IPS-blokkering configureren met IME

Inhoud

Inleiding

Dit document behandelt de configuratie van het IPS-blokkering (Inbraakpreventiesysteem) met het gebruik van de IPS Manager Express (IME). IME en IPS Sensors worden gebruikt om een Cisco-router te beheren voor blokkering. Denk aan deze punten wanneer u deze configuratie bekijkt:

- 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.

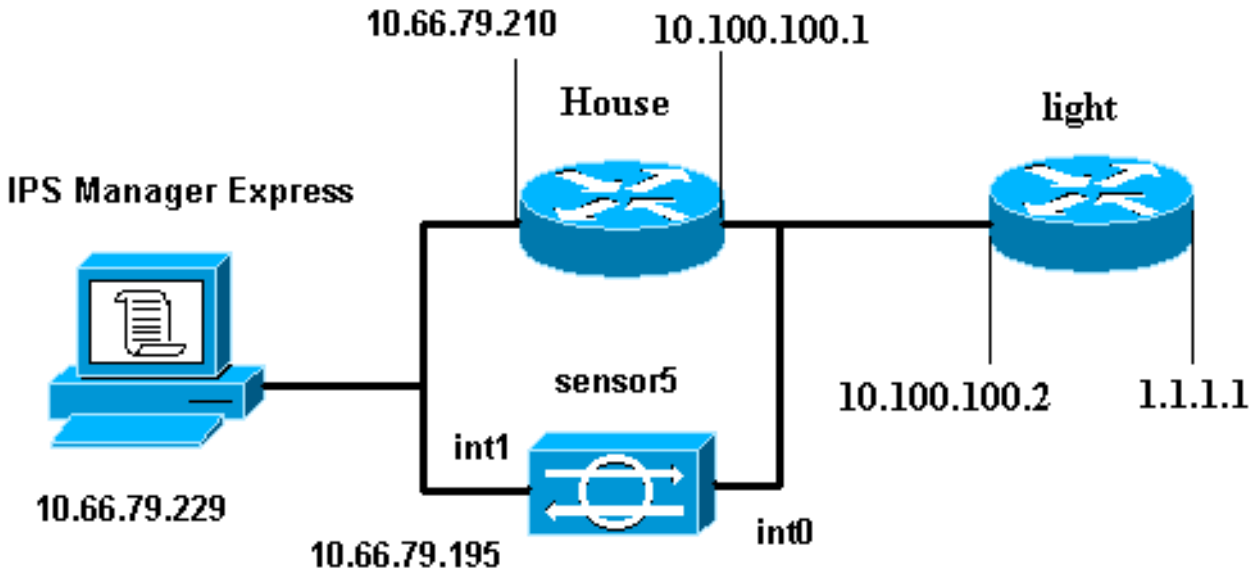
Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Configureren

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd.



Configuraties

Dit document gebruikt deze configuraties.

- 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
 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
```

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 logt, moet u **cisco** invoeren als de gebruikersnaam en **cisco** als het wachtwoord.
2. Wanneer het systeem u vraagt, wijzigt u uw wachtwoord.**Opmerking:** Cisco123 is een woordenboek en is niet toegestaan in het systeem.
3. Type **installatie** en volg de aanwijzingen in het systeem op 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 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
```

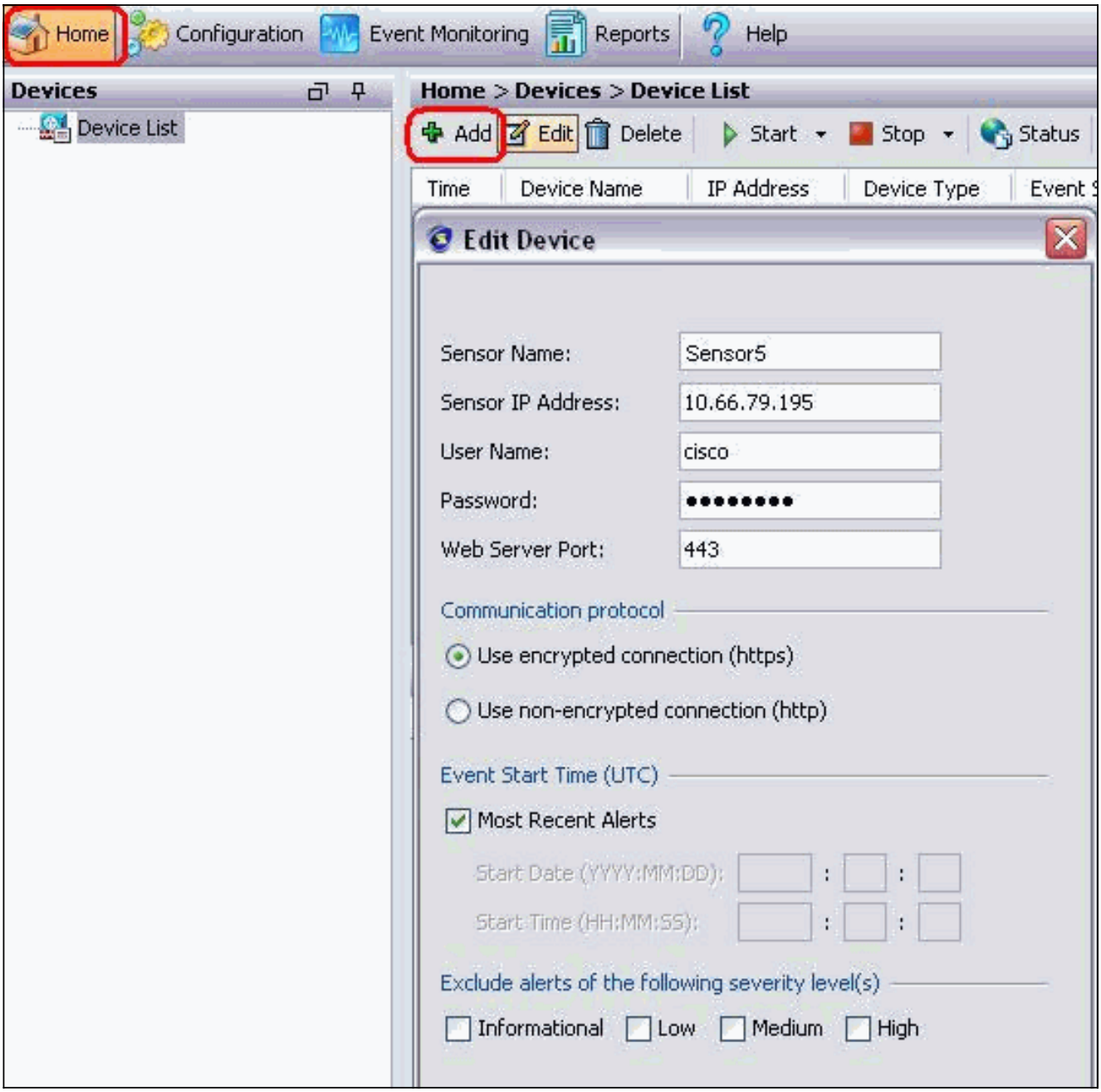
5. Bewaar de configuratie.Het kan een paar minuten duren voor de Sensor de configuratie opslaat.

```
[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
```

