# Router de dos interfaces con la configuración del Firewall Cisco IOS NAT

## Contenido



## Introducción

Esta configuración de ejemplo funciona en una oficina muy pequeña conectada directamente a Internet. Se supone que el Servicio de nombre de dominio (DNS), SMTP (Simple Mail Transfer Protocol) y los servicios web los proporcionan un sistema remoto ejecutado por el Proveedor de servicios de Internet (ISP). No hay servicios en la red interna, lo que hace que esta sea de las configuraciones de firewall más simples, pues hay solamente dos interfaces. No existe inicio de sesión ya que ningún host está disponible para proporcionar servicios de inicio de sesión.

Refiera al Router de tres interfaces sin la configuración del Firewall Cisco IOS NAT para configurar a un router de tres interfaces sin el NAT usando el Firewall de Cisco IOS®.

Refiera al router de dos interfaces sin el NAT usando la configuración del Firewall Cisco IOS para configurar a un router de dos interfaces sin el NAT usando el Firewall Cisco IOS.

## prerrequisitos

### Requisitos

No hay requisitos específicos para este documento.

### Componentes Utilizados

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

- Versión 12.2 del software de Cisco IOS
- Cisco 3640 Router

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 Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

## Antecedentes

Puesto que esta configuración utiliza solamente las listas de acceso de entrada, hace contra spoofing y el filtrado de tráfico con la misma lista de acceso (101). Esta configuración trabaja solamente para un router de dos puertos. El Ethernet1 es la red del “interior”. El serial0 es la interfaz exterior. La lista de acceso (112) en el serial0 ilustra esto usando los IP Address globales del Network Address Translation (NAT) (150.150.150.x) como destinos.

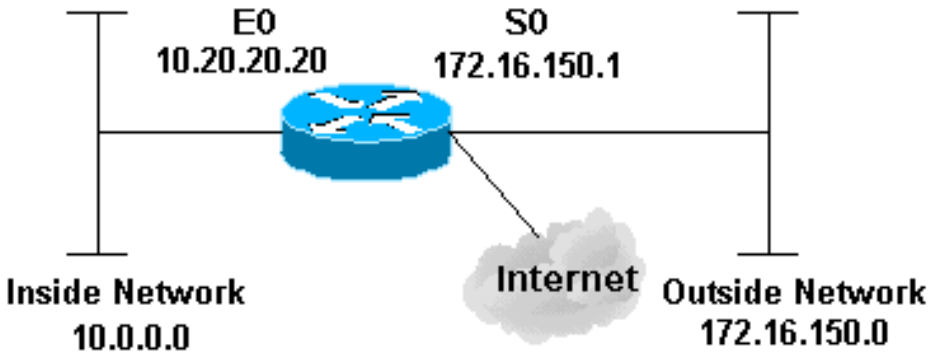
## Configurar

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

Este documento utiliza esta configuración de red:




## Configuración

Este documento utiliza esta configuración.

