無NAT Cisco IOS防火牆配置的三介面路由器

目錄

簡介

本文提供連線到網際網路並運行其自身伺服器的小型企業的典型配置示例。與Internet的連線是通過串列線路進行的。乙太網0連線到內部網路（單個LAN）。 乙太網1連線到DMZ網路，該網路有一個用於為外部世界提供服務的節點。ISP為公司分配了網路塊192.168.27.0/24。此地址在DMZ和內部LAN之間平均分配，子網掩碼為255.255.255.128。基本策略為：

- 允許內部網路上的使用者連線到公共Internet上的任何服務。
- 允許Internet上的任何人連線到DMZ伺服器上的WWW、FTP和簡單郵件傳輸協定(SMTP)服務，並對其執行域名系統(DNS)查詢。這樣，外部人員就可以檢視公司網頁，取回公司發佈供外部消費的檔案，並向公司傳送郵件。
- 允許內部使用者連線到DMZ伺服器上的POP服務（取回他們的郵件）和Telnet到該服務（對其進行管理）。
- 不允許DMZ上的任何內容啟動任何連線，無論是到專用網路還是到Internet。
- 稽核通過防火牆與專用網路上的SYSLOG伺服器之間的所有連線。內部網路上的電腦使用DMZ上的DNS伺服器。輸入存取清單用於所有介面，以防止偽裝。輸出存取清單用於控制哪些流量可傳送到任何指定介面。

請參閱使用Cisco IOS防火牆配置無NAT的雙介面路由器，以使用Cisco IOS®防火牆配置無NAT的雙介面路由器。

請參閱使用NAT Cisco IOS防火牆配置的雙介面路由器，以使用Cisco IOS防火牆配置使用NAT的雙介面路由器。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據軟體和硬體版本：

- 含防火牆功能集的Cisco IOS軟體版本12.2(15)T13
- Cisco 7204 VXR路由器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

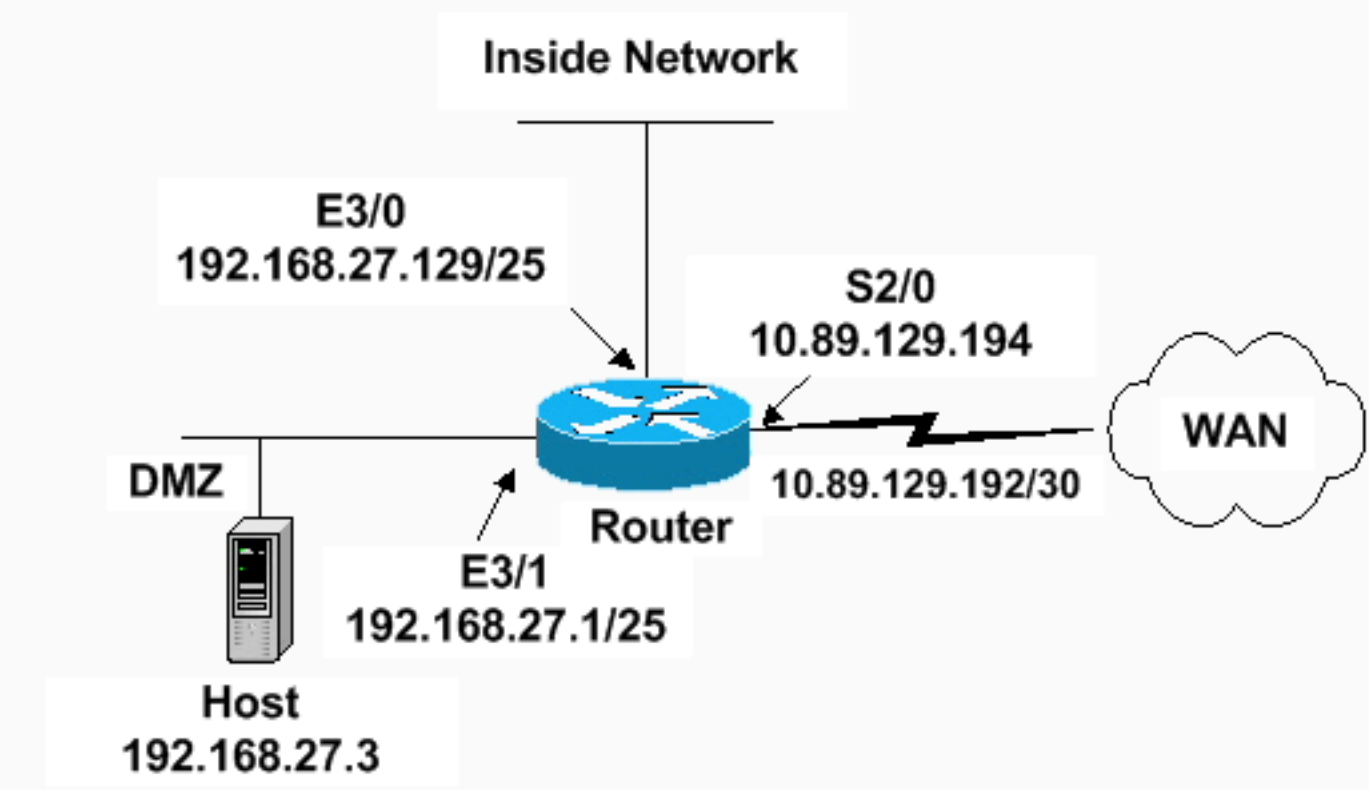
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定：



組態

本檔案會使用此組態。

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
```

驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析。

- show access-list — 驗證運行配置中配置的訪問清單的正確配置。

```
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** — 驗證日誌記錄命令的配置。

```
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** — 驗證每個介面的Cisco IOS防火牆檢查規則的配置。

```
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#
```

疑難排解

設定IOS防火牆路由器後，如果連線無法運作，請確認已在介面上使用**ip inspect（定義名稱）in或out指令啟用檢**測。在此配置中，**ip inspect standard in**應用於介面乙太網路3/0,**ip inspect standard out**應用於介面乙太網路3/1。

有關故障排除的詳細資訊，請參閱Cisco IOS防火牆配置故障排除。

相關資訊

- Cisco IOS防火牆支援頁面
- 技術支援與文件 - Cisco Systems