Konfigurieren der IPS-Blockierung mit IME

Inhalt

Einführung

In diesem Dokument wird die Konfiguration der IPS-Blockierung (Intrusion Prevention System) unter Verwendung von IPS Manager Express (IME) erläutert. IME- und IPS-Sensoren werden zur Blockierung eines Cisco Routers verwendet. Beachten Sie bei 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.

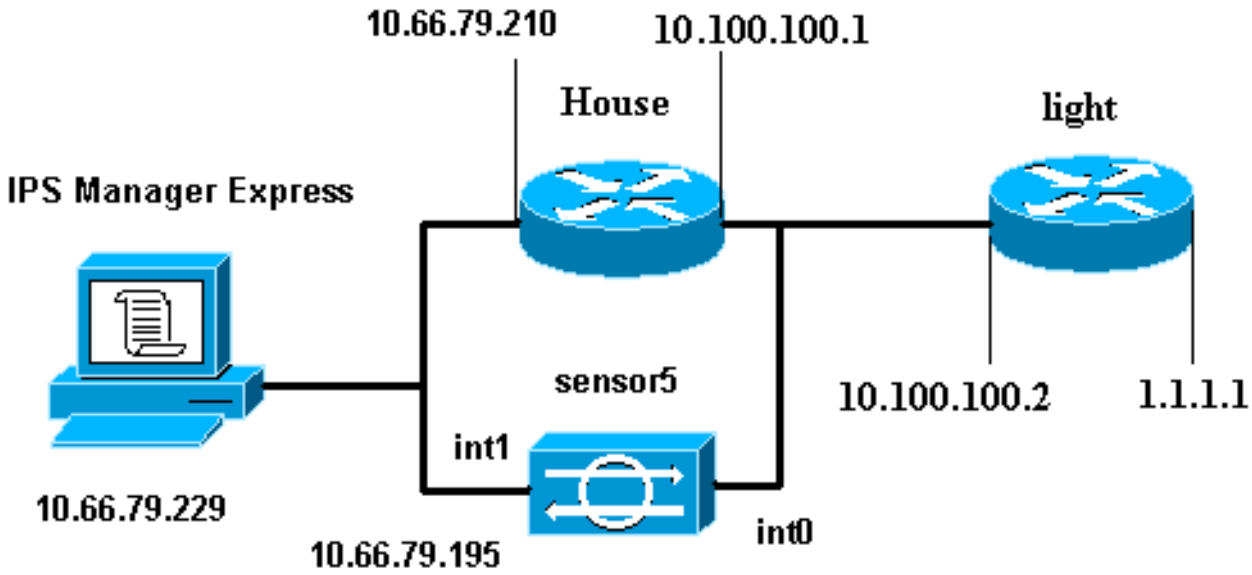
Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Konfigurieren

Netzwerkdiagramm

In diesem Dokument wird diese Netzwerkeinrichtung verwendet.



Konfigurationen

In diesem Dokument werden diese 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
 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
```

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 folgen Sie der Systemaufforderung, um die Basisparameter für die Sensoren festzulegen.
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 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. Speichern Sie die Konfiguration.Es kann einige Minuten dauern, bis der Sensor die Konfiguration gespeichert hat.

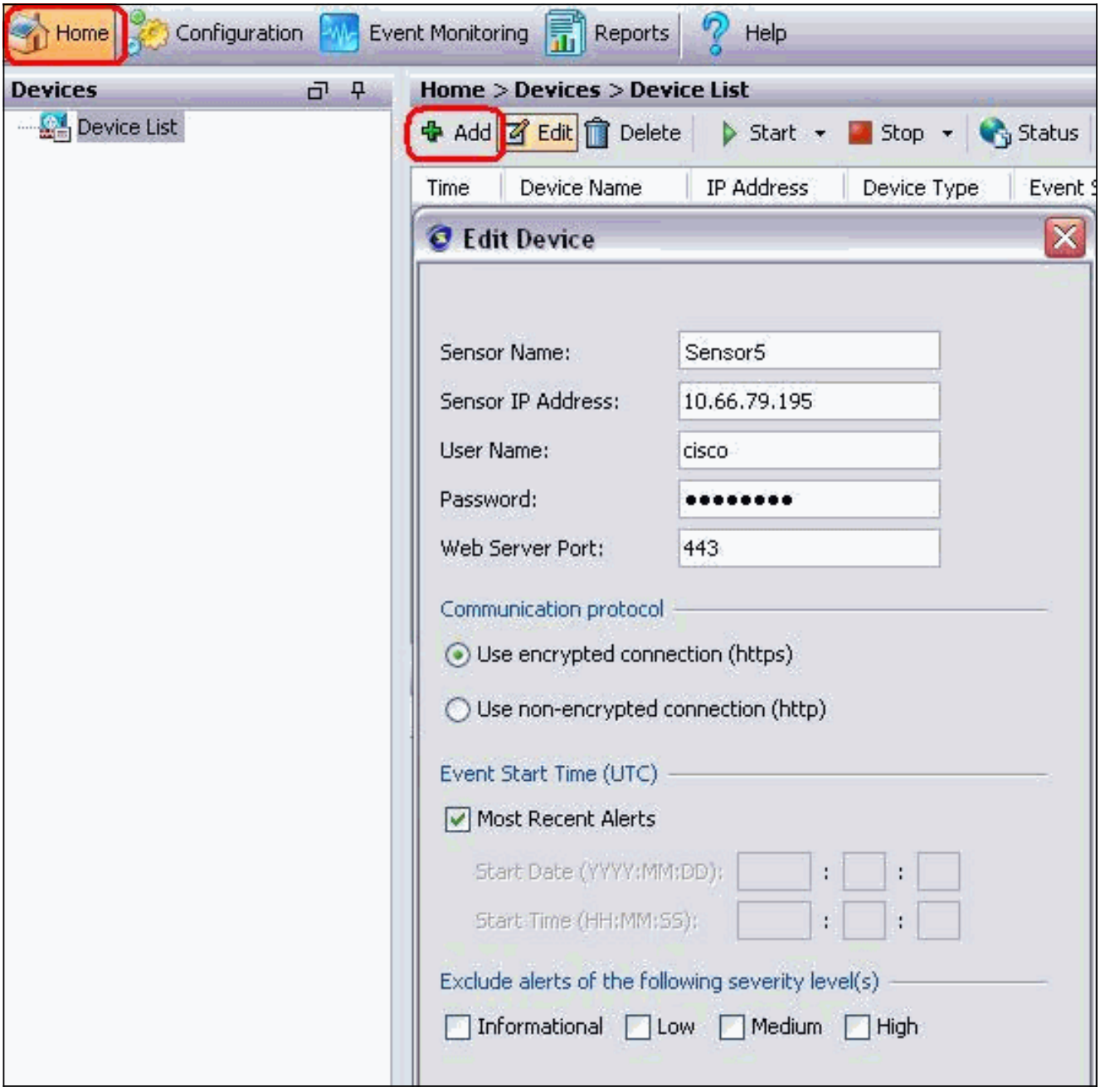
```
[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.
