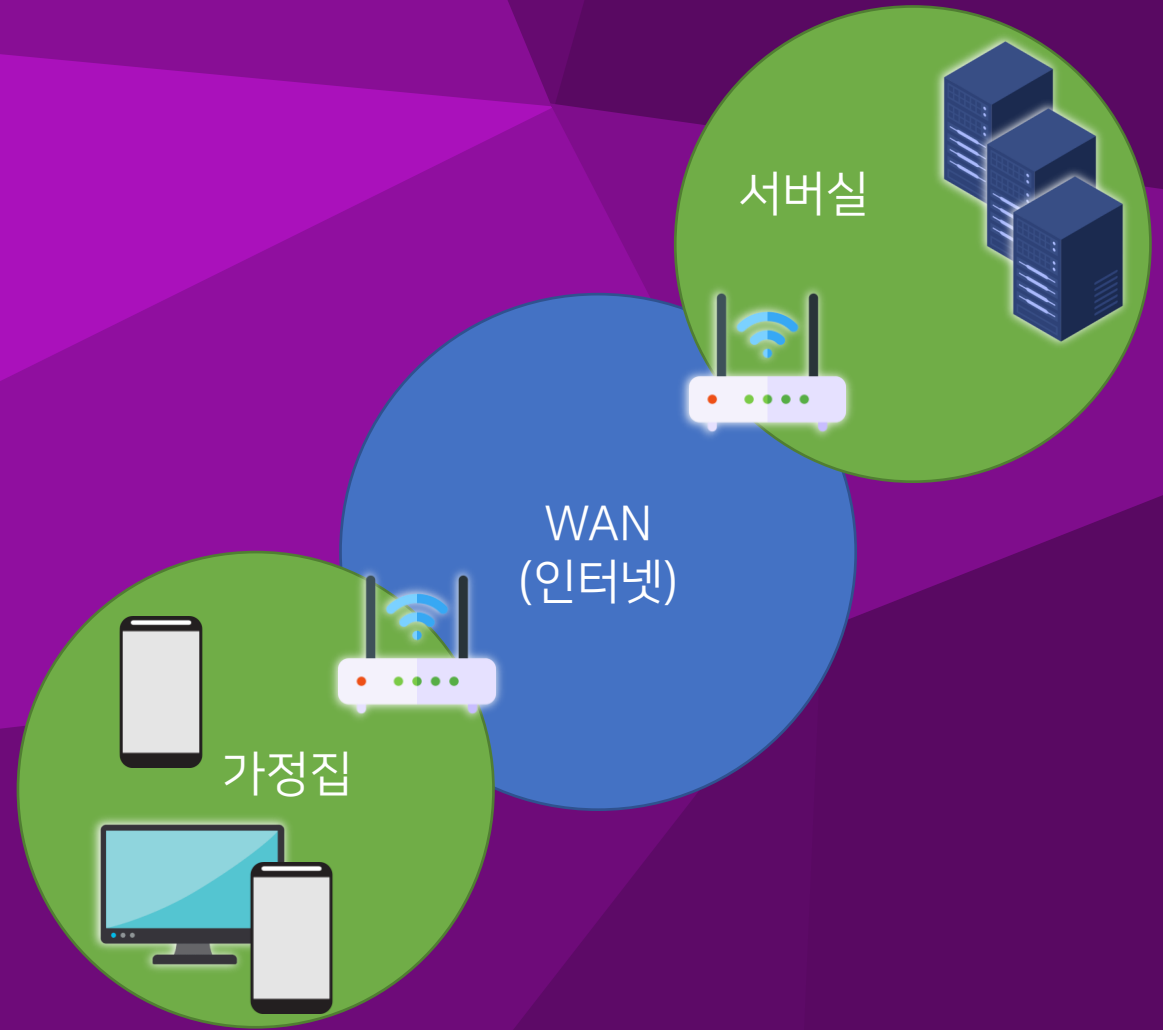


8장. 네트워크 환경 구축

운영 서버에 원격으로 접속할 수 있도록 네트워크를 설정하고,
보안을 위한 방화벽 설정, 외부에서의 접속을 위한 포트포워딩,
간편한 접속을 위한 도메인까지 설정해본다.

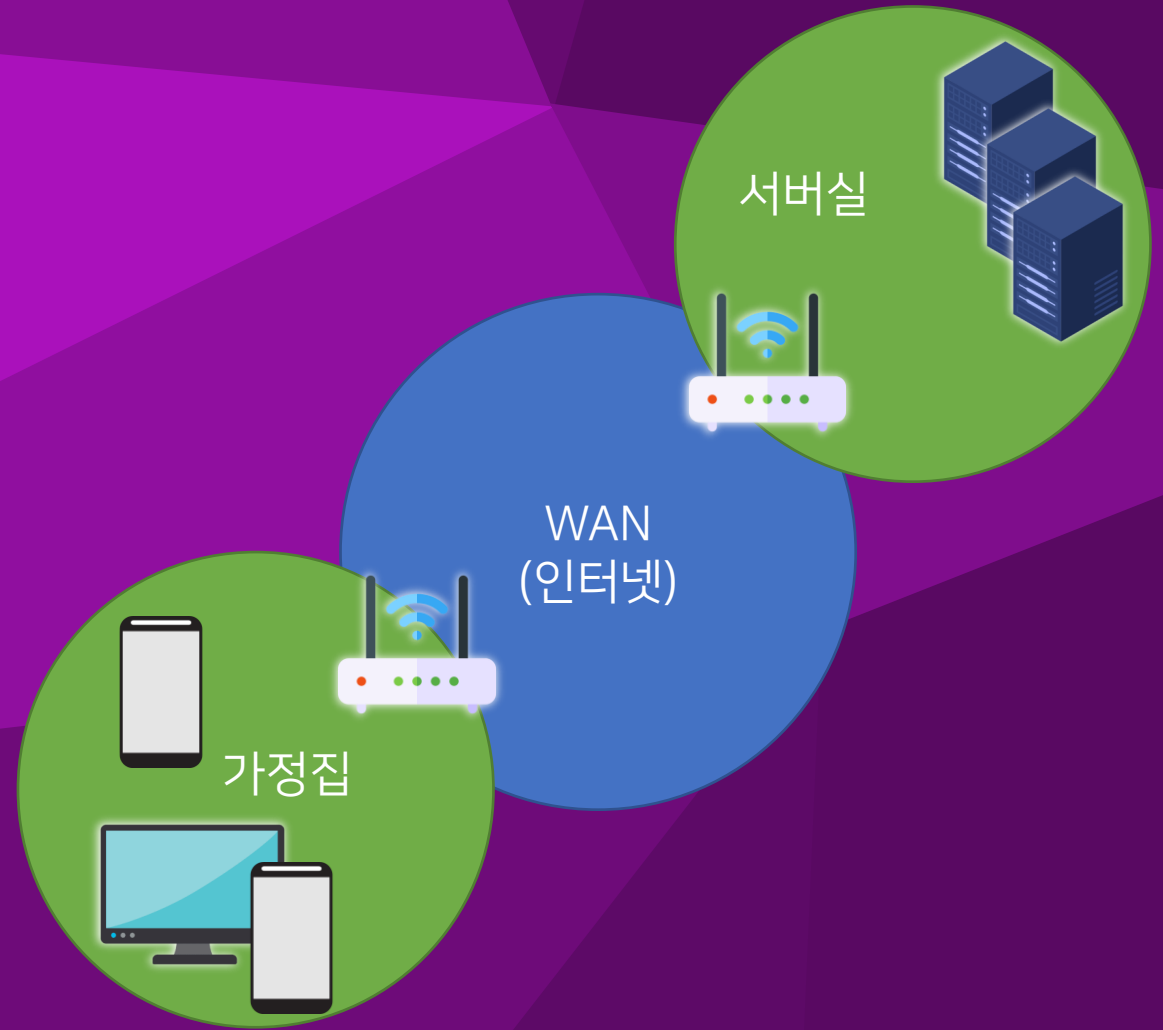
네트워크 다이어그램

- 일반적으로 집, 사무실, 학교 등의 장소에서는 공유기를 사용한다.
- 공유기에 PC, 태블릿, 스마트폰을 연결하여 인터넷을 사용한다.
- 공유기가 있으면 하나의 인터넷 선(케이블)으로 여러 대가 인터넷 사용 가능하다.



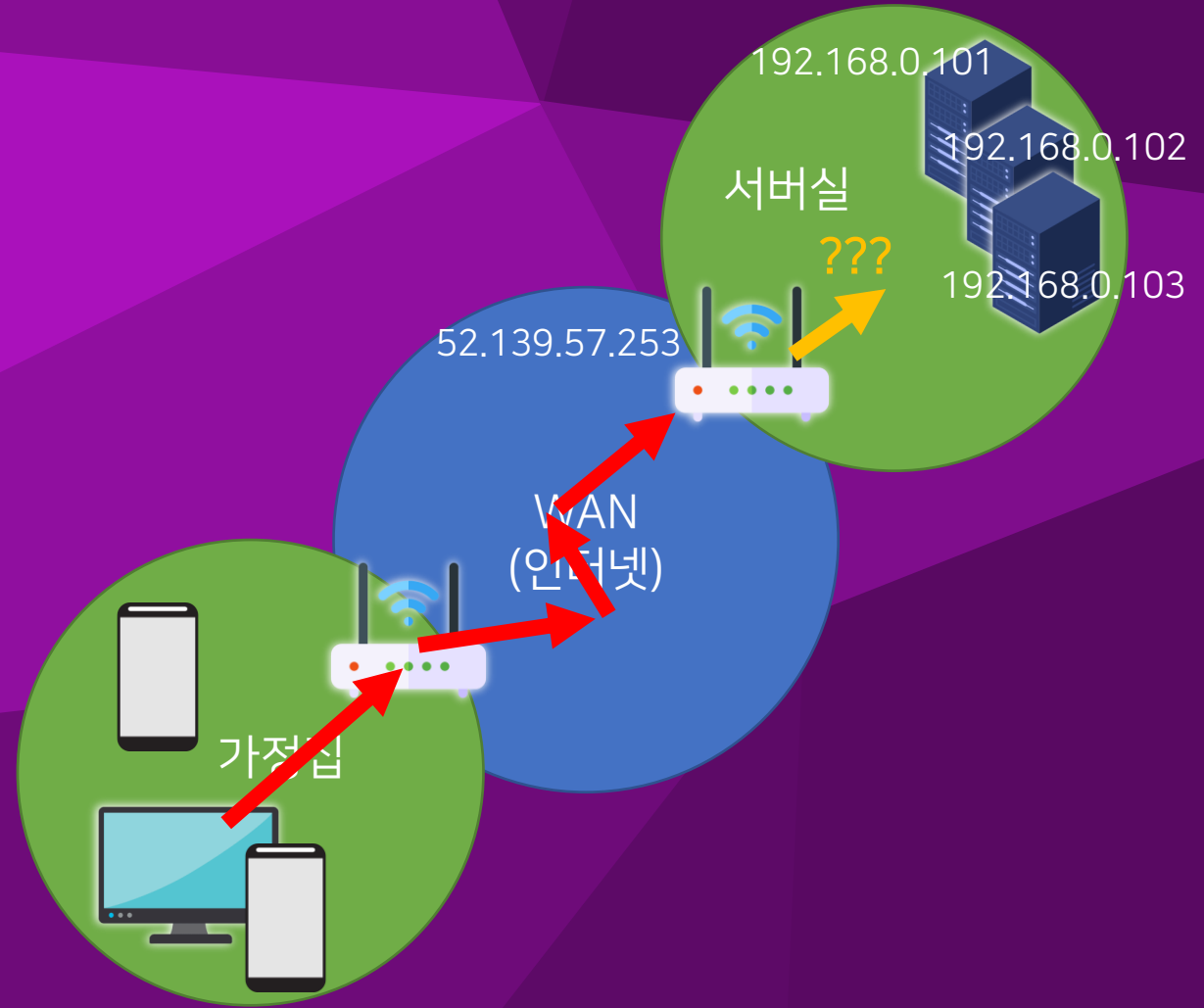
네트워크 다이어그램

- 서버 환경은 서버실마다 다르다.
- 공유기가 존재할 수도 있고 존재하지 않을 수도 있다.



포트 포워딩

- 서버 측이 공유기를 사용하는 환경이라면,
- 포트 포워딩을 해줘야 한다.
- 52.139.57.253:80 으로 연결한다고 할 때,
- 공유기에 연결된 3개의 서버 중 어느 서버로 가야 하는지 공유기는 모른다.
- 80번 포트로 접속하였을 때 어떤 서버로 가야 하는지 설정하는 것이 포트 포워딩이다.



포트 포워딩

- 만약 192.168.0.102 서버에서 웹 서버(:80)를 열었다면,
- 192.168.0.102로 포트 포워딩을 하여야 한다.



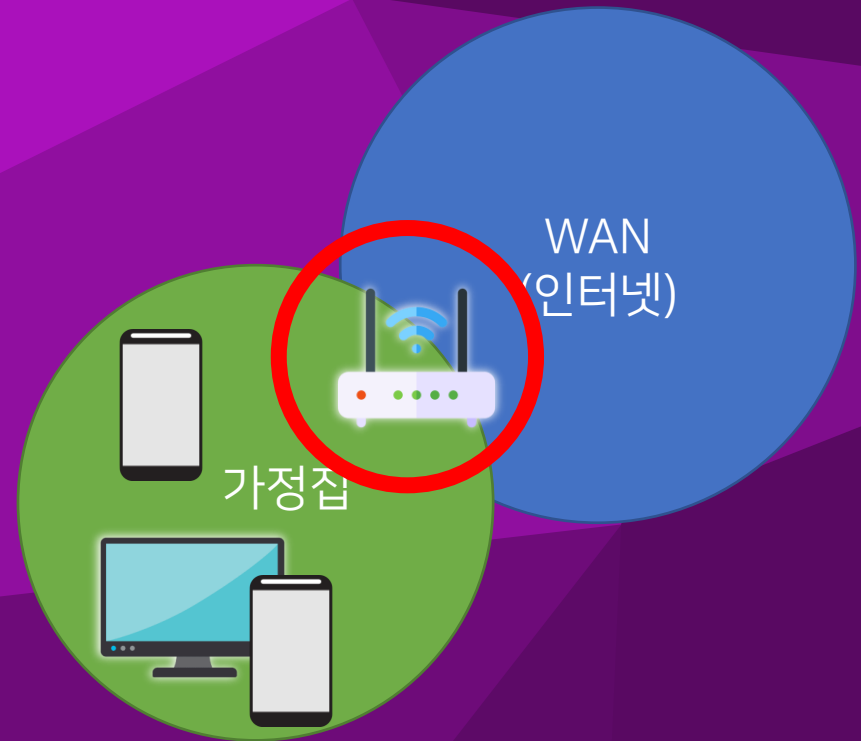
포트 포워딩

- 포트 포워딩은 공유기 설정 페이지에서 할 수 있다.
- 공유기 설정 페이지는 공유기의 IP를 입력하여 접속할 수 있다.
 - 모든 네트워크 장비(PC, 폰, 공유기 등)는 한 개의 IP를 가진다.
 - 따라서 공유기도 자신만의 IP를 가지고 있다.



