Configurazione del blocco IPS con l'IME

Sommario

Introduzione

In questo documento viene descritta la configurazione del blocco IPS (Intrusion Prevention System) tramite l'utilizzo dell'IME (Intrusion Prevention System). I sensori IME e IPS vengono utilizzati per gestire un router Cisco per il blocco. Tenere presente quanto segue quando si considera questa configurazione:

- Installare il sensore e accertarsi che funzioni correttamente.
- Estendere l'interfaccia di sniffing al router esterno all'interfaccia.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco IPS Manager Express 7.0
- Sensore Cisco IPS 7.0(0.88)E3
- Router Cisco IOS® con software Cisco IOS versione 12.4

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

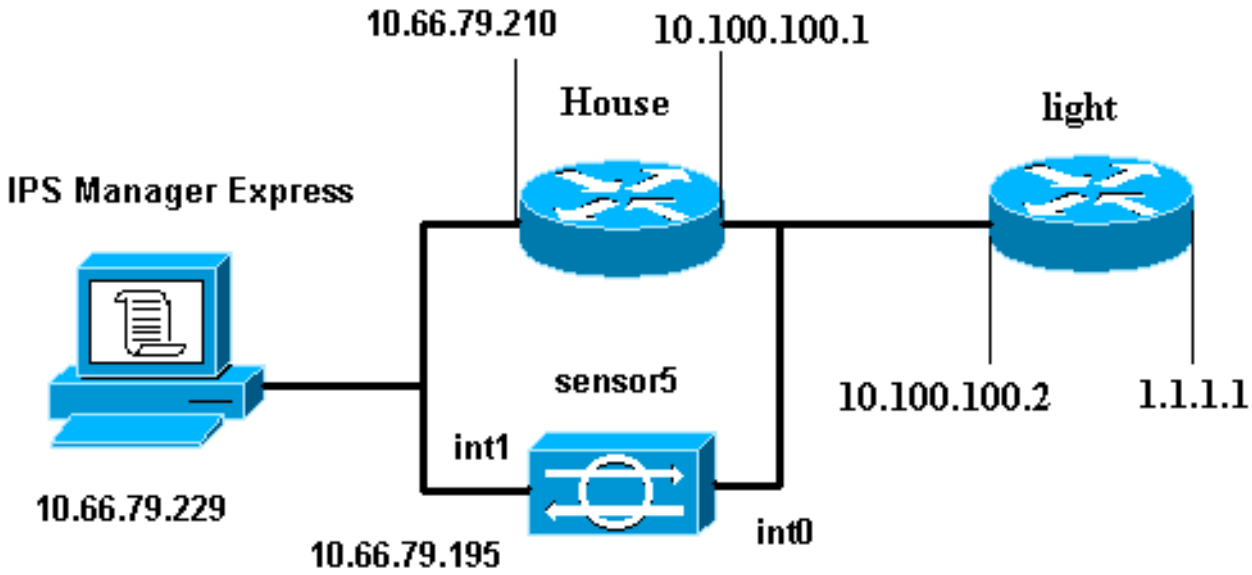
Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Configurazione

Esempio di rete

Nel documento viene usata questa impostazione di rete.



Configurazioni

Nel documento vengono usate queste configurazioni.

- Luce router
- Router House

Luce router
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 House

```
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
```

Avvia la configurazione del sensore

Completare questa procedura per avviare la configurazione del sensore.

1. Al primo accesso al sensore, è necessario immettere **cisco** come nome utente e **cisco** come password.
2. Quando il sistema chiede di cambiare la password.**Nota:** Cisco123 è una parola del dizionario e non è consentita nel sistema.
3. Digitare **setup** e seguire il prompt di sistema per impostare i parametri di base per i sensori.
4. Immettere le informazioni seguenti:

```
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. Salvare la configurazione.Il salvataggio della configurazione da parte del sensore può richiedere alcuni minuti.

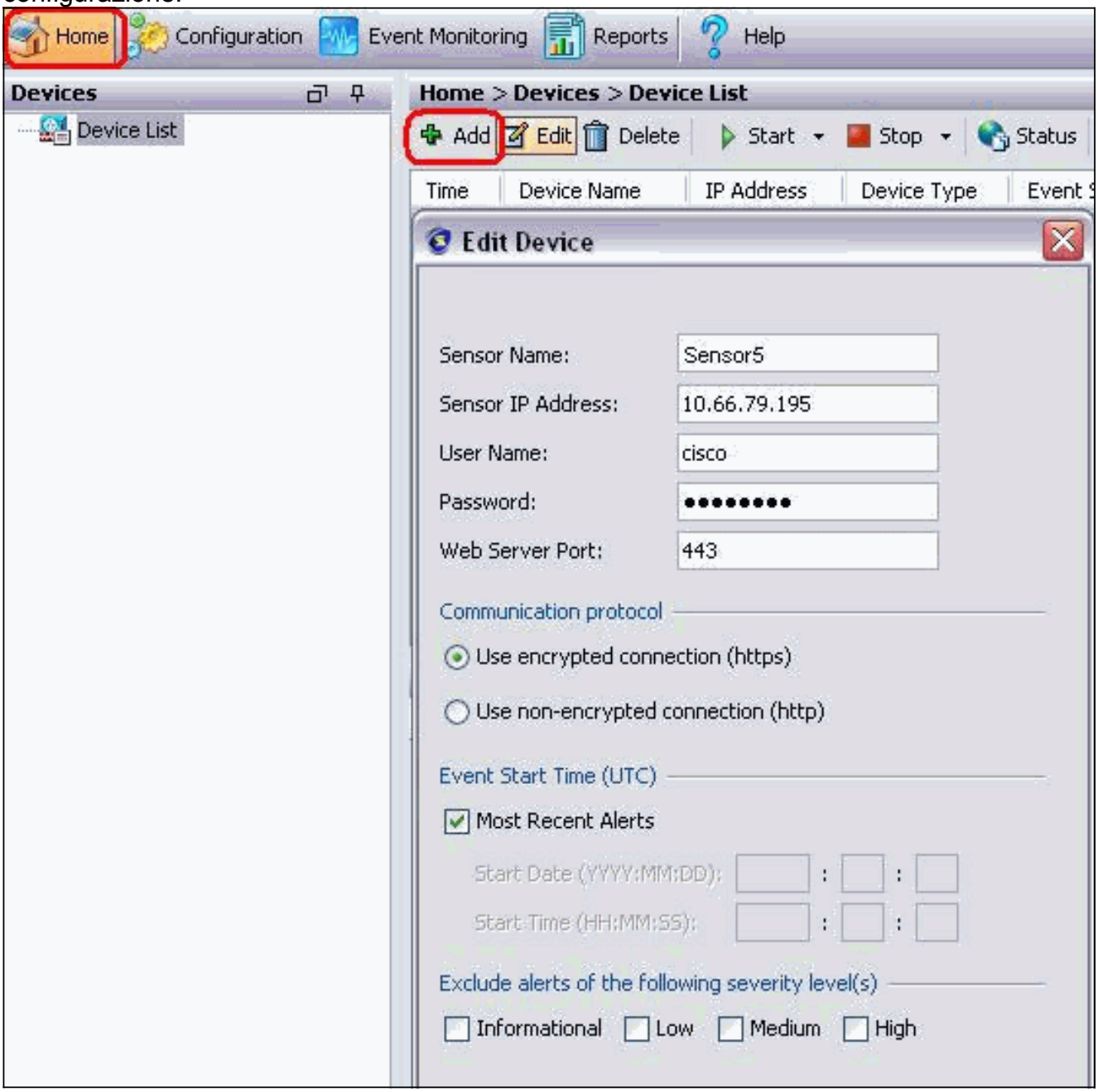
```
[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.

