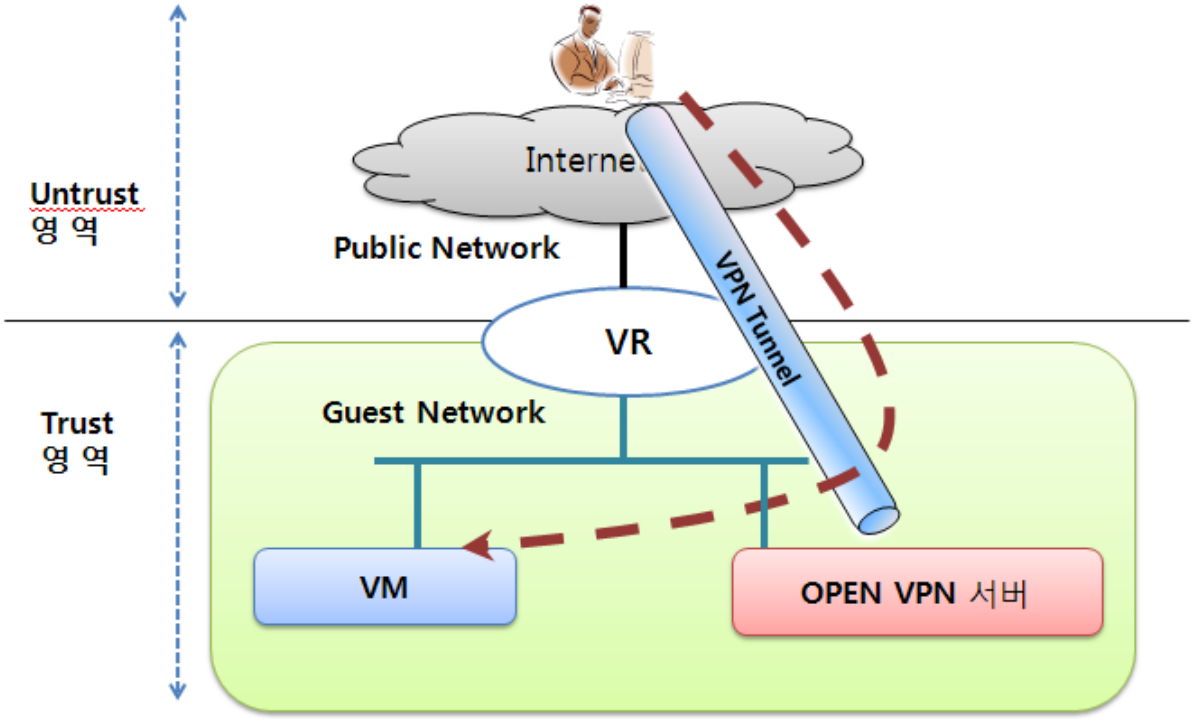
OpenVPN 설정 가이드

2013.2

목 차

1. 활용개념도

외부 네트워크에서 uCloud 내부 Guest 네트워크로의 보안접속 환경은 아래와 같이 제공됩니다.

