Configuración de IPS TCP Reset Usando IME

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Convenciones
Configurar
Diagrama de la red
Configuraciones
Iniciar la configuración del sensor
Agregar el sensor al IME
Configure el reinicio TCP para el router Cisco IOS
Verificación
Iniciar el ataque y el reinicio de TCP
Troubleshoot
Consejos
Información Relacionada

Introducción

Este documento explica la configuración del reinicio de TCP del sistema de prevención de intrusiones (IPS) mediante IPS Manager Express (IME). Los sensores IME e IPS se utilizan para administrar un router Cisco para el reinicio TCP. Cuando revise esta configuración, recuerde estos elementos:

- Instale el sensor y asegúrese de que funciona correctamente.
- Haga que la interfaz de sabueso se expanda al router fuera de la interfaz.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco IPS Manager Express 7.0
- Cisco IPS Sensor 7.0(0.88)E3
- Router Cisco IOS® con Cisco IOS Software Release 12.4

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

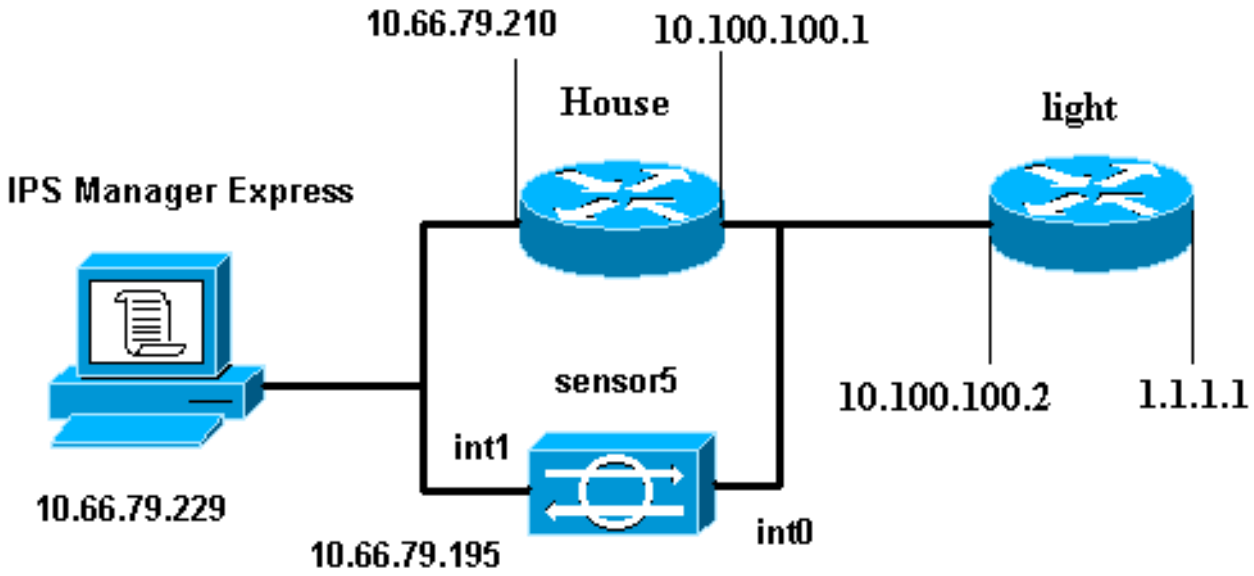
Convenciones

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Configurar

Diagrama de la red

Este documento utiliza la configuración de red que se muestra en el siguiente diagrama.



Configuraciones

Este documento usa las configuraciones detalladas aquí.

- Luz del router
- Base del router

Luz del 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
```

Base del router

```
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
```

Iniciar la configuración del sensor

Complete estos pasos para iniciar la configuración del Sensor.

1. Si es la primera vez que inicia sesión en el Sensor, debe ingresar **cisco** como nombre de usuario y **cisco** como contraseña.
2. Cuando el sistema se lo solicite, cambie la contraseña.**Nota:** Cisco123 es una palabra de diccionario y no se permite en el sistema.
3. Escriba **setup** y complete el mensaje del sistema para configurar los parámetros básicos de los sensores.
4. Ingresar esta información

```
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. Guarde la configuración.El sensor puede tardar unos minutos en guardar la configuración.

