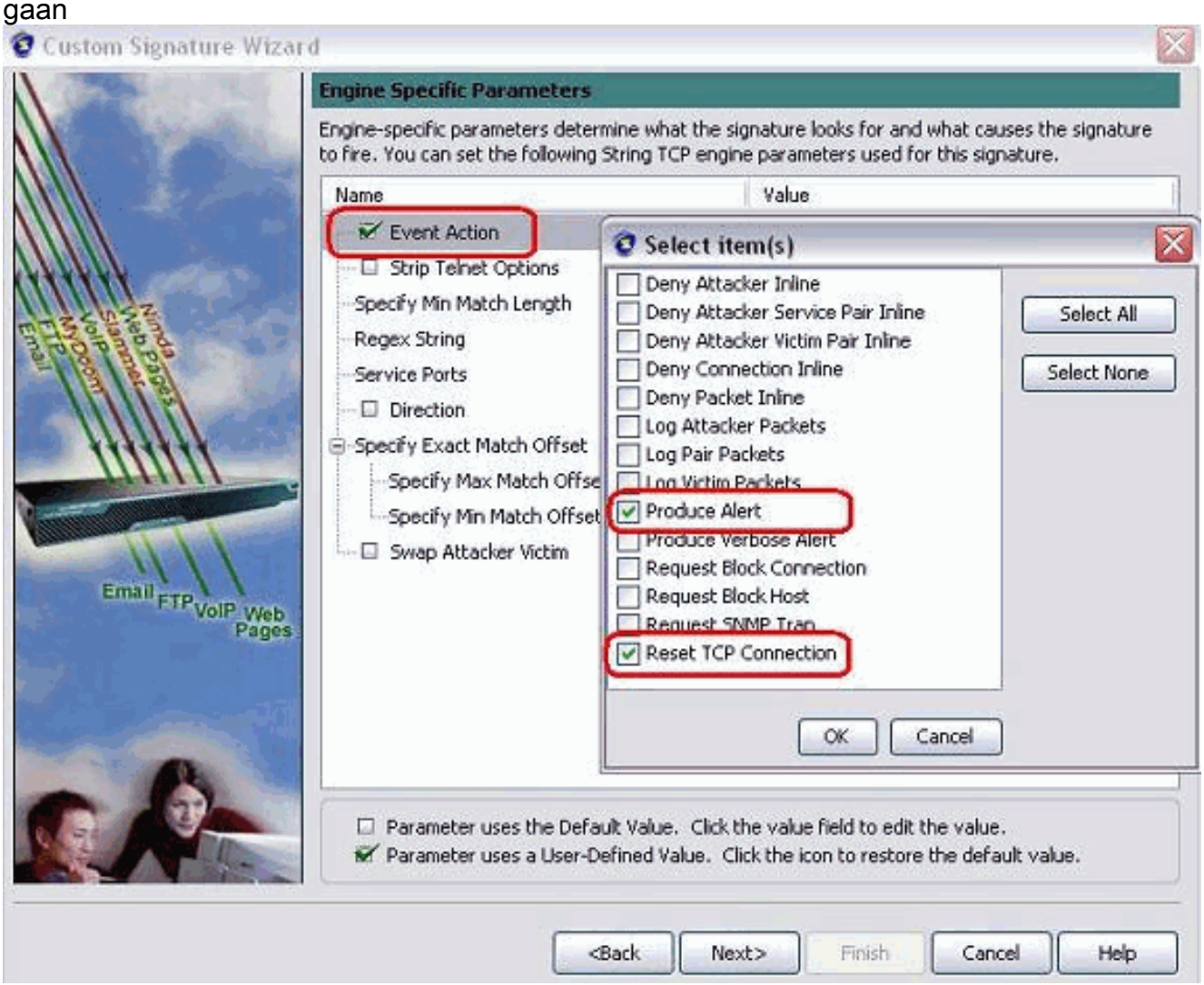
6. In de wizard kiest u **Ja** en kiest u **TCP** als de Signature-motor. Klik op **Volgende**.



