Configurando o IPS que obstrui usando IME

Índice

Introdução

Este documento discute a configuração do Intrusion Prevention System (IPS) que obstrui com o uso do gerente IPS expresso (IME). Os sensores IME e IPS são usados para controlar um roteador Cisco para obstruir. Recorde estes artigos quando você considera esta configuração:

- Instale o sensor e certifique-se dos trabalhos do sensor corretamente.
- Faça com que a interface de monitoramento se estenda até o roteador fora da interface.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- O gerente do ips Cisco expressa 7.0
- Sensor 7.0(0.88)E3 do ips Cisco

- Roteador do ® do Cisco IOS com Cisco IOS Software Release 12.4

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

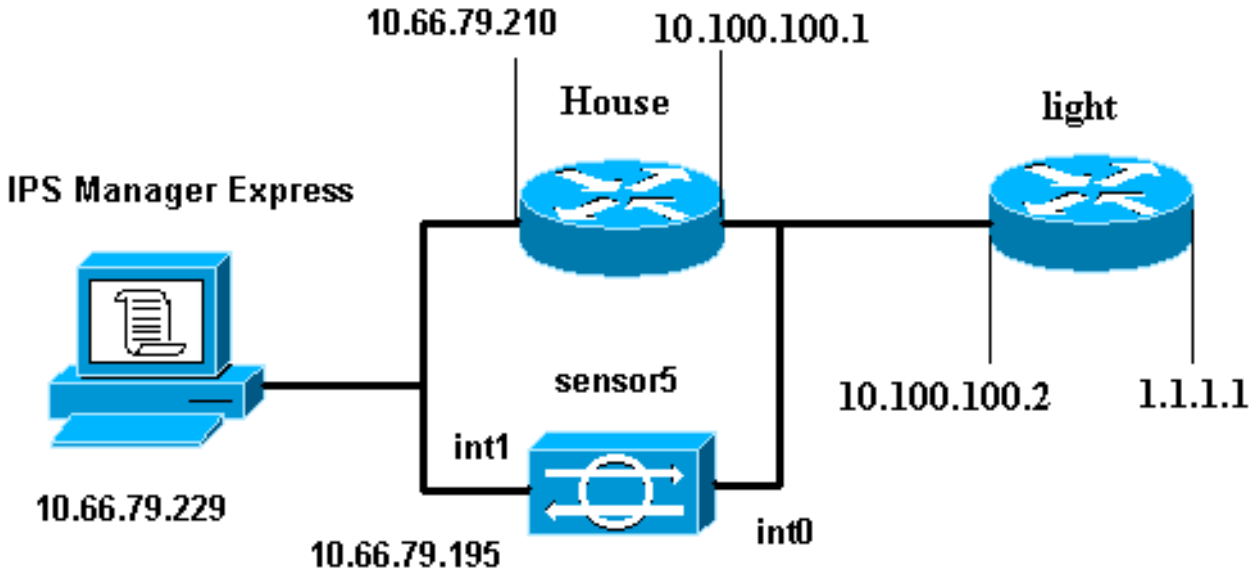
Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede.



Configurações

Este documento utiliza estas configurações.

- Luz do Roteador
- Companhia do Roteador

Luz do Roteador

```
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
```

Companhia do Roteador

```
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
```

Comece a configuração de sensor

Termine estas etapas para começar a configuração do sensor.

1. Se essa for a primeira vez que você efetua logon no Sensor, digite cisco como o nome de usuário e cisco como a senha.
2. Quando o sistema solicitar, altere a senha.**Nota:** O cisco123 é uma palavra do dicionário e não é permitido no sistema.
3. Datilografe a **instalação** e siga a alerta do sistema para setup os parâmetros básicos para os sensores.
4. Insira esta informação:`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
```

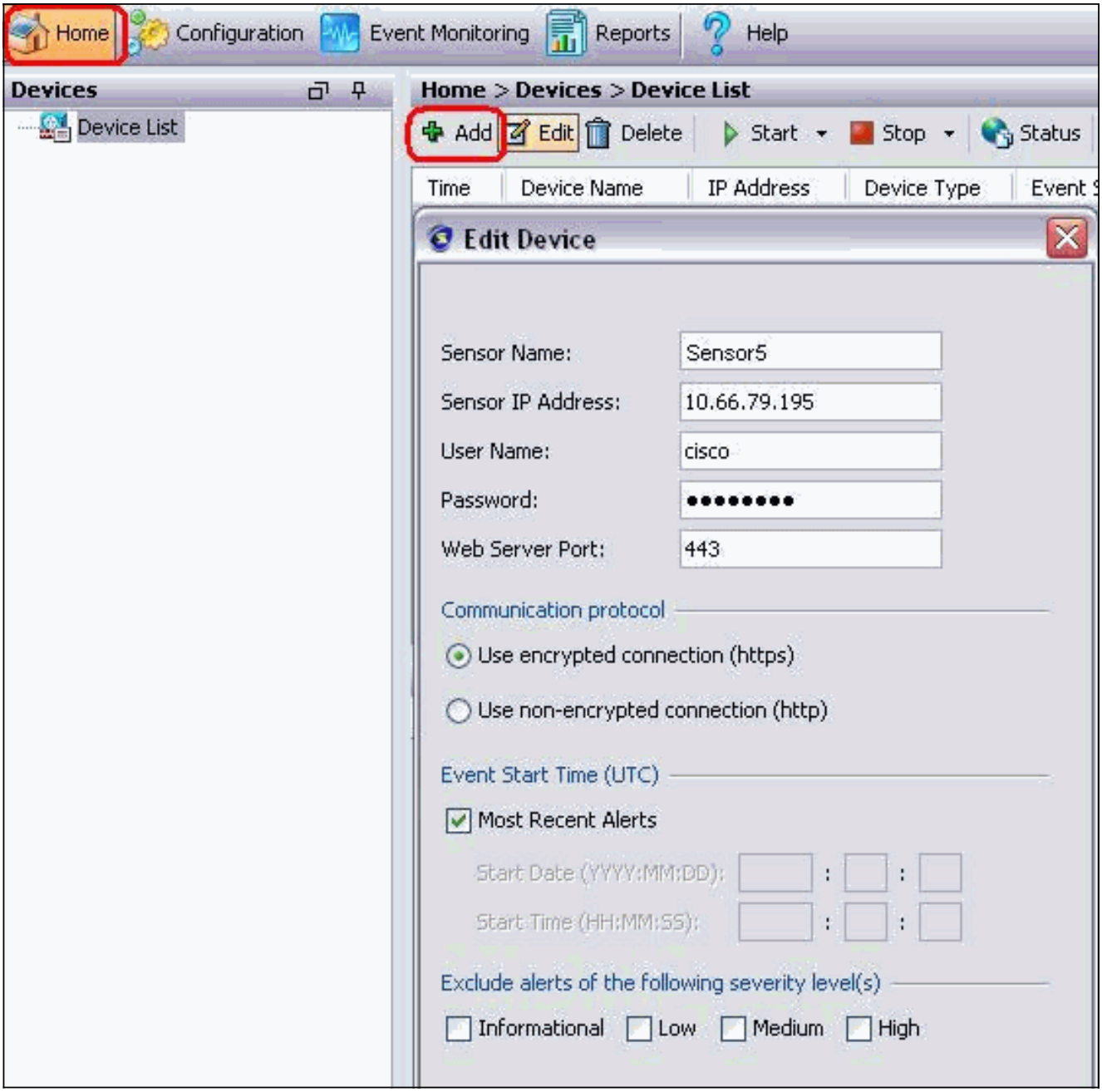
5. Salve a configuração.Pode tomar alguns minutos para que o sensor salvar a configuração.
```
[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.

