

Configurar el Restablecimiento TCP IDS usando los VMS ID MC

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Configuración del sensor inicial](#)

[Importe el sensor en IDS MC](#)

[Importe el sensor en el monitor de la Seguridad](#)

[Utilice IDS MC para las actualizaciones de firma](#)

[Configure el Restablecimiento TCP para el router IOS](#)

[Verificación](#)

[Inicie el ataque y reinicie TCP](#)

[Troubleshooting](#)

[Procedimiento de Troubleshooting](#)

[Información Relacionada](#)

[Introducción](#)

El documento proporciona una configuración de muestra del Sistema de detección de intrusos de Cisco (IDS) vía la solución de administración de seguridad/VPN (VMS), la consola de administración IDS (IDS MC). En este caso, el Restablecimiento TCP del sensor IDS a un router Cisco se configura.

[prerrequisitos](#)

[Requisitos](#)

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- El sensor está instalado y configurado para detectar el tráfico necesario.
- La interfaz de rastreo se atraviesa a la interfaz exterior del router.

[Componentes Utilizados](#)

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- VMS 2.2 con IDS MC y el monitor 1.2.3 de la Seguridad
- Sensor del Cisco IDS 4.1.3S(63)
- Router Cisco que funciona con el Software Release 12.3.5 de Cisco IOS®

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 TécnicosCisco](#) para obtener más información sobre las convenciones del documento.

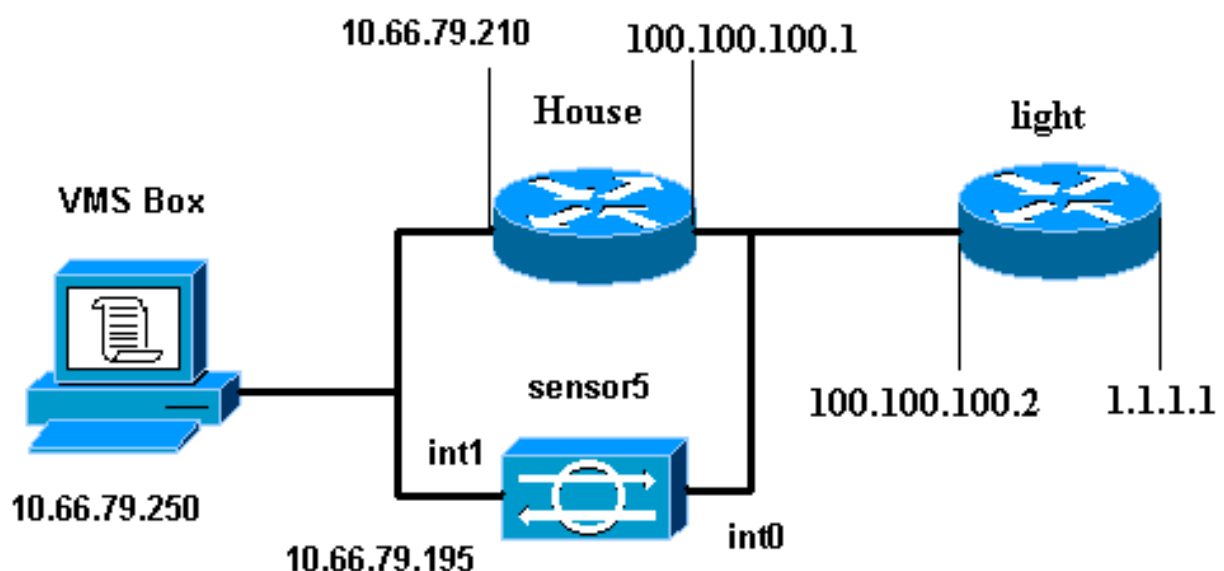
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta [Command Lookup Tool](#) ([clientes registrados solamente](#)) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuraciones

Este documento usa estas configuraciones.

- [Luz del router](#)
- [Base del router](#)

Luz del router
<pre> 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 </pre>
Base del router
<pre> 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 </pre>

[Configuración del sensor inicial](#)

Nota: Si usted ha realizado ya la configuración inicial de su sensor, procede a la [importación el sensor en la sección IDS MC](#).

1. Consola en el sensor. Le indican para un nombre de usuario y contraseña. Si esto está la primera vez usted está consolandó en el sensor, usted debe iniciar sesión con el nombre de usuario cisco y la palabra clave Cisco.
2. A le indican que cambie la contraseña y escriba de nuevo la nueva contraseña a máquina para confirmar.

