

October Technical Presentation

Cheap & Silent firewalls



Registered ☺

Linux User Group of Mauritius -- <http://www.lugm.org/>

Why silent ?

- Old machines pentium 1 make a lot of noise (old hard disks)
- Some people in this room sleep near a pentium 1 acting as firewall at night ☹



How cheap can be cheap ?

Pentium 1 approx Rs 1500 (Orange.mu/annonces.php)

2x crappy Realtek 10/100 Rs 200

Hard disk (40 Gb -- expensive) or Hard disk 6 Gb (hard to find and noisy) Rs 2500

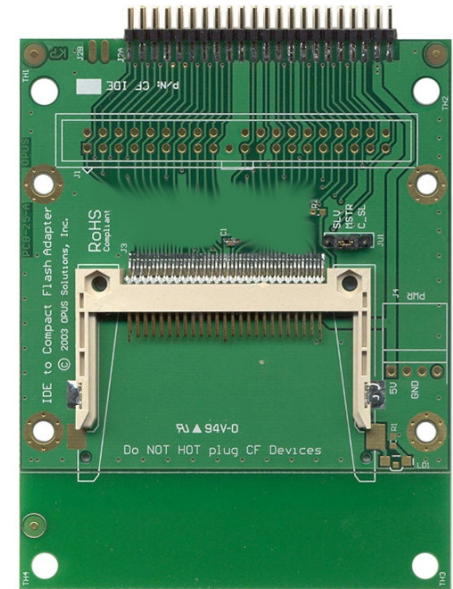
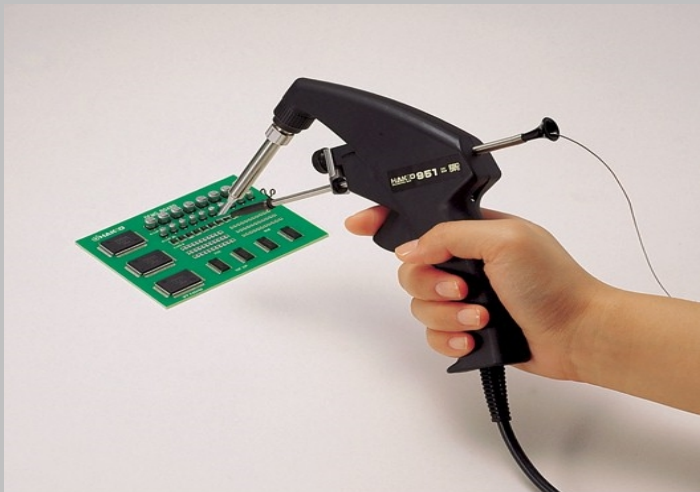
VS

GNU/Linux commercial routers : Linksys/Netgear –Rs 3000-4000



Cool devices™

- IDE-CF adapter are cheap – Rs 500
- CF Card are sold as low as Rs 450
- USB boot does not work on old machines (must be a post 2001 BIOS)
- Soldering gun (hardhack)



I'm no PF/netfilter guy – what can I do ?

- Vertical GNU/Linux distributions :
Zeroshell and iMedia
- Vertical *BSD systems : m0n0wall

ZEROSHELL NetServices
Release 1.0.beta2
About Logout Reboot Shutdown

CPU (1) VIA Nehemiah 800MHz
Uptime 0 days, 8:7
Load Avg 0.08 0.02 0.01
Memrel 2.6.16.21
Memory 450844 kB

FIREWALL Manage

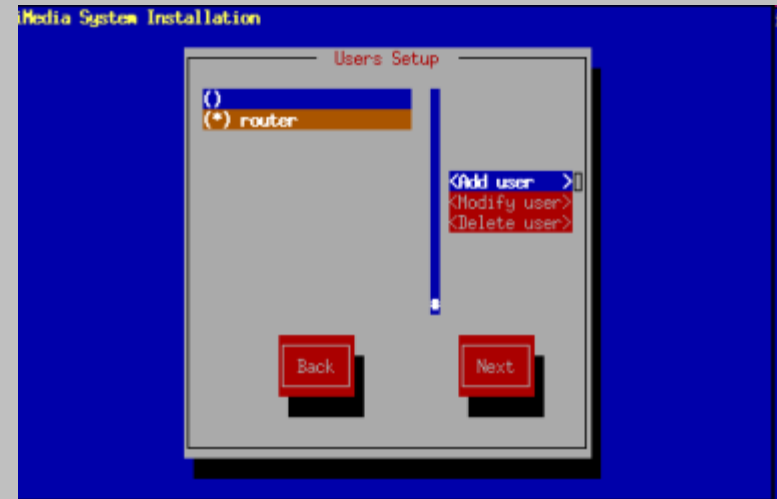
Chain: **INPUT** Policy: **ACCEPT** Chain: **INPUT** New Remove View Show Log

