

Configurando a redefinição de IDS TCP usando VMS IDS MC

Contents

- [Introduction](#)
- [Prerequisites](#)
- [Requirements](#)
- [Componentes Utilizados](#)
- [Conventions](#)
- [Configurar](#)
- [Diagrama de Rede](#)
- [Configurações](#)
- [Configuração inicial do sensor](#)
- [Importar o sensor para o IDS MC](#)
- [Importar o sensor para o monitor de segurança](#)
- [Usar IDS MC para atualizações de assinatura](#)
- [Configurar a redefinição de TCP para o roteador IOS](#)
- [Verificar](#)
- [Iniciar o ataque de TCP Reset \(RST\)](#)
- [Troubleshoot](#)
- [Procedimento de Troubleshooting](#)
- [Informações Relacionadas](#)

Introduction

O documento fornece uma configuração de exemplo do Cisco Intrusion Detection System (IDS) através do VPN/Security Management Solution (VMS), IDS Management Console (IDS MC). Nesse caso, o TCP Reset do IDS Sensor para um roteador Cisco é configurado.

Prerequisites

Requirements

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- O sensor está instalado e configurado para detectar o tráfego necessário.
- A interface de sniffing é expandida para a 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 Security Monitor 1.2.3
- Cisco IDS Sensor 4.1.3S(63)
- Roteador Cisco que executa o Software Cisco IOS® versão 12.3.5

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.

Conventions

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos](#).

