

# VPN 실습

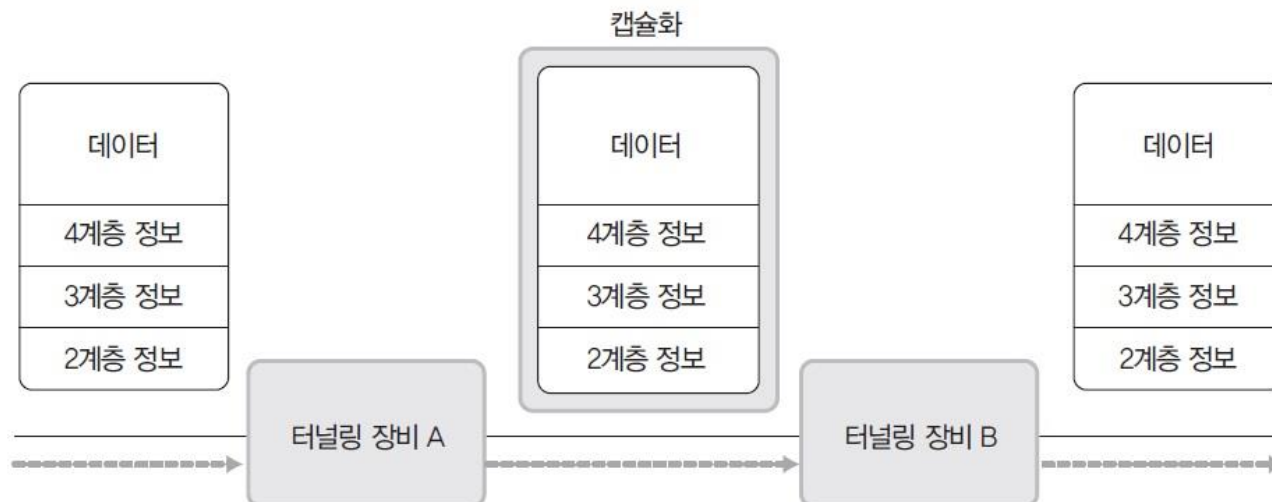
# 터널링

## ▶ 인터넷의 일정 구간에 별도의 채널을 형성하여 사용하는 기법

- 주로 암호화 채널을 통해 보안성을 높이기 위해

## ▶ 캡슐화

- 원래 패킷을 캡슐에 넣어 변경하지 않고 보안성 제고



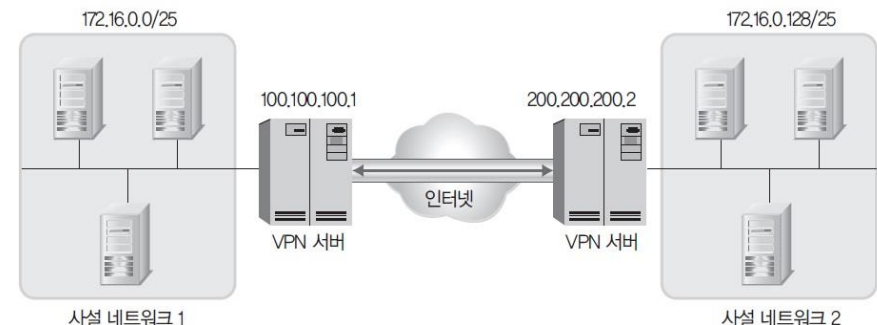
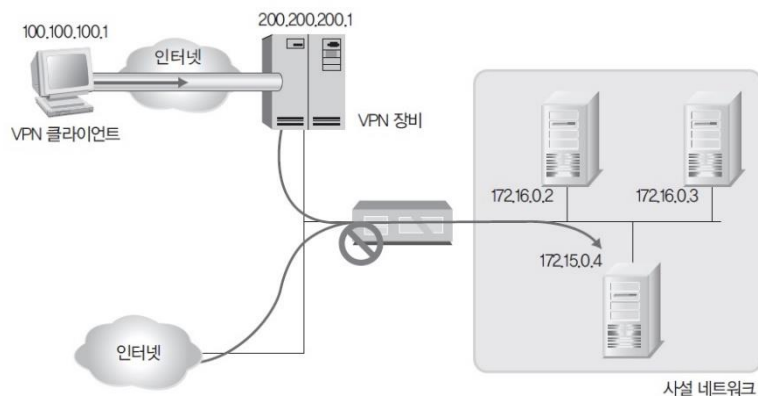
# VPN

## ▶ Virtual Private Network

- 터널링을 통해 전용회선을 가진 것처럼 동작
- SSL, IPSec, PPTP 등을 이용

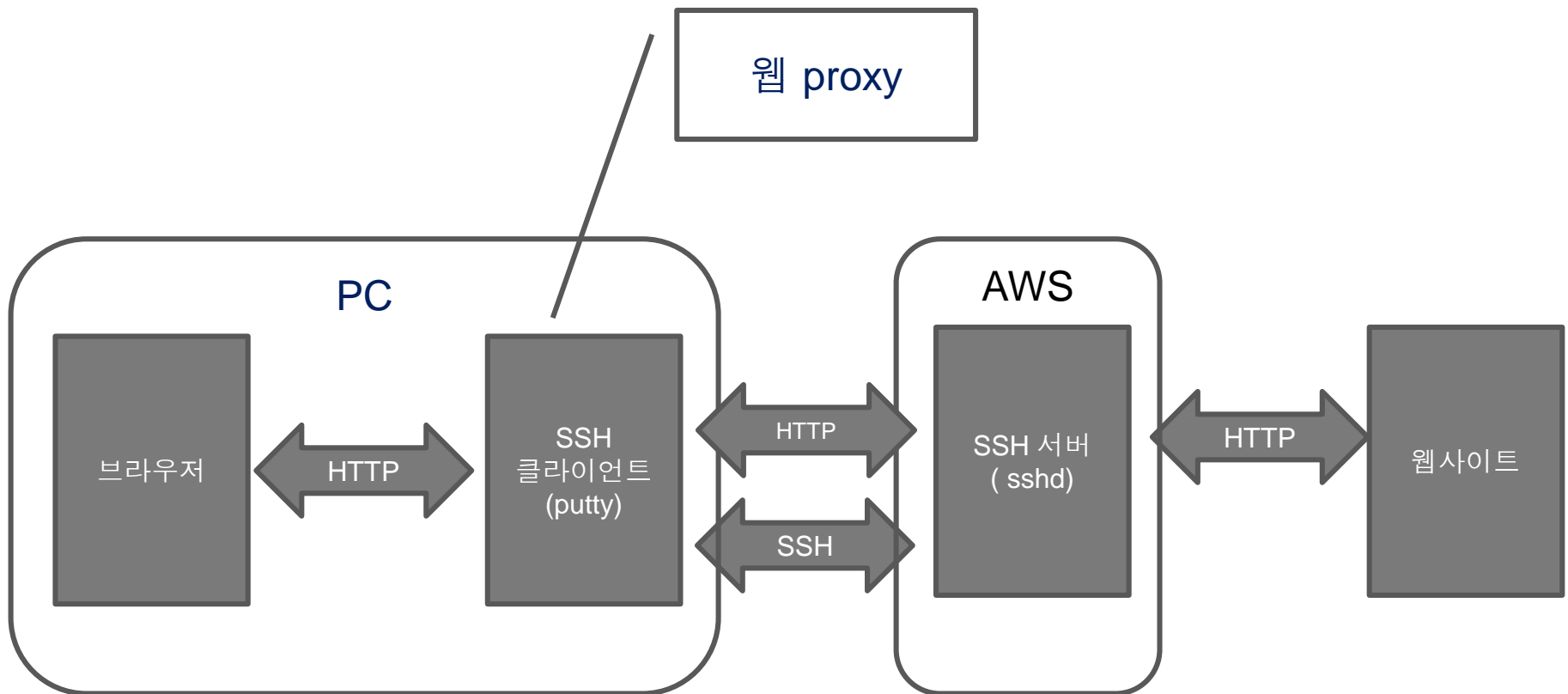
## ▶ 응용

- 외부에서 회사 등에 안전한 접속 또는 회사 지점 간 안전한 통신
- 해외 VPN 서버를 통해 차단된 사이트에 접속
  - 접속 사이트 변경 및 통신 내용 보안



