Cisco IOS 방화벽 컨피그레이션을 사용하는 NAT가 없는 2인터페이스 라우터

목차

소개

이 샘플 구성은 DNS(Domain Name Service), SMTP(Simple Mail Transfer Protocol) 및 웹 서비스가 ISP(Internet Service Provider)가 실행하는 원격 시스템에서 제공된다는 가정 하에 인터넷에 직접 연결되는 소규모 사무실에서 작동합니다. 내부 네트워크에는 서비스가 없으며 인터페이스는 두 개뿐입니다. 로깅 서비스를 제공할 수 있는 호스트가 없기 때문에 로깅도 없습니다.

이 컨피그레이션에서는 입력 액세스 목록만 사용하므로 동일한 액세스 목록을 사용하여 스푸핑 방지 및 트래픽 필터링을 모두 수행합니다. 이 컨피그레이션은 2포트 라우터에서만 작동합니다. 이더넷 0은 "내부" 네트워크입니다. 직렬 0은 ISP에 대한 프레임 릴레이 링크입니다.

Cisco IOS® 방화벽을 사용하여 NAT로 2개의 인터페이스 라우터를 구성하려면 NAT Cisco IOS Firewall 컨피그레이션이 있는 2개의 인터페이스 라우터를 참조하십시오.

Cisco IOS Firewall을 사용하여 NAT를 사용하지 않고 3개의 인터페이스 라우터를 구성하려면 NAT를 사용하지 않는 3개의 인터페이스 라우터를 참조하십시오.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전에 적용됩니다.

- Cisco IOS Software 릴리스 11.3.3.T에서 지원되는 Cisco IOS® Software 릴리스 12.2(15)T13
- Cisco 2611 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.

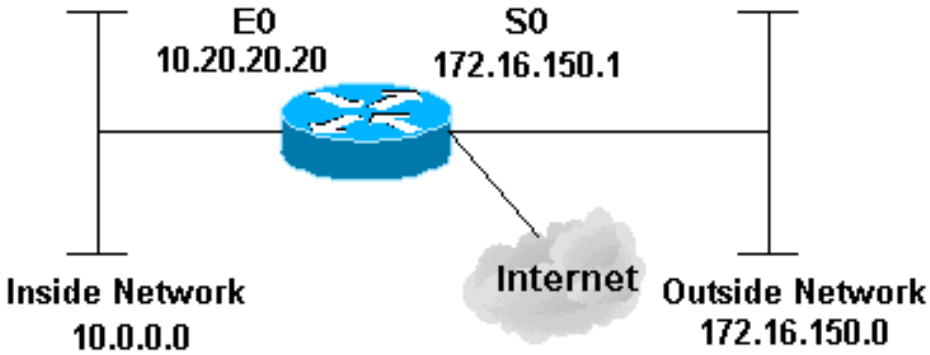
구성

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 다음 구성을 사용합니다.

