Configurar el IPS que bloquea usando IME

Contenido

Introducción

Este documento discute la configuración del Sistema de prevención de intrusiones (IPS) que bloquea con el uso del administrador IPS expreso (IME). Los sensores IME e IPS se utilizan para manejar a un router Cisco para bloquear. Recuerde estos elementos cuando usted considera esta configuración:

- 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 del ® del 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.

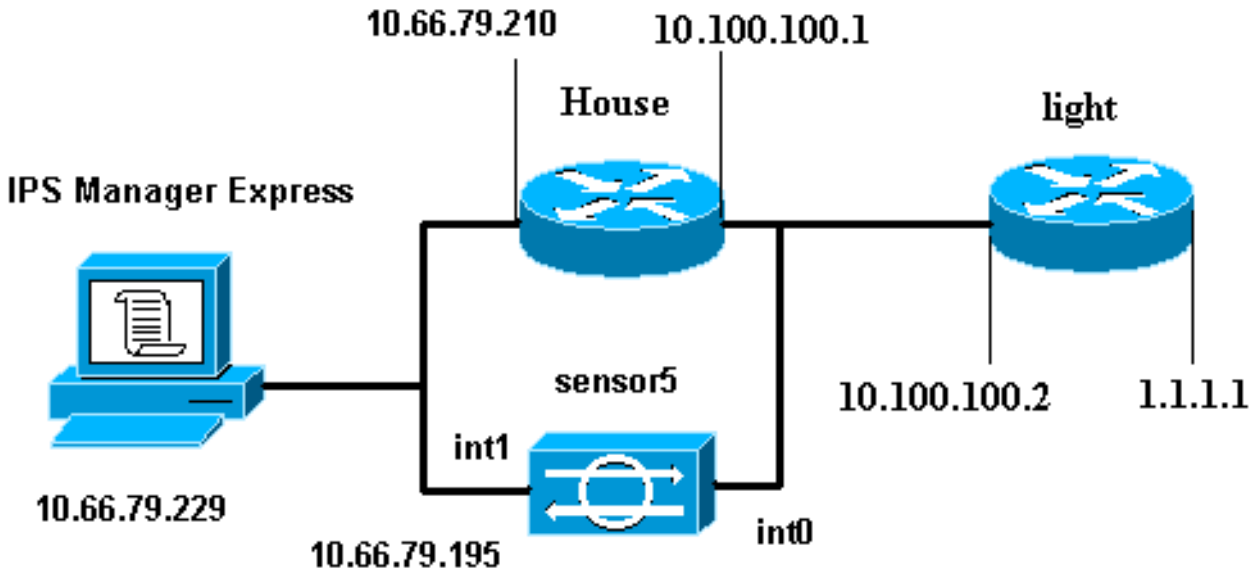
Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configurar

Diagrama de la red

Este documento utiliza esta configuración de red:



Configuraciones

Este documento usa estas configuraciones.

- 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 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
```

Comience la Configuración del sensor

Complete estos pasos para comenzar la configuración del sensor.

1. Si esta es la primera vez que se registra en el Sensor, 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 siga el prompt del sistema para poner 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 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
```

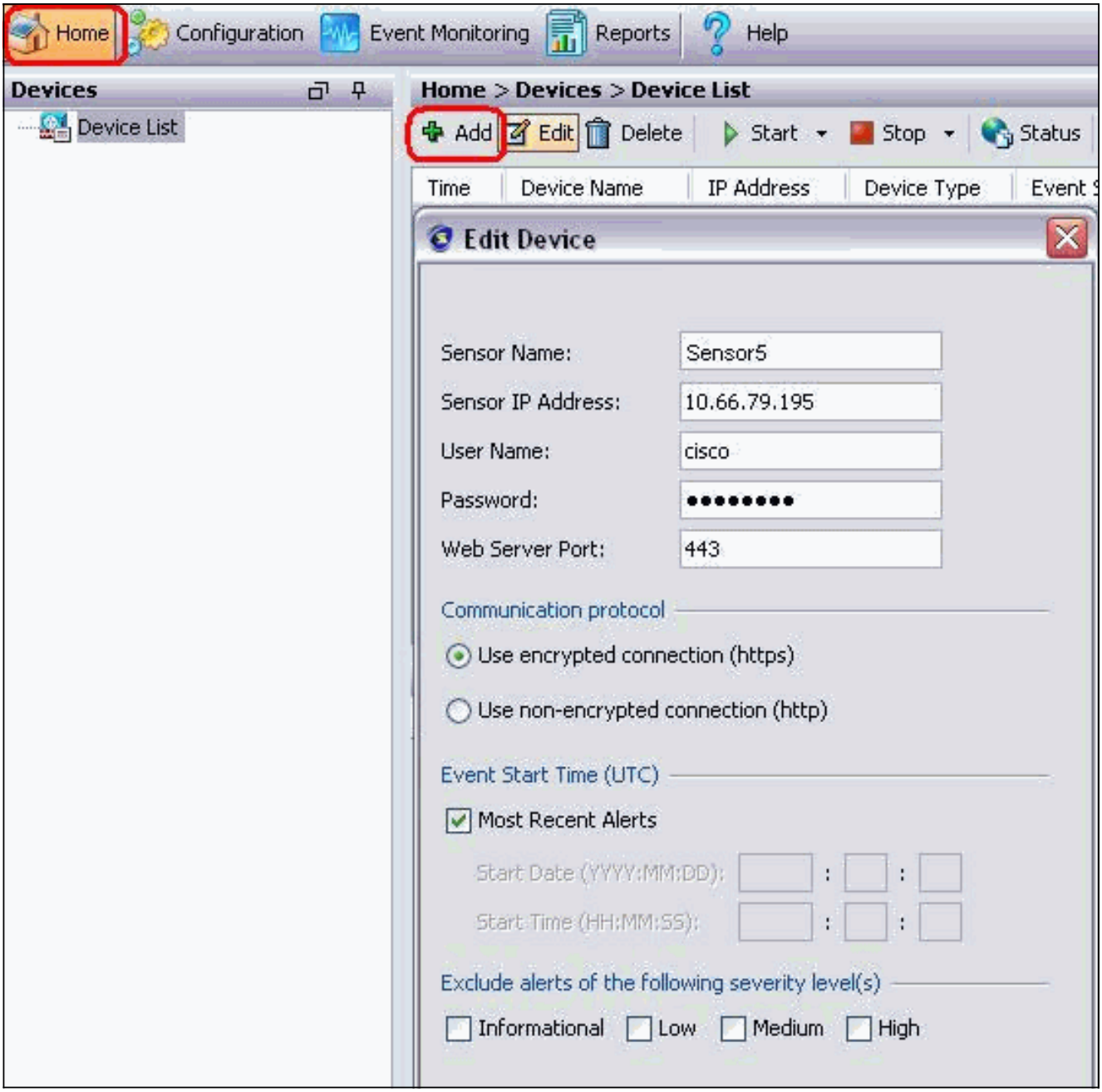
5. Guarde la configuración.Puede tardar algunos minutos para que el sensor salve la configuración.
```
[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.

Enter your selection[2]: 2
```