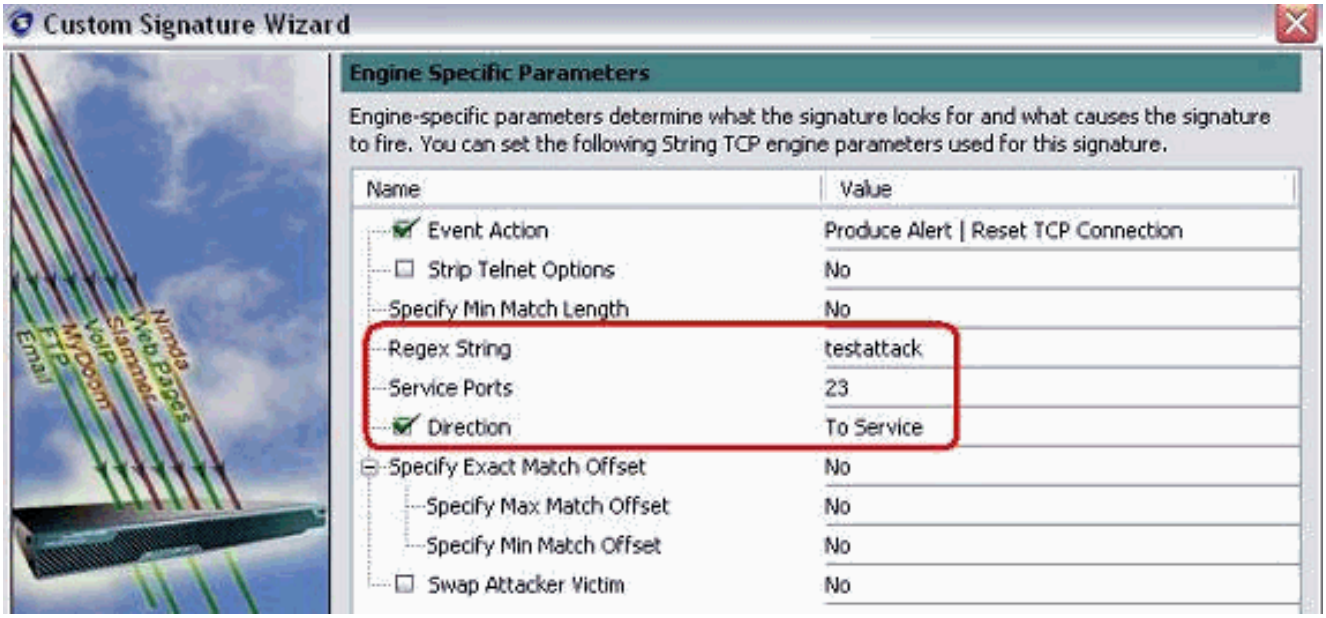
7. U kunt deze informatie als voorbeeld geven of uw eigen handtekening, de naam van de handtekening en de opmerkingen van de gebruiker invoeren. Klik op **Volgende**.



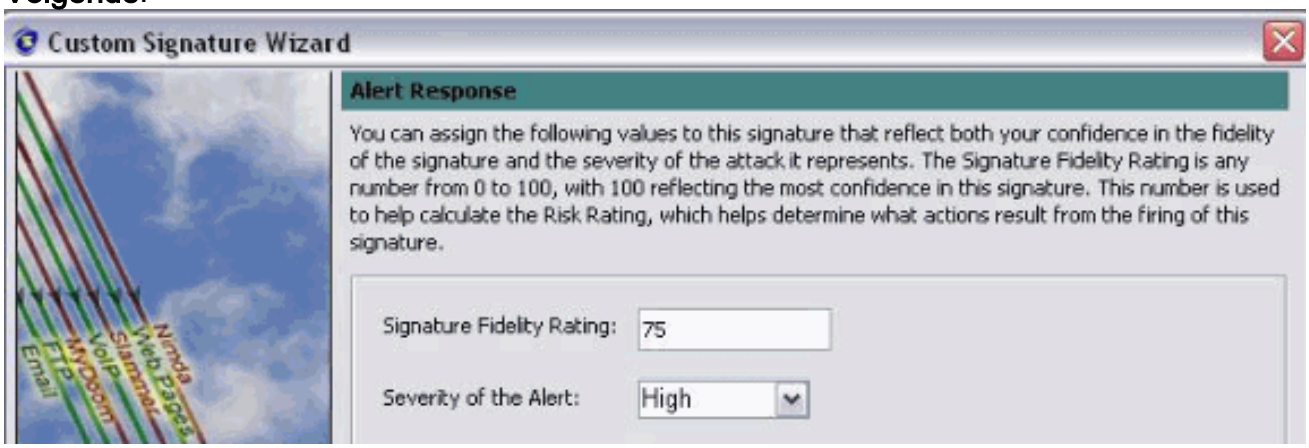
8. Kies **Event Action**, en kies **Waarschuwen** en **Reset TCP verbinding** produceren. Klik op **OK** en vervolgens op **Volgende** om verder te gaan



