Configurar el Restablecimiento TCP IPS usando IME

Contenido

Introducción

Este documento discute la configuración del Restablecimiento TCP del Sistema de prevención de intrusiones (IPS) usando el administrador IPS expreso (IME). Los sensores IME e IPS se utilizan para manejar a un router Cisco para el Restablecimiento TCP. Cuando usted revisa esta configuración, recuerde estos elementos:

- Instale el sensor y aseegurese los trabajos del sensor correctamente.
- Haga que la interfaz de sabueso se expanda al router fuera de la interfaz.

prerrequisitos

Requisitos

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.

- El administrador del IPS de Cisco expresa 7.0
- Sensor 7.0(0.88)E3 del IPS de Cisco
- Router de Cisco IOS® con el Cisco IOS Software Release 12.4

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

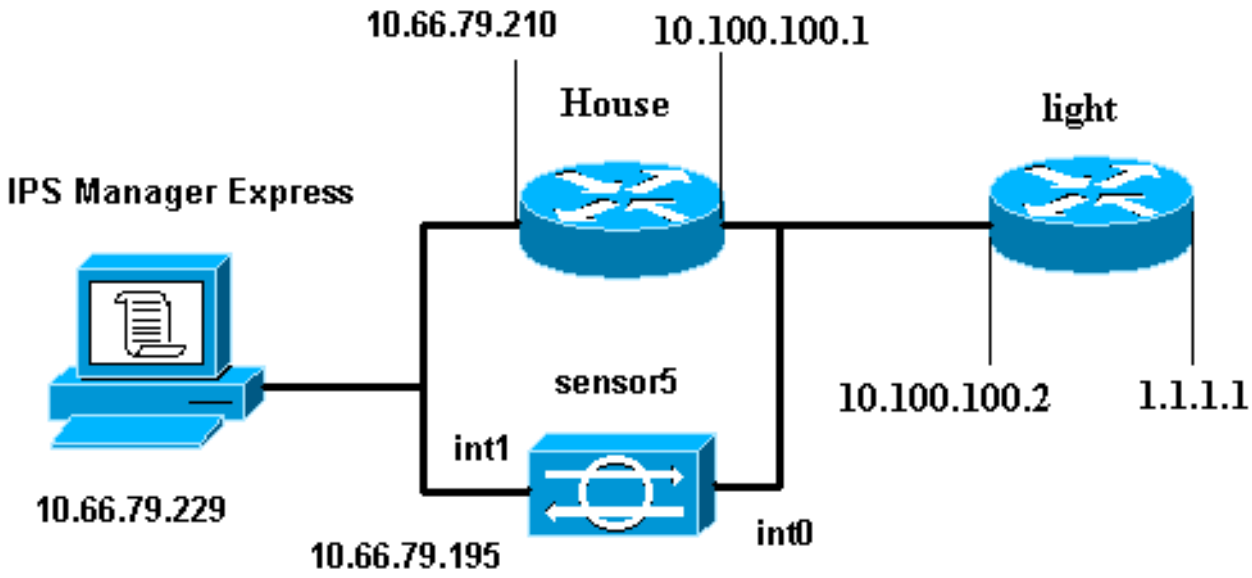
Convenciones

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

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
```

Comience la Configuración del sensor

Complete estos pasos para comenzar la configuración del sensor.

1. Si ésta es su primera vez de registrar en el sensor, usted debe ingresar **Cisco** como el Nombre de usuario y **Cisco** como la contraseña.
2. Cuando el sistema se lo solicite, cambie la contraseña.**Nota:** El cisco123 es una palabra del diccionario y no se permite en el sistema.
3. Teclee la **configuración** y complete el prompt del sistema para configurar los parámetros básicos para 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
```

