没有NAT 的三接口路由器的Cisco IOS防火墙配置

目录

简介

本文提供了连接到互联网、运行自己的服务器的小型办公室的典型配置示例。与互联网的连接是通过串行线路实现。Ethernet 0 连接至内部网络（单个 LAN）。 Ethernet 1 连接至 DMZ 网络，该网络有一个用于为外界提供服务的节点。ISP已为公司分配了网络块192.168.27.0/24。这在DMZ和子网掩码为255.255.255.128的内部LAN之间平均分配。基本策略是：

- 允许内部网络中的用户连接至公用互联网上的任何服务。
- 允许互联网上的任何人连接到DMZ服务器上的WWW、FTP和简单邮件转发协议(SMTP)业务，并进行域名系统(DNS)查询。外部人员因此能够查看公司网页，获取公司发布的供外部调用的文件，并向公司发送邮件。
- 允许内部用户连接到DMZ服务器上的POP服务(收邮件)，并进行远程登录(管理)。
- 不允许DMZ上的任何东西发起任何连接，不管是到专用网络还是互联网的连接均不可以。
- 审计所有越过防火墙与专用网络上的 SYSLOG 服务器进行的连接。内部网络中的计算机使用 DMZ 上的 DNS 服务器。所有接口均使用输入访问列表来防止欺骗。输出访问列表用于控制可以发送到任何指定接口的流量。

要使用 Cisco IOS 防火墙配置不带 NAT 的两接口路由器，请参阅使用 Cisco IOS 防火墙配置的不带 NAT 的两接口路由器。

要使用思科 IOS 防火墙配置带 NAT 的双接口路由器，请参阅使用思科 IOS 防火墙配置带 NAT 的双接口路由器。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 具有防火墙功能集的思科 IOS 软件 12.2(15)T13 版本
- 思科 7204 VXR 路由器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

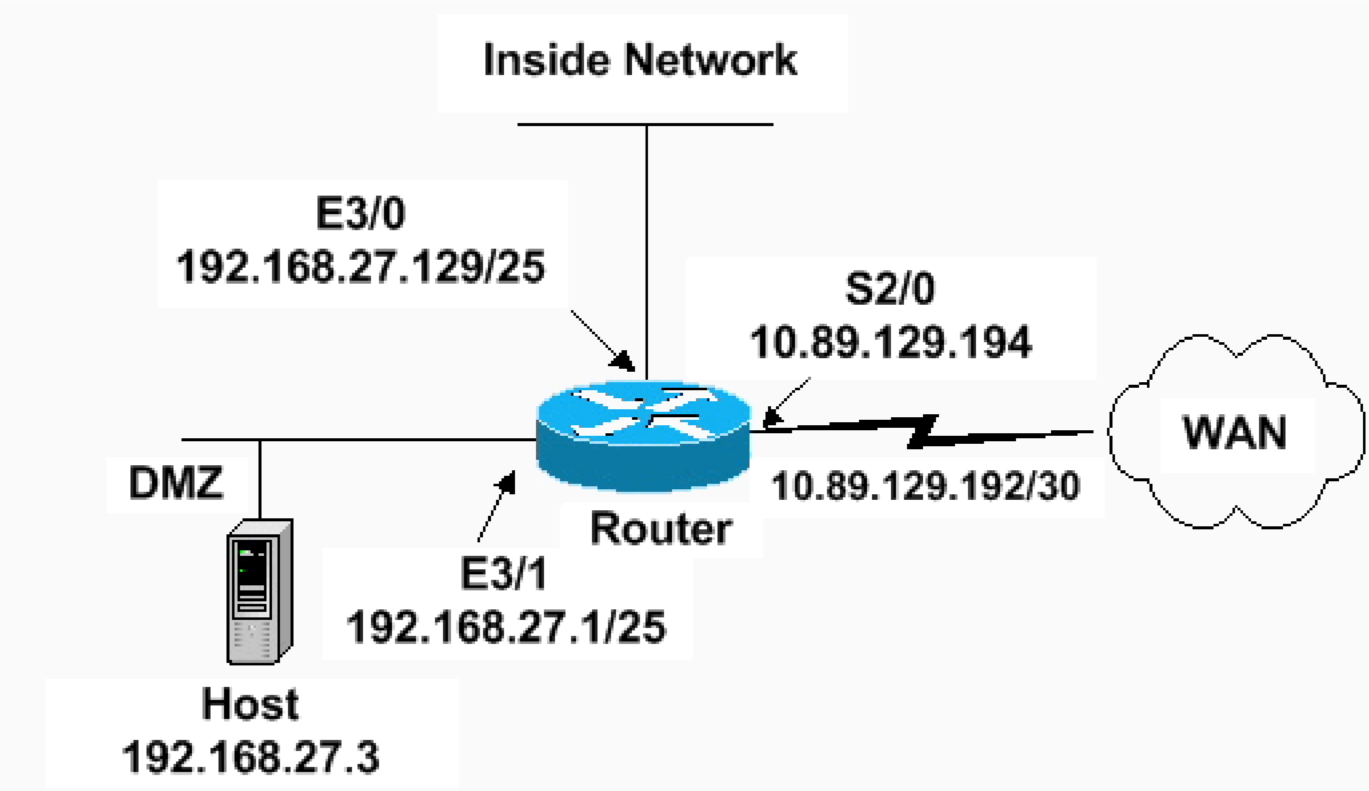
配置

本部分提供有关如何配置本文档所述功能的信息。

注意：使用命令查找工具(仅限注册客户)可获取有关本节中使用的命令的详细信息。

网络图

本文档使用以下网络设置：



配置

本文档使用以下配置。

7204 VXR 路由器

```
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
```

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

- **show access-list - 验证在 running-configuration 中配置的访问列表的配置是否正确。**

```
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 - 验证日志记录命令的配置。

```
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 - 验证每个接口的思科 IOS 防火墙检查规则的配置。

```
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#
```

故障排除

配置 IOS 防火墙路由器后，如果连接不起作用，请确保已使用 **ip inspect (定义的名称) in/out 命令对接口启用检查。**在此配置中，**ip inspect standard in 适用于接口 Ethernet 3/0，ip inspect standard out 适用于接口 Ethernet 3/1。**

有关故障排除的更多信息，请参阅思科 IOS 防火墙配置故障排除。

相关信息

- **Cisco IOS 防火墙支持页**
- **技术支持和文档 - Cisco Systems**