[실습] 포트 포워딩

- 본인의 환경에서 포트 포워딩을 진행해보는 실습을 한다.
- 공유기가 있는 환경에서만 실습 진행이 가능하다.
- 실습을 통해 본인의 PC에서 오픈한 마인크래프트 서버에 외부에서 접속할 수 있도록 해본다.



[실습] 포트 포워딩

- 일반적으로 공유기는 192.168.0.1 아이피를 사용한다.
- 그렇지 않은 경우 ipconfig 명령을 사용하여 확인할 수 있다.
 - 윈도우는 ipconfig
 - 리눅스는 ifconfig
- 게이트웨이 주소가 공유기의 IP 주소이다.

이더넷 어댑터 이더넷 2:

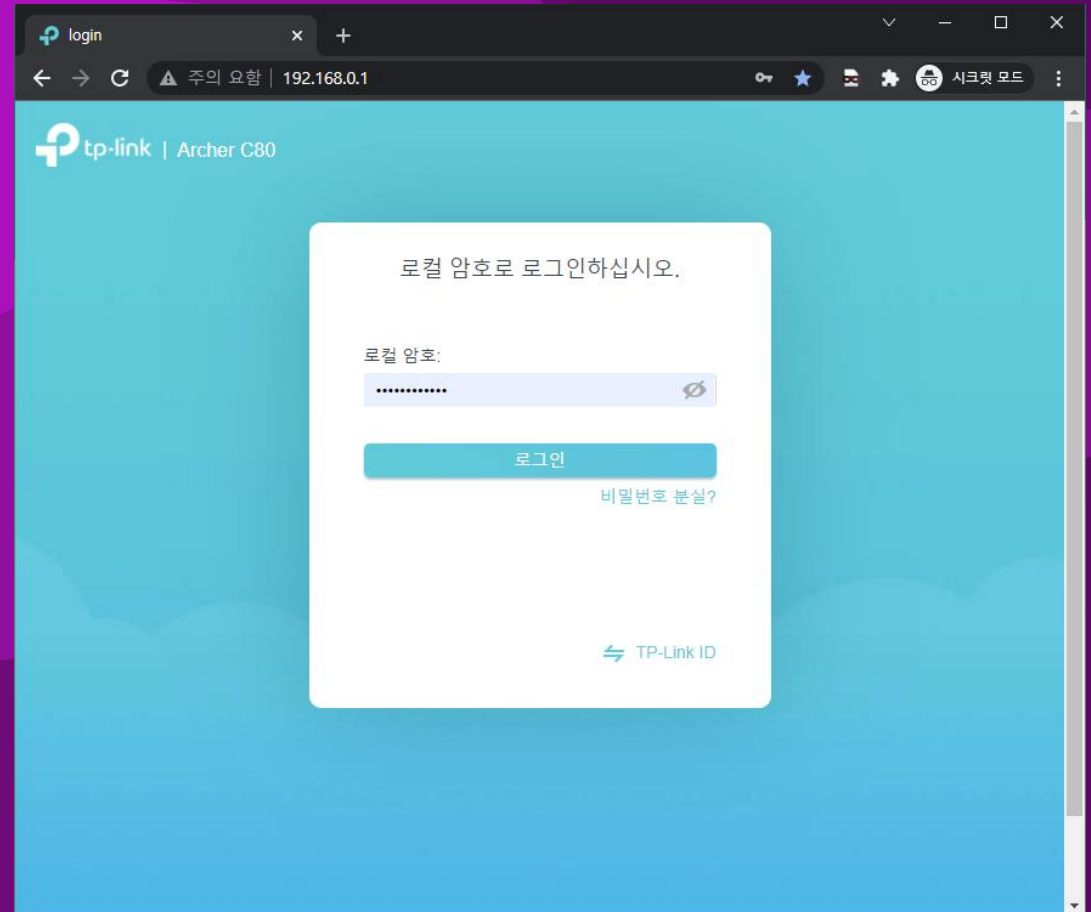
```
연결별 DNS 접미사. . . . . :  
링크-로컬 IPv6 주소 . . . . . : fe80::8477:64c5:259e:d4d5%13  
IPv4 주소 . . . . . : 192.168.0.100  
서브넷 마스크 . . . . . : 255.255.255.0  
기본 게이트웨이 . . . . . : 192.168.0.1
```

이더넷 어댑터 vEthernet (WSL):

```
연결별 DNS 접미사. . . . . :  
링크-로컬 IPv6 주소 . . . . . : fe80::6892:c59d:33eb:b8e4%42  
IPv4 주소 . . . . . : 172.18.160.1  
서브넷 마스크 . . . . . : 255.255.240.0  
기본 게이트웨이 . . . . . :
```

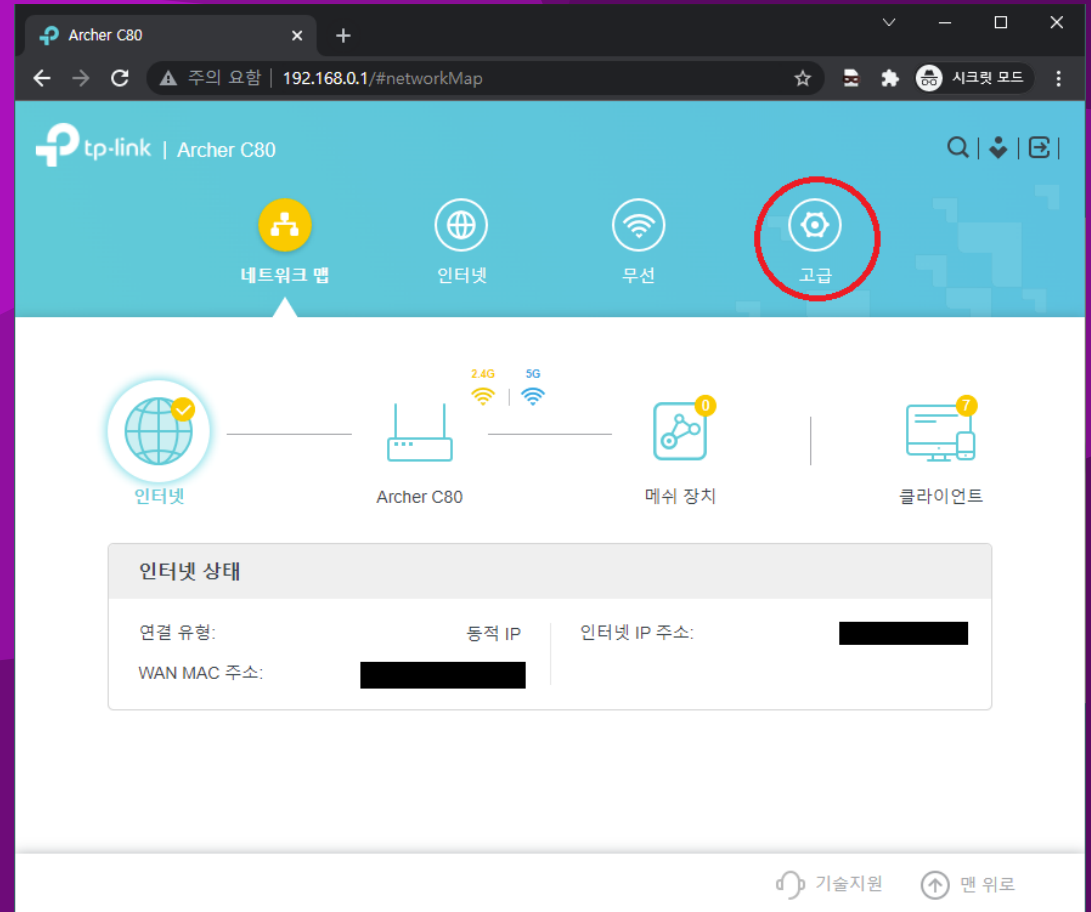

[실습] 포트 포워딩

- 웹 브라우저에서 공유기 IP로 접속하면 공유기에서 제공하는 홈페이지로 접속할 수 있다.
- 아무나 접근하지 못하도록 비밀번호가 설정되어 있다.
- 초기 계정/비밀번호는 보통 admin/admin 이다.
 - 또는 공유기 밑면에 적혀 있는 경우도 있다.
- 만일 admin/admin인 경우 변경해두는 것이 보안에 좋다.



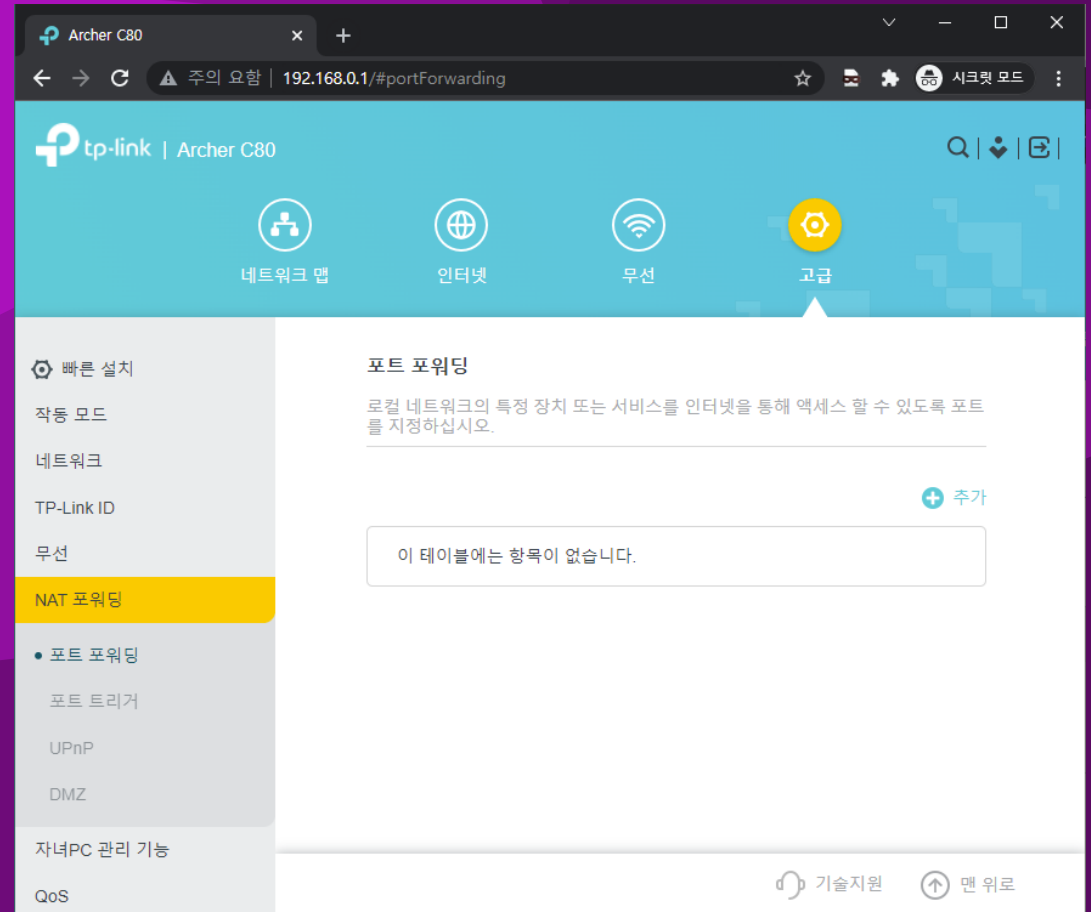
[실습] 포트 포워딩

- 로그인을 하면 메인 화면이 뜬다.
 - 공유기 모델 또는 제조사마다 다를 수 있다.
- 공유기 메뉴 중 설정 또는 고급으로 들어간다.



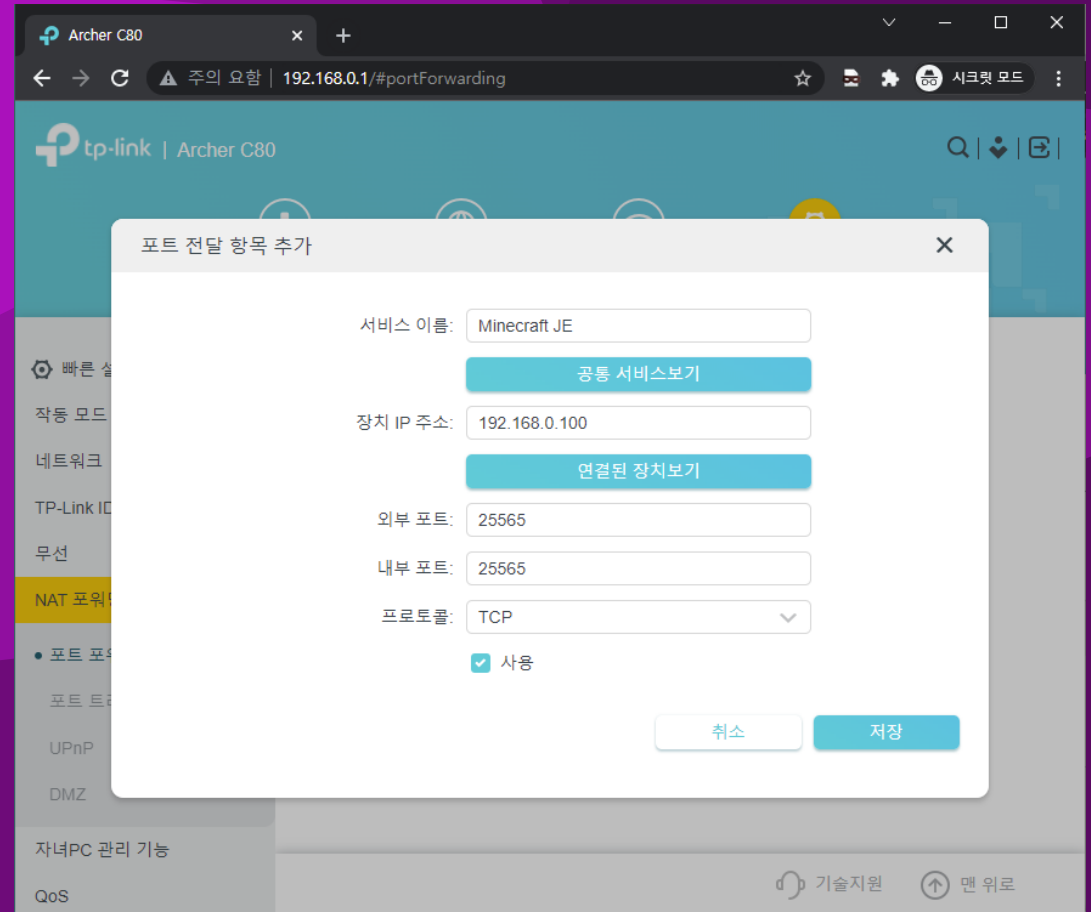
[실습] 포트 포워딩

- NAT 포워딩 > 포트 포워딩으로 들어간다.
 - TP-LINK 공유기 기준이다.
 - 공유기마다 메뉴 구조가 다르기 때문에, 메뉴를 하나씩 열어보며 포트 포워딩을 찾으면 된다.