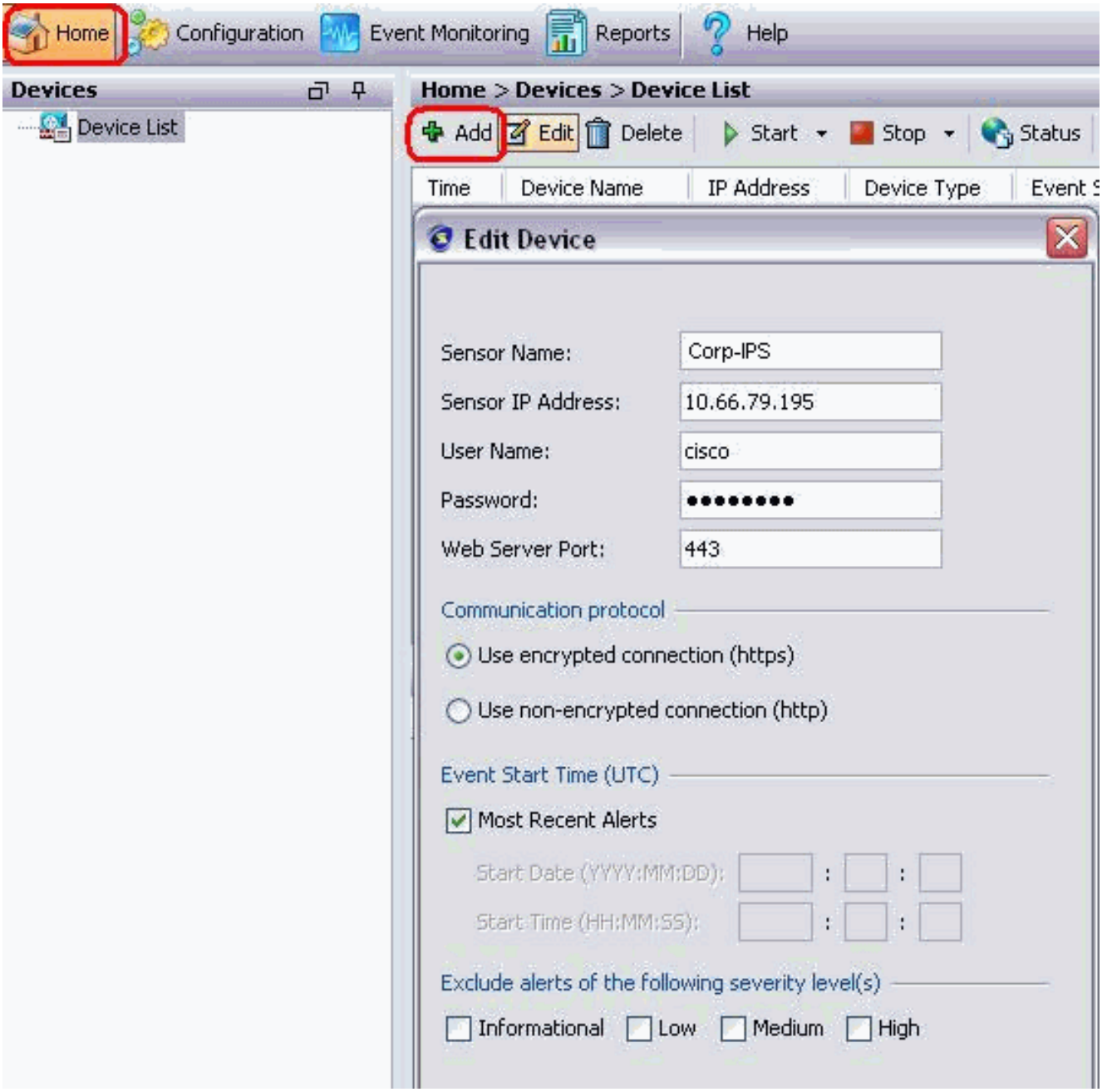
```
[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.

Enter your selection[2]: 2
```

Agregar el sensor al IME

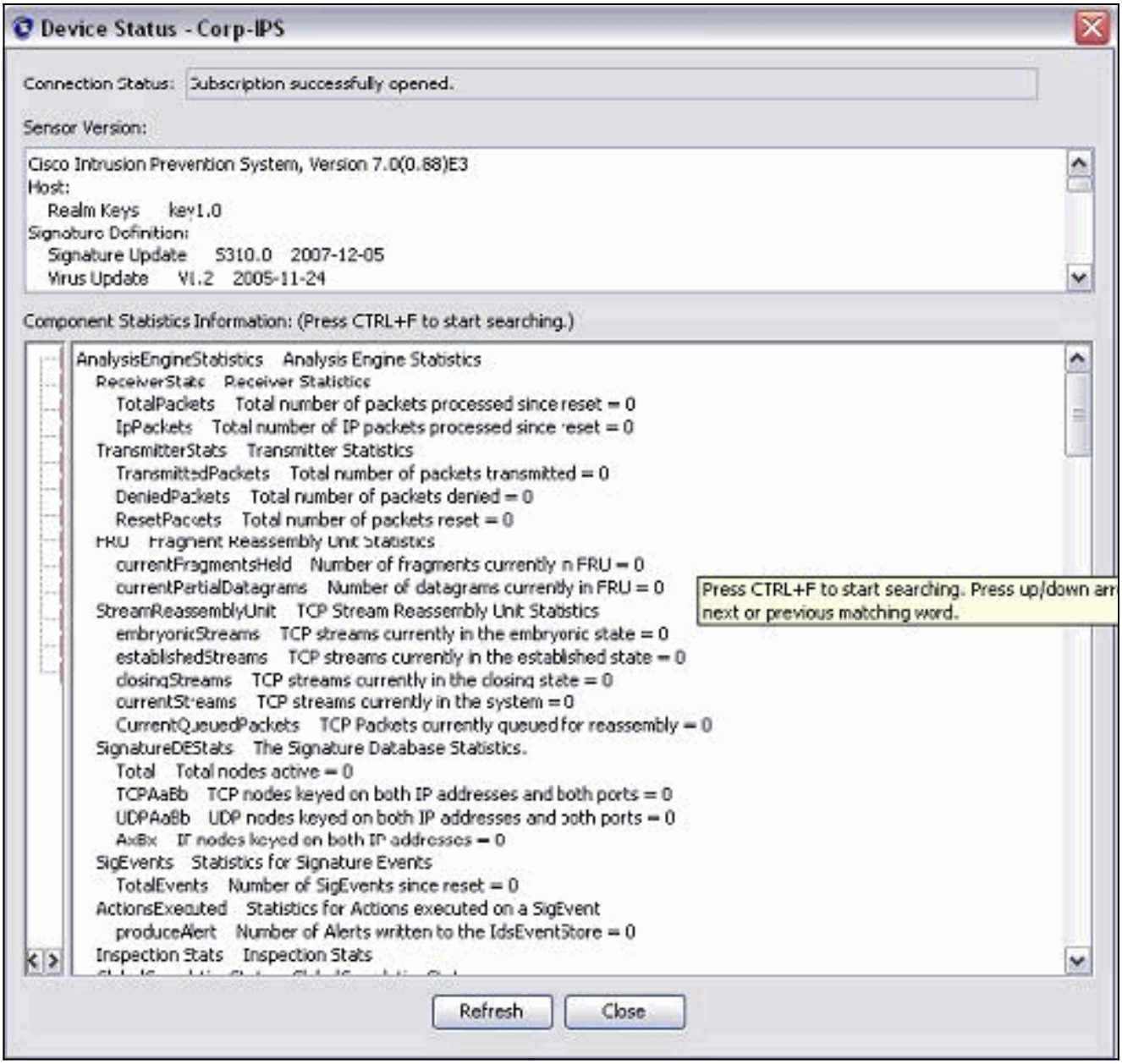
Complete estos pasos para agregar el Sensor al IME:

1. Vaya a la PC con Windows, que instaló IPS Manager Express, y abra IPS Manager Express.
2. Elija **Home > Add**

.



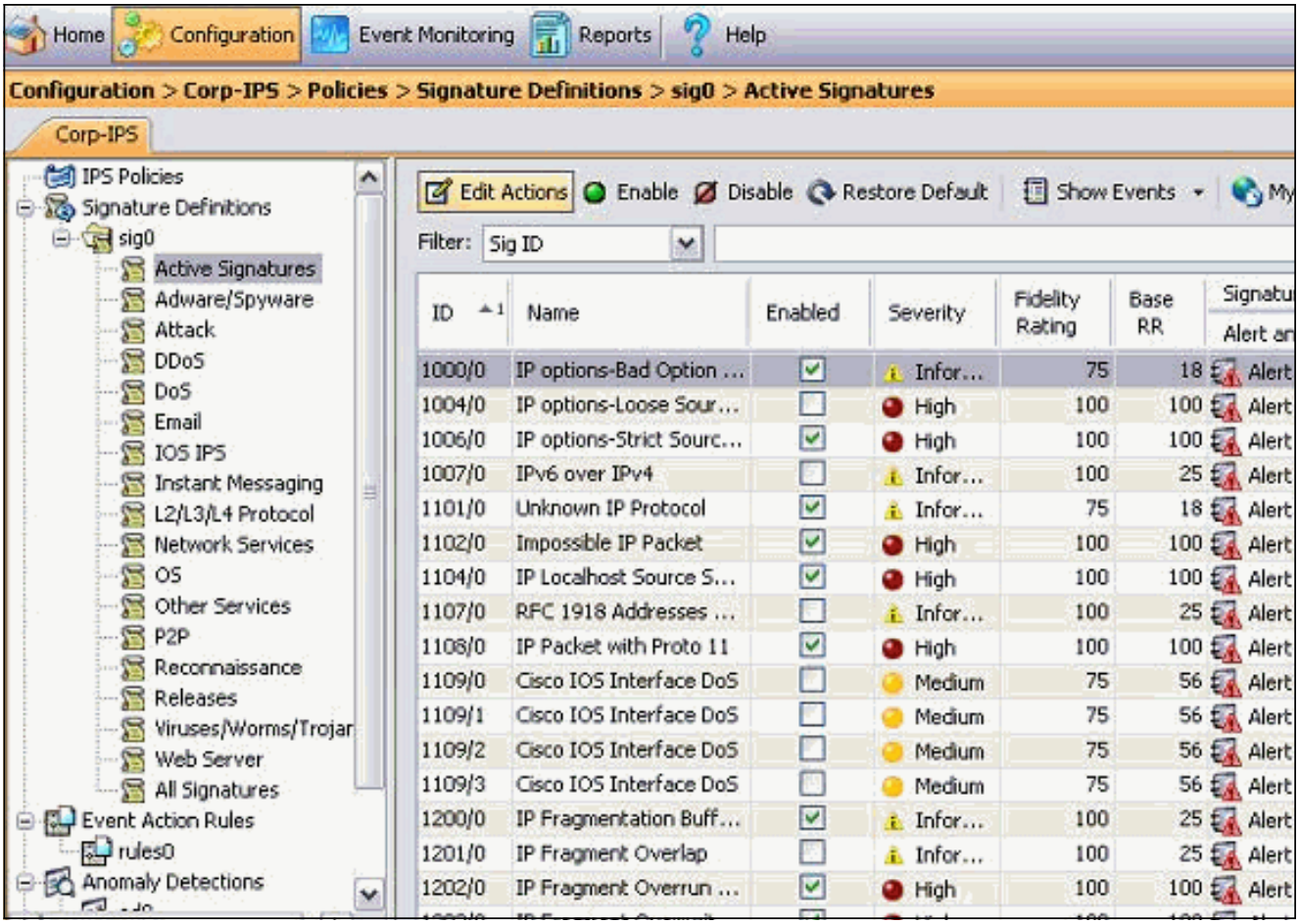
3. Escriba esta información y haga clic en **Aceptar** para finalizar la configuración.
4. Elija **Devices > Corp-IPS** para verificar el estado del Sensor y luego haga clic con el botón derecho para elegir **Device Status**.Asegúrese de que puede ver `Suscripción abierta correctamente.`