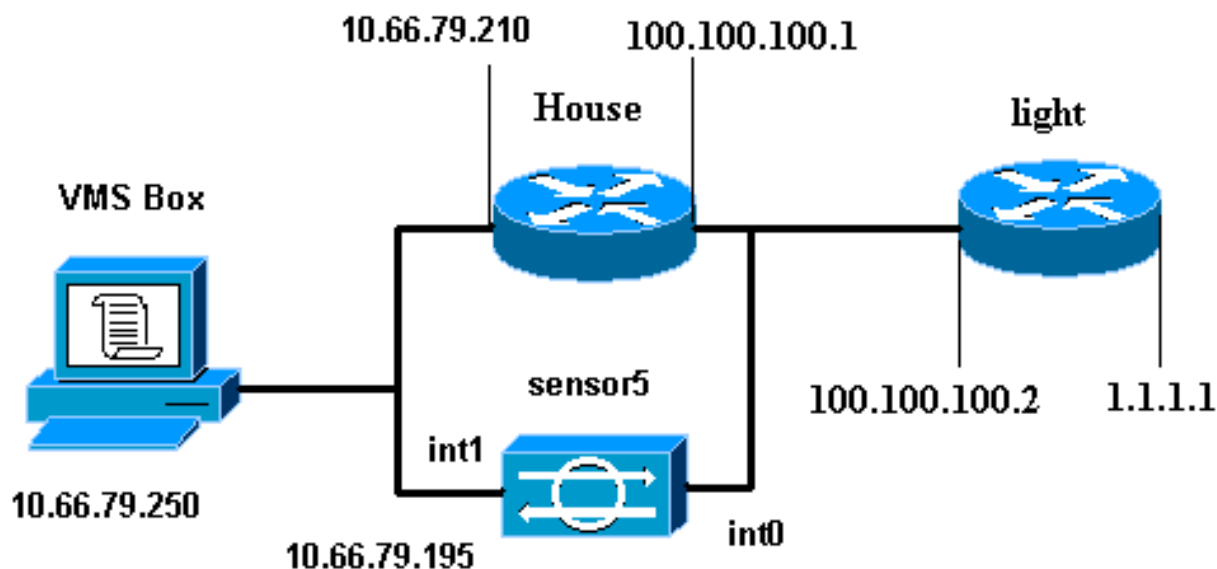
Configurar

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

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

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 12.3
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  
  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  
!  
!  
!  
line con 0  
  stopbits 1  
line vty 0 4  
  password cisco  
  login  
!  
scheduler max-task-time 5000  
end
```

[Configuração inicial do sensor](#)

Observação: se você já tiver executado a configuração inicial do Sensor, vá para a seção [Importar o sensor para o IDS MC](#).

1. Use o console para se conectar ao sensor. Você será solicitado a inserir um nome de usuário e uma senha. Se esta é a primeira vez que você está consolandando no Sensor, você deve fazer login com o nome de usuário **cisco** e a senha **cisco**.
2. Você será solicitado a alterar a senha e a digitar novamente a nova senha para confirmá-la.
3. Digite **setup** e insira as informações apropriadas em cada prompt para configurar parâmetros básicos para o Sensor, de acordo com 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
```

```
