네트워크 초급 과정

Netwrok Beginner Class

Chapter 06 ACL&NAT

01

Access Control List

What is the ACL?

네트워크 간의 통신에서 트래픽을 관리하고
보안성을 높이기 위한 방법은 무엇이 있을까?

그에 대한 해답으로 ACL에 대해서 알아보자.

ACL Concept

What is the Access-List?

Why we use Access-list?

1

특정 사용자의 접근을 제한하고자 하는 경우

수신한 패킷의 출발지 주소를 확인하여 네트워크에 접근할 수 있는 사용자와 그렇지 않은 사용자의 구분을 해주기 위해서 사용한다.

2

특정 서비스의 이용을 제한하고자 하는 경우

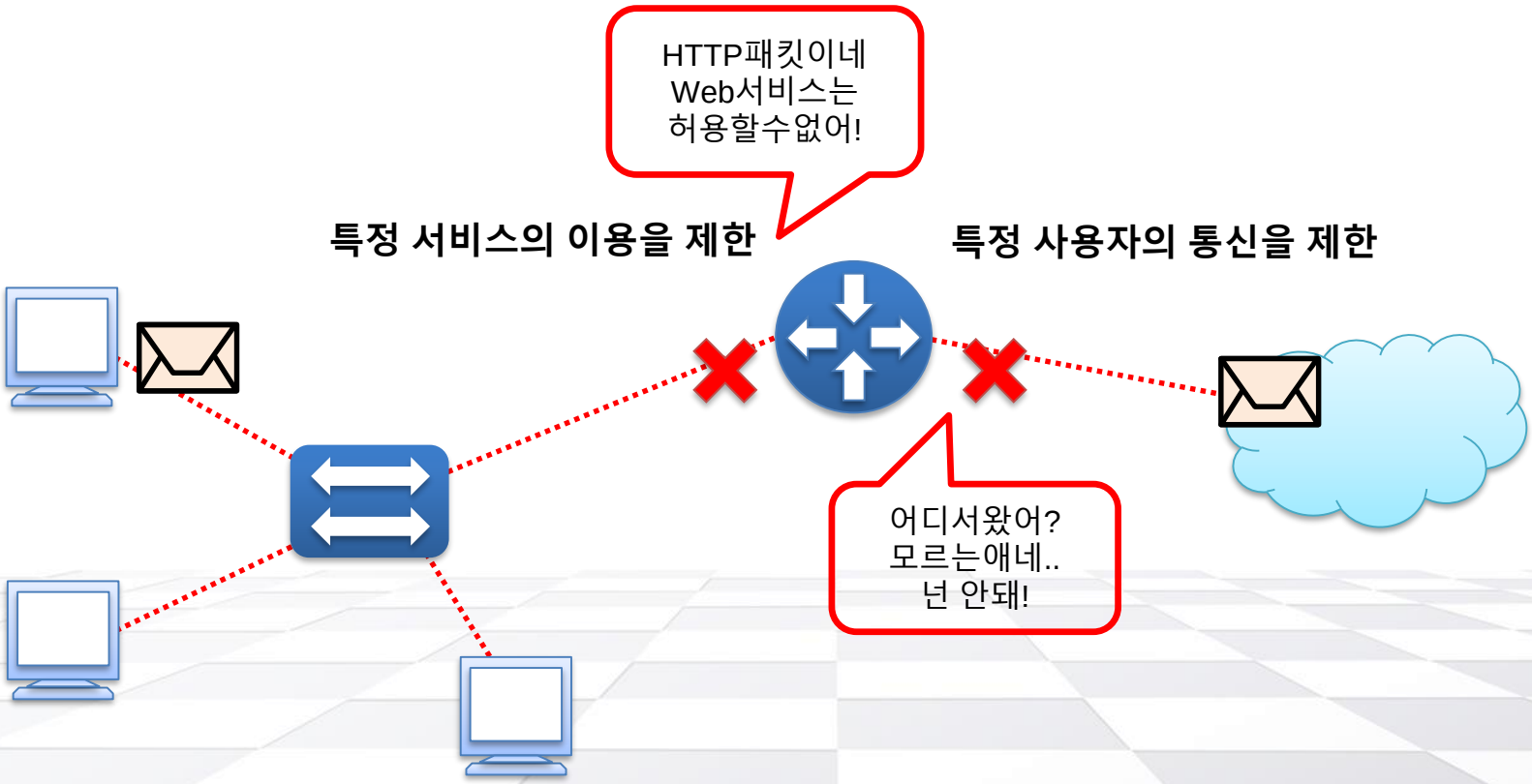
Web 서비스를 막거나 Telnet의 사용을 제한하는 등, 네트워크 별로 제한하고자 하는 프로토콜의 종류를 표시하여 통신 패킷을 필터링할 수 있다.

3

라우팅 경로의 조정이 필요한 경우

Dynamic 방식을 사용하여 라우팅을 한 경우, 관리자가 원하는대로 경로조정이 되지 않은 경우에는 Access-list를 사용하여 추가적인 조정이 가능하다.

Example of Access-list



Access List Type

01 Standard

출발지만 확인하는 기본 ACL

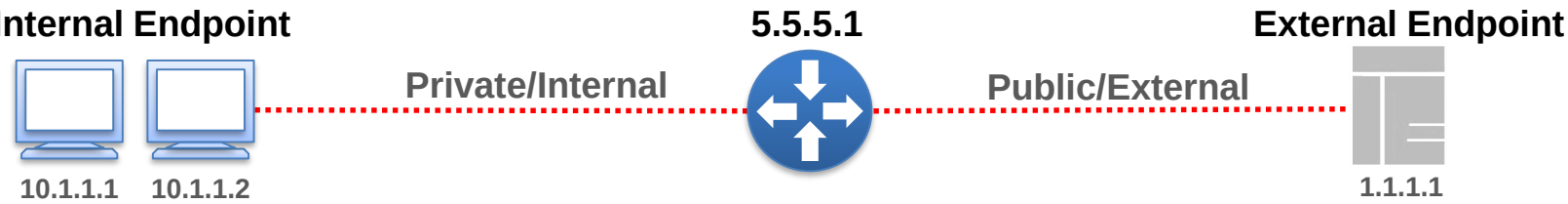
- 수신한 패킷의 내용 중 출발지 주소만 확인하여 필터링하는 방식
- 서비스나 특정 트래픽의 구분 없이 필터링하는 경우에 사용한다.
- 또한, 특정 네트워크의 범위를 지정하여 Object로 사용할 경우에도 쓰인다.

