

Configurar el IDS que bloquea 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 bloqueo para el router IOS](#)

[Verificación](#)

[Ponga en marcha el ataque y el bloqueo](#)

[Troubleshooting](#)

[Procedimiento de Troubleshooting](#)

[Información Relacionada](#)

[Introducción](#)

Este documento proporciona una muestra para la configuración 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, bloqueando del sensor IDS a un router Cisco se configura.

[prerrequisitos](#)

[Requisitos](#)

Antes de que usted configure el bloqueo, asegúrese que usted haya cumplido estas condiciones.

- 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 estas 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](#)

Para obtener más información sobre las convenciones del documento, consulte [Convenciones de Consejos Técnicos de Cisco](#).

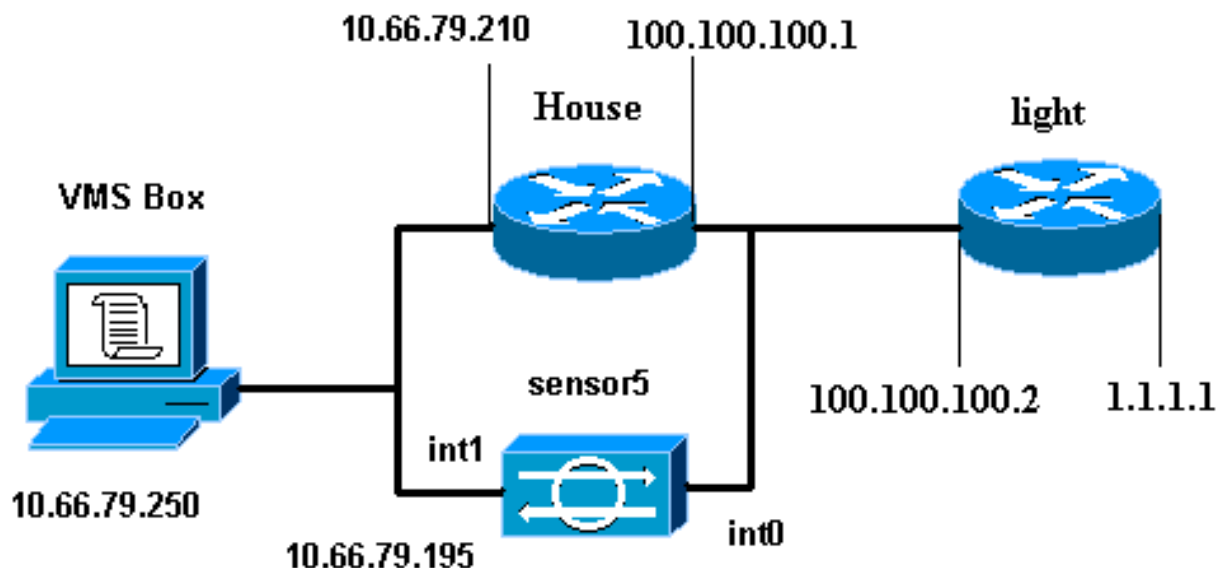
[Configurar](#)

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

Nota: Para obtener información adicional sobre los comandos que se utilizan en este documento, use la Command Lookup Tool (solo para clientes [registrados](#)).

[Diagrama de la red](#)

Este documento utiliza la configuración de red que se muestra en el siguiente diagrama.



[Configuraciones](#)

Este documento usa las configuraciones detalladas aquí.

- [Luz del router](#)

- [Base del router](#)

```

Luz del router
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

```

```

Base del router
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

```

[Configuración del sensor inicial](#)

Complete estos pasos para configurar inicialmente el sensor.

