YEOKSAM
INSTITUTE
TECHNOLOGY

-네트워크 인프라 구축 및 보안 프로젝트-

SUN 교사
이남혁
이정훈
강버들
백정이
장성주
전보라

목차

1. 프로젝트 개요

1.프로젝트 개요

구축 목적

1

내부망 기반의 안정적 네트워크 인프라 구축

사무동·강의동·서버존 등 각 구역을 분리하여 통신 충돌 없이 안정적으로 연결되는 내부망 환경 설계

2

DNS·FTP·TFTP 서비스 서버 직접 운영

DNS·FTP·TFTP 서비스를 사용자들이 내부망 내에서 도메인 조회, 파일 전송, 네트워크 장비 백업 관리가 가능한 자체 서비스 구축 및 운영

3

권한 관리 체계 확립

사용자와 그룹 별 접근 권한을 구분하여 불필요한 접근을 제한 및 관리 효율성을 향상

4

보안 정책 관리 및 강화

방화벽 설정과 설정 파일 값을 통해 공격자의 침입을 차단하고 안전한 서비스 운영을 유지

1.프로젝트 개요

구축 목표

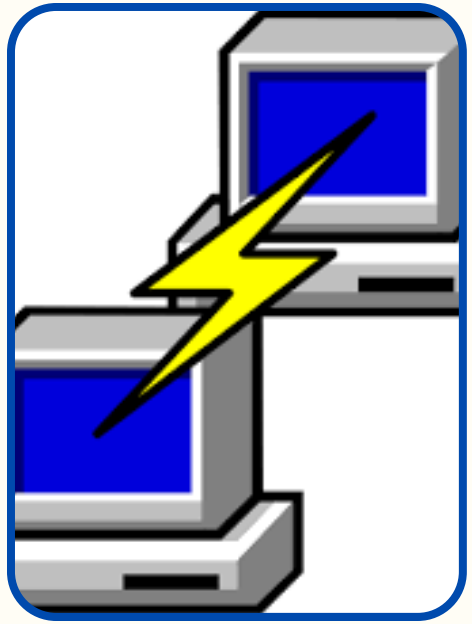
역삼공과대학교 내부망 보안

네트워크 설계 및 서비스 운영

1.프로젝트 개요

수행 환경

- VMWARE 17.X
- ROCKY LINUX 8.10
- KALI LINUX (DEBIAN 10.X)
- PACKET TRACER 8.2.2
- GNS3 1.5.3
- PUTTY RELEASE 0.83



2. 팀원 및 파트 소개

2. 팀원 및 파트 소개

시스템 구축	네트워크 설계	보안 정책	서비스 운영	통합 관리
강버들 장성주	백정이 이남혁 장성주	이정훈 전보라	백정이 이남혁	이정훈 전보라

3. 파트 별 작업 소개

3. 파트 별 작업 소개

시스템 구축

3. 파트 별 작업 소개 - 시스템 구축

설치 환경 & 사양

항목	내용
OS 버전	Rocky Linux 8.10
ISO 파일	Rocky-8.10-x86_64-dvd1.iso
디스크	20GB
메모리	4GB

VMnet 구성

이름	할당 PC	타입	DHCP	대역	서브넷 마스크
VMnet1	FTP 서버	Host-only	X	63.63.63.0	255.255.255.248
VMnet2	TFTP 서버	Host-only	X	63.63.63.8	255.255.255.248
VMnet3	DNS 서버	Host-only	X	63.63.63.16	255.255.255.248
VMnet8	외부 통신	NAT	O	192.168.10.0	255.255.255.0

3. 파트 별 작업 소개 - 시스템 구축

파티션

적재 지점	용량	파일시스템
/boot	1G	ext4
/home	1G	ext4
/var	4G	ext4
/usr	7G	ext4
swap	2G	swap
/	5G	ext4

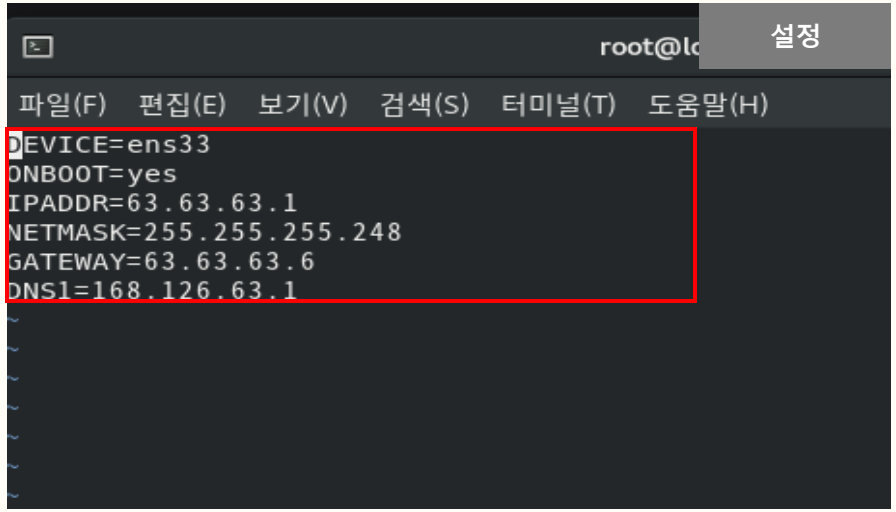
설치 과정 설정

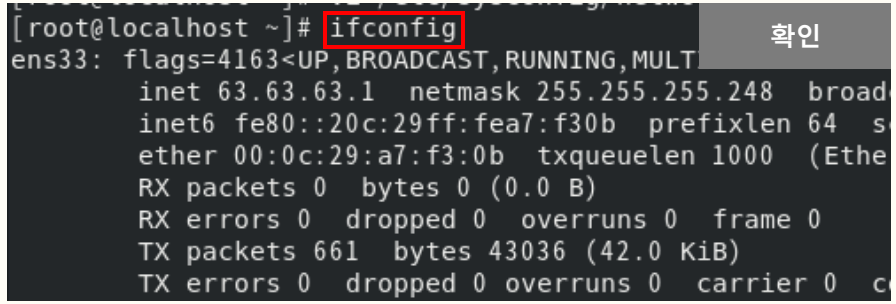
구분	설정 값
설치 목적지	수동 파티션 구성
네트워크	ON / DHCP 자동 할당
소프트웨어 선택	서버 GUI + 레거시 UNIX 호환성
사용자 생성	admin + root 설정
SELinux 모드	disabled

3. 파트 별 작업 소개 - 시스템 구축

네트워크 초기 설정

서비스	FTP	TFTP	DNS
버전	vsftpd-3.0.3-36.el8 .x86_64	ftp-server-5.2-27.el8 .x86_64	bind-9.11.36-16.el8_10.4 .x86_64
ens33 설정	DEVICE=ens33 ONBOOT=yes IPADDR=63.63.63.1 NETMASK =255.255.255.248 GATEWAY=63.63.63.6 DNS1=168.126.63.1	DEVICE=ens33 ONBOOT=yes IPADDR=63.63.63.9 NETMASK =255.255.255.248 GATEWAY=63.63.63.14 DNS1=168.126.63.1 DNS2=3.3.3.30	DEVICE=ens33 ONBOOT=yes IPADDR=63.63.63.17 NETMASK =255.255.255.248 GATEWAY=63.63.63.22 DNS1=168.126.63.1





3. 파트 별 작업 소개 - 시스템 구축

FTP-계정

순번	계정	소속 그룹	보조 그룹	UID
1	admin	admin	-	1000
2	stud1	students	-	1001
3	stud2	students	-	1002
4	profe1	professors	-	1003
5	profe2	professors	-	1004
6	mana1	managers	-	1005
7	mana2	managers	-	1006
8	admis1	admissions	-	1007
0	admis2	admissions	-	1008

3. 파트 별 작업 소개 - 시스템 구축

FTP - 그룹

순번	그룹	GID
1	admin	1000
2	students	1001
3	professors	1002
4	managers	1003
5	admissions	1004