```

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

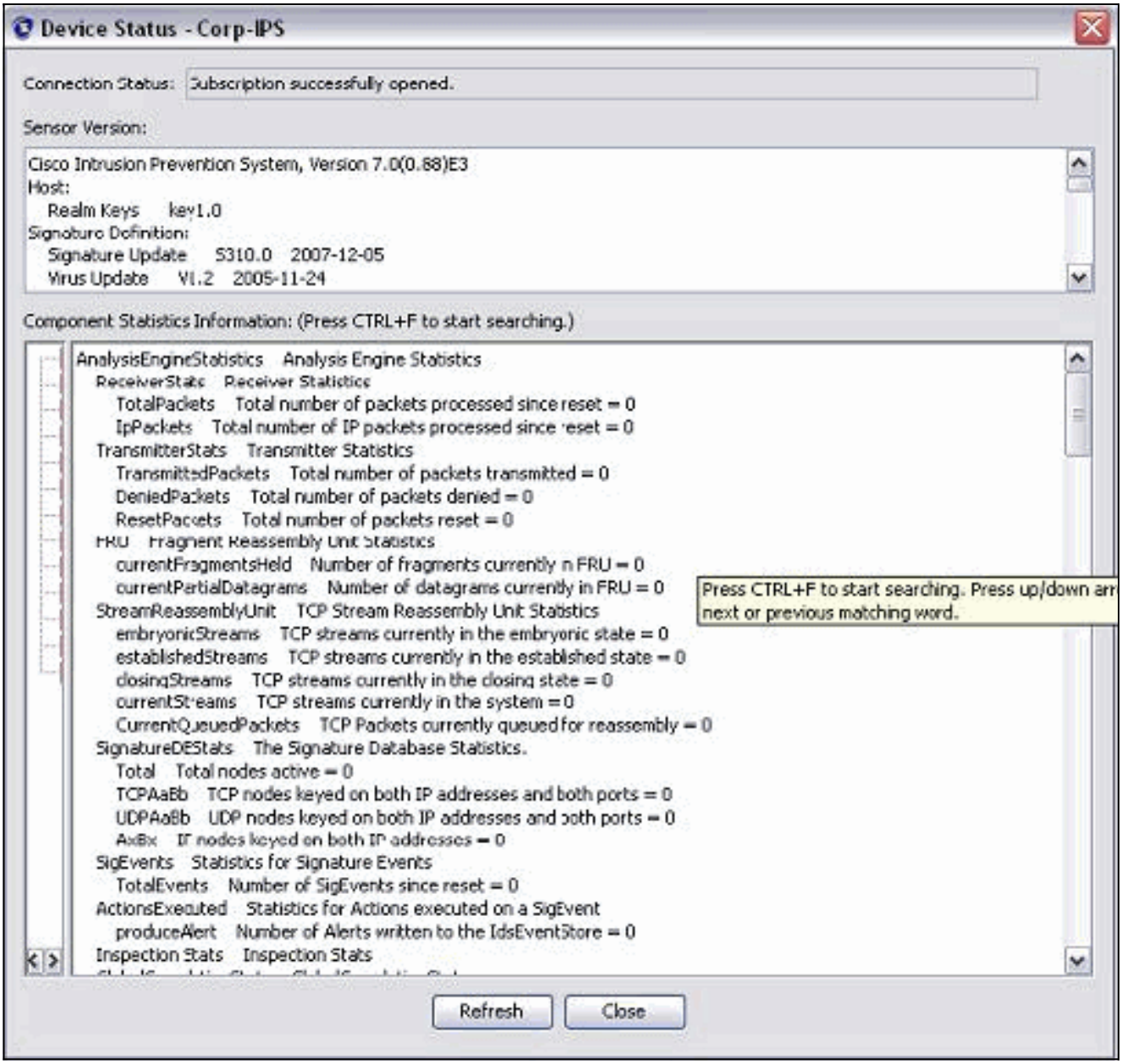
Hinzufügen des Sensors zum IME

Führen Sie diese Schritte aus, um den Sensor in das IME aufzunehmen.

1. Wechseln Sie zum Windows-PC, der IPS Manager Express installiert hat, und öffnen Sie den **IPS Manager Express**.
2. Wählen Sie **Home > Add**.
3. Geben Sie diese Informationen ein und klicken Sie auf **OK**, um die Konfiguration abzuschließen.



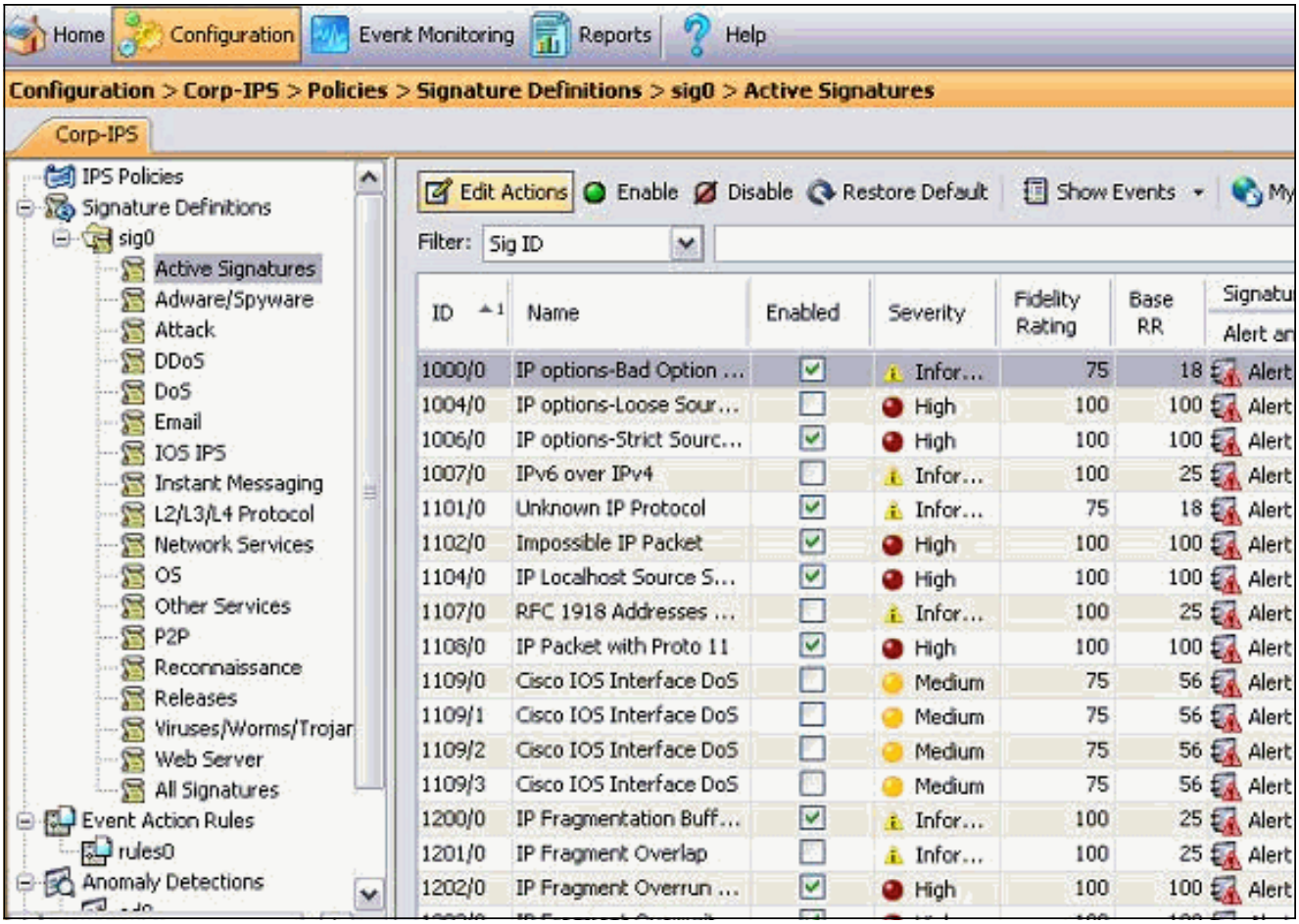
4. Wählen Sie **Geräte > Sensor5**, um den Sensorstatus zu überprüfen, und klicken Sie dann mit der rechten Maustaste auf **Status**.Vergewissern Sie sich, dass das *Abonnement erfolgreich geöffnet wurde.*
   Nachricht.