# VPN 실습1

## ▶ SSH tunneling 을 이용 web proxy를 구축




# 순서

- ▶ AWS 인스턴스 생성
- ▶ Putty SSH tunnel 설정
- ▶ SSH 재접속
- ▶ 브라우저 proxy 설정
- ▶ 브라우저로 웹사이트 접속

# AWS 인스턴스 생성


## - 루트사용자로 로그인 후


 Services


Search for services, features, blogs, docs, and more [Alt+S]


Build a solution Info


Start building with simple wizards and automated workflows.


 Launch a virtual machine  
With EC2 (2 mins)


 Start a development project  
With CodeStar (5 mins)


 Connect an IoT device  
With AWS IoT (5 mins)


 Build using virtual servers  
With Lightsail (2 mins)

 Host a static web app  
With AWS Amplify Console (2 mins)

 Register a domain  
With Route 53 (3 mins)

 Build a web app  
With AWS App Runner (5 mins)

 Deploy a serverless microservice  
With API Gateway (2 mins)

 Start migrating to AWS  
With AWS MGN (2 mins)

# AWS 인스턴스 생성

## - 프리 티어 선택

### Name and tags [Info](#)

Name

sunchoi1

[Add additional tags](#)

### ▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

 Search our full catalog including 1000s of application and OS images

#### Quick Start

Amazon  
Linux



macOS



Ubuntu



Windows



Red Hat



[Browse more AMIs](#)

Including AMIs from  
AWS, Marketplace and  
the Community

Amazon Machine Image (AMI)

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type  
ami-0e9bfdb247cc8de84 (64-bit (x86)) / ami-02a8e74d508493718 (64-bit (Arm))  
Virtualization: hvm    ENA enabled: true    Root device type: ebs

Free tier eligible ▼

# AWS 인스턴스 생성

## - 키 쌍 생성

### ▶ SSH 클라이언트 인증용 키 쌍

▼ Instance type [Info](#)

Instance type

t2.micro  
Family: t2 1 vCPU 1 GiB Memory  
On-Demand Linux pricing: 0.0144 USD per Hour  
On-Demand Windows pricing: 0.019 USD per Hour

Free tier eligible ▼

[Compare instance types](#)

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

Select ▼

[Create new key pair](#)



# AWS 인스턴스 생성

## - 키 쌍 생성

### ▶ SSH 클라이언트 인증용 키 쌍

- 잘 보관해야 => test.ppk

Create key pair

×

Key pairs allow you to connect to your instance securely.

Enter the name of the key pair below. When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** [Learn more](#)

Key pair name

test2

The name can include upto 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

☒ RSA  
RSA encrypted private and public key pair

☐ ED25519  
ED25519 encrypted private and public key pair (Not supported for Windows instances)

Private key file format

☐ .pem  
For use with OpenSSH

☒ .ppk  
For use with PuTTY


Cancel

Create key pair

# AWS 인스턴스 생성 -콘솔 보기

## ▶ 서버 IP 주소 획득

EC2 > Instances > Launch an instance

 **Success**  
Successfully initiated launch of instance (i-0c05d1f7bd25260f6)  
[▶ Launch log](#)



**Next Steps**

**Create billing and free tier usage alerts**  
To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.  
[Create billing alerts](#)

**Connect to your instance**  
Once your instance is running, log into it from your local computer.  
[Connect to instance](#)  
[Learn more](#)

**Connect an RDS database**  
Configure the connection between an EC2 instance and a database to allow traffic flow between them.  
[Connect an RDS database](#)  
[Create a new RDS database](#) [Learn more](#)

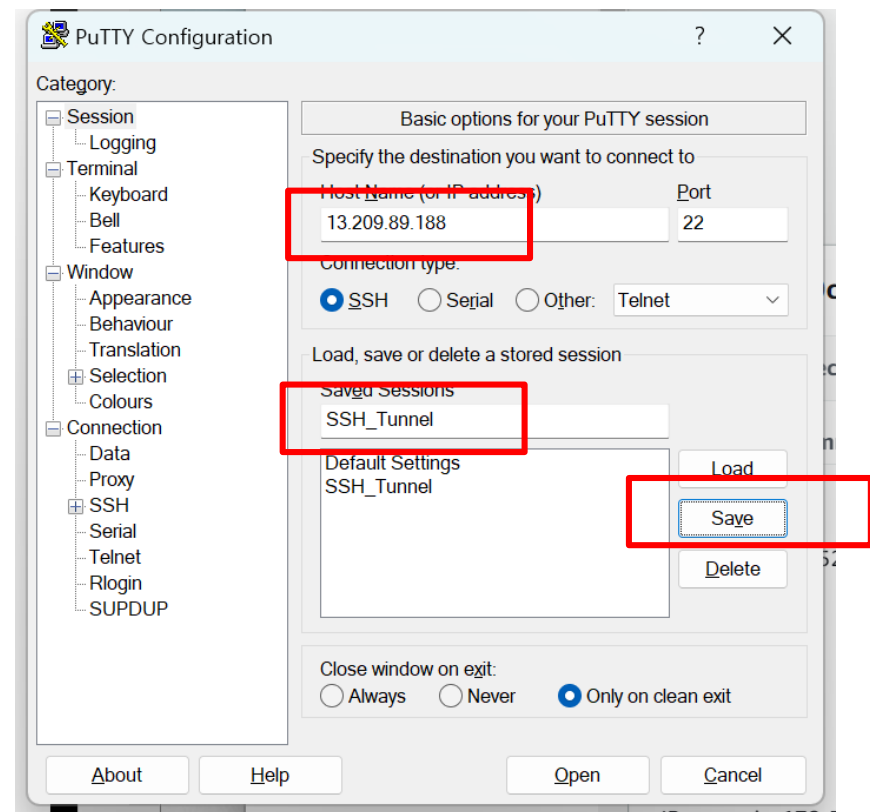
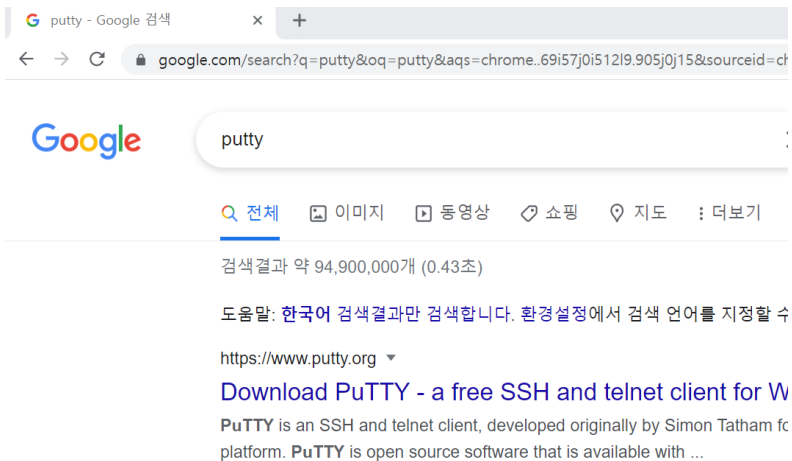
[View all instances](#)