5 Save the config: (It might take a few minutes for the sensor  
saving the configuration)
```

```
[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
```

[Importar o sensor para o IDS MC](#)

Conclua estes passos para importar o sensor para o IDS MC.

1. Navegue até o seu sensor. Nesse caso, seja **http://10.66.79.250:1741** ou **https://10.66.79.250:1742**.
2. Faça login com o nome de usuário e a senha apropriados. Neste exemplo, o nome de usuário é **admin** e a senha é **cisco**.
3. Escolha **VPN/Security Management Solution > Management Center** e clique em **IDS Sensors**.
4. Clique na guia Dispositivos e escolha **Grupo de sensores**.
5. Realce **Global** e clique em **Criar Subgrupo**.
6. Digite o nome do grupo e verifique se **Default** está escolhido e clique em **OK** para adicionar o subgrupo ao IDS

Add Group

Group Name: * test

Parent: Global

Description:

Settings:

Default (use parent values)

Copy settings from group Global

OK Cancel

Note: * - Required Field

MC.

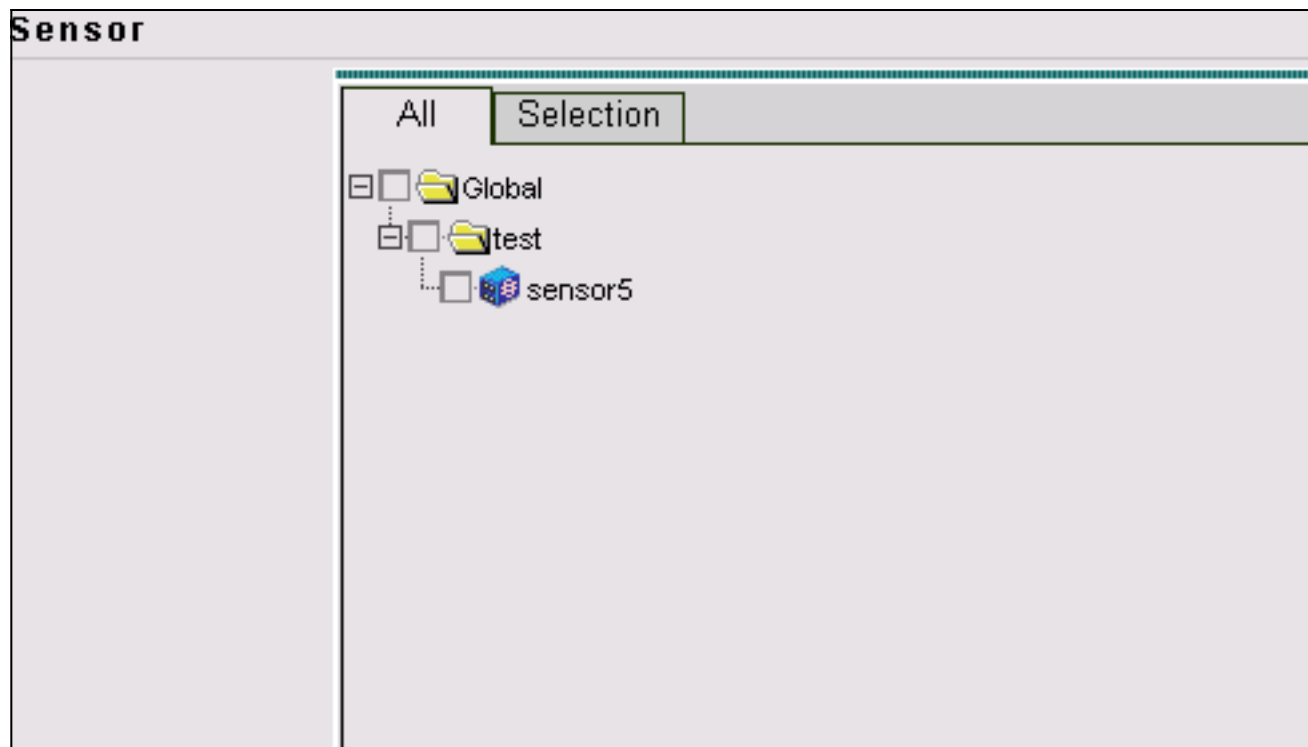
7. Escolha **Dispositivos > Sensor**, realce o subgrupo criado na etapa anterior (nesse caso, **teste**) e clique em **Adicionar**.
8. Realce o subgrupo e clique em **Avançar**.

