# Marketplace AMI 이용 안하고 EC2 프리티어로 OpenVPN 무료 사용하기
# (AMI = Amazon linux 2023 kernel-6.1)

sudo passwd root
(root 비밀번호 지정)

sudo su
(root 유저로 로그인 * 지정한 비밀번호 입력)

dnf update -y
dnf install -y openvpn git tar wget lz4 nftables
(필요 패키지 설치)

mkdir -p /etc/openvpn
cd /etc/openvpn
git clone https://github.com/OpenVPN/easy-rsa.git easy-rsa
cd easy-rsa/easyrsa3
(Easy-RSA 수동 설치 (AMZ2023에는 easy-rsa 패키지가 없음 → GitHub에서 직접 설치))

cp vars.example vars

vi vars
(undefined 오류 방지)

```
set_var EASYRSA_CA_EXPIRE     3650
set_var EASYRSA_CERT_EXPIRE   3650
set_var EASYRSA_REQ_CN        "My-OpenVPN-CA"
```

./easyrsa init-pki
PKI 초기화

./easyrsa build-ca nopass
CA 생성

./easyrsa gen-req server nopass
(서버 키/CSR/인증서 생성 요구사항 나오면 그냥 default 값으로 설정)

./easyrsa sign-req server server <<< "yes"

./easyrsa gen-dh
(Diffie-Hellman 생성)

openvpn --genkey secret ta.key
(TLS-auth 키 생성)

mkdir -p /etc/openvpn/server

cp pki/ca.crt /etc/openvpn/server/
cp pki/issued/server.crt /etc/openvpn/server/
cp pki/private/server.key /etc/openvpn/server/
cp pki/dh.pem /etc/openvpn/server/
cp ta.key /etc/openvpn/server/
(인증서/키 서버 디렉터리로 복사)

vi /etc/openvpn/server/server.conf

(서버 설정 파일(server.conf) 작성)

```
port 1194
proto udp
dev tun

user nobody
group nobody

ca /etc/openvpn/server/ca.crt
cert /etc/openvpn/server/server.crt
key /etc/openvpn/server/server.key
dh /etc/openvpn/server/dh.pem
tls-auth /etc/openvpn/server/ta.key 0

cipher AES-256-CBC
auth SHA256

topology subnet
server 10.8.0.0 255.255.255.0

push "redirect-gateway def1 bypass-dhcp"
push "dhcp-option DNS 8.8.8.8"

keepalive 10 120
persist-key
persist-tun

status /var/log/openvpn-status.log
verb 3
```

**혹시라도 본인이 만든 VPC 대역 안에 위치한다면 밖에 위치하도록 대역을 수정해주세요**

vi /etc/systemd/system/openvpn-server@.service
(OpenVPN systemd 서비스 생성)

```
[Unit]
Description=OpenVPN service for %i
After=network.target

[Service]
Type=simple
ExecStart=/usr/sbin/openvpn --config /etc/openvpn/server/%i.conf

[Install]
WantedBy=multi-user.target
```

systemctl daemon-reload
systemctl enable openvpn-server@server
systemctl start openvpn-server@server
systemctl status openvpn-server@server
(서비스 활성화)

ip route show default
(dev 뒤에 나오는 이름 확인 ex) dev enX0)

vi etc/nftables.conf

(nftables 설정 파일 생성 iptables 아니고 nftables 사용)
저 붉은 부분 꼭 ip route show default 값 확인해서 넣어야 함 >>

```
flush ruleset

table inet filter {
    chain input {
        type filter hook input priority 0;
        policy accept;
    }
    chain forward {
        type filter hook forward priority 0;
        policy accept;
    }
    chain output {
        type filter hook output priority 0;
        policy accept;
    }
}

table ip nat {
    chain postrouting {
        type nat hook postrouting priority srcnat;
        oif "enX0" ip saddr 10.8.0.0/24 counter masquerade
    }
}
```

```
cp /etc/nftables.conf /etc/sysconfig/nftables.conf
systemctl enable --now nftables
nft -f /etc/sysconfig/nftables.conf
nft list ruleset
```

