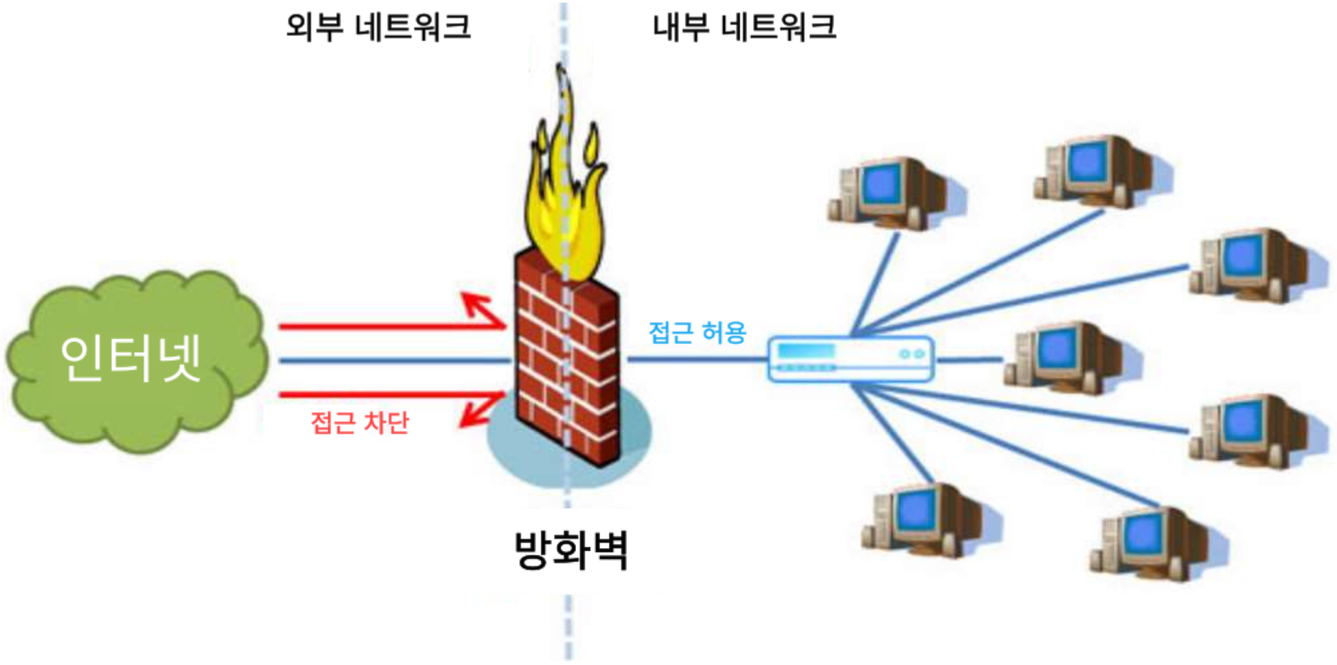
방화벽

목차

01.방화벽이란?

네트워크의 보안을 높이는 데 필요한 기본적인 보안 솔루션으로 신뢰하지 않는 외부 네트워크와 신뢰하는 내부 네트워크 사이를 지나는 패킷을 미리 정한 정책에 따라 차단하거나 허용하는 기능을 하는 하드웨어 또는 소프트웨어이다.



02. 방화벽의 기능

방화벽의 기능

-접근 제어

통과시킬 접근과 차단할 접근을 관리자가 명시해주면 방화벽은 지시받은대로 이행

-로깅과 감사 추적

허용 또는 거부된 접근에 대한 기록을 유지

-인증

메시지 인증: 전송되는 메시지에 대한 신뢰성 보장
사용자 인증: 패스워드를 통한 단순 인증부터 OTP나 토큰 기반과 같은 높은 수준의 인증까지 가능
클라이언트 인증: 특수한 접속을 요구하는 호스트 자체가 정당한 접속 호스트인지 확인

-데이터 암호화

방화벽에서 다른 방화벽까지 전송되는 데이터를 암호화해서 보냄

03. 방화벽의 한계

방화벽의 한계

-바이러스 차단 불가

데이터의 내용 자체는 검사하지 않음

-내부 공격 차단 불가

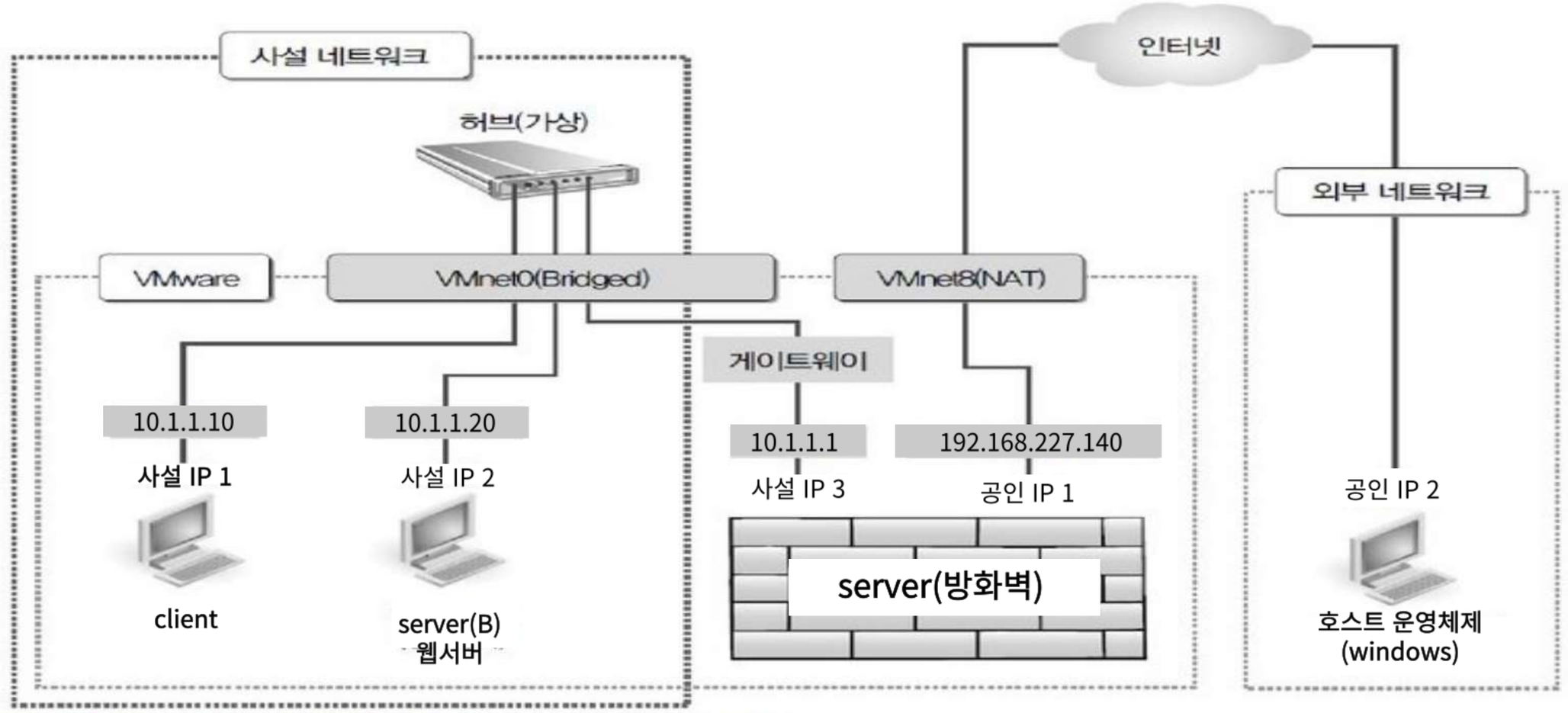
경계에 대한 보안 정책을 수행할 뿐 내부 공격자에게 보안 정책을 적용할 수 없음