Select Sensor Group

[-] Global

[-] test

9. Insira os detalhes conforme este exemplo e clique em **Avançar** para continuar.



[Importar o sensor para o monitor de segurança](#)

Conclua estes passos para importar o sensor para o Security Monitor.

1. No menu do Servidor VMS, escolha **VPN/Security Management Solution > Monitoring Center > Security Monitor**.
2. Selecione a guia Dispositivos, clique em **Importar** e insira as Informações do servidor IDS MC, conforme este

Enter IDS MC server contact information:	
IP Address/Host Name: *	<input type="text" value="10.66.79.250"/>
Web Server Port: *	<input type="text" value="443"/>
Username: *	<input type="text" value="admin"/>
Password: *	<input type="password" value="*****"/>

Note: * - Required Field

exemplo.


3. Selecione o Sensor (nesse caso, **sensor5**) e clique em **Avançar** para continuar.


Showing 1 records

	<input type="checkbox"/>	Name	IP Address	NAT Address	Type	Comment
1.	<input checked="" type="checkbox"/>	sensor5	10.66.79.195		RDEP IDS	Comment

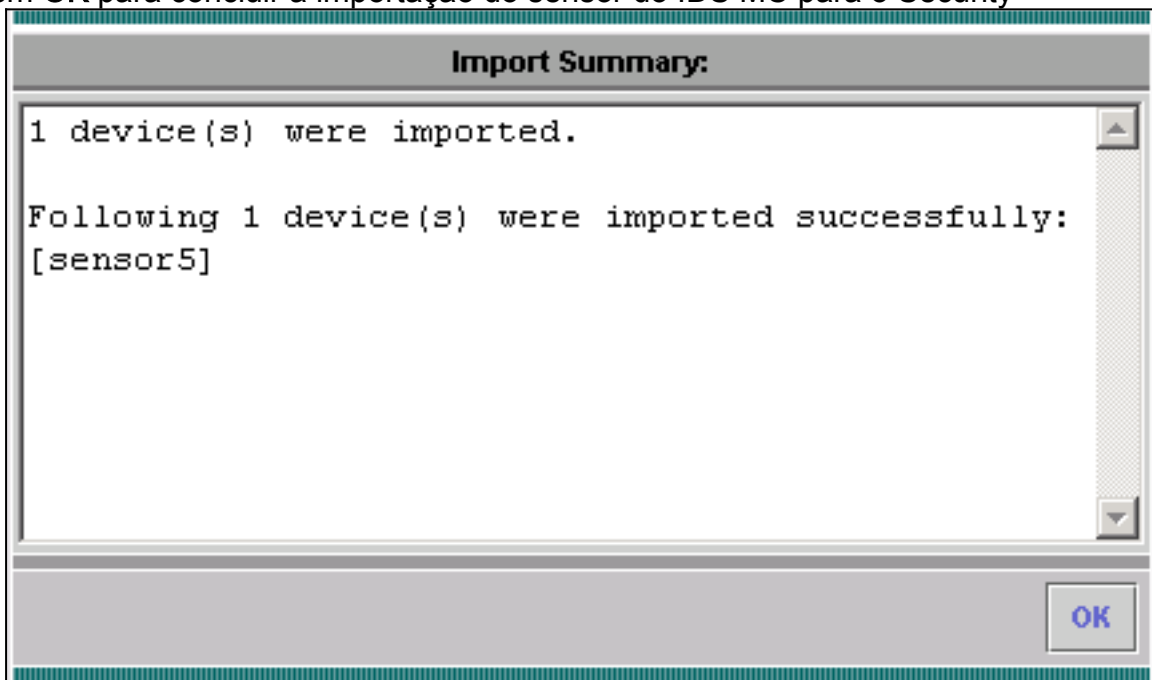
4. Se necessário, atualize o endereço NAT do seu sensor e clique em **Concluir** para continuar.