**Router 3640**

```
version 12.2
service timestamps debug datetime msec localtime show-
timezone
service timestamps log datetime msec localtime show-
timezone
no service password-encryption
!
hostname pig
!
boot system flash flash:c3640-jk9o3s-mz.122-21a.bin
logging buffered 4096 debugging
enable secret 5 $1$chHU$wiC58FP/IDloZuorCkzEz1
enable password ww
!
clock timezone CET 1
clock summer-time CET recurring
ip subnet-zero
!
!
no ip domain-lookup
!
!--- This is the Cisco IOS Firewall !--- configuration
and what to inspect. ip inspect name ethernetin cuseeme
timeout 3600 ip inspect name ethernetin ftp timeout 3600
ip inspect name ethernetin h323 timeout 3600 ip inspect
name ethernetin http timeout 3600 ip inspect name
ethernetin rcmd timeout 3600 ip inspect name ethernetin
realaudio timeout 3600 ip inspect name ethernetin smtp
timeout 3600 ip inspect name ethernetin sqlnet timeout
3600 ip inspect name ethernetin streamworks timeout 3600
ip inspect name ethernetin tcp timeout 3600 ip inspect
name ethernetin tftp timeout 30 ip inspect name
ethernetin udp timeout 15 ip inspect name ethernetin
vdolive timeout 3600 ip audit notify log ip audit po
max-events 100 ! call rsvp-sync ! ! ! ! ! ! !--- This
```

```
is the inside of the network. interface Ethernet0/0 ip
address 10.20.20.20 255.255.255.0 ip access-group 101 in
ip nat inside ip inspect ethernetin in half-duplex !
interface Ethernet0/1 no ip address shutdown half-duplex
! interface Serial1/0 no ip address shutdown ! interface
Serial1/1 no ip address shutdown ! interface Serial1/2
no ip address shutdown ! !--- This is the outside of the
interface. interface Serial1/3 ip address 172.16.150.1
255.255.255.0 ip access-group 112 in ip nat outside ! !-
-- Define the NAT pool. ip nat pool mypool 172.16.150.3
172.16.150.255 netmask 255.255.255.0 ip nat inside
source list 1 pool mypool ip classless ip route 0.0.0.0
0.0.0.0 172.16.150.2 ip http server ! access-list 1
permit 10.0.0.0 0.255.255.255 !--- Access list applied
on the inside for anti-spoofing reasons. access-list 101
permit tcp 10.0.0.0 0.255.255.255 any access-list 101
permit udp 10.0.0.0 0.255.255.255 any access-list 101
permit icmp 10.0.0.0 0.255.255.255 any access-list 101
deny ip any any log !--- Access list applied on the
outside for security reasons. access-list 112 permit
icmp any 172.16.150.0 0.0.0.255 unreachable access-list
112 permit icmp any 150.150.150.0 0.0.0.255 echo-reply
access-list 112 permit icmp any 172.16.150.0 0.0.0.255
packet-too-big access-list 112 permit icmp any
172.16.150.0 0.0.0.255 time-exceeded access-list 112
permit icmp any 172.16.150.0 0.0.0.255 traceroute
access-list 112 permit icmp any 172.16.150.0 0.0.0.255
administratively-prohibited access-list 112 permit icmp
any 172.16.150.0 0.0.0.255 echo access-list 112 deny ip
any any log ! ! dial-peer cor custom ! ! ! ! ! line con
0 exec-timeout 0 0 line 97 102 line aux 0 line vty 0 4
exec-timeout 0 0 password ww login ! end
```

# Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- **versión de la demostración** — Información de las visualizaciones sobre la versión de software actualmente cargada junto con el hardware y la información del dispositivo.
- **IP del debug nacional** — Visualiza la información sobre los paquetes del IP traducida por la función NAT IP.
- **muestre a IP las traducciones nacionales** — Visualiza los NAT activos.
- **registro de la demostración** — Visualiza la información de ingreso al sistema.
- **muestre la lista de acceso del IP** — Visualiza el contenido de todas las listas de acceso por IP actuales.
- **el IP de la demostración examina la sesión** — Visualiza a las sesiones existentes que son seguidas y examinadas actualmente por el Firewall Cisco IOS.
- **debug ip inspect tcp** — Visualiza los mensajes sobre los eventos del Firewall Cisco IOS.

Ésta es salida del comando de ejemplo del **comando show version**.

```
pig#show version Cisco Internetwork Operating System Software IOS (tm) 3600 Software (C3640-
JK9O3S-M), Version 12.2(21a), RELEASE SOFTWARE (fc2) Copyright (c) 1986-2004 by cisco Systems,
Inc. Compiled Fri 09-Jan-04 16:23 by kellmill Image text-base: 0x60008930, data-base: 0x615DE000
```

```
ROM: System Bootstrap, Version 11.1(19)AA, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1) pig uptime is
59 minutes System returned to ROM by reload at 16:05:44 CET Wed Jan 14 2004 System image file is
"flash:c3640-jk9o3s-mz.122-21a.bin" This product contains cryptographic features and is subject
to United States and local country laws governing import, export, transfer and use. Delivery of
Cisco cryptographic products does not imply third-party authority to import, export, distribute
or use encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with applicable laws
and regulations. If you are unable to comply with U.S. and local laws, return this product
immediately. A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html If you require further assistance please
contact us by sending email to export@cisco.com. cisco 3640 (R4700) processor (revision 0x00)
with 126976K/4096K bytes of memory. Processor board ID 10577176 R4700 CPU at 100Mhz,
Implementation 33, Rev 1.0 MICA-6DM Firmware: CP ver 2730 - 5/23/2001, SP ver 2730 - 5/23/2001.
Bridging software. X.25 software, Version 3.0.0. SuperLAT software (copyright 1990 by Meridian
Technology Corp). TN3270 Emulation software. 2 Ethernet/IEEE 802.3 interface(s) 4 Low-speed
serial(sync/async) network interface(s) 6 terminal line(s) 1 Virtual Private Network (VPN)
Module(s) DRAM configuration is 64 bits wide with parity disabled. 125K bytes of non-volatile
configuration memory. 32768K bytes of processor board System flash (Read/Write)
```