Instances (1) <a href="#">Info</a>									
<input type="text" value="Find instance by attribute or tag (case-sensitive)"/>									
Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IP	
 Running	t2.micro	 Initializing	No alarms +	ap-northeast-2c	ec2-13-209-89-188.ap-...	13.209.89.188	-	-	

# AWS 인스턴스 생성 - 터미널 실행

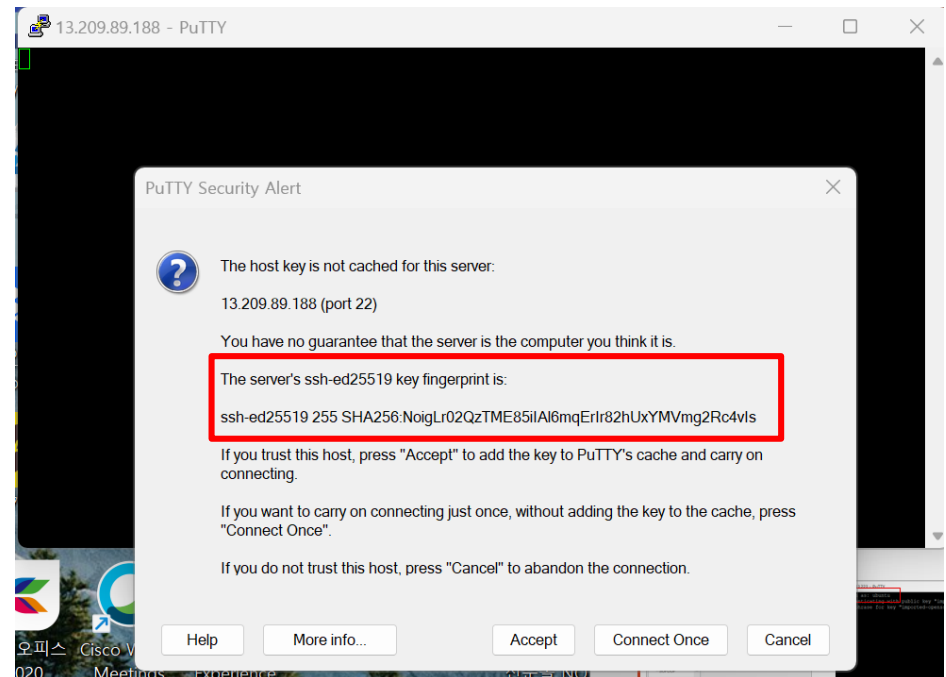
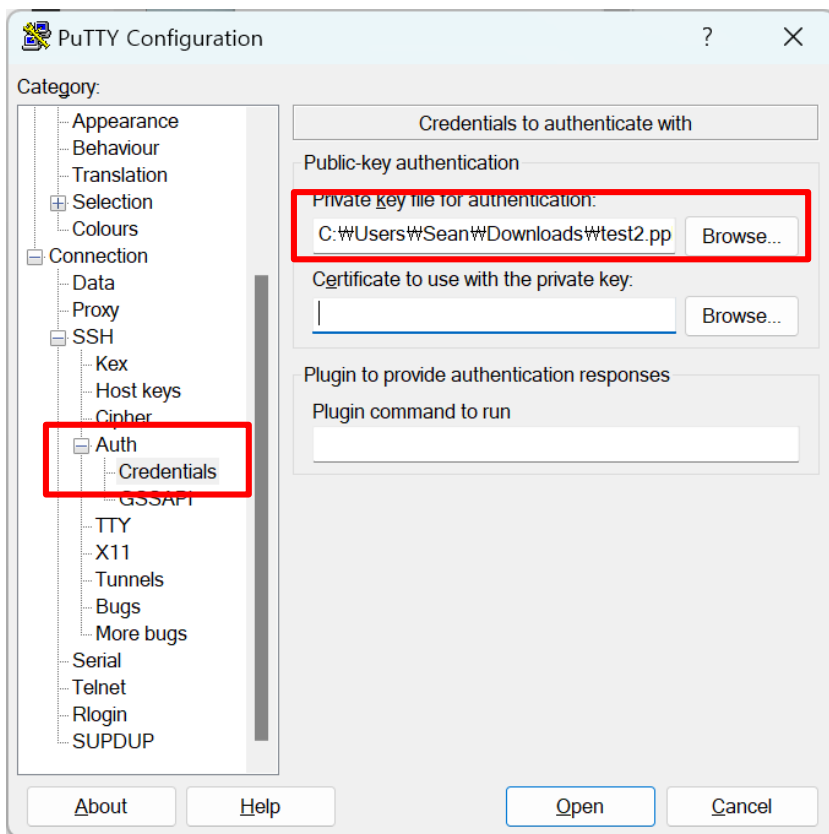
## ▶ Putty 를 다운로드하여 설치 및 실행

- 서버 주소 저장



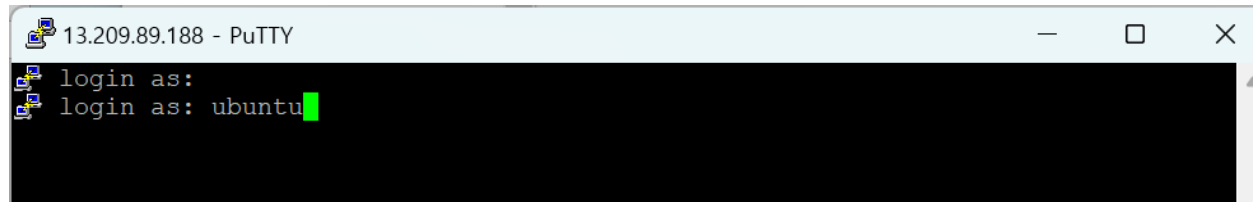
# AWS 인스턴스 생성 -터미널 실행

- ▶ 클라이언트 개인키 지정
- ▶ 서버 공개키 fingerprint 확인



# AWS 인스턴스 생성 -로그인

- ▶ uid : ubuntu 로, 인증은 ppk 키쌍으로 이뤄짐



```
13.209.89.188 - PuTTY
login as:
login as: ubuntu
```

