Configurando o IDS que obstrui usando os ID de VMS MC

Índice

Introdução

Este documento fornece uma amostra para a configuração do Sistema de Detecção de Intrusão da Cisco (IDS) através do VPN/Security Management Solution (VMS), o console de gerenciamento IDS (IDS MC). Neste caso, obstruindo do sensor de IDS a um roteador Cisco é configurado.

Pré-requisitos

Requisitos

Antes que você configure a obstrução, assegure-se de que você esteja conformes estas circunstâncias.

- O sensor é instalado e configurado detectando o tráfego necessário.
- O farejando interface é medido à interface externa do roteador.

Componentes Utilizados

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

- VMS 2.2 com IDS MC e monitor 1.2.3 da Segurança
- Sensor do Cisco IDS 4.1.3S(63)
- Roteador Cisco que executa o Software Release 12.3.5 de Cisco IOS®

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

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

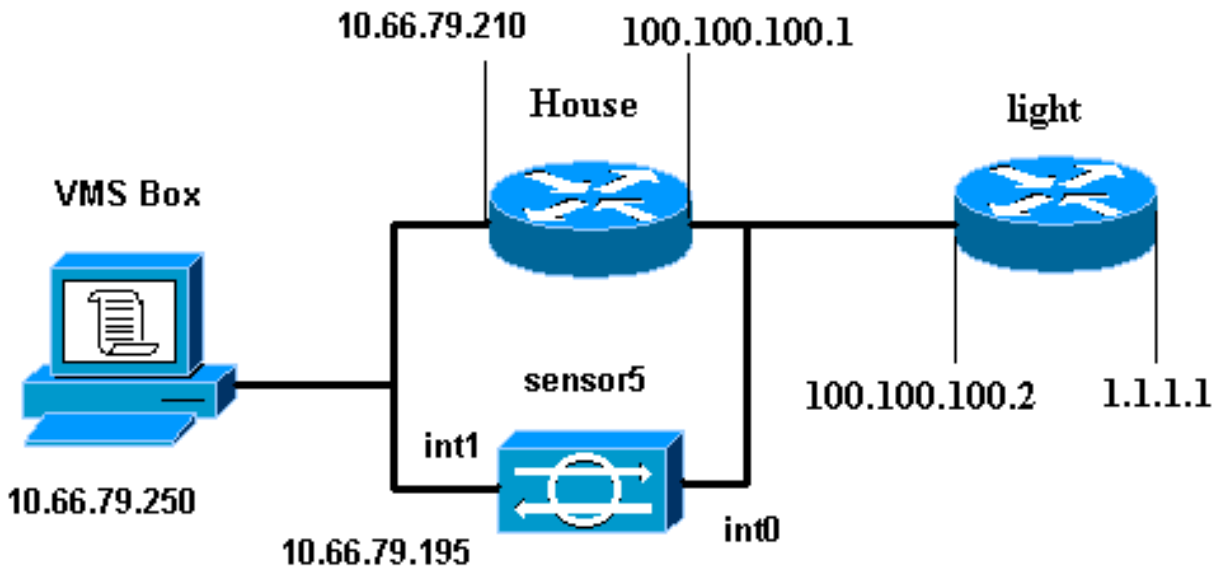
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Para localizar informações adicionais sobre os comandos usados neste documento, utilize a Ferramenta Command Lookup (somente clientes registrados).

Diagrama de Rede

Este documento utiliza a configuração de rede mostrada neste diagrama.



Configurações

Este documento utiliza as configurações mostradas aqui.

- Luz do Roteador
- Companhia do Roteador

Luz do Roteador

```
Current configuration : 906 bytes
!
version 12.3
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 100.100.100.2 255.255.255.0
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
100.100.100.1 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

```
Building configuration...

