ACL - 실습가이드

김민경

목차

Ⅰ. 개념정리

1. ACL (Access Control List, 접근 제어 리스트)

1) 정의

- 방화벽

- 특정 사용자의 접근 or 특정 서비스의 이용 제한 시, 데이터 분류 작업을 할 때 필요함

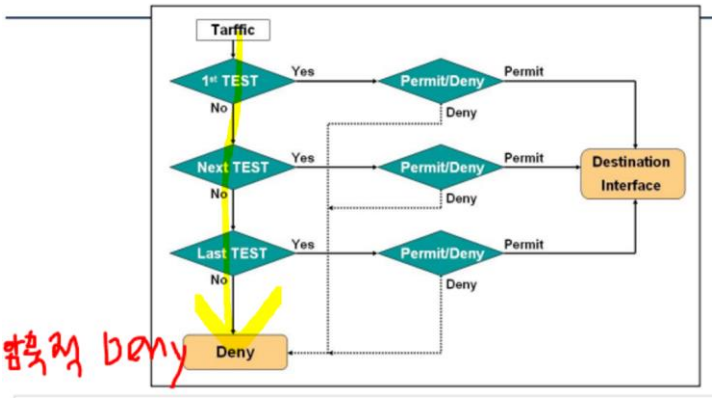
2) 종류

① Standard	- 출발지 주소만 확인하여 필터링하는 방식 - 사용이 매우 제약적인 곳에서만 사용함
② Extended	- 출발지, 목적지주소, 프로토콜, 포트번호까지 확인하여 필터링 하는 방식 - 선택적 제한을 함

3) 생성 방법

① Numberic (넘버형)	- 숫자를 사용해 ACL 생성하는 방식 - ex) access-list 10 permit host 10.10.10.10
② Named	- 각 정책에 문자를 사용해 이름을 지정해주는 방식 - ex) ip access-list standard test (test 라는 정책)

4) 순차적 매칭

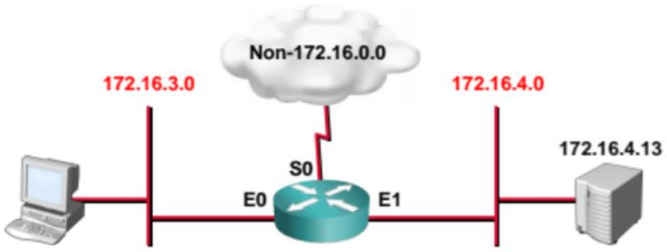


-정책을 순차적으로 위에서부터 매칭함

-암묵적 Deny

: 순차적으로 존재하는 모든 정책을 살펴봐도 매칭되는 것이 없을 때 deny 함

5) 명령어 예시

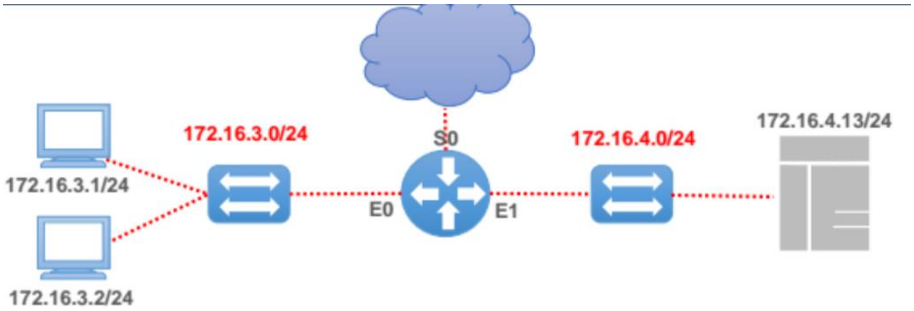


Router(config)# access-list 1 deny 172.16.4.0 0.0.0.255 //172.16.4.0 의 접근 거부

Router(config)# access-list 1 permit any //나머지는 다 허용

Router(config)# int ethernet 0

Router(config-if)# ip access-group 1 out //정책 1 의 outbound 설정



Router(config)# access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.4.0 0.0.0.255 eq 21 // 포트 21 번으로 172.16.3.0 → 172.16.4.0 으로의 거부