FTP 디렉터리 권한

디렉터리	경로	권한	소유자:그룹
college	/college	755	root:root
ftp	/college/ftp	2775	admin:ftp
professor	/college/ftp/professor	2774	admin:professors
student	/college/ftp/student	774	admin:students
manage	/college/ftp/manage	2754	admin:managers
admission	/college/ftp/admission	2774	admin:admissions

3. 파트 별 작업 소개 - 시스템 구축

FTP - 설정

계정

```
[root@localhost ~]# tail -9 /etc/passwd
admin:x:1000:1000:admin:/home/admin:/bin/bash
stud1:x:1001:1001::/home/stud1:/bin/bash
stud2:x:1002:1001::/home/stud2:/bin/bash
profe1:x:1003:1002::/home/profe1:/bin/bash
profe2:x:1004:1002::/home/profe2:/bin/bash
mana1:x:1005:1003::/home/mana1:/bin/bash
mana2:x:1006:1003::/home/mana2:/bin/bash
admis1:x:1007:1004::/home/admis1:/bin/bash
admis2:x:1008:1004::/home/admis2:/bin/bash
[root@localhost ~]#
```

디렉터리

```
[root@localhost ~]# tree /college
/college
└── ftp
    ├── admssion
    ├── manage
    ├── professor
    └── student

5 directories, 0 files
[root@localhost ~]#
```

그룹

```
[root@localhost ~]# tail -5 /etc/group
admin:x:1000:
students:x:1001:
professors:x:1002:
managers:x:1003:
admissions:x:1004:
[root@localhost ~]#
```

권한

```
[root@localhost ftp]# ls -l / | grep college
drwxr-xr-x    3 root root  4096 10월  25 10:32 college
[root@localhost ftp]# ls -l /college | grep ftp
drwxrwsr-x 6 admin ftp 4096 10월  25 10:54 ftp
[root@localhost ftp]# ls -l /college/ftp | grep -E "admission|manage|professor|student"
drwxrwsr-- 2 admin admissions 4096 10월  25 10:54 admssion
drwxr-sr-- 2 admin managers   4096 10월  25 10:53 manage
drwxrwsr-- 2 admin professors 4096 10월  25 10:32 professor
drwxrwxr-- 3 admin students   4096 10월  28 03:09 student
[root@localhost ftp]#
```

3. 파트 별 작업 소개 - 시스템 구축

TFTP - 그룹

순번	그룹	GID
1	admin	1000
2	tftp	1001
3	Netengineer	1002

TFTP - 계정

순번	계정	소속 그룹	보조 그룹	UID
1	admin	admin	-	1000
2	admin1	admin	tftp	1001
3	net1	netengineer	tftp	1002
4	net2	netengineer	tftp	1003

3. 파트 별 작업 소개 - 시스템 구축

DNS - 그룹

순번	그룹	GID
1	admin	1000
2	netengineer	1001
3	dns	1002

DNS - 계정

순번	계정	소속 그룹	보조 그룹	UID
1	admin	admin	-	1000
2	admin1	admin	dns	1001
3	net1	netengineer	dns	1002
4	net2	netengineer	dns	1003

3. 파트 별 작업 소개 - 시스템 구축

DNS 권한 결과

```
[root@localhost ~]# tail -5 /etc/passwd
admin:x:1000:1000:admin:/home/admin:/bin/bash
named:x:25:25:Named:/var/named:/bin/false
admin1:x:1001:1000::/home/admin1:/bin/bash
net1:x:1002:1001::/home/net1:/bin/bash
net2:x:1003:1001::/home/net2:/bin/bash
[root@localhost ~]#
```

```
[root@localhost ~]# tail -4 /etc/group
admin:x:1000:
named:x:25:
netengineer:x:1001:
dns:x:1002:admin1,net1,net2
[root@localhost ~]#
```

TFTP 권한 및 디렉터리 결과

```
[root@localhost ~]# tail -4 /etc/passwd
admin:x:1000:1000:admin:/home/admin:/bin/bash
admin1:x:1001:1000::/home/admin1:/bin/bash
net1:x:1002:1002::/home/net1:/bin/bash
net2:x:1003:1002::/home/net2:/bin/bash
[root@localhost ~]#
```

```
[root@localhost ~]# tail -3 /etc/group
admin:x:1000:
tftp:x:1001:admin1,net1,net2
netegineer:x:1002:
[root@localhost ~]#
```

```
[root@localhost ~]# tree /tftp
/tftp

0 directories, 0 files
[root@localhost ~]#
```

```
[root@localhost ~]# ls -l / | grep tftp
drwxrwxr-x    2 admin tftp  4096 10월  25 11:32 tftp
[root@localhost ~]#
```

3. 파트 별 작업 소개

네트워크 설계

3. 파트 별 작업 소개 - 네트워크 설계

외부 인터넷

구분	네트워크 대역	장비	IP 주소	설명
외부 게이트웨이	203.0.113.0/30	R4-ISP Router	**R4** 203.0.113.2 **ISP** 203.0.113.1	전체 트래픽 최종 출구

사무동(관리부 & 입학 센터) - PAT

구분	내부 네트워크 대역	NAT 공인 대역	게이트웨이	비고
관리부	10.0.1.64/28	1.1.1.0/30	10.0.1.78	2층 관리부
입학 센터	10.0.1.80/28	1.1.1.0/30	10.0.1.94	1층 입학 센터

3. 파트 별 작업 소개 - 네트워크 설계

서버 존 (Static NAT)

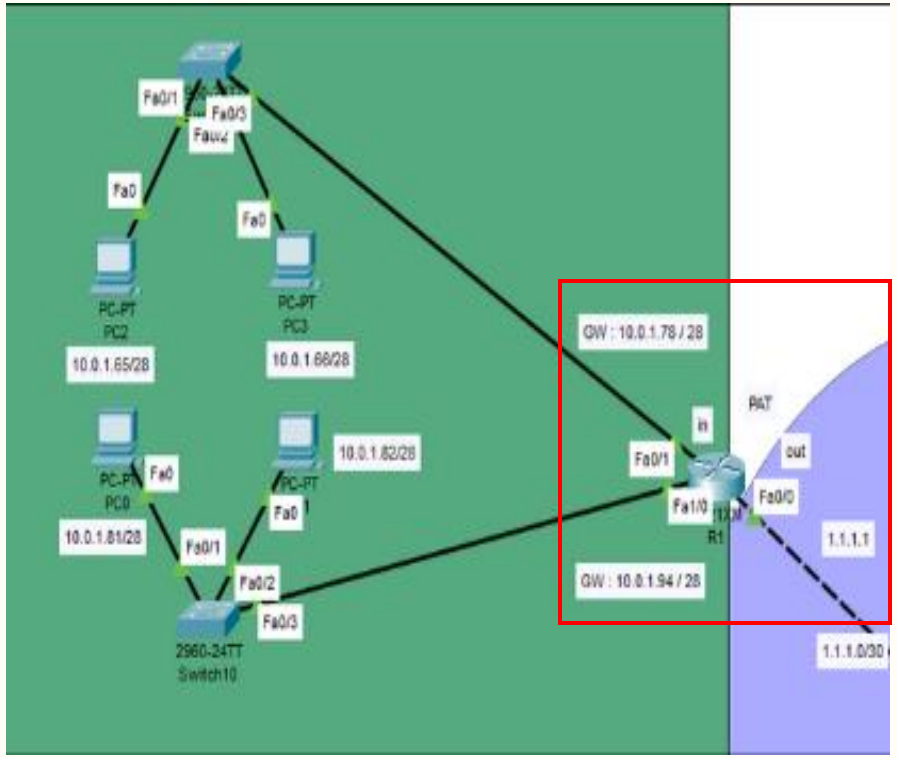
구분	내부 IP	공인 IP	비고
FTP 서버	63.63.63.1/29	3.3.3.10	DB 및 문서 파일 저장
TFTP 서버	63.63.63.9/29	3.3.3.20	장비 설정 파일 관리
DNS 서버	63.63.63.17/29	3.3.3.30	내부 DNS 서비스