- ▶ 여기까지는 일반적인 ec2 설정임

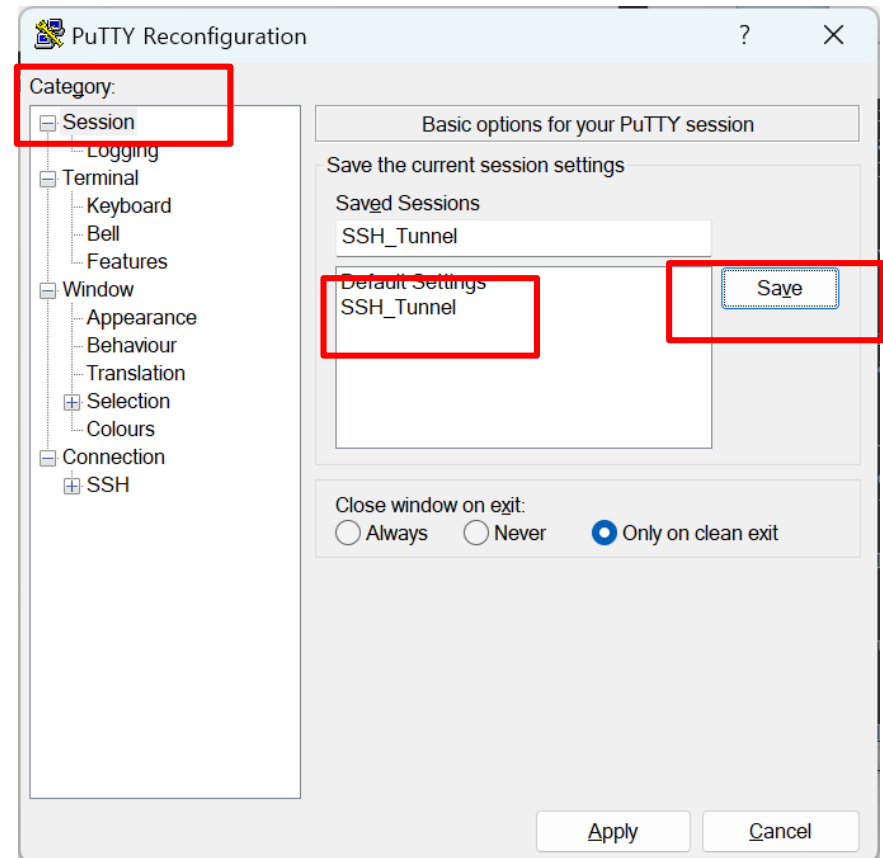
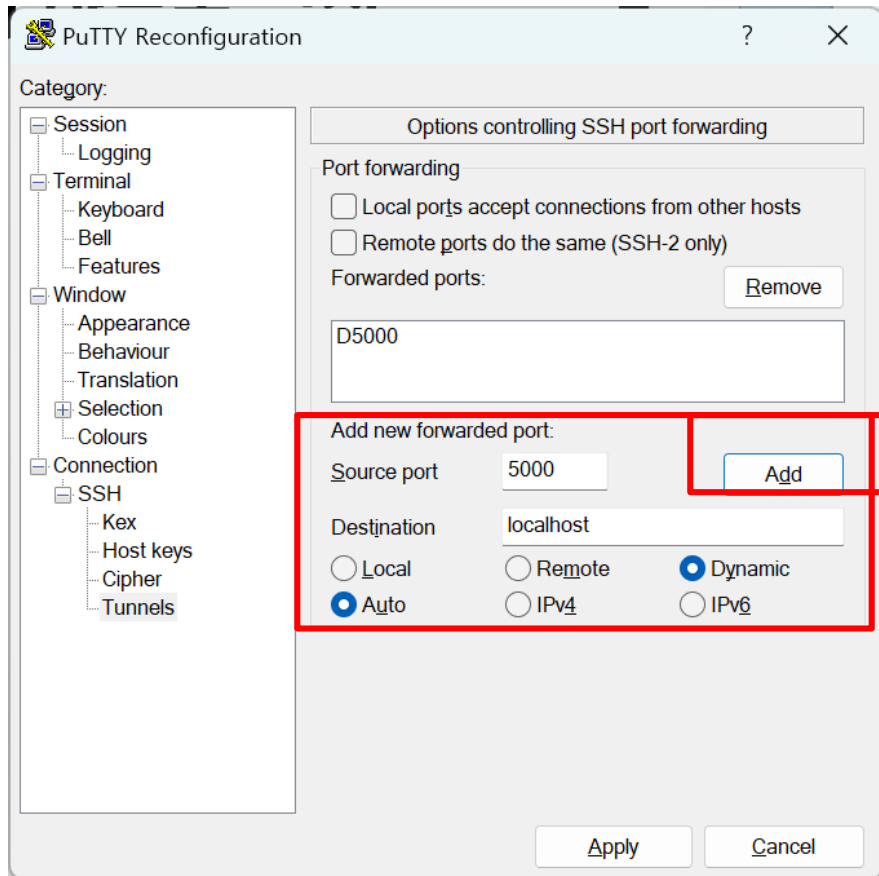
- ▶ SSH 터널을 위한 필요 프로그램 설치

```
ubuntu@ip-172-31-42-122:~$ sudo snap install root-framework
```