Enter your selection[2]: 2
```

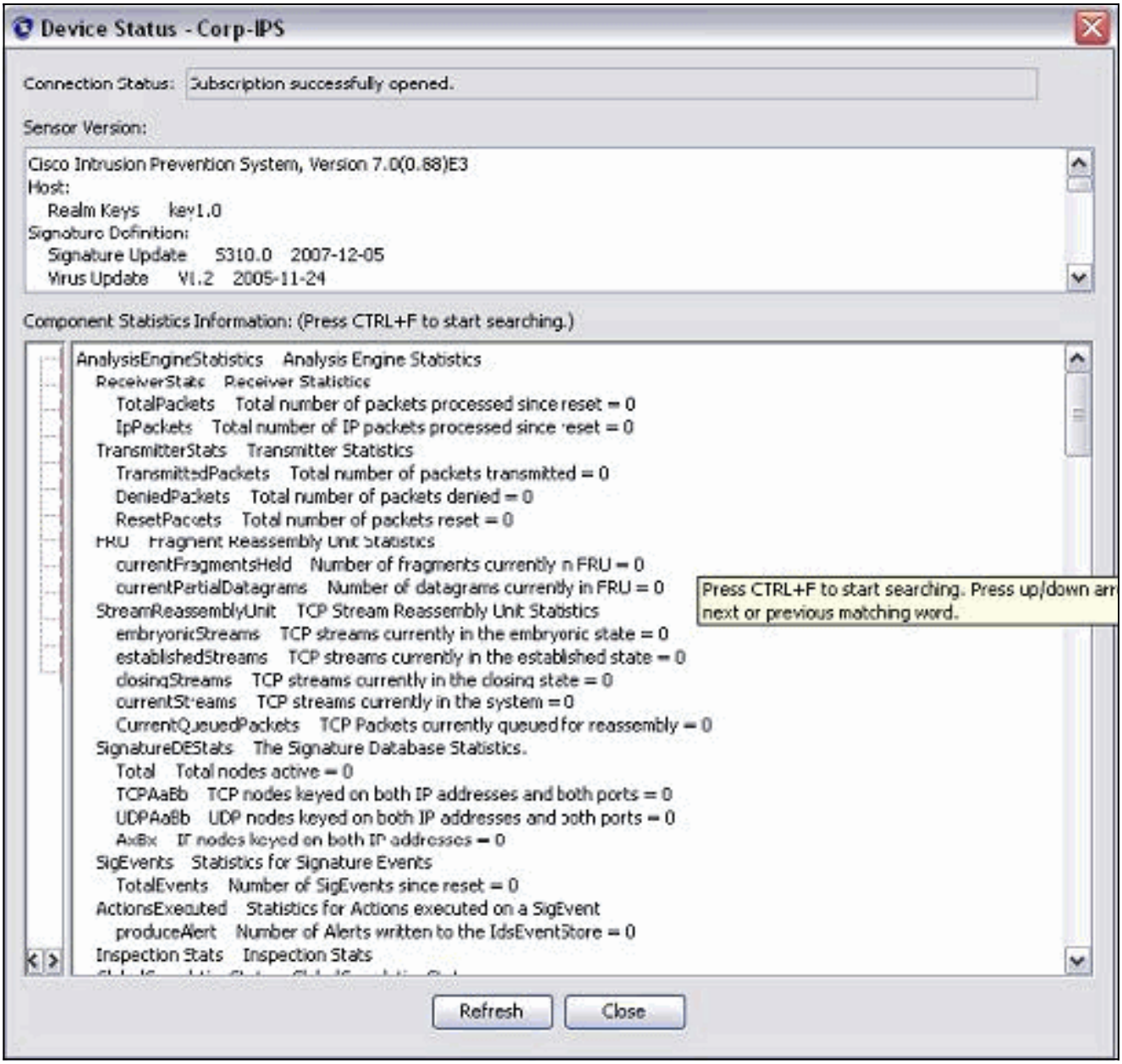
Adicionar o sensor no IME

Termine estas etapas a fim adicionar o sensor no IME.

1. Vá ao PC Windows, que instalaram o gerente IPS expresso e abrem o **gerente IPS expresso**.
2. Escolha o **> Add home**.
3. Datilografe dentro esta informação e clique a **APROVAÇÃO** a fim terminar a configuração.



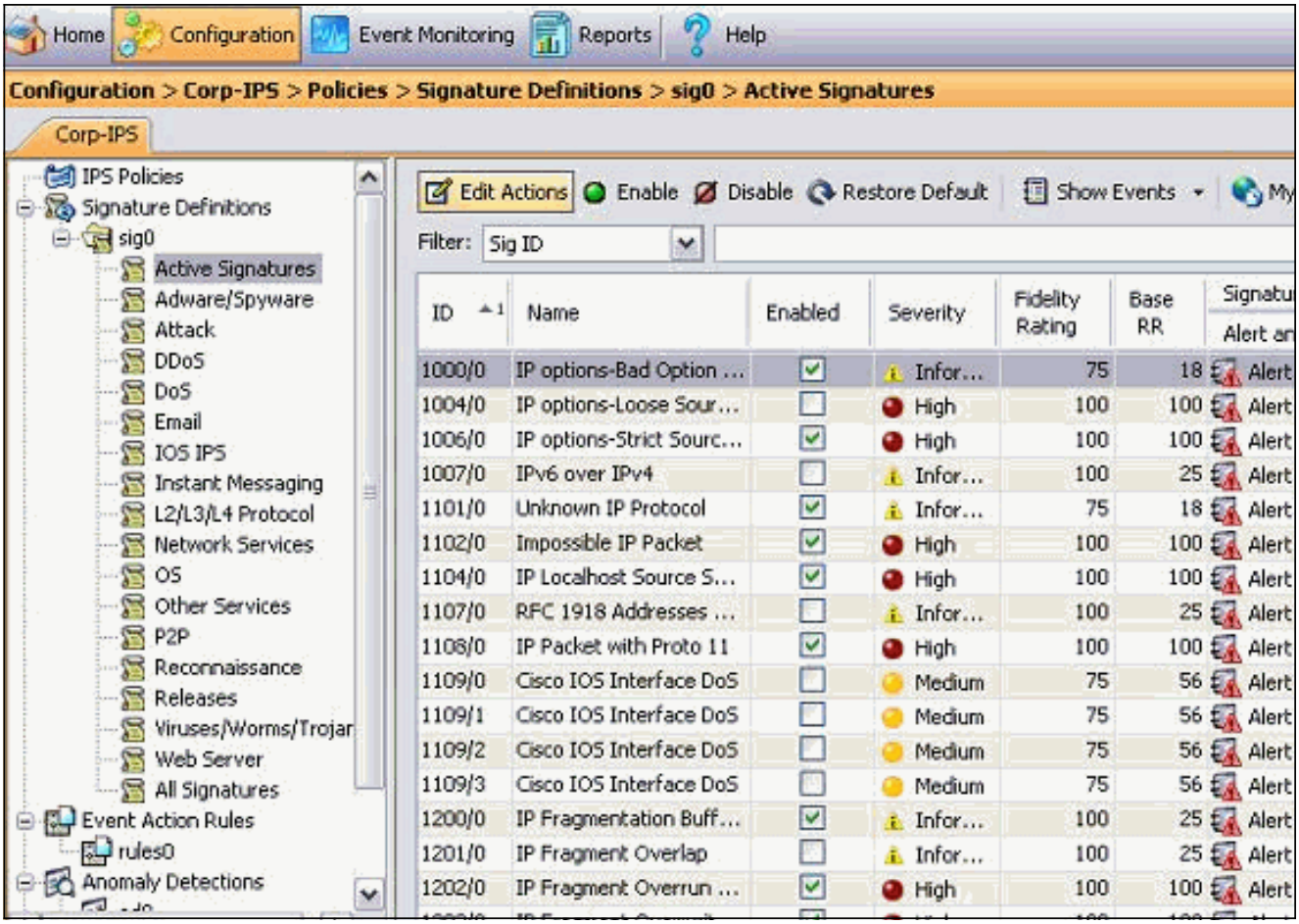
4. Escolha **dispositivos > sensor5** a fim verificar o Status do sensor e clicar com o botão direito então para escolher o **estado**.Certifique-se de que você pode ver a *assinatura aberta com sucesso.*
mensagem.



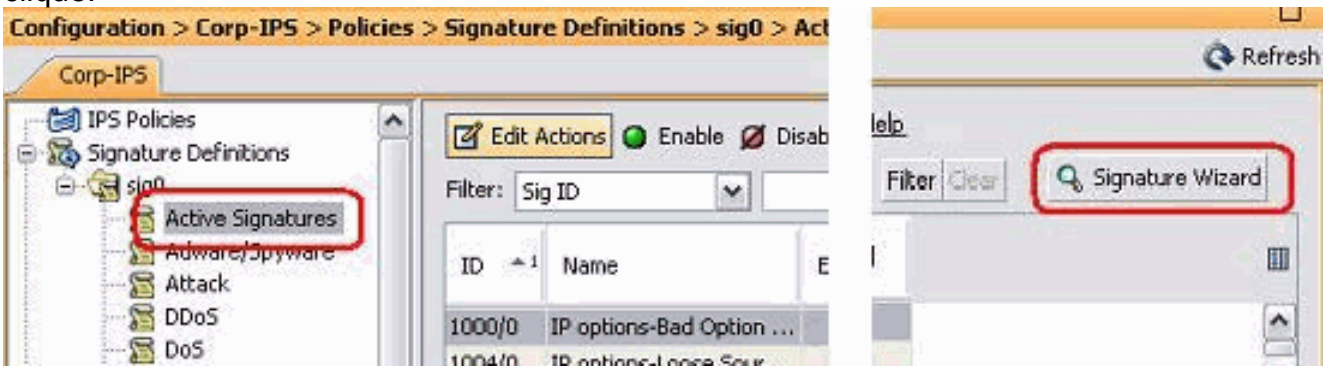
Configurar a obstrução para o roteador do Cisco IOS