Current configuration : 797 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname House ! logging queue-limit 100 enable password
cisco ! ip subnet-zero no ip domain lookup ! ! interface
Ethernet0 ip address 10.66.79.210 255.255.255.224 hold-
queue 100 out ! interface Ethernet1 ip address
100.100.100.1 255.255.255.0 !--- After Blocking is
configured, the IDS Sensor !--- adds this access-group
ip access-group. IDS_Ethernet1_in_0 in ip classless ip
route 0.0.0.0 0.0.0.0 10.66.79.193 ip route 1.1.1.0
255.255.255.0 100.100.100.2 ip http server no ip http
secure-server ! !--- After Blocking is configured, the
IDS Sensor !--- adds this access list. ip access-list
extended IDS_Ethernet1_in_0. permit ip host 10.66.79.195
any permit ip any any ! line con 0 stopbits 1 line vty 0
4 password cisco login ! scheduler max-task-time 5000
end
```

Configuração de sensor inicial

Termine estas etapas para configurar inicialmente o sensor.

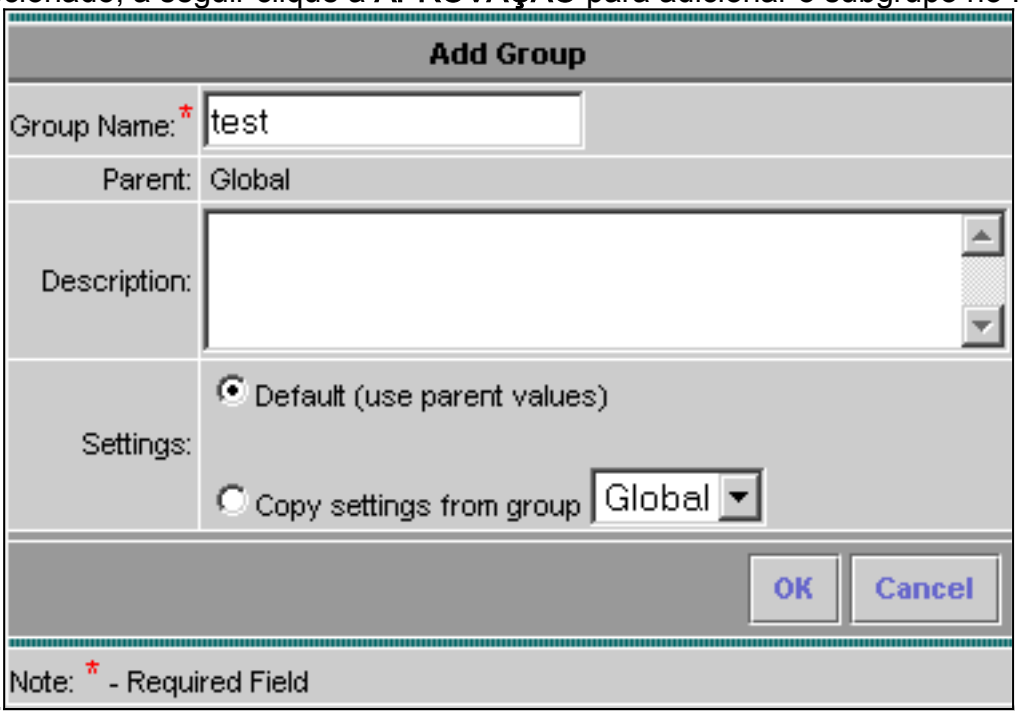
Nota: Se você executou a instalação inicial de seu sensor, continue à seção que importa o sensor em IDS MC.

1. Console no sensor.Você é alertado para um nome de usuário e senha. Se isto é a primeira vez você está consolando no sensor, você deve entrar com o username **Cisco** e senha **Cisco**.
2. Você é alertado mudar a senha e datilografar então a senha nova para confirmar.
3. Datilografe a **instalação** e incorpore a informação apropriada em cada alerta para estabelecer parâmetros básicos para seu sensor, conforme este exemplo:`sensor5#setup --- System Configuration Dialog --- At any point you may enter a question mark '?' for help. User ctrl-c to abort 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 sensor5 telnetOption enabled 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`
4. Imprensa **2** a fim salvar sua configuração.

Importe o sensor em IDS MC

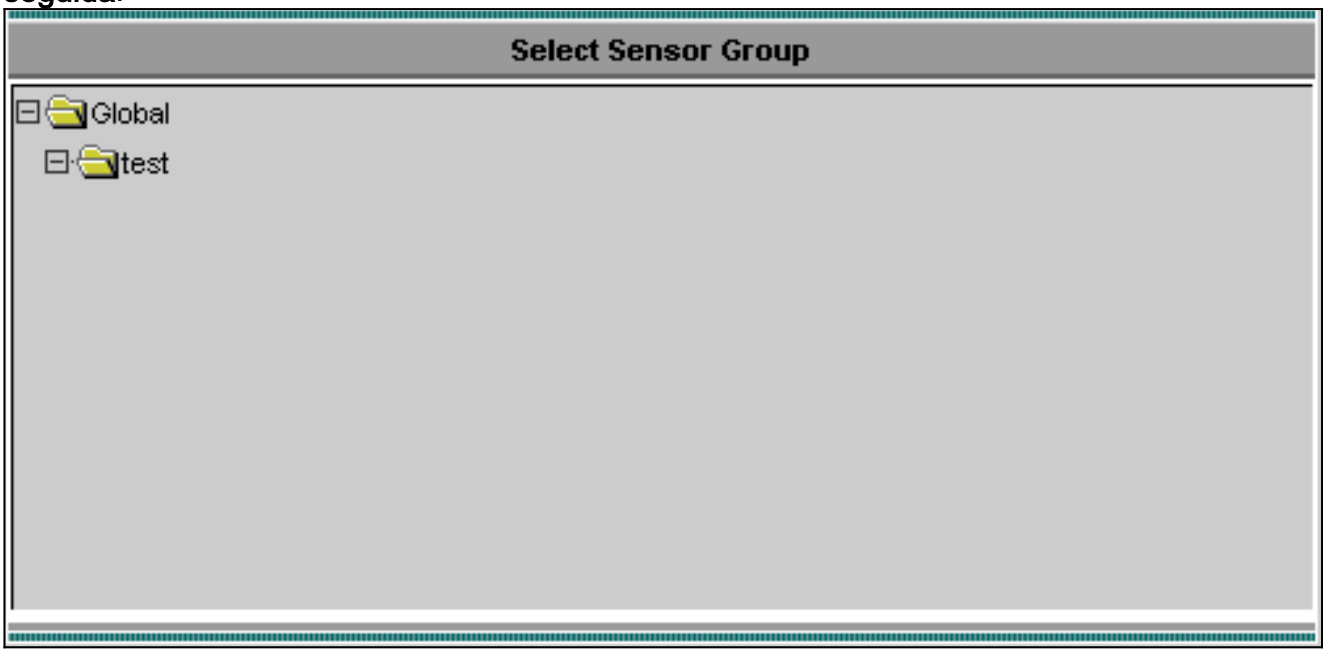