# PUTTY SSH 터널설정

▶ window header에 오른쪽 마우스 클릭

- 5000번 포트를 SSH서버로 forwarding 하도록 설정



▶ 세션 저장

# SSH재접속

▶ window console 에서 터널링 확인

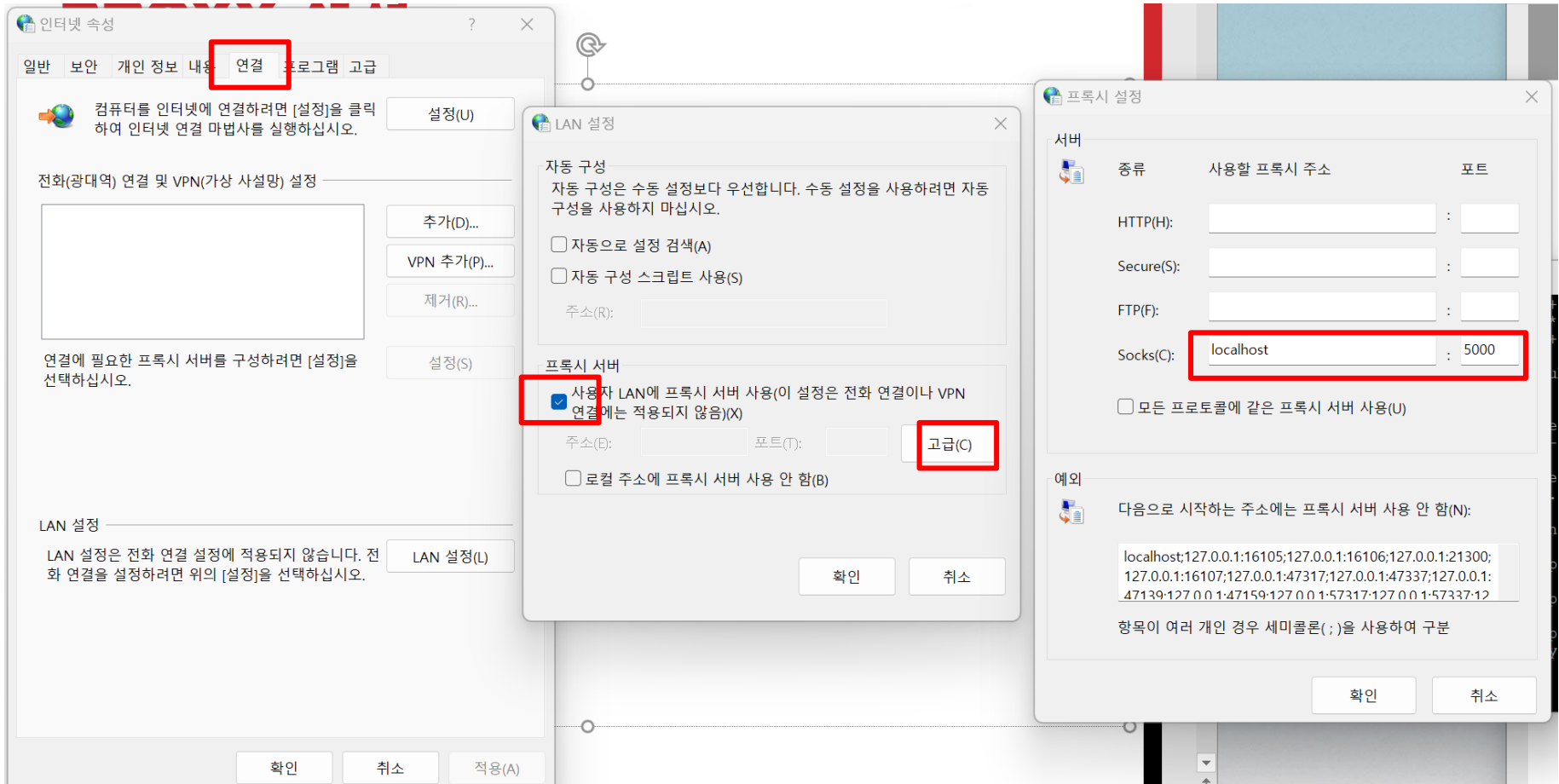
> netstat -an

```

명령 프롬프트
TCP    10.21.1.26:58097      142.250.196.100:443  TIME_WAIT
TCP    10.21.1.26:58098      15.197.193.217:443   TIME_WAIT
TCP    10.21.1.26:58099      15.197.193.217:443   TIME_WAIT
TCP    10.21.1.26:58104      23.53.32.51:80       ESTABLISHED
TCP    10.21.1.26:58107      211.115.106.74:80    CLOSE_WAIT
TCP    10.21.1.26:58108      211.115.106.74:80    CLOSE_WAIT
TCP    10.21.1.26:58156      172.217.174.99:443   TIME_WAIT
TCP    10.21.1.26:58157      211.115.106.80:80    CLOSE_WAIT
TCP    10.21.1.26:58158      211.115.106.80:80    CLOSE_WAIT
TCP    10.21.1.26:58178      20.189.173.2:443     TIME_WAIT
TCP    10.21.1.26:58183      203.253.28.199:1688  ESTABLISHED
TCP    127.0.0.1:4441        0.0.0.0:0            LISTENING
TCP    127.0.0.1:5000        0.0.0.0:0            LISTENING
TCP    127.0.0.1:8380        0.0.0.0:0            LISTENING
TCP    127.0.0.1:8884        0.0.0.0:0            LISTENING
TCP    127.0.0.1:9012        0.0.0.0:0            LISTENING
TCP    127.0.0.1:14098       0.0.0.0:0            LISTENING
TCP    127.0.0.1:14315       0.0.0.0:0            LISTENING
TCP    127.0.0.1:14319       0.0.0.0:0            LISTENING
TCP    127.0.0.1:14461       0.0.0.0:0            LISTENING
TCP    127.0.0.1:16106       0.0.0.0:0            LISTENING
TCP    127.0.0.1:16107       0.0.0.0:0            LISTENING
TCP    127.0.0.1:19812       0.0.0.0:0            LISTENING
TCP    127.0.0.1:31026       0.0.0.0:0            LISTENING
TCP    127.0.0.1:31027       0.0.0.0:0            LISTENING
TCP    127.0.0.1:34581       0.0.0.0:0            LISTENING
TCP    127.0.0.1:41028       0.0.0.0:0            LISTENING
TCP    127.0.0.1:41029       0.0.0.0:0            LISTENING
TCP    127.0.0.1:47317       0.0.0.0:0            LISTENING
TCP    127.0.0.1:47317       127.0.0.1:58102      TIME_WAIT
  
```

# PROXY 설정

## ▶ 윈도우즈 인터넷 옵션



The image shows three overlapping Windows dialog boxes related to network settings, with red boxes highlighting specific areas:

- 인터넷 속성 (Internet Options):** The '연결' (Connections) tab is selected. The '설정(U)' (Settings) button is highlighted.
- LAN 설정 (LAN Settings):** The '프록시 서버' (Proxy server) section is expanded. The checkbox '사용자 LAN에 프록시 서버 사용(이 설정은 전화 연결이나 VPN 연결에는 적용되지 않음)(X)' (Use proxy server for user's LAN (this setting does not apply to dial-up or VPN connections)) is checked and highlighted. The '고급(C)' (Advanced) button is also highlighted.
- 프록시 설정 (Proxy Settings):** The 'Socks(C):' field is set to 'localhost' and the port is '5000', both highlighted with a red box. The '예외' (Exceptions) section shows a list of addresses that do not use the proxy server.

**예외 (Exceptions):**

다음으로 시작하는 주소에는 프록시 서버 사용 안 함(N):

```
localhost;127.0.0.1:16105;127.0.0.1:16106;127.0.0.1:21300;
127.0.0.1:16107;127.0.0.1:47317;127.0.0.1:47337;127.0.0.1:
47139-127.0.0.1-47159;127.0.0.1-57317-127.0.0.1-57337-12
```

항목이 여러 개인 경우 세미콜론(;)을 사용하여 구분



# 브라우저로 웹사이트 접속

▶ putty를 끄면 웹접속이 되지 않음

**N** | ip 주소 확인



**통합** VIEW 이미지 지식iN 인플루언서<sup>N</sup> 동영상 쇼핑 뉴스 어학사전 지도 ...

IP주소 조회

18.188.73.244

관련정보 [IP주소란?](#)

