자주 사용되는 IP ACL 설정

목차

소개

이 문서에서는 IP 패킷을 필터링하는, 일반적으로 사용되는 IP ACL(Access Control List)의 샘플 컨피그레이션에 대해 설명합니다.

사전 요구 사항

요구 사항

이 설정을 시도하기 전에 이러한 요건을 충족해야 합니다.

- IP 주소 지정에 대한 기본 이해

자세한 내용은 새 사용자의 IP 주소 지정 및 서브네팅을 참조하십시오.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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

배경 정보

IP Access Control은 다음을 기반으로 필터 패킷을 나열합니다.

- Source address
- 대상 주소
- 패킷 유형
- 이러한 항목의 모든 조합

네트워크 트래픽을 필터링하기 위해 ACL은 라우팅된 패킷을 라우터 인터페이스에서 전달할지 아니면 차단할지를 제어합니다. 라우터는 ACL 내에서 지정하는 기준에 따라 패킷을 전달할지 또는 삭제할지 결정하기 위해 각 패킷을 검사합니다. ACL 기준은 다음과 같습니다.

- 트래픽의 소스 주소
- 트래픽의 대상 주소
- 상위 계층 프로토콜

이 문서의 예에 나와 있는 것처럼 ACL을 구성하려면 다음 단계를 완료합니다.

1. ACL을 생성합니다.
2. ACL을 인터페이스에 적용합니다.

IP ACL은 IP 패킷에 적용되는 허용 및 거부 조건을 순차적으로 모아 놓은 것입니다. 라우터는 ACL의 조건에 대해 패킷을 한 번에 하나씩 테스트합니다.

첫 번째 일치는 Cisco IOS® 소프트웨어가 패킷을 수락할지 또는 거부할지를 결정합니다. Cisco IOS Software는 첫 번째 일치 이후 조건 테스트를 중지하므로 조건의 순서가 중요합니다. 조건이 일치하지 않을 경우, 라우터는 묵시적 모두 거부 절로 인해 패킷을 거부합니다.

다음은 Cisco IOS 소프트웨어에서 구성할 수 있는 IP ACL의 예입니다.

- 표준 ACL
- 확장된 ACL
- 동적(잠금 및 키) ACL
- IP 이름이 지정된 ACL
- 재귀 ACL
- 시간 범위를 사용하는 시간 기준 ACL
- 코멘트 있는 IP ACL 항목
- 상황 기반 ACL
- 인증 프록시
- 터보 ACL
- 분산 시간 기준 ACL

이 문서에서는 일반적으로 사용되는 표준 및 확장 ACL에 대해 설명합니다. Cisco IOS 소프트웨어에서 지원되는 다양한 유형의 ACL 및 ACL 구성과 편집 방법에 대한 자세한 내용은 IP 액세스 목록 구성을 참조하십시오.

표준 ACL의 명령 구문 형식은 **access-list access-list-number{permit|deny} {host|source source-wildcard|any}**입니다.

표준 ACL은 트래픽을 제어하기 위해 IP 패킷의 소스 주소를 ACL에 구성된 주소와 비교합니다.

확장 ACL은 트래픽을 제어하기 위해 IP 패킷의 소스 및 대상 주소를 ACL에 구성된 주소와 비교합니다. 또한 다음과 같은 기준으로 트래픽을 필터링하도록 확장 ACL을 더 세부적으로 구성할 수 있습니다.

- 프로토콜
- 포트 번호
- DSCP(Differentiated Services Code Point) 값
- 우선 순위 값
- 동기화 시퀀스 번호(SYN) 비트의 상태

확장 ACL의 명령 구문 형식은 다음과 같습니다.

IP

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} protocol source source-wildcard destination destination-wildcard
 [precedence precedence] [tos tos] [log | log-input]
[time-range time-range-name][fragments]
```

Internet Control Message Protocol (ICMP)

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} icmp source source-wildcard destination destination-wildcard
[[icmp-type] [icmp-code] | [icmp-message]] [precedence precedence] [tos tos] [log | log-input]
[time-range time-range-name][fragments]
```

TCP(Transmission Control Protocol)

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} tcp source source-wildcard [operator [port]] destination destination-wildcard
[operator [port]]
[established] [precedence precedence] [tos tos] [log | log-input]
[time-range time-range-name][fragments]
```

UDP(User Datagram Protocol))

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} udp source source-wildcard [operator [port]] destination destination-wildcard
[operator [port]]
[precedence precedence] [tos tos] [log | log-input] [time-range time-range-name][fragments]
```