(작성한 nftables 적용 & 영구 저장)
nft list ruleset 값이 oif "enX0" ip saddr 10.8.0.0/24 counter masquerade 이 나타나면 정상(openvpn 대역대 안바꿨다면)

```
echo "net.ipv4.ip_forward = 1" >> /etc/sysctl.conf
sysctl -p

sysctl net.ipv4.ip_forward
```

IP 포워딩 활성화
0나오면 안됨 1나와야 함

## vi /usr/local/bin/gen_ovpn.sh

(OVPN 자동 생성 스크립트 왼쪽 박스 먼저 입력하고
이어서 오른쪽 박스 입력해야 함 ppt 화면 때문에 나눠놓은 것)

## chmod +x /usr/local/bin/gen_ovpn.sh

(스크립트 실행 권한 부여)

## cd /usr/local/bin/gen_ovpn.sh

## ./gen_ovpn.sh client1

(스크립트가 위치한 곳으로 이동해 스크립트 실행)

자동 스크립트라 스크립트 명 뒤에 client1 같이 클라이언트 이름 지정해주면 자동으로 생성

## ls /etc/openvpn/clients

```
[root@ip-10-0-1-253 clients]# ls /etc/openvpn/clients
client1.ovpn
[root@ip-10-0-1-253 clients]#
```

```
#!/bin/bash

CLIENT_NAME=$1
OVERRIDE_IP=$2
PORT=1194

EASYRSA_DIR="/etc/openvpn/easy-rsa/easyrsa3"
OUTPUT_DIR="/etc/openvpn/clients"
TA_KEY="/etc/openvpn/server/ta.key"
CONFIG_FILE="$OUTPUT_DIR/${CLIENT_NAME}.ovpn"

if [ -z "$CLIENT_NAME" ]; then
    echo "사용법: $0 <client_name> [server_ip]"
    exit 1
fi

mkdir -p "$OUTPUT_DIR"

if [ -n "$OVERRIDE_IP" ]; then
    SERVER_IP="$OVERRIDE_IP"
else
    TOKEN=$(curl -sX PUT
"http://169.254.169.254/latest/api/token" ₩
        -H "X-aws-ec2-metadata-token-ttl-seconds: 21600")

    SERVER_IP=$(curl -s ₩
        -H "X-aws-ec2-metadata-token: $TOKEN" ₩
        http://169.254.169.254/latest/meta-data/public-ipv4)
fi

cd "$EASYRSA_DIR"

./easyrsa gen-req "$CLIENT_NAME" nopass
./easyrsa sign-req client "$CLIENT_NAME" <<< "yes"

CA_CRT="$EASYRSA_DIR/pki/ca.crt"
CLIENT_CRT="$EASYRSA_DIR/pki/issued/$CLIENT_NAME.cr
t"
CLIENT_KEY="$EASYRSA_DIR/pki/private/$CLIENT_NAME.k
ey "

#이어서 왼쪽 박스에 있는 내용 입력
```

```
echo "client
dev tun
proto udp
remote $SERVER_IP $PORT
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
cipher AES-256-CBC
auth SHA256
verb 3
key-direction 1

<ca>" > "$CONFIG_FILE"

cat "$CA_CRT" >> "$CONFIG_FILE"
echo "</ca>" >> "$CONFIG_FILE"

echo "<cert>" >> "$CONFIG_FILE"
grep -A 1000 "BEGIN CERTIFICATE" "$CLIENT_CRT" >>
"$CONFIG_FILE"
echo "</cert>" >> "$CONFIG_FILE"

echo "<key>" >> "$CONFIG_FILE"
cat "$CLIENT_KEY" >> "$CONFIG_FILE"
echo "</key>" >> "$CONFIG_FILE"

echo "<tls-auth>" >> "$CONFIG_FILE"
cat "$TA_KEY" >> "$CONFIG_FILE"
echo "</tls-auth>" >> "$CONFIG_FILE"
echo "" >> "$CONFIG_FILE"
```