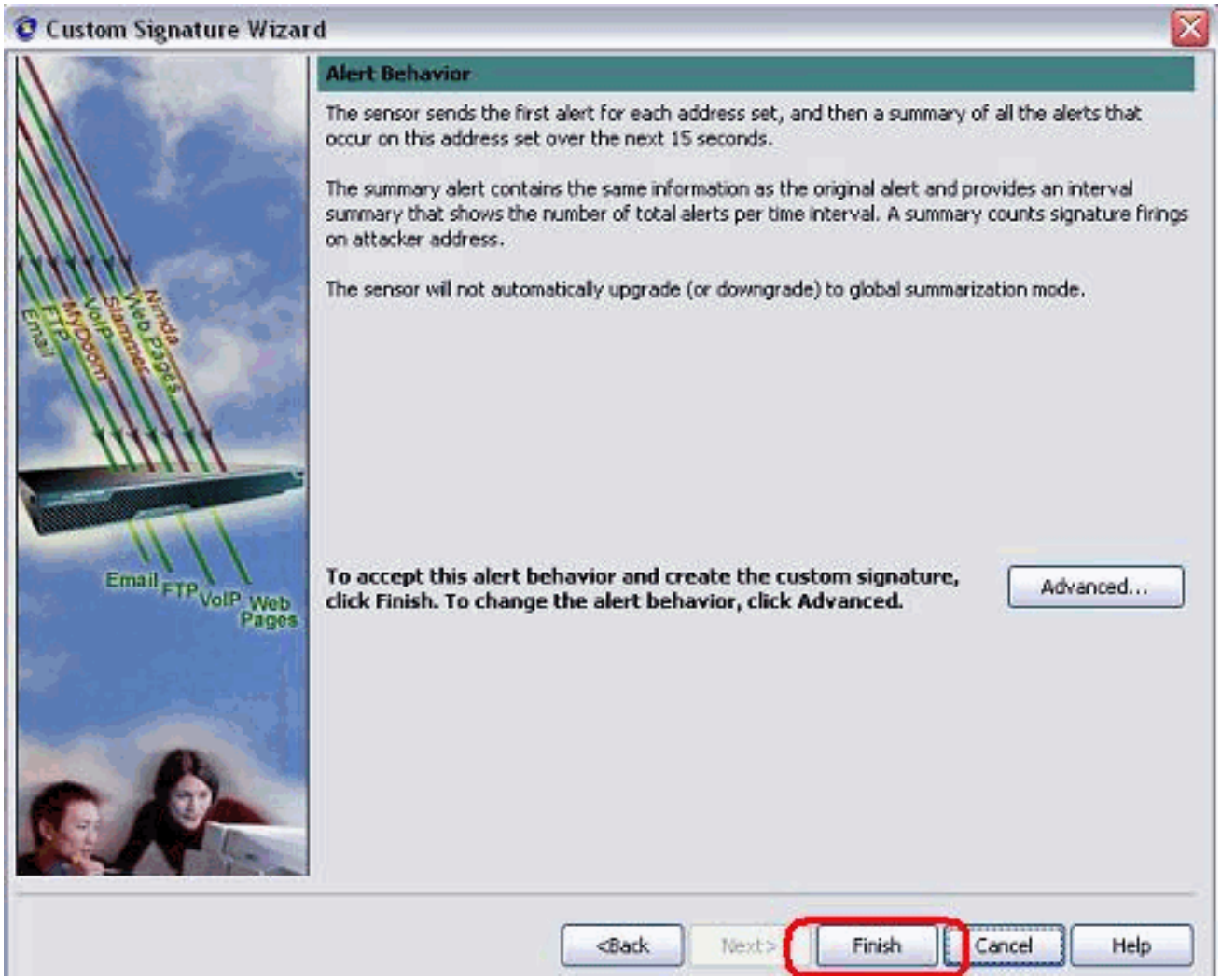
9. Voer een reguliere expressie in en in dit voorbeeld wordt `testattack` gebruikt. Voer **23** in voor servicepoorten, kies **voor** de **service** voor de draairichting en klik op **Volgende** om verder te gaan.