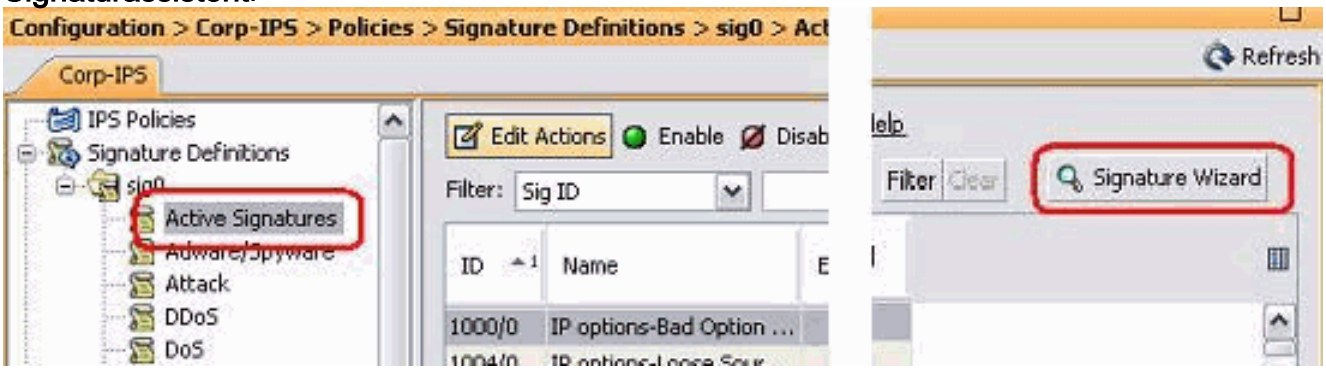
Konfigurieren der Blockierung für den Cisco IOS-Router

Gehen Sie wie folgt vor, um die Blockierung für die Cisco IOS-Route 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:

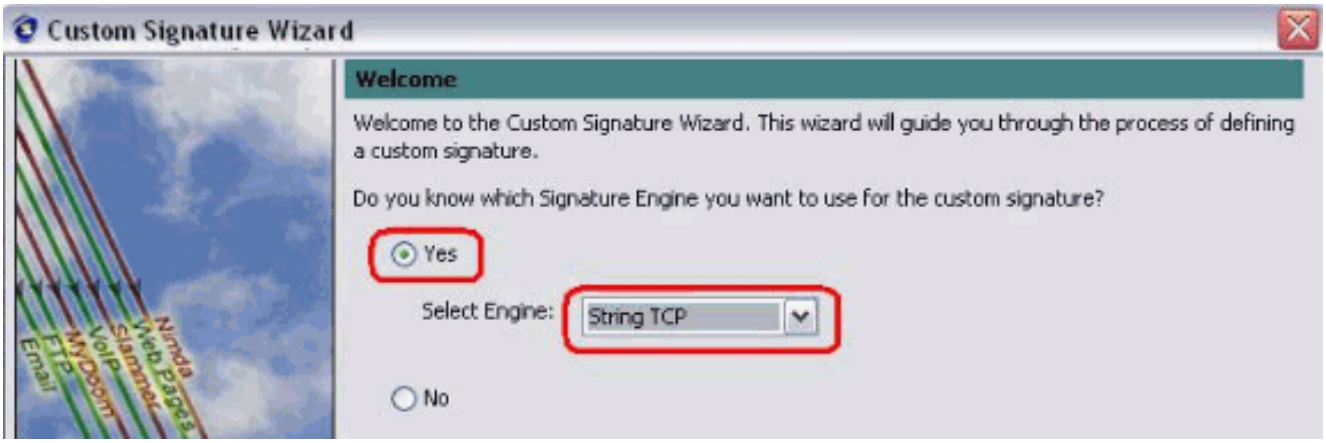