02 Extended

여러 옵션을 확인하는 확장 ACL

- 출발지·목적지 주소, 프로토콜과 포트번호까지 확인하여 필터링 하는 방식
- 특정 서비스나 트래픽의 구분을 통해 좀 더 상세한 필터링을 할 수 있다.

Standard Access-list



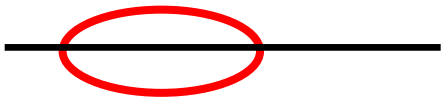
ACL 조건

출발지 IP가 10.1.1.1인 경우만 통과

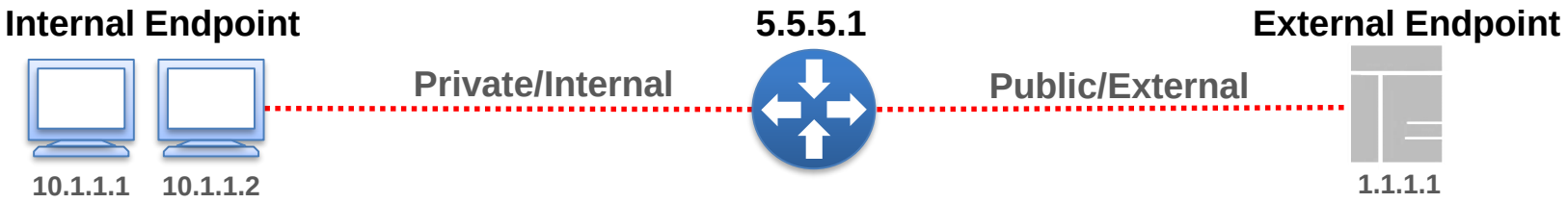
출발지		목적지	
포트	IP주소	포트	IP주소
5000	10.1.1.1	80	1.1.1.1
6000	10.1.1.2	80	1.1.1.1

허용 or 거부?

허용 or 거부?



Extended Access-list



ACL 조건

출발지 주소 10.1.1.0/24 ,목적지 주소 1.1.1.1
포트 80(HTTP)만 통과

출발지		목적지	
포트	IP주소	포트	IP주소
5000	10.1.1.1	80	1.1.1.1
6000	10.1.1.2	23	1.1.1.3

허용 or 거부? **허용**

허용 or 거부? **거부**

Access List Making type

01 Numberic

숫자를 사용하여 ACL 생성

- 리스트 번호를 지정하여 해당 액세스 리스트가 어떤 타입인지 결정
- STANDARD 방식인 경우, 기본 1~ 99 확장 1300 ~ 1699를 사용
- EXTENDED 방식의 경우, 기본 100 ~ 199 확장 2000 ~ 2699를 사용

Ex) access-list 10 permit host 10.10.10.10
=> 번호를 '10'을 사용하여 STANDARD인 것을 알 수 있다.