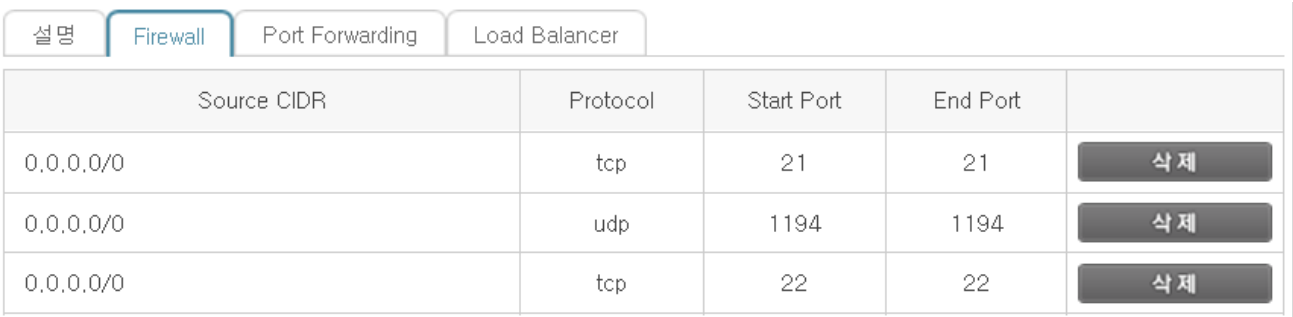


1.1.1 네트워크 구성

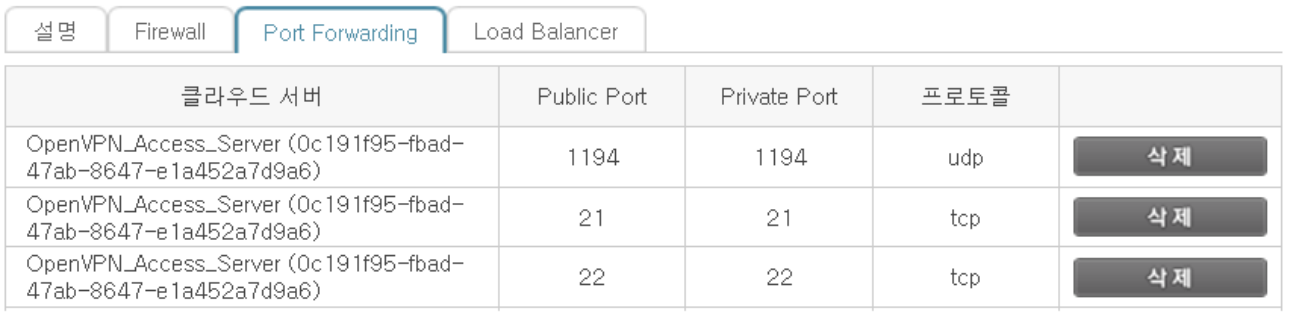
항 목	부 연
Public Network	VR 에 주어진 공인 IP 를 이용하여 인터넷 통신을 하는 구간입니다.
Guest Network	고객별 주어지는 내부네트워크로서 172.27.0.0/16 대역이 고객의 VM eth0 IP 로 부여됩니다.
Tunneling Network	OpenVPN 서버가 보안통신을 위한 사용하는 터널링 대역으로서 초기 서버구동시 10.8.0.0/24 대역이 부여됩니다. 이 때 사용하는 포트는 UDP 1194 입니다.

1.1.2 uCloud 포탈 방화벽, 포트포워딩 설정시 고려사항

[방화벽 설정]



[포트포워딩 설정]



각 Port 의 용도는 아래와 같습니다.

Port	Description
UDP 1194	OpenVPN Access Serve의 Daemon이 사용하는 Port입니다.
TCP 21	Client가 CA인증서와 사용메뉴얼을 다운받기 위한 VSFTP서버의 Passive Mode 동작용 Port입니다
TCP 22	SSH 접속용 Port 입니다.

2. Server Side 설정

2.1 OpenVPN Access Server

초기 접속시 OpenVPN/FTP 서버의 구동정보를 Dynamic Motd 를 통하여 확인하실 수 있으며 Access Server 의 설정을 아래와 같이 확인 및 변경 하실 수 있습니다.

2.1.1 Access Server 의 Config 확인

확인 위치 : /etc/openvpn/server.conf

주요 컨피그	부연
port 1194	
proto udp	
dev tun	routed IP tunnel
ca ca.crt	인증기관(자체) 인증서
cert server.crt	Access 서버 인증서(공개키 포함)
key server.key	Access 서버 개인키
dh dh1024.pem	
server 10.8.0.0 255.255.255.0	Tunneling 용 IP 배포 대역
ifconfig-pool-persist ipp.txt	IP 부여 내역 기록
push "route 172.27.0.0 255.255.0.0"	Client 의 라우팅테이블에 추가

2.1.2 Access Server 계정 추가

Client 는 발급된 User 용 "아이디/패스워드"로 VPN 접속이 가능합니다.

```
# useradd  [아이디]
# passwd  [아이디]  엔터 후 2 회 패스워드 입력
```

2.1.3 Access Server 및 vsFTP 구동방식 변경

현재는 리부팅시 자동구성 설정되어 있으며 수동 구동은 아래와 같이 하시면 됩니다.

```
# chkconfig openvpn off
# chkconfig  --list openvpn
# service openvpn start

# chkconfig  vsftpd off
# chkconfig  --list vsftpd
# service vsftpd start
```

2.2 Ucloud VM

외부에서 터널링을 이용하여 Guest 네트워크내의 VM 에 접속하기 위해서는 터널링 대역에 대한 라우팅 설정이 필요합니다.

2.2.1 Linux(CentOS 5.X) 설정

(1) 임시 적용(리부팅시 라우팅 테이블 사라짐)

```
# route add -net 10.8.0.0 netmask 255.255.255.0 gw [openvpn 서버 eth0 IP]
```

(2) 영구 적용(리부팅시에도 라우팅 테이블 유지됨)

```
# vi /etc/sysconfig/network-scripts/route-eth0
10.8.0.0/24 via [openvpn 서버 eth0 IP]
# service network restart
```

2.2.2 Windows VM 설정

(1) 임시 적용(리부팅시 라우팅 테이블 사라짐)

```
# route add 10.8.0.0 mask 255.255.255.0   [openvpn 서버 eth0 IP]
```

(2) 영구 적용(리부팅시에도 라우팅 테이블 유지됨)

```
# route add –p 10.8.0.0 mask 255.255.255.0   [openvpn 서버 eth0 IP]
```

3. Client Side 구성

3.1 Windows Client

3.1.1 Client 프로그램 설치

- ㅇ http://www.openvpn.net 에 접속
- ㅇ Downloads ➔ Community Downloads 선택
- ㅇ Windows Installer (openvpn-2.2.2-install.exe) 다운로드 후 설치

