

2개의 ISP 연결을 위한 IOS NAT 로드 밸런싱 및 영역 기반 정책 방화벽

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[구성](#)

[네트워크 다이어그램](#)

[방화벽 정책 논의](#)

[구성](#)

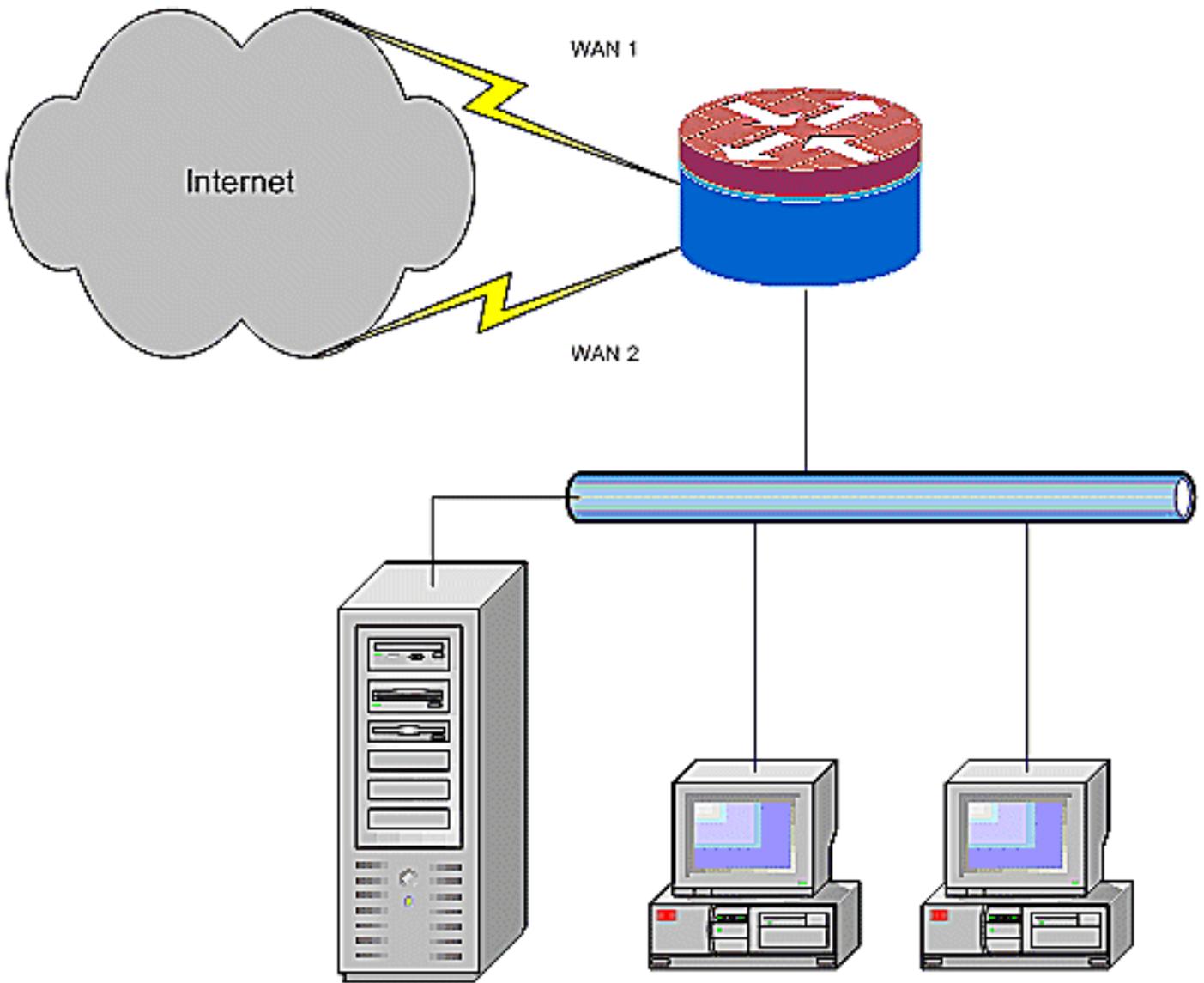
[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 두 개의 ISP 연결을 통해 NAT(Network Address Translation)를 사용하여 네트워크에 연결하는 Cisco IOS[®] 라우터의 샘플 컨피그레이션을 제공합니다. Cisco IOS 소프트웨어 NAT는 지정된 대상에 대한 동일 비용 경로를 사용할 수 있는 경우 여러 네트워크 연결을 통해 후속 TCP 연결 및 UDP 세션을 배포할 수 있습니다.