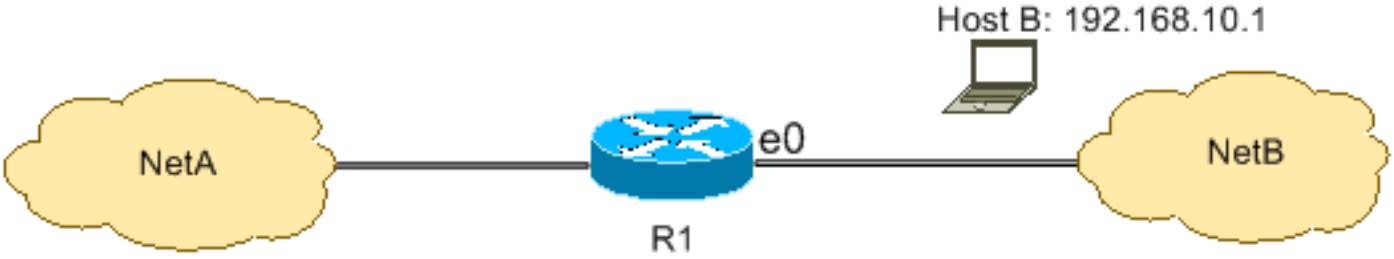
구성

이 설정 예에서는 가장 일반적인 IP ACL을 사용합니다.

선택 호스트가 네트워크에 액세스하도록 허용

이 그림에서는 네트워크에 액세스할 수 있는 권한이 부여된 선택 호스트를 보여줍니다. 호스트 B에서 NetA로 향하는 모든 소싱된 트래픽이 허용되며, NetB에서 NetA로 향하는 다른 모든 소싱된 트래

픽은 거부됩니다.



R1 테이블의 출력은 네트워크에서 호스트에 대한 액세스 권한을 부여하는 방법을 보여줍니다. 이 출력은 다음을 보여줍니다.

- 설정에서는 R1의 Ethernet 0 interface를 통해 IP 주소가 192.168.10.1인 호스트만 허용합니다.
- 이 호스트는 NetA의 IP 서비스에 액세스할 수 있습니다.
- NetB의 다른 호스트는 NetA에 액세스할 수 없습니다.
- ACL에 거부 명령문이 구성되지 않았습니다.

기본적으로 모든 ACL 끝에는 묵시적 모두 거부 절이 있습니다. 명시적으로 허용되지 않은 항목은 거부됩니다.

R1

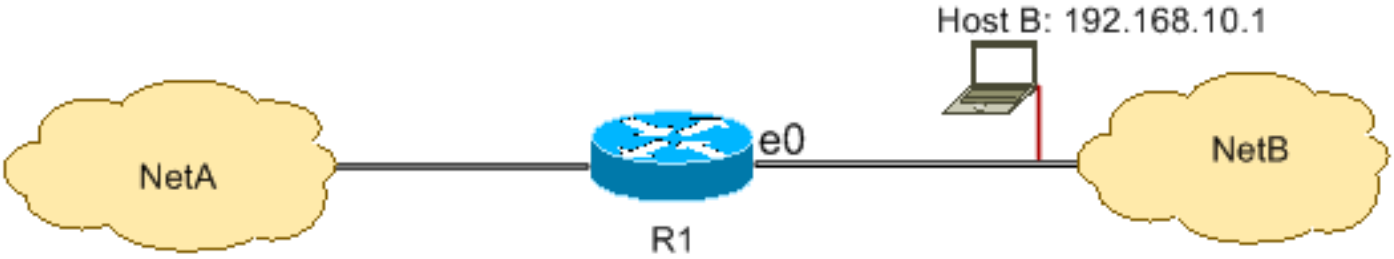
```
hostname R1
!
interface ethernet0
 ip access-group 1 in
!
access-list 1 permit host 192.168.10.1
```

> **참고**: ACL은 호스트 B에서 소싱된 패킷을 제외하고 NetB에서 NetA로의 IP 패킷을 필터링합니다. 호스트 B에서 NetA로 소싱된 패킷은 여전히 허용됩니다.

> **참고:** ACL **access-list 1 permit 192.168.10.1 0.0.0.0**은 동일한 규칙을 구성하는 또 다른 방법입니다.

네트워크에 액세스하기 위한 호스트 선택 거부

이 그림은 호스트 B에서 NetA로 향하는 소싱된 트래픽은 거부되는 반면, NetB에서 NetA에 액세스하는 다른 모든 트래픽은 허용됨을 보여줍니다.



이 설정은 호스트 192.168.10.1/32에서 R1의 Ethernet 0까지의 모든 패킷을 거부하고 다른 모든 패킷은 허용합니다. 모든 ACL에는 묵시적 모두 거부 절이 있으므로 **access list 1 permit any** 명령을 사용하여 다른 모든 항목을 명시적으로 허용해야 합니다.

