

# Ccontrols OpenVPN 설정 매뉴얼



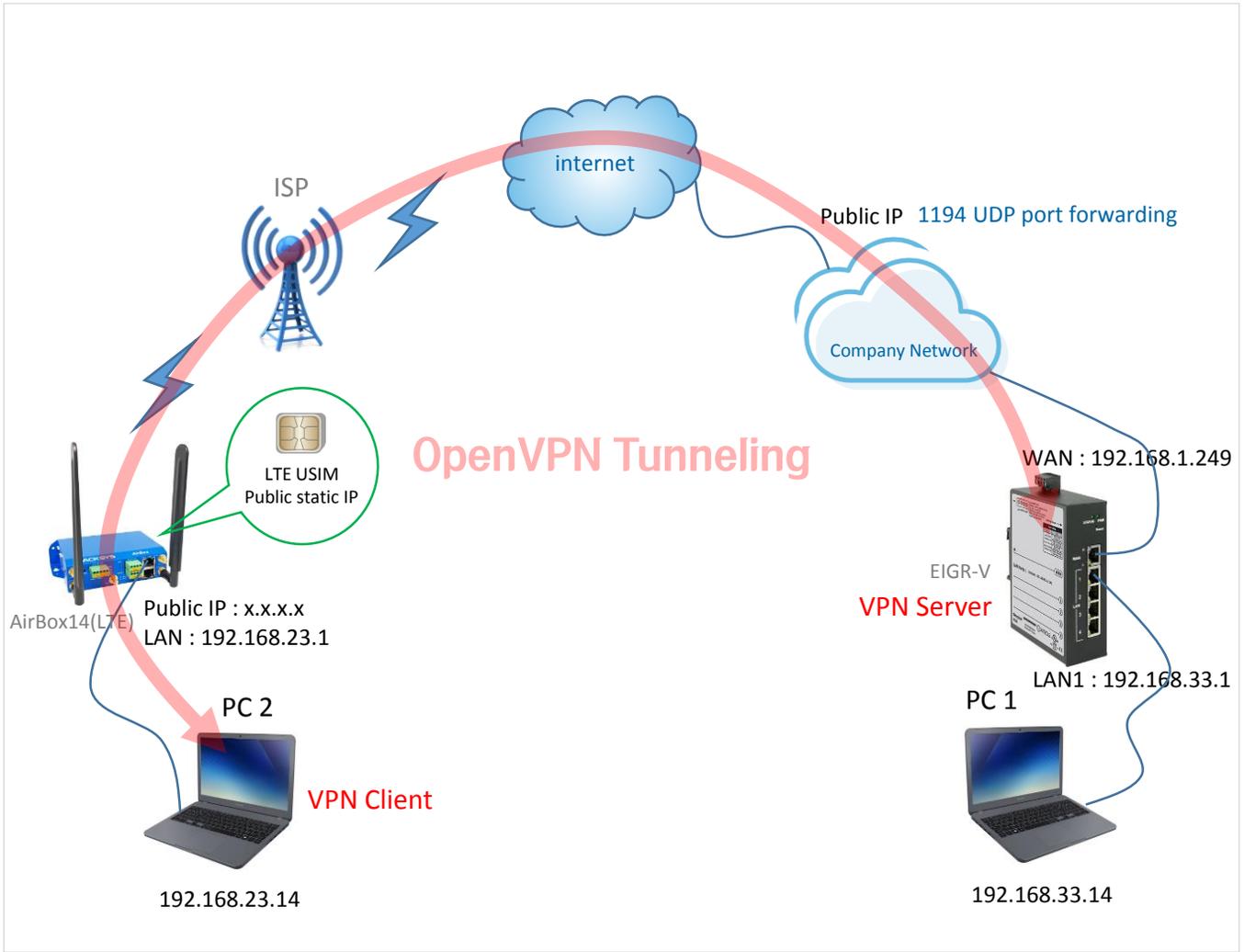
EIGR-V

## 1. 구성도 및 개요

## 2. OpenVPN 서버 설정 (EIGR-V)

- 기본 설정
- 인증서/키 생성
- 라우터 설정

## 3. OpenVPN 클라이언트 설정 (PC)



PC에 설치된 OpenVPN 클라이언트가 외부망을 통해 사무실 백본에 있는 EIGR-V OpenVPN 서버에 연결되는 예시입니다. 사내 네트워크망에서는 VPN 클라이언트의 트래픽이 VPN 서버에 전달될 수 있도록 라우터에 포트포워딩 규칙(여기서는 1194 포트)을 설정해주세요.