-자신을 통하지 않은 통신에 대한 제어 불가

-새로운 형태의 공격 차단 불가

예측된 접속에 대한 규칙을 세우고 이에 대해서만 방어함

04.방화벽 구축 구상도


사설 네트워크
인터넷
허브(가상)
외부 네트워크
VMware
VMnet0(Bridged)
VMnet8(NAT)
게이트웨이
10.1.1.10
10.1.1.20
10.1.1.1
192.168.227.140
사설 IP 1
사설 IP 2
사설 IP 3
공인 IP 1
공인 IP 2
server(방화벽)
client
server(B)
웹서버
호스트 운영체제
(windows)

05.방화벽 구축 실습

-실습 환경 구축

가상 머신 생성(4대) - sever(방화벽), sever(B), client, 호스트 운영체제(windows)

server, sever(B) - 방화벽 모듈 iptables 패키지 설치

```
파일(F)  편집(E)  보기(V)  검색(S)  터미널(T)  도움말(H)
[root@localhost server]# dnf -y install iptables-services
```

selinux 비활성화를 위한 vi편집기 실행

```
파일(F)  편집(E)  보기(V)  검색(S)  터미널(T)  도움말(H)
[root@localhost serverb]# vi /etc/sysconfig/selinux
```

selinux 비활성화 방법 enforcing을 disabled로 변경

```
serverb@localhost:/home/serverb
파일(F)  편집(E)  보기(V)  검색(S)  터미널(T)  도움말(H)

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of these three values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

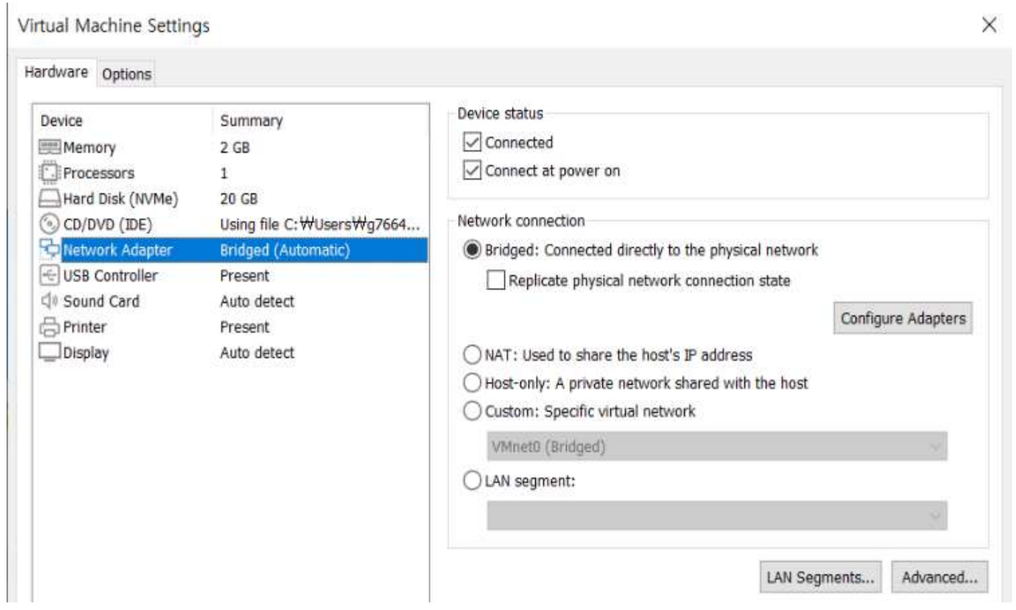
```
serverb@localhost:/home/serverb
파일(F)  편집(E)  보기(V)  검색(S)  터미널(T)  도움말(H)

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of these three values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
"/etc/sysconfig/selinux" 14L, 547C
```

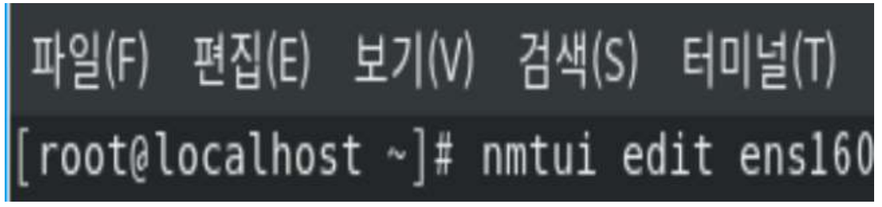
05.방화벽 구축 실습

-client 설정

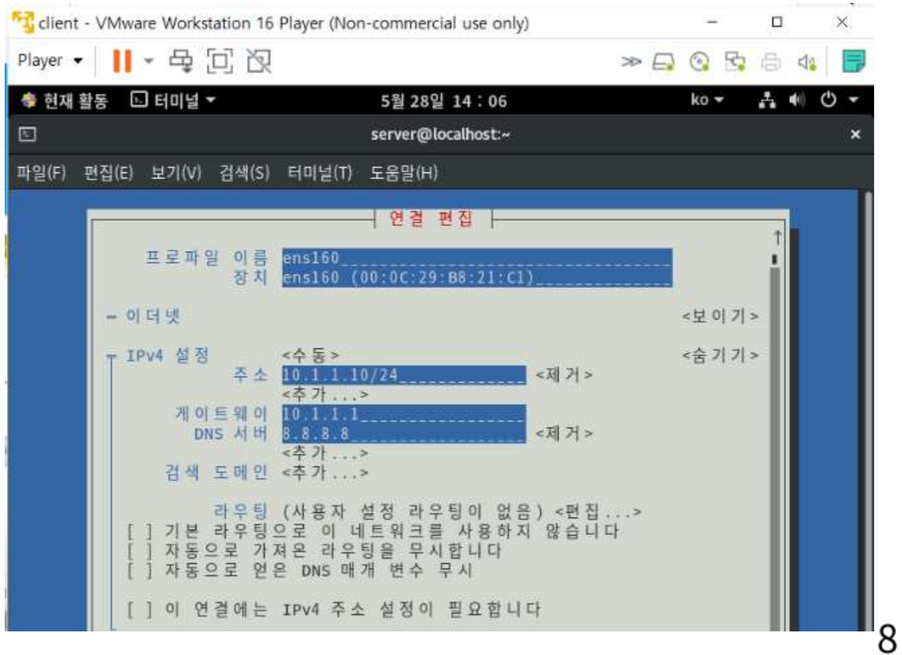
Network Adaptor 변경



nmtui 명령어 사용



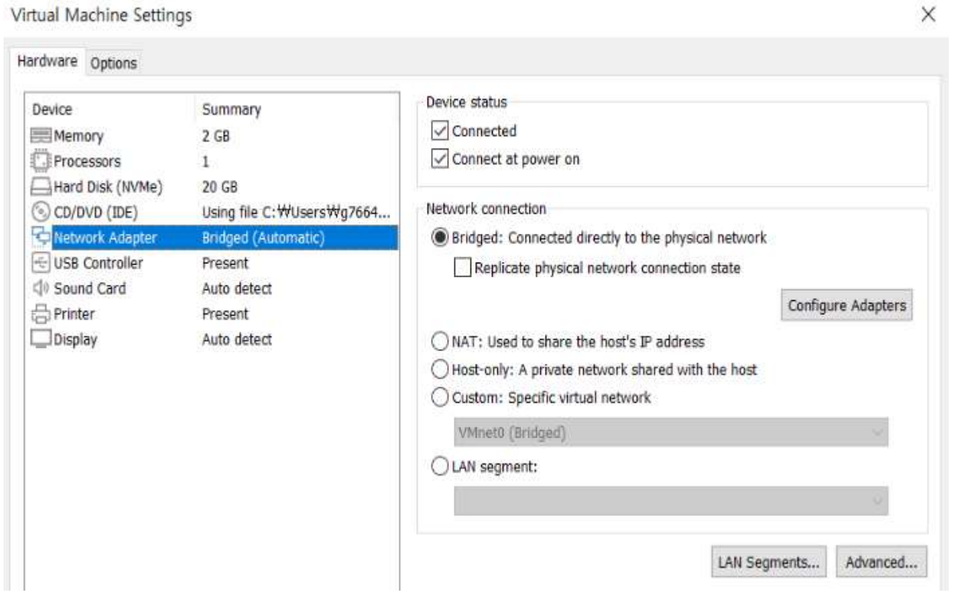
사설 IP 1 편집



05.방화벽 구축 실습

-sever(B) 설정

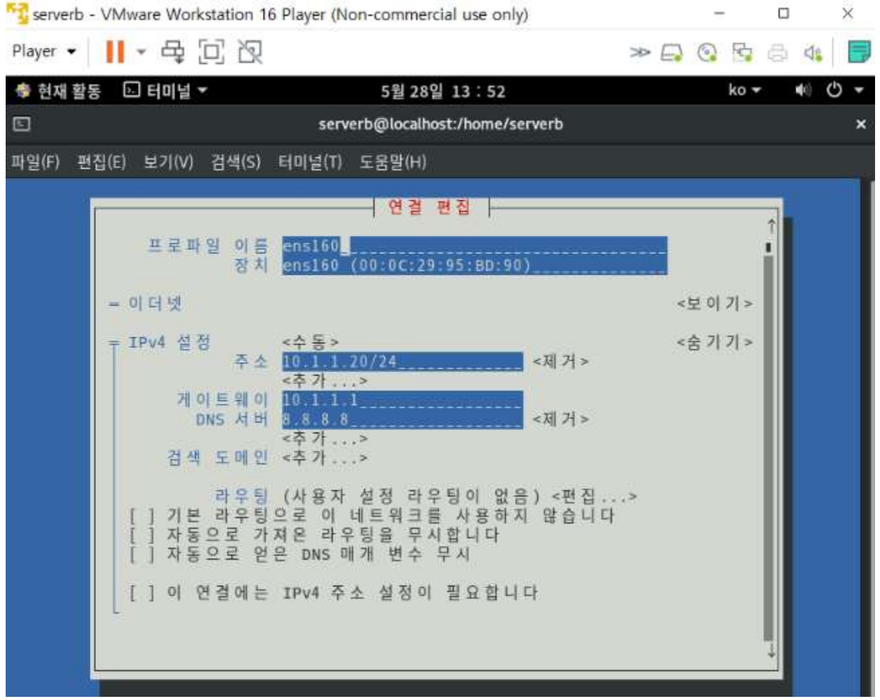
Network Adaptor 변경



nmtui 명령어 사용

