Roteador de três interfaces sem a configuração do Cisco IOS Firewall NAT

Contents

Introduction

Este documento fornece um exemplo de configuração típica de empresa de pequeno porte conectada à Internet, que executa seus próprios servidores. A conexão com a Internet ocorre via linha serial. Ethernet 0 está conectada à rede interna (uma LAN única). A Ethernet 1 está conectada a uma rede DMZ, que tem um único nó usado para fornecer serviços ao mundo externo. O ISP atribuiu à empresa o netblock 192.168.27.0/24. Ele é igualmente dividido entre o DMZ e a LAN interna com máscara de sub-rede 255.255.255.128. A política básica é:

- Permitir que os usuários na rede interna se conectem a qualquer serviço na Internet pública.
- Permitir que qualquer pessoa na Internet se conecte aos serviços WWW, FTP e SMTP no servidor DMZ, e fazer com que o DNS os consulte. Isso permite que pessoas externas vejam páginas da Web da empresa, captem arquivos que a empresa publicou para consumo externo e enviem e-mails para a empresa.
- Permita que os usuários internos conectem-se aos serviço POP no servidor DMZ (para selecionar correio) e estabeleçam uma sessão Telnet (para administrá-lo).
- Não permita que nada no DMZ inicie nenhuma conexão, seja com a rede privada, seja com a internet.
- Auditoria de todas as conexões que cruzam o firewall com um servidor SYSLOG na rede privada. As máquinas na rede interna usam o servidor DNS na DMZ. As listas de acesso de entrada são usadas em todas as interfaces para evitar falsificação. As listas de acesso de saída são usadas para controlar qual tráfego pode ser enviado a qualquer interface específica.

Consulte Roteador de duas interfaces sem NAT usando a configuração do Cisco IOS Firewall para configurar um roteador de duas interfaces sem NAT usando o Cisco IOS® Firewall.

Consulte Roteador de Duas Interfaces com a Configuração do Cisco IOS Firewall NAT para configurar um roteador de duas interfaces com NAT usando um Cisco IOS Firewall.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Software Cisco IOS versão 12.2(15)T13 com conjunto de recursos de firewall
- Roteador Cisco 7204 VXR

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.

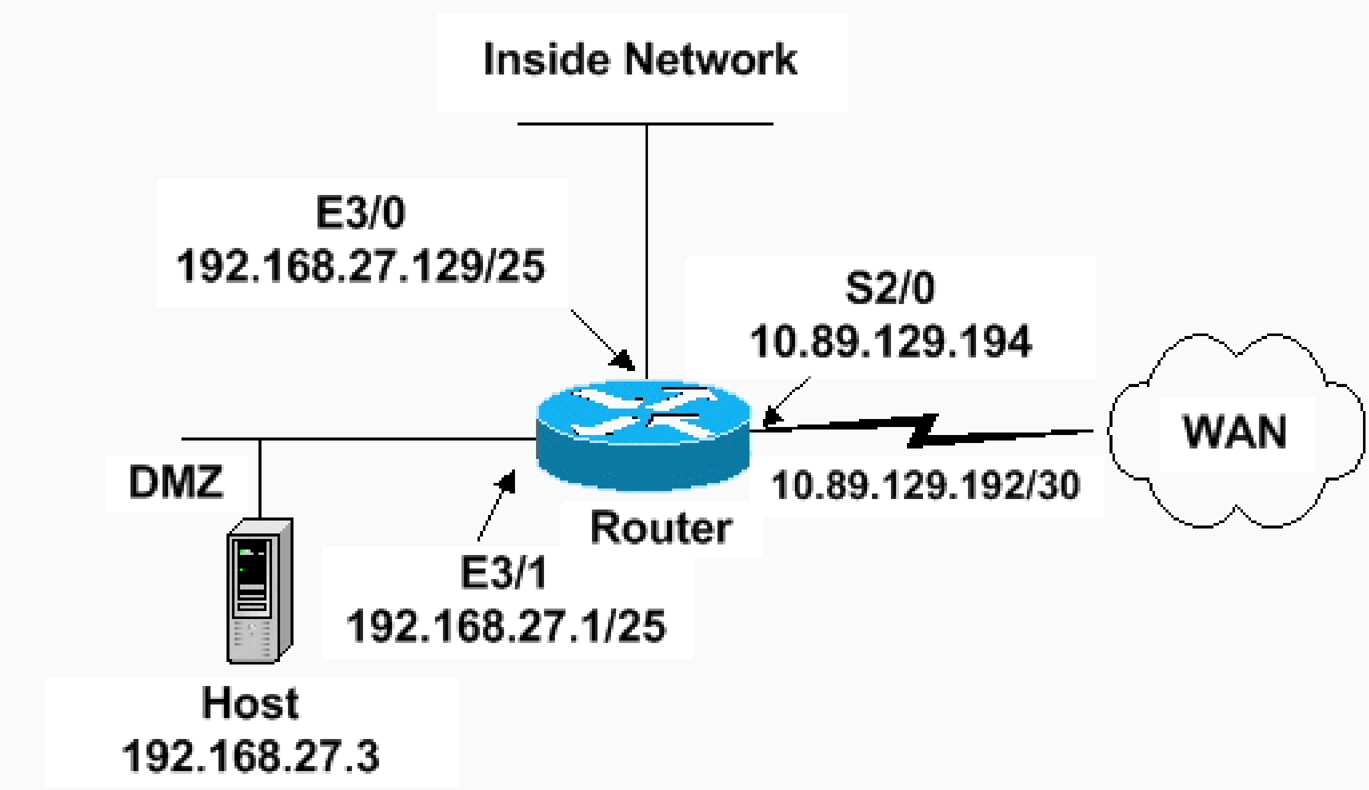
Configurar

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:



Configurações

Este documento utiliza esta configuração.

Roteador 7204 VXR

```
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
```

Verificar

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

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **show access-list** —Verifica a configuração correta das listas de acesso configuradas na configuração atual.

  ```
  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#
  ```

- **show ip audit all** — Verifica a configuração dos 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#
  ```

- **show ip inspect all** —Verifica a configuração das regras de inspeção do Cisco IOS Firewall por interface.

  ```
  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
       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
Interface Configuration
     Interface Ethernet3/0
       Inbound 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
       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#
```

Troubleshoot

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, o **padrão ip inspect em** é aplicado para a interface ethernet 3/0 e o **padrão ip inspect out** é aplicado para a interface ethernet 3/1.

Consulte Troubleshooting Cisco IOS Firewall Configurations para obter mais informações sobre como solucionar problemas.

Informações Relacionadas

- **Página de suporte do Cisco IOS Firewall**
- **Suporte Técnico e Documentação - Cisco Systems**