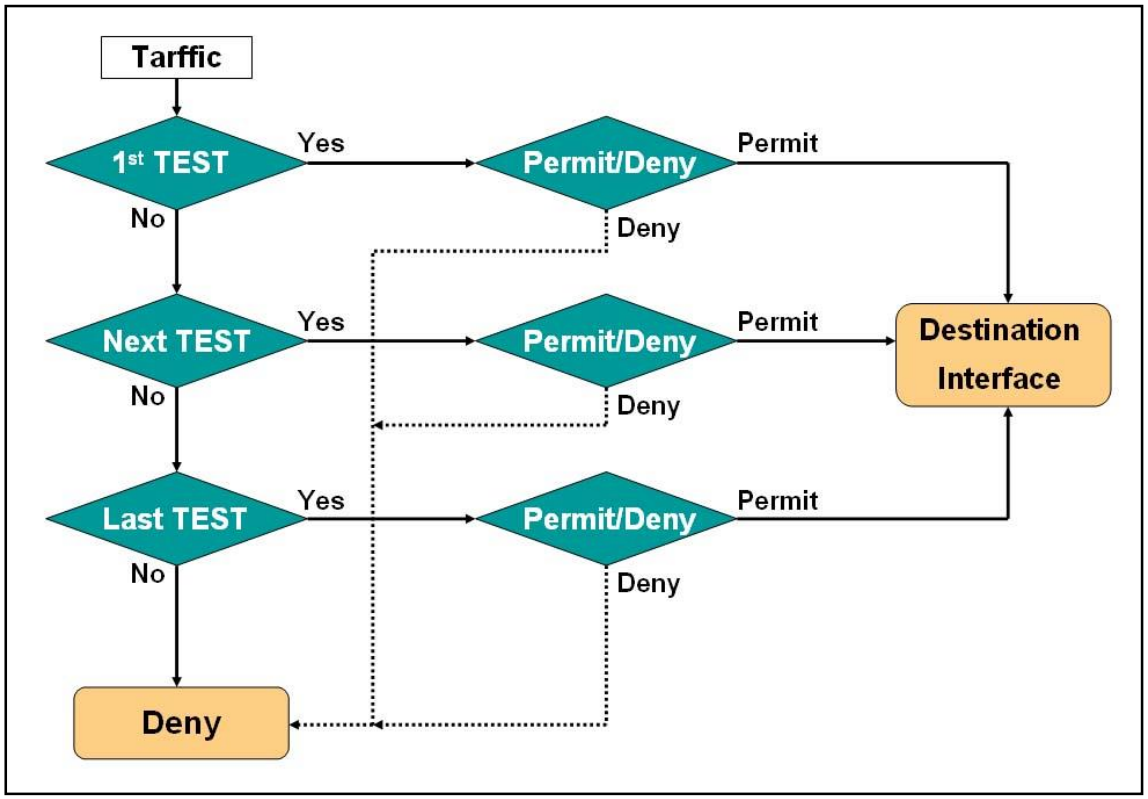
02 Named

문자를 사용하여 ACL 생성

- 각 Access List에 고유한 이름을 지정
- List 생성시 STANDARD, EXTENDED 방식 중에 하나를 선택해 사용

Ex) ip access-list standard test
=> 이름 'test'을 사용하여 List를 구분하여 지정

ACL First match rule

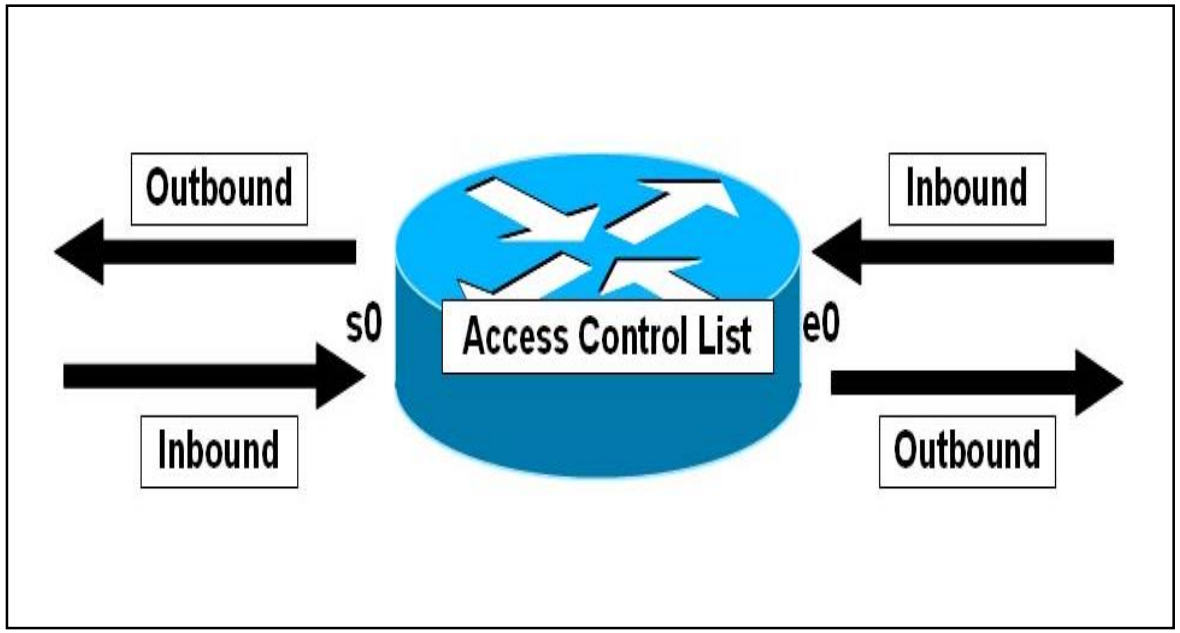


Access-list policy

- 패킷 필터링시 Access-list의 정책의 위에서 부터 비교를 하며, 패킷의 내용과 부합하는 정책이 발견되면 해당 정책에 의해 처리된다.
- ACL의 마지막 줄에는 모든 대상에 대한 차단 정책이 기본적으로 생성되며, 그 어떠한 정책에도 부합하지 않는 패킷은 이 차단정책에 의해 필터링 된다.

ACL 정책 적용 순서

Inbound or Outbound



Access-list policy on interface

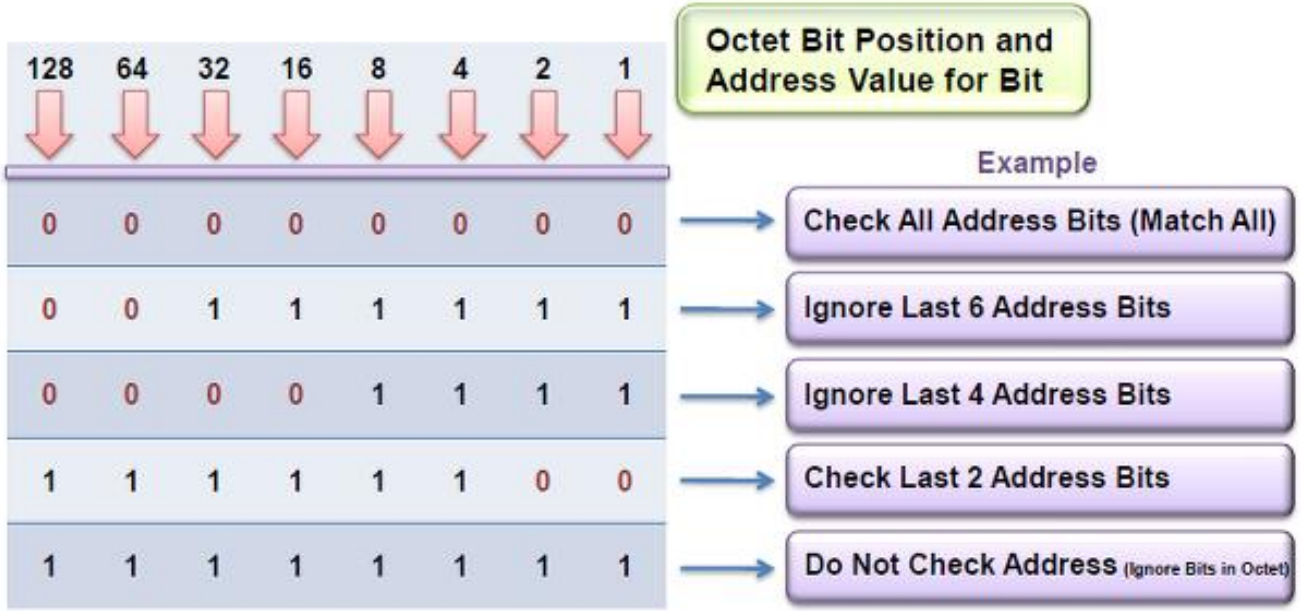
- Inbound는 패킷이 유입될 때 필터링을 하는 방식이다.
- Outbound는 패킷이 빠져나갈 때 필터링을 하는 방식이다.
- 포트에 정책 적용시 Inbound와 Outbound의 방향은 라우터의 관점에서 따지게 된다.

