

Roteador de duas interfaces com configuração do Cisco IOS Firewall NAT

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configuração](#)

[Verificar](#)

[Troubleshooting](#)

[Problema](#)

[Solução](#)

[Informações Relacionadas](#)

[Introdução](#)

Esta configuração de exemplo funciona para um escritório muito pequeno conectado diretamente à Internet. A suposição é que o Serviço de Nome de Domínio (DNS), o protocolo SMTP e os serviços web são fornecidos por um sistema remoto executado pelo provedor de Internet (ISP). Não há quaisquer serviços na rede interna, o que faz desta uma das configurações de firewall mais simples, pois há apenas duas interfaces. Não há login, pois não há host disponível para fornecer serviços de login.

Refira o [roteador de três interfaces sem configuração do Cisco IOS Firewall NAT](#) a fim configurar um roteador de três relações sem NAT usando o Firewall de Cisco IOS®.

Refira o [roteador de duas interfaces sem NAT usando a configuração do Cisco IOS Firewall](#) a fim configurar um roteador de duas relações sem NAT usando o Cisco IOS Firewall.

[Pré-requisitos](#)

[Requisitos](#)

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão do Cisco IOS Software 12.2
- Cisco 3640 Router

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

[Convenções](#)

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

[Informações de Apoio](#)

Desde que esta configuração usa somente listas de acesso de entrada, faz anti-falsificação e o filtragem de tráfego com a mesma lista de acessos (101). Esta configuração trabalha somente para um roteador de duas portas. Ethernet1 é a rede do “interior”. O Serial 0 é a interface externa. A lista de acessos (112) no Serial 0 ilustra esta que usa os endereços IP globais do Network Address Translation (NAT) (150.150.150.x) como destinos.

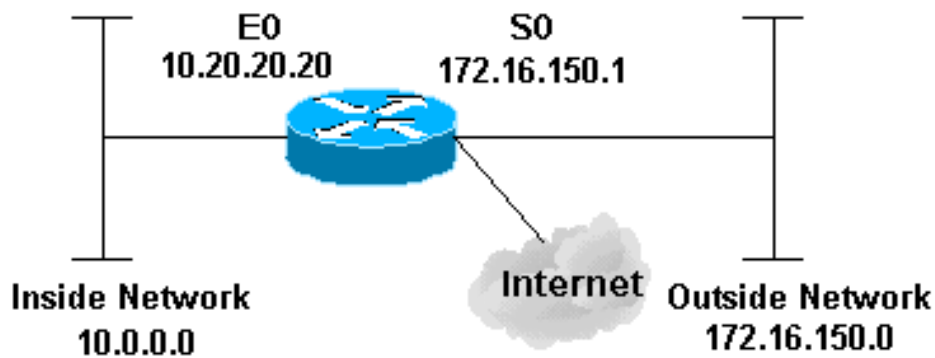
[Configurar](#)

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Note: Use a [Command Lookup Tool](#) ([somente clientes registrados](#)) para obter mais informações sobre os comandos usados nesta seção.

[Diagrama de Rede](#)

Este documento utiliza a seguinte configuração de rede.



Configuração

Este documento usa esta configuração.

3640 Router

```

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 Serial11/0
  no ip address
  shutdown
!
interface Serial11/1
  no ip address
  shutdown
!
interface Serial11/2
  no ip address
  shutdown
!
!--- This is the outside of the interface. interface
Serial11/3 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
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A [Output Interpreter Tool \(apenas para clientes registrados\)](#) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **versão da mostra** — Informação dos indicadores sobre a versão de software atualmente carregada junto com o hardware e a informação do dispositivo.
- **debugar o IP nat** — Indica a informação sobre pacotes IP traduzida pelos recursos NAT IP.
- **mostre a IP traduções nat** — Indica NAT ativos.
- **log da mostra** — Indica a informação de registro.
- **mostre a lista de acesso IP** — Indica os índices de todas as listas de acesso IP atuais.
- **a mostra IP inspeciona a sessão** — Indica as sessões existentes que atualmente são seguidas e inspecionadas pelo Cisco IOS Firewall.
- **debug ip inspect tcp** — Indica mensagens sobre eventos do Cisco IOS Firewall.

Este é exemplo de saída de comando do **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)

Primeiramente, verifique que os trabalhos NAT que se usam corretamente debuga o IP nat e mostre a IP traduções nat segundo as indicações desta saída.

```
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         ---                ---
```

Sem adicionar o IP inspecione a indicação, confirmam que as Listas de acesso trabalham corretamente. O deny ip any any com a palavra-chave do log diz-lhe que pacotes são obstruídos.

Neste caso, este é o tráfego de retorno de uma sessão de Telnet a 172.16.150.2 de 10.0.0.1 (traduzido a 172.16.150.4).

Este é exemplo de saída do 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
```

Use o comando **show ip access-lists** a fim ver quantos pacotes combinam a lista de acessos.

```
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#
```

Uma vez que você adicionou o **IP inspecione a** indicação, você pode ver que esta linha esteve adicionada dinamicamente na lista de acessos a fim permitir esta sessão de Telnet:

```
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#
```

```
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#
```

Você pode igualmente verificar usando o **comando show ip inspect session** que mostra as sessões atuais que foram estabelecidas com o Firewall.

```
pig#show ip inspect session
```

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

Eventualmente, a nível mais avançado, você pode igualmente permitir o **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

Depois que você configura o roteador do firewall de IOS, se as conexões não trabalham, assegure-se de que você permita a inspeção com o **IP inspecione (nome definido) dentro ou comando out** na relação. Nesta configuração, o **IP inspeciona o ethernetin** é dentro aplicado para o **Ethernet0/0** da relação.

Para o Troubleshooting geral nesta configuração, refira [pesquisando defeitos configurações do Cisco IOS Firewall](#) e [pesquisando defeitos o Proxy de autenticação](#).

Problema

Você não pode executar transferências HTTP porque falha ou é cronometrado para fora. Como isto é resolvido?

Solução

A edição pode ser resolvida removendo o **IP inspeciona** para o tráfego HTTP de modo que o tráfego HTTP não seja inspecionado e a transferência ocorra como esperado.

Informações Relacionadas

- [Página de suporte de firewall do IOS](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)