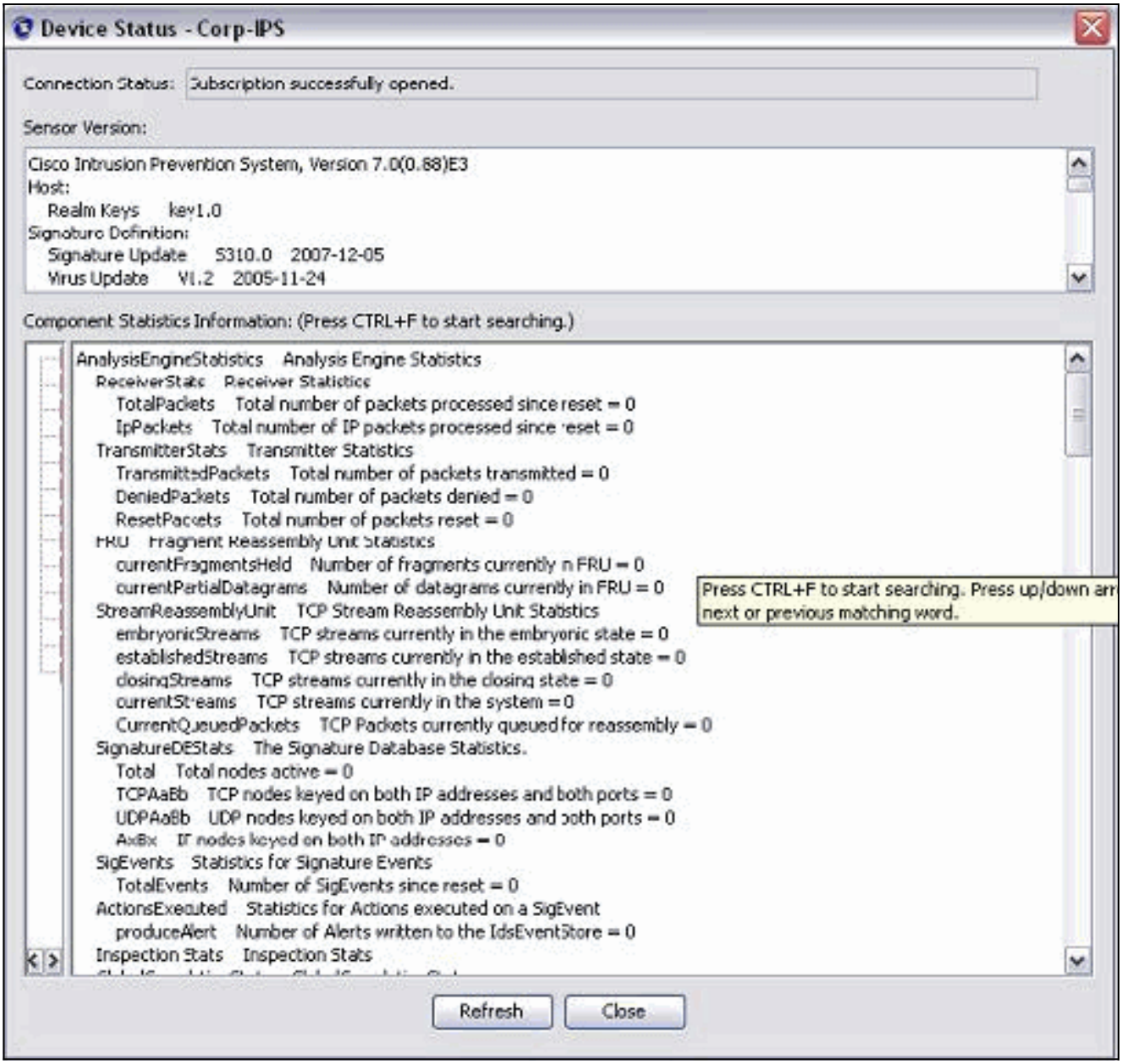
Agregue el sensor en el IME

Complete estos pasos para agregar el sensor en el IME.

1. Vaya al PC de Windows, que instalaron al administrador IPS expreso y abren al **administrador IPS expreso**.
2. Elija **a casa > Add**.
3. Teclee adentro esta información y haga clic la **AUTORIZACIÓN** para acabar la configuración.