ACL 정책 적용방식

Wildcard Mask

Usage of wildcard-mask

Wildcard-mask



Feature of Wildcard-mask

- 와일드카드 마스크를 사용하면 원하는 특정 IP의 주소 혹은 네트워크 범위를 지정할 수 있다.
- 2진수 0과 1을 사용하여 표시하며, **고정(Match)시킬 특정 bit를 검사하기 위해 0을 사용**한다.

- 예를 들어 1.1.1.0/24 범위의 주소만 허용하고자 할 경우, 반드시 매칭되어야 할 첫번째 옥텟부터 세번째 옥텟까지 24bit를 0으로 표시하여 고정하고 나머지는 1을 사용하여 표시한다.
- 따라서 1.1.1.0/24를 표현하기 위해 사용될 와일드카드 마스크는 0.0.0.255가 된다.

와일드카드 마스크란?

Wildcard-mask

Usage of Wildcard-mask

- **와일드카드 마스크로 IP 지정하는 방식**
  - IP address 뒤에 이어서 적어준다.
  - Usage : ***IP-address Wildcard-mask***
- **특정 호스트 IP 하나를 지정** (모든 bit를 검사)
  - 32bit를 모두 검사하여 지정한 특정 호스트의 IP가 맞는지 확인하는 방식으로 모든 bit를 0으로 표시해준다.
  - ex) **192.168.2.2 0.0.0.0**
- **특정 네트워크 주소 범위를 지정**
  - 네트워크 범위를 지정하기 위해 Net-ID로 사용된 부분을 고정하는 0으로 표시하고, 어떤 값이 와도 상관없는 Host-ID는 1로 표시한다.
  - ex) 172.16.0.0/16 >> **172.16.0.0 0.0.255.255**
- **모든 IP를 지정** (모든 bit를 무시)
  - 모든 주소(All IP address) 라는 뜻으로 사용하기 위해 모든 bit를 1로 표시한다.
  - ex) **0.0.0.0 255.255.255.255**

와일드카드 마스크 사용법

ACL Configuration

How can I configure ACL?

Configurations of ACL

Step 1

R1(config)# **access-list** *access-list-number* { **permit** | **deny** } {*test conditions*}

- **Access-list** : Access list 설정 명령어
- ***Access-list-number*** : Access-list를 구분하는 숫자, Standart와 Extended등을 구분
- { **permit** | **deny** } : Entry 허용 여부 결정
- {**test conditions**} : Entry 검사 조건 내용

Access-list 정책 만들기

Step 2

R1(config-if)# {*protocol*} **access-group** *access-list-number* { **in** | **out** }

- **{protocol} :** Access-list 사용하는 통신 프로토콜. 주로 IP라고 적으면 된다.
- **Access-group** : Access list 인터페이스 적용 설정 명령어
- ***Access-list-number*** : Access-list를 구분하는 숫자, 만들어진 Access-list 조건문 번호를 입력
- { **in** | **out** } : Access list 검사 적용 정책. (in : 인터페이스로 들어가는 데이터, out : 나가는 데이타

필터링 적용하기

Configure Standard ACL

Access-list IP Traffic Filter list Entry 작성

R1(config)# **access-list** *access-list-number* { **permit** | **deny** } ***source source-wildcard***

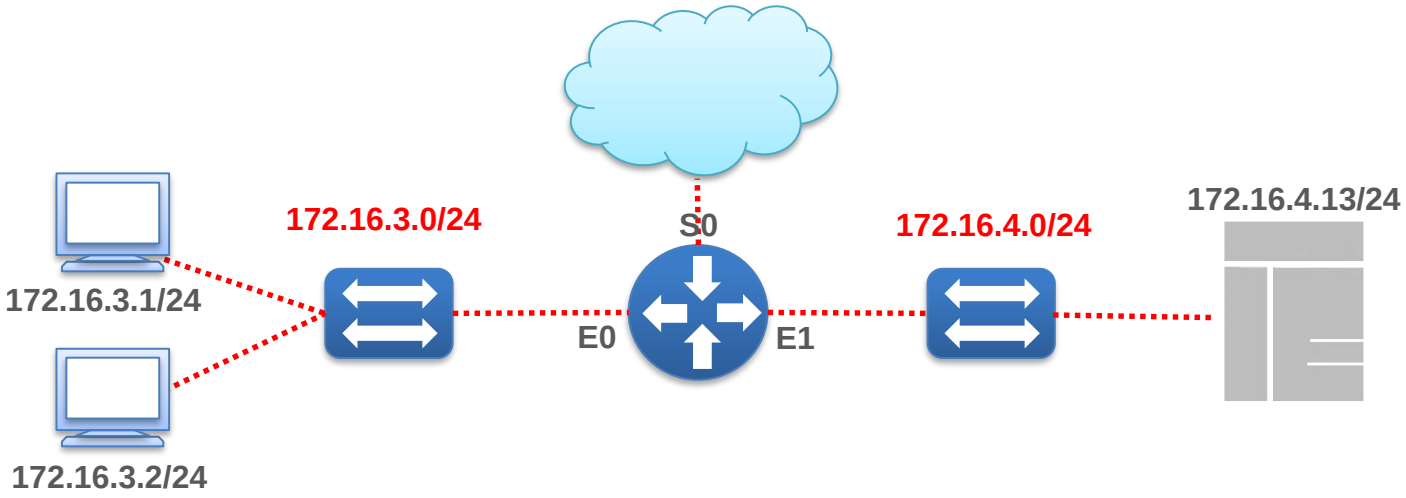
- **Access-list-number :** Entry가 속할 list 번호 설정. 1~99, 1300~1999사이의 번호
- **permit | deny | remark**는 해당 Entry에 매치되면 취할 Action을 정의
- **Source**는 송신지 IP Address를 정의
- **mask**는 Wildcard mask를 사용하여 Address 필드의 어느 비트들이 일치되어야 하는지 설정

Access-list를 interface에 적용

R1(config-if)# **ip access-group** *access-list-number* { **in** | **out** }

- **List**를 적용할 **Interface**에서 설정
- **Inbound**또는 **Outbound**시 검사하도록 설정
- **Default = outbound**
- **Interface**에서 **"no ip access-group *access-list-number*"**명령을 사용하여 적용된 **Access-list**를 제거