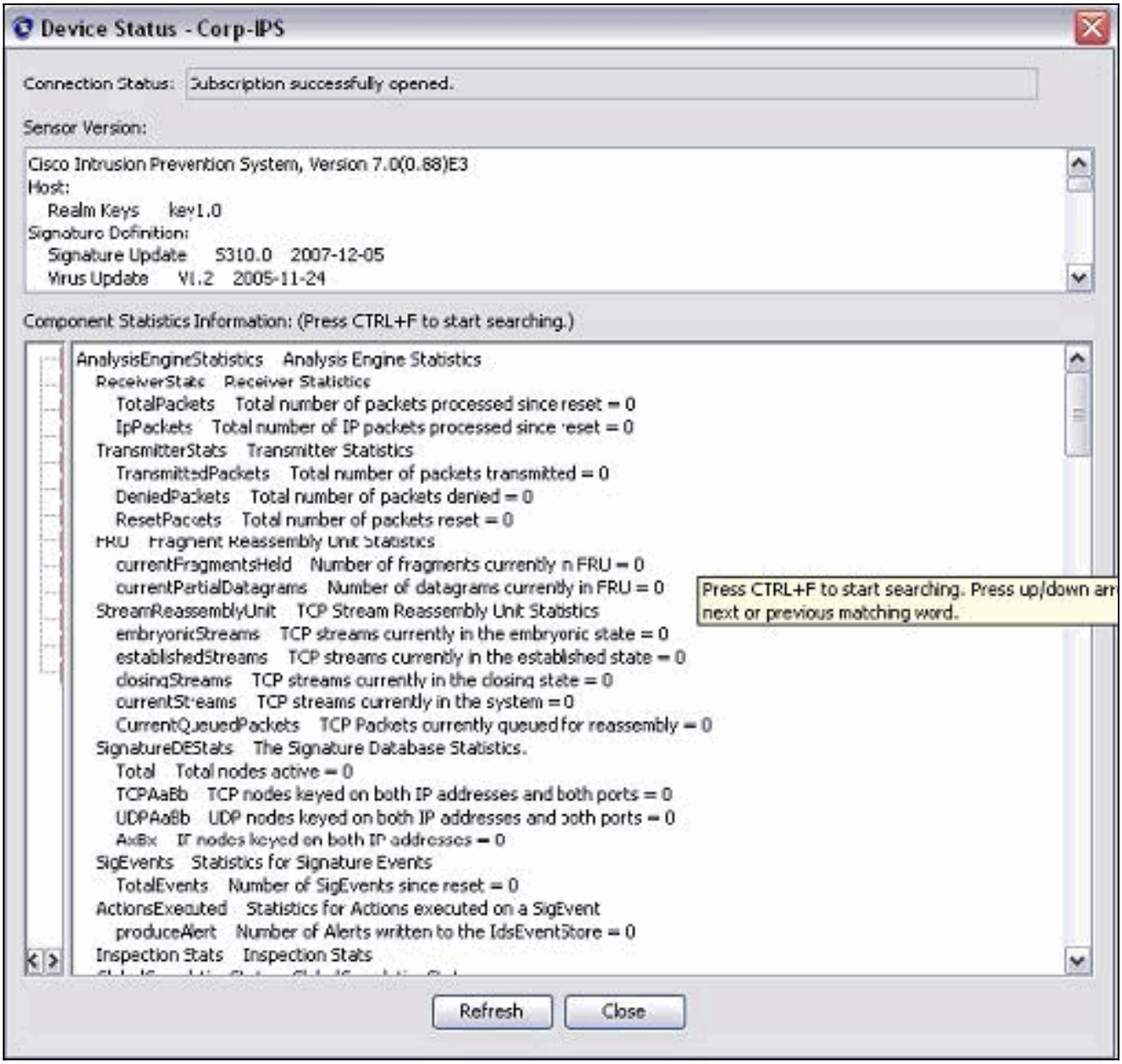
Stop de sensor in het IME

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 de **IPS Manager Express** opent.
2. Kies **startpunt > Toevoegen**.
3. Typ deze informatie en klik op **OK** om de configuratie te voltooien.



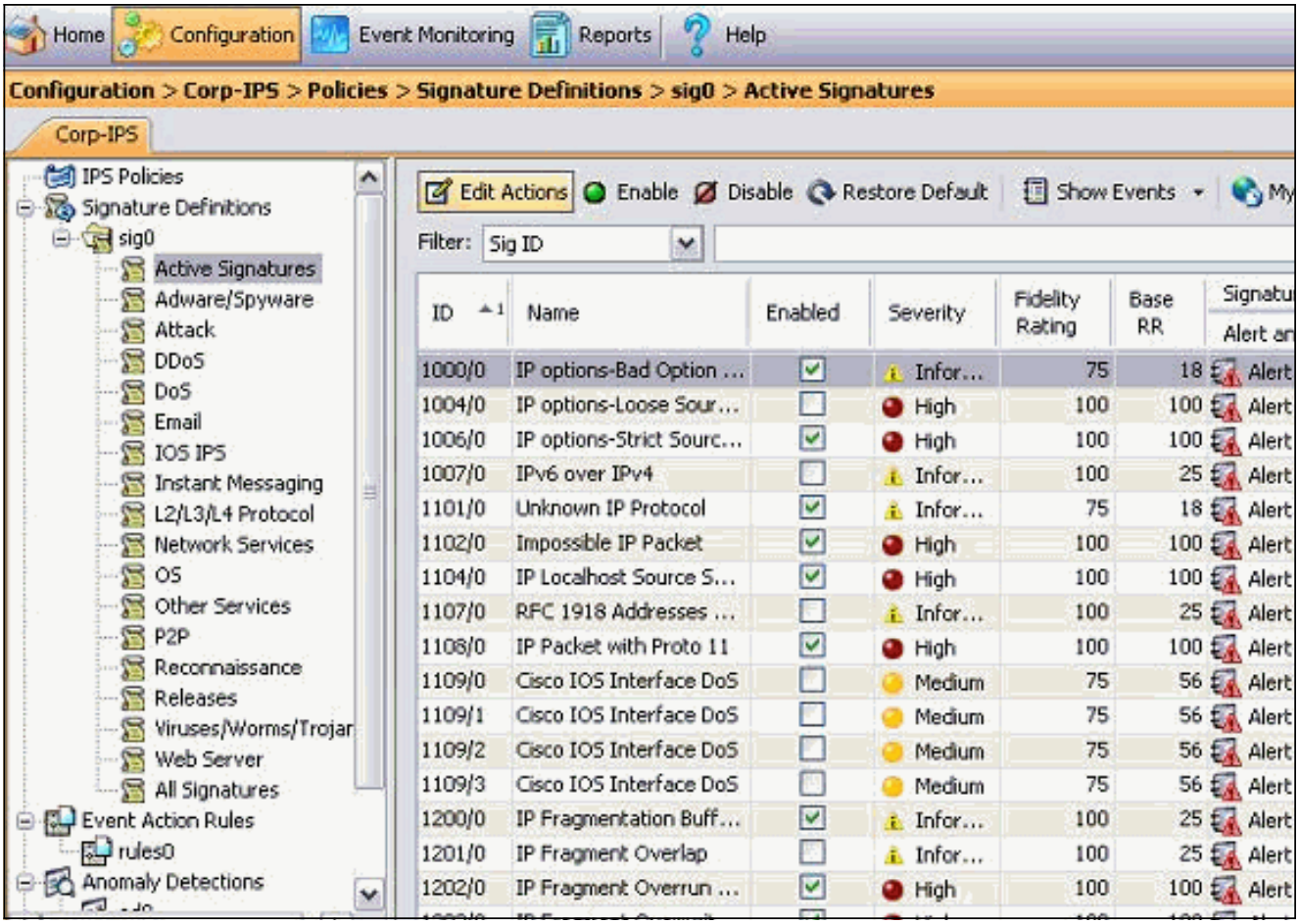
4. Kies **Apparaten > sensor5** om de status van de Sensor te controleren en klik dan met de rechtermuisknop om de **Status** te kiezen.Zorg dat u het *abonnement* kunt zien *openen.* bericht.



