

Router de tres interfaces sin la configuración del Firewall Cisco IOS NAT

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

[Introducción](#)

Este documento contiene un ejemplo de una configuración típica para una pequeña empresa que está conectada a Internet y ejecuta sus propios servidores. La conexión a Internet se produce en una línea serial. Ethernet 0 se conecta a la red interna (una sola LAN). Ethernet 1 está conectada a una red DMZ, la cual solo usa un nodo para prestar servicios al exterior. El ISP ha asignado a la compañía el netblock 192.168.27.0/24. Se divide equitativamente entre la DMZ y la LAN interna con la máscara de subred 255.255.255.128. La política básica es la siguiente:

- Permita que los usuarios en la red interna conecten con cualquier servicio en el Internet pública.
- Permita que cualquiera en Internet se conecte a los servicios de WWW, FTP y Protocolo simple de transferencia de correo (SMTP) en el servidor DMZ, y permita hacerle consultas acerca del Sistema de nombre de servicio (DNS). Esto permite que la gente exterior vea las páginas web de la compañía, coger clasifía a la compañía ha fijado para el consumo exterior, y enviar el correo en la compañía.
- Permitir a los usuarios internos conectarse al servicio POP en el servidor DMZ (para acceder a su correo) y comunicarse al mismo a través de Telnet (para administrarlo).
- Sin permitir que algún elemento del DMZ inicie actividad alguna, ya sea con la red privada o con Internet.
- Auditoría todas las conexiones que crucen el Firewall a un servidor de Syslog en la red privada. Las máquinas en la red interna utilizan al servidor DNS en el DMZ. Las listas de acceso de entrada se utilizan en todas las interfaces para prevenir el spoofing. Las listas de accesos de salida se utilizan para controlar qué tráfico se puede enviar a cualquier interfaz dada.

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 de Cisco IOS®.

Refiera al [router de dos interfaces con la configuración del Firewall Cisco IOS NAT](#) para configurar a un router de dos interfaces con el NAT usando un Firewall Cisco IOS.

[prerrequisitos](#)

[Requisitos](#)

No hay requisitos específicos para este documento.

[Componentes Utilizados](#)

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

- Cisco IOS Software Release 12.2(15)T13 con el Conjunto de características de firewall
- Router del Cisco 7204 VXR

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.

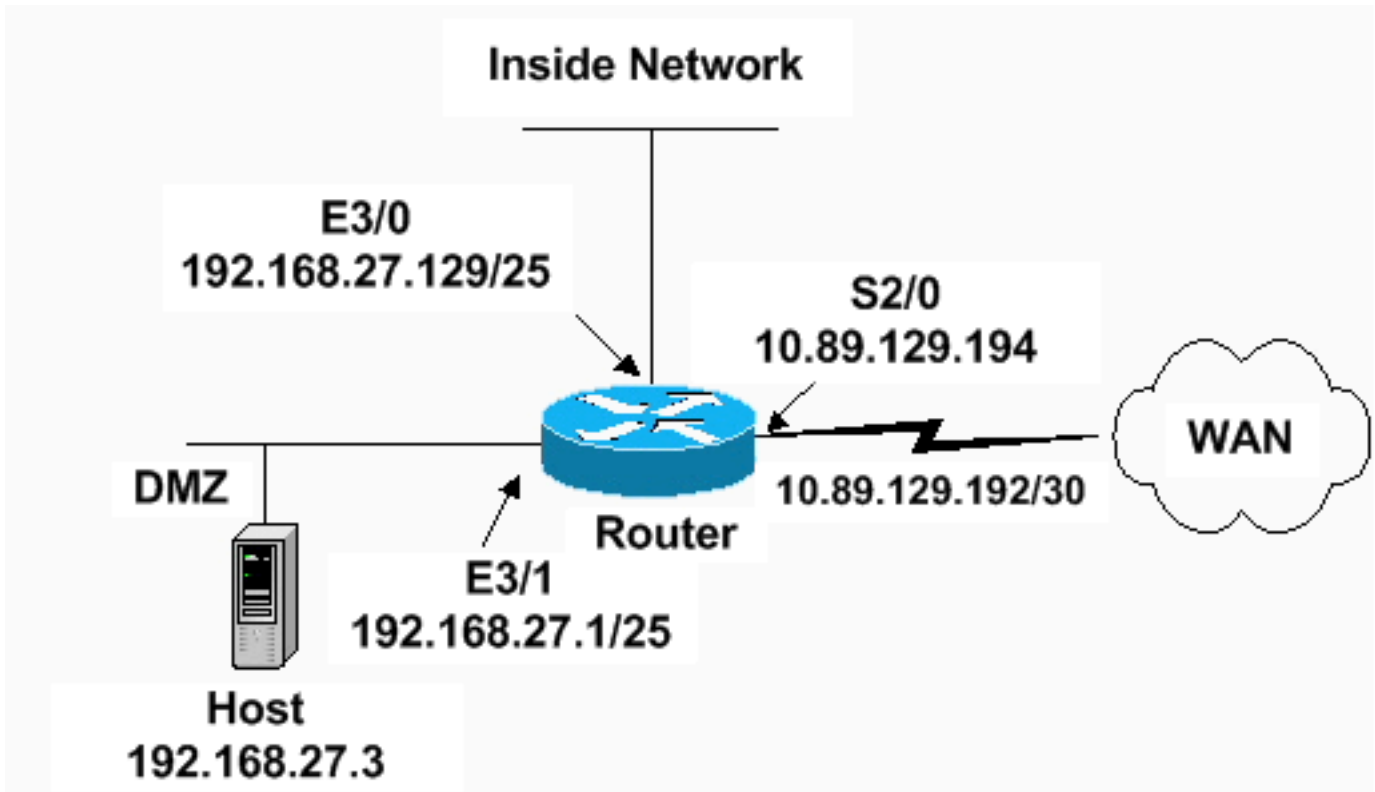
[Configurar](#)