4. Klicken Sie auf der Registerkarte Konfiguration auf **Aktive Signaturen**.
5. Klicken Sie anschließend auf **Signaturassistent**.

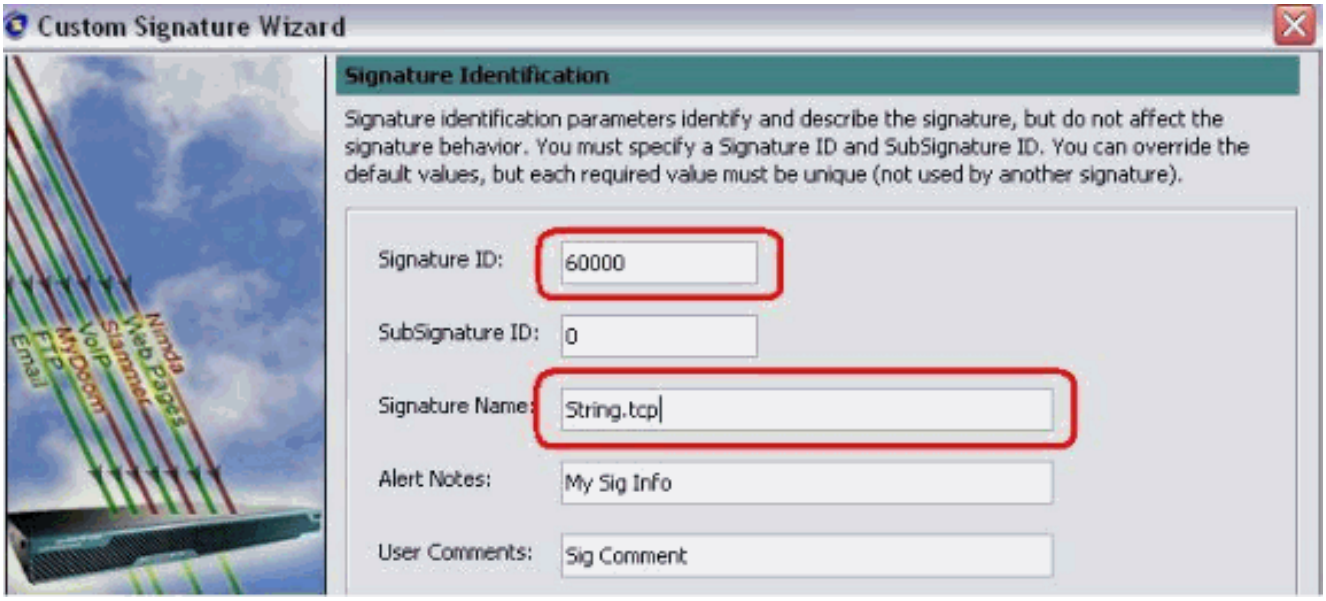


Hinweis: Der vorherige Screenshot wurde aufgrund der Platzbeschränkung in zwei Teile geschnitten.

