

# Small Business Security Easier Than You Might Think

*Samuel Gordon-Stewart*



LCA 2005  
Security  
Miniconf

# About Me

- My IT history
  - My work

# Common Perception Of Security

- Expensive
- Mysterious

# SmoothWall



# SmoothWall

- SmoothWall is a network firewall Linux distro
  - Proxy Server
  - DHCP Server
    - More....

# SmoothWall

- Two varieties
  - SmoothWall Express (GPL)
  - SmoothWall Corporate Server (Proprietary)
    - Similar to Red Hat model

# SmoothWall

- Green/Orange/Red

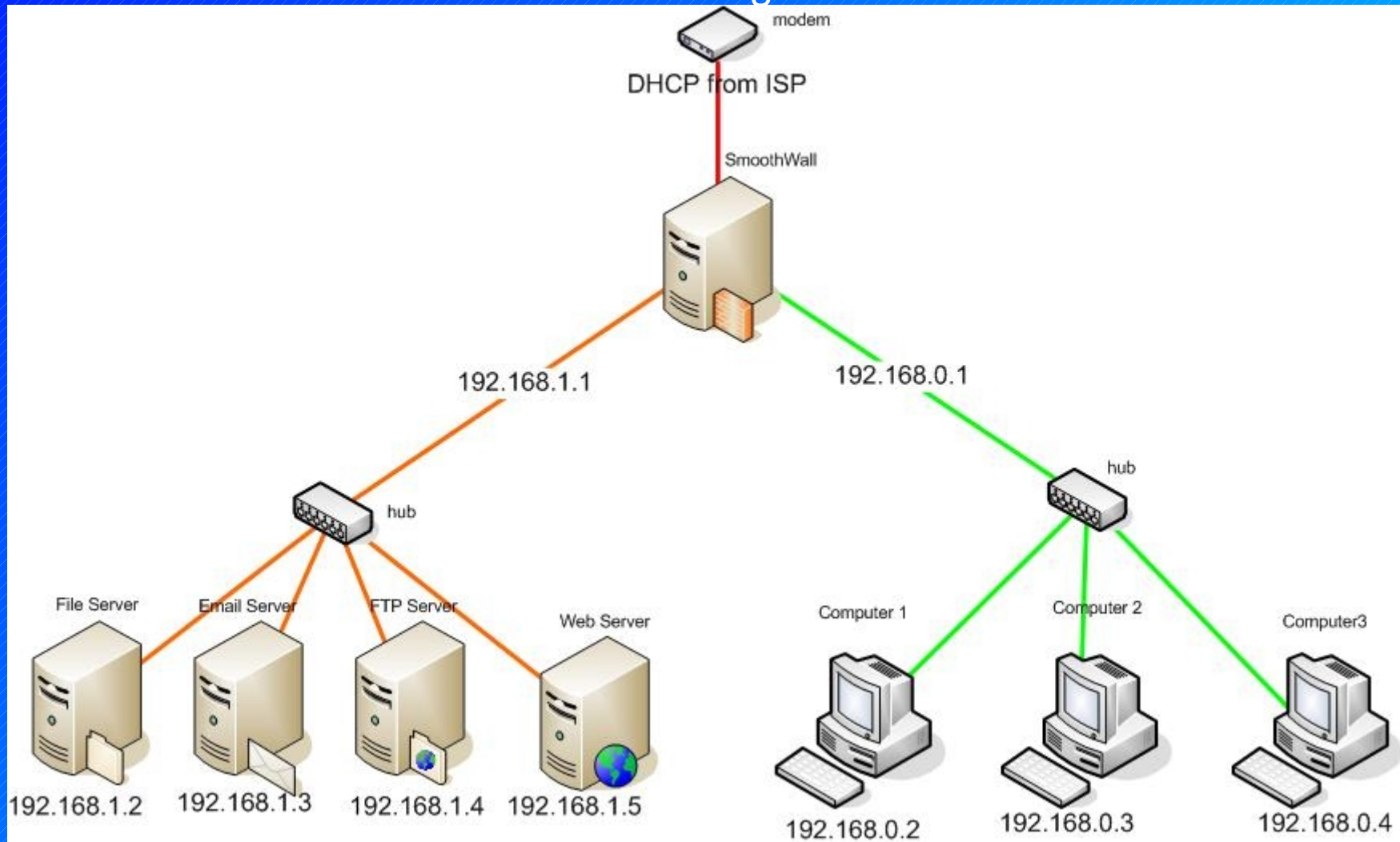


Image courtesy of SmoothWall user AwPhuch <http://awphuch2000.dyndns.org>

# SmoothWall

- Green/Red

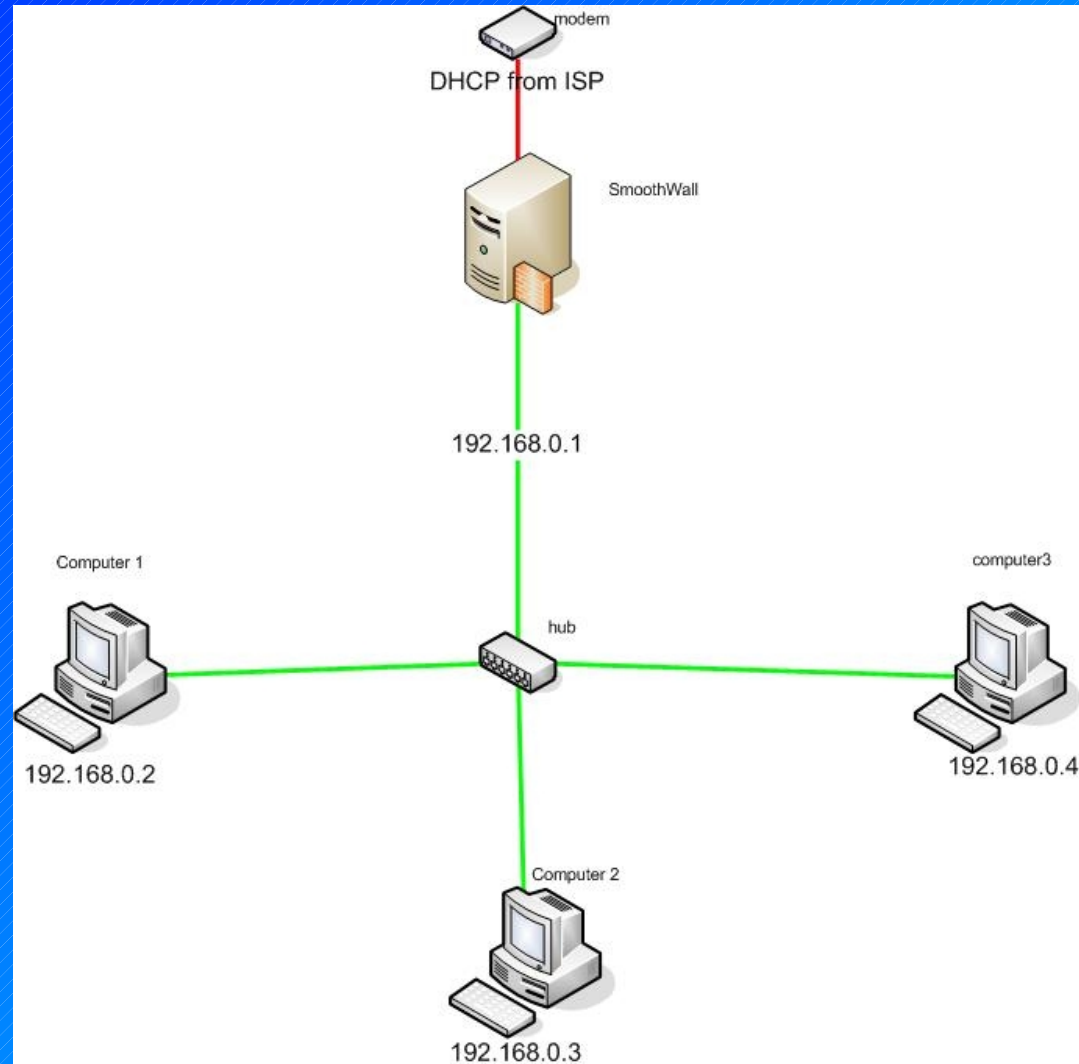


Image courtesy of SmoothWall user AwPhuch <http://awphuch2000.dyndns.org>

# SmoothWall

- Support

# Small Business Network Example

- ADSL Internet Connection
  - 6 PCs
  - One Printer
- OS Supported File Sharing
  - One Switch

# Small Business Network Example

*Why Use SmoothWall?*

- Price
- Functionality
- Adaptability
- Centralisation
- No specialist staff required