이 문서에서는 NAT에서 제공하는 기본 네트워크 보호를 강화하기 위한 상태 기반 검사 기능을 추가하기 위해 Cisco IOS ZFW(Zone-Based Policy Firewall)를 적용하기 위한 추가 컨피그레이션에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에서는 사용자가 LAN 및 WAN 연결을 사용하고 초기 연결을 설정하기 위한 컨피그레이션 또는 문제 해결 배경을 제공하지 않는다고 가정합니다. 이 문서에서는 경로를 구별하는 방법을 설명하지 않으므로 덜 바람직한 연결보다 더 바람직한 연결을 선호할 수 없습니다.

사용되는 구성 요소

이 문서의 정보는 12.4(15)T3 Advanced IP Services 소프트웨어가 포함된 Cisco Series 1811 Router를 기반으로 합니다. 다른 소프트웨어 버전을 사용하는 경우 일부 기능을 사용할 수 없거나 구성 명령이 이 문서에 표시된 것과 다를 수 있습니다. 인터페이스 컨피그레이션은 다른 플랫폼에

따라 다를 수 있지만 모든 Cisco IOS 라우터 플랫폼에서도 유사한 컨피그레이션을 사용할 수 있습니다.

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 규칙](#)을 참조하십시오.

[구성](#)

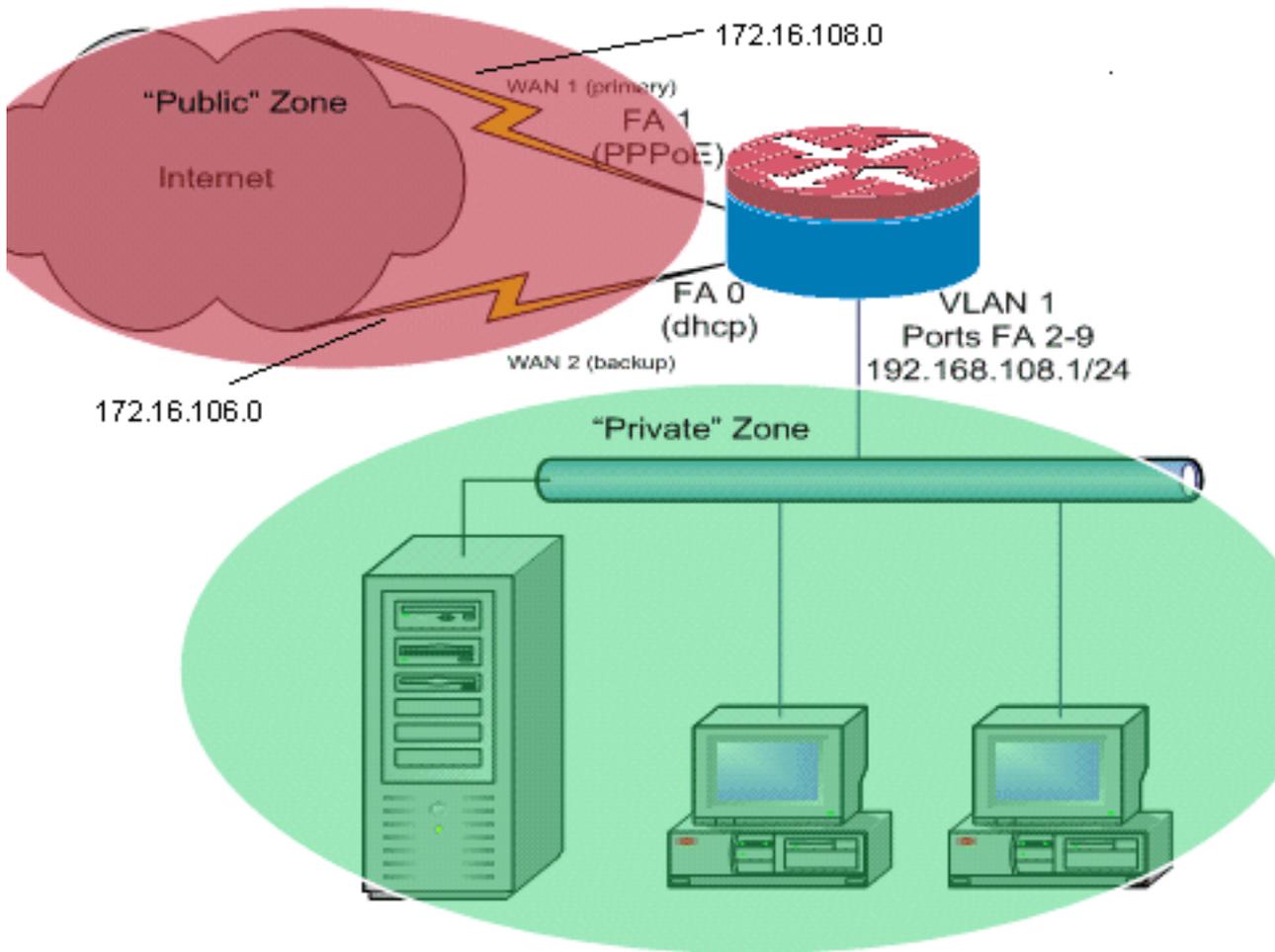
이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

