

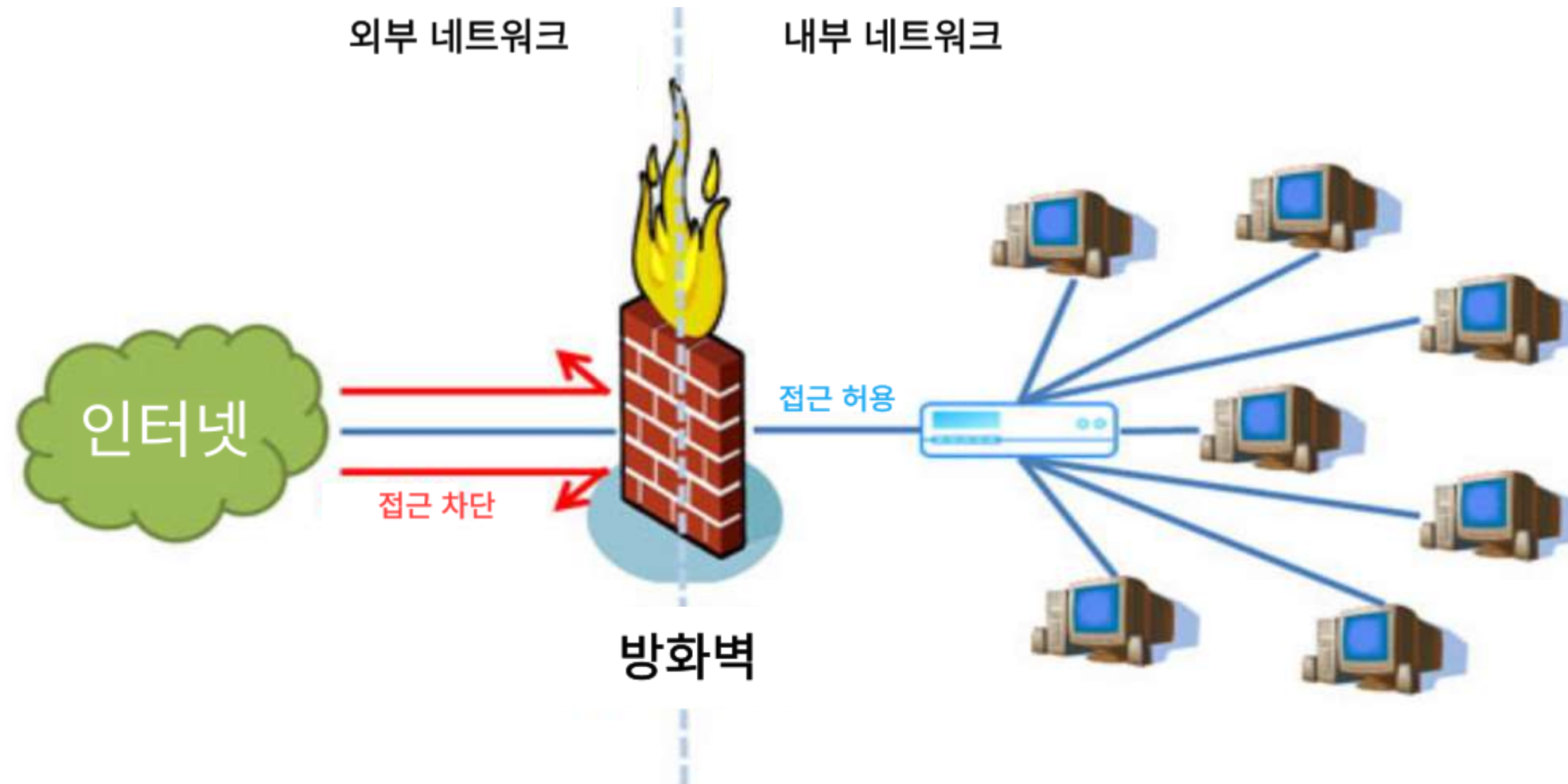
방화벽

목차

- 01. 방화벽이란?
- 02. 방화벽의 기능
- 03. 방화벽의 한계
- 04. 방화벽 구축 구상도
- 05. 방화벽 구축 실습

01. 방화벽이란?

네트워크의 보안을 높이는 데 필요한 기본적인 보안 솔루션으로 신뢰하지 않는 외부 네트워크와 신뢰하는 내부 네트워크 사이를 지나는 패킷을 미리 정한 **정책**에 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

