

OpenVPN server and client on DD-WRT -- Bridged

Contributed by Kevan

SCENARIO:

We wanted to connect two small business offices with a VPN. Our existing firewalls were Linksys WRT54Gs. We chose to run the DD-WRT VPN firmware and utilize OpenVPN to help resolve our need. (These instructions should also work on the DD-WRT support models like the Allnet ALL0277, Buffalo WHR-G54S, Buffalo WHR-HP-G54S, ASUS WL500G-Deluxe, Motorola WR850G, Siemens Gigaset SE505, Ravo W54-R, and Askey RT210W.) This guide offers a guide to setting up a bridged VPN setup.

SCENARIO:

We wanted to connect two small business offices with a VPN. Our existing firewalls were Linksys WRT54Gs. We chose to run the DD-WRT VPN firmware and utilize OpenVPN to help resolve our need. (These instructions should also work on the DD-WRT support models like the Allnet ALL0277, Buffalo WHR-G54S, Buffalo WHR-HP-G54S, ASUS WL500G-Deluxe, Motorola WR850G, Siemens Gigaset SE505, Ravo W54-R, and Askey RT210W.)

OpenVPN can be run in two modes: routed and bridged. The steps below set up a bridged VPN where both sites are on the same subnet. If you are looking for routed VPN instructions click here. One of the WRTs should be the VPN server and the other should be the VPN client. This senerio works well when one site has a static internet IP address and a valid DNS entry while the other site is setup with DHCP. If both sites are setup with DHCP internet addresses, the server VPN should have a Dynamic DNS entry at a provider like www.dyndns.com. DynDNS.com is a free service and there is a client built into DD-WRT.

These instructions are written assuming that you will configure the VPN server WRT first and the client WRT second.

STEPS:

1) Install the v.23 SP1 dd-wrt VPN final or beta version of firmware available [HERE](#) -- Instructions for installing DD-WRT are available [HERE](#) MAKE SURE YOU USE A VERSION DATED BEFORE 6/15/06! Versions after 6/15/06 do not support brctl for bridging.

2) Logon to the web management interface in DD-WRT. Select the Administration tab. Scoll down until you find the JFFS2 Support information. JFFS2 must be enabled. If you have never enabed JFFS2 before you will also need to select the Clean JFFS2 enable button to initialize the file system. Scroll to the bottom and select Save Settings.

3) Select the Administration tab and then the Services subtab. Scroll down to the OpenVPN client section and make sure that Start OpenVPN is set to Disable. If you had to disable it, make sure you scroll to the bottom and click Save Settings. You have to leave this disable because the configuration in DD-WRT is design to act as a client to a vPN server running on a full-blown linux or other host.

4) Telnet to your router and enter the username of root and your administrative password.

5a) If this is your second WRT (the VPN client DD-WRT) skip to step 5b. If this is the VPN server WRT type in `openvpn --genkey --secret /jffs/static.key` and hit `<enter>`. This will generate the static key we will use for our VPN. (Once the command is complete the WRT will return to the bash prompt. Now type `cat /jffs/static.key` and hit `<enter>`. Copy and paste the output into notepad or wordpad. You will need the key information for the next router. Now you can skip to step 6.

Below is a static key example. DO NOT USE THIS KEY YOUR VPN WILL NOT BE SECURE.## 2048 bit OpenVPN

static key#-----BEGIN OpenVPN Static key V1-----

```
2754944c2f86e3d3d7a834f1f87290c7
373d292c8aba802c2dc9536a60ec33c7
be283c5fe97a26e121864d78504a642c
37cabb7f24d39037b3172ed0a5f9e25c
1e4a48fecc040c74194b113d9c6c8395
720c5cc540427fd2cb5c6789d3c398a4
a9a28a1657812bb3e9b69613f7d6d72a
```

```

109e57aa274336989e3cdb651be058ed
3ad66761840b971ac00c19e748146ea3
47e44d9ccb5eda0542eda75641ab45d7
8dd0c703ce9daae43a75998b84145c68
fe3826b5855b0098d96e6c7db57add52
aecfd1720e86e0db981946b93ff3b8ef
60fd1efca7c81553fa16ebac6e7abbcc
fcb63ed412631cec55fa7c24918841e8
3e3c9736724be10b8b6721caf8630d44
-----END OpenVPN Static key V1-----

```

5b) At the prompt type `vi /jffs/static.key` and hit `<enter>`. Hit `i` to enter insert mode and then paste in the static key information you copied into notepad when working on your VPN server WRT. After you are done pasting, hit escape and then type `:wq` and hit `<enter>`

6) At the prompt type `chmod 700 /jffs/static.key` and hit `<enter>`

7a) If you are working on the VPN client WRT skip to step 7b. On the VPN server WRT copy the following script and paste on the command line. (Check the script for comments on the few items that need to be updated to match your environment.)

----- Copy starting below this line. -----

```

nvram set rc_firewall='

#!/bin/sh

##

##

##

#copy openvpn binary to myvpn. Otherwise, something will kill the process
cp /usr/sbin/openvpn /tmp/myvpn

/tmp/myvpn --mktun --dev tap0

brctl addif br0 tap0
ifconfig tap0 0.0.0.0 promisc up

/tmp/myvpn --dev tap0 --secret /jffs/static.key --comp-lzo --port 1194 --proto udp --verb 3 --daemon --ping 30 --ping-
restart 120
'

```

----- Stop here when selecting text to copy -----

7b) On the VPN client WRT copy the following script and paste on the command line. (Check the script for comments on the few items that need to be updated to match your environment.)

----- Copy starting below this line. -----

```
nvramp set rc_firewall='
```

```
#!/bin/sh
```

```
##
```

```
##
```

```
##
```

```
#copy openvpn binary to myvpn. Otherwise, something will kill the process  
cp /usr/sbin/openvpn /tmp/myvpn
```

```
/tmp/myvpn --mktun --dev tap0brctl addif br0 tap0  
ifconfig tap0 0.0.0.0 promisc up
```

```
/tmp/myvpn --dev tap0 --secret /jffs/static.key --comp-lzo --port 1194 --proto udp --verb 3 --daemon --remote  
VPNSERVER.dnsalias.com --ping 30 --ping-restart 120
```

```
,
```

----- Stop here when selecting text to copy -----

8) Type `nvramp commit` and hit `<enter>`

9) Now reboot you routers and attempt to ping hosts accross the VPN tunnel. (You will not be able to ping the WRTs addresses. You have to ping a host on the network other than the WRT.).

10) Remember that both sites need the same internal IP subnets.

That should be it and good luck!