Save Cancel Enabled ☒

INPUT Rules Add Change Delete

Seq	Input	Output	Description	Log	Active
1	ppp0	*	ACCEPT udp -- 0.0.0.0/0 0.0.0.0/0 udp spt:88	no	<input checked="" type="checkbox"/>
2	ppp0	*	DROP all -- 0.0.0.0/0 0.0.0.0/0	no	<input checked="" type="checkbox"/>

Oct 01 20:07:51 SUCCESS: Kerberos 5 Bidirectional trust relationship between EXAMPLE.COM and TEST.COM successfully added.
Oct 01 20:08:12 SUCCESS: Kerberos 5 Outgoing trust relationship between EXAMPLE.COM and X.EXAMPLE.COM successfully added.



m0n0wall webGUI Configuration
m0n0wall_neon1.net

System: General setup

Hostname: m0n0wall
name of the firewall host, without domain part
e.g. firewall

Domain: neon1.net
e.g. mycorp.com

DNS servers:
IP addresses; these are also used for the DHCP service, DNS forwarder and for PPTP-VPN clients

☒ Allow DNS server list to be overridden by DHCP/PPP on WAN
If this option is set, m0n0wall will use DNS servers assigned by a DHCP/PPP server on WAN for its own purposes (including the DNS forwarder). They will not be assigned to DHCP and PPTP-VPN clients, though.

Username: admin
If you want to change the username for accessing the webGUI, enter it here.

Password:
(confirmation)
If you want to change the password for accessing the webGUI, enter it here twice.

webGUI protocol: ☒ HTTP ☐ HTTPS

webGUI port:
Enter a custom port number for the webGUI above if you want to override the default (80 for HTTP, 443 for HTTPS).

Time zone: Europe/Zurich
Select the location closest to you

Time update interval: 300
Minutes between network time sync.; 300 recommended, or 0 to disable

NTP time server: pool.ntp.org
Use a space to separate multiple hosts (only one required). Remember to set up at least one DNS server if you enter a host name here!

Save

m0n0wall is © 2002-2005 by Manuel Kasper. All rights reserved. [view license]

Step: download your image and phywrite to write to your CF card

I'm a GNU/*BSD guru: vtty is my breakfast!

- Filesystems : Write as little as possible !
- Logging : serial console or send to (unused consoles)



noatime,nodirtime,sync,syncdir,rw

. /dev/ttyS0



rw,sync,noatime

. /dev/ttyS0

Unix koans of Master-foo

`mount -t tmpfs -o size=2m tmpfs /var/log`

`mount_mfs -s 2048 /dev/ad0s1b /var/log`

YaFFS

JFFS v2

LogFS

NetBSD: LFS

“It has never worked reliably”
-- netbsd wiki



Tip: Use syslogd/newsyslogd to rotate and rm old log files

How hot is it in there ?