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

1. Consola en el sensor. Le indican para un nombre de usuario y contraseña. Si esto está la primera vez usted está consolandose 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 después 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
```
4. Prensa **2** para salvar su configuración.

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, hojee a <http://10.66.79.250:1741> o a <https://10.66.79.250:1742>.
2. Inicie sesión con el nombre de usuario y contraseña apropiado. En este ejemplo, el nombre del usuario administrador y la palabra clave Cisco fueron utilizados.
3. Seleccione el **VPN/Security Management Solution (Solución de administración de seguridad/VPN) > Management Center (Centro de administración)** y elija los sensores IDS.
4. Haga clic la lengüeta de los dispositivos, **grupo selecto del sensor**, resalte **global**, y el tecleo **crea al subgrupo**.
5. Ingrese el nombre del grupo y asegúrese que el botón de radio **predeterminado** está seleccionado, después que hace clic la **AUTORIZACIÓN** para agregar al subgrupo en el IDS

Add Group

Group Name: * test

Parent: Global

Description:

Settings:

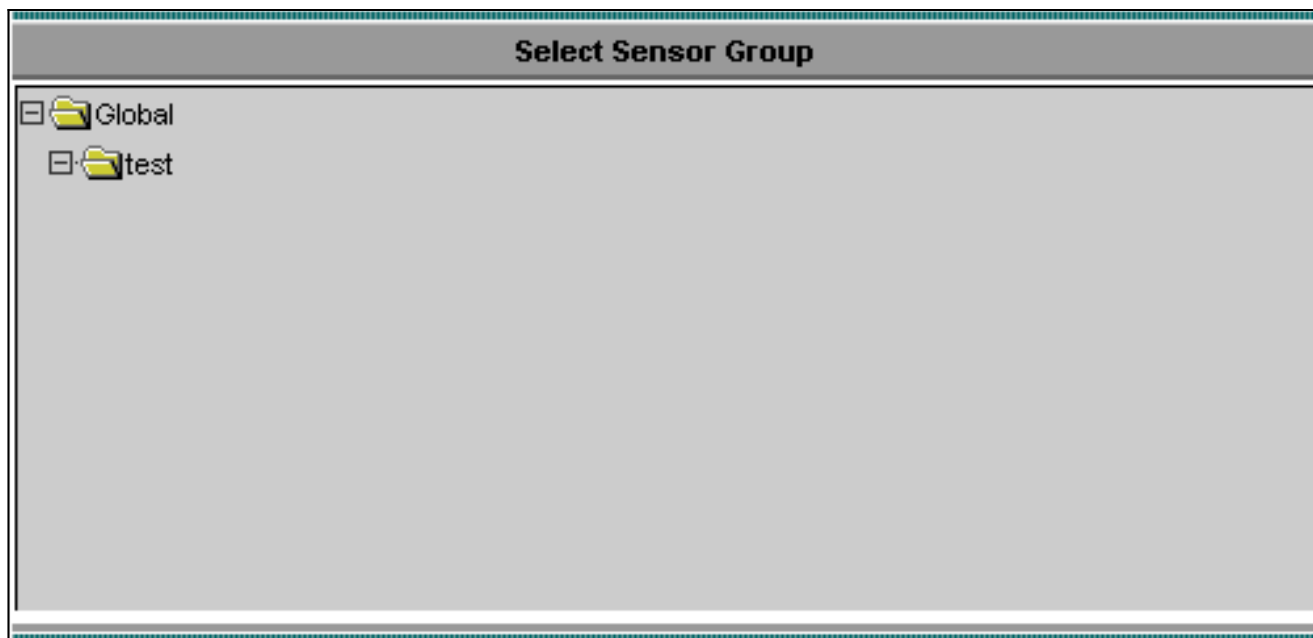
Default (use parent values)

Copy settings from group Global

OK Cancel

Note: * - Required Field

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

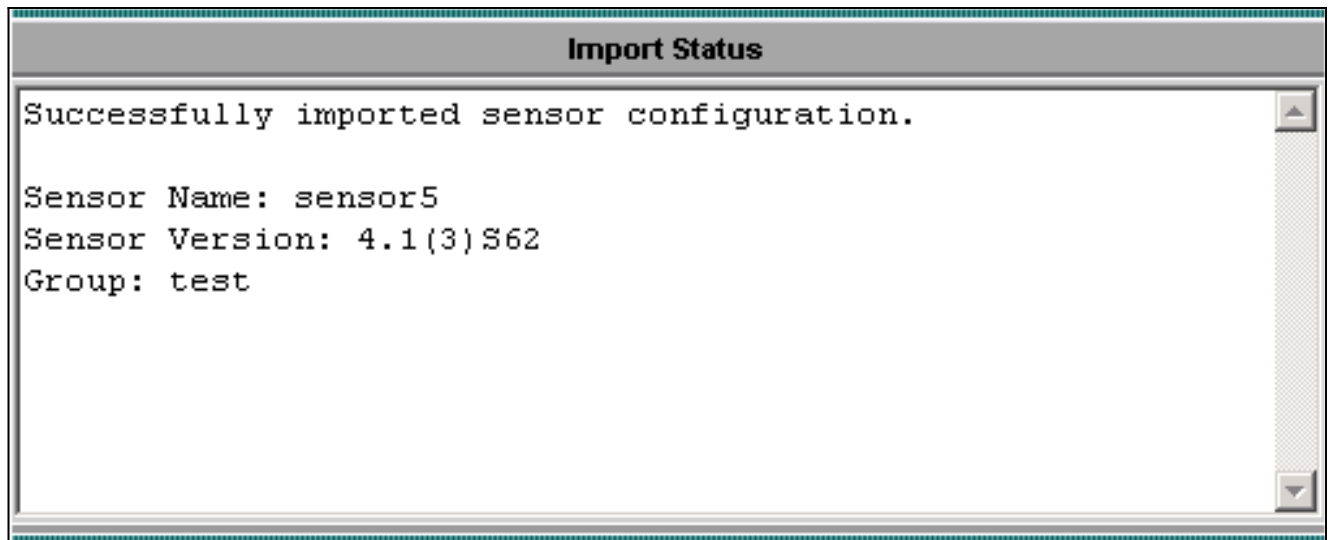


8. Ingrese los detalles según este ejemplo, después haga clic **al lado de** continúan.

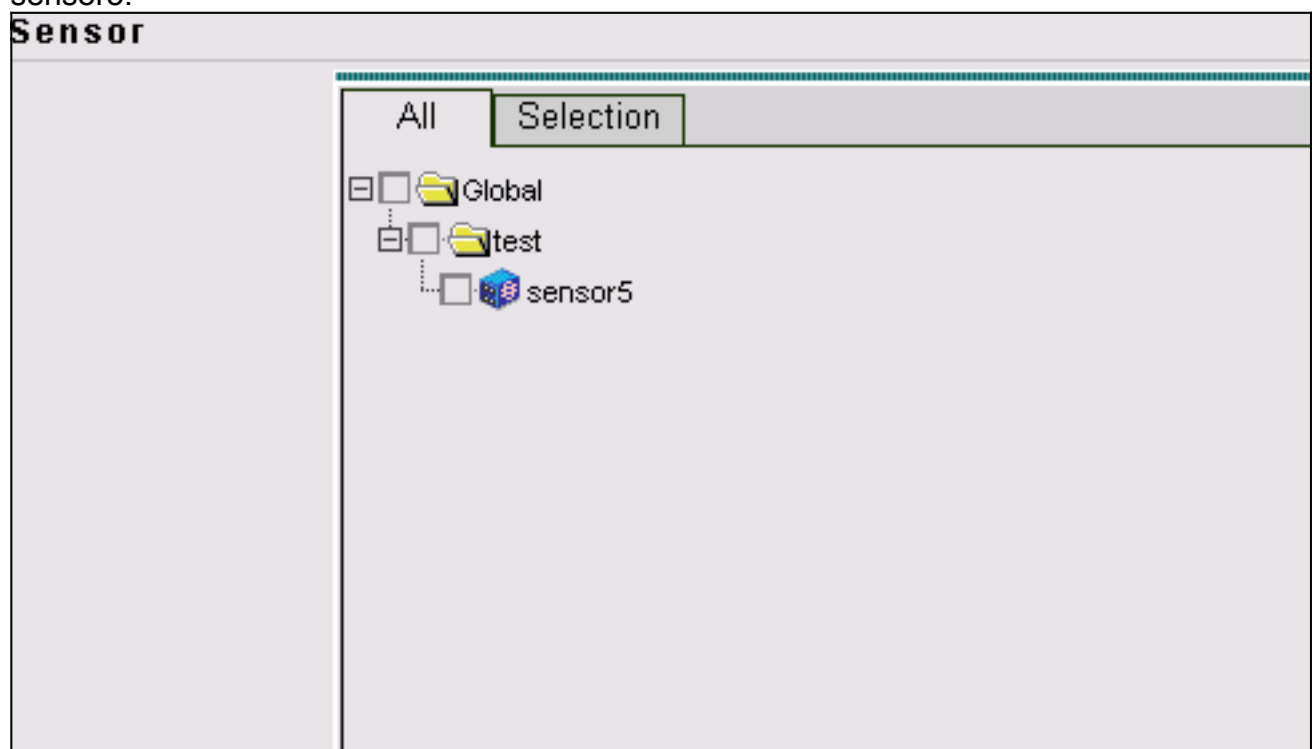
Identification	
IP Address: *	<input type="text" value="10.66.79.195"/>
NAT Address:	<input type="text"/>
Sensor Name (required if not Discovering Settings):	<input type="text" value="sensor5"/>
Discover Settings:	<input checked="" type="checkbox"/>
SSH Settings:	
User ID: *	<input type="text" value="cisco"/>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

Note: * - Required Field

9. Después de que le presenten con un mensaje que estado la Configuración del sensor con éxito importada, clic en Finalizar a continuar.



10. Su sensor se importa en el IDS MC. En este caso, se importa sensor5.



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

Complete este procedimiento para importar el sensor en el monitor de la Seguridad.