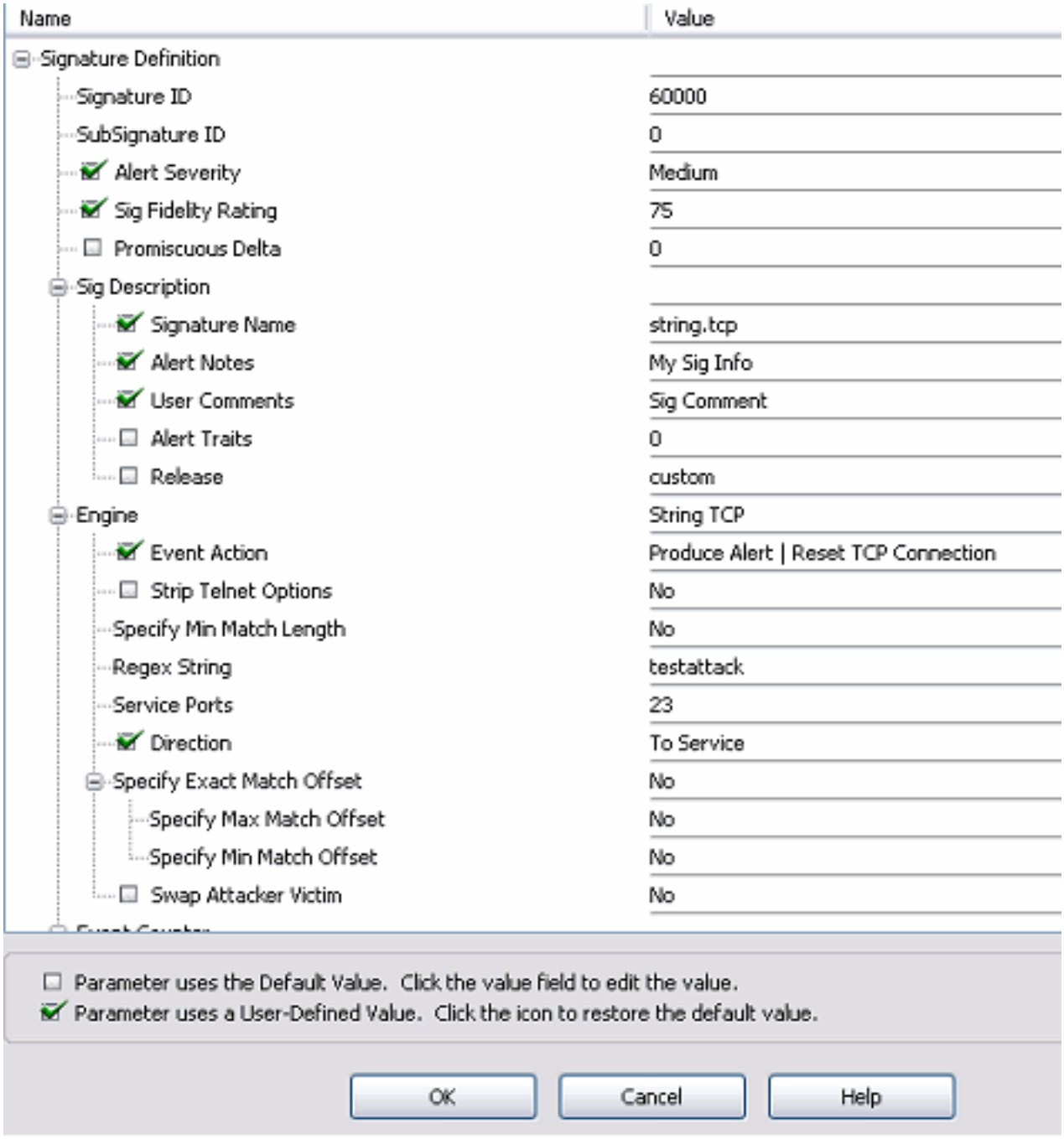
10. U kunt deze informatie als standaard opgeven. Klik op **Volgende**.



