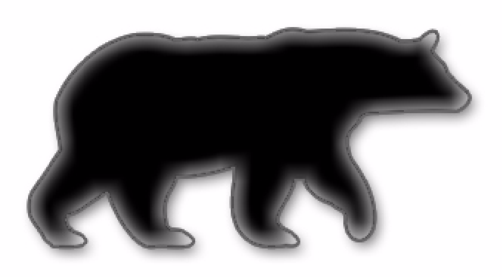


SmoothWall Express

Administrator's Guide

SmoothWall Express, Administrator's Guide, SmoothWall Limited, July 2007

Trademark and Copyright Notices

This document was created and published in the United Kingdom on behalf of the SmoothWall open source project by SmoothWall Limited.

Acknowledgements

We acknowledge the work, effort and talent of all those who have contributed to the SmoothWall open source project. For the latest team list, visit http://www.smoothwall.org/

We would particularly like to thank: Lawrence Manning and Gordon Allan, William Anderson, Jan Erik Askildt, Daniel Barron, Emma Bickley, Imran Chaudhry, Alex Collins, Dan Cuthbert, Bob Dunlop, Moira Dunne, Nigel Fenton, Mathew Frank, Dan Goscomb, Pete Guyan, Nick Haddock, Alan Hourihane, Martin Houston, Steve Hughes, Eric S. Johansson, Stephen L. Jones, Toni Kuokkanen, Luc Larochelle, Osmar Lioi, Richard Morrell, Piere-Yves Paulus, John Payne, Martin Pot, Stanford T. Prescott, Ralf Quint, Guy Reynolds, Kieran Reynolds, Paul Richards, Chris Ross, Scott Sanders, Emil Schweickerdt, Paul Tansom, Darren Taylor, Hilton Travis, Jez Tucker, Bill Ward, Rebecca Ward, Lucien Wells, Adam Wilkinson, Simon Wood, Nick Woodruffe, Marc Wormgoor.

Contents

Chapter 1

Welcome to SmoothWall Express

In this chapter:

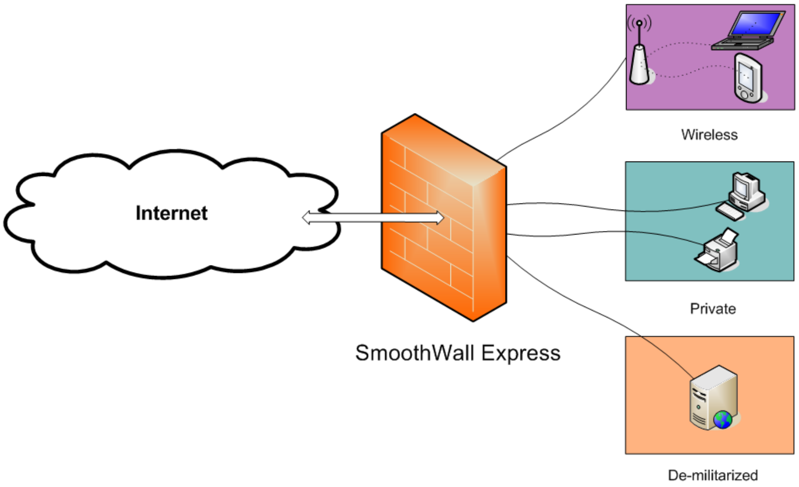
- An overview of SmoothWall Express
- About this documentation and who should read it
- Support information.

Welcome

Welcome to SmoothWall Express and secure Internet connectivity.

SmoothWall Express is an open source firewall distribution based on the GNU/Linux operating system. Designed for ease of use, SmoothWall Express is configured via a web-based GUI and requires absolutely no knowledge of Linux to install or use.

SmoothWall Express enables you to easily build a firewall to securely connect a network of computers to the Internet.



Almost any Pentium class PC can be used, for example, an old, low specification PC long redundant as a user workstation or server. SmoothWall Express creates a dedicated hardware firewall, offering the facilities and real security associated with hardware devices.

SmoothWall Express comes pre-configured to stop all incoming traffic that is not the result of an outgoing request. The rules files that implement this policy are part of the system configuration and should not normally be edited by other than the configuration procedure. Should any of the Linux system or configuration files be changed by other than SmoothWall Express configuration and installation procedures there is a risk of compromising security, for which the SmoothWall Project Team cannot be held responsible. However, we do not discourage people from experimenting with and further developing their SmoothWall Express system – it is just that we must point out that ill-conceived or badly executed changes might compromise the security of the SmoothWall Express system.

Who should read this guide?

Anyone maintaining and deploying SmoothWall Express should read this guide.

Other Documentation and User Information

SmoothWall Express Installation Guide contains information on system and hardware requirements and installing, migrating to and accessing SmoothWall Express for the first time.

- https://my.smoothwall.org/ – where you can create a my.SmoothWall profile, access documentation, sign up for newsletters and get fun stuff, themes and much more.

Need some help?

Support for SmoothWall Express is provided by way of mailing lists and forums accessible by visiting the SmoothWall Express community at: http://community.smoothwall.org/

This support is provided on an entirely voluntary basis by members of the SmoothWall Express Open Source community - nobody is paid to provide support for SmoothWall Express. Thus, the SmoothWall Express Open Source Project Team cannot be held responsible for the quality, accuracy or timeliness of the information provided by the volunteers who are kind enough to offer their time and knowledge to the benefit of others.

For those users, particularly commercial users, who want professional support, we recommend the use of the commercial products of SmoothWall Limited, which are fully supported by both SmoothWall Limited and its world-wide network of re-sellers. For further details see SmoothWall Limited's web site at: http://www.smoothwall.net/

Chapter 2

SmoothWall Express Overview

In this chapter:

- Security concepts used by SmoothWall Express
- How to access SmoothWall Express
- An overview of the pages used to configure and manage SmoothWall Express.

Security Concepts

SmoothWall Express supports a De-Militarized Zone (DMZ), a network normally used for servers that need to be accessible from the Internet, such as mail and web servers.

By default SmoothWall Express blocks all traffic to hosts and servers behind SmoothWall Express that originates from the Internet. If external users need to use servers behind SmoothWall Express then access to these servers has to be specifically unblocked - see *Chapter 3, Controlling Network Traffic* on page 13 for details.

Obviously, the less un-blocking that is configured, the more secure the firewall. It is better that such un-blocking is limited to the DMZ network, where the information stored is not highly confidential.

Keep private and confidential information on servers and hosts within the local (green) network that cannot be accessed from the Internet.

Be very careful about un-blocking traffic going from the Internet (red) to the local (green) network as you are opening a potential hole for hackers.

Unlike many firewalls, SmoothWall Express does not support Telnet connections to gain access to the configuration and management facilities. This is considered to be unsafe by the designers.

Normally, you should use an encrypted https connection to configure and manage SmoothWall Express. You can also enable Secure Shell access to SmoothWall Express allowing login using either the root or setup user account. Do not enable this facility when it is not needed – the less that is enabled the better from a security viewpoint.

Remember SmoothWall Express is only part of a security solution. There is little point in having the most impenetrable front door in the world yet the back door is left wide open. Security is a specialist area; experience, knowing what to look for, understanding how hackers and crackers operate, being up to date with the latest security threats etc. Commercial networks should be subjected to regular security audit and penetration testing.

SmoothWall Limited strongly recommends that all computers, especially public Internet facing servers, are kept up-to-date with all available security patches from the suppliers of the system software. This particularly applies to SmoothWall Express itself – please check regularly that all available security updates have been applied.

Accessing SmoothWall Express

Note: The following sections assume that you have followed the instructions in the *SmoothWall Express Installation Guide* and successfully connected to the Internet.

To access SmoothWall Express:

1 In the browser of your choice, enter the address of your SmoothWall Express, for example:

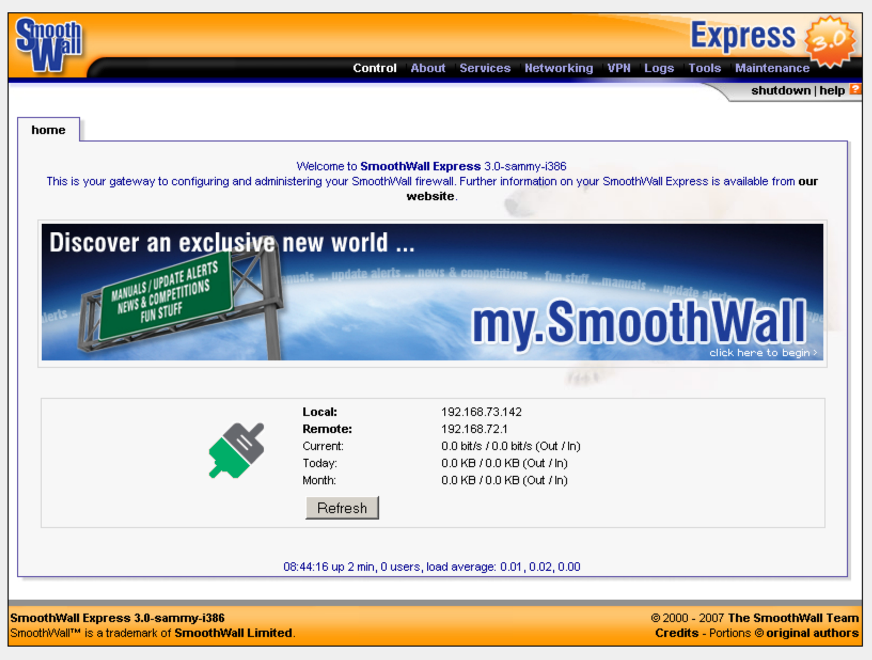
```
https://192.168.110.1:441
```

Note: The example address uses HTTPS to ensure secure communication with your SmoothWall Express. It is possible to use HTTP on port 81 if you are satisfied with less security.

2 Accept SmoothWall Express's certificate. When prompted, enter the following information:

Field	Information
Username	Enter `admin`. This is the name of the default SmoothWall Express administrator account.
Password	Enter the password you specified for the admin account when installing SmoothWall Express.

3 Click **Login**.The home page opens:



Welcome to **SmoothWall Express** 3.0-sammy-i386
This is your gateway to configuring and administering your SmoothWall firewall. Further information on your SmoothWall Express is available from **our website**.

Local: 192.168.73.142
Remote: 192.168.72.1
Current: 0.0 bit/s / 0.0 bit/s (Out / In)
Today: 0.0 KB / 0.0 KB (Out / In)
Month: 0.0 KB / 0.0 KB (Out / In)

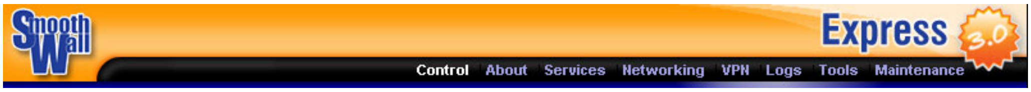
08:44:16 up 2 min, 0 users, load average: 0.01, 0.02, 0.00

SmoothWall Express 3.0-sammy-i386
SmoothWall™ is a trademark of **SmoothWall Limited**.
© 2000 - 2007 **The SmoothWall Team**
Credits - Portions © **original authors**

The following sections describe SmoothWall Express's sections and pages.

SmoothWall Express Sections and Pages

A navigation bar is displayed at the top of every page. It contains links to SmoothWall Express's sections and pages.



The following sections give an overview of SmoothWall Express's default sections and pages.

Control

The control section contains the following pages:

Pages	Description
home	SmoothWall Express's default home page which displays network and connection information, for more information, see *Chapter 8, Home* on page 63.

About

The about section contains the following sub-sections and pages:

Pages	Description
status	Displays a list of SmoothWall Express core and optional services, for more information, see *Chapter 8, Status* on page 64.
advanced	Displays information on memory, disk usage, hardware, modules and more, for more information, see *Chapter 8, Advanced* on page 65.
traffic graphs	Displays traffic statistics, for more information, see *Chapter 8, Traffic Graphs* on page 66.
bandwidth bars	Displays realtime usage of bandwidth, for more information, see *Chapter 8, Bandwidth Bars* on page 67.
traffic monitor	Displays recent, realtime usage of bandwidth, for more information, see *Chapter 8, Traffic Monitor* on page 68.
my smoothwall	Displays SmoothWall Express development information and enables you to, optionally, register your SmoothWall Express, for more information, see *Chapter 8, Your SmoothWall Express* on page 69.

Services

The services section contains the following pages:

Pages	Description
web proxy	This is where you configure and enable SmoothWall Express’s web proxy service, for more information, see *Chapter 6, Using the Web Proxy* on page 39.
im proxy	This is where you configure and enable SmoothWall Express’s instant messaging proxy service, for more information, see *Chapter 6, Configuring Instant Messaging Proxy* on page 42.
pop3 proxy	This is where you configure and enable SmoothWall Express’s POP3 proxy service, for more information, see *Chapter 6, AV Scanning the POP3 Proxy* on page 43.
dhcp	This is where you configure and enable SmoothWall Express’s Dynamic Host Configuration Protocol (dhcp) service, to automatically allocate LAN IP addresses to your network clients, for more information, see *Chapter 6, Configuring the DHCP Service* on page 45.
sip proxy	This is where you configure the SIP proxy service, for more information, see *Chapter 6, Configuring the SIP Proxy* on page 44.
dynamic dns	This is where you can configure SmoothWall Express to manage and update dynamic Domain Name System (dns) names from popular services, for more information, see *Chapter 6, Dynamic DNS* on page 48.
static dns	This is where you can add static DNS entries to SmoothWall Express’s in-built DNS server, for more information, see *Chapter 6, Static DNS* on page 50.
ids	This is where you enable the Snort IDS service to detect potential security breach attempts from outside your network, for more information, see *Chapter 6, Managing the Intrusion Detection System* on page 51.
remote access	This is where you enable secure shell access to SmoothWall Express, and restrict access based on referral URLs, for more information, see *Chapter 6, Configuring Remote Access* on page 52.
time	Here you can configure time zones, time and date, time synchronisation and enable SmoothWall Express’s time server, for more information, see *Chapter 6, Configuring Time Settings* on page 53.

Networking

The networking section contains the following pages:

Pages	Description
incoming	Here you forward traffic on ports from your external IP address to ports on clients on your local network(s). For more information, see *Chapter 3, Port Forwarding Incoming Traffic* on page 13.
outgoing	Here you can create rules to control local clients' access to external services. For more information, see *Chapter 3, Controlling Outgoing Traffic* on page 15.
internal	This is where you can enable access from a host on your orange or purple networks to a port on a host on your Green network. For more information, see *Chapter 3, Controlling Internal Traffic* on page 18.
external access	Here you can set up connections from external machines to specified ports on SmoothWall Express. For more information, see *Chapter 3, Managing Access to Services* on page 20.
ip block	This is where you create rules to prevent access from specified IP addresses or networks. For more information, see *Chapter 3, Selectively Blocking IPs Addresses* on page 21.
timed access	This is where you configure when clients on your protected network may have access to the external network or Internet. For more information, see *Chapter 3, Configuring Timed Access to the Internet* on page 22.
qos	Here you can prioritise the different types of traffic on your network. For more information, see For more information, see *Chapter 3, Managing Quality of Service for Traffic* on page 23.
advanced	This is where you can advanced networking features. For more information, see *Chapter 3, Configuring Advanced Network Options* on page 24.
ppp settings	This is where you configure modem, ADSL and ISDN connections. For more information, see *Chapter 3, Configuring Dial-up Connections* on page 26.
interfaces	Here you configure NIC IP addresses, DNS and gateway settings. For more information, see *Chapter 3, Working with Interfaces* on page 29.

VPN

The VPN section contains the following pages:

Pages	Description
control	Here you manage VPN connections. For more information, see *Chapter 4, Working with VPNs* on page 31.
connections	Here you create, edit and manage VPN connections. For more information, see *Chapter 4, Creating VPN Connections* on page 31.

Logs

The Logs section contains the following pages:

Pages	Description
system	Contains logged system information for SmoothWall Express, including: DHCP, IPSec, updates and core kernel activity. For more information, see *Chapter 8, Accessing System Logs* on page 70.
web proxy	Contains logged web proxy information for SmoothWall Express. For more information, see *Chapter 8, Web Proxy Logs* on page 71.
firewall	Contains logged information on attempted access to your network stopped by SmoothWall Express. For more information, see *Chapter 8, Firewall Logs* on page 72.
ids	Contains logged information on potentially malicious attempted access to your network. For more information, see *Chapter 8, IDS Logs* on page 73.
instant messages	Displays logged instant messaging conversations in realtime. For more information, see *Chapter 8, Instant Messages Logs* on page 74.
email	Contains logged information on the emails passing though the POP3 proxy and anti-virus engine. For more information, see *Chapter 8, Email Logs* on page 75.

Tools

The Tools section contains the following pages:

Pages	Description
ip information	Here you can run a whois lookup on an IP address or domain name. For more information, see *Chapter 5, Whois – Getting IP Information* on page 35.
ip tools	Here you can run ping and traceroute network diagnostics. For more information, see *Chapter 5, Using IP Tools* on page 35.
shell	Here you can connect to SmoothWall Express using a Java SSH applet. For more information, see *Chapter 5, Running the SSH Client* on page 37.

Maintenance

The Maintenance section contains the following pages:

Pages	Description
updates	Displays the latest updates and fixes available for SmoothWall Express, and an installation history of updates previously applied. For more information, see *Chapter 7, Updating SmoothWall Express Software* on page 55.

Pages	Description
modem	Here you can apply specific settings for your PSTN modem or ISDN TA. For more information, see *Chapter 7, Configuring Modems* on page 57.
speedtouch usb firmware	Here you can upload firmware to enable SmoothWall Express to use the Alcatel/ Thomson Speedtouch Home USB ADSL modem. For more information, see *Chapter 7, Using Speedtouch USB ADSL Modems* on page 58.
passwords	This is where you manage administrator and dial account passwords. For more information, see *Chapter 7, Managing Passwords* on page 59.
backup	Here you can backup your SmoothWall Express settings. For more information, see *Chapter 7, Configuring Backups* on page 60.
preferences	Here you can configure the SmoothWall Express user interface. For more information, see *Chapter 7, Setting User Interface Preferences* on page 61.
shutdown	Here you can shut down or reboot SmoothWall Express. For more information, see *Chapter 7, Shutting down/Restarting SmoothWall Express* on page 61.

Configuration Conventions

The following sections explain how to enter suitable values for frequently required settings.

IP Addresses

An IP address defines the network location of a single network host. The following format is used:

```
192.168.10.1
```

IP Address Ranges

An IP address range defines a sequential range of network hosts, from low to high. IP address ranges can span subnets. Examples:

```
192.168.10.1-192.168.10.20
192.168.10.1-192.168.12.255
```

Subnet Addresses

A network or subnet range defines a range of IP addresses that belong to the same network. The format combines an arbitrary IP address and a network mask, and can be entered in two ways:

```
192.168.10.0/255.255.255.0
192.168.10.0/24
```

Netmasks

A netmask defines a network or subnet range when used in conjunction with an arbitrary IP address. Some pages allow a network mask to be entered separately for ease of use. Examples:

```
255.255.255.0
```

```
255.255.0.0
255.255.248.0
```

Service and Ports

A service or port identifies a particular communication port in numeric format. For ease of use, a number of well known services and ports are provided in Service drop-down lists. To use a custom port number, choose the User defined option from the drop-down list and enter the numeric port number into the adjacent User defined field. Examples:

```
21
7070
```

Port Ranges

A port range can be entered into most User defined port fields, in order to describe a sequential range of communication ports from low to high.

The following format is used:

```
137:139
```

Connecting via the Console

You can access SmoothWall Express via a console using the Secure Shell (SSH) protocol.

Note: By default, SmoothWall Express only allows SSH access if it has been specifically configured. See *Chapter 6, Configuring Remote Access* on page 52 for more information.

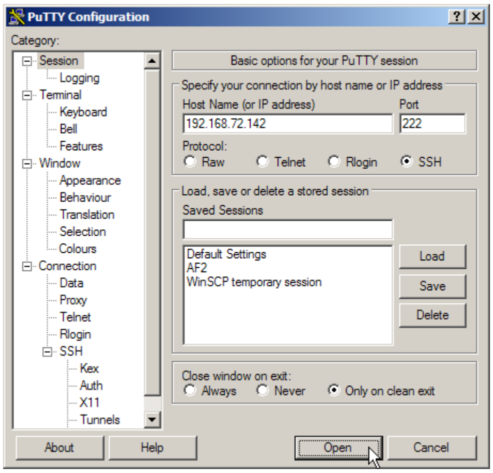
Connecting Using a Client

When SSH access is enabled, you can connect to SmoothWall Express via a secure shell application, such as PuTTY.

To connect using an SSH client:

1 Check SSH access is enabled on SmoothWall Express, see *Chapter 6, Configuring Remote Access* on page 52.

2 Start PuTTY or an equivalent client:



Host Name (or IP address): 192.168.72.142
Port: 222
Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH
Saved Sessions:
Default Settings
AF2
WinSCP temporary session
Close window on exit: ○ Always ○ Never ● Only on clean exit

3 Enter the following information:

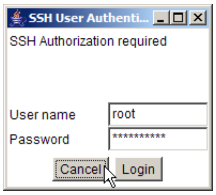
Field	Description
Host Name (or IP address)	Enter SmoothWall Express's host name or IP address.
Port	Enter `222`
Protocol	Select **SSH**.

4 Click **Open**. When prompted, enter `root`, and the password associated with it. You are given access to the SmoothWall Express command line.

Connecting Using Web-based SSH

To connect via the web-based SSH:

1 Navigate to the **tools > shell** page:



SSH Authorization required

User name: root

Password: **********

2 Enter the username `root`, and the password associated with it. As a root user, you will access the SmoothWall Express command line.

Chapter 3

Controlling Network Traffic

In this chapter:

- Managing incoming and outgoing traffic
- Controlling internal traffic and access to services
- Blocking specific IP
- Configuring timed access to the Internet
- Managing Quality of Service (QoS)
- Configuring Dial-up Connections
- Working with interfaces.

Port Forwarding Incoming Traffic

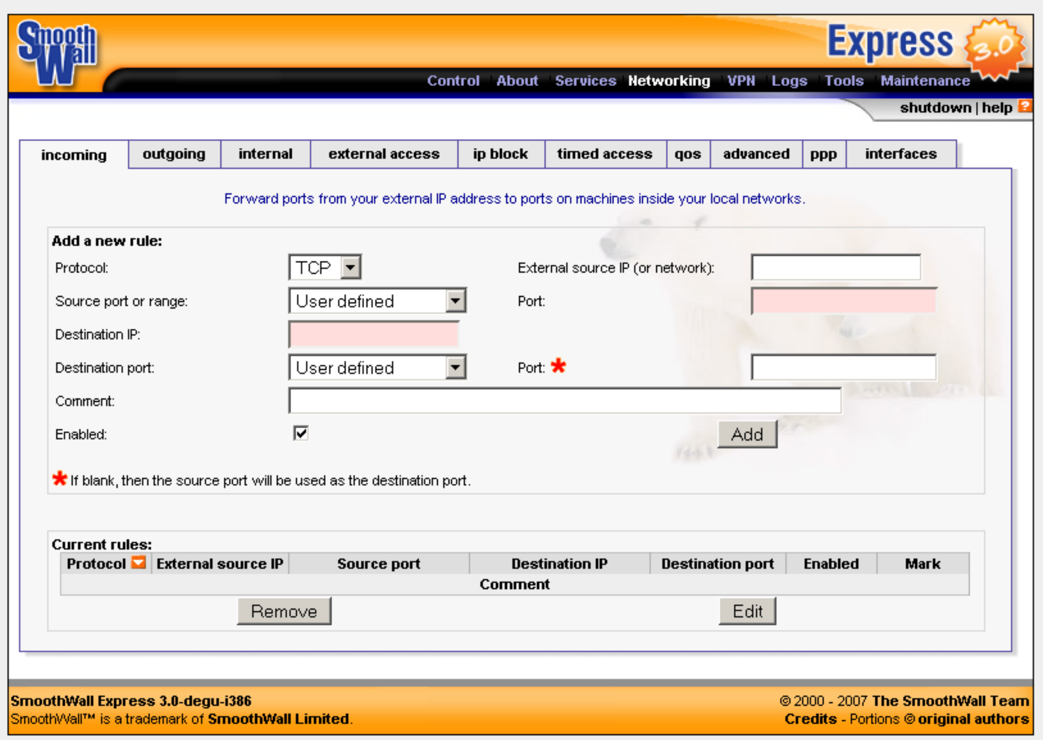
SmoothWall Express, by default, blocks all traffic that comes from the red interface. Therefore, all IP addresses/ports with traffic you want to allow through, must have a port forward rule configured.

You can create a list of port forwarding rules, where traffic arriving at a port on the red (Internet) interface is forwarded to another IP address and port, normally in the DMZ (orange) but potentially within the local (green) protected network.

Port forward rules are usually used to allow servers within the DMZ to communicate with the outside world on the Internet without exposing their IP address or more services or ports than is necessary. Small networks behind a dial-up or ISDN link are unlikely to use this facility.