# Small Business Network Example

## *Other Options*

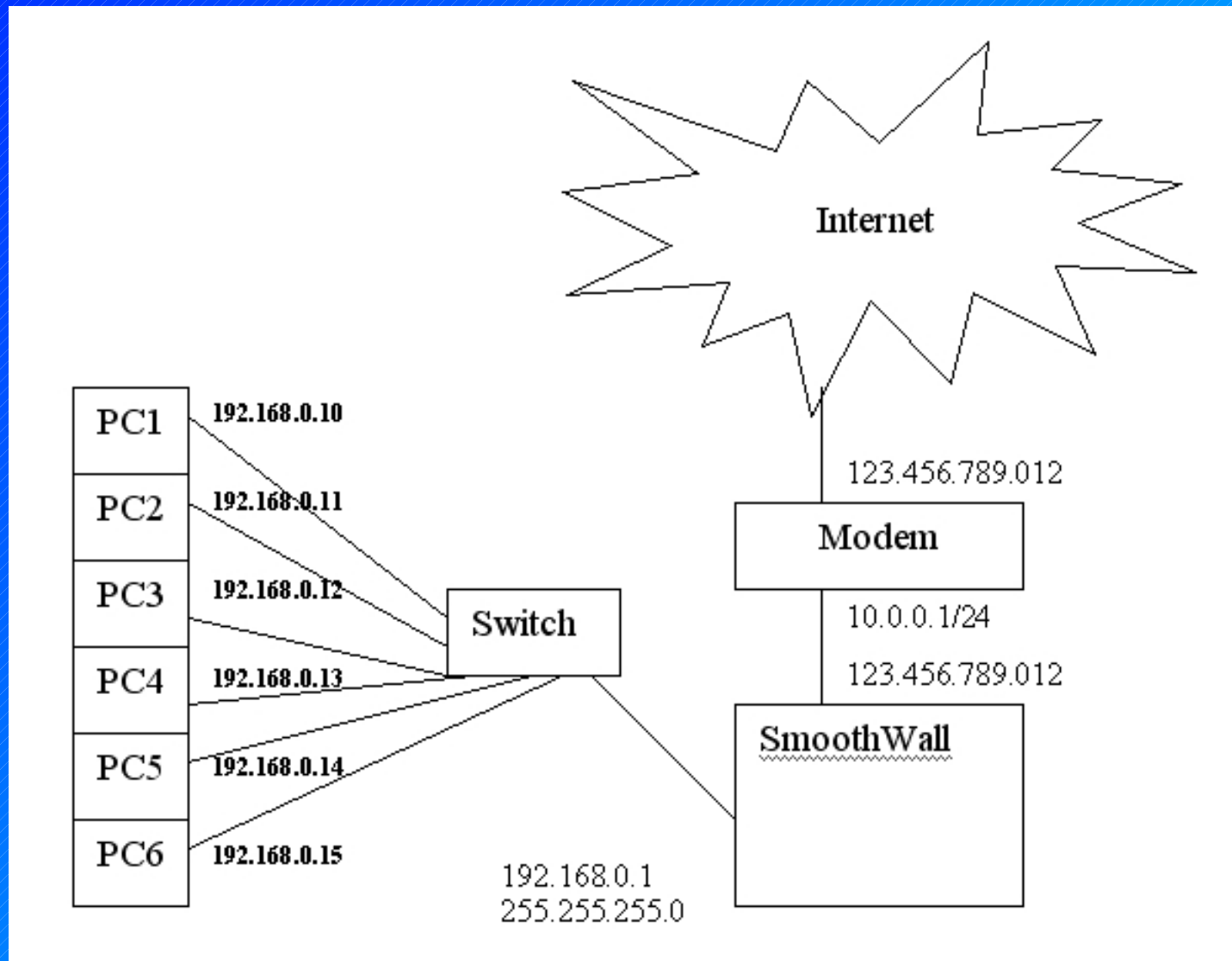
- Windows ICS
- SOHO Router
- Cisco Router
- Proprietary Gateway Device



# Small Business Network Example

## *Installing SmoothWall*

- Network Diagram



## Quick Configuration

Use this page to quickly configure the system.

Refresh Rate:

Operation Mode:	<input checked="" type="radio"/> PPP <input type="radio"/> Bridge
Connection Type:	PPPoA VC-Mux
VPI:	8
VCI:	35
Security Protocol:	<input checked="" type="radio"/> PAP <input type="radio"/> CHAP
Username:	*****@L2TP.tpg
Password:	*****

PPP Information			
IP Address	Mask	Gateway	Connection Status
*****	255.255.255.255	202.7.162.164	Connected <input type="button" value="Disconnect"/>

- D-Link
  - Quick Configuration
  - System View
  - LAN
    - LAN Config
    - DHCP Mode
  - WAN
    - DSL Status
    - DSL Mode
    - PPP
    - EOA
    - IPOA
  - Bridging
    - Bridging
    - ATM VCC
  - Admin
    - User Config
    - Save & Reboot
    - Image Upgrade
    - Alarm
    - Diagnostics
    - Remote Access



# SmoothWall Express 2.0

The SmoothWall Open Source Project

The CDROM image is published by and is the Copyright of the SmoothWall Open Source Team, and of the original authors of its component parts. Visit [smoothwall.org/team](http://smoothwall.org/team) on the web for the list of contributors.

## W A R N I N G !

\* The installation process will delete all existing partitions and data \*  
\* on the PC on which SmoothWall is installed. Do not continue the \*  
\* installation if there is data on the hard disk you wish to retain! \*

Please also be aware that upon successful install, your SmoothWall install will return benign and anonymous system information (CPU type, speed, RAM, HD size, NIC/connection type [modem/ISDN/ASDL/etc]) to our servers for statistics aggregation, the results of which will be published at [smoothwall.org/about/statistics.html](http://smoothwall.org/about/statistics.html) Opt-out info is also on that page

Keep updated with the latest software updates and news at [smoothwall.org](http://smoothwall.org)  
Contribute to the community site at [community.smoothwall.org](http://community.smoothwall.org)

- Press RETURN to continue the install of SmoothWall Express -

boot: \_

Select installation media

SmoothWall Express can be installed from multiple sources. The simplest is to use the machines CDROM drive. If the computer lacks a drive, you may install via another machine on the LAN which has the installation files available via HTTP.

**CDROM**

HTTP

Ok

Cancel

!!! WARNING !!!

You are about to PERMANENTLY ERASE the contents of the harddisk. This will OVERWRITE ALL DATA ON ALL PARTITIONS on your first IDE harddisk. If you would like to continue with the installation of SmoothWall Express, press the Ok button. Otherwise press Cancel to ABORT the installation process. There is NO UNDO FEATURE once this has been done.

Ok

Cancel

## Configure networking

You should now configure networking by first loading the correct driver for the GREEN interface. You can do this by either auto-probing for a network card, or by choosing the correct driver from a list. Note that if you have more than one network card installed, you will be able to configure the others later on in the installation. Also note that if you have more than one card which is the same type as GREEN and each card requires special module parameters, you should enter parameters for all cards of this type such that all cards can become active when you configure the GREEN interface.

Probe

Select

Cancel



**GREEN interface**

Enter the IP address information for the GREEN interface.