2514 라우터
version 12.2 ! service password-encryption

```
no service udp-small-servers
no service tcp-small-servers
no cdp run
!
hostname cbac-cisco
!
no ip source-route
!
enable secret 5 $1$FrMn$wBu0Xgv/Igy5Y.DarCmrm/
!
username cisco privilege 15 password 7 0822455D0A16
no ip source-route
ip domain-name cisco.com
ip name-server 172.16.150.5
!
!--- Set up inspection list "myfw". !--- Inspect for the
protocols that actually get used. ! ip inspect name myfw
cuseeme timeout 3600
ip inspect name myfw ftp timeout 3600
ip inspect name myfw http timeout 3600
ip inspect name myfw rcmd timeout 3600
ip inspect name myfw realaudio timeout 3600
ip inspect name myfw smtp timeout 3600
ip inspect name myfw tftp timeout 30
ip inspect name myfw udp timeout 15
ip inspect name myfw tcp timeout 3600
!
interface Ethernet0/0
description Cisco Ethernet RTP
 ip address 10.20.20.20 255.255.255.0
 no ip directed-broadcast
 !
 !--- Apply the access list in order to allow all
legitimate traffic !--- from the inside network but
prevent spoofing. ! ip access-group 101 in ! no ip
proxy-arp ! !--- Apply inspection list "myfw" to
Ethernet 0 inbound. !--- When conversations are
initiated from the internal network !--- to the outside,
this inspection list causes temporary additions !--- to
the traffic allowed in by serial interface 0 acl 111
when !--- traffic returns in response to the initiation.
! ip inspect myfw in
 no ip route-cache
 !
 no cdp enable
 !
 interface Serial0/0
 description Cisco FR
 ip address 172.16.150.1 255.255.255.0
 encapsulation frame-relay IETF
 no ip route-cache
 no arp frame-relay
 bandwidth 56
 service-module 56 clock source line
 service-module 56k network-type dds
 frame-relay lmi-type ansi
 !
 !--- Access list 111 allows some ICMP traffic and
administrative Telnet, !--- and does anti-spoofing.
There is no inspection on Serial 0. !--- However, the
inspection on the Ethernet interface adds temporary
entries !--- to this list when hosts on the internal
network make connections !--- out through the Frame
Relay. ! ip access-group 111 in no ip directed-broadcast
```

```
no ip route-cache bandwidth 56 no cdp enable frame-relay
interface-dlci 16 ! ip classless ip route 0.0.0.0
0.0.0.0 Serial0 ! !--- Access list 20 is used to control
which network management stations !--- can access
through SNMP. ! access-list 20 permit 172.16.150.8 ! !--
- The access list allows all legitimate traffic from the
inside network !--- but prevents spoofing. ! access-list
101 permit tcp 172.16.150.0 0.0.0.255 any access-list
101 permit udp 172.16.150.0 0.0.0.255 any access-list
101 permit icmp 172.16.150.0 0.0.0.255 any !--- This
deny is the default. access-list 101 deny ip any any !
!--- Access list 111 controls what can come from the
outside world !--- and it is anti-spoofing. ! access-
list 111 deny ip 127.0.0.0 0.255.255.255 any access-list
111 deny ip 172.16.150.0 0.0.0.255 any ! !--- Perform an
ICMP stuff first. There is some danger in these lists.
!--- They are control packets, and allowing *any* packet
opens !--- you up to some possible attacks. For example,
teardrop-style !--- fragmentation attacks can come
through this list. ! access-list 111 permit icmp any
172.16.150.0 0.0.0.255 administratively-prohibited
access-list 111 permit icmp any 172.16.150.0 0.0.0.255
echo access-list 111 permit icmp any 172.16.150.0
0.0.0.255 echo-reply access-list 111 permit icmp any
172.16.150.0 0.0.0.255 packet-too-big access-list 111
permit icmp any 172.16.150.0 0.0.0.255 time-exceeded
access-list 111 permit icmp any 172.16.150.0 0.0.0.255
traceroute access-list 111 permit icmp any 172.16.150.0
0.0.0.255 unreachable ! !--- Allow Telnet access from
10.11.11.0 corporate network administration people. !
access-list 111 permit tcp 10.11.11.0 0.0.0.255 host
172.16.150.1 eq telnet ! !--- This deny is the default.
! access-list 111 deny ip any any ! !--- Apply access
list 20 for SNMP process. ! snmp-server community secret
RO 20 ! 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.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

IOS Firewall 라우터를 구성한 후 연결이 작동하지 않을 경우 인터페이스에서 **ip inspect(name defined) 또는 out** 명령**으로** 검사를 활성화했는지 확인합니다. 이 컨피그레이션에서는 **ip inspect myfw in**이 인터페이스 Ethernet0/0에 적용됩니다.

이러한 명령과 다른 문제 해결 정보는 인증 프록시 문제 해결을 참조하십시오.

참고: 디버그 명령을 실행하기 전에 디버그 명령에 대한 중요 정보**를** 참조하십시오.

관련 정보

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