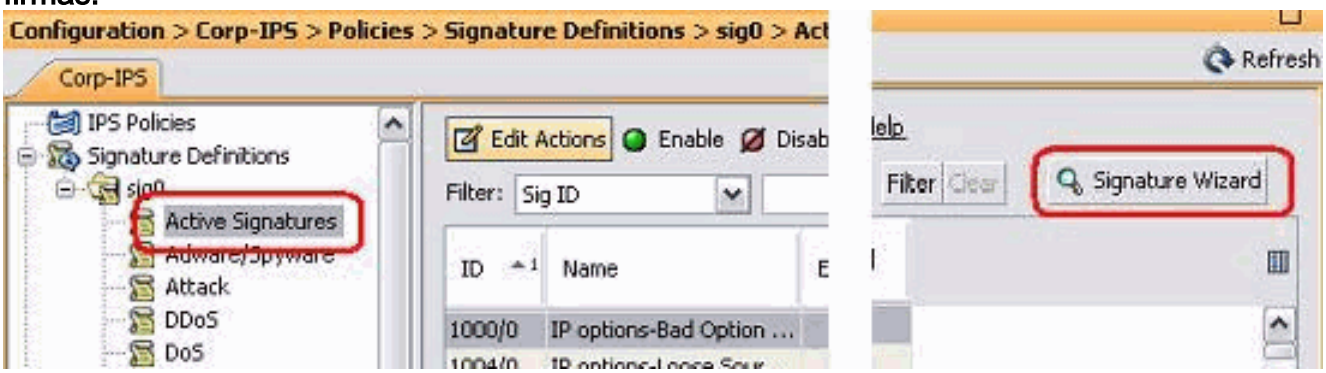
Configure el reinicio TCP para el router Cisco IOS

Complete estos pasos para configurar el reinicio TCP para el router Cisco IOS:

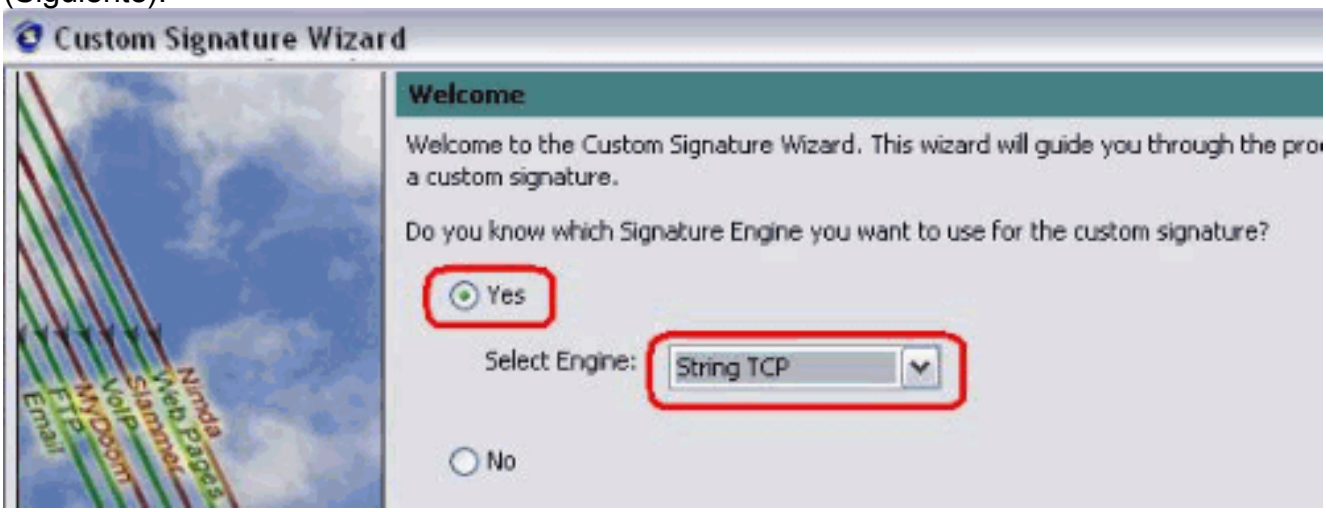
1. Desde el ordenador IME, abra su navegador web y vaya a **https://10.66.79.195**.
2. Haga clic en **Aceptar** para aceptar el certificado HTTPS descargado del Sensor.
3. En la ventana de registro, ingrese como nombre de usuario cisco y 123cisco123 como contraseña.Aparece esta interfaz de administración IME:



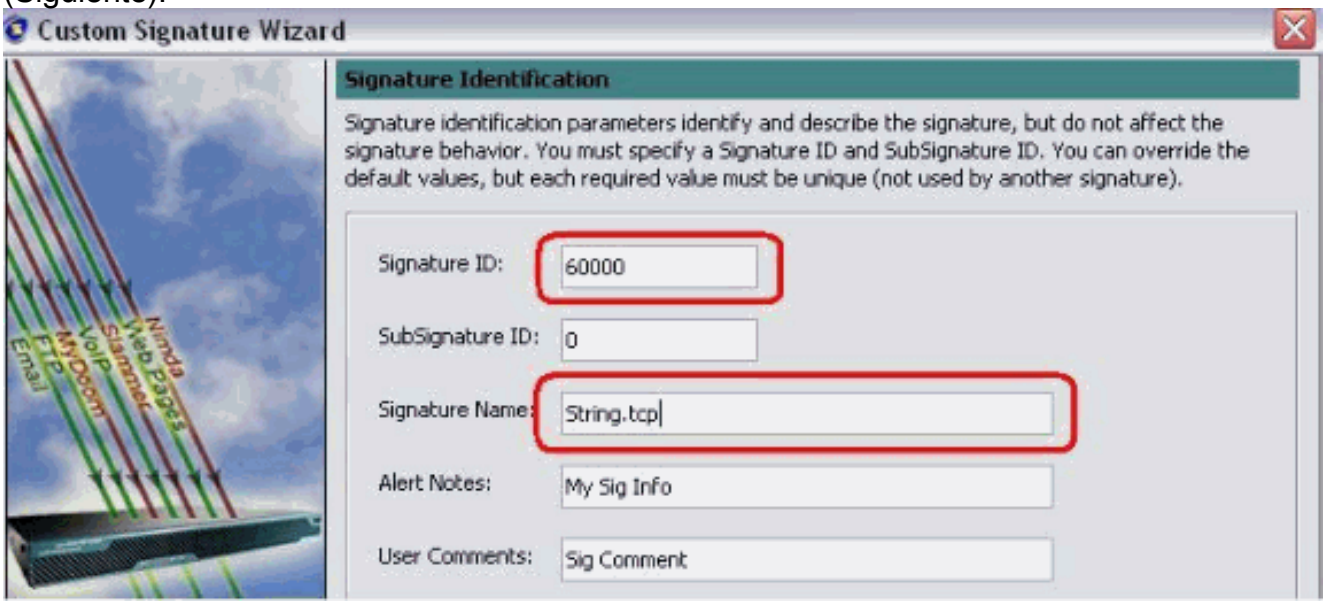
4. En la ficha Configuración, haga clic en **Firmas activas**.
5. A continuación, haga clic en **Asistente para firmas.**



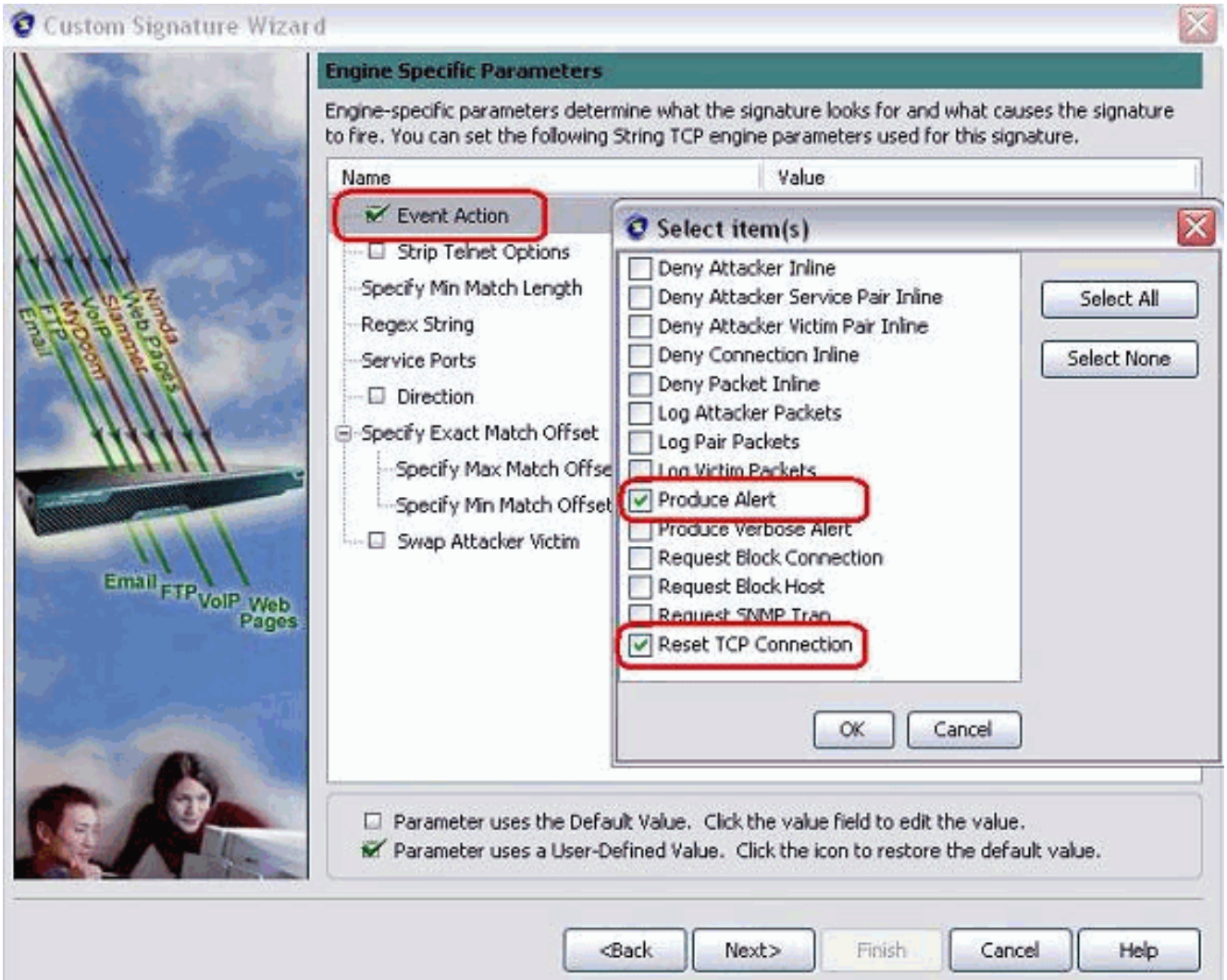
6. En el asistente, elija **Yes** y elija **String TCP** como motor de firma. Haga clic en Next (Siguiente).