IP address: 192.168.0.1\_\_\_\_\_

Network mask: 255.255.255.0\_\_\_\_\_

Ok Cancel



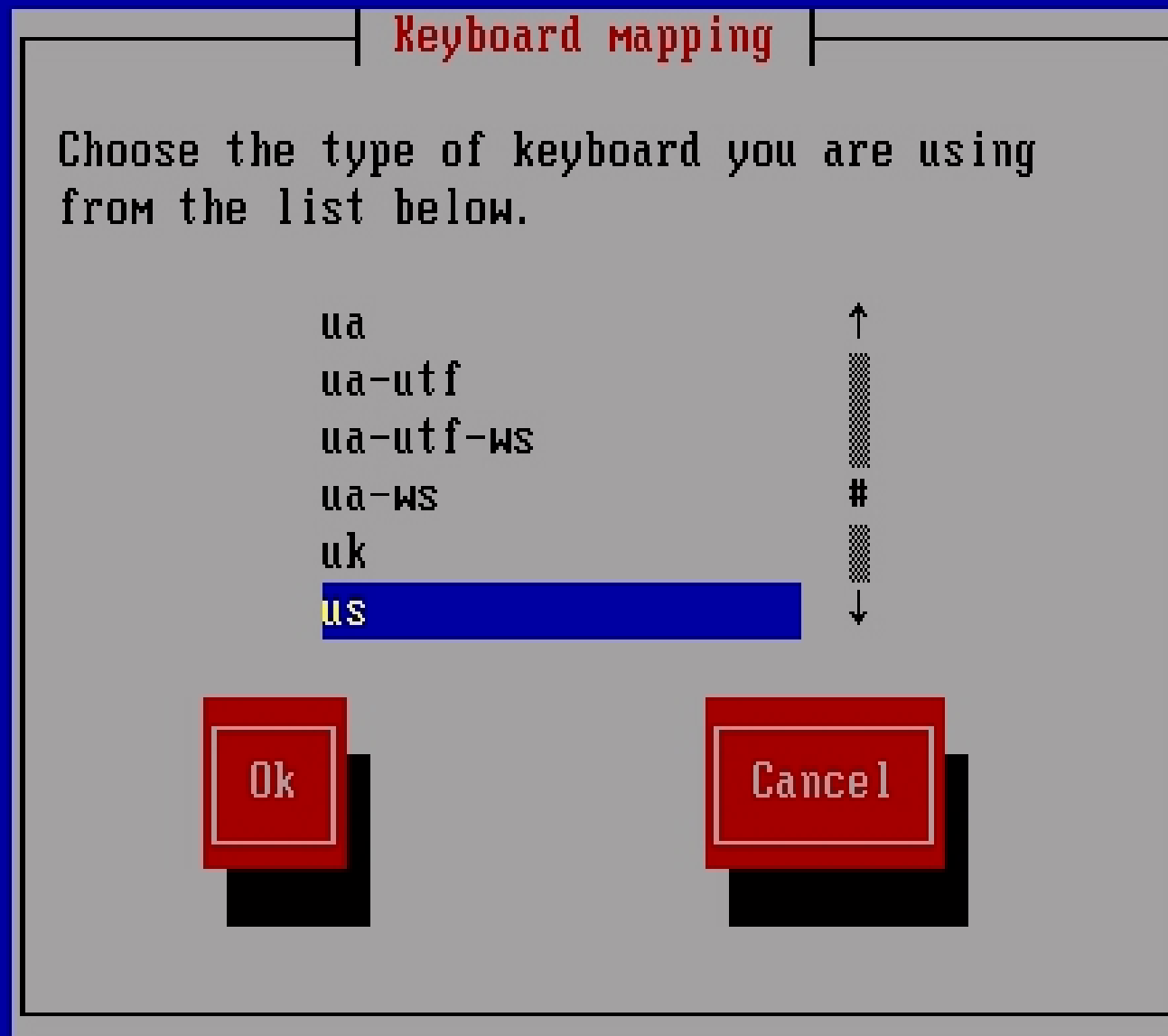


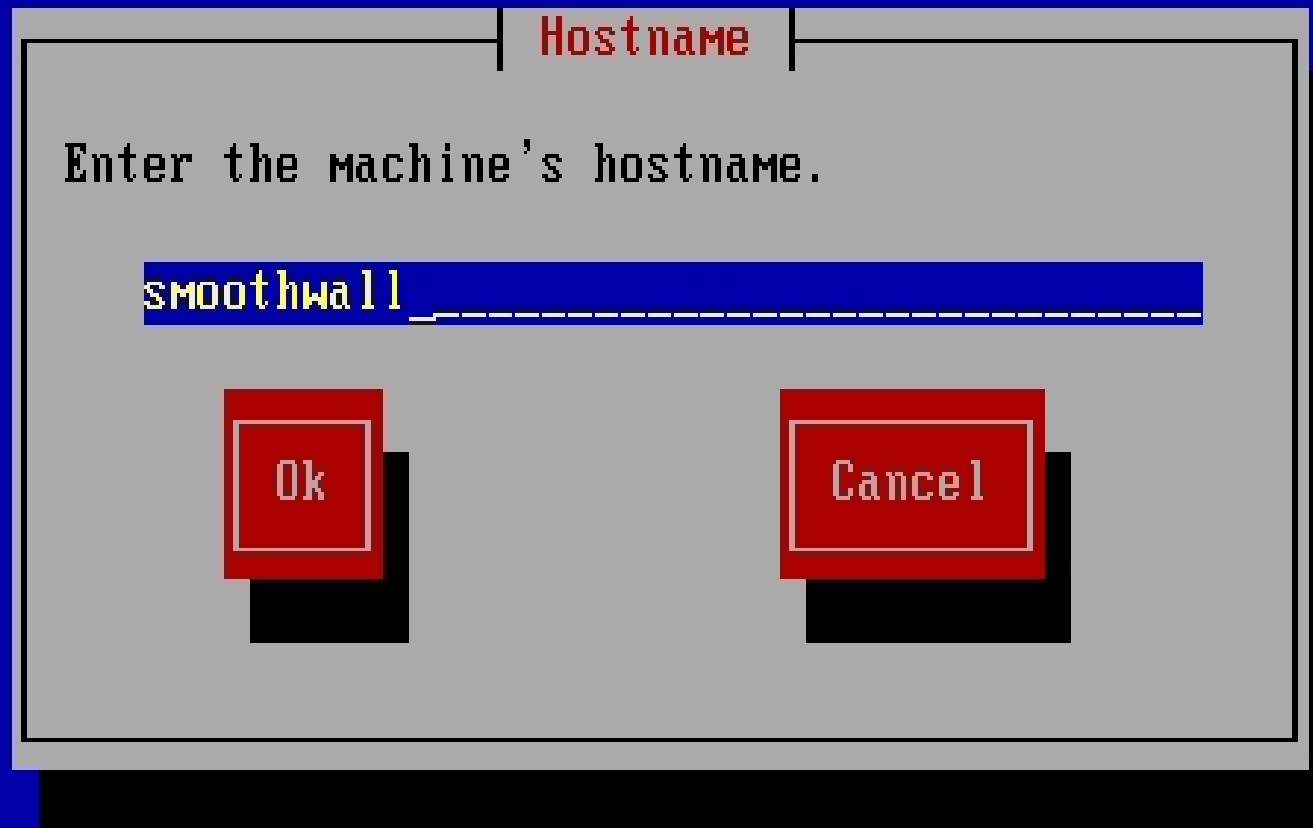
SmoothWall Express 2.0

Do you want to restore the configuration for this SmoothWall Express from a previous installation using a backup floppy disk? If you select 'Yes', the areas which were restored from the backup will be automatically configured and will not be displayed to you.

No

Yes





<Tab>/<Alt-Tab> between elements    ;    <Space> selects

## Web proxy

When requesting the Update list, SmoothWall Express must connect to a webserver. Some ISPs will block this direct traffic, and instead they will require SmoothWall Express to access this server indirectly, via a web proxy. If your ISP requires you to connect this way, please enter the web proxy Hostname and Port. Most ISPs do not require you to connect through a web proxy, in which case you should leave these settings blank. Note that this setting has nothing to do with SmoothWall Express' built in proxy service.

Hostname: Port: 

Ok

Cancel

ISDN configuration menu

ISDN is currently Disabled.

Protocol: UNSET

Card: UNSET

Local phone number: UNSET

Select the item you wish to reconfigure, or  
choose to use the current settings.

**Protocol/Country**

Set additional module parameters

ISDN card

Local phone number (MSN/EAZ)

Ok

Enable ISDN

Disable ISDN

**ADSL configuration**

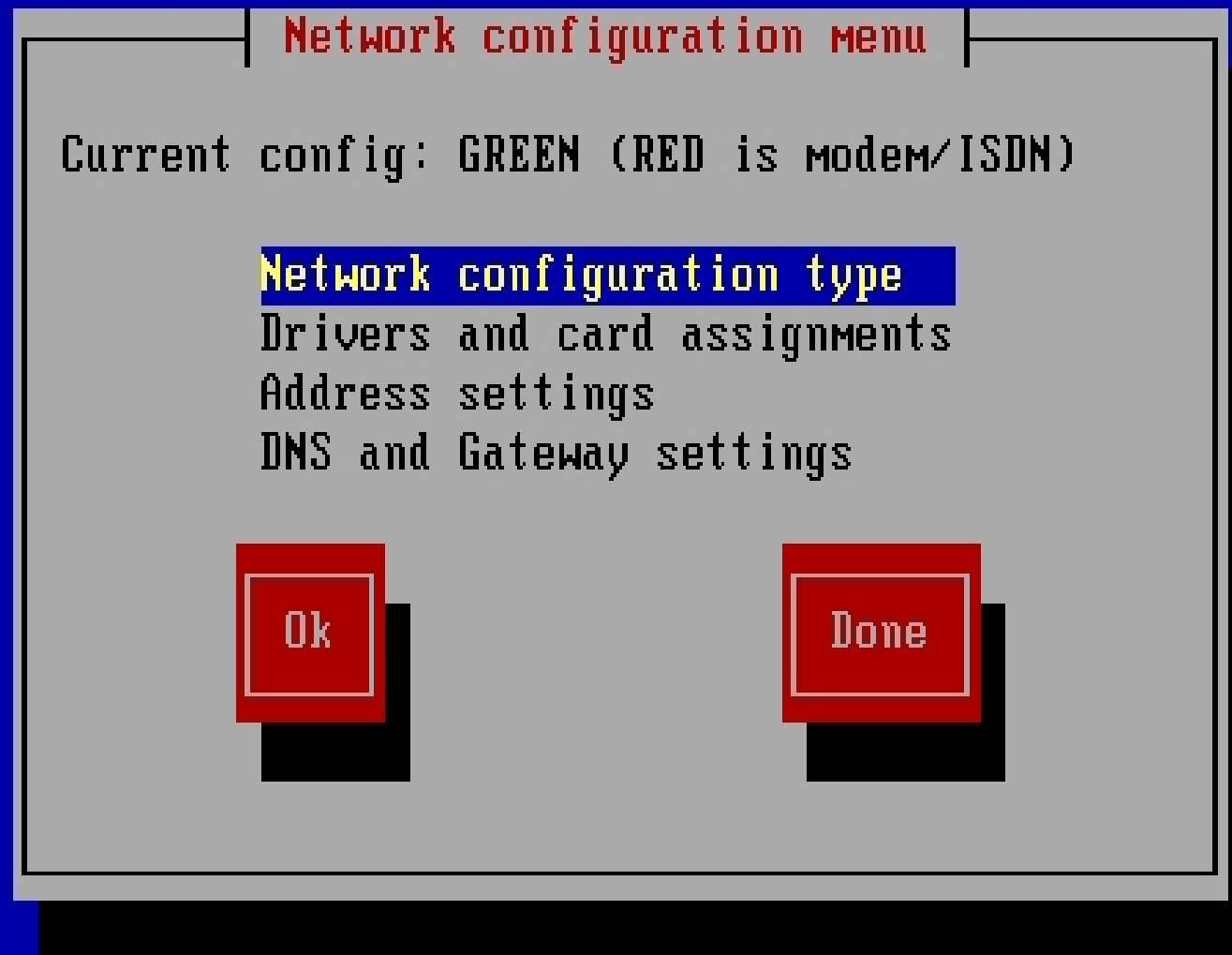
ADSL is currently: Disabled

Device type: UNSET  
UPI: UNSET VCI: UNSET

Select the item you wish to reconfigure, or  
choose to use the current settings.

**Device type**  
Other settings

**Ok**      **Enable ADSL**      **Disable ADSL**





Network configuration type

Select the network configuration for SmoothWall Express. The following configuration types list those interfaces which have ethernet attached. If you change this setting, a network restart will be required, and you will have to reconfigure the network driver assignments.