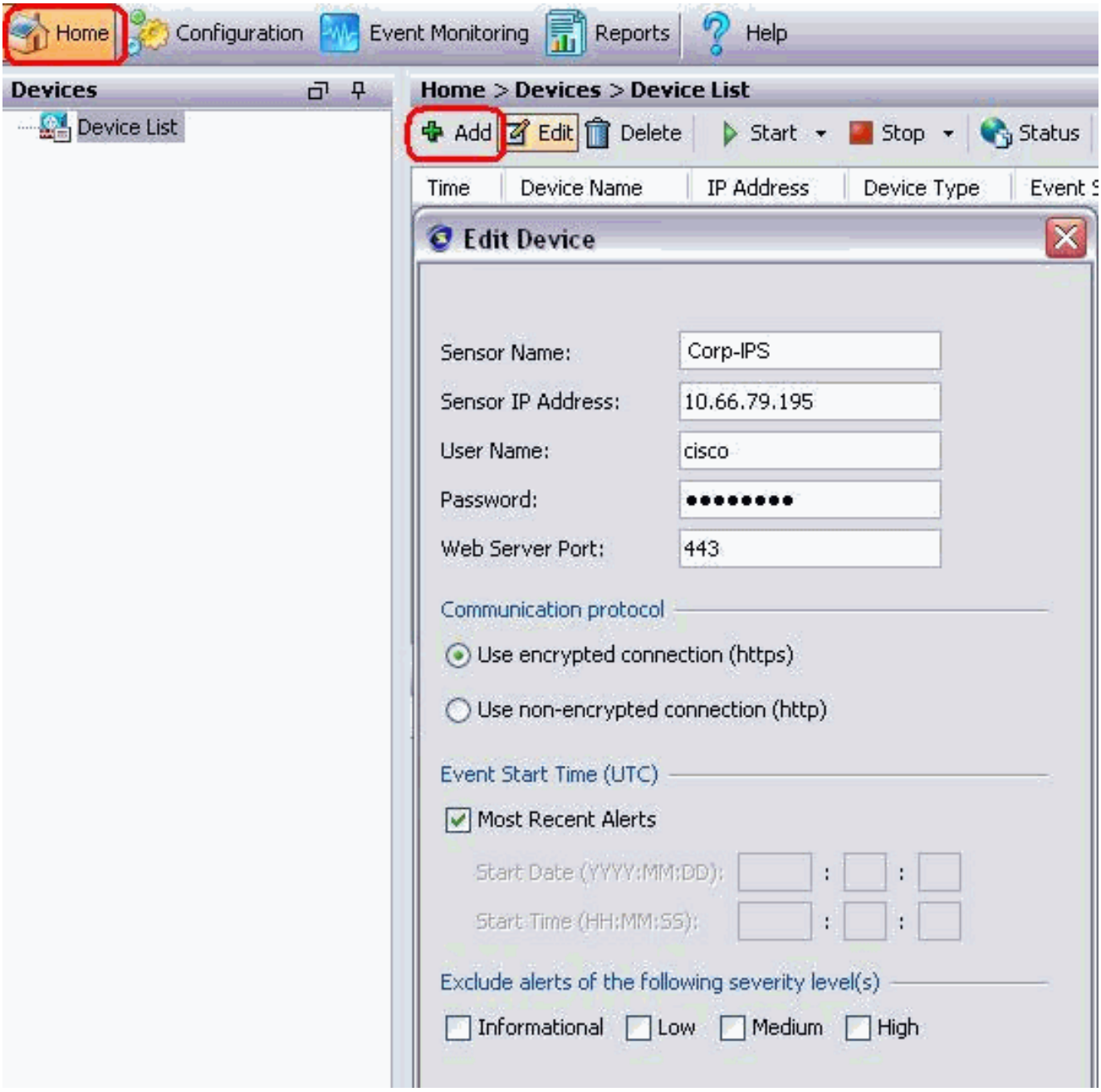
5. Guarde la configuración.Puede tardar algunos minutos para que el sensor salve la configuración.
```
[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.

Enter your selection[2]: 2
```

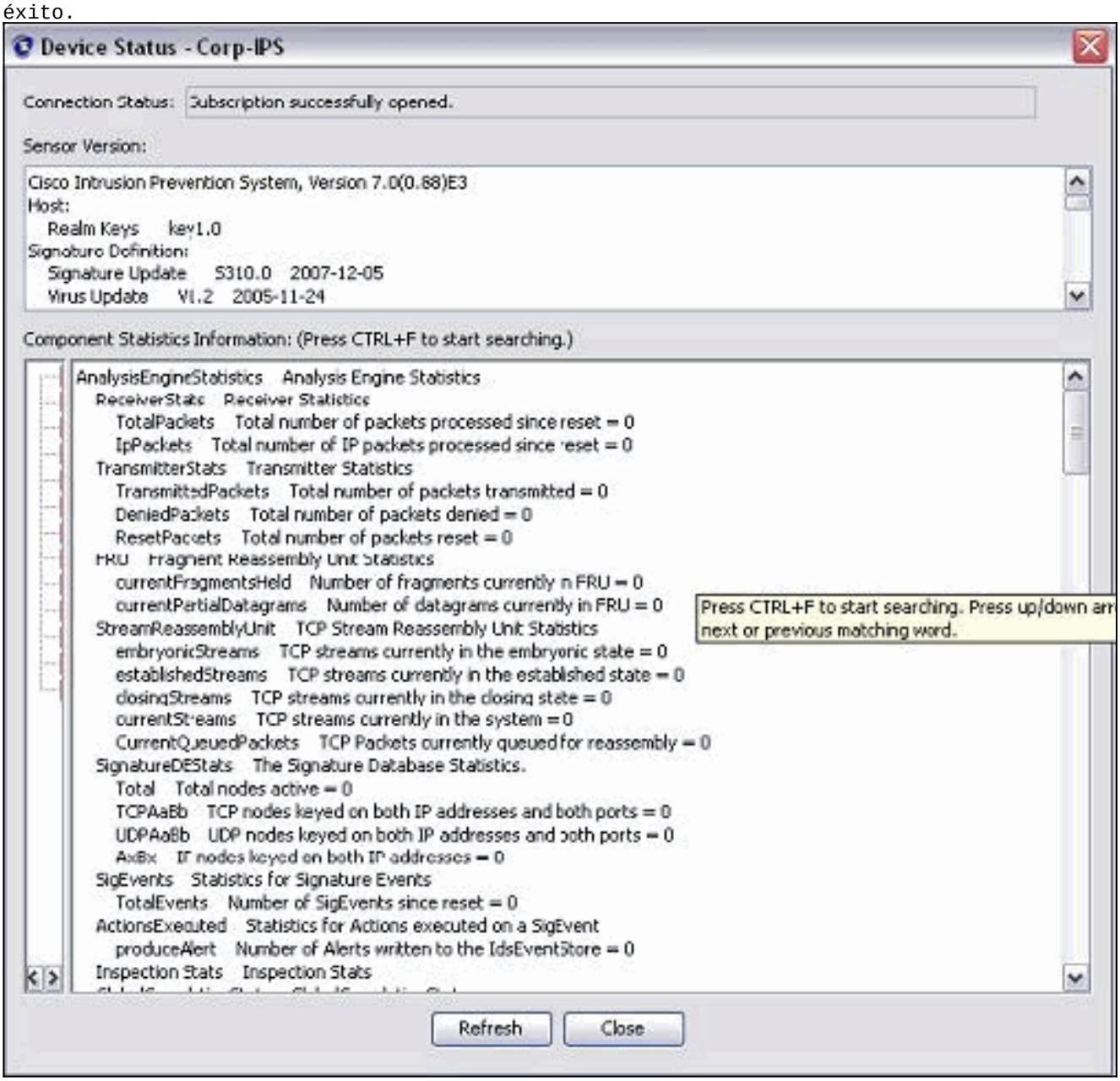
Agregue el sensor en el IME

Complete estos pasos para agregar el sensor en el IME:

1. Vaya al PC de Windows, que instalaron al administrador IPS expreso, y abra al administrador IPS expreso.
2. Elija **a casa >** **Add**.



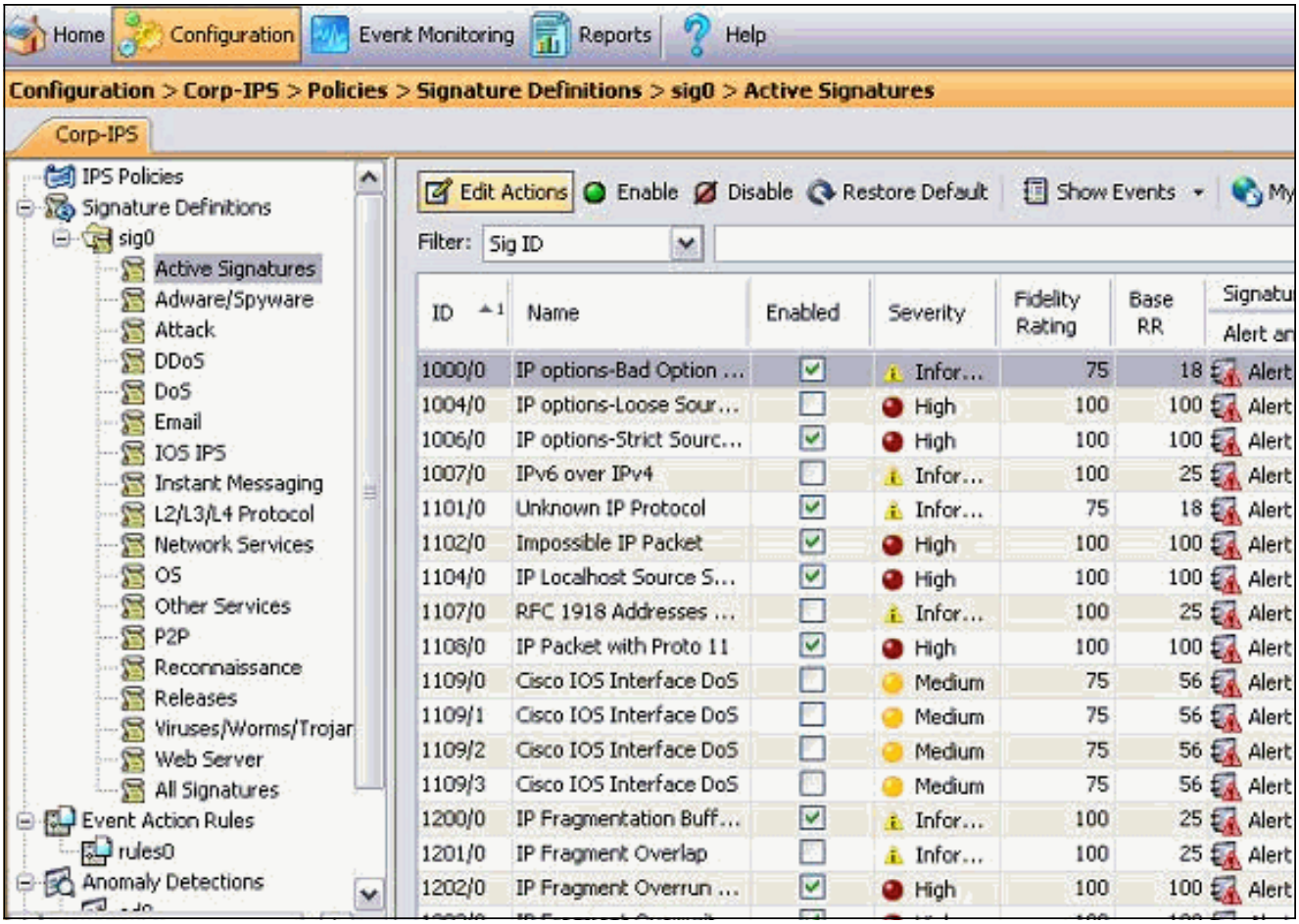
3. Teclee adentro esta información y haga clic la **AUTORIZACIÓN** para acabar la configuración.
4. Elija los **dispositivos > el Corp-IPS** para verificar el estado del sensor y después hacer clic con el botón derecho del ratón para elegir el **estado del dispositivo**.Aseegurese que usted puede ver la `suscripción abierta con éxito.`