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](#)

En este documento, se utiliza esta configuración de red:



[Configuraciones](#)

Este documento utiliza esta configuración.

Router VXR 7204

```

version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Router
!
logging queue-limit 100
enable secret 5 <something>
!
ip subnet-zero
ip cef
no ip domain lookup
!
ip inspect audit-trail
!
!--- Sets the length of time a TCP session !--- is
still managed after no activity. ! ip inspect tcp idle-
time 14400 ! !--- Sets the length of time a UDP session
!--- is still managed after no activity. ! ip inspect
udp idle-time 1800 ! !--- Sets the length of time a DNS
name lookup session !--- is still managed after no
activity. ! ip inspect dns-timeout 7 ! !--- Sets up
inspection list "standard" !--- to be used for
inspection of inbound Ethernet 0 !--- and inbound serial
(applied to both interfaces). ! ip inspect name standard
cuseeme ip inspect name standard ftp ip inspect name
standard h323 ip inspect name standard http ip inspect
name standard rcmd ip inspect name standard realaudio ip
inspect name standard smtp ip inspect name standard
sqlnet ip inspect name standard streamworks ip inspect

```

```

name standard tcp ip inspect name standard tftp ip
inspect name standard udp ip inspect name standard
vdolive ip audit notify log ip audit po max-events 100 !
no voice hpi capture buffer no voice hpi capture
destination ! mta receive maximum-recipients 0 !
interface ethernet 3/0 ip address 192.168.27.129
255.255.255.128 ! !--- Apply the access list to allow
all legitimate !--- traffic from the inside network and
prevent spoofing. ! ip access-group 101 in ! !--- Apply
inspection list "standard" for inspection !--- of
inbound Ethernet traffic. This inspection opens !---
temporary entries on access lists 111 and 121. ! ip
inspect standard in duplex full interface ethernet 3/1
ip address 192.168.27.1 255.255.255.128 ! !--- Apply the
access list to permit DMZ traffic (except spoofing) !---
on the DMZ interface inbound. The DMZ is not permitted
to initiate !--- any outbound traffic except Internet
Control Message Protocol (ICMP). ! ip access-group 111
in ! !--- Apply inspection list "standard" for
inspection of outbound !--- traffic from e1. This adds
temporary entries on access list 111 !--- to allow
return traffic, and protects servers in DMZ from !---
distributed denial of service (DDoS) attacks. ip inspect
standard out duplex full ! interface serial 2/0 ip
address 10.89.129.194 255.255.255.252 !--- Apply the
access list to allow legitimate traffic. ! ip access-
group 121 in serial restart_delay 0 ! ip classless no ip
http-server !--- A syslog server is located at this
address. logging 192.168.27.131 !--- This command
enables the logging of session !--- information
(addresses and bytes). !--- Access list 20 is used to
control which !--- network management stations can
access via SNMP. ! access-list 20 permit 192.168.27.5 !
!--- Use an access list to allow all legitimate traffic
from !--- the inside network and prevent spoofing. The
inside !--- network can only connect to the Telnet and
POP3 !--- service of 192.168.27.3 on DMZ, and can ping
(ICMP) to the DMZ. !--- Additional entries can be added
to permit SMTP, WWW, and !--- so forth, if necessary. In
addition, the inside network can !--- connect to any
service on the Internet. ! access-list 101 permit tcp
192.168.27.128 0.0.0.127 host 192.168.27.3 eq pop3
access-list 101 permit tcp 192.168.27.128 0.0.0.127 host
192.168.27.3 eq telnet access-list 101 permit icmp
192.168.27.128 0.0.0.127 192.168.27.0 0.0.0.127 access-
list 101 deny ip 192.168.27.128 0.0.0.127 192.168.27.0
0.0.0.127 access-list 101 permit ip 192.168.27.128
0.0.0.127 any access-list 101 deny ip any any ! ! !---
The access list permits ping (ICMP) from the DMZ and
denies all !--- traffic initiated from the DMZ.
Inspection opens !--- temporary entries to this list. !
access-list 111 permit icmp 192.168.27.0 0.0.0.127 any
access-list 111 deny ip any any ! ! ! !--- Access list
121 allows anyone on the Internet to connect to !---
WWW, FTP, DNS, and SMTP services on the DMZ host. It
also !--- allows some ICMP traffic. access-list 121
permit udp any host 192.168.27.3 eq domain access-list
121 permit tcp any host 192.168.27.3 eq domain access-
list 121 permit tcp any host 192.168.27.3 eq www access-
list 121 permit tcp any host 192.168.27.3 eq ftp access-
list 121 permit tcp any host 192.168.27.3 eq smtp
access-list 121 permit icmp any 192.168.27.0 0.0.0.255
administratively-prohibited access-list 121 permit icmp
any 192.168.27.0 0.0.0.255 echo access-list 121 permit

```

```

icmp any 192.168.27.0 0.0.0.255 echo-reply access-list
121 permit icmp any 192.168.27.0 0.0.0.255 packet-too-
big access-list 121 permit icmp any 192.169.27.0
0.0.0.255 time-exceeded access-list 121 permit icmp any
192.168.27.0 0.0.0.255 traceroute access-list 121 permit
icmp any 192.168.27.0 0.0.0.255 unreachable access-list
121 deny ip any any ! !--- Apply access list 20 for SNMP
process. ! snmp-server community secret RO 20 snmp-
server enable traps tty ! call rsvp-sync ! mgcp profile
default ! dial-peer cor custom ! gatekeeper shutdown !
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

```

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.