Showing 1 records

	Name	IP Address	 NAT Address
1.	sensor5	10.66.79.195	<input type="text"/>

 -- Editable columns

5. Clique em **OK** para concluir a importação do sensor do IDS MC para o Security



Monitor.

6. Agora você pode ver que seu sensor foi importado com êxito

Showing 1-1 of 1 records

	Device Name	IP Address	NAT Address	Device Type	Description
1. <input type="radio"/>	sensor5	10.66.79.195		RDEP IDS	Comment

Rows per page: << Page 1 >>

Usar IDS MC para atualizações de assinatura

Este procedimento explica como usar o IDS MC para atualizações de assinatura.

1. Baixe as [atualizações de assinatura do IDS de rede](#) (somente clientes [registrados](#)) e salve-as no diretório `C:\PROGRA~1\CSCOPx\MDC\etc\ids\updates\` no seu Servidor VMS.
2. No console do servidor VMS, escolha **VPN/Security Management Solution > Management Center > IDS Sensors**.
3. Selecione a guia Configuração e clique em **Atualizações**.
4. Clique em **Atualizar assinaturas de IDS de rede**.
5. Selecione a assinatura que deseja atualizar no menu suspenso e clique em **Apply** para continuar.

Update Network IDS Signature Settings

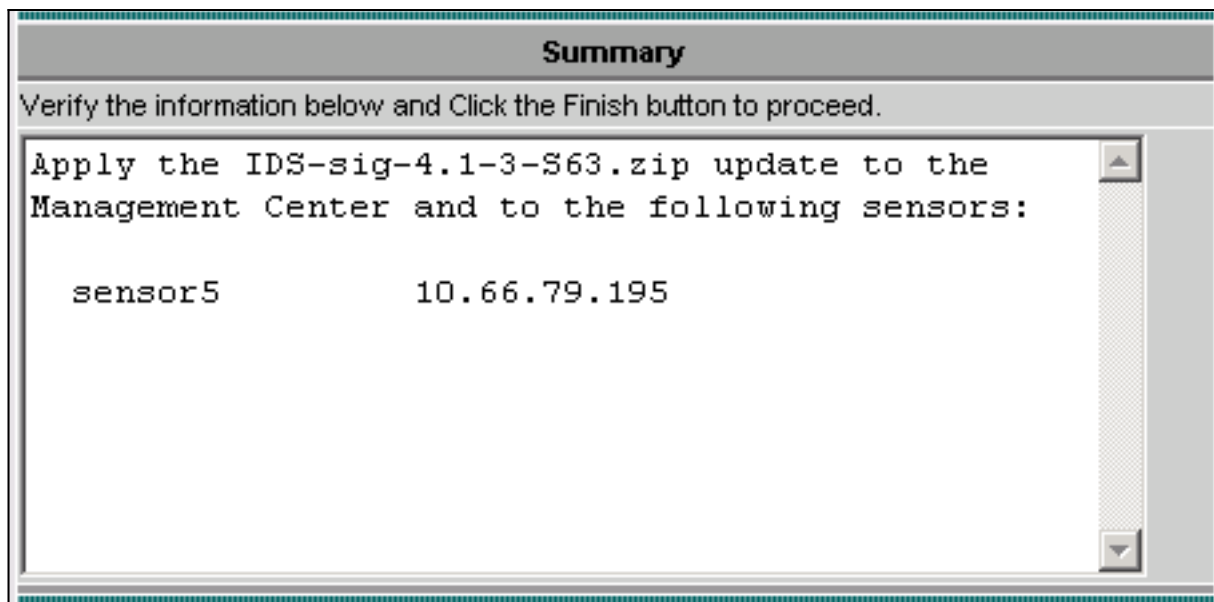
Update File: ▼

6. Selecione o(s) sensor(es) a atualizar e clique em **Avançar** para continuar.

Showing 1 records

	<input type="checkbox"/>	IP Address	Sensor Name	Version	Created By	Created On
1.	<input checked="" type="checkbox"/>	10.66.79.195	sensor5	4.1(3)S62	admin	2003-12-15 11:32:13

7. Depois de ser solicitado a aplicar a atualização ao Management Center, bem como ao Sensor, clique em **Finish** para continuar.



8. Faça Telnet ou console na interface de linha de comando do Sensor. Você vê informações semelhantes a estas:

```
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.
```

9. Aguarde alguns minutos para permitir que a atualização seja concluída e insira **show version** 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 redefinição de TCP para o roteador IOS](#)

Conclua estes passos para configurar a redefinição de TCP para o roteador IOS.

1. Escolha **VPN/Security Management Solution > Management Center > IDS Sensors**.
2. Selecione a guia **Configuração**, selecione seu sensor no Seletor de objeto e clique em **Configurações**.
3. Selecione **Assinaturas**, clique em **Personalizar** e clique em **Adicionar** para adicionar uma nova assinatura.

Signature Group: Filter Source:

Showing 0-0 of 0 records

<input type="checkbox"/>	ID	Signature	Subsig ID	Engine	Enabled	Severity	Action
No records.							

Rows per page: << Page 1 >>

- Insira o novo Nome da assinatura e selecione o Mecanismo (nesse caso, **STRING.TCP**).
- Marque o botão de opção apropriado para personalizar os parâmetros disponíveis e clique em **Editar**. Neste exemplo, o parâmetro ServicePorts é editado para alterar seu valor para **23** (para a porta 23). O parâmetro RegexString também é editado para adicionar o valor **testattack**. Quando terminar, clique em **OK** para continuar.

Tune Signature Parameters

Signature Name: *

Engine: *

Engine Description:

Showing 25 records

	Parameter Name	Value	Default	Required
1.	<input type="radio"/> ServicePorts	23		Yes
2.	<input type="radio"/> StorageKey	STREAM	STREAM	Yes
3.	<input type="radio"/> RegexString	testattack		Yes
4.	<input type="radio"/> SummaryKey	AaBb	AaBb	Yes
5.	<input type="radio"/> Direction	ToService	ToService	Yes
6.	<input type="radio"/> Protocol	TCP	TCP	Yes
7.	<input type="radio"/> AlarmDelayTimer			No
8.	<input type="radio"/> AlarmInterval			No
9.	<input type="radio"/> AlarmThrottle	Summarize	Summarize	No

- Clique no nome da assinatura para editar a Gravidade da assinatura e as ações ou para Habilitar/Desabilitar a assinatura.

Signature Group: Filter Source:

Showing 1-1 of 1 records

<input type="checkbox"/>	ID	Signature	Subsig ID	Engine	Enabled	Severity	Action
1. <input type="checkbox"/>	20001	mytest	0	STRING.TCP	Yes	Medium	None

Rows per page: << Page 1 >>

7. Nesse caso, a gravidade é alterada para **Alto** e a ação **Log & Reset** é escolhida. Clique em **OK** para

Edit Signature(s)

Signature:

Enable

Severity:

Actions: Log Reset Block Host Block Connection

continuar.