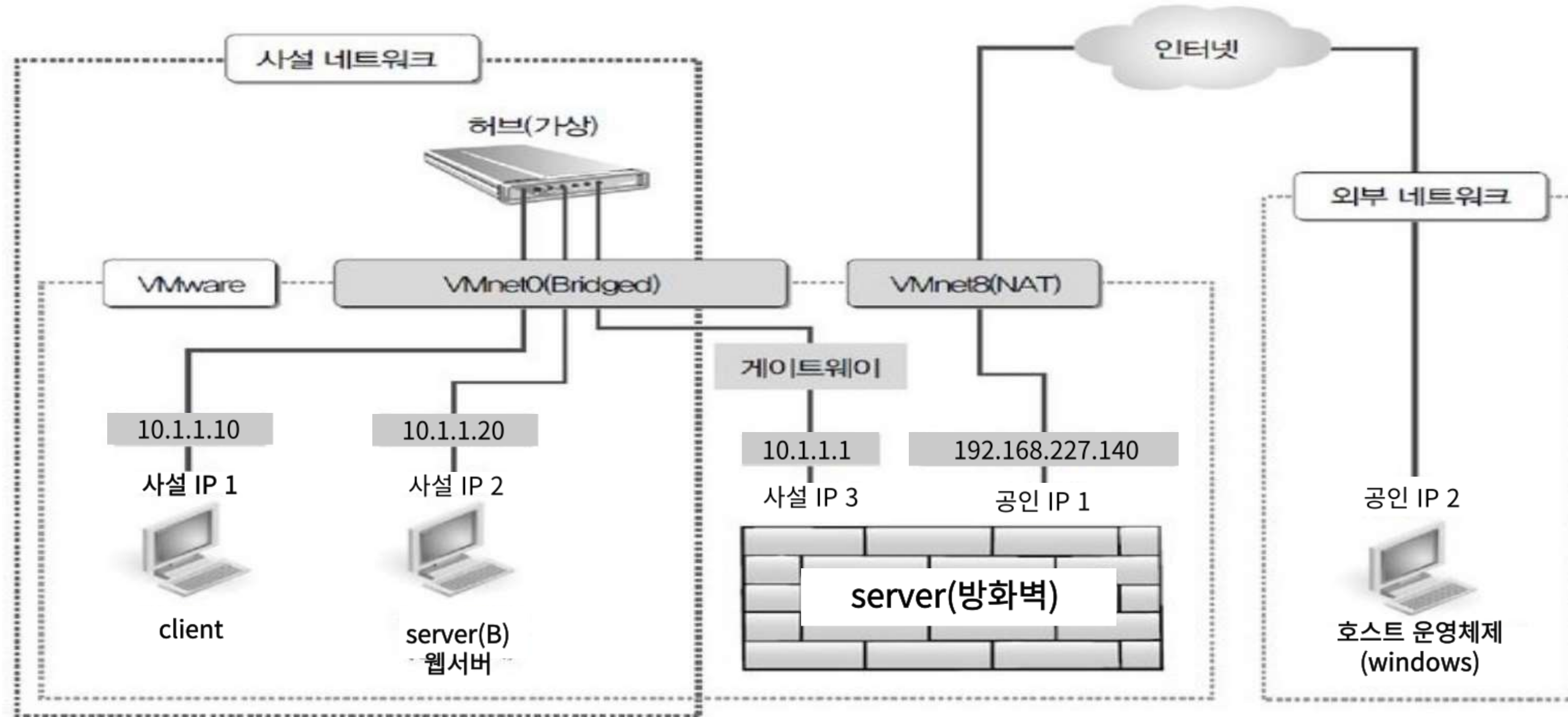
경계에 대한 보안 정책을 수행할 뿐 내부 공격자에게 보안 정책을 적용할 수 없음