**GREEN (RED is modem/ISDN)**

GREEN + ORANGE (RED is modem/ISDN)

GREEN + RED

GREEN + ORANGE + RED

Ok

Cancel

### Drivers and card assignments

Configure network drivers, and which interface each card is assigned to. The current configuration is as follows:

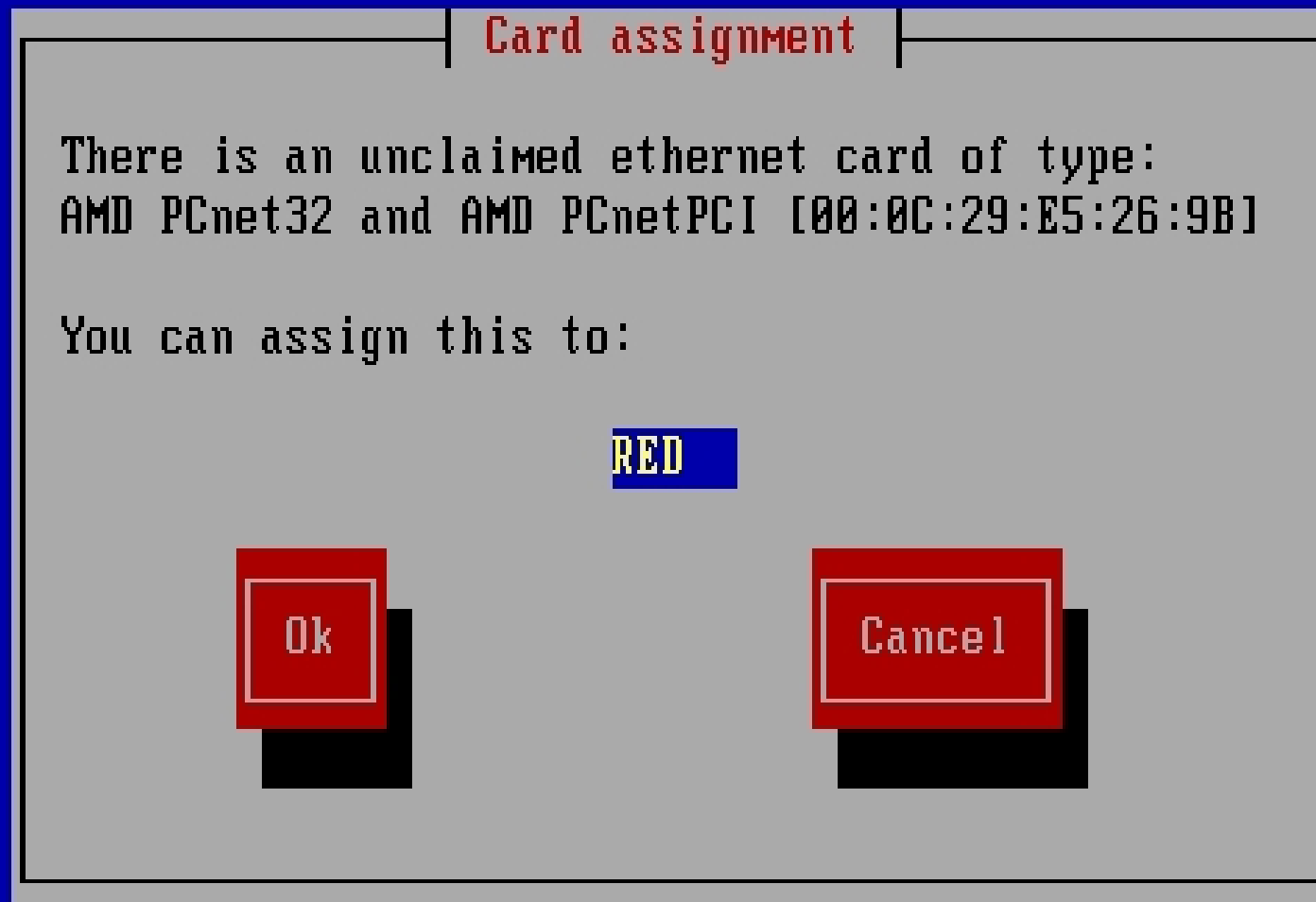
GREEN: AMD PCnet32 and AMD PCnetPCI (eth0) [00:0C:29:E5:26:91]

RED: UNKNOWN (UNSET)

Do you wish to change these settings?

Ok

Cancel



RED interface

Enter the IP address information for the RED interface.

Static

DHCP

PPPOE

DHCP Hostname: smoothwall\_\_\_\_\_

IP address: \_\_\_\_\_

Network mask: 255.255.255.0\_\_\_\_\_

Ok

Cancel

**DNS and Gateway settings**

Enter the DNS and gateway information. These settings are used only if DHCP is disabled on the RED interface.

Primary DNS:

Secondary DNS:

Default Gateway:

DHCP server configuration

Configure the DHCP server by entering the settings information.

**[\*] Enabled**

Start address:	192.168.0.10_____
End address:	192.168.0.200_____
Primary DNS:	192.168.0.1_____
Secondary DNS:	_____
Default lease (mins):	300_____
Max lease (mins):	600_____
Domain name suffix:	_____

Ok

Cancel

**SmoothWall Express 2.0**

Enter SmoothWall admin password. This is the user to use for logging into the SmoothWall web administration pages.

Password:

Again:

SmoothWall Express 2.0

Enter the 'root' user password. Login as this user for commandline access.

Password: \*\*\*\*\*  
Again: \*\*\*\*\*

Ok Cancel



SmoothWall Express 2.0

Enter the 'setup' user password. Login as this user to access the setup program.

Password: \*\*\*\*\*

Again: \*\*\*\*\*

Ok Cancel





# SmoothWall

## SmoothWall Express 2.0

SmoothWall

Press Return, or wait 10 seconds for SmoothWall to load

(C) 2000 - 2003 THE SMOOTHWALL TEAM  
PORTIONS (C) THE ORIGINAL AUTHORS  
FOR TEAM DETAILS AND FULL CREDITS, VISIT [SMOOTHWALL.ORG/TEAM](http://SMOOTHWALL.ORG/TEAM)


VISIT OUR WEBSITE AT [SMOOTHWALL.ORG](http://SMOOTHWALL.ORG) FOR UPDATES AND LATEST INFO.

SmoothWall Express 2.0 - <http://smoothwall.org/>


smoothwall login: \_

# SmoothWall's Web Interface

- Unsecure <http://ip.address.of.smoothwall:81>
- Secure <https://ip.address.of.smoothwall:441>

**SmoothWall Express 2.0** connection status » 

[control](#) | [about your smoothie](#) | [services](#) | [networking](#) | [vpn](#) | [logs](#) | [tools](#) | [maintenance](#)



[home](#) | [credits](#) [shutdown](#) | [help](#) 



Welcome to **SmoothWall Express 2.0**  
 This is your gateway to configuring and administering your SmoothWall firewall. Please make sure you read the Administration Guide before reconfiguring your SmoothWall — the guide is available with our other documentation from **our website**.



9:25pm up 25 days, 14:16, 0 users, load average: 0.00, 0.00, 0.00

Produced in association with  **U.S. Robotics** 

express 2.0 fixes6 ui-3.6.1  
 SmoothWall™ is a trademark of **SmoothWall Limited**.

© 2000 - 2003 **The SmoothWall Team**  
**Credits** - Portions © **original authors**

**SmoothWall Express 2.0** connection status »

control about your smoothie services networking vpn logs tools maintenance

status | advanced | traffic graphs

shutdown | help ?



### About Your SmoothWall

Active service status of your Smoothie.

**Services:**

Logging server	<b>RUNNING</b>
DHCP server	<b>RUNNING</b>
DNS proxy server	<b>RUNNING</b>
Kernel logging server	<b>RUNNING</b>
Web proxy	<b>STOPPED</b>
Web server	<b>RUNNING</b>
Secure shell server	<b>RUNNING</b>
Intrusion Detection System	<b>RUNNING</b>
CRON server	<b>RUNNING</b>
VPN	<b>STOPPED</b>

Produced in association with

express 2.0 fixes6 ui-3.6.1

SmoothWall™ is a trademark of **SmoothWall Limited**.

© 2000 - 2003 **The SmoothWall Team**  
Credits - Portions © **original authors**



## Advanced Status

Pertinent information about your Smoothie, current configuration and resource usage.

### Memory:

	Total	Used	Free	Used %	Shared	Buffers	Cached
Mem:	253312K	124072K	129240K	48%	0K	68500K	34868K
Swap:	24088K	0K	24088K	0%			
<b>Total:</b>	<b>277400K</b>	<b>124072K</b>	<b>153328K</b>	<b>44%</b>			

### Disk usage:

Filesystem	Mount point	Size	Used	Available	Used %
/dev/harddisk4	/	7.5G	157M	6.9G	3%
/dev/harddisk1	/boot	7.6M	3.4M	3.8M	47%
/dev/harddisk3	/var/log	1.9G	50M	1.7G	3%

### Inode usage:

Filesystem	Mount point	Inodes	Used	Free	Used %
/dev/harddisk4	/	997472	12374	985098	2%
/dev/harddisk1	/boot	2008	26	1982	2%
/dev/harddisk3	/var/log	250368	207	250161	1%

### Uptime and users:

9:26pm up 25 days, 14:17, 0 users, load average: 0.00, 0.00, 0.00

USER	TTY	FROM	LOGING	IDLE	JCPU	PCPU	WHAT

### Interfaces:

```
eth0      Link encap:Ethernet  HWaddr 00:10:5A:99:0D:7C
          inet addr:192.168.0.1  Bcast:192.168.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2758815  errors:0  dropped:0  overruns:0  frame:0
          TX packets:3658065  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:458062074 (436.8 Mb)  TX bytes:4256240955 (4059.0 Mb)
```



```
UP BROADCAST NOTRAILERS RUNNING MULTICAST MTU:1500 Metric:1
RX packets:3768018 errors:0 dropped:0 overruns:0 frame:0
TX packets:2850764 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:4291785048 (4092.9 Mb) TX bytes:493454520 (470.5 Mb)
Interrupt:5 Base address:0xd400
```

```
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
UP LOOPBACK RUNNING MTU:16384 Metric:1
RX packets:7408 errors:0 dropped:0 overruns:0 frame:0
TX packets:7408 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:1040419 (1016.0 Kb) TX bytes:1040419 (1016.0 Kb)
```

