How to Make Asus RT-N15U Wireless Router (Tomato by Shibby Fimware) Mirror Traffic to Snort

Written by: Teo En Ming
Email: teo.en.ming@gmail.com

Date: 7 April 2014 6:04 P.M. SGT
Version: 1.0

The latest dd-wrt v24-SP2 and OpenWRT 12.09 firmwares (all based on the Linux Kernel 3.x) do not support port mirroring any more.

I tried port mirroring with dd-wrt v24-SP2 firmwares (from the year 2011 to 2014) on Buffalo WZR-HP-G300NH2 wireless router but failed.

I tried port mirroring with OpenWRT attitude adjustment 12.09 firmware on Buffalo WZR-HP-G300NH2 wireless router but failed.

I tried port mirroring with Tomato by Shibby firmware on Asus RT-N15U wireless router successfully.

Instructions:

1. Put your Asus RT-N15U wireless router in RESCUE mode. Unplug the power cord to your router. Press and hold down on the RESET button on the back panel of your router. Plug back the power cord to your router. Wait for the POWER LED to blink. Release the RESET button.

2. Put the Asus RT-N15U wireless router support CD in your CD-ROM/DVD/Blu-ray drive. Click on “Install ASUS Wireless Router Utilities”. Click on Start > All Programs > ASUS Utility > RT-N15U Wireless Router > Firmware Restoration to launch the Firmware Restoration Utility.

3. Download the latest Tomato by Shibby version 116 firmware from the following URL: http://tomato.groov.pl/download/K26RT-N/build5x-116-EN/Asus%20RT-Nxx/tomato-K26USB-1.28.RT-N5x-MIPSR2-116-Big-VPN.trx

4. In the Firmware Restoration Utility, click on “Browse” to select the firmware file tomato-K26USB-1.28.RT-N5x-MIPSR2-116-Big-VPN.trx you have just downloaded. Click on “Upload” and wait for the firmware uploading and flashing to complete. Click on “Close”.

5. Put your Asus RT-N15U wireless router into RESCUE mode again (see point 1). Open your web browser and browse to http://192.168.1.1 Click on “Clear NVRAM”. Then click on “Reboot” to reboot your router. Wait for the router to finish rebooting. The lowest 3 LED lights on your router will light up.

6. Browse to http://192.168.1.1 and start configuring your router. Remember to save your changes.

7. Open a SSH connection to your Asus RT-N15U wireless router using the Putty client. I assume you have already downloaded the Putty client. Use the IP address of 192.168.1.1 and Port 22. The username is "root" and the password is "admin".

8. On the Linux root prompt on your Asus RT-N15U router, execute the following command:

   # modprobe ipt_ROUTE

   to load the ipt_ROUTE kernel module. A Linux kernel module is also known as a driver in Windows speak.

9. Execute the following 2 commands to enable port mirroring.

   # iptables -A PREROUTING -t mangle -j ROUTE --gw 192.168.1.40 –tee

   # iptables -A POSTROUTING -t mangle -j ROUTE --gw 192.168.1.40 –tee

   where # is the Linux root prompt on your router. Assume your Snort network intrusion detection system (IDS) is installed on a box (physical or virtual) with the IP address 192.168.1.40.

10. To make sure you have successfully added the 2 port mirroring commands, execute the following command on your Linux root prompt on the router:

    # iptables -t mangle -L

    You should see something like the following:

```
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
ROUTE      all  --  anywhere             anywhere            ROUTE gw:192.168.1.40 tee

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
ROUTE      all  --  anywhere             anywhere            ROUTE gw:192.168.1.40 tee
```

11. The installation of Snort IDS is not covered in this manual. Please refer to http://www.snort.org/docs for the Snort IDS installation manuals written by William/Bill Parker.