



네트워크야 놀자! (실습)

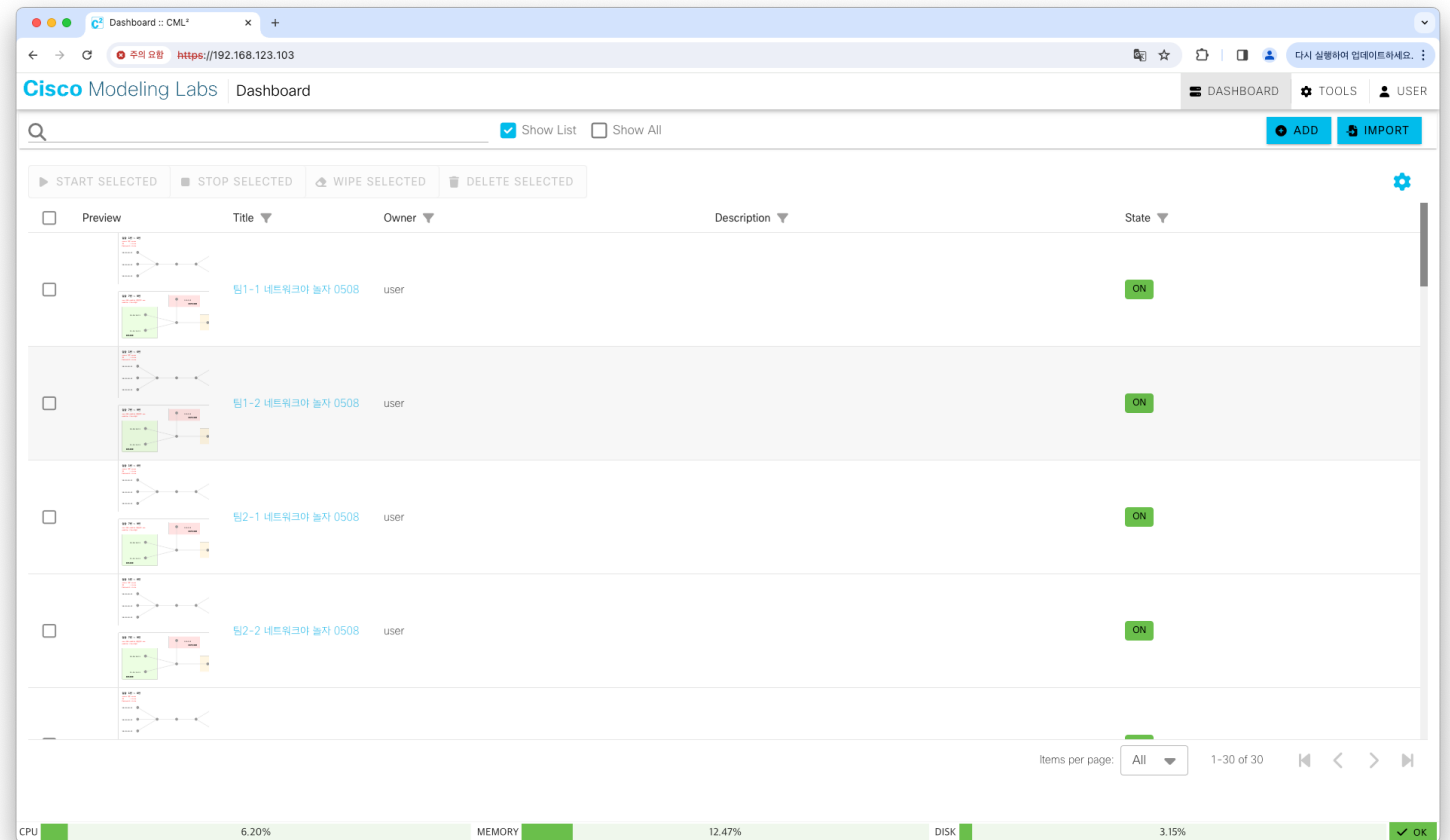
Level 4. 방화벽

김기동 프로
광운대-시스코 이노베이션 센터

2024.05.08.