강의동 (교수실 & 강의실) - PAT

구분	내부 네트워크 대역	NAT 공인 대역	게이트웨이	비고
3층 교수실	192.168.53.0/27	2.2.2.0/30	192.168.53.1	게임/보안/디자인/IT
2층 C·D 강의실	192.168.53.64/26	2.2.2.0/30	192.168.53.65	실습 강의실
1층 A·B 강의실	192.168.53.128/26	2.2.2.0/30	192.168.53.129	실습 강의실

3. 파트 별 작업 소개 - 네트워크 설계

사무동 네트워크



네트워크 대역 할당 이유

필요한 만큼만 할당하고, 불필요한 낭비를 줄인 효율적 설계

NAT 방식 : PAT

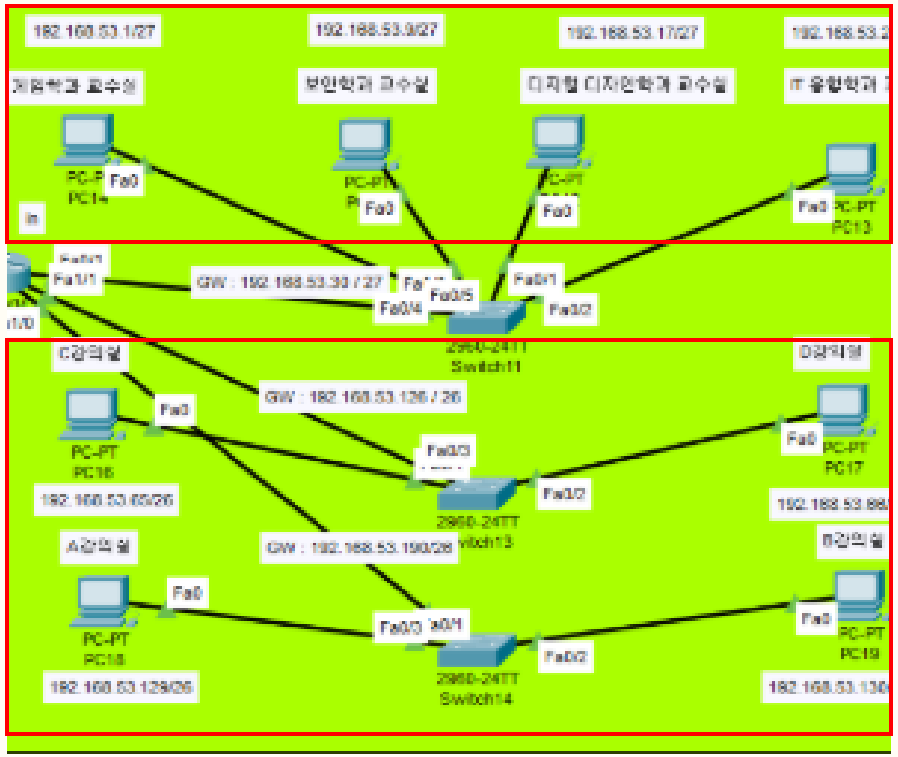
한정된 공인 IP 자원을 효율적으로 활용하면서도 관리 통제

보안 정책 고려

행정업무 중심의 안정성과 신뢰성을 확보한 네트워크 설계

3. 파트 별 작업 소개 - 네트워크 설계

강의동 네트워크



네트워크 대역 할당 이유

사용자 수가 많아 대역을 넓게 확보하여 IP 충돌 방지 및 관리 효율 향상

NAT 방식 : PAT

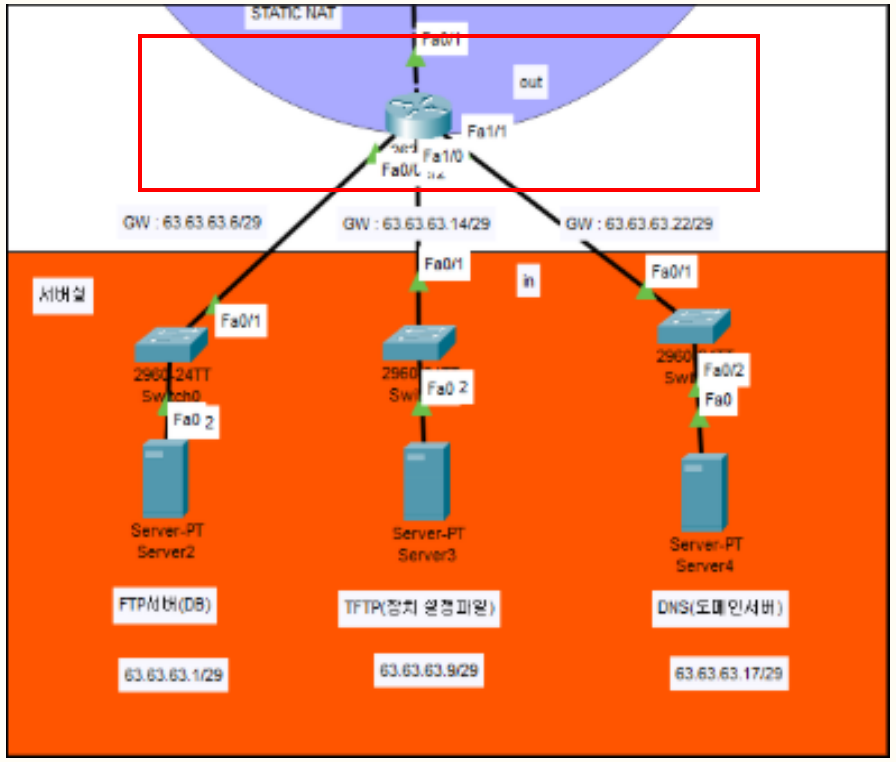
내부 사용자는 개별 IP 유지,
외부엔 단일 IP(2.2.2.2)로 표현되어 공인 IP 자원 절약

보안 정책 고려

실습 중 불필요한 접근을 차단하고 교육망의 안정성 확보

3. 파트 별 작업 소개 - 네트워크 설계

서버존 네트워크



네트워크 대역 할당 이유

서버 별로 독립된 스위치 포트를 구성해
확장성과 유지보수성 확보

NAT 방식 : STATIC NAT

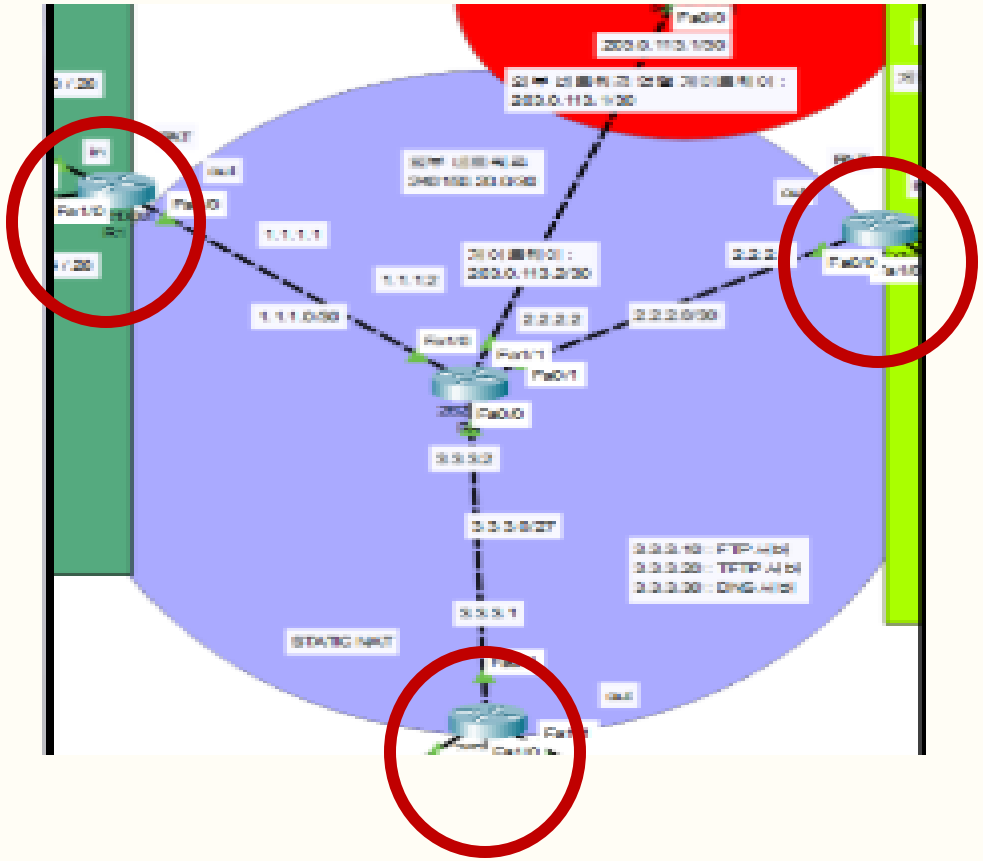
외부에서도 서버 접근이 가능해야 하므로
내부 IP와 공인 IP를 1:1로 고정 매핑

