

Roteador de duas interfaces sem NAT usando a configuração do Cisco IOS Firewall

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configuração](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

[Introduction](#)

Esta configuração de exemplo funciona para um escritório muito pequeno que se conecta diretamente à Internet, supondo que o Domain Name Service (DNS), o Simple Mail Transfer Protocol (SMTP) e os serviços Web sejam fornecidos por um sistema remoto executado pelo ISP (Internet Service Provider, Provedor de Serviços de Internet). Não há serviços na rede interna e apenas duas interfaces. Também não há registro porque não há host disponível para fornecer serviços de registro.

Como essa configuração usa apenas listas de acesso de entrada, ela faz anti-falsificação e filtragem de tráfego com a mesma lista de acesso. Essa configuração só funciona para um roteador de duas portas. A Ethernet 0 é a rede "interna". Serial 0 é um link de Frame Relay para o ISP.

Consulte [Roteador de Duas Interface com a Configuração do Cisco IOS Firewall NAT](#) para configurar um roteador de duas interfaces com NAT usando um Cisco IOS® Firewall.

Consulte [Roteador de Três Interfaces sem a Configuração do Cisco IOS Firewall NAT](#) para configurar um roteador de três interfaces sem NAT usando um Cisco IOS Firewall.

[Prerequisites](#)

[Requirements](#)

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento se aplicam a estas versões de software e hardware:

- Software Cisco IOS® versão 12.2(15)T13, suportado pelo Cisco IOS Software versão 11.3.3.T
- Cisco 2611 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.

Conventions

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

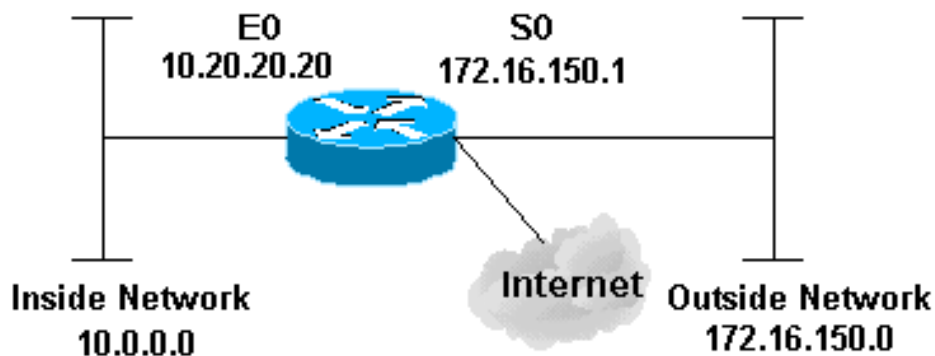
Configurar

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

Nota: 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 utiliza esta configuração:

2514 Router

```
version 12.2
!
service password-encryption
no service udp-small-servers
no service tcp-small-servers
no cdp run
!
hostname cbac-cisco
!
no ip source-route
!
enable secret 5 $1$FrMn$wBu0Xgv/Igy5Y.DarCmrm/
!
username cisco privilege 15 password 7 0822455D0A16
no ip source-route
ip domain-name cisco.com
ip name-server 172.16.150.5
!
!--- Set up inspection list "myfw". !--- Inspect for the
protocols that actually get used. ! ip inspect name myfw
cuseeme timeout 3600
ip inspect name myfw ftp timeout 3600
ip inspect name myfw http timeout 3600
ip inspect name myfw rcmd timeout 3600
ip inspect name myfw realaudio timeout 3600
ip inspect name myfw smtp timeout 3600
ip inspect name myfw tftp timeout 30
ip inspect name myfw udp timeout 15
ip inspect name myfw tcp timeout 3600
!
interface Ethernet0/0
description Cisco Ethernet RTP
 ip address 10.20.20.20 255.255.255.0
 no ip directed-broadcast
 !
 !--- Apply the access list in order to allow all
legitimate traffic !--- from the inside network but
prevent spoofing. ! ip access-group 101 in ! no ip
proxy-arp ! !--- Apply inspection list "myfw" to
Ethernet 0 inbound. !--- When conversations are
initiated from the internal network !--- to the outside,
this inspection list causes temporary additions !--- to
the traffic allowed in by serial interface 0 acl 111
when !--- traffic returns in response to the initiation.
! ip inspect myfw in
 no ip route-cache
 !
 no cdp enable
 !
interface Serial0/0
description Cisco FR
 ip address 172.16.150.1 255.255.255.0
 encapsulation frame-relay IETF
 no ip route-cache
 no arp frame-relay
 bandwidth 56
 service-module 56 clock source line
 service-module 56k network-type dds
 frame-relay lmi-type ansi
 !
 !--- Access list 111 allows some ICMP traffic and
```

```

administrative Telnet, !--- and does anti-spoofing.
There is no inspection on Serial 0. !--- However, the
inspection on the Ethernet interface adds temporary
entries !--- to this list when hosts on the internal
network make connections !--- out through the Frame
Relay. ! ip access-group 111 in no ip directed-broadcast
no ip route-cache bandwidth 56 no cdp enable frame-relay
interface-dlci 16 ! ip classless ip route 0.0.0.0
0.0.0.0 Serial0 ! !--- Access list 20 is used to control
which network management stations !--- can access
through SNMP. ! access-list 20 permit 172.16.150.8 ! !--
- The access list allows all legitimate traffic from the
inside network !--- but prevents spoofing. ! access-list
101 permit tcp 172.16.150.0 0.0.0.255 any access-list
101 permit udp 172.16.150.0 0.0.0.255 any access-list
101 permit icmp 172.16.150.0 0.0.0.255 any !--- This
deny is the default. access-list 101 deny ip any any !
!--- Access list 111 controls what can come from the
outside world !--- and it is anti-spoofing. ! access-
list 111 deny ip 127.0.0.0 0.255.255.255 any access-list
111 deny ip 172.16.150.0 0.0.0.255 any ! !--- Perform an
ICMP stuff first. There is some danger in these lists.
!--- They are control packets, and allowing *any* packet
opens !--- you up to some possible attacks. For example,
teardrop-style !--- fragmentation attacks can come
through this list. ! access-list 111 permit icmp any
172.16.150.0 0.0.0.255 administratively-prohibited
access-list 111 permit icmp any 172.16.150.0 0.0.0.255
echo access-list 111 permit icmp any 172.16.150.0
0.0.0.255 echo-reply access-list 111 permit icmp any
172.16.150.0 0.0.0.255 packet-too-big access-list 111
permit icmp any 172.16.150.0 0.0.0.255 time-exceeded
access-list 111 permit icmp any 172.16.150.0 0.0.0.255
traceroute access-list 111 permit icmp any 172.16.150.0
0.0.0.255 unreachable ! !--- Allow Telnet access from
10.11.11.0 corporate network administration people. !
access-list 111 permit tcp 10.11.11.0 0.0.0.255 host
172.16.150.1 eq telnet ! !--- This deny is the default.
! access-list 111 deny ip any any ! !--- Apply access
list 20 for SNMP process. ! snmp-server community secret
RO 20 ! line con 0 exec-timeout 5 0 password 7
14191D1815023F2036 login local line vty 0 4 exec-timeout
5 0 password 7 14191D1815023F2036 login local length 35
end

```

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Depois de configurar o roteador IOS Firewall, se as conexões não funcionarem, certifique-se de que você tenha habilitado a inspeção com o comando **ip inspect (nome definido) in ou out** na interface. Nesta configuração, **ip inspect myfw in** é aplicado à interface Ethernet0/0.

Para esses comandos, juntamente com outras informações de troubleshooting, consulte [Proxy de Autenticação de Troubleshooting](#).

Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar os comandos debug.

[Informações Relacionadas](#)

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