# 과제1

▶ aws 콘솔 주소와 네이버 ip 주소 확인 화면 캡처

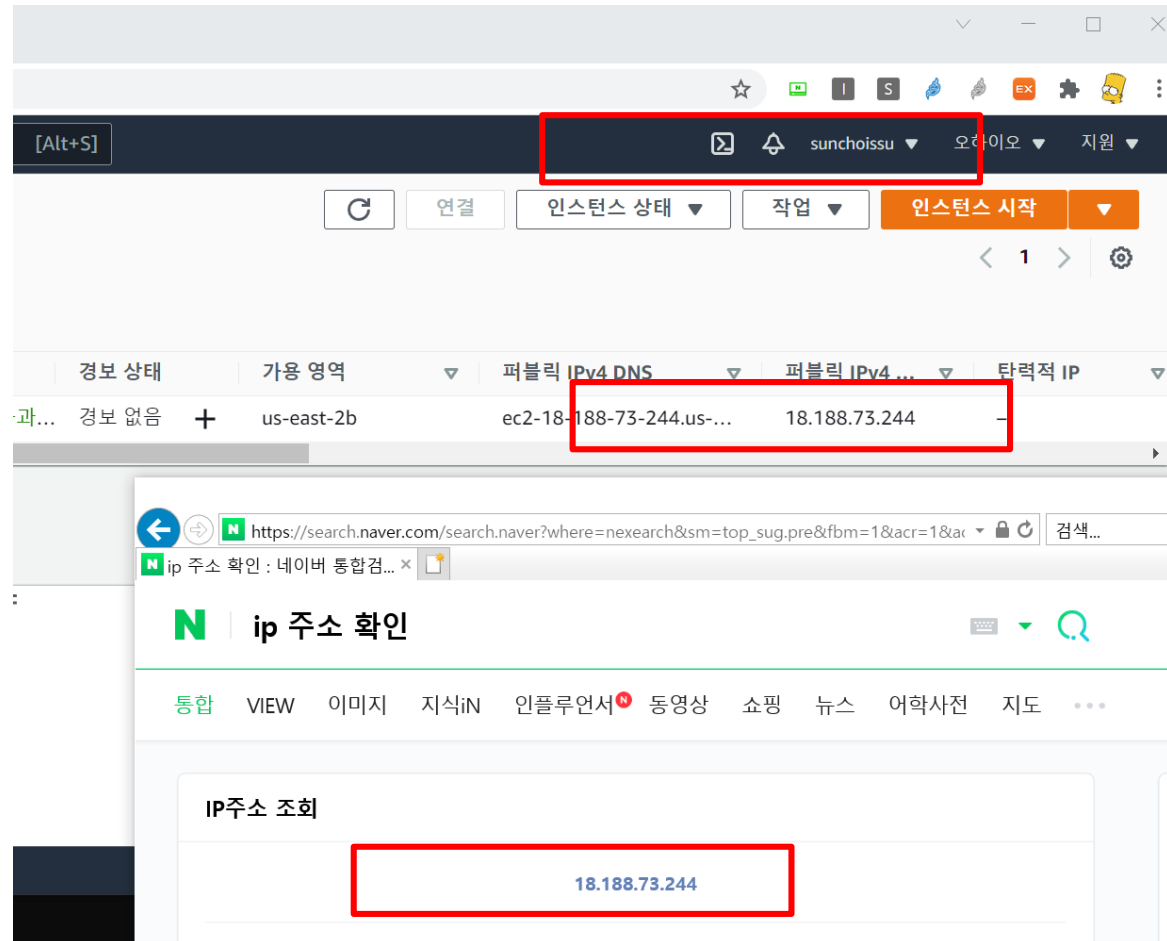
▶ 1.jpg

▶ 종료 후

proxy

설정

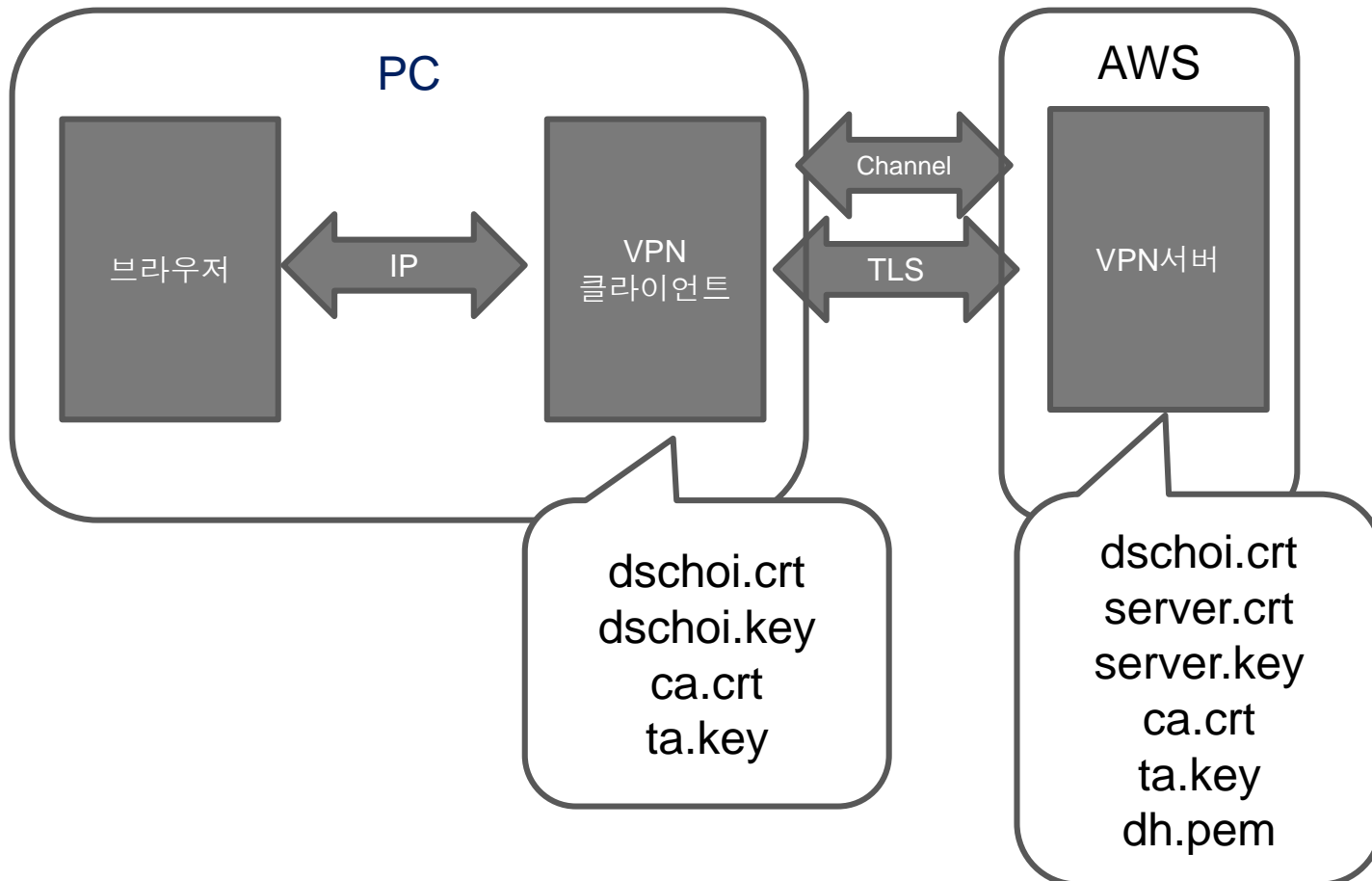
풀기!!



# VPN 실습 2

## ▶ VPN SW를 이용하여 VPN 구축

- 새로운 가상 IP 획득



# 순서

## ▶ 서버

- openvpn 설치
- CA키쌍 생성, 인증서 self sign
- 서버 키 쌍 생성, 인증서 발행, dh 파라미터 & ta.key 생성 및 이동
- 서버 설정
- 방화벽 열기
- 클라이언트 키 쌍 생성, 인증서 발행

## ▶ 클라이언트

- openvpn 설치
- 클라이언트 인증서, 비밀키, ta.key, ca 인증서 다운 받기
- 클라이언트 설정
- 접속

# 서버 - OPENVPN설치

▶ aws 터미널에서

```
$ sudo apt install openvpn
```

# CA 키쌍 생성, 인증서 SS

## ▶ openssl 간략화 도구 설치

```
$ sudo apt-get update
```

```
$ sudo apt install easy-rsa
```

## ▶ 폴더 및 script 설치

```
$ make-cadir ca
```

## ▶ pki 폴더 설치

```
$ cd ca
```

```
$ ./easyrsa init-pki
```

## ▶ CA 키쌍 생성 및 인증서 self sign

```
$ ./easyrsa build-ca nopass
```

# 서버 키 쌍 생성, 인증서 발행, DH 파라미터 & TA.KEY 생성 및 이동

- ▶ 서버 키 쌍, 인증요청서 생성

```
$ ./easyrsa gen-req server nopass
```

- ▶ 서버 인증서 발행

```
$ ./easyrsa sign-req server server
```

- ▶ dh 생성

```
$ ./easyrsa gen-dh
```

- ▶ ta 생성

```
$ openvpn --genkey secret ta.key
```

- ▶ 서버 키 등 이동

```
$ sudo cp pki/ca.crt pki/private/server.key pki/issued/server.crt pki/dh.pem ta.key /etc/openvpn
```

