

Linux Router Implementation Plan

Needs: A robust router based on a secured OS to allow only VPN traffic through while scanning traffic for possible intrusion attempts.

Step 1) Using a Gentoo linux Live! CD, boot the computer into the Gentoo Live OS. This is where you will be setting up the drives, partitions, and then install and configure the OS.

Step 2) When configuring the drives you need to have a minimum of two partitions. Since there will be no users other than for maintenance, then no /home or /usr partition needs to be specifically created. All that needs to be create are:

- a) a SWAP partition that is approximately twice the size of amount of installed memory in the PC.
- b) A root ("/) partition using the ReiserFS that is assigned the rest of the free space on the hard disk.

Step 3) Follow the "[Gentoo Installation Handbook](#)" for the complete installation instructions.

- a) Network Configuration:
 - a. Eth0 should be the internal adapter, set it's IP to 172.16.0.1
 - b. Eth1 should be the external adapter, set it to use DHCP

Step 4) Follow the "[Gentoo Home Router Guide](#)" for setting up IPTables initially for routing and filtering and dnsmasq for DNS forwarding and DHCP for local clients.

Step 5) In order to remotely administer the router, you will need to enable the ssh server. To do so you just need to type " /etc/init.d/sshd start" and then "rc-update add sshd default".

Step 6) Insert the following rules for IPTables:

- a) `$IPTABLES -A INPUT -p 47 -j ACCEPT`
- b) `$IPTABLES -A FORWARD -p 47 -s 0/0 -j ACCEPT`
- c) `$IPTABLES -t nat -A PREROUTING -p 47 -i eth0 -j DNAT --to 172.16.0.10`
- d) `$IPTABLES -A FORWARD -i eth1 -p 47 -d 172.16.0.10 -j ACCEPT`
- e) `$IPTABLES -A INPUT -p tcp --dport 1723 -j ACCEPT`
- f) `$IPTABLES -t nat -A PREROUTING -p tcp -i eth1 --dport 1723 -j DNAT --to 172.16.0.10:1723`
- g) `$IPTABLES -A FORWARD -i eth1 -p tcp -d 172.16.0.10 --dport 1723 -j ACCEPT`
- h) `$IPTABLES -A FORWARD -p TCP -s 0/0 --dport 1723 -j ACCEPT`

Step 7) Follow the instructions on the "[HOWTO Use Snort, Acid, and MySQL Effectively](#)" wiki. This will give ample information on setting up and configuring the intrusion detection software as well as reporting software

Step 8) Now we want to receive daily reports for the system with as much detail as possible as to possible unauthorized user logons or installs. For this we use the Logwatch application. Simply type in “emerge logwatch” and the install will commence. After the compile is completed you need to configure it to e-mail daily reports to the Information Security Officer with a detail level of 10.

Step 9) To maintain records of logs, it is recommended that logrotate be installed. Little if any configuration is required as the install inserts the needed scripts to rotate the logs every two weeks. To install the application, type: “emerge logrotate”.

Step 10) Handy application to have for testing the strength of the ISA firewall would be nmap, nessus or any other tools that could be used for verifying the integrity of the firewall.