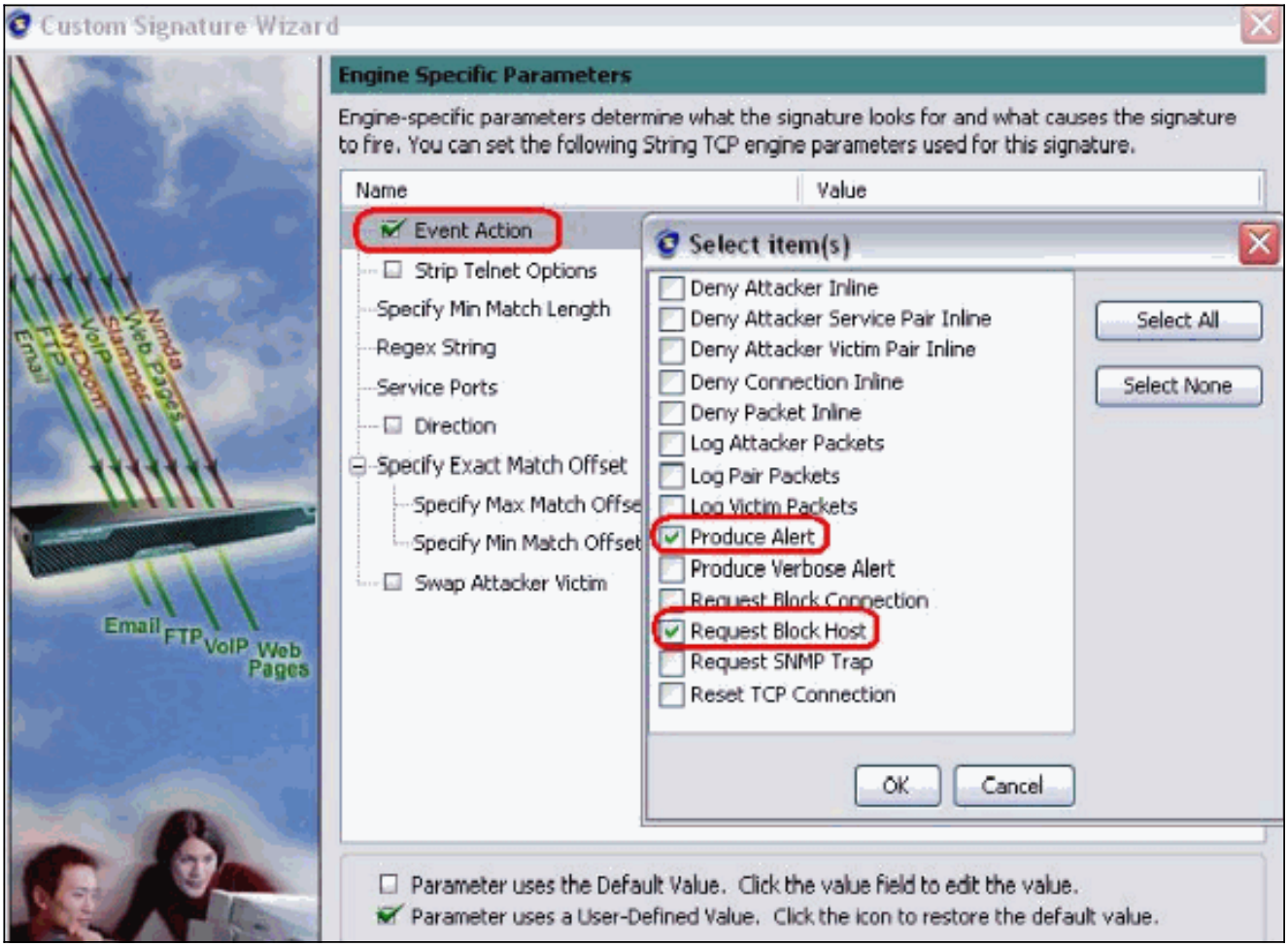
6. Wählen Sie **Yes** und **String TCP** als Signature-Engine aus. Klicken Sie auf **Weiter**.



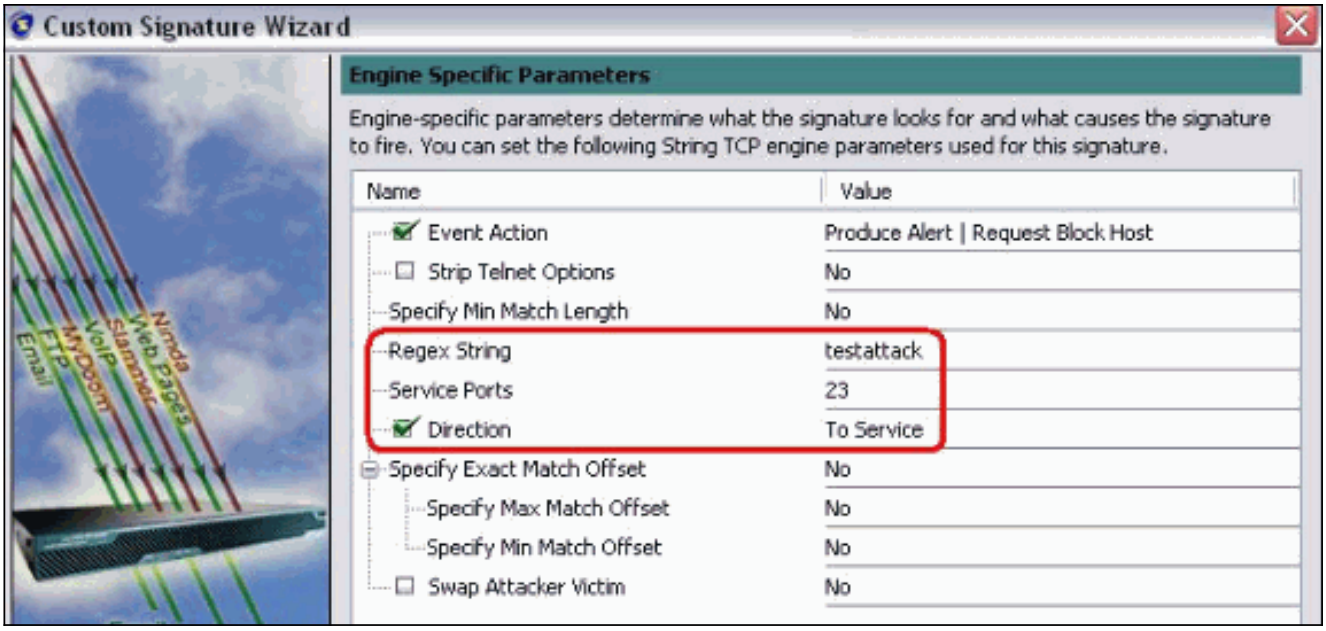
7. Sie können diese Informationen als Standard belassen oder Ihre eigene Signature-ID, Signaturname und Benutzerhinweise eingeben. Klicken Sie auf **Weiter**.



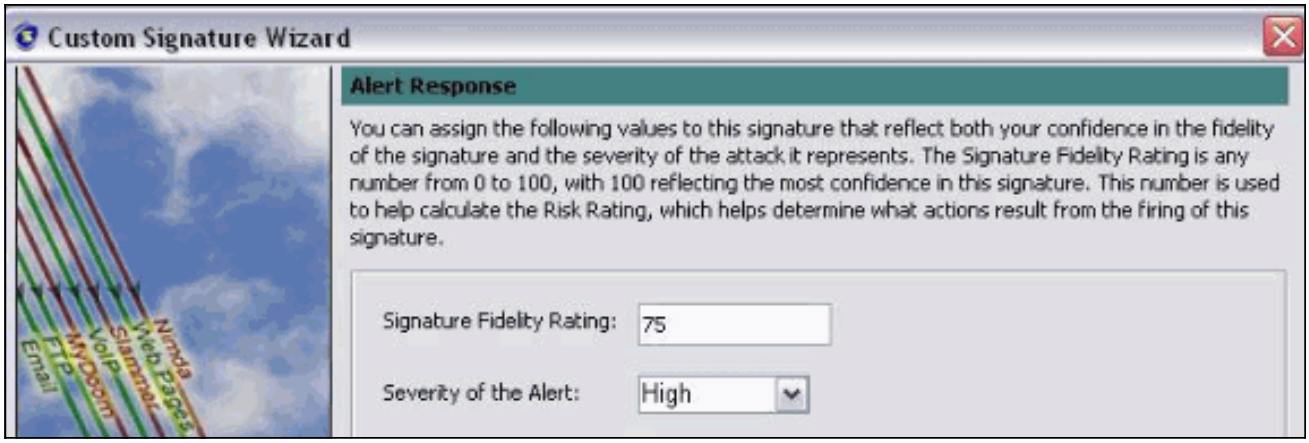
8. Wählen Sie **Event Action (Ereignisaktion)** und **Produce Alert** and **Request Block Host**. Klicken Sie auf **Weiter**, um fortzufahren.



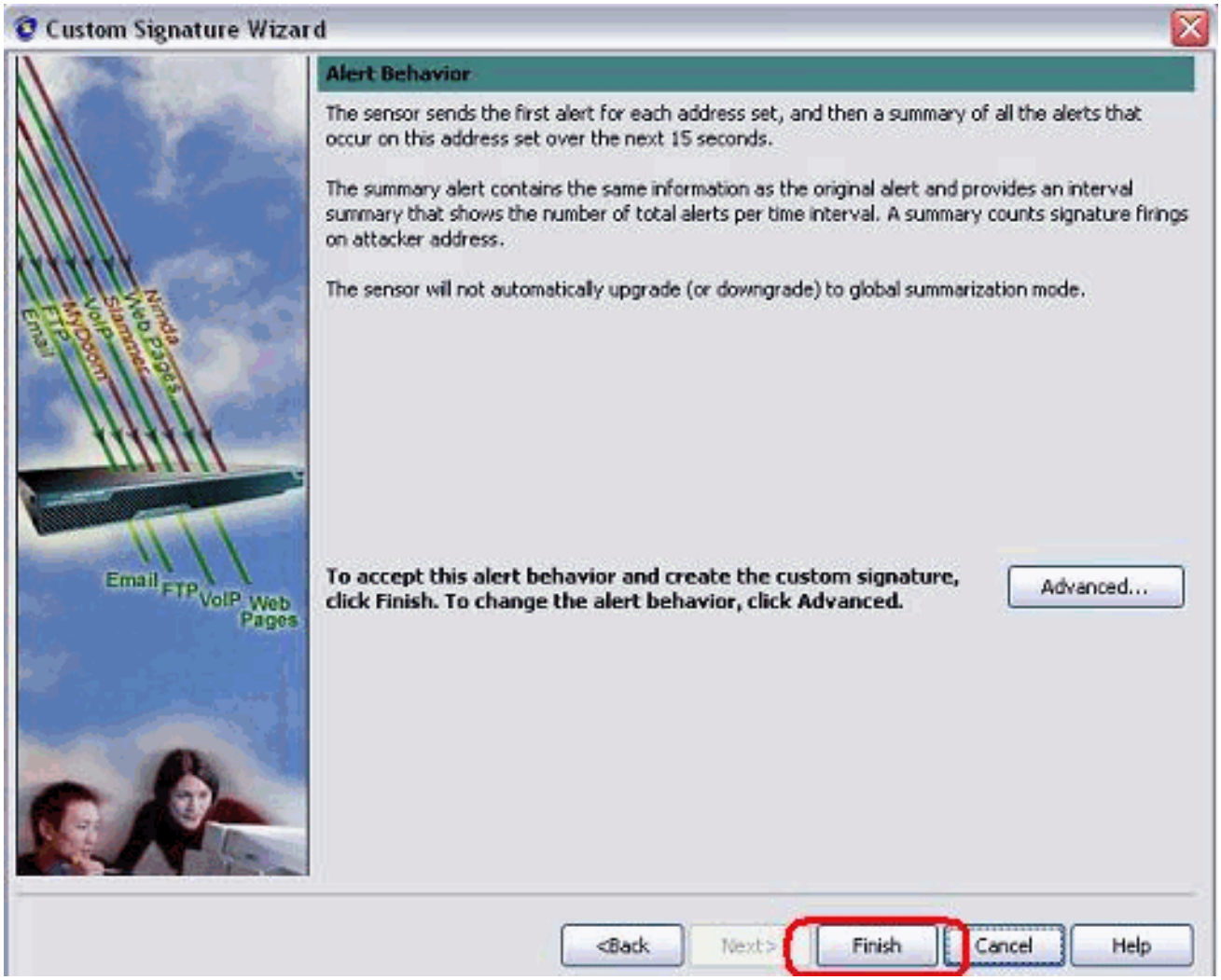
9. Geben Sie einen regulären Ausdruck ein, der in diesem Beispiel *testattack* ist, geben Sie **23** für Service-Ports ein, wählen Sie **To Service** for the Direction aus, und klicken Sie auf **Weiter**, um fortzufahren.