Router(config)# access-list 101 permit ip any any

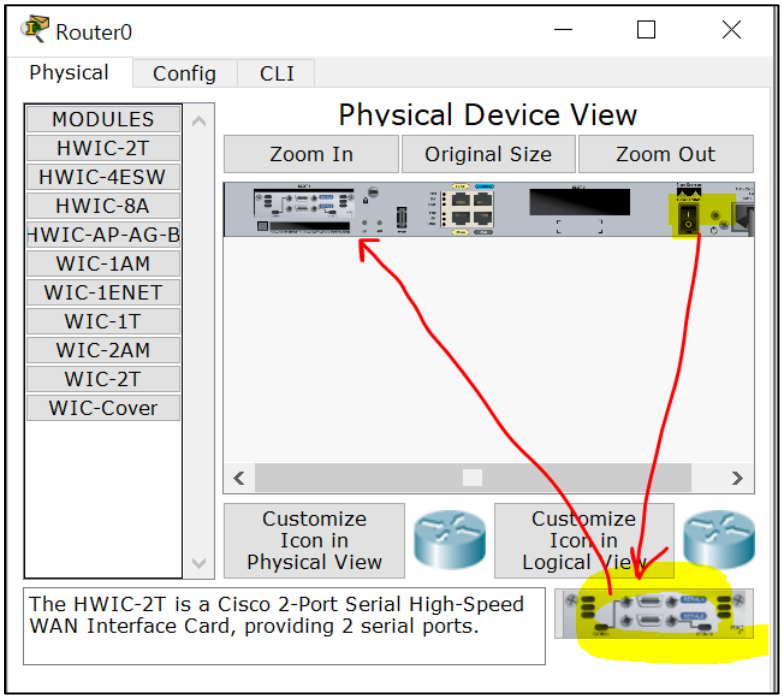
Router(config)# int ethernet 1

Router(config)# ip access-group 101 out

Ⅱ. 문제 1

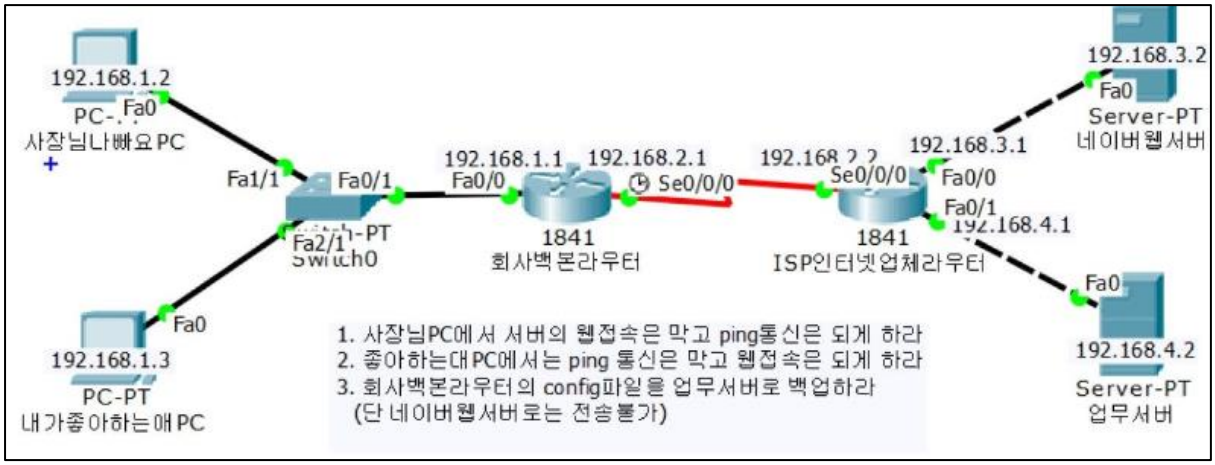
1. 환경 구성하기

1) 라우터 serial 설정하기



2) 아래 환경 구성하기

• IP, gw, 부여



참고)