To create a port forwarding rule:

1 Browse to the **Networking > incoming** page:


Smooth Wall
Express 3.0
Control About Services Networking VPN Logs Tools Maintenance
shutdown | help
incoming outgoing internal external access ip block timed access qos advanced ppp interfaces
Add
Remove
Edit

Forward ports from your external IP address to ports on machines inside your local networks.

Add a new rule:

Protocol:	TCP	External source IP (or network):	
Source port or range:	User defined	Port:	
Destination IP:			
Destination port:	User defined	Port: *	
Comment:			
Enabled:	☑		

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

Current rules:

Protocol	External source IP	Source port	Destination IP	Destination port	Enabled	Mark

Comment

SmoothWall Express 3.0-degu-i386
SmoothWall™ is a trademark of SmoothWall Limited.
© 2000 - 2007 The SmoothWall Team
Credits - Portions © original authors

2 Configure the following settings:

Setting	Description
Protocol	Select one of the following: **TCP** – The default protocol **UDP** – the connection-less UDP protocol.
External source IP (or network)	Specify which external IP or network can send traffic to the specified destination IP. Or, leave this field empty if all traffic to the destination IP is to be allowed, for example a publicly accessible web server. Each permitted network or IP address requires its own rule.
Source port or range	Specify which port on the source IP address the traffic will be coming from. For example, port 80, the standard HTTP port number, would normally be specified for traffic to be forwarded to a web server. It is not logical or sensible to allow traffic on other ports through to the web server, the less that is allowed through the firewall, the more secure will be the servers and networks behind it.

Setting	Description
Port	Each rule must contain either a single port number, or a port range specified as two port numbers separated by a colon (:) character. For example, 123:456 would forward all ports from 123 through to an including 456. Except for the colon separator character, port numbers must be numeric and have a value of less than 65536.
Destination IP	Specify the IP address in the DMZ or the local (green) network where the traffic is to be forwarded to. **Note:** Forwarding ports to the local (green) network is not generally recommended – publicly accessible servers should be located in the DMZ if at all possible.
Destination port	From the drop-down menu, select the destination port. Or, select User defined.
Port	If User defined is selected as the destination port, enter a destination port. Normally, this will be the same as the source port; e.g. port 80 goes to port 80 for a web server. However, it is not uncommon to use non-standard port numbers for security reasons. SmoothWall Express uses port 81 for HTTP access to these configuration pages. If the Destination Port is left blank then it will be set to the same port or port range as the source port.
Comment	Optionally, enter a comment describing this rule.
Enabled	Select to enable the rule.

3 Click **Add** and the information will be transferred to the Current rules section below. The rule takes effect immediately.

Editing and Removing Rules

To edit or remove a rule:

1 In the Current rules area, select the rule and click **Edit** or **Remove**.

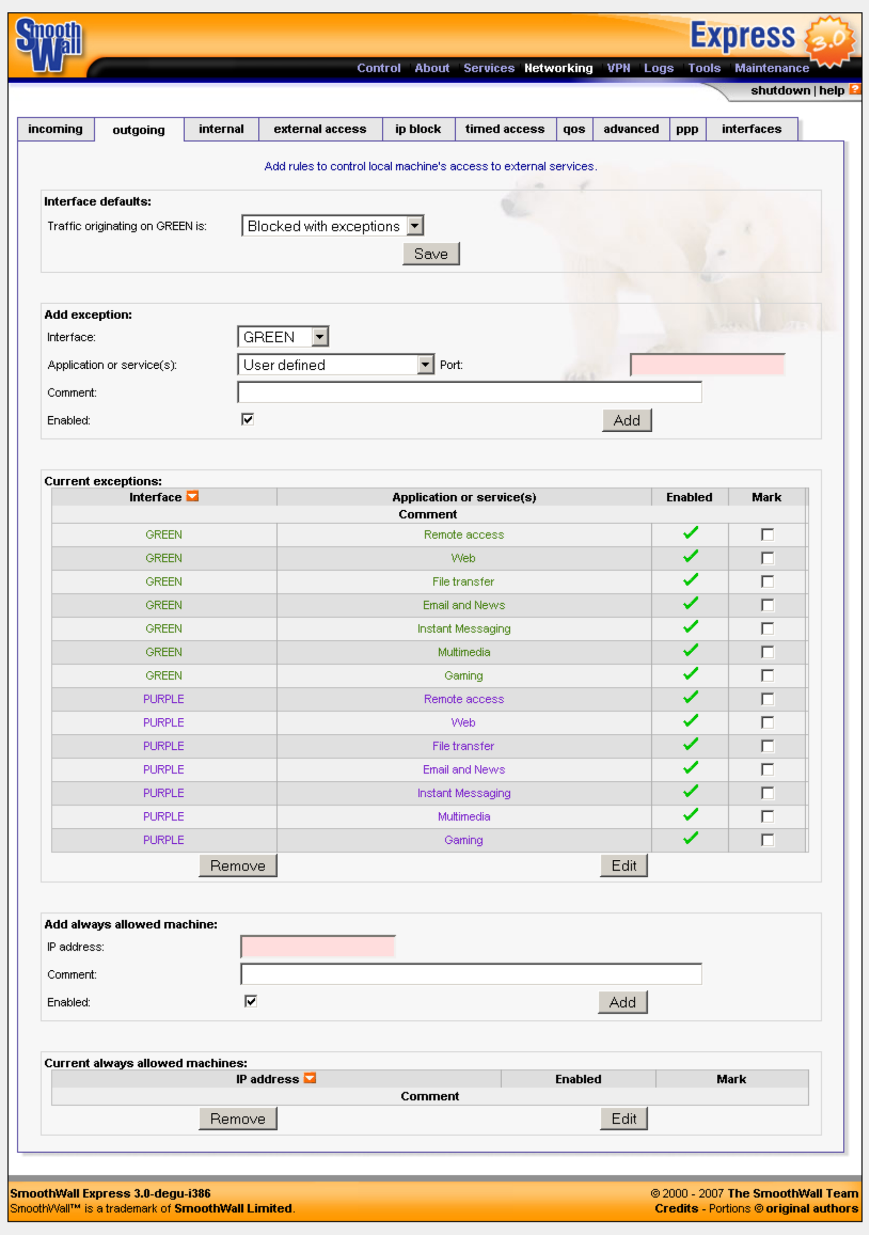
Controlling Outgoing Traffic

You can allow, disable or limit access to the Internet based on each internal interface. In addition, you can specify a list of IP address which are not subject to any blocking.

Default access is determined when SmoothWall Express is installed and is either Open, all traffic is allowed onto the Internet, Half-open, some traffic is allowed, with the rest being blocked or Closed, all traffic being blocked unless you explicitly add a rule to allow it.

To create an outgoing access rule:

1 Browse to the **Networking > outgoing** page:



Smooth Wall
Express 3.0
Control About Services Networking VPN Logs Tools Maintenance
shutdown | help
incoming outgoing internal external access ip block timed access qos advanced ppp interfaces

Add rules to control local machine's access to external services.

Interface defaults:

Traffic originating on GREEN is: Blocked with exceptions

Save

Add exception:

Interface: GREEN

Application or service(s): User defined Port:

Comment:

Enabled: ☑ Add

Current exceptions:

Interface Comment	Application or service(s)	Enabled	Mark
GREEN	Remote access	✓	□
GREEN	Web	✓	□
GREEN	File transfer	✓	□
GREEN	Email and News	✓	□
GREEN	Instant Messaging	✓	□
GREEN	Multimedia	✓	□
GREEN	Gaming	✓	□
PURPLE	Remote access	✓	□
PURPLE	Web	✓	□
PURPLE	File transfer	✓	□
PURPLE	Email and News	✓	□
PURPLE	Instant Messaging	✓	□
PURPLE	Multimedia	✓	□
PURPLE	Gaming	✓	□

Remove Edit

Add always allowed machine:

IP address:

Comment:

Enabled: ☑ Add

Current always allowed machines:

IP address Comment	Enabled	Mark

Remove Edit

SmoothWall Express 3.0-degu-i386
SmoothWall™ is a trademark of SmoothWall Limited.
© 2000 - 2007 The SmoothWall Team
Credits - Portions © original authors

2 Configure the following settings:

Setting	Description
Traffic originating ...	In the Interface defaults area, locate the interface you want to configure traffic for and select from the following options: **Blocked with exceptions** – Block all traffic originating on the interface except for the exceptions listed in the current exceptions area. **Allowed with exceptions** – Allow all traffic originating on the interface except for the exceptions listed in the current exceptions area. Click **Save** to save your selection.

Setting	Description
Interface	To add an exception, select from the following options: **GREEN** – Select to add an exception for traffic on the green interface. **ORANGE** – Select to add an exception for traffic on the orange interface. **PURPLE** – Select to add an exception for traffic on the purple interface.
Application or service(s)	From the drop-down list, select the application, service or user defined option.
Port	If you select User defined as the application or service, enter the applicable port.
Comment	Optionally, enter a description of the rule.
Enabled	Select to enable the rule.

3 Click **Add**. The rule is added to the list in the Current exceptions area.

Always Allow Traffic

You can always allow certain clients access to the Internet.

To always allow outgoing traffic:

1 Browse to the **Networking > outgoing** page.

2 In the Add always allowed machine area, configure the following settings:

Setting	Description
IP address	Enter the IP address of the client you want to always allow access to the Internet.
Comment	Optionally, enter a description of the rule.
Enabled	Select to enable the rule.

3 Click **Add**. The rule is added to the list in the Current always allowed machines area.

Editing and Removing Rules

To edit or remove a rule:

1 In the Current rules area, select the rule and click **Edit** or **Remove**.

Controlling Internal Traffic

It is possible to configure ‘holes’ between the DMZ (orange network) and the local (green) network on the internal page to allow and manage internal traffic. The standard configuration, without any holes configured, blocks any host in the DMZ from connecting to a host on the local (green) network.

Every hole you open is a potential security risk and the name pinhole implies the size of the hole that should be opened.

There may be good reasons for doing so, for example, where web servers located in the DMZ need to access back-end SQL database servers on the local network. Another example is where external (facing) mail servers in the DMZ relay messages to internal mail servers on the local network.

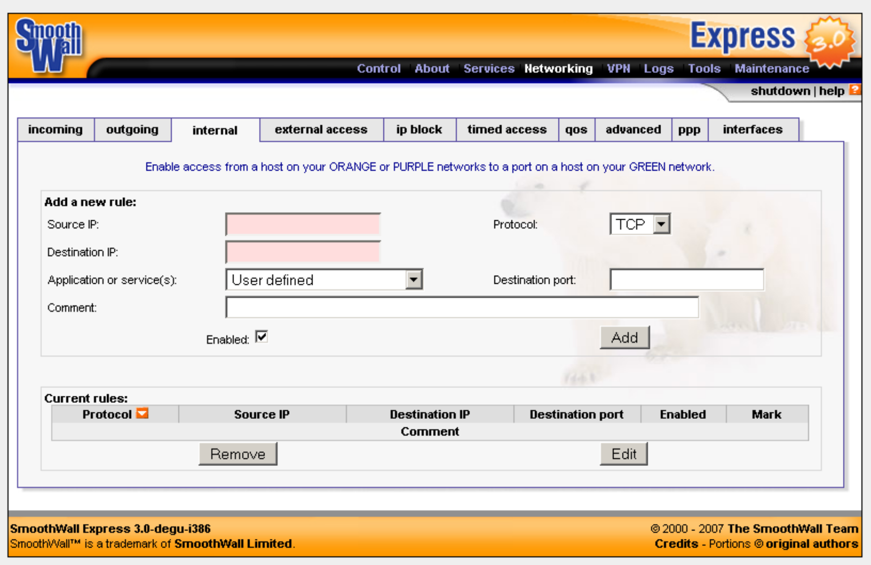
Note: The internal page only applies to networks where a De-Militarized Zone (DMZ) is configured on the orange interface.

The standard configuration, without any pinholes setup, is as follows:

- Green can talk to purple and orange
- Purple can talk to orange
- Orange can talk to nothing
- By default, all interfaces can talk to red and the Internet. This will depend, of course, on how you configure outgoing filtering.

To create a pinhole and allow traffic internally:

1 Browse to the **Networking > internal** page:



Enable access from a host on your ORANGE or PURPLE networks to a port on a host on your GREEN network.

Add a new rule:

Source IP:

Destination IP:

Application or service(s): User defined

Comment:

Protocol: TCP

Destination port:

Enabled: ☑

Current rules:

Protocol	Source IP	Destination IP	Destination port	Enabled	Mark
		Comment			

SmoothWall Express 3.0-degu-i386
SmoothWall™ is a trademark of SmoothWall Limited.

© 2000 - 2007 The SmoothWall Team
Credits - Portions © original authors

2 Configure the following settings:

Setting	Description
Source IP	Specify the IP address of the server in the DMZ (orange) network that needs to communicate with a host on the local (green) network.

Setting	Description
Protocol	From the drop-down list, select the protocol to use: **TCP** – for TCP/IP, but can be set for the connection-less UDP protocol **UDP** – for a PING pinhole. **Note:** UDP pinholes are best avoided as the connection-less UDP protocol represents a greater security risk than does TCP.
Destination IP	Specify the IP address on the local (green) network which is to receive the traffic from the Source IP address.
Application or service(s)	From the drop-down list, select the application, service or user defined port.
Destination port	If user defined is selected, enter which port on the destination IP address is to receive the traffic.
Comment	Optionally, enter a description.
Enabled	Select to enable the traffic.

3 Click **Add**. The rule is listed in the Current rules area.

Editing and Removing Rules

To edit or remove a rule:

1 In the Current rules area, select the rule and click **Edit** or **Remove**.

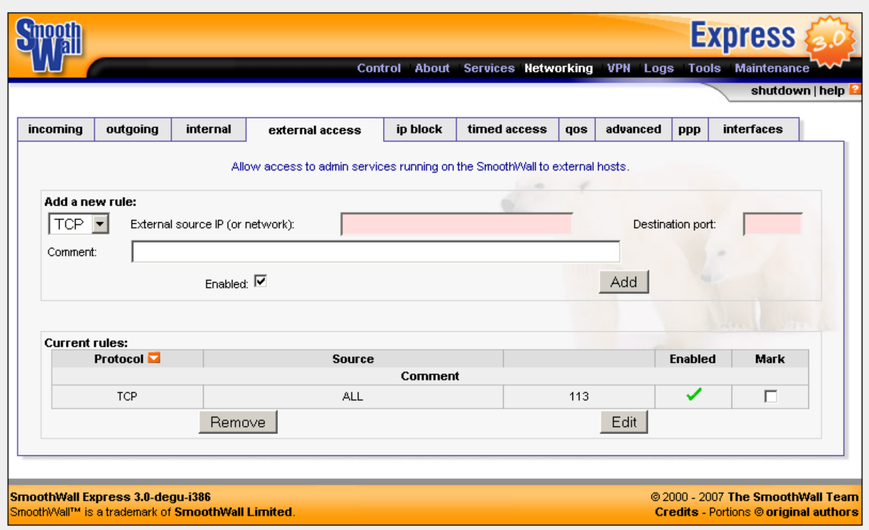
Managing Access to Services

You can set up a list of allowed connections from external computers to your network via IP address/ports on the Internet (red) interface. This is typically used to grant HTTP, HTTPS or SSH access for remote administration of SmoothWall Express.

Ports opened for forwarding are not affected by the settings on this page.

To manage access to services:

1 Browse to the **Networking > external access** page:



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

Add a new rule:

TCP External source IP (or network): Destination port:

Comment:

Enabled: ☑ Add

Current rules:

Protocol	Source		Enabled	Mark
	Comment			
TCP	ALL	113	✓	□

Remove Edit

SmoothWall Express 3.0-degu-i386
SmoothWall™ is a trademark of SmoothWall Limited.

© 2000 - 2007 The SmoothWall Team
Credits - Portions © original authors

2 Configure the following settings:

Setting	Description
Protocol	Select from the following: **TCP** – The default protocol. **UDP** – The connection-less UDP protocol.
External source IP (or network)	Enter the IP address of the external source allowed to access admin services running on SmoothWall Express. We strongly advise that you specify only one known and trusted remote computer to use to administer gain or root access to SmoothWall Express – this will stop anybody else being able to open the port.
Destination port	Enter the port on SmoothWall Express which will accept data from the specified source address. All other ports will be blocked. For HTTPS specify port 441, for SSH specify port 222. **Note:** External access using HTTP is not recommended because this protocol does not encrypt the data.
Comment	Optionally, enter a description.
Enabled	Select to enable the rule.

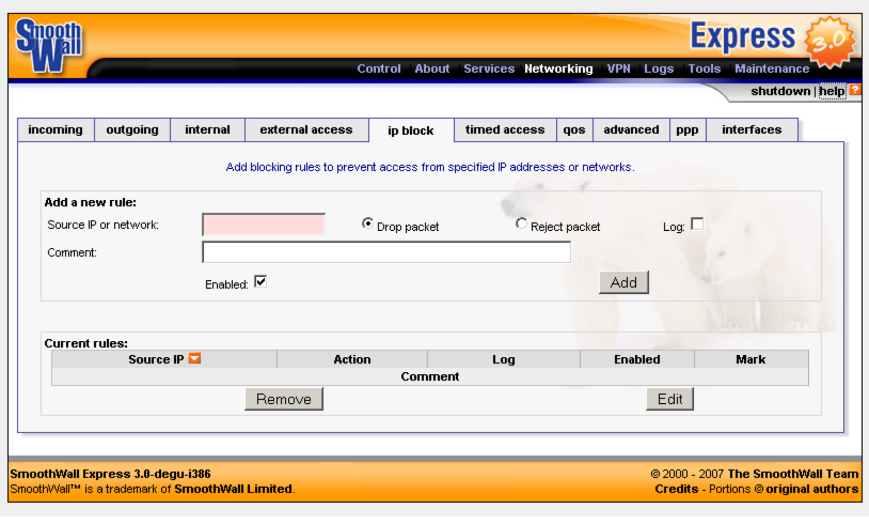
3 Click **Add**. The rule is listed in the Current rules are.

Selectively Blocking IPs Addresses

You can selectively block external IP addresses from accessing SmoothWall Express and any machines behind it.

To block external IP addresses:

1 Browse to the **Networking > ip block** page:



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: □

Comment:

Enabled: ☑

Current rules:

Source IP	Action	Log	Enabled	Mark
Comment				

SmoothWall Express 3.0-degu-i386
SmoothWall™ is a trademark of SmoothWall Limited.

© 2000 - 2007 The SmoothWall Team
Credits - Portions © original authors

2 Configure the following settings:

Setting	Description
Source IP or network	Enter the remote source IP of the machine you want to block.
Drop packet	Select to drop packet: and completely ignore any request from the specified IP.
Reject packet	Select to reject the packet. In this mode, an ICMP Connection Refused message will be sent to the originating IP, but no connection will be possible.
Log	Select to log activity.
Comment	Optionally, enter a description of what the rule is for.
Enabled	Select to enable the rule.

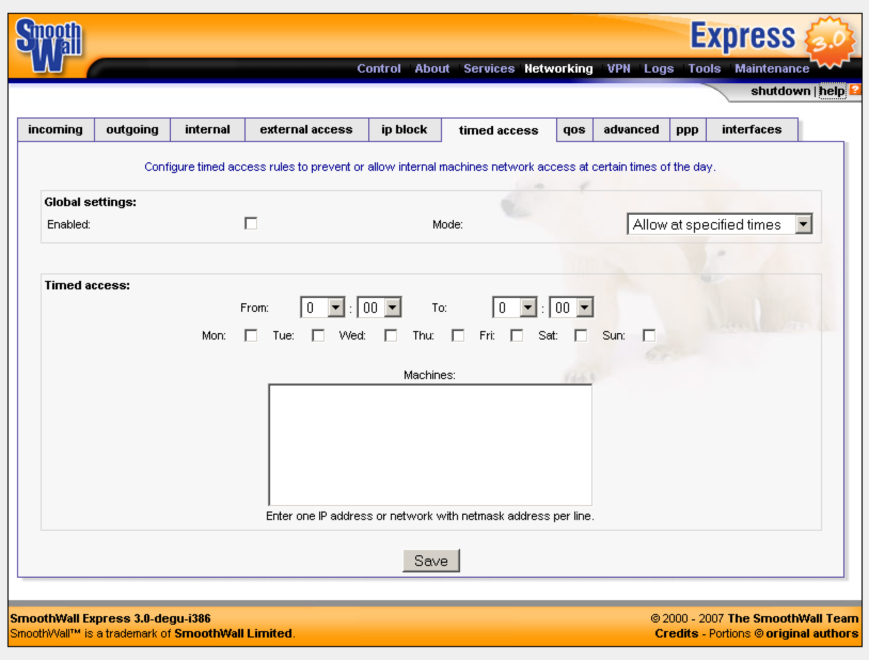
3 Click **Add**. The rule is added to the Current rules area.

Configuring Timed Access to the Internet

SmoothWall Express can allow or disallow Internet access at certain times of the day, for a specified group of clients.

To configure timed access to the Internet:

1 Browse to the **Networking > timed access** page:


Express 3.0
Control About Services Networking VPN Logs Tools Maintenance
shutdown | help
incoming outgoing internal external access ip block timed access qos advanced ppp interfaces

Configure timed access rules to prevent or allow internal machines network access at certain times of the day.

Global settings:
Enabled: □ Mode: Allow at specified times

Timed access:
From: 0 : 00 To: 0 : 00
Mon: □ Tue: □ Wed: □ Thu: □ Fri: □ Sat: □ Sun: □

Machines:
Enter one IP address or network with netmask address per line.

Save

SmoothWall Express 3.0-degu-i386
SmoothWall™ is a trademark of **SmoothWall Limited**.
© 2000 - 2007 **The SmoothWall Team**
Credits - Portions © **original authors**

2 Configure the following settings:

Setting	Description
Enabled	Select to enable the settings.
Mode	From the drop-down list, select from the following options: **Allow at specified times** – Internet access is allowed at the specified times. **Reject at specified times** – Internet access is blocked at the specified times.
From – To	Select from when to when and the days of the week to allow or block Internet access.
Machines	Enter one IP address or network with netmask per line.

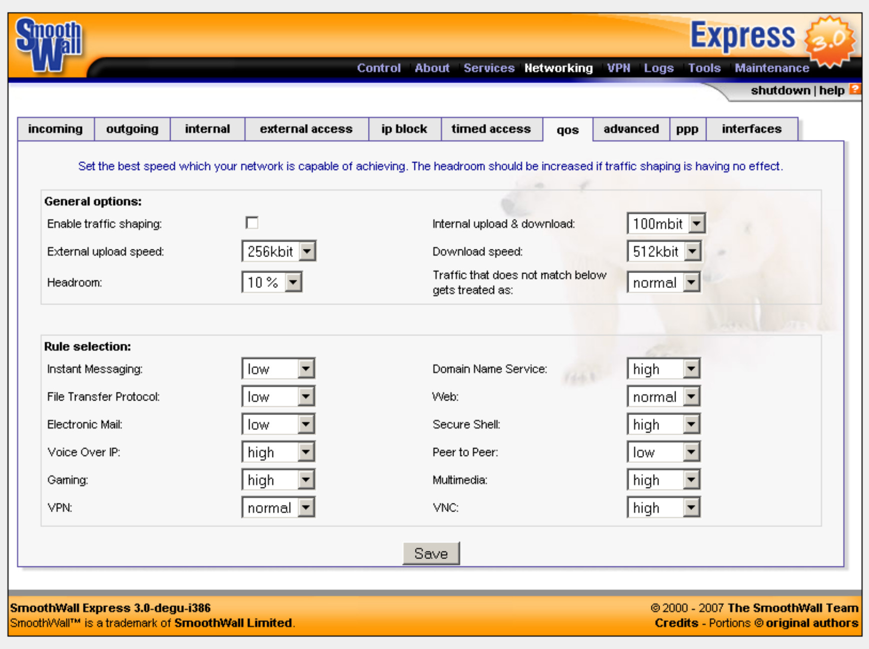
3 Click **Save**.

Managing Quality of Service for Traffic

You can ensure traffic quality of service (QoS) by prioritising traffic in SmoothWall Express.

To manage qos:

1 Browse to the **Networking > qos** page:



Set the best speed which your network is capable of achieving. The headroom should be increased if traffic shaping is having no effect.

General options:

Enable traffic shaping:	□	Internal upload & download:	100mbit
External upload speed:	256kbit	Download speed:	512kbit
Headroom:	10 %	Traffic that does not match below gets treated as:	normal

Rule selection:

Instant Messaging:	low	Domain Name Service:	high
File Transfer Protocol:	low	Web:	normal
Electronic Mail:	low	Secure Shell:	high
Voice Over IP:	high	Peer to Peer:	low
Gaming:	high	Multimedia:	high
VPN:	normal	VNC:	high

SmoothWall Express 3.0-degu-i386
SmoothWall™ is a trademark of SmoothWall Limited.

© 2000 - 2007 The SmoothWall Team
Credits - Portions © original authors

2 Configure the following settings:

Setting	Description
Enable traffic shaping	Select to enable QoS.
Internal upload & download	From the drop-down list, select the speed of your internal upload and download connections.
External upload speed	From the drop-down list, select the speed of your external upload connection.
Download speed	From the drop-down list, select the speed of your download connection.
Headroom	Accept the default or, from the drop-down list, select the amount of headroom required for SmoothWall Express to handle fluctuating traffic levels.
Traffic that does not match below gets treated as	From the drop-down list, select how to handle traffic types that are not listed in the Rule selection area.