8. A assinatura completa é semelhante a esta:

Signature Group: Filter Source:

Showing 1-1 of 1 records

<input type="checkbox"/>	ID	Signature	Subsig ID	Engine	Enabled	Severity	Action
1. <input type="checkbox"/>	20001	mytest	0	STRING.TCP	Yes	High	Log,Reset

Rows per page: << Page 1 >>

9. Escolha **Configuration > Pending**, marque a configuração pendente para garantir que está correta e clique em

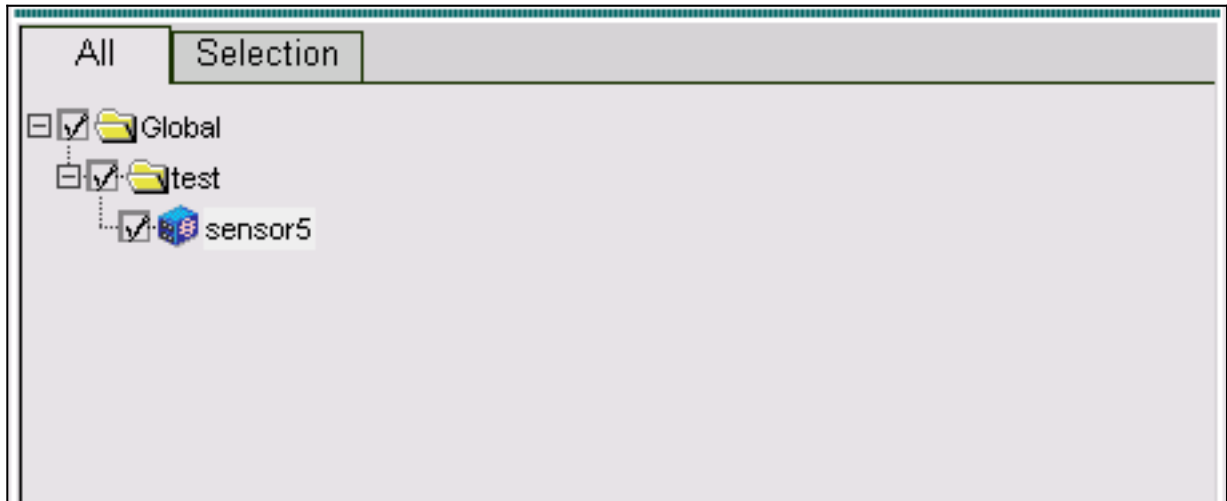
Showing 1-1 of 1 records

<input type="checkbox"/>	Pending Configuration	Type	Last Modified On	Last Modified By
1. <input checked="" type="checkbox"/>	Global.test.sensor5	Sensor	2003-12-15 14:07:39	admin

Rows per page: << Page 1 >>

Save.

10. Escolha **Deployment > Generate** e clique em **Apply** para enviar as alterações de configuração para o Sensor.



11. Escolha **Deployment > Deploy** e clique em **Submit**.
12. Marque a caixa de seleção ao lado de seu sensor e clique em **Implantar**.
13. Marque a caixa de seleção do trabalho na fila e clique em **Avançar** para continuar.

Showing 1-1 of 1 records				
<input type="checkbox"/>	Configuration File Name	Sensor Name	Generated On	Generated By
1. <input checked="" type="checkbox"/>	sensor5_2003-12-15_17:00:14	Global.test.sensor5	2003-12-15 17:00:14	admin

Rows per page: 10 < >> Page 1 <<

14. Insira o Nome do trabalho e agende-o como **Imediato** e clique em **Concluir**.

Schedule Type

Job Name:

Immediate

Scheduled

Start Time: : :

Retry Options

Maximum Number Of Attempts

Time Between Attempts minutes

Failure Options

Overwrite conflicting sensor(s) configuration?

Require correct sensor versions?

Notification Options

Email report to:

(When specifying more than one recipient, comma separate the addresses.)