CML 접속

- <https://192.168.123.103> 접속
- ID / PW: user / 1234Qwer!
- 팀에 맞춰서 랩 접속



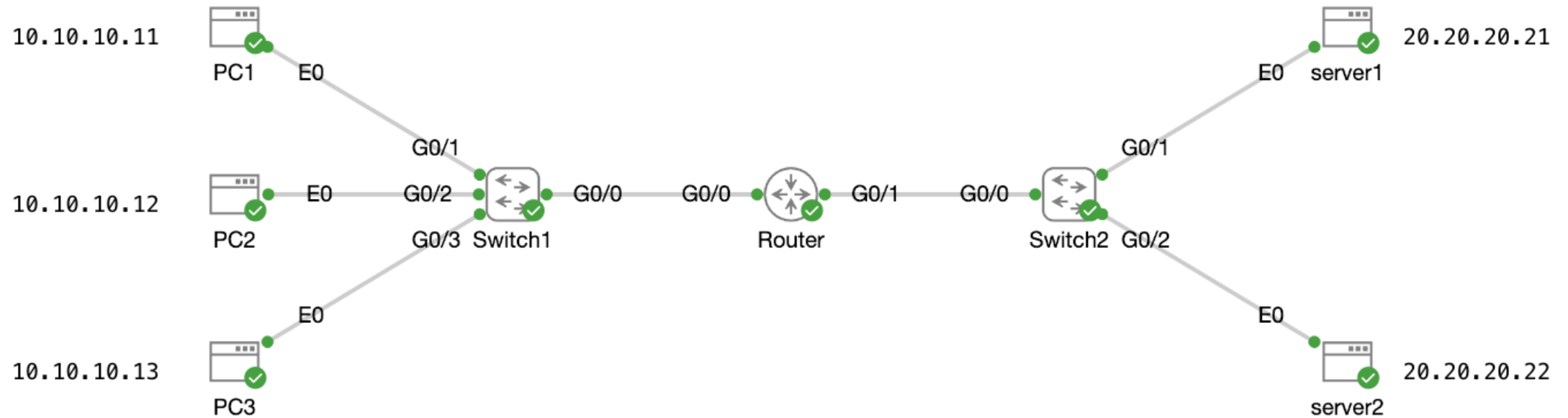
실습1번 ~ 6번 토폴로지

실습 1번 ~ 6번

***** 계정 *****

ID : cisco

Password: cisco



실습 1. Standard ACL 설정

조건

- Router에서 Standard ACL을 생성하고 10.10.10.11만 통신 허용하는 엔트리를 생성합니다.
 - ACL number로 1 사용
- Router의 interface gi 0/0에 ACL을 적용합니다.
- Hint: p.31

확인

- PC1에서 Server1으로 핑 성공(ping 20.20.20.21)
- PC2에서 Server1으로 핑 실패(ping 20.20.20.21)
- Router에서 show ip access-lists 1 명령어로 증가된 카운터 확인

실습 1. Standard ACL 설정 (답)

```
Router(config)#ip access-list standard 1
Router(config-std-nacl)#permit 10.10.10.11 log
Router(config-std-nacl)#
Router(config-std-nacl)#interface gi 0/0
Router(config-if)#ip access-group 1 in
```

```
Router#show ip access-lists 1
Standard IP access list 1
  10 permit 10.10.10.11 log
Router#
```

실습2. Standard ACL 엔트리 추가

조건

- 실습1에서 생성한 ACL에 10.10.10.0/24 대역을 허용하는 엔트리를 추가합니다.
- Router의 privilege mode에서 clear access-list counters 1 명령어를 실행합니다.
 - 실습1에서 증가한 카운터가 초기화 됩니다.
- Hint: p.41

확인

- PC1에서 Server1으로 핑 성공(ping 20.20.20.21)
- PC2에서 Server1으로 핑 성공(ping 20.20.20.21)
- Router에서 show ip access-lists 1 명령어로 증가된 카운터 확인