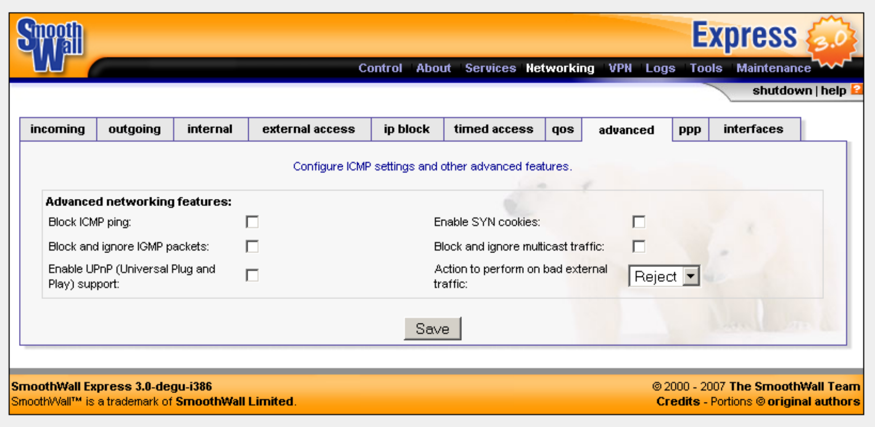
Setting	Description
Rule selection	Accept the default priorities for the services, traffic and protocols listed, or, adjust them to suit your requirements. The following priority levels are available: **none** – traffic is treated as specified by the Traffic that does not match below gets treated as option, see above for more information **slow** – force traffic to go slow even if the connection is empty **low** – traffic use up to 40% of the available connection but if there is other traffic on the connection this is limited to 15% **normal** – traffic can use 90% of the capacity of the connection if the connection is empty and at least 40% in busier conditions **high** – traffic can use 90% of an otherwise empty connection and is guaranteed 20% if the connection is busy. Traffic prioritised as high has first call on any spare capacity.

Configuring Advanced Network Options

SmoothWall Express can be configured to manage Internet Control Message Protocol (ICMP) and other advanced network options.

To manage qos:

1 Browse to the **Networking > advanced** page:



Configure ICMP settings and other advanced features.

Advanced networking features:

Block ICMP ping: □

Block and ignore IGMP packets: □

Enable UPnP (Universal Plug and Play) support: □

Enable SYN cookies: □

Block and ignore multicast traffic: □

Action to perform on bad external traffic: Reject

SmoothWall Express 3.0-degu-i386
SmoothWall™ is a trademark of **SmoothWall Limited**.

© 2000 - 2007 **The SmoothWall Team**
Credits - Portions © **original authors**

2 Configure the following settings:

Setting	Description
Block ICMP ping	Select to stop SmoothWall Express responding to PING messages from either the Internet or from the local network.
Enable SYN cookies	Select to enable SYN cookies as a defence mechanism against SYN Flood attacks, and avoid a Denial of Service (DOS) situation where SmoothWall Express is too busy to do any real work.

Setting	Description
Block and ignore IGMP packets	Select to block and ignore Internet Group Management Protocol (IGMP) packets. This reduces spurious messages in your log files.
Block and ignore multicast traffic	Select to block multi-cast messages and stop them being logged.
Enable UPnP (Universal Plug and Play) support	Select to enable support for Universal Plug and Play (UPnP) clients.
Action to perform on bad external traffic	From the drop-down list, select how to handle traffic that is not forwarded. The options available are: **Reject** – Reply with a port unreachable ICMP message. **Note:** This will make it easier for an attacker to determine what ports SmoothWall Express has open. **Drop** – Do not reply. The attacker will have a harder time finding open ports on SmoothWall Express. **Tip:** For maximum stealth ability, combine Drop with Block ICMP ping.

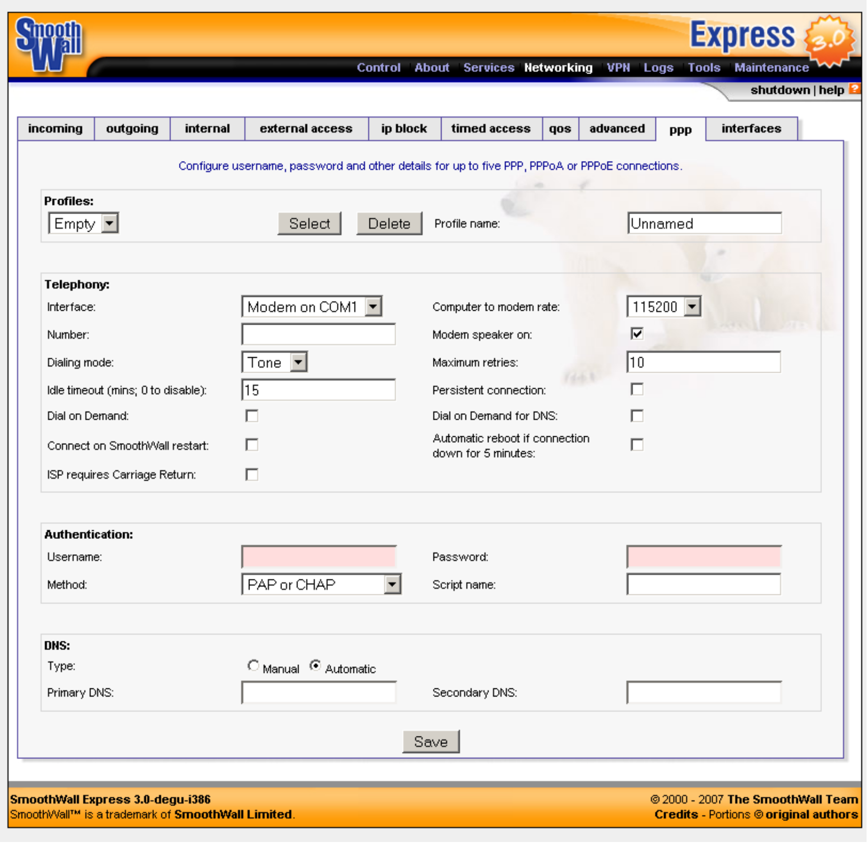
3 Click **Save** to save the settings.

Configuring Dial-up Connections

You can configure up to five different dial-up connections that can be used to connect SmoothWall Express to an ISP via ISDN, USB ADSL or an analogue modem.

To configure a dial-up connection:

1 Browse to the **Networking > ppp** page:



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

Profiles:

Empty		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:	

SmoothWall Express 3.0-degu-i386
SmoothWall™ is a trademark of SmoothWall Limited.
© 2000 - 2007 The SmoothWall Team
Credits - Portions © original authors

Note: The settings available depend on the type of connection you are configuring.

2 Consult the connection information your ISP has provided and then enter the following information:

Setting	Information
Profile name	Enter a descriptive name for the connection.
Interface	From the drop-down list, depending on the type of connection you are creating, select one of the following: **Modem on COM** – the modem and the COM port it is on **Single ISDN** – if your connection uses single ISDN **Dual ISDN** – if your connection uses dual ISDN **PPPoE** – if your connection is Point-to-Point Protocol over Ethernet **ADSL** – if your connection uses an ADSL modem.

Setting	Information
Computer to modem rate	The default is usually sufficient and ensures that modems with data compression capabilities run at their maximum possible speed. **Note:** Old 486 PCs may need this rate to be reduced to 57,600 bits/second.
Number	Enter your ISP's dial-in access modem number.
Modem speaker on	Select to turn on the modem speaker, if it has one.
Dialing mode	From the drop-down list, select the dialling mode used by your telephone exchange.
Maximum retries	Accept the default number or enter a different number of failed dial attempts before SmoothWall Express stops trying to connect. After this number, SmoothWall Express will not try to dial again until you click Dial on the Control > home page. **Note:** This number applies even if the Persistent connection option is enabled.
Idle timeout (mins; 0 to disable)	Determines the length of inactivity before SmoothWall Express drops the connection when used in non-persistent connections. The default is 15 minutes. Set this option to zero (0), to disable it. **Note:** When disabled, you will have to disconnect and hang-up manually.
Persistent connection	Select to enable SmoothWall Express to keep the link to your ISP up and available for use all of the time – if the connection drops, it will automatically be re-dialled.
Dial on Demand	Select to configure SmoothWall Express to automatically connect to the ISP detailed in the current profile whenever a user on the network initiates a connection to the Internet. **Note:** If dial on demand is enabled and your Internet connection is charged on a per minute basis, you may get an unpleasant surprise when the next telephone bill arrives! **Note:** You still have to click Connect on the Control > home page to start SmoothWall Express.
Dial on Demand for DNS	Select to configure SmoothWall Express to dial up to the Internet each time a DNS request is made by any machine on the local network – this can happen a lot when reading e-mail with embedded HTML, for example. **Note:** If not selected, SmoothWall Express will not dialup to the Internet each time a DNS request is made, but only when a specific connection is requested. This is one simple way to help reduce telephone charges when the ISP connection is one that is paid for on a per minute basis.
Connect on SmoothWall restart	Select to configure SmoothWall Express to automatically connect to the ISP after being rebooted.

Setting	Information
Automatic reboot if connection down for 5 minutes	Select to configure SmoothWall Express to automatically reboot if the red interface is detected as being down for 5 minutes. This option is primarily intended for users of Alcatel USB ADSL modems which appear not to automatically reconnect in some circumstances. **Note:** This option cannot be used in conjunction with Dial on Demand.
ISP requires Carriage Return	Select this option if your ISP requires that the modem send a carriage return to signal it has finished sending.
Service name	For PPPoE connections, enter the name of the PPPoE service.
Concentrator name	For PPPoE connections, enter the name of the PPPoE concentrator.
Keep second channel up	For ISDN connections, select this option to control the action of the second data channel for high-speed, 128Kbit access. If the data throughput keeps changing, this may cause the ISDN channel to go up and down. Selecting this option will force the second channel to remain up, instead of automatically closing once the data-rate decreases below a threshold where the second channel is of no benefit.
Minimum time to keep second channel up (sec)	For ISDN connections, select this option to stop the second channel repeatedly going up and down due to the threshold being exceeded for short periods of time. You can enter a higher value to force the second channel to stay up for longer, so a momentary lull in the data traffic will not cause the second channel to go down.
Username	Enter the username supplied by your ISP.
Password	Enter the password supplied by your ISP.
Method	Select one of the following authentication methods: **PAP or CHAP** – this is the most common method used by ISPs **Standard login script** – uses a standard text-based login script **Demon login script** – uses the UK Demon Internet ISP's modified version of the standard login script to connect to Demon's authentication servers **Other login script** – enables you to use a custom login script if none of the other methods are suitable. **Note:** If you need this, you will need to login to SmoothWall Express as the root user and create the file in `/etc/ppp`
Script name	If you have selected the Other login script method, enter the script's name.
Type	Here you determine DNS details. Select form the following: **Manual** – enter the IP addresses of your ISP's DNS server **Automatic** – select if your ISP supports automatic DNS server configuration.

Setting	Information
Primary DNS	If you select Manual as the DNS type, enter the primary DNS server IP address.
Secondary DNS	Optionally, if you select Manual as the DNS type, enter the secondary DNS server IP address.

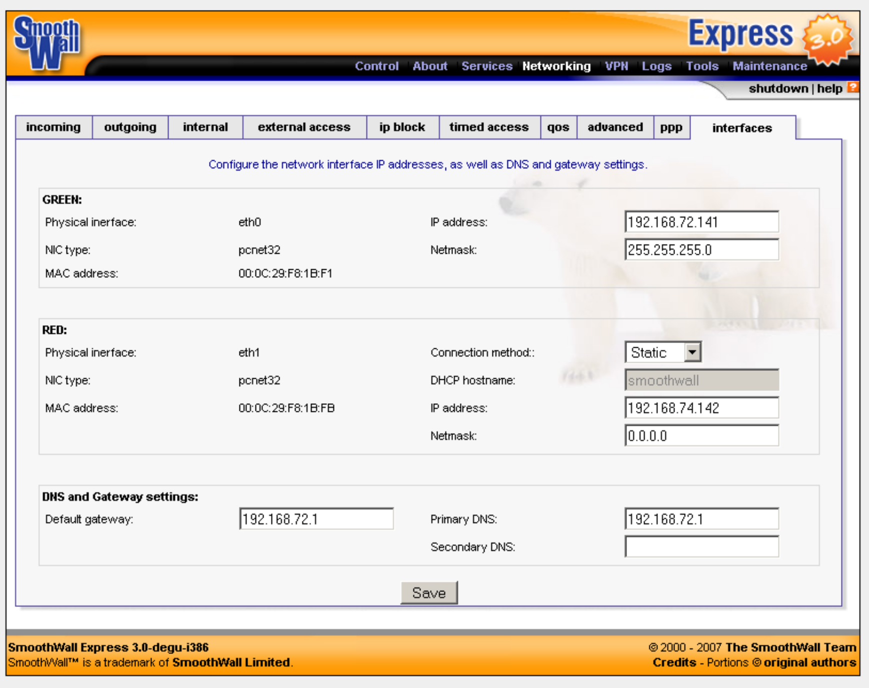
3 Click Save to save your settings and create the connection.

Working with Interfaces

You can configure and edit network interfaces, DNS and gateway settings.

To configure a network interface:

1 Browse to the Networking > interfaces pages, for example:



Configure the network interface IP addresses, as well as DNS and gateway settings.

GREEN:

Physical inerface: eth0
IP address: 192.168.72.141
NIC type: pcnet32
Netmask: 255.255.255.0
MAC address: 00:0C:29:F8:1B:F1

RED:

Physical inerface: eth1
Connection method:: Static
NIC type: pcnet32
DHCP hostname: smoothwall
MAC address: 00:0C:29:F8:1B:FB
IP address: 192.168.74.142
Netmask: 0.0.0.0

DNS and Gateway settings:

Default gateway: 192.168.72.1
Primary DNS: 192.168.72.1
Secondary DNS:

SmoothWall Express 3.0-degu-i386
SmoothWall™ is a trademark of **SmoothWall Limited**.
© 2000 - 2007 **The SmoothWall Team**
Credits - Portions © **original authors**

Note: The settings displayed here depend on the number of NICs in your system and/or the type of external connection you have configured.

2 For the interface you want to configure, enter the following information:

Setting	Description
IP address	For an internal interface, enter the IP address.
Netmask	For an internal interface, accept the default or enter a new netmask.

Setting	Description
Connection method:	To configure an external ethernet connection, you can select from the following connection methods: **Static** – Select this method if you want SmoothWall Express to use a static IP address that has been assigned by your Internet Service Provider (ISP). **DHCP** – Select this method if your ISP dynamically assigns you a different IP address each time you connect to the Internet. **PPPoE** – Select this method if your ISP uses Point-to-Point Protocol over Ethernet (PPPoE) to connect you to the Internet.
DHCP hostname	If you are using the DHCP connection method, enter the DHCP hostname.
IP address	If you are using the Static connection method, enter the IP address for the external interface.
Netmask	If you are using the Static connection method, enter the netmask for the external interface.
Default gateway	If you are using the Static connection method, enter the default gateway's IP address.
Primary DNS	If you are using the Static connection method, enter the IP address of the primary DNS.
Secondary DNS	Optionally, if you are using the Static connection method, enter the IP address of the secondary DNS.

3 Click **Save** to save your settings.

Working with VPNs

In this chapter:

- How to create and manage virtual private network (VPN) connections.

Creating VPN Connections

SmoothWall Express enables you to create Pre-Shared Key, IPSec VPN connections to other SmoothWall Express systems or IPSec-compliant hosts which have static IP addresses.

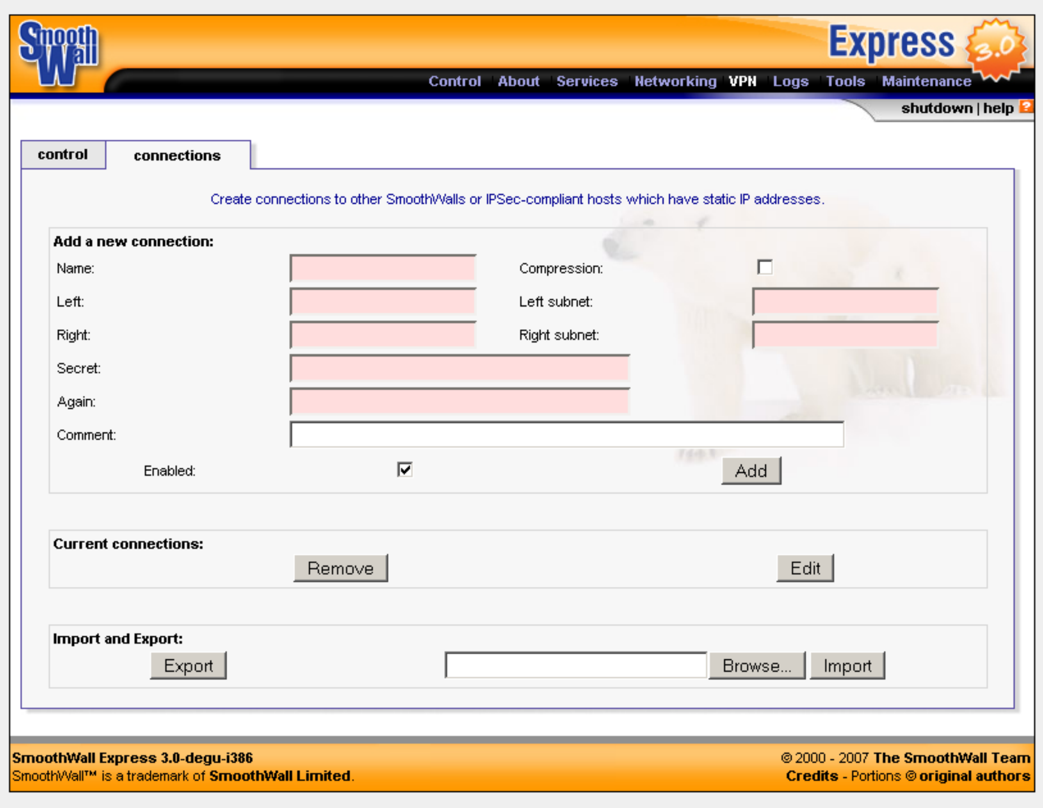
The following sections explain how to configure a connection between a local SmoothWall Express and a remote SmoothWall Express.

Configuring the Local SmoothWall Express

The following section explains how to configure the settings for the local SmoothWall Express and how to export the settings for use when configuring the remote SmoothWall Express.

To configure the local settings:

1 On the local SmoothWall Express, browse to the **VPN > connections** page:



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

Add a new connection:

Name:

Compression: □

Left:

Left subnet:

Right:

Right subnet:

Secret:

Again:

Comment:

Enabled: ☑

Current connections:

Import and Export:

SmoothWall Express 3.0-degu-i386
SmoothWall™ is a trademark of **SmoothWall Limited**.

© 2000 - 2007 **The SmoothWall Team**
Credits - Portions © **original authors**

2 Configure the following settings:

Setting	Description
Name	Enter a name for the connection. We suggest you use a meaningful name that relates to the left/right concept which identifies the ends of the VPN connection.
Compression	Select to enable data compression in the connection.
Left	Enter the public IP address of the SmoothWall Express on the left, local, end of the VPN connection. This must be the public IP address of the Internet (red) interface. Therefore, you need a static IP address from your ISP. **Note:** A dynamic IP address can work, but every time your ISP allocates a new IP address you will have to reconfigure the VPN connection.
Left subnet	Enter the network address of the subnet from which the VPN connection originates. Normally, this will be the local (green) network. This must be entered in the netmask format, `/16` for class B, `/24` for a normal class C subnet. For example, `192.168.1.0/24`. **Note:** Left and right subnets must have different network addresses.
Right	Enter the public IP address of the SmoothWall Express on the right, remote end of the VPN connection. This must be the public IP address of the Internet (red) interface. Therefore, you need a static IP address from your ISP. **Note:** A dynamic IP address can work, but every time your ISP allocates a new IP address you will have to reconfigure the VPN connection.
Right subnet	Enter the network address of the subnet to which the VPN connection goes. Normally, this will be the local (green) network. This must be entered in the / netmask format, `/16` for class B, `/24` for a normal class C subnet. For example, `192.168.1.0/24`. **Note:** Left and right subnets must have different network addresses.
Secret	Enter a secret string to exchange between the two SmoothWall Express systems to authenticate the connection. This secret should be at least twenty characters long and contain a mixture of lower and upper case letters and numerics. **Note:** It's a good idea to use a string you can remember.
Again	Re-enter the string to confirm it.
Comment	Optionally, enter information on the connection for future reference.
Enabled	Select to enable the connection.

3 Click **Add** to add the connection to the list of current connections.

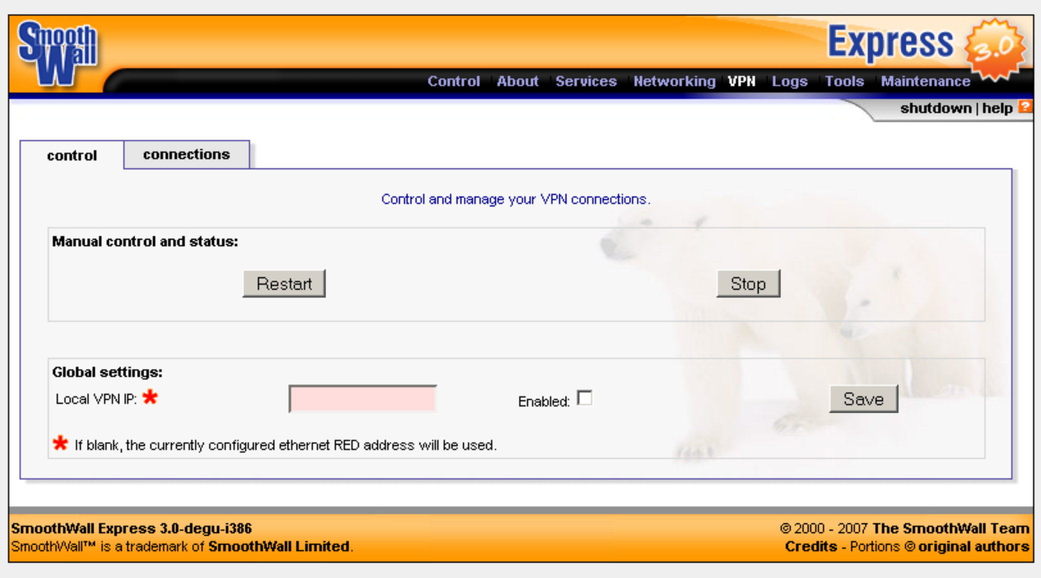
4 Click **Export**. SmoothWall Express creates the file `vpnconfig.dat` and enters the current connections in it. When prompted by your browser, save the file to a secure location.

Note: The information, including the secret, in this file is stored in clear text. Make sure that it is transferred securely to the other end of the connection.

Configuring Remote Connection Settings

To configure the remote connection settings:

1 On the remote SmoothWall Express, browse to the **VPN > control** page:



Control and manage your VPN connections.

Manual control and status:

Global settings:

Local VPN IP: * Enabled: □

* If blank, the currently configured ethernet RED address will be used.

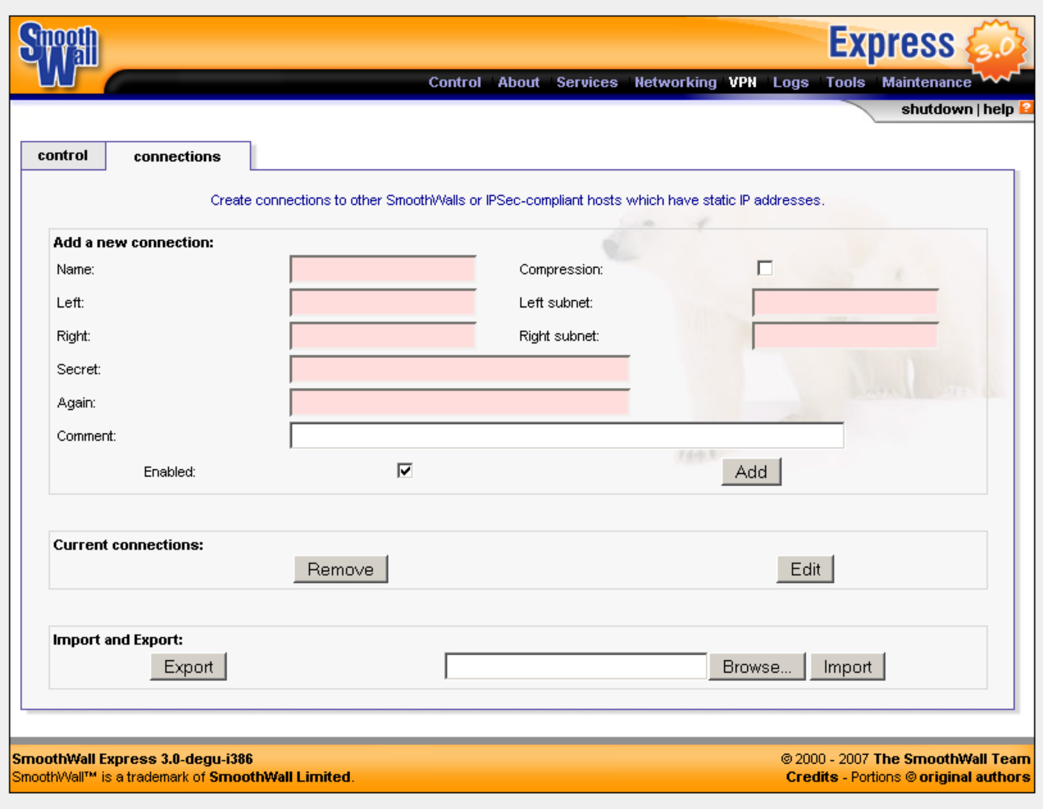
SmoothWall Express 3.0-degu-i386
SmoothWall™ is a trademark of SmoothWall Limited.