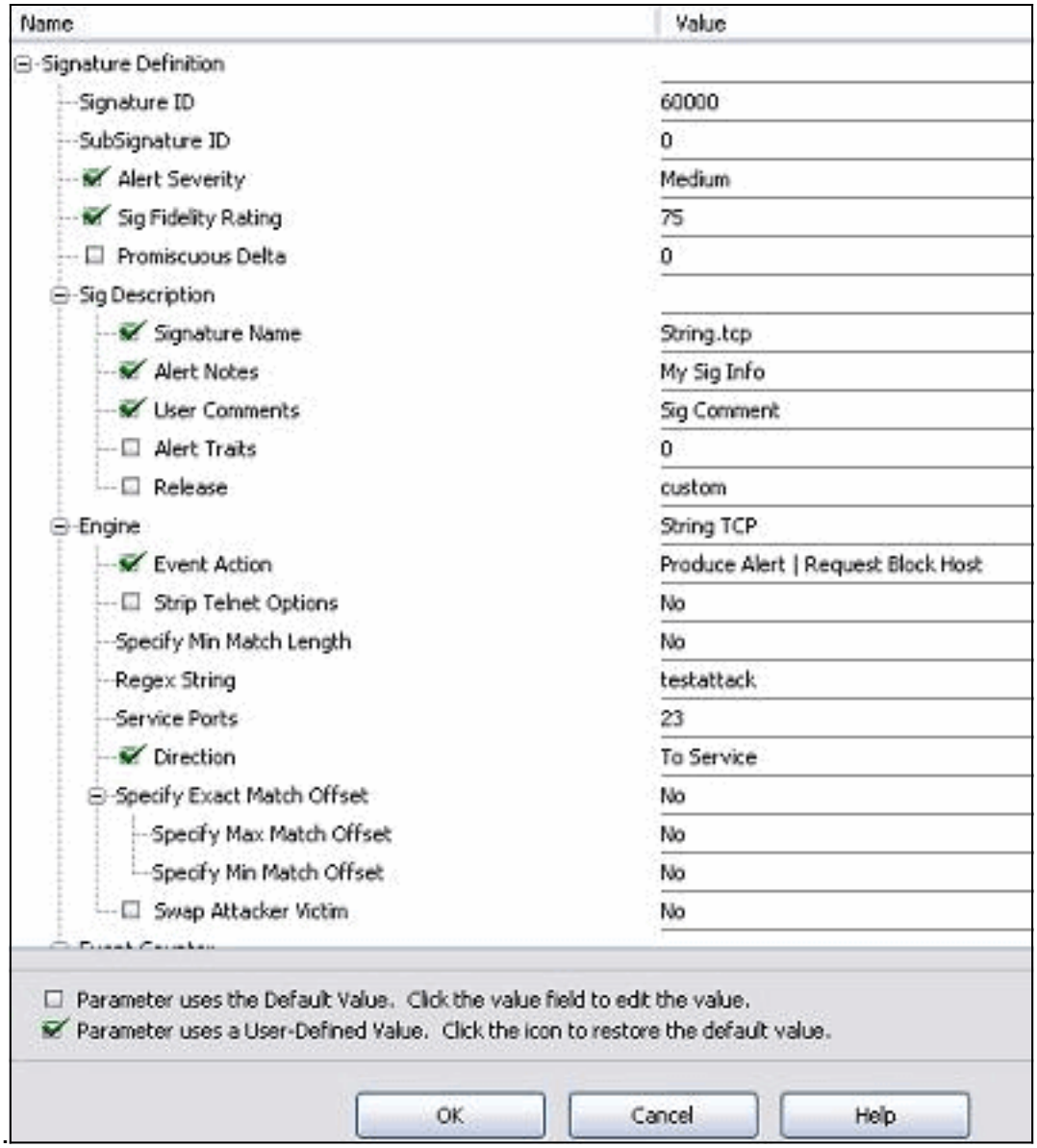
10. Sie können diese Informationen als Standard belassen. Klicken Sie auf **Weiter**.



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

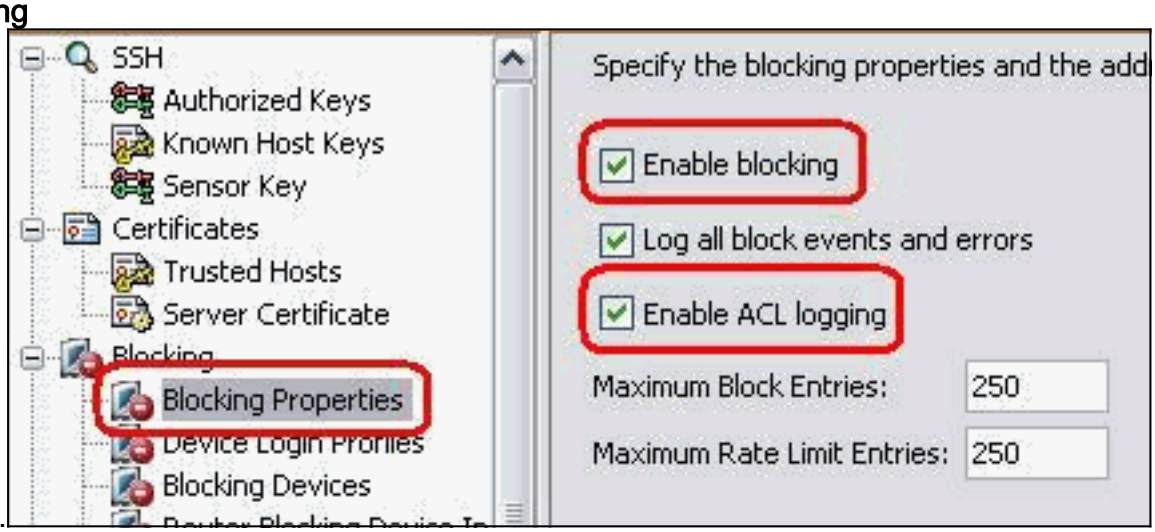


12. Wählen Sie **Configuration > sig0 > Active Signatures (Konfiguration > sig0 > aktive Signaturen)**, um die neu erstellte Signatur mithilfe der **Signature-ID** oder des **Signaturnamens** zu suchen. Klicken Sie auf **Bearbeiten**, um die Signatur



anzuzeigen.