실습2. Standard ACL 엔트리 추가 (답)

```
Router(config)#ip access-list standard 1  
Router(config-std-nacl)#permit 10.10.10.0 0.0.0.255 log
```

```
Router#show ip access-lists 1  
Standard IP access list 1  
  10 permit 10.10.10.11 log (3 matches)  
  20 permit 10.10.10.0, wildcard bits 0.0.0.255 log (5 matches)  
Router#
```

실습3. Standard ACL 엔트리 삭제 및 추가하기

조건

- 실습1에서 생성한 10.10.10.11을 허용하는 엔트리를 제거합니다.
- 10.10.10.11을 차단하는 엔트리 생성하며 이때 sequence number를 5로 하여 생성합니다.
- Hint: p.36, 37

확인

- PC1에서 Server1으로 핑 실패(ping 20.20.20.21)
- PC2에서 Server1으로 핑 성공(ping 20.20.20.21)
- Router에서 show ip access-lists 1 명령어로 증가된 카운터 확인

실습3. Standard ACL 2 제거하고 추가 (답)

```
Router(config)#ip access-list standard 1  
Router(config-std-nacl)#no 10  
Router(config-std-nacl)#5 deny 10.10.10.11
```

```
Router#show ip access-lists 1  
Standard IP access list 1  
    5 deny 10.10.10.11 (6 matches)  
    20 permit 10.10.10.0, wildcard bits 0.0.0.255 log (7 matches)  
Router#
```

실습4. Extended ACL 설정

조건

- Router에서 Extended ACL을 생성하고 이때 ACL name은 extACL로 합니다.
- PC1에서 Server1으로 가는 통신을 허용하는 엔트리를 생성합니다.
 - protocol: IP, source: host 10.10.10.11, destination: 20.20.20.21
- Router의 interface gi 0/0에 ACL을 적용합니다.
- Hint: p.55

확인

- PC1에서 Server1으로 핑 성공(ping 20.20.20.21)
- PC1에서 Server1으로 SSH 성공(ssh cisco@20.20.20.21)
- PC1에서 Server2으로 핑 실패(ping 20.20.20.22)
- PC2에서 Server1으로 핑 실패(ping 20.20.20.21)

Router에서 `show ip access-lists extACL` 명령어로 증가된 카운터 확인

실습4. Extended ACL 설정 (답)

```
Router(config)#ip access-list extended extACL
Router(config-ext-nacl)#permit ip host 10.10.10.11 host 20.20.20.21 log
Router(config-ext-nacl)#
Router(config-ext-nacl)#interface gi 0/0
Router(config-if)#ip access-group extACL in
```

```
Router#show ip access-lists extACL
Extended IP access list extACL
  10 permit ip host 10.10.10.11 host 20.20.20.21 log (2 matches)
Router#
```

실습5. Extended ACL - SSH차단

조건

- 실습4에서 생성한 ACL에서 PC1(10.10.10.11)에서 Server1로 SSH 통신 차단하는 엔트리를 추가합니다
 - sequence number:5, protocol: TCP, source: 10.10.10.11, destination: 20.20.20.21, destination port: 22
- Hint: p.53, 55

확인

- PC1에서 Server1으로 핑 성공(ping 20.20.20.21)
- PC1에서 Server1으로 SSH 실패(ssh cisco@20.20.20.21)
- Router에서 show ip access-lists extACL 명령어로 증가된 카운터 확인

실습5. Extended ACL - SSH차단 (답)

```
Router(config)#ip access-list extended extACL  
Router(config-ext-nacl)#5 deny tcp host 10.10.10.11 host 20.20.20.21 eq 22
```

```
Router#show ip access-lists extACL  
Extended IP access list extACL  
    5 deny tcp host 10.10.10.11 host 20.20.20.21 eq 22 (1 match)  
    10 permit ip host 10.10.10.11 host 20.20.20.21 log (51 matches)  
Router#
```