# 서버 설정

## ▶ 샘플 config 파일 복사

```
$ sudo cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf /etc/openvpn/
```

## ▶ /etc/openvpn/server.conf 파일 수정 ( sudo )

```
34 # TCP or UDP server?  
35 proto tcp  
36 ;proto udp  
37
```

```
82 # Diffie hellman parameters.  
83 # Generate your own with:  
84 #   openssl dhparam -out dh2048.pe  
85 dh dh.pem  
86
```



# 서버 설정

```
188 # and DNS lookups to go through the VPN
189 # (The OpenVPN server machine may need to NAT
190 # or bridge the TUN/TAP interface to the internet
191 # in order for this to work properly).
192 push "redirect-gateway def1 bypass-dhcp"
193
```

```
198 # The addresses below refer to the public
199 # DNS servers provided by opendns.com.
200 push "dhcp-option DNS 208.67.222.222"
201 push "dhcp-option DNS 208.67.220.220"
```

```
272 # You can uncomment this out on
273 # non-Windows systems.
274 user nobody
```

```
315 ;explicit-exit-notify 1
```

# 서버 설정

- ▶ ip forwarding이 되도록 설정

/etc/sysctl.conf 에서 28 라인 net.ipv4.ip\_forward=1로 수정

```
sudo sysctl -p
```

- ▶ 시험 구동

```
sudo systemctl start openvpn@server
```

- ▶ 상태 확인

```
sudo systemctl status openvpn@server
```

# 클라이언트 키 쌍 생성, 인증서 발행

- ▶ 서버에서 실행

- ▶ 클라이언트 키 쌍, 인증요청서 생성

```
~/ca$ ./easysrsa gen-req dschoi nopass
```

- ▶ 인증서 발행

```
$ ./easysrsa sign-req client dschoi
```

- ▶ 인증서, 키 등 이동

```
$ mkdir client
```

```
$ cp pki/ca.crt pki/private/dschoi.key pki/issued/dschoi.crt ta.key client/
```

# OPENVPN 클라이언트 설치

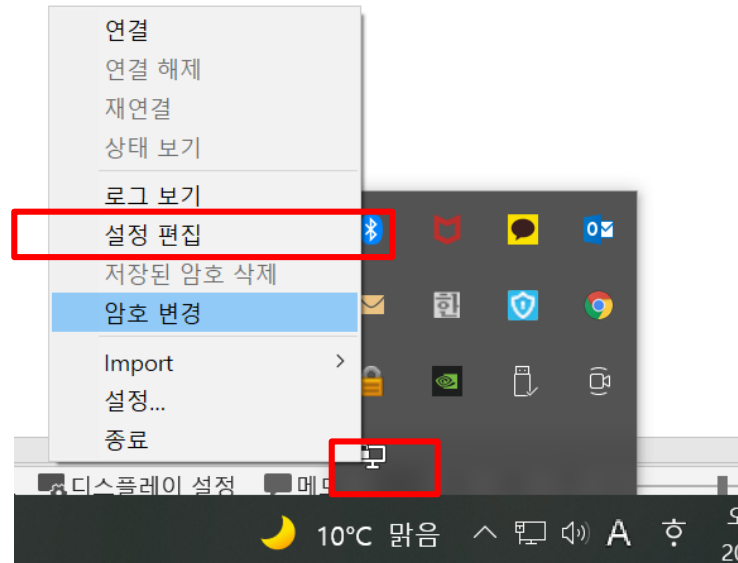
▶ <https://openvpn.net/index.php/open-source/downloads.html>