```
[root@localhost serverb]# nmtui edit ens160
```

사설 IP 2 편집

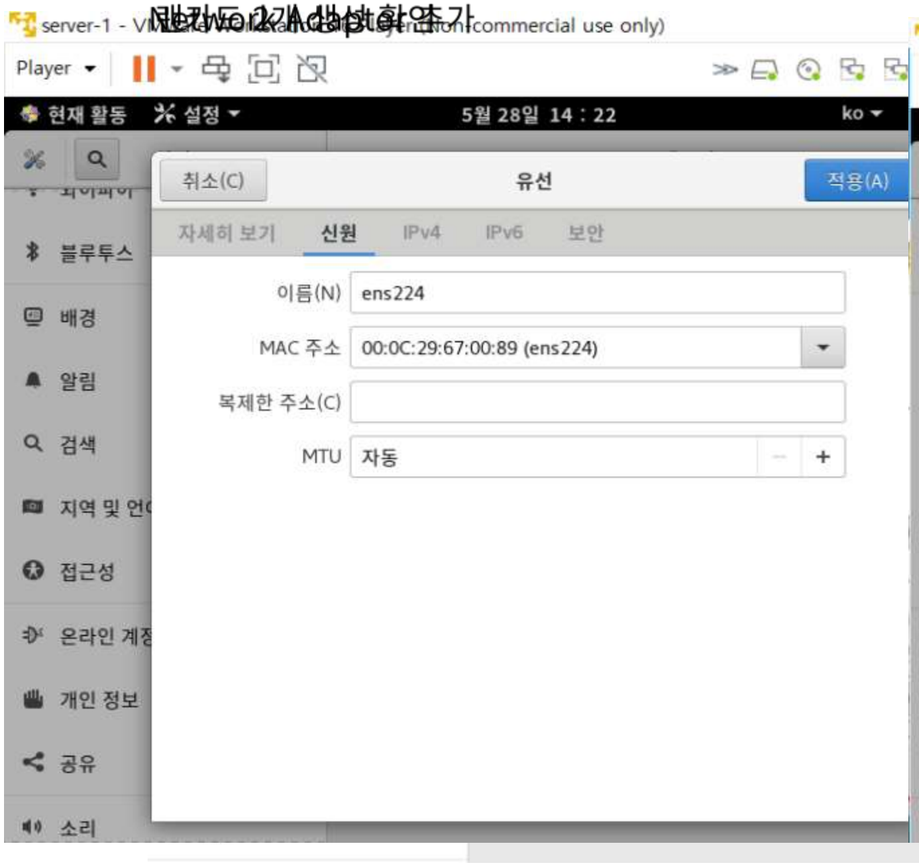


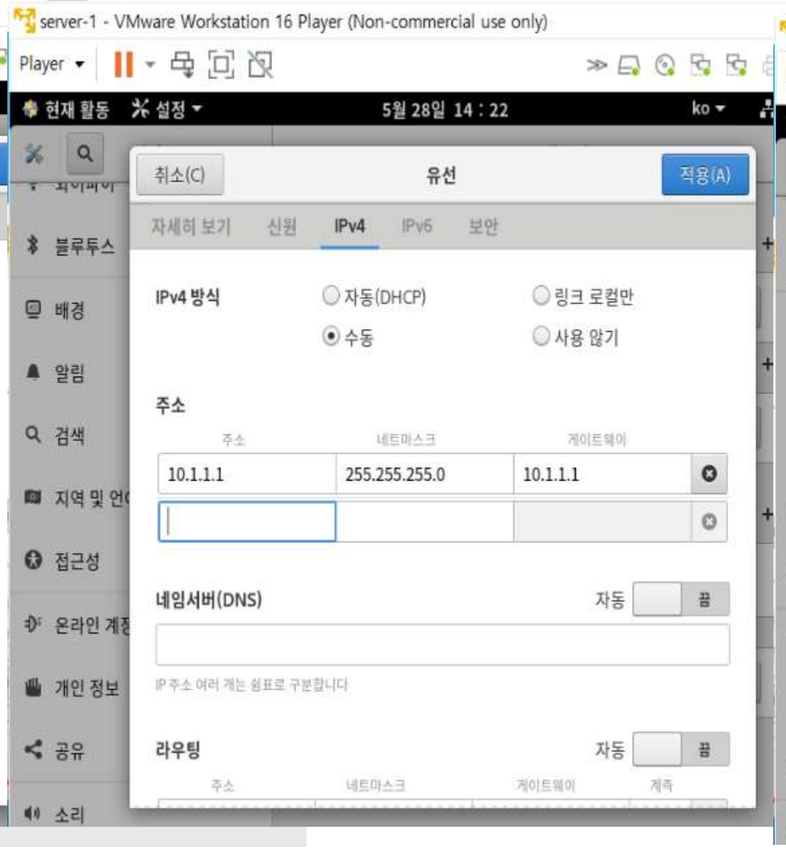
05.방화벽 구축 실습

