# Configuración Reset TCP (reinicio TCP) mediante el director IDS

# Contenido

Introducción Prerequisites Requirements Componentes Utilizados Convenciones Configurar Diagrama de la red Configuraciones Configure el sensor Agregue el sensor al Director Configuración del reinicio TCP para el router Cisco IOS Inicie el ataque y reinicie TCP Verificación Troubleshoot Información Relacionada

# **Introducción**

Este documento describe cómo configurar un Director y Sensor del Sistema de detección de intrusiones (IDS, anteriormente NetRanger) para enviar reinicios TCP en un Telnet intentado a un rango de direcciones que incluyen el router administrado si la cadena enviada es "testattack".

# **Prerequisites**

### **Requirements**

Al considerar esta configuración, recuerde:

- Instale el sensor y verifique que funcione correctamente antes de realizar esta configuración.
- Asegúrese de que la interfaz de rastreo se expanda a la interfaz externa del router administrado.

#### **Componentes Utilizados**

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

- Cisco IDS Director 2.2.3
- Sensor IDS de Cisco 3.0.5
- Router Cisco IOS<sup>®</sup> que ejecuta la versión de software 12.2.6

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.

#### **Convenciones**

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

## **Configurar**

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

**Nota:** Para encontrar información adicional sobre los comandos usados en este documento, utilice la <u>Command Lookup Tool</u> (<u>sólo</u> clientes registrados).

#### Diagrama de la red

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



#### **Configuraciones**

Este documento usa estas configuraciones.

- Luz del router
- Base del router

#### Luz del router

Current configuration : 906 bytes

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
1
hostname light
!
enable password cisco
1
username cisco password 0 cisco
ip subnet-zero
1
ip ssh time-out 120
ip ssh authentication-retries 3
!
call rsvp-sync
!
1
1
fax interface-type modem
mta receive maximum-recipients 0
1
controller E1 2/0
!
!
!
interface FastEthernet0/0
 ip address 100.100.100.2 255.255.255.0
 duplex auto
 speed auto
1
interface FastEthernet0/1
 ip address 1.1.1.1 255.255.255.0
 duplex auto
 speed auto
1
interface BRI4/0
no ip address
shutdown
1
interface BRI4/1
no ip address
shutdown
ļ
interface BRI4/2
no ip address
shutdown
!
interface BRI4/3
no ip address
shutdown
1
ip classless
ip route 0.0.0.0 0.0.0.0 100.100.100.1
ip http server
ip pim bidir-enable
!
1
dial-peer cor custom
!
Ţ
line con 0
```

```
line 97 108
line aux 0
line vty 0 4
login
!
end
Base del router
Current configuration : 2187 bytes
1
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
1
hostname house
1
enable password cisco
!
1
1
ip subnet-zero
!
1
fax interface-type modem
mta receive maximum-recipients 0
1
1
!
1
interface FastEthernet0/0
 ip address 100.100.100.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.64.10.45 255.255.255.224
 duplex auto
 speed auto
1
interface FastEthernet4/0
no ip address
 shutdown
 duplex auto
 speed auto
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.64.10.33
ip route 1.1.1.0 255.255.255.0 100.100.100.2
ip http server
ip pim bidir-enable
!
1
1
snmp-server manager
1
call rsvp-sync
!
!
mgcp profile default
```

```
!
dial-peer cor custom
!
!
!
!
line con 0
line aux 0
line vty 0 4
password cisco
login
!
!
end
house#
```

#### Configure el sensor

Complete estos pasos para configurar el Sensor.

- 1. Telnet a 10.64.10.49 (el sensor IDS) con el nombre de usuario **root** y el **ataque de** contraseña.
- 2. Escriba sysconfig-sensor.
- Cuando se le solicite, introduzca la información de configuración, como se muestra en este ejemplo:

```
1 - IP Address: 10.64.10.49
2 - IP Netmask: 255.255.254
3 - IP Host Name: sensor-2
4 - Default Route: 10.64.10.33
5 - Network Access Control
        64.
        10.
6 - Communications Infrastructure
Sensor Host ID: 49
Sensor Organization ID: 900
Sensor Host Name: sensor-2
Sensor Organization Name: cisco
Sensor IP Address: 10.64.10.49
IDS Manager Host ID: 50
IDS Manager Organization ID: 900
IDS Manager Host Name: dir3
IDS Manager Organization Name: cisco
IDS Manager IP Address: 10.64.21.50
```

4. Cuando se le solicite, guarde la configuración y permita que el sensor se reinicie.

#### Agregue el sensor al Director

Complete estos pasos para agregar el Sensor al Director.

- 1. Telnet a 10.64.21.50 (el Director IDS) con el nombre de usuario **netrangr** y el **ataque de** contraseña.
- 2. Escriba ovw& para iniciar HP OpenView.
- 3. En el menú principal, vaya a **Seguridad > Configurar**.
- 4. En Configuration File Management Utility, vaya a file > Add Host y haga clic en Next.

5. Complete la información del host Sensor, como se muestra en este ejemplo. Haga clic en Next

Use this panel to specify the remote machine to which you wish to establish connectivity. If you need to add a new organization, click Create.				
Organization name	cisco —	Create		
Organization ID	900			
Host name	sensor-2į́			
Host ID	49 <u>ĭ</u>			
Host IP Address	10.64.10.49	[		
Secondary Director				
🗖 IOS IDS				
🕱 Sensor / IDSM				

(Siguiente).

6. Acepte la configuración predeterminada para el tipo de máquina y haga clic en **Siguiente**, como se muestra en este

Use this dialog box to define the type of machine you are adding.

Please remember that in order for connectivity to be established, the remote machine must already know the IDs and IP address of this Director. For Sensors, this is accomplished at install time by running sysconfig-sensor. For remote (secondary) Directors, this is accomplished by running nrConfigure on the remote machine and modifying the hosts and routes System Files accordingly.

Initialize a newly installed Sensor

Connect to a previously configured Sensor

C Forward alarms to a secondary Director

ejemplo.

7. Puede cambiar el registro y evitar minutos o aceptar los valores predeterminados. Sin embargo, debe cambiar el nombre de la interfaz de red por el nombre de la interfaz de rastreo. En este ejemplo, es "iprb0". Puede ser "spwr0" o cualquier otra cosa dependiendo del tipo de sensor y de cómo conecte su sensor.

Use this dialog box to set the time in minutes for automatic logging and shunning, the name of the Sensor network interface performing packet capture, and the addresses and netmasks of networks protected by the Sensor.				
Number of minutes to log on an event.	15]			
Number of minutes to shun on an event.	15			
Network Interface Name	jiprb0			
Sensor Protected Networks				

8. Continúe haciendo clic en **Next** y, a continuación, haga clic en **Finish** para agregar el sensor al Director. En el menú principal, ahora debería ver sensor-2, como en este ejemplo

ejemp	JIO.										
Map	Edit	View	Perform	mance	Config	uration	Fault	Security	Tools	Options	
1012											
wind	low										нетр
⊿	â /	<u>a</u> 1	s ⇒⊗	Q							
							_				
	1		<b>`</b>			8			/y		
		1 <b>(D</b> )	<u> </u>			-57	<mark>°                                    </mark>		<b>0</b>		
		$\mathbf{T}$	<b>/</b>							<b>T</b> /	
	se	ensor-	2			dir3			ser	nsor-3	
	_		_								

## Configuración del reinicio TCP para el router Cisco IOS

Complete estos pasos para configurar el reinicio TCP para el router Cisco IOS.

- 1. En el menú principal, vaya a **Seguridad > Configurar**.
- 2. En Configuration File Management Utility, resalte sensor-2 y haga doble clic en él.
- 3. Abra Device Management (Administración de dispositivos).
- Haga clic en Dispositivos > Agregar. Introduzca la información del dispositivo, como se muestra en el ejemplo siguiente. Para continuar, haga clic en OK (Aceptar). Tanto Telnet como enable password son Cisco.

IP Address	User Name
10.64.10.45	Ĭ
Device Type	Password
Cisco Router[Including Cat5kRSM,Cat6kMSFC] —	*****
Sensor's NAT IP Address	Enable Password
<b>V</b>	*****
Enable SSH	

5. Abra la ventana Detección de intrusiones y haga clic en **Redes protegidas**. Agregue el rango de direcciones de 10.64.10.1 a 10.64.10.254 a la red

Source Address			
Enter range of IP addresses to be protected			
OEnter a network address to be protected			
Start Address:			
10.64.10.1			
End Address:			
10.64.10.254			

protegida.

6. Haga clic en Profile y seleccione Manual Configuration. A continuación, haga clic en Modificar firmas. Elija Cadenas coincidentes con un ID de 8000. Haga clic en Expandir > Agregar para agregar una nueva cadena llamada testattack. Ingrese la información de cadena, como se muestra en este ejemplo, y haga clic en Aceptar para continuar.

Str	ring	Occurrences	
žes	stattack	þ	
ID		Action	
513	304	TCP Reset	-
Por	t	sensor-2₊cisco loggerd	
23		đ	
Dir	rection	dir3₊cisco smid	
То	& From —	þ	

- 7. Ha finalizado esta parte de la configuración. Haga clic en **Aceptar** para cerrar la ventana Detección de intrusiones.
- 8. Abra la carpeta Archivos del sistema y, a continuación, la ventana Daemons. Asegúrese de tener estos demonios

napiillados.		
Daemons		
	▼ nr.postofficed	🕱 nr.configd
	🕱 nr.loggerd	nr.smid
	🕱 nr.sensord	nr.eventd
	🕱 nr.packetd	🕱 nr.sapd
	🕱 nr.managed	🕱 nr.fileXferd

- 9. Para continuar, haga clic en OK (Aceptar).
- 10. Elija la versión que acaba de modificar, haga clic en Guardar y, a continuación, Aplicar. Espere a que el sistema le diga que el sensor ha terminado de reiniciar los servicios y, a continuación, cierre todas las ventanas para la configuración de Director.

Version / Item	Creation Time	Open			
📥 👼 Version 11	Mon Apr 22 21:04:57 EDT 2002	· '			
- 🔤 Communications	Mon Apr 22 21:04:57 EDT 2002	View			
- 🔊 Data Management	Mon Apr 22 21:04:57 EDT 2002				
- 🔜 Device Management	Mon Apr 22 21:04:57 EDT 2002	Save			
- ;o <sup>†</sup> Event Processing	Mon Apr 22 21:04:57 EDT 2002				
- 🖓 Intrusion Detection	Mon Apr 22 21:04:57 EDT 2002	Apply			
🚽 🖻 🏳 System Files	_				
- 💷 Authorization	Mon Apr 22 21:04:57 EDT 2002	Delete			
- 🎝 Daemons	Mon Apr 22 21:04:57 EDT 2002	-			
•		_			
Close					

#### Inicie el ataque y reinicie TCP

Telnet de Router Light a Router House y escriba **testattack**. Tan pronto como pulse la tecla Space o Enter, la sesión Telnet se restablecerá. Se conectará a Router House.