R1

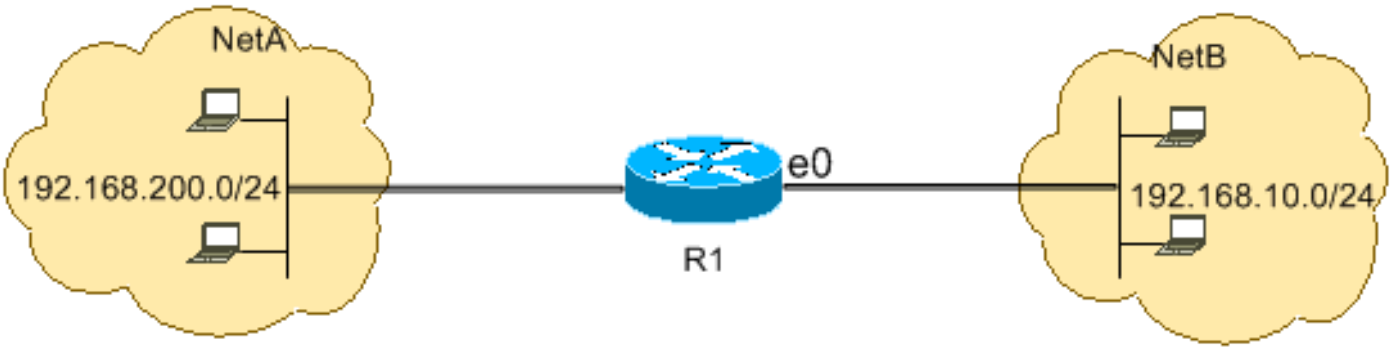
```
hostname R1
!
interface ethernet0
 ip access-group 1 in
!
access-list 1 deny host 192.168.10.1
access-list 1 permit any
```

> **참고:** 명령문의 순서는 ACL 작업에 중요합니다. 이 명령이 표시하는 것처럼 항목의 순서가 반대인 경우 첫 번째 줄은 모든 패킷 소스 주소와 일치합니다. 따라서 ACL이 호스트 192.168.10.1/32에서 NetA에 액세스하는 것을 차단하지 못합니다.

```
access-list 1 permit any
access-list 1 deny host 192.168.10.1
```

연속 IP 주소 범위에 대한 액세스 허용

이 그림은 네트워크 주소가 192.168.10.0/24인 NetB의 모든 호스트가 NetA의 네트워크 192.168.200.0/24에 액세스할 수 있음을 보여줍니다.



이 설정에서는 네트워크 192.168.10.0/24의 소스 주소와 네트워크 192.168.200.0/24의 대상 주소가 있는 IP 헤더가 있는 IP 패킷이 NetA에 액세스할 수 있습니다. ACL의 끝에는 R1의 Ethernet 0 인바운드를 통한 다른 모든 트래픽 통과를 거부하는 묵시적 모두 거부 절이 있습니다.

R1

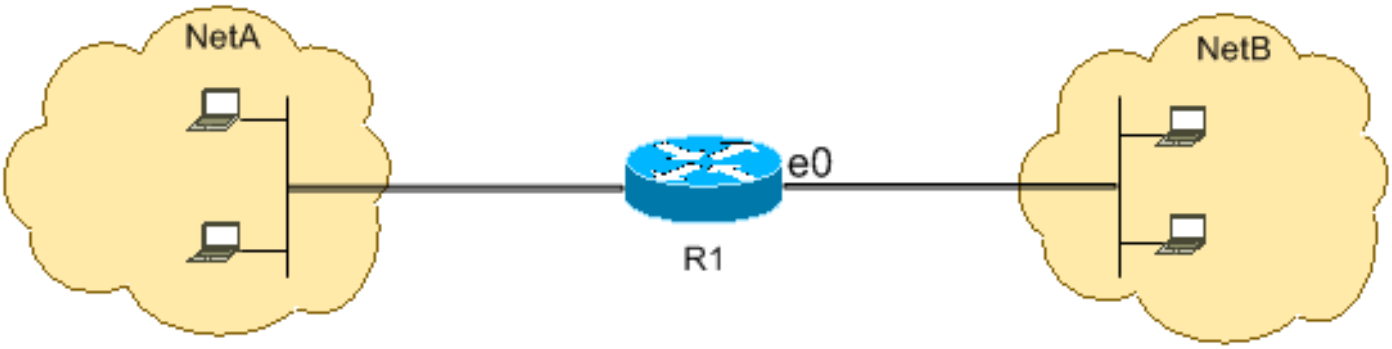
```
hostname R1
!
interface ethernet0
 ip access-group 101 in
!
access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.200.0 0.0.0.255
```

> **참고:** access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.200.0 0.0.0.255 **명령에서** "0.0.0.255"는 네트워크 192.168.10.0과 마스크 255.255.255.0의 역 마스크입니다. ACL은 네트워크 주소에서 일치해야 하는 비트 수를 확인하기 위해 역 마스크를 사용합니다. 테이블에서 ACL은 192.168.10.0/24 네트워크의 소스 주소 및 192.168.200.0/24 네트워크의 대상 주소가 있는 모든 호스트를 허용합니다.