실습6. Extended ACL 엔트리 추가

조건

- 실습4에서 생성한 ACL에서 10.10.10.0/24 대역이 모두 대상으로 ping 요청을 허용하는 엔트리를 추가합니다.
 - protocol: ICMP, source: 10.10.10.0/24, destination: any, option: echo
- Hint: p.54, 55

확인

- PC2에서 Server1으로 핑 성공(ping 20.20.20.21)
- PC2에서 Server1으로 SSH 실패(ssh cisco@20.20.20.21)
- Router에서 show ip access-lists extACL 커맨드 확인 시 카운터 증가

실습6. Extended ACL 엔트리 추가 (답)

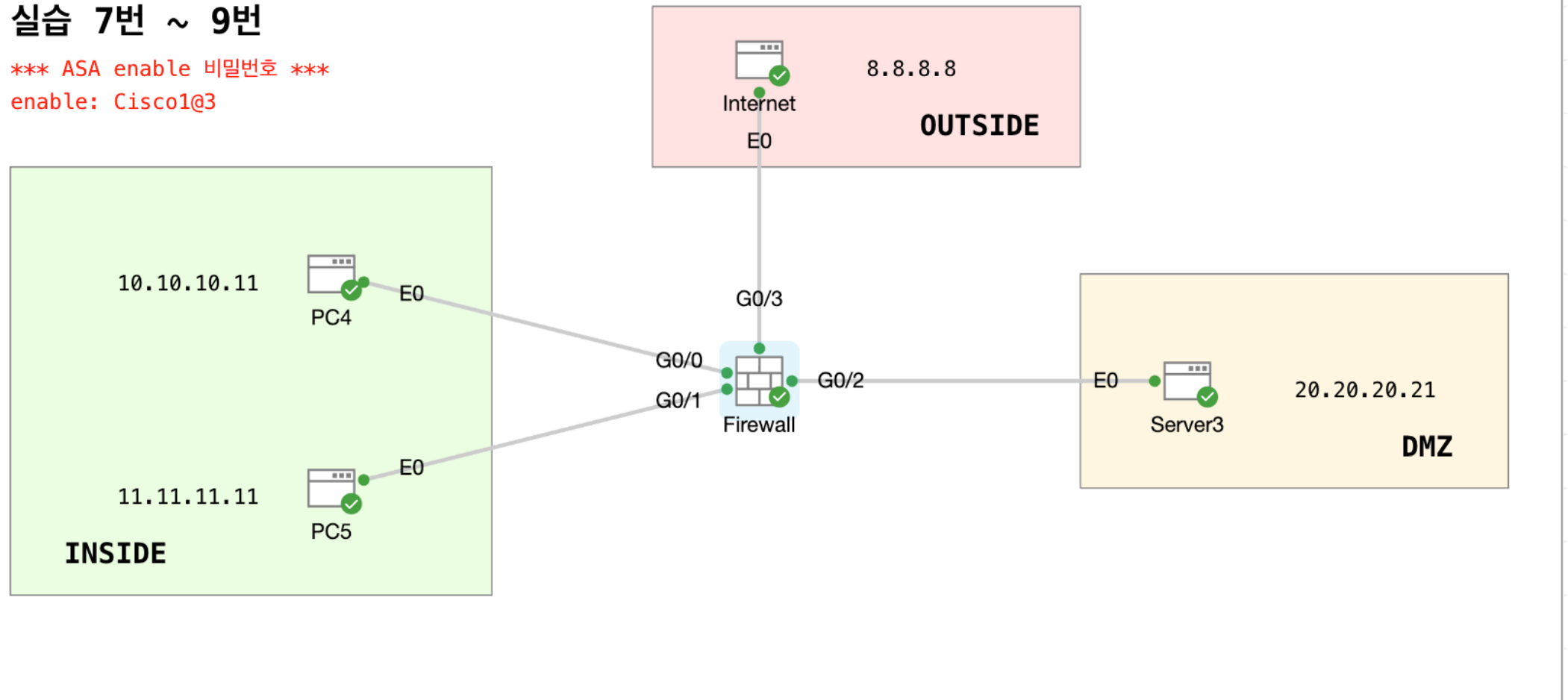
```
Router(config)#ip access-list extended extACL  
Router(config-ext-nacl)#permit ICMP 10.10.10.0 0.0.0.255 any echo
```

```
Router#show ip access-lists extACL  
Extended IP access list extACL  
  5 deny tcp host 10.10.10.11 host 20.20.20.21 eq 22 (1 match)  
 10 permit ip host 10.10.10.11 host 20.20.20.21 log (51 matches)  
 20 permit icmp 10.10.10.0 0.0.0.255 any echo (1 match)  
Router#
```

