액세스 리스트

① 액세스 리스트

네트워크에서 특정 트래픽(들어오고 나가는 패킷)의 접근을 제어하기 위해 사용되는 리스트(필터링)

1. 적용 목적에 따른 구분

1) 액세스 그룹 : 트래픽 필터링에 사용 → 특정 인터페이스에 적용해 In/Out 패킷을 제어

2) 분산 리스트 : 라우팅 업데이트를 필터링할 때 사용 → 특정 경로가 전파되지 않도록, 불필요한 경로 학습하지 않도록 → 일반적으로 라우팅 프로토콜 (예: OSPF, EIGRP)과 함께 사용

2. 액세스 리스트의 규칙

1) 액세스 리스트가 작동할 때, 라우터는 설정된 ACL의 각 번호(조건)를 위→아래로 순차적으로 비교

2) 액세스 리스트에서 설정한 조건과 실제로 들어오는 패킷의 조건이 일치할 때 까지 실행

→ 만약 일치하면, 해당 작업을 실행하고 나머지 부분은 더 이상 작업을 진행하지 않음

3) 액세스 리스트는 디폴트 값이 항상 거부로 설정되어 있기 때문에, 나머지 조건에 대해서 허용이 필요할 경우 명령어를 따로 지정해줘야 함 → Router(config)#access-list 1 deny any

Router(config)#access-list 1 deny 172.16.10.0 0.0.0.255

Router(config)#access-list 1 permit any → 두 번째 명령어는 첫 번째 조건 뒤에 추가되어 적용

② 와일드카드 마스크

1. 개념

IP 주소의 특정 부분을 선택적으로 비교하기 위해 사용되는 마스크, IP 주소를 필터링할 때 사용

→ IP 주소의 특정 비트를 필터링하고, 나머지 비트는 유연하게 설정할 수 있는 방법을 제공

2. 원리

0 0 0 0 0 0 0 0	→ 호스트 주소와 반드시 일치해야 함(특정 호스트를 제어해야 하는 경우)
0 0 1 1 1 1 1 1	→ 주소에서 마지막 6 비트를 무시한 범위
0 0 0 0 1 1 1 1	→ 주소에서 마지막 4 비트를 무시한 범위
1 1 1 1 1 1 0 0	→ 마지막 2비트를 주소와 체크
1 1 1 1 1 1 1 1	→ 주소 체크 안함(모든 호스트를 제어하기 위해 사용)
→ 액세스 리스트에서 any는 와일드카드 마스크가 255.255.255.255임	

와일드 카드 마스크를 0.0.0.255로 지정하면 .0~.255 사이의 IP 주소를 액세스 리스트로 제어 가능

→ 0 부분은 엄격히 비교, 255 부분은 아무 값과 일치할 수 있음을 의미

→ 예를 들어 00001111이면, 마지막 옥텟의 마지막 4비트(1111)는 일치하지 않아도 됨(모두 허용)

3. 예제

액세스 리스트가 172.10.16.0 0.0.15.255로 필터링

→ 와일드 마스크가 0.0.00001111.11111111 → 허용 범위가 4094개(=172.10.16.0/24~172.10.31.0/24)

→ ∵ 00010000.00000000~00011111.11111111까지

③ 표준 액세스 리스트 커맨드

1. 정의

```
(config)#Access-list ①{access-list-number} ②{permit|deny} ③{source-address} ④{wildcard-mask}
```

① Access-list-number : 표준 IP 액세스 리스트에서 사용되는 번호 1~99
② permit | deny : 액세스 리스트를 선언한 후 허용할 것인지 또는 차단할 것인지 지정
③ Source-address : 출발지 IP 주소를 지정
④ wildcard-mask : 출발지 IP 주소의 와일드 카드마스크를 지정, 어디까지 허용/차단할 것인지

2. 제거

```
Router(config)# no Access-list ①{access-list-number}
```

"no"라는 명령어를 사용하여 설정했던 표준 액세스 리스트를 제거, 리스트 번호를 반드시 지정

3. 액세스 그룹 설정

```
Router(config-if)# IP access-group ①{access-list-number} ②{in|out}
```

액세스 그룹은 어느 인터페이스로 들어오는 패킷을 차단을 할 것인지 지정하는 것
→ 표준 액세스 리스트를 설정한 후 액세스 그룹을 설정하지 않으면 무용지물임
② in|out: 패킷이 해당 인터페이스로 들어오거나 나가는 방향을 설정하여 액세스 리스트를 적용

④ 표준 액세스 리스트와 액세스 그룹

1. 액세스 리스트 유형에 따른 분류

1) 표준 액세스 리스트 : 출발지 IP 주소만으로 필터링 → 네트워크 계층 → 전송 계층
2) 확장 액세스 리스트 : 출발지와 목적지 IP 주소, 프로토콜, 포트 번호 등 세부적으로 필터링