Enter your selection[2]: 2
```

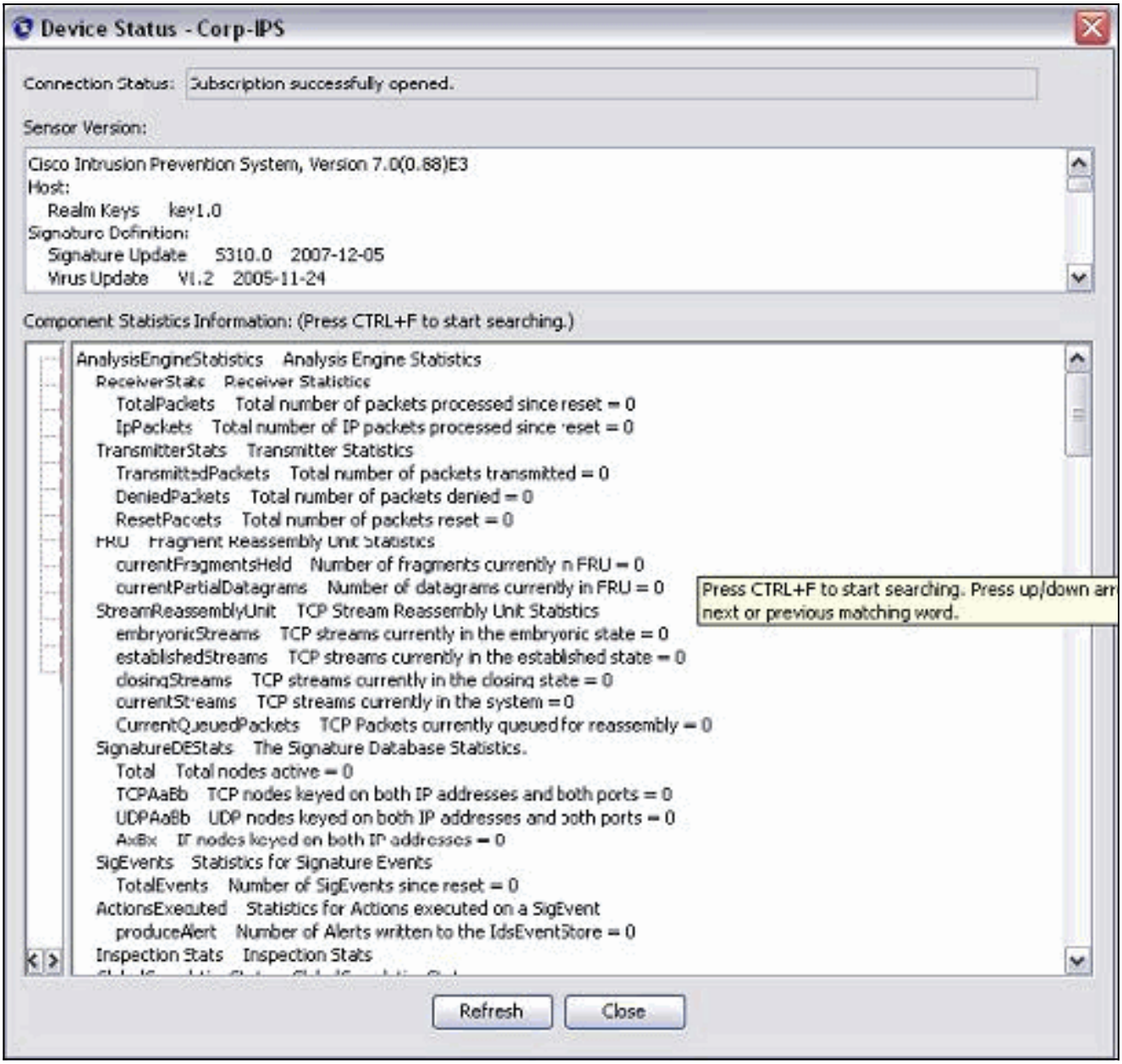
Aggiungere il sensore all'IME

Completare questa procedura per aggiungere il sensore all'IME.

1. Passare al PC Windows, in cui è stato installato IPS Manager Express e aprire **IPS Manager Express**.
2. Scegliete **Home > Aggiungi**.
3. Digitare queste informazioni e fare clic su **OK** per completare la configurazione.



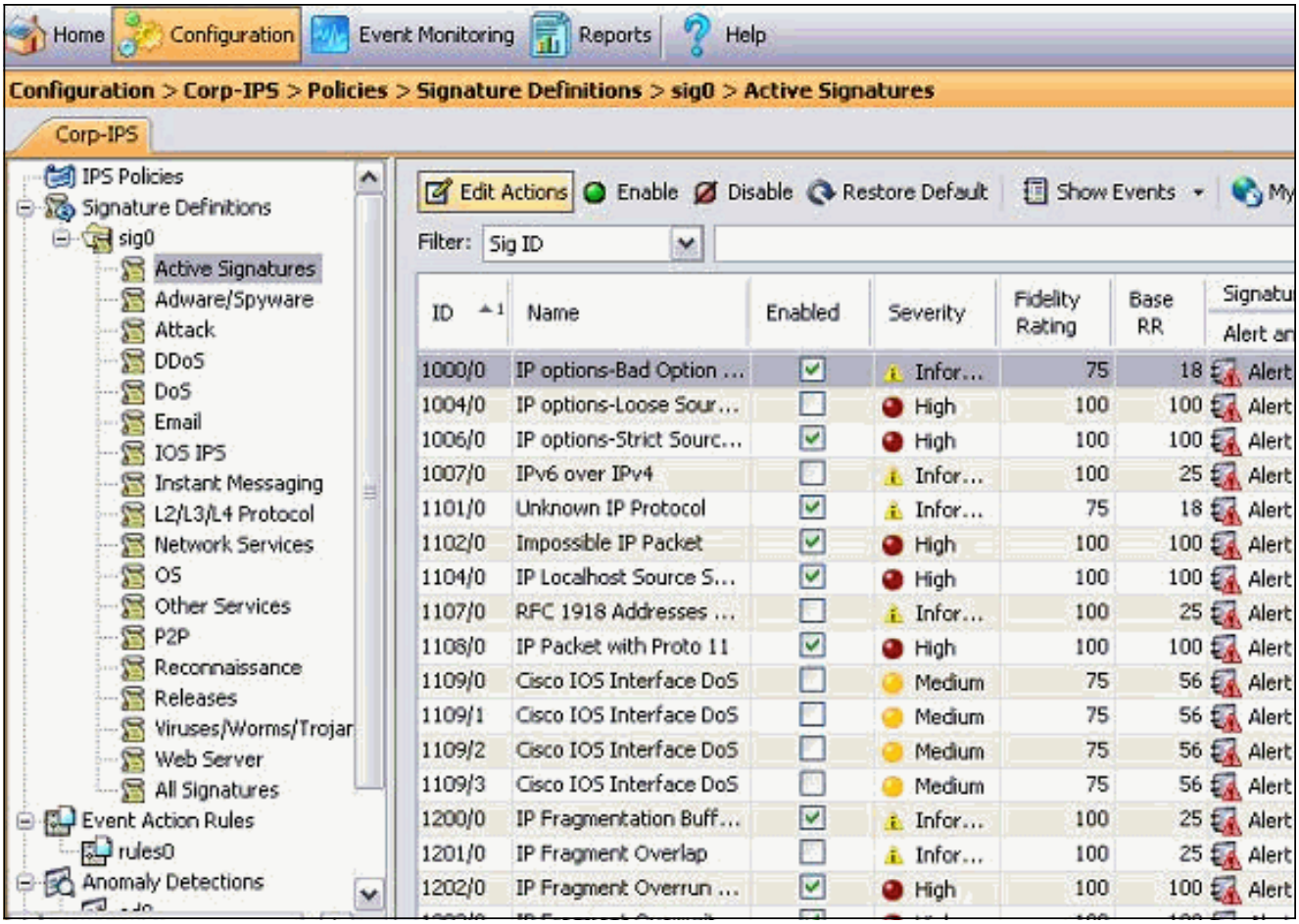
4. Scegliere **Dispositivi > sensore5** per verificare lo stato del sensore, quindi fare clic con il pulsante destro del mouse per scegliere **Stato**.Verificare che la *sottoscrizione sia stata aperta correttamente.*
messaggio.



