

# VPN

## PPTP

- [PPTP Server](#)

## PPTP in LAN not working

LAN ????????????? PPTP VPN Server

???OpenWRT ????? PPTP ?????? `kmod-nf-nathelper-extra` ?

```
opkg update
opkg install kmod-nf-nathelper-extra
```

????????????????

## OpenVPN

- [\[OpenWrt Wiki\] OpenVPN](#)
- YT: [OpenWRT - VPN into your Home network using OpenVPN | Roadwarrior - YouTube](#)

## OpenVPN Server

Preparation

```
# Install packages
opkg update
opkg install openvpn-openssl openvpn-easy-rsa luci-app-openvpn luci-i18n-openvpn-zh-tw
```

## Generate PKI (Public Key Infrastructure)

```
# Configuration parameters
cat << EOF > /etc/profile.d/50-openvpn-easy-rsa.sh
export EASYRSA_PKI="/etc/openvpn/pki"
export EASYRSA_TEMP_DIR=${EASYRSA_TEMP_DIR:-${TMPDIR:-/tmp/}}
```

```

export EASYRSA_CERT_EXPIRE="3650"
export EASYRSA_BATCH="1"
EOF
. /etc/profile.d/50-openvpn-easy-rsa.sh

# Remove and re-initialize PKI directory
easyrsa init-pki

# Generate DH parameters
easyrsa gen-dh

# Create a new CA
easyrsa build-ca nopass

# Generate server keys and certificate
easyrsa build-server-full server nopass
openvpn --genkey tls-crypt-v2-server ${EASYRSA_PKI}/server.pem

# Generate client keys and certificate
easyrsa build-client-full client nopass
openvpn --tls-crypt-v2 ${EASYRSA_PKI}/server.pem \
--genkey tls-crypt-v2-client ${EASYRSA_PKI}/client.pem

```

## OpenVPN Service Configuration

1. LuCI UI ? VPN ? OpenVPN ? Delete : custom\_config/sample\_server/sample\_client
2. LuCI UI ? VPN ? OpenVPN ? Add : Template based configuration
  - Name : ovpnServer
  - Template : Server configuration for a routed multi-client VPN
3. LuCI UI ? VPN ? OpenVPN ? Edit : ovpnServer
  - server : 10.9.8.0 255.255.255.0 ( ??? tun ????)
  - ca : /etc/openvpn/pki/ca.crt
  - dh : /etc/openvpn/pki/dh.pem
  - cert : /etc/openvpn/pki/issued/server.crt
  - key : /etc/openvpn/pki/private/server.key
  - port : 1194
  - proto : UDP
  - dev\_type : tun
  - client\_to\_client : check
4. LuCI UI ? VPN ? OpenVPN ? Edit : ovpnServer (**Advanced configuration**)
  1. Cryptography
    - tls\_crypt\_v2 : /etc/openvpn/pki/server.pem
  2. Networking

- persist\_tun : check
- persist\_key : check
- topology : subnet

### 3. VPN

- client\_to\_client : check
- duplicate\_cn : check
- push : route 192.168.8.0 255.255.255.0 (??? LAN ??)
- push : redirect-gateway

## Firewall Configuration

### 1. LuCI UI ? Network ? Firewall ? Traffic Rules ? Add:

- Name : Allow-OpenVPN
- Protocol : UDP
- Source zone : wan/wan6
- Destination zone : Device (input)
- Destination port : 1194
- Action: accept

### 2. LuCI UI ? Network ? Firewall ? General Settings ? Edit: lan ? Advances Settings

- Covered devices : tun0

## Generate client configuration file

```
VPN_CONF="/etc/openvpn/client.ovpn"
VPN_SERV="192.168.0.12"
VPN_PORT="1194"
VPN_PROTO="udp"
VPN_TC="$(cat /etc/openvpn/pki/server.pem)"
VPN_KEY="$(cat /etc/openvpn/pki/private/server.key)"
VPN_CERT="$(openssl x509 -in /etc/openvpn/pki/issued/server.crt)"
VPN_CA="$(openssl x509 -in /etc/openvpn/pki/ca.crt)"
cat << EOF > ${VPN_CONF}
remote ${VPN_SERV} ${VPN_PORT} ${VPN_PROTO}
dev tun
nobind
client
auth-nocache
remote-cert-tls server
<tls-crypt-v2>
${VPN_TC}
</tls-crypt-v2>
<key>
```

```
${VPN_KEY}  
</key>  
<cert>  
${VPN_CERT}  
</cert>  
<ca>  
${VPN_CA}  
</ca>  
EOF
```

# Wireguard

- [\[OpenWrt Wiki\] WireGuard](#)
- YT: [Configuring Wireguard on OpenWRT - Step by Step Guides - YouTube](#)
- YT: [WireGuard - How to Install and Configure WireGuard VPN Client on Ubuntu | Debian | LinuxMint - YouTube](#)

## Preparation

```
opkg update  
opkg install wireguard-tools kmod-wireguard luci-proto-wireguard qrencode  
reboot
```

## Create Wireguard Interface

1. LuCI ? Network ? Interfaces ? Add new interface
  - Name : Wireguard
  - Protocol : Wireguard VPN
2. LuCI ? Network ? Interfaces ? Wireguard ? General Settings
  - Generate new key pair
  - Listen Port : 51820
  - IP Addresses : 10.9.7.1/24
3. LuCI ? Network ? Interfaces ? Wireguard ? Advanced Settings
  1. Use custom DNS servers : 8.8.8.8
4. Save & Apply
5. LuCI ? Network ? Interfaces ? Devices ? Configure: Wireguard
  1. Save
6. Save & Apply

## Configure Firewall

1. LuCI ? Network ? Firewall ? Add zone
  - Name :
  - Input/Output/Forward : Accept
  - Masquerading : check
  - MSS Clamping : check
  - Covered networks : lan/Wireguard
  - Allow forward to destination zones : wan/wan6
  - Allow forward from source zones : lan
  - Save
2. Save & Apply

## Configure Port Forwarding

1. LuCI ? Network ? Firewall ? Port Forwards ? Add
  - Name : Wireguard
  - Restrict to address family : automatic
  - Protocol : TCP/UDP
  - Source zone : wan/wan6
  - External port : 51820
  - Destination zone : lan
  - Internal IP address : 10.9.7.1
  - Internal port : 51820
  - Save
2. Save & Apply

## Configure Peer Settings

1. LuCI ? Network ? Interfaces ? Edit: Wireguard ? Peers ? Add peer
  - Description : My Linux Fedora
  - Generate new key pair
  - Allowed IPs : 10.9.7.2/32
  - Save ? Save
2. Save & Apply
3. LuCI ? Network ? Interfaces ? Wireguard ? Restart
4. LuCI ? Network ? Interfaces ? Edit: Wireguard ? Peers ? Edit: My Linux Fedora ?  
Generate Configuration
  - DNS Servers : 8.8.8.8

---

Revision #56

Created 24 April 2025 13:31:44 by Admin

Updated 4 May 2025 16:44:58 by Admin