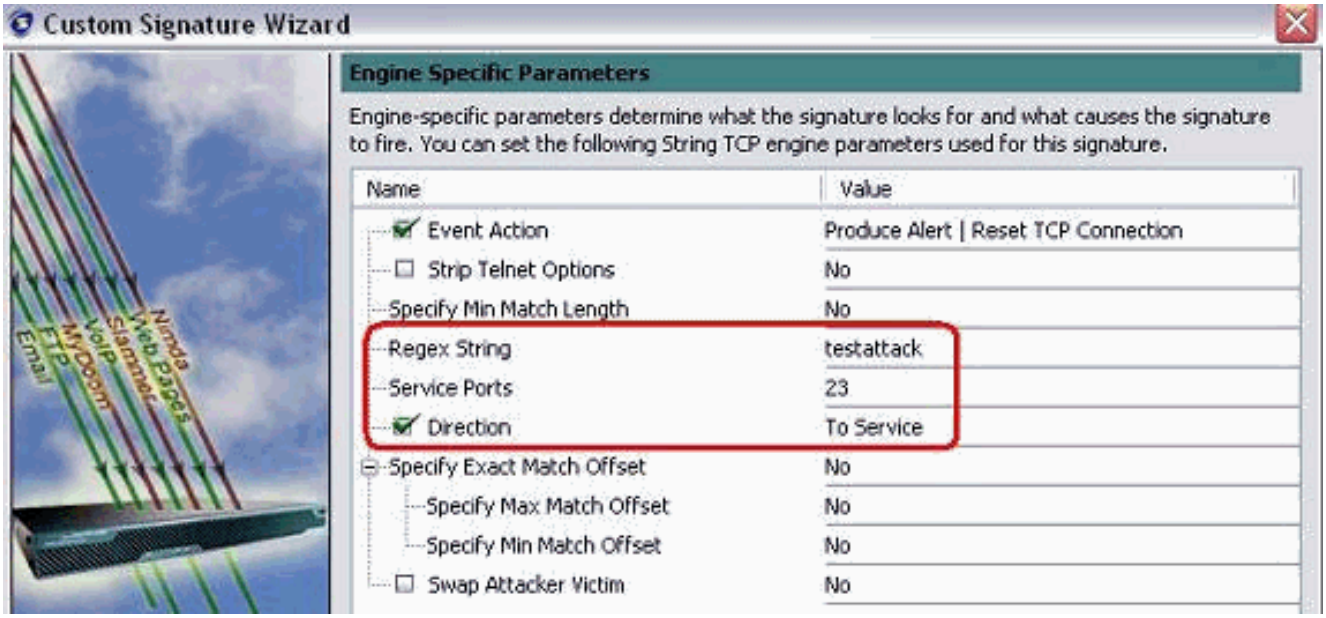
7. Puede dejar esta información como predeterminada o introducir su propia ID de firma, nombre de firma y notas del usuario. Haga clic en Next (Siguiente).



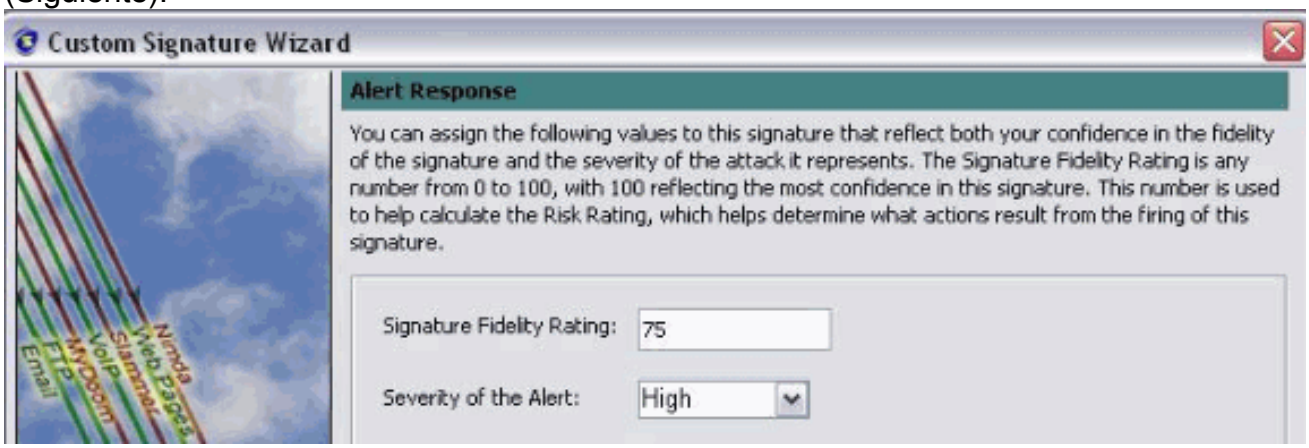
8. Elija **Acción de evento**, y elija **Producir alerta** y **Restablecer conexión TCP**. Haga clic en **Aceptar** y luego **Siguiente** para continuar.