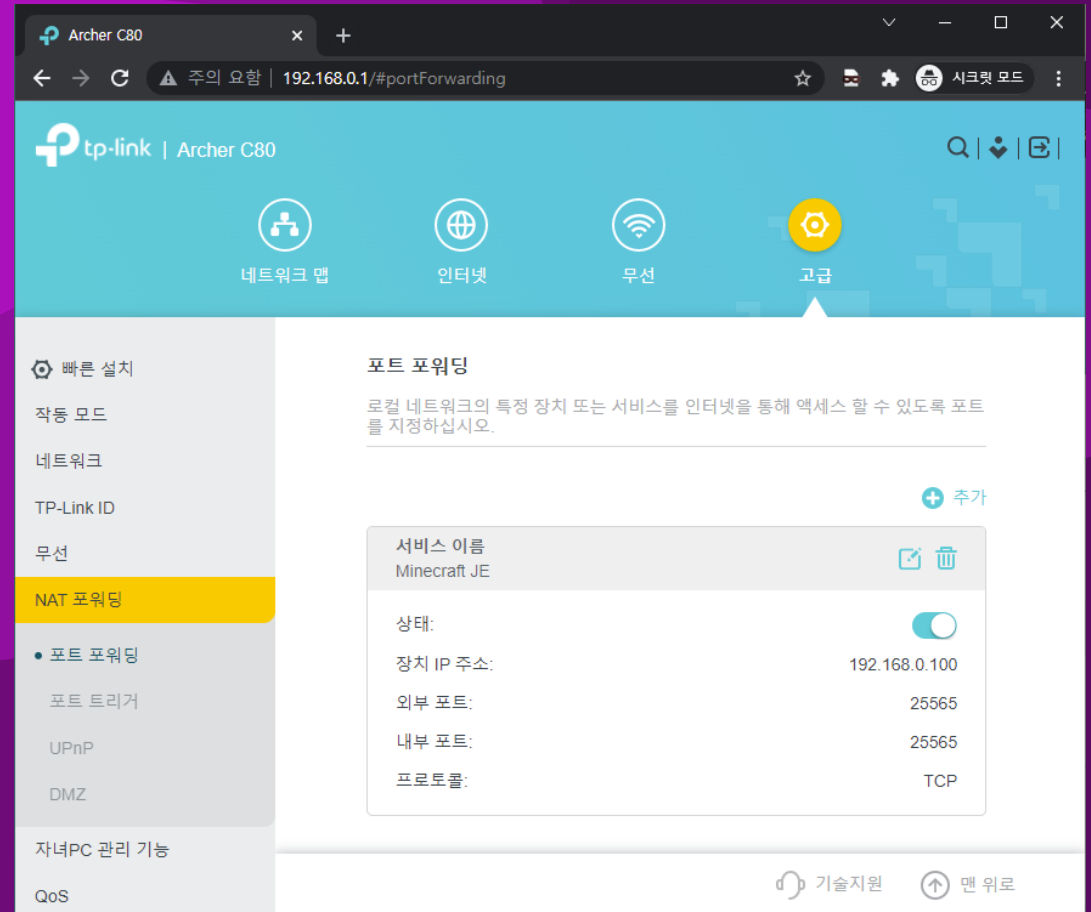
[실습] 포트 포워딩

- 추가를 클릭하고 포트포워딩할 IP, PORT를 입력하면 된다.
 - 본인의 PC IP 주소를 넣고
 - 자바 에디션의 포트를 설정한다.
- 마인크래프트 자바 에디션은 25565/TCP로 입력해 주면 된다.
- 베드락 에디션은 19132/UDP이다.
- 웹 서비스를 포트 포워딩한다면 80/TCP로 설정하면 된다.



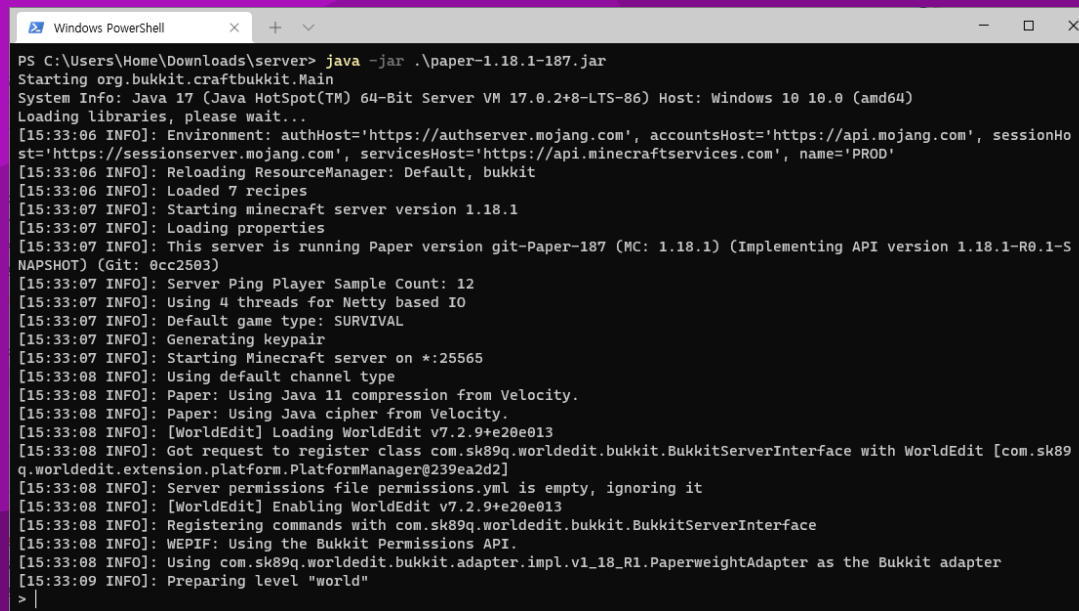
[실습] 포트 포워딩

- 저장을 누르고 포트 포워딩이 추가된 것을 확인한다.
- 포트 포워딩을 설정해두면 지정된 포트로 외부에서 접속할 수 있다.



[실습] 포트 포워딩

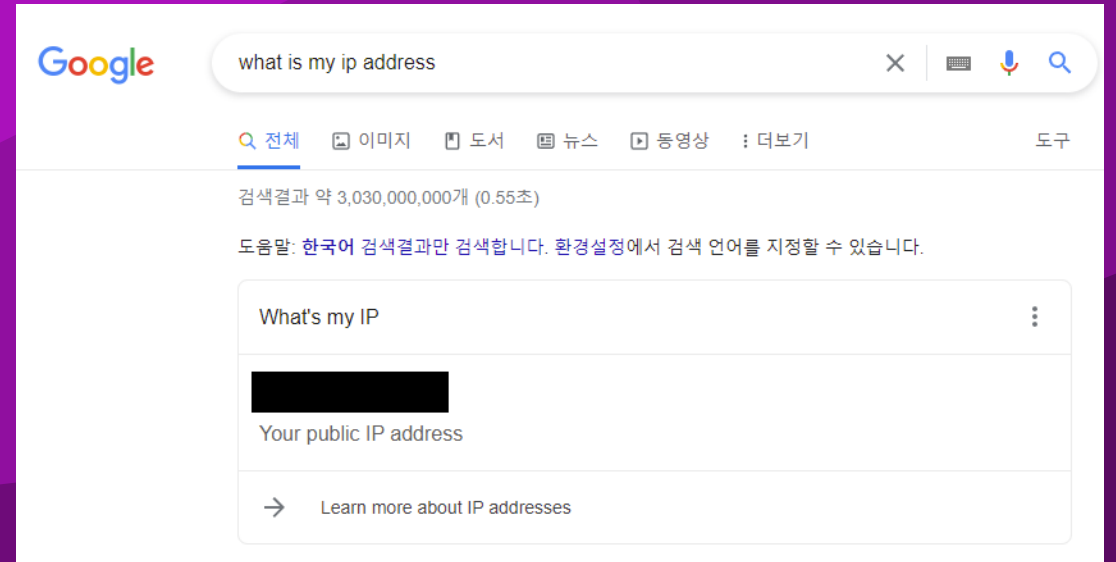
- 외부에서의 접속을 테스트하기 위해,
- 마인크래프트 서버를 켜다.



```
PS C:\Users\Home\Downloads\server> java -jar .\paper-1.18.1-187.jar
Starting org.bukkit.craftbukkit.Main
System Info: Java 17 (Java HotSpot(TM) 64-Bit Server VM 17.0.2+8-LTS-86) Host: Windows 10 10.0 (amd64)
Loading libraries, please wait...
[15:33:06 INFO]: Environment: authHost='https://authserver.mojang.com', accountsHost='https://api.mojang.com', sessionHost='https://sessionserver.mojang.com', servicesHost='https://api.minecraftservices.com', name='PROD'
[15:33:06 INFO]: Reloading ResourceManager: Default, bukkit
[15:33:06 INFO]: Loaded 7 recipes
[15:33:07 INFO]: Starting minecraft server version 1.18.1
[15:33:07 INFO]: Loading properties
[15:33:07 INFO]: This server is running Paper version git-Paper-187 (MC: 1.18.1) (Implementing API version 1.18.1-R0.1-SNAPSHOT) (Git: 0cc2503)
[15:33:07 INFO]: Server Ping Player Sample Count: 12
[15:33:07 INFO]: Using 4 threads for Netty based IO
[15:33:07 INFO]: Default game type: SURVIVAL
[15:33:07 INFO]: Generating keypair
[15:33:07 INFO]: Starting Minecraft server on *:25565
[15:33:08 INFO]: Using default channel type
[15:33:08 INFO]: Paper: Using Java 11 compression from Velocity.
[15:33:08 INFO]: Paper: Using Java cipher from Velocity.
[15:33:08 INFO]: [WorldEdit] Loading WorldEdit v7.2.9+e20e013
[15:33:08 INFO]: Got request to register class com.sk89q.worldedit.bukkit.BukkitServerInterface with WorldEdit [com.sk89q.worldedit.extension.platform.PlatformManager@239ea2d2]
[15:33:08 INFO]: Server permissions file permissions.yml is empty, ignoring it
[15:33:08 INFO]: [WorldEdit] Enabling WorldEdit v7.2.9+e20e013
[15:33:08 INFO]: Registering commands with com.sk89q.worldedit.bukkit.BukkitServerInterface
[15:33:08 INFO]: WEPIF: Using the Bukkit Permissions API.
[15:33:08 INFO]: Using com.sk89q.worldedit.bukkit.adapter.impl.v1_18_R1.PaperweightAdapter as the Bukkit adapter
[15:33:09 INFO]: Preparing level "world"
> |
```

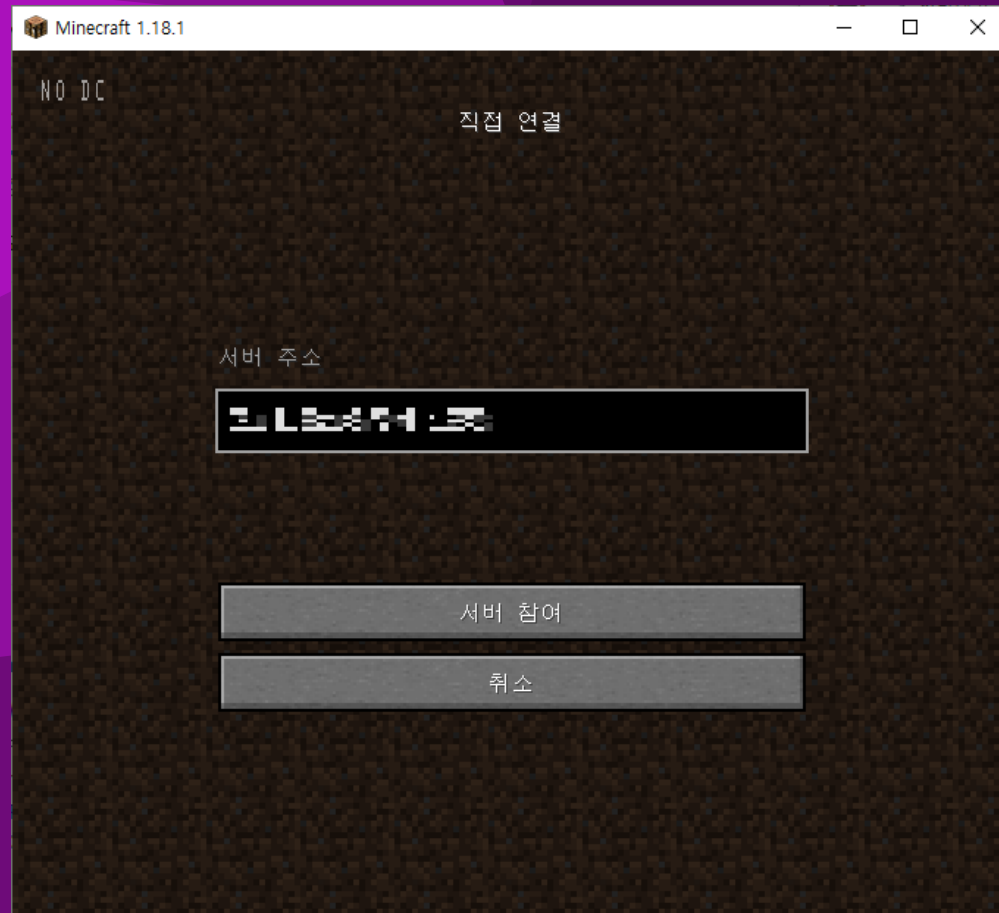
[실습] 포트 포워딩

- 외부에서의 접속을 위해 공인 IP 주소를 확인한다.
- 구글에서 what is my ip address 를 검색해보자.



