

How to Setup OpenVPN on OpenWRT 18.06

Want to configure and install OpenVPN on your OpenWrt device? Just follow this step-by-step guide.

OpenVPN on OpenWRT Router immediately protects your internet privacy and security while giving you full internet freedom and instant access to content streaming. The steps below were tested on OpenWrt 18.06 running set on a Linksys E900 router that has the luci app OpenVPN plugin on-site, so it might not be the same on your firmware:

1 Update and install OpenVPN client package.

Log in as root to the router via SSH using Terminal, or a client of your choice i.e PuTTY

By default, the address is 192.168.1.1 but it might differ from yours. If you do not know the address of your router, consult the router's vendor support.

The default username and password are both set as root but it may differ if you have changed it from your end.

Ensure your package is up to date on your system. Run the command below:

```
opkg update
```

Install OpenVPN client package:

```
opkg install openvpn-openssl luci-app-openvpn
```

Now head to /etc/openvpn/

Create a file called tls-auth.key

```
vi tls-auth.key
```

```
root@OpenWrt:~# cd /etc
root@OpenWrt:/etc# cd \openvpn
root@OpenWrt:/etc/openvpn# vi tls-auth.key
```

Open the Wdc.key file from the Open VPN files folder (you just downloaded), copy and paste its content in the text editor, and save it.

Next, create a file called userpass.txt

```
vi userpass.txt
```

Enter your PureVPN Username and Password on the first line and the second line respectively and save it.

```
Purevpn0sxxxx
```

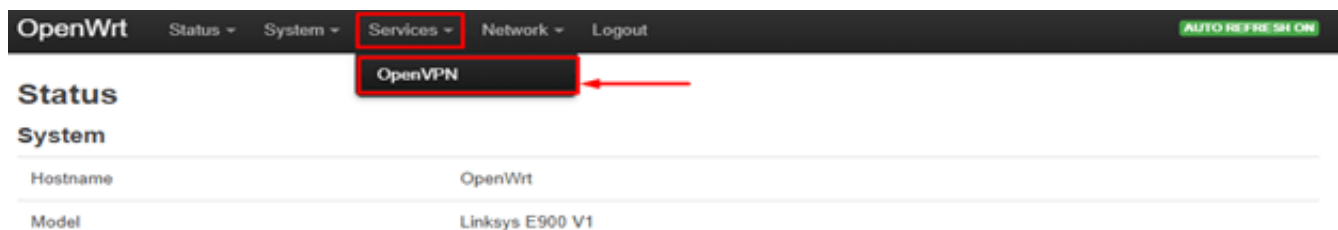
```
VPN Password
```

2 Create OpenVPN configuration.

Login to the router's Luci Web panel from your browser.