3. Teclee la **configuración** y ingrese la información apropiada en cada prompt para configurar los parámetros básicos para su sensor, según este ejemplo:
- ```
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
```

## Importe el sensor en IDS MC

Complete estos pasos para importar el sensor en el IDS MC.

1. Hojee a su sensor. En este caso, <http://10.66.79.250:1741> o <https://10.66.79.250:1742>.
2. Login con el nombre de usuario y contraseña apropiado. En este ejemplo, el nombre de usuario es **admin** y la contraseña es **Cisco**.
3. Elija el **VPN/Security Management Solution (Solución de administración de seguridad/VPN) > Management Center (Centro de administración)** y haga clic los **sensores IDS**.
4. Haga clic la lengüeta de los dispositivos y elija el **grupo del sensor**.
5. Resalte **global** y el tecleo **crea al subgrupo**.
6. Ingrese el nombre del grupo y asegúrese de que el **valor por defecto** está elegido, después hacen clic la **AUTORIZACIÓN** para agregar al subgrupo en el IDS

**Add Group**

Group Name: \* test

Parent: Global

Description:

Settings:

Default (use parent values)

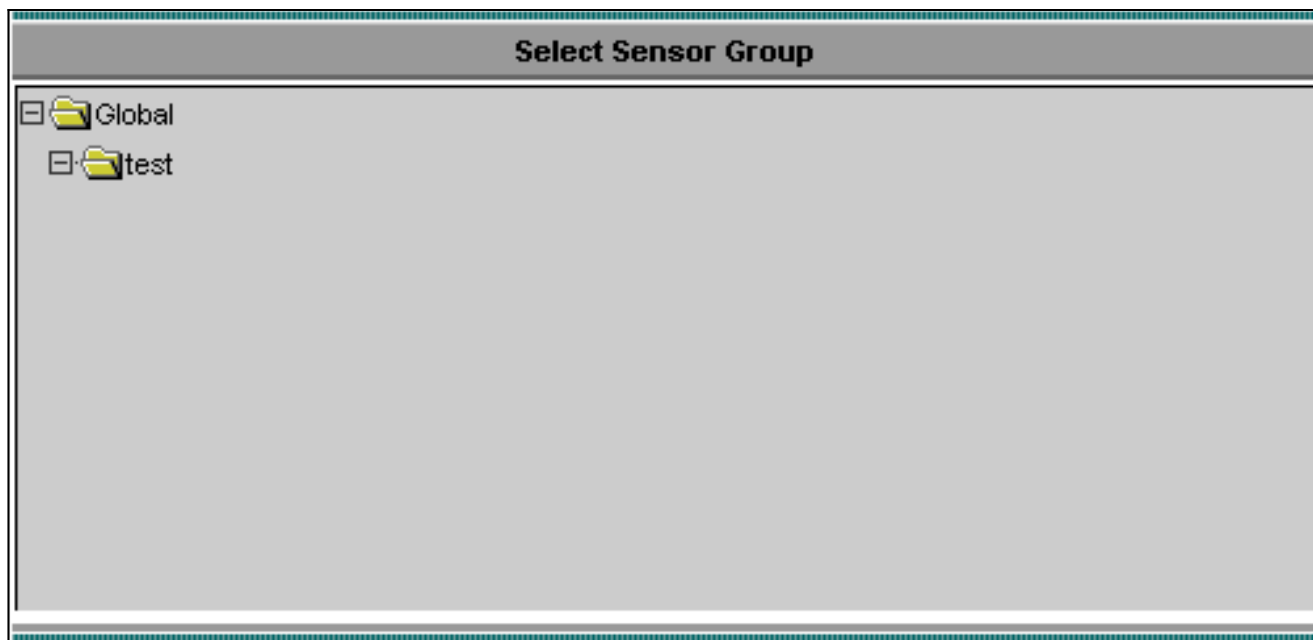
Copy settings from group Global

OK Cancel

Note: \* - Required Field

MC.

7. Elija los **dispositivos > el sensor**, resalte el subgrupo creado en el paso anterior (en este caso, **prueba**), y el haga click en **Add**
8. Resalte al subgrupo y haga clic **después**.