Example : Standard ACL



Standard Access list 설정 예제

Router(config)#access-list 1 permit 172.16.0.0 0.0.255.255

(access-list 1 deny 0.0.0.0 255.255.255.255)

Router(config)#interface ethernet 0
Router(config-if)#ip access-group 1 out
Router(config)#interface ethernet 1
Router(config-if)#ip access-group 1 out

Configure Extended ACL

Access-list IP Traffic Filter list Entry 작성

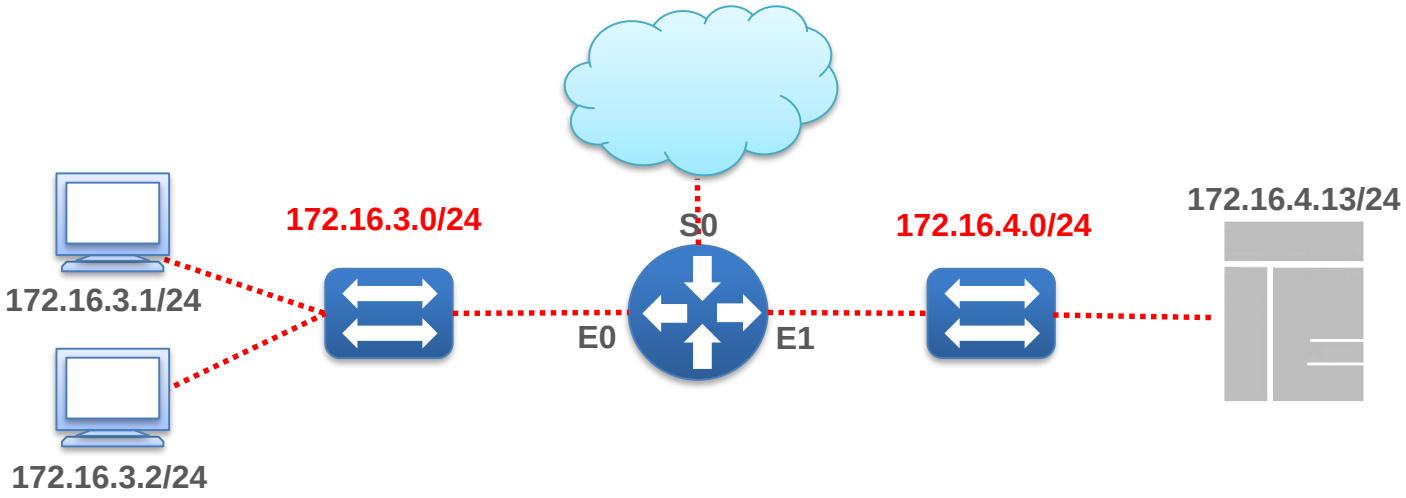
R1(config)# **access-list** *access-list-number* { **permit** | **deny** } ***protocol source src-wildcard*** [*operator port*] ***destination dst-wildcard*** [***operator port***] [established] [log]

- **Access-list-number :** Entry가 속할 list 번호 설정. 100~199, 2000~2699사이의 번호를 사용
- **Permit | deny | remark**는 해당 Entry에 매치되면 취할 Action을 정의
- **Source와 Destination**은 송수신지 IP Address를 정의
- **mask는 Wildcard mask**를 사용하여 Address 필드의 어느 비트들이 일치되어야 하는지 설정
- **Operator port는 lt(less than), gt(greater than), eq(equal to), neq(not equal to)와 Protocol Port번호를 명시**
- **established**는 Inbound TCP에 대해서만 사용된다
- **log는 Console로 log Message를 보낸다**

Access-list를 interface에 적용

R1(config-if)# **ip access-group** *access-list-number* { **in** | **out** }

Example : Extended ACL



Extended Access list 설정 예제

Router(config)#access-list 101 deny tcp 172.16.3.0 0.0.0.255 172.16.4.0 0.0.0.255 eq 21

Router(config)#access-list 101 deny tcp 172.16.3.0 0.0.0.255 172.16.4.0 0.0.0.255 eq 20

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

(access-list 101 deny 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255)

Router(config)#interface ethernet 1

Router(config)#ip access-group 101 out

Configure Named ACL

Access-list IP Traffic Filter list Entry 작성

R1(config)# **ip access-list** {**standard** | **extended**} *Name*

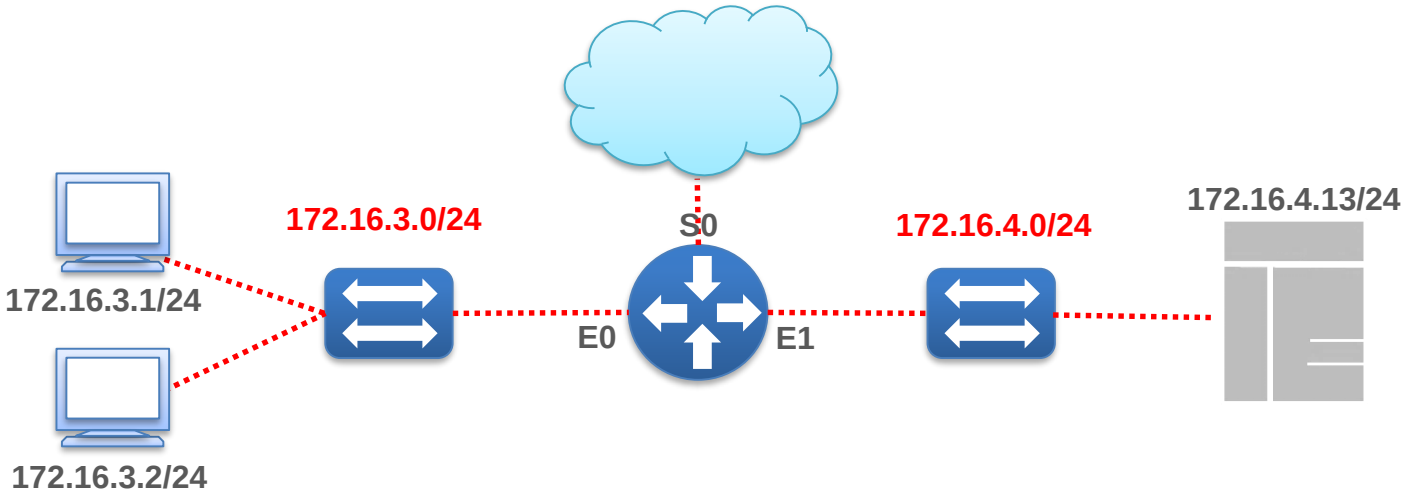
R1(config-std or ext)# {permit | deny} {test conditions} => Entry 생성