pc1 gw : 192.168.1.1

• Static Route 구성

-회사백본라우터

ip route 192.168.3.0 255.255.255.0 192.168.2.2

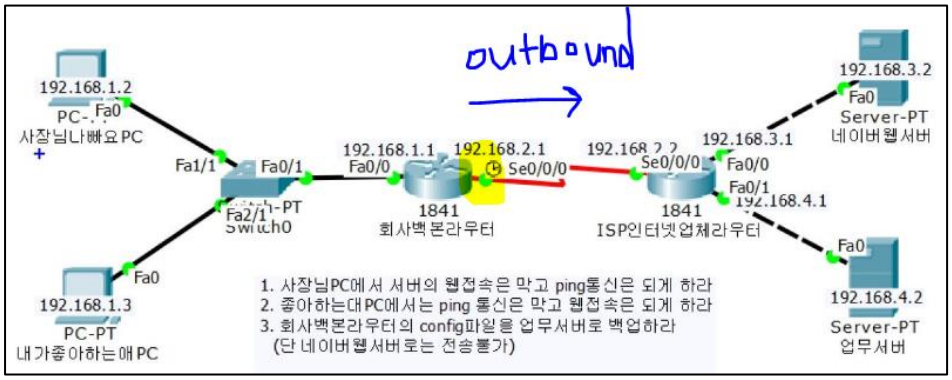
ip route 192.168.4.0 255.255.255.0 192.168.2.2

-ISP 인터넷업체라우터

ip route 192.168.1.0 255.255.255.0 192.168.2.1

2. 정책 생성하기

1) 거부 정책 생성하기



•원래 outbound deny 정책을 ISP 인터넷업체라우터의 F0/0 & F0/1 에 해줬음

⇒ 하지만 ISP 인터넷업체라우터는 우리가 원하는 대로 바꾸는 등의 관리를 할 수 X

⇒ 따라서 회사백본라우터의 s0/0/0 에 정책을 적용해 줄 것임

•사장님 pc → 네이버 웹서버 접속 차단 정책 생성 및 적용하기

-회사백본라우터에서 설정하기

```
Router(config)#access-list 101 deny tcp 192.168.1.2 0.0.0.0 192.168.3.2 0.0.0.0 eq 80
Router(config)#access0list 101 permit ip any any
                 ^
% Invalid input detected at '^' marker.

Router(config)#access-list 101 permit ip any any
Router(config)#
Router(config)#int s0/0/0
Router(config-if)#ip access
Router(config-if)#ip access-group 101 out
Router(config-if)#
Router(config-if)#
```

•사장님 pc → 업무서버 접속 차단 정책 생성 및 적용하기

-회사백본라우터에서 설정하기

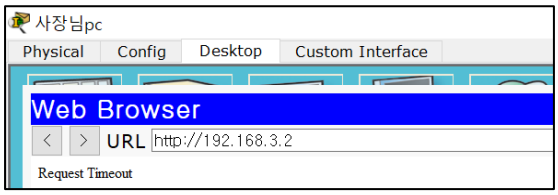
```
Router(config)#access-list 104 deny tcp 192.168.1.2 0.0.0.0 192.168.4.2 0.0.0.0 eq 80
Router(config)#access-list 104 permit ip any any
Router(config)#
Router(config)#int s0/0/0
Router(config-if)#ip access-group 104 out
Router(config-if)#
```

2) 결과 확인하기

•사장님 pc → 네이버웹서버 ping 통신 ⇒ O

```
PC>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time=8ms TTL=126
Reply from 192.168.3.2: bytes=32 time=9ms TTL=126
Reply from 192.168.3.2: bytes=32 time=1ms TTL=126
Reply from 192.168.3.2: bytes=32 time=6ms TTL=126

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%
loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 9ms, Average = 6ms
```

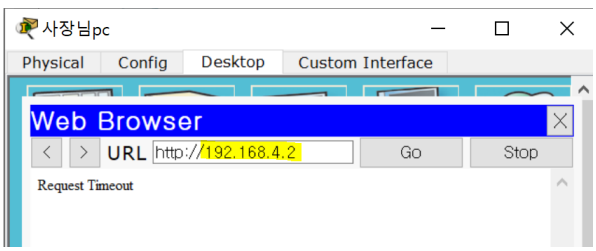
• 사장님 pc → 네이버웹서버 웹 접속 ⇒ X



•사장님 pc → 업무서버 ping 통신 ⇒ O

```
PC>ping 192.168.4.2

Pinging 192.168.4.2 with 32 bytes of data:

Reply from 192.168.4.2: bytes=32 time=2ms TTL=126
Reply from 192.168.4.2: bytes=32 time=4ms TTL=126
Reply from 192.168.4.2: bytes=32 time=4ms TTL=126
Reply from 192.168.4.2: bytes=32 time=8ms TTL=126

Ping statistics for 192.168.4.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%
loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 8ms, Average = 4ms
```

