

Router de dos interfaces con configuración de firewall NAT Cisco IOS

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración](#)

[Verificación](#)

[Troubleshoot](#)

[Problema](#)

[Solución](#)

[Información Relacionada](#)

[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.

Consulte [Router de Tres Interfaces sin NAT Cisco IOS Firewall Configuration](#) para configurar un router de tres interfaces sin NAT usando Cisco IOS® Firewall.

Consulte [Router de Dos Interfaces sin NAT Usando la Configuración de Firewall de Cisco IOS](#) para configurar un router de dos interfaces sin NAT usando el Firewall de Cisco IOS.

[Prerequisites](#)

[Requirements](#)

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

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](#)

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

[Antecedentes](#)

Puesto que esta configuración utiliza sólo listas de acceso de entrada, realiza tanto la antisimulación como el filtrado de tráfico con la misma lista de acceso (101). Esta configuración sólo funciona para un router de dos puertos. Ethernet 1 es la red "interna". Serial 0 es la interfaz externa. La lista de acceso (112) en Serial 0 ilustra esto usando las direcciones IP globales de traducción de direcciones de red (NAT) (150.150.150.x) como destinos.

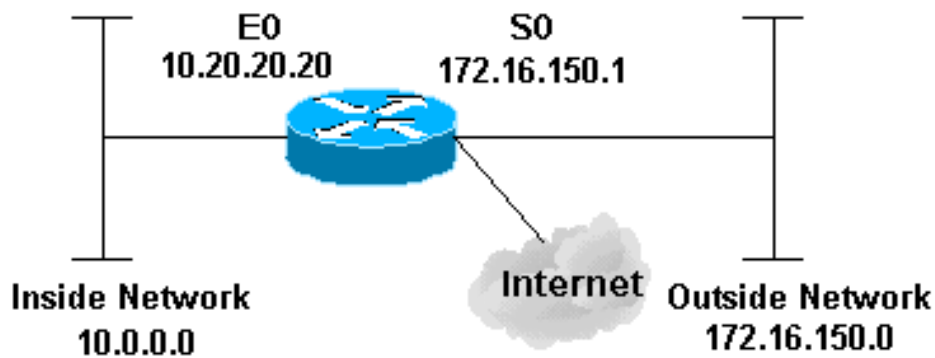
[Configurar](#)

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

Nota: Utilice la herramienta [Command Lookup](#) (sólo para clientes [registrados](#)) 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 usa 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.

- **show version**—Muestra información sobre la versión de software cargada actualmente junto con información de hardware y dispositivo.
- **debug ip nat**: muestra información sobre los paquetes IP traducidos por la función IP NAT.
- **show ip nat translations**—Muestra las NAT activas.
- **show log**—Muestra información de registro.
- **show ip access-list**—Muestra el contenido de todas las listas de acceso IP actuales.
- **show ip inspect session**: muestra las sesiones existentes que actualmente son controladas e inspeccionadas por Cisco IOS Firewall.
- **debug ip inspect tcp**—Muestra mensajes acerca de los eventos de Cisco IOS Firewall.

Este es un ejemplo de resultado 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/wvl/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 que NAT funcione correctamente usando `debug ip nat` y `show ip nat translations` como se muestra en este resultado.

```
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 la instrucción `ip inspect`, confirme que las listas de acceso funcionan correctamente. La palabra clave `deny ip any any with the log` indica qué paquetes están bloqueados.

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

Este es un ejemplo de salida 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 coinciden con 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 haya agregado la instrucción **ip inspect**, puede ver que esta línea se ha agregado dinámicamente en la lista de acceso para permitir 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)
```

pi#

También puede verificar usando el comando **show ip inspect session** que muestra las sesiones actuales que se han establecido a través del firewall.

```
pi#show ip inspect session
```

Established Sessions

```
Session 624C31A4 (10.0.0.1:11006)=>(172.16.150.2:23) tcp SIS_OPEN
```

Finalmente, a un nivel más avanzado, también puede habilitar el comando **debug ip inspect tcp**.

```
pi#debug ip inspect tcp
```

INSPECT TCP Inspection debugging is on

pi#

```
*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)
```

Troubleshoot

Después de configurar el router de firewall del IOS, si las conexiones no funcionan, asegúrese de haber habilitado la inspección con el comando **ip inspect (nombre definido) in o out** en la interfaz. En esta configuración, **ip inspect ethernet in** se aplica para la interfaz **Ethernet0/0**.

Para la resolución general de problemas en esta configuración, refiérase a [Troubleshooting de Configuraciones de Cisco IOS Firewall](#) y [Troubleshooting de Proxy de Autenticación](#).

Problema

No puede realizar descargas http porque falla o se agota el tiempo de espera. ¿Cómo se resuelve esto?

Solución

El problema se puede resolver eliminando **ip inspect** para el tráfico http de modo que el tráfico http no se inspeccione y la descarga se produzca como se esperaba.

Información Relacionada

- [Página de soporte de firewall de IOS](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)