Windows 64-bit MSI installer

GnuPG Signature

OpenVPN-2.5.7-I602-amd64.msi

▶ 설치 후 실행



# 클라이언트 설정

## ▶ 설정편집 메뉴 = client.ovpn 파일 변경

# Are we connecting to a TCP or

# UDP server? Use the same setting as

# on the server.

proto tcp

;proto udp

# to load balance between the servers.

remote 서버주소 1194

ca ca.crt

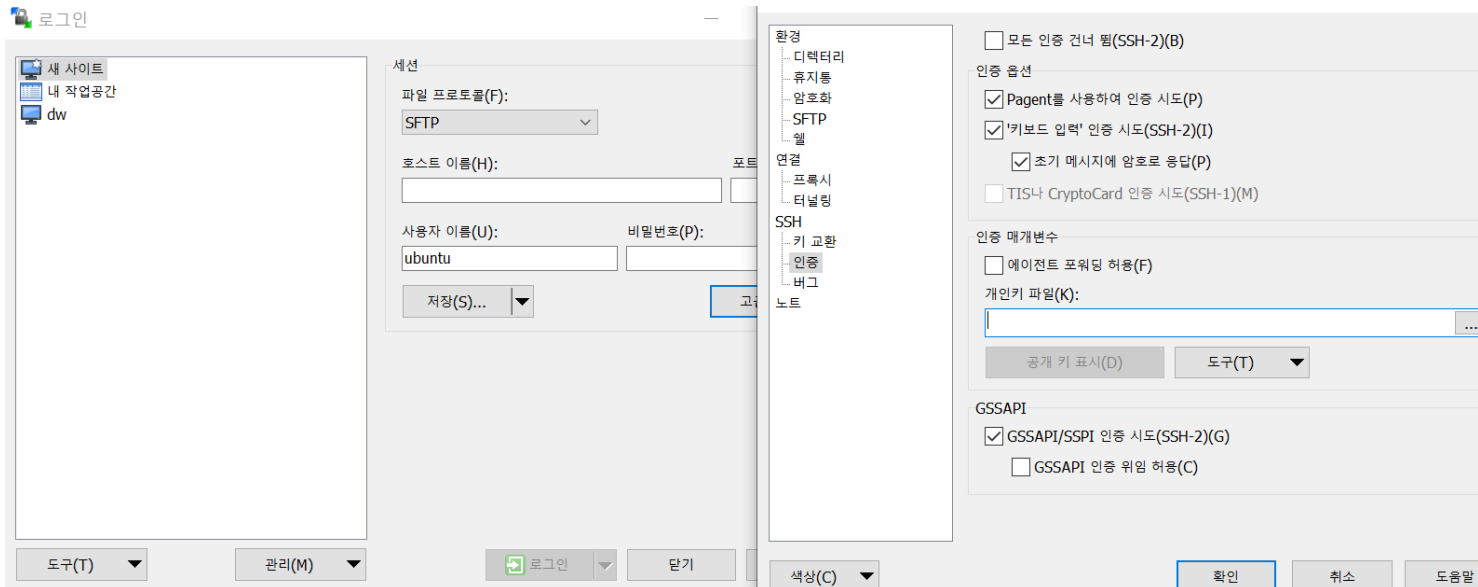
cert dschoi.crt           <= 이름 변경

key dschoi.key            <= 이름 변경

# 클라이언트 키, 인증서 가져오기

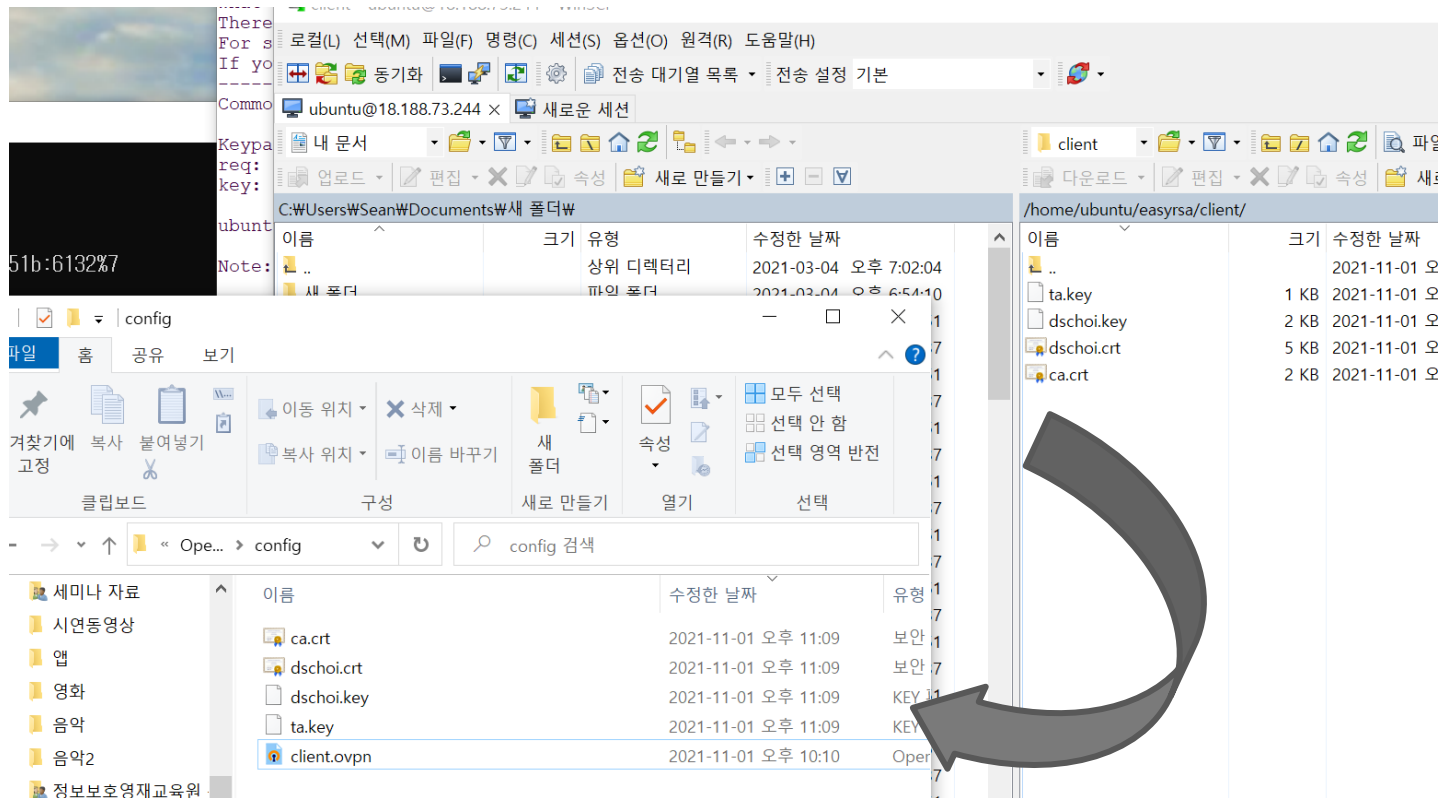
## ▶ winscp

- 다운로드 후 설치 [기존 것은 업그레이드, 안하면 안됨]
- 관리자 권한으로 실행
- putty 와 동일한 ssh 설정



# 클라이언트 키, 인증서 가져오기

▶ client 폴더에서 C:\Program Files\OpenVPN\config 폴더로



# 방화벽 열기

## ▶ ec2 instance 보안 설정

인스턴스 (1/3) 정보

Q 인스턴스 필터링

	Name ▼	인스턴스 ID	인스턴스 상태 ▼	인스턴스 유형 ▼	상태 검사	경보 상태
<input type="checkbox"/>	-	i-0eff794da65a06f65	⊖ 중지됨	t2.micro	-	경보 없음
<input type="checkbox"/>	-	i-05470ae5a761c2539	⊖ 중지됨	t2.micro	-	경보 없음
<input checked="" type="checkbox"/>	- <a href="#">↗</a>	i-0bc7e817f2df48aa8	⊕ 실행 중	t2.micro	⊕ 2/2개 검사 통과...	경보 없음

인스턴스: i-0bc7e817f2df48aa8

세부 정보	보안	네트워킹	스토리지	상태 검사	모니터링	태그
▼ 보안 세부 정보						
IAM 역할			소유자 ID			
-			294922154890			
보안 그룹						
sg-0820e2f1972c67a4f (launch-wizard-7)						

### 인바운드 규칙 정보

Security group rule ID

sgr-05fbd9f570237fa46

유형 정보

사용자 지정 TCP

프로토콜 정보

TCP

포트 범위 정보

1194

소스 정보

사용자 지정

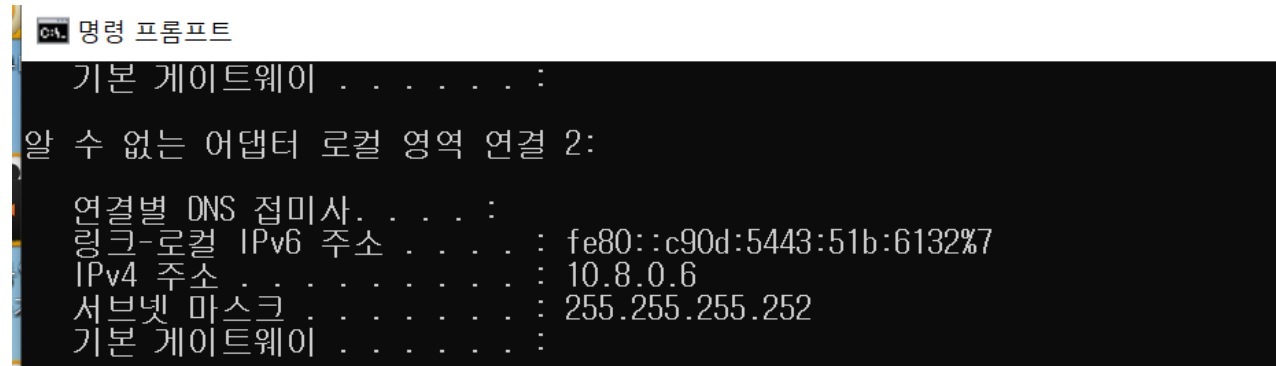
Q

0.0.0.0/0 X



# 접속 및 확인

## ▶ ipconfig



```
C:\> 명령 프롬프트

기본 게이트웨이 . . . . . :
알 수 없는 어댑터 로컬 영역 연결 2:

연결별 DNS 접미사 . . . . :
링크-로컬 IPv6 주소 . . . : fe80::c90d:5443:51b:6132%7
IPv4 주소 . . . . . : 10.8.0.6
서브넷 마스크 . . . . . : 255.255.255.252
기본 게이트웨이 . . . . . :
```

## ▶ ping 10.8.0.1

# 과제2

## ▶ vpn 상태 창 : 2.jpg