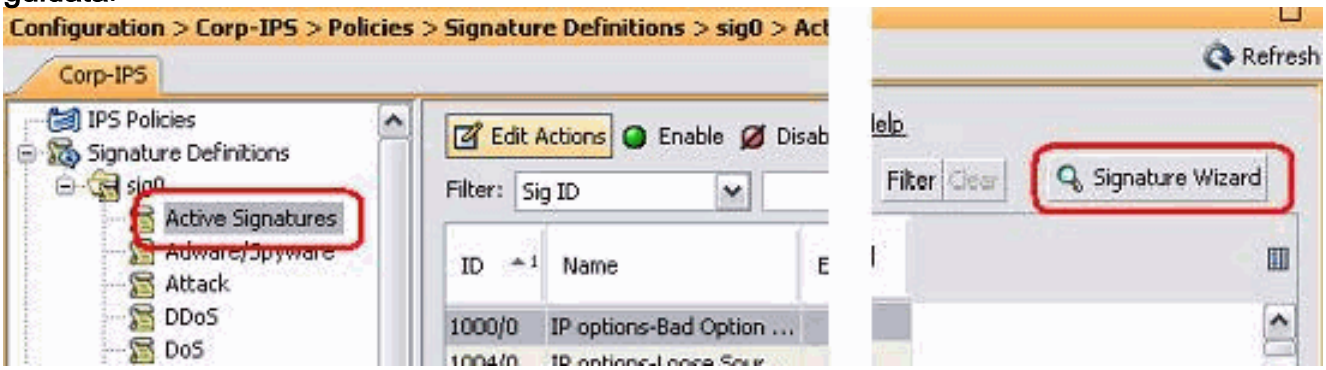
Configurazione del blocco per il router Cisco IOS

Completare questa procedura per configurare il blocco per il router Cisco IOS:.

1. Dal PC IME, aprire il browser Web e visitare il sito **https://10.66.79.195**.
2. Fare clic su **OK** per accettare il certificato HTTPS scaricato dal sensore.
3. Nella finestra Login, immettere **cisco** come nome utente e **123cisco123** come password.Viene visualizzata la seguente interfaccia di gestione IME:

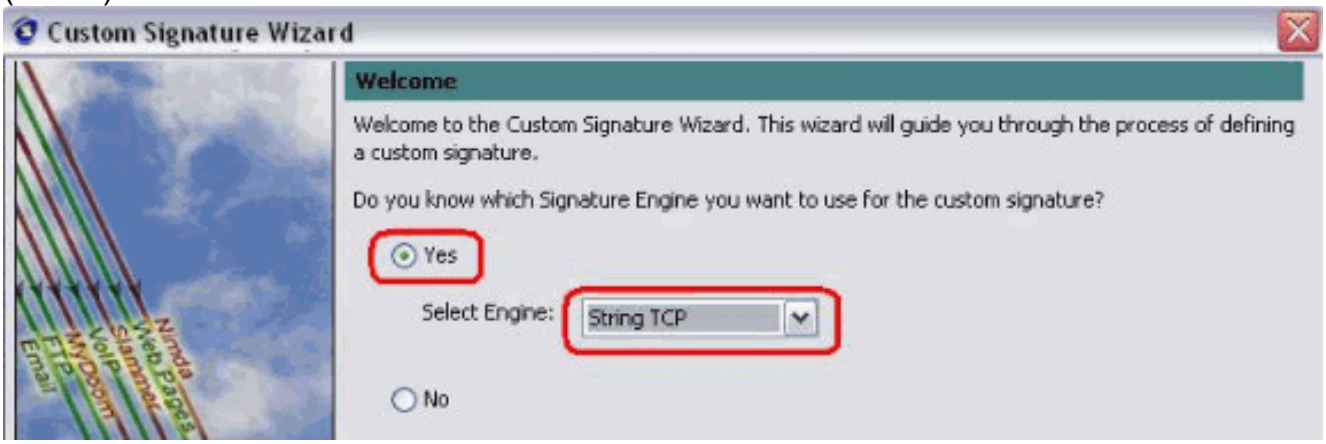


4. Nella scheda Configurazione fare clic su **Firme attive**.
5. Fare quindi clic su **Firma guidata**.



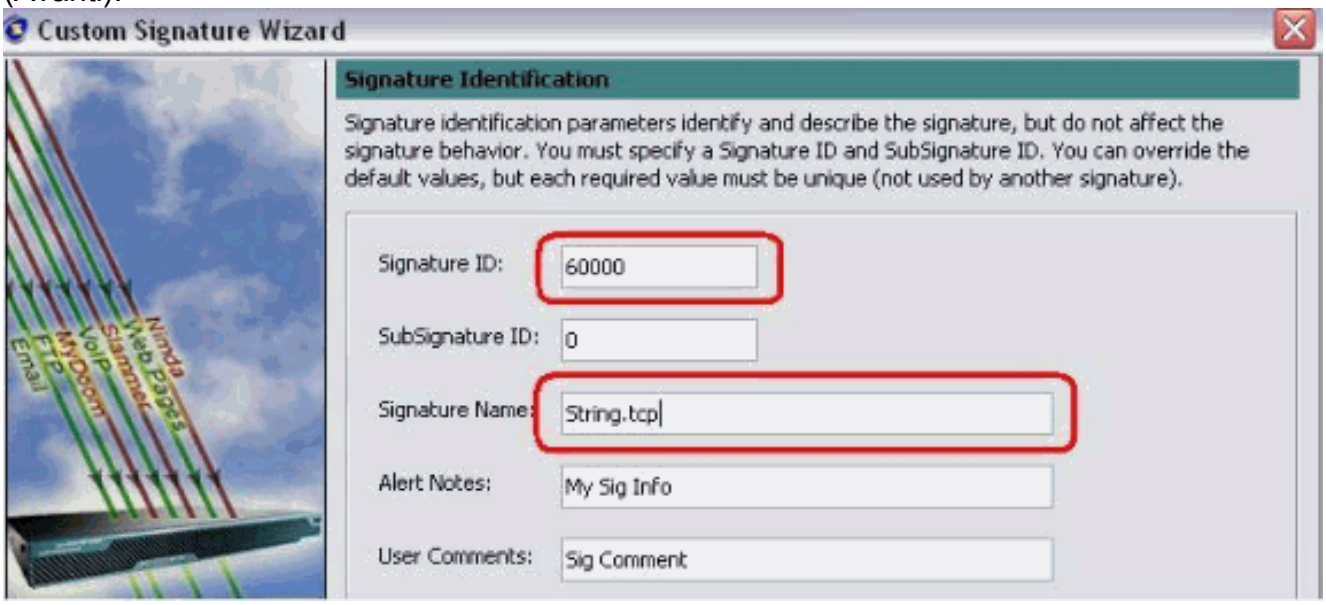