2. 액세스 그룹

액세스 그룹은 특정 인터페이스에 액세스리스트를 적용하는 설정, in/out 패킷을 제어하기 위해 사용

3. 액세스 리스트 명령어 과정(예제)

Q. 라우터가 Nework 130.100.0.0/16으로 오는 패킷을 막고 나머지를 허용하자
A. Router(config)#access-list 1 deny 130.100.0.0 0.0.255.255
Router(config)#access-list 1 permit any
Router#sh ip access-list
Standard IP access list 1
deny 130.100.0.0, wildcard bits 0.0.255.255
permit any

Q. 라우터가 Nework 130.100.0.0/16으로 오는 패킷만 라우터를 지나가도록 하자
A. Router(config)#access-list 2 permit 130.100.0.0 0.0.255.255
Router(config)#access-list 2 deny any → Default가 deny이므로 해당 명령어는 불필요
Router#sh ip access-list
Standard IP access list 2
permit 130.100.0.0, wildcard bits 0.0.255.255
default any

4. 액세스 그룹 명령어 과정(예제)

```
Router(config-if)#ip access-group access-list-number {in|out}
Router#sh ip access-list
Standard IP access list 1
deny 130.100.0.0, wildcard bits 0.0.255.255
permit any
Router#config t
Router(config)#int s 0
Router(config-if)#ip access-group 1 in
```

→ 해당 인터페이스로 들어오는 패킷에 대해서만 액세스 리스트 1의 규칙이 적용됨

예제) 라우터가 130.100.16.0/20 Network 으로 오는 패킷을 막고 나머지를 허용하자

→∴서브넷 마스크가 20이므로, Wildcard mask가 0.0.15.255가 된다.

```
Router(config)# access-list 1 deny 130.100.16.0 0.0.15.255
Router(config)# access-list 1 permit any
Router(config)# int s 0
Router(config-if)# ip access-group 1 in
```

Q. in 접근 제어랑, out 접근 제어 중 뭐가 더 관리가 측면에서 편한지?

Q. 다양한 출발지 IP 주소에서 오는 패킷의 경우는 in 접근 제어, 특정 출발지에서만 오는 패킷들은 out으로 접근 제어하는게 나은지?

⑤ 표준 액세스 리스트 예제

1. 172.16.10.0/24의 모든 네트워크들은 E0과 E1로 접근하는 것을 차단하고자 하는 설정

```
①#access-list 1 deny 172.16.10.0 0.0.0.255
②#access-list 1 permit any
③#interface ethernet 0
④#ip access-group 1 out
⑤#interface ethernet 1
⑥#ip access-group 1 out
```

```
①#access-list 1 deny 172.16.10.0 0.0.0.255
②#access-list 1 permit any
③#interface s0
④#ip accessgroup 1 in
```

2. 특정한 호스트만 E0로 전송되는 패킷을 차단, 나머지 인터페이스는 모두 허용 하고자 하는 설정

```
①Router(config)#access-list 1deny 172.16.4.13 0.0.0.0
②Router(config)#access-list 1 permit any
③Router(config)#interface ethernet 0
④Router(config-if)#ip access-group 1 out
```

3. 172.16.4.0 네트워크는 E0로 나가는 패킷을 차단하고, 나머지 인터페이스로는 허용 하는 설정

```
①Router(config)#access-list 1 deny 172.16.4.0 0.0.0.255
②Router(config)#access-list 1 permit any
③Router(config)#interface ethernet 0
④Router(config-if)#ip access-group 1 out
```

⑥ 표준 액세스 리스트 확인 커맨드

1. Show access-list 110

```
Router#show access-list 110
Extended IP access list 110
   deny tcp any host 172.16.10.5 eq ftp
   deny tcp any host 172.16.10.5 eq telnet
   permit ip any any
```

설정된 액세스 리스트 중 액세스 리스트 번호 110번에 적용된 보안정책을 보여주는 메시지를 확인하고자 할 때 사용하는 명령어 → 정의한 특정 트래픽에 대한 허용 또는 거부 조건 등을 의미

2. Show ip access-list

```
Router#sh ip access-list
Extended IP access list 101
   deny tcp host 172.16.10.10 any eq www (8 matches)
   permit tcp any any
Extended IP access list 110
   deny tcp any host 172.16.10.5 eq ftp
   deny tcp any host 172.16.10.5 eq telnet
   permit ip any any
```

라우터에 설정된 IP 액세스 리스트 설정에 대한 전체적인 보안정책을 모두 확인할 수 있는 명령어