•사장님 pc → 업무서버 웹 접속 ⇒ X



Ⅲ. 문제 2

1. 정책 생성하기

1) 거부 정책 생성하기

• 좋아하는 pc → 네이버웹서버 접속 차단 정책 생성 및 적용하기

-회사백본라우터에서 설정하기

```
Router#configure ter
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 102 deny icmp 192.168.1.3 0.0.0.0 192.168.3.2 0.0.0.0
Router(config)#access-list 101 permit ip any any
Router(config)#interface s0/0/0
Router(config-if)#ip access-group 102 out
Router(config-if)#
```

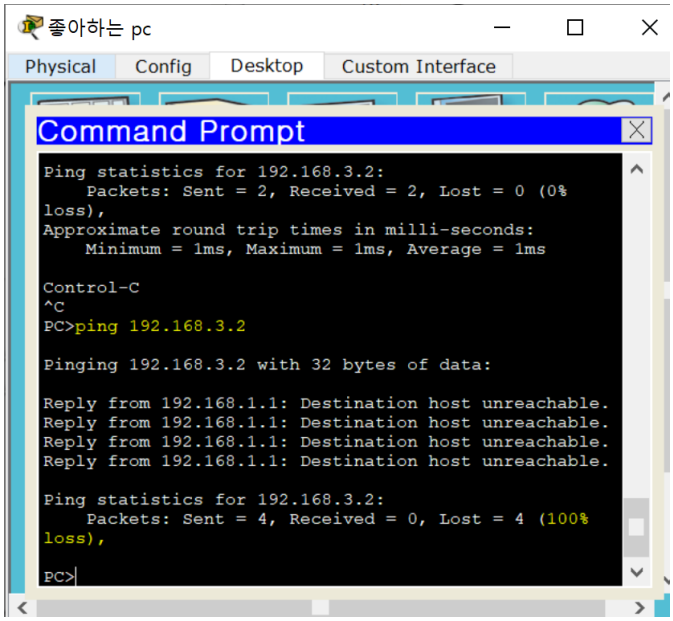
• 좋아하는 pc → 업무서버 접속 차단 정책 생성 및 적용하기

-회사백본라우터에서 설정하기

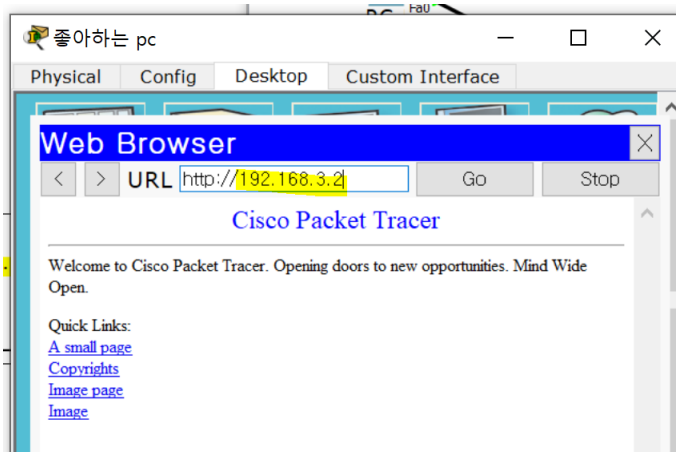
```
Router(config)#access-list 103 deny icmp 192.168.1.3 0.0.0.0 192.168.4.2 0.0.0.0
Router(config)#access-list 103 permit ip any any
Router(config)#
Router(config)#int s0/0/0/0
                        ^
% Invalid input detected at '^' marker.

Router(config)#int s0/0/0
Router(config-if)#ip access-group 193 out
Router(config-if)#ip access-group 103 out
Router(config-if)#
```