### Routing:

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.0.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
0.0.0.0	220.245.222.74	0.0.0.0	UG	0	0	0	eth1

### Loaded modules:

Module	Size	Used by	Not tainted
sis900	14220	1	
crc32	3560	0 [sis900]	
3c59x	28240	1	
ip_nat_quake3	2472	0 (unused)	
ip_conntrack_quake3	2472	1	
ip_nat_h323	3132	0 (unused)	
ip_conntrack_h323	2848	1	
ip_nat_nms	3376	0 (unused)	
ip_conntrack_nms	3664	1	
ip_nat_ftp	3216	0 (unused)	
ip_conntrack_ftp	4496	1	
ip_nat_irc	2640	0 (unused)	
ip_conntrack_irc	3408	1	
ppp_async	7936	0 (unused)	
ppp_synctty	6344	0 (unused)	
ppp_generic	21084	0 [ppp_async ppp_synctty]	
slhc	5624	0 [ppp_generic]	
usb-ohci	19848	0 (unused)	
usbcore	67840	1 [usb-ohci]	

### Kernel version:

Linux smoothwall 2.4.29 #1 Thu Jan 27 15:15:02 GMT 2005 i686 i686 i386 GNU/Linux



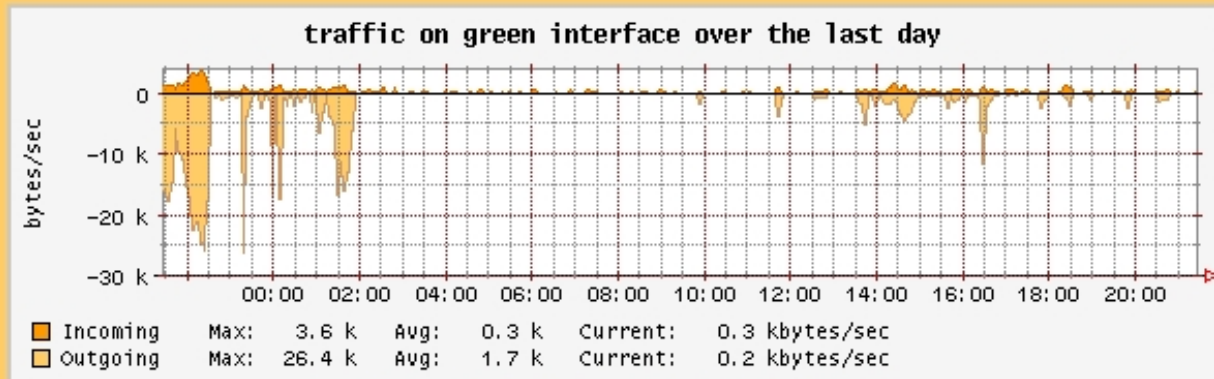
## Traffic Graphs

Statistical graphs based upon traffic usage across your SmoothWall's network interfaces.

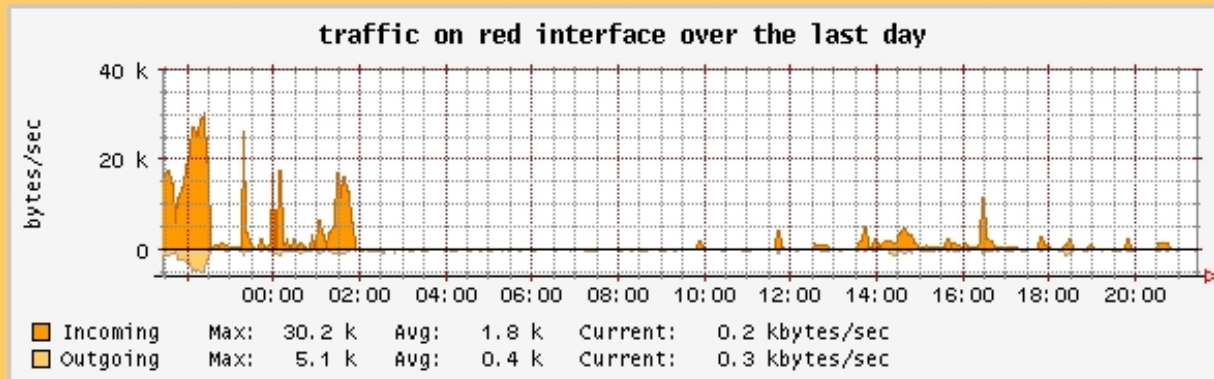
### Network traffic graphs:

last updated Sun Apr 17 21:25:00 2005  
with data to Sun Apr 17 21:25:00 2005

### Summary network traffic graphs:



[click for detailed graphs for the green interface »](#)



[click for detailed graphs for the red interface »](#)



## Web Proxy

Configure and enable your SmoothWall's integrated caching web proxy service.

**Web proxy:**

Cache size (MB):	<input type="text" value="500"/>	Remote proxy: *	<input type="text"/>
Remote proxy username: *	<input type="text"/>	Remote proxy password:	<input type="text"/>
Max object size (KB):	<input type="text" value="4096"/>	Min object size (KB):	<input type="text" value="0"/>
Max outgoing size (KB):	<input type="text" value="0"/>	Max incoming size (KB):	<input type="text" value="0"/>
Transparent:	<input type="checkbox"/>	Enabled:	<input type="checkbox"/>

\* These fields may be blank.



### DHCP

Configure and enable your SmoothWall's DHCP service, to automatically allocate LAN IP addresses to your network clients.

#### DHCP:

Start address:	<input type="text" value="192.168.0.10"/>	End address:	<input type="text" value="192.168.0.200"/>
Primary DNS:	<input type="text" value="192.168.0.1"/>	Secondary DNS:	<input type="text"/>
Primary WINS:	<input type="text"/>	Secondary WINS:	<input type="text"/>
Default lease time (mins):	<input type="text" value="300"/>	Max lease time (mins):	<input type="text" value="600"/>
Domain name suffix: *	<input type="text"/>	Enabled:	<input checked="" type="checkbox"/>

\* This field may be blank.

#### Add a new static assignment:

Description:	<input type="text"/>	MAC address:	<input type="text"/>
IP address:	<input type="text"/>	<input type="button" value="Add"/>	

#### Current static assignments:

Description	MAC address	IP address	Mark
Server	00:10:5A:99:0E:3F		<input type="checkbox"/>
Workhorse	00:30:BD:2E:25:FC		<input type="checkbox"/>
Gamenet	00:40:F4:7C:09:B3		<input type="checkbox"/>
ClarkConnect	00:A1:B0:09:CC:A8		<input type="checkbox"/>

#### Note:



## Dynamic DNS

Especially suited when your ISP assigned you a different IP address every time you connect, you can configure your SmoothWall to manage and update your dynamic DNS names from several popular services.

### Add a host:

Service:    
 Hostname: \*   
 Username:

Behind a proxy:       Enable wildcards:   
 Domain:   
 Password:

Enabled:

\* Hostname is not necessary for dyndns.org(custom) service.

### Current hosts:

Service	Hostname	Domain	Proxy	Wildcards	Enabled	Mark
dyndns	goggo	dyndns.org	✗	✓	✓	<input type="checkbox"/>



## Intrusion Detection System (IDS)

Enable the Snort IDS service to detect potential security breach attempts from outside your network. Note that Snort **does not** prevent these attempts — your port forwarding and access rules are used to allow and deny inbound access from the outside.

**Intrusion Detection System:**  
Snort:





## Remote Access

Enable Secure Shell access to your SmoothWall, and restrict access based upon referral URL to ignore external links to your SmoothWall.

**Remote access:**

SSH:  Allow admin access only from valid referral URLs:  \*

\* In order to be certain that the request for an admin function is from the SmoothWall server and not some third party web page, a referral check is done. Enabling this feature means it is only possible to administer the SmoothWall if the URL you visit contains either the local GREEN IP, the local hostname, or the RED IP address. It will not be possible to administer the SmoothWall if you connect via a DNS or Dynamic DNS name.

Save



## Time settings

Change timezone, manually set the time and date, and configure time synchronisation.

**Timezone:**  
Timezone:

**Time and date:**  
Set:  Time:  :  :  Date:

**Network time retrieval:**  
Enabled:  Interval:   
Save time to RTC:  Next update in:

**Network time servers:**  
 Multiple random public servers  
 Selected single public server:   
 User defined single public or local server:





## Port Forwarding

Forward ports from your external IP address to ports on machines inside your LAN or DMZ.

### Add a new rule:

External source IP, or network (blank for "ALL"):

Source port or range:

Destination IP:

Destination port:  \*

TCP

Enabled:

\* If blank, then the source port will be used as the destination port.

### Current rules:

Proto	External source IP	Source port	Destination IP	Destination port	Enabled	Mark
TCP	ALL	80		N/A	<input checked="" type="checkbox"/>	<input type="checkbox"/>



## External Service Access

Allow access to admin services running on the SmoothWall to external hosts.

### Add a new rule:

TCP  External source IP, or network (blank for "ALL"):  Destination port:

Enabled:

### Current rules:

Proto	Source	Destination port	Enabled	Mark
	<input type="button" value="Remove"/>	<input type="button" value="Edit"/>		



## DMZ Pinholes

Enable access from a host on your DMZ to a port on a host on your LAN.

**Add a new rule:**

TCP  Source IP:  Destination IP:  Destination port:

Enabled:

**Current rules:**

Proto	Source IP	Destination IP	Destination port	Enabled	Mark
	<input type="button" value="Remove"/>		<input type="button" value="Edit"/>		



## PPP Settings

Configure username, password and other details for up to five PPP, PPPoA or PPPoE connections.

