

# Routers

## DD-WRT

### a) Installing DD-WRT

DD-WRT is an alternative Linux based firmware for many today routers. It has many useful functions including OpenVPN client.

Well supported routers are for example ASUS RT-N66U, ASUS RT-N16, ASUS RT-N18U, TP-LINK TL-WR842ND and others. You can see the full list [here](#). You should look for routers with at least 8MB of Flash memory as you need to use Big or Mega version of DD-WRT to get OpenVPN client running.

You can see compare DD-WRT firmware versions [here](#).

The latest Firmware (beta) can be found at their [FTP](#). All versions are not always available via web.

Please read the [instructions](#) for flashing carefully as improper installation can brick your router.

I have used factory-to-ddwrt.bin on my TP-LINK TL-WR842ND as this image is the first DD-WRT installation.

So we are up and running.

# Routers

dd-wrt.com ... control panel

Firmware: DD-WRT v3.0-r29048 std (02/05/16)  
Time: 19:51:20 up 5:29, load average: 0.01, 0.02, 0.04  
WAN IP: 192.168.0.11

Setup Wireless Services Security Access Restrictions NAT / QoS Administration Status

## System Information

**Router**

Router Name	DD-WRT
Router Model	TP-Link TL-WR842ND v2
LAN MAC	60:E3:27:B5:A2:18
WAN MAC	60:E3:27:B5:A2:18
Wireless MAC	60:E3:27:B5:A2:18
WAN IPv4	192.168.0.11
LAN IP	192.168.1.1

**Services**

WRT-radauth	Disabled
CIFS Automount	Disabled
Sputnik Agent	Disabled
USB Support	Disabled

**Memory**

Total Available	28.6 MB / 32.0 MB
Free	5.6 MB / 28.6 MB
Used	22.9 MB / 28.6 MB
Buffers	2.9 MB / 22.9 MB
Cached	8.5 MB / 22.9 MB
Active	6.6 MB / 22.9 MB
Inactive	6.4 MB / 22.9 MB

**Space Usage**

NVRAM	22.18 KB / 64 KB
CIFS	(Not mounted)
JFFS2	(Not mounted)

**Wireless**

Radio	Radio is On
Mode	AP
Network	Mixed
SSID	dd-wrt
Channel	11 (2462 MHz)
TX Power	16 dBm
Rate	144.444 Mb/s

**Wireless Packet Info**

Received (RX)	0 OK, no error
Transmitted (TX)	15718 OK, no error

## Wireless

**Clients**

MAC Address	Interface	Uptime	TX Rate	RX Rate	Info	Signal	Noise	SNR	Signal Quality
- None -									

## DHCP

**DHCP Clients**

Hostname	IP Address	MAC Address	Client Lease Time
WIN-ESI86DP2EEB	192.168.1.109	xx:xx:xx:xx:03:0D	1 day 00:00:00
Petr-PC	192.168.1.114	xx:xx:xx:xx:4D:AC	1 day 00:00:00

Auto-Refresh is On

DD-WRT  


## b) Using DD-WRT OpenVPN Client

Please follow these instructions for using Identity Cloaker OpenVPN:

- 1) Click the "VPN" tab in the "Services" section, or just scroll down the "Services" page if you are using an old version of DD-WRT.
- 2) Enable the OpenVPN Client.

# Routers

- 3) Set the Server IP/name to SERVER\_NAME.identitycloaker.net \* (Server Names described below the tutorial)
- 4) Set "Port" to 443.
- 5) Set "Tunnel Device" to TUN.
- 6) Set "Tunnel Protocol" to UDP.
- 7) Set "Encryption Cipher" to AES-256
- 8) Set "Hash Algorithm" to SHA1
- 9) Set the option "User Pass Authentication" to Enabled
- 10) Fill up your Identity Cloaker username and password (please see your Welcome mail).

Please note that Identity Cloaker username needs to be entered in lowercase. And it is not your email address. Identity Cloaker password is case sensitive.

- 11) Enable "Advanced Options"
- 12) Set TLS Cipher to "None"
- 13) Enable "LZO Compression" (Yes option)
- 14) Enable "NAT"
- 15) Disable Firewall protection option
- 16) Set Tunnel UDP Fragment to 1450.
- 17) Enable the option Tunnel UDP Fragment
- 18) Keep "nsCertType" unchecked
- 19) In the "Additional Config" copy and paste the following:

```
persist-key
persist-tun
tls-client
```

- 19) Copy and paste the contents of "ca.crt" into the CA cert field.

You can get it from this [package](#) (keys folder)

# Routers

dd-wrt.com ... control panel

Firmware: DD-WRT v3.0-r29048 std (02/05/16)  
Time: 20:23:17 up 6:01, load average: 0.21, 0.13, 0.11  
WAN IP: 192.168.0.11

Setup Wireless Services Security Access Restrictions NAT / QoS Administration Status

Services VPN USB NAS Hotspot

**PTP Server**

PTP Server  Enable  Disable

**PTP Client**

PTP Client Options  Enable  Disable

**OpenVPN Server/Daemon**

OpenVPN Server/Daemon  Enable  Disable

**OpenVPN Client**

OpenVPN Client

Start OpenVPN Client  Enable  Disable

Server IP Name: uk14.identitycloaker.net

Port: 443 (Default: 1194)

Tunnel Device: TUN

Tunnel Protocol: UDP

Encryption Cipher: AES-256 CBC

Hash Algorithm: SHA1

User Pass Authentication  Enable  Disable

Username: your\_idc\_username

Password: your\_idc\_password

Advanced Options  Enable  Disable

TLS Cipher: None

LZO Compression: Yes

NAT  Enable  Disable

Firewall Protection  Enable  Disable

IP Address:

Subnet Mask:

Tunnel MTU setting: 1500 (Default: 1500)

Tunnel UDP Fragment: 1450 (Default: Disable)

Tunnel UDP MSS-Fix  Enable  Disable

nsCertType verification:

TLS Auth Key:

Additional Config:

```
persist-key
persist-tun
tls-client
```

Policy based Routing:

PKCS12 Key:

Static Key:

CA Cert:

```
-----BEGIN CERTIFICATE-----
MIExzCCA6+gAwIBAgIDANdhb4gPTq/MA0GCSqGSIb3DQEBBQUAMIGdMQswCQYD
VQQGEwJDWjEXMBUGA1UECBMOQ3pY2ggUmVwdWJsaWMxDzANBgNVBAcTBIBYYWd1
```

Public Client Cert:

Private Client Key:

Save Apply Settings Cancel Changes

Page 4 / 6

(c) 2026 TFR Technology s.r.o <munzarp@gmail.com> | 2026-01-14 12:58

URL: http://kb.identitycloaker.net/faq/content/11/15/en/dd\_wrt.html

# Routers

20) Click the "**Apply settings**" button and check VPN status at **Status menu -> OpenVPN** . You should see **Connected** notice there.

# Routers

You can test your IP address [here](#).

**Your IP address is:**

**78.129.183.80**

**Your Real IP address is cloaked with Identity Cloaker**

\*Available servers (enter instead of the SERVER\_NAME in step 5):

AU2, AT1, CA2, CZ1, FR5, DE3, IE4, IT2, NL2, NO1, PL1, PT1, RU1, SG1, SP1, SE2, CH1, UK4, UK9, UK12, UK13, UK14, US4, US7

Updated version of our servers list can be found at your [member area](#).

Unique solution ID: #1014

Author: Petr Munzar

Last update: 2017-08-01 12:33