-자신을 통하지 않은 통신에 대한 제어 불가

-새로운 형태의 공격 차단 불가

예측된 접속에 대한 규칙을 세우고 이에 대해서만 방어함

04. 방화벽 구축 구상도



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
```



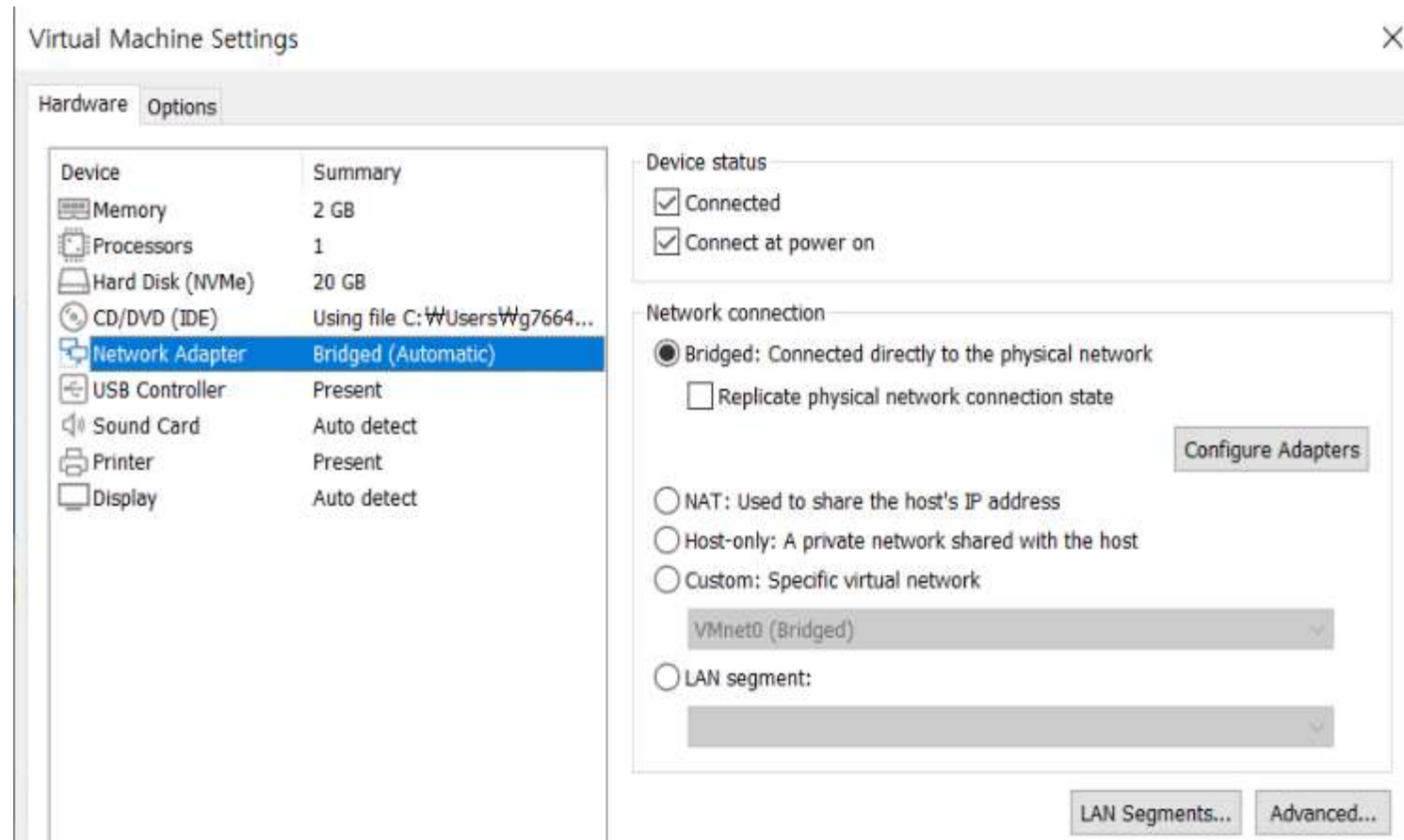
```
serverb@localhost:/home/serverb
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - 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
```

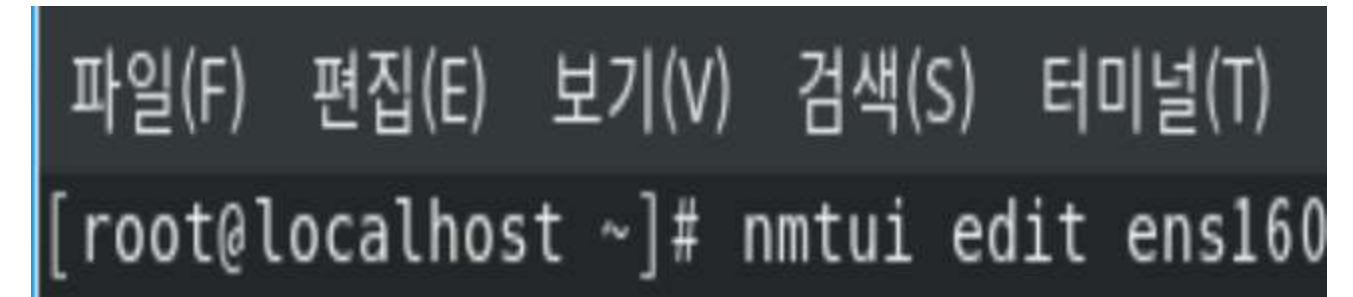

05. 방화벽 구축 실습

-client 설정

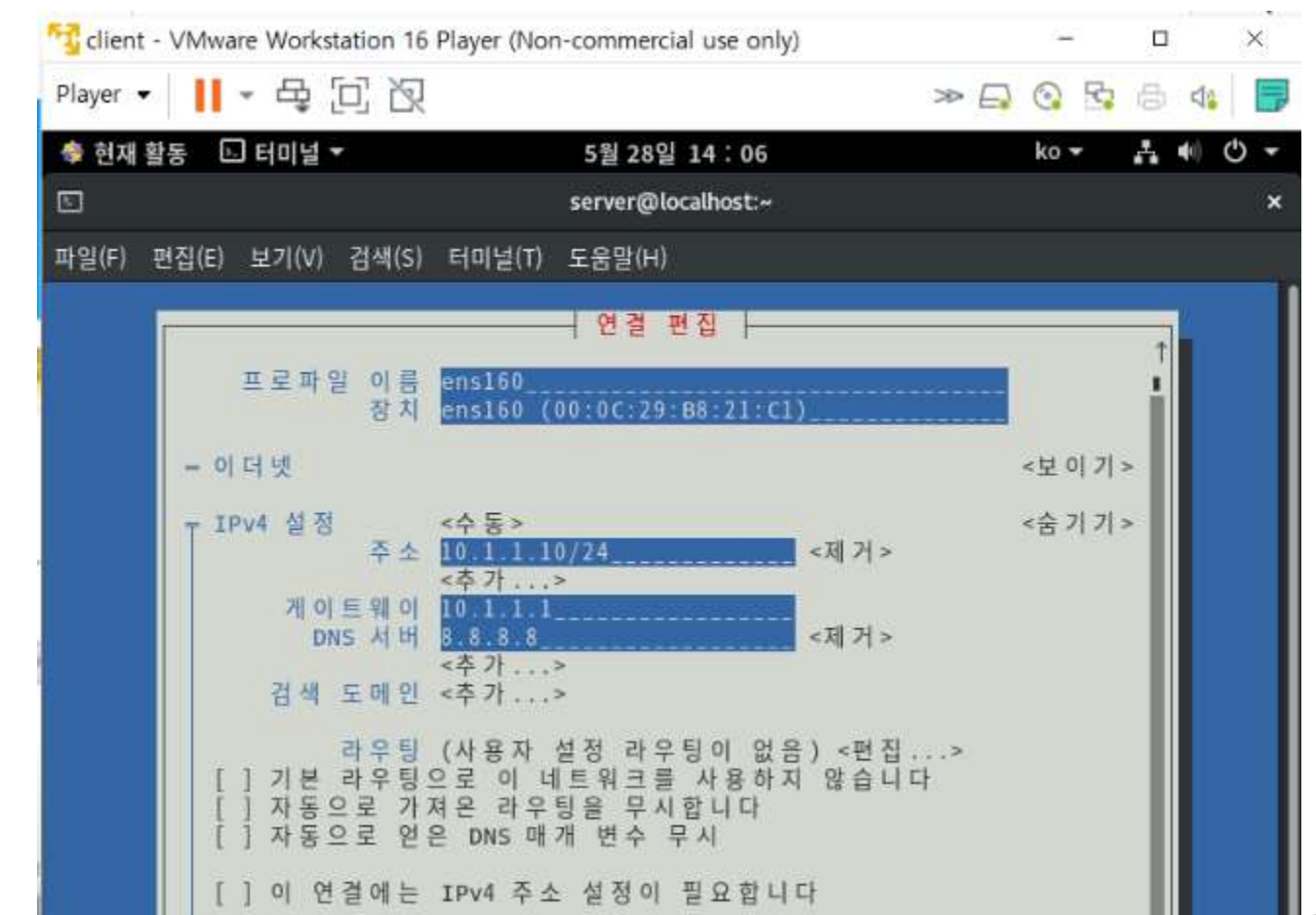
Network Adaptor 변경



nmtui 명령어 사용



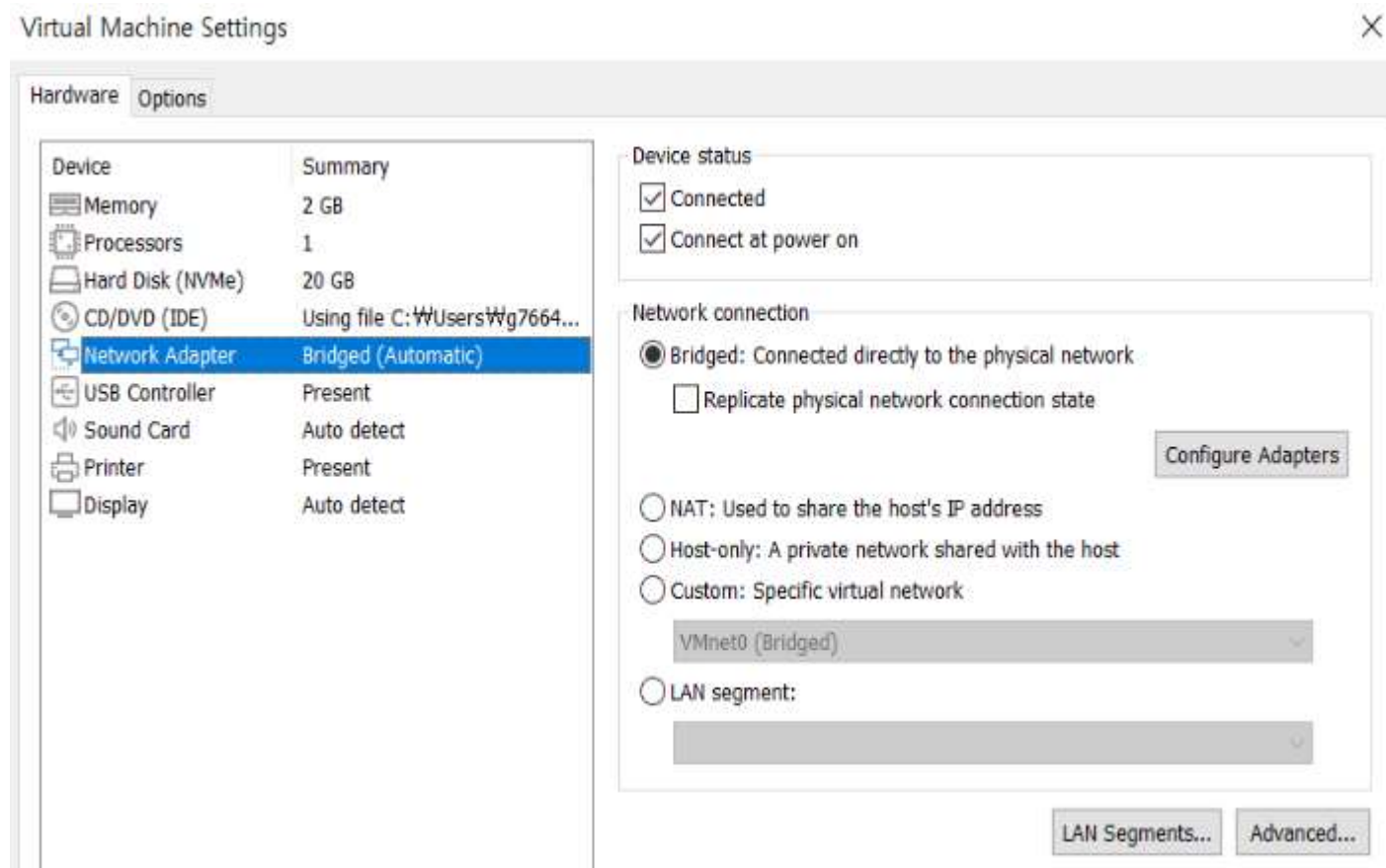
사설 IP 1 편집



05. 방화벽 구축 실습

-sever(B) 설정