R1(config-std or ext)# no {permit | deny} {test conditions} => Entry 삭제

Access-list를 interface에 적용

R1(config-if)# **ip access-group** *Name* { in | out }

Example : Named ACL



Named Access list 설정 예제

Router(config)#ip access-list extended screen

Router(configext-nacl)#deny tcp 172.16.3.0 0.0.0.255 172.16.4.0 0.0.0.255 eq 23

Router(configext-nacl)#permit ip any any

Router(config)#interface ethernet 1

Router(config-if)#ip access-group screen out

02

Network Address Translation

Translation of IP address for communications

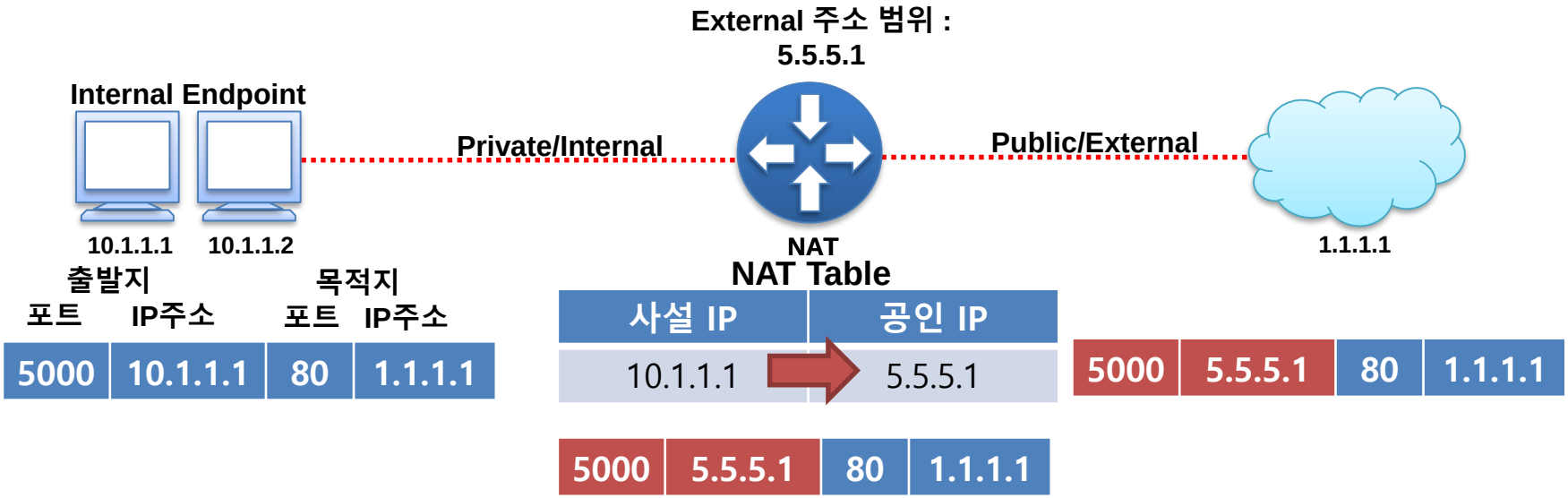
IP의 부족현상을 완화시키기 위해 내부 네트워크에서 사설IP를 사용하는 경우가 많은데, 이런 경우 외부와 통신하기 위해 주소를 변환해주는 기술이 필요하다.

네트워크 통신을 위해 주소를 변환해주는 NAT에 대해서 알아보자.

NAT Concept

What is the NAT?

NAT (Network Address Translation)



NAT(Network Address Translation)

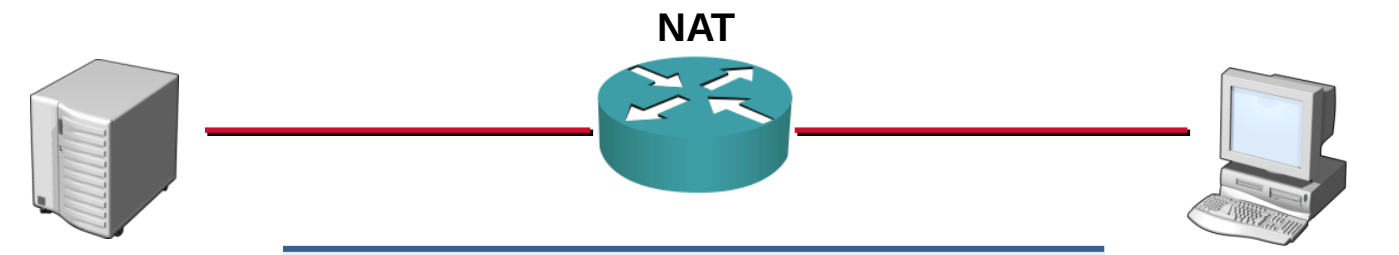
NAT란? RFC 1631에 정의된 것으로 IP 헤더에 있는 주소를 다른 주소로 바꾸는 기술.

주로 NAT는 사설주소를 사용하는 호스트들이 인터넷 서비스를 이용할 있게 하려고 사용.

동작은 NAT 설정된 장비를 거치면서 주소가 설정된 주소로 변경되고, 변경정보를 저장했다가 패킷이 돌아오면 다시 원래 패킷으로 변경해서 사용.

종류는 **Dynamic NAT, NAT-PAT, Static NAT** 등이 있다.