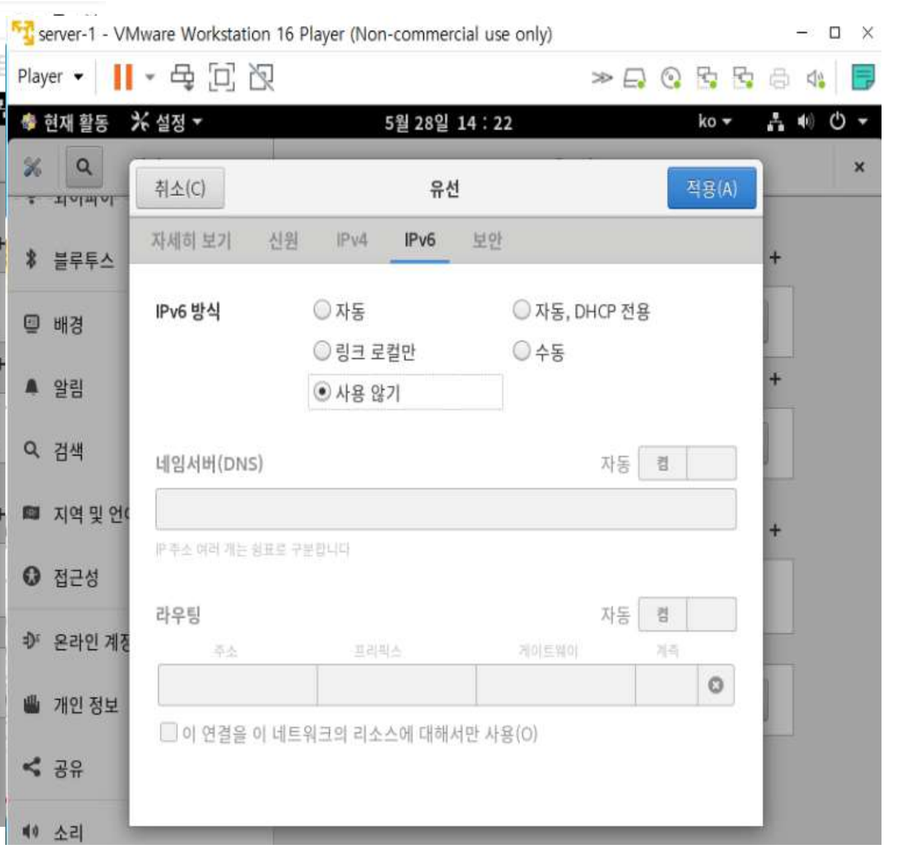
-server 설정

사설 IP 3 편집

네트워크 기본 생성 확인







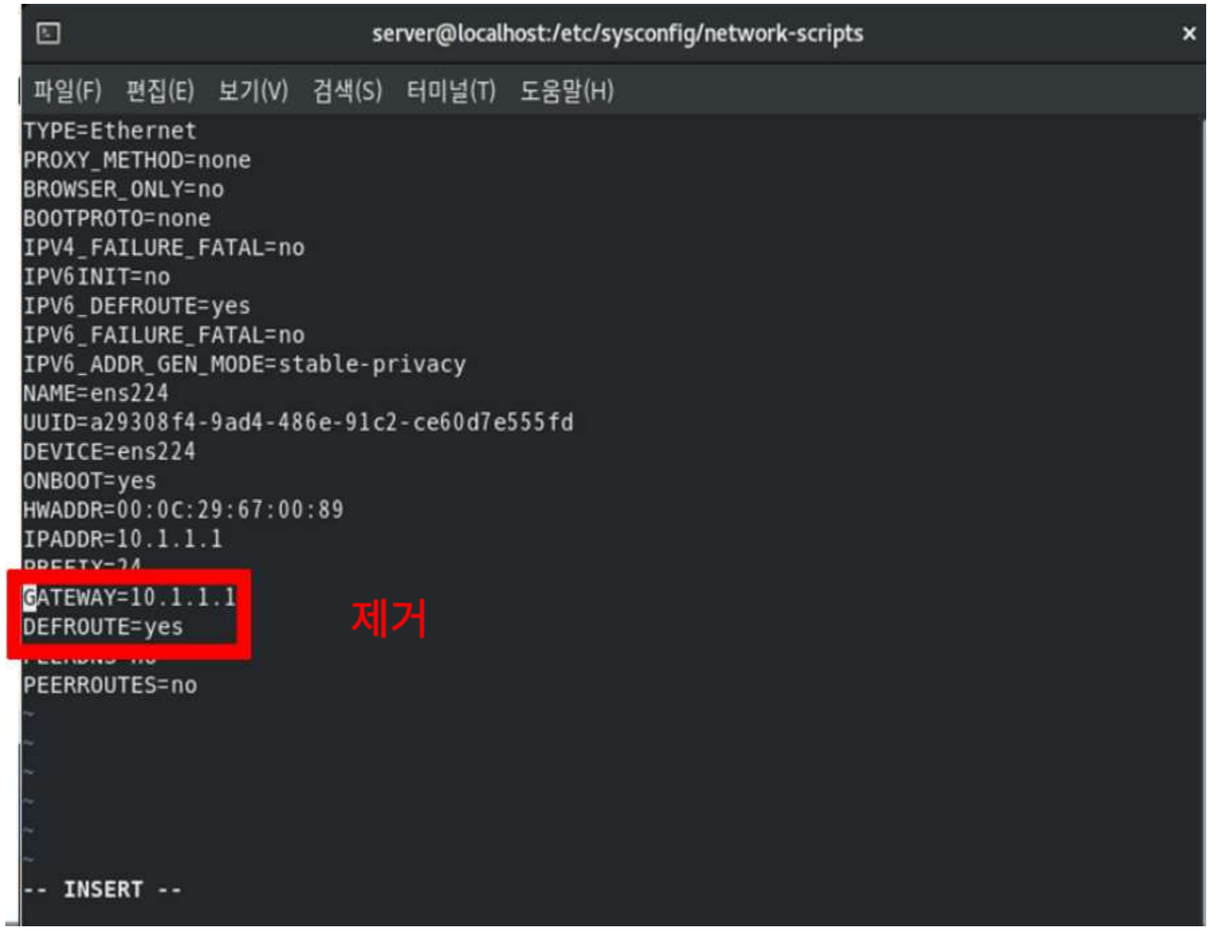
05.방화벽 구축 실습

-server 설정

사설 IP 3 설정