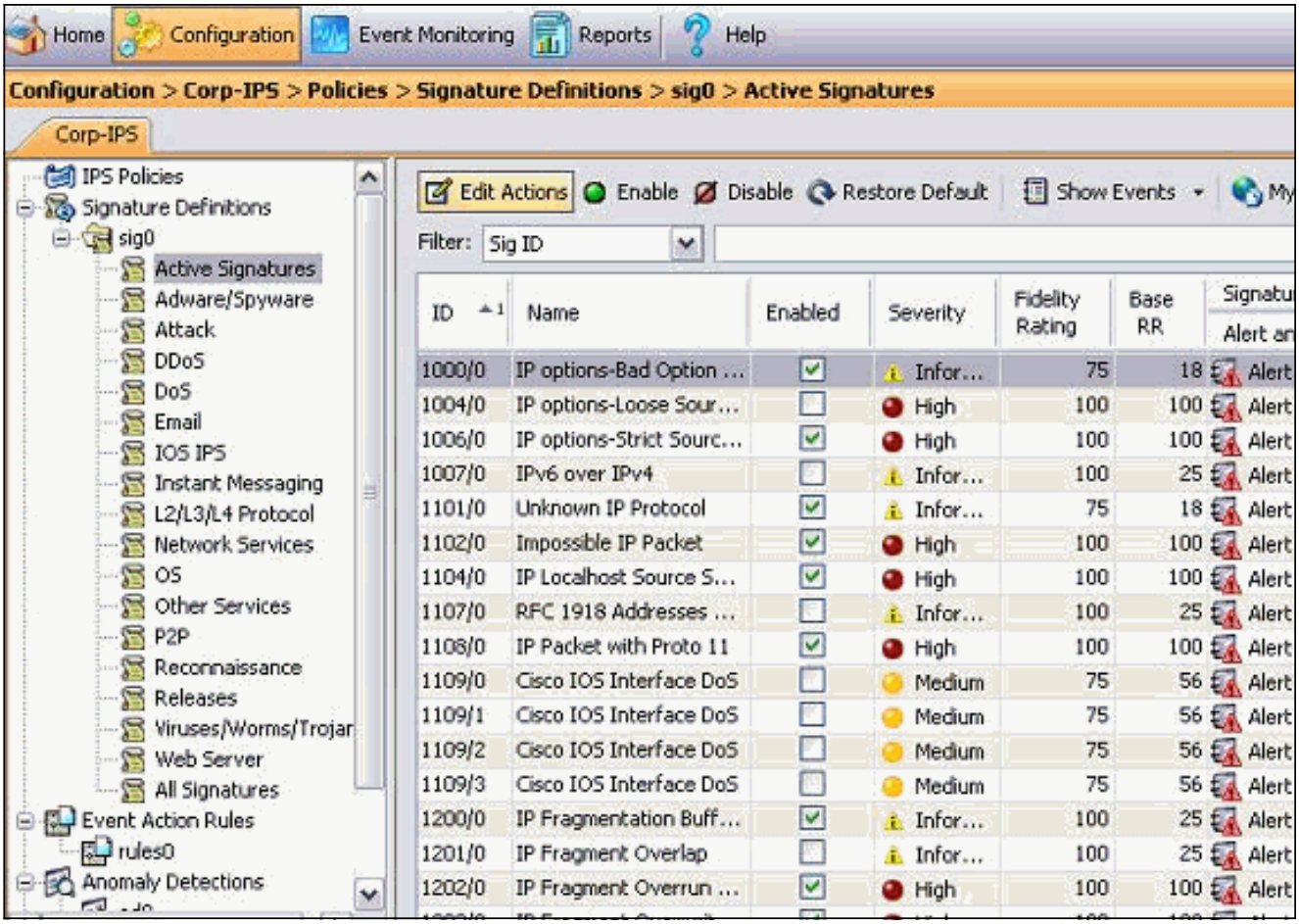
4. Elija los **dispositivos > sensor5** para verificar el estado del sensor y después hacer clic con el botón derecho del ratón para elegir el **estatus**.Aseegurese que usted puede ver la *suscripción abierta con éxito.*
mensaje.



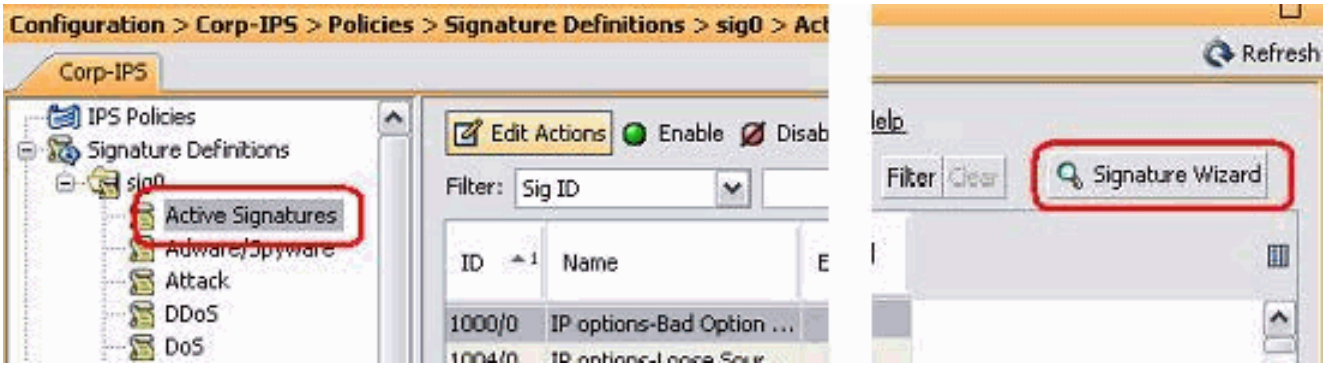
Configuración que bloquea para el router del Cisco IOS

Complete estos pasos para configurar el bloqueo para la ruta 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:

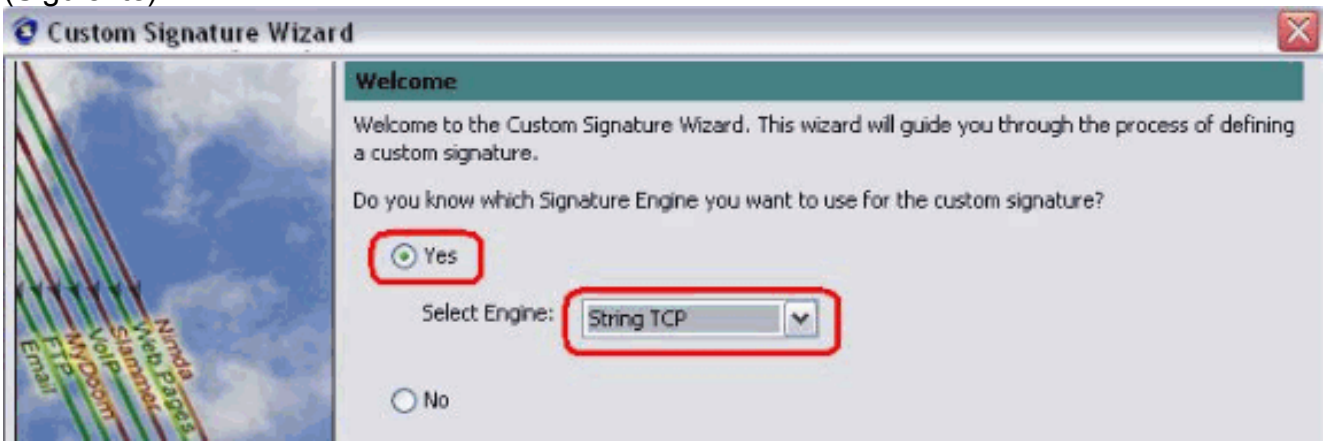


4. De la ficha de configuración, haga clic las **firmas activas**.
5. Entonces, **Asistente de firmas del** tecleo.

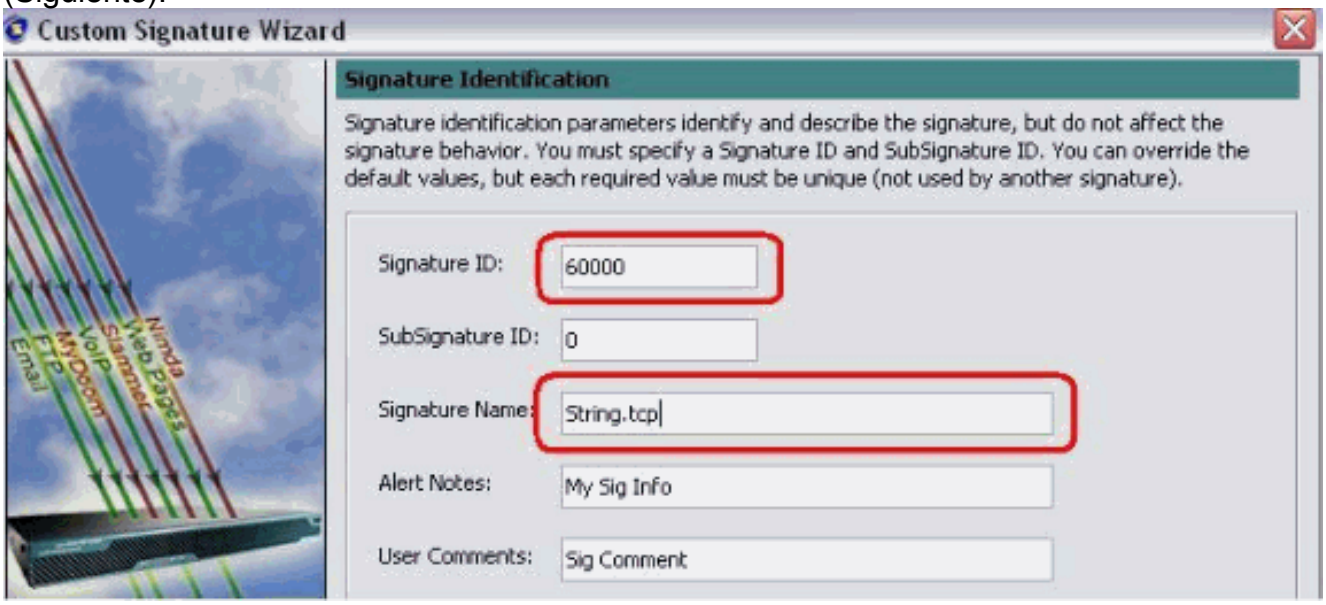


Nota: El tiro de pantalla anterior se ha cortado en dos porciones debido a la limitación de espacio.

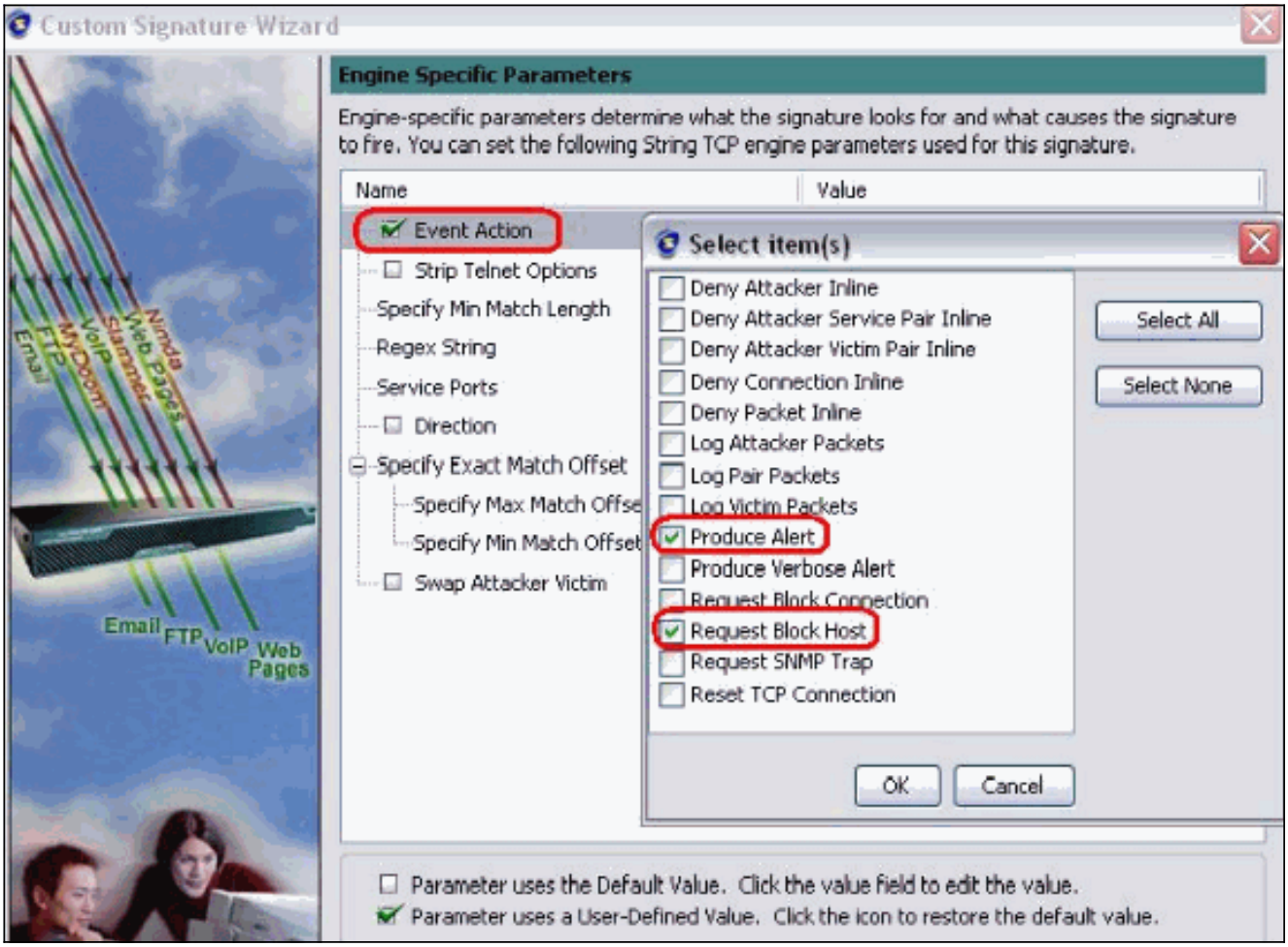
6. Elija **sí** y **ate el TCP** como motor de firma. Haga clic en Next (Siguiente).