Nota: lo screenshot precedente è stato suddiviso in due parti a causa dei limiti di spazio.

6. Scegliere **Yes** e **String TCP** come motore della firma. Fare clic su **Next** (Avanti).

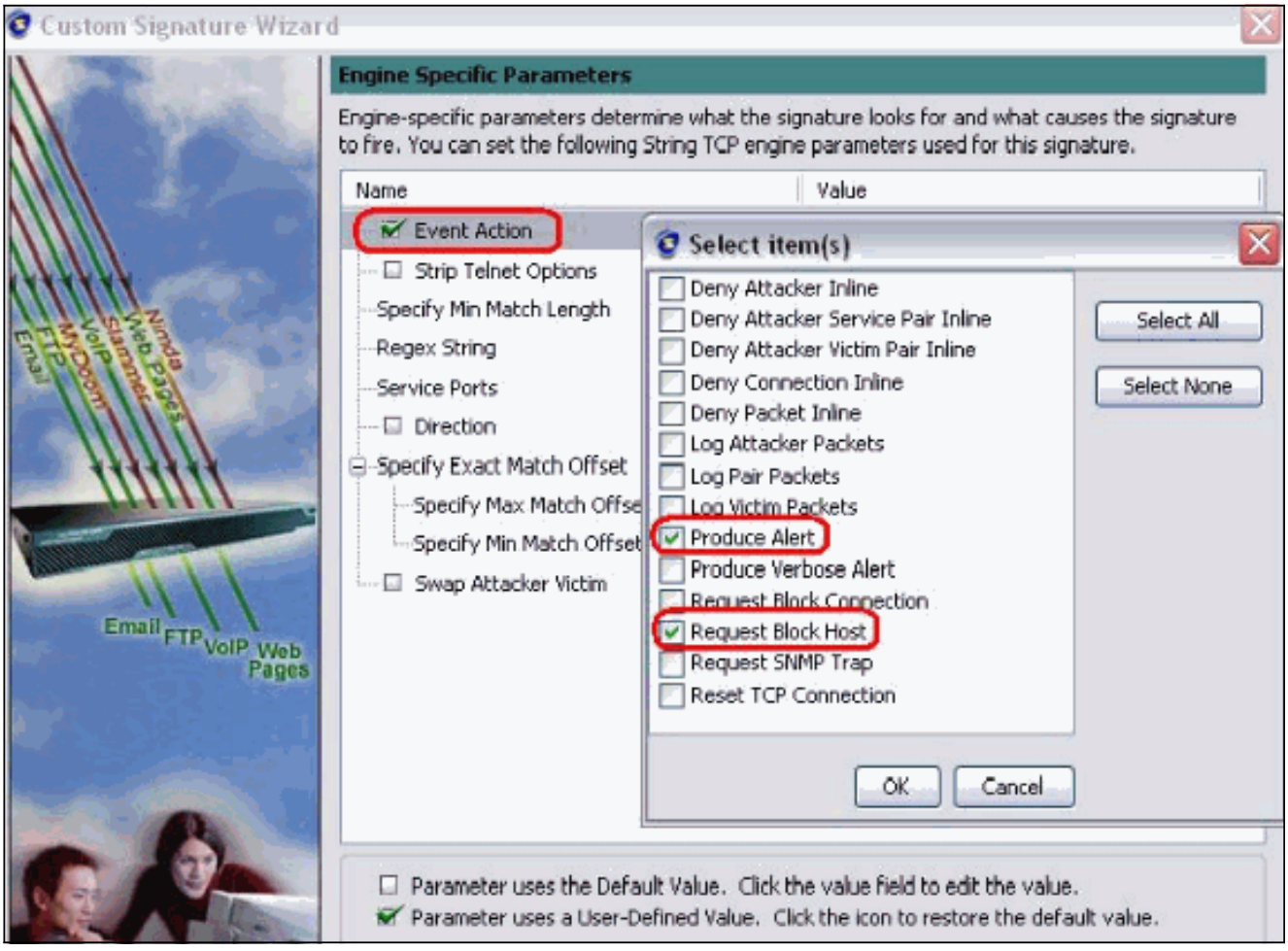


7. Èpossibile lasciare queste informazioni come predefinite oppure immettere il proprio

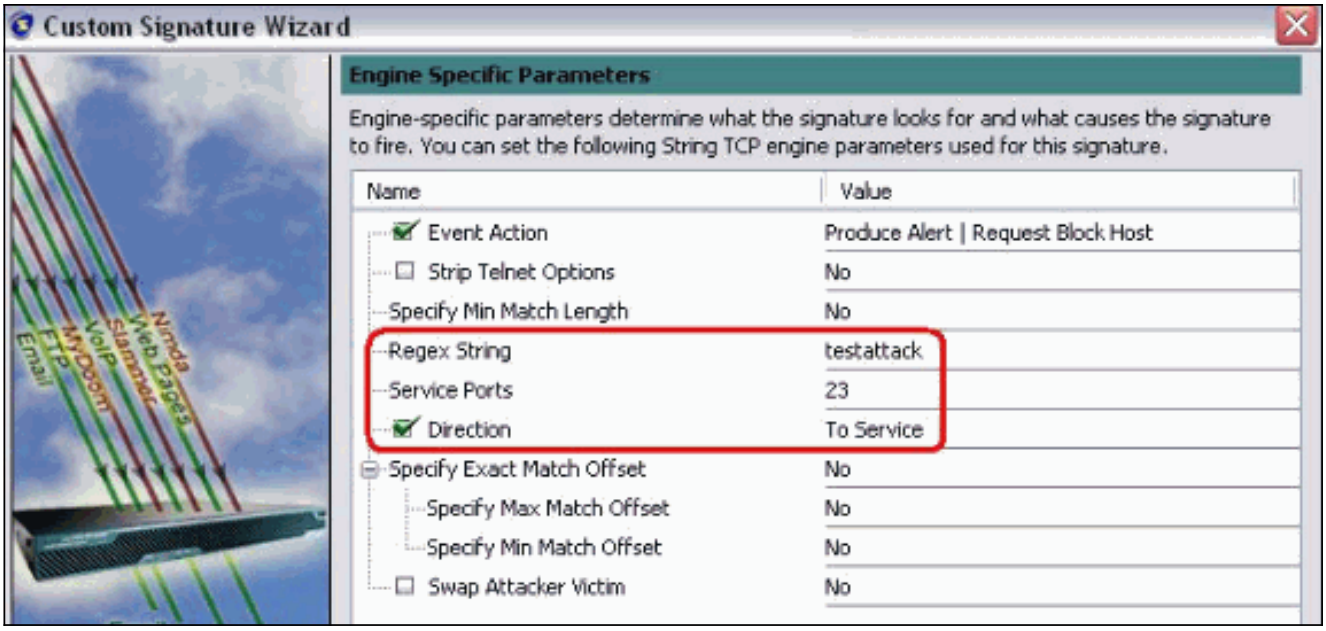
Signature ID, il nome della firma e le note utente. Fare clic su **Next** (Avanti).



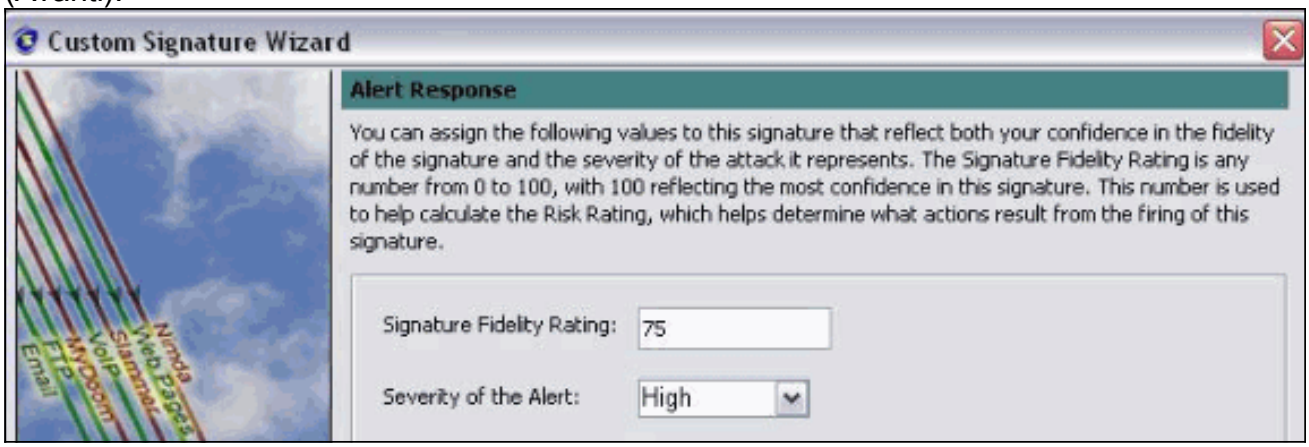
8. Scegliere **Azione evento**, quindi **Genera avviso** e **Host richieste bloccate**. Per continuare, fare clic su **Avanti**.



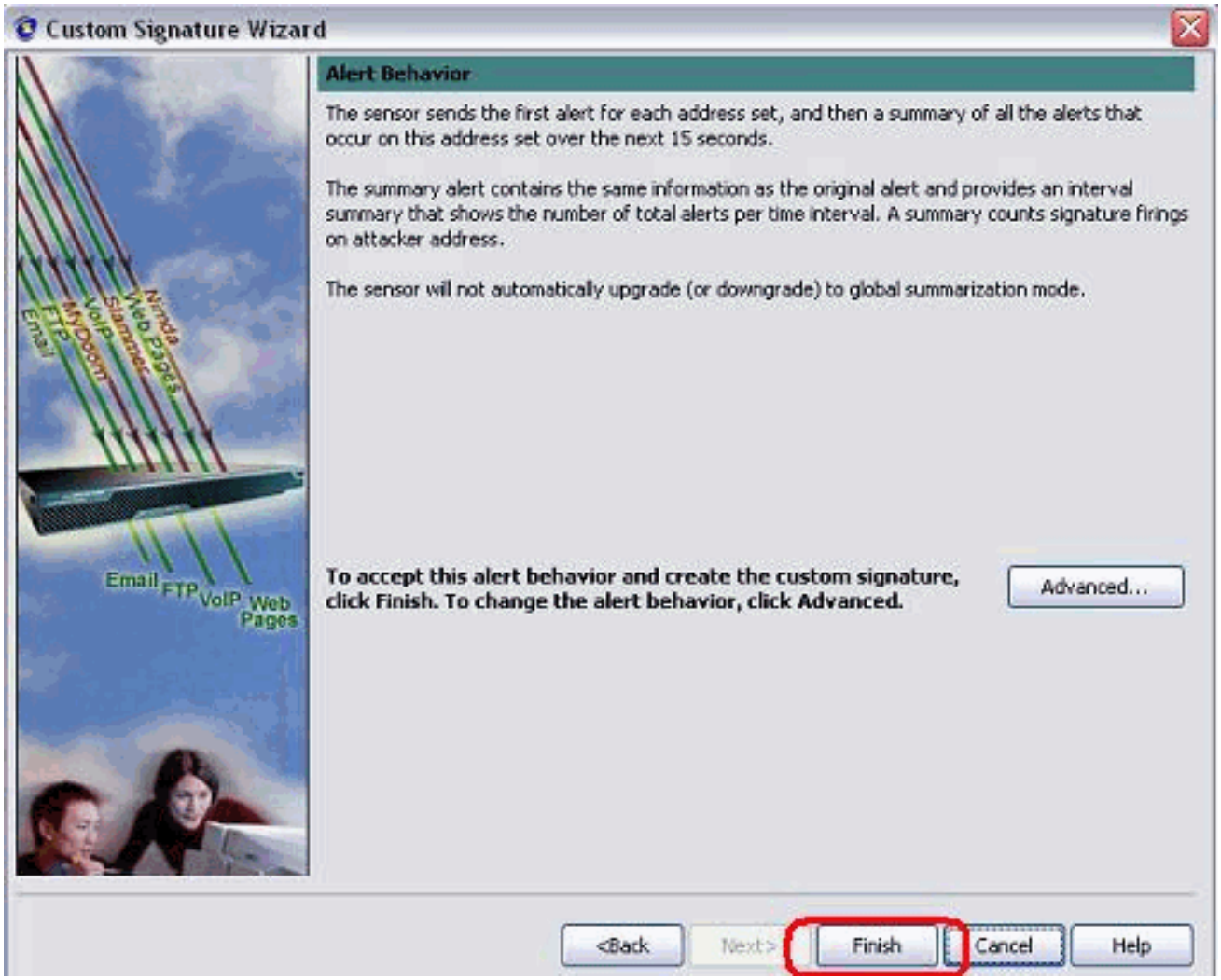