Termine estas etapas para importar o sensor no IDS MC.

1. Consulte a seu sensor.Neste caso, consulte a **http://10.66.79.250:1741** ou a **https://10.66.79.250:1742**.
2. Entre com o nome de usuário e senha apropriado.Neste exemplo, o admin de nome de usuário e a senha **Cisco** foram usados.
3. Selecione o **Solução de Gerenciamento de VPN/de Segurança > Centro de Gerenciamento** e escolha **sensors de IDS**.
4. Clique a aba dos dispositivos, **grupo** seleto do **sensor**, destaque **global**, e o clique **cria o subgrupo**.
5. Dê entrada com o nome do grupo e assegure-se de que o botão de rádio do **padrão** esteja selecionado, a seguir clique a **APROVAÇÃO** para adicionar o subgrupo no IDS MC.

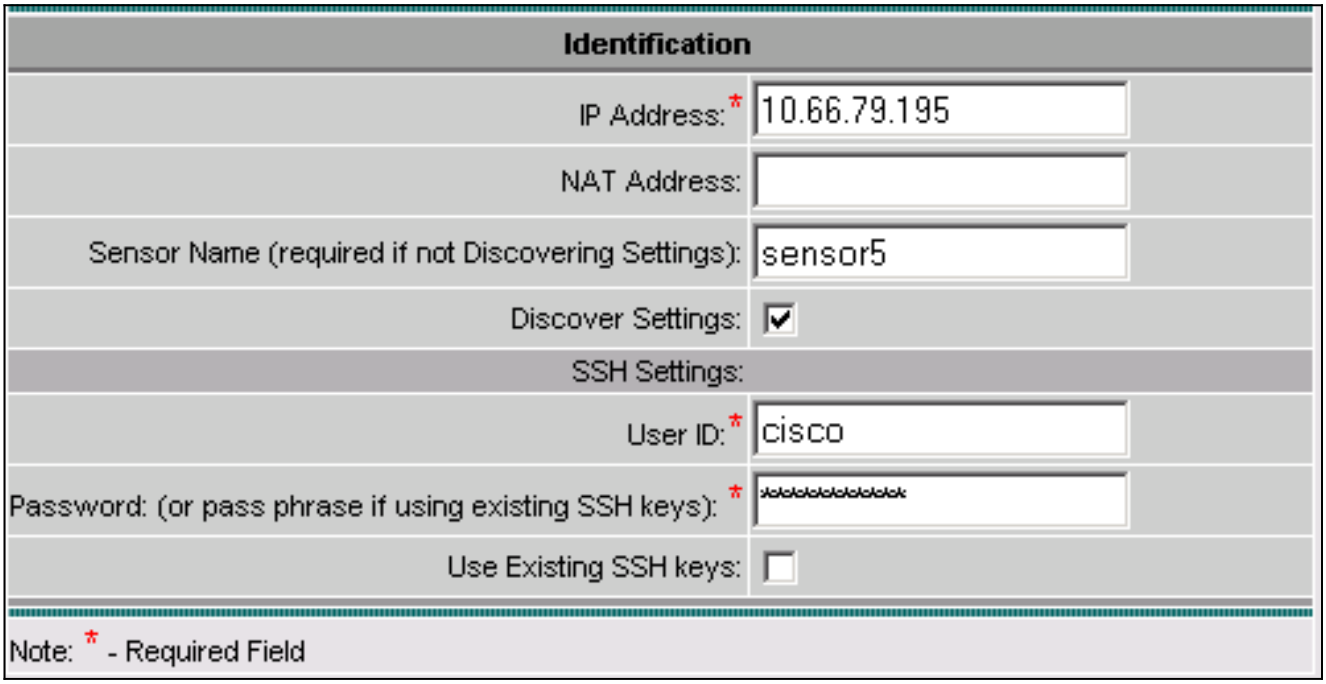


6. Selecione **dispositivos > sensor**, destaque o subgrupo criado na etapa precedente (neste caso, **teste**), e o clique **adiciona**.

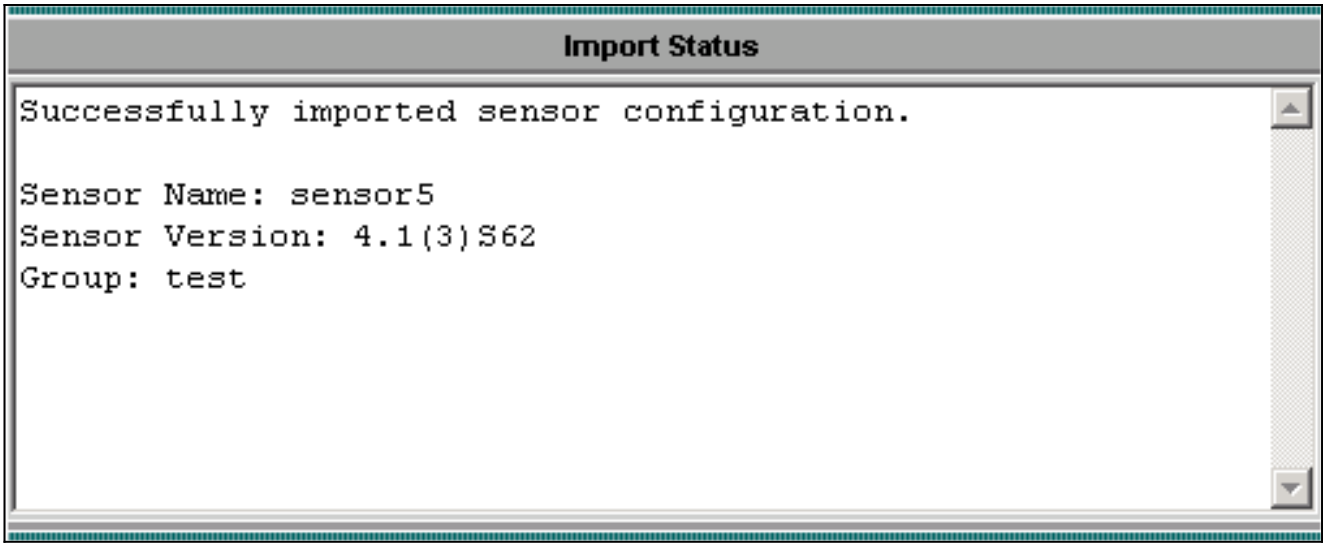
7. Destaque o subgrupo, e clique-o **em seguida**.



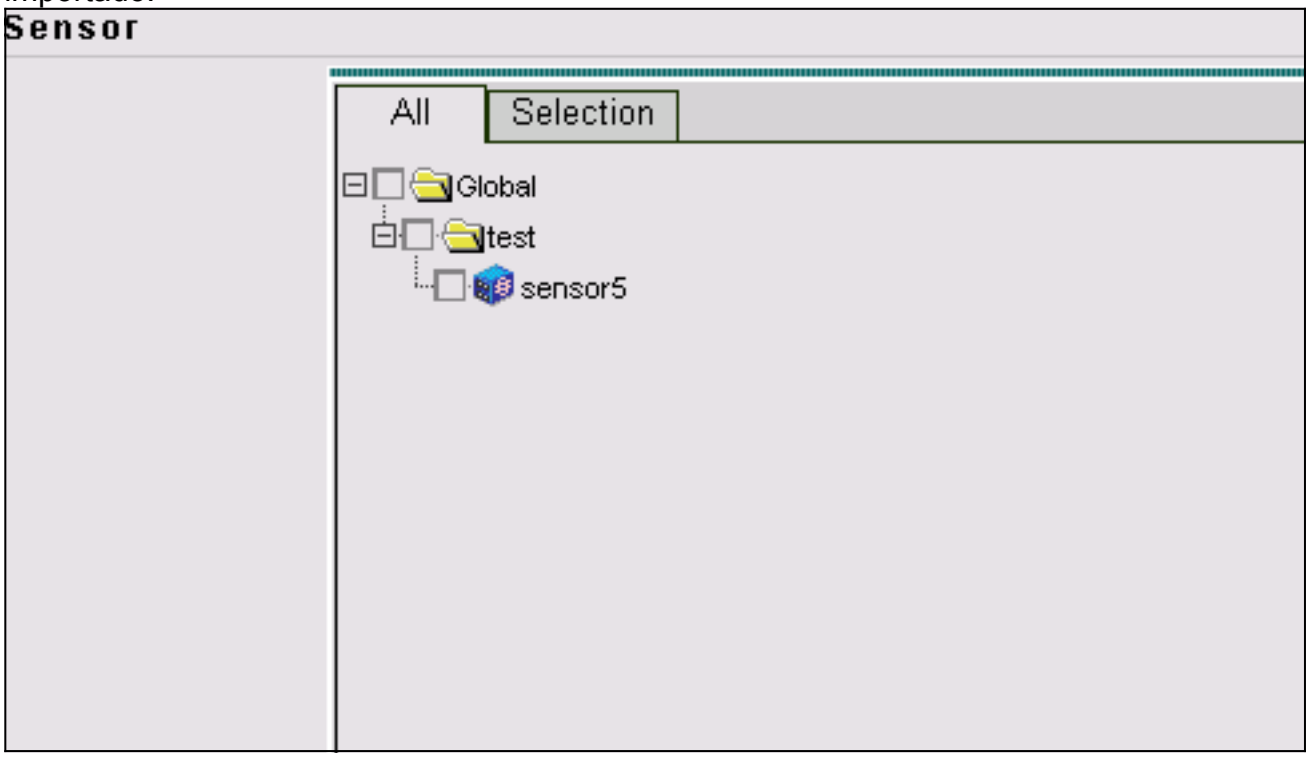
8. Incorpore os detalhes conforme este exemplo, a seguir clique-os **ao lado de** continuam.



9. Depois que você é presentado com uma mensagem que os estados `importem com sucesso a configuração de sensor`, clique o **revestimento** para continuar.



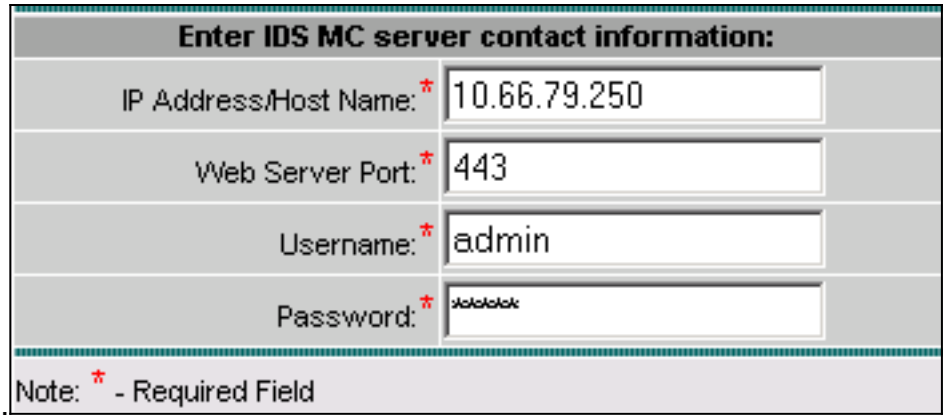
10. Seu sensor é importado no IDS MC. Neste caso, sensor5 é importado.



Importe o sensor no monitor da Segurança

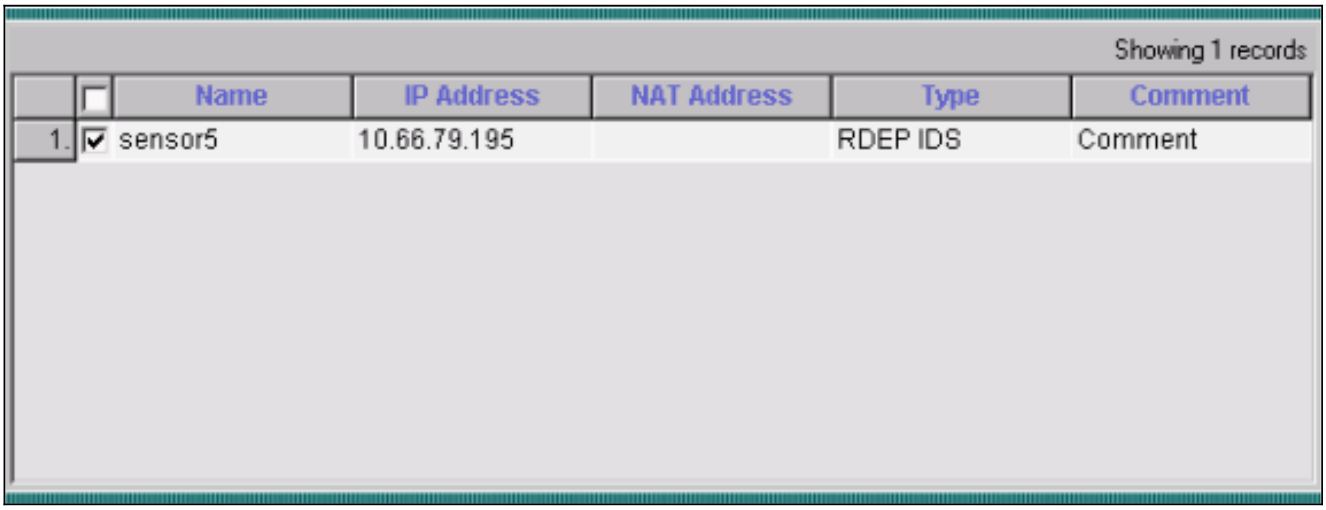
Termine este procedimento para importar o sensor no monitor da Segurança.

1. No menu de servidor VMS, selecione **monitor Center do** > segurança do **VPN/Security Management Solution** > da **monitoração**.
2. Selecione a aba dos dispositivos, a seguir clique a **importação** e incorpore a informação do servidor IDS MC, conforme este

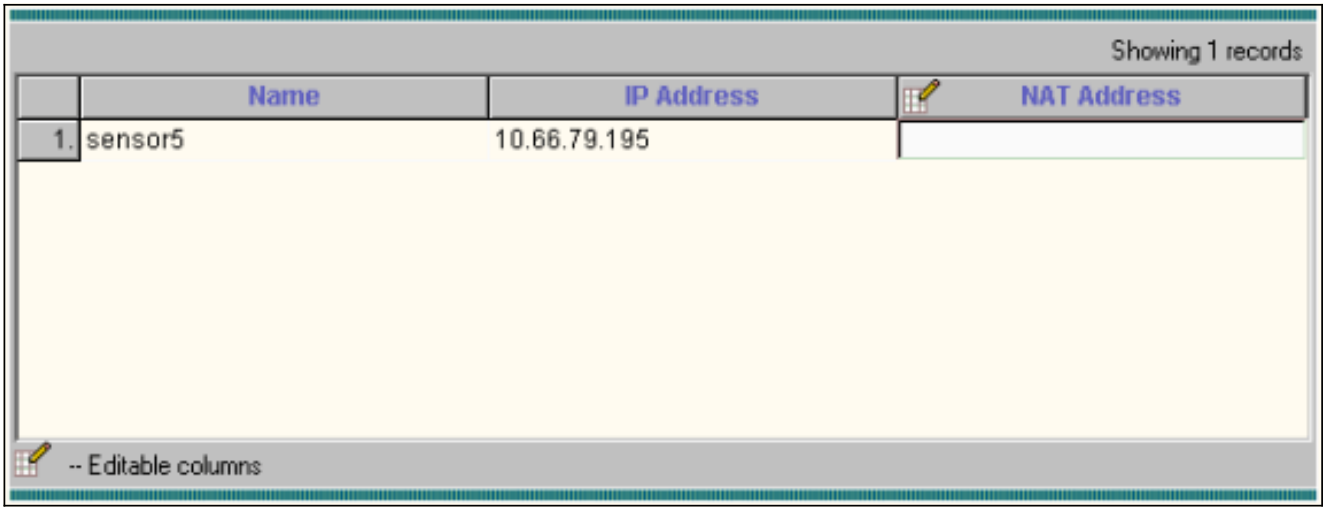


exemplo.

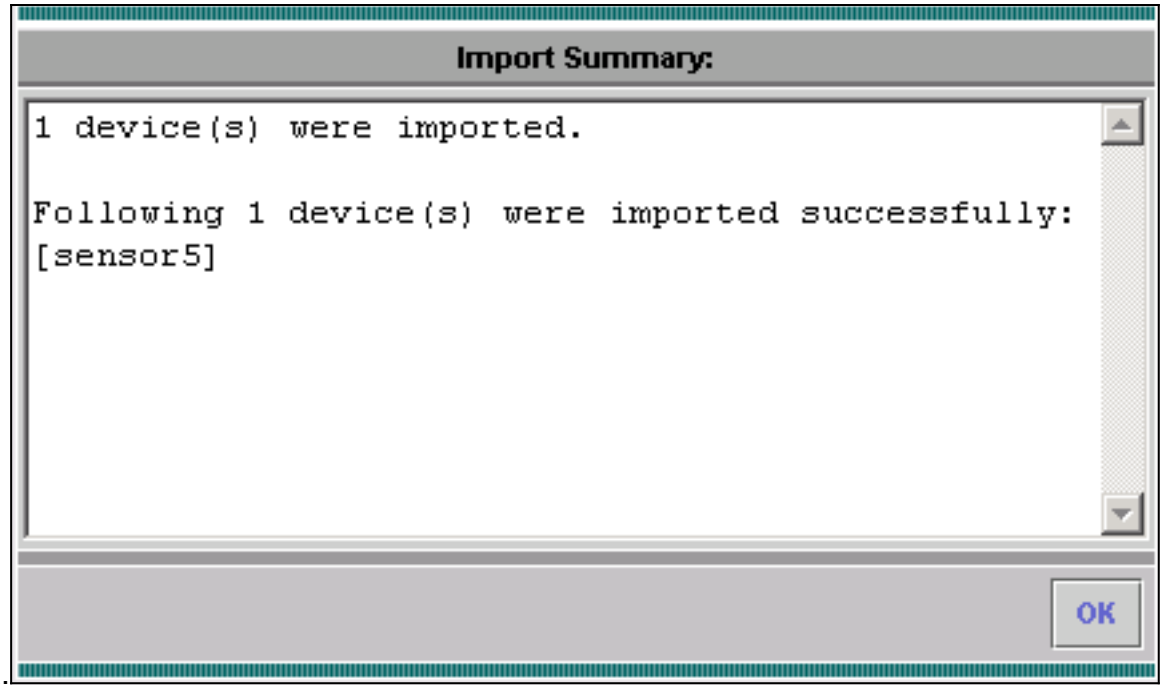