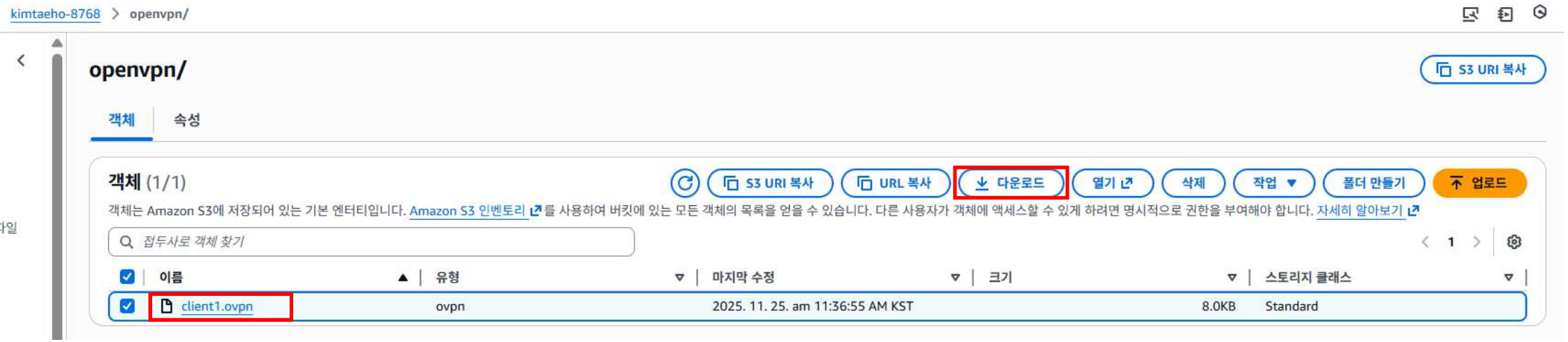
## aws configure  (awscli 안 깔려있으면 끝 페이지 확인)

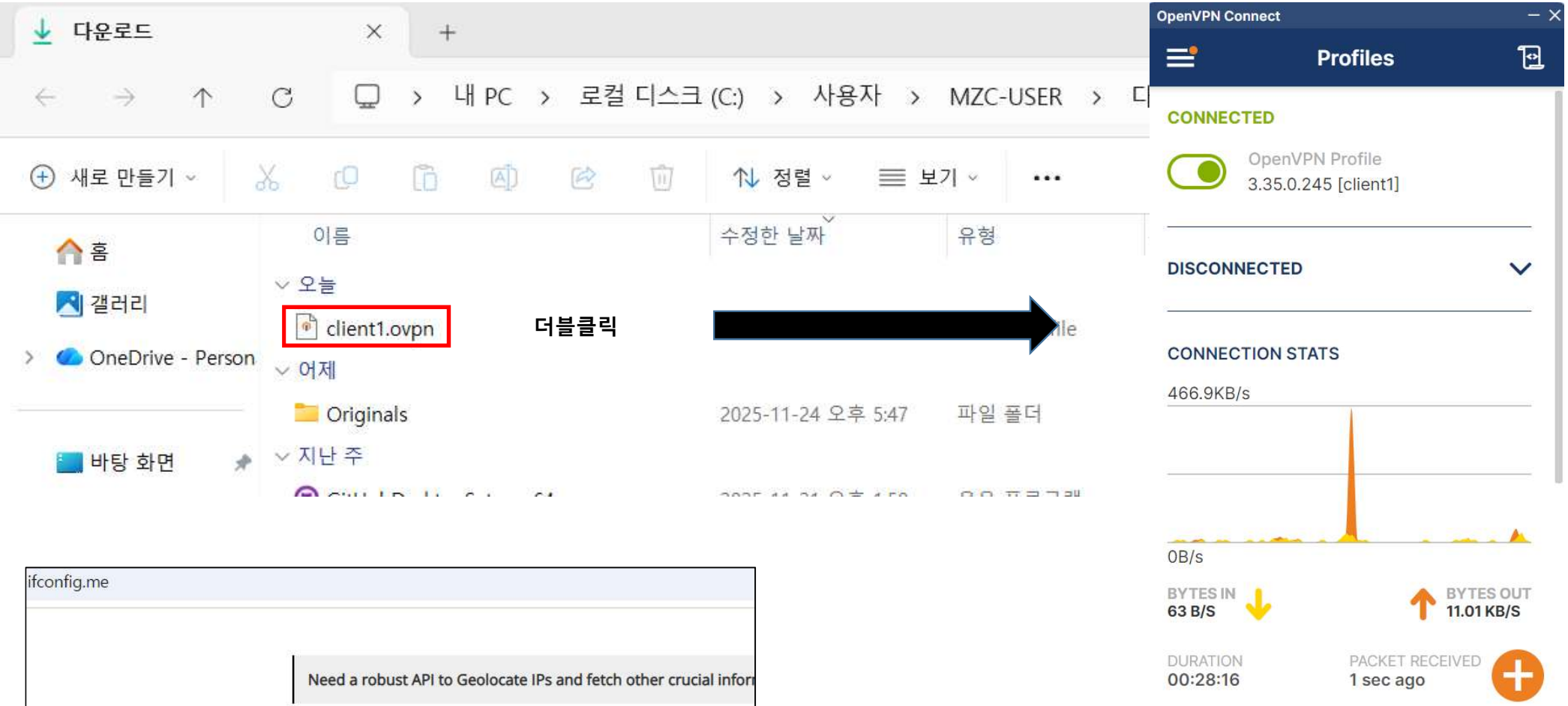
AWS Access Key ID: (키 입력)
AWS Secret Access Key: (비밀키 입력)
Default region name: (S3 위치한 리전 입력)
Default output format: json