네트워크 주소의 마스크 및 ACL에 필요한 역 마스크 계산 방법에 대한 자세한 내용은 IP 액세스 목록 구성의 마스크 섹션을 참조하십시오.

텔넷 트래픽 거부(TCP, 포트 23)

더 높은 보안 문제를 해결하기 위해 공용 네트워크에서 사설 네트워크에 대한 텔넷 액세스를 비활성화할 수 있습니다. 이 그림은 NetB(퍼블릭)에서 NetA(프라이빗)로 향하는 텔넷 트래픽이 거부되는 방식을 보여줍니다. 이를 통해 다른 모든 IP 트래픽이 허용되는 동안 NetA가 NetB와의 텔넷 세션을 시작하고 설정할 수 있습니다.



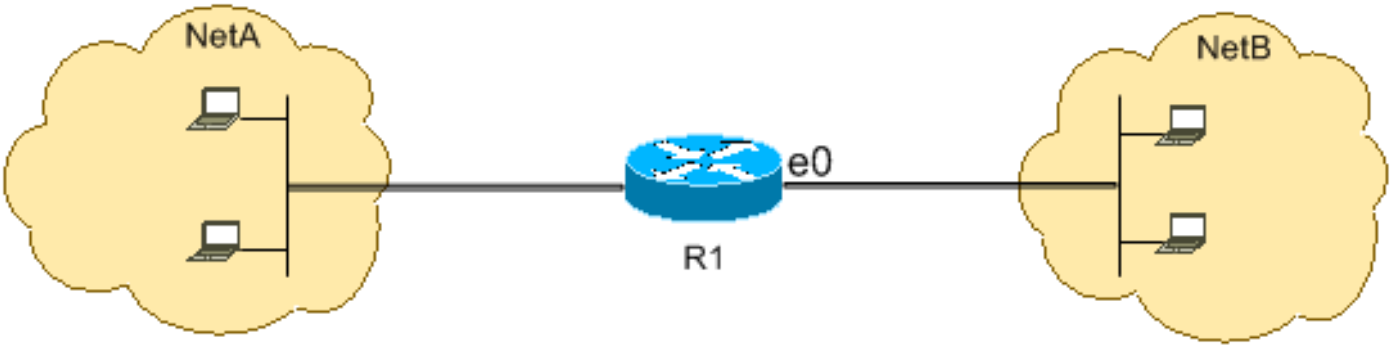
텔넷은 TCP, 포트 23을 사용합니다. 이 설정에서는 포트 23의 NetA로 향하는 모든 TCP 트래픽이 차단되고 다른 모든 IP 트래픽이 허용됨을 보여줍니다.

R1

```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 deny tcp any any eq 23
access-list 102 permit ip any any
```

내부 네트워크만 TCP 세션을 시작하도록 허용

이 그림은 NetA에서 NetB로 향하는 소싱된 TCP 트래픽은 허용되는 반면 NetB에서 NetA로 향하는 TCP 트래픽은 거부됨을 보여줍니다.



이 예에서 ACL의 목적은 다음과 같습니다.

- NetA의 호스트가 NetB의 호스트에 대한 TCP 세션을 시작하고 설정하도록 허용합니다.
- NetB의 호스트가 NetA의 호스트로 향하는 TCP 세션을 시작하고 설정하는 것을 거부합니다.

이 구성을 사용하면 데이터그램이 다음과 같을 때 데이터그램은 R1의 interface Ethernet 0 인바운드를 통과할 수 있습니다.

- Acknowledged(ACK) 또는 reset(RST) 비트 세트(설정된 TCP 세션을 나타냄)

- 1023보다 큰 대상 포트 값

R1

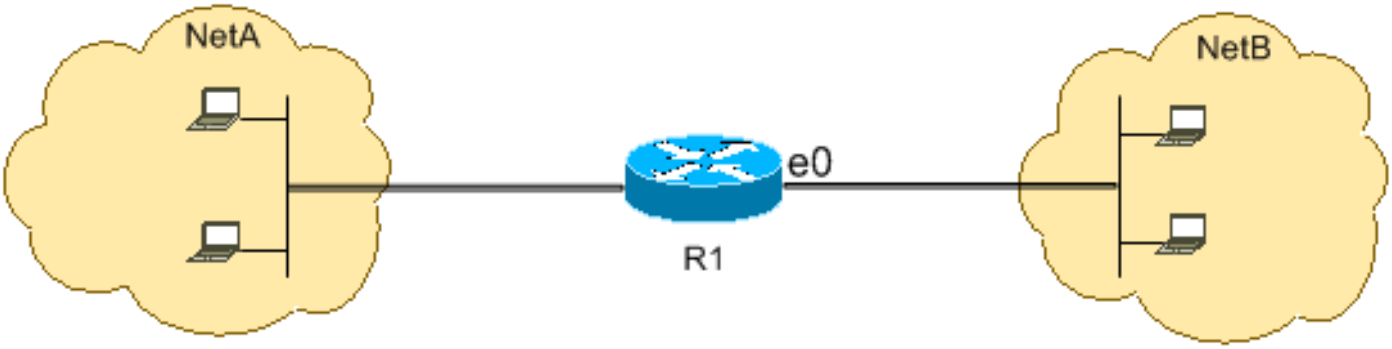
```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit tcp any any gt 1023 established
```