© 2000 - 2007 The SmoothWall Team
Credits - Portions © original authors

2 In the Global settings area, in the **Local VPN IP** field, enter this SmoothWall Express's public IP address of the Internet (red) interface.

3 Click **Save.**

4 Browse to the **VPN > connections** page:


SmoothWall
Express 3.0
Control About Services Networking VPN Logs Tools Maintenance
shutdown | help
control
connections

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

Add a new connection:

Name:		Compression:	□
Left:		Left subnet:	
Right:		Right subnet:	
Secret:			
Again:			
Comment:			
Enabled:	☑		Add

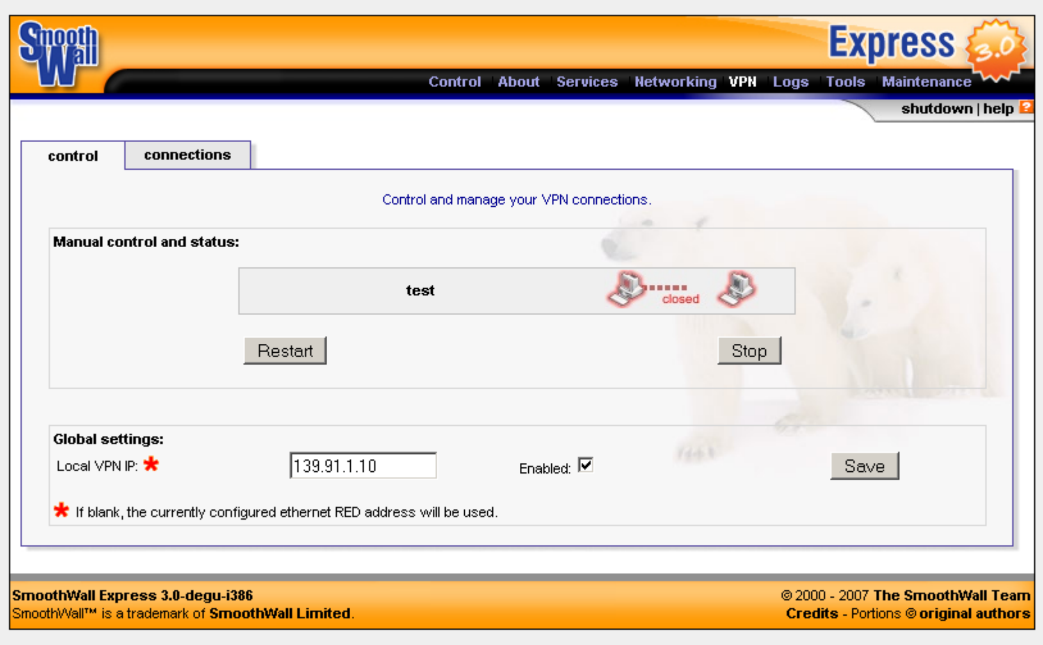
Current connections:

Import and Export:

SmoothWall Express 3.0-degu-i386
SmoothWall™ is a trademark of **SmoothWall Limited**.
© 2000 - 2007 **The SmoothWall Team**
Credits - Portions © **original authors**

5 Click **Browse**. Navigate to and select `vpnconfig.dat`. Click **Import**. SmoothWall Express uses the settings to configure the remote end of the connection.

6 Browse to the **VPN > control** page:


SmoothWall
Express 3.0
Control About Services Networking VPN Logs Tools Maintenance
shutdown | help
control
connections

Control and manage your VPN connections.

Manual control and status:

test — closed

Global settings:

Local VPN IP: * 139.91.1.10 Enabled: ☑ Save

* If blank, the currently configured ethernet RED address will be used.

SmoothWall Express 3.0-degu-i386
SmoothWall™ is a trademark of **SmoothWall Limited**.
© 2000 - 2007 **The SmoothWall Team**
Credits - Portions © **original authors**

7 Click **Restart** to open the connection.

Chapter 5

Using SmoothWall Express Tools

In this chapter:

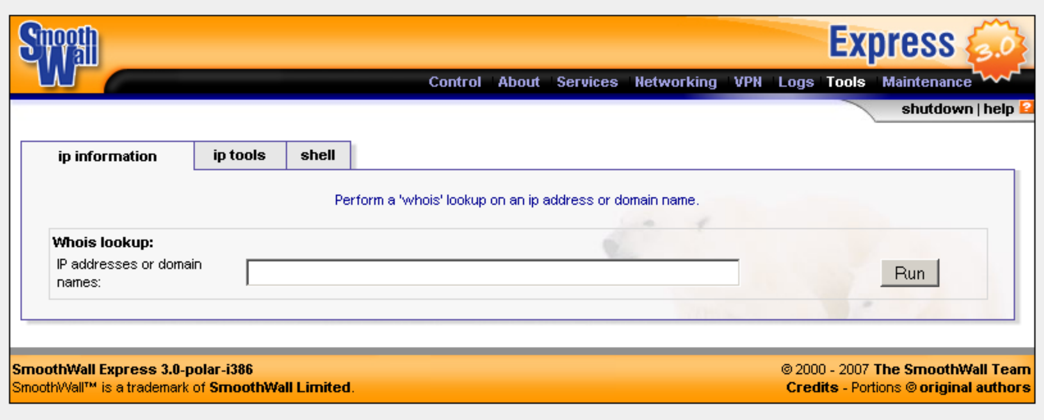
- How to use whois, ping, traceroute and shell tools.

Whois – Getting IP Information

Whois displays ownership information for an IP address or domain name. A major use for this is to determine the source of requests appearing in logs.

To use whois:

1 Navigate to the **Tools > ip information** page:



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

Whois lookup:

IP addresses or domain names:

SmoothWall Express 3.0-polar-i386
SmoothWall™ is a trademark of **SmoothWall Limited**.

© 2000 - 2007 **The SmoothWall Team**
Credits - Portions © **original authors**

2 In the IP addresses or domain name field, enter the IP address or domain name you want to lookup

3 Click **Run**. SmoothWall Express displays any information available.

Using IP Tools

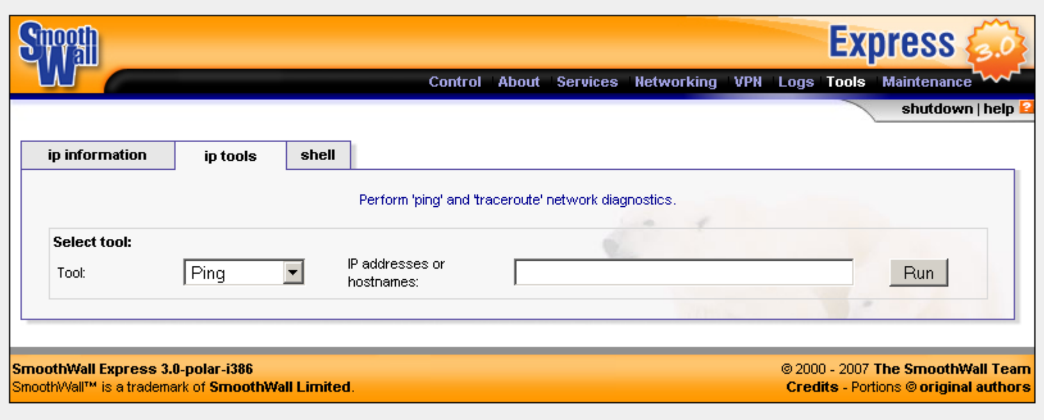
SmoothWall Express provides ping and traceroute tools

Pinging

Ping establishes that basic connectivity to a specified host can be made. Use it to prove that SmoothWall Express can communicate with its local networks and external hosts on the Internet.

To use Ping

1 Navigate to the **Tools > ip tools** page:



Perform 'ping' and 'traceroute' network diagnostics.

Select tool:

Tool: Ping

IP addresses or hostnames:

SmoothWall Express 3.0-polar-i386
SmoothWall™ is a trademark of SmoothWall Limited.

© 2000 - 2007 The SmoothWall Team
Credits - Portions © original authors

2 From the Tool drop-down menu, select **Ping**.

3 In the IP addresses or hostnames field, enter the IP address or hostname you want to ping.

4 Click **Run**. The result of the ping command is displayed.

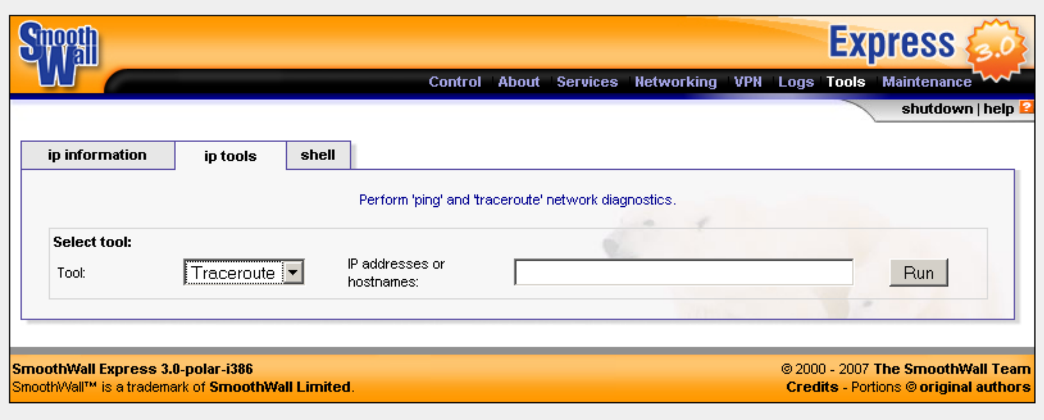
Tracing Routes

Traceroute is used to reveal the routing path to Internet hosts, shown as a series of hops from one system to another. A greater number of hops indicates a longer (and therefore slower) connection.

The output of these commands is as it would be if the commands were run directly by the root user from the console of the SmoothWall Express system. It is of course, more convenient to run them from this page.

To use Traceroute:

1 Navigate to the **Tools > ip tools** page:



Perform 'ping' and 'traceroute' network diagnostics.

Select tool:

Tool: Traceroute

IP addresses or hostnames:

SmoothWall Express 3.0-polar-i386
SmoothWall™ is a trademark of SmoothWall Limited.

© 2000 - 2007 The SmoothWall Team
Credits - Portions © original authors

2 From the Tool drop-down menu, select **Traceroute**.

3 In the IP addresses or hostnames field, enter the IP address or hostname you want to ping.

4 Click **Run**. The result of the command is displayed.

Running the SSH Client

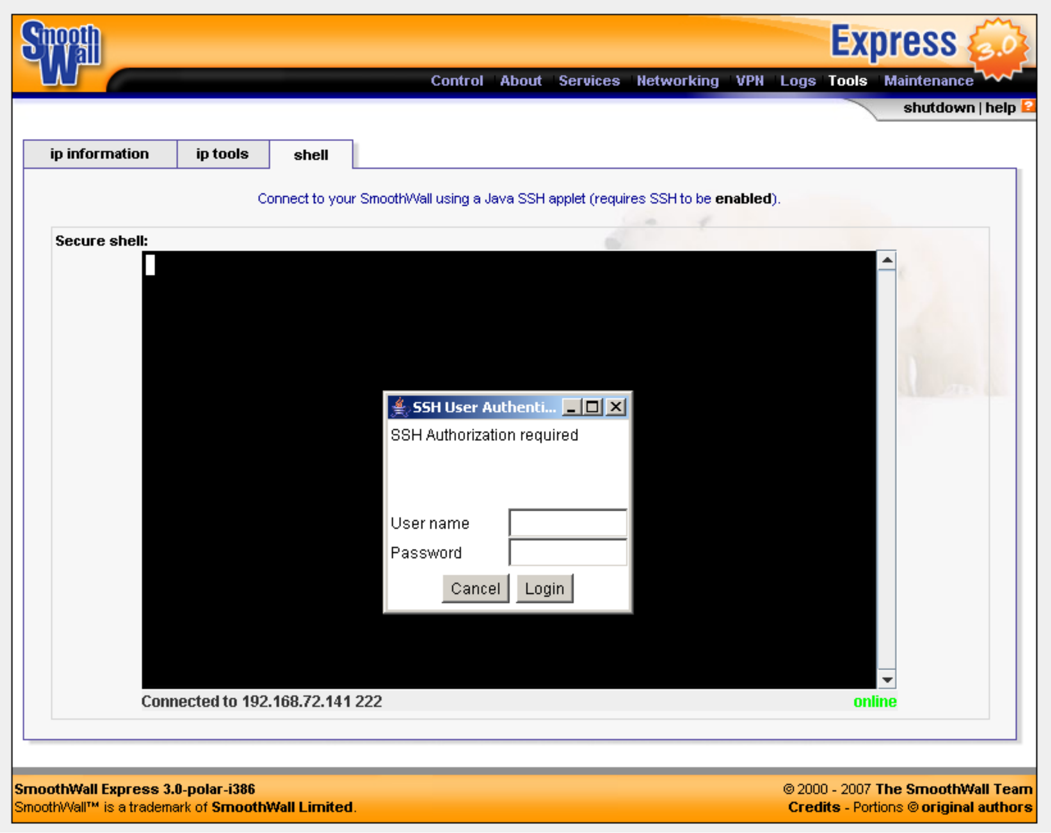
The web-based secure shell (SSH) remote access tool enables command line administration of the SmoothWall Express system through a web browser.

Note: In order to use this feature, SSH access must be enabled. See *Chapter 6, Configuring Remote Access* on page 52 for more information.

Your browser must have Java Virtual Machine capability installed. For details on setting your browser up in this way, consult your browser help system.

To use the shell tool:

1 Navigate to the **Tools > shell** page:



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

Secure shell:

SSH Authorization required

User name

Password

Connected to 192.168.72.141 222 online

SmoothWall Express 3.0-polar-i386
SmoothWall™ is a trademark of SmoothWall Limited.

© 2000 - 2007 The SmoothWall Team
Credits - Portions © original authors

2 Click on the shell window once the Java applet has loaded.

3 Enter the user name `root` and password credentials to log into the shell.

Managing SmoothWall Express Services

In this chapter:

- How to configure, enable and manage web, instant messaging, POP3, SIP DHCP, dynamic DHCP and intrusion detection system services.

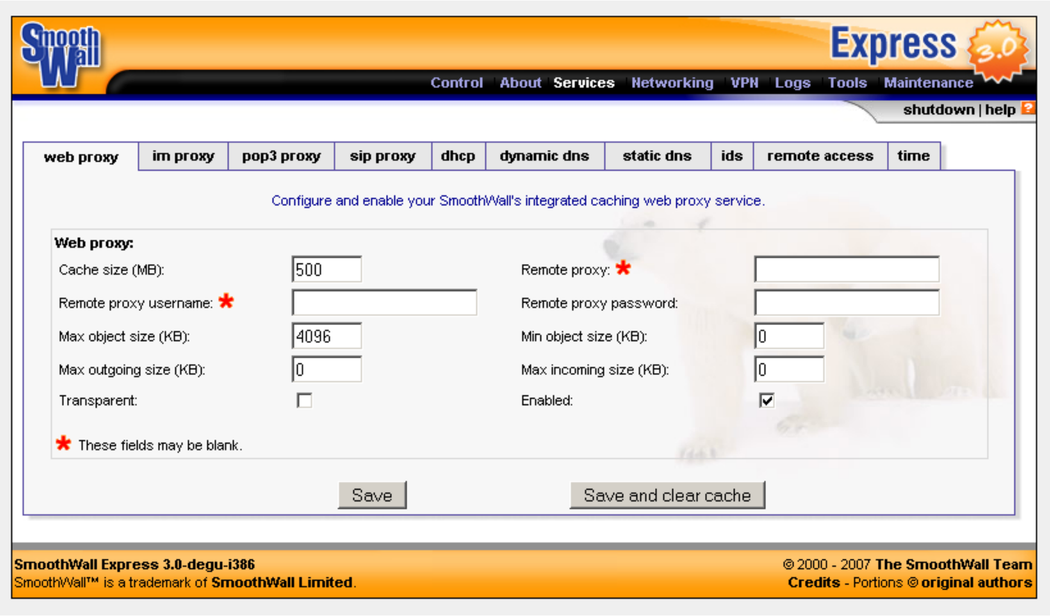
Using the Web Proxy

SmoothWall Express provides a configurable web proxy which can cache requested Internet objects. SmoothWall Express caches web and FTP requests.

Note: SmoothWall Express does not cache HTTPS requests or pages containing username and password information for privacy reasons.

To configure web proxy caching:

1 Browse to the **Services > web proxy** page:



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

Web proxy:

Cache size (MB):	500	Remote proxy: *	
Remote proxy username: *		Remote proxy password:	
Max object size (KB):	4096	Min object size (KB):	0
Max outgoing size (KB):	0	Max incoming size (KB):	0
Transparent:	□	Enabled:	☑

* These fields may be blank.

SmoothWall Express 3.0-degu-i386
SmoothWall™ is a trademark of **SmoothWall Limited**.

© 2000 - 2007 **The SmoothWall Team**
Credits - Portions © **original authors**

2 Configure the following settings:

Setting	Description
Cache size (MB)	Enter the amount of disk space that SmoothWall Express uses to cache web and FTP requested information. Correctly configured, especially where relatively slow Internet connections are used, the cache will provide faster access to pages that have recently been visited by users on the same SmoothWall Express system. The cache size must not exceed the amount of free disk space available. As a rough guide, it should be at least 100 M Bytes smaller than hard disk size. This allows adequate room for the `/var/logs`, `/boot`, `/swap` partitions and SmoothWall Express software. **Note:** An excessively large cache size may slow down information access, causing SmoothWall Express to spend more time and resources managing a large cache that the time saved retrieving pages over a fast connection. We recommend that you experiment with different cache sizes to achieve optimum performance. For more information on caching, visit: http://wiki.squid-cache.org/SquidFaq/
Remote proxy	Optionally, enter the IP address of a remote proxy server. Some large networks use a dedicated proxy server; alternatively there might be a remote proxy server available on your ISP's network, in which case your ISP will be able to provide you with the necessary information.
Remote proxy username	If using a remote proxy which requires authentication, enter the user name required.
Remote proxy password	If using a remote proxy which requires authentication, enter the password required.
Max object size (KB)	Enter the largest object size to be stored in the cache or accept the default value. This option enables you to ensure that large downloads do not clog up the cache. The default is not to cache objects larger then 4096 K Bytes (4 M Bytes).
Min object size (KB)	Optionally, enter the smallest object size that will be stored in the cache.
Max outgoing size (KB)	Optionally, enter the maximum amount of data, for example – file uploads or form submissions, that a browser is allowed to send through SmoothWall Express, regardless of whether the data is cached or not.
Max incoming size (KB)	Optionally, enter the maximum download file size that can pass through SmoothWall Express. This option can be used to stop people from downloading excessively large files that would slow down your Internet connection

Setting	Description
Transparent	Select this option to enable transparent mode and avoid the need to configure users' web browsers to work with SmoothWall Express. In transparent mode, all requests are automatically redirected through SmoothWall Express. **Prerequisites** In order to deploy a web security policy transparently, the following must be in place: 4 DNS must be set up correctly on your network so that user workstations can resolve the short form of SmoothWall Express's hostname, for example: resolve `mysmoothwall` for the hostname `mysmoothwall.london.com` 4 Configure your network to use SmoothWall Express as the default gateway to the Internet 4 User workstations and SmoothWall Express must be within the same DNS domain 4 Internet Explorer must be configured to authenticate automatically with intranet sites. If transparent mode is not enabled, you must configure users' browsers to use port 800 rather than the standard port 80.
Enabled	Select to enable the web proxy service.

3 Click **Save** to save and implement your settings. Click **Save and clear cache** to save and implement your settings and clear any information currently in the cache.

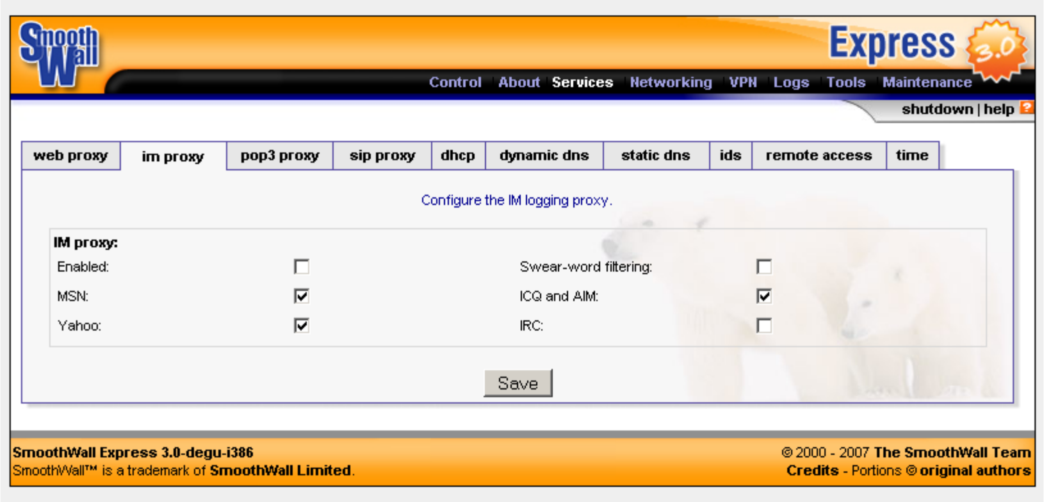
Configuring Instant Messaging Proxy

SmoothWall Express's Instant Messenger (IM) proxy service enables you to log IM conversations and file transfers on the green network and the purple network if it is enabled.

Note: SmoothWall Express cannot monitor HTTP-based IM sessions, or sessions made using any kind of end-to-end encryption.

To configure the instant messaging proxy service:

1 Browse to the **Services > im proxy** page:



Configure the IM logging proxy.

IM proxy:

Enabled:	□	Swear-word filtering:	□
MSN:	☑	ICQ and AIM:	☑
Yahoo:	☑	IRC:	□

SmoothWall Express 3.0-degu-i386
SmoothWall™ is a trademark of **SmoothWall Limited.**

© 2000 - 2007 **The SmoothWall Team**
Credits - Portions © **original authors**

2 Configure the following settings:

Setting	Description
Enabled	Select to enable the instant messaging proxy service.
Swear-word filtering	Select to filter English swearwords.
MSN	Select to proxy and monitor Microsoft Messenger conversations.
ICQ and AIM	Select to proxy and monitor ICQ and AIM conversations.
Yahoo	Select to proxy and monitor Yahoo conversations.
IRC	Select to proxy and monitor IRC conversations.

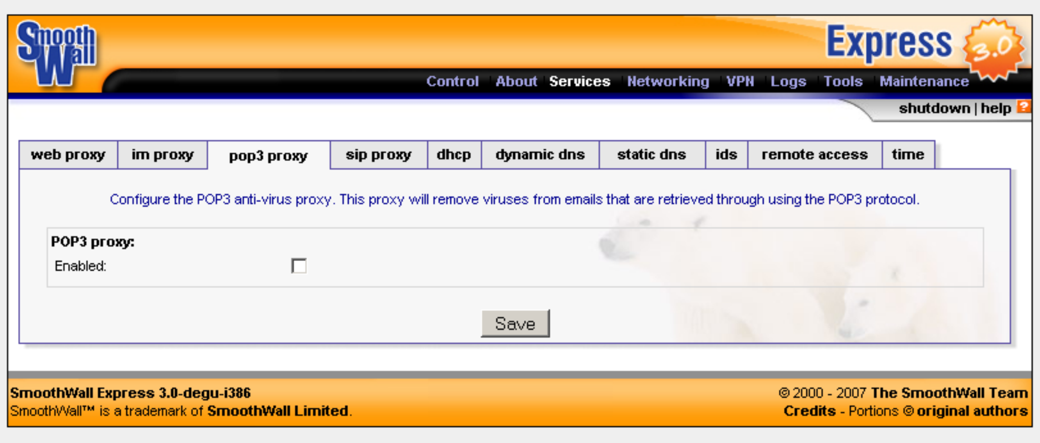
3 Click **Save** to save and implement your settings.

AV Scanning the POP3 Proxy

SmoothWall Express can Anti-Virus (AV) scan POP3 emails as they are downloaded from external mail servers to clients running on the green and purple networks.