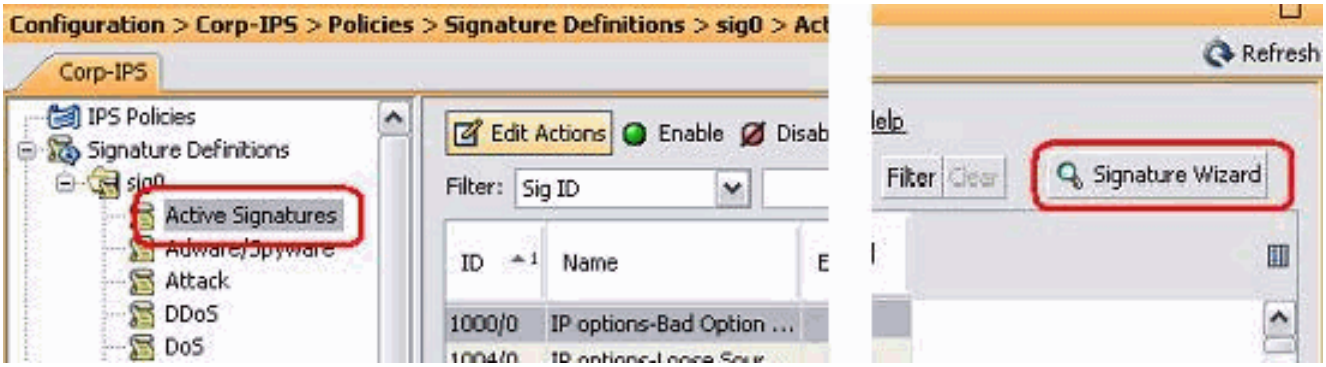
Configure el Restablecimiento TCP para el router del Cisco IOS

Complete estos pasos para configurar el Restablecimiento TCP para el router del Cisco IOS:

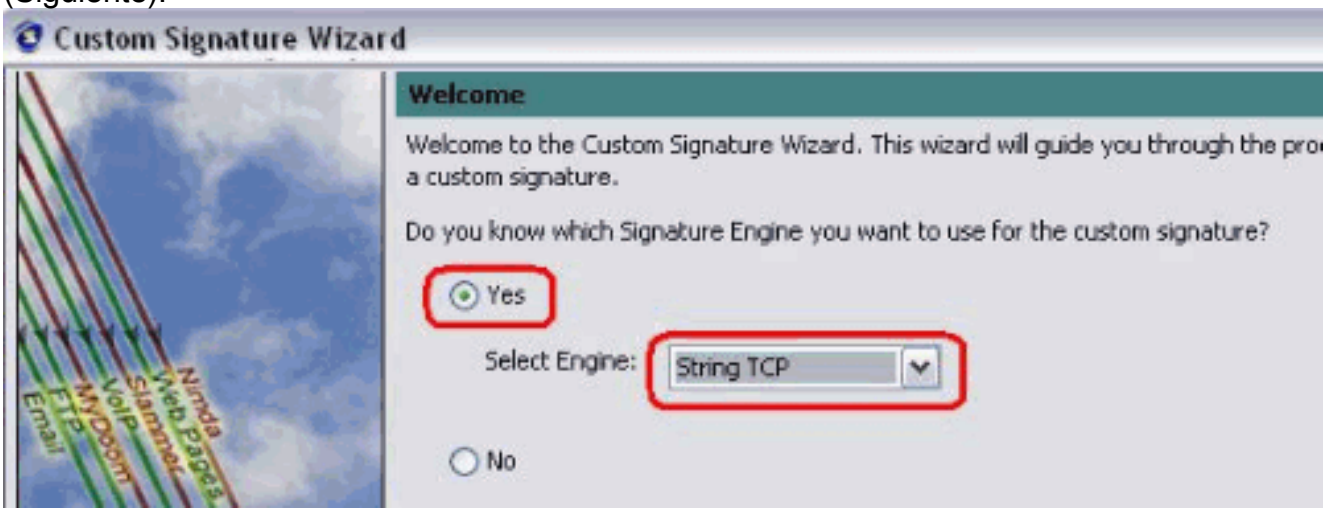
1. Del IME PC, abra a su buscador Web y vaya a **https://10.66.79.195**.
2. Haga Click en OK para validar el certificado HTTPS descargado del sensor.
3. En la ventana de registro, ingrese como nombre de usuario cisco y 123cisco123 como contraseña.Esta interfaz de administración IME aparece:



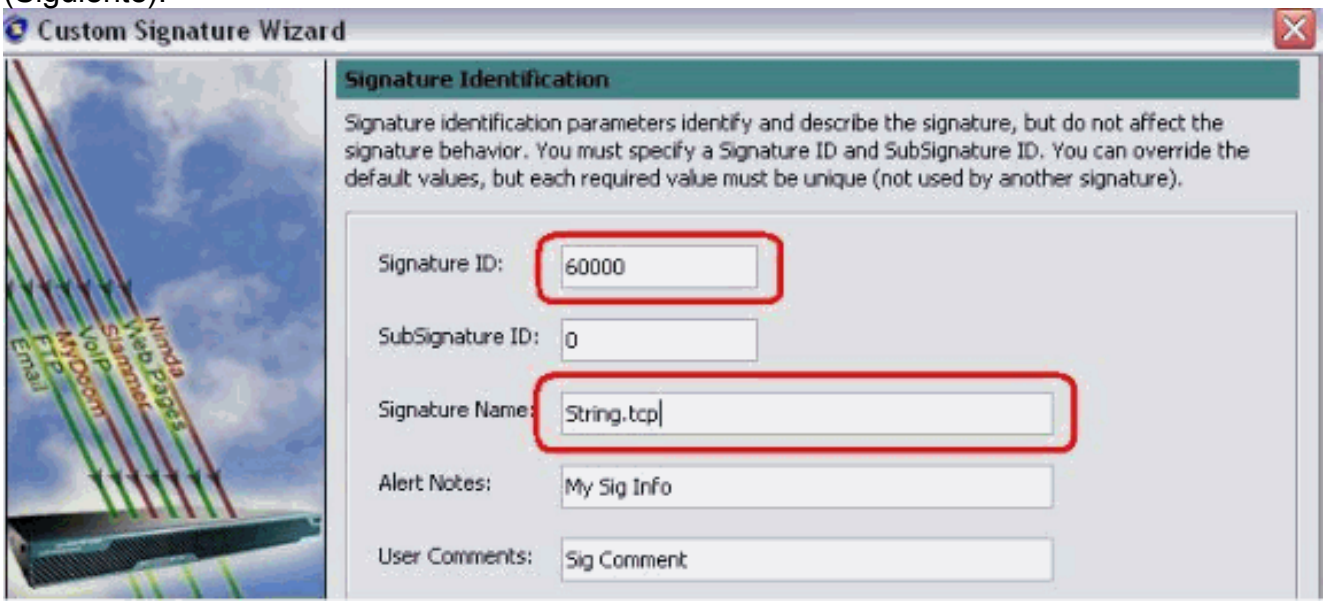
4. De la ficha de configuración, haga clic las **firmas activas**.
5. Entonces haga clic al **Asistente de firmas.**



