NAT 없는 3인터페이스 라우터 Cisco IOS 방화벽 컨피그레이션

목차

소개

이 문서에서는 인터넷에 연결되어 있고 자체 서버를 실행하는 소기업을 위한 일반적인 구성의 예를 제공합니다. 인터넷에 대한 연결이 직렬 회선을 통해 이루어집니다. 이더넷 0은 내부 네트워크(단일 LAN)에 연결됩니다. 이더넷 1은 외부 세계에 서비스를 제공하는 데 사용되는 단일 노드가 있는 DMZ 네트워크에 연결됩니다. ISP에서 회사에 netblock 192.168.27.0/24을 할당했습니다. 이는 DMZ와 내부 LAN 간에 균등하게 분할되며 서브넷 마스크 255.255.255.128. 기본 정책은 다음과 같습니다.

- 내부 네트워크의 사용자가 공용 인터넷의 모든 서비스에 연결하도록 허용합니다.
- 인터넷에 있는 모든 사용자가 DMZ 서버의 WWW, FTP 및 SMTP(Simple Mail Transfer Protocol) 서비스에 연결하고 DNS(Domain Name System) 쿼리를 만들 수 있습니다. 이를 통해 외부 사용자는 회사 웹 페이지를 보고, 회사가 외부 사용을 위해 게시한 파일을 수거하고, 회사에 메일을 보낼 수 있습니다.
- 내부 사용자가 DMZ 서버의 POP 서비스(메일 받기)와 텔넷에 연결하여(관리)할 수 있습니다.
- DMZ에서 사설 네트워크 또는 인터넷에 대한 연결을 시작할 수 없습니다.
- 방화벽을 통과하는 모든 연결을 사설 네트워크의 SYSLOG 서버로 감사합니다. 내부 네트워크의 시스템은 DMZ의 DNS 서버를 사용합니다. 스푸핑을 방지하기 위해 모든 인터페이스에서 입력 액세스 목록이 사용됩니다. 출력 액세스 목록은 어떤 트래픽이 지정된 인터페이스로 전송될 수 있는지를 제어하는 데 사용됩니다.

Cisco IOS® Firewall을 사용하여 NAT를 사용하지 않고 2개의 인터페이스 라우터를 구성하려면 Cisco IOS Firewall Configuration을 사용하여 NAT가 없는 2개의 인터페이스 라우터를 참조하십시오.

Cisco IOS Firewall을 사용하여 NAT로 2개의 인터페이스 라우터를 구성하려면 NAT Cisco IOS Firewall이 있는 2개의 인터페이스 라우터를 참조하십시오.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS Software 릴리스 12.2(15)T13(방화벽 기능 집합 포함)
- Cisco 7204 VXR 라우터

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

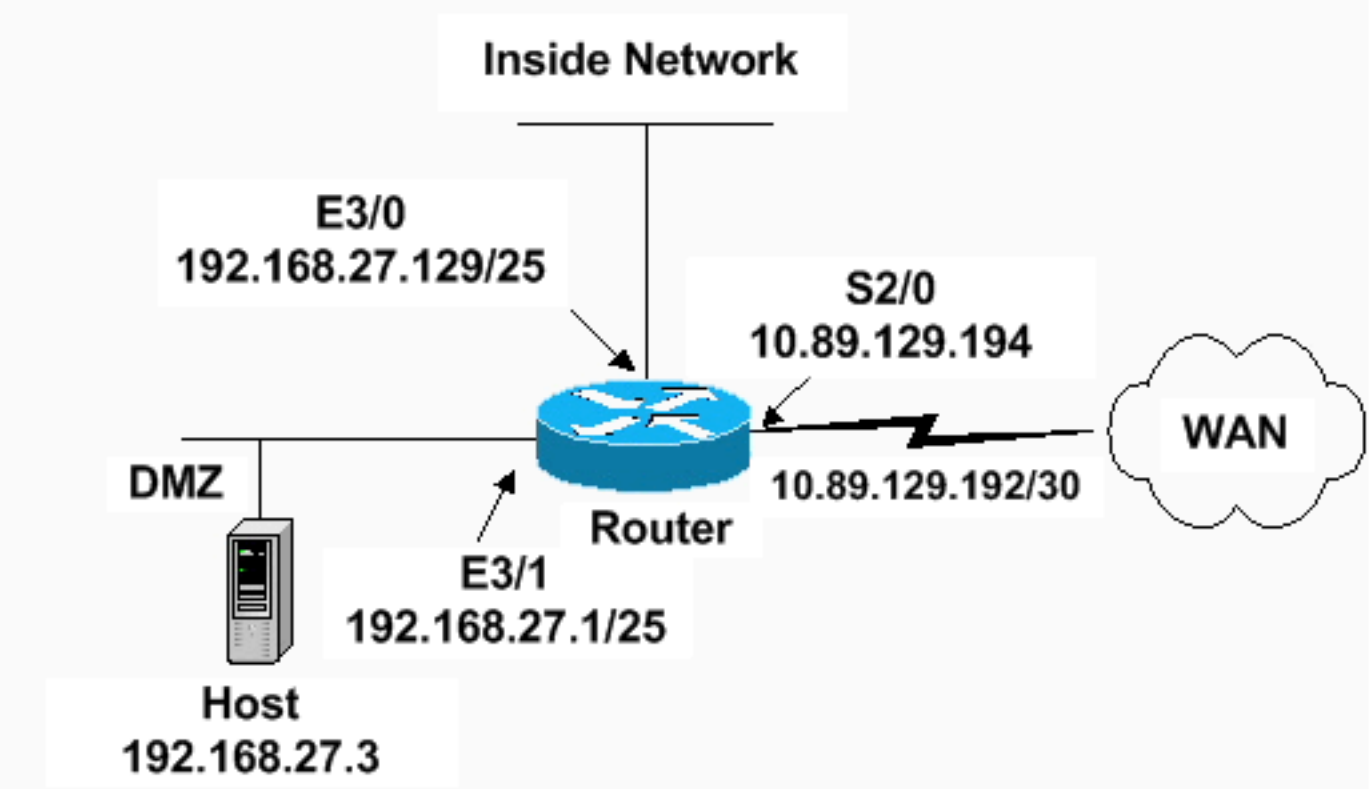
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



구성

이 문서에서는 이 구성을 사용합니다.

7204 VXR 라우터

```
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
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다. OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

- **show access-list** - running-configuration에 구성된 액세스 목록의 올바른 구성을 확인합니다.

```
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** - logging 명령의 컨피그레이션을 확인합니다.

```
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** - 인터페이스당 Cisco IOS Firewall 검사 규칙의 컨피그레이션을 확인합니다.

```
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#
```

문제 해결

IOS Firewall 라우터를 구성한 후 연결이 작동하지 않을 경우 인터페이스에서 **ip inspect(name defined) 또는 out** 명령으로 검사를 활성화했는지 확인합니다. 이 컨피그레이션에서는 **ip inspect 표**

준이 인터페이스 이더넷 3/0에 적용되며 **ip inspect 표준 출력**이 인터페이스 이더넷 3/1에 적용됩니다.

트러블슈팅에 대한 자세한 내용은 Cisco IOS 방화벽 구성 트러블슈팅을 참조하십시오.

관련 정보

- Cisco IOS 방화벽 지원 페이지
- 기술 지원 및 문서 – Cisco Systems