9. Immettere un'espressione regolare , che in questo esempio è *testattack*, immettere **23** per le porte di servizio, scegliere **Al servizio** per la direzione e fare clic su **Avanti** per continuare.



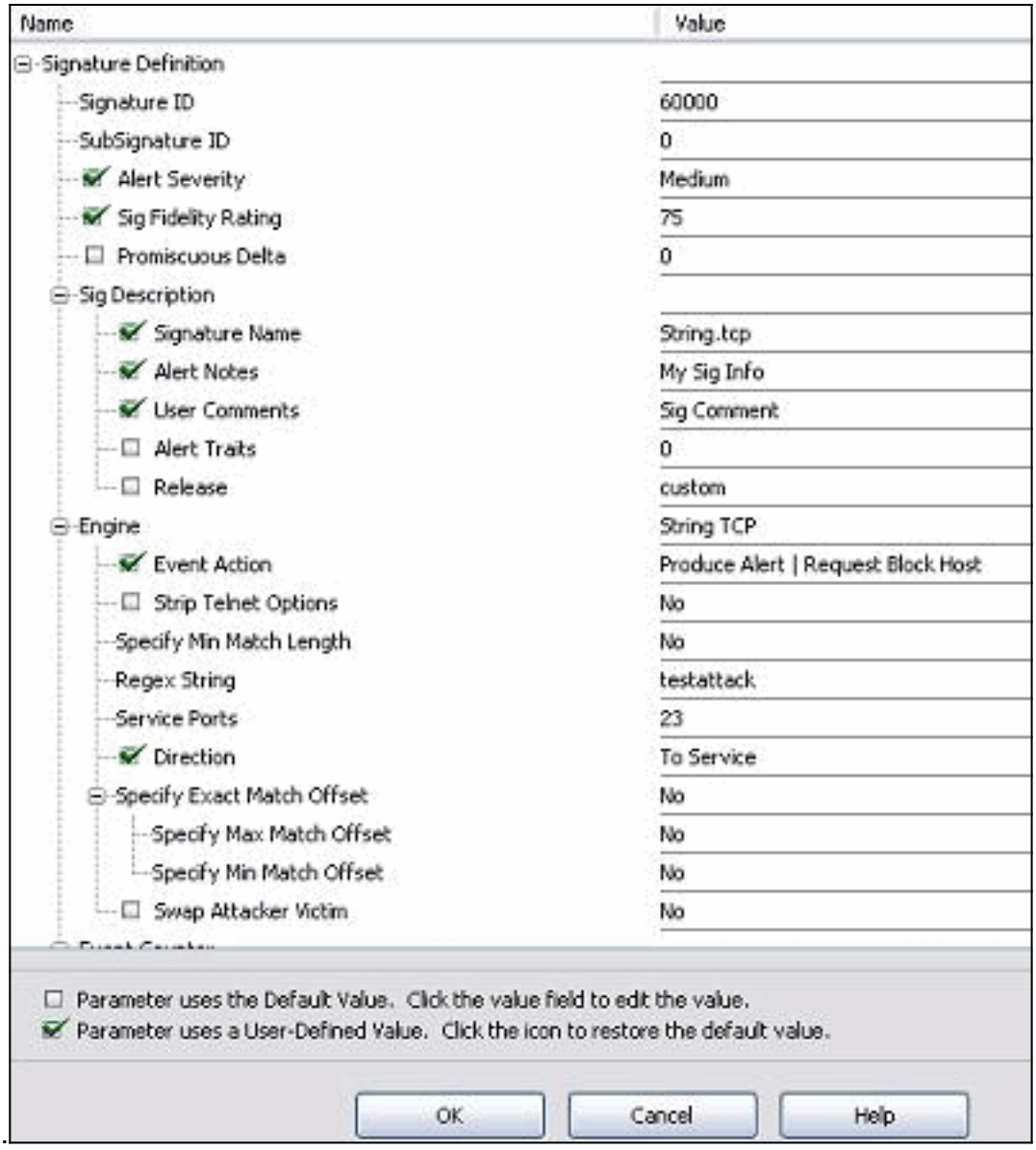
10. Èpossibile lasciare queste informazioni come predefinite. Fare clic su **Next** (Avanti).



11. Per completare la procedura guidata, fare clic su **Fine**.

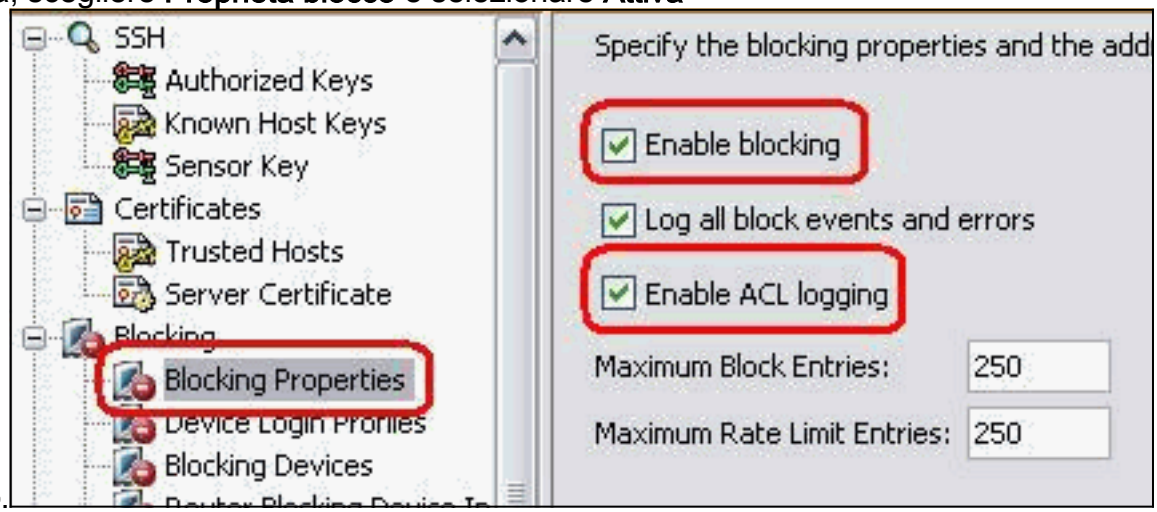


12. Scegliere **Configurazione > sig0 > Firme attive** per individuare la nuova firma creata in base all'**ID** o al **nome del** segno. Per visualizzare la firma, fare clic su



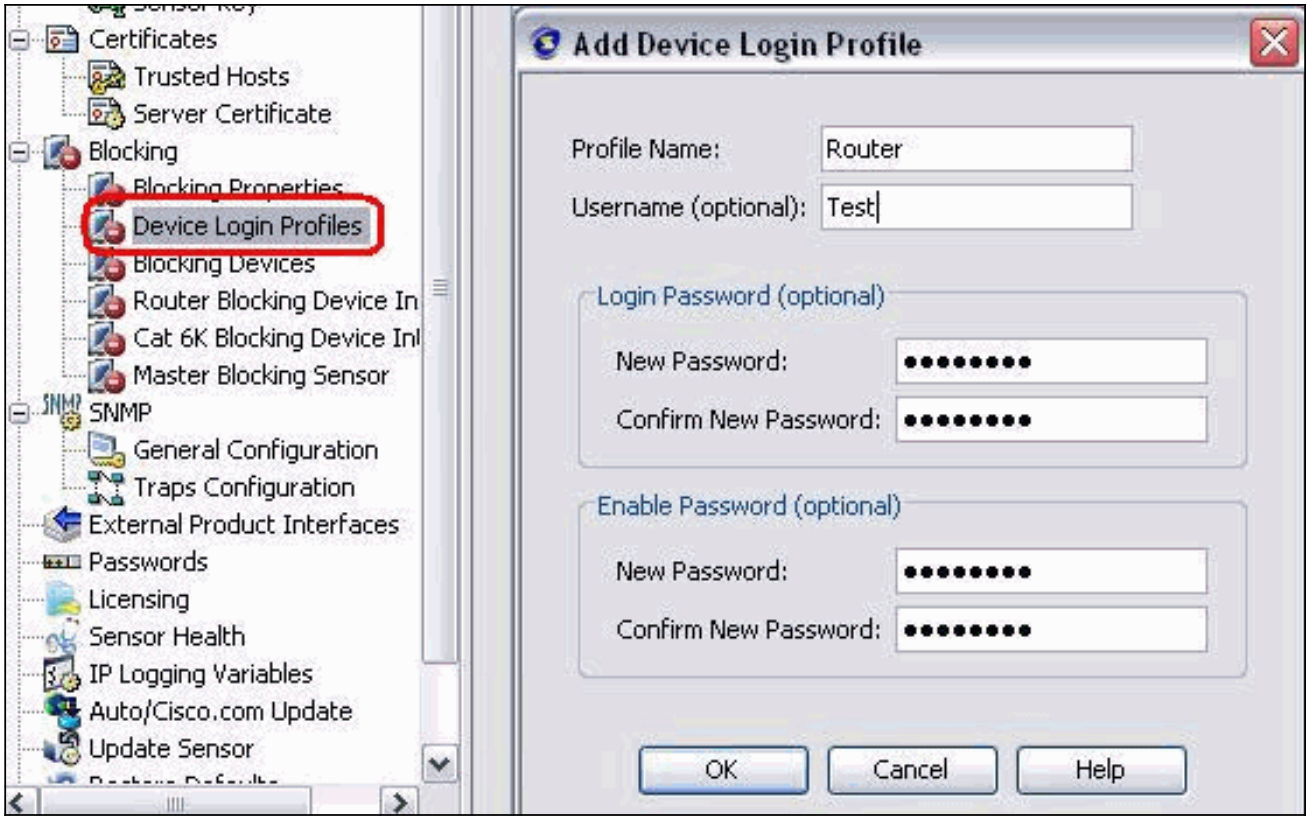
Modifica.