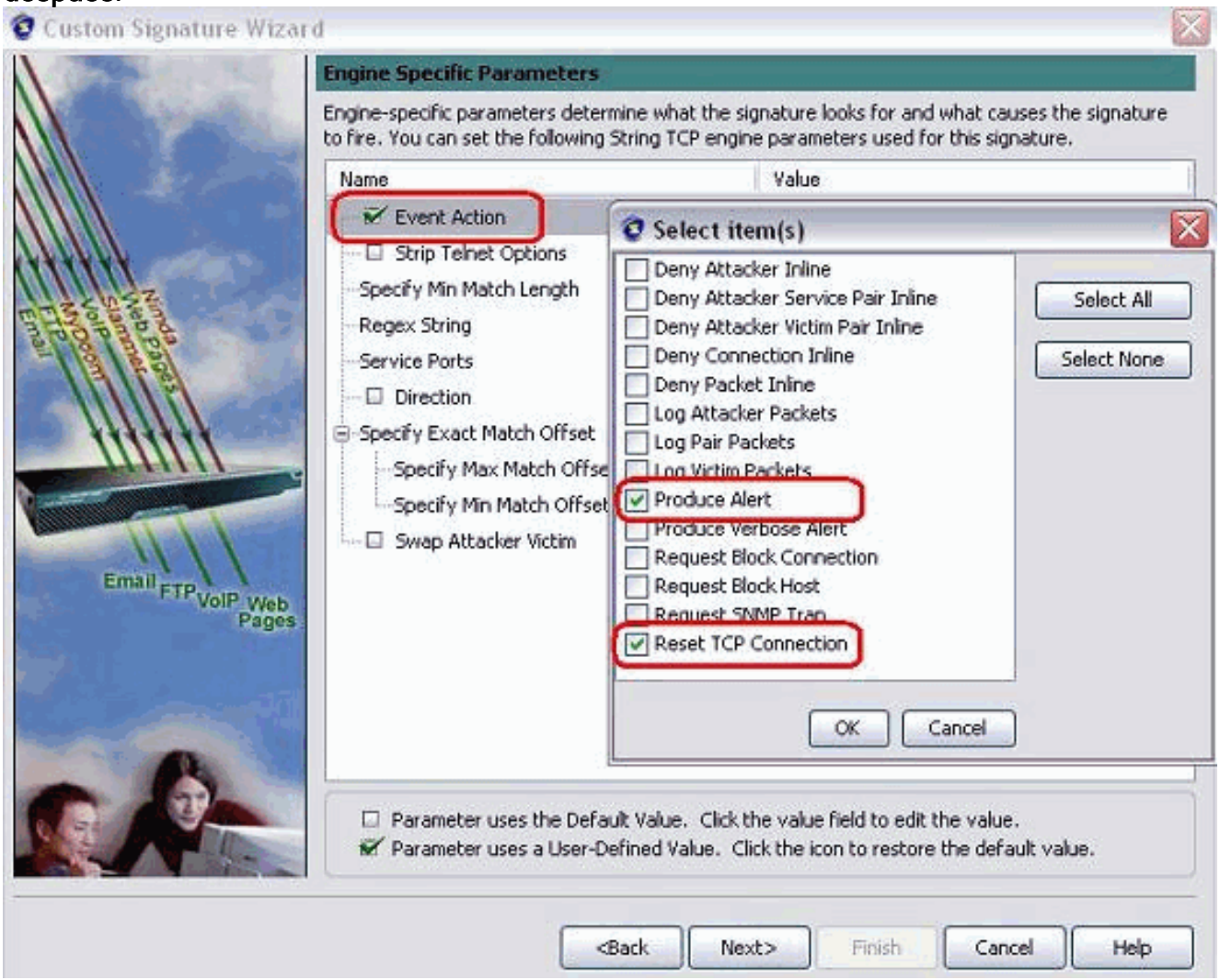
6. En el Asisitente, elija **sí** y elija la **cadena TCP** como el motor de firma. Haga clic en Next (Siguiente).