IP 서비스에 대해 잘 알려진 대부분의 포트는 1023 미만의 값을 사용하므로 대상 포트가 1023 미만이거나 ACK/RST 비트가 설정되지 않은 데이터그램은 ACL 102에서 거부됩니다. 따라서 NetB의 호스트가 TCP 연결을 시작하고 1023 미만의 포트 번호에 대해 첫 번째 TCP 패킷(SYN/RST(synchronize/start packet) 비트 세트가 없는 경우 거부되고 TCP 세션이 실패합니다. NetA에서 NetB로 시작되는 TCP 세션은 패킷 반환을 위해 ACK/RST 비트가 설정되어 있으며 1023보다 큰 포트 값을 사용하므로 허용됩니다.

전체 포트 목록은 RFC 1700을 참조하십시오.

FTP 트래픽 거부(TCP, 포트 21)

이 그림은 NetB에서 NetA로 향하는 FTP(TCP, 포트 21) 및 FTP 데이터(포트 20) 소싱된 트래픽은 거부되는 반면 다른 모든 IP 트래픽은 허용됨을 보여줍니다.



FTP는 포트 21 및 포트 20을 사용합니다. 포트 21 및 포트 20으로 향하는 TCP 트래픽은 거부되며 다른 모든 트래픽은 명시적으로 허용됩니다.

R1

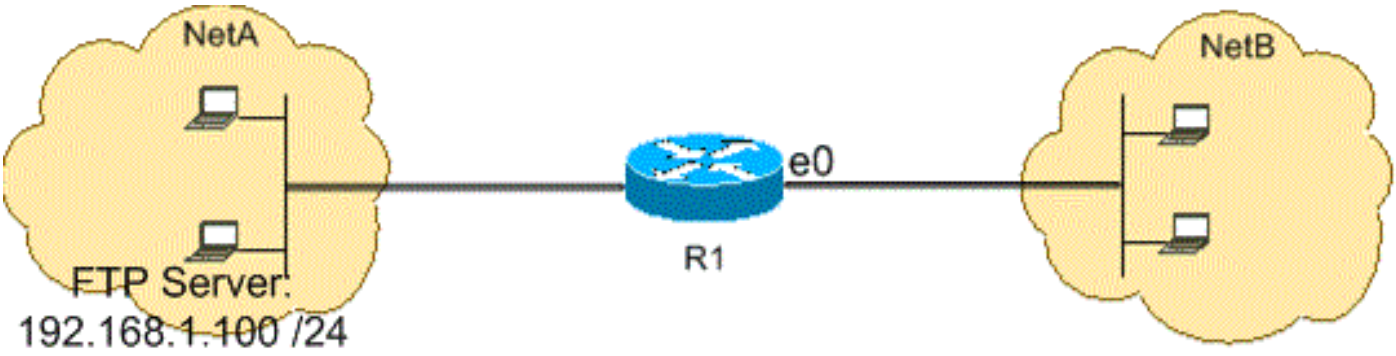
```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 deny tcp any any eq ftp
access-list 102 deny tcp any any eq ftp-data
access-list 102 permit ip any any
```

FTP 트래픽 허용(활성 FTP)

FTP는 활성 및 수동이라는 두 가지 모드로 작동할 수 있습니다.

FTP가 활성 모드에서 작동하는 경우 FTP 서버는 제어를 위해 포트 21을 사용하고 데이터를 위해 포트 20을 사용합니다. FTP 서버(192.168.1.100)는 NetA에 있습니다. 이 그림은 NetB에서 FTP 서

버(192.168.1.100)로 향하는 FTP(TCP, 포트 21) 및 FTP 데이터(포트 20) 소싱된 트래픽은 허용되지만 다른 모든 IP 트래픽은 거부됨을 보여줍니다.