```
light#telnet 10.64.10.45
Trying 10.64.10.45 ... Open
User Access Verification
Password:
house>en
Password:
house#testattack
[Connection to 10.64.10.45 closed by foreign host]
 !--- Telnet session has been reset because the !--- signature testattack was triggered.
```

## **Verificación**

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

## **Troubleshoot**

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

Telnet a 10.64.10.49, el Sensor, usando el nombre de usuario **root** y el **ataque** de contraseña. Escriba **cd /usr/nr/etc**. Escriba **cat packetd.conf**. Si configura correctamente el reinicio de TCP para el ataque de prueba, debería ver un cuatro (4) en el campo Códigos de Acción. Esto indica el reinicio de TCP como se muestra en este ejemplo.

netrangr@sensor-2:/usr/nr/etc
>cat packetd.conf | grep "testattack"
RecordOfStringName 51304 23 3 1 "testattack"
SigOfStringMatch 51304 4 5 5 # "testattack"

Si configura accidentalmente la acción en "ninguno" en la firma, verá un cero (0) en el campo Códigos de acción. Esto indica que no hay ninguna acción como se ve en este ejemplo.

netrangr@sensor-2:/usr/nr/etc
>cat packetd.conf | grep "testattack"
RecordOfStringName 51304 23 3 1 "testattack"
SigOfStringMatch 51304 0 5 5 # "testattack"

Los reinicios de TCP se envían desde la interfaz de rastreo del Sensor. Si hay un switch que conecta la interfaz Sensor a la interfaz exterior del router administrado, cuando configura usando el comando **set span** en el switch, utilice esta sintaxis:

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
!--- Connect to FastEthernet0/0 of Router House. Oper Source : Port 2/12
Direction : transmit/receive
Incoming Packets: enabled
Learning : enabled
Multicast : enabled
```

## Información Relacionada

- Field Notices
- Página de soporte de Cisco Secure Intrusion Prevention