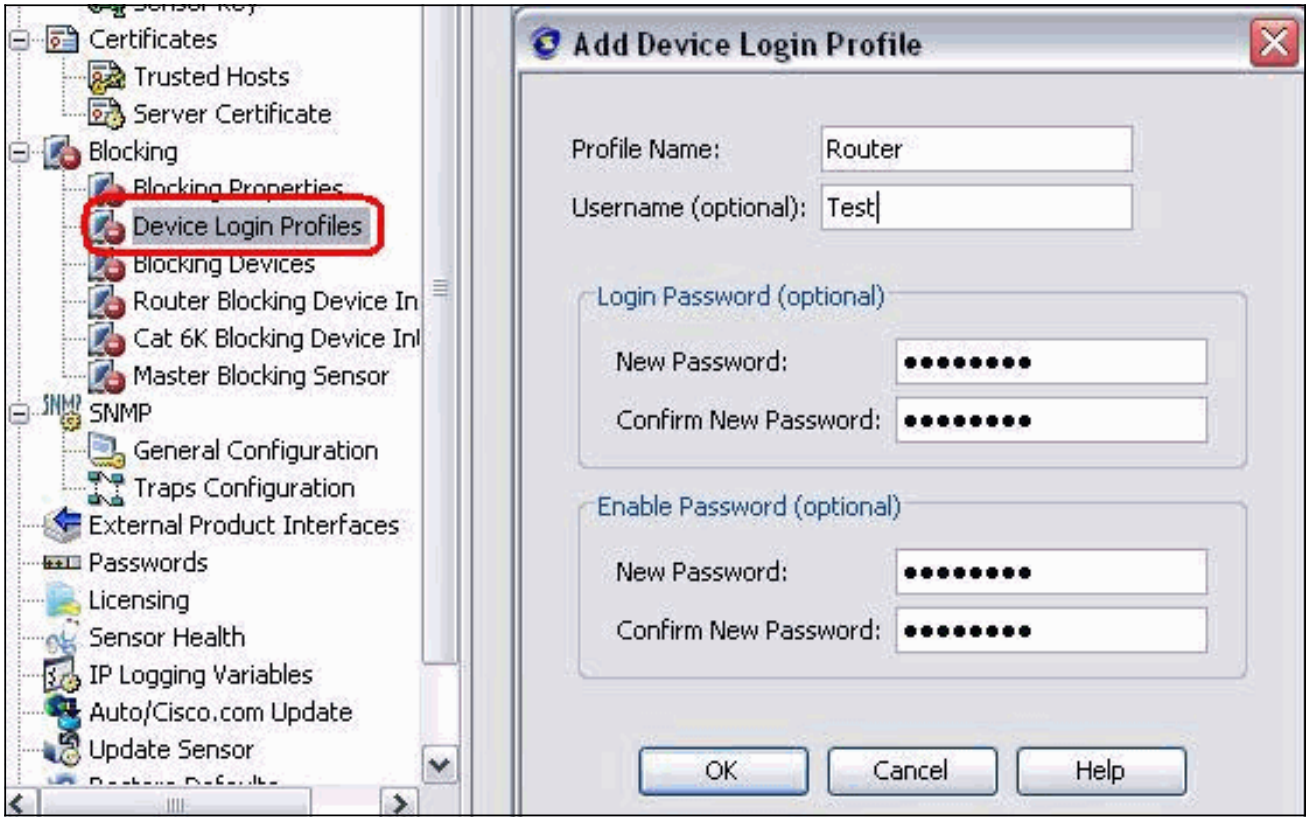
13. Klicken Sie nach der Bestätigung auf **OK** und anschließend auf die Schaltfläche **Übernehmen**, um die Signatur auf den Sensor anzuwenden.
14. Klicken Sie auf der Registerkarte Konfiguration unter Sensorverwaltung auf **Blockieren**. Wählen Sie im linken Bereich **Blockierungseigenschaften** aus, und aktivieren Sie **Blockierung**



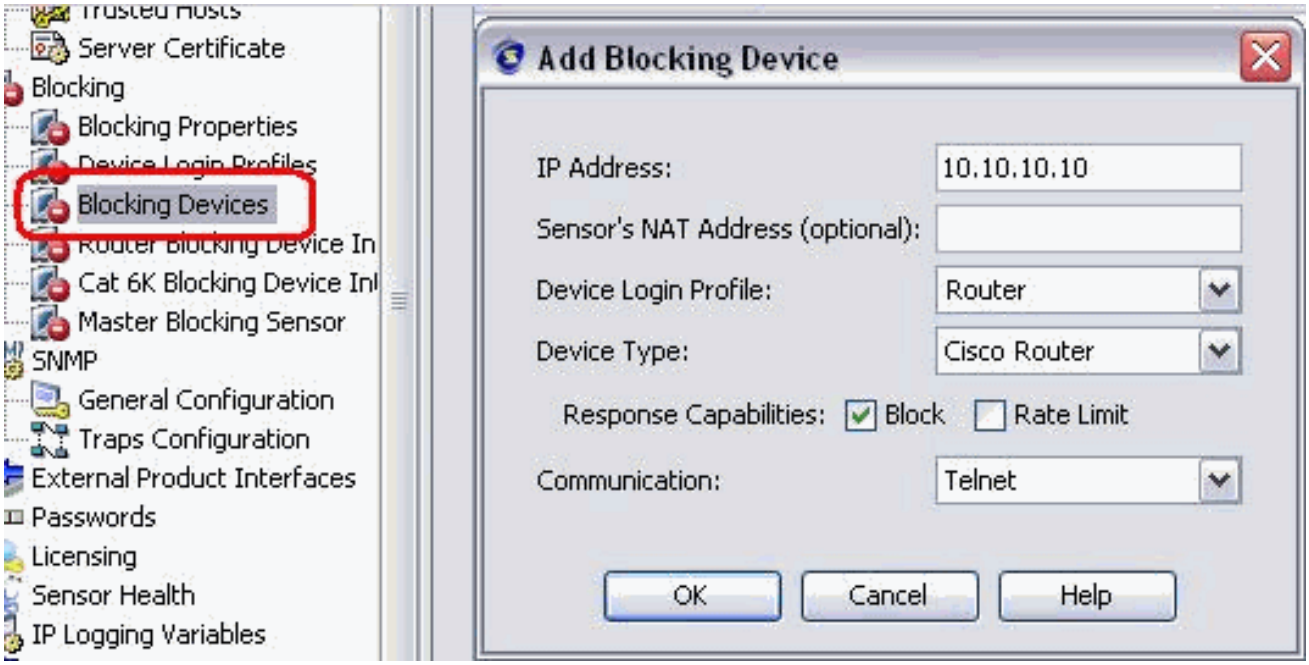
aktivieren.