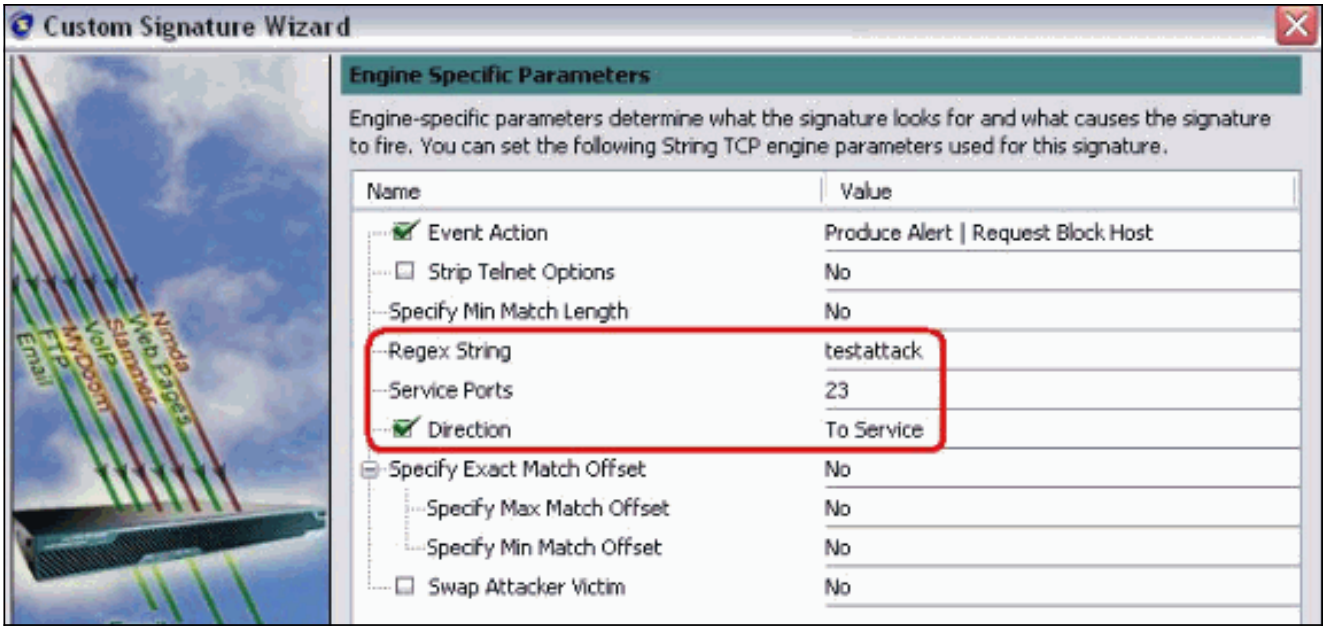
7. Usted puede dejar esta información como valor por defecto o ingresar su propio ID de la firma, nombre de la firma y notas del usuario. Haga clic en Next (Siguiente).



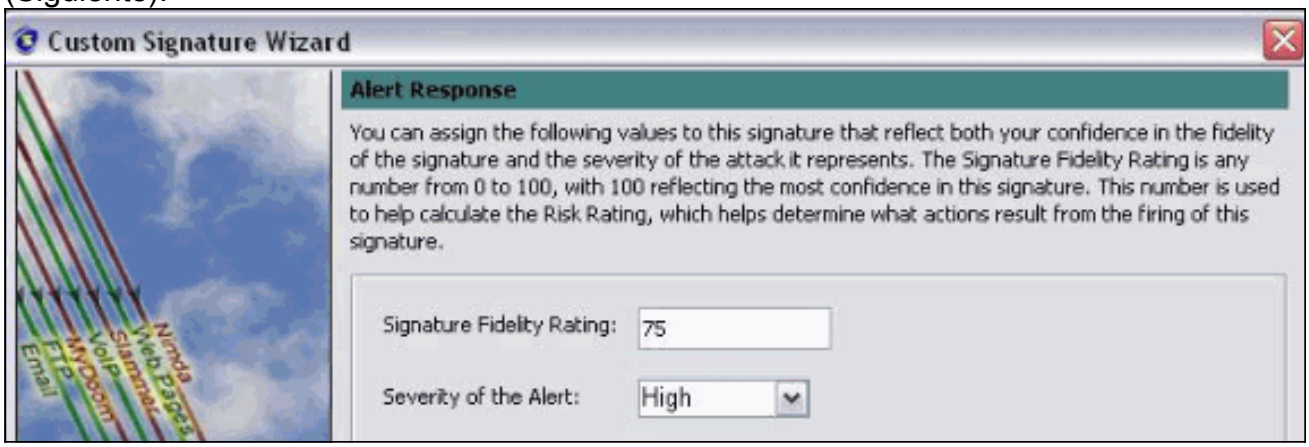
8. Elija la **acción del evento** y elija la **alerta de la producción** y el **host del bloque de petición**. Haga clic **después** para continuar.