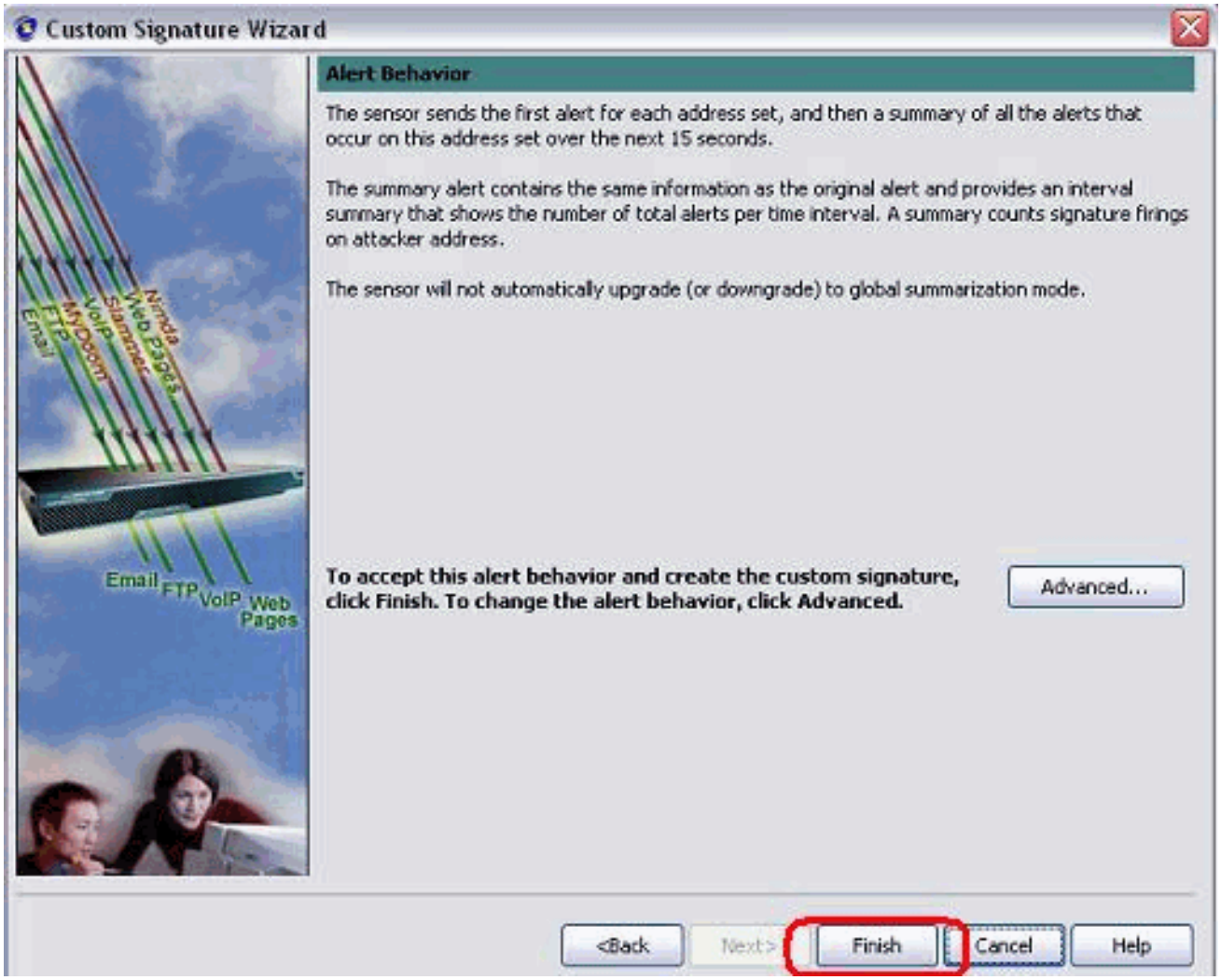
9. Ingrese una expresión regular y en este ejemplo se utiliza el `ataque de prueba`. Ingrese **23** para los puertos de servicio, elija **To Service** para la dirección y haga clic en **Next** para continuar.