15. Escolha **Deployment > Deploy > Pending**.Aguarde alguns minutos até que todos os trabalhos pendentes tenham sido concluídos. A fila deve estar vazia.
16. Escolha **Configuration > History** para confirmar a implantação.Verifique se o status da configuração é exibido como **Implantado**. Isso significa que a configuração do sensor foi atualizada com

Showing 1-1 of 1 records				
<input type="checkbox"/>	Configuration File Name	Status	Generated	Deployed
1. <input type="checkbox"/>	sensor5_2003-12-15_23:04:36	Deployed	2003-12-15 23:04:36	2003-12-15 23:09:55

Rows per page: << Page 1 >>

êxito.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Iniciar o ataque de TCP Reset (RST)

Inicie um ataque de teste e verifique os resultados para verificar se o processo de bloqueio funciona corretamente.

1. Antes de iniciar o ataque, escolha **VPN/Security Management Solution > Monitoring Center > Security Monitor**.

- Escolha **Monitor** no menu principal e clique em **Eventos**.
- Clique em **Iniciar Visualizador de Eventos**.

The screenshot shows a dialog box titled "Launch Event Viewer". It has several sections:

- Event Type:** A dropdown menu set to "Network IDS Alarms".
- Column Set:** A dropdown menu set to "Last Saved".
- Event Start Time:** Radio buttons for "At Earliest" (selected) and "At Time". The "At Time" option has date and time pickers set to December 15, 2003, 22:26:06.
- Event Stop Time:** Radio buttons for "Don't Stop" (selected) and "At Time". The "At Time" option has date and time pickers set to December 15, 2003, 22:26:06.
- A "Launch Event Viewer" button is located at the bottom right.

- Execute telnet de um roteador para o outro e digite **testattack** para iniciar o ataque. Nesse caso, fizemos Telnet do roteador Light para o roteador House. Assim que você pressionar **<space>** ou **<enter>**, depois de digitar **testattack**, sua sessão Telnet deverá ser redefinida.

```
light#telnet 100.100.100.1
Trying 100.100.100.1 ... Open
User Access Verification
Password:
house>en
Password:
house#testattack
```

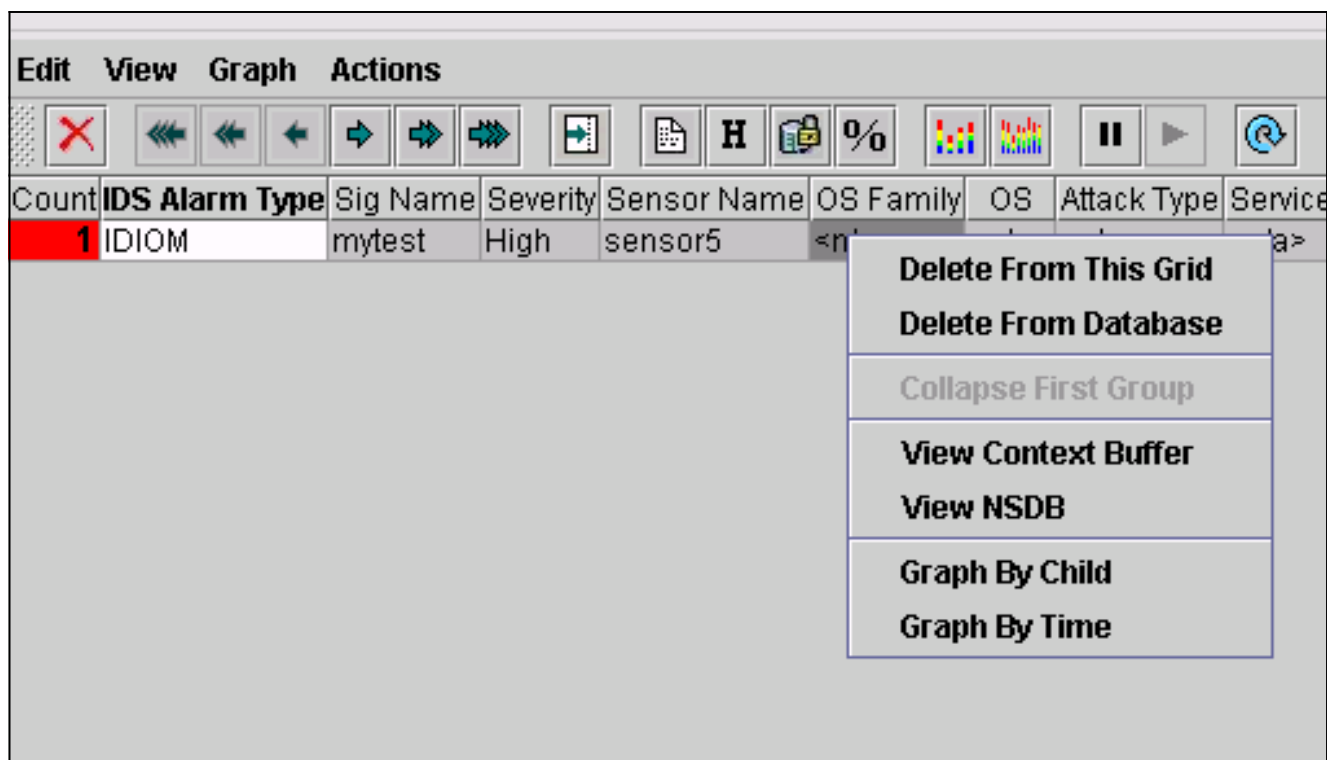
!--- The Telnet session is reset due to the !--- signature "testattack" being triggered. [Connection to 100.100.100.1 lost]

