OpenVPN 서버 구축

구축 목적

: 특정한 서버의 사설망으로 접근이 필요할때 OpenVPN 서버로부터 가상 터널링 인터페이스 IP를 할당받아 접속하기 위하여

```
ex) 내 컴퓨터에서 VPN 서버를 통해서 KT Cloud의 사설 VM 으로 접속 ( conf에서 push
route에 사설 IP 대역대를 적용하여 접속 )
     내 컴퓨터           ->    VPN 서버        ->  KT 사설망
(218.154.31.75/32)          (10.8.0.0/16)        (172.27.0.0/16)
```

OpenVPN 구축

서버 설정

```
# yum -y install epel-release
# yum -y install openvpn openssl easy-rsa

# cp /usr/share/doc/openvpn-2.4.11/sample/sample-config-files/server.conf
/etc/openvpn
( server.conf 복사 )

# mkdir easy-rsa
# cp -R /usr/share/easy-rsa/3.0.8/* /etc/openvpn/easy-rsa/
( easy-rsa 모두 복사 )

# cd /etc/openvpn/easy-rsa/
# cp openssl-easyrsa.cnf openssl.cnf
( easyrsa cnf 백업 )

# mkdir /var/log/openvpn
( 로그 저장 디렉토리 생성 )

# cd /etc/openvpn
# vi server.conf
-----------------------------------------------------
port 1194

proto tcp
;proto udp

;dev tap
dev tun

;dev-node MyTap

ca /etc/openvpn/easy-rsa/keys/ca.crt
```

```
cert /etc/openvpn/easy-rsa/keys/cloud.crt
key /etc/openvpn/easy-rsa/keys/cloud.key  # This file should be kept secret
dh /etc/openvpn/easy-rsa/keys/dh.pem

topology subnet

server 10.8.0.0 255.255.255.0

;ifconfig-pool-persist ipp.txt

;server-bridge 10.8.0.4 255.255.255.0 10.8.0.50 10.8.0.100

;server-bridge

push "route 172.27.0.0 255.255.0.0"
;push "route 192.168.20.0 255.255.255.0"

;client-config-dir ccd
;route 192.168.40.128 255.255.255.248
;client-config-dir ccd
;route 10.9.0.0 255.255.255.252

;learn-address ./script

;push "redirect-gateway def1 bypass-dhcp"
;push "dhcp-option DNS 8.8.8.8"
;push "dhcp-option DNS 8.8.4.4"

;client-to-client

;duplicate-cn

keepalive 10 120

;tls-auth ta.key 0 # This file is secret

cipher AES-256-GCM
auth SHA512

;compress lz4-v2
;push "compress lz4-v2"

;comp-lzo

;max-clients 100

user nobody
group nobody

persist-key
persist-tun

status /var/log/openvpn/openvpn-status.log
log-append /var/log/openvpn/openvpn.log
```

```
verb 3

;mute 20

explicit-exit-notify 0
-----------------------------------------------------------

# vi /etc/yum.repos.d/epel.repo
-----------------------------------------------------------
2 baseurl=http://download.fedoraproject.org/pub/epel/7/$basearch
3 #metalink=https://mirrors.fedoraproject.org/metalink?repo=
-----------------------------------------------------------
( 2번 주석풀고 , 3번 주석처리 )

# vi /etc/openvpn/easy-rsa/vars
( 필요에 따라 키 생성 시 사용할 설정 정보를 수정하는곳 )

ex )
-----------------------------------------------------------
export KEY_COUNTRY="KR"
export KEY_PROVINCE=""
export CITY="Seoul"
export ORG="TEST"
export KEY_EMAIL="test@gmail.com"
export KEY_OU="TEST"
export KEY_NAME="server"
export KEY_CN="test.example.co.kr"
-----------------------------------------------------------
# source ./vars
( 적용 )


# cd easy-rsa/
# ./easyrsa init-pki
( PKI 초기화 및 디렉토리 생성 )

# ./easyrsa build-ca nopass
( CA 인증서 및 키 생성 - ca.crt, ca.key)
-> 패스워드 설정 , 서버 이름 설정 (cloud)

# ./easyrsa gen-req cloud nopass
( OpenVPN에서 사용할 키 생성 - server.req, server.key )
-> 서버 이름 설정 (cloud)

# ./easyrsa sign-req server cloud
( request 타입과 서버이름 설정 후 인증서 생성 - server.crt)
- yes

# ./easyrsa gen-dh
( diffie-hellman 키 교환 파일 생성 )


# mkdir -p /etc/openvpn/esay-rsa/keys
```

```
# cp /etc/openvpn/server/easy-rsa/pki/ca.crt /etc/openvpn/easy-rsa/keys/
# cp /etc/openvpn/server/easy-rsa/pki/private/cloud.key /etc/openvpn/easy-
rsa/keys/
# cp /etc/openvpn/server/easy-rsa/pki/issued/cloud.crt /etc/openvpn/easy-rsa/keys/
# cp /etc/openvpn/server/easy-rsa/pki/dh.pem  /etc/openvpn/easy-rsa/keys/
( 4개의 키 및 인증서 파일을 한곳으로 옮겨놓기 )

# vi /etc/sysctl.conf
-----------------------------------------------------
net.ipv4.ip_forward = 1
-----------------------------------------------------
( 수신된 패킷을 외부로 포워딩해주는 기능 활성화 )
( 맨 밑줄에 추가 )

# sysctl -p
( 적용 )
```