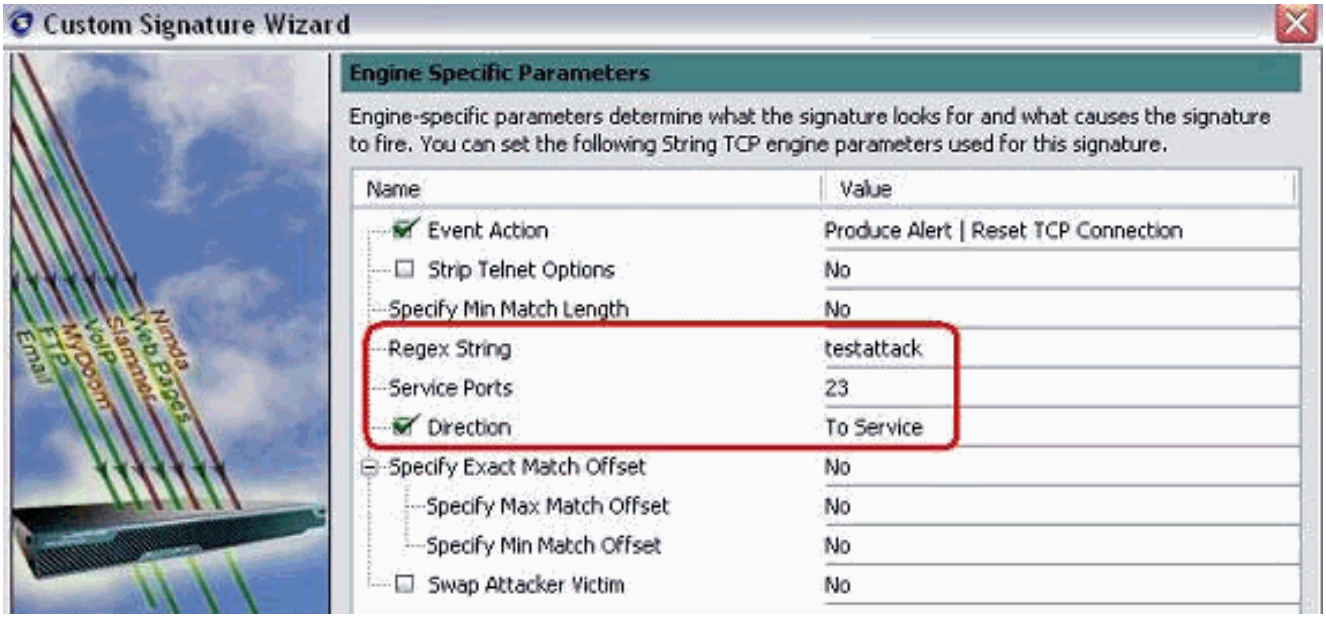
7. Usted puede dejar esta información como efdault o ingresar su propio ID de la firma, nombre de la firma y notas del usuario. Haga clic en Next (Siguiente).



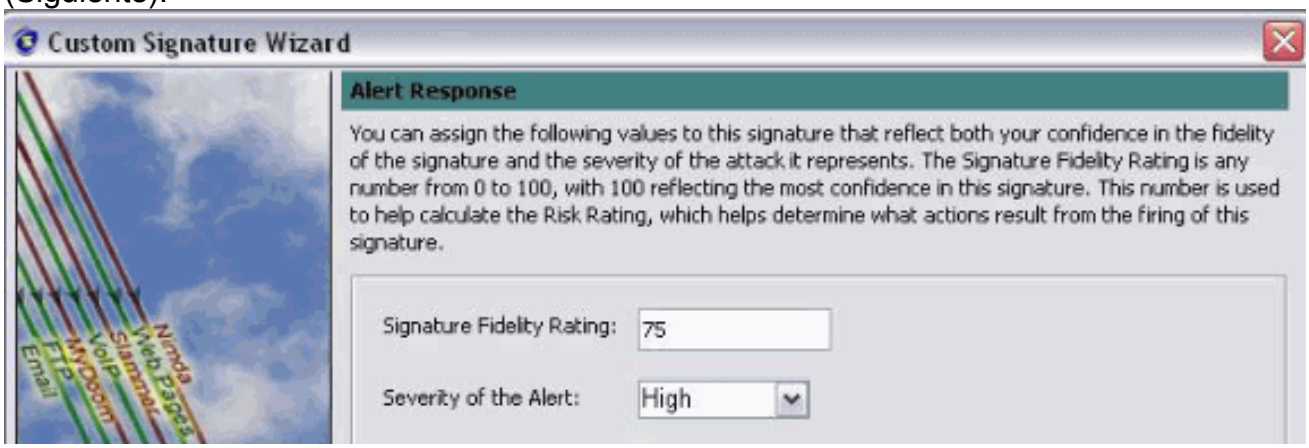
8. Elija la **acción del evento**, y elija la **alerta de la producción** y la **conexión TCP de la restauración**. Haga Click en OK y entonces para continuar **después**.



