

# 윈도우 리눅스 VPN

📅 날짜	@2024년 10월 11일
⚙️ 상태	진행 중

윈도우 WireGuard 설치 링크

<https://www.wireguard.com/install/>

이번엔 윈도우가 ServerPC이고 두 리눅스가 Client 역할을 하도록 ..



## 환경 구성

- 서버
  - Window
  - 192.168.0.207
  - VPN IP : 192.168.10.3으로 지정
- 클라이언트
  - Ubuntu
  - 10.10.10.13
  - VPN IP : 192.168.10.2로 지정

윈도우는 공개키/비밀키가 자동 생성

공개키 = dmBG/7/zbifCKYPsstduk81sf2Lwz4vc7oHiEjP/f1E=

비밀키 = 8N9/QdeqwBUubnxgK6ZAgCwaRJJpe9HYKd3Kk3LUglM=

[Interface]

PrivateKey = 8N9/QdeqwBUubnxgK6ZAgCwaRJJpe9HYKd3Kk3LUglM=

ListenPort = 51820

Address = 192.168.10.3/24

[Peer]

PublicKey = Klb8N1dqlxTZ0zJLBEyJp9xmdv9W7E6PooZkPMH+nUM=

AllowedIPs = 192.168.10.2/32

**[Interface]**  
PrivateKey = 8N9/QdeqwBUubnxgK6ZAgCwaRJJpe9HYKd3Kk3LUglM=  
ListenPort = 51820  
Address = 192.168.10.3/24

**[Peer]**  
PublicKey = Klb8N1dqlxTZ0zJLBEyJp9xmdv9W7E6PooZkPMH+nUM=  
AllowedIPs = 192.168.10.2/32

이더넷 어댑터 이더넷 :

```
연결별 DNS 접미사 . . . . . :  
링크-로컬 IPv6 주소 . . . . . : fe80::a71f:8094:1d53:e4d2%7  
IPv4 주소 . . . . . : 192.168.0.207  
서브넷 마스크 . . . . . : 255.255.255.0  
기본 게이트웨이 . . . . . : 192.168.0.1
```

window 서버의 ip주소는 192.168.0.207

[Interface]

Address = 192.168.10.2/24

# 클라이언트의 VPN

PrivateKey = GITuyew7XWuDkpJ3ZjRHow1RiLxqbgm1GDb0MCMtpno=

[Peer]

PublicKey = dmBG/7/zbifCKYPsstduk81sf2Lwz4vc7oHiEjP/f1E=

Endpoint = 192.168.0.207:51820 # 서버의 IP 주소 및 포트 번호

AllowedIPs = 0.0.0.0/0, ::/0 # 전체 트래픽을 VPN을 통

PersistentKeepalive = 25 # 연결이 유지되도록 keep

```
root@vegemil-vm: /etc/wireguard
[Interface]
Address = 192.168.10.2/24 # 클라이언트의 VPN IP 주소
PrivateKey = GITuyew7XWuDkpJ3ZjRHoW1RiLxqbgm1GDb0MCMtpno= # 클라이언트의 >
비밀키 (wg genkey로 생성)

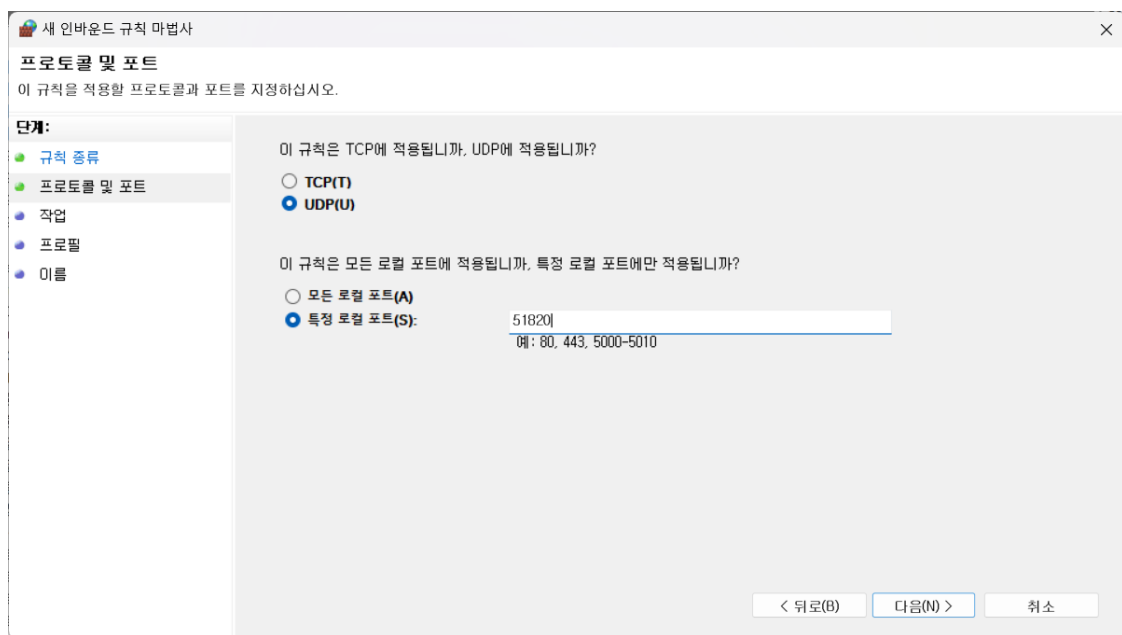
[Peer]
PublicKey = dmBG/7/zbifCKYPsstduk81sf2Lwz4vc7oHiEjP/f1E= # 서버의 공
개 키
Endpoint = 192.168.0.207:51820 # 서버의 IP 주소 및 포트 번호
AllowedIPs = 0.0.0.0/0, ::/0 # 전체 트래픽을 VPN을 통해 전송 (라우팅
설정)
PersistentKeepalive = 25 # 연결이 유지되도록 keepalive 설정 (NAT
환경에서 유용)
```