Client 연결

1. 키 생성

```
# ./easyrsa gen-req dw nopass
# ./easyrsa sign-req client dw

# cp /etc/openvpn/easy-rsa/pki/issued/dw.crt /etc/openvpn/easy-rsa/keys
# cp /etc/openvpn/easy-rsa/pki/private/dw.key /etc/openvpn/easy-rsa/keys
```

2. 키 이동 SFTP 프로그램을 이용하여 Client(window)에 C:\Program Files\OpenVPN안에 keys 폴더 생성 후 ca.crt, dw.crt, dw.key 등 파일 이동

3. Ovpn 파일 생성 C:\Program Files\OpenVPN\config 폴더 안에 Client 전용 conf파일 ovpn 생성

```
-----------------------------------------------------

remote 211.251.236.200 1194

client

remote-cert-tls server

dev tun0

proto tcp

auth SHA512
cipher AES-256-GCM

resolv-retry infinite
```

```
nobind

persist-key

persist-tun

float

ca "C:\\Program Files\\OpenVPN\\keys\\ca.crt"

cert "C:\\Program Files\\OpenVPN\\keys\\dw.crt"

key "C:\\Program Files\\OpenVPN\\keys\\dw.key"
-----------------------------------------------------

# systemctl start openvpn@server
# systemctl enable openvpn@server
# systemctl daemon-reload

# vi /usr/lib/systemd/system/openvpn@.service
( 필요에 따라 경로 변경하는곳 )
```

TEST

1. 윈도우에 설치한 OpenVPN GUI를 실행시켜서 연결 잘 되는지 확인

2. cmd에서 ipconfig로 OpenVPN ip가 잘 올라가있는지 확인

3. VPN 서버에서 ip a 명령어로 장비가 잘 올라갔는지 IP 맞는지 확인

★ 정상적으로 작동된다면 OpenVPN 서버 구축 완료 ! ★

참조

- Server : https://hiteit.tistory.com/5 https://indienote.tistory.com/142
- config : http://www.t8.co.kr/bbs/board.php?bo_table=networking&wr_id=2 https://hook.tistory.com/entry/Windows-%EC%9A%B4%EC%98%81%EC%B2%B4%EC%A0%9C%EC%97%90-OpenVPN-Client-%EC%84%A4%EC%A0%95%ED%95%98%EA%B8%B0