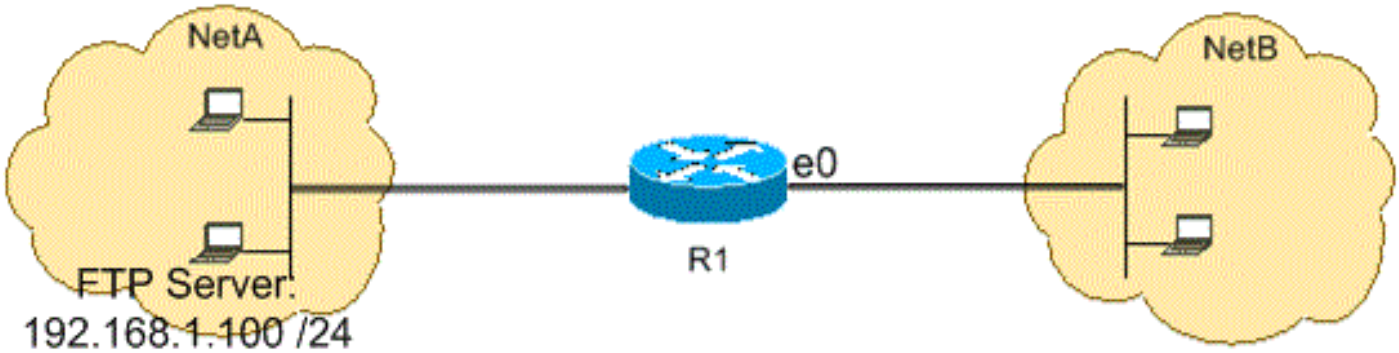
R1

```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit tcp any host 192.168.1.100 eq ftp
access-list 102 permit tcp any host 192.168.1.100 eq ftp-data established
!
interface ethernet1
 ip access-group 110 in
!
access-list 110 permit host 192.168.1.100 eq ftp any established
access-list 110 permit host 192.168.1.100 eq ftp-data any
```

FTP 트래픽 허용(수동 FTP)

FTP는 활성 및 수동이라는 두 가지 모드로 작동할 수 있습니다.

FTP가 수동 모드에서 작동하는 경우 FTP 서버는 제어를 위해 포트 21을 사용하고 데이터를 위해 1024 이상의 동적 포트를 사용합니다. FTP 서버(192.168.1.100)는 NetA에 있습니다. 이 그림은 NetB에서 FTP 서버(192.168.1.100)로 향하는 FTP(TCP, 포트 21) 및 FTP 데이터(1024보다 크거나 같은 포트) 소싱된 트래픽은 허용되지만 다른 모든 IP 트래픽은 거부됨을 보여줍니다.



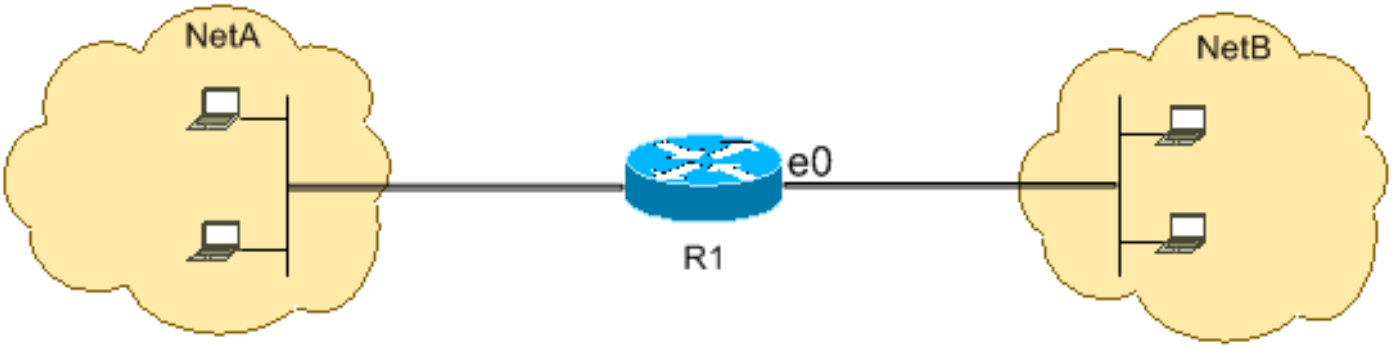
R1

```
hostname R1
!
interface ethernet0
 ip access-group 102 in
```

```
!
access-list 102 permit tcp any host 192.168.1.100 eq ftp
access-list 102 permit tcp any host 192.168.1.100 gt 1023
!
interface ethernet1
 ip access-group 110 in
!
access-list 110 permit host 192.168.1.100 eq ftp any established
access-list 110 permit host 192.168.1.100 gt 1023 any established
```

Ping 허용(ICMP)

이 그림은 NetA에서 NetB로 전달되는 ICMP가 허용되며 NetB에서 NetA로 향하는 소싱된 ping이 거부되었음을 보여줍니다.