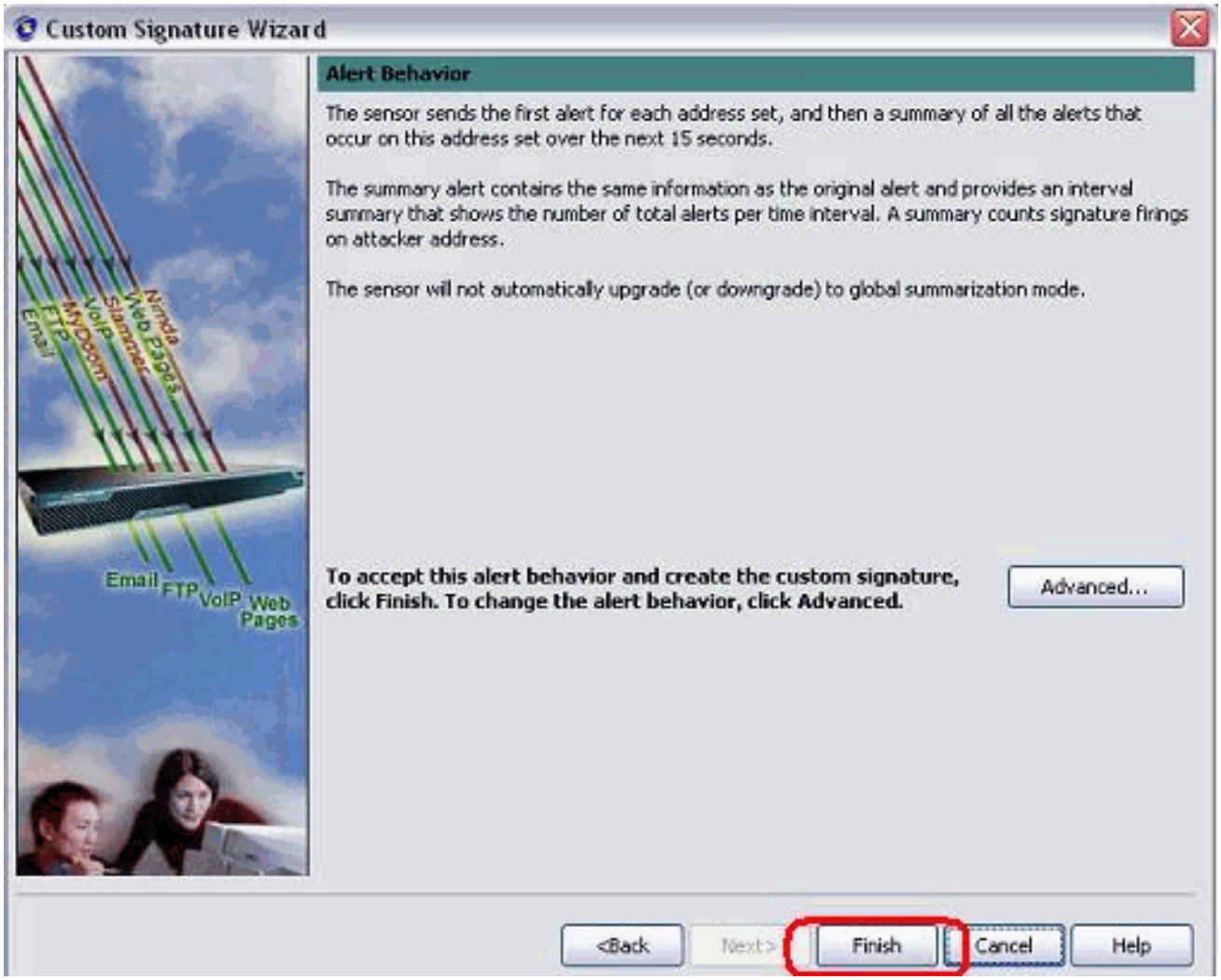
9. Ingrese una expresión normal, y el `testattack` se utiliza en este ejemplo. Ingrese **23** para los puertos del servicio, elija **mantener** para la dirección, y el tecleo **después** para continuar.



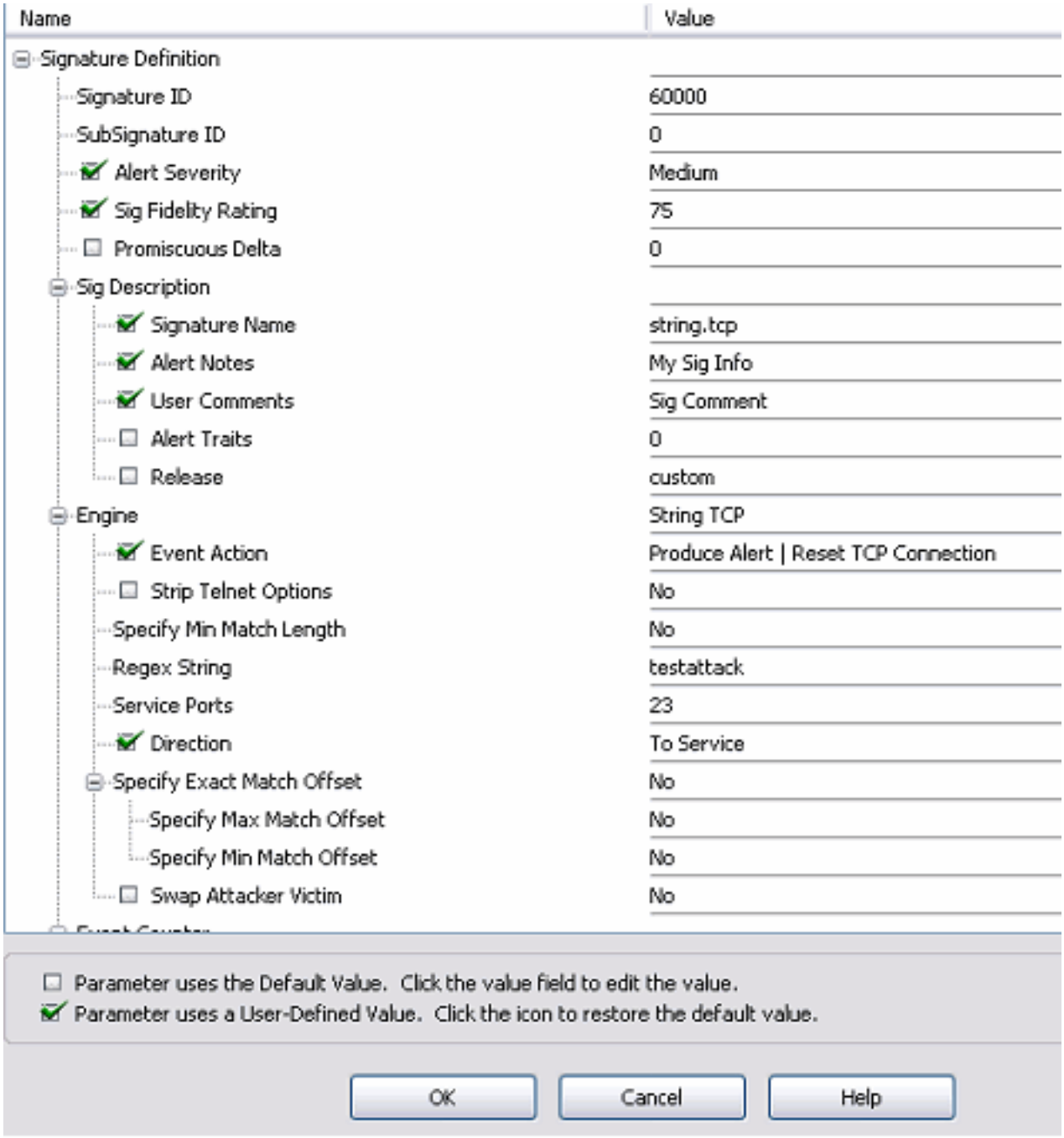
10. Usted puede dejar esta información como valor por defecto. Haga clic en Next (Siguiente).