3. Selecione seu sensor (neste caso, **sensor5**) e clique-o **ao lado de** continuam.



4. Se necessário, atualize o endereço do Network Address Translation (NAT) para seu sensor, a seguir clique o **revestimento** para continuar.

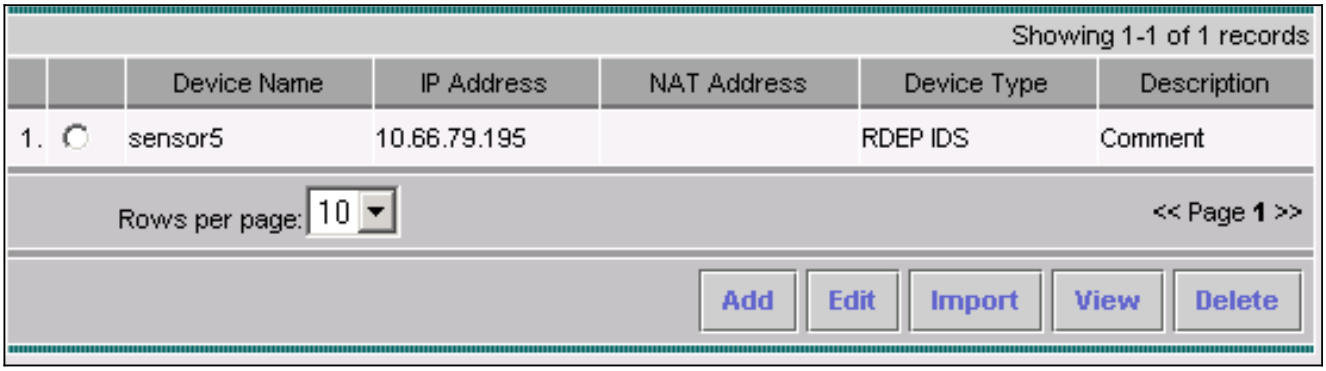


5. Clique a **APROVAÇÃO** para terminar importar o sensor de IDS MC no monitor da



Segurança.

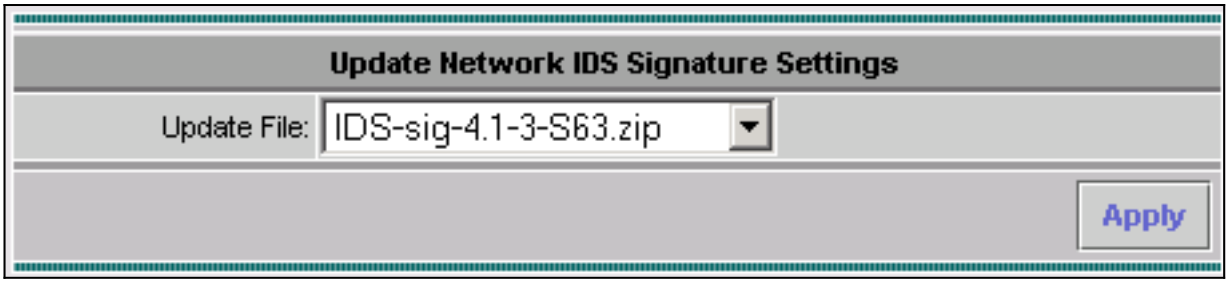
6. Seu sensor é importado com sucesso.



Use IDS MC para atualizações de assinatura

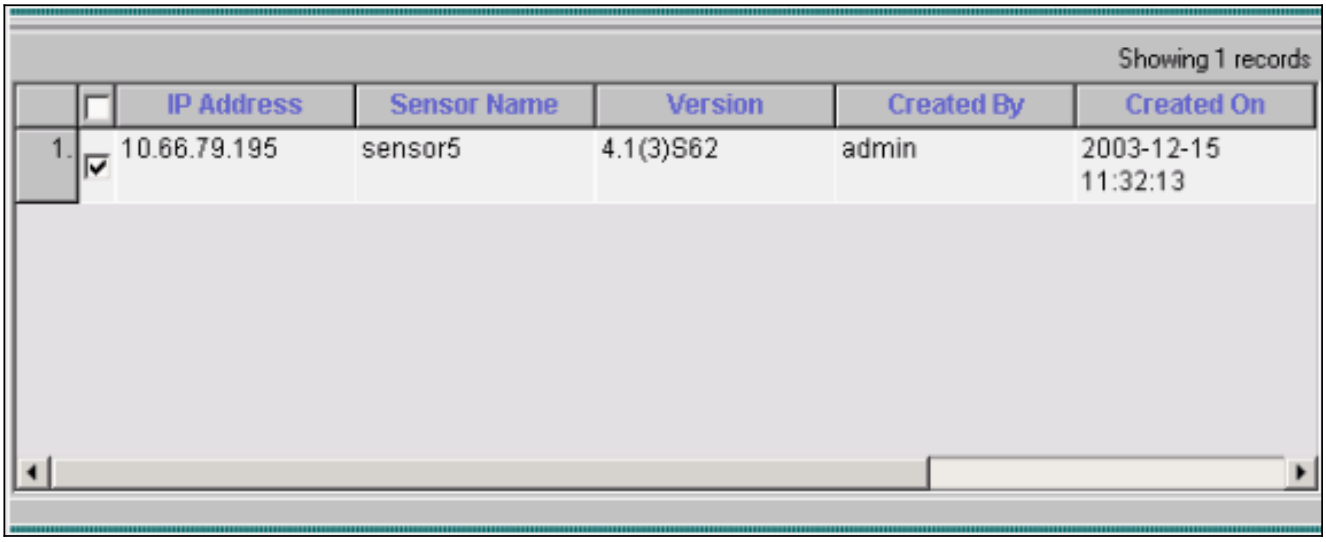
Termine este procedimento para usar o IDS MC para atualizações de assinatura.

1. Transfira as atualizações de assinatura dos ID de rede (clientes registrados somente) das transferências e salvar as no diretório C:\PROGRA~1\CSCOpx\MDC\etc\ids\updates\ em seu servidor VMS.
2. No console do servidor VMS, selecione o **Solução de Gerenciamento de VPN/de Segurança > Centro de Gerenciamento >** os **sensores**.
3. Clique o guia de configuração, as **atualizações** seletas, e as **assinaturas dos ID de rede da atualização do** clique.
4. Selecione a assinatura que você quer promover do menu suspenso e o clique **aplica-se** para continuar.

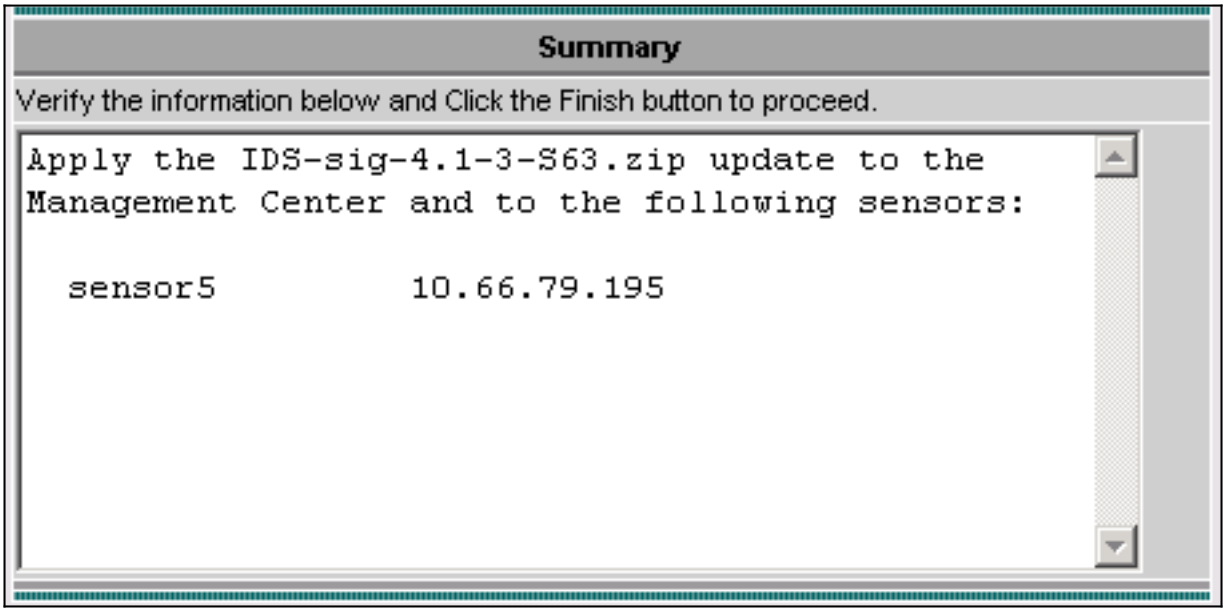


5. Selecione os sensores para atualizar, e o clique **ao lado de**

continua.



6. Depois que você é alertado aplicar a atualização ao centro de gerenciamento, assim como o sensor, **revestimento do** clique a
continuar.



7. Telnet ou console na interface da linha de comando do sensor. A informação similar a esta aparece:`sensor5#`
`Broadcast message from root (Mon Dec 15 11:42:05 2003):`
`Applying update` **`IDS-sig-4.1-3-S63. This may take several minutes.`** `Please do not reboot the sensor during this update. Broadcast message from root (Mon Dec 15 11:42:34 2003):` **`Update complete. sensorApp is restarting This may take several minutes.`**