Primero, verifique los trabajos NAT correctamente usando el **IP del debug nacional** y **muestre a IP las traducciones nacionales** tal y como se muestra en de esta salida.

```
pig#debug ip nat IP NAT debugging is on pig# *Mar 1 01:40:47.692 CET: NAT: s=10.0.0.1-
>172.16.150.4, d=172.16.150.2 [80] *Mar 1 01:40:47.720 CET: NAT*: s=172.16.150.2,
d=172.16.150.4->10.0.0.1 [80] *Mar 1 01:40:47.720 CET: NAT*: s=10.0.0.1->172.16.150.4,
d=172.16.150.2 [81] *Mar 1 01:40:47.748 CET: NAT*: s=172.16.150.2, d=172.16.150.4->10.0.0.1 [81]
*Mar 1 01:40:47.748 CET: NAT*: s=10.0.0.1->172.16.150.4, d=172.16.150.2 [82] *Mar 1 01:40:47.784
CET: NAT*: s=172.16.150.2, d=172.16.150.4->10.0.0.1 [82] *Mar 1 01:40:47.784 CET: NAT*:
s=10.0.0.1->172.16.150.4, d=172.16.150.2 [83] *Mar 1 01:40:47.836 CET: NAT*: s=172.16.150.2,
d=172.16.150.4->10.0.0.1 [83] *Mar 1 01:40:47.836 CET: NAT*: s=10.0.0.1->172.16.150.4,
d=172.16.150.2 [84] *Mar 1 01:40:47.884 CET: NAT*: s=172.16.150.2, d=172.16.150.4->10.0.0.1 [84]
pig#show ip nat translations Pro Inside global Inside local Outside local Outside global ---
172.16.150.4 10.0.0.1 --- ---
```

Sin agregar el **IP examine la** declaración, confirman que las Listas de acceso trabajan correctamente. **El deny ip any any** con la palabra clave del **registro** le dice se bloquean qué paquetes.

En este caso, éste es el tráfico de retorno de una sesión telnet a 172.16.150.2 de 10.0.0.1 (traducido a 172.16.150.4).

Ésta es salida de muestra del **comando show log**.

```
pig#show log Syslog logging: enabled (0 messages dropped, 0 messages rate-limited, 0 flushes, 0
overruns) Console logging: level debugging, 92 messages logged Monitor logging: level debugging,
0 messages logged Buffer logging: level debugging, 60 messages logged Logging Exception size
(4096 bytes) Trap logging: level informational, 49 message lines logged Log Buffer (4096 bytes):
*Mar 1 01:24:08.518 CET: %SYS-5-CONFIG_I: Configured from console by console *Mar 1 01:26:47.783
CET: %SYS-5-CONFIG_I: Configured from console by console *Mar 1 01:27:09.876 CET: %SEC-6-
IPACCESSLOGP: list 112 denied tcp 172.16.150.2(23) -> 172.16.150.4(11004), 1 packet *Mar 1
01:33:03.371 CET: %SEC-6-IPACCESSLOGP: list 112 denied tcp 172.16.150.2(23) ->
172.16.150.4(11004), 3 packets
```

Utilice el **comando show ip access-lists** para ver cuántos paquetes hacen juego la lista de acceso.

```
pig#show ip access-lists Standard IP access list 1 permit 10.0.0.0, wildcard bits 0.255.255.255
(28 matches) Extended IP access list 101 permit tcp 10.0.0.0 0.255.255.255 any (32 matches)
permit udp 10.0.0.0 0.255.255.255 any permit icmp 10.0.0.0 0.255.255.255 any (22 matches) deny
ip any any log Extended IP access list 112 permit icmp any 172.16.150.0 0.0.0.255 unreachable
permit icmp any 172.16.150.0 0.0.0.255 echo-reply (10 matches) permit icmp any 172.16.150.0
0.0.0.255 packet-too-big permit icmp any 172.16.150.0 0.0.0.255 time-exceeded permit icmp any
172.16.150.0 0.0.0.255 traceroute permit icmp any 172.16.150.0 0.0.0.255 administratively-
prohibited permit icmp any 172.16.150.0 0.0.0.255 echo deny ip any any log (12 matches) pig#
```

