Configurazione della reimpostazione TCP IPS con l'IME

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Convenzioni
Configurazione
Esempio di rete
Configurazioni
Avvia la configurazione del sensore
Aggiungere il sensore all'IME
Configurare il ripristino TCP per il router Cisco IOS
Verifica
Avvia l'attacco e reimposta TCP
Risoluzione dei problemi
Suggerimenti
Informazioni correlate

Introduzione

In questo documento viene descritta la configurazione del ripristino TCP IPS (Intrusion Prevention System) tramite l'IME (IPS Manager Express). I sensori IME e IPS vengono utilizzati per gestire un router Cisco per il reset TCP. Quando si esamina la configurazione, tenere presente quanto segue:

- 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.

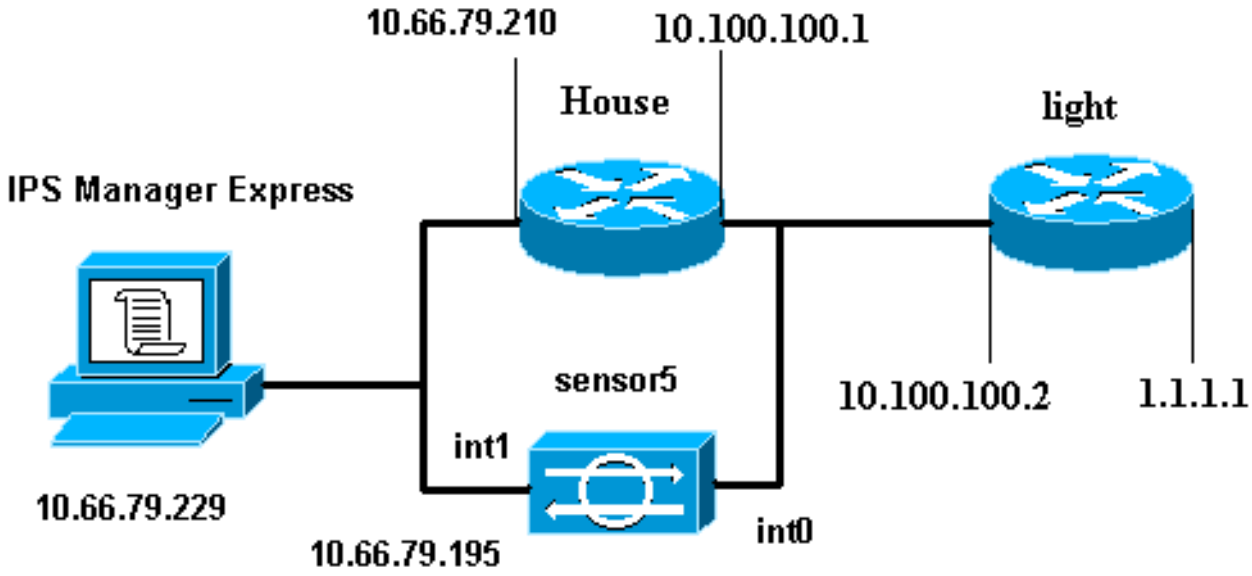
Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Configurazione

Esempio di rete

Nel documento viene usata l'impostazione di rete mostrata nel diagramma.



Configurazioni

Nel documento vengono usate le configurazioni mostrate di seguito.

- 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
 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
```

Avvia la configurazione del sensore

Completare questa procedura per avviare la configurazione del sensore.

1. Se è la prima volta che si accede 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 completare 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 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. Salvare la configurazione.Il salvataggio della configurazione da parte del sensore può

richiedere alcuni minuti.

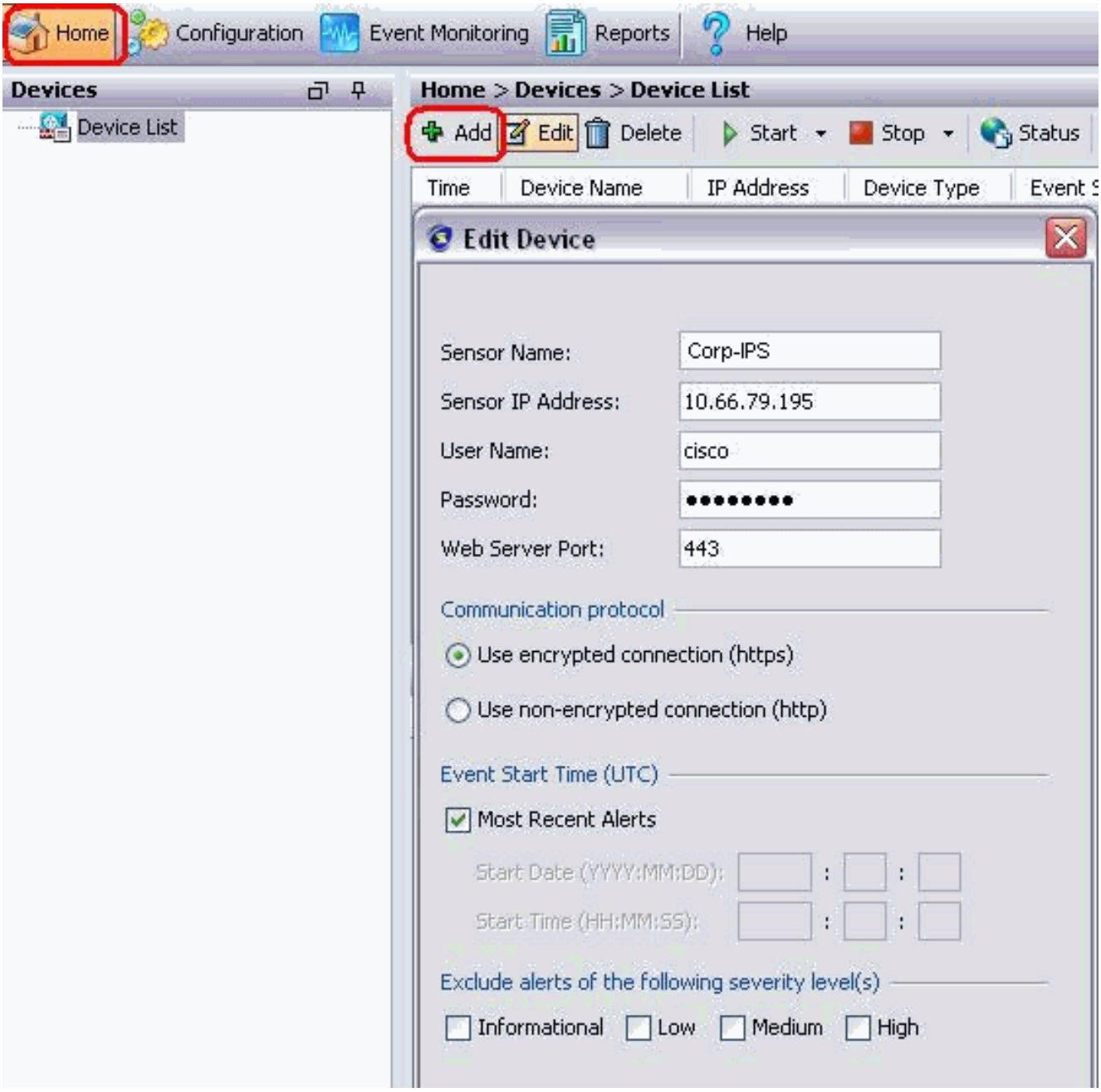
```
[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.