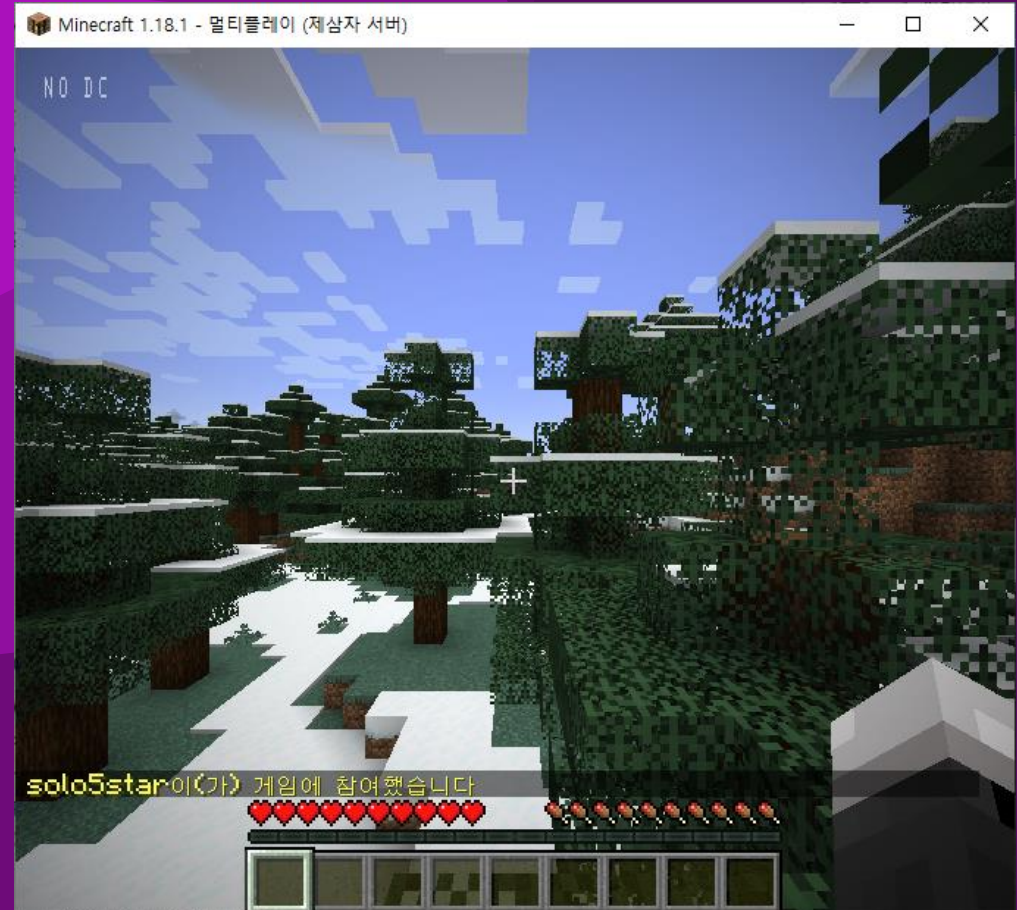
[실습] 포트 포워딩

- 마인크래프트를 켜고, 멀티 플레이 > 직접 연결에서 공인 IP 주소를 입력하고 접속한다.



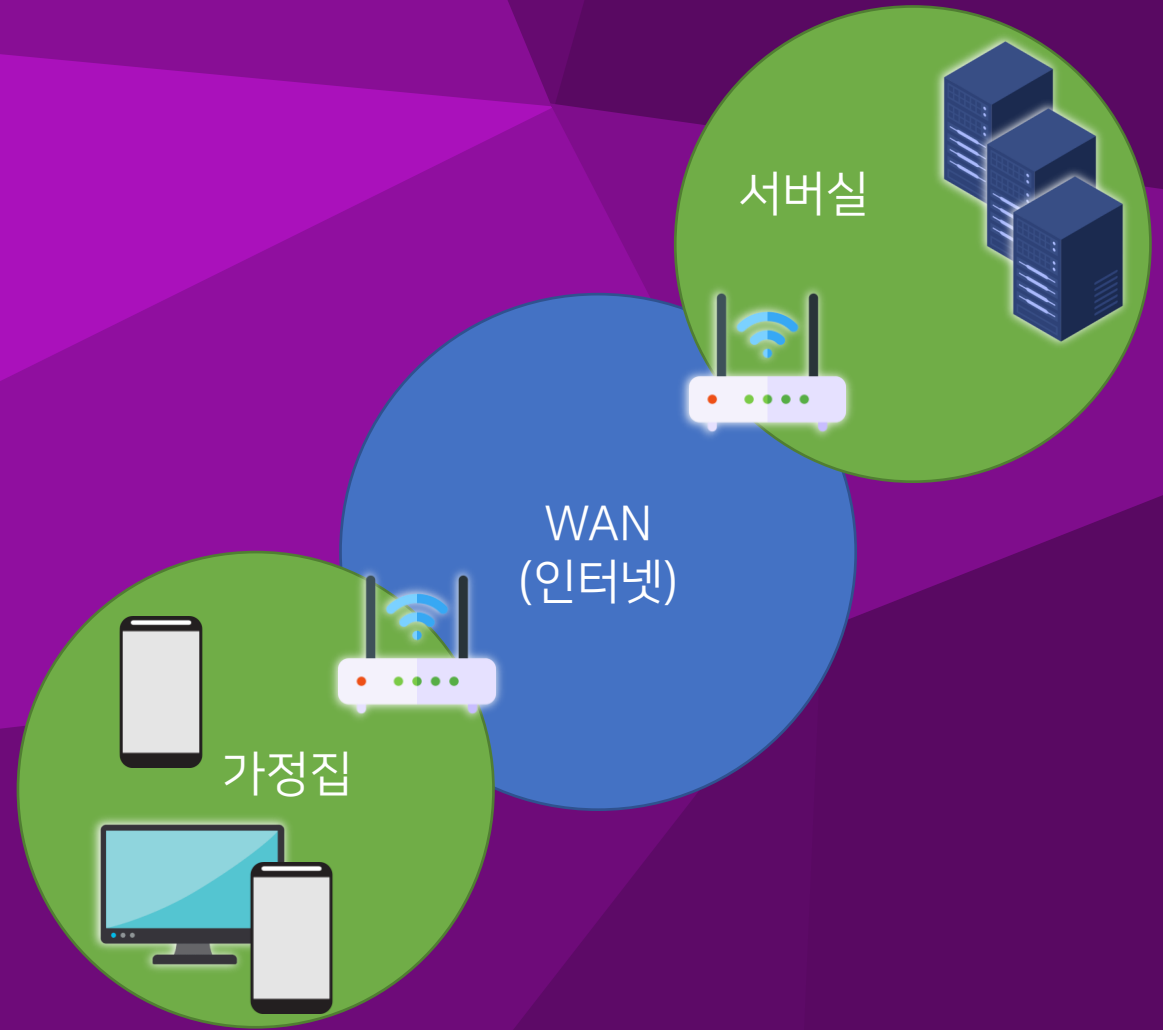
[실습] 포트 포워딩

- 서버에 접속이 잘 되는지 확인한다.
- 접속에 성공하였다면 포트 포워딩은 성공적으로 설정된 것이다.
- 다른 사람에게 공인 IP 주소를 알려주면 서버에 접속할 수 있다.



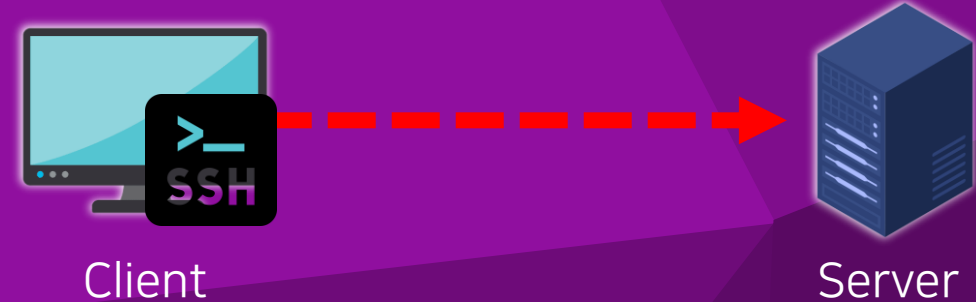
서버 원격 접속

- 일반적으로 서버는 서버실에 24시간 가동시키고,
- 다른 장소에서 서버 PC에 원격으로 접속하여 사용한다.
- 리눅스 터미널(Bash) 원격은 SSH,
- 파일 전송은 SFTP를 사용한다.



서버 원격 접속 - SSH

- SSH(Secure Shell Protocol)는 서버 PC에 접속하기 위해 사용하는 프로토콜이다.
 - 이름 그대로 암호화를 지원한다.
 - SSH 이전에는 Telnet이 주로 사용되었는데, 암호화가 이루어지지 않아 보안에 취약하였다.



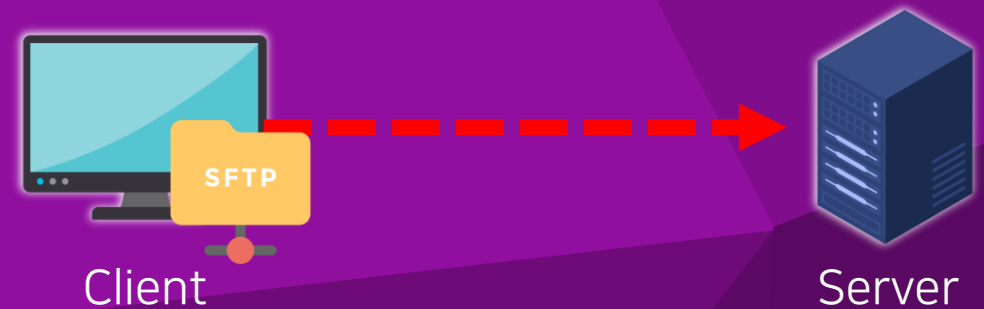
서버 원격 접속 - SSH

- 서버 측이 SSH Server가 되고,
- 접속하는 측이 SSH Client가 된다.
- 윈도우 10에는 SSH 접속을 위한 SSH Client가 기본적으로 설치되어 있다.
- 리눅스도 마찬가지로 SSH Client가 설치되어 있으며, SSH Server도 설치되어 있다.
 - *Ubuntu Server 기준



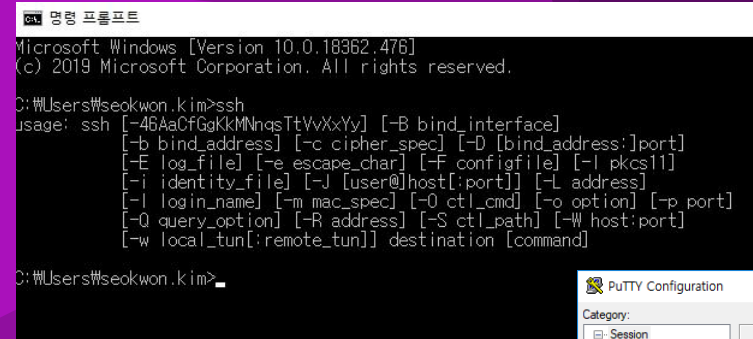
서버 원격 접속 - SFTP

- SFTP는 서버에 파일을 전송하는 방법이다.
- SSH를 기반으로 하기 때문에, SSH로 접속이 가능하다면 SFTP로도 연결할 수 있다.
- SSH는 터미널(Bash)만 사용이 가능하지만,
- SFTP는 파일 전송 또는 다운로드가 가능하다.



[실습] 서버 원격 접속 - SSH

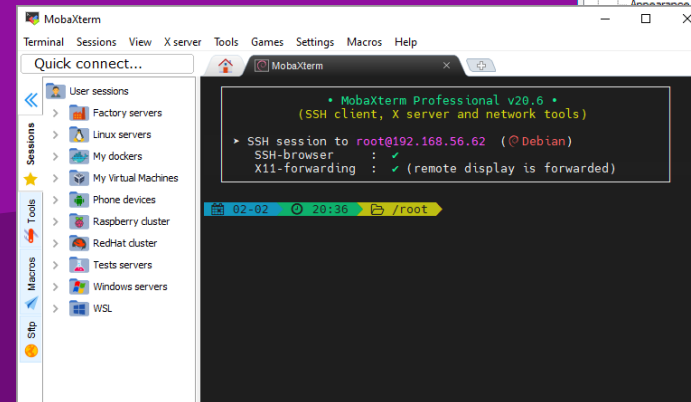
- 서버에 SSH로 접속하려면 SSH Client를 사용하여야 한다.
- 윈도우 10은 기본적으로 SSH Client가 내장되어 있다.
- 이 외에도 Putty, MobaXTerm 같은 별도 프로그램을 사용하여도 된다.