15. Wechseln Sie im linken Teilfenster zum **Geräteanmeldeprofil**. Klicken Sie zum Erstellen eines neuen Profils auf **Hinzufügen**. Klicken Sie nach der Erstellung auf **OK** und **Übernehmen**, um den Sensor auszuwählen und

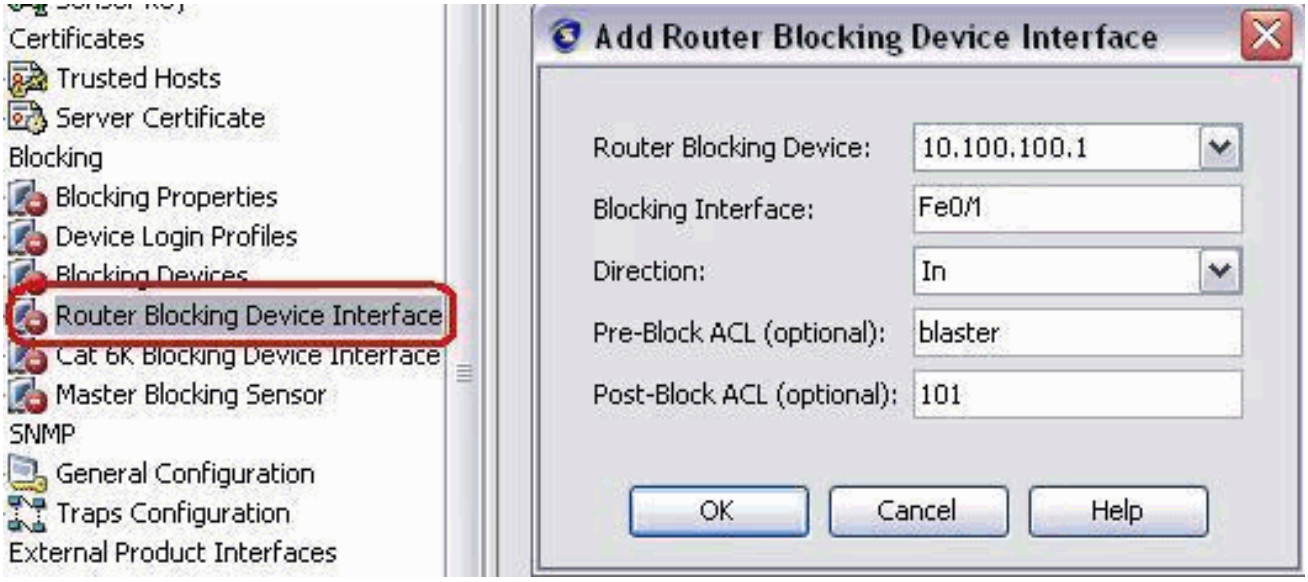
fortzufahren.



16. Im nächsten Schritt wird der Router als Blockierungsgerät konfiguriert. Wählen Sie im linken Teilfenster **Blockierungsgerät** aus, und klicken Sie auf **Hinzufügen**, um diese Informationen hinzuzufügen. Klicken Sie dann auf **OK** und **Übernehmen**.



17. Konfigurieren Sie jetzt im linken Bereich die Geräteschnittstellen blockieren. Fügen Sie die Informationen hinzu, klicken Sie auf **OK** und **Übernehmen**.



Überprüfen

Angriff und Blockierung starten

Gehen Sie wie folgt vor, um den Angriff zu starten und zu blockieren:

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. Telnet zu Router House und überprüfen Sie die Kommunikation vom Server mit diesen Befehlen.

```
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. Von Router Light, Telnet zu Router House und geben **testattack ein**.Drücken Sie entweder **<Leerzeichen>** oder **<Eingabe>**, um Ihre Telnet-Sitzung zurückzusetzen.

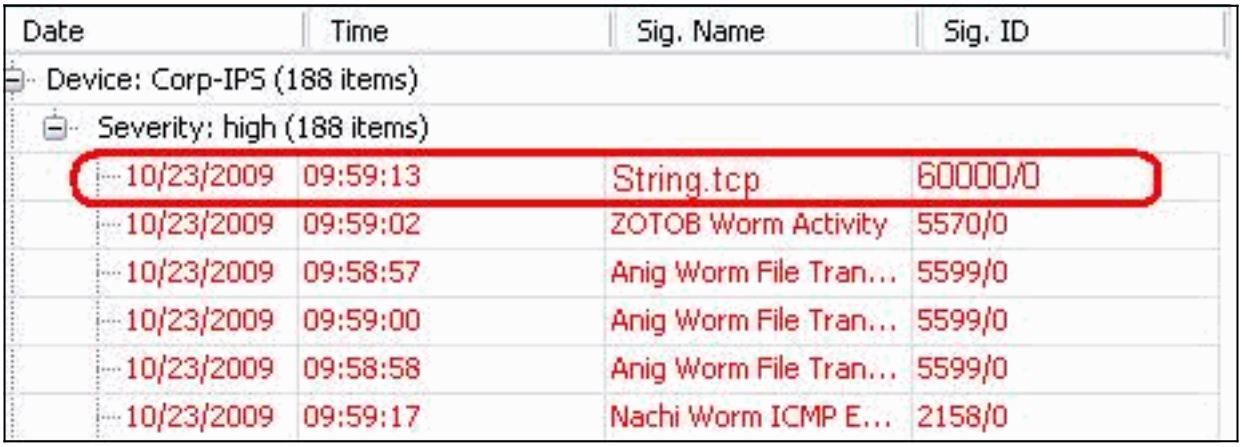
```
light#telnet 10.100.100.1
    Trying 10.100.100.1 ... Open

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

4. Telnet zu Router House und verwenden den Befehl **show access-list** wie hier gezeigt.

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



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

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Tipps

Tipps zur Fehlerbehebung:

- Sehen Sie sich den Sensor an, um die **Ausgabe statistischer Netzwerkzugriffsdaten** anzuzeigen und sicherzustellen, dass der `Status` aktiv ist. Von der Konsole oder SSH zum Sensor werden diese Informationen angezeigt:

```
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#
```

- Stellen Sie sicher, dass der Kommunikationsparameter anzeigt, dass das richtige Protokoll verwendet wird, z. B. Telnet oder SSH mit 3DES. Sie können ein manuelles SSH oder Telnet von einem SSH/Telnet-Client auf einem PC ausprobieren, um die Richtigkeit von

Benutzername und Kennwort zu überprüfen. Versuchen Sie dann, Telnet oder SSH vom Sensor selbst zum Router zu starten, und prüfen Sie, ob Sie sich erfolgreich beim Router anmelden können.

Zugehörige Informationen

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