Enter your selection[2]: 2
```

Aggiungere il sensore all'IME

Completare questa procedura per aggiungere il sensore all'IME:

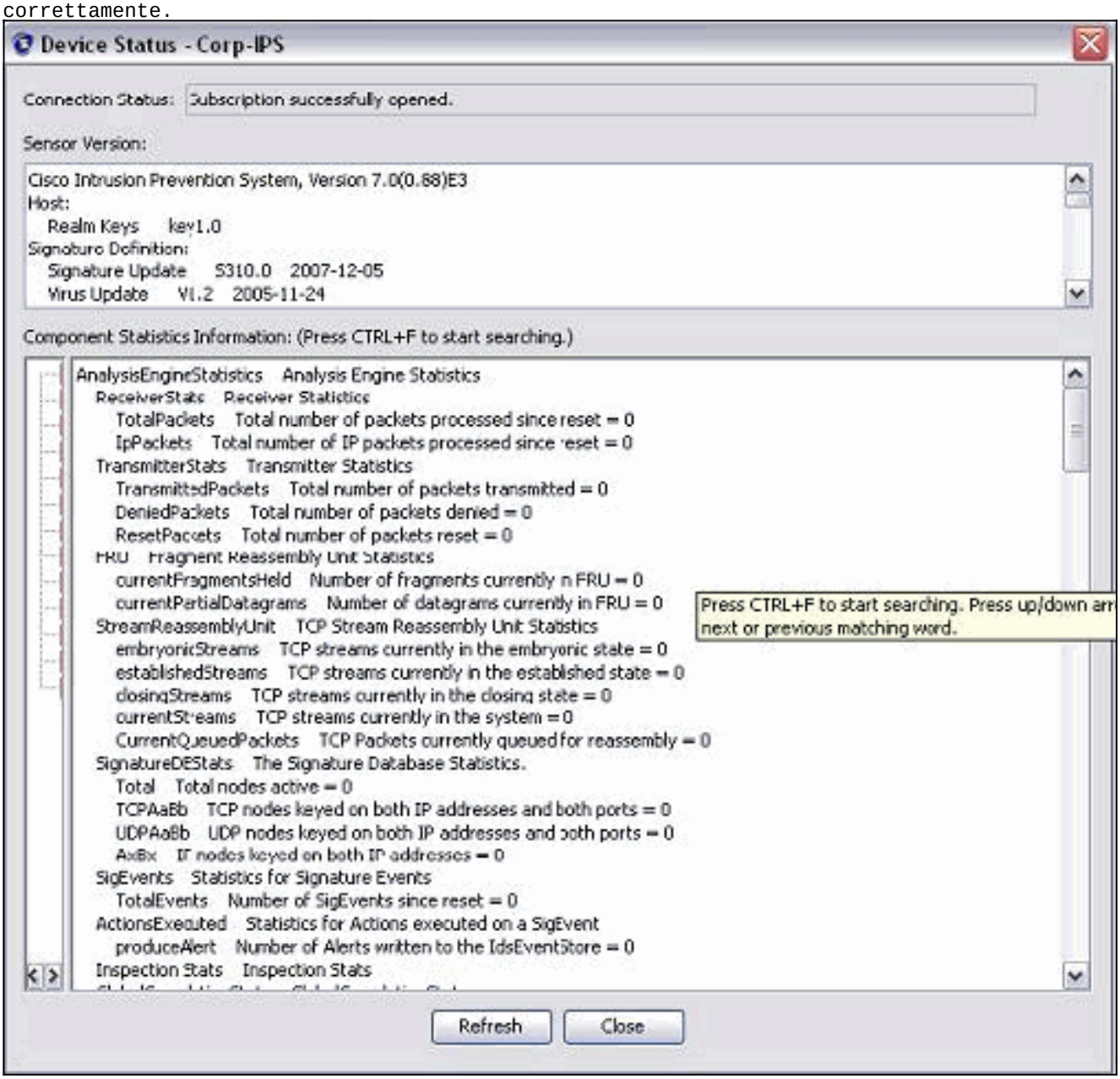
1. Accedere al PC Windows in cui è installato IPS Manager Express e aprire IPS Manager Express.
2. Scegliete **Home > Aggiungi**

.



3. Digitare queste informazioni e fare clic su **OK** per completare la configurazione.
4. Scegliere **Devices > Corp-IPS** per verificare lo stato del sensore, quindi fare clic con il pulsante destro del mouse per scegliere **Device Status** (Stato dispositivo).Verificare che la

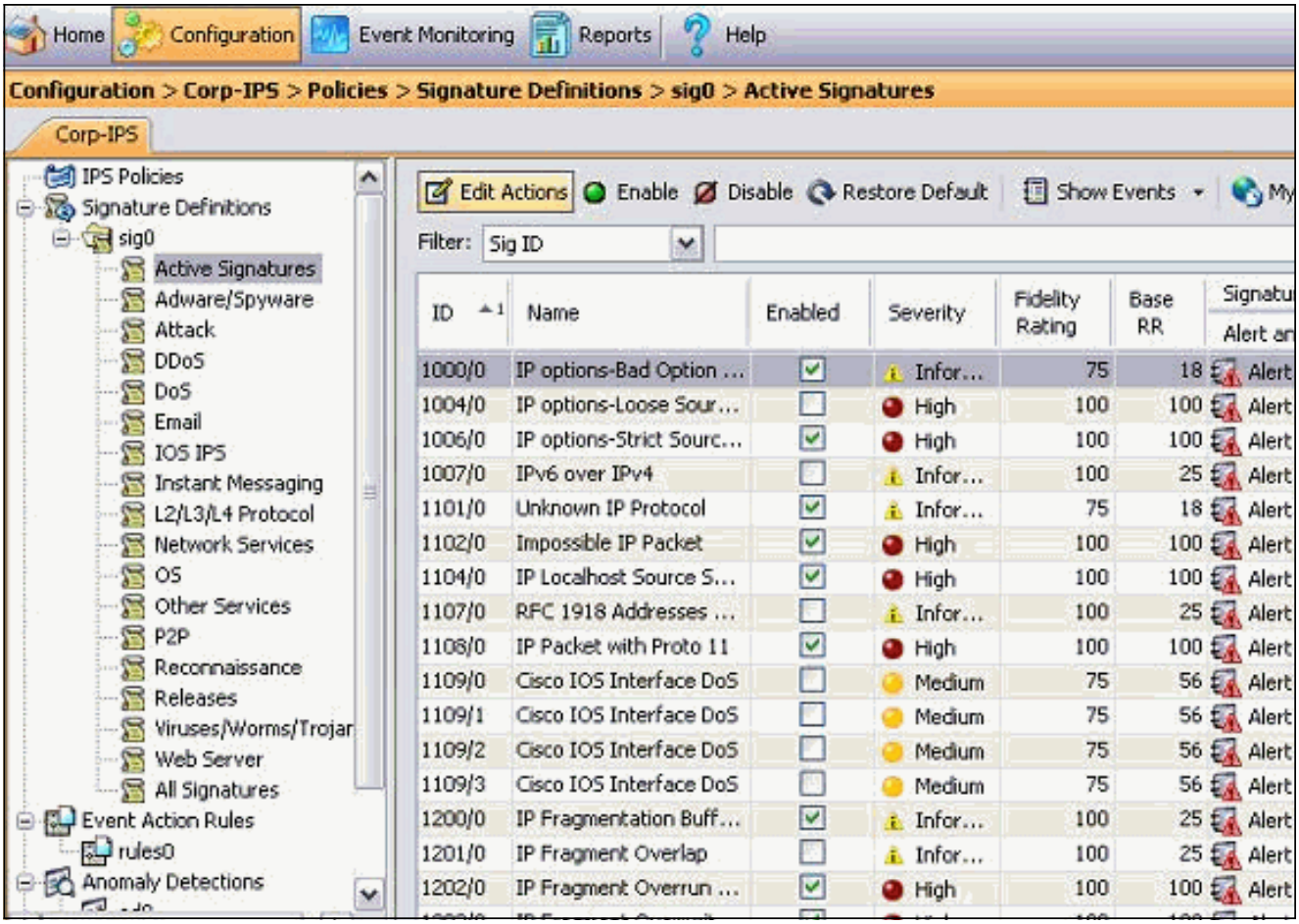