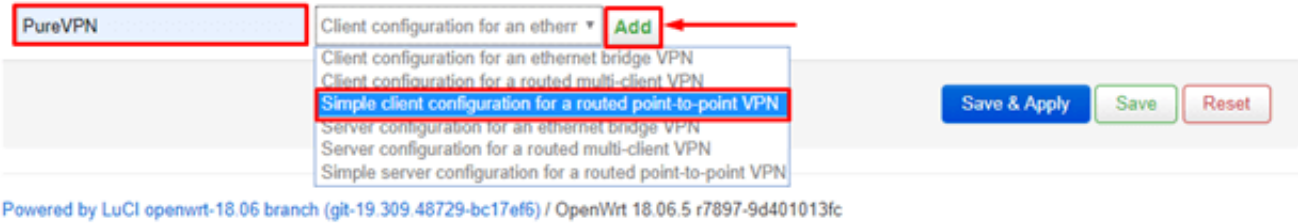


Navigate to **Services > OpenVPN**

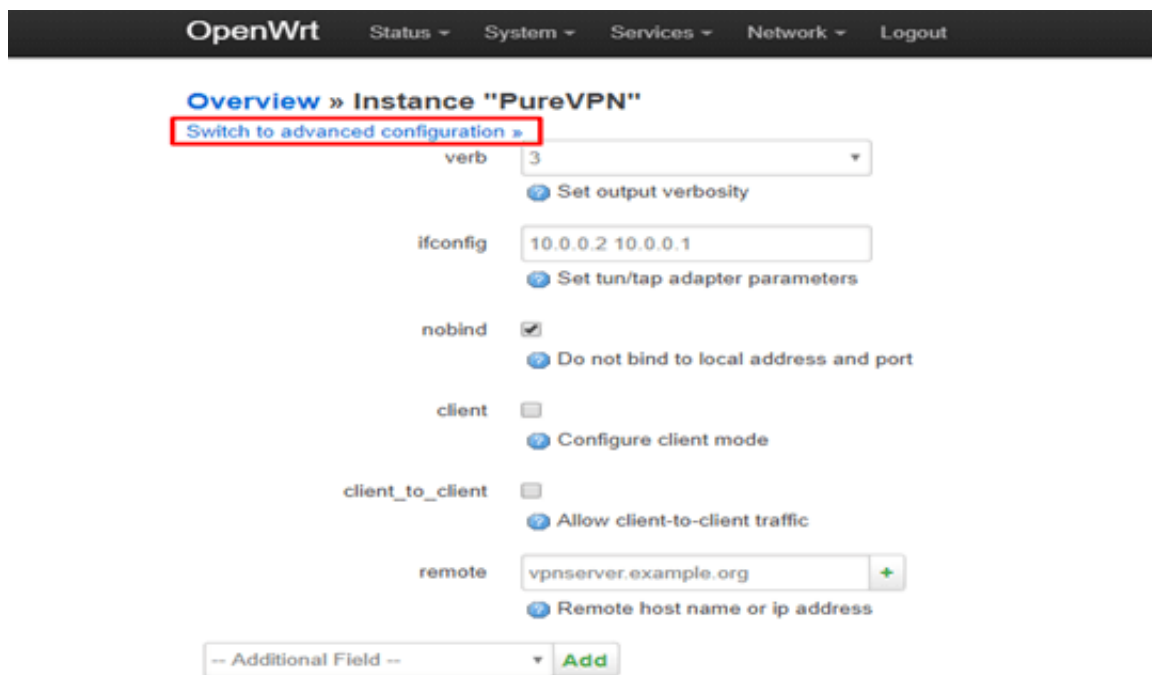


Create a new instance named PureVPN and select the 3rd option from the drop-down: Simple client configuration for a routed point-to-point VPN.

Click Add.

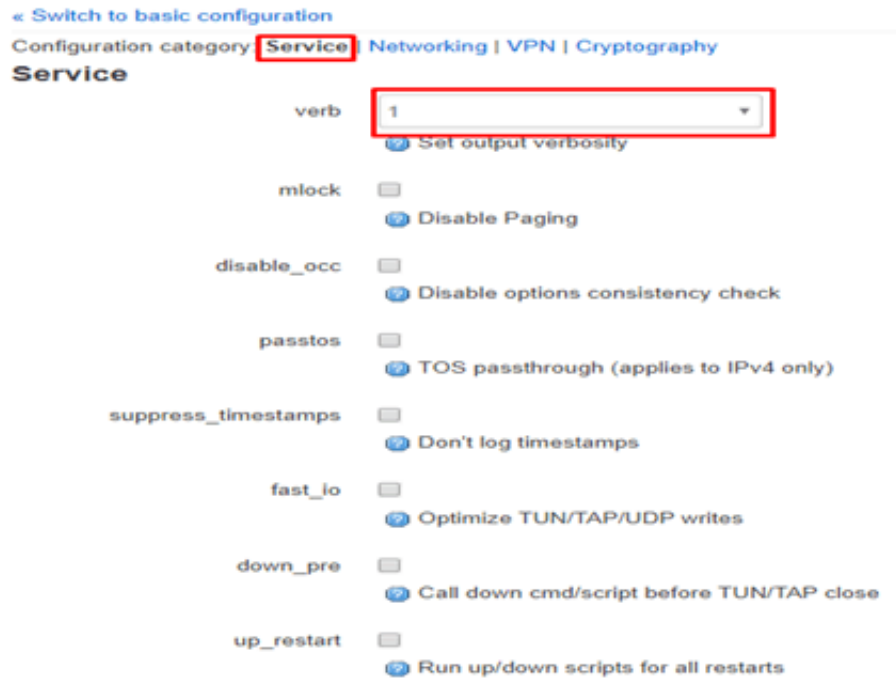


Click on Switch to the advanced configuration at the top right corner of the page to start configuring the OpenVPN connection.



Under the Services tab, just ensure the verb is set to 1

Click Save.



Next, click on the Networking tab

Ensure these details are as below, leave others as it is.

port: 53

nobind: Checked

persist_tun : Checked

Note: If the stated field is not there, scroll down and select it from the Additional Field drop-down and click Add

Click Save.