보안 정책 고려

서버 보호 및 침입 위험 최소화

3. 파트 별 작업 소개 - 네트워크 설계

NAT 설정 / 외부 인터넷 연결



NAT 라우터 설계 이유

학교 전체의 인터넷 출구 게이트웨이

NAT 및 라우팅 구조

공인 IP를 단일화해 관리 효율과 보안성 확보

보안 정책 고려

외부에서 내부로 직접 접근 불가
* 모든 통신은 NAT를 거쳐야 함

3. 파트 별 작업 소개

보안 정책

3. 파트 별 작업 소개 - 보안 정책

firewalld 설정

항목	명령어	설명
FTP 서버	firewall-cmd --permanent --add-port=21/tcp	FTP 포트 허용 추가
	firewall-cmd --permanent --add-service=ftp	FTP 서비스 허용 추가
TFTP 서버	firewall-cmd --permanent --add-port=69/udp	TFTP 포트 허용 추가
	firewall-cmd --permanent --add-service=tftp	TFTP 서비스 허용 추가
DNS 서버	firewall-cmd --permanent --add-service=dns	DNS 서비스 허용 추가
	firewall-cmd --permanent --add-port=53/udp firewall-cmd --permanent --add-port=53/tcp	DNS 포트 허용 추가
공통 적용 사항	firewall-cmd --permanent --add-port=22/tcp firewall-cmd --permanent --add-service=ssh	SSH 포트 및 서비스 허용 추가
	firewall-cmd --permanent --add-icmp-block={echo-request,echo-reply,timestamp-reply,timestamp-request}	ICMP 메세지 차단
	firewall-cmd --permanent --direct --add-rule ipv4 filter OUTPUT 0 -p icmp --icmp-type 3 -j DROP	ICMP Type 3 관련 규칙 추가

3. 파트 별 작업 소개 - 보안 정책

firewalld 활성화

```
┌──(root㉿kali)-[~]
└─# nmap -sA -p 20-30 3.3.3.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-27 15:27 KST
Note: Host seems down. If it is really up, but blocking our ping probes, try
-Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.07 seconds
```

kali (공격자)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	ca:03:19:84:00:3b	ca:03:19:84:00:3b	LOOP	60	Reply
2	0.038874	20.20.20.20	3.3.3.10	ICMP	60	Echo (ping) request id=0x0907, seq=0/0,
3	0.038989	20.20.20.20	3.3.3.10	TCP	60	62051 → 443 [SYN] Seq=0 Win=1024 Len=0
4	0.039020	20.20.20.20	3.3.3.10	TCP	60	62051 → 80 [ACK] Seq=1 Ack=1 Win=1024 Le
5	0.039040	20.20.20.20	3.3.3.10	ICMP	60	Timestamp request id=0x4033, seq=0/0,
6	2.041573	20.20.20.20	3.3.3.10	ICMP	60	Timestamp request id=0xfbb1, seq=0/0, ttl=37
7	2.041626	20.20.20.20	3.3.3.10	TCP	60	62053 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
8	2.041647	20.20.20.20	3.3.3.10	TCP	60	62053 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9	2.041666	20.20.20.20	3.3.3.10	ICMP	60	Echo (ping) request id=0x06ba, seq=0/0, ttl=54 (no response found!)
10	5.174403	VMware_42:10:eb	ca:03:19:84:00:3b	ARP	60	Who has 20.20.20.254? Tell 20.20.20.20

서버 (희생자)

tcp_ack_ftp.pcapng

파일(F) 편집(E) 보기(V) 이동(G) 캡처(C) 분석(A) 통계(S) 전화(Y) 무선(W) 도구(T) 도움말(H)

표시 필터 적용 … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Lengt	Info
1	0.000000	1.1.1.1	63.63.63.1	ICMP	42	Echo (ping) request id=0x0907, seq=0/0, ttl=53 (no response found!)
2	0.000037	1.1.1.1	63.63.63.1	TCP	58	62051 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3	0.000054	1.1.1.1	63.63.63.1	TCP	54	62051 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
4	0.000142	1.1.1.1	63.63.63.1	ICMP	54	Timestamp request id=0x4033, seq=0/0, ttl=37
5	2.012284	1.1.1.1	63.63.63.1	ICMP	54	Timestamp request id=0xfbb1, seq=0/0, ttl=34
6	2.012396	1.1.1.1	63.63.63.1	TCP	54	62053 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
7	2.012437	1.1.1.1	63.63.63.1	TCP	58	62053 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
8	2.012462	1.1.1.1	63.63.63.1	ICMP	42	Echo (ping) request id=0x06ba, seq=0/0, ttl=51 (no response found!)

Ping 확인

```
PC1> ping 3.3.3.10
84 bytes from 3.3.3.10 icmp_seq=1 ttl=61 time=92.902 ms
84 bytes from 3.3.3.10 icmp_seq=2 ttl=61 time=94.155 ms
84 bytes from 3.3.3.10 icmp_seq=3 ttl=61 time=93.889 ms
84 bytes from 3.3.3.10 icmp_seq=4 ttl=61 time=91.744 ms
84 bytes from 3.3.3.10 icmp_seq=5 ttl=61 time=93.896 ms

PC1>
PC1> ping 3.3.3.10
3.3.3.10 icmp_seq=1 timeout
3.3.3.10 icmp_seq=2 timeout
3.3.3.10 icmp_seq=3 timeout
3.3.3.10 icmp_seq=4 timeout
3.3.3.10 icmp_seq=5 timeout

PC1>
```

```
  rich rules:
[root@localhost ~]# service firewalld stop
Redirecting to /bin/systemctl stop firewalld.service
[root@localhost ~]# service firewalld start
Redirecting to /bin/systemctl start firewalld.service
[root@localhost ~]#
```

3. 파트 별 작업 소개 - 보안 정책

firewalld 비활성화

kali (공격자)

tcp_ack_kali(ftp)_방화벽x.pcapng

파일(F) 편집(E) 보기(V) 이동(G) 캡처(C) 분석(A) 통계(S) 전화(Y) 무선(W) 도구(T) 도움말(H)

표시 필터 적용 … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Lengt	Info
19	0.506804	20.20.20.20	3.3.3.10	TCP	60	45529 → 20 [ACK] Seq=1 Ack=1 Win=1024 Len=0
20	0.506831	20.20.20.20	3.3.3.10	TCP	60	45529 → 30 [ACK] Seq=1 Ack=1 Win=1024 Len=0
21	0.506850	20.20.20.20	3.3.3.10	TCP	60	45529 → 28 [ACK] Seq=1 Ack=1 Win=1024 Len=0
22	0.587072	3.3.3.10	20.20.20.20	TCP	54	23 → 45529 [RST] Seq=1 Win=0 Len=0
23	0.587085	3.3.3.10	20.20.20.20	TCP	54	25 → 45529 [RST] Seq=1 Win=0 Len=0
24	0.587106	3.3.3.10	20.20.20.20	TCP	54	22 → 45529 [RST] Seq=1 Win=0 Len=0
25	0.587114	3.3.3.10	20.20.20.20	TCP	54	26 → 45529 [RST] Seq=1 Win=0 Len=0
26	0.587116	3.3.3.10	20.20.20.20	TCP	54	27 → 45529 [RST] Seq=1 Win=0 Len=0
27	0.587118	3.3.3.10	20.20.20.20	TCP	54	29 → 45529 [RST] Seq=1 Win=0 Len=0
28	0.587120	3.3.3.10	20.20.20.20	TCP	54	20 → 45529 [RST] Seq=1 Win=0 Len=0
29	0.587123	3.3.3.10	20.20.20.20	TCP	54	30 → 45529 [RST] Seq=1 Win=0 Len=0
30	0.587125	3.3.3.10	20.20.20.20	TCP	54	28 → 45529 [RST] Seq=1 Win=0 Len=0