8. Espere por alguns minutos para permitir que a elevação termine, a seguir incorpore a **versão da mostra** para verificar.`sensor5#`**`show version`** `Application Partition:` **`Cisco Systems Intrusion Detection Sensor, Version 4.1(3)S63 Upgrade History: * IDS-sig-4.1-3-S62 07:03:04 UTC Thu Dec 04 2003 IDS-sig-4.1-3-S63.rpm.pkg 11:42:01 UTC Mon Dec 15 2003`**

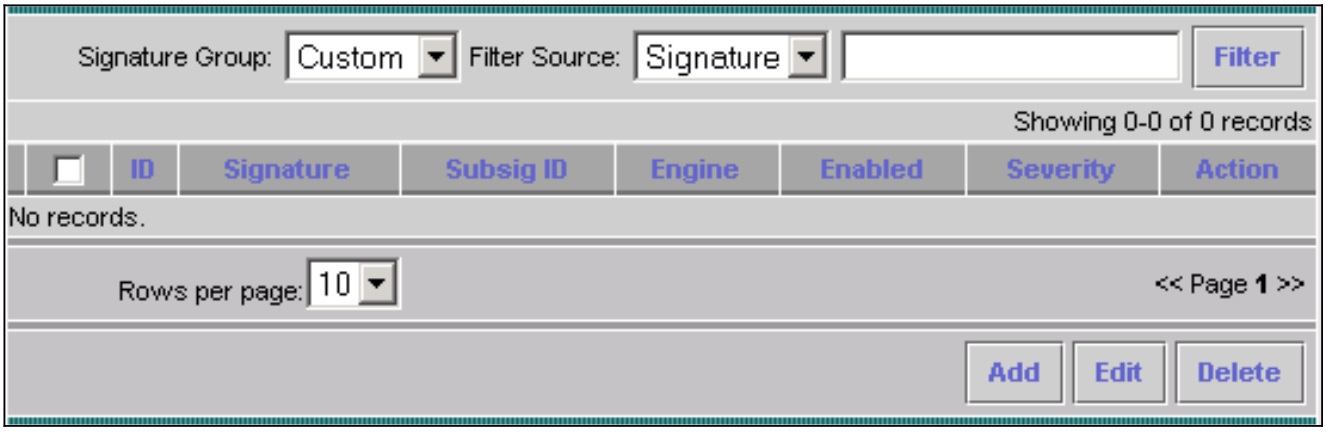
Configurar a obstrução para o IOS Router

Termine este procedimento para configurar a obstrução para o IOS Router.

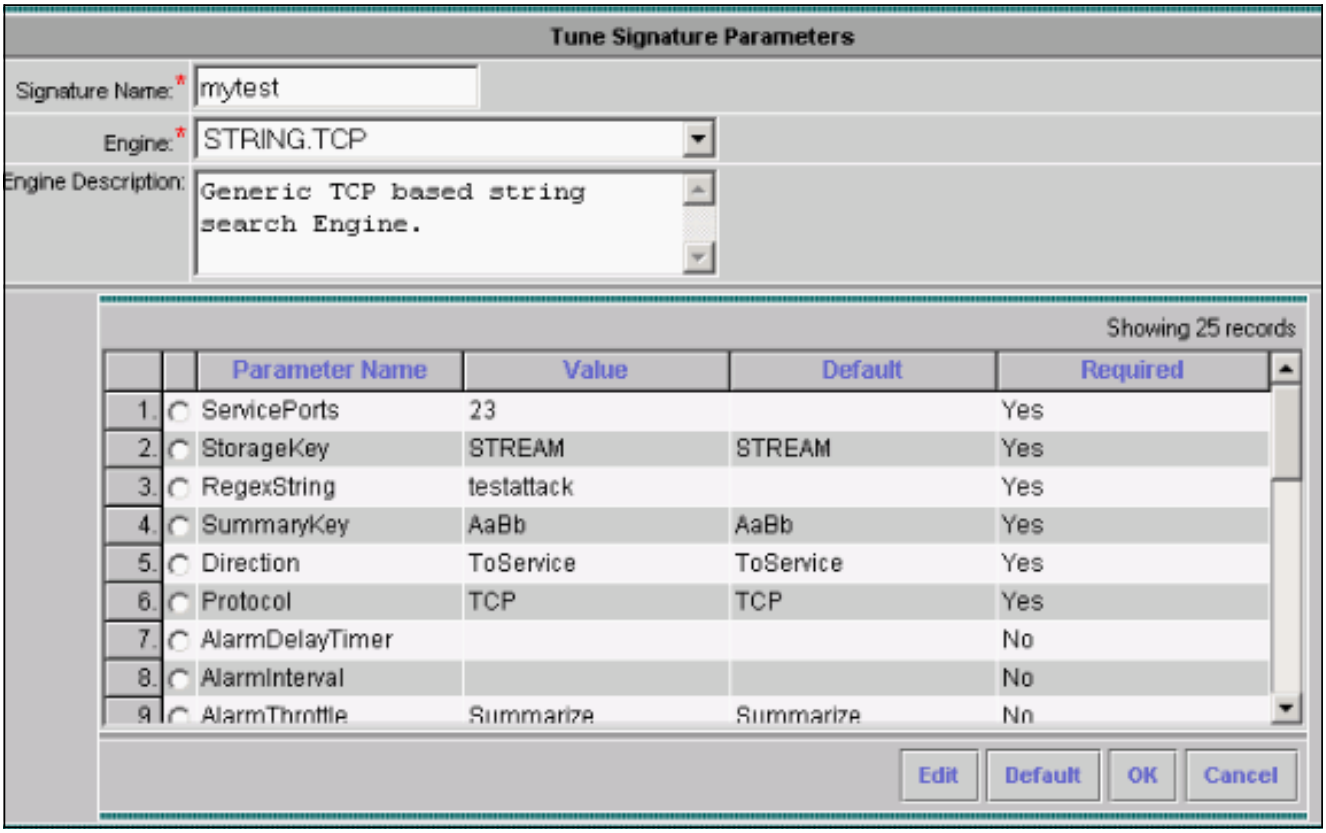
1. No console do servidor VMS, selecione o **Solução de Gerenciamento de VPN/Segurança > Centro de Gerenciamento > Sensores de IDS**.
2. Selecione o guia de configuração, selecione seu sensor do seletor do objeto, e clique

ajustes.

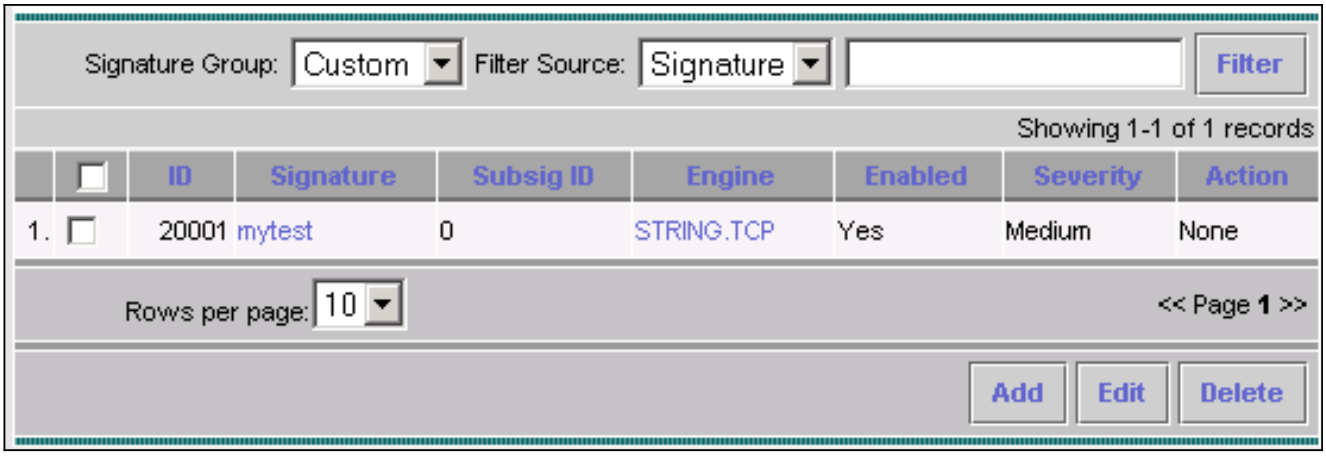
3. Selecione **assinaturas**, clique o **costume**, a seguir clique-o **adicionam** para adicionar uma assinatura
nova.

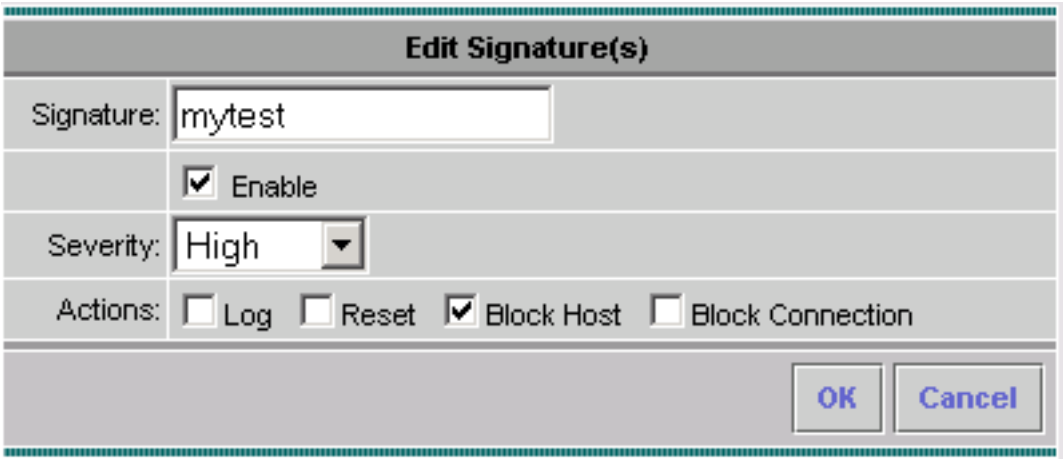


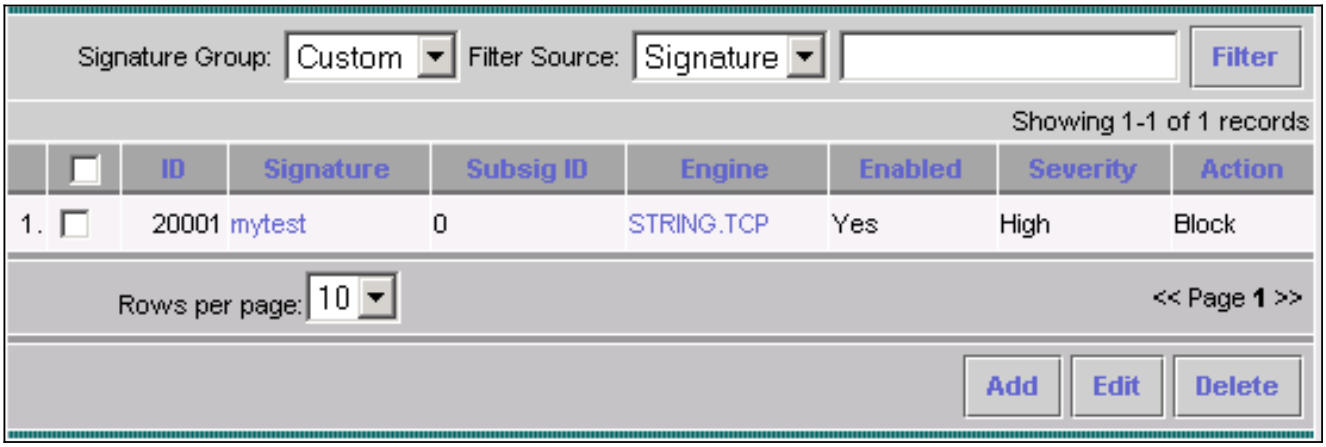
4. Dê entrada com o nome novo da assinatura, a seguir selecione o motor (neste caso, **STRING.TCP**).
5. Você pode personalizar os parâmetros disponíveis verificando o botão Appropriate Radio Button e clicando **edite**.Neste exemplo, o parâmetro de ServicePorts é editado para mudar seu valor a 23 (para a porta 23). O parâmetro RegexString é editado igualmente para adicionar o **ataque de teste do** valor. Quando isto está completo, clique a **APROVAÇÃO** para continuar.



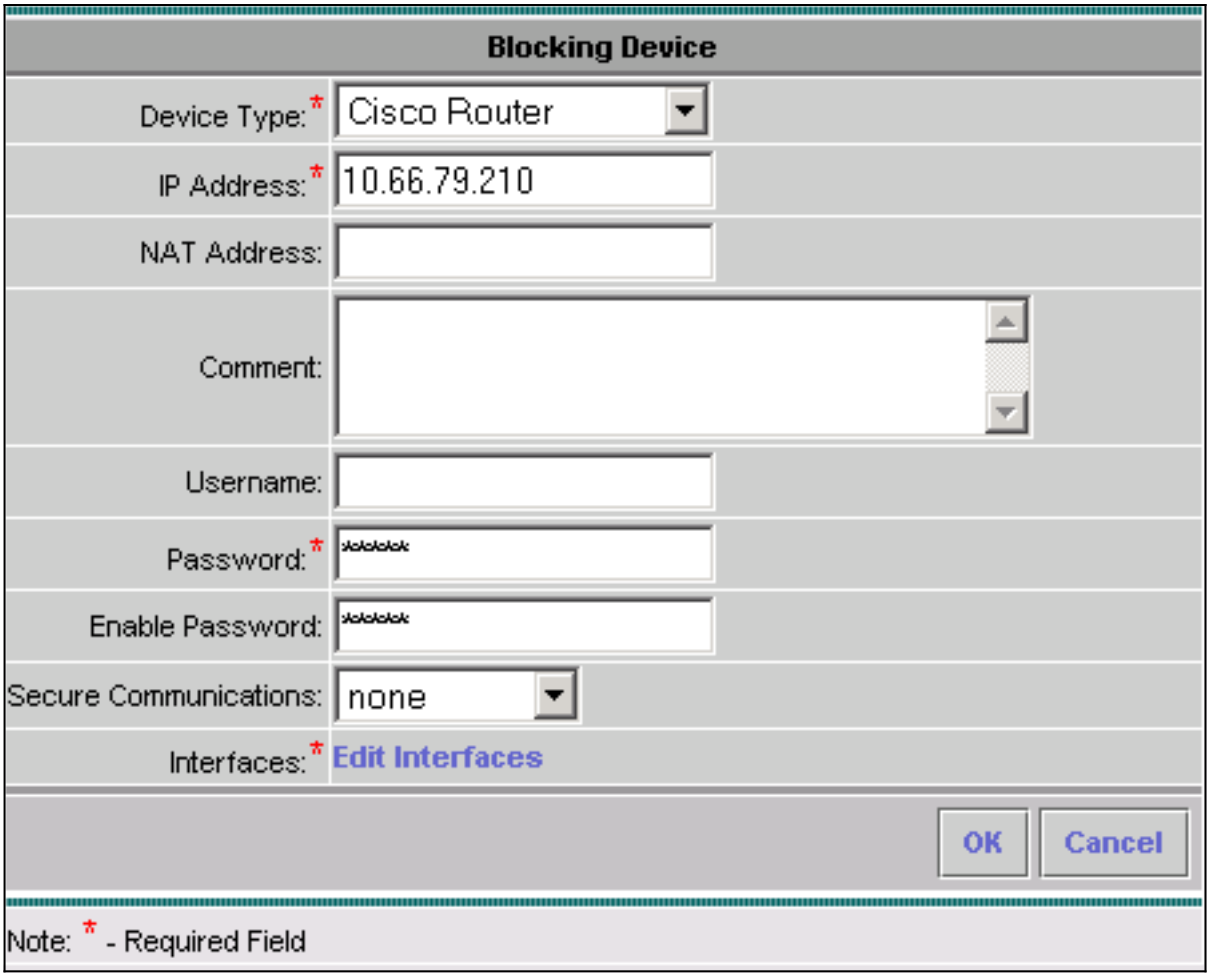
6. Para editar a gravidade da assinatura e as ações ou permiti-los/desabilitam a assinatura, clicam o nome da
assinatura.



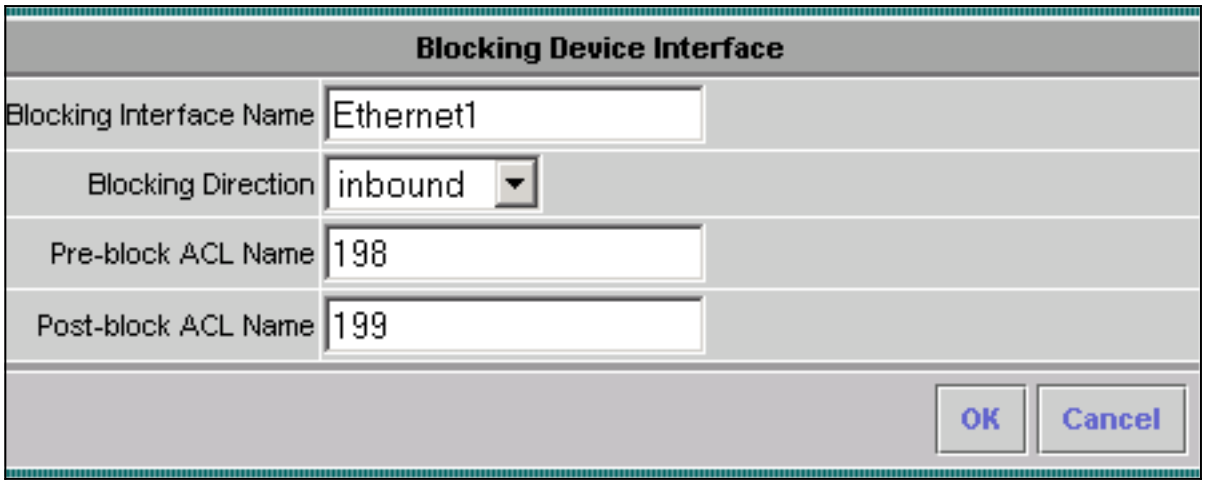
7. Neste caso, a severidade é mudada à **elevação** e a ação do **host do bloco** é selecionada. Clique em OK para continuar.O host do bloco obstrui Host IP de ataque ou sub-redes IP.Os blocos TCP da conexão do bloco ou portas UDP (baseadas em atacar o TCP ou as conexões de


UDP).