Termine estas etapas a fim configurar a obstrução para a rota do Cisco IOS:.

1. Do IME PC, abra seu navegador da Web e vá a **https://10.66.79.195**.
2. Clique a **APROVAÇÃO** a fim aceitar o certificado HTTPS transferido do sensor.
3. Na janela Login, insira cisco como o nome de usuário e 123cisco123 como a senha.Esta interface de gerenciamento IME
   aparece:

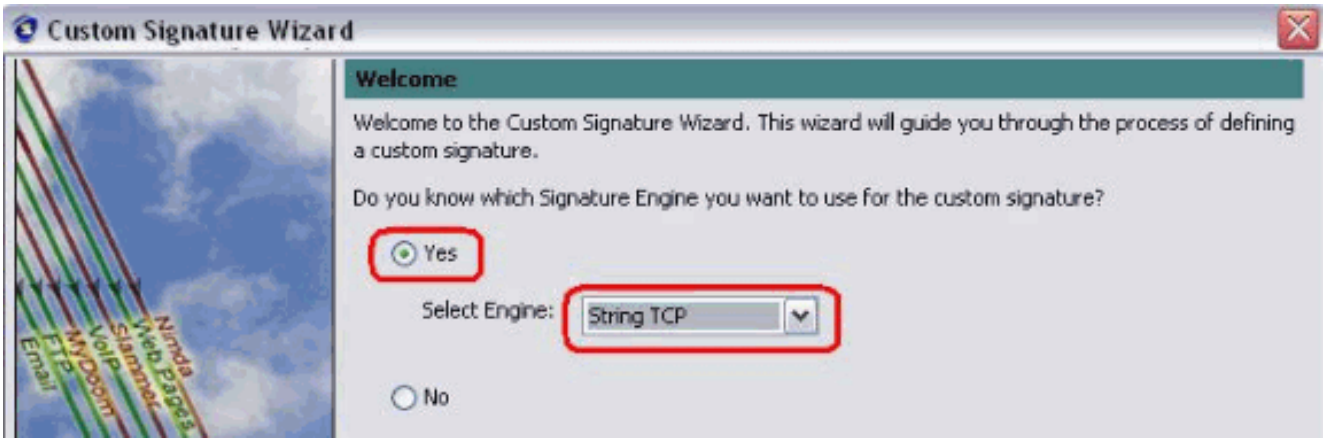


4. Do guia de configuração, clique **assinaturas ativas**.
5. Então, **Wizard de Assinatura do**
   clique.



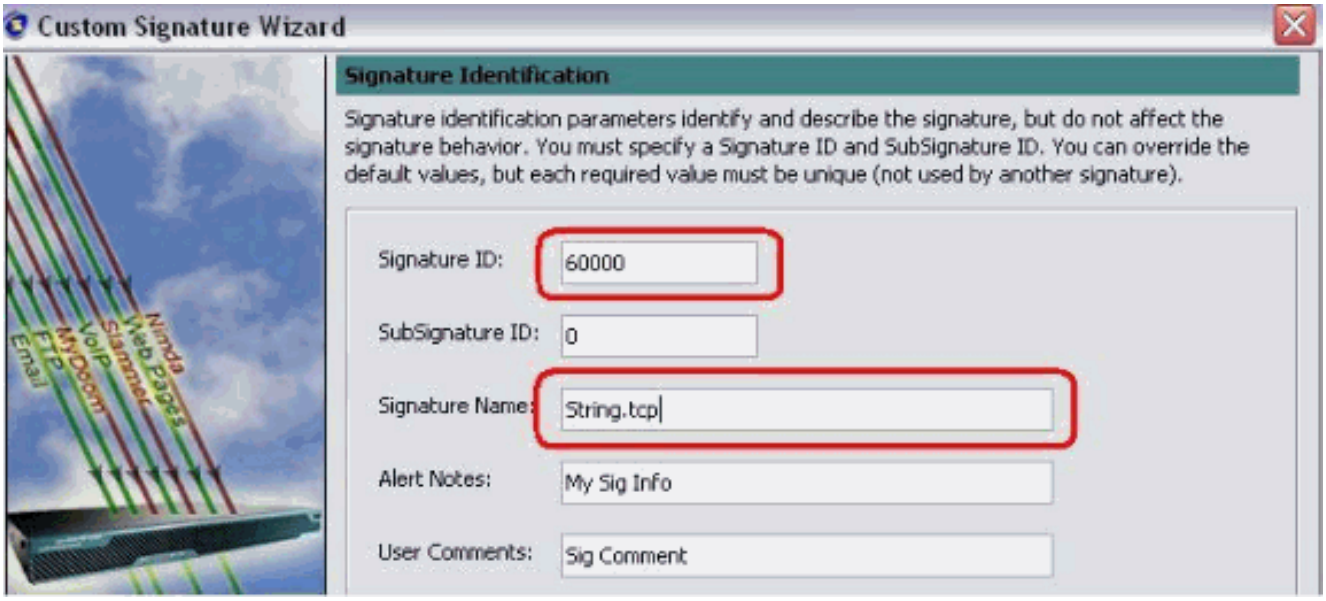
Nota: O tiro de tela precedente foi cortado em duas porções devido à limitação de espaço.

6. Escolha **sim** e **amarre o TCP** como o Engine de assinatura. Clique em
   Next.

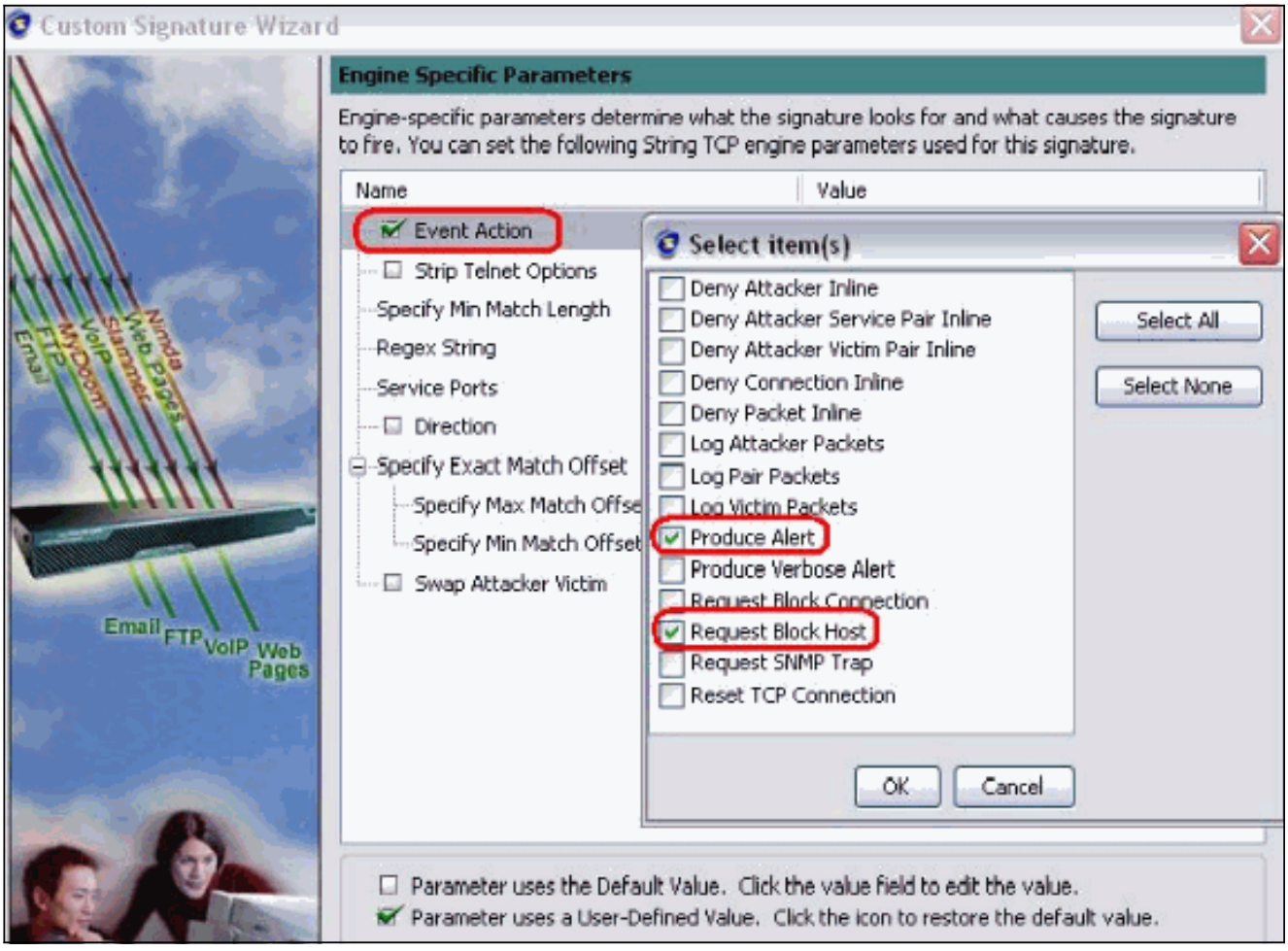