sottoscrizione sia stata aperta correttamente.



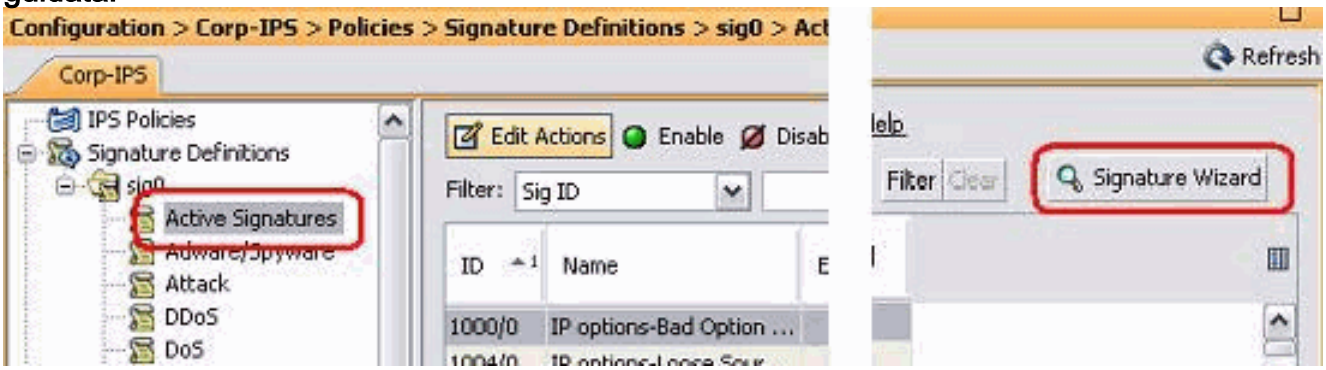
Configurare il ripristino TCP per il router Cisco IOS

Completare questa procedura per configurare il ripristino TCP per il router Cisco IOS:

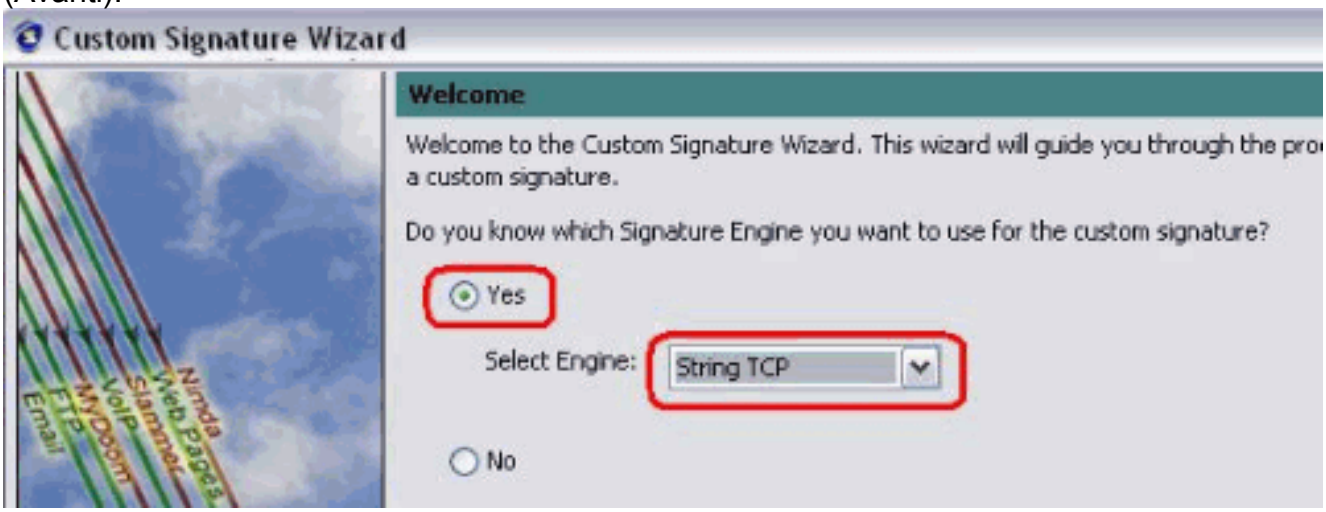
1. Dal PC IME, aprire il browser Web e visitare il sito **https://10.66.79.195**.
2. Fare clic su **OK** per accettare il certificato HTTPS scaricato dal sensore.
3. Nella finestra di accesso, immettere **cisco** come nome utente e **123cisco123** come password.Viene visualizzata la seguente interfaccia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



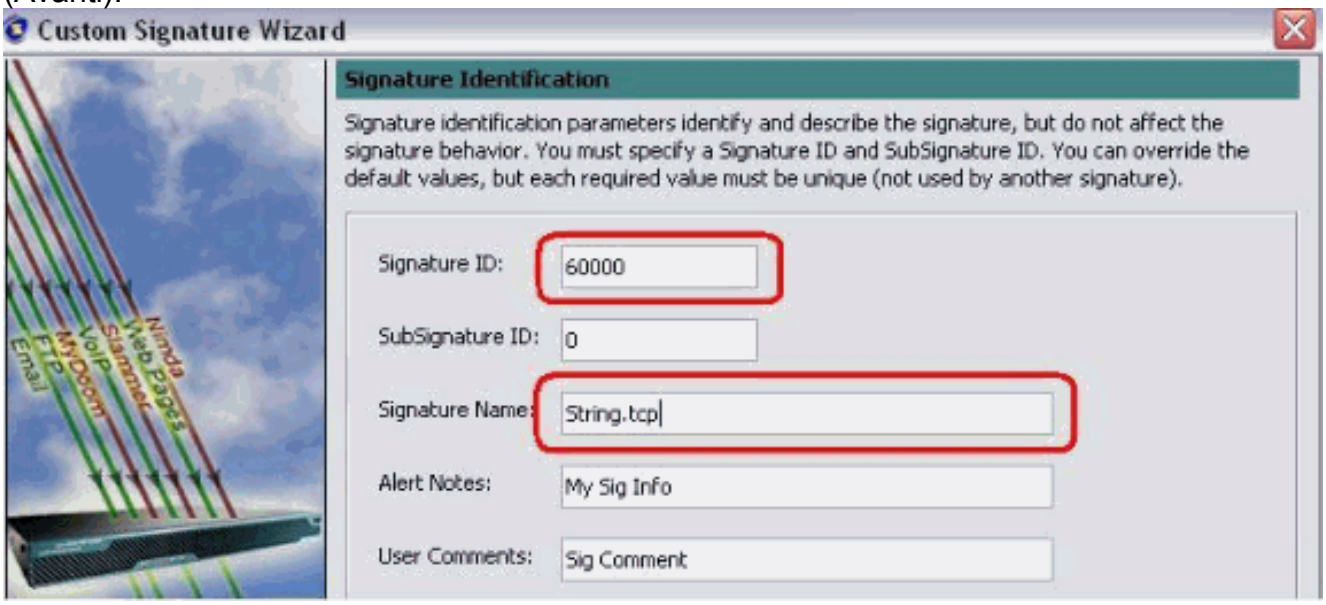