위의 구성도 처럼 OpenVPN 클라이언트는 LTE 라우터를 통해 공인 IP로 구성하실 수 있고, 서버측과 분리된 사무실 네트워크로도 구성하실 수 있습니다.

윈도우 PC에서는 기본적으로 방화벽에 의해 ping 응답이 비활성화 되어 있으므로 들어오는 ping 트래픽을 허용하는 규칙을 추가하세요. PC1과 PC2는 아래처럼 설정하실 수 있으며, 이 매뉴얼에서의 모든 IP는 네트워크 환경에 따라 적절하게 변경하실 수 있습니다.

구분	PC1		PC2	
IP	192.168.33.14		192.168.23.14	
Subnet Mask	255.255.255.0		255.255.255.0	
Gateway	192.168.33.1		192.168.23.1	
DNS	기본	168.126.63.1	기본	211.36.129.4
	보조	168.126.63.2	보조	117.111.29.4

## ① 기본설정 » ② 인증서/키생성 » ③ 라우팅 설정



Setup Administration Status Advanced Save Cha

Setup 메뉴를 클릭합니다.



### WAN Setup

Connection Type:

IP Address:

Subnet Mask:

Default Gateway:

Static DNS 1:

Static DNS 2:

Static DNS 3:

Optional Settings (required by some ISPs)

Host Name:

Domain Name:

MTU:  Enable  Disable Size:

WAN 설정을 네트워크 환경에 맞춰 입력합니다. 해당 IP와 VPN 통신 포트번호 (여기서는 1194)는 사내 라우터에서 포트포워딩 해주시기 바랍니다.

### LAN Setup

Router IP

Local IP Address:

Subnet Mask:

Network Address Server Settings (DHCP)

Local DHCP Server:  Enable  Disable

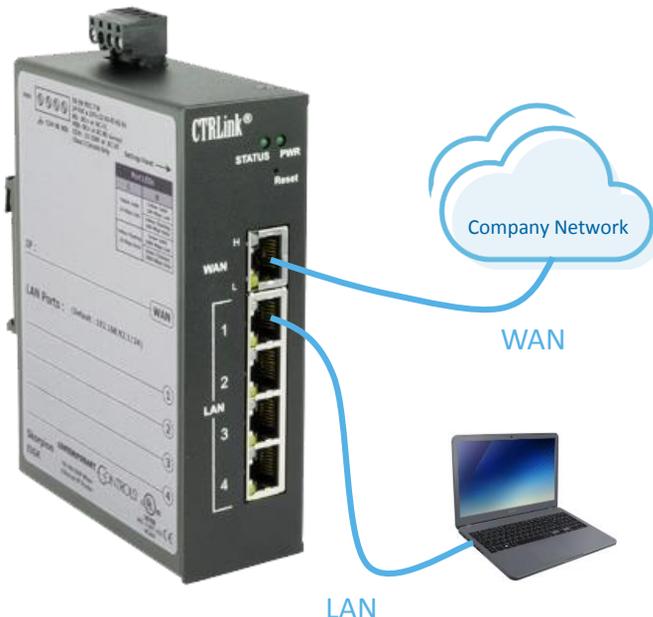
Start IP Address:

Number of Addresses:  (1 to 254)

Client Lease Time:  minutes (0 means one day)

LAN 설정도 네트워크 환경에 맞춰 입력합니다.

입력 후 'Save'를 눌러 설정을 저장합니다.



## ① 기본설정 » ② 인증서/키생성 » ③ 라우팅 설정

Advanced > VPN



Setup

Administration

Status

Advanced

Save Char



## VPN

- Status:  Enable  Disable
- Mode:  Server  Client
- Internet Access:  Enable  Disable
- Masquerade:  Enable  Disable

Save

Cancel

VPN 모드 선택 및 활성화 설정을 합니다.