```
파일(F)  편집(E)  보기(V)  검색(S)  터미널(T)  도움말(H)
[root@localhost server]# cd /etc/sysconfig/network-scripts
[root@localhost network-scripts]# ls
ifcfg-ens160  ifcfg-유선_연결_1
[root@localhost network-scripts]# vi /etc/sysconfig/network-scripts/ifcfg-유선_연결_1
```

(유선_연결_1 = 생성된 사설 IP 3)



05.방화벽 구축 실습

-방화벽 정책 설정

ip.forward 항상 활성화

```
파일(F)  편집(E)  보기(V)  검색(S)  터미널(T)  도움말(H)
[root@localhost network-scripts]# vi /etc/sysctl.conf
```

server@localhost:/etc/sysconfig/network-scripts

```
파일(F)  편집(E)  보기(V)  검색(S)  터미널(T)  도움말(H)
# sysctl settings are defined through files in
# /usr/lib/sysctl.d/, /run/sysctl.d/, and /etc/sysctl.d/.
#
# Vendors settings live in /usr/lib/sysctl.d/.
# To override a whole file, create a new file with the same in
# /etc/sysctl.d/ and put new settings there. To override
# only specific settings, add a file with a lexically later
# name in /etc/sysctl.d/ and put new settings there.
#
# For more information, see sysctl.conf(5) and sysctl.d(5).

net.ipv4.ip.forward = 1
~
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/sysctl.conf" 12L, 474C
```

ip 포워딩 확인

```
파일(F)  편집(E)  보기(V)  검색(S)  터미널(T)  도움말(H)
[root@localhost network-scripts]# vi /etc/sysctl.conf
[root@localhost network-scripts]# echo 1 > /proc/sys/net/ipv4/ip_forward
[root@localhost network-scripts]# cat /proc/sys/net/ipv4/ip_forward
1
```

기본 정책 DROP

```
[root@localhost ~]# iptables --policy FORWARD DROP
[root@localhost ~]# iptables --policy INPUT DROP
[root@localhost ~]# iptables --policy OUTPUT DROP
```

05.방화벽 구축 실습

-방화벽 정책 설정

```
[root@localhost ~]#
[root@localhost ~]# iptables --append INPUT --in-interface ens224 --source 10.1.1.0/24
--match state --state NEW,ESTABLISHED --jump ACCEPT
[root@localhost ~]# iptables --append OUTPUT --out-interface ens224 --destination 10.1.
1.0/24 --match state --state NEW,ESTABLISHED --jump ACCEPT
[root@localhost ~]# iptables --append FORWARD --in-interface ens224 --source 10.1.1.0/2
4 --destination 0.0.0.0/0 --match state --state NEW,ESTABLISHED --jump ACCEPT
[root@localhost ~]# iptables --append FORWARD --in-interface ens160 --destination 10.1.
1.0/24 --match state --state ESTABLISHED --jump ACCEPT
[root@localhost ~]# iptables --table nat --append POSTROUTING --out-interface ens160 --
jump MASQUERADE
[root@localhost ~]#
```

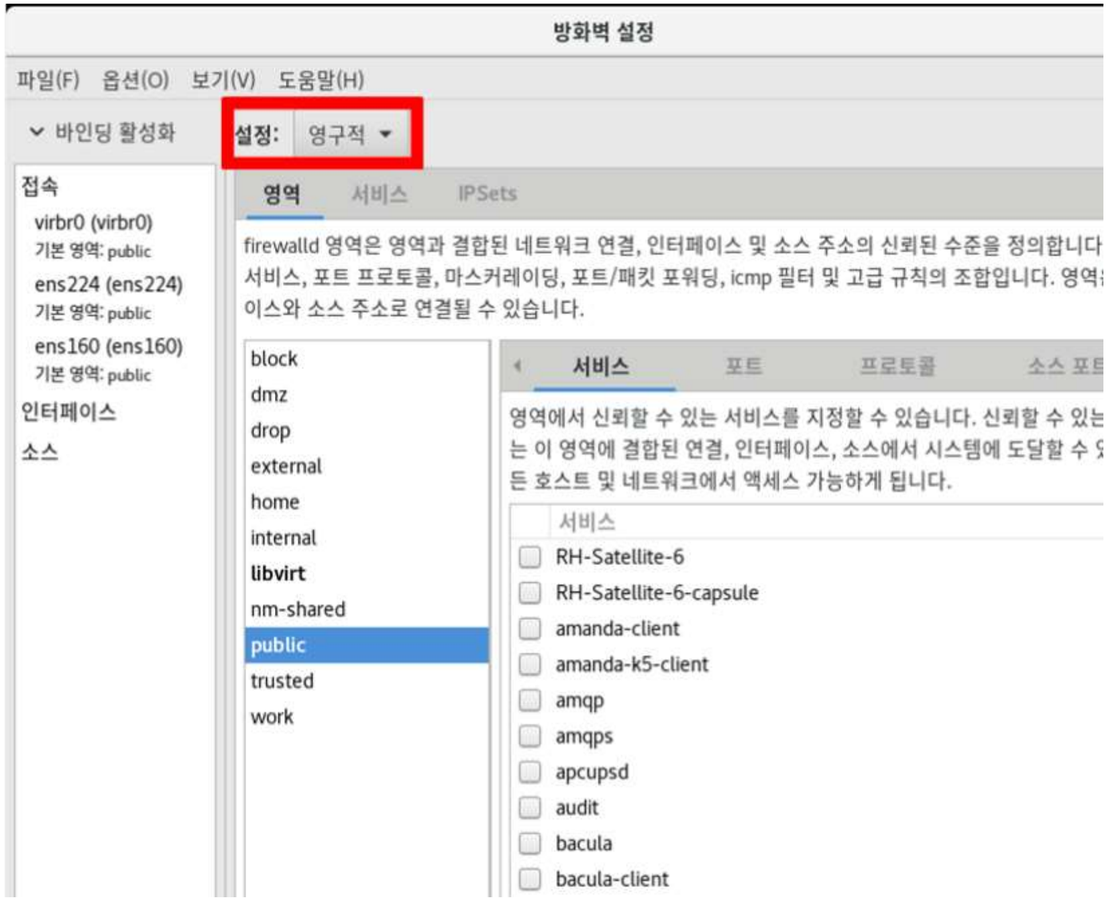
설정 저장과 방화벽 설정