To configure the POP3 AV scanning service:

1 Browse to the **Services > pop3 proxy** page:


Express 3.0
Control About Services Networking VPN Logs Tools Maintenance
shutdown | help
web proxy im proxy pop3 proxy sip proxy dhcp dynamic dns static dns ids remote access time
Save

Configure the POP3 anti-virus proxy. This proxy will remove viruses from emails that are retrieved through using the POP3 protocol.

POP3 proxy:

Enabled: □

SmoothWall Express 3.0-degu-i386
SmoothWall™ is a trademark of SmoothWall Limited.

© 2000 - 2007 The SmoothWall Team
Credits - Portions © original authors

2 Configure the following settings:

Setting	Description
Enabled	Select to enable the service. Clients which download mail using POP3 on port 110, will have all of their emails AV scanned by SmoothWall Express's in-built ClamAV engine. Emails which contain a virus will be replaced with an explanation email containing details of the email including the name of the detected virus. AV signatures are automatically updated daily. **Note:** POP3 over SSL, on port 995, is not currently supported by this service.

3 Click **Save** to save and implement your settings.

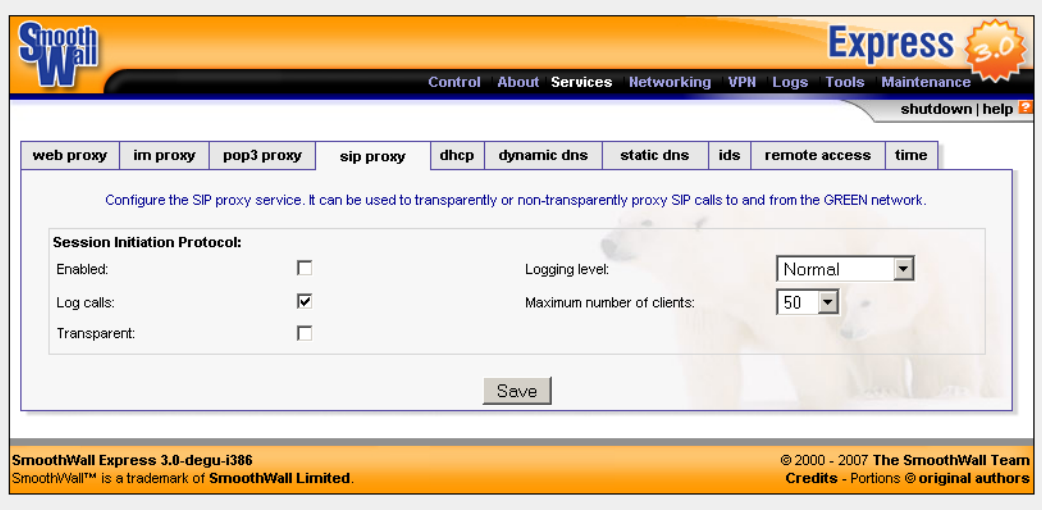
Configuring the SIP Proxy

SmoothWall Express’s SIP proxy service manages Session Initiation Protocol (SIP) traffic. SIP is often used to set up calls in Voice over Internet Protocol (VoIP) systems.

The SIP proxy service is also able to proxy Real-time Transport Protocol (RTP) traffic, and will solve some of the problems involved in setting up VoIP behind NAT.

To configure the SIP proxy service:

1 Browse to the **Services > sip proxy** page:



Configure the SIP proxy service. It can be used to transparently or non-transparently proxy SIP calls to and from the GREEN network.

Session Initiation Protocol:

Enabled:	□	Logging level:	Normal
Log calls:	☑	Maximum number of clients:	50
Transparent:	□		

Save

SmoothWall Express 3.0-degu-i386
SmoothWall™ is a trademark of **SmoothWall Limited**.

© 2000 - 2007 **The SmoothWall Team**
Credits - Portions © **original authors**

2 Configure the following settings:

Setting	Description
Enabled	Select to enable the service.
Logging level	From the drop-down list, select the level of logging required.
Log calls	Select to log individual calls.
Maximum number of clients	From the drop-down list, select the maximum number of clients which can use the service.
Transparent	Select to run the SIP proxy service in transparent mode. When operating transparently, the SIP proxy service is not used as a registrar, but will allow internal SIP devices to communicate properly with an external registrar such as an Internet Telephony Service Provider (ITSP). An ITSP offers an Internet data service for making telephone calls using VoIP.

3 Click **Save** to save and implement your settings.

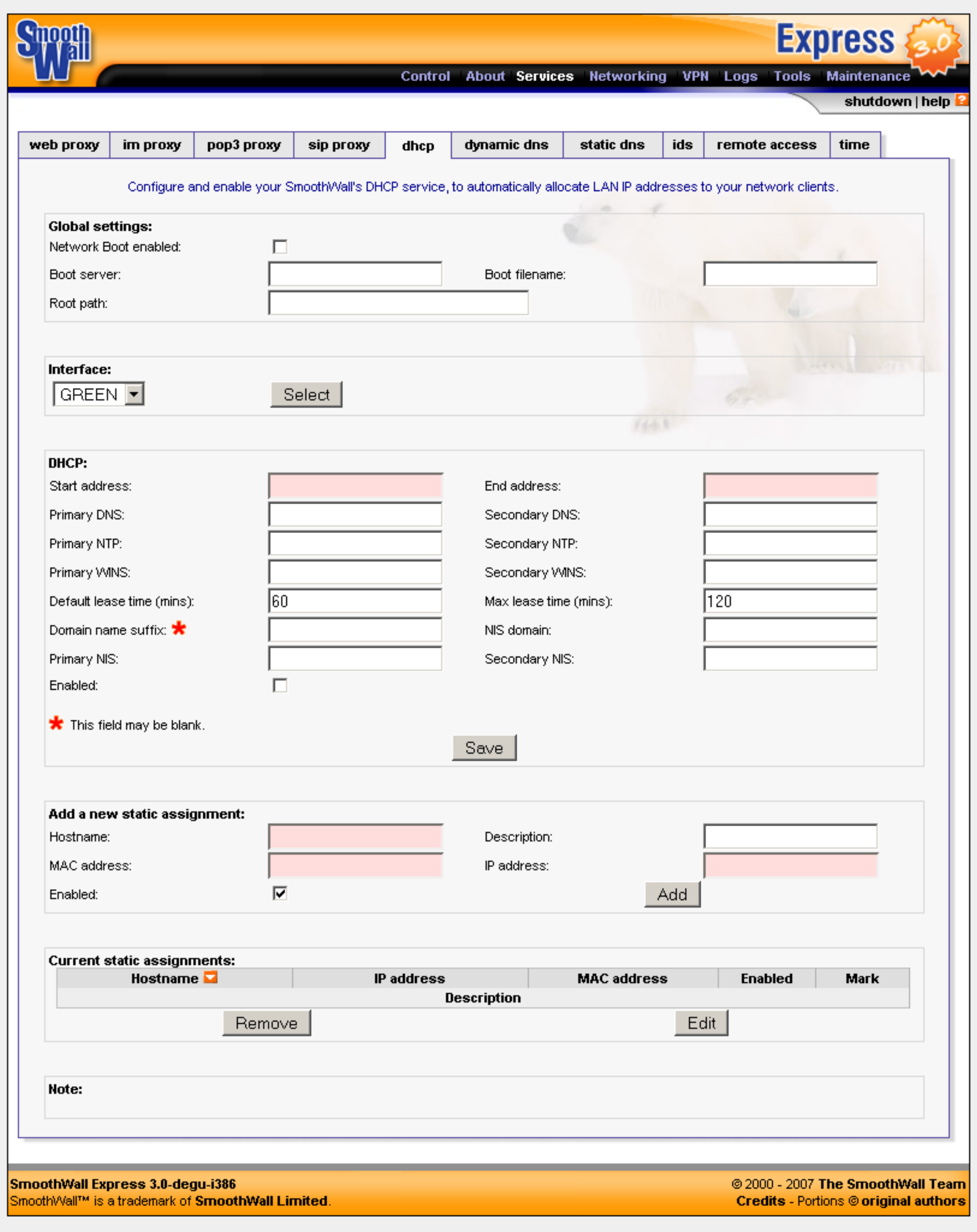
Configuring the DHCP Service

SmoothWall Express's Dynamic Host Configuration Protocol (DHCP) service enables you to automatically configure computers on your network. DHCP provides computers with an IP address, DNS settings, and gateway information.

Both the green and purple networks can use the DHCP service.

To configure the DHCP service:

1 Browse to the **Services > dhcp** page:



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

Global settings:

Network Boot enabled:	□		
Boot server:		Boot filename:	
Root path:			

Interface:

GREEN

DHCP:

Start address:		End address:	
Primary DNS:		Secondary DNS:	
Primary NTP:		Secondary NTP:	
Primary WINS:		Secondary WINS:	
Default lease time (mins):	60	Max lease time (mins):	120
Domain name suffix: *		NIS domain:	
Primary NIS:		Secondary NIS:	
Enabled:	□		

* This field may be blank.

Add a new static assignment:

Hostname:		Description:	
MAC address:		IP address:	
Enabled:	☑		

Current static assignments:

Hostname	IP address	MAC address	Enabled	Mark
Description				

Note:

SmoothWall Express 3.0-degu-i386
SmoothWall™ is a trademark of **SmoothWall Limited**.

© 2000 - 2007 **The SmoothWall Team**
Credits - Portions © **original authors**

2 Configure the following settings:

Setting	Description
Network Boot enabled	Select to enable network booting for diskless workstations.
Boot server	If network booting is enabled, enter the IP address of the server running Trivial File Transfer Protocol (TFTP)
Boot filename	If network booting is enabled, enter the name of the file workstations or devices should use to boot.
Root path	If network booting is enabled, enter the path to the file workstations or devices should use to boot.
Interface	From the drop-down list, select the network you want to configure the service for.
Start address	Enter the first IP address you want SmoothWall Express to offer to its client PCs. There is no need for the start address to be consecutive with SmoothWall Express's IP address. The first three parts of the IP address should normally be the same as that of the SmoothWall Express. The default address range suggested by SmoothWall Express is from 192.168.0.100 to 192.168.0.200. This allows addressing space below the DHCP range for computers using fixed IP addresses, such as file and print servers. Obviously, no other computers on the local network should use a fixed IP address within the DHCP range specified.
End address	Enter the highest IP address to be allocated by SmoothWall Express.
Primary DNS	Enter which DNS server SmoothWall Express should tell its clients to use. Because SmoothWall Express runs a DNS proxy, you will probably want to set the Primary DNS server to SmoothWall Express's IP address.
Secondary DNS	If you run a local DNS server and want your desktops to use it, enter its IP address.
Primary NTP	Enter the IP address of the primary Network Time Protocol (NTP) server SmoothWall Express should tell its clients to use.
Secondary NTP	Optionally, enter the IP address of a secondary Network Time Protocol (NTP) server SmoothWall Express should tell its clients to use.
Primary WINS	Enter the IP address of the Windows Internet Name Service (WINS) server SmoothWall Express should tell its clients to use.
Secondary WINS	Optionally, enter the IP address of a secondary Windows Internet Name Service (WINS) server SmoothWall Express should tell its clients to use.

Setting	Description
Default lease time (mins)	Enter the time in minutes that a client PC can retain an IP address provided by SmoothWall Express. Upon expiry of the lease, the client PC has to re-request a new IP address. For most users, this field should be left at its default value.
Max lease time (mins)	Enter the maximum time in minutes that a client PC can retain an IP address provided by SmoothWall Express. For most users, this field should be left at its default value.
Domain name suffix	Enter the domain name that will be given to systems requesting an IP address. For most small networks this can be left blank.
NIS domain	Enter the Network Information Service (NIS) domain name.
Primary NIS	Enter the IP address of the primary NIS server SmoothWall Express should tell its clients to use.
Secondary NIS	Optionally, enter the IP address of the secondary NIS server SmoothWall Express should tell its clients to use.
Enabled	Select to enable the DHCP service.

3 Click **Save** to save and implement your settings.

Assigning Static IP Addresses

SmoothWall Express enables you to allocate fixed IP addresses to nominated clients.

To statically assign an IP address:

1 In the Add a new static assignment area, configure the following settings:

Setting	Description
Hostname	Enter the hostname of the client to be allocated a static IP address.
Description	Optionally, enter a description about this assignment.
MAC address	Enter the client's Network Interface Card's (NIC's) Media Access Control (MAC) address. The MAC address must be entered as six pairs of hexadecimal numbers, with a space, colon or other separator character between each pair, e.g. `12 34 56 78 9A BC` or `12:34:56:78:9A:BC`.
IP address	Enter the IP address you want to assign to the client.
Enabled	Select to enable the assignment.

2 Click **Add** to add the assignment to the list of current static assignments.

Dynamic DNS

SmoothWall Express, together with a dynamic DNS service such as dyndns.org or no-ip.com, enables you to have a sub-domain name point to your workstation. This, in turn, enables you to run services such as a web server even if you do not have a static IP address.

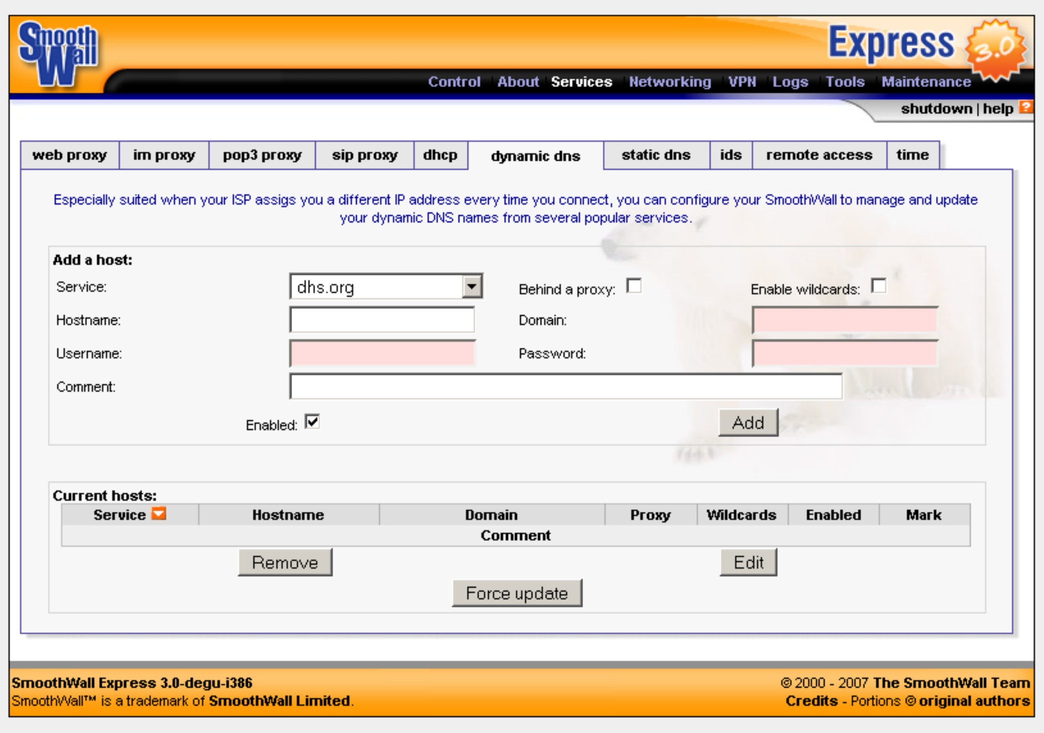
To configure the dynamic DNS service:

1 Subscribe to a dynamic DNS service. Currently, SmoothWall Express supports the following services and providers:

Service	Provider
dhs.org	DHS International provides Internet services through the help of contributions and volunteer assistance from the Internet community. For more information, visit: http://www.dhs.org/
dyndns.org	Dynamic Network Services, Inc. (DynDNS) provides domain name system (DNS) services. For more information, visit: http://www.dyndns.com/
dyndns.org (Custom)	Dynamic Network Services, Inc. (DynDNS) provides domain name system (DNS) services. For more information, visit: http://www.dyndns.com/
dyns.cx	DyNS provides a number of free and premium DNS related services for home or office use. For more information, visit: http://www.dyns.cx/
hn.org	Hammernode provides a free DNS service. For more information, visit: http://hn.org **Note:** At the time of writing, it is unclear if Hammernode’s service is still available.
no-ip.com	No-IP is a managed DNS service provider. For more information, visit: http://www.no-ip.com/
zonedit.com	zoneedit supplies Internet domain name management. For more information, visit: http://www.zonedit.com/
easydns.com	easyDNS provides domain name registration and a DNS management service. For more information, visit: http://www.easydns.com/
ods.org	ODS provides DNS management services. For more information, visit: http://www.easydns.com/

Note: We encourage users to donate to organisations which rely largely on donations for funding.

2 Browse to the **Services > dynamic dns** page:



Especially suited when your ISP assigs 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:	dhs.org	Behind a proxy: ☐	Enable wildcards: ☐
Hostname:		Domain:	
Username:		Password:	
Comment:			
Enabled: ☑			

Current hosts:

Service	Hostname	Domain	Proxy	Wildcards	Enabled	Mark
Comment						

SmoothWall Express 3.0-degu-i386
SmoothWall™ is a trademark of **SmoothWall Limited**.
© 2000 - 2007 **The SmoothWall Team**
Credits - Portions © **original authors**

3 Configure the following settings:

Setting	Description
Service	From the drop-down list, select the dynamic DNS service you have registered with.
Behind a proxy	Select this option if you are using no-ip.com as the service provider or if SmoothWall Express is behind a proxy server.
Enable wildcards	Select this option to have all the sub-domains of your dynamic dns hostname point to the same IP as your hostname. For example, when selected, www.mysmoothwall.dyndns.org will point to the same IP as smoothwall.dyndns.org. **Note:** This option does not work with the noip.com service, as they only allow this feature to be activated or deactivated directly from their web site.
Hostname	Enter the hostname you registered with your service provider.
Domain	Enter the service provider's domains you selected.
Username	Enter the user name you registered with the service provider.
Password	Enter the password you registered with the service provider.
Comment	Optionally, enter a description.
Enabled	Select to enable the service.

4 Click **Add** to add the service to the list of current hosts.

Forcing Updates

You can force SmoothWall Express to refresh current dynamic IP addresses for all the enabled hostnames back to their respective dynamic DNS service providers.

Note: Don't do it too often. Dynamic DNS service providers don't like people who update their IP when it hasn't changed – they may consider you an abusive user and block your hostnames.

To force updates:

1 Browse to the **Services > dynamic dns** page.

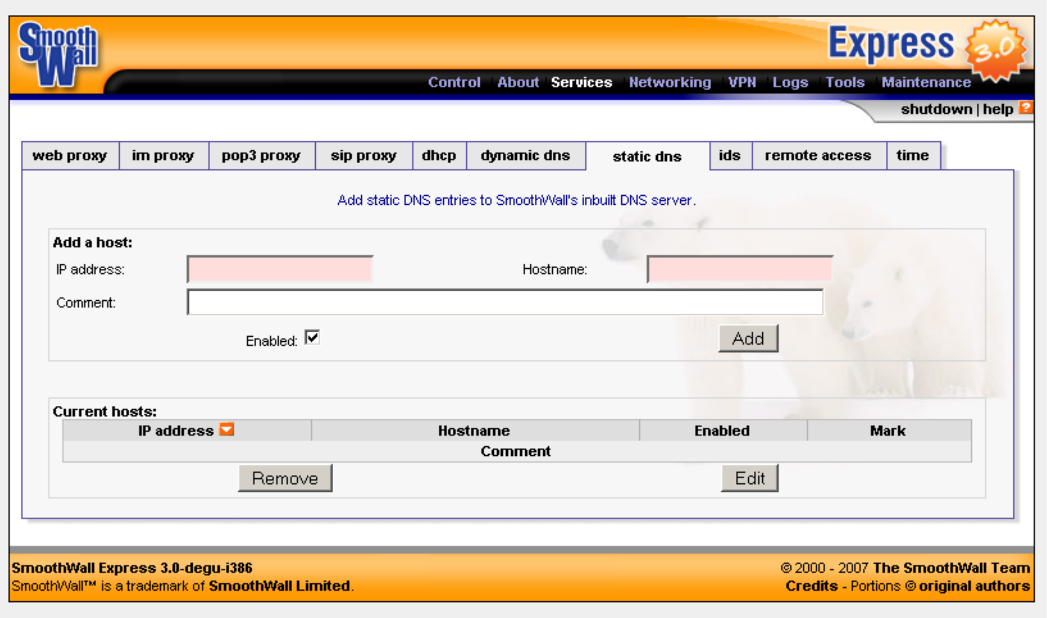
2 In the Current hosts area, click **Force update**. SmoothWall Express refreshes the current dynamic IP addresses.

Static DNS

SmoothWall Express can create a local hostname table that can be used by SmoothWall Express and computers on the green and purple networks. This makes hostnames resolvable to all hosts using SmoothWall Express's DNS service. This includes SmoothWall Express itself.

To configure the static DNS service:

1 Browse to the **Services > static dns** page:



Add static DNS entries to SmoothWall's inbuilt DNS server.

SmoothWall Express 3.0-degu-i386
SmoothWall™ is a trademark of SmoothWall Limited.
© 2000 - 2007 The SmoothWall Team
Credits - Portions © original authors

2 Configure the following settings:

Setting	Description
IP address	Enter the IP address of the host.
Hostname	Enter the host's name.
Comment	Optionally, enter a description
Enabled	Select to enable the entry.

3 Click **Add** to add the settings to the list of current hosts.

Managing the Intrusion Detection System

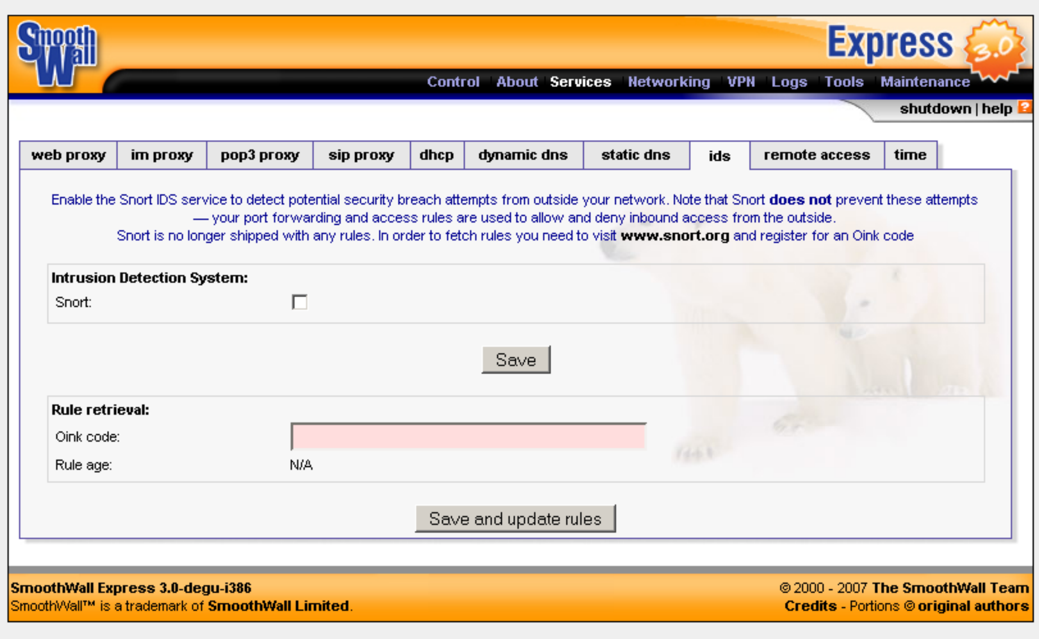
SmoothWall Express's intrusion detection service (IDS) detects potential security breach attempts from outside your network.

Note: This service only detects intrusion attempts, it does not prevent them.

To enable IDS:

1 SmoothWall Express requires Snort IDS rules. Visit http://www.snort.org/ to subscribe and get an Oink code which will entitle you to download rules and keep them up to date.

2 Browse to the **Services > ids** page:



Smooth Wall
Express 3.0
Control About Services Networking VPN Logs Tools Maintenance
shutdown | help
web proxy im proxy pop3 proxy sip proxy dhcp dynamic dns static dns ids remote access time
Save
Save and update rules

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.
Snort is no longer shipped with any rules. In order to fetch rules you need to visit **www.snort.org** and register for an Oink code

Intrusion Detection System:
Snort: □

Rule retrieval:
Oink code:
Rule age: N/A

SmoothWall Express 3.0-degu-i386
SmoothWall™ is a trademark of **SmoothWall Limited**.
© 2000 - 2007 **The SmoothWall Team**
Credits - Portions © **original authors**

3 Configure the following settings:

Setting	Description
Snort	Select to enable IDS. Click **Save**.
Oink code	Enter the code you have received from Snort.

4 Click **Save and Update rules** to fetch the IDS rules and restart the service.

Note: Fetching the rules and restarting the service may take a while.

You are only permitted to download the rules at a limited frequency.