**Status** : VPN 기능 활성화 및 비활성화

**Mode** : OpenVPN 서버 및 클라이언트 설정

**Internet Access** : VPN 기능이 활성화 된 상태에서 인터넷에 액세스 가능

**Masquerade** : 이 제품의 LAN에 연결된 장치에 액세스 가능

## ① 기본설정 » ② 인증서/키생성 » ③ 라우팅 설정

Advanced > VPN > OpenVPN Server > Config Connection Settings



Setup

Administration

Status

Advanced

Save Char



## Skorpion EIGR GigE Router

Automation Firewall/Router

### OpenVPN Connection Settings

Public IP Address:	<input type="text" value="X.X.X.X"/>
OpenVPN Port:	<input type="text" value="1194"/>
Ping Interval:	<input type="text" value="30"/> (secs)
Ping Timeout:	<input type="text" value="120"/> (secs)

Save

Cancel

Public IP는 사내에서 사용하는 공인 IP를 입력해주시고, OpenVPN Port는 통신할 포트번호를 입력합니다. 그 외에는 기본 설정을 사용합니다.

① 기본설정 » ② 인증서/키생성 » ③ 라우팅 설정

Advanced > VPN > OpenVPN Server > Config Certificate Authority(CA)



Setup

Administration

Status

Advanced

Save Char



## OpenVPN Certificate Authority (CA) Setup

Country Code (2 letter code):	<input type="text" value="KR"/>
State or Province Name (full name):	<input type="text" value="KOREA"/>
Locality or City Name:	<input type="text" value="SEOUL"/>
Organization Name [eg, Company]:	<input type="text" value="WITREE"/>
Organization Unit Name [eg, Section]:	<input type="text" value="TECH"/>
Common Name [eg, Your Name or your Server Hostname]:	<input type="text" value="WIT"/>
Email Address:	<input type="text" value="robert@witree.co.kr"/>

Save

Cancel

Generate OpenVPN CA

OpenVPN 인증 권한 구성을 진행합니다.

위의 예시처럼 항목에 적절한 내용을 입력(추후 정보 수정 불가)하시고 'Save'를 클릭한 후 'Generate OpenVPN CA' 버튼을 눌러 CA 인증서와 키를 생성합니다.

주의 : 이 설정은 OpenVPN에 대한 다른 구성 또는 인증서 생성 전에 수행해야 합니다.

CA는 한 번만 생성되며 변경되지 않으므로 다른 모든 인증서와 키가 무효가 되며, OpenVPN 클라이언트에 의한 추가 연결이 금지되므로 되돌릴 수 없습니다. 추후 정보 수정이 되지 않기에 신중하게 입력하세요.

- ① 기본설정 » ② 인증서/키생성 » ③ 라우팅 설정

Advanced > VPN > OpenVPN Server > Config Device Names



Setup Administration Status **Advanced** Save Changes



## Set OpenVPN Server and Clients Name

### Server:

Server Name:

### Clients:

No.	EIPR/EIGR Router Clients Name
1	<input type="text" value="AirBox14"/>
2	<input type="text"/>
3	<input type="text"/>
4	<input type="text"/>
5	<input type="text"/>

No.	PC Clients Name
1	<input type="text" value="toshiba_notebook"/>
2	<input type="text"/>
3	<input type="text"/>
4	<input type="text"/>
5	<input type="text"/>

OpenVPN 장치의 이름을 구성합니다.

각 이름은 고유해야하고 이름에 공백이 없어야 합니다. 클라이언트로 사용할 라우터 또는 PC 항목에 이름을 기입하고 저장합니다.