4. Nella scheda Configurazione fare clic su **Firme attive**.
5. Fare quindi clic su **Firma guidata.**



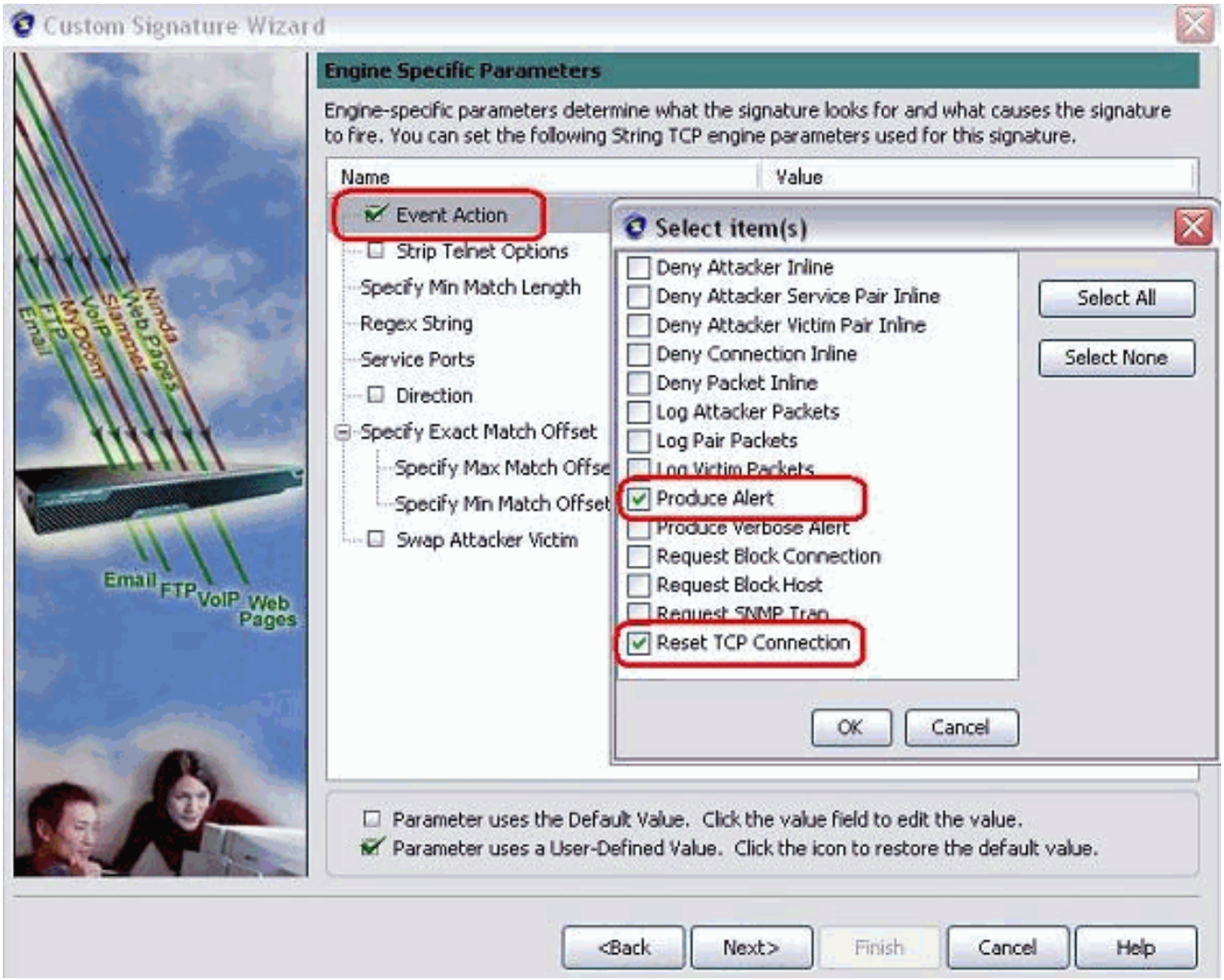
6. Nella procedura guidata scegliere **Sì** e **Stringa TCP** come motore firma. Fare clic su **Next** (Avanti).



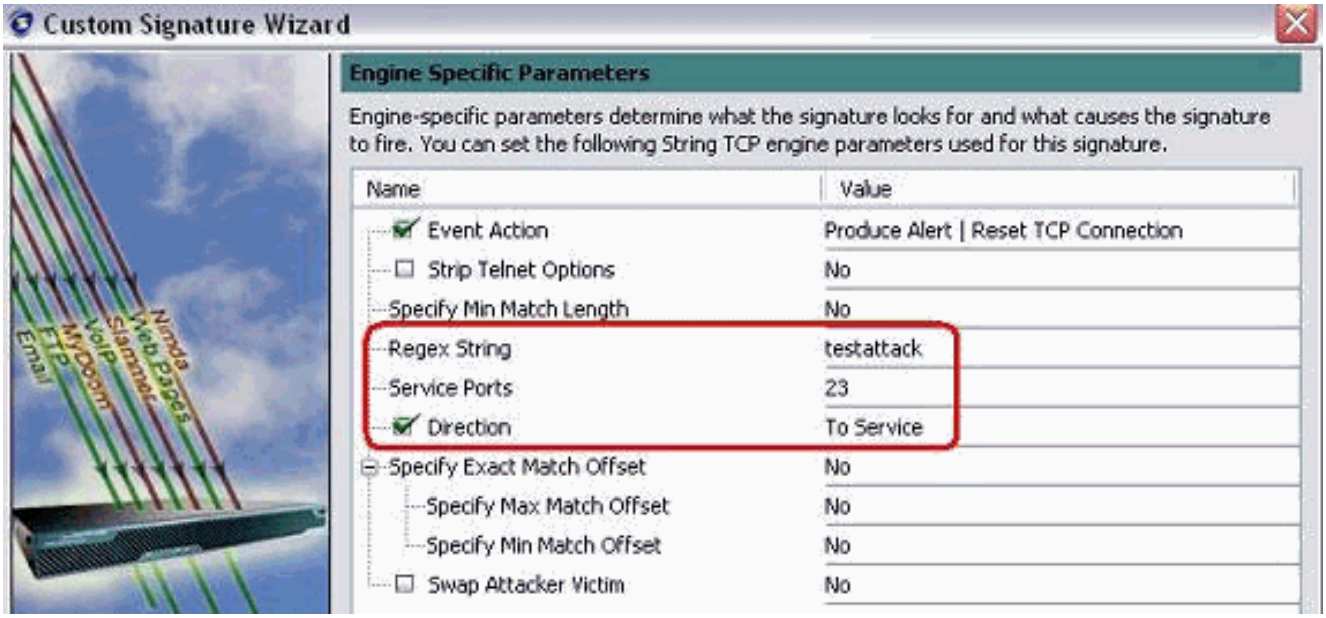
7. Èpossibile lasciare queste informazioni predefinite oppure immettere il proprio Signature ID, il nome della firma e le note utente. Fare clic su **Next** (Avanti).



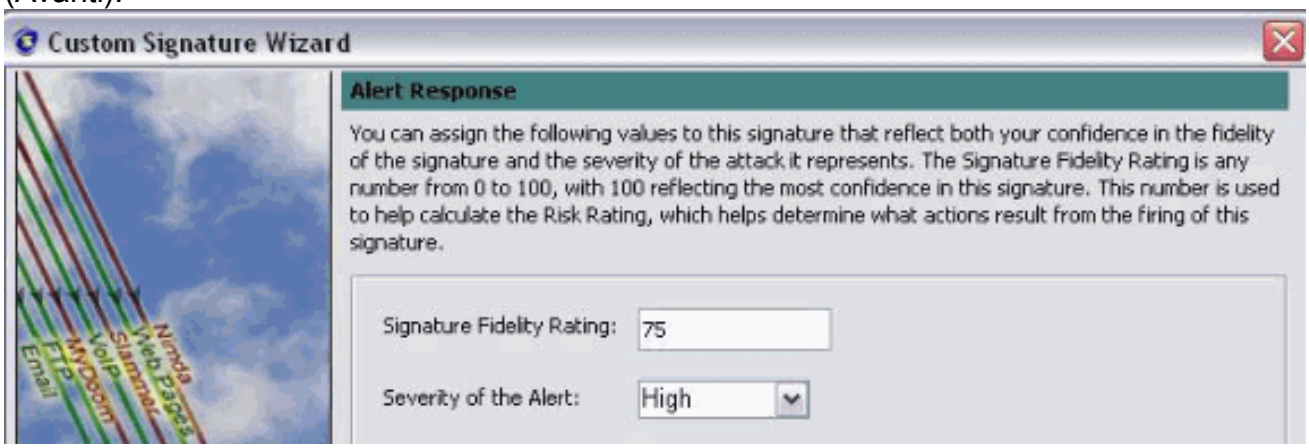
8. Scegliere **Azione evento**, quindi **Genera avviso** e **Reimposta connessione TCP**. Per continuare, fare clic su **OK** e quindi su **Avanti**.