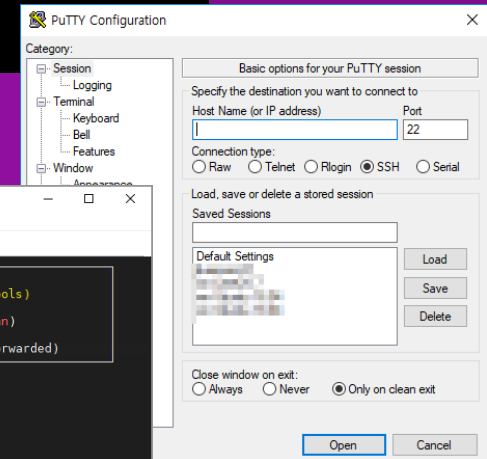
```
Microsoft Windows [Version 10.0.18362.476]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\seokwon.kim>ssh
usage: ssh [-46AaCfGgKkMnNqsTtVvXxYy] [-B bind_interface]
           [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
           [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
           [-i identity_file] [-J [user@]host[:port]] [-L address]
           [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
           [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
           [-w local_tun[:remote_tun]] destination [command]
```

Windows OpenSSH



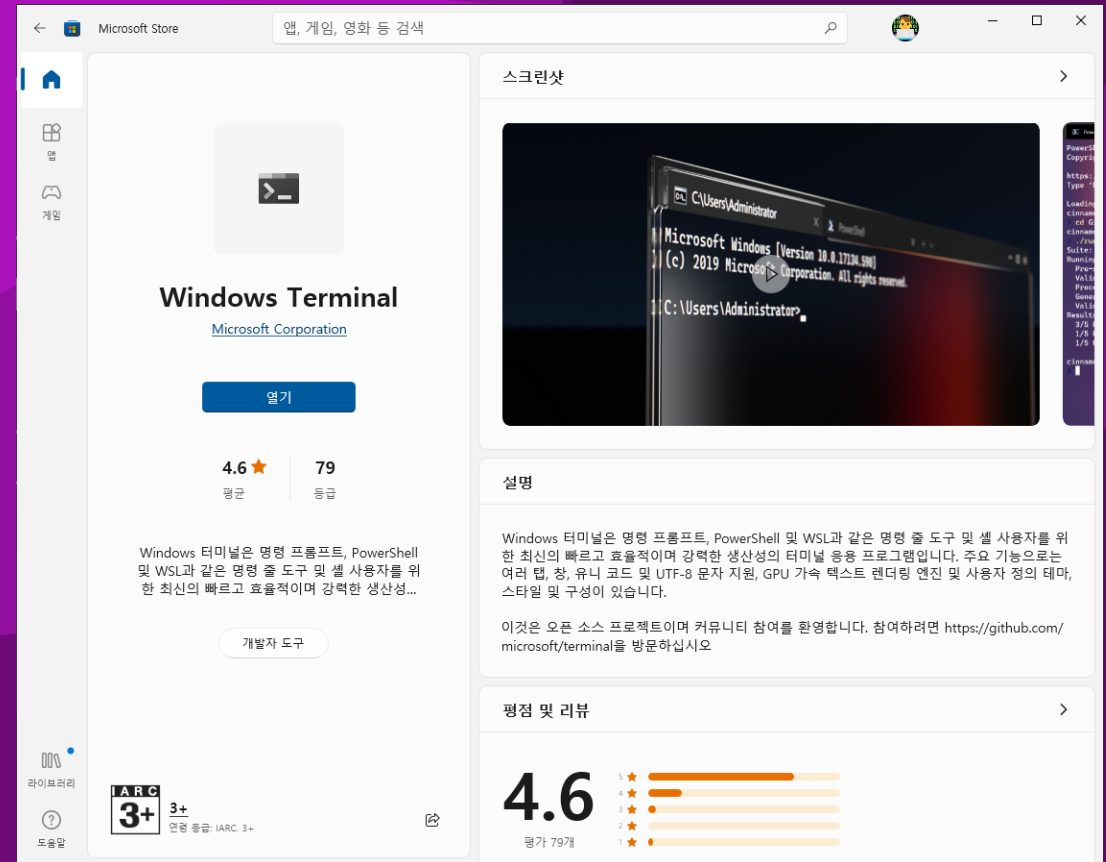
MobaXTerm



Putty

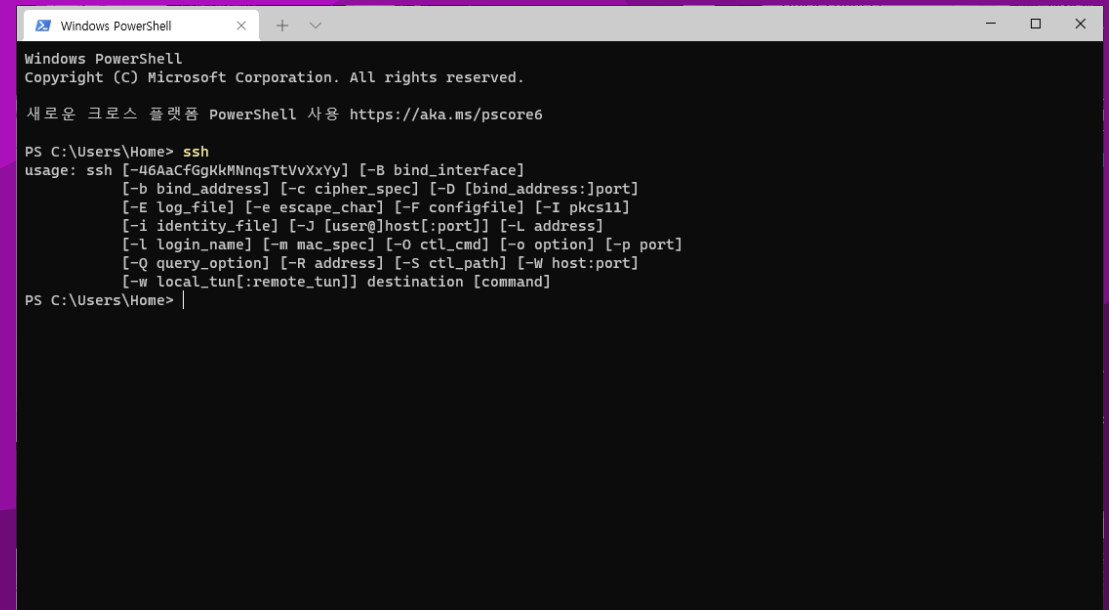
[실습] 서버 원격 접속 - SSH

- 실습에서는 Windows Terminal + Windows OpenSSH 를 사용하여 SSH 접속을 진행한다.
- Windows Terminal 이 설치되어 있지 않다면 Microsoft Store에서 다운받아 설치한다.



[실습] 서버 원격 접속 - SSH

- Windows Terminal을 켜고, ssh 를 입력한다.
- SSH usage가 뜬다면 SSH Client를 정상적으로 사용할 수 있다.



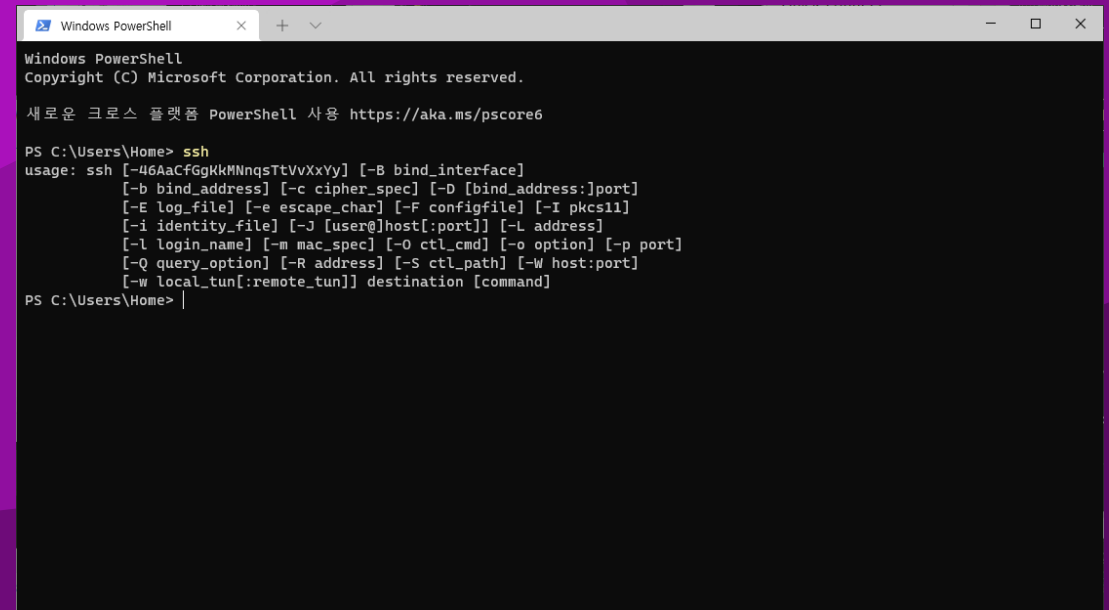
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

새로운 크로스 플랫폼 PowerShell 사용 https://aka.ms/pscore6

PS C:\Users\Home> ssh
usage: ssh [-46AaCfGgKkMnqsTtVvXxYy] [-B bind_interface]
          [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
          [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
          [-i identity_file] [-J [user@]host[:port]] [-L address]
          [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
          [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
          [-w local_tun[:remote_tun]] destination [command]
```


[실습] 서버 원격 접속 - SSH

- ssh 명령은 몇 가지 옵션을 제공한다. 그 중 자주 쓰는 것들은 아래와 같다.
 - -i <계정>: SSH 접속 시 사용할 계정
 - -p <포트번호>: SSH 접속 시 사용할 포트 번호. 기본 값은 22번이다.
- 서버 측에서 SSH 포트를 22번으로 쓴다면 -p 옵션은 생략하여도 된다.
- ssh -l myaccount <아이피 주소> 와 같은 형식으로 입력하여 서버에 접속할 수 있다.



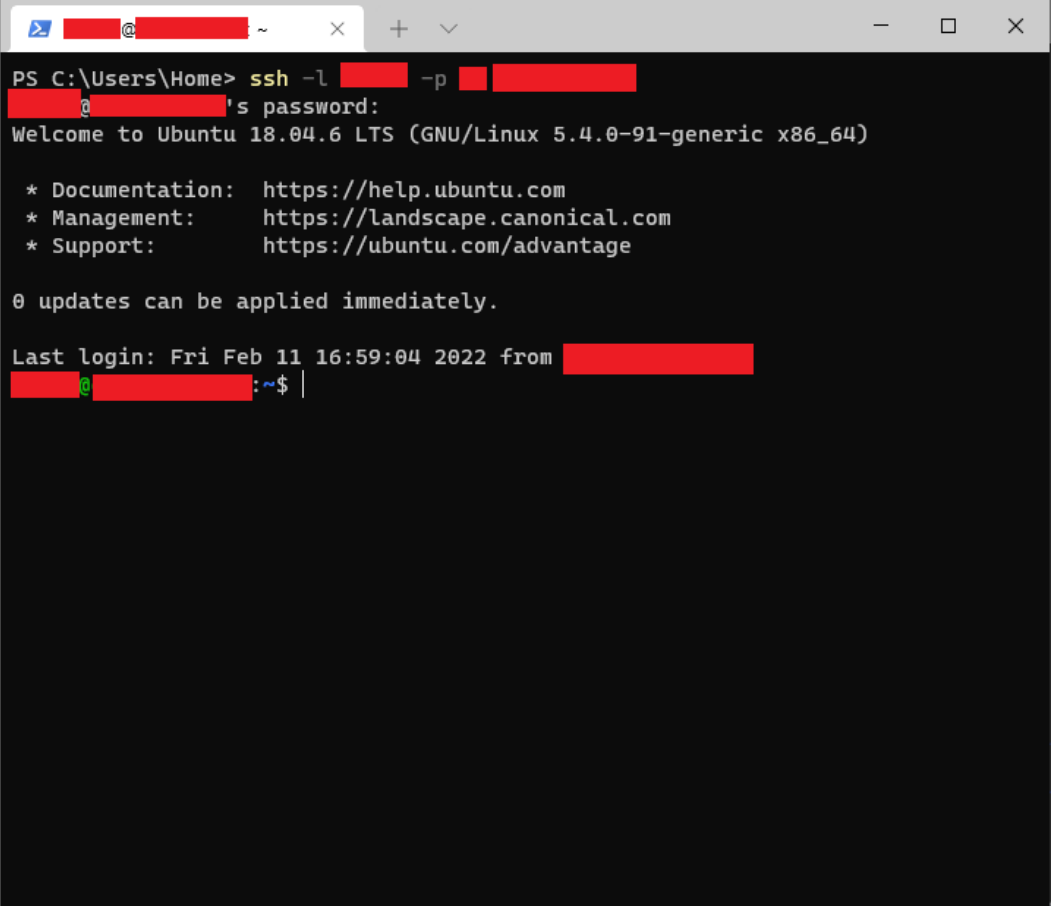
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

새로운 크로스 플랫폼 PowerShell 사용 https://aka.ms/pscore6

PS C:\Users\Home> ssh
usage: ssh [-46AaCfGgKkMnNqsTtVvXxYy] [-B bind_interface]
          [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
          [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
          [-i identity_file] [-J [user@]host[:port]] [-L address]
          [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
          [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
          [-w local_tun[:remote_tun]] destination [command]
```

[실습] 서버 원격 접속 - SSH

- SSH 명령을 사용하여 서버에 연결하면,
- 해당 계정에 대한 패스워드를 입력하여야 한다.
- 패스워드가 일치하다면 셸이 나타난다.
- 원격 접속에 성공하였다면 터미널에서 작업을 진행하면 된다.



```
PS C:\Users\Home> ssh -l [redacted] -p [redacted]
[redacted]'s password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-91-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

0 updates can be applied immediately.

Last login: Fri Feb 11 16:59:04 2022 from [redacted]
[redacted]@[redacted]:~$ |
```

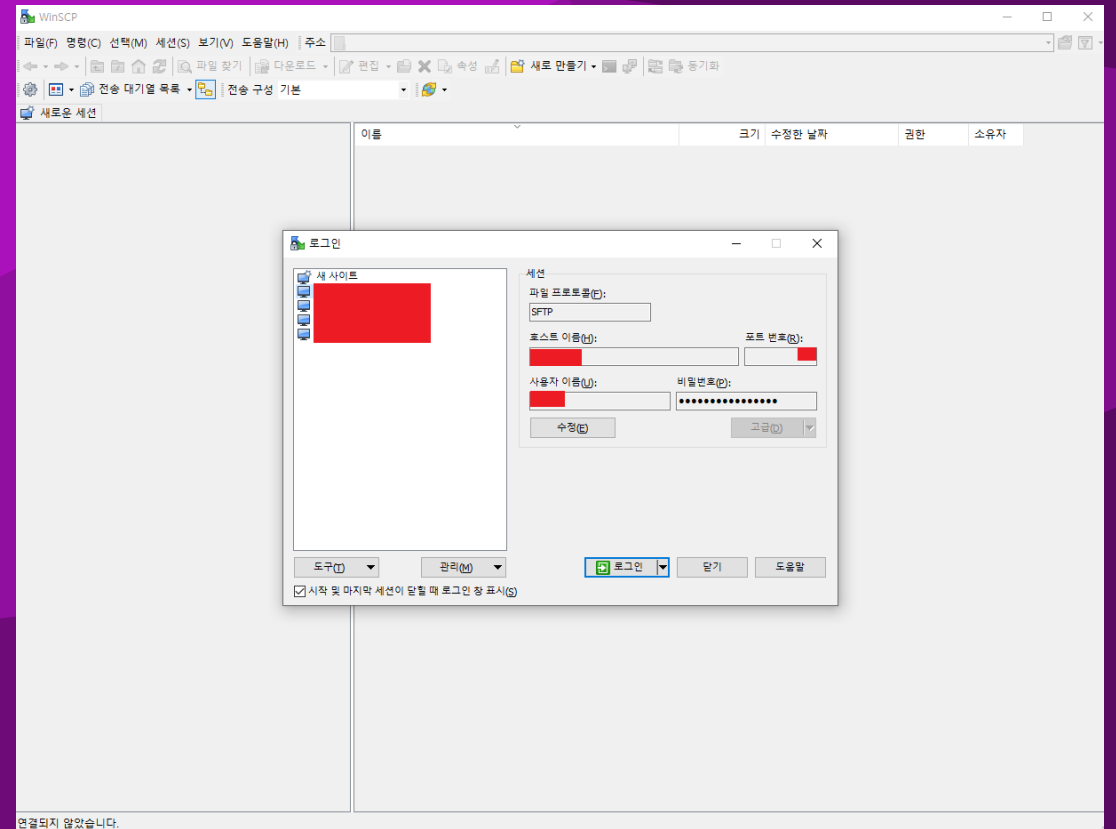
[실습] 서버 원격 접속 - SFTP

- SFTP는 별도 클라이언트를 설치하여야 한다.
- 가장 많이 사용되는 프로그램에는 WinSCP가 있다.
- WinSCP 다운로드 링크
 - <https://winscp.net/eng/download.php>