13. Per applicare la firma al sensore, fare clic su **OK** dopo aver confermato e fare clic sul pulsante **Apply** (Applica).
14. Nella scheda Configurazione, in Gestione sensori fare clic su **Blocco**. Nel riquadro di sinistra, scegliere **Proprietà blocco** e selezionare **Attiva**

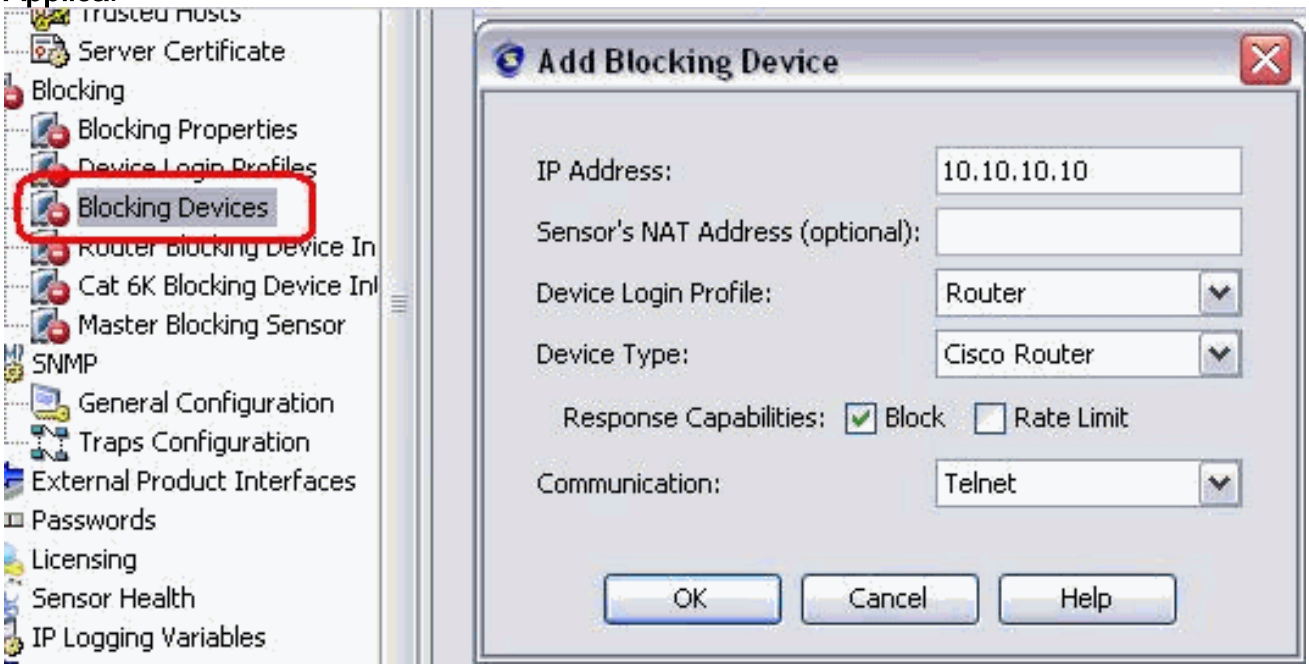


blocco.

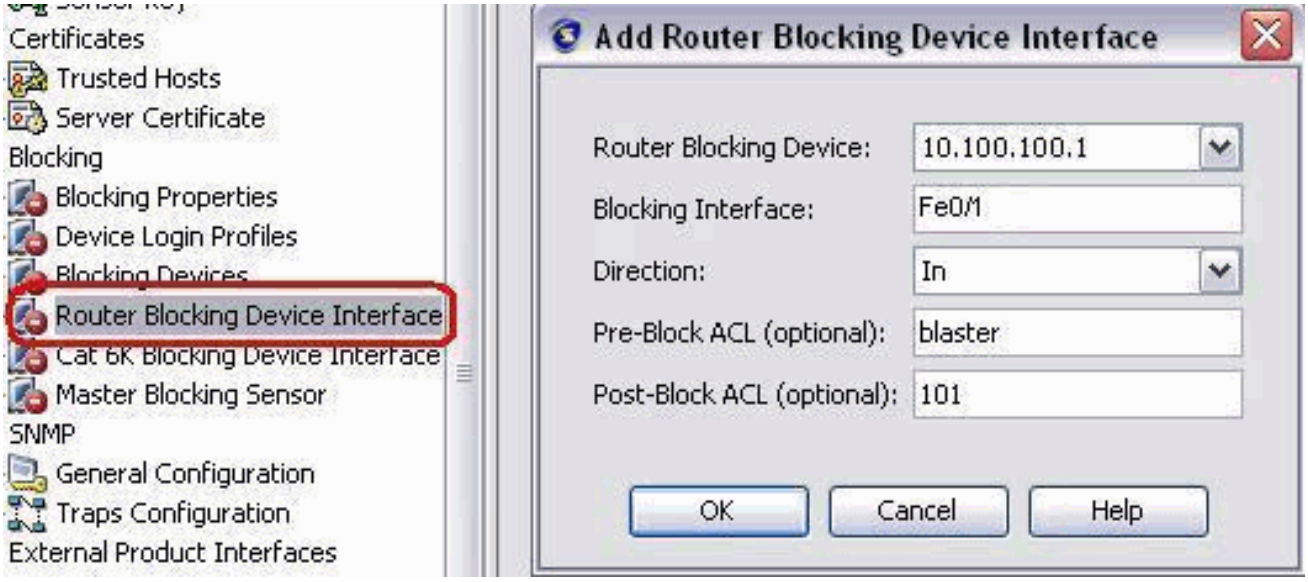
15. Dal riquadro di sinistra, passare al **profilo di accesso al dispositivo**. Per creare un nuovo profilo, fare clic su **Aggiungi**. Una volta creato, fare clic su **OK** e su **Apply** (Applica) per effettuare il rilevamento e
continuare.



16. Il passaggio successivo è configurare il router come dispositivo di blocco. Per aggiungere queste informazioni, dal riquadro di sinistra scegliere **Periferica di blocco**, fare clic su **Aggiungi**. Quindi fare clic su **OK** e su **Applica**.



17. A questo punto, dal riquadro di sinistra configurare le interfacce dei dispositivi di blocco. Aggiungere le informazioni desiderate, quindi fare clic su **OK** e su **Applica**.



Verifica

Lanciare l'attacco e il blocco

Completare questi passaggi per lanciare l'attacco e bloccare:

1. Prima di lanciare l'attacco, andare all'IME, scegliere **Monitoraggio eventi > Vista attacchi scartati** e scegliere il sensore sulla destra.
2. Telnet su Router House e verificare la comunicazione dal server con questi comandi.