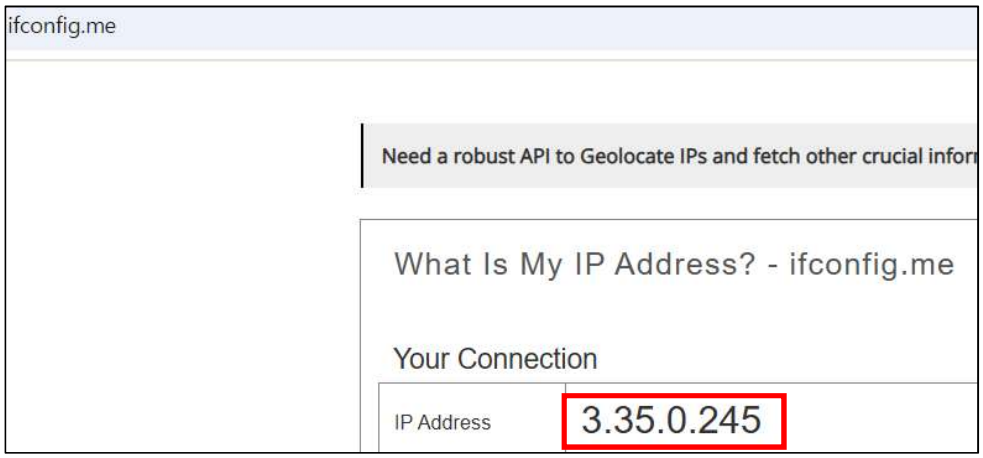
## aws s3 cp /etc/openvpn/clients/client1.ovpn s3://[내 버킷 이름]/openvpn/client1.ovpn

Ex) aws s3 cp /etc/openvpn/clients/client1.ovpn s3://kimtaeho-8768/openvpn/client1.ovpn

## aws s3 ls s3://kimtaeho-8768/openvpn/




다운로드
내 PC
로컬 디스크 (C:)
사용자
MZC-USER
새로 만들기
정렬
보기
이름
수정한 날짜
유형
홈
갤러리
OneDrive - Person
바탕 화면
오늘
client1.ovpn
더블클릭
어제
Originals
2025-11-24 오후 5:47
파일 폴더
지난 주
OpenVPN Connect
Profiles
CONNECTED
OpenVPN Profile
3.35.0.245 [client1]
DISCONNECTED
CONNECTION STATS
466.9KB/s
0B/s
BYTES IN
63 B/S
BYTES OUT
11.01 KB/S
DURATION
00:28:16
PACKET RECEIVED
1 sec ago


ifconfig.me
Need a robust API to Geolocate IPs and fetch other crucial infor
What Is My IP Address? - ifconfig.me
Your Connection
IP Address
3.35.0.245

**curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip“**

**unzip awscliv2.zip**

**sudo ./aws/install**

**aws --version**