2) 결과 확인하기

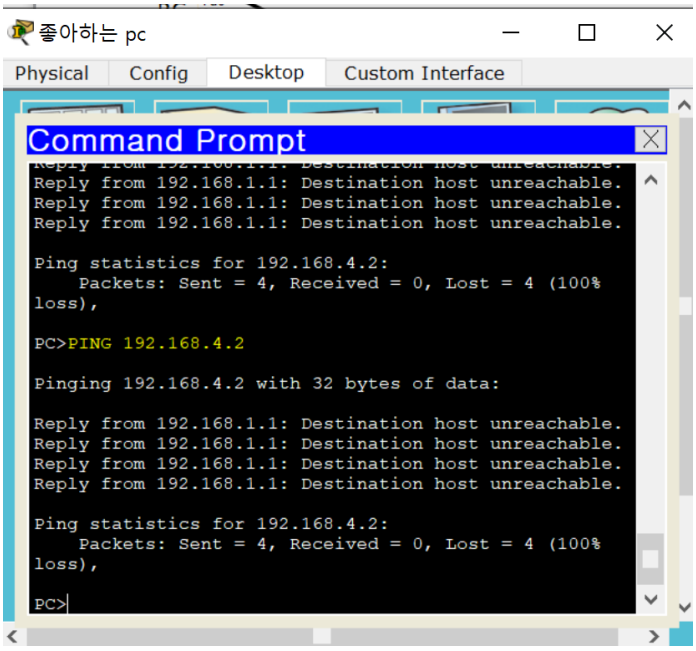
•좋아하는 pc → 네이버웹서버 ping 통신 ⇒ X



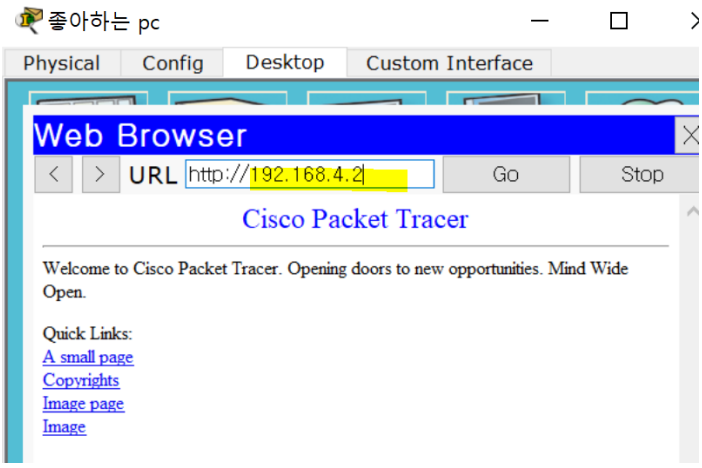
• 좋아하는 pc → 네이버웹서버 웹 접속 ⇒ O



•좋아하는 pc → 업무서버 ping 통신 ⇒ X



• 좋아하는 pc → 업무서버 웹 접속 ⇒ O



Ⅳ. 문제 3

1. 정책 생성하기

1) 거부 정책 생성하기

•회사백본라우터에서 outbound 정책을 설정하면 될 것 같지만, **자신이 만든 정책에 자신의 패킷은 필터링되지 않고 통과함**

⇒즉, 회사백본라우터에서 아래의 deny 정책을 만들어도, 192.168.2.1 에서 192.168.3.로 tftp 접근이 가능함

-**deny u 에 192.168.2.1 0.0.0.0 192.168.3.2 0.0.0.0 eq 69**

⇒따라서 회사백본라우터의 s0/0/0 에서 outbound 로 설정하는 것이 아닌, **ISP 인터넷 업체라우터의 s0/0/0 으로의 inbound 에 거부 정책을 설정**해야 함

•ISP 인터넷업체라우터의 s0/0/0 에 inbound 로 deny 정책 설정하기

```
Router(config)#access-list 106 deny udp host 192.168.2.1 host 192.168.3.2 eq 69
Router(config)#access-
Router(config)#access-list  106 per
Router(config)#access-list  106 permit ip any any
Router(config)#
Router(config)#int s0/0/0
Router(config-if)#ip acce
Router(config-if)#ip access-group 106 in
Router(config-if)#
```

2. 백업하기

•회사백본라우터 → 네이버웹서버 백업하기 ⇒ 안됨

```
Router#copy running-config tftp:
Address or name of remote host []? 192.168.3.2
Destination filename [Router-confg]? mk.file

Writing running-config.......
%Error opening tftp://192.168.3.2/mk.file (Timed out)
Router#
```

• 회사백본라우터 → 업무서버 백업하기 ⇒ 성공

```
Router#copy running-config tftp:
Address or name of remote host []? 192.168.4.2
Destination filename [Router-confg]? mk.file

Writing running-config....!!
[OK - 1319 bytes]

1319 bytes copied in 3.024 secs (436 bytes/sec)
```