How to make a Consumer Grade Router (also known as a Home or Small Office Router) mirror (copy) network traffic to a SNORT sensor running on a standalone system or to a virtual machine running in VirtualBox, VMWare, or Xen.

This document last revised on July 31, 2013.

The information below describes how the owner of a Consumer Grade Router (i.e. - Linksys, D-Link, NetGear, Buffalo, etc) can utilize it to mirror (copy) network traffic to a standalone or virtual machine which is running a SNORT sensor. A router which has any of the firmware options listed below can be used to mirror (copy) network traffic:

DD-WRT http://www.dd-wrt.com

OpenWRT http://www.openwrt.org

Tomato http://www.polarcloud.com/tomato

The environment I am using to do this is as follows:

Microsoft Windows 7 Ultimate Edition w/SP1 as the HOST operating system
VirtualBox 4.2.x/4.1.x with Oracle Extension Pack 4.2.x/4.1.x (I use version 4.2.16)
OpenSuSE 12.x (32 or 64 bit) as the GUEST operating system (which runs SNORT)
Buffalo WHR-G54S wireless router with DD-WRT v2.4 SP2 firmware (Build 14929)
SNORT 2.9.5.x or 2.9.4.x, DAQ 2.0.x, and a set of snort rules (www.snort.org)

The document below uses the following color codes for things the user should be aware of during configuration of DD-WRT/OpenWRT/Tomato for mirroring network traffic:

Blue - informational messages and comments
Violet - additional features the above firmware provides
Orange - These are commands that the user types at the shell prompt
Red - **Read carefully before proceeding**.

Note - This document is **NOT INTENDED** to show a user how to install or change the firmware in an existing router to use DD-WRT, OpenWRT, or Tomato firmware.

Instructions on how change or upgrade the firmware in an existing router can be found at the above websites, but there is **always a possibility** that you **may render your router inoperable** (aka **BRICKED**). Use **EXTREME CAUTION** if your intention is to replace the firmware in your existing router with DD-WRT, OpenWRT, or Tomato firmware.

Also, some of the above router manufacturers sell consumer grade routers with one of the firmware options listed above pre-installed from the factory.

Other services the above mentioned firmware may provide are **VPN**, **LAN port aggregation**, **ToS/QoS**, **MAC Address Cloning**, **VLAN support**, **IP Tunneling**, improved **security** and **access controls**, **remote system logging**, bandwidth graphing and usage, **wireless hotspot**, **Telnet/Secure Shell** command line access, **GUI based** router management, the ability to **increase wireless transmitting power**, and so forth.

Additional ways to mirror traffic is to use a high end switch (Cisco/HP/Juniper) which is equipped with one or more SPAN/Mirror ports, in which a snort sensor is attached to, or by the use of a network hub (these are usually 10/100 Megabit/sec based devices, but can still be found via an internet search, etc).

This document assumes you already have SNORT configured, tested, and running and that it is monitoring network traffic on 'eth0/em0/wm0' (ethernet 0).

This is where we get your home router (if it is running DD-WRT, OpenWRT, or Tomato firmware) to actually mirror packets to the IP address you assigned to 'eth0/em0/wm0' in your Linux or Unix system (I gave my box a static IP address of 192.168.1.40), the gateway IP address of my router is 192.168.1.1, and the actual IP address of my Host OS (Windows 7) is 192.168.1.10.

Note: for users of **Tomato** firmware, some of them have reported that you may have to add the following command (for certain firmware build numbers in Tomato**)**:

modprobe ipt ROUTE

To the startup script in Tomato to enable the use of 'iptables mangle' with the --tee option.

Additionally, for users of **OpenWRT** (current release is 10.03.1) you must use the TEE option for IPtables (provided by module iptables-mod-tee) in order to mirror traffic to a specific IP or network. The module 'iptables-mod-tee' must be loaded/enabled before the command below will work:

iptables -t mangle -A PREROUTING -j TEE --gateway x.x.x.x

Where x.x.x.x is an IP address you wish to mirror traffic to (usually a system running a Snort sensor).

Also, in the latest version of OpenWRT (10.03.1), it appears that the iptables-mod-tee module is NOT enabled by default, which will require a rebuild/re-enabling of modules for OpenWRT. To accomplish this, visit the following URL:

https://lists.openwrt.org/pipermail/openwrt-users/2012-January/001936.html

For additional information on the iptables-mod-tee module for OpenWRT 10.03.1

Special thanks to Sandor Borcsok (s.borcsok at gmail dot com) for providing the OpenWRT information listed above.

Use the DD-WRT or Tomato GUI (or SSH/Telnet into the router running DD-WRT/Tomato) and issue the commands below:

iptables -A PREROUTING -t mangle -j ROUTE --gw 192.168.1.40 --tee <enter>
iptables -A POSTROUTING -t mangle -j ROUTE --gw 192.168.1.40 --tee <enter>

The above commands will make a copy of all of the traffic entering and leaving your network to the gateway IP address 192.168.1.40 (use whatever IP you assigned to your Linux or Unix system on Ethernet 0 (eth0/em0/wm0)).

If you want to stop mirroring traffic (examples would be shutting down SNORT, or rebooting your Linux or Unix system), execute the following commands in the DD-WRT, OpenWRT, Tomato GUI or via SSH/Telnet while logged into the router:

iptables -F -t mangle <enter>

The above command will flush the 'mangle' table and stop mirroring traffic to IP address 192.168.1.40 without rebooting the router.

This document is a work in progress, and as additional information becomes available, it will be added to this document.

If you have any questions, comments, or suggestions, please email me at:

wp02855@gmail.com (wp02855 at gmail dot com)

Bill Parker