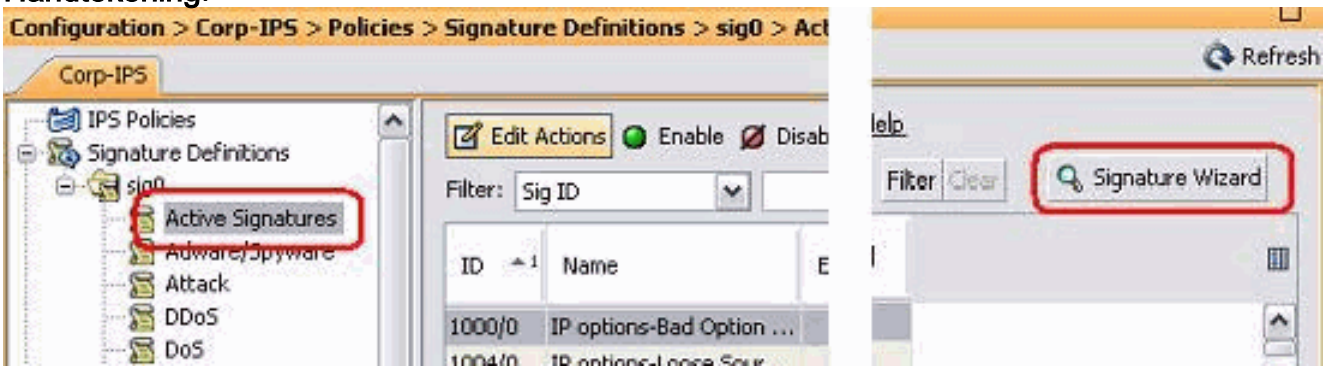
Blokken configureren voor Cisco IOS-router

Voltooi deze stappen om de blokkering voor de Cisco IOS-route 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:

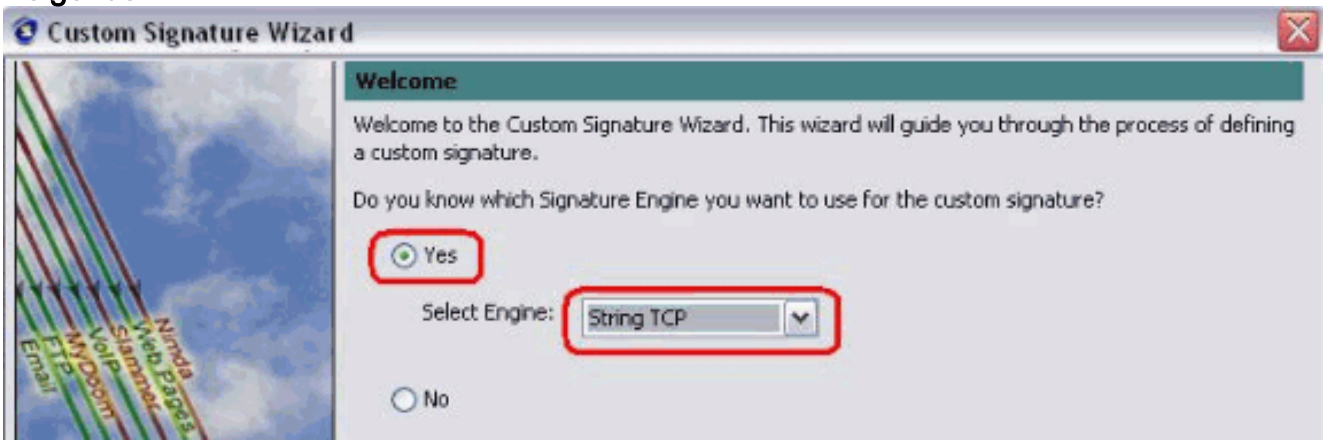


4. Klik in het tabblad Configuration op **actieve handtekeningen**.
5. Klik vervolgens op **Wizard Handtekening**.



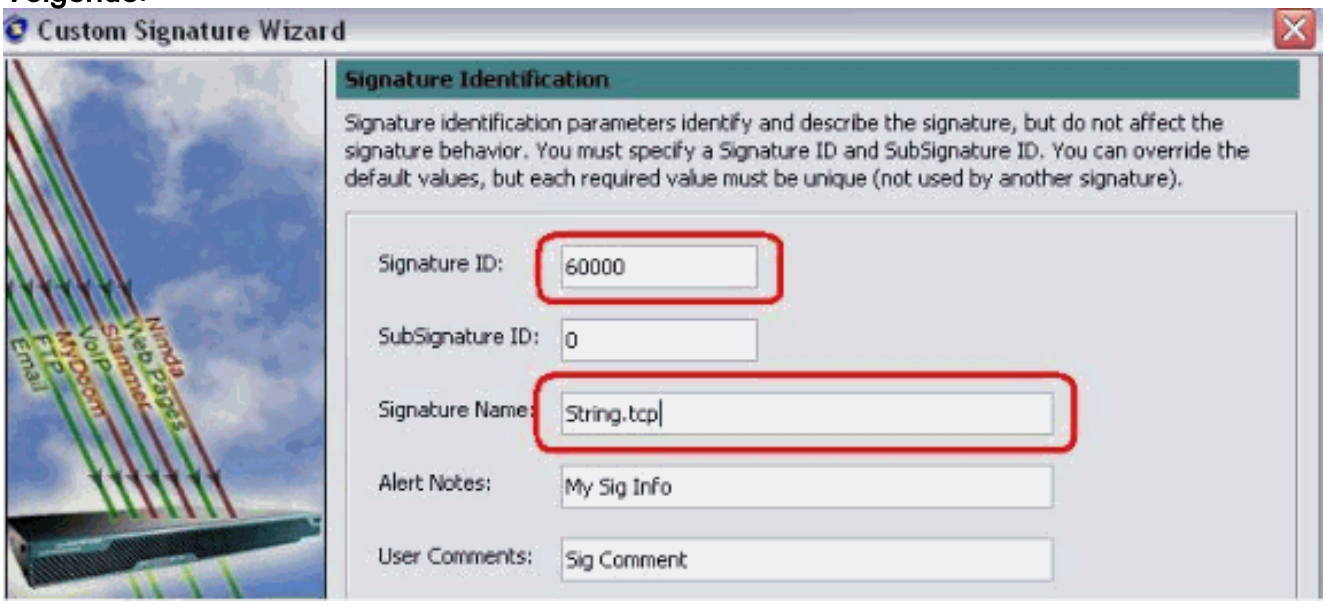
Opmerking: het vorige screenshot is door de beperkte ruimte in twee delen gesneden.