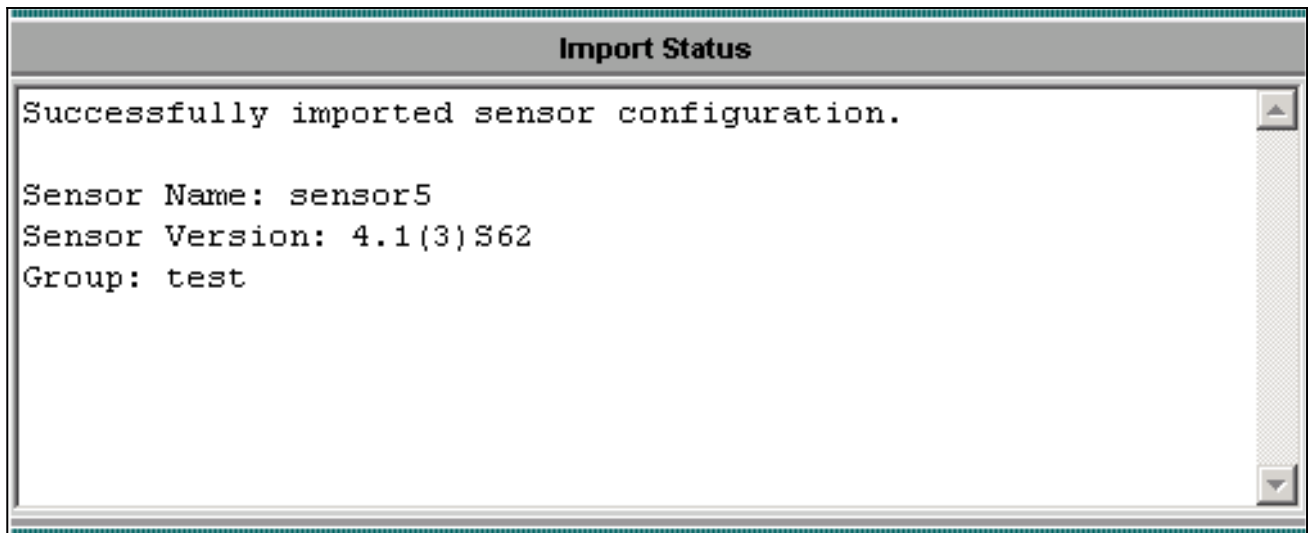


9. Ingrese los detalles según este ejemplo y haga clic **después** para continuar.

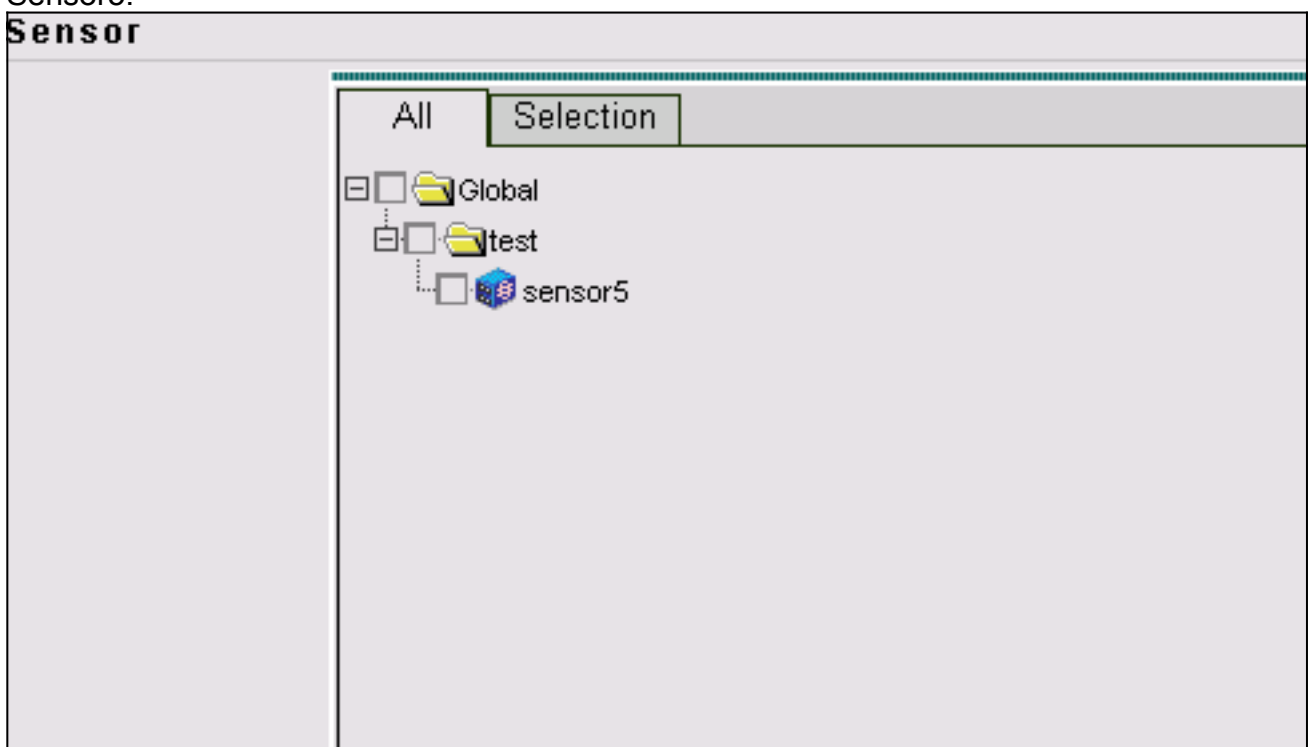
| Identification                                           |                                               |
|----------------------------------------------------------|-----------------------------------------------|
| IP Address: *                                            | <input type="text" value="10.66.79.195"/>     |
| NAT Address:                                             | <input type="text"/>                          |
| Sensor Name (required if not Discovering Settings):      | <input type="text" value="sensor5"/>          |
| Discover Settings:                                       | <input checked="" type="checkbox"/>           |
| SSH Settings:                                            |                                               |
| User ID: *                                               | <input type="text" value="cisco"/>            |
| Password: (or pass phrase if using existing SSH keys): * | <input type="password" value="XXXXXXXXXXXX"/> |
| Use Existing SSH keys:                                   | <input type="checkbox"/>                      |