Sensors -- package

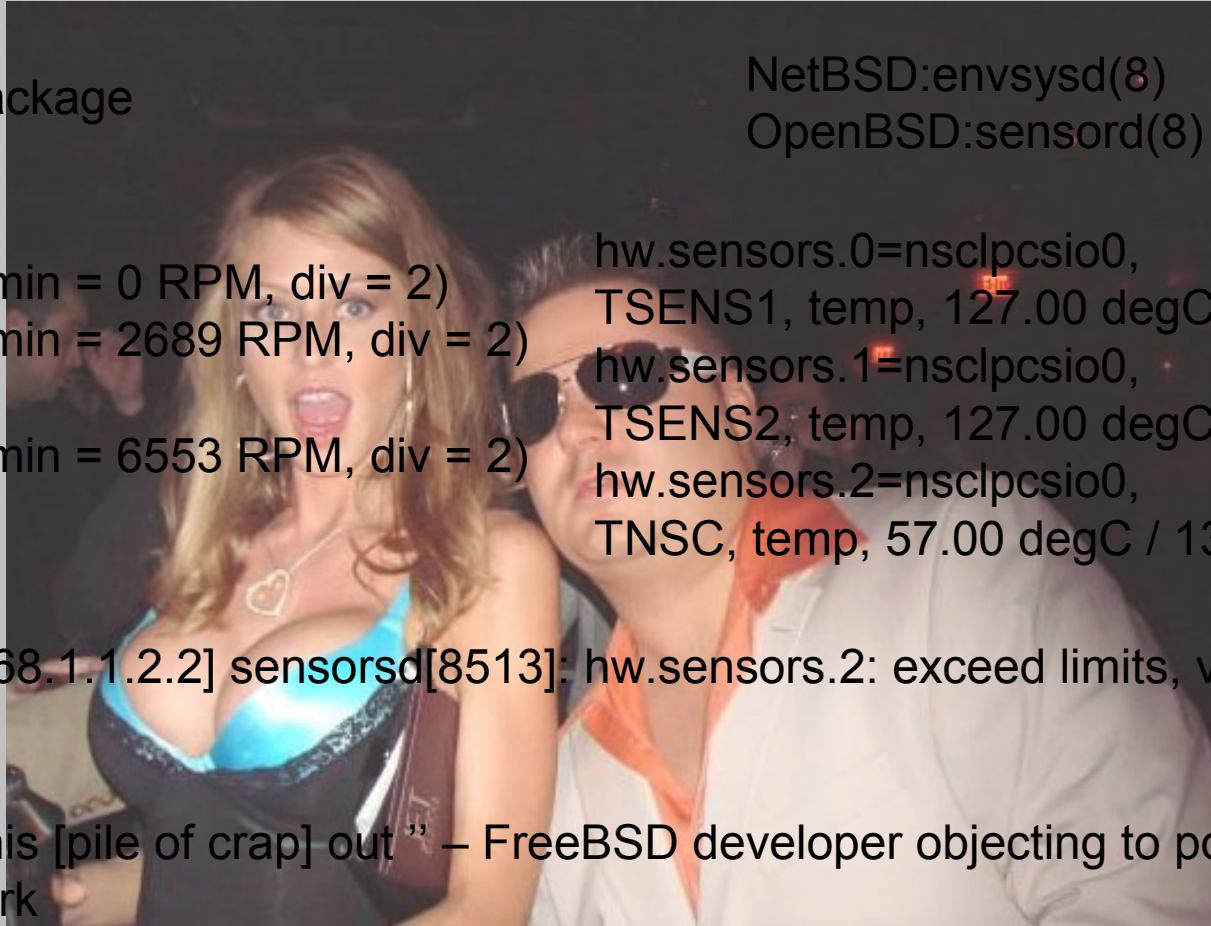
NetBSD:envsysd(8)
OpenBSD:sensord(8)

fan1: 0 RPM (min = 0 RPM, div = 2)
fan2: 0 RPM (min = 2689 RPM, div = 2)
ALARM
fan3: 0 RPM (min = 6553 RPM, div = 2)
ALARM

hw.sensors.0=nsclpcsio0,
TSENS1, temp, 127.00 degC / 260.60 degF
hw.sensors.1=nsclpcsio0,
TSENS2, temp, 127.00 degC / 260.60 degF
hw.sensors.2=nsclpcsio0,
TNSC, temp, 57.00 degC / 134.60 degF

18:27:42 [192.168.1.1.2.2] sensord[8513]: hw.sensors.2: exceed limits, value:
56.00C/132.80

``Please back this [pile of crap] out `` – FreeBSD developer objecting to porting openbsd
sensor framework



Questions ?

“The Atheros HAL on MIPS uses %s7 as a general purpose register, but the rest of the kernel uses it to store the value of curlwp. **Sam won't recompile the HAL for us (fair enough)**, and we can't modify the HAL to use another register **because doing so could put us in breach of the license** (v. crappy). So, do a save/set/restore on %s7 in KernIntr() and in the stubs that the HAL uses to call back into the kernel”.

--NetBSD developers discussing how to work with high-quality FreeBSD blob (.o files)

“Full source for the operating system is freely available”
-- FreeBSD Goals (introduction page)



Zen sysadmin

