Contents

Router to Router Bridged Configuration Alternative (Hardware VPN)

(for hardware "like" vpn access for multiple computers or appliances)

This is a quick and dirty guide to creating a VPN between (2) DD-WRT v24 SP2 routers (both flashed with VPN version).

This will allow for hardware like VPN access on the client side to more than one client, device, and or appliance that does NOT have built in VPN capabilities, but has either wireless and/or DHCP capabilities.

Examples Include:

- Internet Video box that is service and region limited
- Region limited gaming console.
- You can in theory use a video device or gaming console outside of the US, while still using US services. So long as the DD-WRT server is in the US.
- ISPs that limit service to their IP ranges.
- Devices that don't have native VPN clients such as: A Tablet or PDA device that you want to use in a coffee shop and back to your home or business.

When setup correctly, all traffic is routed and encrypted over the VPN. The DHCP lease is provided by the remote DD-WRT server. All clients will share the WAN IP of the server (NAT).

- you can route specific traffic to the local DD-WRT router or PC, but that is outside the scope of this guide (via route command and changing the default gateway via manual IP assignments)

Assumptions:

1. Local router's WAN port will be connected to a network with internet access (either directly with a real IP address or a NAT/reserved address... this setup works with double NAT). This guide assumes you are getting a WAN address of 192.168.1.10
2. Remote router IP address is 10.19.77.1 (50 clients MAX, start IP 10.19.77.2). Has functional internet service :)
3. Local router IP address is 10.19.77.77 (dhcp is off!!!!)
4. This is operating in bridged mode and is less efficient than routed mode when dealing with network broadcasts and other traffic.
5. Port 8080 will be used in this example, change this if you like.
6. An item in red is something you can OR should change

- you can setup the local DD-WRT router to use a proxy or socks server, but that is outside the scope of this guide.

- you can setup the remote DD-WRT router to be behind a firewall/proxy/nat and/or act as a switch/access point (NAT OFF) and get DHCP leases for local devices from ANOTHER remote DHCP server, but that it outside the scope of this guide.

The Quick and Dirty:

1. Turn off dhcp on local router.
2. Change the local lan ip to something beyond dhcp lease of remote dhcp server. Ex. 10.19.77.77
3. Timezones and ntp time set the same on both local and remote router.

I suggest using a remote server with something outside the range of the WAN side of the local router. Ex. If you're local router's WAN ip is 192.168.1.10, don't use 192.168.1.x as the remote server's LAN range.

I HIGHLY suggest using certificates and NOT a static key (please look elsewhere for assistance on this). The static key was omitted for security reasons, USE YOUR OWN when testing. Switch to certificates when done.

The remote server's host and domain have been altered. Use your own here!

I suggest using UDP and not TCP (use "--proto udp" on both remote and local routers configuration scripts). TCP will help when using socks or HTTP proxies since they generally only allow TCP. Some ISPs throttle UDP traffic, but not TCP. There is a performance penalty when using TCP however in congested or slow connections. I suggest using dynamic DNS on remote DD-WRT router. Look elsewhere for information on this.

Remote Router Scripts:

Firewall Script:

```
iptables -I INPUT 1 -p tcp --dport 8080 -j ACCEPT
```

- (will need to change to udp IF you intend to use udp and NOT tcp)

Startup Script:

```
openvpn --mktun --dev tap0
brctl addif br0 tap0
ifconfig tap0 0.0.0.0 promisc up
echo "
-----BEGIN OpenVPN Static key V1-----

ATTN get your own static key!

-----END OpenVPN Static key V1-----
" > /tmp/static.key
ln -s /usr/sbin/openvpn /tmp/myvpn
/tmp/myvpn --dev tap0 --secret /tmp/static.key --comp-lzo --port 8080 --proto tcp-server --keepal
```

- (use "udp" instead of "tcp-server if you intend to use udp)

Local Router Scripts:

Firewall Script:

- nothing to enter here :)

Startup Script:

```
cd /tmp
ln -s /usr/sbin/openvpn /tmp/myvpn
./myvpn --mktun --dev tap0
brctl addif br0 tap0
ifconfig tap0 0.0.0.0 promisc up
sleep 5

echo "
-----BEGIN OpenVPN Static key V1-----

ATTN get your own static key!

-----END OpenVPN Static key V1-----
" > /tmp/static.key

chmod 600 /tmp/static.key

ln -s /usr/sbin/openvpn /tmp/myvpn
/tmp/myvpn --secret static.key --dev tap0 --remote MYHOST.DYNAMICdns.xxx --proto tcp-client --por
```

- (use "udp" instead of "tcp-client if you intend to use udp)

I had problems with the other scripts in this entire wiki which cover OpenVPN setups. You will notice that my above scripts don't have the use of the .conf file. I was not able to get those to work. So I did it the old script way, which has since been removed from this wiki (and now re-entered by me). --S19303cc 20:29, 16 January 2011 (CET)