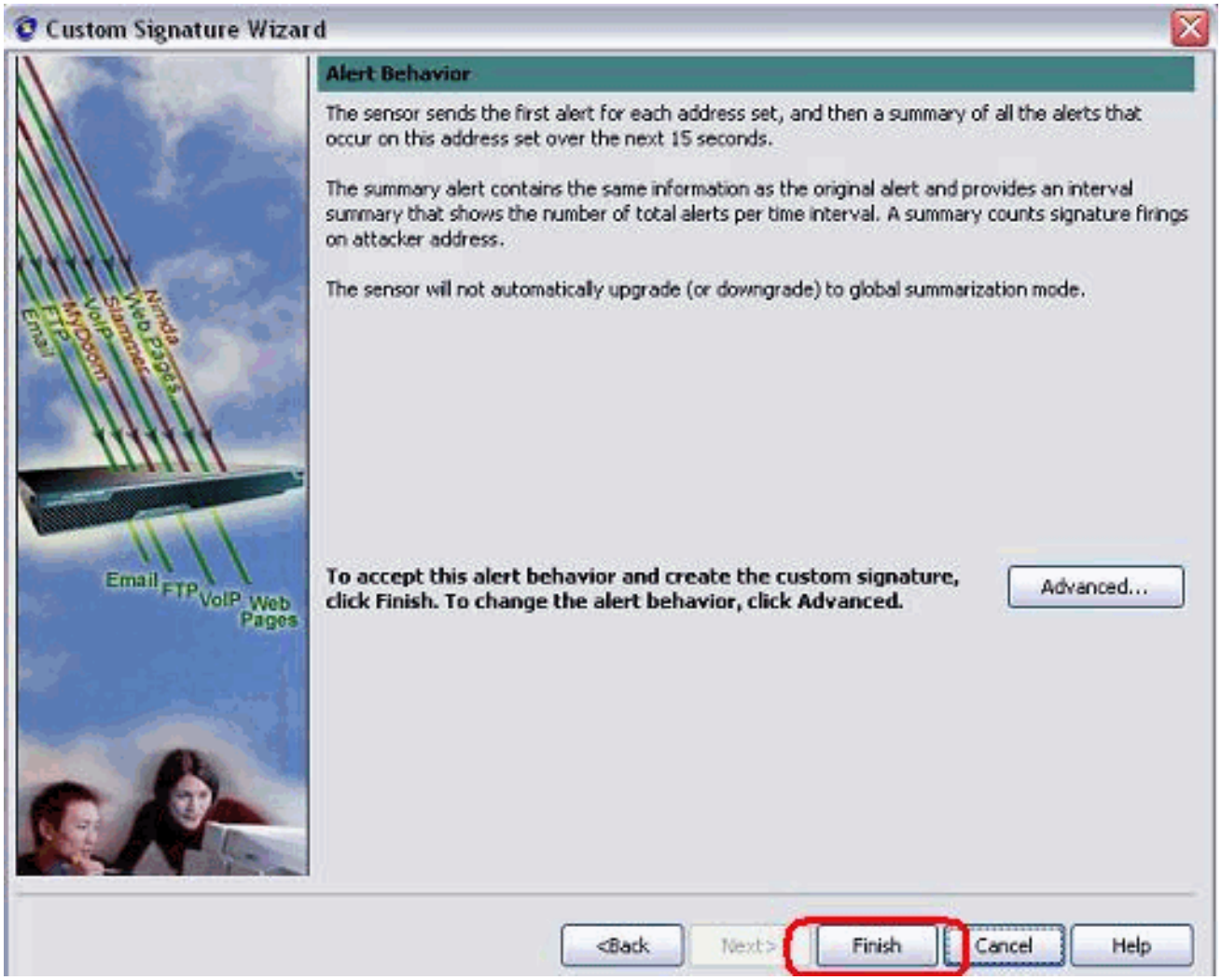
9. Ingrese una expresión normal, que en este ejemplo es *testattack*, ingresan **23** para los puertos del servicio, eligen **mantener** para la dirección, y el tecleo **después** para continuar.



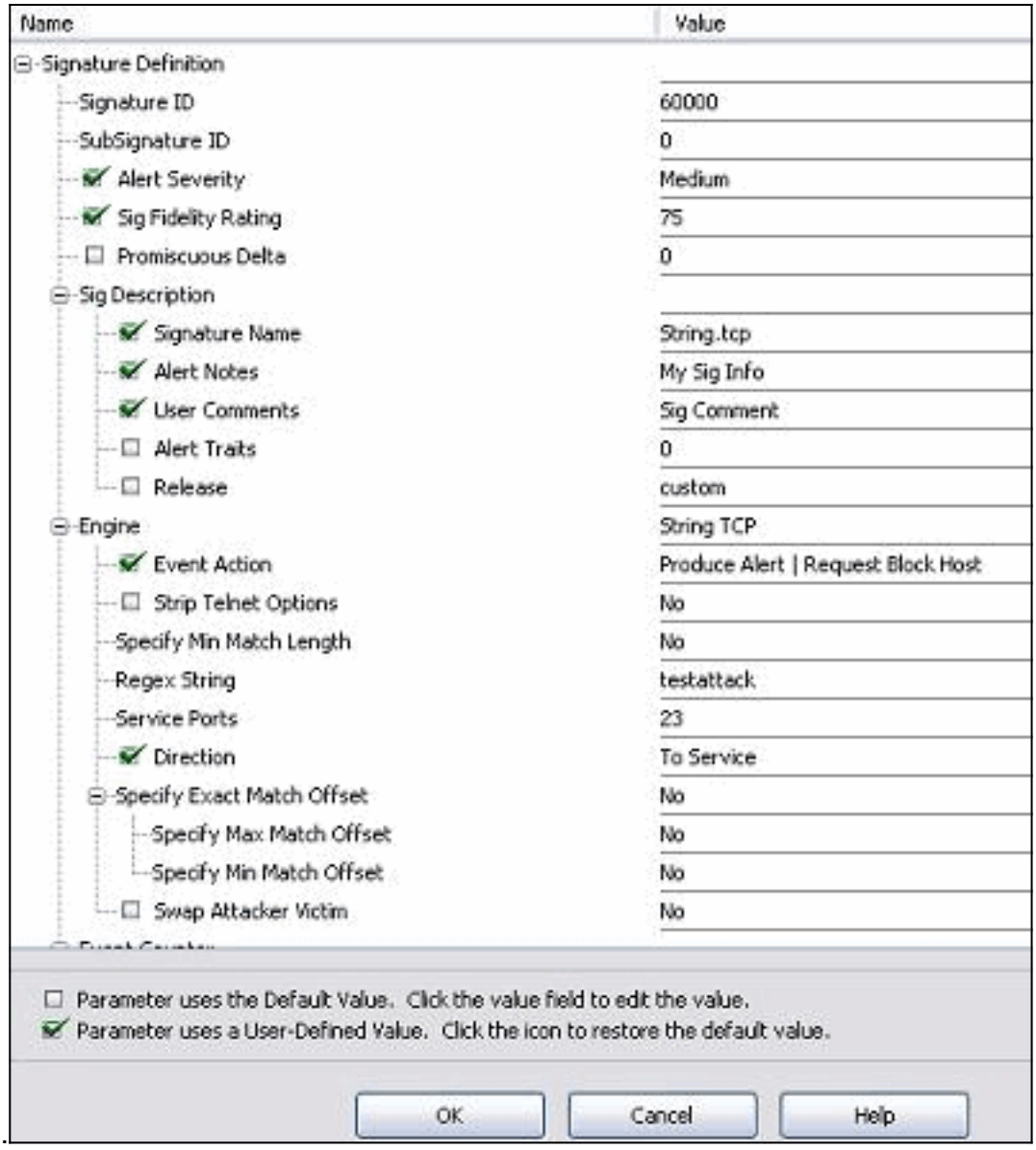
10. Usted puede dejar esta información como valor por defecto. Haga clic en Next (Siguiente).