Note: \* - Required Field

10. Cuando le presentan con un mensaje que estado la Configuración del sensor con éxito importada, clic en Finalizar para continuar.



11. Su sensor se importa en el IDS MC. En este caso, se importa Sensor5.



### [Importe el sensor en el monitor de la Seguridad](#)

Complete estos pasos para importar el sensor en el monitor de la Seguridad.

1. En el menú del servidor VMS, elija **monitor de centro del > Security (Seguridad) de la solución de administración de seguridad/VPN > de la supervisión.**
2. Seleccione la lengüeta de los dispositivos, después haga clic la **importación** y ingrese la información del servidor IDS MC, según este

**Enter IDS MC server contact information:**

|                         |              |
|-------------------------|--------------|
| IP Address/Host Name: * | 10.66.79.250 |
| Web Server Port: *      | 443          |
| Username: *             | admin        |
| Password: *             | *****        |

Note: \* - Required Field

ejemplo.


3. Seleccione su sensor (en este caso, **sensor5**) y haga clic **después** 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 |

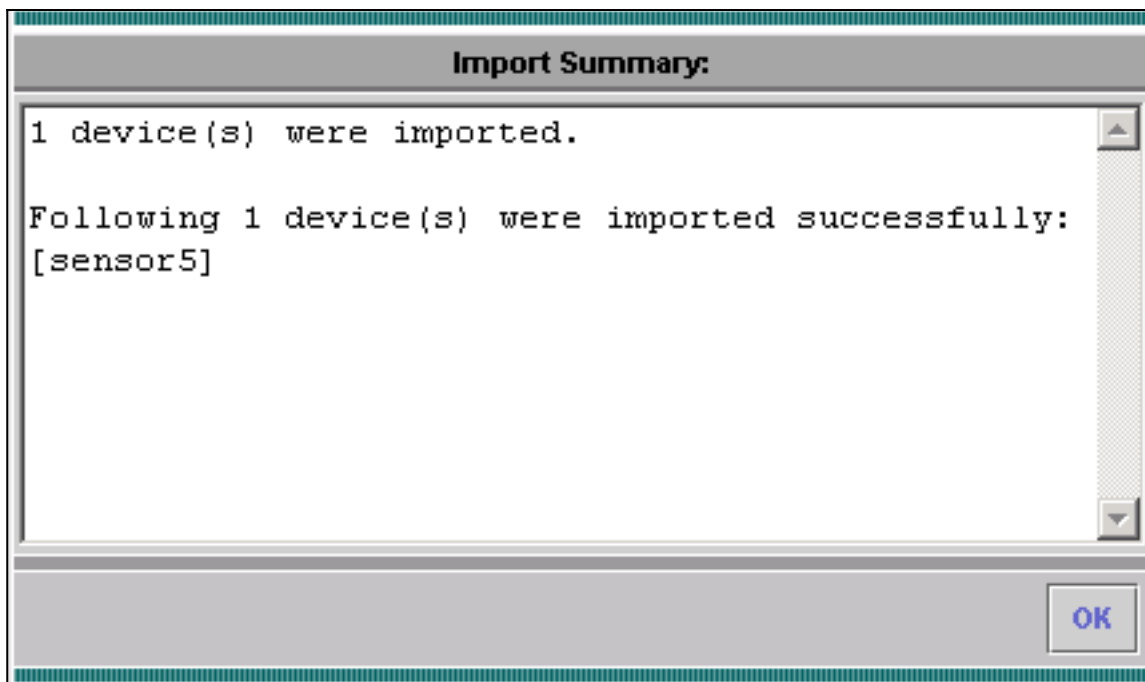
4. Si es necesario, ponga al día el direccionamiento NAT para su sensor, después clic en Finalizar para continuar.