Networking

port	<input type="text" value="53"/>	? TCP/UDP port # for both local and remote
float	<input type="checkbox"/>	? Allow remote to change its IP or port
nobind	<input checked="" type="checkbox"/>	? Do not bind to local address and port
dev	<input type="text" value="tun"/>	? tun/tap device
ifconfig_noexec	<input type="checkbox"/>	? Don't actually execute ifconfig
ifconfig_nowarn	<input type="checkbox"/>	? Don't warn on ifconfig inconsistencies
route_noexec	<input type="checkbox"/>	? Don't add routes automatically
route_nopull	<input type="checkbox"/>	? Don't pull routes automatically
mtu_test	<input type="checkbox"/>	? Empirically measure MTU
keepalive	<input type="text" value="10 60"/>	? Helper directive to simplify the expression of --ping and --ping-restart in server mode configurations
ping_timer_rem	<input type="checkbox"/>	? Only process ping timeouts if routes exist
persist_tun	<input checked="" type="checkbox"/>	? Keep tun/tap device open on restart

Next, click on the VPN tab.

Ensure these details are as below, leave others as it is.

client : Checked

auth_user_pass: /etc/openvpn/userpass.txt

remote: de2-ovpn-udp.pointtoserver.com

proto: udp

PureVPN Support

Solution of Your Problems

<https://support.purevpn.com>

resolv_retry: infinite

The example above is set to connect to our German server i.e. de2-ovpn-udp.pointtoserver.com. If you wish to connect to another country, please refer to the full list of server names that you can connect by [clicking here](#).

Note: If the stated field is not there, scroll down and select it from the Additional Field drop-down and click Add

Click Save.

VPN

client
Configure client mode

pull
Accept options pushed from server

auth_user_pass /etc/openvpn/userpass.bd
Authenticate using username/password

remote de2-ovpn-udp.pointtoserver.com +
Remote host name or ip address

remote_random
Randomly choose remote server

proto udp
Use protocol

http_proxy_retry
Retry indefinitely on HTTP proxy errors

resolv_retry infinite
If hostname resolve fails, retry

-- Additional Field -- Add

Save & Apply Save Reset

Next, click on the Cryptography tab.

Ensure these details are as below, leave others as it is.

auth: SHA1

cipher: AES-256-CBC

mute_replay_warnings: Checked

PureVPN Support

Solution of Your Problems

<https://support.purevpn.com>

tls_client: Checked

ca: Upload the CA file that you downloaded earlier

tls_auth: /etc/openvpn/tls-auth.key

auth_nocache: Checked

remote_cert_tls: server

key_direction: 1

Note: If the stated field is not there, scroll down and select it from the Additional Field dropdown and click Add

Click on Save & Apply.

Cryptography

auth
[HMAC authentication for packets](#)

cipher
[Encryption cipher for packets](#)

mute_replay_warnings
[Silence the output of replay warnings](#)

tls_client
[Enable TLS and assume client role](#)

ca
[Certificate authority](#)

reneg_sec
[Renegotiate data chan. key after seconds](#)

single_session
[Allow only one session](#)

tls_exit
[Exit on TLS negotiation failure](#)

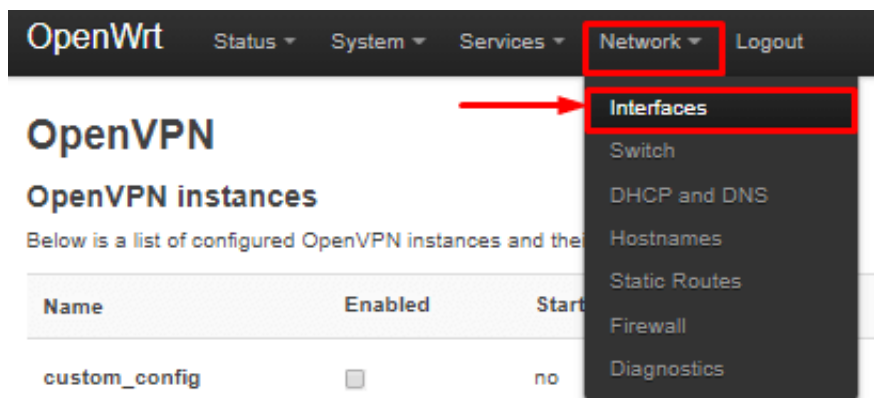
tls_auth
[Additional authentication over TLS](#)

auth_nocache
[Don't cache --askpass or --auth-user-pass passwords](#)

remote_cert_tls
[Require explicit key usage on certificate](#)