11. Clic en Finalizar para acabar al Asisitente.

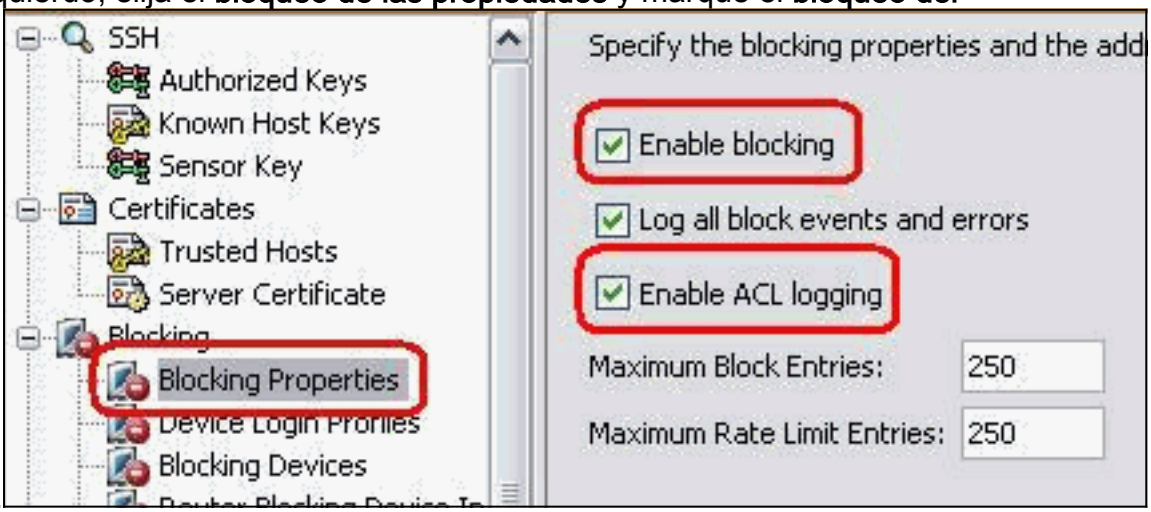


12. Elija la **configuración > sig0 > las firmas activas** en la orden localizan la firma creada recientemente por los **Sig ID** o el **nombre de los Sig**. El tecleo **edita** para ver la



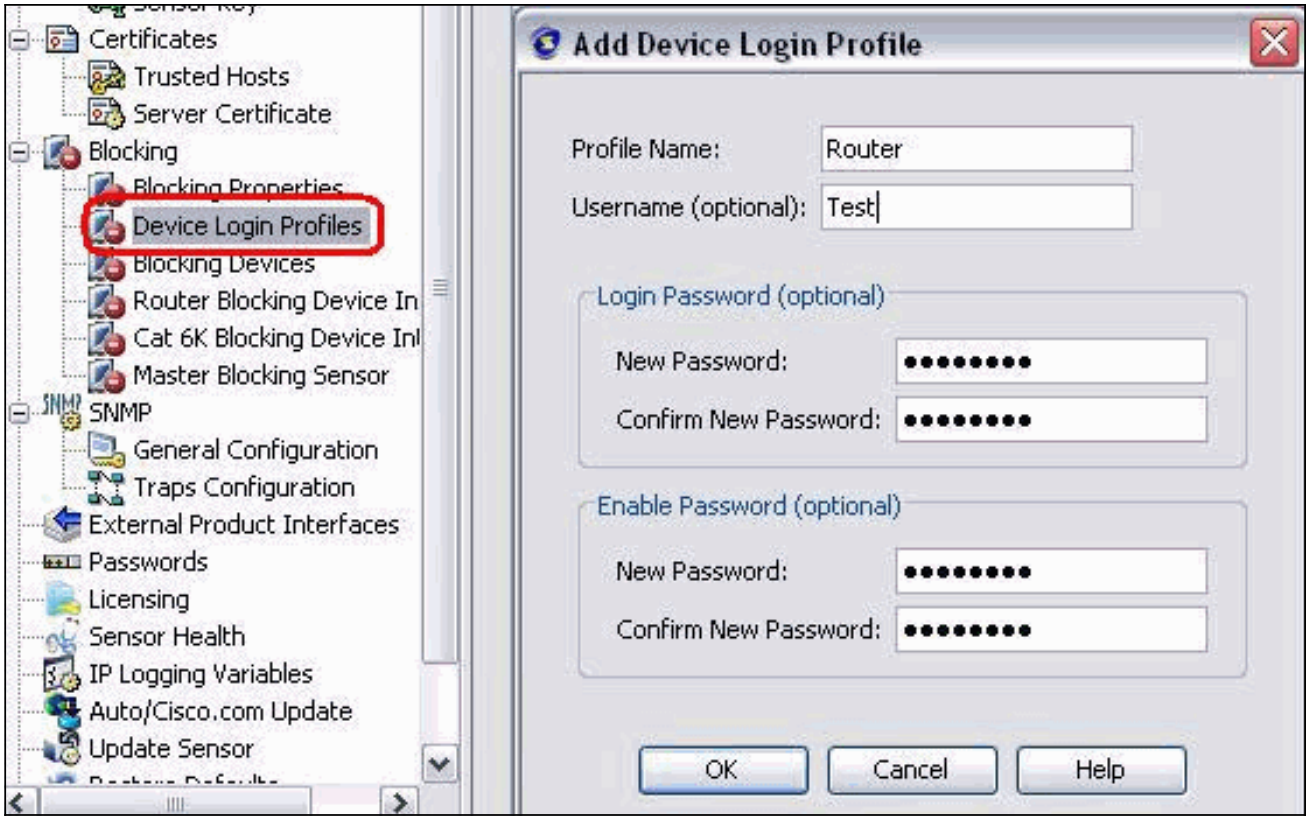
firma.

13. Haga Click en OK después de que usted confirme y haga clic el **botón Apply Button** para aplicar la firma al sensor.
14. De la ficha de configuración, bajo **bloqueo del** tecleo de la Administración del sensor. Del panel izquierdo, elija el **bloqueo de las propiedades** y marque el **bloqueo del**