Showing 1 records

|    | Name    | IP Address   |  NAT Address |
|----|---------|--------------|---------------------------------------------------------------------------------------------------|
| 1. | sensor5 | 10.66.79.195 |                                                                                                   |

 -- Editable columns

5. Haga Click en OK para acabar de importar el sensor de IDS MC en el monitor de la



Seguridad.

6. Usted puede ahora ver que su sensor está importado con éxito

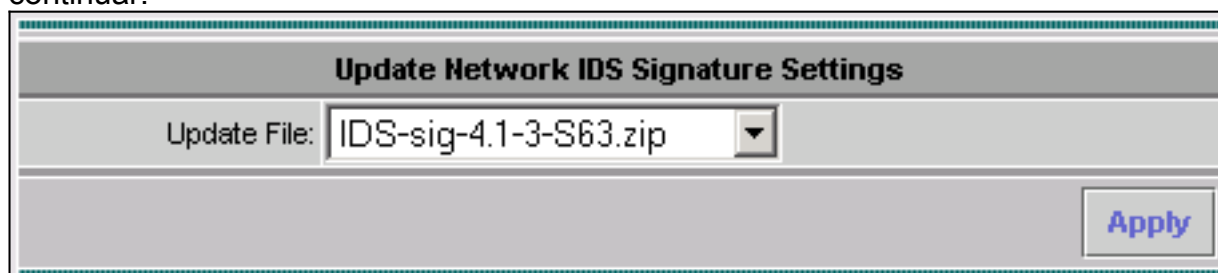
| Showing 1-1 of 1 records |                               |              |             |             |             |  |
|--------------------------|-------------------------------|--------------|-------------|-------------|-------------|--|
|                          | Device Name                  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

Rows per page:  << Page 1 >>

## [Utilice IDS MC para las actualizaciones de firma](#)

Este procedimiento explica cómo utilizar IDS MC para las actualizaciones de firma.

1. Descargue las [actualizaciones de firma de los ID de la red \(clientes registrados solamente\)](#) y sávelas en el directorio `C:\PROGRA~1\CSCOpX\MDC\etc\ids\updates\` en su servidor VMS.
2. En la consola del servidor VMS, elija el **VPN/Security Management Solution (Solución de administración de seguridad/VPN) > Management Center (Centro de administración) > IDS Sensors (Sensores IDS)**.
3. Seleccione la ficha de configuración y haga clic las **actualizaciones**.
4. Haga clic las **firmas de los ID de la red de la actualización**.
5. Seleccione la firma que usted quiere actualizar del menú desplegable y el tecleo **se aplica** para continuar.