- ① 기본설정 » ② 인증서/키생성 » ③ 라우팅 설정

Advanced > VPN > OpenVPN Server > Generate Certificates/Keys



## Generate Certificates and Keys for OpenVPN Server and Clients

Server:

Clients:

No.	Certificates and Keys for EIPR/EIGR Router Clients	
1	AirBox14	<input type="button" value="Generate Certs"/>
2		<input type="button" value="Generate Certs"/>
3		<input type="button" value="Generate Certs"/>
4		<input type="button" value="Generate Certs"/>
5		<input type="button" value="Generate Certs"/>
No.	Certificates and Keys for PC Clients	
1	toshiba_notebook	<input type="button" value="Generate Certs"/>
2		<input type="button" value="Generate Certs"/>
3		<input type="button" value="Generate Certs"/>
4		<input type="button" value="Generate Certs"/>
5		<input type="button" value="Generate Certs"/>

OpenVPN 서버 및 클라이언트에 대한 인증서와 키를 생성합니다.

앞서 진행된 장치 이름이 구성되면 해당 'Generate Certs' 버튼이 활성화 됩니다.

'Generate Server Certs' 버튼을 클릭하면 서버 인증서와 키가 생성되는데 최대 15분이 소요됩니다.

**백그라운드에서 진행되므로 화면에 아무런 표시가 나오지 않지만 15분 동안 제품을 재부팅하거나 전원을 껐다 켜지 마세요.**

라우터 클라이언트 및 PC 클라이언트 인증서는 개별적으로 또는 일괄적으로 생성할 수 있습니다.

- ① 기본설정 » ② 인증서/키생성 » ③ 라우팅 설정

Advanced > VPN > OpenVPN Server > Download Certificates/Keys



## Download Certificates and Keys for OpenVPN Clients

No.	EIPR/EIGR Router Clients	
1	AirBox14	<a href="#">Download</a>
2		
3		
4		
5		

No.	PC Clients	
1	toshiba_notebook	<a href="#">Download</a>
2		
3		
4		
5		

클라이언트 인증서와 키가 생성되면 해당 클라이언트 구성 파일에 대한 다운로드 링크가 제공됩니다. 이 파일은 TGZ 압축파일로 제공되고 OpenVPN 서버에 연결하는 데 필요한 모든 구성 정보, 인증서 및 키가 있습니다.

<클라이언트가 EIGR-V, EIPR-V인 경우>

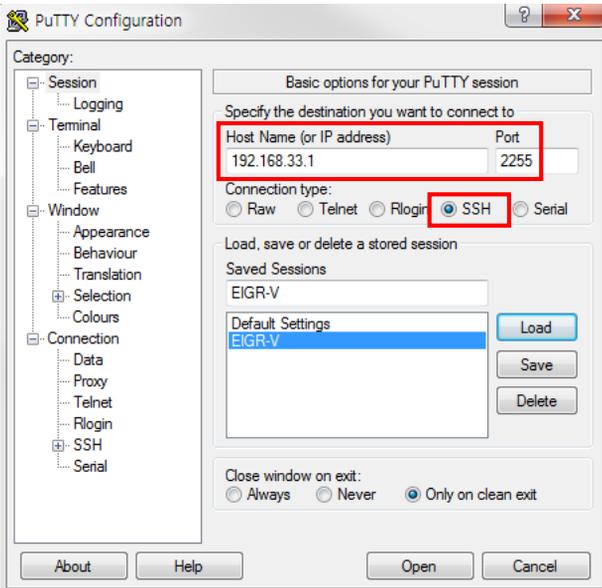
압축파일 그대로 클라이언트 해당 페이지에 업로드 합니다.

<클라이언트가 PC, 랩톱, 태블릿, 스마트폰인 경우>

압축을 풀고 OpenVPN 클라이언트를 실행하는 장치 및 OS에 따라 해당 폴더에 파일을 저장합니다.