3 Create VPN interface.

Navigate to Network > Interfaces



Click on Add New Interface

Interfaces

Interface Overview

Network	Status	Actions
LAN br-lan	Uptime: 0h 17m 18s MAC-Address: C0:56:27:0B:C8:D3 RX: 714.33 KB (3843 Pkts.) TX: 2.50 MB (4306 Pkts.) IPv4: 192.168.1.1/24 IPv6: FD26:5B1A:10BF:0:0:0:0:1/60	Connect Stop Edit Delete
WAN eth0.2	Uptime: 0h 17m 13s MAC-Address: C0:56:27:0B:C8:D3 RX: 2.33 MB (4781 Pkts.) TX: 631.13 KB (2679 Pkts.) IPv4: 192.168.101.56/24	Connect Stop Edit Delete
WAN6 eth0.2	Uptime: 0h 17m 5s MAC-Address: C0:56:27:0B:C8:D3 RX: 2.33 MB (4781 Pkts.) TX: 631.13 KB (2679 Pkts.) IPv4: 192.168.101.56/24	Connect Stop Edit Delete

Add new interface...

Global network options

IPv6 ULA-Prefix

Save & Apply Save Reset

Enter the details as below:

Name of the new interface: PureVPN

The protocol of the new interface: *select* Unmanaged from the drop-down menu

Cover the following interface: Custom Interface – tun0

Create Interface

Name of the new interface
The allowed characters are: A-Z, a-z, 0-9 and _

Note: interface name length
Maximum length of the name is 15 characters including the automatic protocol/bridge prefix (br-, 6in4-, pppoe- etc.)

Protocol of the new interface

Create a bridge over multiple interfaces

Cover the following interface

Click Submit.

4 Set Firewall Rule for VPN connection.

Navigate to Network > Firewall

Click Add.

Firewall - Zone Settings

The firewall creates zones over your network interfaces to control network traffic flow.

General Settings

Enable SYN-flood protection

Drop invalid packets

Input

Output

Forward

Zones

Zone → Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
lan: lan: <input type="text" value="lan"/> → wan: mpavpn	<input type="text" value="accept"/>	<input type="text" value="accept"/>	<input type="text" value="accept"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
wan: wan: <input type="text" value="wan"/> wan6: <input type="text" value="wan6"/> → REJECT	<input type="text" value="reject"/>	<input type="text" value="accept"/>	<input type="text" value="reject"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Configure the firewall as below.

Name: Pure_fw

Input: reject

Output: accept

Forward: reject

Masquerading: Checked

MSS clamping: Checked

Covered networks: Select PureVPN

For Inter-Zone Forwarding:

Select Allow forward from source zones

lan: Checked

wifi: Checked(if you have wifi interface configured)

Once that is done, click on Save & Apply.

General Settings **Advanced Settings**

Name:

Input:

Output:

Forward:

Masquerading:

MSS clamping:

Covered networks:

Inter-Zone Forwarding

The options below control the forwarding policies between this zone (newzone) and other zones. *Destination zones* cover forwarded traffic originating from "newzone". *Source zones* match forwarded traffic from other zones targeted at "newzone". The forwarding rule is *unidirectional*, e.g. a forward from lan to wan does *not* imply a permission to forward from wan to lan as well.

Allow forward to destination zones:

Allow forward from source zones:

5 Connection complete.

Pure VPN is now configured in your OpenWRT router!

Go to Services > OpenVPN, check the box for Enabled next to PureVPN, then click the Start button to initiate the connection.

OpenVPN

OpenVPN instances

Below is a list of configured OpenVPN instances and their current state

Name	Enabled	Started	Start/Stop	Port	Protocol		
custom_config	<input type="checkbox"/>	no	<input type="button" value="start"/>	1194	udp	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
sample_server	<input type="checkbox"/>	no	<input type="button" value="start"/>	1194	udp	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
sample_client	<input type="checkbox"/>	no	<input type="button" value="start"/>	1194	udp	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
Test	<input type="checkbox"/>	no	<input type="button" value="start"/>	53	udp	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
PureVPN	<input checked="" type="checkbox"/>	no	<input type="button" value="start"/>	53	udp	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

Client configuration for an etherr

The connection should be completed within seconds, once connected you can confirm this by checking from the website: www.ipaddress.com

If the VPN connection doesn't start then go to the `/var/etc/client.conf` directory, open the OpenVPN file and remove the line "secret shared-secret.key" save the file, and then recheck to connect.

If you are unable to access the Internet when the VPN is connected, look through the Firewall settings again, and ensure it's set correctly before trying again.

If you are unable to connect to the VPN, navigate to **Status > System Log** and share it with us on your [24/7 support](#).