서버 (희생자)

tcp_ack_ftp_방화벽x.pcapng

파일(F) 편집(E) 보기(V) 이동(G) 캡처(C) 분석(A) 통계(S) 전화(Y) 무선(W) 도구(T) 도움말(H)

표시 필터 적용 … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Lengt	Info
7	0.000370	1.1.1.1	63.63.63.1	ICMP	54	Timestamp request id=0x6e84, seq=0/0, ttl=54
8	0.000515	63.63.63.1	1.1.1.1	ICMP	60	Timestamp reply id=0x6e84, seq=0/0, ttl=64
9	0.201216	1.1.1.1	63.63.63.1	TCP	54	45529 → 23 [ACK] Seq=1 Ack=1 Win=1024 Len=0
10	0.201313	63.63.63.1	1.1.1.1	TCP	60	23 → 45529 [RST] Seq=1 Win=0 Len=0
11	0.201339	1.1.1.1	63.63.63.1	TCP	54	45529 → 25 [ACK] Seq=1 Ack=1 Win=1024 Len=0
12	0.201477	63.63.63.1	1.1.1.1	TCP	60	25 → 45529 [RST] Seq=1 Win=0 Len=0
13	0.201481	1.1.1.1	63.63.63.1	TCP	54	45529 → 22 [ACK] Seq=1 Ack=1 Win=1024 Len=0
14	0.201563	63.63.63.1	1.1.1.1	TCP	60	22 → 45529 [RST] Seq=1 Win=0 Len=0
15	0.201604	1.1.1.1	63.63.63.1	TCP	54	45529 → 26 [ACK] Seq=1 Ack=1 Win=1024 Len=0
16	0.201721	1.1.1.1	63.63.63.1	TCP	54	45529 → 27 [ACK] Seq=1 Ack=1 Win=1024 Len=0
17	0.201731	63.63.63.1	1.1.1.1	TCP	60	26 → 45529 [RST] Seq=1 Win=0 Len=0
18	0.201768	63.63.63.1	1.1.1.1	TCP	60	27 → 45529 [RST] Seq=1 Win=0 Len=0
19	0.201829	1.1.1.1	63.63.63.1	TCP	54	45529 → 29 [ACK] Seq=1 Ack=1 Win=1024 Len=0
20	0.201946	1.1.1.1	63.63.63.1	TCP	54	45529 → 20 [ACK] Seq=1 Ack=1 Win=1024 Len=0
21	0.201984	63.63.63.1	1.1.1.1	TCP	60	29 → 45529 [RST] Seq=1 Win=0 Len=0

```
┌──(root㉿kali)-[~]
└─# nmap -sA -p 20-30 3.3.3.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-27 15:33 KST
Nmap scan report for 3.3.3.10
Host is up (0.085s latency).

PORT   STATE      SERVICE
20/tcp unfiltered ftp-data
21/tcp unfiltered ftp
22/tcp unfiltered ssh
23/tcp unfiltered telnet
24/tcp unfiltered priv-mail
25/tcp unfiltered smtp
26/tcp unfiltered rsftp
27/tcp unfiltered nsw-fe
28/tcp unfiltered unknown
29/tcp unfiltered msg-icp
30/tcp unfiltered unknown

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
```

3. 파트 별 작업 소개 - 보안 정책

설정 파일 적용

파일	설정 값	설명
/etc/ssh/sshd_config	AllowGroups admin	SSH 접속 허용 그룹 지정
	PermitRootLogin no	관리자 계정의 SSH 직접 접근 차단 설정
	PasswordAuthentication yes	SSH 접속 시 사용자 인증을 위해 비밀번호 입력 설정
/etc/vsftpd/vsftpd.conf	userlist_file=/etc/vsftpd/user_list	userlist 파일 경로 지정
	userlist_enable=YES	userlist 파일에 있는 사용자 목록 허용 설정
	userlist_deny=NO	
/etc/crontab	* 0 9 * * 1 root find / -xdev ₩(-nouser -o -nogroup ₩) -exec chown root:root {} ₩; > > /var/log/cron_fix.log 2> &1	소유자 또는 소유 그룹이 없는 파일/디렉터리의 소유자 및 소유 그룹을 관리자로 자동 변경 설정
/etc/login.defs	PASS_MAX_DAYS 90	비밀번호 최대 사용 일을 90일로 지정
	PASS_MIN_DAYS 1	비밀번호 최소 사용 일을 1일로 지정
	PASS_MIN_LEN 10	비밀번호 최소 길이를 10으로 지정
	PASS_WARN_AGE 7	비밀번호 만료 전 경고 표시 일을 7일로 지정

3. 파트 별 작업 소개 - 보안 정책

설정 파일 적용 (서비스 접속 확인)

FTP

```
[root@localhost ~]# ftp 63.63.63.1
Connected to 63.63.63.1 (63.63.63.1).
220 (vsFTPd 3.0.3)
Name (63.63.63.1:root): root
530 Permission denied.
Login failed.
ftp> quit
221 Goodbye.
[root@localhost ~]# ftp 63.63.63.1
Connected to 63.63.63.1 (63.63.63.1).
220 (vsFTPd 3.0.3)
Name (63.63.63.1:root): admin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 Entering Passive Mode (63,63,63,1,113,119).
150 Here comes the directory listing.
drwxrwsr-x    2 1000     1004         4096 Oct 25 01:54 admssion
drwxrwsr-x    2 1000     1003         4096 Oct 25 01:53 manage
drwxrwsr-x    2 1000     1002         4096 Oct 25 01:32 professor
drwxrwsr-x    2 1000     1001         4096 Oct 25 01:34 student
226 Directory send OK.
ftp> quit
221 Goodbye.
[root@localhost ~]#
```

SSH

```
[admin@localhost ~]$ ssh root@63.63.63.1
The authenticity of host '63.63.63.1 (63.63.63.1)' can't be established.
ECDSA key fingerprint is SHA256:+sbOCt6b84YYrqR9PN6ZBgNynoup6brIs9KbvRxxR3I.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '63.63.63.1' (ECDSA) to the list of known hosts.

root@63.63.63.1's password:
root@63.63.63.1: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,passw
ord).
[admin@localhost ~]$ ssh admin@63.63.63.1
admin@63.63.63.1's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Mon Oct 27 01:22:14 2025 from 63.63.63.9
[admin@localhost ~]$ exit
logout
Connection to 63.63.63.1 closed.
[admin@localhost ~]$ ssh admis1@63.63.63.1
admis1@63.63.63.1's password:
Permission denied, please try again.
admis1@63.63.63.1's password:
Permission denied, please try again.
admis1@63.63.63.1's password:
admis1@63.63.63.1: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,pas
sword).
[admin@localhost ~]$
```

3. 파트 별 작업 소개 - 보안 정책

설정 파일 적용 (계정 및 파일 관련)

계정 생성

```
[root@localhost ~]# useradd test
[root@localhost ~]# tail -1 /etc/shadow
test:!!:20388:1:90:7:::
[root@localhost ~]#
```