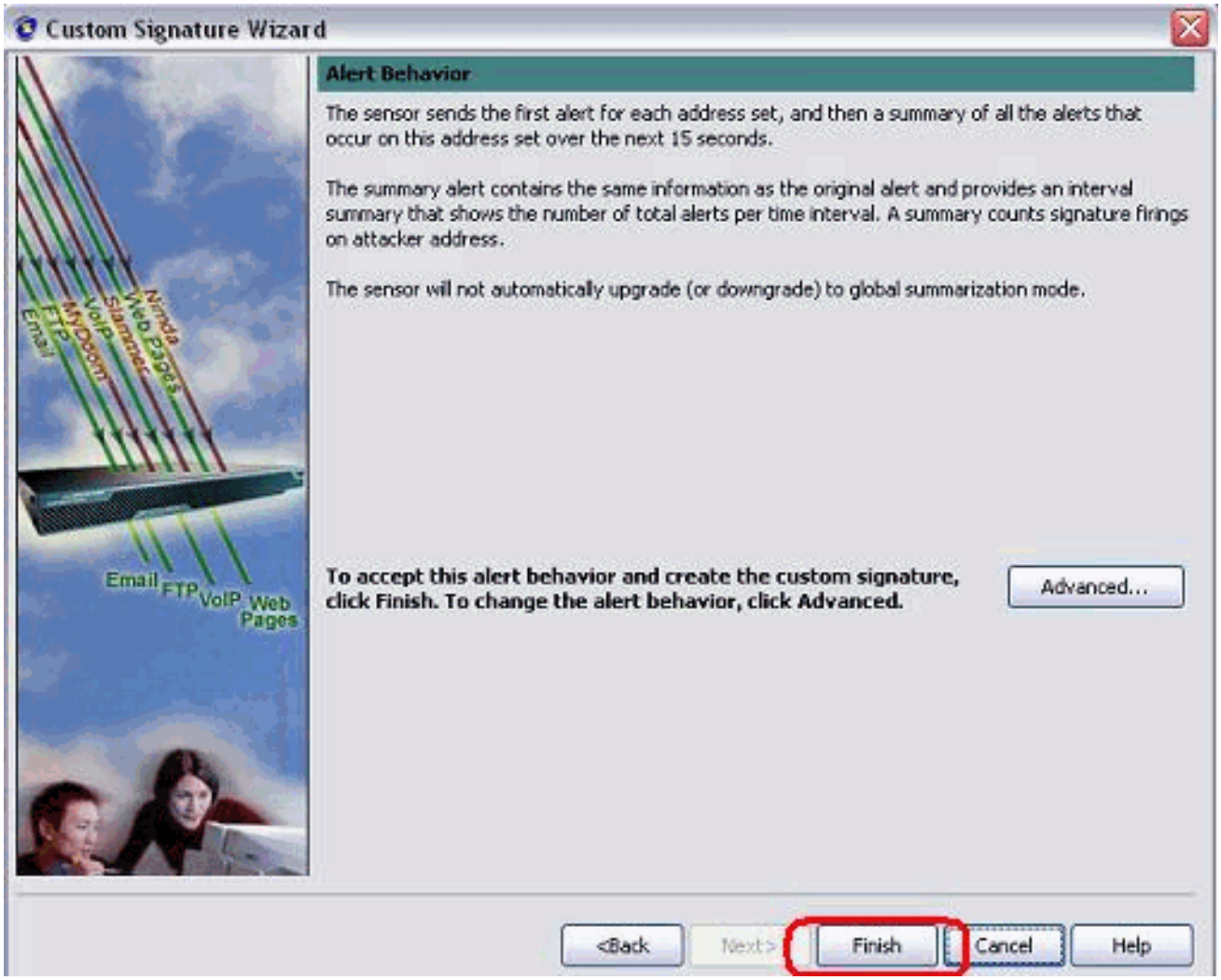
9. Immettere un'espressione regolare. Nell'esempio viene utilizzato `testattack`. Immettere **23** per le porte di servizio, scegliere **Da servire** per la direzione e fare clic su **Avanti** per continuare.



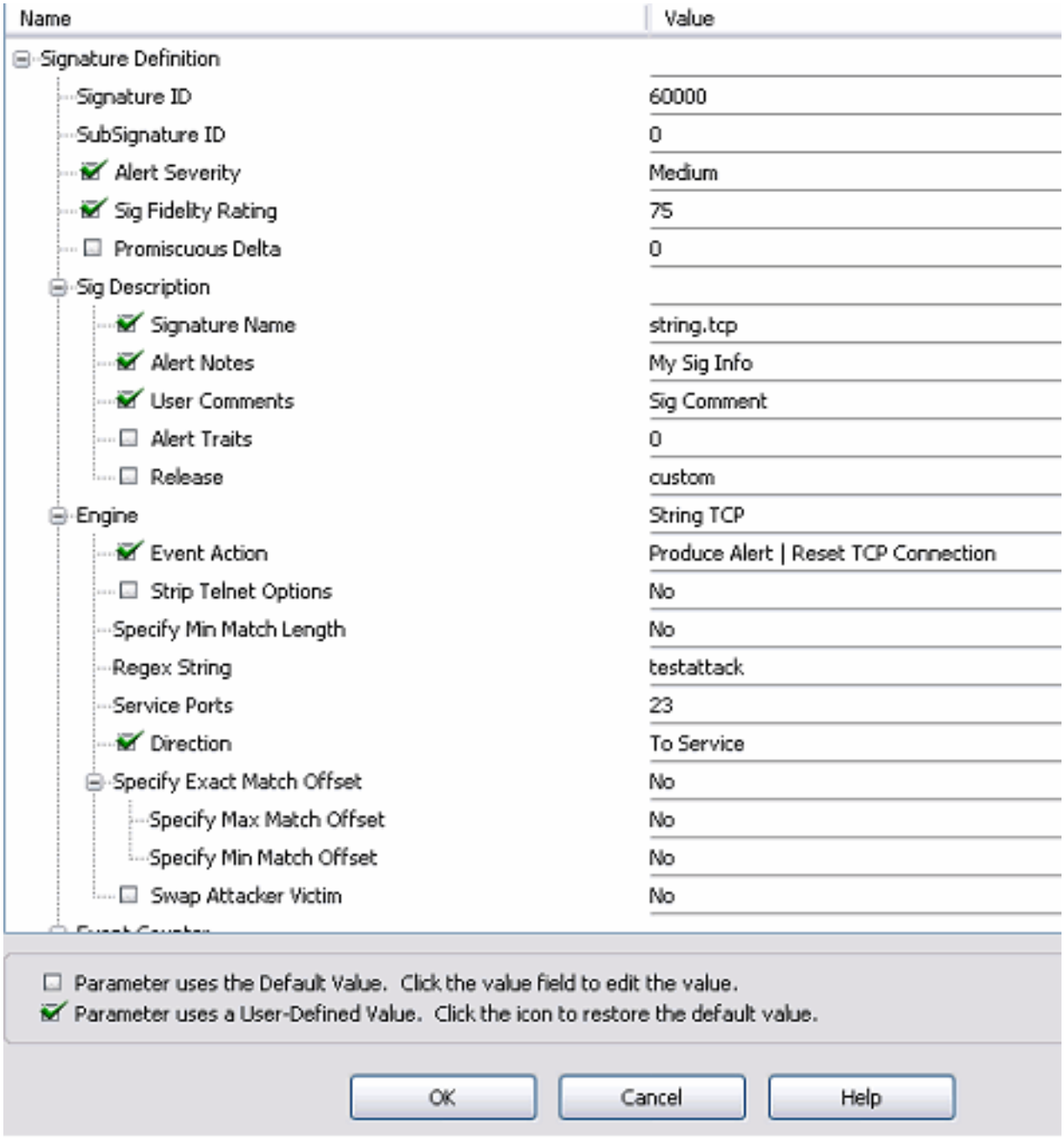
10. Èpossibile lasciare queste informazioni come predefinite. Fare clic su **Next** (Avanti).



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



12. Scegliere **Configurazione > sig0 > Firme attive** per individuare la nuova firma creata con il **Signature ID** o il **Nome del Signature**. 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).