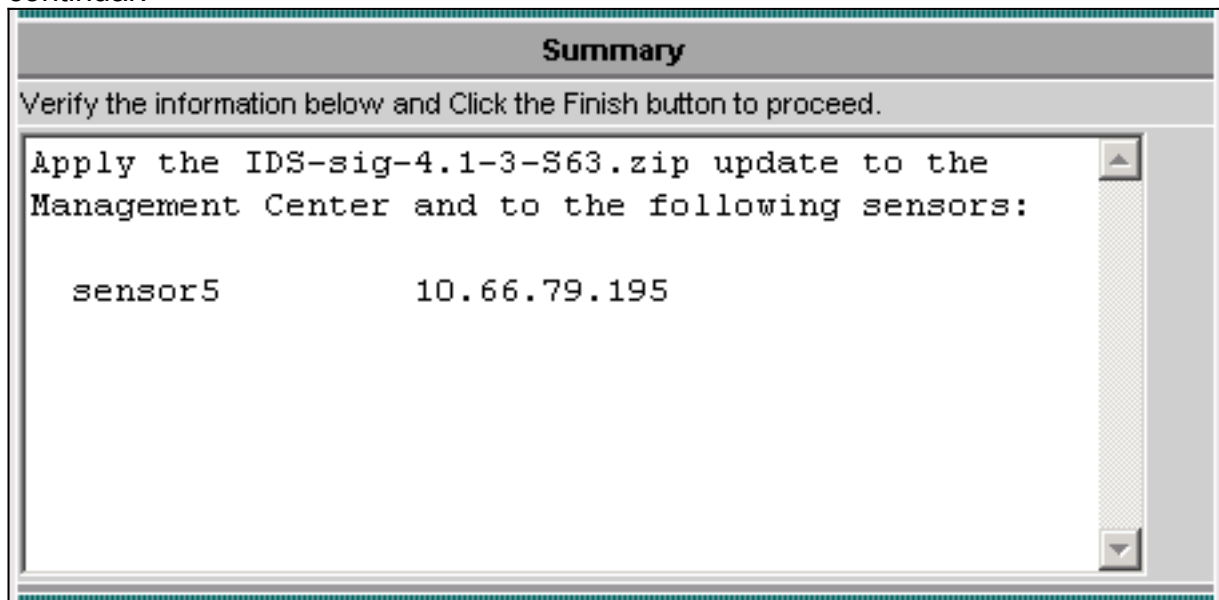




6. Seleccione los sensores para ponerse al día y para hacer clic **después** para continuar.

| 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. Después de que a le indiquen que aplique la actualización al centro de administración, así como el sensor, clic en Finalizar para continuar.



8. Telnet o consola en la interfaz de línea de comando del sensor. Usted ve la información similar a esto:

```
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. Espere algunos minutos para permitir que la actualización complete, después ingrese la **versión de la demostración** 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
```

[Configure el Restablecimiento TCP para el router IOS](#)

Complete estos pasos para configurar el Restablecimiento TCP para el router IOS.

1. Elija el VPN/Security Management Solution (Solución de administración de seguridad/VPN) > Management Center (Centro de administración) > IDS Sensors (Sensores IDS).

2. Seleccione la ficha de configuración, seleccione su sensor del selector del objeto, después haga clic las **configuraciones**.
3. Seleccione las **firmas**, haga clic la **aduana**, y el tecleo **agrega** para agregar una nueva firma.

4. Ingrese el nuevo nombre de la firma, después seleccione el motor (en este caso, **STRING.TCP**).
5. Marque el botón Appropriate Radio Button para personalizar los parámetros disponibles y entonces hacer clic **edite**. En este ejemplo, el parámetro de ServicePorts se edita para cambiar su valor a **23** (para el puerto 23). El parámetro RegexString también se edita para agregar el **testattack** del valor. Cuando esto es completo, haga clic la **AUTORIZACIÓN** para continuar.

	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

6. Haga clic el nombre de la firma para editar el Signature Severity (severidad de firma) y las acciones o habilitarlos/neutralización la firma.

Signature Group: Custom Filter Source: Signature Filter

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: 10 << Page 1 >>

Add Edit Delete

7. En este caso, la gravedad se cambia al **alto** y se elige el **registro** y la **restauración de la acción**. Haga Click en OK para

Edit Signature(s)

Signature:

Enable

Severity:

Actions: Log Reset Block Host Block Connection

OK Cancel

continuar.