파일 권한 변경

```
[root@localhost ~]# mkdir /test
[root@localhost ~]# echo "test" > /test/test.txt
[root@localhost ~]# cat /test/test.txt
test
[root@localhost ~]# ls -al /test
합계 12
drwxr-xr-x   2 root root 4096 10월  28 00:09 .
dr-xr-xr-x. 20 root root 4096 10월  28 00:09 ..
-rw-r--r--   1 root root    5 10월  28 00:09 test.txt
[root@localhost ~]# chown test:test /test
[root@localhost ~]# chown test:test /test/test.txt
[root@localhost ~]# ls -al /test
합계 12
drwxr-xr-x   2 test test 4096 10월  28 00:09 .
dr-xr-xr-x. 20 root root 4096 10월  28 00:09 ..
-rw-r--r--   1 test test    5 10월  28 00:09 test.txt
[root@localhost ~]#
```

소유권 변경 확인

```
[root@localhost ~]# userdel -r test
[root@localhost ~]# ls -al /test
합계 12
drwxr-xr-x   2 1009 1009 4096 10월  28 00:09 .
dr-xr-xr-x. 20 root root 4096 10월  28 00:09 ..
-rw-r--r--   1 1009 1009    5 10월  28 00:09 test.txt
[root@localhost ~]# find / -xdev \( -nouser -o -nogroup \) -exec chown root
:root {} \; >> /var/log/cron_fix.log 2>&1
[root@localhost ~]# ls -al /test
합계 12
drwxr-xr-x   2 root root 4096 10월  28 00:09 .
dr-xr-xr-x. 20 root root 4096 10월  28 00:09 ..
-rw-r--r--   1 root root    5 10월  28 00:09 test.txt
[root@localhost ~]#
[root@localhost ~]# cat /var/log/cron_fix.log
[root@localhost ~]#
```

3. 파트 별 작업 소개 - 보안 정책

sysctl 설정 (시스템의 커널 파라미터 설정)

항목	설정 값	설명
/etc/sysctl.conf	net.ipv4.conf.all.accept_redirects = 0	ICMP 리다이렉트 차단(ICMP Redirect 공격 대응)
	net.ipv4.conf.all.send_redirects = 0	ICMP Redirect 송신 차단
	net.ipv4.tcp_syncookies = 1	SYN Cookies 활성화 (TCP SYN Flooding 공격 대응)
	net.ipv4.conf.all.rp_filter = 1 net.ipv4.conf.default.rp_filter = 1	역방향 경로 필터링 활성화 (IP Spoofing 공격 대응)

3. 파트 별 작업 소개

서비스 운영

3. 파트 별 작업 소개 - 서비스 운영

firewalld 설정

작업	명령어	설명
vsftpd 설치	dnf install -y vsftpd	FTP 서버 설치
데몬 즉시 시작	systemctl start vsftpd	서비스 시작
서비스 활성화 (부팅 시 자동)	systemctl enable vsftpd	자동 실행
데몬 재시작	systemctl restart vsftpd	변경 적용
서비스 상태 확인	systemctl status vsftpd	로그·상태 확인

방화벽 설정

작업	명령어	설명
FTP 서비스 허용	firewall-cmd --permanent --add-service=ftp	FTP 서비스 자동 등록
패시브 포트 허용(선택)	firewall-cmd --permanent --add-port=50000-50005/tcp	자동 추적 없을 경우 허용
방화벽 적용	firewall-cmd --reload	규칙 반영

3. 파트 별 작업 소개 - 서비스 운영

vsftpd.conf 주요 옵션 설정

항목	설정 내용	설명
익명 로그인 제한	anonymous_enable=NO	보안 강화
로컬 계정 허용	local_enable=YES	/etc/passwd 등록 계정
쓰기 허용	write_enable=YES	업로드/삭제 허용
사용자 루트 제한	chroot_local_user=YES	탈출 방지
쓰기 가능 루트 디렉터리 접근 허용	allow_writeable_chroot=YES	보안 주의
로그인 홈 지정	local_root=/college/ftp	로그인 시 위치
패시브 모드 설정	pasv_enable=YES pasv_min_port=50000(선택) pasv_max_port=50005(선택)	패시브 on 기준
SSL (선택)	ssl_enable=YES	TLS 암호화, 키/인증서 필요

3. 파트 별 작업 소개 - 서비스 운영

ftp 서버 도메인 접속

```
[root@localhost ~]# ftp ftp.yeoksam.ac.local
Connected to ftp.yeoksam.ac.local (3.3.3.10).
220 (vsFTPd 3.0.3)
Name (ftp.yeoksam.ac.local:root): profe1
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> _
```

```
ftp> cd student
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
student.txt
226 Directory send OK.
ftp: 0.00초 16000.00KB/초
ftp> delete student.txt
550 Delete operation failed.
```

디렉터리 파일 업로드 성공

professor

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
admssion
manage
professor
student
226 Directory send OK.
ftp: 0.00초 20.50KB/초
ftp> cd professor
250 Directory successfully changed.
ftp> put professor.txt
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
```

3. 파트 별 작업 소개 - 서비스 운영

디렉터리 파일 삭제 실패

student

```
ftp> cd student
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
student.txt
226 Directory send OK.
ftp: 0.00초 16000.00KB/초
ftp> delete student.txt
550 Delete operation failed.
```

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
admssion
manage
professor
student
226 Directory send OK.
ftp: 0.00초 20.50KB/초
ftp> cd professor
250 Directory successfully changed.
ftp> put professor.txt
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
ftp>
```

디렉터리 파일 삭제 성공

professor

```
ftp> pwd
257 "/professor" is the current directory
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
professor.txt
226 Directory send OK.
ftp: 0.00초 18000.00KB/초
ftp> delete professor.txt
250 Delete operation successful.
```

3. 파트 별 작업 소개 - 서비스 운영

루트 → 상위 경로 이동 불가

/college/ftp

```
ftp> pwd
257 "/" is the current directory
ftp> ls
227 Entering Passive Mode (3,3,3,10,82,167).
150 Here comes the directory listing.
drwxrwsr-x    2 1000     1004         4096 Oct 25 01:54 admssion
drwxrwsr-x    2 1000     1003         4096 Oct 25 01:53 manage
drwxrwsrwx    2 1000     1002         4096 Oct 27 16:23 professor
drwxrwsr-x    2 1000     1001         4096 Oct 27 15:45 student
226 Directory send OK.
ftp> cd ..
250 Directory successfully changed.
ftp> ls
227 Entering Passive Mode (3,3,3,10,73,151).
150 Here comes the directory listing.
drwxrwsr-x    2 1000     1004         4096 Oct 25 01:54 admssion
drwxrwsr-x    2 1000     1003         4096 Oct 25 01:53 manage
drwxrwsrwx    2 1000     1002         4096 Oct 27 16:23 professor
drwxrwsr-x    2 1000     1001         4096 Oct 27 15:45 student
226 Directory send OK.
ftp>
```

/var/log/xferlog 에서 로그 기록 확인

xferlog

```
-rw-r--r-- 1 profe1 professors 16 10월  28 01:14 professortest2.txt
[root@localhost professor]#
[root@localhost professor]#
[root@localhost professor]#
[root@localhost professor]#
[root@localhost professor]# cat /var/log/xferlog
Tue Oct 28 01:13:28 2025 1 ::ffff:2.2.2.1 16 /professor/professortest2.txt b _ i r profe1 ftp 0 * c
Tue Oct 28 01:14:59 2025 1 ::ffff:2.2.2.1 16 /professor/professortest2.txt b _ i r profe1 ftp 0 * c
[root@localhost professor]#
```

3. 파트 별 작업 소개 - 서비스 운영

설치 & 서비스 활성화 표

작업	명령어	설명
TFTP 패키지 설치	dnf -y install tftp-server	TFTP 서버 설치
소켓 활성화	systemctl enable tftp.socket	부팅 시 자동 시작
소켓 시작	systemctl start tftp.socket	즉시 실행
상태 확인	systemctl status tftp.socket	동작 확인