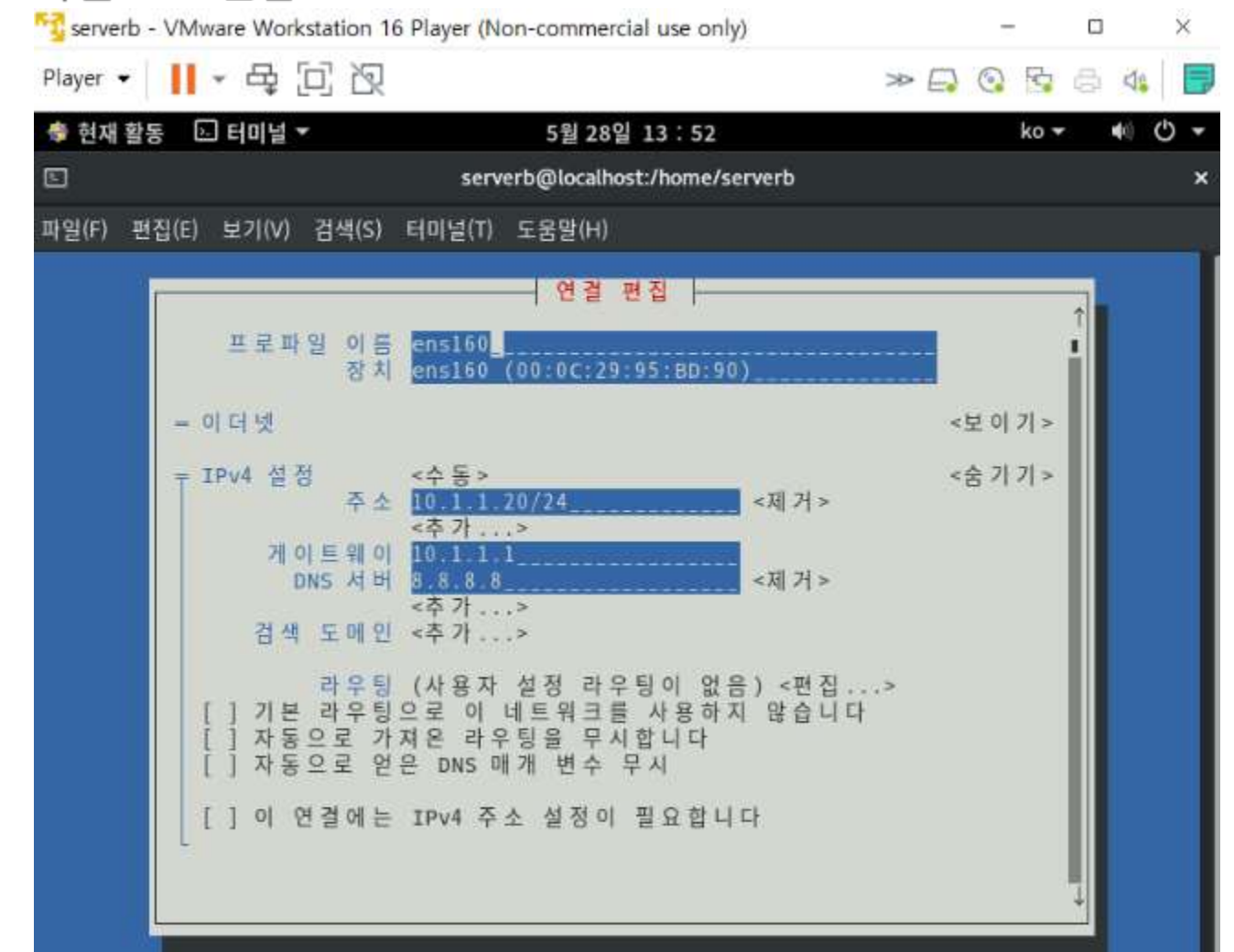
Network Adaptor 변경



nmtui 명령어 사용

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

사설 IP 2 편집

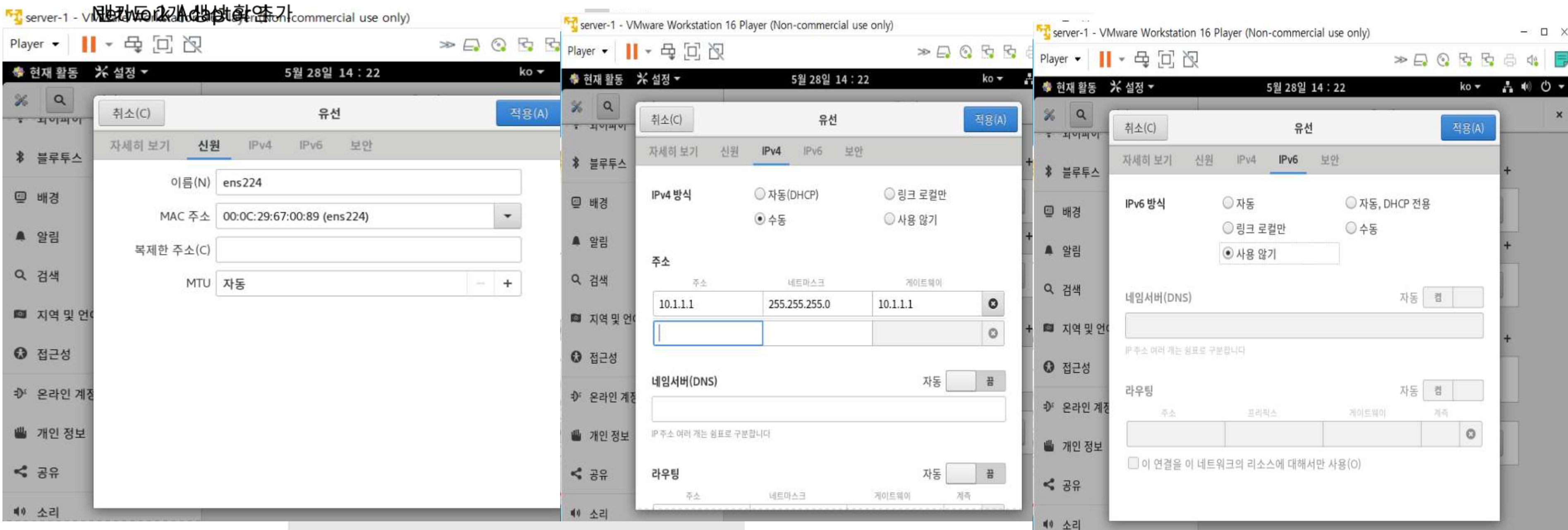


05. 방화벽 구축 실습

-server 설정

Network Adapter 추가

사설 IP 3 편집



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)