```
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. Da Router Light, Telnet a Router House e digitare **testattack**.Premere **<space>** o **<enter>** per ripristinare la sessione Telnet.

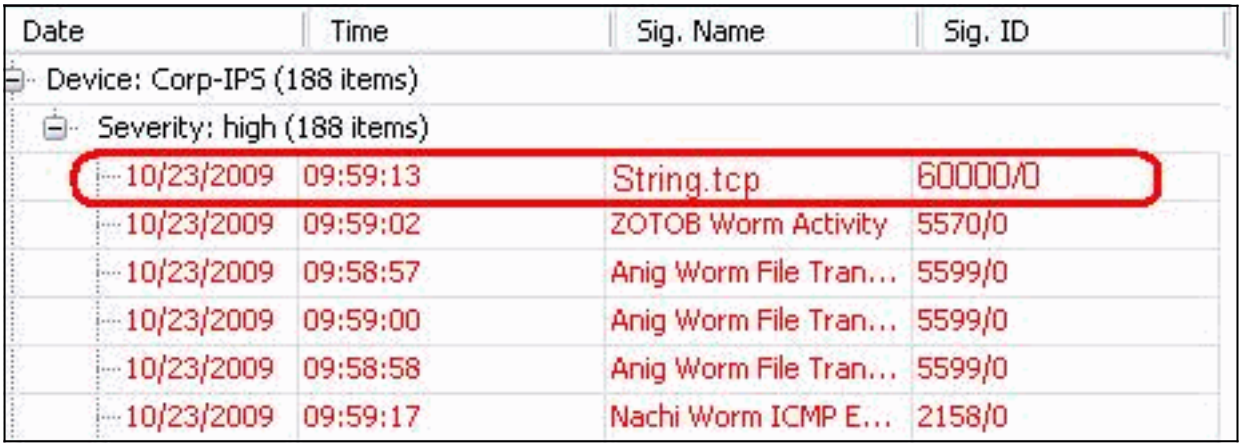
```
light#telnet 10.100.100.1
    Trying 10.100.100.1 ... Open

    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 su Router House e utilizzare il comando **show access-list**, come mostrato di seguito.

```
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. Dal Dashboard del Visualizzatore eventi IDS, viene visualizzato l'allarme rosso una volta avviato l'attacco.



Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Suggerimenti

Suggerimenti per la risoluzione dei problemi:

- Dal sensore, controllare l'output **show statistics network-access** e verificare che `lo stato` sia attivo. Dalla console o dal protocollo SSH al sensore, vengono visualizzate le seguenti informazioni:

```
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#
```

- Verificare che il parametro di comunicazione indichi che viene utilizzato il protocollo corretto, ad esempio Telnet o SSH con 3DES. È possibile provare un'autenticazione SSH o Telnet manuale da un client SSH/Telnet su un PC per verificare che le credenziali di nome utente e

password siano corrette. Quindi, provare a raggiungere il router in modalità Telnet o SSH dal sensore stesso e verificare se è possibile accedere al router correttamente.

Informazioni correlate

- Pagina di supporto per Cisco Secure Intrusion Prevention
- Documentazione e supporto tecnico – Cisco Systems