6. Kies **ja** en **string TCP** als Signature engine. Klik op **Volgende**.

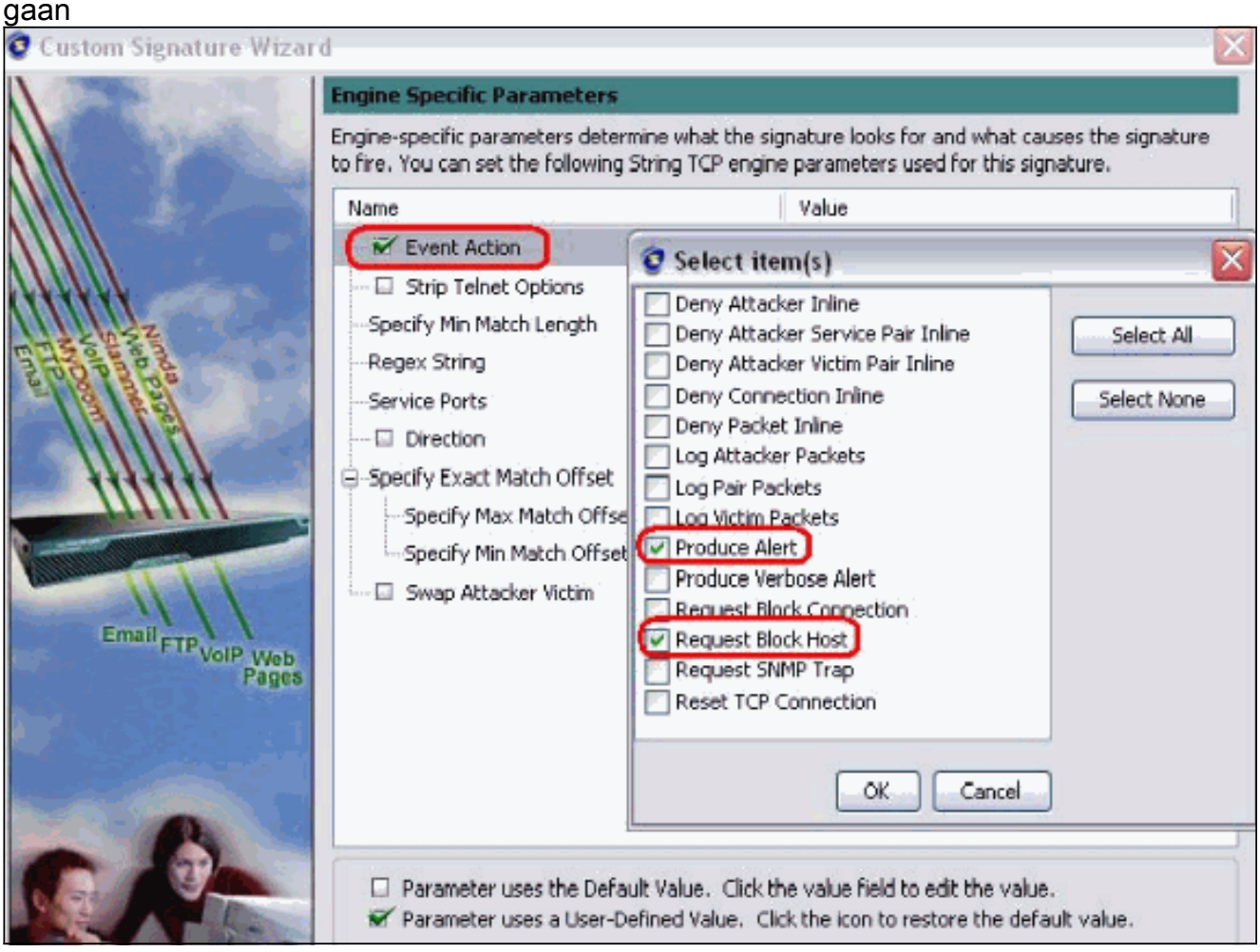


7. U kunt deze informatie als standaard achterlaten of uw eigen handtekening, handtekening en

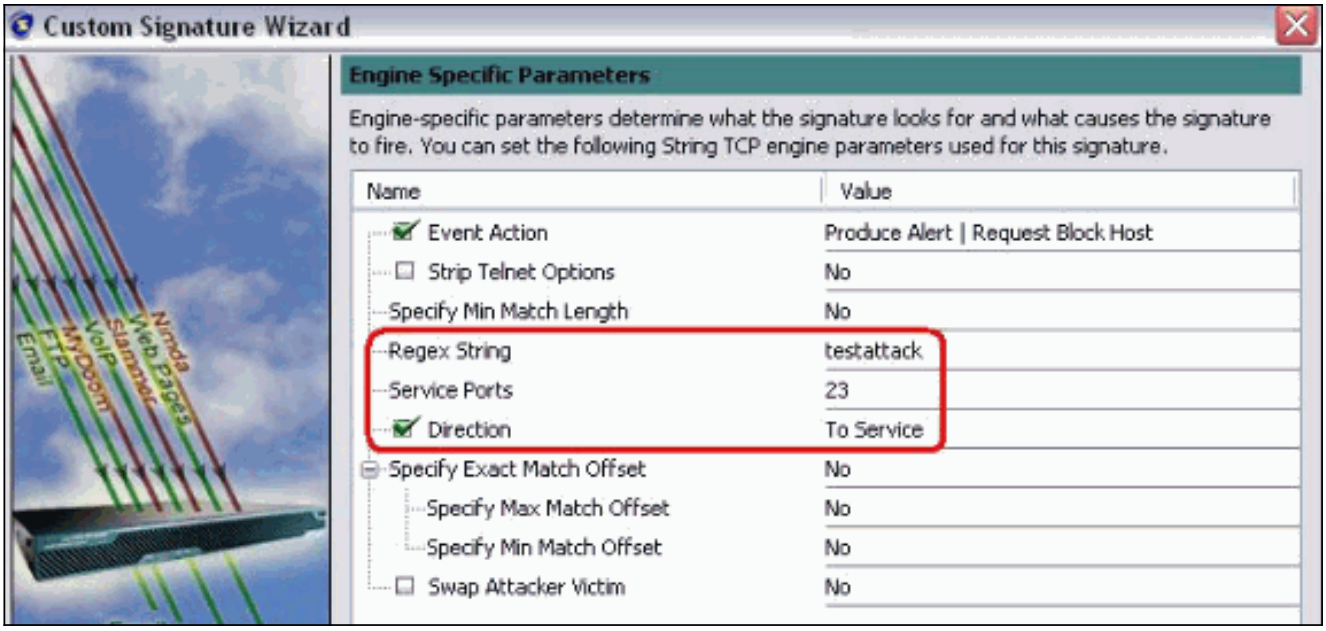
opmerkingen van de gebruiker invoeren. Klik op **Volgende**.



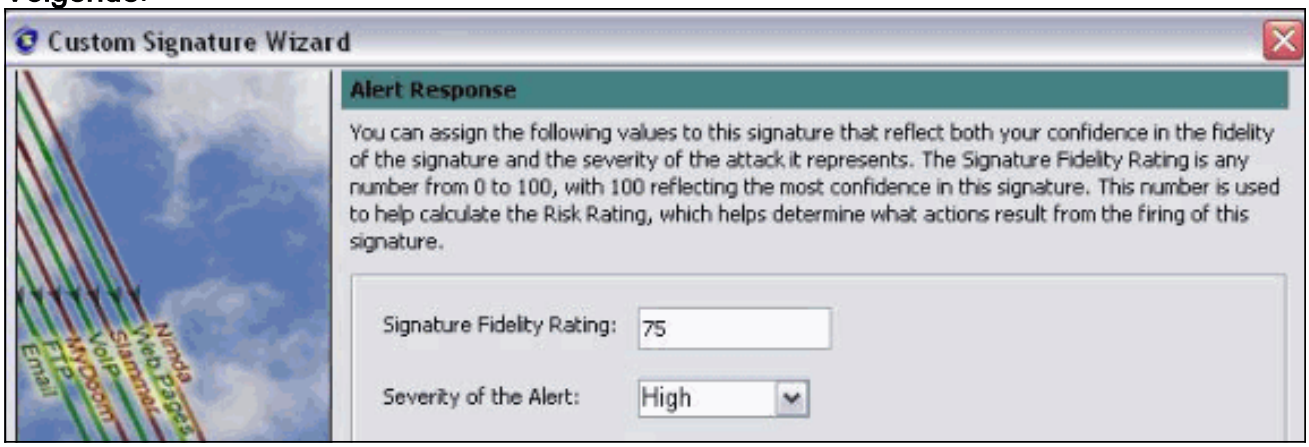
8. Kies **Event Action** en kies **Waarschuwen** en **Aanvraag Blokhost**. Klik op **Volgende** om verder te gaan



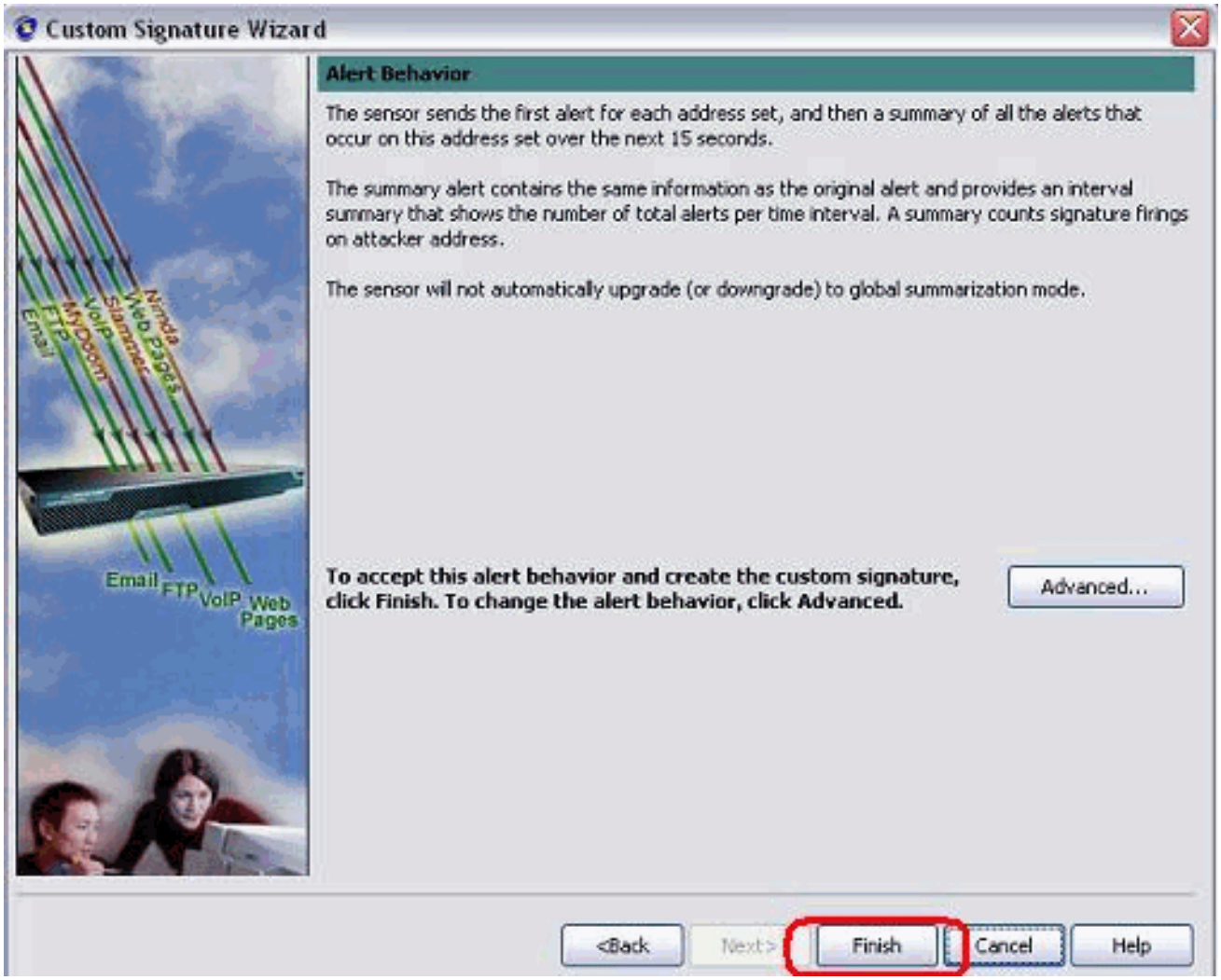
9. Voer een reguliere expressie in, die in dit voorbeeld *testattack* is, voer **23** voor servicepoorten in, kies **To Service** for the Direction en klik op **Next** om verder te gaan.