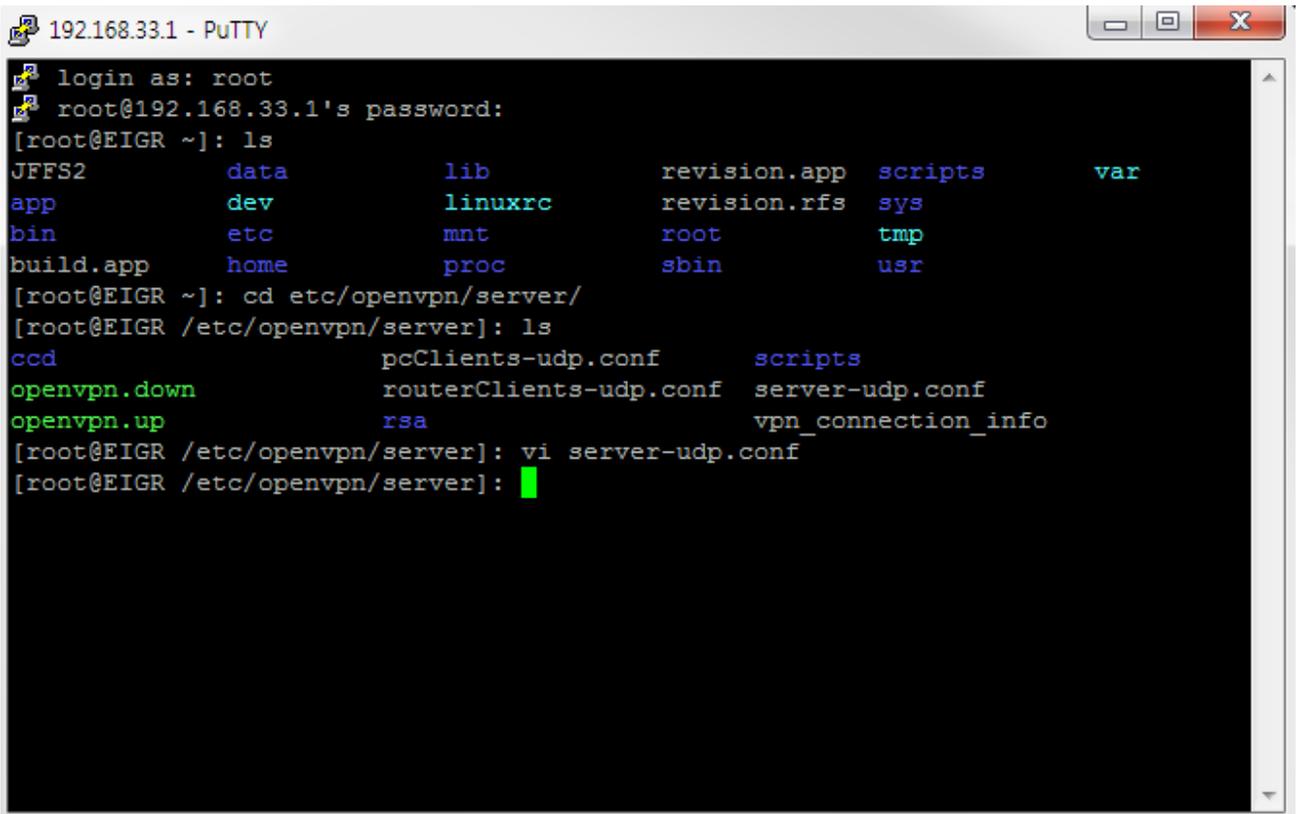
## ① 기본설정 » ② 인증서/키생성 » ③ 라우팅 설정

OpenVPN 클라이언트가 서버(EIGR-V)의 LAN에 연결된 장치와 통신하기 위해 라우팅 설정을 진행합니다. SSH 연결 방식이 가능한 프로그램을 통해 서버의 IP와 지정된 포트번호(2255)로 접속합니다.



OpenVPN 서버 (EIGR-V) IP, Port

SSH 연결



로그인 아이디와 패스워드로 접속합니다. (계정은 와이트리에 문의)  
 cd etc/openvpn/server 명령으로 해당 디렉토리에 접근합니다.  
 vi server-udp.conf 명령으로 서버 환경 파일에 다음과 같이 라우팅 경로를 추가합니다.

참고 : EIGR-V 제품은 VPN 통신 시 UDP 프로토콜로만 통신이 가능합니다.

## ① 기본설정 » ② 인증서/키생성 » ③ 라우팅 설정

vi 에디터로 server-udp.conf 파일을 오픈하였으면, 커서를 맨 아래 행에 위치시키고 다음과 같이 입력합니다.