설정 수정 표

작업	파일/명령	설명
설정파일 수정	vi /usr/lib/systemd/system/tftp.service	systemd 기준 설정
실행 설정	-s /tftp	상위 디렉터리 접근 차단 / TFTP 루트 디렉터리 지정
쓰기 허용	-c	파일 업로드 허용
보안 옵션	ProtectHome=yesNoNewPrivileges=yes	/home 접근 차단 / 권한상승 방지
설정 반영	systemctl daemon-reload	서비스 설정 갱신
재시작	systemctl restart tftp.socket	소켓 재시작

3. 파트 별 작업 소개 - 서비스 운영

방화벽 설정 표

작업	명령어	설명
TFTP 서비스 허용	firewall-cmd --permanent --add-service=tftp	TFTP 서비스 허용
방화벽 적용	firewall-cmd --reload	규칙 반영

디렉터리 생성 & 권한 설정 표

작업	명령어	설명
디렉터리 생성	mkdir -p /tftp/router mkdir -p /tftp/firmware	라우터 설정 저장 용도, 펌웨어 저장 용도
백업용 파일 생성	touch /tftp/R4_sta	R4 설정 업로드용 파일
루트디렉터리 권한	chmod g+w /tftp	그룹 쓰기 허용
setgid 적용	chmod 2775 /tftp/router chmod 2775 /tftp/firmware	생성파일 소유 그룹 유지
허가권 변경	chmod 662 /tftp/R4_sta	업로드 가능하도록 쓰기 권한 부여
소유권 변경	chown admin:netengineer /tftp/router chown admin:admin /tftp/firmware chown admin:netengineer /tftp/R4_sta	admin 그룹 접근 가능, netengineer 그룹 설정 파일 조회 가능, 폴더 접근 가능

3. 파트 별 작업 소개 - 서비스 운영

TFTP서버에 파일 업로드

```
[root@localhost tftp]# chmod 662 R4_sta
[root@localhost tftp]# chown admin:netegineer R4_sta
[root@localhost tftp]# ll
합계 8
-rw-rw--w- 1 admin netegineer    0 10월  27 20:32 R4_sta
drwxrwsr-x 2 admin admin      4096 10월  26 04:21 firmware
drwxrwsr-x 2 admin netegineer 4096 10월  26 04:21 router
R4#copy sta tftp:
Address or name of remote host []? tftp.yeoksam.ac.local
Destination filename [r4-confg]? R4_sta
!!
1519 bytes copied in 0.204 secs (7446 bytes/sec)
```

TFTP서버 파일 확인

R4_sta

```
[root@localhost tftp]# ll
합계 12
-rw-rw--w- 1 admin netegineer 1519 10월  27 20:36 R4_sta
drwxrwsr-x 2 admin admin      4096 10월  26 04:21 firmware
drwxrwsr-x 2 admin netegineer 4096 10월  26 04:21 router
[root@localhost tftp]# cat R4_sta
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R4
!
```

3. 파트 별 작업 소개 - 서비스 운영

BIND 설치

작업	명령어	비고
BIND 설치	dnf -y install bind	named 포함

ZONE 파일 연결 설정

작업	명령어/파일	설명	비고
zone 등록	vi /etc/named.rfc1912.zones	zone 파일 경로 지정	domain ↔ zone 파일 연결
정방향 Zone 선언	zone "yeoksam.ac.local"	.zone 파일 지정	/var/named/yeoksam.ac.local.zone

3. 파트 별 작업 소개 - 서비스 운영

ZONE 파일 작성

작업	파일	설명	예시
정방향 zone 생성	/var/named/yeoksam.ac.local.zone	도메인 → IP(DB)	ftp/tftp/dns
TTL 설정	zone 파일 내부	캐시 유지시간 설정	1D 또는 86400
A 레코드 등록	ftp/tftp/dns → IP	내부 서버 주소 매핑	아래 표

서비스 활성화 & 방화벽 설정

작업	명령어	설명
named 데몬 활성화	systemctl enable named	자동 실행 등록
named 재시작	systemctl restart named	설정 적용
named 상태 확인	systemctl status named	오류 확인
방화벽 DNS 허용	firewall-cmd --permanent --add-service=named	DNS 서비스 허용
방화벽 적용	firewall-cmd --reload	규칙 반영

3. 파트 별 작업 소개 - 서비스 운영

질의 허용 네트워크

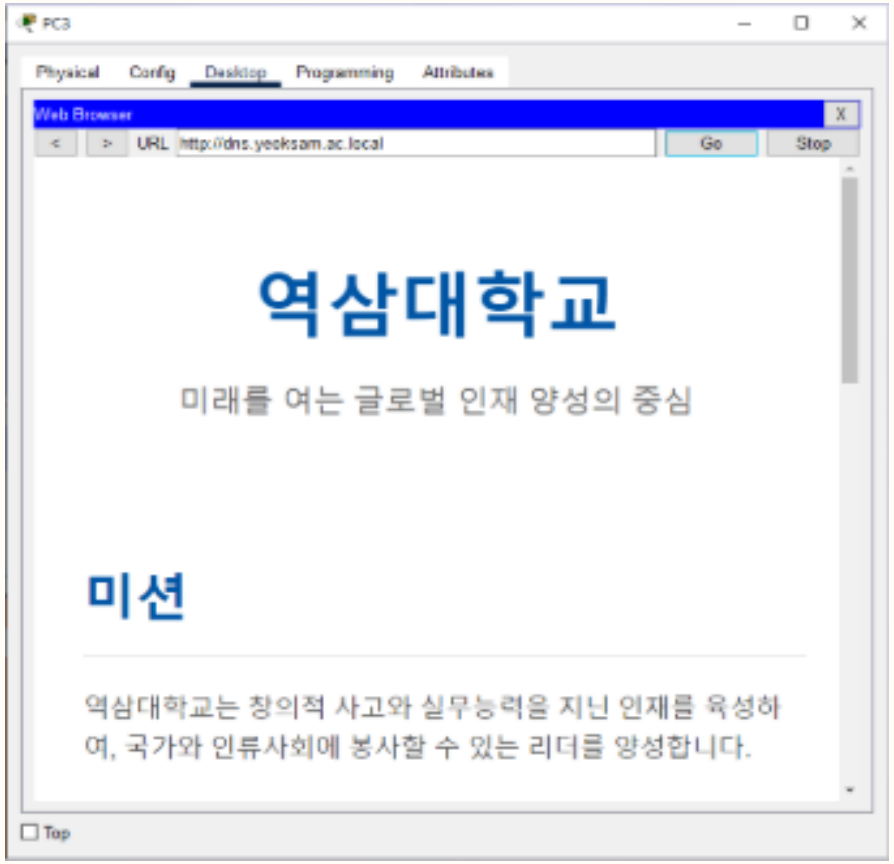
네트워크	의미
63.63.63.0/29	FTP 서버존
63.63.63.8/29	TFTP 서버존
63.63.63.16/29	DNS 서버존
1.1.1.0/30	사무동 NAT 라우터
2.2.2.0/30	강의동 NAT 라우터
3.3.3.0/27	공인(서버존)

DNS 메인 설정

설정 항목	파일	설명	예제
설정 파일 수정	/etc/named.conf	listen-on, allow-query, recursion 설정	vi /etc/named.conf
listen-on	named.conf	DNS 요청 수신할 인터페이스 지정	listen-on port 53 { any; };
IPv6 비활성화	named.conf	IPv6 사용 안함	listen-on-v6 port 53 { none; };
zone 파일 저장 경로 지정	named.conf	zone 파일 위치	directory "/var/named";
질의 허용 네트워크	named.conf	허용 IP 대역 지정	(왼쪽 표의 대역 허용)
재귀 질의 허용	named.conf	내부 DNS 캐싱 기능	recursion yes;