```
server@localhost:/etc/sysconfig/network-scripts
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=none
IPV4_FAILURE_FATAL=no
IPV6INIT=no
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=ens224
UUID=a29308f4-9ad4-486e-91c2-ce60d7e555fd
DEVICE=ens224
ONBOOT=yes
HWADDR=00:0C:29:67:00:89
IPADDR=10.1.1.1
PREFIX=24
GATEWAY=10.1.1.1
DEFROUTE=yes
PEERROUTES=no
-- INSERT --
```

제거

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

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

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
[root@localhost network-scripts]#
```

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
```

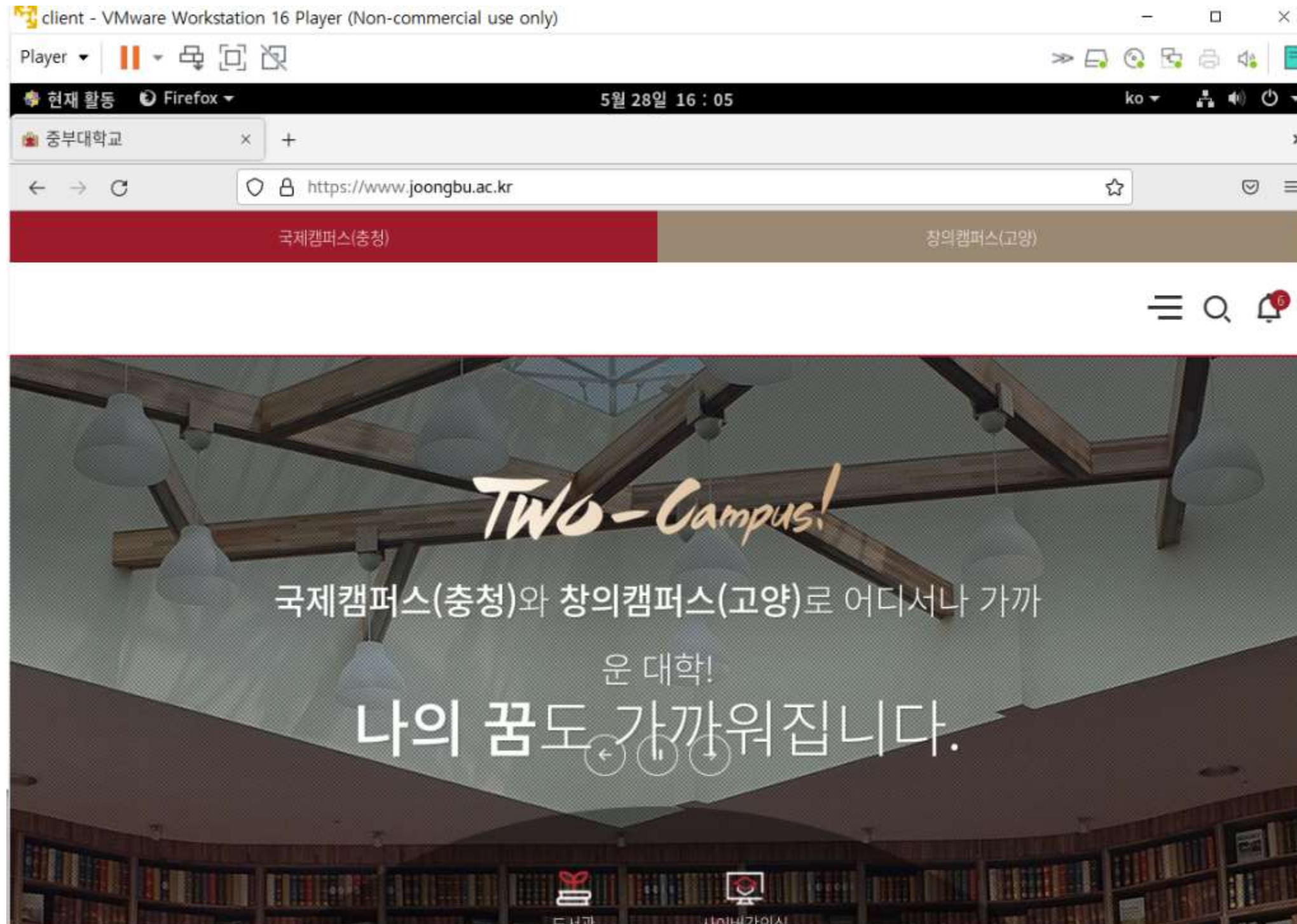
-방화벽 정책 설정

The screenshot shows the VMware Workstation 16 Player interface. The title bar indicates 'server-1 - VMware Workstation 16 Player (Non-commercial use only)'. The main window displays the '방화벽 설정' (Firewall Settings) for the 'server-1' VM. The '바인딩 활성화' (Binding Activation) section is