- a → 입력모드로 전환
- route 192.168.33.0 255.255.255.0 → 지정된 경로 입력
- push "route 192.168.33.0 255.255.255.0"
- 키보드의 ESC 키를 누름 → 입력모드에서 명령모드로 전환
- :wq → 입력한 내용을 저장하고 종료

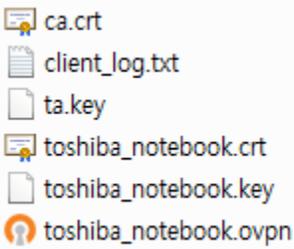
```

server 172.20.0.0 255.255.224.0
port 1194
proto udp
dev tun0
comp-lzo
keepalive 30 120
dh /etc/openvpn/server/rsa/keys/dh1024.pem
ca /etc/openvpn/server/rsa/keys/ca.crt
key /etc/openvpn/server/rsa/keys/EIGR_openVPNserver.key
cert /etc/openvpn/server/rsa/keys/EIGR_openVPNserver.crt
#crl-verify /etc/openvpn/server/rsa/keys/crl.pem
script-security 2
client-config-dir /etc/openvpn/server/ccd
client-connect /etc/openvpn/server/scripts/connect.sh
client-disconnect /etc/openvpn/server/scripts/disconnect.sh
up /etc/openvpn/server/openvpn.up
down /etc/openvpn/server/openvpn.down
tls-auth /etc/openvpn/server/rsa/keys/ta.key 0
client-to-client
route 10.24.0.0 255.255.192.0
route 192.168.33.0 255.255.255.0
push "route 192.168.33.0 255.255.255.0"

[root@EIGR /etc/openvpn/server]: █
    
```

OpenVPN 클라이언트가 설치된 PC에 OpenVPN 서버(EIGR-V)에서 생성한 인증서와 키 파일이 담긴 압축파일을 다운로드 받아 압축을 해제합니다.

No.	PC Clients	
1	toshiba_notebook	<a href="#">Download</a>
2		
3		



ovpn 파일을 실행시켜 VPN 서버와 연결합니다.

**OpenVPN 접속 (toshiba\_notebook)**

현재 상태: 연결됨

```

Fri Apr 10 15:40:32 2020 WARNING: --ns-cert-type is DEPRECATED. Use --remote-cert-tls instead.
Fri Apr 10 15:40:32 2020 TCP/UDP: Preserving recently used remote address: [AF_INET] [redacted]:1194
Fri Apr 10 15:40:32 2020 UDP link local: (not bound)
Fri Apr 10 15:40:32 2020 UDP link remote: [AF_INET] [redacted]:1194
Fri Apr 10 15:40:32 2020 [EIGR_openVPNserver] Peer Connection Initiated with [AF_INET] [redacted]:1194
Fri Apr 10 15:40:34 2020 WARNING: INSECURE cipher with block size less than 128 bit (64 bit). This allows attacks like SWEET
Fri Apr 10 15:40:34 2020 WARNING: INSECURE cipher with block size less than 128 bit (64 bit). This allows attacks like SWEET
Fri Apr 10 15:40:34 2020 WARNING: cipher with small block size in use, reducing reneg-bytes to 64MB to mitigate SWEET32 at
Fri Apr 10 15:40:34 2020 open_tun
Fri Apr 10 15:40:34 2020 TAP-WIN32 device [로컬 영역 연결 3] opened: \\.\\Global\{E25AF66E-F298-4EF5-A4F7-4A501
Fri Apr 10 15:40:34 2020 Notified TAP-Windows driver to set a DHCP IP/netmask of 172.20.0.6/255.255.255.252 on interface {
Fri Apr 10 15:40:34 2020 Successful ARP Flush on interface [21] {E25AF66E-F298-4EF5-A4F7-4A501CA78735}
Fri Apr 10 15:40:39 2020 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prev
Fri Apr 10 15:40:39 2020 Initialization Sequence Completed
        
```

할당된 IP: 172.20.0.6

수신 바이트: 19371 (18.9 KiB) 전송 바이트: 42864 (41.9 KiB)

OpenVPN GUI 11.13.0.0/2.4.7

OpenVPN 서버와 연결되었습니다. 이후 서버와 주고 받는 모든 데이터는 암호화 처리가 되어 데이터를 보호받을 수 있는 안전한 통신망이 구축됩니다.