### Profiles:

Empty ▾

Select

Delete

Profile name:

Unnamed

### Telephony:

Interface:

Modem on COM1 ▾

Computer to modem rate:

115200 ▾

Number:

Modem speaker on:

Dialing mode:

Tone ▾

Maximum retries:

10

Idle timeout (mins; 0 to disable):

15

Persistent connection:

Dial on Demand:

Dial on Demand for DNS:

Connect on SmoothWall restart:

Automatic reboot if connection down for 5 minutes:

ISP requires Carriage Return:

### Authentication:

Username:

Password:

Method:

PAP or CHAP ▾

Script name:

### DNS:

Type:

Manual  Automatic

Primary DNS:

Secondary DNS:

Save

Restore



## IP block configuration

Add blocking rules to prevent access from specified IP addresses or networks.

**Add a new rule:**

Source IP or network:

Drop packet       Reject packet      Log:

Enabled:

**Current rules:**

Source IP	Action	Log	Enabled	Mark
<input type="button" value="Remove"/>			<input type="button" value="Edit"/>	



## Advanced networking features

Configure ICMP settings, and other advanced features.

**Advanced networking features:**

Block ICMP ping:	<input type="checkbox"/>	Enable SYN cookies:	<input type="checkbox"/>
Block and ignore IGMP packets:	<input type="checkbox"/>	Block and ignore multicast traffic:	<input type="checkbox"/>
Enable UPnP (Universal Plug and Play) support:	<input type="checkbox"/>		





## VPN Connections

Create connections to other SmoothWalls or IPSec-compliant hosts which have static IP addresses.

### Add a new connection:

Name:

Left:  Left subnet:

Right:  Right subnet:

Secret:

Again:

Compression:  Enabled:

### Current connections:

### Import and Export:

## Log Viewer

Check activity logs for services operating on your SmoothWall, such as DHCP, IPSec, updates and core kernel activity

### Settings:

Section:  Month:  Day:

- SmoothWall
- PPP
- ISDN
- DHCP server
- SSH
- Login/Logout
- Kernel
- IPSec
- Update transcript
- NTP

### Log

```

00:30:04 smoo successfully updated; using server(s) time.deakin.edu.au ntp.ourconcord.net
tick.cs.unlv.my.pool.ntp.org.
01:30:05 smoo successfully updated; using server(s) it.pool.ntp.org ntp.linux.org.ve ntp.tuxfamily.net
louie.udel.ed
02:30:04 smoo successfully updated; using server(s) ntp.cs.unp.ac.za gilbreth.ecn.purdue.edu
si.pool.ntp.o ucsc.edu.
03:30:05 smoo successfully updated; using server(s) fartein.ifi.uio.no au.pool.ntp.org ntp.ip.ro
no.pool.ntp.o
04:30:06 smoo successfully updated; using server(s) se.pool.ntp.org ntp.tuxfamily.net se.pool.ntp.org
no.pool.ntp.o
05:30:05 smoothwall System clock successfully updated; using server(s) dk.pool.ntp.org ns.pool.ntp.org tk1.ihug.co.nz
ntp.cs.unp.ac.za it.pool.ntp.org.
06:30:07 smoothwall System clock successfully updated; using server(s) ntp.psn.ru ntp.incaf.net ntp.incaf.net
ntp5.tamu.edu calvus.rzs-hm.si.
07:30:24 smoothwall System clock successfully updated; using server(s) at.pool.ntp.org ntpl.demon.co.uk no.pool.ntp.org
ntp.cyber-fleet.net uk.pool.ntp.org.
08:30:05 smoothwall System clock successfully updated; using server(s) time.nrc.ca tick.tanac.net sushi.compsci.lyon.edu
tk1.ihug.co.nz es.pool.ntp.org.
09:30:05 smoothwall System clock successfully updated; using server(s) ntp.incaf.net time.deakin.edu.au ntp.ip.ro
tk1.ihug.co.nz no.pool.ntp.org.
10:30:05 smoothwall System clock successfully updated; using server(s) gilbreth.ecn.purdue.edu no.pool.ntp.org time.nrc.ca
ntp3.cs.wisc.edu ntps.net4u.it.
11:30:02 smoothwall System clock successfully updated; using server(s) dk.pool.ntp.org sushi.compsci.lyon.edu
ntp.incaf.net ntp.karpo.cs sh2.ntp.carnet.hr.
12:30:22 smoothwall System clock successfully updated; using server(s) ntp.cs.strath.ac.uk ntp.shim.org
gilbreth.ecn.purdue.edu si.pool.ntp.org es.pool.ntp.org.
13:30:02 smoothwall System clock successfully updated; using server(s) tk1.ihug.co.nz sushi.compsci.lyon.edu
ch.pool.ntp.org ntp.cs.strath.ac.uk clock.psu.edu.
14:30:06 smoothwall System clock successfully updated; using server(s) sh2.ntp.carnet.hr fartein.ifi.uio.no
tick.nap.com.ar ntp.cs.strath.ac.uk tick.nap.com.ar.
15:30:25 smoothwall System clock successfully updated; using server(s) ntpl.demon.co.uk ntp.cyber-fleet.net
dk.pool.ntp.org time.nrc.ca ntpl.demon.co.uk.
16:30:03 smoothwall System clock successfully updated; using server(s) us.pool.ntp.org my.pool.ntp.org ntp2.mainecoon.com
ph.pool.ntp.org de.pool.ntp.org.
17:30:03 smoothwall System clock successfully updated; using server(s) ntp5.tamu.edu ntp.public.otago.ac.nz
ntp2b.audiotel.com.mx at.pool.ntp.org ntp.ucsd.edu.
18:30:03 smoothwall System clock successfully updated; using server(s) clock.psu.edu at.pool.ntp.org au.pool.ntp.org
ntp2.cs.wisc.edu

```





## Web Proxy Log Viewer

Check logs for the web proxy service.

**Settings:**

Month:  Day:  Source IP:

Ignore filter:  Enable ignore filter:

Log		Website
Time	Source IP	
	Older	Newer

## Firewall Log Viewer

Check logs for attempted access to your network from outside hosts. Connections listed here **have** been blocked.

### Settings:

Month:

April

Day:

17

### Firewall log:

Time	In	Out	Proto		Source	Src Port	Destination	Dst Port
20:00:26	eth1	-	TCP	<input type="checkbox"/>	145.254.179.217	3958	<input type="checkbox"/> 220.245.222.74	445(MICROSOFT-DS)
20:00:29	eth1	-	TCP	<input type="checkbox"/>	145.254.179.217	3958	<input type="checkbox"/> 220.245.222.74	445(MICROSOFT-DS)
20:00:32	eth1	-	TCP	<input type="checkbox"/>	220.245.144.68	3143	<input type="checkbox"/> 220.245.222.74	445(MICROSOFT-DS)
20:00:35	eth1	-	TCP	<input type="checkbox"/>	145.254.179.217	3958	<input type="checkbox"/> 220.245.222.74	445(MICROSOFT-DS)
20:00:35	eth1	-	TCP	<input type="checkbox"/>	220.245.144.68	3143	<input type="checkbox"/> 220.245.222.74	445(MICROSOFT-DS)
20:00:35	eth1	-	UDP	<input type="checkbox"/>	61.172.249.201	43187	<input type="checkbox"/> 220.245.222.74	1026
20:00:35	eth1	-	UDP	<input type="checkbox"/>	61.172.249.201	43187	<input type="checkbox"/> 220.245.222.74	1027
20:00:52	eth1	-	TCP	<input type="checkbox"/>	220.159.13.11	3331	<input type="checkbox"/> 220.245.222.74	135
20:00:55	eth1	-	TCP	<input type="checkbox"/>	220.159.13.11	3331	<input type="checkbox"/> 220.245.222.74	135
20:01:27	eth1	-	TCP	<input type="checkbox"/>	220.245.145.204	3354	<input type="checkbox"/> 220.245.222.74	445(MICROSOFT-DS)
20:01:30	eth1	-	TCP	<input type="checkbox"/>	220.245.145.204	3354	<input type="checkbox"/> 220.245.222.74	445(MICROSOFT-DS)
20:02:38	eth1	-	TCP	<input type="checkbox"/>	220.245.244.115	2325	<input type="checkbox"/> 220.245.222.74	445(MICROSOFT-DS)
20:02:40	eth1	-	TCP	<input type="checkbox"/>	220.245.244.115	2325	<input type="checkbox"/> 220.245.222.74	445(MICROSOFT-DS)
20:03:13	eth1	-	TCP	<input type="checkbox"/>	60.240.58.125	3914	<input type="checkbox"/> 220.245.222.74	445(MICROSOFT-DS)
20:03:16	eth1	-	TCP	<input type="checkbox"/>	60.240.58.125	3914	<input type="checkbox"/> 220.245.222.74	445(MICROSOFT-DS)
20:05:42	eth1	-	TCP	<input type="checkbox"/>	211.120.176.5	3853	<input type="checkbox"/> 220.245.222.74	445(MICROSOFT-DS)
20:05:45	eth1	-	TCP	<input type="checkbox"/>	211.120.176.5	3853	<input type="checkbox"/> 220.245.222.74	445(MICROSOFT-DS)
20:05:48	eth1	-	TCP	<input type="checkbox"/>	83.24.89.50	2680	<input type="checkbox"/> 220.245.222.74	445(MICROSOFT-DS)
20:05:51	eth1	-	TCP	<input type="checkbox"/>	83.24.89.50	2680	<input type="checkbox"/> 220.245.222.74	445(MICROSOFT-DS)