Verifica

Avvia l'attacco e reimposta TCP

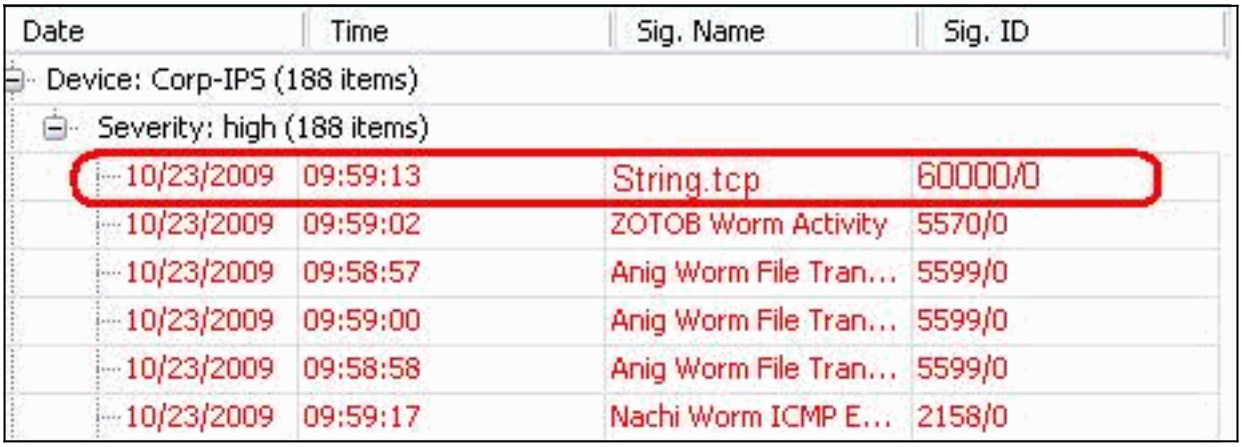
Completare questi passaggi per avviare l'attacco e il Reset TCP:

1. Prima di lanciare l'attacco, andare all'**IME**, scegliere **Monitoraggio eventi > Vista attacchi scartati** e scegliere il sensore sulla destra.
2. Dalla spia del router, passare da Telnet a Router House e iniziare il **test di attacco**.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 closed by foreign host]
!--- Telnet session has been reset due to the !--- signature "String.tcp" triggered.
```

3. Dal Dashboard del Visualizzatore eventi IPS, l'Allarme rosso viene visualizzato 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:

- Lo shun esce dalla porta di comando e di controllo per riprogrammare gli elenchi di controllo di accesso (ACL) del router. I Reset TCP vengono inviati dall'**interfaccia** di **sniffing** del sensore. Quando si **imposta lo span** nello switch, usare il comando **set span <src_mod/src_port><dest_mod/dest_port>** con entrambi i pacchetti in arrivo abilitati, come mostrato di seguito.

```
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
```

- Se il Reset TCP funziona, verificare se l'allarme viene attivato per il tipo di azione Reset TCP. Se viene visualizzato l'avviso, verificare che il tipo di firma sia impostato su TCP reset.Effettuare l'accesso utilizzando l'account del servizio su per eseguire la radice ed

eseguire questo comando. Questo comando presuppone che l'interfaccia di rilevamento sia impostata su eth0.

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

Nota: un centinaio di reimpostazioni tcp vengono inviate alla vittima/al destinatario, quindi un centinaio vengono inviate all'aggressore/al cliente.Questo è l'output di esempio:

```
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
```

Informazioni correlate

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