11. Clic en Finalizar para acabar al Asisitente.



12. Elija la **configuración > sig0 > las firmas activas** para localizar la firma creada recientemente por los **Sig ID** o el **nombre de los Sig**. El tecleo **edita** para ver la firma.



13. Haga Click en OK después de que usted confirme y haga clic el **botón Apply Button** para aplicar la firma al sensor.

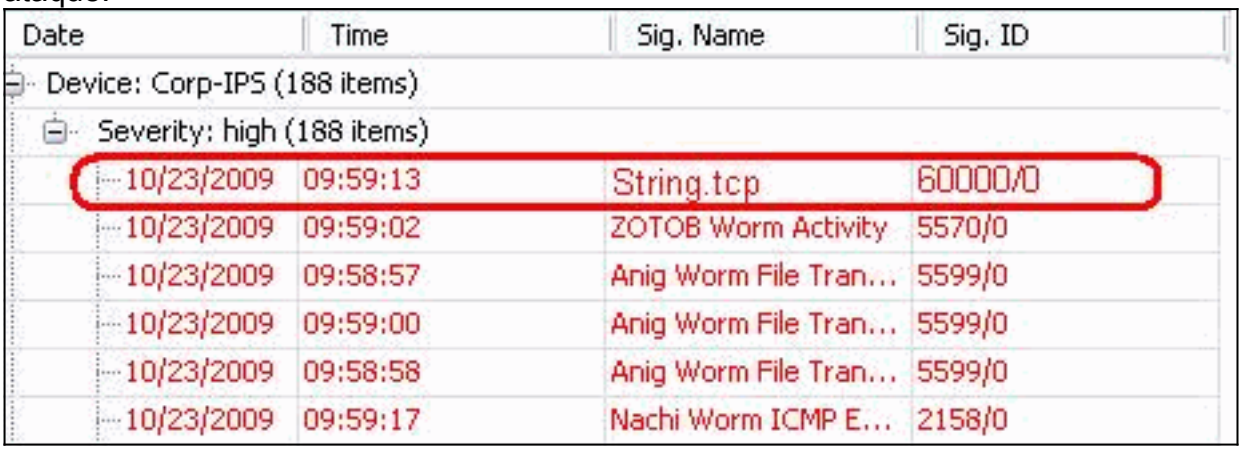
Verificación

Inicie el ataque y el Restablecimiento TCP

Complete estos pasos para iniciar el ataque y el Restablecimiento TCP:

1. Antes de que usted ponga en marcha el ataque, va al **IME**, elige el **monitoreo de evento > la opinión caída de los ataques** y elige el sensor a la derecha.
2. Desde el router Light, realice una conexión Telnet al router House e ingrese testattack.Golpee **<space>** o **<enter>** para reajustar a su 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. Del panel del visor de eventos IPS, la alarma roja aparece 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

Troubleshooting

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

Consejos

Utilice estos consejos de Troubleshooting:

- El evitar se resuelve del comando y del puerto de control de reprogramar los Router Access Control List (ACL). Las restauraciones TCP se envían de la **interfaz de rastreo del** sensor. Cuando usted **fija el palmo** 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 las restauraciones TCP están trabajando, marque si la alarma se acciona para el Restablecimiento TCP del tipo de la acción. Si aparece la alarma, marque que fijan al tipo de la firma al Restablecimiento TCP.Inicie sesión usando la Cuenta de servicio su para arraigar y para publicar este comando. Este comando asume que la interfaz de detección está fijada al eth0.`[root@sensor1 root]#`**`tcpdump -i eth0 -n`** **Nota:** Cientos restauraciones tcp consiguen enviadas a la víctima/a la blanco entonces ciento consiguen enviadas al atacante/al 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 segura de la prevención de intrusiones de Cisco
- La documentación para Cisco asegura el sistema de prevención de intrusiones
- Soporte Técnico y Documentación - Cisco Systems