SmoothWall firewall log  
Date: 19 April

00:00:12	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=220.245.72.242	DST=220.245.222.74	LEN=48	TOS=0x00	PRE
00:00:15	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=220.245.72.242	DST=220.245.222.74	LEN=48	TOS=0x00	PRE
00:00:46	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=61.172.244.164	DST=220.245.222.74	LEN=411	TOS=0x00	PF
00:01:08	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=220.245.204.78	DST=220.245.222.74	LEN=48	TOS=0x00	PRE
00:01:11	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=220.245.204.78	DST=220.245.222.74	LEN=48	TOS=0x00	PRE
00:03:52	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=218.83.155.71	DST=220.245.222.74	LEN=411	TOS=0x00	PRE
00:04:14	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=200.43.175.3	DST=220.245.222.74	LEN=48	TOS=0x00	PREC
00:04:16	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=220.245.176.235	DST=220.245.222.74	LEN=48	TOS=0x00	PF
00:05:18	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=61.172.249.201	DST=220.245.222.74	LEN=583	TOS=0x00	PF
00:05:59	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=220.245.248.118	DST=220.245.222.74	LEN=48	TOS=0x00	PF
00:06:02	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=220.245.248.118	DST=220.245.222.74	LEN=48	TOS=0x00	PF
00:07:38	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=220.245.95.26	DST=220.245.222.74	LEN=48	TOS=0x00	PREC
00:07:41	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=220.245.95.26	DST=220.245.222.74	LEN=48	TOS=0x00	PREC
00:08:01	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=219.93.220.82	DST=220.245.222.74	LEN=48	TOS=0x00	PREC
00:08:08	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=219.93.220.82	DST=220.245.222.74	LEN=48	TOS=0x00	PREC
00:08:40	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=213.186.240.61	DST=220.245.222.74	LEN=48	TOS=0x00	PRE
00:08:43	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=213.186.240.61	DST=220.245.222.74	LEN=48	TOS=0x00	PRE
00:08:45	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=60.240.153.192	DST=220.245.222.74	LEN=48	TOS=0x00	PRE
00:08:47	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=81.131.150.247	DST=220.245.222.74	LEN=48	TOS=0x00	PRE
00:08:48	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=60.240.153.192	DST=220.245.222.74	LEN=48	TOS=0x00	PRE
00:08:49	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=213.186.240.61	DST=220.245.222.74	LEN=48	TOS=0x00	PRE
00:08:49	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=81.131.150.247	DST=220.245.222.74	LEN=48	TOS=0x00	PRE
00:08:53	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=220.245.176.235	DST=220.245.222.74	LEN=48	TOS=0x00	PF
00:08:56	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=81.131.150.247	DST=220.245.222.74	LEN=48	TOS=0x00	PRE
00:08:56	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=220.245.176.235	DST=220.245.222.74	LEN=48	TOS=0x00	PF
00:08:57	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=222.111.77.55	DST=220.245.222.74	LEN=48	TOS=0x00	PREC
00:08:58	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=222.111.77.55	DST=220.245.222.74	LEN=48	TOS=0x00	PREC
00:09:00	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=222.111.77.55	DST=220.245.222.74	LEN=48	TOS=0x00	PREC
00:09:50	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=220.245.222.80	DST=220.245.222.74	LEN=48	TOS=0x00	PRE
00:09:53	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=220.245.222.80	DST=220.245.222.74	LEN=48	TOS=0x00	PRE
00:10:03	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=220.245.176.235	DST=220.245.222.74	LEN=48	TOS=0x00	PF
00:10:19	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=220.220.128.84	DST=220.245.222.74	LEN=48	TOS=0x00	PRE
00:10:22	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=220.220.128.84	DST=220.245.222.74	LEN=48	TOS=0x00	PRE
00:10:28	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=220.220.128.84	DST=220.245.222.74	LEN=48	TOS=0x00	PRE
00:10:55	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=220.245.177.19	DST=220.245.222.74	LEN=48	TOS=0x00	PRE
00:10:58	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=220.245.177.19	DST=220.245.222.74	LEN=48	TOS=0x00	PRE
00:12:09	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=220.217.241.243	DST=220.245.222.74	LEN=48	TOS=0x00	PF
00:12:12	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=220.217.241.243	DST=220.245.222.74	LEN=48	TOS=0x00	PF
00:14:08	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=220.245.204.78	DST=220.245.222.74	LEN=48	TOS=0x00	PRE
00:14:11	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=220.245.204.78	DST=220.245.222.74	LEN=48	TOS=0x00	PRE
00:14:16	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=220.184.65.2	DST=220.245.222.74	LEN=48	TOS=0x00	PREC
00:14:34	IN=eth1	OUT=	MAC=00:e0:18:1f:53:99:00:0f:3d:ce:ce:49:08:00	SRC=220.245.155.42	DST=220.245.222.74	LEN=48	TOS=0x00	PRE

## IDS Log Viewer

Check logs for potentially malicious attempted access to your network from outside hosts. Connections listed here **have not necessarily** been blocked — use the Firewall Log Viewer to confirm blocked access.

### Settings:

Month:

April

Day:

17

Update

Export

### Log

**Date:** 04/17 04:39:59 **Name:** (snort\_decoder) WARNING: TCP Data Offset is less than 5!  
**Priority:** n/a **Type:** n/a  
**IP info:** 221.14.148.19:0 -> 220.245.222.74:0  
**References:** none found

**Date:** 04/17 04:43:07 **Name:** WEB-IIS ISAPI .ida attempt  
**Priority:** 1 **Type:** Web Application Attack  
**IP info:** 201.138.98.121:62742 -> 220.245.222.74:80  
**References:** 1 2 3

**Date:** 04/17 04:43:07 **Name:** WEB-IIS cmd.exe access  
**Priority:** 1 **Type:** Web Application Attack  
**IP info:** 201.138.98.121:62742 -> 220.245.222.74:80  
**References:** none found

**Date:** 04/17 05:02:05 **Name:** ICMP PING CyberKit 2.2 Windows  
**Priority:** 3 **Type:** Misc activity  
**IP info:** 220.248.27.194:n/a -> 220.245.222.74:n/a  
**References:** 1

**Date:** 04/17 09:35:47 **Name:** WEB-IIS ISAPI .ida attempt  
**Priority:** 1 **Type:** Web Application Attack  
**IP info:** 61.218.225.12:4588 -> 220.245.222.74:80  
**References:** 1 2 3

**Date:** 04/17 09:35:47 **Name:** WEB-IIS cmd.exe access  
**Priority:** 1 **Type:** Web Application Attack





## IP Information

Perform a 'whois' lookup on an ip address or domain name.

### Whois lookup:

IP addresses or domain names:

### linux.org.au (digital.linux.org.au)

```
EW whois 2.9 by Bill Weinman (http://whois.bw.org/)
Copyright 1999-2001 William E. Weinman
Request: linux.org.au
whois server for *.au is whois.aunic.net ...
connecting to whois.aunic.net [203.18.56.30:43] ...
Domain Name:          linux.org.au
Last Modified:        19-Sep-2003 05:51:32 UTC
Registrar ID:         R00013-AR
Registrar Name:       Enetica
Status:               OK

Registrant:           Linux Australia Inc
Registrant ID:        ABN 56 987 117 479

Registrant R0ID:      C1335669-AR
Registrant Contact Name: Managing Committee
Registrant Email:     committee@linux.org.au

Tech ID:              C1028387-AR
Tech Name:            Gary Allpike
Tech Email:           spice@spice.net.au

Name Server:          linux.spice.net.au
Name Server IP:       203.31.127.100
Name Server:          orgo.progsoc.uts.edu.au
Name Server:          digital.linux.org.au
Name Server IP:       202.0.185.5
```



## IP Tools

Perform 'ping' and 'traceroute' network diagnostics.

**Select tool:**

Tool:  IP addresses or hostnames:

*(Dropdown menu options: Ping, Traceroute)*

```

83.136.68.62 (no-rev.ip62.intrascapenet)

PING 83.136.68.62 (83.136.68.62) from 220.245.222.74 : 56(84) bytes of data.
64 bytes from 83.136.68.62: icmp_seq=1 ttl=43 time=423 ms
64 bytes from 83.136.68.62: icmp_seq=2 ttl=43 time=452 ms
64 bytes from 83.136.68.62: icmp_seq=3 ttl=43 time=397 ms
64 bytes from 83.136.68.62: icmp_seq=4 ttl=43 time=436 ms
64 bytes from 83.136.68.62: icmp_seq=5 ttl=43 time=387 ms

--- 83.136.68.62 ping statistics ---
5 packets transmitted, 5 received, 0% loss, time 4035ms
rtt min/avg/max/mdev = 387.245/419.447/452.678/24.126 ms

```



## Secure Shell

Connect to your SmoothWall using a Java SSH applet (requires SSH to be **enabled**).

**Secure shell:**

```
SSH-1.99-OpenSSH_3.7.1p1
      Login & password accepted
Last login: Mon Apr  4 19:45:10 2005 from 192.168.0.7
[root@smoothwall root]#
```

Connected to 192.168.0.1 222 online



## Updates

See the latest updates and fixes available for your SmoothWall, and an installation history of updates previously applied.