11. Klik op **Voltooien** om de wizard te voltooien.



12. Kies **Configuration > Sg0 > Active Signatures** om de nieuwe handtekening te plaatsen onder **Sig-ID** of **Sig-naam**. Klik op **Bewerken** om de handtekeningen te bekijken.



13. Klik op **OK** nadat u hebt bevestigd en klik op de knop **Toepassen** om de handtekening op de sensor toe te passen.

Verifiëren

Start de aanval en de TCP-reset

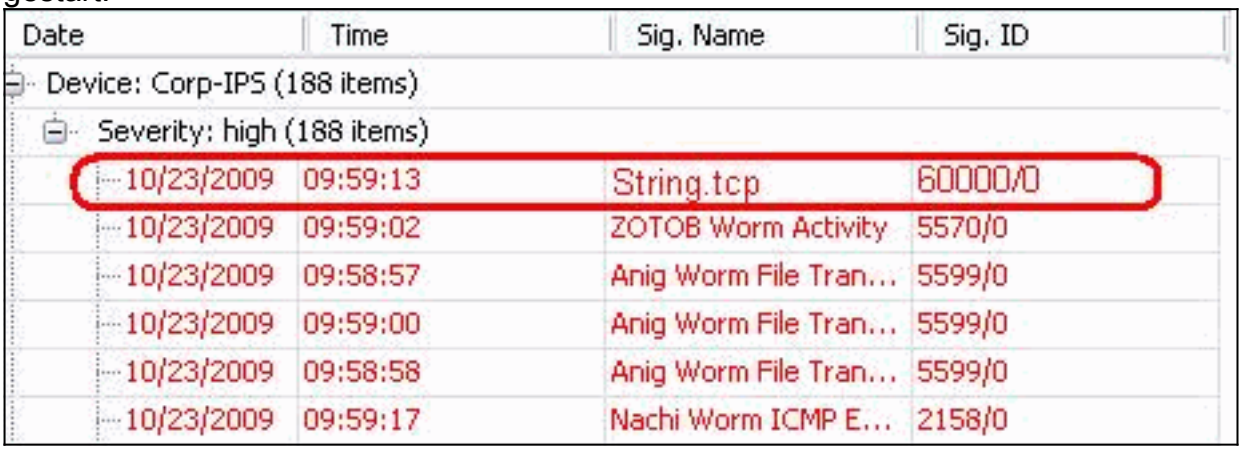
Voltooi deze stappen om de aanval te starten en de TCP-reset uit te voeren:

1. Voordat u de aanval start, gaat u naar de **IME**, kiest u **Event Monitoring > Dropped Attacks View** en kiest u de sensor aan de rechterkant.
2. Van het Licht van de router, van het telnet tot het Huis van de router en ga **testattack** in.Sluit of **<space>** of **<enter>** om uw Telnet-sessie te resetten.

```
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. Vanuit het Dashboard van het IPS Event Viewer verschijnt de Rode Alarm zodra de aanval is gestart.



Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Tips

Gebruik deze tips voor probleemoplossing:

- Shunning werkt uit de bevels- en controlepoort om de controlelijsten van de routertoegang (ACL's) opnieuw te programmeren. De TCP resets worden verzonden vanuit de **snuifinterface** van de sensor. Wanneer u **span** in de switch **instelt**, gebruikt u de opdracht **set span <src_mod/src_port><dest_mod/dest_port>**, waarbij beide inkomende pakketten zijn ingeschakeld zoals hier wordt getoond.

```
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
```

- Als de TCP-reset werkt, controleer of het alarm is geactiveerd voor het handelstype TCP Reset. Als het alarm verschijnt, controleer dan of het signatuur type is ingesteld op TCP resetten.Meld u aan met behulp van de serviceklasse om deze opdracht te worstelen en uit te geven. Deze opdracht neemt aan dat de sensatieinterface op eth0 is ingesteld.

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

Opmerking: Honderd tcp resets worden naar het slachtoffer/doelwit gestuurd en 100 worden naar de aanvaller/cliënt gestuurd.Dit is een voorbeeld-uitvoer:

```
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
```

Gerelateerde informatie

- Cisco-pagina voor beveiligde inbraakpreventie
- Documentatie voor Cisco Secure Inbraakpreventiesysteem
- Technische ondersteuning en documentatie – Cisco Systems