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

특정 트래픽이 항상 하나의 ISP 연결을 사용하도록 하려면 정책 기반 라우팅을 추가해야 합니다. 이러한 동작을 필요로 하는 트래픽의 예로는 IPSec VPN 클라이언트, VoIP 텔레포니 트래픽 및 ISP 연결 옵션 중 하나만 사용하여 동일한 IP 주소, 더 빠른 속도 또는 연결 지연 시간을 선호하는 기타 트래픽이 있습니다.

[네트워크 다이어그램](#)

이 문서에서는 다음 네트워크 설정을 사용합니다.



이 컨피그레이션 예에서는 하나의 ISP에 DHCP 구성 IP 연결을 사용하는 액세스 라우터 (FastEthernet 0에 표시됨)와 다른 ISP 연결을 통한 PPPoE 연결을 설명합니다. 연결 유형은 컨피그레이션에 특별한 영향을 주지 않지만 일부 연결 유형은 특정 장애 시나리오에서 이 컨피그레이션의 사용성을 방해할 수 있습니다. 특히 이더넷 연결 WAN 서비스를 통한 IP 연결이 사용되는 경우, 예를 들어 추가 디바이스가 WAN 연결을 종료하고 Cisco IOS 라우터에 이더넷 핸드오프를 제공하는 케이블 모뎀 또는 DSL 서비스 등이 여기에 해당됩니다. DHCP 할당 주소 또는 PPPoE가 아닌 고정 IP 주소 지정이 적용되고 WAN 오류가 발생하는 경우, 이더넷 포트가 WAN 연결 디바이스에 대한 이더넷 링크를 계속 유지하면 라우터는 정상 및 잘못된 WAN 연결 모두에서 연결 로드 밸런싱을 계속 시도합니다. 구축에서 비활성 경로를 로드 밸런싱에서 제거해야 하는 경우, 경로 유효성을 모니터링하기 위해 최적화된 에지 라우팅을 추가하는 [것을 설명하는 2개의 인터넷 연결에 대해 최적화된 에지 라우팅을 사용하는 Cisco IOS NAT 로드 밸런싱 및 영역 기반 정책 방화벽](#)에 제공된 컨피그레이션을 참조하십시오.

[방화벽 정책 논의](#)

이 컨피그레이션 예에서는 "내부" 보안 영역에서 "외부" 보안 영역으로 단순 TCP, UDP 및 ICMP 연결을 허용하고, 활성 및 수동 FTP 전송을 위해 아웃바운드 FTP 연결 및 그에 상응하는 데이터 트래픽을 수용하는 방화벽 정책을 설명합니다. VoIP 신호 처리 및 미디어 등의 복잡한 애플리케이션 트래픽은 이 기본 정책에 의해 처리되지 않으며 성능이 저하되거나 완전히 실패할 수 있습니다. 이 방화벽 정책은 "공용" 보안 영역에서 "전용" 영역으로 연결되는 모든 연결을 차단하며, 여기에는 NAT 포트 전달에 의해 수용되는 모든 연결이 포함됩니다. 필요한 경우 애플리케이션 프로필 및 보안 정책을 반영하도록 방화벽 검사 정책을 조정해야 합니다.