1. En el menú del servidor VMS, **monitor de centro del > Security (Seguridad)** de la **solución de administración de seguridad/VPN** selecta **>** 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 **al lado de** continúan.


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

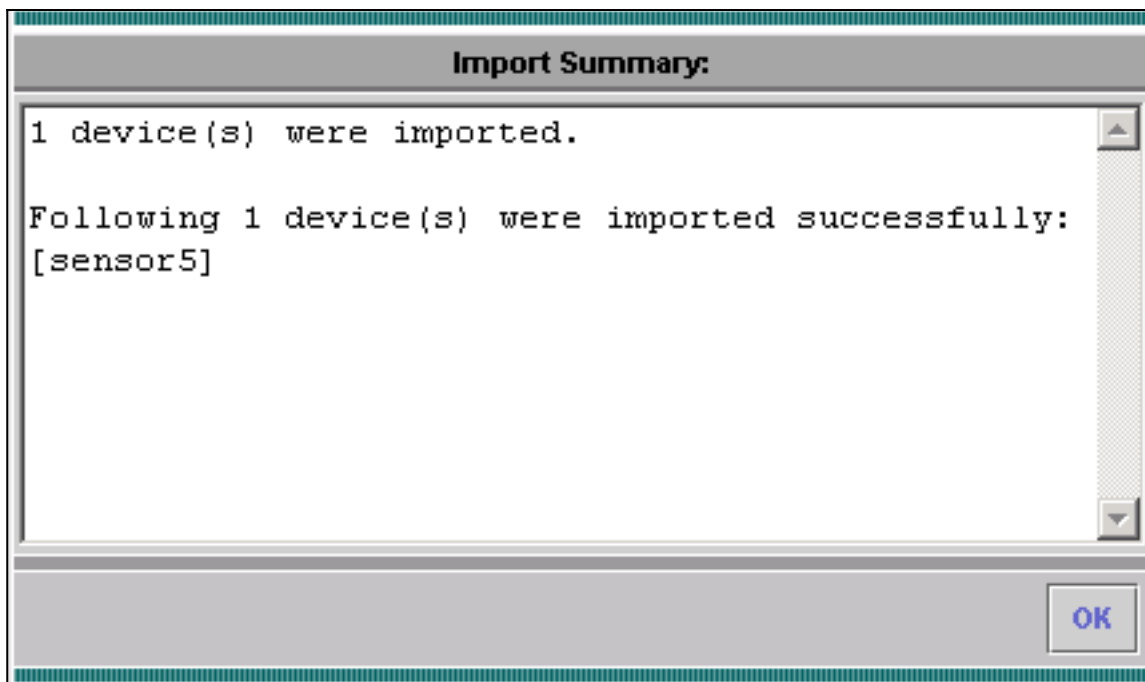
4. Si se da el caso, ponga al día el direccionamiento del Network Address Translation (NAT) para que su sensor, después clic en Finalizar continúen.

Showing 1 records

	Name	IP Address	 NAT Address
1.	sensor5	10.66.79.195	

 -- Editable columns

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



Seguridad.

6. Su sensor se importa 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](#)

Complete este procedimiento para utilizar el IDS MC para las actualizaciones de firma.

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

Update Network IDS Signature Settings

Update File:

5. Seleccione los sensores para ponerse al día, y el tecleo **al lado de** continúa.

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

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

Summary

Verify the information below and Click the Finish button to proceed.