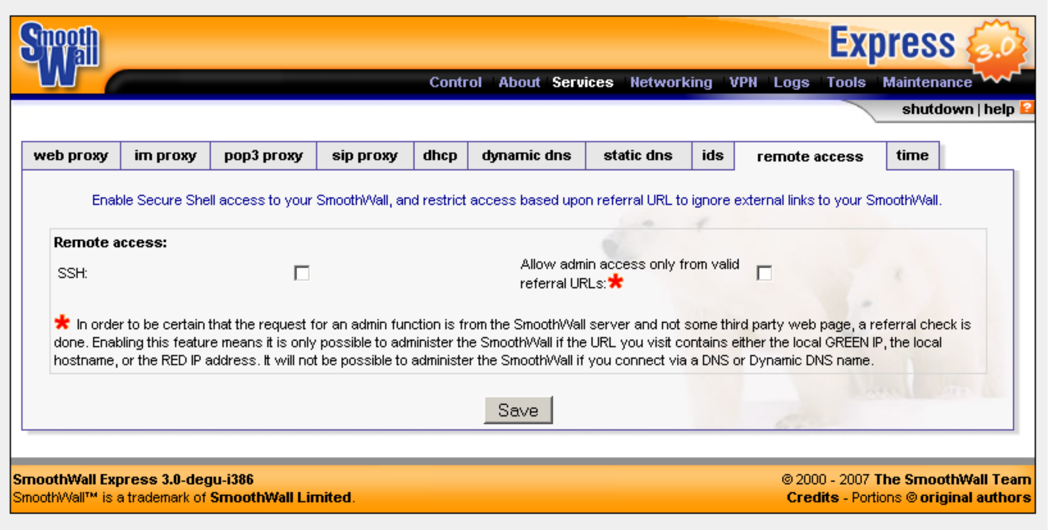
Do not share the same Oink code between different SmoothWall Express systems.

Configuring Remote Access

When enabled, you can access SmoothWall Express remotely using the secure shell (SSH) service.

To configure remote access:

1 Browse to the **Services > remote access** page:



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.

SmoothWall Express 3.0-degu-i386
SmoothWall™ is a trademark of **SmoothWall Limited**.

© 2000 - 2007 **The SmoothWall Team**
Credits - Portions © **original authors**

2 Configure the following settings:

Setting	Description
SSH	Select to enable remote access using SSH.
Allow admin access only from valid referral URLs	Optionally, select to make a referral check that ensures that any request for an admin function is from SmoothWall Express and not a third party web page. **Note:** Enabling this feature means it is only possible to administer SmoothWall Express 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 SmoothWall Express if you connect via a DNS or dynamic DNS name.

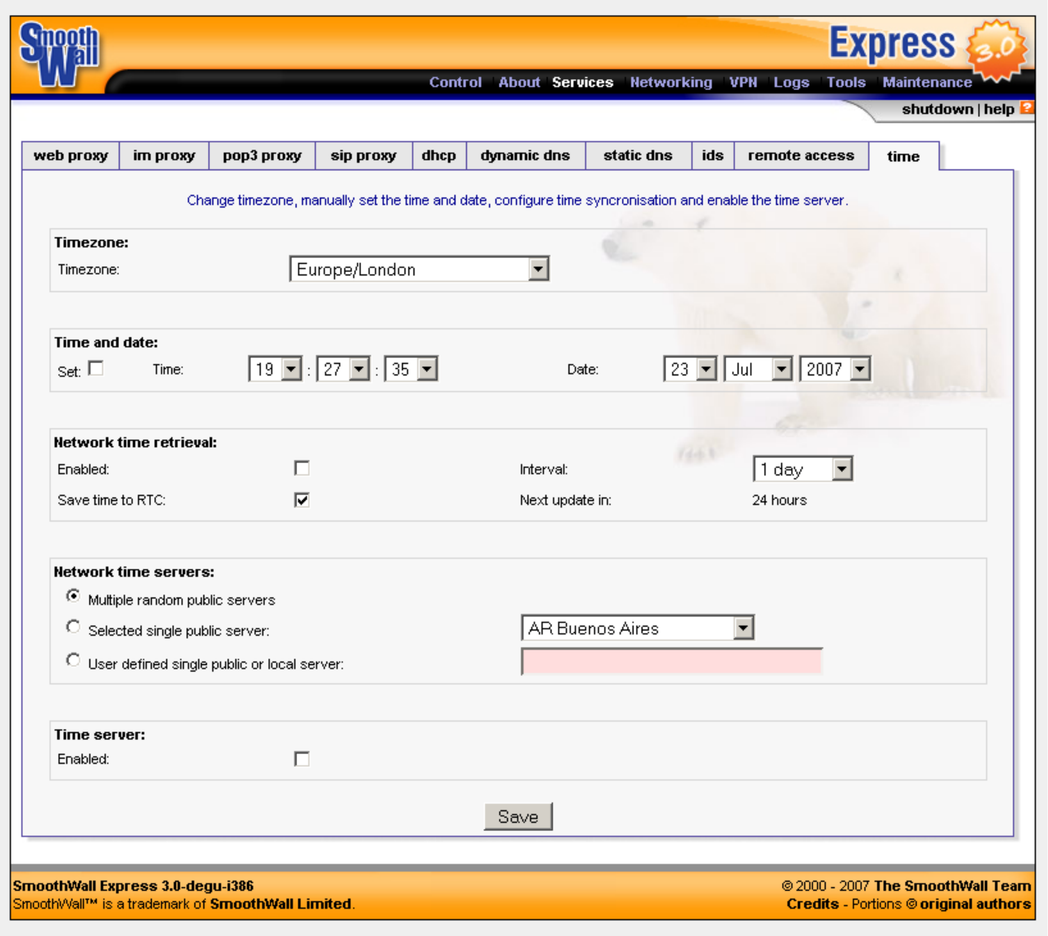
3 Click **Save** to implement the settings and start the SSH service.

Configuring Time Settings

You can configure SmoothWall Express with the date and time, synchronise time with a network time server and enable the inbuilt time server.

To configure time settings:

1 Browse to the **Services > time** page:



Change timezone, manually set the time and date, configure time syncronisation and enable the time server.

Timezone:
Timezone: Europe/London

Time and date:
Set: □ Time: 19 : 27 : 35 Date: 23 Jul 2007

Network time retrieval:
Enabled: □ Interval: 1 day
Save time to RTC: ☑ Next update in: 24 hours

Network time servers:
● Multiple random public servers
○ Selected single public server: AR Buenos Aires
○ User defined single public or local server:

Time server:
Enabled: □

SmoothWall Express 3.0-degu-i386
SmoothWall™ is a trademark of **SmoothWall Limited**.
© 2000 - 2007 **The SmoothWall Team**
Credits - Portions © **original authors**

2 Configure the following settings:

Setting	Description
Timezone	From the drop-down list, select your time zone.
Set	Select to set the time and date.
Time	From the drop-down lists, select the current time.
Date	From the drop-down lists, select the date.
Enabled	In the Network time retrieval area, select to enable SmoothWall Express to synchronise its date and time with network time servers that are accessible on the Internet.

Setting	Description
Interval	From the drop-down list, select how often SmoothWall Express should synchronise the time and date with the network time server.
Save time to RTC	Select to make SmoothWall Express update the Real-Time Clock (RTC) of the workstation on which it is running with the time retrieved from the network time server.
Next update in	Displays when the next synchronisation will take place.
Multiple random public servers	Select to use a different network time server each time SmoothWall Express synchronises the time settings. This is the default and recommended option.
Selected single public server	Select to use the same network time server each time SmoothWall Express synchronises the time settings.
User defined single public or local server	Select to specify the network time server to be used and enter the server's address.
Enabled	In the Time server area, select to enable SmoothWall Express's built in time server. This time server, when running, can service the green and purple networks with the time using the Network Time Protocol (NTP).

Chapter 7

Managing SmoothWall Express

In this chapter:

- How to administer and manage SmoothWall Express.

Updating SmoothWall Express Software

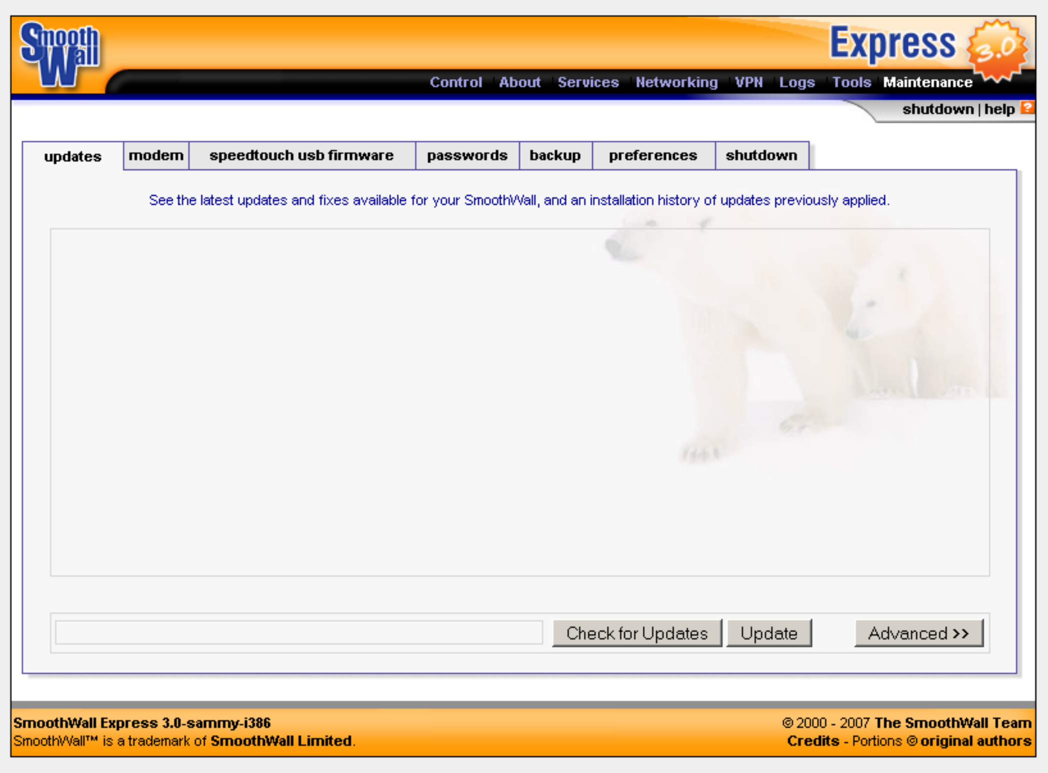
From time to time, security and product updates are rolled out to all SmoothWall Express systems. You can use SmoothWall Express to check for and install updates automatically or you can update SmoothWall Express manually.

Note: Only official patches will work with SmoothWall Express. Some patches may automatically reboot your SmoothWall Express, read the instructions carefully before installing any patch.

Updating Automatically

To update SmoothWall Express automatically:

1 Browse to the **Maintenance > updates** page:



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

SmoothWall Express 3.0-sammy-i386
SmoothWall™ is a trademark of SmoothWall Limited.

© 2000 - 2007 The SmoothWall Team
Credits - Portions © original authors

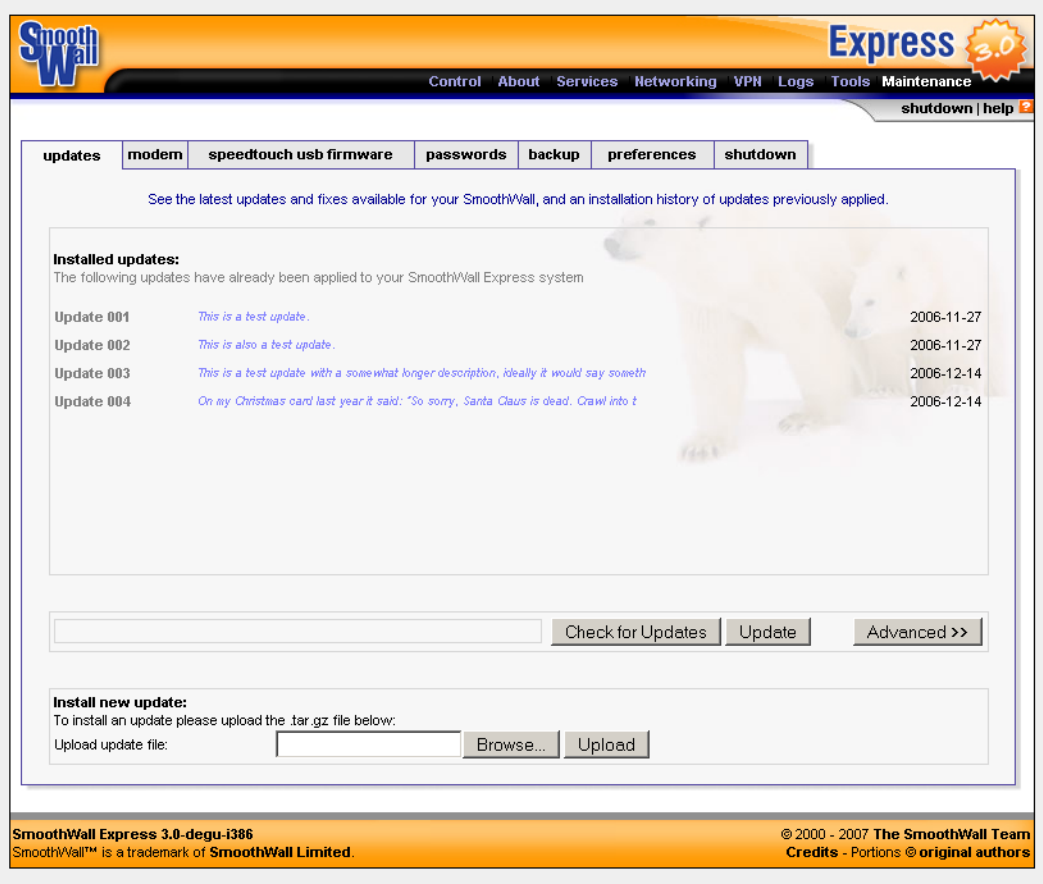
2 Click **Check for Updates**. SmoothWall Express checks for and displays any available updates.

3 Click **Update**. SmoothWall Express downloads and installs the available updates. Once installed, the updates

Updating Manually

To update SmoothWall Express manually:

1 Browse to the **Maintenance > updates** page:



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

Installed updates:
The following updates have already been applied to your SmoothWall Express system

Update 001	*This is a test update.*	2006-11-27
Update 002	*This is also a test update.*	2006-11-27
Update 003	*This is a test update with a somewhat longer description, ideally it would say someth*	2006-12-14
Update 004	*On my Christmas card last year it said: "So sorry, Santa Claus is dead. Crawl into t*	2006-12-14

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

SmoothWall Express 3.0-degu-i386
SmoothWall™ is a trademark of **SmoothWall Limited**.
© 2000 - 2007 **The SmoothWall Team**
Credits - Portions © **original authors**

2 Click **Advanced** to access manual options.

3 In the Install new update area, click **Browse**. Navigate to and select the update file.

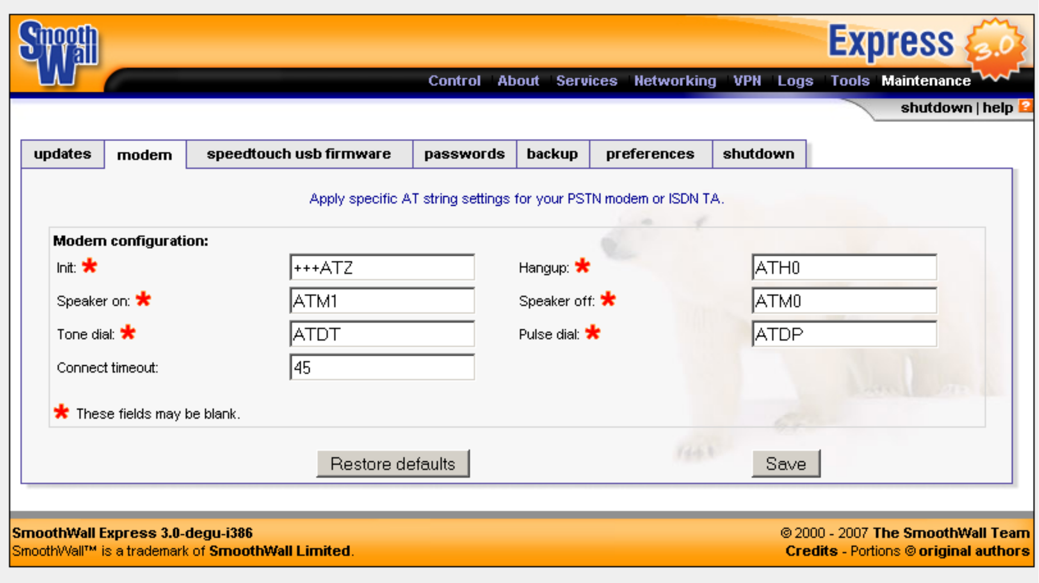
4 Click **Upload** to upload and install the update.

Configuring Modems

SmoothWall Express’s default modem command settings work for the vast majority of modems. However, you can customise modem commands to suit the modem you are using. Consult your modem documentation for full documentation on the commands required.

To configure your modem:

1 Browse to the **Maintenance > modem** page:


Smooth Wall
Express 3.0
Control About Services Networking VPN Logs Tools Maintenance
shutdown | help
updates
modem
speedtouch usb firmware
passwords
backup
preferences
shutdown
Restore defaults
Save
SmoothWall Express 3.0-degu-i386
SmoothWall™ is a trademark of SmoothWall Limited.
© 2000 - 2007 The SmoothWall Team
Credits - Portions © original authors

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

Modem configuration:

Init: *	+++ATZ	Hangup: *	ATH0
Speaker on: *	ATM1	Speaker off: *	ATM0
Tone dial: *	ATDT	Pulse dial: *	ATDP
Connect timeout:	45		

* These fields may be blank.

2 Depending on your modem requirements, you can configure the following settings:

Setting	Description
Init	Accept the default initalization command string, or consult your modem documentation. The default string contains two elements: `+++` and `ATZ`. `+++` ensures the modem is in command rather than data mode, `ATZ` performs a reset. However, some modems have support for two stored profiles, which might require the use of `ATZ0` or `ATZ1`.
Hangup	Accept the default hangup command string, or consult your modem documentation.
Speaker on	Accept the default speaker on command string, or consult your modem documentation. Usually, the modem’s speaker is turned on while dialling using the ATM1 command. A few modems and external ISDN terminal adapters object to this command, so try blanking it out.
Speaker off	Accept the default speaker off command string, or consult your modem documentation.
Tone dial	Accept the default tone dial command string, or consult your modem documentation.

Setting	Description
Pulse dial	Accept the default pulse dial command string, or consult your modem documentation.
Connect timeout	Enter the length of time to allow the modem to attempt to connect. After this number of seconds without proper response on the receiving side, it will stop trying to connect.

3 Click **Save** to save and implement your settings.

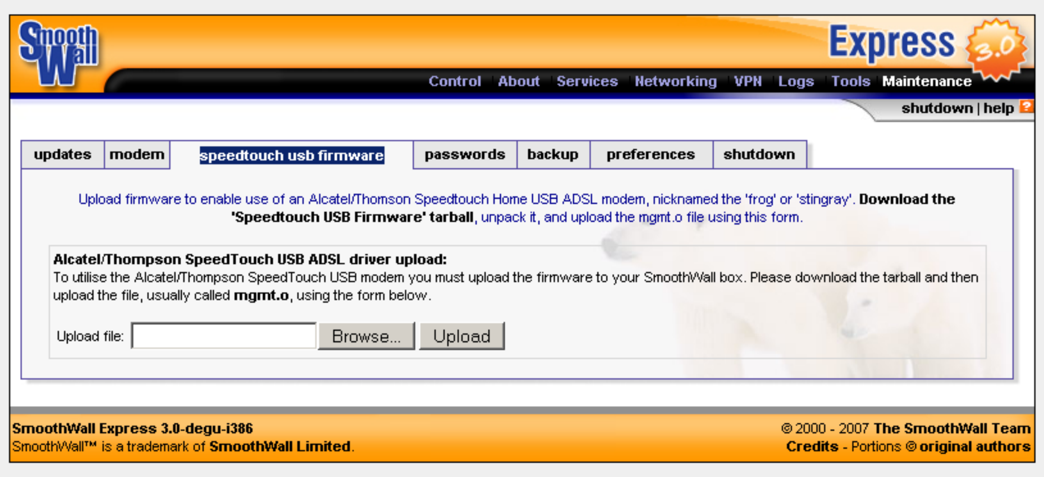
Using Speedtouch USB ADSL Modems

Here you can upload the Alcatel USB driver software for the original Stingray (frog) modem and the 330 model to SmoothWall Express.

To upload the driver:

1 Visit www.thomson.net/dsl/ or http://speedtouch.sourceforge.net/ and download the latest driver.

2 Browse to the **Maintenance > speedtouch usb firmware** page:



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

Upload file:

SmoothWall Express 3.0-degu-i386
SmoothWall™ is a trademark of **SmoothWall Limited**.

© 2000 - 2007 **The SmoothWall Team**
Credits - Portions © **original authors**

3 Click **Browse**, navigate to and select the driver file.

4 Click **Upload**. The file is uploaded to SmoothWall Express.

Managing Passwords

Here you manage the passwords for the admin and dial accounts.

Passwords for SmoothWall Express accounts should be chosen carefully, ideally it should contain a mixture of upper and lower case letter and numbers – and should be known to as few a people as possible.

About SmoothWall Express Accounts

The admin account is the most important SmoothWall Express account. Users of this account are allowed to change all SmoothWall Express settings, can view the log files and perform maintenance on the system.

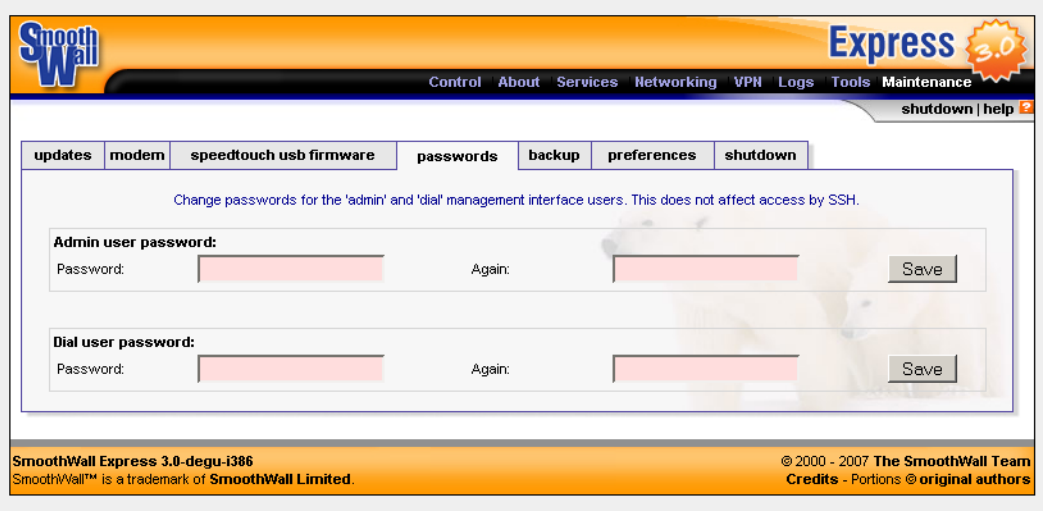
Users of the dial account are only allowed access to the SmoothWall Express home page and may connect, disconnect and refresh the Internet connection.

Changing Passwords

It is always good security practice to use strong passwords and change them on a regular basis

To change passwords:

1 Browse to the **Maintenance > passwords** page:



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:

SmoothWall Express 3.0-degu-i386
SmoothWall™ is a trademark of **SmoothWall Limited**.
© 2000 - 2007 **The SmoothWall Team**
Credits - Portions © **original authors**

2 Configure the following settings for the admin account:

Setting	Description

Password	Enter a new, strong password for the account.
	Minimum = 6 characters
	Maximum = 25 characters

Again	Re-enter the password to confirm it.

3 Click **Save** to change the password

4 Repeat the steps above for the dial account.

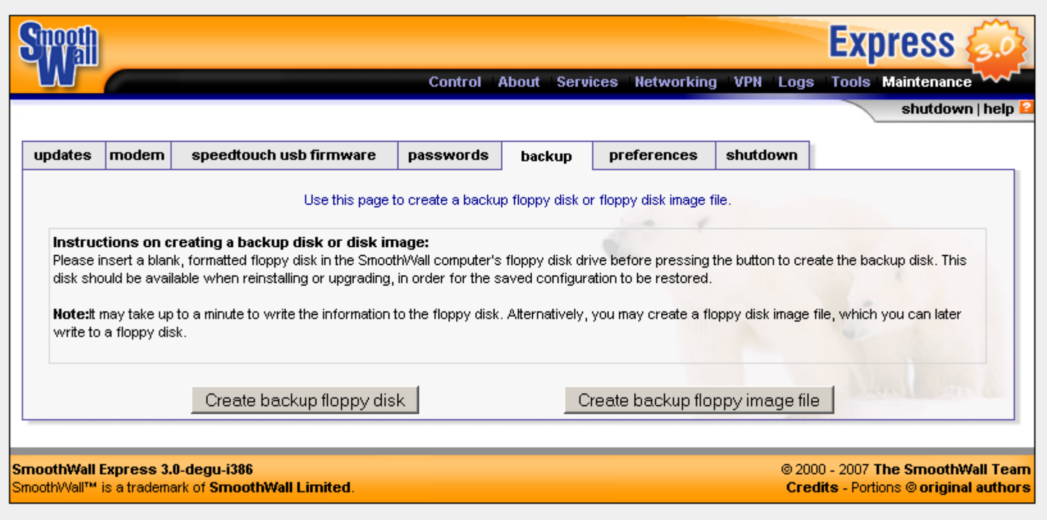
Configuring Backups

You can back up your SmoothWall Express's configuration settings to a floppy disk.