Zone-Based Policy Firewall 정책 설계 및 컨피그레이션에 대한 질문이 있는 경우 [Zone-Based Policy Firewall Design and Application Guide](#)를 참조하십시오.

구성

이 문서에서는 다음 구성을 사용합니다.

구성

```
class-map type inspect match-any priv-pub-traffic
  match protocol ftp
  match protocol tcp
  match protocol udp
  match protocol icmp
! policy-map type inspect priv-pub-policy class type
inspect priv-pub-traffic inspect class class-default !
zone security public zone security private zone-pair
security priv-pub source private destination public
service-policy type inspect priv-pub-policy ! interface
FastEthernet0 ip address dhcp ip nat outside ip virtual-
reassembly zone security public ! interface
FastEthernet1 no ip address pppoe enable no cdp enable !
interface FastEthernet2 no cdp enable !--- Output
Suppressed interface Vlan1 description LAN Interface ip
address 192.168.108.1 255.255.255.0 ip nat inside ip
virtual-reassembly ip tcp adjust-mss 1452 zone security
private !---Define LAN-facing interfaces with "ip nat
inside" Interface Dialer 0 description PPPoX dialer ip
address negotiated ip nat outside ip virtual-reassembly
ip tcp adjust-mss zone security public !---Define ISP-
facing interfaces with "ip nat outside" ! ip route
0.0.0.0 0.0.0.0 dialer 0 ! ip nat inside source route-
map fixed-nat interface Dialer0 overload ip nat inside
source route-map dhcp-nat interface FastEthernet0
overload !---Configure NAT overload (PAT) to use route-
maps ! access-list 110 permit ip 192.168.108.0 0.0.0.255
any !---Define ACLs for traffic that will be NATed to
the ISP connections route-map fixed-nat permit 10 match
ip address 110 match interface Dialer0 route-map dhcp-
nat permit 10 match ip address 110 match interface
FastEthernet0 !---Route-maps associate NAT ACLs with NAT
outside on the !--- ISP-facing interfaces
```

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 ip nat translation** - 호스트 내부 NAT 및 NAT 외부 호스트 간 NAT 활동을 표시합니다. 이 명령은 내부 호스트가 두 NAT 외부 주소로 변환되는지 확인합니다.

```
Router# show ip nat translation
Pro Inside global      Inside local          Outside local         Outside global
tcp 172.16.108.44:54486 192.168.108.3:54486 172.16.104.10:22     172.16.104.10:22
tcp 172.16.106.42:49620 192.168.108.3:49620 172.16.102.11:80     172.16.102.11:80
tcp 172.16.108.44:1623 192.168.108.4:1623 172.16.102.11:445    172.16.102.11:445
Router#
```

- **show ip route** - 인터넷에 대한 여러 경로를 사용할 수 있는지 확인합니다.

Router# **show ip route**

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is 172.16.108.1 to network 0.0.0.0

```
C    192.168.108.0/24 is directly connected, Vlan1
    172.16.0.0/24 is subnetted, 2 subnets
C      172.16.108.0 is directly connected, FastEthernet4
C      172.16.106.0 is directly connected, Vlan106
S*    0.0.0.0/0 [1/0] via 172.16.108.1
      [1/0] via 172.16.106.1
```

- **show policy-map type inspect zone-pair sessions** - "private"-zone 호스트와 "public"-zone 호스트 간의 방화벽 검사 활동을 표시합니다. 이 명령은 호스트가 "외부" 보안 영역에서 서비스와 통신할 때 내부 호스트의 트래픽이 검사되는지 확인합니다.

문제 해결

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

NAT를 사용하여 Cisco IOS 라우터를 구성한 후 연결이 작동하지 않을 경우 다음 사항을 확인하십시오.

- NAT는 외부 및 내부 인터페이스에 적절하게 적용됩니다.
- NAT 컨피그레이션이 완료되었으며 ACL은 NATed여야 하는 트래픽을 반영합니다.
- 인터넷/WAN에 대한 여러 경로를 사용할 수 있습니다.
- 방화벽 정책은 라우터를 통해 허용할 트래픽의 특성을 정확하게 반영합니다.

관련 정보

- [음성 기술 지원](#)
- [음성 및 통합 커뮤니케이션 제품 지원](#)
- [Cisco IP 텔레포니 문제 해결](#)
- [Zone-Based Policy Firewall 설계 및 애플리케이션 가이드](#)
- [기술 지원 및 문서 - Cisco Systems](#)