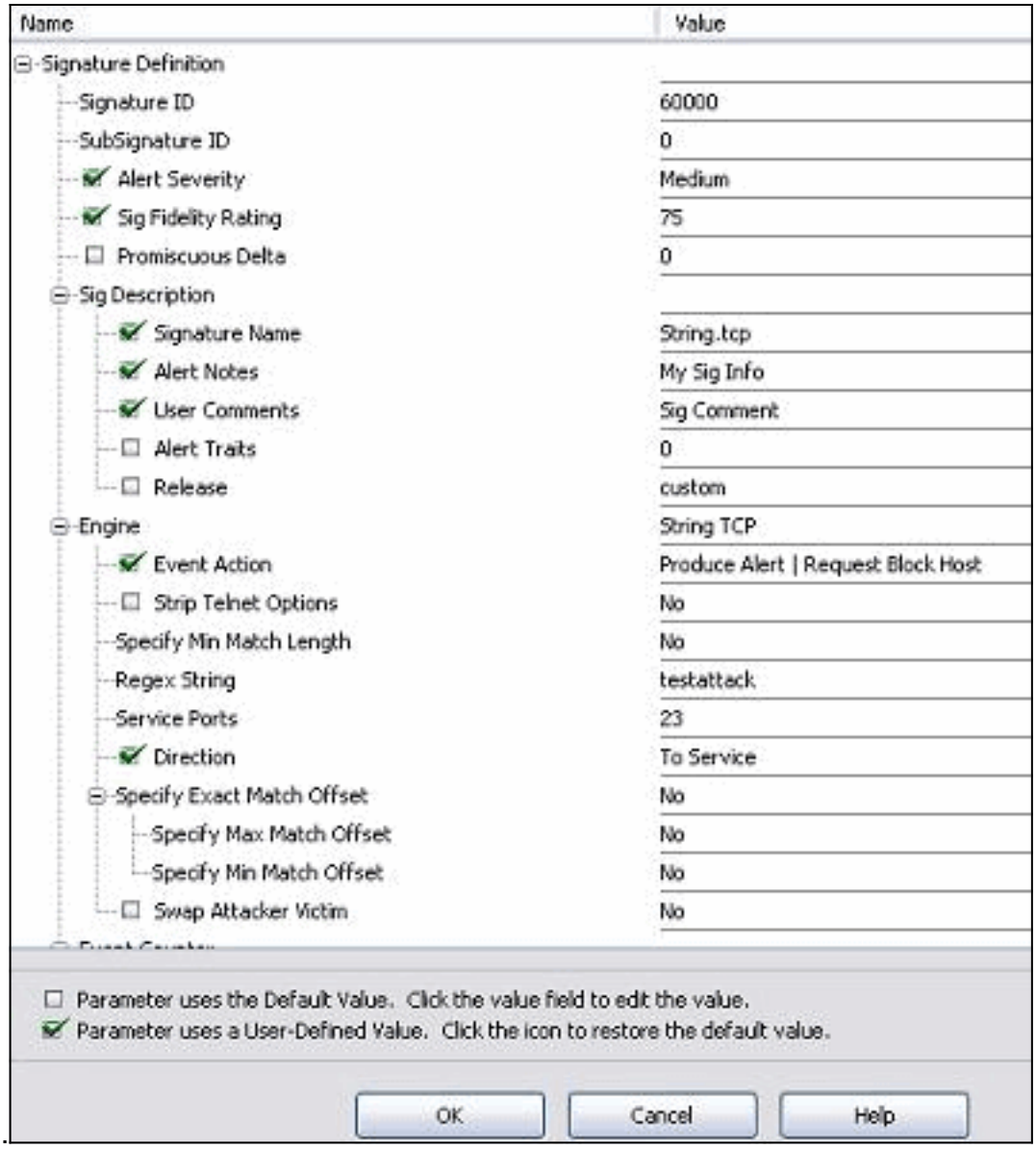
10. U kunt deze informatie als standaard opgeven. Klik op **Volgende**.



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

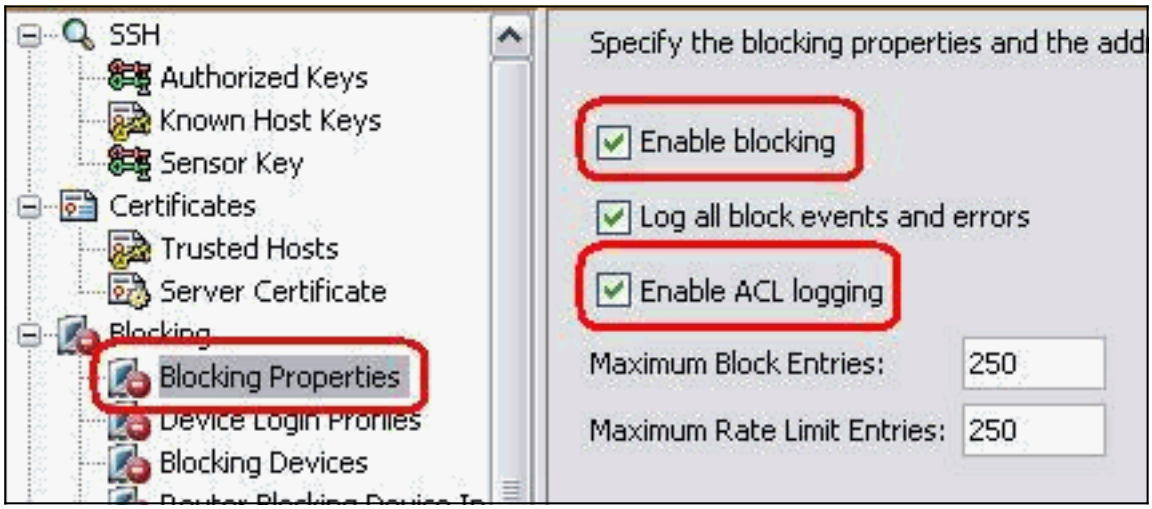


12. Kies **Configuration > Sg0 > Active Signatures** om de nieuwe handtekening te plaatsen onder **Sig ID** of **Sig Name**. Klik op **Bewerken** om de handtekening te