8. La firma completa parece similar a esto:

Signature Group: Custom Filter Source: ID Filter

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: 10 << Page 1 >>

Add Edit Delete

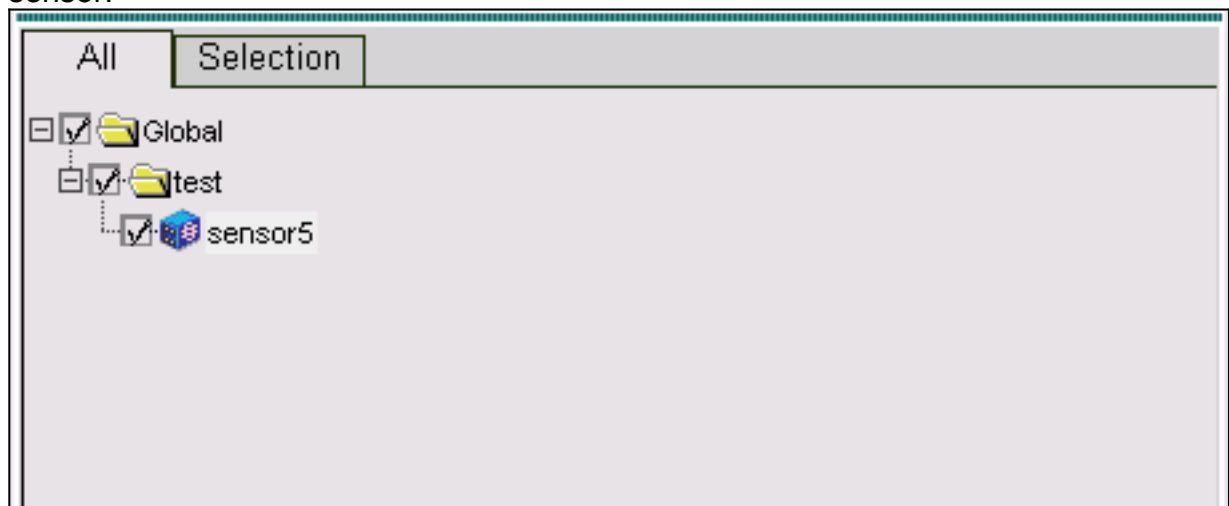
9. Elija la **configuración > pendiente**, marque la configuración pendiente para asegurarse que está correcta, y que hace clic la **salvaguardia**.

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: 10 << Page 1 >>

Save Delete

10. Elija el **despliegue > generan**, y después hacen clic **se aplican** para avanzar los cambios de configuración al sensor.



11. Elija el **Deployment (Implementación) > Deploy (Implementar)** y el tecleo **somete**.
 12. Marque el checkbox al lado de su sensor y el tecleo **despliega**.
 13. Marque el checkbox para el trabajo en la cola y haga clic **después** 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. Ingrese el Nombre de trabajo y programe el trabajo como **inmediato**, después haga clic el **final**.

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. Elija el **Deployment (Implementación) > Deploy (Implementar) pendiente**. Espere algunos minutos hasta que se hayan completado todas las tareas pendientes. La cola debe entonces estar vacía.
16. Elija la **configuración > el historial** para confirmar el despliegue. Asegúrese que el estatus de la configuración esté visualizado según lo **desplegado**. Esto significa que la Configuración del sensor está puesta al día con

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 >>

éxito.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Inicie el ataque y reinicie TCP

Ponga en marcha un ataque de la prueba y marque los resultados para verificar que los trabajos de proceso de bloqueo correctamente.

1. Antes de que se inicie el ataque, elija **monitor de centro del > Security (Seguridad)** de la

solución de administración de seguridad/VPN > de la supervisión.

2. Elija el **monitor** del menú principal y de los eventos click.
3. Haga clic el **visor de eventos del lanzamiento**.

Launch Event Viewer

Event Type: Network IDS Alarms

Column Set: Last Saved

Event Start Time: At Earliest
 At Time December 15 2003 22 : 26 : 06

Event Stop Time: Don't Stop
 At Time December 15 2003 22 : 26 : 06

Launch Event Viewer

4. Telnet a partir de un router al otro y al **testattack** del tipo para poner en marcha el ataque. En este caso, nosotros telnetted del indicador luminoso del router a la Casa del router. Tan pronto como usted presione **<space>** o **<enter>**, después de que usted teclee el **testattack**, su sesión telnet debe ser reajustada.
`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]`
5. Del visor de eventos, **base de datos de la interrogación del teclado** para los nuevos eventos ahora. Usted ve la alerta para el ataque previamente iniciado