3.1.2 Client 컨피그 파일 복사

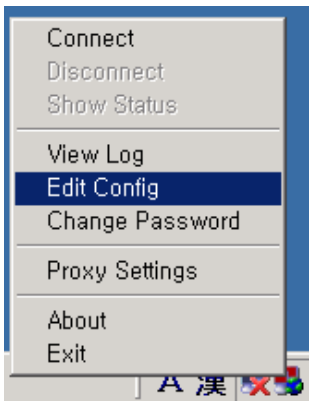
- ㅇ C:₩Program Files₩OpenVPN₩sample-config 의 client.ovpn을 복사하여 C:₩Program Files₩OpenVPN₩config 에 붙여 넣음

3.1.3 CA 인증서 복사

- ㅇ 웹브라우져의 창에 ftp://[*OpenVPN 서버IP*]를 입력
- ㅇ 아이디/패스워드 입력 후 로그인 하여 pub 디렉토리의 ca.crt 복사
- ㅇ C:₩Program Files₩OpenVPN₩config 에 붙여 넣음

3.1.4 컨피그 설정 접속

Windows 오른편 하단 아이콘 메뉴 선택



3.1.5 컨피그 설정

[추가설정]

remote [*OpenVPN 서버IP*] 1194

auth-user-pass

[주석처리]

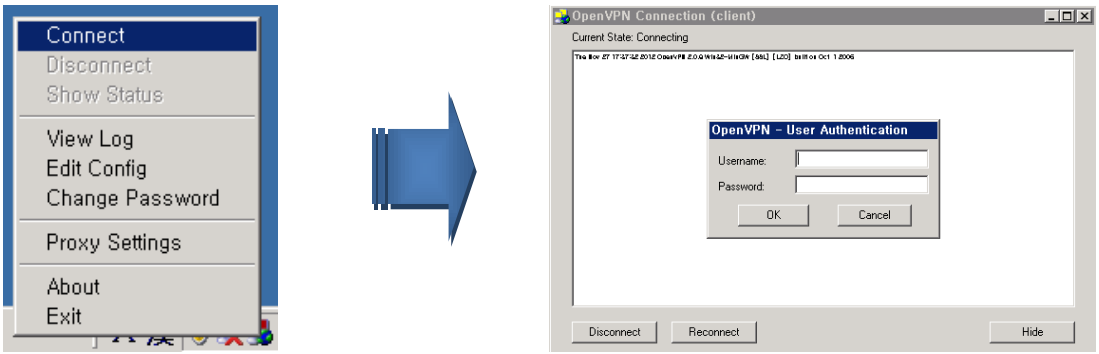
cert client.crt

key client.key

☞ auth-user-pass : Access Server(리눅스)상의 user정보를 사용하도록 함

3.1.6 OpenVPN Client 프로그램 구동을 통한 접속

ㅇ Windows 오른편 하단 아이콘 메뉴 선택 후 아이디/패스워드 입력



3.2 Linux Client (Cento0S 5.x 기준)

3.2.1 RPMforge 설치

wget http://pkgs.repoforge.org/rpmforge-release/rpmforge-release-0.5.2-2.el5.rf.x86_64.rpm

rpm -ivh rpmforge-release-0.5.2-2.el5.rf.x86_64.rpm

rm rpmforge-release-0.5.2-2.el5.rf.x86_64.rpm

3.2.2 OpenVPN 설치

```
# yum install openvpn
```

3.2.3 디렉토리 이동 및 컨피그/키 파일 복사

```
# cp -R /usr/share/doc/openvpn-2.2.2/* /etc/openvpn
# cp /etc/openvpn/sample-config-files/client.conf /etc/openvpn
# cp /etc/openvpn/sample-keys/ca.crt   /etc/openvpn
```

3.2.4 컨피그 설정

[추가설정]

remote [*OpenVPN 서버IP*] 1194

auth-user-pass

[주석처리]

cert client.crt

key client.key

☞ auth-user-pass : Access Server(리눅스)상의 user정보를 사용하도록 함

4. 참고사항

4.1 Access Server 에서 Client 에 배포되는 IP 확인

ㅇ 아이디별로 한 번 할당된 IP가 재접속시에도 동일하게 배정됩니다.

ㅇ **아이디별 IP할당 내역은 /etc/openvpn/ipp.txt**를 보시면 됩니다.

- IP할당내역은 Openvpn서버를 재구동 할 때 배포내역이 현행화 됩니다.

ㅇ 접속자 로그 확인 : /etc/openvpn/openvpn-status.log

4.2 인증서 인증방식 추가

ㅇ공식싸이트 매뉴얼을 참조하시면 됩니다

- www.openvpn.net ➔ Community(상단플래쉬 메뉴)➔ HOWTO(좌측메뉴)

➔ Setting up your own Certificate Authority (CA) and generating certificates and keys for an OpenVPN server and multiple clients