8. A assinatura completa olha similar a
esta:


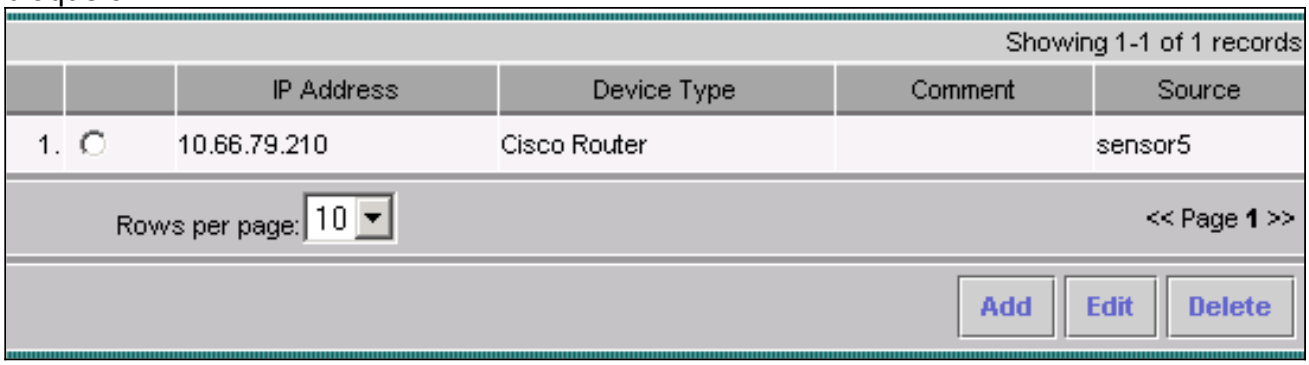
9. A fim configurar o dispositivo de bloqueio, a **obstrução** seleta > **dispositivos de bloqueio do** seletor do objeto (o menu no lado esquerdo da tela), e o clique **adicionam** para incorporar a informação
seguinte:



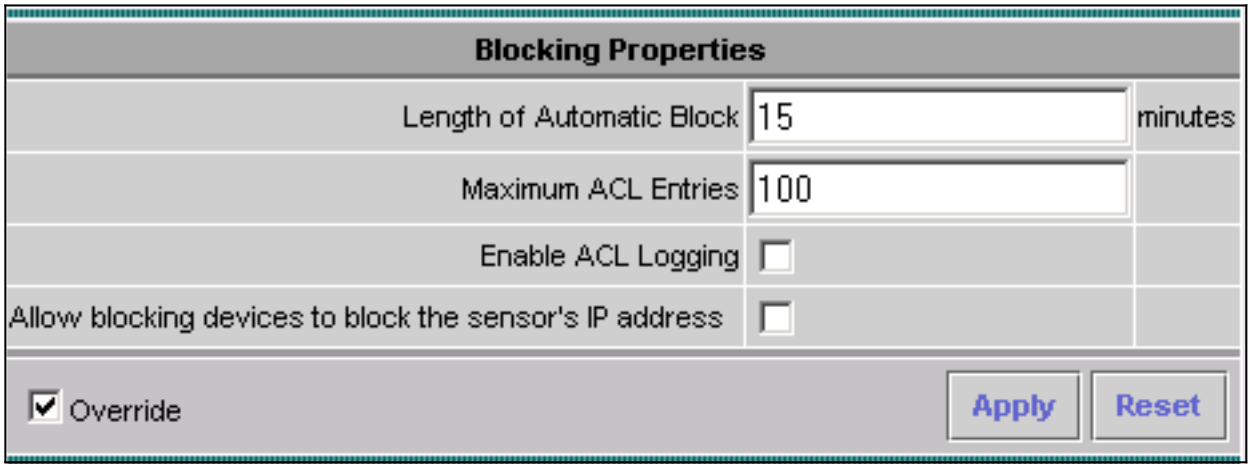
10. O clique **edita relações** (veja a captura de tela precedente), clique **adiciona**, incorpora esta informação, a seguir clica a **APROVAÇÃO** para continuar.



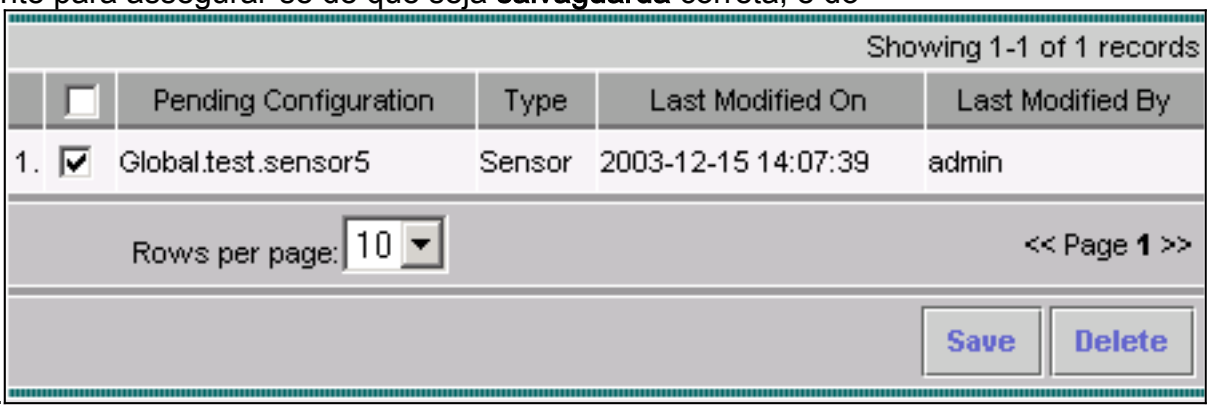
11. Clique a **APROVAÇÃO** duas vezes para terminar a configuração do dispositivo de bloqueio.



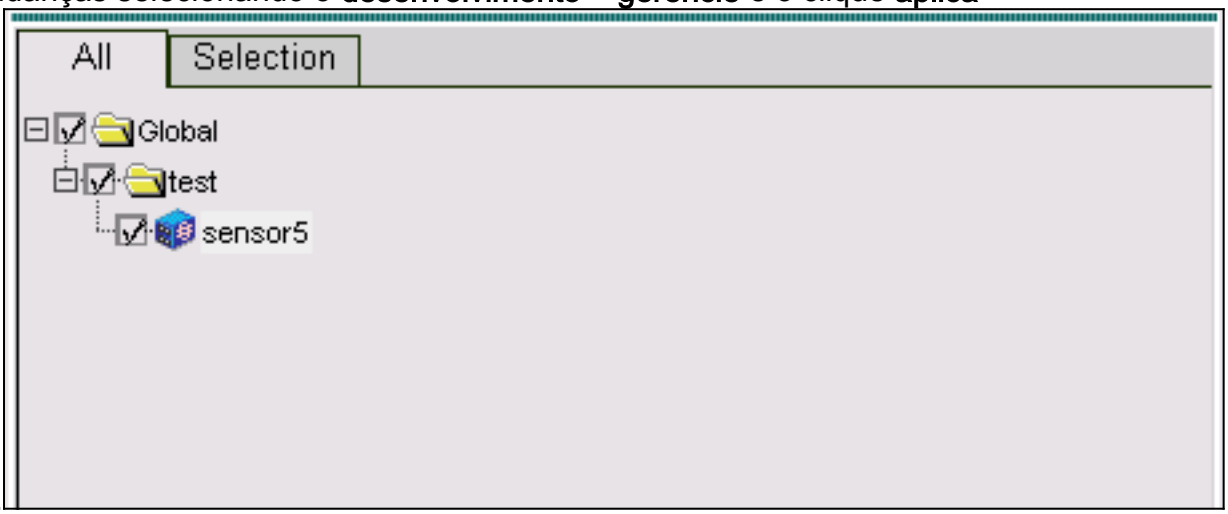
12. Para configurar a obstrução de propriedades, selecione a **obstrução** > a **obstrução de propriedades**.O comprimento do bloco automático pode ser alterado. Neste caso, é mudado a **15 minutos**. O clique **aplica-se** para continuar.



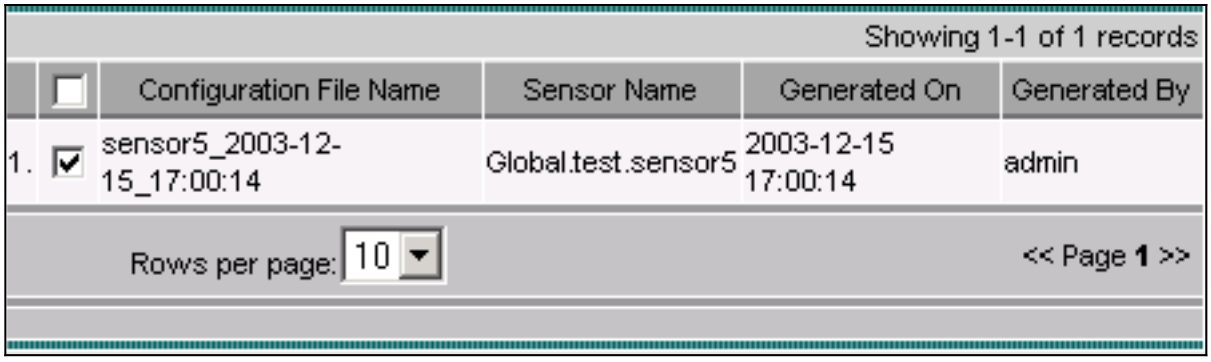
13. **A configuração** seleta do menu principal, seleciona então **pendente**, verifica a configuração pendente para assegurar-se de que seja **salvaguarda** correta, e do clique.



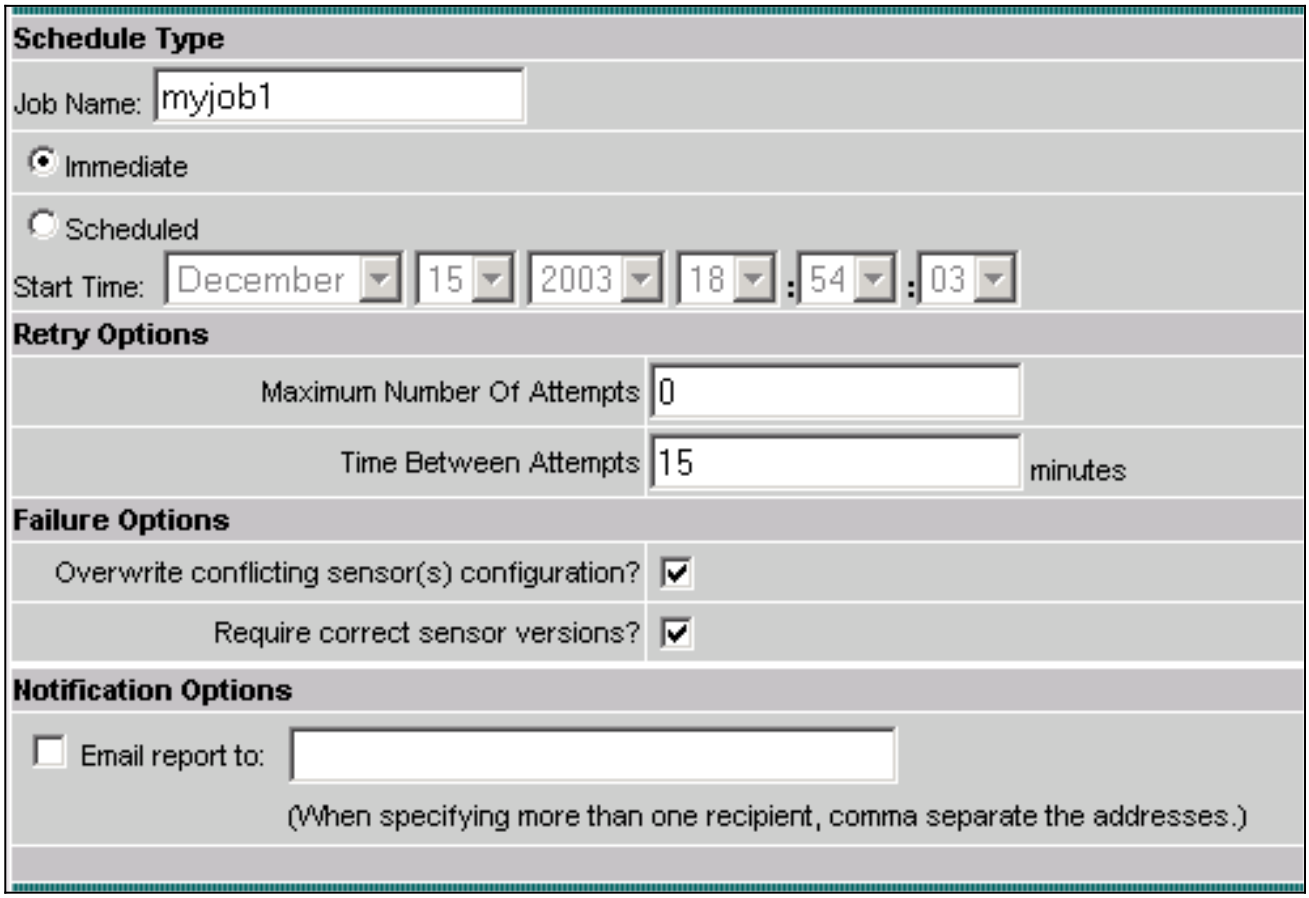
14. Para empurrar as alterações de configuração para o sensor, para gerar e distribuir então as mudanças selecionando o **desenvolvimento** > **gerencie** e o clique **aplica-se**.



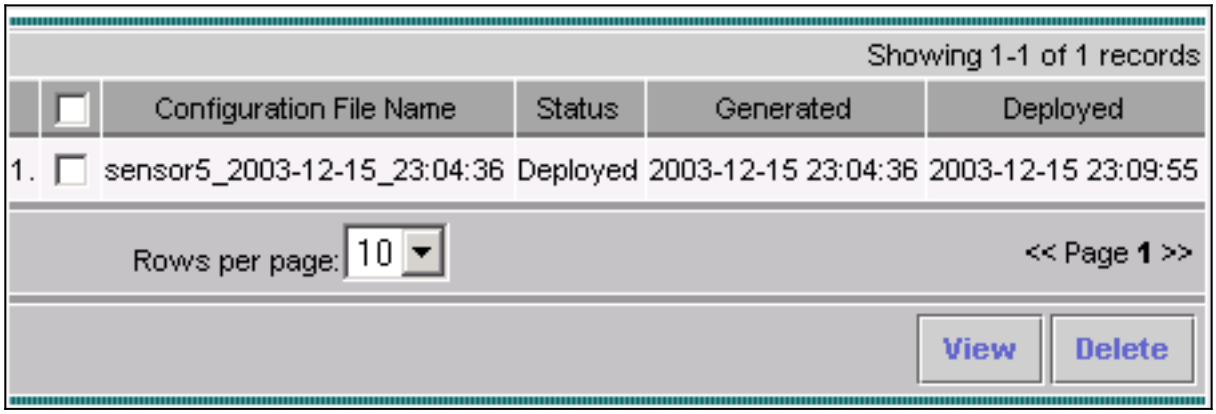
15. **O distribuição** > **distribuir** seleto, clica então **submete-se**.
16. Verifique a caixa de seleção ao lado de seu sensor, a seguir clique-a **distribuem**.
17. Verifique a caixa de seleção para ver se há o trabalho na fila, a seguir clique-a **ao lado de** continuam.



18. Dê entrada com o nome do trabalho e programe o trabalho como imediato, a seguir clique o
revestimento.



19. Selecione o **distribuição > distribuir > pendente**.Espere alguns minutos até que todos os trabalhos pendentes estejam terminados. A fila está então vazia.