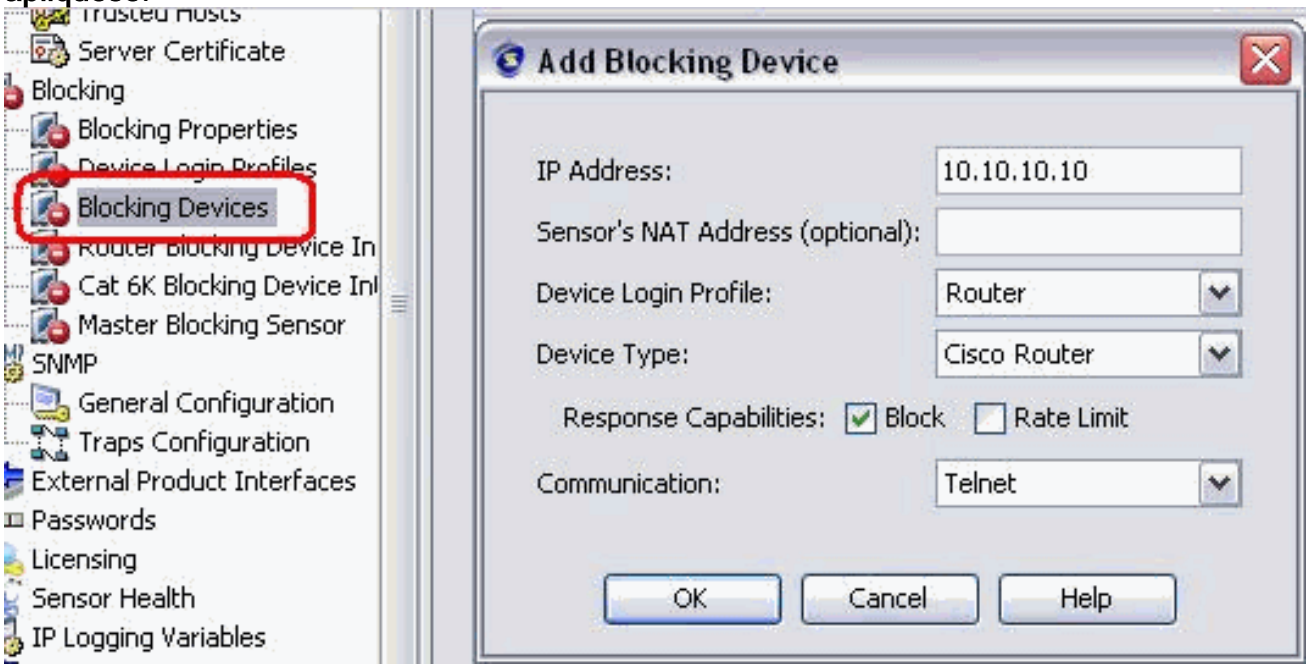


permiso.

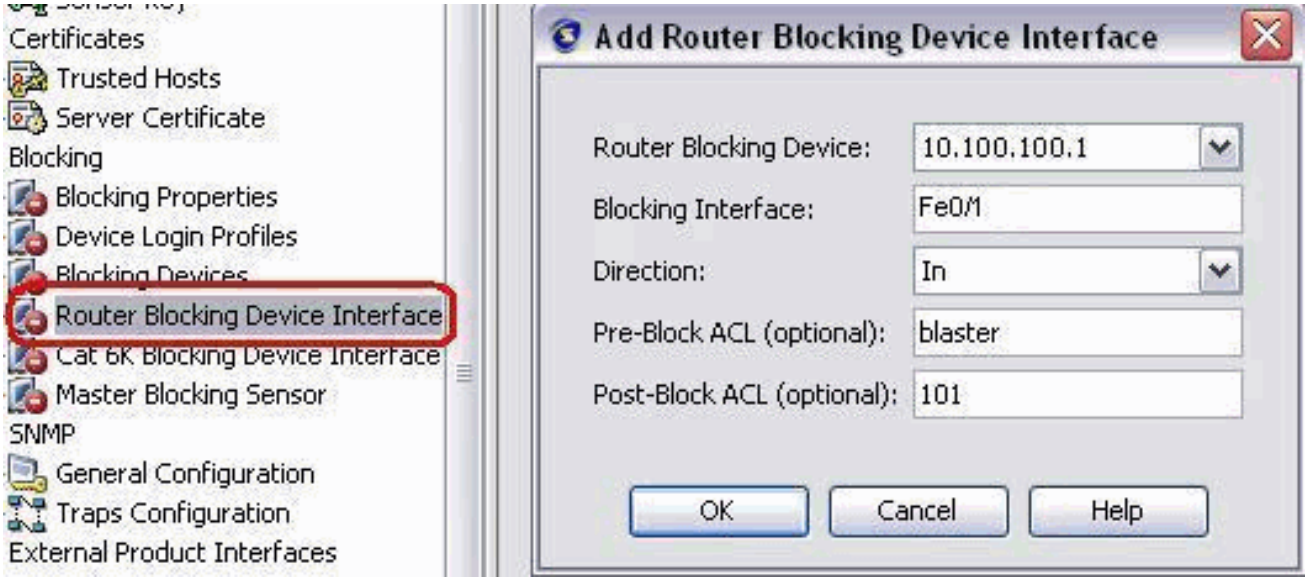
15. Ahora del panel izquierdo, vaya al **perfil del login del dispositivo**. Para crear un nuevo perfil, haga click en Add **La AUTORIZACIÓN** una vez creada del tecleo y **aplica** para el sensor y continúa.



16. El siguiente paso es configurar al router como dispositivo de bloqueo. Del panel izquierdo, elija el **dispositivo de bloqueo**, tecleo **agregan** para agregar esta información. Después haga clic la **AUTORIZACIÓN** y **apliqúese**.



17. Ahora de la configuración del panel izquierdo las interfaces de dispositivo de bloqueo. Agregue la información, haga clic la **AUTORIZACIÓN** y **apliqúese**.



Verificación

Ponga en marcha el ataque y el bloqueo

Complete estos pasos para poner en marcha el ataque y el bloqueo:

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. Telnet a la Casa del router y verifica la comunicación del servidor con estos comandos.`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. Desde el router Light, realice una conexión Telnet al router House y escriba 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 lost] !--- Host 10.100.100.2 has been blocked due to the !--- signature "testattack" triggered.`
4. Telnet a la Casa del router y utiliza el **comando show access-list** como se muestra aquí.`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. Del panel del IDS Event Viewer, la alarma roja aparece una vez que se inicia el ataque.

Troubleshooting

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

Consejos

Utilice estos consejos de Troubleshooting:

- Del sensor mire el **acceso a la red de las estadísticas de la demostración** hecho salir y aseegurese que el `estado` " es activo. De la consola o de SSH al sensor, se ve esta información:`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#`
- Aseegurese el parámetro de comunicación muestra que el protocolo correcto está utilizado por ejemplo Telnet o SSH con el 3DES. Usted puede intentar SSH manual o Telnet de un cliente SSH/Telnet en un PC para marcar las credenciales del nombre de usuario y contraseña está correcto. Entonces el intento a Telnet o SSH del sensor sí mismo al router y considera si usted puede iniciar sesión con éxito al router.

Información Relacionada

- Página de soporte segura de la prevención de intrusiones de Cisco
- Soporte Técnico y Documentación - Cisco Systems