

OpenWRT's OpenVPN

Client setup

replace DNS from VPN server connection

```
script-security 2
up /etc/openvpn/client.sh
down /etc/openvpn/client.sh
```

```
#!/bin/sh
env | sed -n -e "
/^foreign_option_.*=dhcp-option.*DNS/s//nameserver/p
/^foreign_option_.*=dhcp-option.*DOMAIN/s//search/p
" | sort -u > /tmp/resolv.conf.vpn
case ${script_type} in
(up) uci set dhcp.@dnsmasq[0].resolvfile="/tmp/resolv.conf.vpn" ;;
(down) uci set dhcp.@dnsmasq[0].resolvfile="/tmp/resolv.conf.auto" ;;
esac
/etc/init.d/dnsmasq restart &
```

```
chmod +x /etc/openvpn/client.sh
```

NOTE: In case of VPN failure, default DNS server will be set to server behind VPN which is unreachable. If VPN client is set to connect to domain names, it will also fail. Either set VPN client to use remote IP addressess or add some remote VPN domains to `/etc/hosts` file.

Server setup

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

Enable incoming OpenVPN connections:

```
uci add firewall rule
uci set firewall.@rule[-1]._name=openvpn
uci set firewall.@rule[-1].src=wan
uci set firewall.@rule[-1].target=ACCEPT
uci set firewall.@rule[-1].proto=udp
uci set firewall.@rule[-1].dest_port=1194
uci commit firewall

echo "iptables -I OUTPUT -o tap+ -j ACCEPT" >> /etc/firewall.user
echo "iptables -I INPUT -i tap+ -j ACCEPT" >> /etc/firewall.user
echo "iptables -I FORWARD -o tap+ -j ACCEPT" >> /etc/firewall.user
echo "iptables -I FORWARD -i tap+ -j ACCEPT" >> /etc/firewall.user
```

```
mkdir -o /etc/openvpn
uci set openvpn.uservpn=openvpn
uci set openvpn.uservpn.config=/etc/openvpn/user-vpn.conf
uci set openvpn.uservpn.enable=1
uci commit openvpn
```

cat > /etc/openvpn/user-vpn.conf

```
port 1194
proto udp
dev tap0
keepalive 10 120
status /tmp/openvpn-status.log
verb 3
secret /etc/openvpn/secret.key
```

Add VPN to local LAN bridge:

```
cat > /etc/init.d/openvpn-bridge
#!/bin/sh /etc/rc.common

START=94

start() {
    openvpn --mktun --dev tap0
    brctl addif br-lan tap0
    ifconfig tap0 0.0.0.0 promisc up
}

stop() {
    ifconfig tap0 0.0.0.0 down
    brctl delif br-lan tap0
    openvpn --rmtun --dev tap0
}

chmod 755 /etc/init.d/openvpn-bridge
/etc/init.d/openvpn-bridge enable
/etc/init.d/openvpn-bridge start
```

```
openvpn --genkey --secret /etc/openvpn/secret.key
```

Start VPN:

```
/etc/init.d/openvpn enable
/etc/init.d/openvpn start
```

From:

<https://niziak.spox.org/wiki/> - **niziak.spox.org**

Permanent link:

<https://niziak.spox.org/wiki/linux:openwrt:openvpn>

Last update: **2021/03/05 14:13**