You can deploy your current settings on a new SmoothWall Express installation by using a backup. This is useful for cloning SmoothWall Express systems and enabling people with little or no knowledge of SmoothWall Express to configure a firewall and Internet gateway.

To create a backup:

1 Browse to the **Maintenance > backup** page:


Smooth Wall
Express 3.0
Control About Services Networking VPN Logs Tools Maintenance
shutdown | help
updates modem speedtouch usb firmware passwords backup preferences shutdown
Create backup floppy disk
Create backup floppy image file

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.

Note: 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.

SmoothWall Express 3.0-degu-i386
SmoothWall™ is a trademark of **SmoothWall Limited**.

© 2000 - 2007 **The SmoothWall Team**
Credits - Portions © **original authors**

2 Depending on how you want to store the backup, select one of the following options:

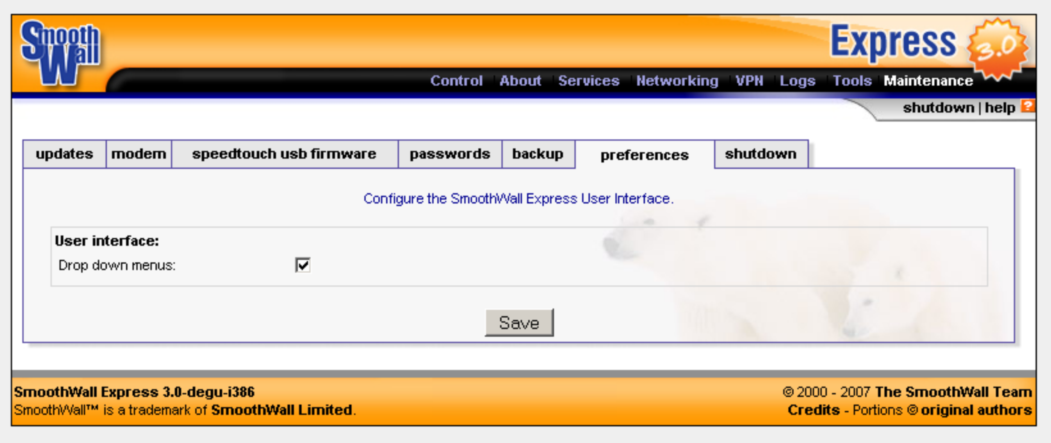
Option	Description
Create backup floppy disk	This option creates a backup floppy disk. **To create a backup floppy disk:** 1 Insert a blank, formatted floppy disk in the SmoothWall Express's floppy disk drive. 2 Click **Create backup floppy disk** to create the disk. **Note:** It may take up to a minute to write the information to the floppy disk. 3 Store the disk securely for when you need to clone or restore your SmoothWall Express.
Create backup floppy image	This option creates a backup floppy image which can be useful if you do not have physical access to SmoothWall Express. **To create a backup floppy image:** 1 Click **Create backup floppy image** to create the backup file. 2 Store the file securely for when you need to clone or restore your SmoothWall Express.

Setting User Interface Preferences

You can configure SmoothWall Express's user interface to display or hide its drop-down menus.

To configure the user interface:

1 Browse to the **Maintenance > preferences** page:


Express 3.0
Control About Services Networking VPN Logs Tools Maintenance
shutdown | help
updates modem speedtouch usb firmware passwords backup preferences shutdown
Save
SmoothWall Express 3.0-degu-i386
SmoothWall™ is a trademark of SmoothWall Limited.
© 2000 - 2007 The SmoothWall Team
Credits - Portions © original authors

Configure the SmoothWall Express User Interface.

User interface:

Drop down menus: ☑

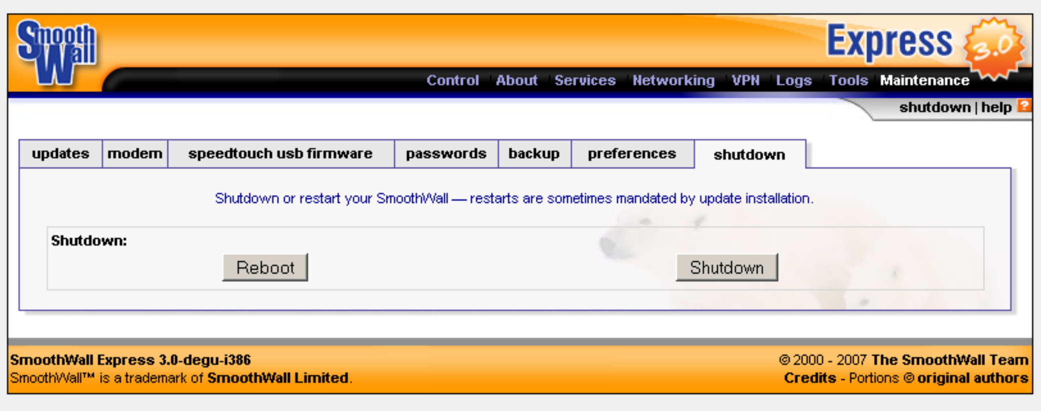
2 Select or de-select the **Drop down menus** option to display or hide the menus.

3 Click **Save** to save and implement your preference.

Shutting down/Restarting SmoothWall Express

To shut down or restart SmoothWall Express:

1 Browse to the **Maintenance > shutdown** page:


Express 3.0
Control About Services Networking VPN Logs Tools Maintenance
shutdown | help
updates modem speedtouch usb firmware passwords backup preferences shutdown
Reboot
Shutdown
SmoothWall Express 3.0-degu-i386
SmoothWall™ is a trademark of SmoothWall Limited.
© 2000 - 2007 The SmoothWall Team
Credits - Portions © original authors

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

Shutdown:

2 Select from the following options:

Setting	Description
Reboot	Click to reboot SmoothWall Express. This is usually only required after applying a patch.
Shutdown	Click to shut down. When the machine has finished shutting down, SmoothWall Express will beep once indicating that you can disconnect the power.

Information and Logs

In this chapter:

- SmoothWall Express's home page
- Service status, configuration, resource usage, bandwidth and traffic information
- How to register your SmoothWall Express
- Logs.

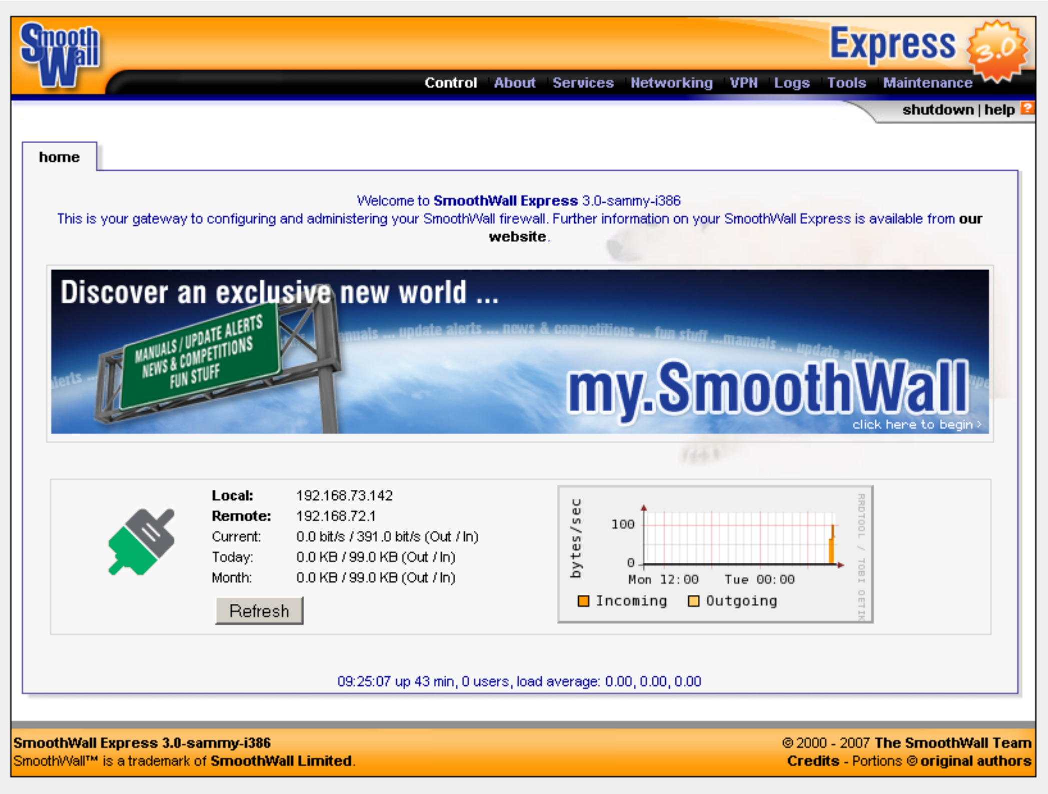
Control

The Control section contain SmoothWall Express's home page which is the main status page.

Home

To access the home page:

1 Browse to the **Control > home** page:



Welcome to **SmoothWall Express** 3.0-sammy-i386
This is your gateway to configuring and administering your SmoothWall firewall. Further information on your SmoothWall Express is available from **our website**.

Local:	192.168.73.142
Remote:	192.168.72.1
Current:	0.0 bit/s / 391.0 bit/s (Out / In)
Today:	0.0 KB / 99.0 KB (Out / In)
Month:	0.0 KB / 99.0 KB (Out / In)

09:25:07 up 43 min, 0 users, load average: 0.00, 0.00, 0.00

SmoothWall Express 3.0-sammy-i386
SmoothWall™ is a trademark of **SmoothWall Limited**.

© 2000 - 2007 **The SmoothWall Team**
Credits - Portions © **original authors**

Note: When using PPP as the external connection method, buttons will be available to connect or disconnect the connection.

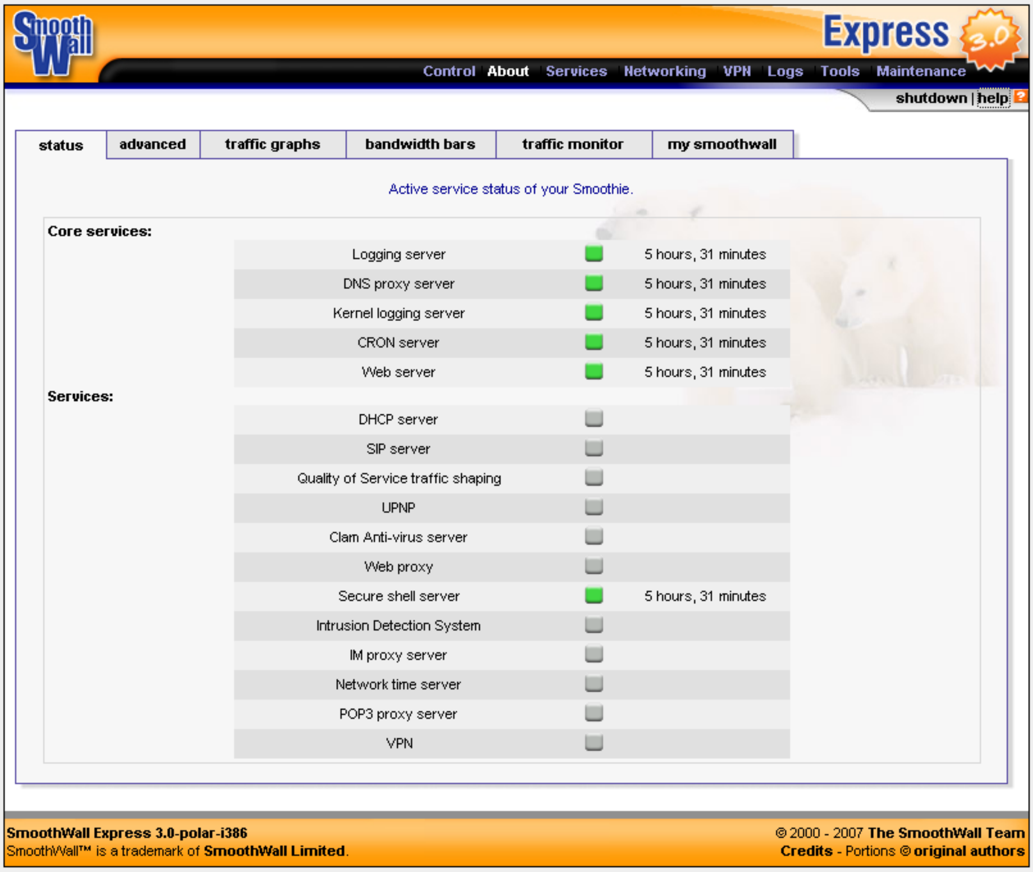
About SmoothWall Express

The following sections reviewSmoothWall Express information.

Status

Displays a list of core and optional services.

Note: On machines with low amounts of memory, 64 megabytes or less, or heavy web proxy caching, some services may get swapped out to disk to save memory. This will be indicated on this page and is not an error condition.



Active service status of your Smoothie.

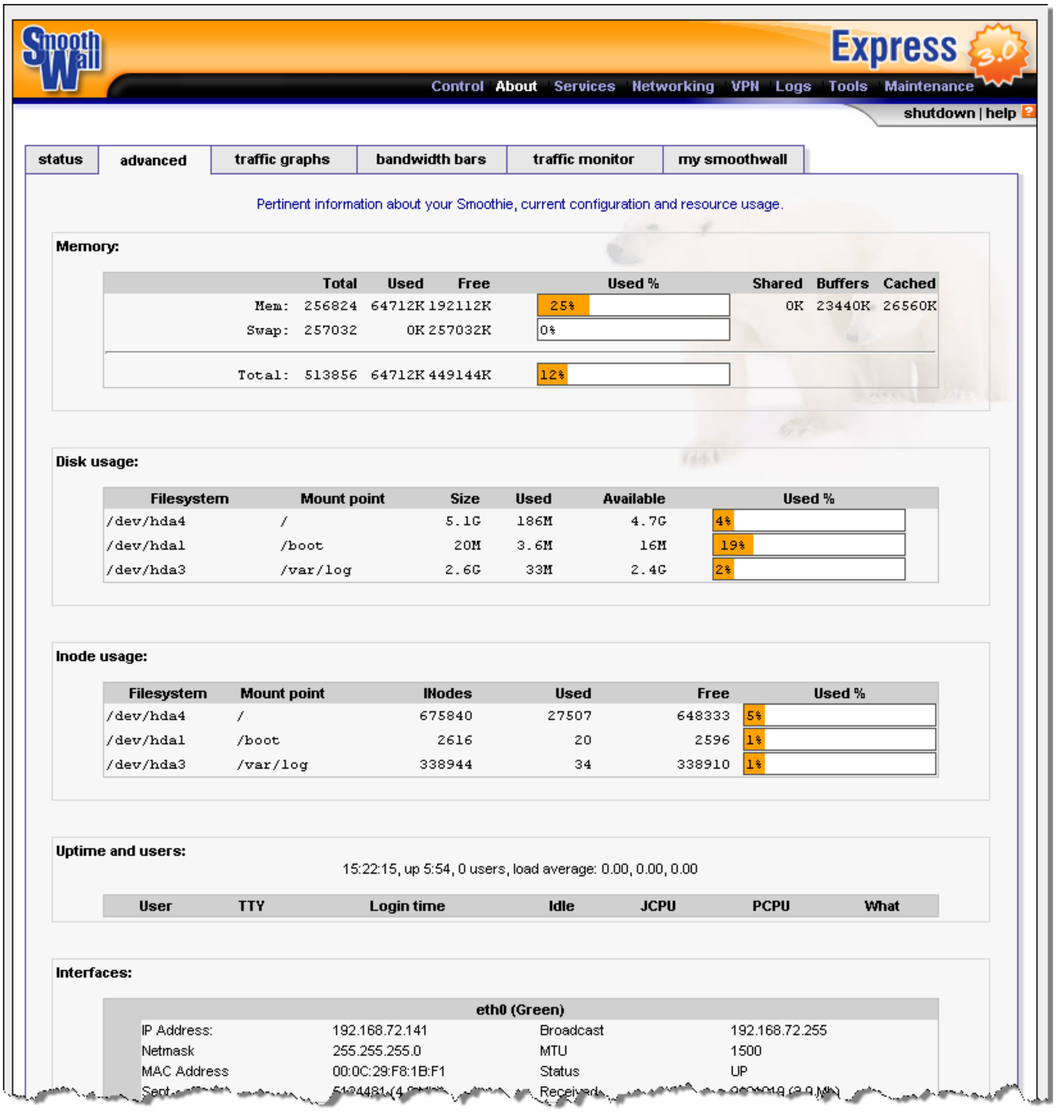
Core services:	Logging server	🟩	5 hours, 31 minutes
	DNS proxy server	🟩	5 hours, 31 minutes
	Kernel logging server	🟩	5 hours, 31 minutes
	CRON server	🟩	5 hours, 31 minutes
	Web server	🟩	5 hours, 31 minutes
Services:			
	DHCP server	⬜	
	SIP server	⬜	
	Quality of Service traffic shaping	⬜	
	UPNP	⬜	
	Clam Anti-virus server	⬜	
	Web proxy	⬜	
	Secure shell server	🟩	5 hours, 31 minutes
	Intrusion Detection System	⬜	
	IM proxy server	⬜	
	Network time server	⬜	
	POP3 proxy server	⬜	
	VPN	⬜	

SmoothWall Express 3.0-polar-i386
SmoothWall™ is a trademark of **SmoothWall Limited**.

© 2000 - 2007 **The SmoothWall Team**
Credits - Portions © **original authors**

Advanced

Displays current configuration and resource usage about SmoothWall Express, for example:



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

Memory:

	Total	Used	Free	Used %	Shared	Buffers	Cached
Mem:	256824	64712K	192112K	25%	0K	23440K	26560K
Swap:	257032	0K	257032K	0%			
Total:	513856	64712K	449144K	12%			

Disk usage:

Filesystem	Mount point	Size	Used	Available	Used %
/dev/hda4	/	5.1G	186M	4.7G	4%
/dev/hda1	/boot	20M	3.6M	16M	19%
/dev/hda3	/var/log	2.6G	33M	2.4G	2%

Inode usage:

Filesystem	Mount point	INodes	Used	Free	Used %
/dev/hda4	/	675840	27507	648333	5%
/dev/hda1	/boot	2616	20	2596	1%
/dev/hda3	/var/log	338944	34	338910	1%

Uptime and users:

15:22:15, up 5:54, 0 users, load average: 0.00, 0.00, 0.00

User	TTY	Login time	Idle	JCPU	PCPU	What

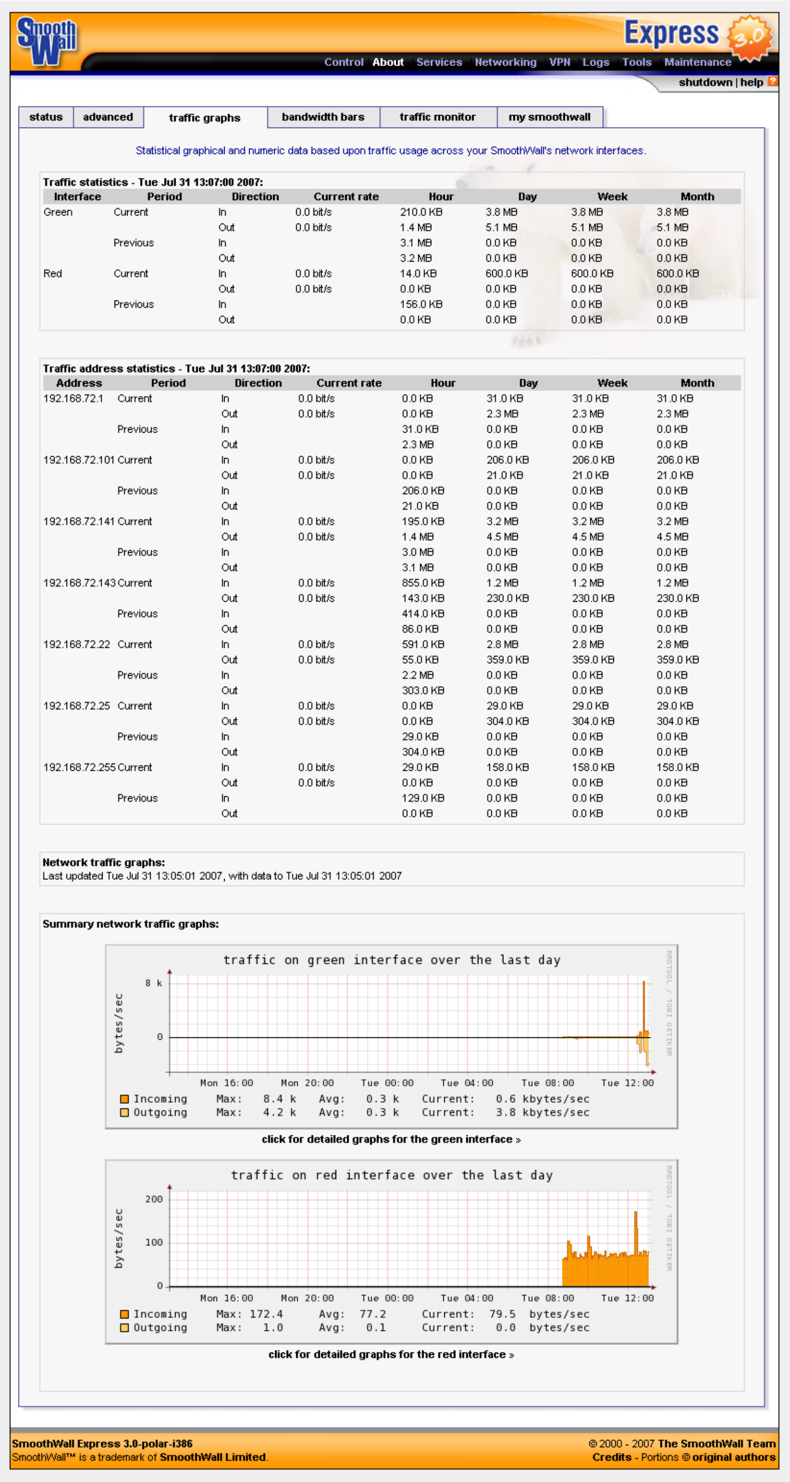
Interfaces:

eth0 (Green)			
IP Address:	192.168.72.141	Broadcast	192.168.72.255
Netmask	255.255.255.0	MTU	1500
MAC Address	00:0C:29:F8:1B:F1	Status	UP
Sent	5124481 (4	Received	(3.9 MB)

Note: Unfortunately, we have had to crop this screenshot – it's too long to fit.

Traffic Graphs

Displays statistical graphical and numeric data based on traffic across SmoothWall Express's network interfaces.



Statistical graphical and numeric data based upon traffic usage across your SmoothWall's network interfaces.