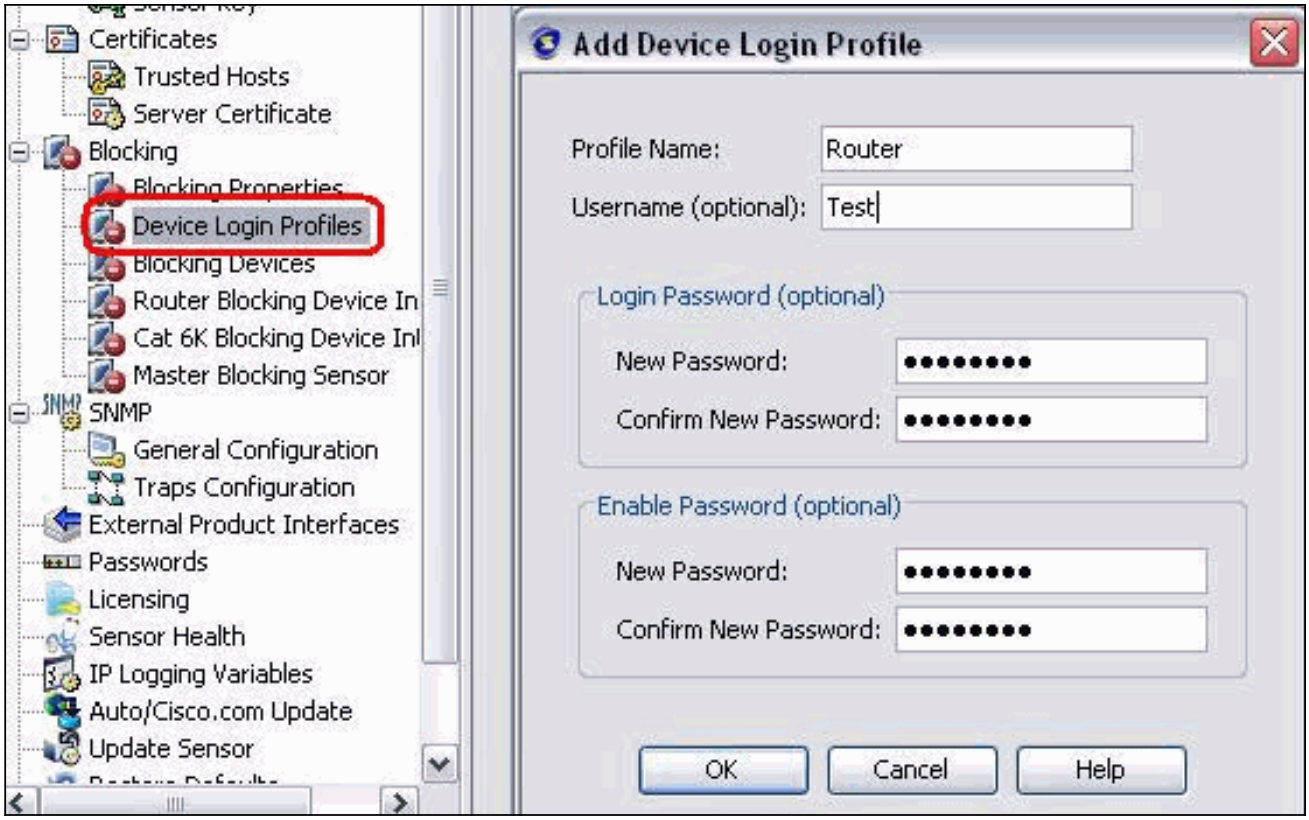


bekijken.

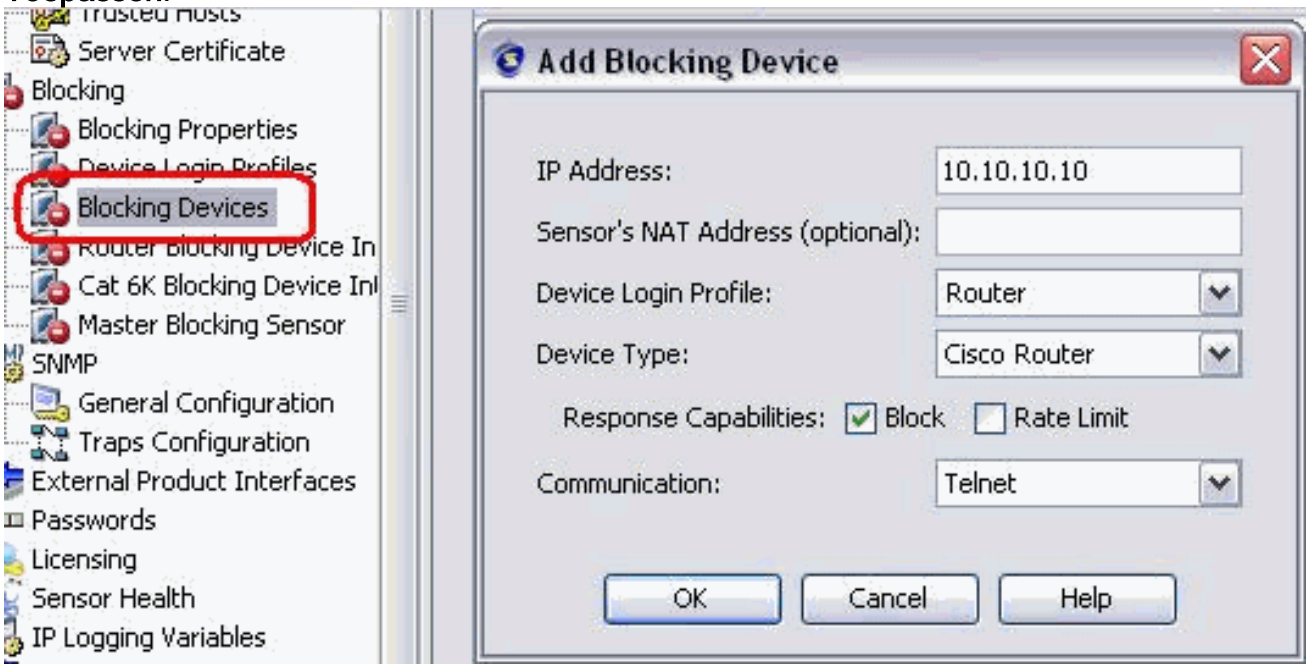
13. Klik op **OK** nadat u hebt bevestigd en klik op de knop **Toepassen** om de handtekening op de sensor toe te passen.
14. Klik onder Sensor Management op **Block** van het tabblad Configuration. Kies in het linker venster de optie **Eigenschappen blokkeren** en controleer **Blokken inschakelen**.