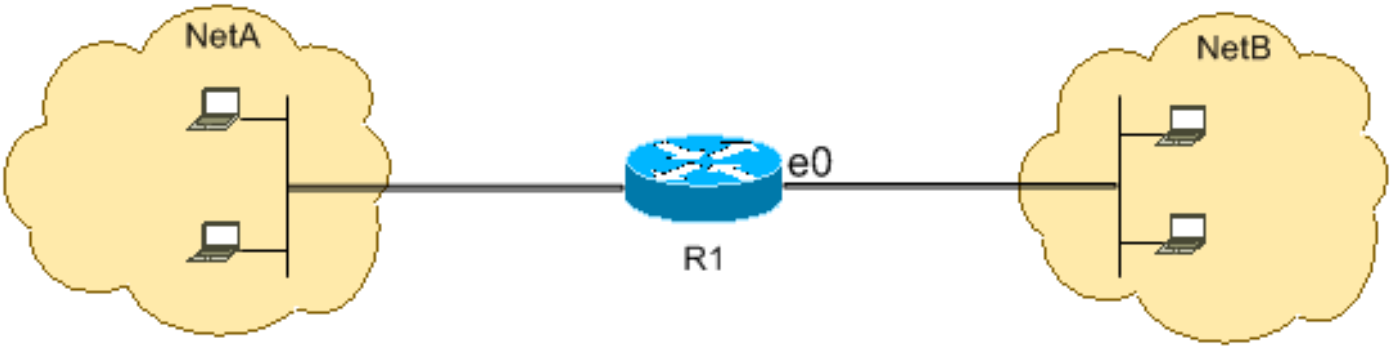
이 설정은 에코 응답(ping 응답) 패킷만 NetB에서 NetA로 향하는 interface Ethernet 0으로 들어오는 것을 허용합니다. 그러나 ping이 NetB에서 제공되고 NetA로 향하는 경우 설정은 모든 에코 요청 ICMP 패킷을 차단합니다. 따라서 NetA의 호스트는 NetB의 호스트를 ping할 수 있지만 NetB의 호스트는 NetA의 호스트를 ping할 수 없습니다.

R1

```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit icmp any any echo-reply
```

HTTP, 텔넷, 메일, POP3, FTP 허용

이 그림은 HTTP, 텔넷, SMTP(Simple Mail Transfer Protocol), POP3 및 FTP 트래픽만 허용되며, NetB에서 NetA로 향하는 나머지 소싱된 트래픽은 거부됨을 보여줍니다.



이 설정은 WWW(포트 80), 텔넷(포트 23), SMTP(포트 25), POP3(포트 110), FTP(포트 21) 또는 FTP 데이터(포트 20)와 일치하는 대상 포트 값의 TCP 트래픽을 허용합니다. ACL의 끝에 있는 묵시

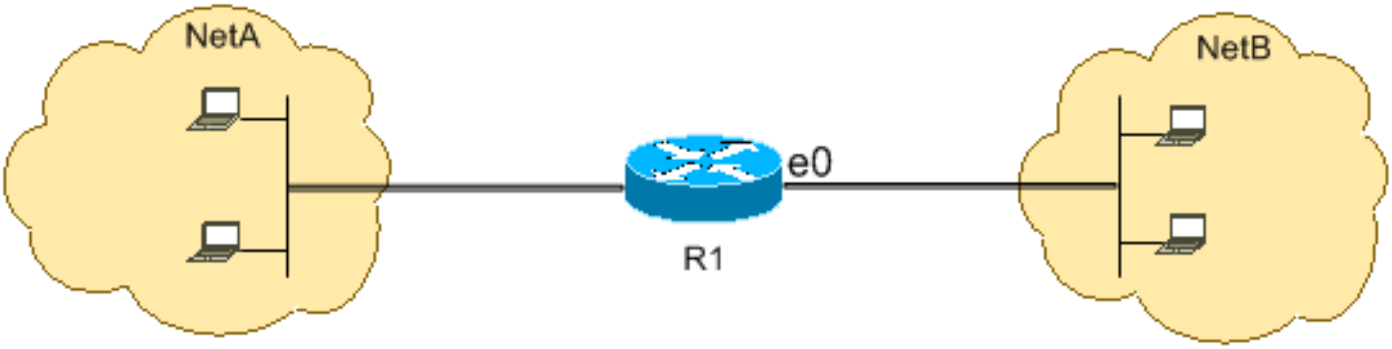
적 모두 거부 절은 permit 절과 일치하지 않는 다른 모든 트래픽을 거부합니다.

R1

```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit tcp any any eq www
access-list 102 permit tcp any any eq telnet
access-list 102 permit tcp any any eq smtp
access-list 102 permit tcp any any eq pop3
access-list 102 permit tcp any any eq 21
access-list 102 permit tcp any any eq 20
```

DNS 허용

이 그림은 DNS(Domain Name System) 트래픽만 허용되며, NetB에서 NetA로 전송되는 나머지 소싱된 트래픽은 거부됨을 보여줍니다.