Static NAT

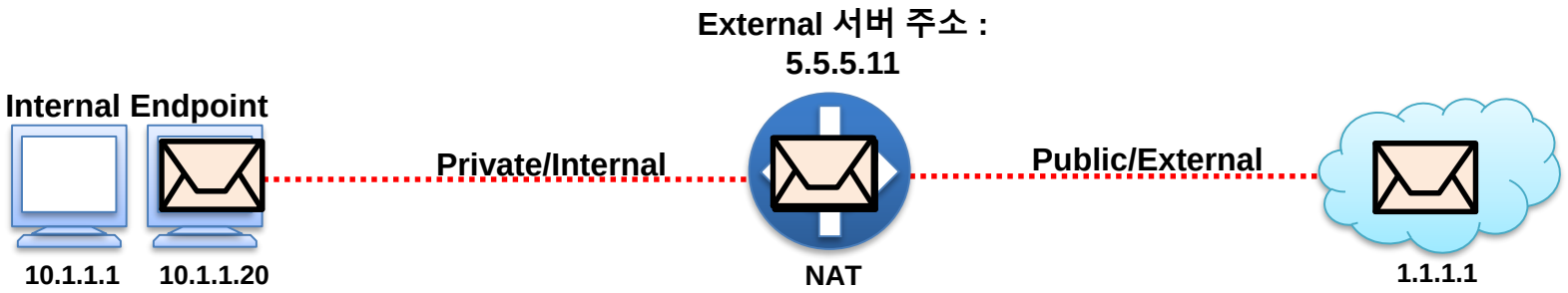


Static NAT	
Private Address	**Public Address**
192.168.100.1	210.123.94.1
192.168.100.2	210.123.94.2

Static NAT

- 하나의 사설 IP와 하나의 공인 IP 주소를 1:1로 Mapping 하는 방식이다.
- 서버가 동작중인 사설 네트워크인 경우, 외부 사용자들이 접속할 수 있도록 고정적인 주소 Mapping이 필요하기 때문에 Static 방식을 사용한다.

Static NAT



사설 IP	공인 IP
10.1.1.20	5.5.5.11

출발지	목적지
10.1.1.20	1.1.1.1

5.5.5.11	1.1.1.1

1.1.1.1	10.1.1.20

1.1.1.1	5.5.5.11

Configure Static NAT

Configure Static NAT

Configuration of Static NAT

고정적인 변환을 위한 Static NAT 설정

R1(config)# ip nat inside source static *local-IP global-IP*

- **ip nat inside source static**: 사설IP와 공인IP가 고정적으로 변환되도록 Static NAT설정
- **local-IP :** 사설IP의 주소
- **global-IP** : 공인IP의 주소

NAT를 interface에 적용

R1(config-if)# ip nat inside => 변환할 패킷이 들어오는 인터페이스에 설정

R1(config-if)# ip nat outside => 변환된 패킷이 나가는 인터페이스에 지정

Verifying Static NAT

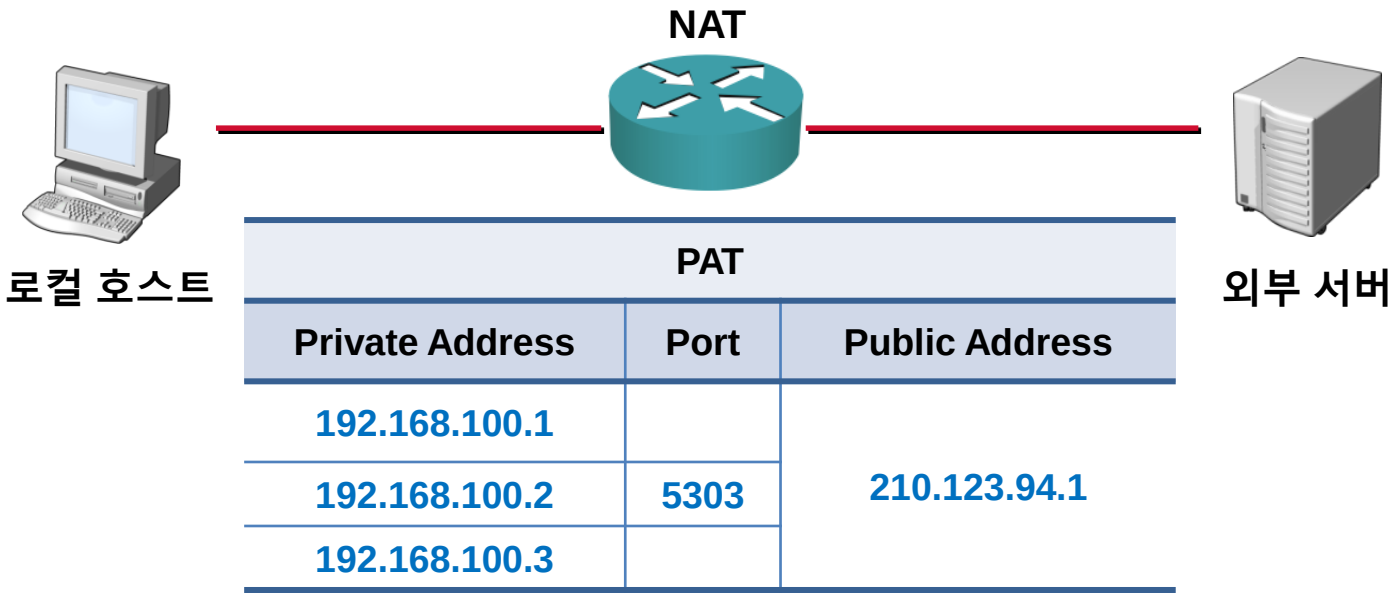
NAT Table 확인 명령어

```
R1# show ip nat translations
Pro     Inside global     Inside local       Outside local      Outside global
-       210.1.0.1         10.10.10.1         -                  -
```