- No Visualizador de Eventos, clique em **Consultar Banco de Dados** para novos eventos agora. Você vê o alerta para o ataque iniciado anteriormente

The screenshot shows the "Event Viewer" interface. At the top, it says "You Are Here: Monitor > Events". Below that is a menu bar with "Edit", "View", "Graph", and "Actions". A toolbar contains various icons for navigation and actions. Below the toolbar is a table of events:

Count	IDS Alarm Type	Sig Name	Severity	Sensor Name	OS Family	OS	Attack Type	Service	Protocol	Prot
1	IDIOM	mytest	High	sensor5	<n/a>	<n/a>	<n/a>	<n/a>	<n/a>	<n/a>

- No Visualizador de Eventos, realce o alarme, clique com o botão direito do mouse nele e selecione **Exibir Buffer de Contexto** ou **Exibir NSDB** para exibir informações mais detalhadas sobre o alarme.



[Troubleshoot](#)

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

[Procedimento de Troubleshooting](#)

Complete estas etapas para resolver problemas.

1. No IDS MC, escolha **Reports > Generate**. Dependendo do tipo de problema, mais detalhes devem ser encontrados em um dos sete relatórios disponíveis.

Report Group: Audit Log		
Showing 1-7 of 7 records		
Available Reports ▼		
1.	<input type="radio"/>	Subsystem Report
2.	<input type="radio"/>	Sensor Version Import Report
3.	<input type="radio"/>	Sensor Configuration Import Report
4.	<input checked="" type="radio"/>	Sensor Configuration Deployment Report
5.	<input type="radio"/>	IDS Sensor Versions
6.	<input type="radio"/>	Console Notification Report
7.	<input type="radio"/>	Audit Log Report

Rows per page: << Page 1 >>

2. Enquanto o bloqueio utiliza a porta de comando e controle para configurar as listas de acesso do roteador, as redefinições de TCP são enviadas da interface de sniffing do sensor. Certifique-se de que você tenha estendido a porta correta, usando o comando **set span** no switch, semelhante a este:

set span

```
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
!--- In this case, connect to Ethernet1 of Router House. Oper Source : Port 2/12
Direction       : transmit/receive
Incoming Packets: enabled
Learning        : enabled
Multicast       : enabled
```

3. Se TCP Reset não estiver funcionando, faça login no Sensor e digite o comando **show event**. Inicie o ataque e verifique se o alarme é disparado ou não. Se o alarme for disparado, verifique se ele está definido para o tipo de ação **TCP reset**.

[Informações Relacionadas](#)

- [Página de suporte do Cisco Secure Intrusion Detection](#)
- [Documentação para Cisco Secure Intrusion Detection System](#)
- [Página de Suporte da Solução de Gerenciamento de Segurança/VPN CiscoWorks](#)

- [Suporte Técnico e Documentação - Cisco Systems](#)