expanded, showing a list of networks: 'virbr0 (virbr0)', 'ens224 (ens224)', and 'ens160 (ens160)'. The '인터페이스' (Interface) section is also expanded, showing a list of interfaces: 'block', 'dmz', 'drop', 'external', 'home', 'internal', 'libvirt', 'nm-shared', 'public', 'trusted', and 'work'. The 'public' interface is selected. The '서비스' (Service) section is expanded, showing a list of services: 'block', 'dmz', 'drop', 'external', 'home', 'internal', 'libvirt', 'nm-shared', 'public', 'trusted', and 'work'. The 'Masquerading' tab is selected, and the 'Masquerading' checkbox is checked. The 'Masquerading' section explains that this feature allows a local network to be connected to the Internet through a router, and that the local network is visible as a single address on the Internet. It also states that Masquerading is only supported for IPv4.

05.방화벽 구축 실습

-사설 네트워크에서 외부 인터넷으로 접속

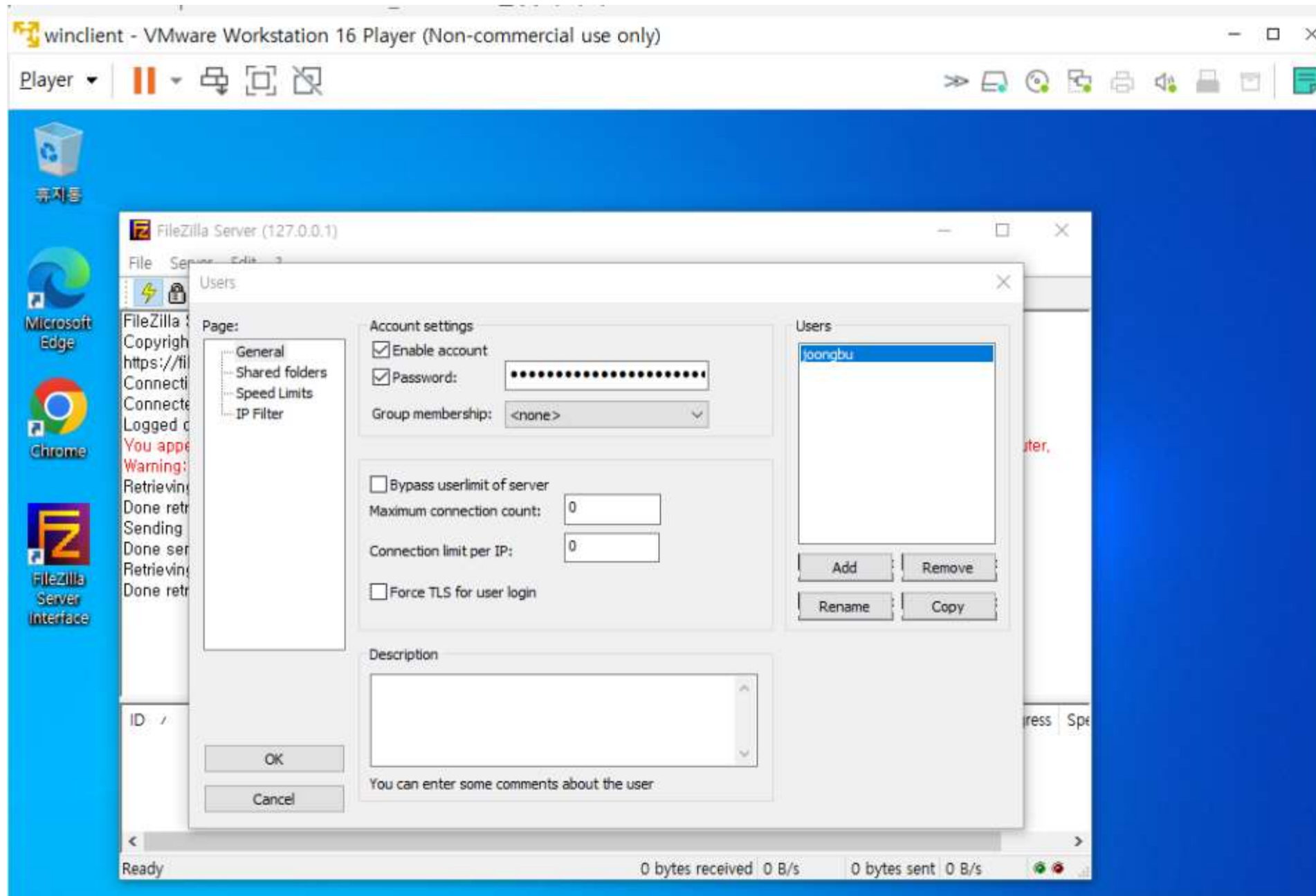
네트워크 접속 확인



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