```
Apply the IDS-sig-4.1-3-S63.zip update to the
Management Center and to the following sensors:

sensor5          10.66.79.195
```

7. Telnet o consola en la interfaz de línea de comando del sensor. La información similar a esto aparece:

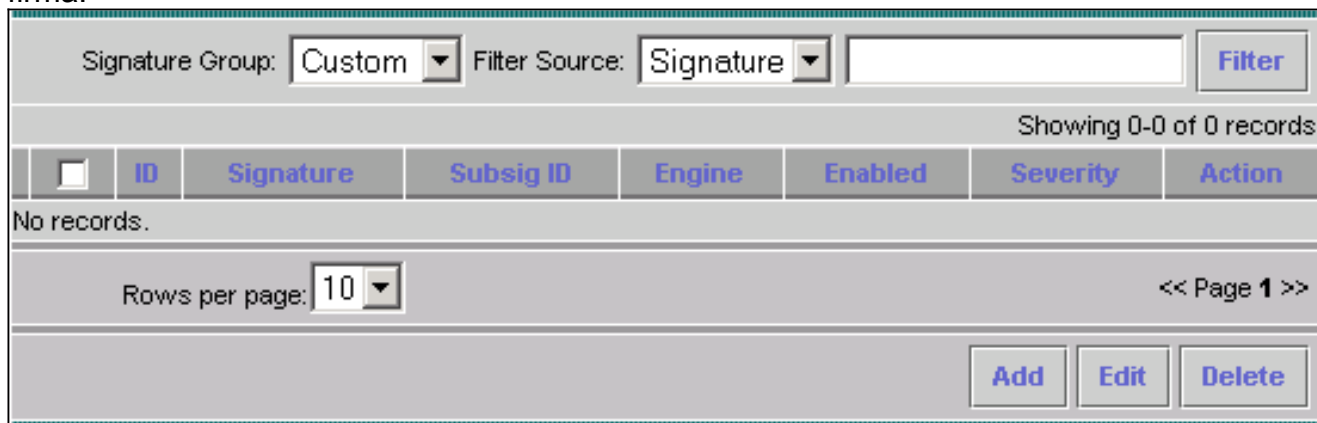
```
sensor5#
Broadcast message from root (Mon Dec 15 11:42:05 2003):
Applying update IDS-sig-4.1-3-S63. This may take several minutes. Please do not reboot the
sensor during this update. Broadcast message from root (Mon Dec 15 11:42:34 2003): Update
complete. sensorApp is restarting This may take several minutes.
```

8. Espere 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 bloqueo para el router IOS](#)

Complete este procedimiento para configurar el bloqueo para el router IOS.

1. En la consola del servidor VMS, seleccione 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, y haga clic las **configuraciones**.
3. Seleccione las **firmas**, haga clic la **aduana**, después haga clic **agregan** para agregar una nueva firma.



The screenshot shows a web-based configuration interface for IDS Sensors. At the top, there are two dropdown menus: 'Signature Group' set to 'Custom' and 'Filter Source' set to 'Signature'. To the right of these is an empty text input field and a 'Filter' button. Below this is a status bar indicating 'Showing 0-0 of 0 records'. A table with the following columns is displayed: ID, Signature, Subsig ID, Engine, Enabled, Severity, and Action. The table is currently empty, with the text 'No records.' below the header. At the bottom left, there is a 'Rows per page' dropdown set to '10'. At the bottom right, there is a pagination control '<< Page 1 >>'. At the very bottom, there are three buttons: 'Add', 'Edit', and 'Delete'.

4. Ingrese el nuevo nombre de la firma, después seleccione el motor (en este caso, **STRING.TCP**).
5. Usted puede personalizar los parámetros disponibles marcando el botón **Appropriate Radio Button** y haciendo 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.

**Tune Signature Parameters**

Signature Name: \* mytest

Engine: \* STRING.TCP

Engine Description: Generic TCP based string search Engine.

|    | 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 | Nn       |

Showing 25 records

6. Para editar el Signature Severity (severidad de firma) y las acciones o habilitarlos/inhabilite la firma, hacen clic el nombre de la firma.

Signature Group: Custom Filter Source: Signature

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 >>

7. En este caso, la gravedad se cambia al **alto** y se selecciona la acción del **host del bloque**. Para continuar, haga clic en OK (Aceptar). El host del bloque bloquea los host IP o las subredes IP que atacan. Los bloques TCP de la conexión del bloque o puertos UDP (basados en atacar el TCP o las conexiones

**Edit Signature(s)**

Signature: mytest

Enable

Severity: High

Actions:  Log  Reset  Block Host  Block Connection

UDP).

8. La firma completa parece similar a esto:

| Signature Group: <input type="text" value="Custom"/> |       | Filter Source: <input type="text" value="Signature"/> |           | <input type="text"/> |         | <input type="button" value="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                                  | Block                                                                                                        |