20. Para confirmar o desenvolvimento, selecione a **história de Configuration>**.Assegure-se de que o estado da configuração esteja indicado como **distribuído**. Isto significa que a configuração de sensor esteve atualizada com
sucesso.



Verificar

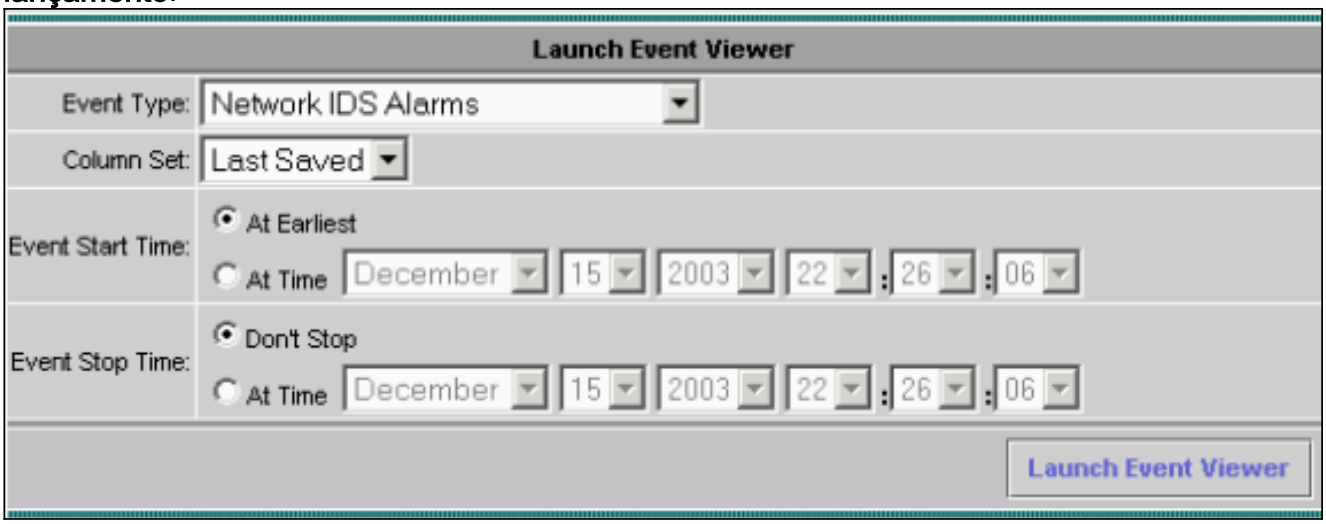
Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

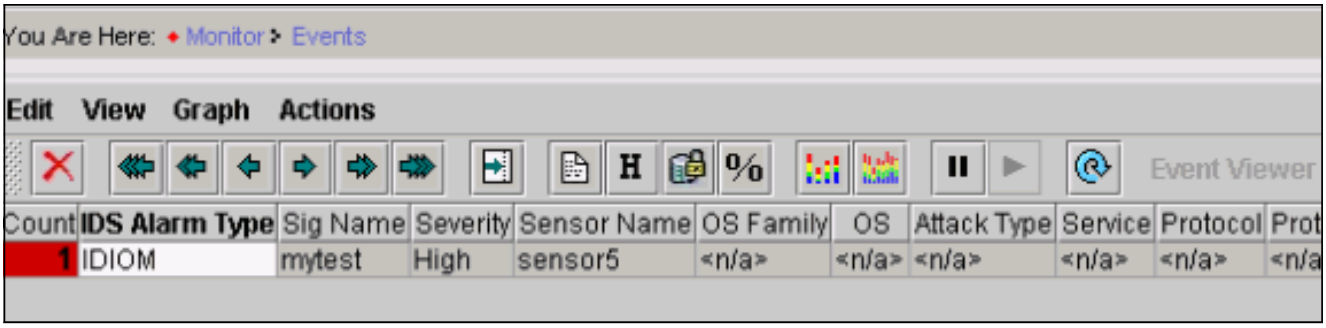
Lance o ataque e a obstrução

Para verificar que o processo de bloqueio está trabalhando corretamente, lance um ataque do teste e verifique os resultados.

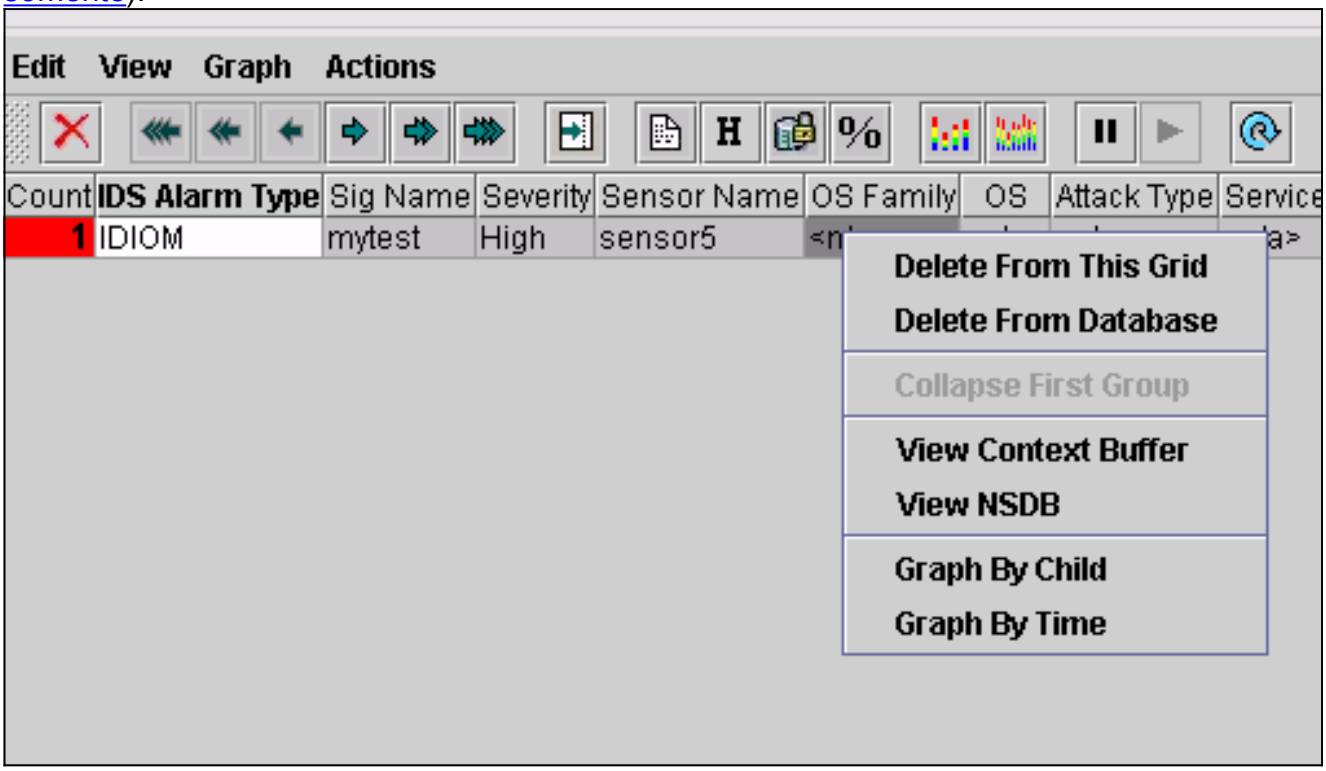
1. Antes de lançar o ataque, selecione **monitor Center do** > segurança do **VPN/Security Management Solution** > da **monitoração**.
2. Escolha o **monitor do** menu principal, clique **eventos** e clique então o **visualizador de eventos do lançamento**.



3. Telnet ao roteador (neste caso, telnet ao roteador da casa), para verificar a comunicação do sensor.`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_Ethernet1_in_0 10 permit ip host 10.66.79.195 any 20 permit ip any any (20 matches) House#`
4. Para lançar o ataque, o telnet de um roteador ao outro e o tipo **ataque de teste**.Neste caso, nós usamos o telnet para conectar do roteador leve ao roteador da casa. Assim que você pressionar o **<space>** ou o **<enter>**, após o ataque de teste de datilografia, sua sessão de Telnet devem ser restaurados.`light#`**`telnet 100.100.100.1`** `Trying 100.100.100.1 ... Open User Access Verification Password: house>en Password: house#`**`testattack`** *`!--- Host 100.100.100.2 has been blocked due to the !--- signature "testattack" being triggered.`* **`[Connection to 100.100.100.1 lost]`**