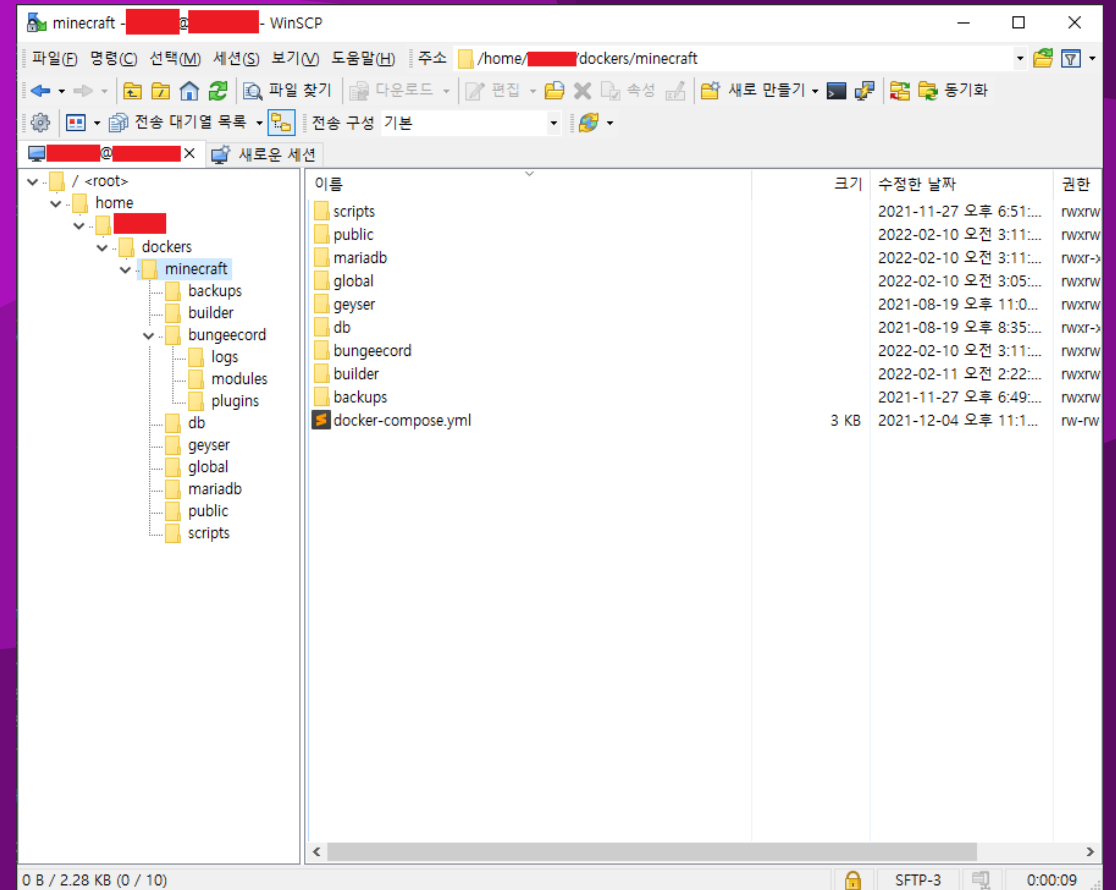
[실습] 서버 원격 접속 - SFTP

- WinSCP를 다운로드하고 열면, 로그인 창이 뜬다.
- SSH에서 사용하던 것들을 그대로 사용하면 된다.
- 호스트 이름(서버의 IP 주소), 포트 번호, 사용자 이름, 비밀번호를 입력한다.
- 로그인 버튼을 누르면 입력된 계정으로 접속된다.



[실습] 서버 원격 접속 - SFTP

- 성공적으로 로그인하면 파일 탐색기 화면이 나타난다.
- 윈도우 파일 탐색기처럼 파일을 이동하거나, 로컬의 파일을 전송할 수도 있다.



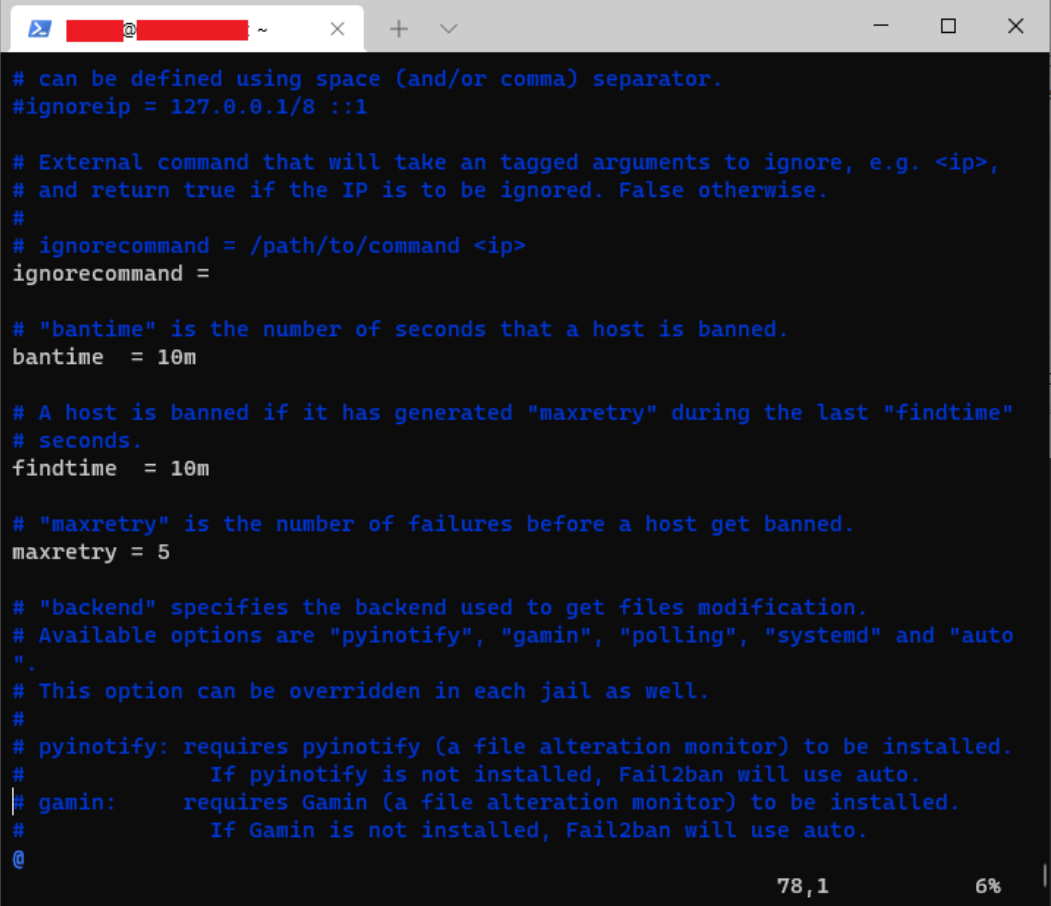
보안 및 방화벽 설정

- 서버의 보안은 중요하다.
- 서버를 열어두면 전 세계 어디서든, 누구나 접속할 수 있다.
- 불특정 누군가가 악의를 가지고 해킹을 시도할 수도 있다.
- 서버는 중요한 데이터도 있기 때문에 일반 PC보다 보안을 엄중히 신경써야 한다.



[실습] 보안 및 방화벽 설정 - fail2ban

- 가장 기본적인 SSH 보안부터 설정한다.
- fail2ban은 apt install 로 설치할 수 있는 패키지이다.
- SSH 로그인 시도가 일정 횟수가 넘으면 자동으로 차단시켜주는 역할을 한다.
- sudo apt install fail2ban 으로 설치하면 된다.
- 기본적으로 5회 실패 시 10분간 차단되도록 설정되어 있다.



```
# can be defined using space (and/or comma) separator.
#ignoreip = 127.0.0.1/8 ::1

# External command that will take an tagged arguments to ignore, e.g. <ip>,
# and return true if the IP is to be ignored. False otherwise.
#
# ignorecommand = /path/to/command <ip>
ignorecommand =

# "bantime" is the number of seconds that a host is banned.
bantime = 10m

# A host is banned if it has generated "maxretry" during the last "findtime"
# seconds.
findtime = 10m

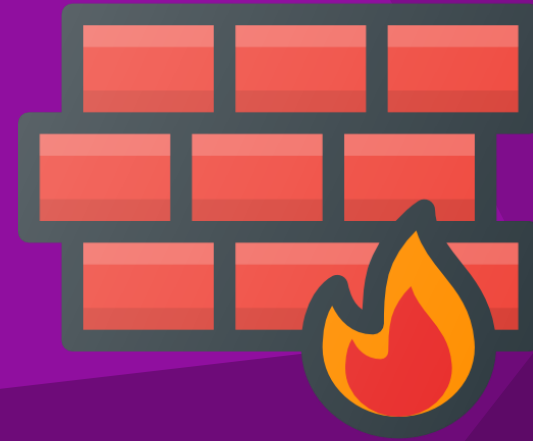
# "maxretry" is the number of failures before a host get banned.
maxretry = 5

# "backend" specifies the backend used to get files modification.
# Available options are "pyinotify", "gamin", "polling", "systemd" and "auto".
# This option can be overridden in each jail as well.
#
# pyinotify: requires pyinotify (a file alteration monitor) to be installed.
#             If pyinotify is not installed, Fail2ban will use auto.
# gamin:     requires Gamin (a file alteration monitor) to be installed.
#             If Gamin is not installed, Fail2ban will use auto.
@
```

78,1 6%

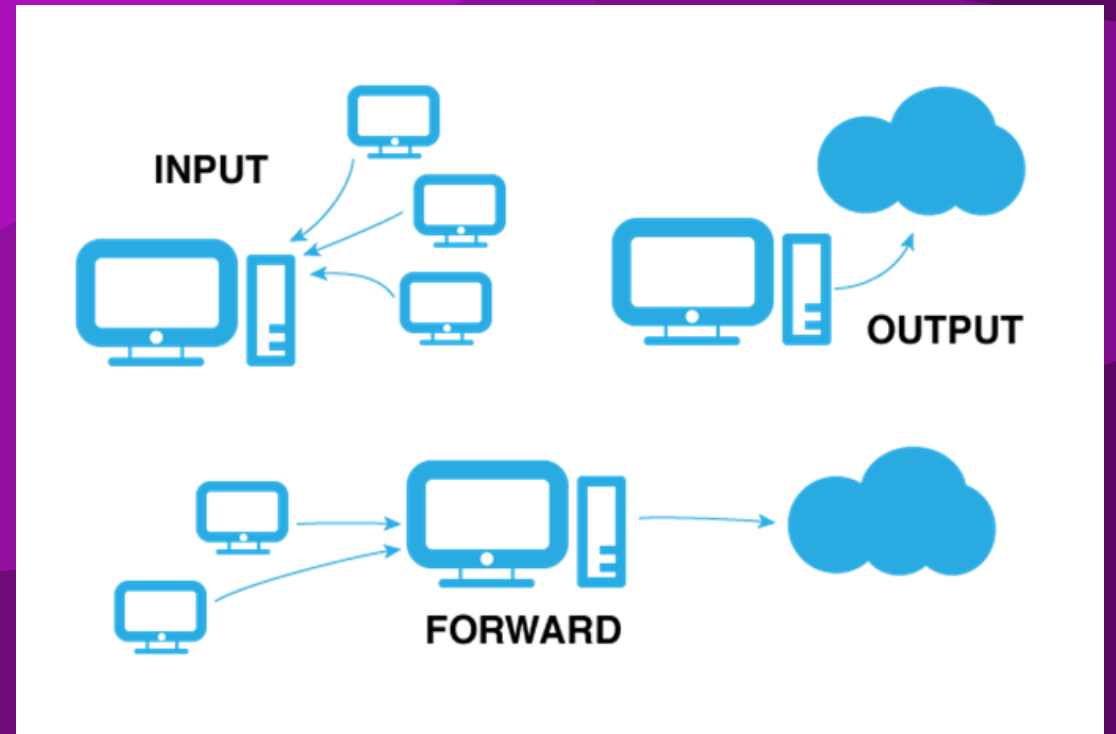
보안 및 방화벽 설정 - iptables

- 방화벽은 특정 IP 또는 특정 포트를 막거나 허용하는 역할을 한다.
- 사용하지 않는 포트는 방화벽에서 막아 두는 것이 좋다.
- 간혹 특정 포트에서 취약점이 발생하여 해킹 사고가 발생할 수도 있기 때문이다.
 - *2017년 랜섬웨어 사태는 445번 포트의 취약점을 이용한 해킹 공격이다.



보안 및 방화벽 설정 - iptables

- 방화벽은 iptables를 이용하여 설정한다.
 - Ubuntu 사용 시 기본적으로 설치되어 있다.
- PC 기준에서, 패킷의 흐름은 크게 3가지가 있다.
 - INPUT
 - 외부에서 서버로 들어올 때
 - OUTPUT
 - 서버에서 외부로 나갈 때
 - FORWARD
 - 외부에서 서버를 통과하여 나갈 때
- 일반적으로 INPUT 설정에 많은 비중을 둔다.