| Rows per page: <input type="text" value="10"/>       |       | << Page 1 >>                                          |           |                      |         |                                       |                                                                                                              |
|                                                      |       |                                                       |           |                      |         |                                       | <input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> |

9. Para configurar el dispositivo de bloqueo, el **bloqueo** selecto > los **dispositivos de bloqueo del** selector del objeto (el menú en el lado izquierdo de la pantalla), y el tecleo **agregan** para ingresar la siguiente información:

| Blocking Device                                                         |                                                |
|-------------------------------------------------------------------------|------------------------------------------------|
| Device Type: *                                                          | <input type="text" value="Cisco Router"/>      |
| IP Address: *                                                           | <input type="text" value="10.66.79.210"/>      |
| NAT Address:                                                            | <input type="text"/>                           |
| Comment:                                                                | <input type="text"/>                           |
| Username:                                                               | <input type="text"/>                           |
| Password: *                                                             | <input type="password" value="*****"/>         |
| Enable Password:                                                        | <input type="password" value="*****"/>         |
| Secure Communications:                                                  | <input type="text" value="none"/>              |
| Interfaces: *                                                           | <input type="button" value="Edit Interfaces"/> |
| <input type="button" value="OK"/> <input type="button" value="Cancel"/> |                                                |

Note: \* - Required Field

10. El tecleo **edita las interfaces** (véase a la captura de pantalla anterior), tecleo **agrega**, ingresa esta información, después hace clic la **AUTORIZACIÓN** para continuar.

| Blocking Device Interface                                               |                                        |
|-------------------------------------------------------------------------|----------------------------------------|
| Blocking Interface Name                                                 | <input type="text" value="Ethernet1"/> |
| Blocking Direction                                                      | <input type="text" value="inbound"/>   |
| Pre-block ACL Name                                                      | <input type="text" value="198"/>       |
| Post-block ACL Name                                                     | <input type="text" value="199"/>       |
| <input type="button" value="OK"/> <input type="button" value="Cancel"/> |                                        |

11. Haga Click en OK dos veces para completar la configuración del dispositivo de bloqueo.

| Showing 1-1 of 1 records                                                                                     |              |              |         |              |