### Installed updates:

ID	Title	Description	Released	Installed
001	fixes1 update	This update contains an updated kernel to version 2.4.24 to correct recently discovered, locally exploitable, vulnerabilities. It also corrects known issues and a problem with dynamic DNS.	2004-01-12	2005-02-26
002	fixes2 update	This update contains an updated kernel to version 2.4.25 to correct recently discovered, locally exploitable vulnerabilities.	2004-02-26	2005-02-26
003	fixes3 update	This update contains an updated kernel to version 2.4.26 to correct recently discovered, locally exploitable vulnerabilities. It also updates Apache and OpenSSL to correct several recently discovered vulnerabilities. In addition, it adds support for the latest SpeedTouch modem (revision 4). It also corrects issues with custom dyndns.org accounts.	2004-05-26	2005-02-26
004	fixes4 update	This update contains an updated kernel to version 2.4.27 to correct recently discovered, locally exploitable vulnerabilities. It also updates mod_ssl to correct a recently discovered vulnerability.	2004-08-10	2005-02-26
005	fixes5 update	This update contains an upgrade to Apache 1.3.33 as well as fixes to local timezone problems with Squid.	2005-01-06	2005-02-26
006	fixes6 update	This update contains an updated kernel to version 2.4.29 to correct recently discovered local vulnerability. This update also includes updates to Squid and TCP Dump to correct recently discovered vulnerabilities.	2005-02-10	2005-02-26



002	fixes2 update	corrects known issues and a problem with dynamic DNS. This update contains an updated kernel to version 2.4.25 to correct recently discovered, locally exploitable vulnerabilities.	2004-02-26	2005-02-26
003	fixes3 update	This update contains an updated kernel to version 2.4.26 to correct recently discovered, locally exploitable vulnerabilities. It also updates Apache and OpenSSL to correct several recently discovered vulnerabilities. In addition, it adds support for the latest SpeedTouch modem (revision 4). It also corrects issues with custom dyndns.org accounts.	2004-05-26	2005-02-26
004	fixes4 update	This update contains an updated kernel to version 2.4.27 to correct recently discovered, locally exploitable vulnerabilities. It also updates mod_ssl to correct a recently discovered vulnerability.	2004-08-10	2005-02-26
005	fixes5 update	This update contains an upgrade to Apache 1.3.33 as well as fixes to local timezone problems with Squid.	2005-01-06	2005-02-26
006	fixes6 update	This update contains an updated kernel to version 2.4.29 to correct recently discovered local vulnerability. This update also includes updates to Squid and TCP Dump to correct recently discovered vulnerabilities.	2005-02-10	2005-02-26

**Available updates:**  
All updates installed

**Install new update:**  
To install an update please upload the .tar.gz file below:

Upload update file:



## Modem Configuration

Apply specific AT string settings for your PSTN modem or ISDN TA.

**Modem configuration:**

Init: *	<input type="text" value="+++ATZ"/>	Hangup: *	<input type="text" value="ATH0"/>
Speaker on: *	<input type="text" value="ATM1"/>	Speaker off: *	<input type="text" value="ATM0"/>
Tone dial: *	<input type="text" value="ATDT"/>	Pulse dial: *	<input type="text" value="ATDP"/>
Connect timeout:	<input type="text" value="45"/>		

\* These fields may be blank.



## USB ADSL Firmware Upload

Upload firmware to enable use of an Alcatel/Thomson Speedtouch Home USB ADSL modem, nicknamed the 'frog' or 'stingray'. **Download the 'Speedtouch USB Firmware' tarball**, unpack it, and upload the mgmt.o file using this form.

**Alcatel SpeedTouch USB ADSL driver upload:**  
To utilise the Alcatel SpeedTouch USB modem you must upload the firmware to your SmoothWall box. Please download the tarball from Alcatel and then upload the file **mgmt.o** using the form below.

Upload file:



## Change Passwords

Change passwords for the 'admin' and 'dial' management interface users. This does not affect access by SSH.

**Admin user password:**

Password:  Again:

**Dial user password:**

Password:  Again:



## Backup

Use this page to create a backup floppy disk or floppy disk image file.

**Instructions on creating a backup disk or disk image:**  
Please insert a blank, formatted floppy disk in the SmoothWall computer's floppy disk drive before pressing the button to create the backup disk. This disk should be available when reinstalling or upgrading, in order for the saved configuration to be restored. It may take up to a minute to write the information to the floppy disk. Alternatively, you may create a floppy disk image file, which you can later write to a floppy disk.

Create backup floppy disk

Create backup floppy image file



## Shutdown / Restart

Shutdown or restart your SmoothWall — restarts are sometimes mandated by update installation.

**Shutdown:**



CLOSE THIS WINDOW X

# Online Help

## Shutdown Control

This page contains two buttons, "Shutdown" and "Reboot". When the machine has finished shutting down, SmoothWall will beep once indicating that you can disconnect the power. You should generally not have to reboot a SmoothWall, unless you have just applied a patch and it requires you to do so.

Alternatively, you can shutdown SmoothWall from the console. Press Ctrl+Alt+Del to start the shutdown sequence, as per the shutdown button. The machine will NOT reboot.

CLOSE THIS WINDOW X



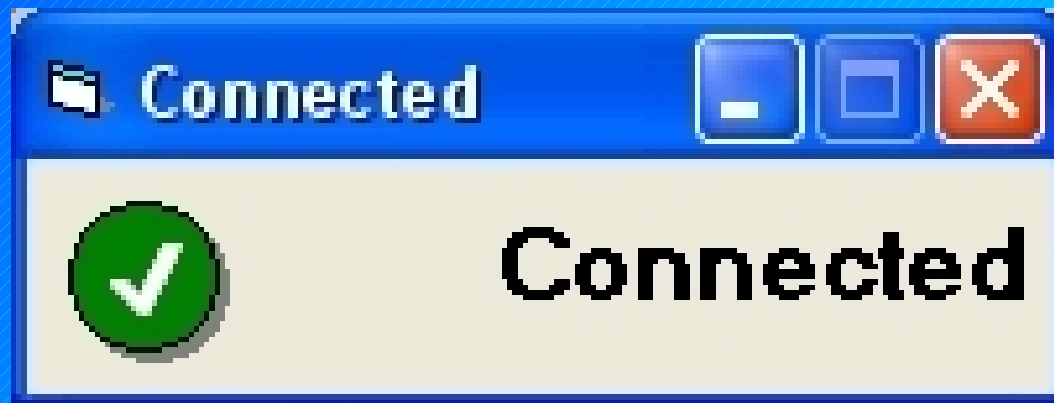
# Adding More Features

- Community mods (modifications)
  - No guarantees
- Beware of potential security implications



# Adding More Features

- Monitoring traffic
  - Traffic shaping
- Intrusion prevention
  - DansGuardian
- Automatic Updates
  - Windows systray app that checks the internet connection.



# Adding More Features

- <http://martybugs.net/smoothwall/>

The screenshot shows a Mozilla Firefox browser window titled "Martin's Smoothwall Express Info - Mozilla Firefox". The address bar contains "http://martybugs.net/smoothwall/". The page content includes:

- Navigation:** MartyBugs home, Smoothwall home
- Smoothwall info:** my box, connect speed display, red IP address display, bytes in/out, VNC over SSH, time sync, ad zapping, ip accounting on 0.9.9 / 1.0, ip accounting on 2.0, status LEDs, adding web users, iptables config, internal PPTP VPN, RRDTOol traffic graphs, password reset, proxy log analysis, RRDTOol memory graphs, Squid config, adding shell users, Smoothwall links
- modem config:** (partially visible)
- Introductory Information:**
  - Smoothwall Express** is an internet firewall, which allows you to protect your network, as well as providing NAT functionality. It is distributed under the GNU Public License, which allows free use and distribution.
  - Refer to the [Smoothwall.org](http://Smoothwall.org) website for more information on Smoothwall, including download links.
  - This site contains unofficial and unsupported information on modifying/customising your SmoothWall GPL/Express installation.
  - It's either information I've put together myself, or have linked to.
  - Note that if you modify your Smoothwall GPL/Express installation based on information found on this site, you can no longer expect support from the Smoothwall GPL/Express mailing list, the Smoothwall #help IRC channel on [irc.smoothwall1.org](http://irc.smoothwall1.org), or the Smoothwall [Community Forums](#).
  - Do not contact the Smoothwall developers for support on any of the information on this site - contact the person who documented that modification.
  - Ensure that you make a backup copy of any file on your Smoothwall before you make changes to it, so you can easily revert back to a known working configuration.
  - The vast majority of these modifications/enhancements should work fine on [IPCop](#) (a code-fork from Smoothwall) - with minimal changes to some of the directory names used in the various scripts.
  - Smoothwall Express 2.0 is now available - see [this thread](#) on the Smoothwall Community [Forums](#) for details of all known issues.
- Advertisements:**
  - SmoothWall Firewall Suite:** Affordable Enterprise Security Firewall, VPN, Content filtering. [www.smoothwall.net](http://www.smoothwall.net)
  - Vpn Firewall:** 1 Card LAN, VPN & building access. Unhackable and easy to deploy. [www.cryptocard.com](http://www.cryptocard.com)
  - Secure Your Network:** Sydney-based corporate firewall and network security specialists. [www.nullcube.com.au](http://www.nullcube.com.au)
  - WinGate VPN:** Powerful, easy to use VPN software. NAT traversal, built-in firewall. [www.wingate.com](http://www.wingate.com)

last updated 19 Sep 2004

Footer: [ MartyBugs home | about this site | copyright | disclaimer | privacy | appreciation | contact details | site map ]

Image © Martin Pot 2004, used with permission.

# Adding More Features

- SmoothWall Corporate Server
  - Has guarantees!!

# More Network Security

*Because security doesn't stop at the firewall*

- Only use required privileges
  - Anti-malware
- Securing Windows
  - Firefox
  - Thunderbird
  - File sharing
  - Floppy disks
- Common sense security
  - Move to Linux!!!

# Guaranteed Support

## SmoothWall Corporate Server

- More powerful out of the box
- Modular
- Global reseller & support network
- Ease of use, powerful product
- Pays & contributes to the open source project



# Summary

- Security doesn't have to be expensive
- SmoothWall makes it easier to secure a network
  - The firewall isn't the whole story



LCA 2005  
Security  
Miniconf



LCA 2005  
Security  
Miniconf

# Questions

- Smoothwall [www.smoothwall.org](http://www.smoothwall.org)
- SmoothWall Ltd [www.smoothwall.net](http://www.smoothwall.net)
- SmoothWall forums <http://community.smoothwall.org/forum>
- Best reference site for SmoothWall <http://martybugs.net>
- My Blog <http://smoothwallsamuel.blogspot.com>



Yes I Am  
Insane