```
[root@localhost ~]# iptables-save > /etc/sysconfig/iptables
[root@localhost ~]# firewall-config
```

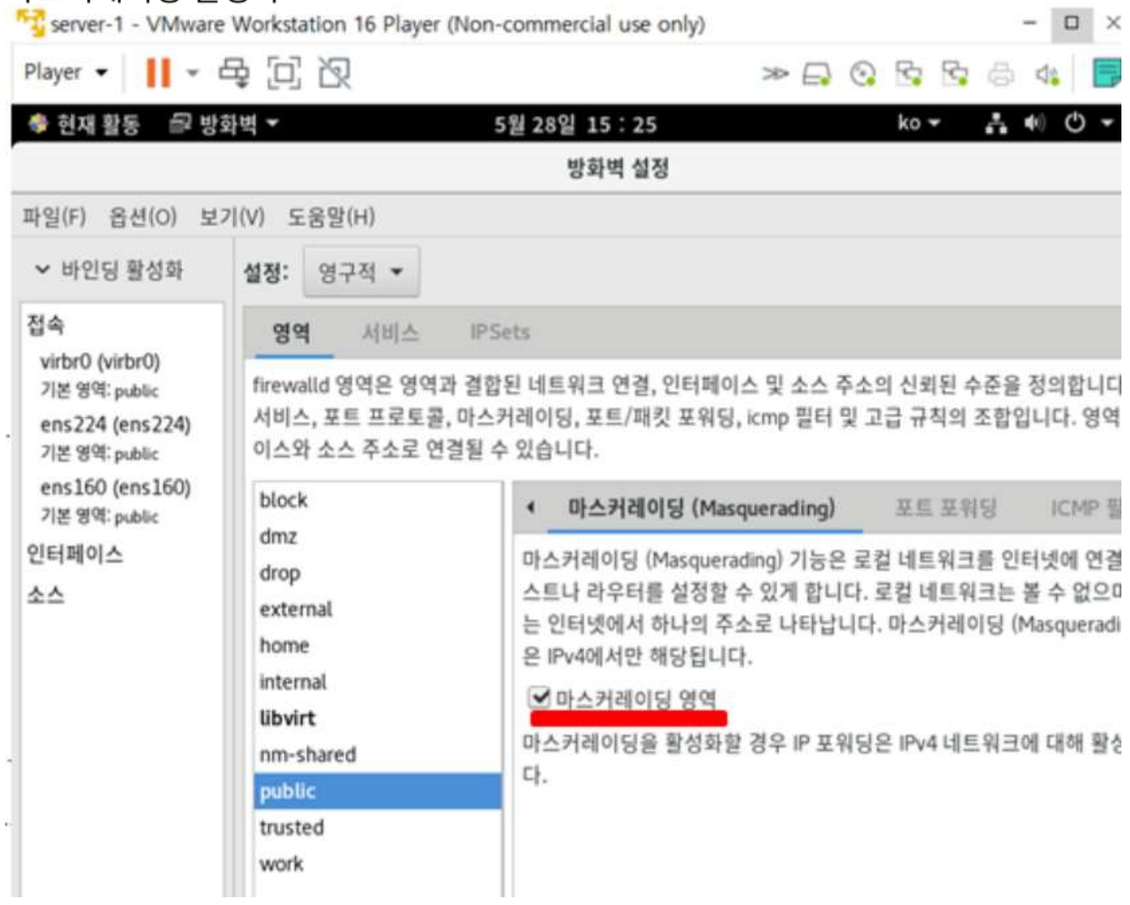
05.방화벽 구축 실습

-방화벽 정책 설정

방화벽 설정



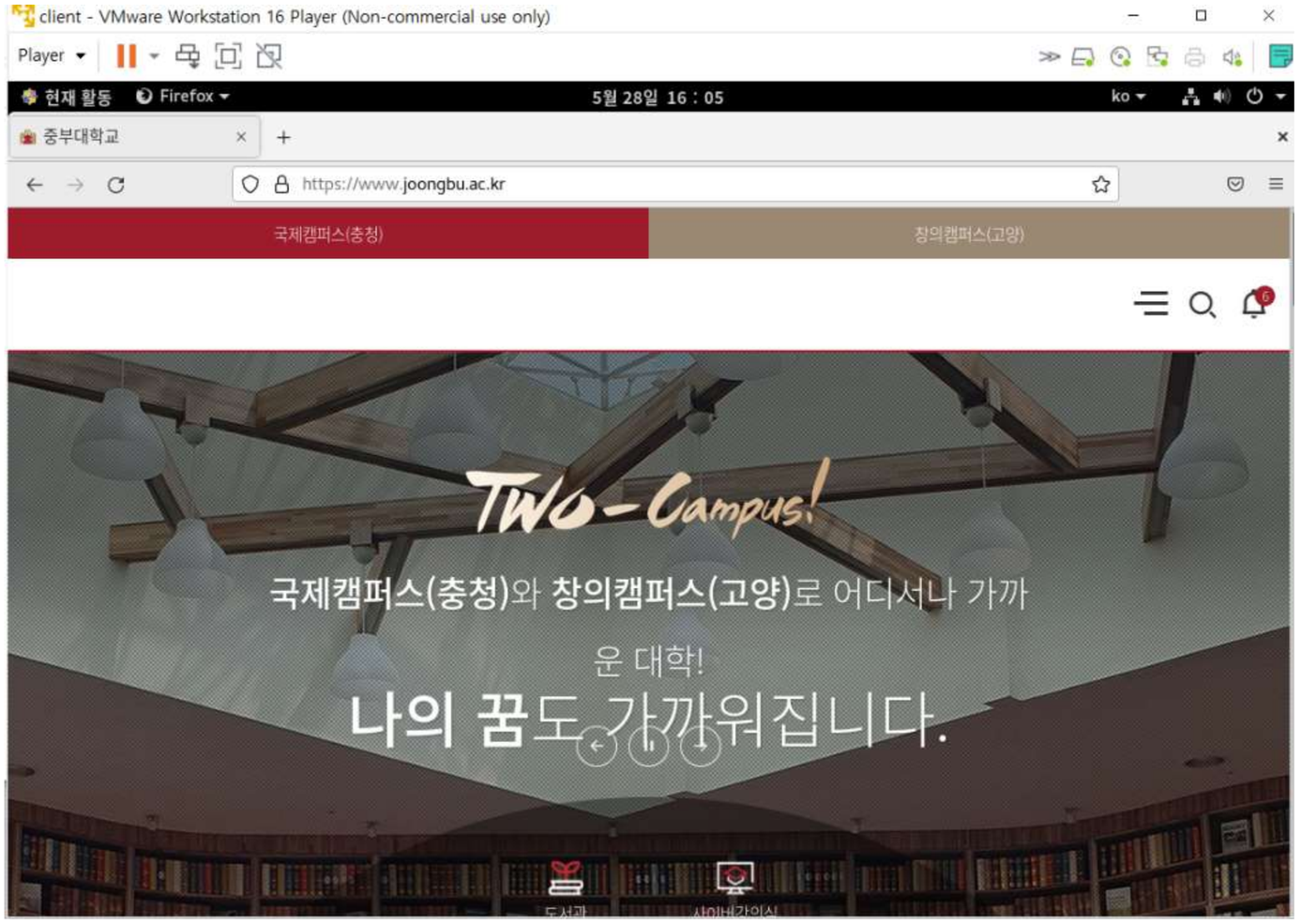
마스커레이딩 활성화



05.방화벽 구축 실습