7. Você pode deixar esta informação como o padrão ou incorporar seus próprios ID de

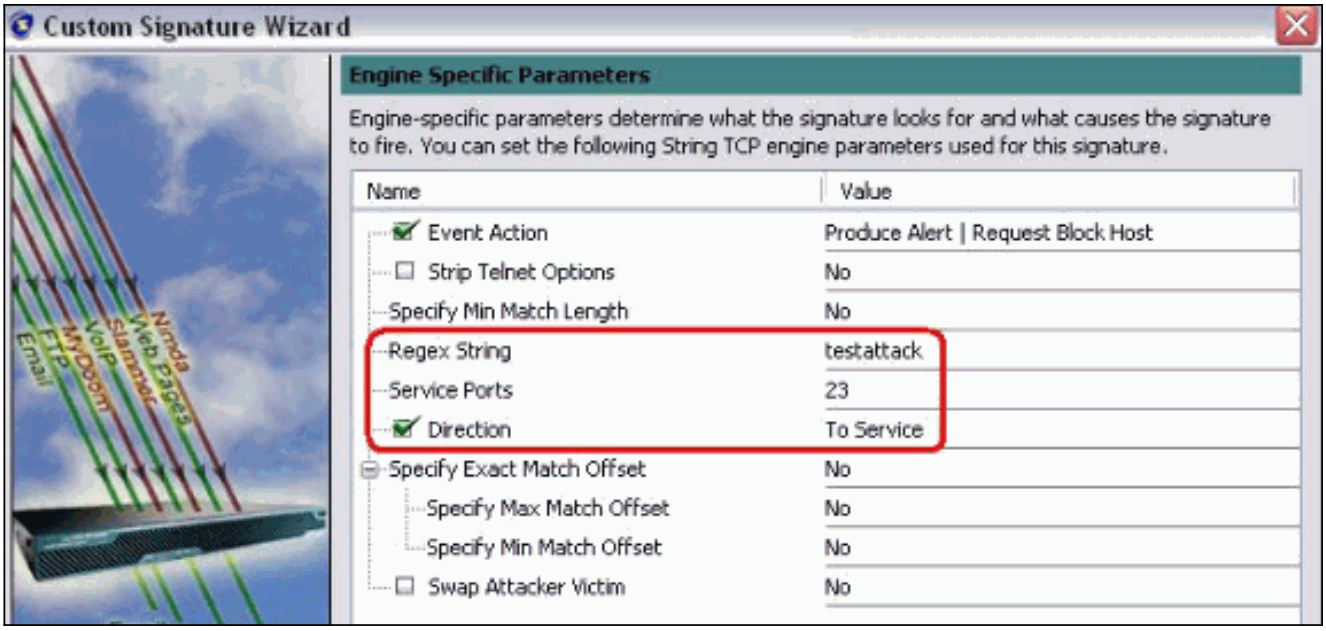
assinatura, nome da assinatura e notas do usuário. Clique em
Next.



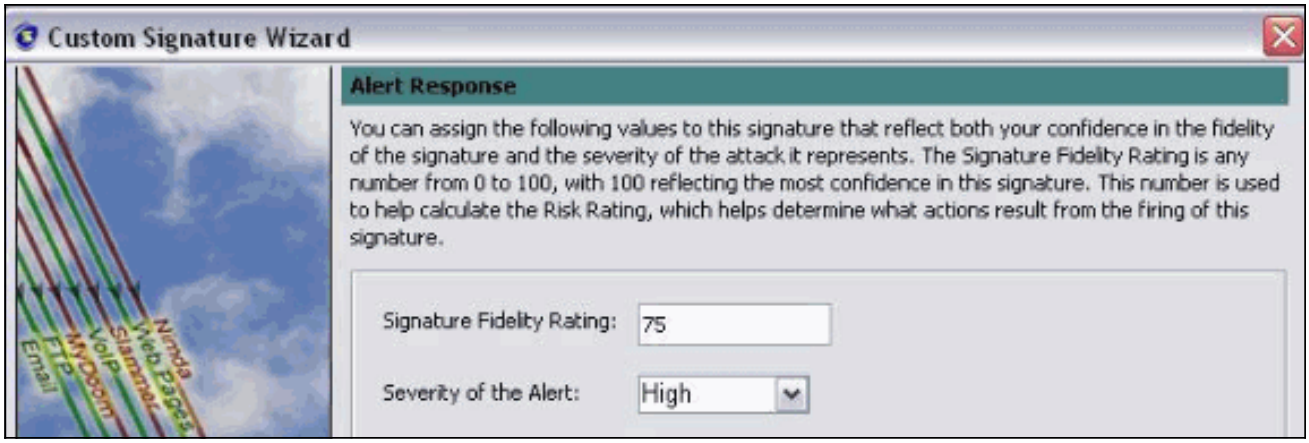
8. Escolha a **ação do evento** e escolha o **alerta do produto** e o **host do bloco de pedido**. Clique **em seguida** a fim
continuar.



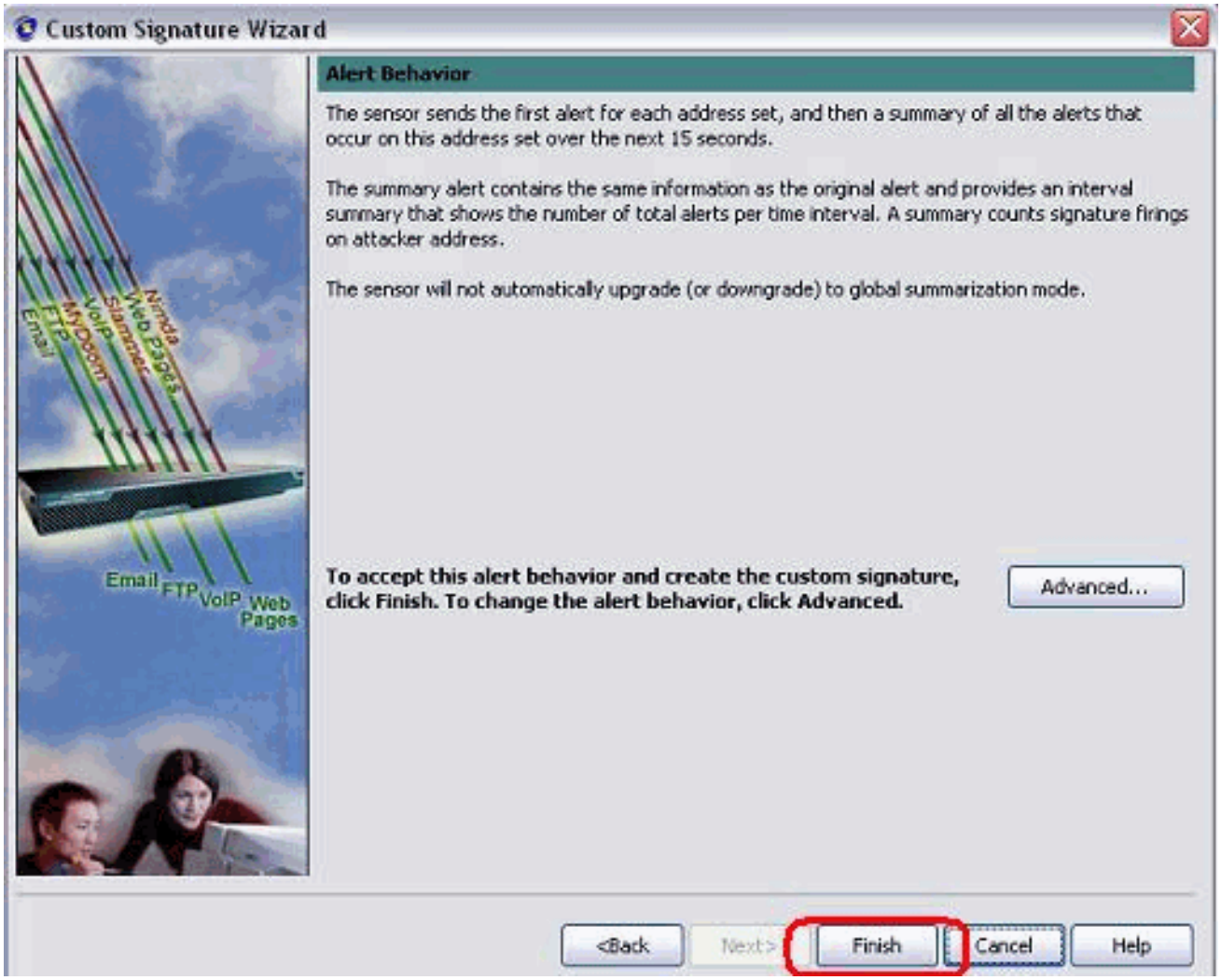
9. Incorpore uma expressão regular, que neste exemplo seja *ataque de teste*, incorporam **23** para portas do serviço, escolhem-nos **prestar serviços de manutenção em seguida** para o sentido, e o clique a fim
continuar.



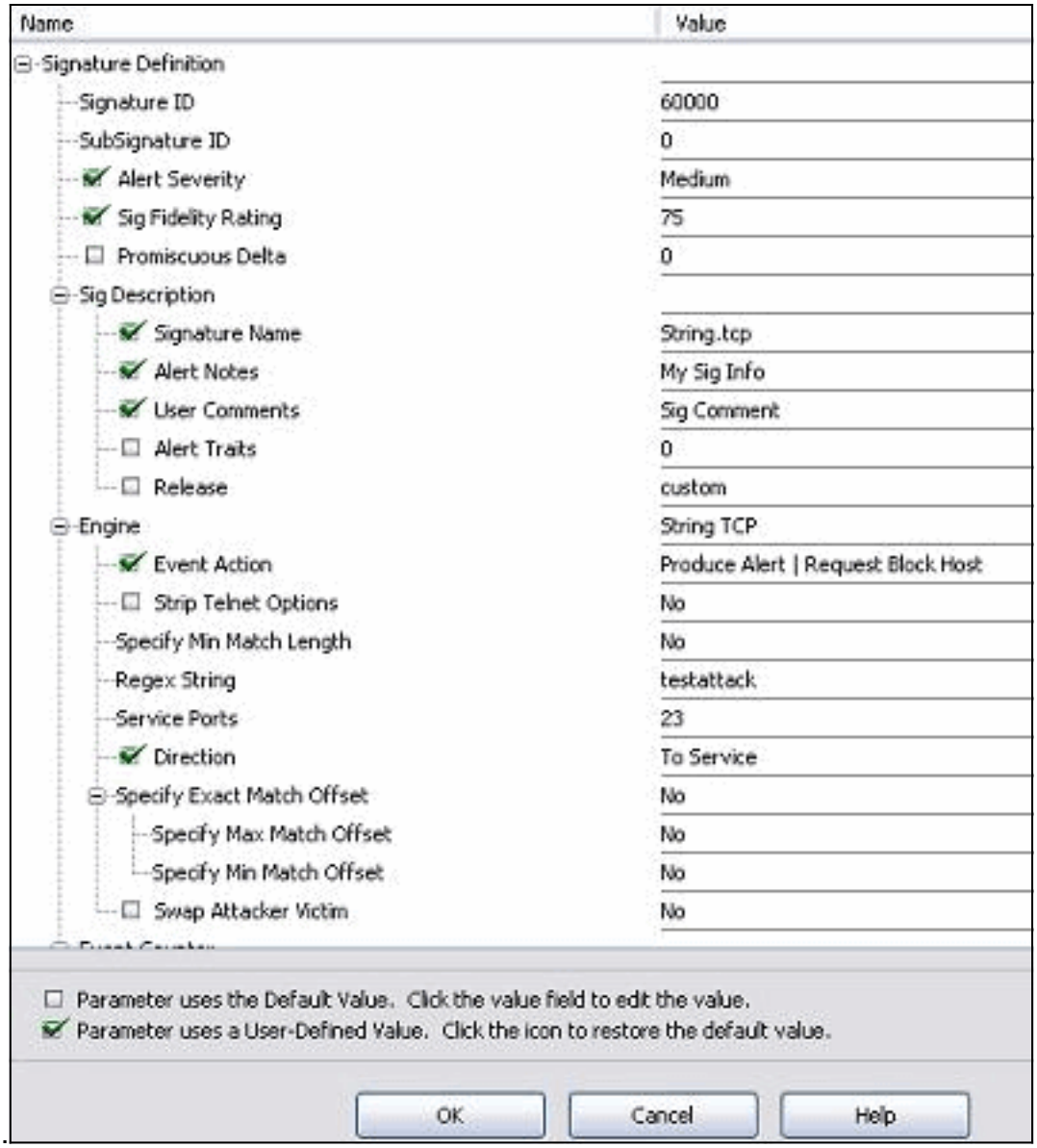
10. Você pode deixar esta informação como o padrão. Clique em Next.



