MLUG

(Melbourne Linux Users Group)

Firewalls

Hosted by: Rob Moonen and Michael Pope

Date: 30/10/2009

Intro

Cool things this month

Two Firewalls will be presented tonight

1. Smoothwall (Linux based)
2. pfsense (FreeBSD based)

Too Hard Basket

Beer

Cool things this month

zsync http://zsync.moria.org.uk/- Download only the new parts of a file. Works with compressed files such as ISO as well.

APTonCD - put your favourite packages on a CD easily. You can tell the program to copy packages you have installed or get a hold repository and put that on a DVD.

XBMC - Cool music/video/image player.

Games for ubuntu website - http://www.playdeb.net

Miro - Internet TV app which I found through Tim's OSGUI (www.osgui.com) website, which has heaps of good videos about linux etc.

Smoothwall Express3

Smoothwall is a complete 4 zone, IPTABLES based firewall in an 80MB CD image, the zones are designated Red(internet), Green(internal network), Orange(DMZ) and Purple(internal wireless network).
Where Green can talk to all, Purple to Orange and Orange to none, except through pinholes. All interfaces can of course talk to Red.

Smoothwall main page

From here one can control the internet connection directly and scan monthly data totals.

Status page

On this page we can see advanced status information about the connections within smoothwall.
There are also traffic graphs available for all interfaces.

Status advanced 2
Status advanced 3
Status advanced 4
Status advanced 5

In the next tab we have traffic graphs for machines connected to the smoothwall as well as the individual interfaces.

Traffic graphs 1
Traffic graphs 2

There are also more services available from the Status pages, like "bandwidth bars", "traffic monitor" and "my-smoothwall".

But these are beyond the scope of this article.

Services page
first is a web proxy that can greatly speed internet access to commonly visited sites.
An Instant messaging proxy
handles most available clients and allows concerned parents to supervise their childrens use of IM.
Email pop3 proxy with clamAV
will scan incoming email for virii so that unsuspecting users aren't caught flat footed.
VOIP sip proxy
this is a very useful service to buffer SIP phone streams, so that the conversation remains fluid.
DHCP server 1
there are two dhcp servers, one for the main green network and another for the purple network subnet.
DHCP server 2
but I have not printed the second, this is just the next page of the first dhcp server.

Dynamic DNS client
included is a bonus that enable seamless use of dynamic dns for your services.
Smoothwall remote access
is sometimes required from outside of your network, say if you are on the road and need to change some network setup for some reason. This is provided via ssh on port 222(security by obscurity), on both the RED and GREEN interfaces.
Keeping the time synchronised
is also quite important, so that your logs are actually meaningful, so this page allows the admin to set up smoothwall to synchronise with one of many available NTP sources on the internet.

Networking pages

Port forwarding

is useful for when you want to forward incoming internet network service requests to certain machines within your network or DMZ.

Outgoing allowed 1

can be configured as either "blocked with exceptions" or "allowed with exceptions" I chose the former paradigm.

Outgoing allowed 2

blocking is administered to all 3 network facing interfaces, so you must remember to allow rules for orange(dmz) if using one.

Pinholes from DMZ

here we allow certain ports to access the green network from orange for networking purposes.

Logs page

here we have the firewall logs page, this list is quite long so I went straight to the end.

IP Block

where we see that we can directly block problem IP's from the logs page. :-)

Logs intrinsic to smoothwall

these allow the admin to observe the functioning of various services provided.

Checking for newly installed computers

can be acomplished for instance by checking the DHCP logs.

Analyzing the web proxy

can also be done here, allowing one to see what clients have accessed and also what is now cached for speedy access.

Installation manuals

Smoothwall-Express-3.0-install-guide
here is the quick install guide to help get things working quickly.

SmoothWall_Express_3_Administrator_Guide_V2
and here is the full administrator guide, giving full details on every aspect of fine tuning your smoothwall, this is also supported by user forums at:
http://community.smoothwall.org/forum/

pfSense 1.2.1 stable

Hardware used

Jetway 1.6Ghz Atom N230
2GB Ram
DVDRW slimline (notebook IDE) drive.
Netgear USB ethernet (wired)
100GB SATA 5400rpm seagate drive.

5 port switch for the LAN.

pfSense 1.2.1 stable

pfSense features

- Stateful firewall using PF (OpenBSD's Packet Filter)
- DMZ support
- Wireless hotspot support
- Full NAT ability
- Clustering
- Proxy for speed and controlling content.
- hardware failover (if one server goes down the second kicks in)
- load balancing
- VPN (OpenVPN & PPTP). RADIUS support is included (centralized Authentication, Authorization and Accounting).
- Great documentation.
- Small in size
- Can run on embedded systems, many architectures

pfSense 1.2.1 stable

1. First you are asked if you want to setup the VLAN's now: **No.**

(VLAN stands for 'Virtual Local Area Network'. This links networks which are not physically in the same location together as if they were on the were.)

Refer: http://doc.pfsense.org/index.php/InstallationGuide

pfSense 1.2.1 stable

2. Enter the LAN interface: **axe0**

On the jetway it comes up with two interfaces rl0 and fxp0.
re0 = motherboard (WAN)
axe0 = PCI card (LAN)

pfSense 1.2.1 stable

3. Enter WAN interface: **re0**

4. Enter the Optional 1 interface: <Leave blank and hit Enter>
The Optional 1 interface is used if you want to setup a DMZ (DeMilitarized Zone).

5. Do you want to proceed: **y**

pfSense 1.2.1 stable

The Console

- Run a firewall from CD
- Creates ram drives
- Access config through web interface on lan side.

pfSense 1.2.1 stable

HD Install

Enter 99 to install to hard drive.

Refer http://forum.pfsense.org/index.php/topic,7356.0.html

Too hard basket

How do you get Internet sharing happening through bluetooth using Ubuntu 904 & N95?

Refer: https://help.ubuntu.com/community/BluetoothDialup#Listing%20Bluetooth%20devices

Questions?