실습 7번 ~ 9번 토폴로지

실습 7번 ~ 9번

*** ASA enable 비밀번호 ***
enable: Cisco1@3



실습7. Security Level 설정 및 확인

조건

- 방화벽과 PC5가 연결된 gi 0/1의 Security level 를 100으로 수정합니다.
- Hint: p.65

접속 및 show 명령어 사용 방법(비밀번호: Cisco1@3)

```
Firewall> enable
Password: *****
Firewall#
Firewall#
Firewall# show run int gi 0/1
```

확인

- PC4(Inside)에서 PC5(Inside) 으로 핑 성공(ping 11.11.11.11)
- PC4 (Inside)에서 Internet(Outside)으로 SSH 접속 성공(ssh cisco@8.8.8.8)
- Internet(Outside) 에서 Server3(DMZ)로 SSH 접속 실패(ssh cisco@20.20.20.21)

실습8. 방화벽 ACL 설정

조건

- Outside에서 DMZ로 SSH 통신 가능하게 하는 ACL 생성, 이때 이름은 test8 사용
 - protocol: TCP, source: 8.8.8.8, destination: any, destination port: ssh
- ACL을 inbound로 outside interface에 적용
- Hint: p.66

확인

- Internet(Outside)에서 Server3(DMZ)로 SSH 통신 성공 (ssh cisco@20.20.20.21)
- Internet(Outside)에서 Server3(DMZ)로 ping 통신 실패 (ping 20.20.20.21)
- Firewall에서 show access-list test8 커맨드 확인 시 카운터 증가

실습8. 방화벽 ACL 설정 (답)

```
Firewall(config)# access-list test8 extended permit tcp host 8.8.8.8 any eq ssh log  
Firewall(config)# access-group test8 in interface outside  
Firewall(config)#
```

```
Firewall# show access-list test8  
access-list test8; 1 elements; name hash: 0x135a5213  
access-list test8 line 1 extended permit tcp host 8.8.8.8 any eq ssh log informational interval 300  
(hitcnt=1) 0x3d3fc857  
Firewall#
```

실습9. Global ACL 설정

조건

- Outside에서 DMZ로 구간(실습8)을 제외한 모든 구간의 SSH를 차단하는 ACL 생성, 이때 이름은 test9 사용
 - protocol: TCP, source: any, destination: any, destination port: SSH
- Global ACL 로 적용합니다.
- Hint: p.69

확인

- PC4(Inside)에서 Internet(Outside)으로 SSH 통신 실패 (ssh cisco@8.8.8.8)
- PC4(Inside)에서 Server3(DMZ)으로 SSH 통신 실패 (ssh cisco@20.20.20.21)
- Server3(DMZ)에서 Internet(Outside)로 SSH 통신 실패 (ssh cisco@8.8.8.8)
- Internet(Outside)에서 Server3(DMZ)로 SSH 통신 성공 (ssh cisco@20.20.20.21)
- Firewall에서 show access-lists test9 커맨드 확인 시 카운터 증가

실습9. Global ACL 설정 (답)

```
Firewall(config)# access-list test9 extended deny tcp any any eq ssh  
Firewall(config)# access-group test9 global
```

```
Firewall(config)# show access-list test9  
access-list test9; 1 elements; name hash: 0x2f3bca52  
access-list test9 line 1 extended deny tcp any any eq ssh (hitcnt=2) 0xe99392ba  
Firewall(config)#
```



The bridge to possible