11. **Revestimento do** clique a fim terminar o assistente.

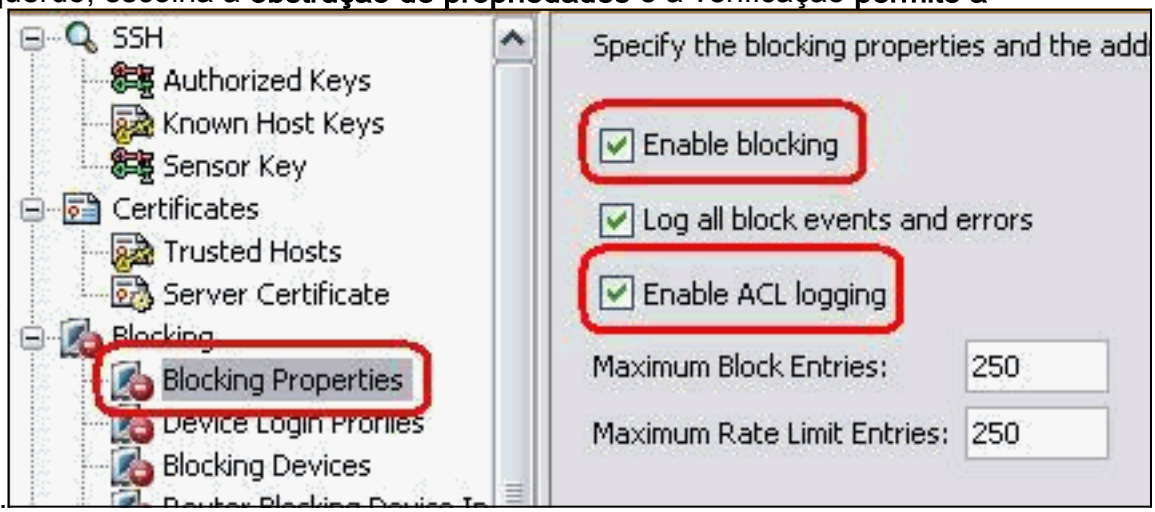


12. Escolha a **configuração > o sig0 > assinaturas ativas** em ordem encontram a assinatura recém-criado pelos **Sig ID** ou pelo **nome dos Sig**. O clique **edita** a fim ver a



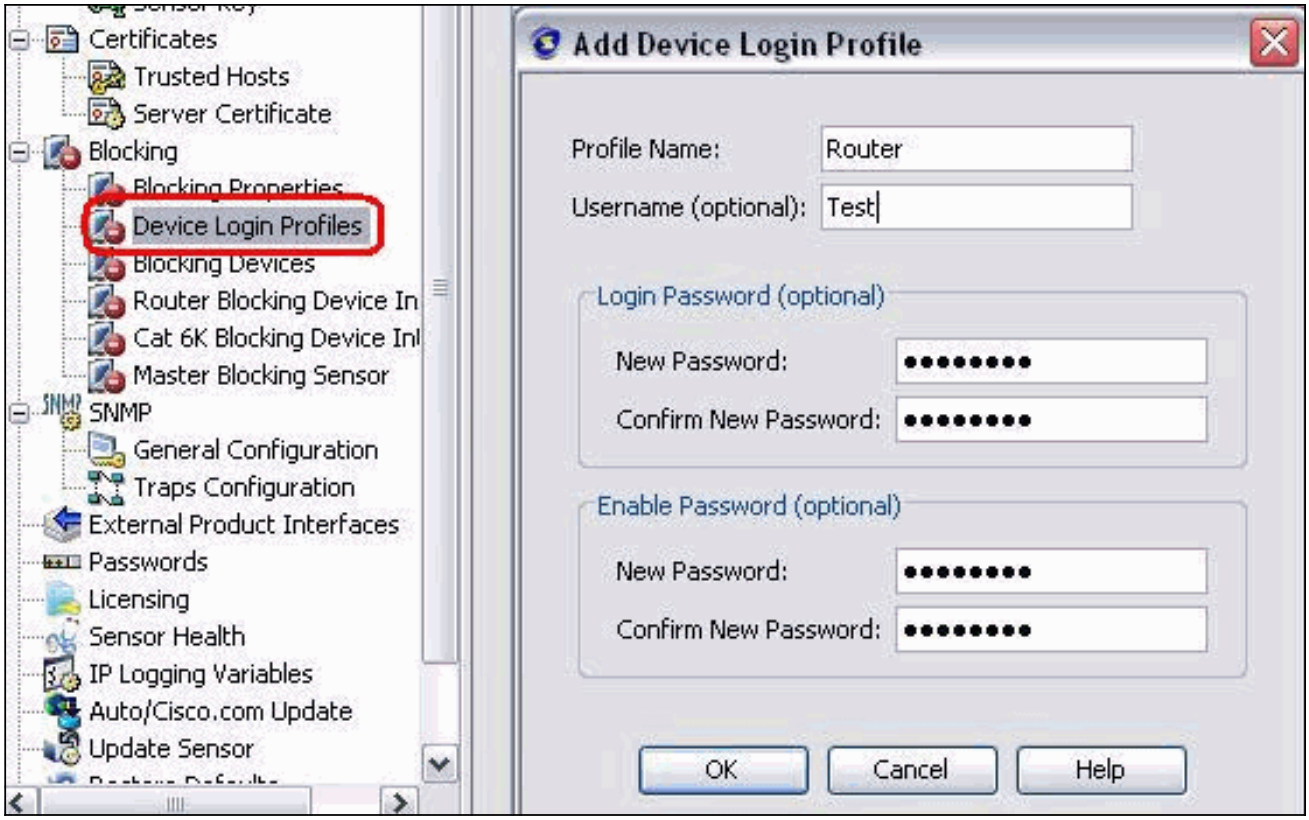
assinatura.

13. Clique a **APROVAÇÃO** depois que você confirma e clica o **botão Apply Button** a fim aplicar a assinatura ao sensor.
14. Do guia de configuração, sob a **obstrução do** clique do Gerenciamento do sensor. Do painel esquerdo, escolha a **obstrução de propriedades** e a verificação **permite a**

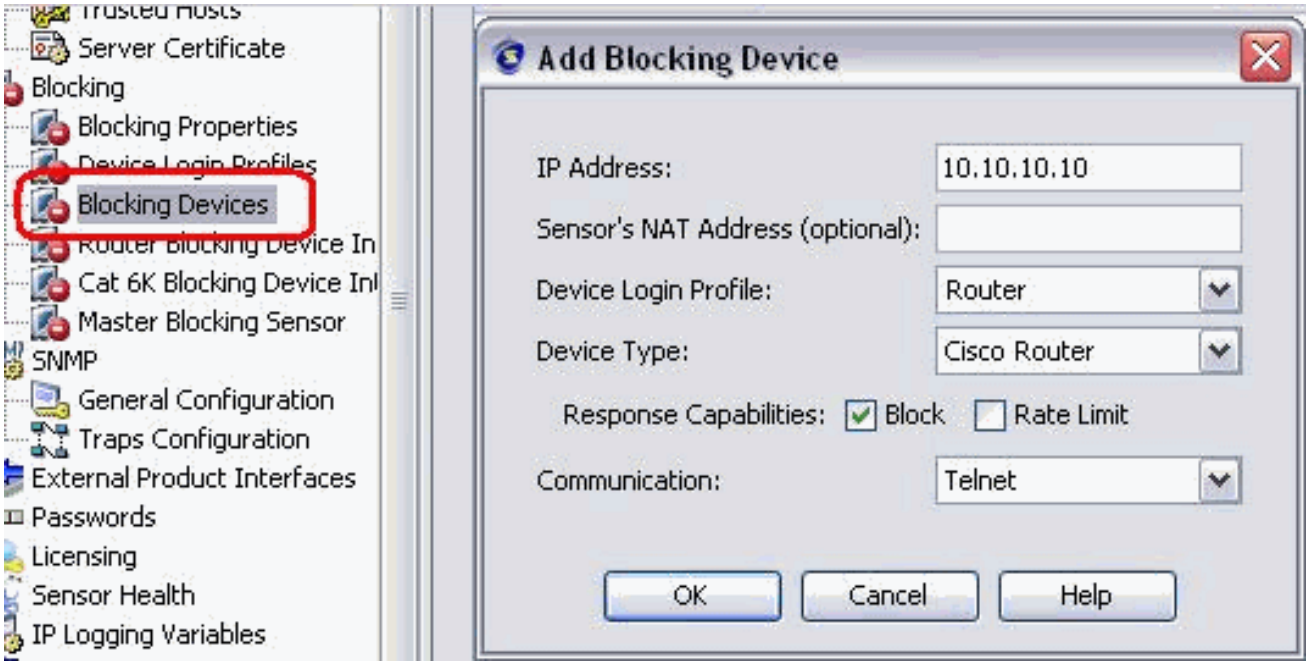


obstrução.

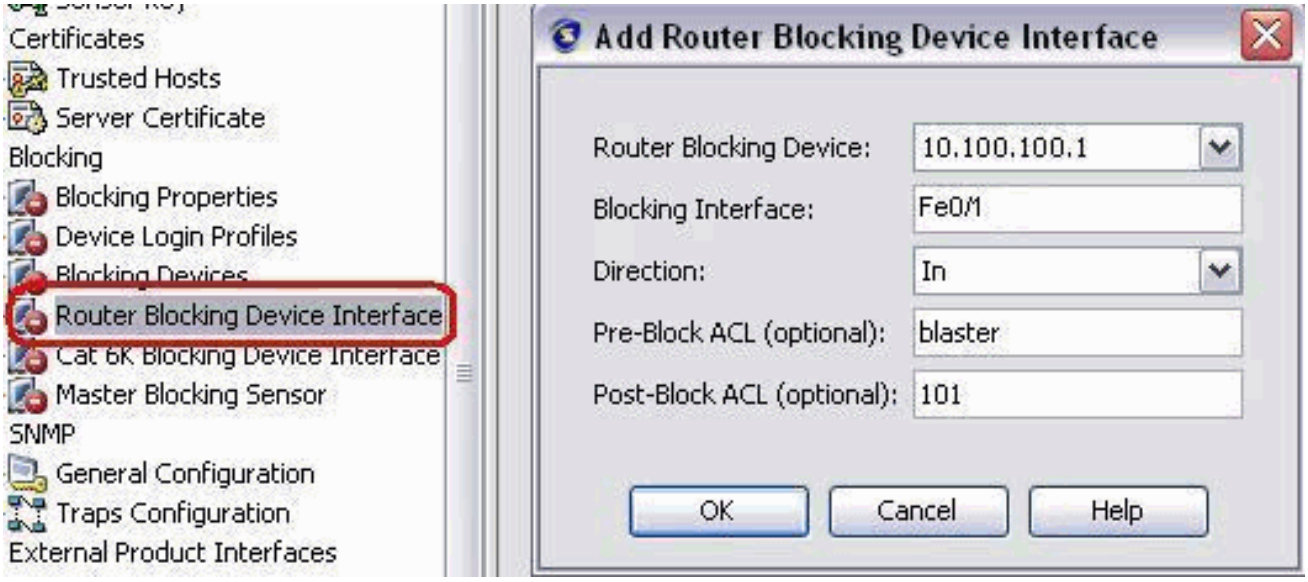