|--------------------------------------------------------------------------------------------------------------|--------------|--------------|---------|--------------|
|                                                                                                              | IP Address   | Device Type  | Comment | Source       |
| 1. <input type="radio"/>                                                                                     | 10.66.79.210 | Cisco Router |         | sensor5      |
| Rows per page: <input type="text" value="10"/>                                                               |              |              |         | << Page 1 >> |
| <input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> |              |              |         |              |

12. Para configurar el bloqueo de las propiedades, seleccione el **bloqueo** > el **bloqueo de las propiedades**. La longitud del bloque automático puede ser modificada. En este caso, se cambia a **15 minutos**. El tecleo **se aplica** para continuar.

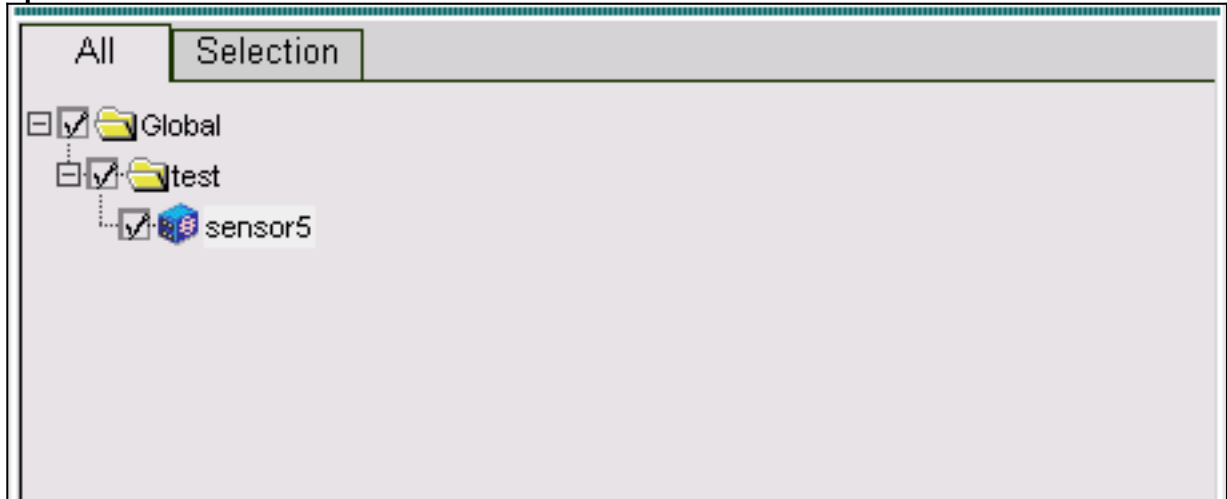
| Blocking Properties                                     |                                                                           |
|---------------------------------------------------------|---------------------------------------------------------------------------|
| Length of Automatic Block                               | <input type="text" value="15"/> minutes                                   |
| Maximum ACL Entries                                     | <input type="text" value="100"/>                                          |
| Enable ACL Logging                                      | <input type="checkbox"/>                                                  |
| Allow blocking devices to block the sensor's IP address | <input type="checkbox"/>                                                  |
| <input checked="" type="checkbox"/> Override            | <input type="button" value="Apply"/> <input type="button" value="Reset"/> |

13. La configuración selecta del menú principal, entonces selecciona **pendiente**, marca la configuración pendiente para asegurarse que es **salvaguardia** correcta, y del

| 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: <input type="text" value="10"/>                            |                       |        |                     | << Page 1 >>     |
| <input type="button" value="Save"/> <input type="button" value="Delete"/> |                       |        |                     |                  |

tecleo.

14. Para avanzar los cambios de configuración al sensor, generar y después desplegar los cambios seleccionando el **despliegue > genera** y el tecleo **se aplica**.



15. El **Deployment (Implementación) > Deploy (Implementar)** selecto, entonces hace clic **some**.
16. Marque el checkbox al lado de su sensor, después haga clic **despliegan**.
17. Marque el checkbox para el trabajo en la cola, después haga clic **al lado de continúan**.

| 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 >>

18. 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.)

19. Seleccione el **Deployment (Implementación) > Deploy (Implementar)** pendiente. Espere algunos minutos hasta que se hayan completado todas las tareas pendientes. La cola está entonces vacía.