-사설 네트워크에서 외부 인터넷으로 접속

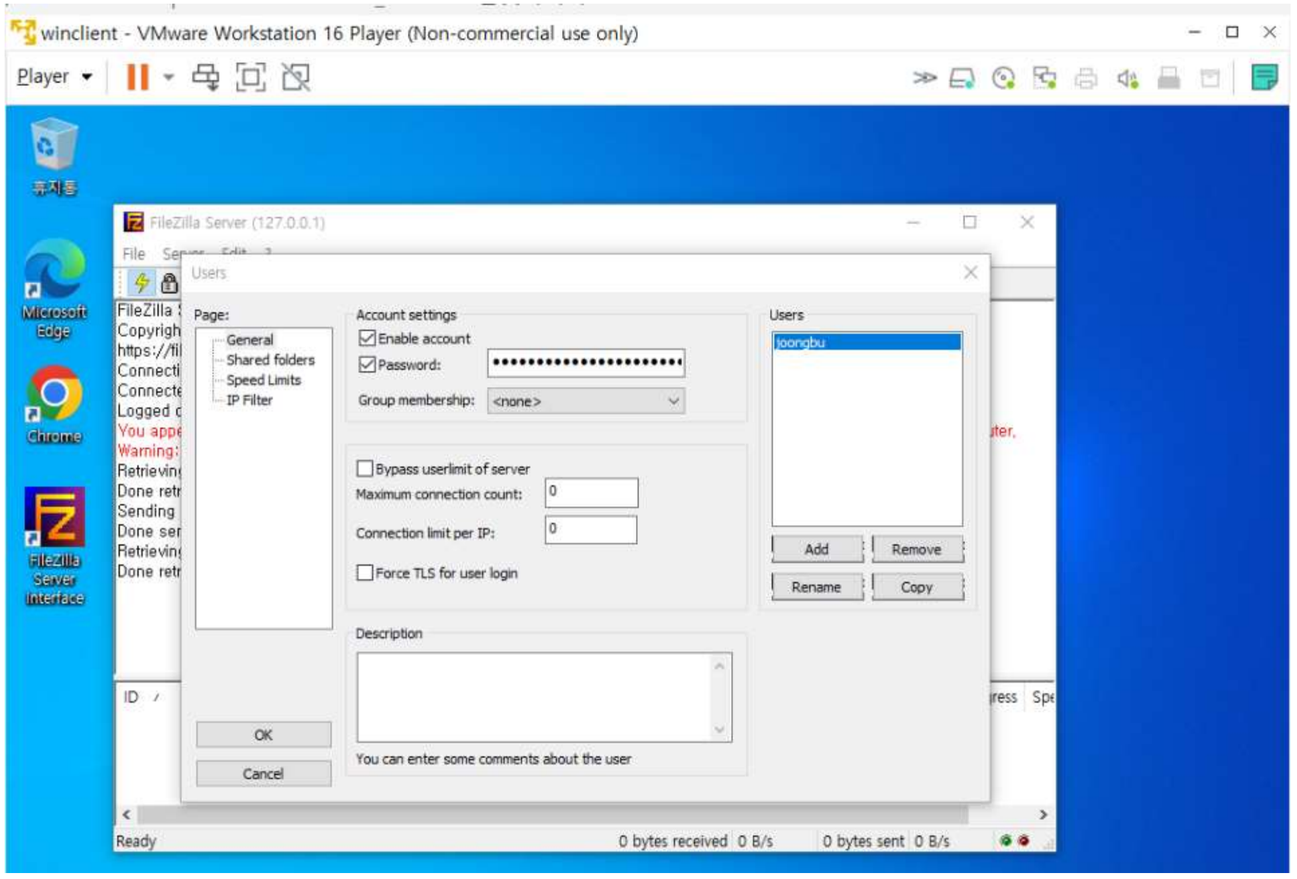
네트워크 접속 확인



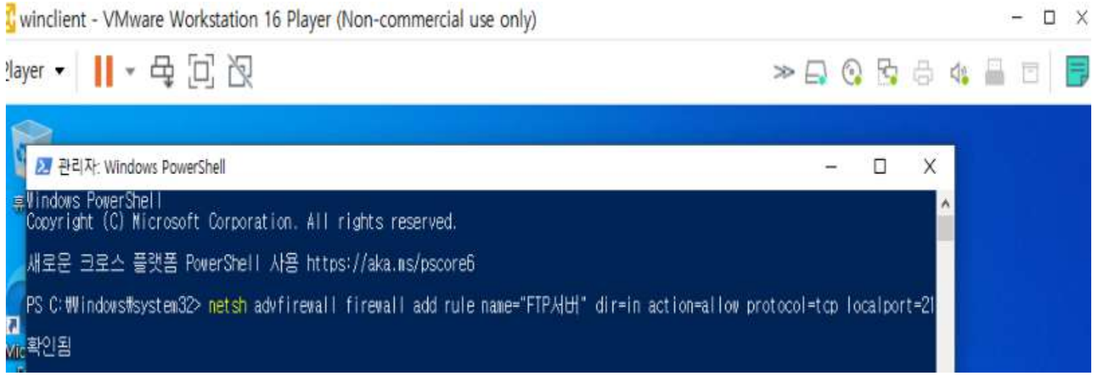
05.방화벽 구축 실습

-방화벽 구축 확인

FTP 서버 추가



FTP 포트 활성화



05.방화벽 구축 실습

-방화벽 구축 확인

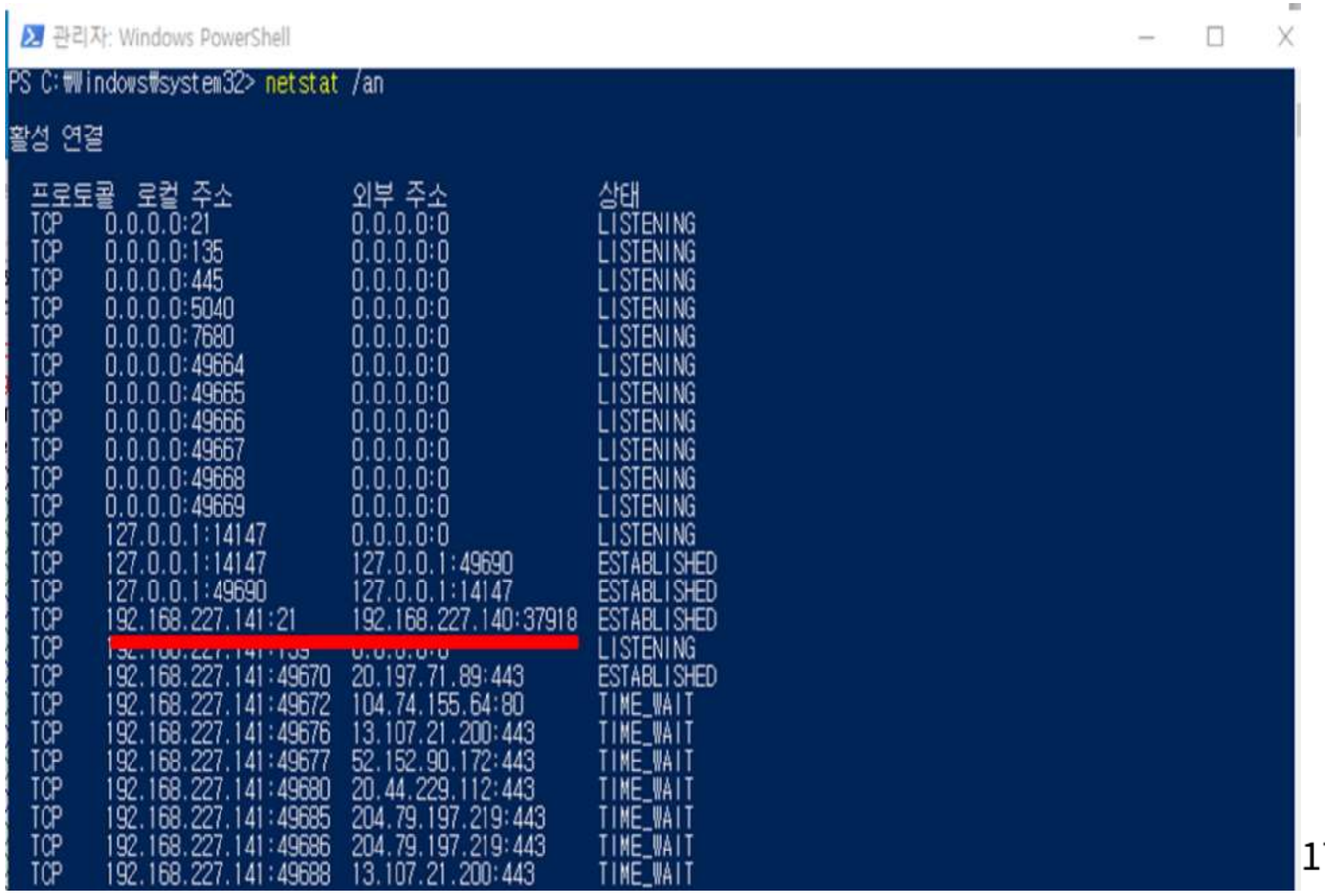
FTP 패키지 설치