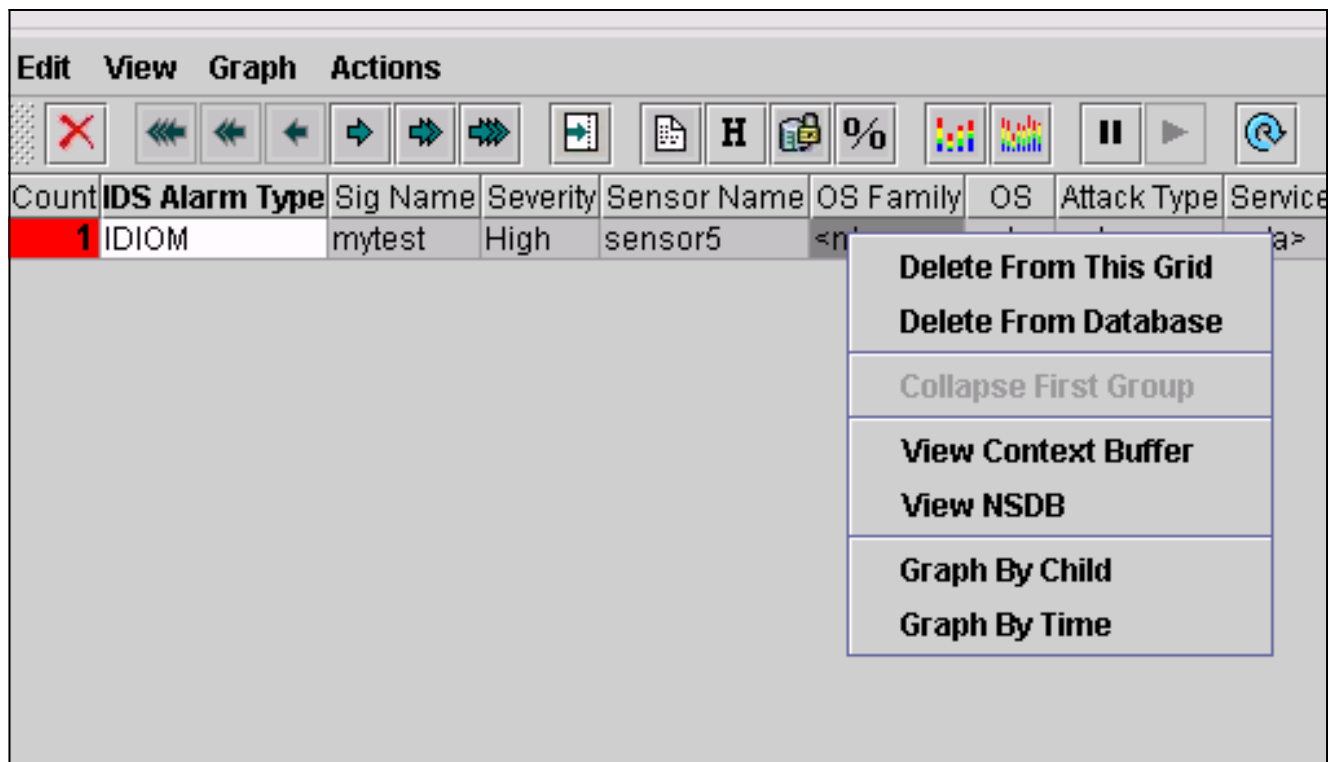
You Are Here: [Monitor](#) > [Events](#)

Edit View Graph Actions

Event Viewer

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>

6. En el visor de eventos, resalte la alarma, hagala clic con el botón derecho del ratón y seleccione el **buffer** o la **visión NSDB del contexto de la visión** para ver más información detallada sobre la alarma.



[Troubleshooting](#)

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

[Procedimiento de Troubleshooting](#)

Complete estos pasos para resolver problemas.

1. En el IDS MC, elija los **informes > generan**. Dependiendo del tipo de problema, otros detalles se deben encontrar en uno de los siete informes disponibles.

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 >>

- Mientras que el bloqueo utiliza el comando y el puerto de control de configurar las listas de acceso del router, las restauraciones TCP se envían de la interfaz de rastreo del sensor. Asegúrese que usted haya atravesado el puerto correcto, usando el **comando set span** en el Switch, similar a esto:

```
set span <src_mod/src_port><dest_mod/dest_port> both inpkts enable 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
```
- Si el Restablecimiento TCP no está trabajando, inicie sesión al sensor y ingrese el **comando show event**. Ponga en marcha el ataque, y el control para ver independientemente de si la alarma está accionada. Si se acciona la alarma, el control para asegurarla se fija para el Restablecimiento TCP del tipo de la acción.

Información Relacionada

- [Página de soporte de Cisco Secure Intrusion Detection](#)
- [Documentación para Cisco Secure Intrusion Detection System](#)
- [Página de soporte de la Solución CiscoWorks VPN/Security Management](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)