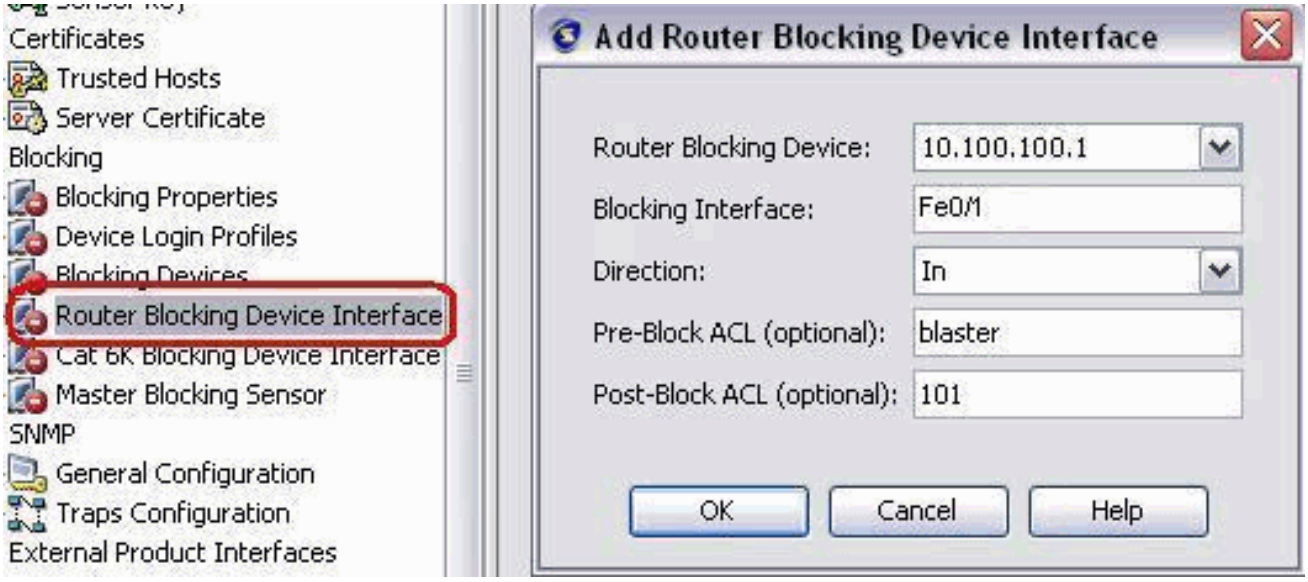
15. Ga nu vanuit het linker deelvenster naar **Apparaatinlogprofiel**. Klik op **Toevoegen** om een nieuw profiel te maken. Klik na het maken op **OK** en **Toepassen** om te sensor en verder te gaan.



16. De volgende stap is router als blokkerend apparaat te configureren. Kies in het linker venster een **blokkerend apparaat** en klik op **Toevoegen** om deze informatie toe te voegen. Klik vervolgens op **OK** en **Toepassen**.



17. Stel nu vanuit het linker deelvenster de interfaces van het blokkerende apparaat in. Voeg de informatie toe, klik op **OK** en **Toepassen**.



Verifiëren

Start de aanval en de blokkering

Voltooi deze stappen om de aanval te starten en het blokkeren:

1. Voordat u de aanval start, ga naar de IME, kies **Bewaking van gebeurtenis > Verlaten Attacks Beeld** en kies de sensor aan de rechterkant.
2. Telnet aan routerhuis en verifieert de communicatie van de server met deze opdrachten.

```
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. Van routerlicht, telnet tot routerhuis en type **testattack**.Sluit of **<space>** of **<enter>** om uw Telnet-sessie te resetten.

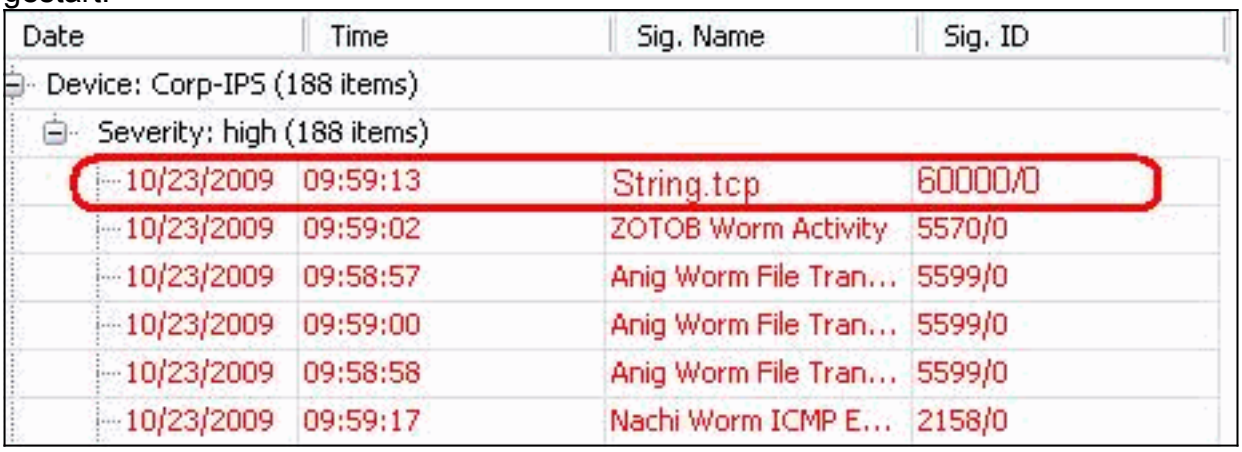
```
light#telnet 10.100.100.1
    Trying 10.100.100.1 ... Open

    User Access Verification
    Password:
    house>en
    Password:
    house#testattack
    [Connection to 10.100.100.1 lost]
    !--- Host 10.100.100.2 has been blocked due to the !--- signature "testattack"
triggered.
```

4. Telnet om Huis van de router te gebruiken en het bevel **van de** show **toegang-lijst** te gebruiken zoals hier getoond.

```
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. Vanuit het Dashboard van het IDS 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:

- Vanaf de Sensor kijk naar de **show statistics network-access** output en zorg ervoor dat de `staat`"actief is. Van de console of SSH tot de sensor, wordt deze informatie bekeken:

```
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#
```

- Zorg ervoor dat de communicatieparameter aangeeft dat het juiste protocol wordt gebruikt, zoals telnet of SSH met 3DES. U kunt een handmatige SSH of telnet van een SSH/telnet-client op een pc proberen om de gebruikersnaam en de wachtwoordreferenties te controleren correct zijn. Probeer dan om net of SSH van de Sensor zelf naar de router te tellen en zie of u met succes kunt inloggen op de router.

Gerelateerde informatie

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