NAT Table 내용 삭제

```
R1# clear ip nat translation *
```

Dynamic NAT

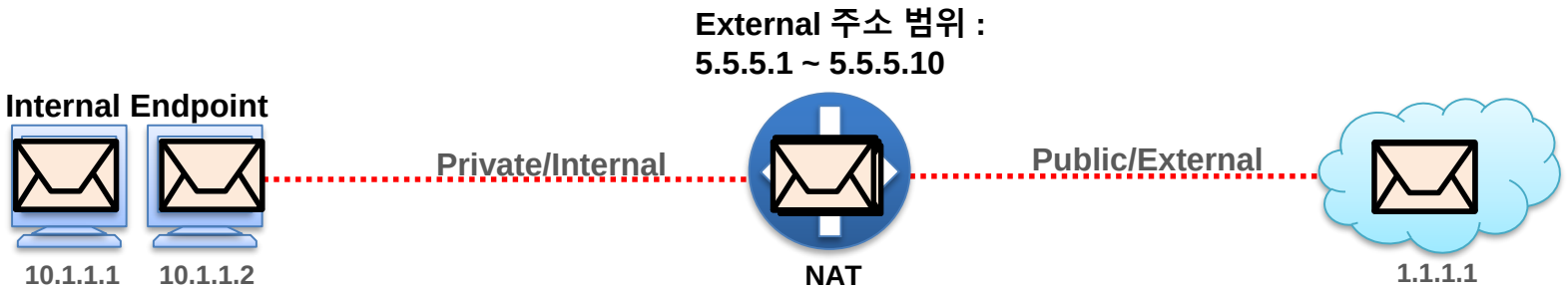


PAT		
Private Address	Port	Public Address
192.168.100.1		210.123.94.1
192.168.100.2	5303	
192.168.100.3		

Dynamic NAT

- 여러 개의 사설 IP와 여러 개 혹은 하나의 공인 IP 주소를 필요에 따라 동적으로 Mapping 하는 방식이다.
- 대부분 공인 IP 주소가 사설 IP 주소보다 적을 경우에 사용한다.
- Basic NAT는 일시적이지만 IP:IP로 Mapping 되기 때문에 하나의 공인 IP를 여러 사설IP가 공유할 수 없지만, Port번호를 사용하는 PAT는 공유할 수 있다.

Dynamic NAT



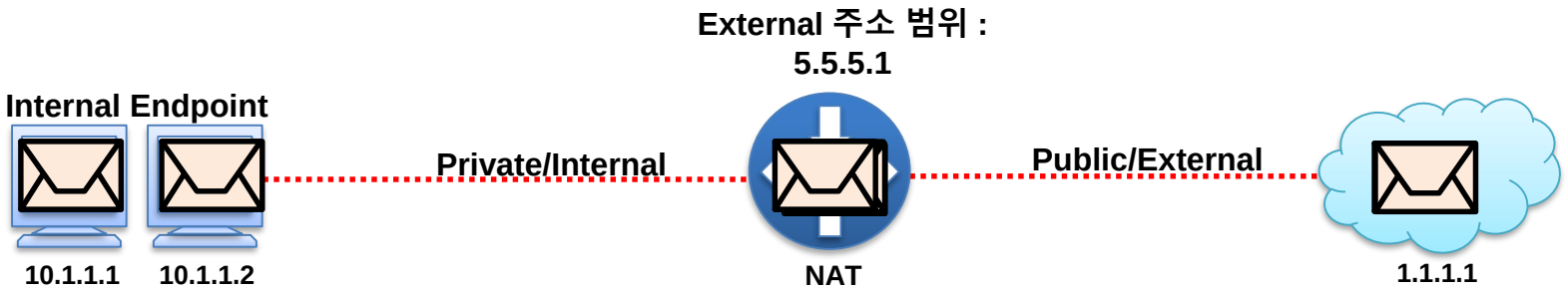
Private	Public
10.1.1.1	5.5.5.1
10.1.1.2	5.5.5.2

출발지	목적지
10.1.1.1	1.1.1.1
10.1.1.2	1.1.1.1

1.1.1.1	10.1.1.1
1.1.1.2	10.1.1.1

1.1.1.1	5.5.5.1
1.1.1.1	5.5.5.2

NAT PAT(Port Address Translation)



Private		Public	
10.1.1.1	5000	5.5.5.1	5000

출발지 목적지

5000	10.1.1.1	80	1.1.1.1
5000	10.1.1.2	80	1.1.1.1

80	1.1.1.1	5000	10.1.1.1
80	1.1.1.1	5001	10.1.1.2

80	1.1.1.1	5000	5.5.5.1
80	1.1.1.1	5001	5.5.5.1

Configure Dynamic NAT

Configuration of Dynamic NAT

IP 변환에 사용할 전역 주소 풀 설정

R1(config)# ip nat pool [name] [start-ip] [end-ip] { netmask *netmask* | prefix-length *prefix* 값}

- **ip nat** : ip 에 대한 nat 설정 명령어
- **Pool** : 변환될 공인 IP가 저장되는 주소 데이터가 있는 공간
- **Start-ip, end-ip** : pool에 저장된 IP주소의 시작과 끝 범위
- **Netmask or prefix** : pool에 저장되는 IP의 네트워크 길이

NAT로 IP변환을 허용할 주소 설정(Standard Access list사용)

R1(config)# access-list [Access-list number] permit source-IP [source-wildcard]

- **Access list** : Access list 명령어
- ***Access-list number*** : IP 변환을 허용할 영역 Access list 번호
- **Permit** : Access list 적용 규칙
- **Sourc & Source-wildcardix** : Source IP 주소 영역

Configuration of Dynamic NAT

동적인 변환을 위한 Dynamic NAT설정

R1(config)# ip nat inside source list *acl-number* pool *pool-name* [overload]

- **ip nat inside source list**: nat 변환 설정 ip source 주소를 Access-list에 맞춰서 변경
- **Acces-list number :** 변환할 IP 주소 범위를 지정한 Access-list number
- **pool [pool 이름]** : 변환해줄 공인 pool의 이름을 지정
- **overload** : 옵션으로 overload를 사용하면 NAT-PAT로 사용.

NAT를 interface에 적용

R1(config-if)# ip nat inside => 변환할 패킷이 들어오는 인터페이스에 설정

R1(config-if)# ip nat outside => 변환된 패킷이 나가는 인터페이스에 지정

Verifying Dynamic NAT

NAT Table 확인 명령어

```
R1# show ip nat translations
Pro     Inside global     Inside local       Outside local      Outside global
udp     210.1.0.1:1438    10.10.10.1:1438    210.1.1.2:69       210.1.1.2:69
udp     210.1.0.1:1439    10.10.10.2:1438    210.1.1.2:69       210.1.1.2:69
```

NAT Table 내용 삭제

```
R1# clear ip nat translation *
```

Verifying Dynamic NAT

NAT 변환 통계 정보보기

```
R1# show ip nat statistics
```

NAT 변환 상태 모니터링

```
R1# debug ip nat
```