보안 및 방화벽 설정 - iptables

- iptables에서는 패킷의 3가지 흐름에 맞게 체인이 3가지 있다.
 - INPUT, FORWARD, OUTPUT
- 체인에 규칙(Rule)을 추가하면, 패킷은 체인의 규칙들을 체크하게 된다.
 - 위에서 아래로
- 예) INPUT 체인에 22/TCP 는 DROP 규칙을 추가하면?
 - 서버에 22/TCP로 들어오는 패킷은 모두 DROP된다.

```
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source               destination
 0      0 ACCEPT      all  --  lo     any     loopback/8          anywhere
 0      0 REJECT      all  --  !lo    any     anywhere             anywhere
 0      0 ACCEPT      icmp --  any    any     anywhere             anywhere    reject-wi
 0      0 ACCEPT      icmp --  any    any     anywhere             anywhere    icmp dest
 0      0 ACCEPT      icmp --  any    any     anywhere             anywhere    icmp echo
 0      0 ACCEPT      icmp --  any    any     anywhere             anywhere    icmp time
 0      0 ACCEPT      tcp  --  any    any     anywhere             anywhere    tcp dpt:s
 0      0 ACCEPT      tcp  --  any    any     anywhere             anywhere    tcp dpt:h
 0      0 ACCEPT      tcp  --  any    any     anywhere             anywhere    tcp dpt:h
 0      0 ACCEPT      all  --  any    any     anywhere             anywhere    state REL
 0      0 LOG         all  --  any    any     anywhere             anywhere    limit: av
 0      0 REJECT      all  --  any    any     anywhere             anywhere    reject-wi

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source               destination
 0      0 LOG         all  --  any    any     anywhere             anywhere    limit: av
 0      0 REJECT      all  --  any    any     anywhere             anywhere    reject-wi

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source               destination
```

보안 및 방화벽 설정 - iptables

- 체인에서 일치하는 규칙을 찾지 못하면 기본 정책을 적용하게 된다.
 - 예) INPUT체인은 기본적으로 DROP 이고, 80/TCP 만 ACCEPT한다면?
 - 서버의 24/TCP로 들어오는 모든 패킷은 DROP
 - 서버의 80/TCP로 들어오는 모든 패킷은 ACCEPT

```
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out    source            destination
0      0 ACCEPT      all  --  lo     any    anywhere          anywhere
0      0 REJECT      all  --  !lo    any    loopback/8        anywhere
0      0 ACCEPT      icmp --  any    any    anywhere          anywhere    reject-wi
0      0 ACCEPT      icmp --  any    any    anywhere          anywhere    icmp dest
0      0 ACCEPT      icmp --  any    any    anywhere          anywhere    icmp echo
0      0 ACCEPT      icmp --  any    any    anywhere          anywhere    icmp time
0      0 ACCEPT      tcp  --  any    any    anywhere          anywhere    tcp dpt:s
0      0 ACCEPT      tcp  --  any    any    anywhere          anywhere    tcp dpt:h
0      0 ACCEPT      tcp  --  any    any    anywhere          anywhere    tcp dpt:h
0      0 ACCEPT      all  --  any    any    anywhere          anywhere    state REL
0      0 LOG         all  --  any    any    anywhere          anywhere    limit: av
0      0 REJECT      all  --  any    any    anywhere          anywhere    reject-wi

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out    source            destination
0      0 LOG         all  --  any    any    anywhere          anywhere    limit: av
0      0 REJECT      all  --  any    any    anywhere          anywhere    reject-wi

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out    source            destination.
```

보안 및 방화벽 설정 - iptables

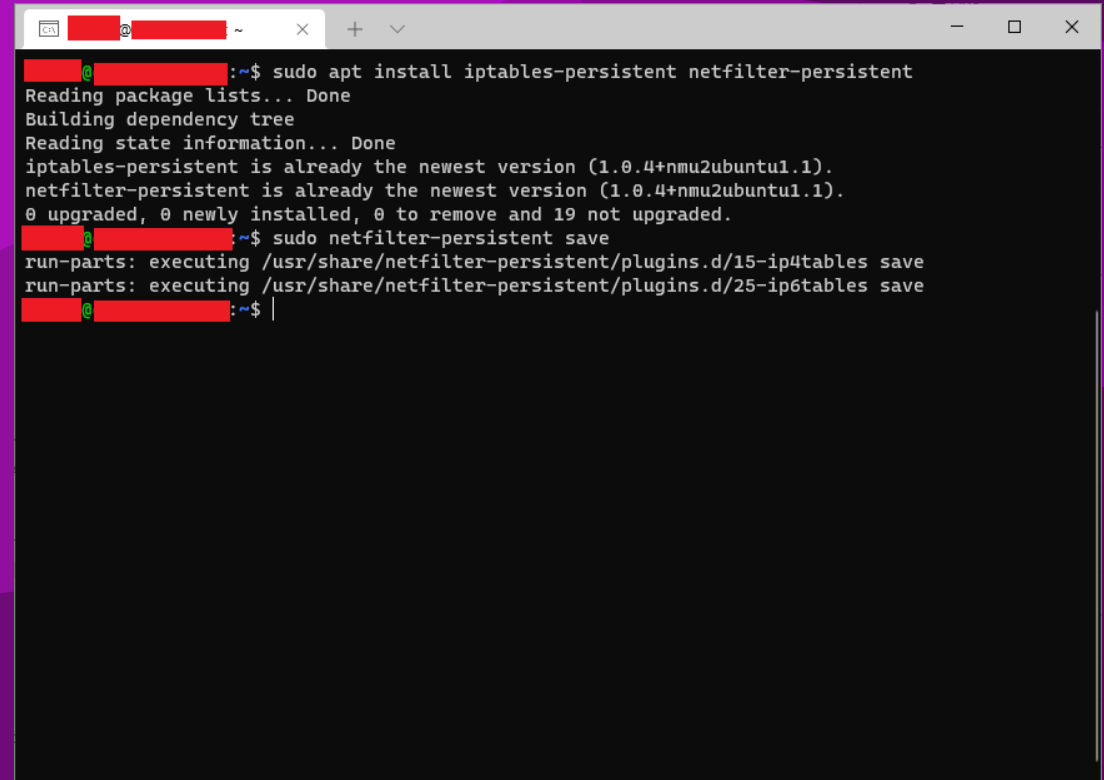
- iptables의 명령을 몇 가지 살펴보도록 하자.
- iptables -A INPUT -p tcp --dport 25565 -j ACCEPT
 - 서버의 25565/TCP로 들어오는 패킷은 허용
- iptables -A INPUT -p tcp --dport 22 -j ACCEPT
 - 서버의 22/TCP로 들어오는 패킷은 허용
- iptables -P INPUT DROP
 - 서버로 들어오는 패킷들은 기본적으로 DROP 정책 적용

```
Chain INPUT (policy DROP)
target    prot opt source                destination
ACCEPT    all  --  anywhere              anywhere
ACCEPT    all  --  anywhere              anywhere
ACCEPT    tcp  --  anywhere              anywhere    state RELATED,ESTABLISHED
ACCEPT    tcp  --  anywhere              anywhere    tcp dpt:smtp
ACCEPT    tcp  --  anywhere              anywhere    tcp dpt:http-alt
ACCEPT    tcp  --  anywhere              anywhere    tcp dpt:25565

Chain FORWARD (policy DROP)
target    prot opt source                destination
DOCKER-USER all -- anywhere            anywhere
DOCKER-ISOLATION-STAGE-1 all -- anywhere            anywhere
ACCEPT    all  --  anywhere              anywhere    ctstate RELATED,ESTABLISHED
DOCKER    all  --  anywhere              anywhere
ACCEPT    all  --  anywhere              anywhere
ACCEPT    all  --  anywhere              anywhere
ACCEPT    all  --  anywhere              anywhere    ctstate RELATED,ESTABLISHED
DOCKER    all  --  anywhere              anywhere
ACCEPT    all  --  anywhere              anywhere
ACCEPT    all  --  anywhere              anywhere    ctstate RELATED,ESTABLISHED
DOCKER    all  --  anywhere              anywhere
ACCEPT    all  --  anywhere              anywhere
ACCEPT    all  --  anywhere              anywhere    ctstate RELATED,ESTABLISHED
DOCKER    all  --  anywhere              anywhere
ACCEPT    all  --  anywhere              anywhere
ACCEPT    all  --  anywhere              anywhere    ctstate RELATED,ESTABLISHED
DOCKER    all  --  anywhere              anywhere
```

보안 및 방화벽 설정 - iptables

- iptables 규칙은 재부팅 시 설정이 초기화된다.
- 규칙을 영구적으로 저장하려면 추가적으로 패키지를 설치하여야 한다.
- `sudo apt install iptables-persistent netfilter-persistent`
 - iptables를 영구적으로 저장해주는 패키지이다.
- `sudo netfilter-persistent save`
 - iptables 규칙들을 저장하는 명령이다.



```
~$ sudo apt install iptables-persistent netfilter-persistent
Reading package lists... Done
Building dependency tree
Reading state information... Done
iptables-persistent is already the newest version (1.0.4+nmu2ubuntu1.1).
netfilter-persistent is already the newest version (1.0.4+nmu2ubuntu1.1).
0 upgraded, 0 newly installed, 0 to remove and 19 not upgraded.
~$ sudo netfilter-persistent save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/25-ip6tables save
~$
```

도메인? IP?

- 지금까지는 IP 주소로 모든 작업을 처리하였다.
 - SSH, SFTP 연결, 마인크래프트 서버 접속 등 ...
- 사용자들이 서비스를 이용할 때 IP주소를 외우기는 힘들다.
- 구글(www.google.com)이나 네이버(www.naver.com)처럼 IP주소가 아닌 도메인을 설정해두면 더 편리하게 접속할 수 있다.

23.78.142.90



myserver.com

도메인? IP?

- 마인크래프트 또는 웹 사이트를 접속할 때, 도메인 (domain)을 입력하면 컴퓨터가 알아서 IP 주소로 바꾼 후 접속한다.
- 도메인은 도메인 사이트에서 등록할 수 있다.

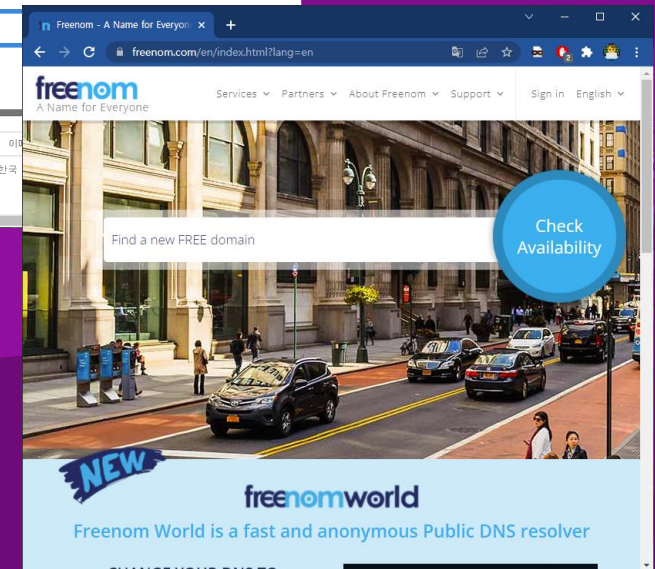
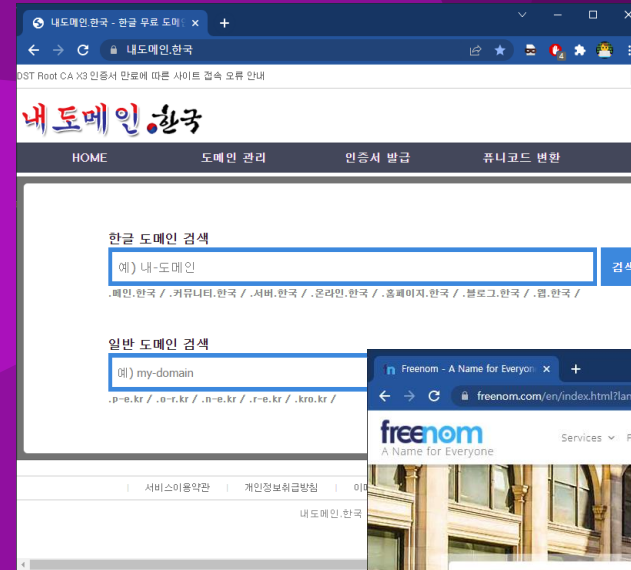
23.78.142.90



myserver.com

무료 도메인 사이트

- 대표적인 무료 도메인 사이트 2가지를 소개한다.
- 내도메인.한국
 - 한국에서 제공되는 서비스이다.
 - .kro.kr, .o-r.kr, .p-e.kr 등의 도메인을 제공한다.
- freenom
 - 외국에서 제공되는 서비스이다.
 - .tk, .cf, .ga, .gq, .ml 도메인을 제공한다.



[실습] 도메인 발급 및 사용

- 내도메인.한국 사이트에 가입하여 무료 도메인을 발급받아보도록 한다.
- 회원가입 절차는 간단하다.
- 필요한 정보를 모두 입력하고 보안 코드를 입력한다.

내도메인.한국 - 한글 무료 도메인

내도메인.한국/page/member_join_step1.php

나)아이디(ID): 회원의 식별과 서비스 이용을 위하여 회원이 설정하고 회사가 승인한 숫자와 문자의 조합을 말한다
다)비밀번호(PW): 회원의 개인정보의 보호를 위하여 회원이 설정하고 회사가 승인한 숫자와 문자의 조합을 말한다
라)광고주: 회사에 일정한 비용을 지불하고 회사의 웹사이트를 통하여 진행중인 광고의 변경 및 종료의 권한을 가진자를 말한다
마)무료도메인: 회사가 제공하는 간혹페이지 주소를 올려주는 도메인 포워딩서비스를 말한다

※ 개인정보의 보유 및 이용기간

원칙적으로, 개인정보 수집 및 이용목적이 달성된 후에는 해당 정보를 지체 없이 파기합니다.
단, 관계법령의 규정에 의하여 보존할 필요가 있는 경우 회사는 아래와 같이 관계법령에서 정한 일정한 기간 동안 회원정보를 보관합니다.
보존 항목 : 로그인ID, 결제기록
보존 근거 : 신용정보의 이용 및 보호에 관한 법률
보존 기간 : 1년
표시/광고에 관한 기록 : 6개월 (전자상거래에서의 소비자보호에 관한 법률)

☐ 동의합니다. ☒ 동의하지 않습니다.