- **lista de acceso de la demostración** — Verifica la configuración correcta de las Listas de acceso configuradas en la ejecutar [configuración](#). Router#**show access-list** Standard IP access list 20 10 permit 192.168.27.5 Extended IP access list 101 10 permit tcp 192.168.27.128 0.0.0.127 host 192.168.27.3 eq pop3 20 permit tcp 192.168.27.128 0.0.0.127 host 192.168.27.3 eq telnet 30 permit icmp 192.168.27.128 0.0.0.127 192.168.27.0 0.0.0.127 40 deny ip 192.168.27.128 0.0.0.127 192.168.27.0 0.0.0.127 50 permit ip 192.168.27.128 0.0.0.127 any 60 deny ip any any Extended IP access list 111 10 permit icmp 192.168.27.0 0.0.0.127 any 20 deny ip any any (9 matches) Extended IP access list 121 10 permit udp any host 192.168.27.3 eq domain 20 permit tcp any host 192.168.27.3 eq domain 30 permit tcp any host 192.168.27.3 eq www 40 permit tcp any host 192.168.27.3 eq ftp 50 permit tcp any host 192.168.27.3 eq smtp 60 permit icmp any 192.168.27.0 0.0.0.255 administratively-prohibited 70 permit icmp any 192.168.27.0 0.0.0.255 echo 80 permit icmp any 192.168.27.0 0.0.0.255 echo-reply 90 permit icmp any 192.168.27.0 0.0.0.255 packet-too-big 100 permit icmp any 192.169.27.0 0.0.0.255 time-exceeded 110 permit icmp any 192.168.27.0 0.0.0.255 traceroute 120 permit icmp any 192.168.27.0 0.0.0.255 unreachable 130 deny ip any any (4866 matches) Router#
- **muestre la auditoría toda del IP** — Verifica la configuración de los comandos logging. Router#**show ip audit all** Event notification through syslog is enabled Event notification through Net Director is disabled Default action(s) for info signatures is alarm Default action(s) for attack signatures is alarm Default threshold of recipients for spam signature is 250 PostOffice:HostID:0 OrgID:0 Msg dropped:0 :Curr Event Buf Size:0 Configured:100 Post Office is not enabled - No connections are active Router#
- **el IP de la demostración examina todos** — Verifica la configuración de las reglas del examen del Firewall Cisco IOS por la interfaz. Router#**show ip inspect all** Session audit trail is enabled Session alert is enabled one-minute (sampling period) thresholds are [400:500] connections max-incomplete sessions thresholds are [400:500] max-incomplete tcp connections per host is 50. Block-time 0 minute. tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec tcp idle-time is 14400 sec -- udp idle-time is 1800 sec dns-timeout is 7 sec Inspection Rule Configuration Inspection name standard coseeme alert is on audit-trail is on timeout 14400 ftp alert is on audit-trail is on timeout 14400 h323 alert is on audit-trail is on timeout 14400 http alert is on audit-trail is on timeout 14400 rcmd alert is on audit-trail is on timeout 14400 realaudio alert is on audit-trail is on timeout 14400 smtp alert is on audit-trail is on timeout 14400 sqlnet alert is on audit-trail is on timeout 14400 streamworks alert is on audit-trail is on timeout 1800 tcp alert is on audit-trail is on timeout 14400 tftp alert is on audit-trail is on timeout 1800 udp alert is on audit-trail is on timeout 1800 vdolive alert is on audit-trail is on timeout 14400 Interface Configuration Interface Ethernet3/0 Inbound inspection rule is standard coseeme alert is on audit-trail is on timeout 14400 ftp alert is on audit-trail is on timeout 14400 h323 alert is on audit-trail

is on timeout 14400 http alert is on audit-trail is on timeout 14400 rcmd alert is on audit-trail is on timeout 14400 realaudio alert is on audit-trail is on timeout 14400 smtp alert is on audit-trail is on timeout 14400 sqlnet alert is on audit-trail is on timeout 14400 streamworks alert is on audit-trail is on timeout 1800 tcp alert is on audit-trail is on timeout 14400 tftp alert is on audit-trail is on timeout 1800 udp alert is on audit-trail is on timeout 1800 vdolive alert is on audit-trail is on timeout 14400 Outgoing inspection rule is not set Inbound access list is 101 Outgoing access list is not set Interface Ethernet3/1 Inbound inspection rule is not set Outgoing inspection rule is standard cuseeme alert is on audit-trail is on timeout 14400 ftp alert is on audit-trail is on timeout 14400 h323 alert is on audit-trail is on timeout 14400 http alert is on audit-trail is on timeout 14400 rcmd alert is on audit-trail is on timeout 14400 realaudio alert is on audit-trail is on timeout 14400 smtp alert is on audit-trail is on timeout 14400 sqlnet alert is on audit-trail is on timeout 14400 streamworks alert is on audit-trail is on timeout 1800 tcp alert is on audit-trail is on timeout 14400 tftp alert is on audit-trail is on timeout 1800 udp alert is on audit-trail is on timeout 1800 vdolive alert is on audit-trail is on timeout 14400 Inbound access list is 111 Outgoing access list is not set Router#

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 examina (nombre definido) adentro o comando out** en la interfaz. En esta configuración, el **IP examina el estándar adentro** es aplicado para las interfaces Ethernet 3/0 y el **IP examina el estándar hacia fuera** es aplicado para las interfaces Ethernet 3/1.

Refiera a las [configuraciones del Firewall Cisco IOS del troubleshooting](#) para más información sobre el troubleshooting.

Información Relacionada

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