5. O telnet ao roteador (casa) e inscreve o comando show access-list.`house#`**`show access-list`** `Extended IP access list IDS_Ethernet1_in_1 10 permit ip host 10.66.79.195 any` *`!--- You will see a temporary entry has been added to !--- the access list to block the router from which you connected via Telnet previously.`* **`20 deny ip host 100.100.100.2 any (37 matches)`** `30 permit ip any any`
6. Do visualizador de eventos, **base de dados da pergunta do** clique para os eventos novos agora para ver o alerta para o ataque previamente lançado.



7. No visualizador de eventos, o destaque e clica com o botão direito o alarme, a seguir seleciona o **buffer do contexto da vista** ou **vê o NSDB** para ver mais informação detalhada sobre o alarme.**Nota:** O NSDB é igualmente acessível em linha na enciclopédia segura de Cisco (clientes registrados somente).

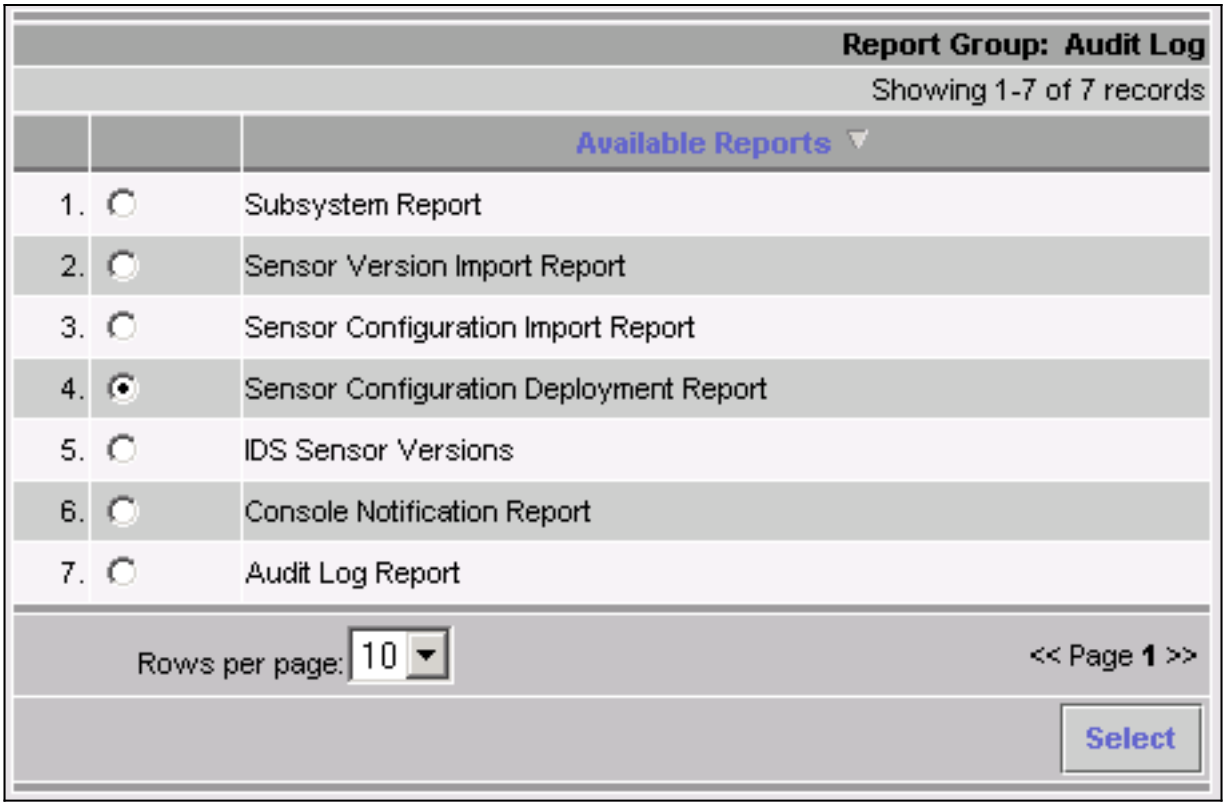


Troubleshooting

Procedimento de Troubleshooting

Use o seguinte procedimento para propósitos de Troubleshooting.

1. No IDS MC, os **relatórios** seletos > **gerenciem**.Segundo o tipo de problema, um detalhe mais adicional deve ser encontrado em um dos sete relatórios disponíveis.



2. No console do sensor, inscreva o comando show statistics networkaccess e verifique a saída para assegurar-se de que o “estado” seja ativo.
```
sensor5#show statistics networkAccess
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 = 100.100.100.2 ShunMinutes
= 15 MinutesRemaining = 12 sensor5#
```
3. Assegure-se de que o parâmetro de comunicação mostre que o protocolo correto está sendo usado, como o telnet ou o Shell Seguro (ssh) com 3DES.Você pode tentar um SSH ou um telnet manual de um cliente SSH/Telnet em um PC verificar credenciais do nome de usuário e senha está correto. Você pode então tentar o telnet ou o SSH do sensor próprio, ao roteador, para assegurá-lo pode entrar com sucesso.

Informações Relacionadas

- Página de suporte do Cisco Secure Intrusion Detection
- Apoio da Solução de gerenciamento de VPN/segurança CiscoWorks
- Suporte Técnico e Documentação - Cisco Systems