이 설정은 대상 포트값이 53인 TCP 트래픽을 허용합니다. ACL의 끝에 있는 묵시적 모두 거부 절은 permit 절과 일치하지 않는 다른 모든 트래픽을 거부합니다.

R1

```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit udp any any eq domain
access-list 102 permit udp any eq domain any
access-list 102 permit tcp any any eq domain
access-list 102 permit tcp any eq domain any
```

라우팅 업데이트 허용

인터페이스에 인바운드 ACL을 적용할 때 라우팅 업데이트가 필터링되지 않도록 해야 합니다. 이 목록의 관련 ACL을 사용하여 라우팅 프로토콜 패킷을 허용합니다.

RIP(Routing Information Protocol)를 허용하려면 이 명령을 입력합니다.

```
access-list 102 permit udp any any eq rip
```

IGRP(Internal Gateway Routing Protocol)를 허용하려면 이 명령을 입력합니다.

```
access-list 102 permit igrp any any
```

EIGRP(Enhanced IGRP)를 허용하려면 이 명령을 입력합니다.

```
access-list 102 permit eigrp any any
```

OSPF(Open Shortest Path First)를 허용하려면 이 명령을 입력합니다.

```
access-list 102 permit ospf any any
```

BGP(Border Gateway Protocol)를 허용하려면 이 명령을 입력합니다.

```
access-list 102 permit tcp any any eq 179
access-list 102 permit tcp any eq 179 any
```

ACL을 기반으로 트래픽 디버그

디버그 명령을 사용하려면 메모리 및 처리 성능과 같은 시스템 리소스를 할당해야 하며, 극한 상황에서는 로드가 많은 시스템이 중단될 수 있습니다. 신중하게 **디버그** 명령을 사용합니다. debug 명령의 영향을 줄이기 위해 검사해야 하는 트래픽을 선택적으로 정의하려면 ACL을 **사용합니다**. 이러한 설정은 패킷을 필터링하지 않습니다.

이 설정은 호스트 10.1.1.1~172.16.1.1 사이의 패킷에 대해서만 **debug ip packet** 명령을 켭니다.

```
R1(config)#access-list 199 permit tcp host 10.1.1.1 host 172.16.1.1
R1(config)#access-list 199 permit tcp host 172.16.1.1 host 10.1.1.1
R1(config)#end
R1#debug ip packet 199 detail IP packet debugging is on (detailed) for access list 199
```

디버그 명령의 영향에 대한 추가 정보는 디버그 명령에 대한 중요 정보를 참조하십시오.

디버그 명령과 함께 ACL을 사용하는 방법에 대한 자세한 내용은 Ping 및 Traceroute 명령 이해의 **디버그 명령 사용** 섹션을 참조하십시오.

MAC 주소 필터링

특정 MAC 레이어 스테이션 소스 또는 대상 주소로 프레임을 필터링할 수 있습니다. 성능 저하 없이 시스템에 원하는 수의 주소를 구성할 수 있습니다. MAC 레이어 주소로 필터링하려면 전역 설정 모드에서 이 명령을 사용합니다.

```
Router#config terminal
Router(config)#bridge irb
Router(config)#bridge 1 protocol ieee
Router(config)#bridge 1 route ip
```

bridge-group <group number> {**input-address-list <ACL number> 명령**으로 만든 액세스 목록과 함께 트래픽을 필터링해야 하는 인터페이스에 **브리지 프로토콜을 적용합니다 | output-address-list <ACL number>}**:

```
Router#config terminal
Router(config-if)#interface fastEthernet0/0
```

```
Router(config-if)#no ip address
Router(config-if)#bridge-group 1 input-address-list 700
Router(config-if)#exit
```

브리지 가상 인터페이스를 생성하고 물리적 이더넷 인터페이스에 할당된 IP 주소를 적용합니다.

```
Router#config terminal
Router(config-if)#int bvi1
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#exit
Router(config)#access-list 700 deny aaaa.bbbb.cccc 0000.0000.0000
Router(config)#access-list 700 permit 0000.0000.0000 ffff.ffff.ffff
```

이 구성에서는 라우터가 액세스 목록 700에 구성된 MAC 주소만 허용합니다. 액세스 목록 명령 access-list <ACL number> deny <mac address> 0000.0000.0000에서는 액세스를 가질 수 없는 MAC 주소를 거부한 다음 나머지를 허용합니다(예: aaaa.bbb.ccc).

> **참고:** 각 MAC 주소에 대한 모든 액세스 목록 행을 생성합니다.

다음을 확인합니다.

현재 이 설정에 사용 가능한 확인 절차는 없습니다.

문제 해결

현재 이 구성의 문제를 해결하는 데 사용할 수 있는 특정 정보가 없습니다.

관련 정보

- IP 액세스 목록 구성
- 액세스 목록 지원 페이지
- IP 라우팅 지원 페이지
- IP 라우팅 프로토콜 지원 페이지
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.