## 클라이언트 설정

```
root@vegemil-vm:/etc/wireguard# wg-quick up wg0
[#] ip link add wg0 type wireguard
[#] wg setconf wg0 /dev/fd/63
[#] ip -4 address add 192.168.10.2/24 dev wg0
[#] ip link set mtu 1420 up dev wg0
[#] wg set wg0 fwmark 51820
[#] ip -6 route add ::/0 dev wg0 table 51820
[#] ip -6 rule add not fwmark 51820 table 51820
[#] ip -6 rule add table main suppress_prefixlength 0
[#] nft -f /dev/fd/63
[#] ip -4 route add 0.0.0.0/0 dev wg0 table 51820
[#] ip -4 rule add not fwmark 51820 table 51820
[#] ip -4 rule add table main suppress_prefixlength 0
[#] sysctl -q net.ipv4.conf.all.src_valid_mark=1
[#] nft -f /dev/fd/63
root@vegemil-vm:/etc/wireguard# wg
interface: wg0
  public key: KLb8N1dqlxTZ0zJLBEyJp9xmdv9W7E6PooZkPMH+nUM=
  private key: (hidden)
  listening port: 45781
  fwmark: 0xca6c

peer: dmBG/7/zbifCKYPsstduk81sf2Lwz4vc7oHiEjP/f1E=
  endpoint: 192.168.0.207:51820
  allowed ips: 0.0.0.0/0, ::/0
  latest handshake: 1 second ago
  transfer: 92 B received, 180 B sent
  persistent keepalive: every 25 seconds
```

Windows Defender Firewall → 고급 설정 → 인바운드 규칙 → 51820 규칙 생성



인바운드 규칙										
이름	그룹	프로필	사용	작업	다시 정의	프로그램	로컬 주소	원격 주소	프로토콜	로컬 포트
Wireguard VPN		모두	예	허용	아니요	모두	모두	모두	UDP	51820

## ping test

```
root@vegemil-vm:/etc/wireguard# ping 192.168.10.3
PING 192.168.10.3 (192.168.10.3) 56(84) bytes of data.
64 bytes from 192.168.10.3: icmp_seq=1 ttl=128 time=1.94 ms
64 bytes from 192.168.10.3: icmp_seq=2 ttl=128 time=1.45 ms
64 bytes from 192.168.10.3: icmp_seq=3 ttl=128 time=3.12 ms
64 bytes from 192.168.10.3: icmp_seq=4 ttl=128 time=2.60 ms
64 bytes from 192.168.10.3: icmp_seq=5 ttl=128 time=2.78 ms
^C
--- 192.168.10.3 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 1.451/2.376/3.116/0.601 ms
root@vegemil-vm:/etc/wireguard#
```

```
C:\Users\USER>ping 192.168.10.2

Ping 192.168.10.2 32바이트 데이터 사용 :
192.168.10.2의 응답 : 바이트=32 시간=1ms TTL=64
192.168.10.2의 응답 : 바이트=32 시간=3ms TTL=64
192.168.10.2의 응답 : 바이트=32 시간=3ms TTL=64
192.168.10.2의 응답 : 바이트=32 시간=3ms TTL=64

192.168.10.2에 대한 Ping 통계 :
패킷 : 보냄 = 4, 받음 = 4, 손실 = 0 (0% 손실),
왕복 시간(밀리초):
최소 = 1ms, 최대 = 3ms, 평균 = 2ms
```

## 양방향 핑 성공