아이디 * 영문, 숫자, _ 조합 4 ~ 12자

비밀번호 * 영문, 숫자, 특수 조합 4 ~ 20자

비밀번호 확인 *

이름 * 공백없이 한글만 가능

이메일 *

 보안코드 입력

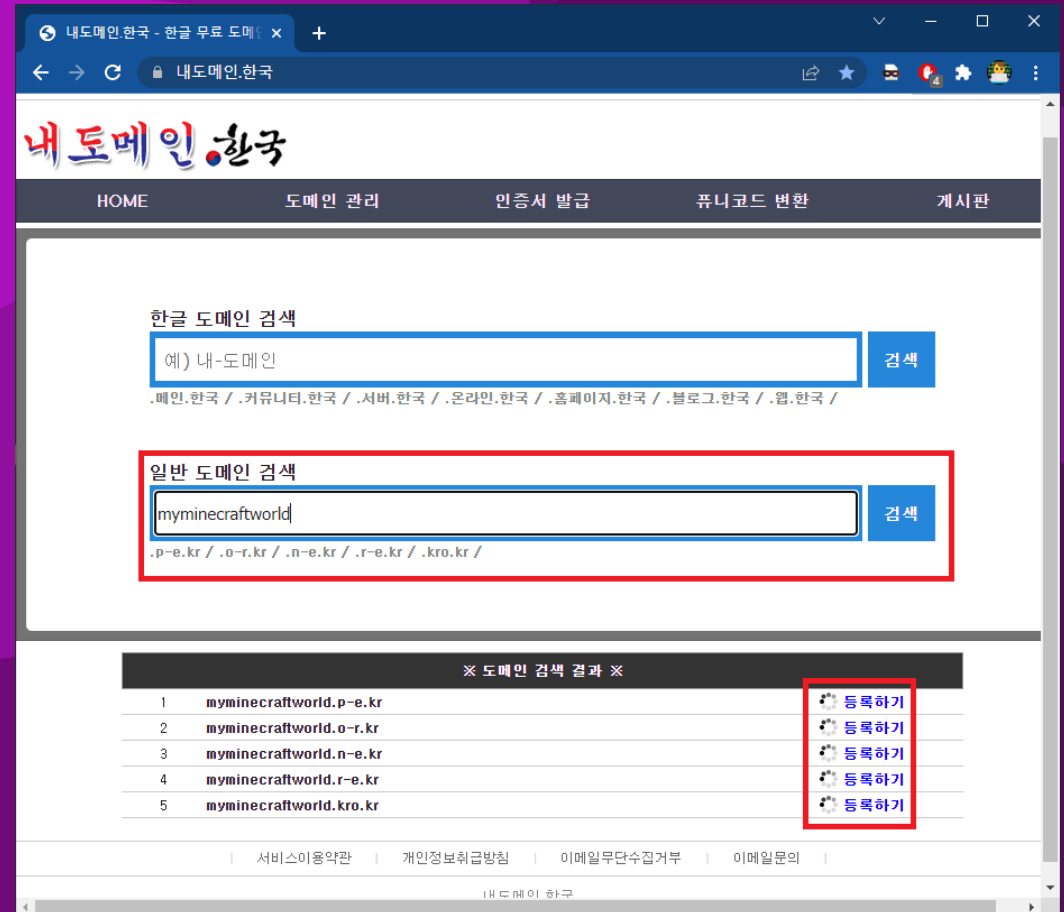
회원가입

서비스이용약관 | 개인정보취급방침 | 이메일무단수집거부 | 이메일문의

내도메인.한국

[실습] 도메인 발급 및 사용

- 회원가입을 완료하였으면, 원하는 도메인을 검색한다.
- 검색 결과에서 도메인을 등록할 수 있는지 여부가 나타난다.
- 등록하기 버튼을 클릭하면 도메인 등록을 진행할 수 있다.



[실습] 도메인 발급 및 사용

- 고급설정 (DNS) 에서 IP연결(A)를 체크하고,
- 서버의 IP 주소를 입력한다.
- 보안코드를 입력하고 수정하기 버튼을 클릭하면 도메인 등록이 완료된다.

내도메인.한국 - 한글 무료 도메인

내도메인.한국/page/domain_conf_view.php?id=1228314&order=&page=1

HOME 도메인 관리 인증서 발급 푸니코드 변환 게시판

수정하실 도메인의 정보를 자세히 입력해 주시기 바랍니다.

도메인 myminecraftworld.kro.kr

웹포워딩 (Redirect)

☐ 웹포워딩 .myminecraftworld.kro.kr http:// [+]

단일페이지 (HTML)

☐ 단일페이지 .myminecraftworld.kro.kr [+]

<html>
<head></head>
<body></body>
</html>

고급설정 (DNS)

<input checked="" type="checkbox"/> IP연결(A)	.myminecraftworld.kro.kr	53.98.104.27	[+]
<input type="checkbox"/> IP연결(AAAA)	.myminecraftworld.kro.kr	예) 2001:0db8:85a3:08d3:1319:8a2e:0370:7334	[+]
<input type="checkbox"/> 별칭(CNAME)	.myminecraftworld.kro.kr	예) www.domain.com	[+]
<input type="checkbox"/> 메일(MX)	.myminecraftworld.kro.kr	예) mx1.domain.com prio	[+]
<input type="checkbox"/> TXT(SPF)	.myminecraftworld.kro.kr	예) v=spf1 ip4:127.0.0.1 ~all	[+]

보안코드 입력

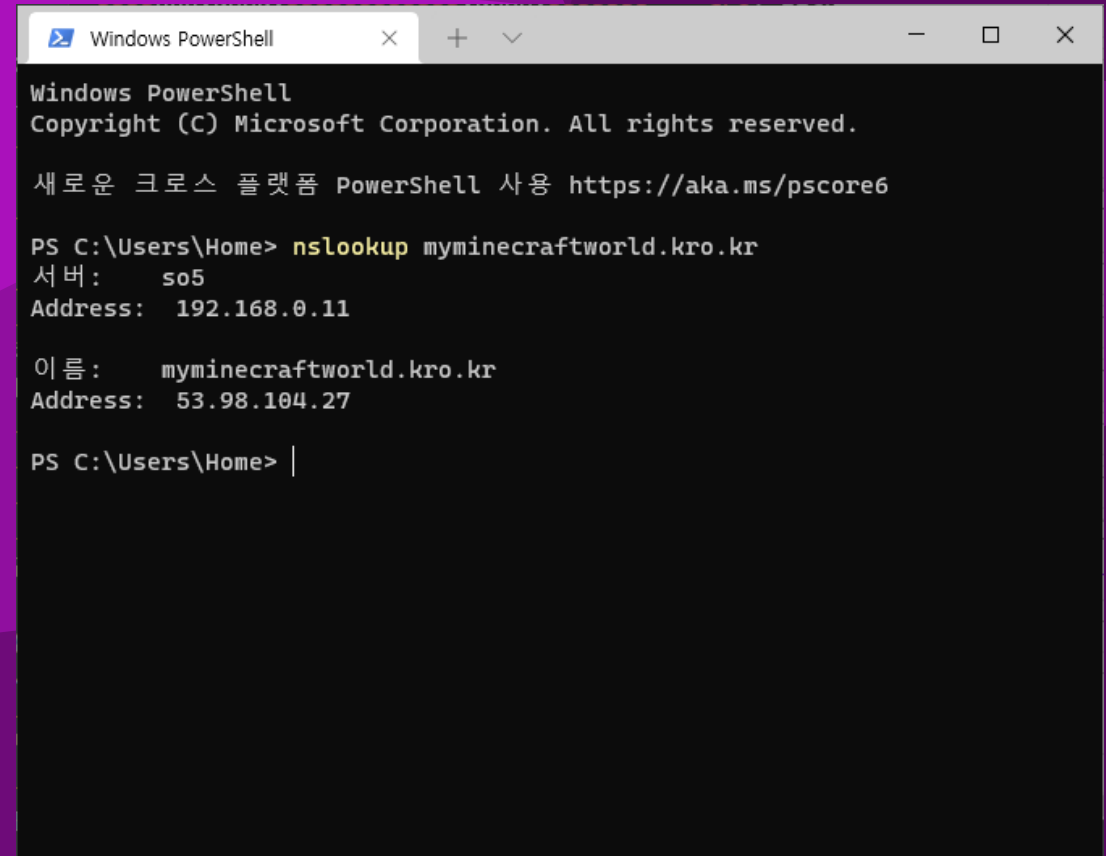
6827

수정하기 취소

서비스이용약관 개인정보취급방침 이메일무단수집거부 이메일문의

[실습] 도메인 발급 및 사용

- Windows Terminal 을 켜고 nslookup 명령을 사용하여 도메인의 IP 주소를 확인해보자.
- nslookup <도메인 주소>
 - nslookup은 도메인의 IP 주소를 알려주는 명령이다.
- 사이트에서 설정한 IP 주소가 뜬다면 성공적으로 설정된 것이다.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

새로운 크로스 플랫폼 PowerShell 사용 https://aka.ms/powershell

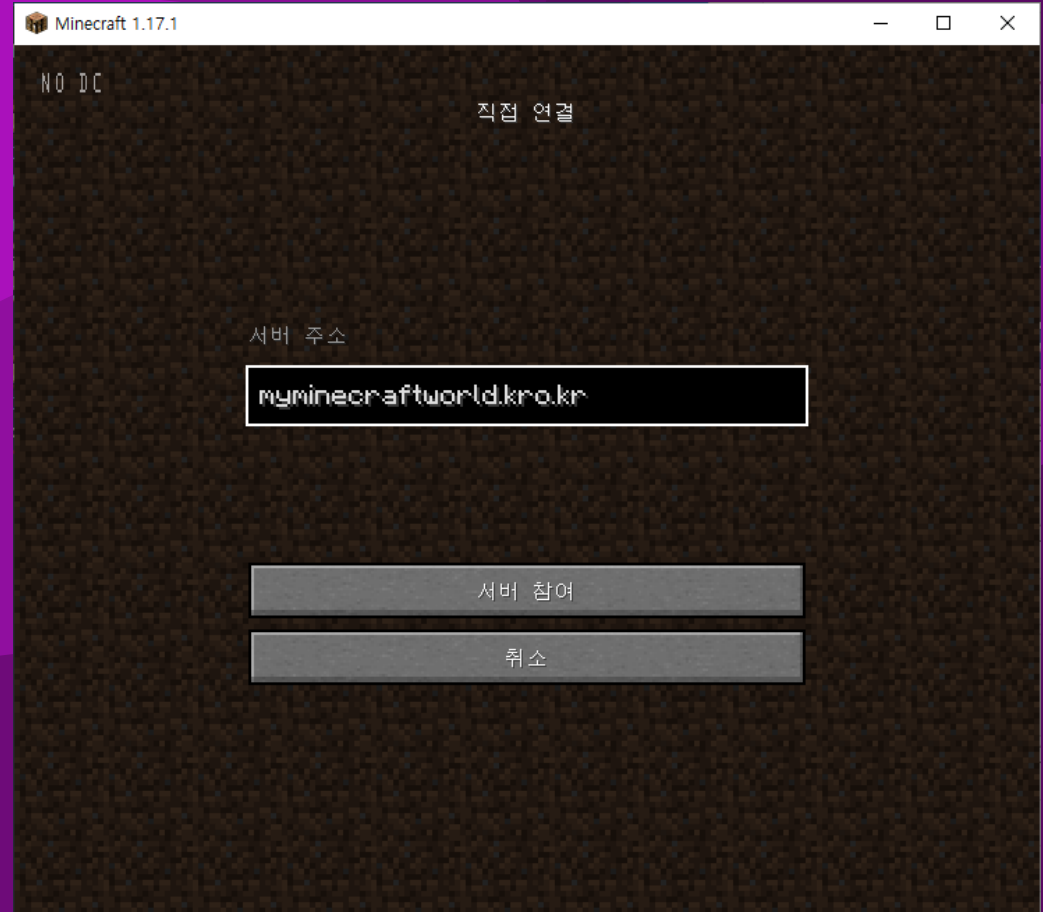
PS C:\Users\Home> nslookup myminecraftworld.kro.kr
서버:      so5
Address:  192.168.0.11

이름:      myminecraftworld.kro.kr
Address:  53.98.104.27

PS C:\Users\Home> |
```

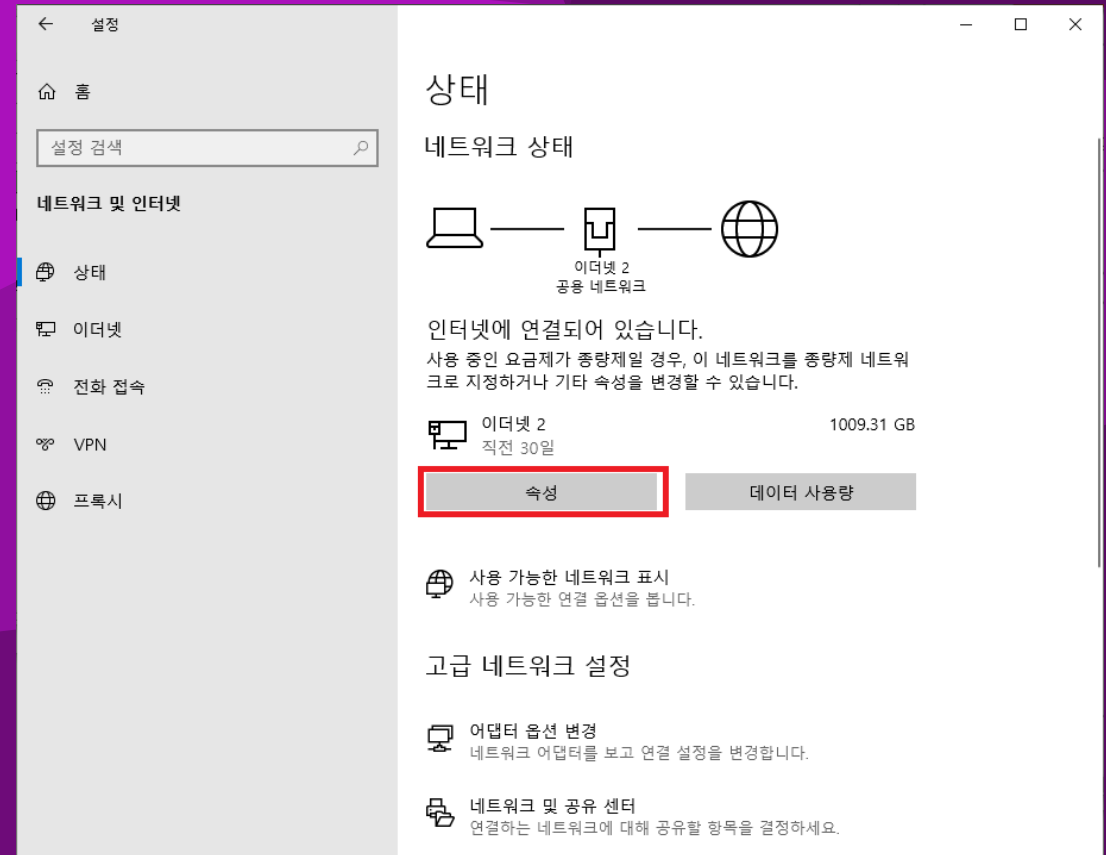
[실습] 도메인 발급 및 사용

- 이제 마인크래프트 서버를 켜고 발급받은 도메인으로 접속해보자.



[실습] 포트 포워딩이 작동하지 않을 때

- 공유기에서 포트 포워딩 설정을 해주었으나 외부에서 해당 포트로 접속이 안될 때, 윈도우 방화벽에서 차단되었을 가능성이 있다.
- Windows 키 + i 를 눌러 설정 창을 열고, 네트워크 및 인터넷 > 상태 > 속성 순서로 클릭한다.



[실습] 포트 포워딩이 작동하지 않을 때

- 개인으로 체크해준다.
- 카페, 도서관 등 공용 네트워크에서 진행하는 경우 실습을 마치고 반드시 공용으로 전환한다.