```
PS C:\Windows\system32> netstat /an

활성 연결

프로토콜 로컬 주소      외부 주소      상태
TCP      0.0.0.0:21      0.0.0.0:0       LISTENING
TCP      0.0.0.0:135     0.0.0.0:0       LISTENING
TCP      0.0.0.0:445     0.0.0.0:0       LISTENING
TCP      0.0.0.0:5040    0.0.0.0:0       LISTENING
TCP      0.0.0.0:7680    0.0.0.0:0       LISTENING
TCP      0.0.0.0:49664   0.0.0.0:0       LISTENING
TCP      0.0.0.0:49665   0.0.0.0:0       LISTENING
TCP      0.0.0.0:49666   0.0.0.0:0       LISTENING
TCP      0.0.0.0:49667   0.0.0.0:0       LISTENING
TCP      0.0.0.0:49668   0.0.0.0:0       LISTENING
TCP      0.0.0.0:49669   0.0.0.0:0       LISTENING
TCP      127.0.0.1:14147 0.0.0.0:0       LISTENING
TCP      127.0.0.1:14147 127.0.0.1:49690 ESTABLISHED
TCP      127.0.0.1:49690 127.0.0.1:14147 ESTABLISHED
TCP      192.168.227.141:21 192.168.227.140:37918 ESTABLISHED
TCP      192.168.227.141:135 0.0.0.0:0       LISTENING
TCP      192.168.227.141:49670 20.197.71.89:443 ESTABLISHED
TCP      192.168.227.141:49672 104.74.155.64:80 TIME_WAIT
TCP      192.168.227.141:49676 13.107.21.200:443 TIME_WAIT
TCP      192.168.227.141:49677 52.152.90.172:443 TIME_WAIT
TCP      192.168.227.141:49680 20.44.229.112:443 TIME_WAIT
TCP      192.168.227.141:49685 204.79.197.219:443 TIME_WAIT
TCP      192.168.227.141:49686 204.79.197.219:443 TIME_WAIT
TCP      192.168.227.141:49688 13.107.21.200:443 TIME_WAIT
```

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

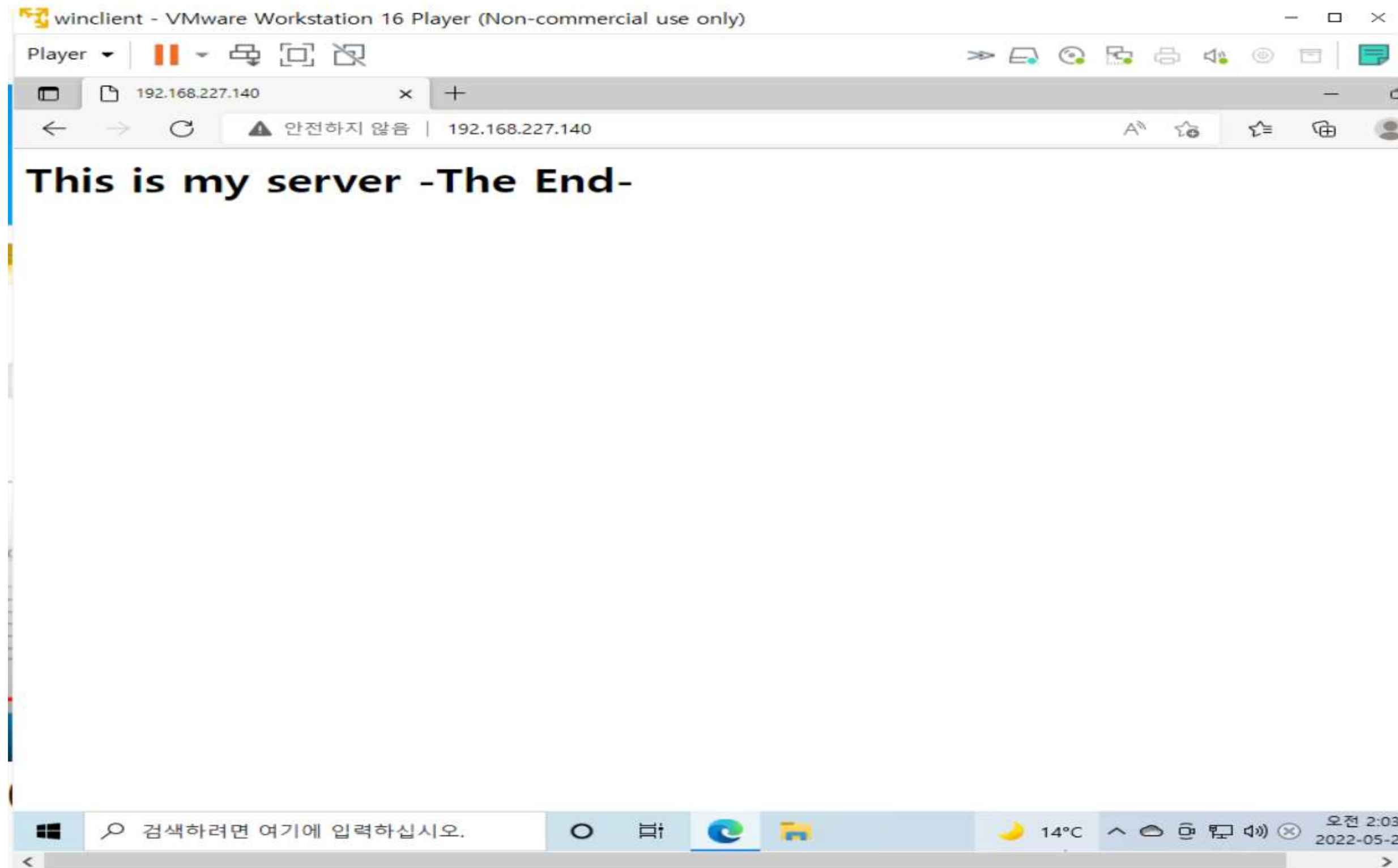
포트 리다이렉션 설정

```
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
[root@localhost server]# iptables --table nat --append PREROUTING --proto tcp --in-ter-
face ens160 --dport 80 --jump DNAT --to-destination 10.1.1.20
[root@localhost server]#
```

05.방화벽 구축 실습

-방화벽 구축 확인

웹 페이지 접속



감사합니다