15. Agora do painel esquerdo, vá ao **perfil do início de uma sessão do dispositivo**. A fim criar um perfil novo, o clique **adiciona**. **A APROVAÇÃO** uma vez criada do clique e **aplica o** sensor e
continua.



16. A próxima etapa é configurar o roteador como o dispositivo de bloqueio. Do painel esquerdo, escolha o **dispositivo de bloqueio**, clique **adicionam** a fim adicionar esta informação. Então clique a **APROVAÇÃO** e **aplique-a**.



17. Agora do painel esquerdo configurar as relações de dispositivo de bloqueio. Adicionar a informação, clique a **APROVAÇÃO** e **aplique-a**.



Verificar

Lance o ataque e a obstrução

Termine estas etapas para lançar o ataque e a obstrução:

1. Antes que você lance o ataque, vai ao IME, escolhe o **monitoramento de evento > a opinião deixada cair dos ataques** e escolhe o sensor à direita.
2. O telnet à casa do roteador e verifica a comunicação do server com estes 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. No Router Light, estabeleça uma conexão Telnet com o Router House e digite testattack.Bata o **<space>** ou o **<enter>** a fim restaurar sua sessão de 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. O telnet à casa do roteador e usa o **comando show access-list** como mostrado aqui.`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. Do painel do IDS Event Viewer, o alarme vermelho aparece uma vez que o ataque é lançado.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Dicas

Use estes dicas de Troubleshooting:

- Do sensor olhe o **acesso de rede das estatísticas da mostra** output e certifique-se de que o `estado` " é ativo. Do console ou do SSH ao sensor, esta informação é vista:`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#`
- Certifique-se que o parâmetro de comunicação mostra que o protocolo correto está usado como o telnet ou o SSH com 3DES. Você pode tentar um SSH ou um telnet manual de um cliente SSH/Telnet em um PC a fim verificar as credenciais do nome de usuário e senha está correto. Então a tentativa ao telnet ou o SSH do sensor próprio ao roteador e consideram se você pode entrar com sucesso ao roteador.

Informações Relacionadas

- Página de suporte segura da prevenção de intrusão de Cisco
- Suporte Técnico e Documentação - Cisco Systems