Configuration of Linksys Routers as IPSec Wireless VPN endpoints

Configuration of Linksys Routers as IPSec Wireless VPN endpoints

A lot of attention has been paid to the implementation of remote working environments for the home and providing connectivity solutions to remote locations. Consumer Linksys routers make an ideal platform to extend your organisational network to a remote location, even providing a central wireless SSID for users.

This set of instructions will demonstrate the configuration of the Linksys router (Linksys WRT54G) with OpenWRT as a hardware IPSec endpoint.

1. The first step is to replace the default image with the latest OpenWRT ‘kamikaze’ release. Firstly, download the latest release, e.g. openwrt-wrt54g-2.4-squashfs.bin, from the main OpenWRT site: http://openwrt.org/ [1]

2. The OpenWRT firmware can be installed onto the router directly using the GUI provided. This can be accessed by navigating to:

```
http://192.168.1.1
```

and selecting Administration -> Firmware Upgrade

OR

```
http://192.168.1.1/Upgrade.asp
```

The default Username and Password combination is admin/admin.

3. Upload the openwrt-wrt54g-2.4-squashfs.bin firmware and wait approximately two minute while the router reboots itself and the upgrade is completed.

4. Once this stage has been completed OpenWRT has been installed and one can connect to the router using the IP address 192.168.1.1

telnet 192.168.1.1

Note: The reason for using the 2.4 kernel release is due to the Open Source Broadcomm driver not yet being available for the 2.6 kernel. Once this has been ported, the 2.6 kernel

can be used for better performance and associated enhancements.

5. At this point the OpenWRT firmware can be upgraded or downgraded:

cd /tmp

wget http://downloads.openwrt.org/kamikaze/7.09/brcm-2.4/openwrt-brcm-2.4-squ... [2]

mtd write /tmp/openwrt-brcm-2.4-squashfs.trx linux && reboot

6. At this point the traditional Linksys web GUI will be unavailable and for connectivity, for the moment, one has to use the telnet interface. The first task is to configure a password to set root's password and disable telnet/enable SSH.

passwd

7. After setting the password, the latest list of OpenWRT packages needs to be downloaded.

ipkg update

ipkg upgrade

8. Once the list of packages has been downloaded and updates, the packages related to the VPN instance need to be downloaded and installed. This can be replicated across a large number of devices later by copying the configuration tarball using SCP.ipkg install vpnc

ipkg install nas

ipkg install wl

9. To enable the wireless interface enter the following:

uci set wireless.wl0.disabled=0

uci commit wireless && wifi

10. Configure the wireless networking by editing /etc/config/wireless and adding/editing the following options:

config wifi-device wl0

option type Broadcom

option channel 1

config wifi-iface

option device wl0

option network lan

option ssid **<Insert SSID to advertise>**

option mode ap

option encryption wpa

option key **<Insert Shared Secret>**

option server **<Insert IP Address of RADIUS Server>**

option port 1812

11. Configure the VPN connection by editing /etc/vpnc/vpnc.conf and adding/editing the following options:

IPSec <Insert IP Address of VPN Concentrator>

IPSec ID WRTRemoteWorker

IPSec secret <Insert secret/password for the above ID>

Xauth username <Linksys username>

Xauth password <Linksys password>

12. Configure the VPN startup processes by creating /etc/init.d/vpnc and adding/editing the following options:

#!/bin/sh /etc/rc.common

START=75

STOP=10

start() {

mkdir -p -m777 /var/run/vpnc

vpnc /etc/vpnc/vpnc.conf

}

stop() {

PID_F=/var/run/vpnc/pid

if [-f $PID_F]; then

PID=$(cat $PID_F)

kill $PID

while [-d /proc/$PID];

```
do
sleep 1
done
fi
}
```

13 Create a softlink to the new script:

```
cd /etc/rc.d
ln -s /etc/init.d/vpnc S75vpnc
```

14. To configure the Cisco LED so that it glows bright white when the VPN connection is established, edit the file /etc/vpnc/vpnc-script. Go to the endof the file and then back up to the start of “if [-z "$reason"]; then” and insert before the if statement the following:

```
# Cisco LED
vpn_led_pending() {
echo "f" >/proc/diag/led/ses_orange
echo "f" >/proc/diag/led/ses_white
}
vpn_led_connected() {
echo "0" >/proc/diag/led/ses_orange
echo "1" >/proc/diag/led/ses_white
}
vpn_led_disconnected() {
echo "0" >/proc/diag/led/ses_orange
echo "0" >/proc/diag/led/ses_white
}
```

15. Then in the same file, edit case “$reason”:

```
case "$reason" in
pre-init)
```

```
do_pre_init

vpn_led_pending

;;

connect)

do_connect

start_vpn_nat

vpn_led_connected

;;

disconnect)

stop_vpn_nat

do_disconnect

vpn_led_disconnected

;;

*)

echo "unknown reason '$reason'. Maybe vpnc-script is out of date" 1>&2

exit 1

;;

esac
```

16. With the router configured a reboot will start broadcasting the configured SSID and connectivity will be established with the home organisation.

Links
[1] http://openwrt.org/
[2] http://downloads.openwrt.org/kamikaze/7.09/brcm-2.4/openwrt-brcm-2.4-squashfs.trx