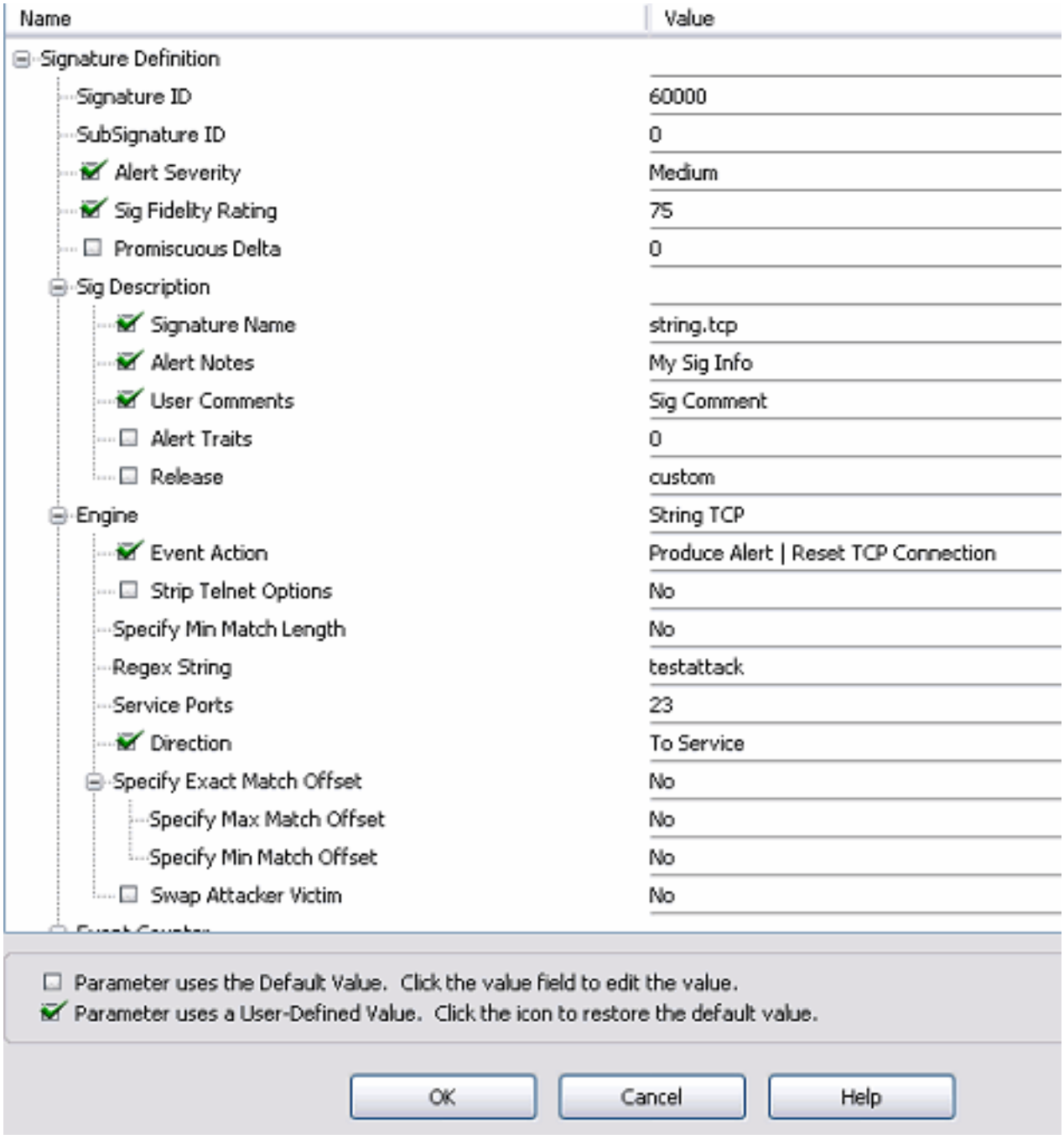
10. Puede dejar esta información como Predeterminada. Haga clic en Next (Siguiente).



11. Haga clic en **Finalizar** para finalizar el asistente.



12. Elija **Configuration > sig0 > Active Signations** para localizar la firma recién creada por **Sig ID** o **Sig Name**. Haga clic en **Editar** para ver la firma.



13. Haga clic en **Aceptar** después de confirmar y haga clic en el **botón Aplicar** para aplicar la firma al Sensor.

Verificación

Iniciar el ataque y el reinicio de TCP

Complete estos pasos para iniciar el ataque y el reinicio de TCP:

1. Antes de iniciar el ataque, vaya al **IME**, elija **Event Monitoring > Dropped Attacks View** y elija el sensor de la derecha.
2. Desde el router Light, realice una conexión Telnet al router House e ingrese testattack.Pulse **<space>** o **<enter>** para reiniciar la sesión 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. Desde el panel del Visor de eventos IPS, aparece la alarma roja una vez que se inicia el ataque.

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

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Consejos

Utilice estas sugerencias para la resolución de problemas:

- El desvío funciona desde el puerto de comando y control para reprogramar las listas de control de acceso (ACL) del router. Los reinicios de TCP se envían desde la **interfaz de rastreo** del Sensor. Cuando **configure span** en el switch, utilice el comando **set span <src_mod/src_port><dest_mod/dest_port>** con ambos paquetes entrantes habilitados como se muestra aquí.

```
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
```

- Si los restablecimientos TCP funcionan, verifique si la alarma se activa para el tipo de acción TCP Reset. Si aparece la alarma, verifique que el tipo de firma esté configurado en TCP reset.Inicie sesión con la cuenta de servicio su para root y ejecute este comando. Este comando asume que la interfaz de detección está configurada en eth0.

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

Nota: Cien restablecimientos tcp se envían a la víctima/el objetivo y cien se envían al atacante/cliente.El siguiente es un ejemplo del resultado:

```
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
```

Información Relacionada

- Página de soporte de Cisco Secure Intrusion Prevention
- Documentación para Cisco Secure Intrusion Prevention System
- Soporte Técnico y Documentación - Cisco Systems