20. Para confirmar el despliegue, seleccione el **historial de Configuration**. Asegúrese que el estatus de la configuración esté visualizado según lo **desplegado**. Esto significa que la Configuración del sensor se ha puesto 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](#)

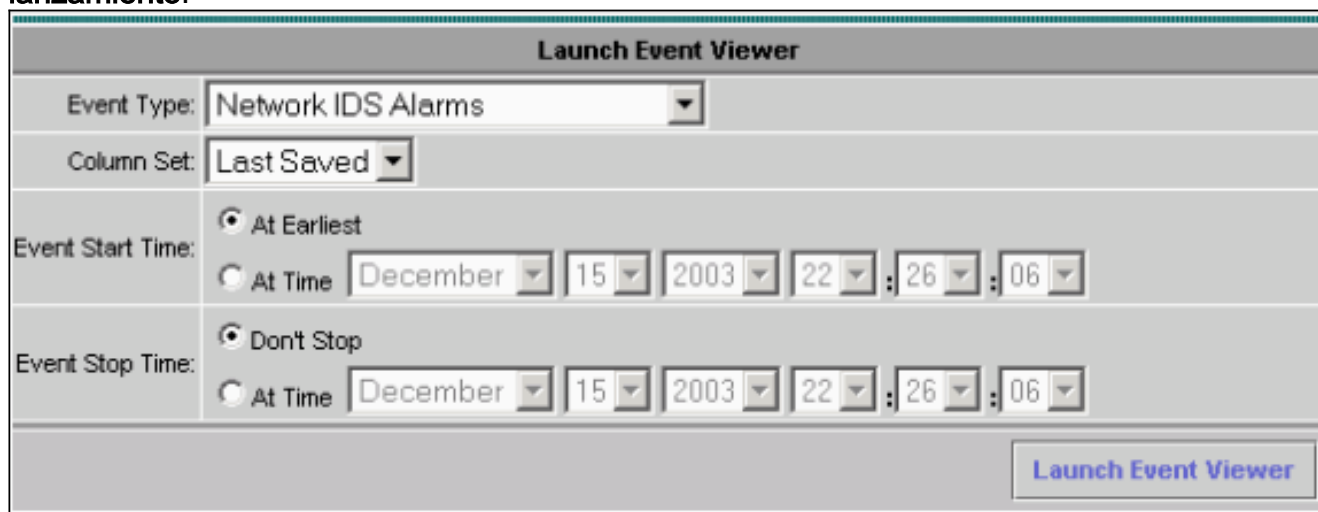
En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

La herramienta [Output Interpreter](#) (sólo para clientes [registrados](#)) permite utilizar algunos comandos "show" y ver un análisis del resultado de estos comandos.

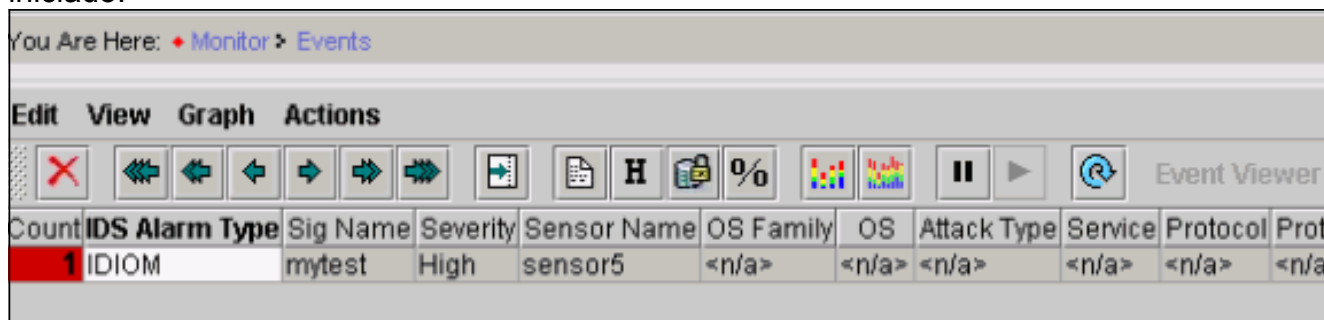
## [Ponga en marcha el ataque y el bloqueo](#)

Para verificar que el proceso de bloqueo esté trabajando correctamente, ponga en marcha un ataque de la prueba y marque los resultados.

1. Antes de iniciar el ataque, **monitor de centro del > Security (Seguridad) de la solución de administración de seguridad/VPN selecta > de la supervisión.**
2. Elija el **monitor del** menú principal, los eventos click y después haga clic el **visor de eventos del lanzamiento.**



3. Telnet al router (en este caso, Telnet al router de la Casa), verificar la comunicación del **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 poner en marcha el ataque, Telnet a partir de un router al otro y al **testattack del** tipo.En este caso, utilizamos Telnet para conectar del router ligero con el router de la Casa. Tan pronto como usted presione **<space>** o el **<enter>**, después de teclear el testattack, su sesión telnet debe ser reajustado.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. El telnet al router (Casa) y ingresa el 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. Del visor de eventos, **base de datos de la interrogación del** teclado para los nuevos eventos ahora para ver la alerta para el ataque previamente iniciado.



7. En el visor de eventos, el resaltado y hace clic con el botón derecho del ratón la alarma, después selecciona el **buffer** o la **visión NSDB del contexto de la visión** ver más información detallada sobre la alarma.**Nota:** El NSDB es también accesible en línea en la [enciclopedia](#)



[segura de Cisco \(clientes registrados solamente\)](#).

The screenshot shows a software interface with a menu bar (Edit, View, Graph, Actions) and a toolbar with various icons. Below the toolbar is a table with the following data:

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

A context menu is open over the first row of the table, containing the following options:

- Delete From This Grid
- Delete From Database
- Collapse First Group
- View Context Buffer
- View NSDB
- Graph By Child
- Graph By Time

## Troubleshooting

### Procedimiento de Troubleshooting

Utilice el siguiente procedimiento para los propósitos de Troubleshooting.

1. En el IDS MC, los **informes** selectos > **generan**. Dependiendo del tipo de problema, el detalle adicional se debe 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 >>

- En la consola del sensor, ingrese el comando `show statistics networkaccess` y marque la salida para asegurarse que el "estado" es activo.
 

```
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#
```
- Asegúrese que el parámetro de comunicación muestre que se está utilizando el protocolo correcto, por ejemplo Telnet o el Secure Shell (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. Usted puede entonces intentar Telnet o SSH del sensor sí mismo, al router, asegurarle puede iniciar sesión con éxito.

## [Información Relacionada](#)

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