```
[root@localhost server]# dnf -y install ftp
CentOS Stream 8 - AppStream
```

FTP 서버 로그인

```
[root@localhost server]# ftp 192.168.227.141
Connected to 192.168.227.141 (192.168.227.141).
220-FileZilla Server 0.9.60 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
Name (192.168.227.141:root): joongbu
331 Password required for joongbu
Password:
230 Logged on
Remote system type is UNIX.
ftp> pwd
257 "/" is current directory.
ftp>
```

netstat 명령어 사용과 방화벽 운영 확인



05.방화벽 구축 실습

-방화벽 구축 확인

http 웹 서비스 허용과 웹서버 제작

```
[root@localhost serverb]# firewall-cmd --permanent --add-service=http
success
[root@localhost serverb]# firewall-cmd --reload
success
[root@localhost serverb]# cd /var/www/html
[root@localhost html]# touch index.html
[root@localhost html]# vi index.html
```

웹서버 내용

```
파일(F)  편집(E)  보기(V)  검색(S)  터미널(T)  도움말(H)
<h1> This is my server -The End- </h1>
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"index.html" 1L, 39C
```

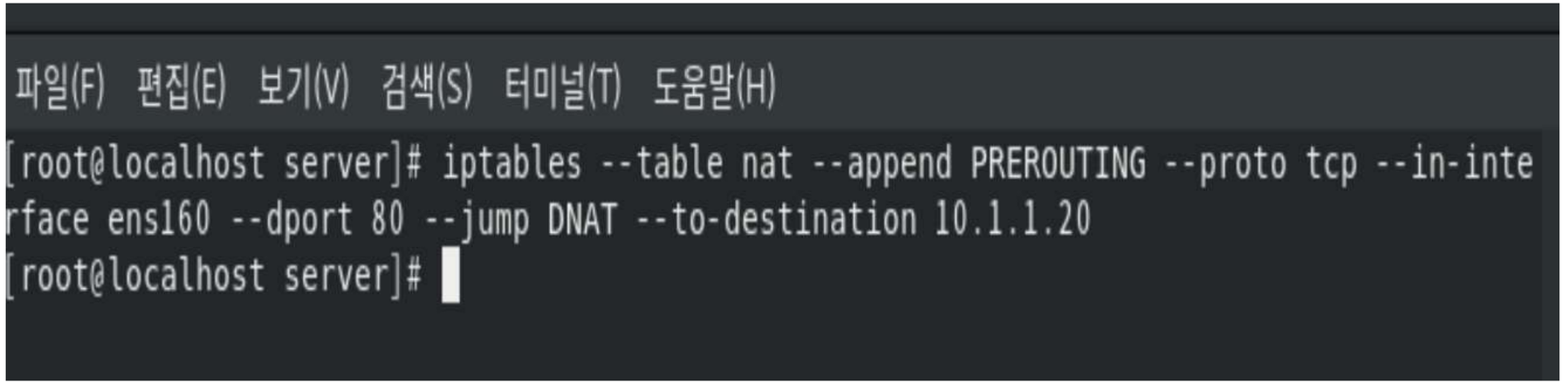
웹서버 재시작

```
파일(F)  편집(E)  보기(V)  검색(S)  터미널(T)  도움말(H)
[root@localhost html]# systemctl restart httpd
[root@localhost html]# systemctl enable  httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service →/usr/lib/sy
stemd/system/httpd.service.
[root@localhost html]#
```

05.방화벽 구축 실습

-방화벽 구축 확인

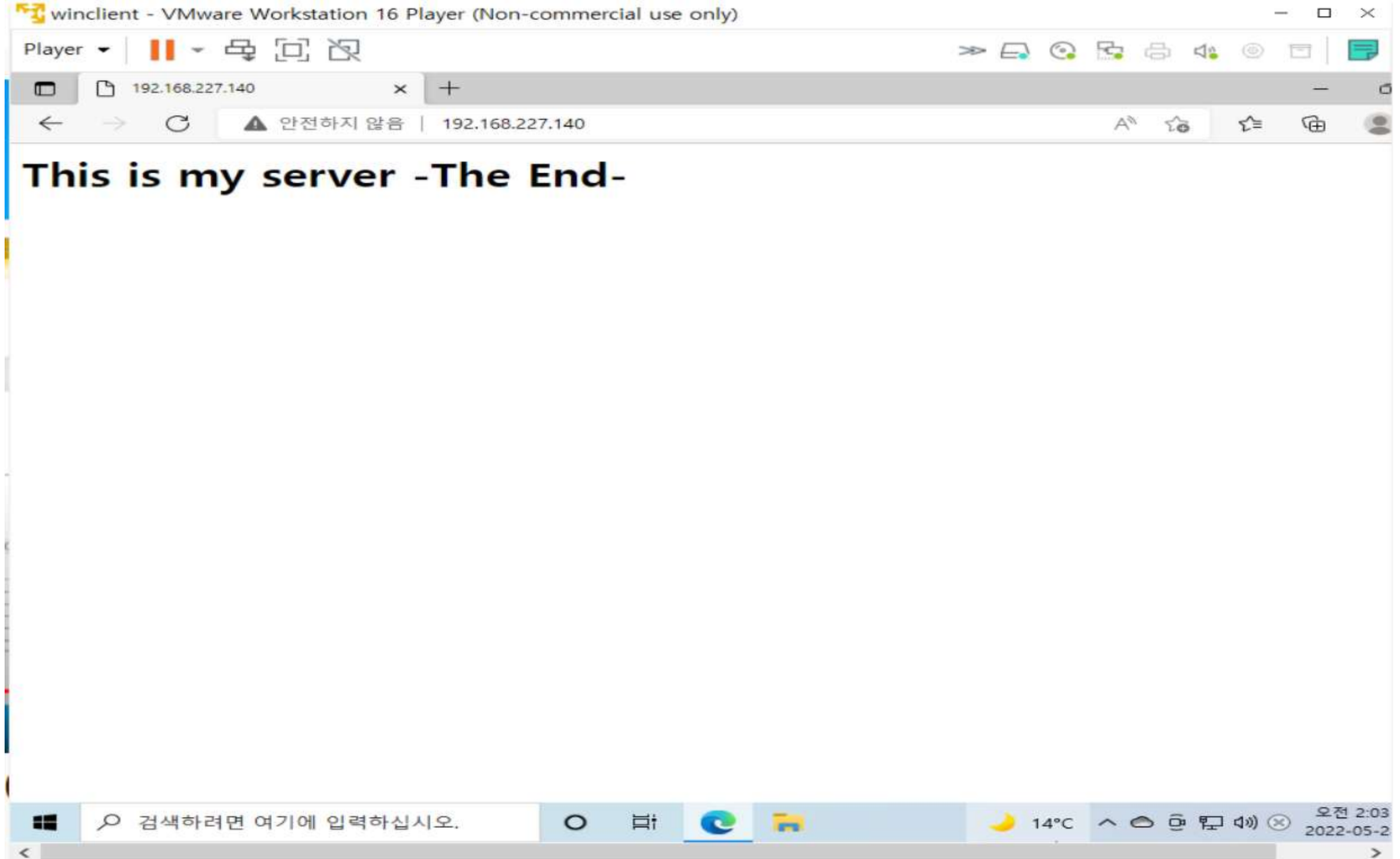
포트 리다이렉션 설정



05.방화벽 구축 실습

-방화벽 구축 확인

웹 페이지 접속



감사합니다