Una vez que usted ha agregado el **IP examine la** declaración, usted puede ver que esta línea se ha agregado dinámicamente en la lista de acceso para permitir a esta sesión telnet:

```
permit tcp host 172.16.150.2 eq telnet host 172.16.150.4 eq 11004 (16 matches)pig#show ip
access-lists Standard IP access list 1 permit 10.0.0.0, wildcard bits 0.255.255.255 (44 matches)
Extended IP access list 101 permit tcp 10.0.0.0 0.255.255.255 any (50 matches) permit udp
10.0.0.0 0.255.255.255 any permit icmp 10.0.0.0 0.255.255.255 any (22 matches) deny ip any any
log Extended IP access list 112 permit tcp host 172.16.150.2 eq telnet host 172.16.150.4 eq
11004 (16 matches) permit icmp any 172.16.150.0 0.0.0.255 unreachable permit icmp any
172.16.150.0 0.0.0.255 echo-reply (10 matches) permit icmp any 172.16.150.0 0.0.0.255 packet-
too-big permit icmp any 172.16.150.0 0.0.0.255 time-exceeded permit icmp any 172.16.150.0
0.0.0.255 traceroute permit icmp any 172.16.150.0 0.0.0.255 administratively-prohibited permit
icmp any 172.16.150.0 0.0.0.255 echo deny ip any any log (12 matches) pig#
```

Usted puede también marcar usando el **comando show ip inspect session** que muestra a las sesiones en curso que se han establecido con el Firewall.

```
pig#show ip inspect session Established Sessions Session 624C31A4
(10.0.0.1:11006)=>(172.16.150.2:23) tcp SIS_OPEN
```

Eventual, en un nivel más avanzado, usted puede también habilitar el **comando debug ip inspect tcp**.

```
pig#debug ip inspect tcp INSPECT TCP Inspection debugging is on pig# *Mar 1 01:49:51.756 CET:
CBAC sis 624C31A4 pak 624D0FA8 TCP S seq 2890060460(0) (172.16.150.4:11006) => (172.16.150.2:23)
*Mar 1 01:49:51.776 CET: CBAC sis 624C31A4 pak 624D0CC4 TCP S ack 2890060461 seq 1393191461(0)
(10.0.0.1:11006) <= (172.16.150.2:23) *Mar 1 01:49:51.776 CET: CBAC* sis 624C31A4 pak 62576284
TCP ack 1393191462 seq 2890060461(0) (172.16.150.4:11006) => (172.16.150.2:23) *Mar 1
01:49:51.776 CET: CBAC* sis 624C31A4 pak 62576284 TCP P ack 1393191462 seq 2890060461(12)
(172.16.150.4:11006) => (172.16.150.2:23) *Mar 1 01:49:51.780 CET: CBAC* sis 624C31A4 pak
62576284 TCP ack 1393191462 seq 2890060473(0) (172.16.150.4:11006) => (172.16.150.2:23)
```

# Troubleshooting

Después de que usted configure al router del escudo de protección IOS, si las conexiones no trabajan, asegúrese de que usted haya habilitado el examen con el **IP examine (nombre definido) adentro o comando out** en la interfaz. En esta configuración, el **IP examina el ethernetin adentro** es aplicado para el **Ethernet0/0 de la** interfaz.

Para el Troubleshooting general en esta configuración, refiera a las configuraciones del Firewall Cisco IOS del troubleshooting y al Proxy de autenticación del troubleshooting.

## Problema

Usted no puede realizar las descargas HTTP porque falla o se mide el tiempo hacia fuera. ¿Cómo se resuelve esto?

## Solución

El problema se puede resolver quitando el **IP examina** para saber si hay tráfico HTTP para no examinar el tráfico HTTP y ocurra la descarga como se esperaba.

# Información Relacionada

- Página de soporte de firewall de IOS
- Soporte Técnico y Documentación - Cisco Systems