3. 파트 별 작업 소개 - 서비스 운영

사무동 → DNS 서버 접근



접근 가능한 외부 공인 IP주소 반환

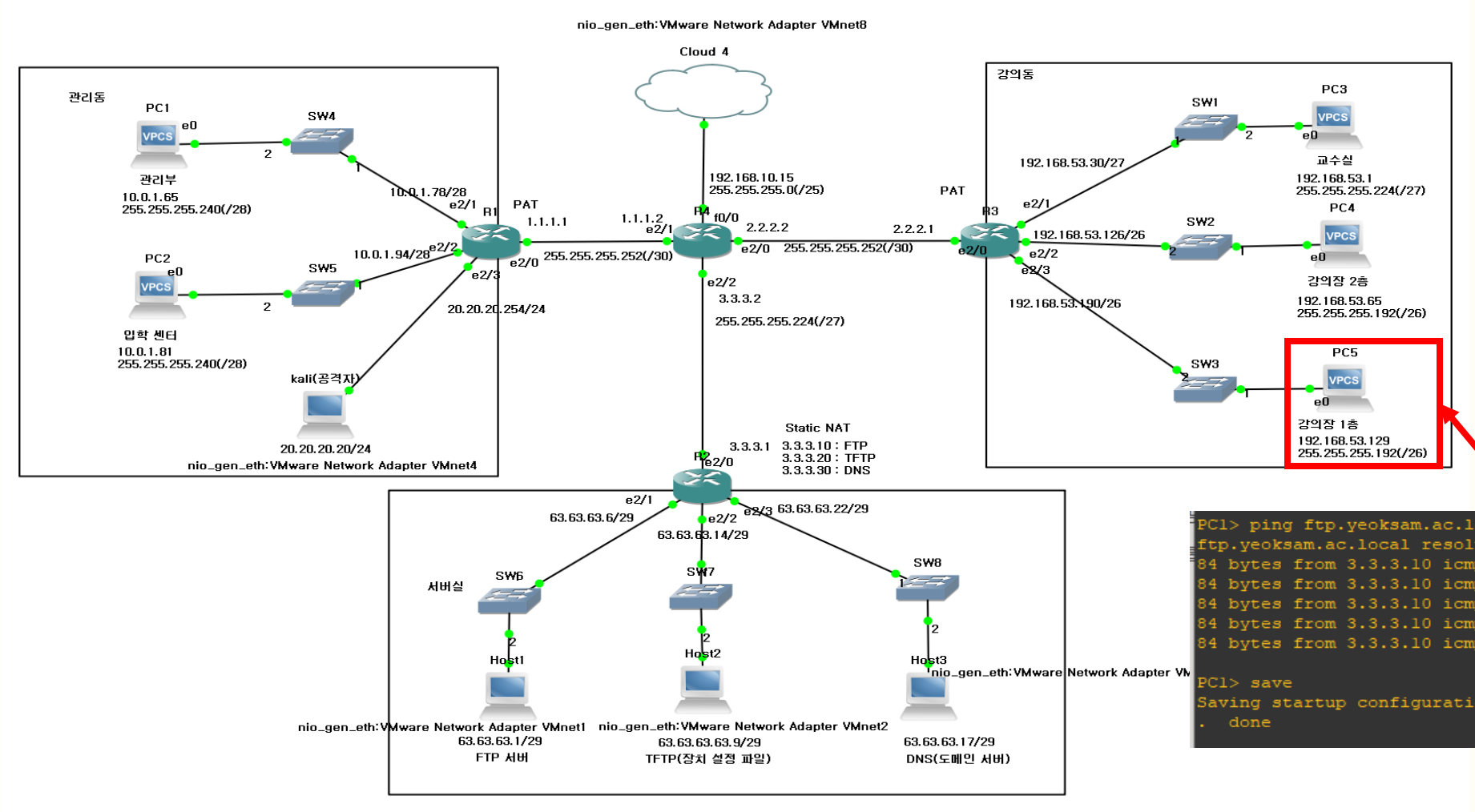
```
[root@localhost ~]# nslookup ftp.yeoksam.ac.local
Server:         3.3.3.30
Address:        3.3.3.30#53

Name:   ftp.yeoksam.ac.local
Address: 3.3.3.10

[root@localhost ~]# nslookup tftp.yeoksam.ac.local
Server:         3.3.3.30
Address:        3.3.3.30#53

Name:   tftp.yeoksam.ac.local
Address: 3.3.3.20

[root@localhost ~]# nslookup dns.yeoksam.ac.local
Server:         3.3.3.30
Address:        3.3.3.30#53

Name:   dns.yeoksam.ac.local
Address: 3.3.3.30
```

3. 파트 별 작업 소개

통합 관리

3. 파트 별 작업 소개 - 통합 관리

GNS 구성 및 서비스 테스트




```
PC1> ping ftp.yeoksam.ac.local
ftp.yeoksam.ac.local resolved to 3.3.3.10
84 bytes from 3.3.3.10 icmp_seq=1 ttl=61 time=92.250 ms
84 bytes from 3.3.3.10 icmp_seq=2 ttl=61 time=92.385 ms
84 bytes from 3.3.3.10 icmp_seq=3 ttl=61 time=92.605 ms
84 bytes from 3.3.3.10 icmp_seq=4 ttl=61 time=92.183 ms
84 bytes from 3.3.3.10 icmp_seq=5 ttl=61 time=92.412 ms

PC1> save
Saving startup configuration to startup.vpc
.  done
```

3. 파트 별 작업 소개 - 통합 관리

GNS 설정

항목	명령어	설명
VPCS	ip [IP주소]/[Prefix] [게이트웨이주소]	IP 주소, 서브넷 마스크, 게이트웨이 주소 설정
	ip dns [DNS서버주소]	DNS 주소 설정
	save	IP 정보 저장 적용
	show ip	IP 설정 정보 출력
Router	-	네트워크 설정의 라우터와 동일

4. 개선사항

4. 개선사항

1. **시스템 구축 및 권한**
   계정·그룹별 접근 권한을 명확히 구분하고, 백업 및 로그 관리 체계 강화 필요

2. **네트워크 설계**
   네트워크 이중화 와 2차 백업 서버 및 DMZ 구역 설계

3. **서비스 운영**
   서버 접근 로그와 자원 모니터링 시스템 도입으로 운영 효율성 강화,
   보조 DNS 서버 및 웹 서버 증설

4. **보안 계획**
   정기적인 백업과 로그 설정으로 재난 복구 계획 수립과 모니터링 및 위협 탐지 능력 강화

5. 느낀 점

5. 느낀 점

이남혁
(총장)

네트워크 구성 이상으로 네트워크,보안,시스템,서비스가 유기적으로 맞물려야
진정한 내부망 환경이 완성된다는 것을 직접 느꼈습니다. 기술적 성취뿐만 아니라
팀워크, 리더십, 문제 해결력 면에서도 한 단계 성장할 수 있었던 경험이었습니다.

이정훈
(학장)

보안 설정을 하며 보안을 강화할수록 안전해지지만 관리가 까다로워진다고 생각했고,
작은 실수 하나에 시스템 접속 자체가 멈출 수 있어 유의해서 작업을 진행해야 한다고 생각했습니다.

강버들

인프라 구축에서는 문서 정리가 전부라는 것을 깨달았고,
매뉴얼이란 실제 업무 환경을 이루는 설계도로써 누구나 이해 가능하고 적용 가능하도록
작성하는 능력이 매우 중요하다는 것을 이해하였습니다.

5. 느낀 점

백정이

네트워크 대역 설정 규칙을 명확히 알고 있어야 함을 깨달았습니다.
서비스 운영 그리고 보안을 위해서 다양한 설정 값
그리고 서비스 기본 동작 원리를 알고 있어야 함을 알게 되었습니다.

장성주

디렉토리 또는 파일마다 권한을 부여하는 방법이 쉽지 않다는 것을 느꼈고,
또한 네트워크 대역을 설정하는 방법을 정확히 알고 있어야 한다는 것을 느낄 수 있었습니다.
네트워크에서 설정이 하나라도 겹치면 안되는 것을 느꼈습니다.

전보라

전체적인 네트워크 구성하고 서비스를 테스트하며 기본 지식 및 이해도의 중요성을 느꼈습니다.
보안 공격의 유형을 알고 대응 방안을 탐색한 후 체계화하는 작업을 진행하며,
네트워크 계층과 프로토콜에 대한 이해도를 높일 수 있었습니다.

THANK YOU

SUN교사