Traffic statistics - Tue Jul 31 13:07:00 2007:

Interface	Period	Direction	Current rate	Hour	Day	Week	Month
Green	Current	In	0.0 bit/s	210.0 KB	3.8 MB	3.8 MB	3.8 MB
		Out	0.0 bit/s	1.4 MB	5.1 MB	5.1 MB	5.1 MB
	Previous	In		3.1 MB	0.0 KB	0.0 KB	0.0 KB
		Out		3.2 MB	0.0 KB	0.0 KB	0.0 KB
Red	Current	In	0.0 bit/s	14.0 KB	600.0 KB	600.0 KB	600.0 KB
		Out	0.0 bit/s	0.0 KB	0.0 KB	0.0 KB	0.0 KB
	Previous	In		156.0 KB	0.0 KB	0.0 KB	0.0 KB
		Out		0.0 KB	0.0 KB	0.0 KB	0.0 KB

Traffic address statistics - Tue Jul 31 13:07:00 2007:

Address	Period	Direction	Current rate	Hour	Day	Week	Month
192.168.72.1	Current	In	0.0 bit/s	0.0 KB	31.0 KB	31.0 KB	31.0 KB
		Out	0.0 bit/s	0.0 KB	2.3 MB	2.3 MB	2.3 MB
	Previous	In		31.0 KB	0.0 KB	0.0 KB	0.0 KB
		Out		2.3 MB	0.0 KB	0.0 KB	0.0 KB
192.168.72.101	Current	In	0.0 bit/s	0.0 KB	206.0 KB	206.0 KB	206.0 KB
		Out	0.0 bit/s	0.0 KB	21.0 KB	21.0 KB	21.0 KB
	Previous	In		206.0 KB	0.0 KB	0.0 KB	0.0 KB
		Out		21.0 KB	0.0 KB	0.0 KB	0.0 KB
192.168.72.141	Current	In	0.0 bit/s	195.0 KB	3.2 MB	3.2 MB	3.2 MB
		Out	0.0 bit/s	1.4 MB	4.5 MB	4.5 MB	4.5 MB
	Previous	In		3.0 MB	0.0 KB	0.0 KB	0.0 KB
		Out		3.1 MB	0.0 KB	0.0 KB	0.0 KB
192.168.72.143	Current	In	0.0 bit/s	855.0 KB	1.2 MB	1.2 MB	1.2 MB
		Out	0.0 bit/s	143.0 KB	230.0 KB	230.0 KB	230.0 KB
	Previous	In		414.0 KB	0.0 KB	0.0 KB	0.0 KB
		Out		86.0 KB	0.0 KB	0.0 KB	0.0 KB
192.168.72.22	Current	In	0.0 bit/s	591.0 KB	2.8 MB	2.8 MB	2.8 MB
		Out	0.0 bit/s	55.0 KB	359.0 KB	359.0 KB	359.0 KB
	Previous	In		2.2 MB	0.0 KB	0.0 KB	0.0 KB
		Out		303.0 KB	0.0 KB	0.0 KB	0.0 KB
192.168.72.25	Current	In	0.0 bit/s	0.0 KB	29.0 KB	29.0 KB	29.0 KB
		Out	0.0 bit/s	0.0 KB	304.0 KB	304.0 KB	304.0 KB
	Previous	In		29.0 KB	0.0 KB	0.0 KB	0.0 KB
		Out		304.0 KB	0.0 KB	0.0 KB	0.0 KB
192.168.72.255	Current	In	0.0 bit/s	29.0 KB	158.0 KB	158.0 KB	158.0 KB
		Out	0.0 bit/s	0.0 KB	0.0 KB	0.0 KB	0.0 KB
	Previous	In		129.0 KB	0.0 KB	0.0 KB	0.0 KB
		Out		0.0 KB	0.0 KB	0.0 KB	0.0 KB

Network traffic graphs:
Last updated Tue Jul 31 13:05:01 2007, with data to Tue Jul 31 13:05:01 2007

Summary network traffic graphs:

traffic on green interface over the last day
bytes/sec
8 k
0
Mon 16:00
Mon 20:00
Tue 00:00
Tue 04:00
Tue 08:00
Tue 12:00
Incoming Max: 8.4 k Avg: 0.3 k Current: 0.6 kbytes/sec
Outgoing Max: 4.2 k Avg: 0.3 k Current: 3.8 kbytes/sec
RRDTOOL / TOBI OETIKER

click for detailed graphs for the green interface »

traffic on red interface over the last day
bytes/sec
200
100
0
Mon 16:00
Mon 20:00
Tue 00:00
Tue 04:00
Tue 08:00
Tue 12:00
Incoming Max: 172.4 Avg: 77.2 Current: 79.5 bytes/sec
Outgoing Max: 1.0 Avg: 0.1 Current: 0.0 bytes/sec
RRDTOOL / TOBI OETIKER

click for detailed graphs for the red interface »

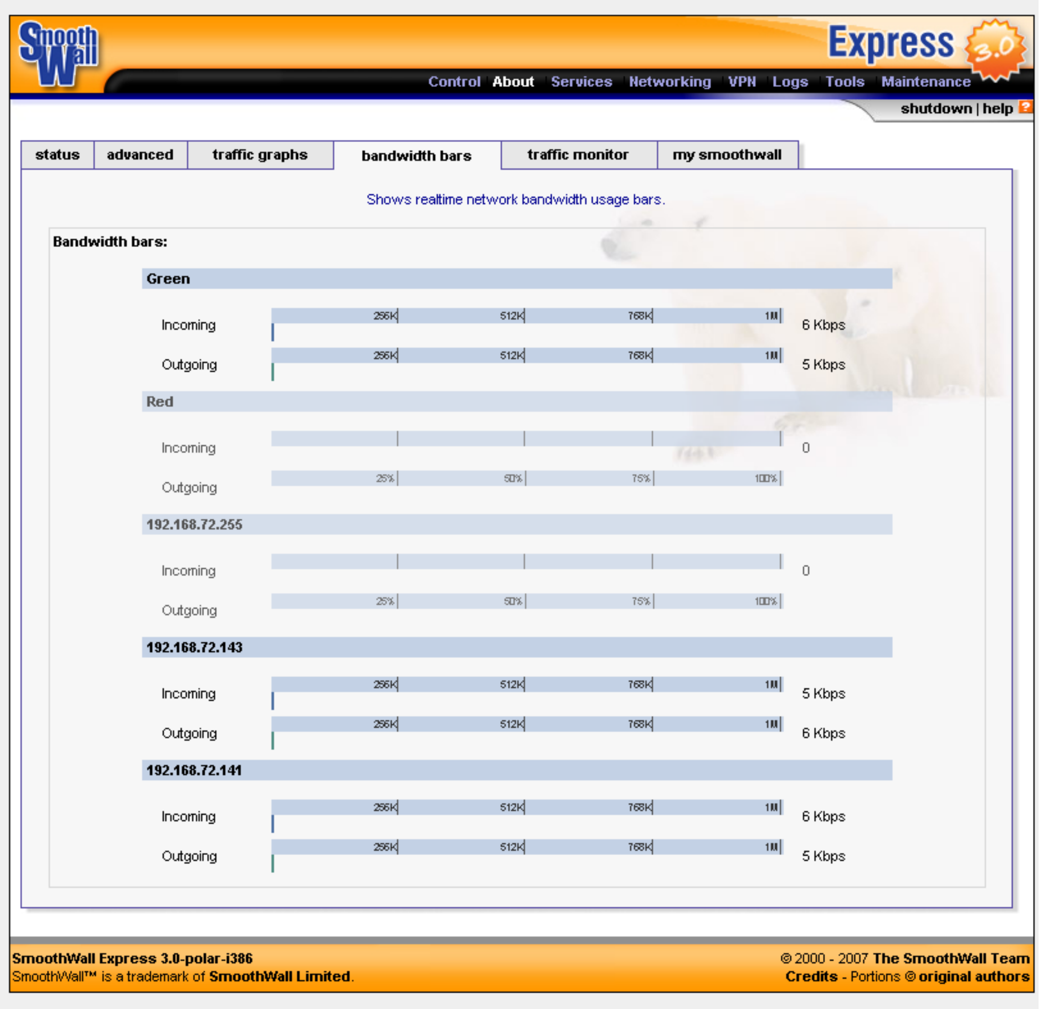
SmoothWall Express 3.0-polar-i386
SmoothWall™ is a trademark of **SmoothWall Limited.**

© 2000 - 2007 **The SmoothWall Team**
Credits - Portions © **original authors**

This page also displays traffic statistics by IP and by protocol, if QoS is enabled. See *Chapter 3, Managing Quality of Service for Traffic* on page 23 for more information.

Bandwidth Bars

Displays realtime network bandwidth usage bars, for example:



Shows realtime network bandwidth usage bars.

Bandwidth bars:

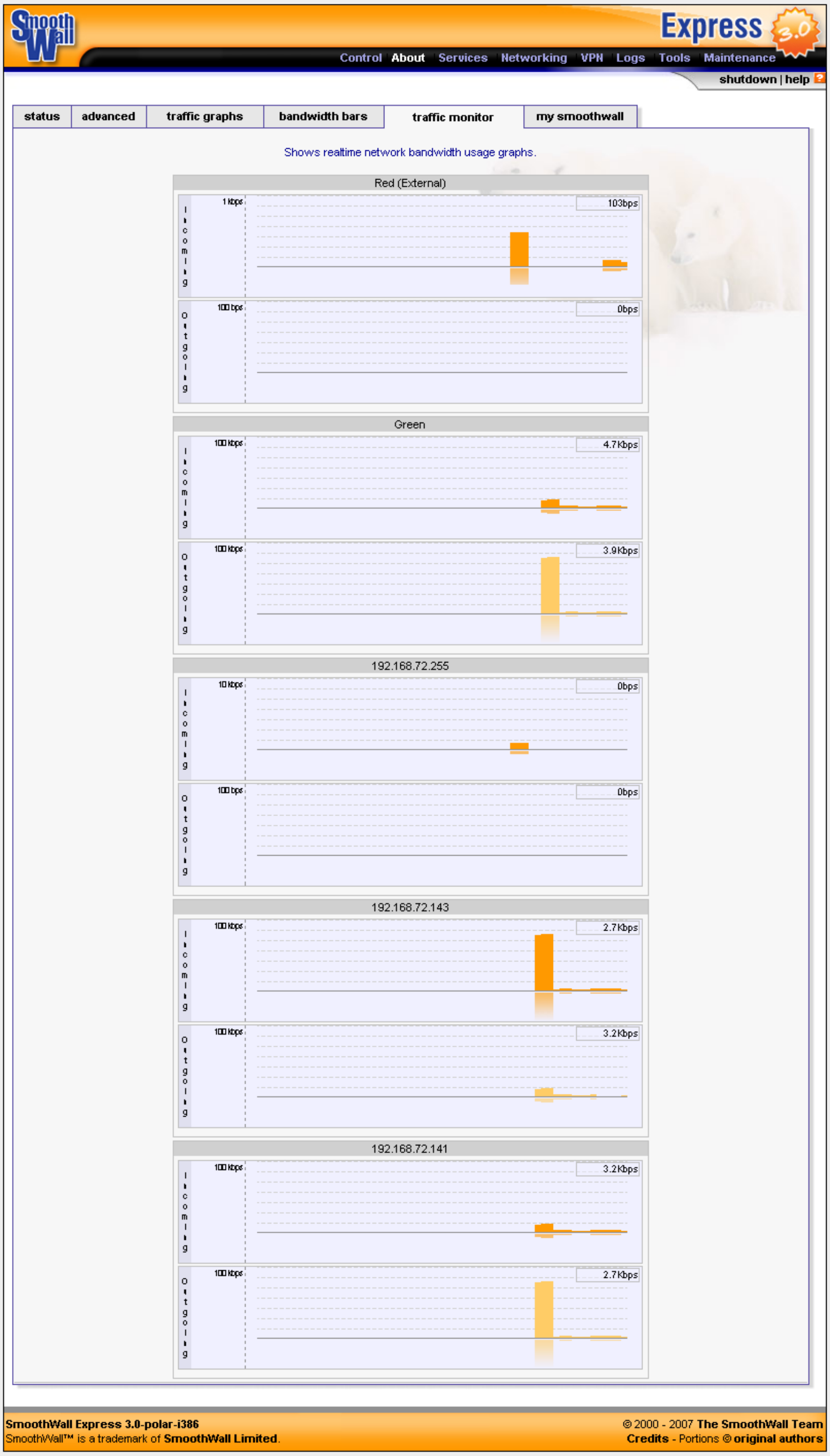
Green	
Incoming	6 Kbps
Outgoing	5 Kbps
Red	
Incoming	0
Outgoing	
192.168.72.255	
Incoming	0
Outgoing	
192.168.72.143	
Incoming	5 Kbps
Outgoing	6 Kbps
192.168.72.141	
Incoming	6 Kbps
Outgoing	5 Kbps

SmoothWall Express 3.0-polar-i386
SmoothWall™ is a trademark of **SmoothWall Limited.**

© 2000 - 2007 **The SmoothWall Team**
Credits - Portions © **original authors**

Traffic Monitor

Displays realtime network bandwidth usage graphs, for example:



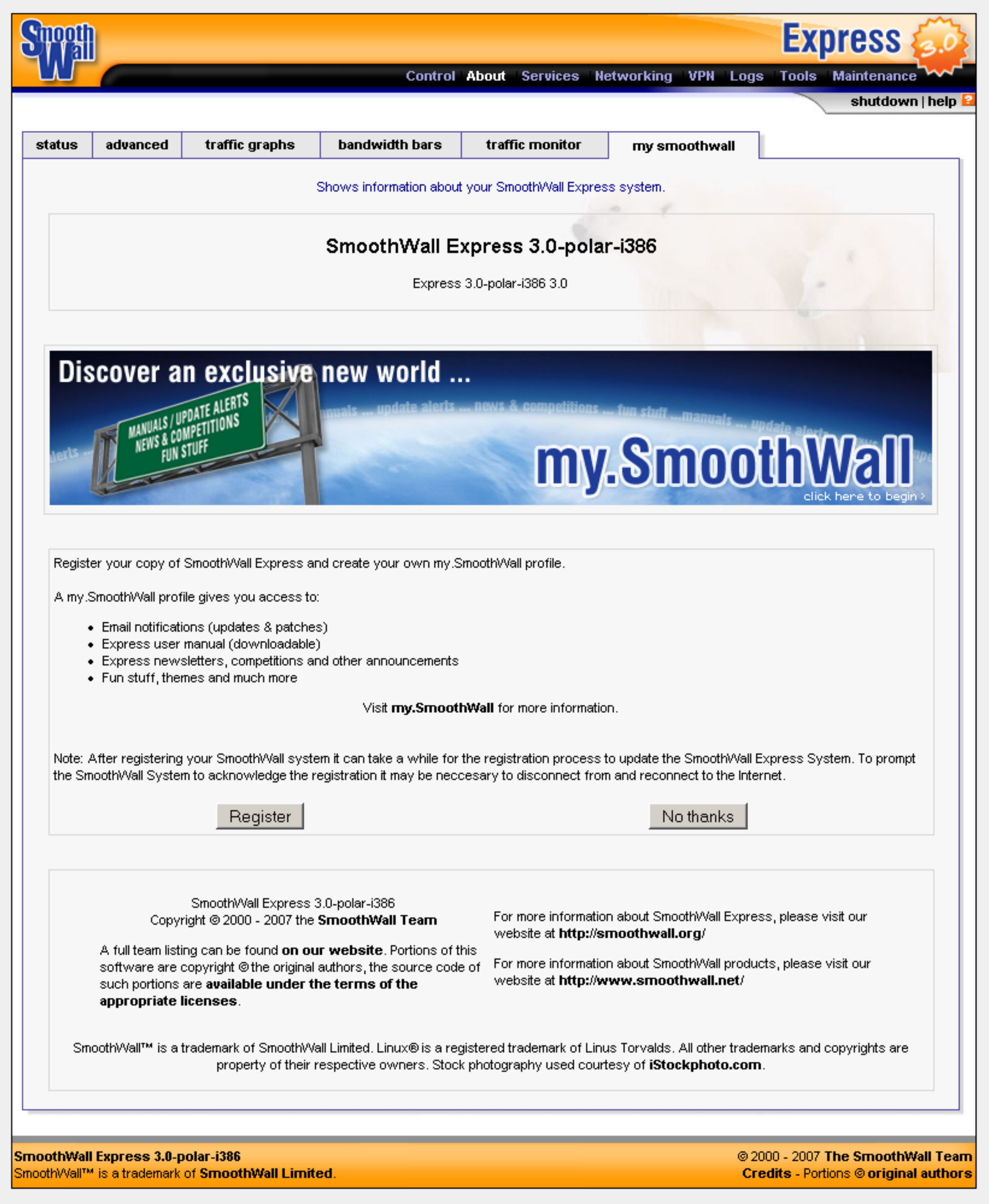
Shows realtime network bandwidth usage graphs.

SmoothWall Express 3.0-polar-i386
SmoothWall™ is a trademark of SmoothWall Limited.

© 2000 - 2007 The SmoothWall Team
Credits - Portions © original authors

Your SmoothWall Express

Displays credits and copyright information and enables you to register your SmoothWall Express and create a MySmoothWall profile.


Smooth Wall
Express 3.0
Control About Services Networking VPN Logs Tools Maintenance
shutdown | help
status advanced traffic graphs bandwidth bars traffic monitor my smoothwall
Discover an exclusive new world ...
MANUALS / UPDATE ALERTS NEWS & COMPETITIONS FUN STUFF
my.SmoothWall
click here to begin ›
Register
No thanks

Shows information about your SmoothWall Express system.

SmoothWall Express 3.0-polar-i386

Express 3.0-polar-i386 3.0

Register your copy of SmoothWall Express and create your own my.SmoothWall profile.

A my.SmoothWall profile gives you access to:

- Email notifications (updates & patches)
- Express user manual (downloadable)
- Express newsletters, competitions and other announcements
- Fun stuff, themes and much more

Visit **my.SmoothWall** for more information.

Note: After registering your SmoothWall system it can take a while for the registration process to update the SmoothWall Express System. To prompt the SmoothWall System to acknowledge the registration it may be neccesary to disconnect from and reconnect to the Internet.

SmoothWall Express 3.0-polar-i386
Copyright © 2000 - 2007 the **SmoothWall Team**

A full team listing can be found **on our website**. Portions of this software are copyright © the original authors, the source code of such portions are **available under the terms of the appropriate licenses**.

For more information about SmoothWall Express, please visit our website at **http://smoothwall.org/**

For more information about SmoothWall products, please visit our website at **http://www.smoothwall.net/**

SmoothWall™ is a trademark of SmoothWall Limited. Linux® is a registered trademark of Linus Torvalds. All other trademarks and copyrights are property of their respective owners. Stock photography used courtesy of **iStockphoto.com**.

SmoothWall Express 3.0-polar-i386
SmoothWall™ is a trademark of **SmoothWall Limited**.

© 2000 - 2007 **The SmoothWall Team**
Credits - Portions © **original authors**

To register your SmoothWall Express:

1 Click **Register** and follow the on-screen instructions.

Working with Logs

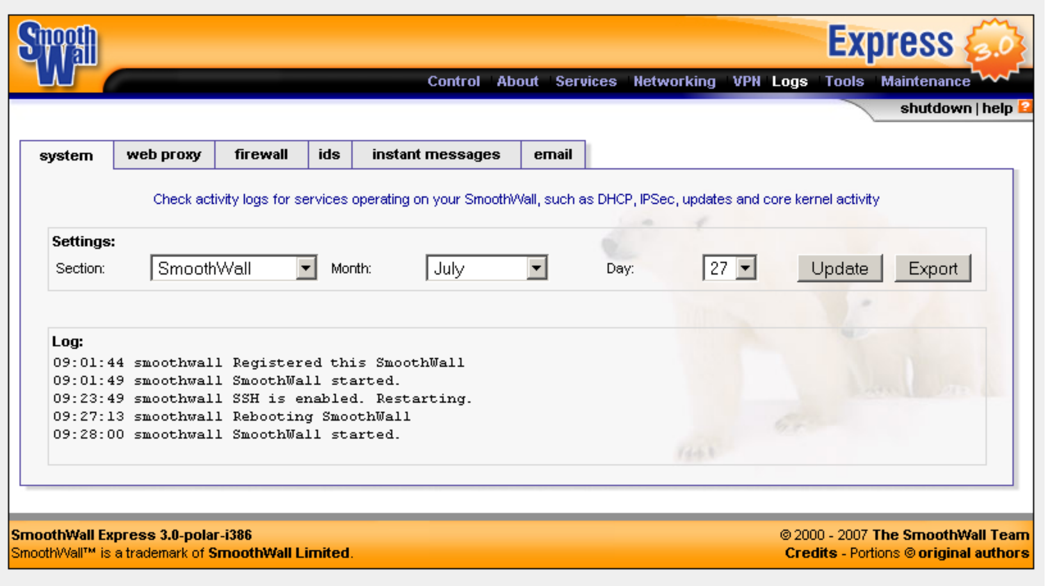
The following sections discuss SmoothWall Express's logs.

Accessing System Logs

Contains logs for the different sub-systems including: PPP logs, DHCP logs, kernel logs, SSH logs, SIP proxy, IM proxy, web proxy, a general SmoothWall log and the IPSec logs.

To access system logs:

1 Browse to the **Logs > system** page:



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

Settings:
Section: SmoothWall Month: July Day: 27

Log:

```
09:01:44 smoothwall Registered this SmoothWall
09:01:49 smoothwall SmoothWall started.
09:23:49 smoothwall SSH is enabled. Restarting.
09:27:13 smoothwall Rebooting SmoothWall
09:28:00 smoothwall SmoothWall started.
```

SmoothWall Express 3.0-polar-i386
SmoothWall™ is a trademark of **SmoothWall Limited**.
© 2000 - 2007 **The SmoothWall Team**
Credits - Portions © **original authors**

2 From the Section drop-down list, select the log you want to access.

3 Optionally, select the month and day.

4 Click **Update** to see the logs.

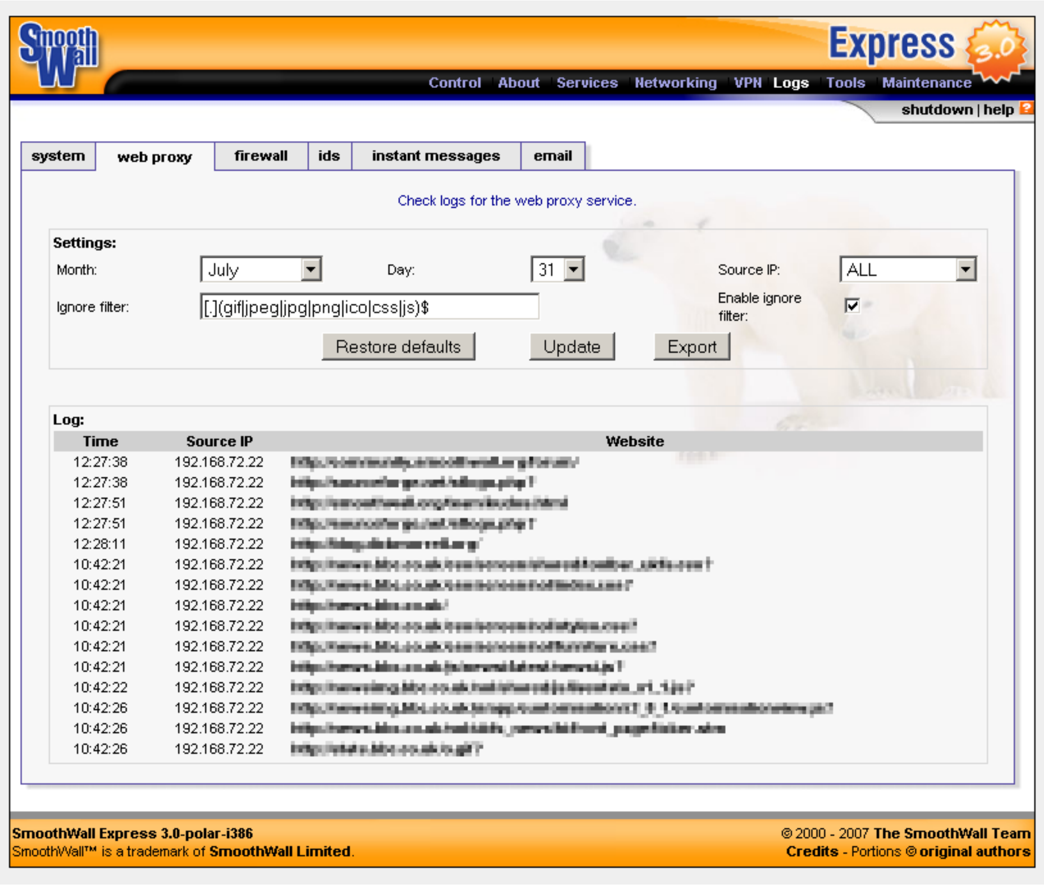
Tip: Check the PPP (dial-up) log if you are unable to establish a modem or USB ADSL (PPPoA) connection. For analogue modems, the commands sent to the modem are recorded along with the responses from the ISP and modem.

Web Proxy Logs

Contains web proxy server logs.

To access system logs:

1 Browse to the **Logs > web proxy** page:


Express 3.0
Control About Services Networking VPN Logs Tools Maintenance
shutdown | help
system web proxy firewall ids instant messages email

Check logs for the web proxy service.

Settings:

Month: July

Day: 31

Source IP: ALL

Ignore filter: [.](gif|jpeg|jpg|png|ico|css|js)$

Enable ignore filter: ☑

Restore defaults
Update
Export

Log:

Time	Source IP	Website
12:27:38	192.168.72.22	[redacted]
12:27:38	192.168.72.22	[redacted]
12:27:51	192.168.72.22	[redacted]
12:27:51	192.168.72.22	[redacted]
12:28:11	192.168.72.22	[redacted]
10:42:21	192.168.72.22	[redacted]
10:42:21	192.168.72.22	[redacted]
10:42:21	192.168.72.22	[redacted]
10:42:21	192.168.72.22	[redacted]
10:42:21	192.168.72.22	[redacted]
10:42:21	192.168.72.22	[redacted]
10:42:22	192.168.72.22	[redacted]
10:42:26	192.168.72.22	[redacted]
10:42:26	192.168.72.22	[redacted]
10:42:26	192.168.72.22	[redacted]

SmoothWall Express 3.0-polar-i386
SmoothWall™ is a trademark of SmoothWall Limited.

© 2000 - 2007 The SmoothWall Team
Credits - Portions © original authors

Note: Some information has been pixelated for privacy reasons.

2 Configure the following settings:

Setting	Description
Month	Select the month you want to view.
Day	Select the day you want to view.
Source IP	Optionally, from the drop-down list, select the IP address whose proxy information you wan to see.
Ignore filter	Accept the default or edit this list of image file extensions to prevent images being listed in the log. If you understand regular expressions, you can make up your own string.
Enable ignore filter	Select to enable the ignore filter.

3 Click **Update** to see the logs.

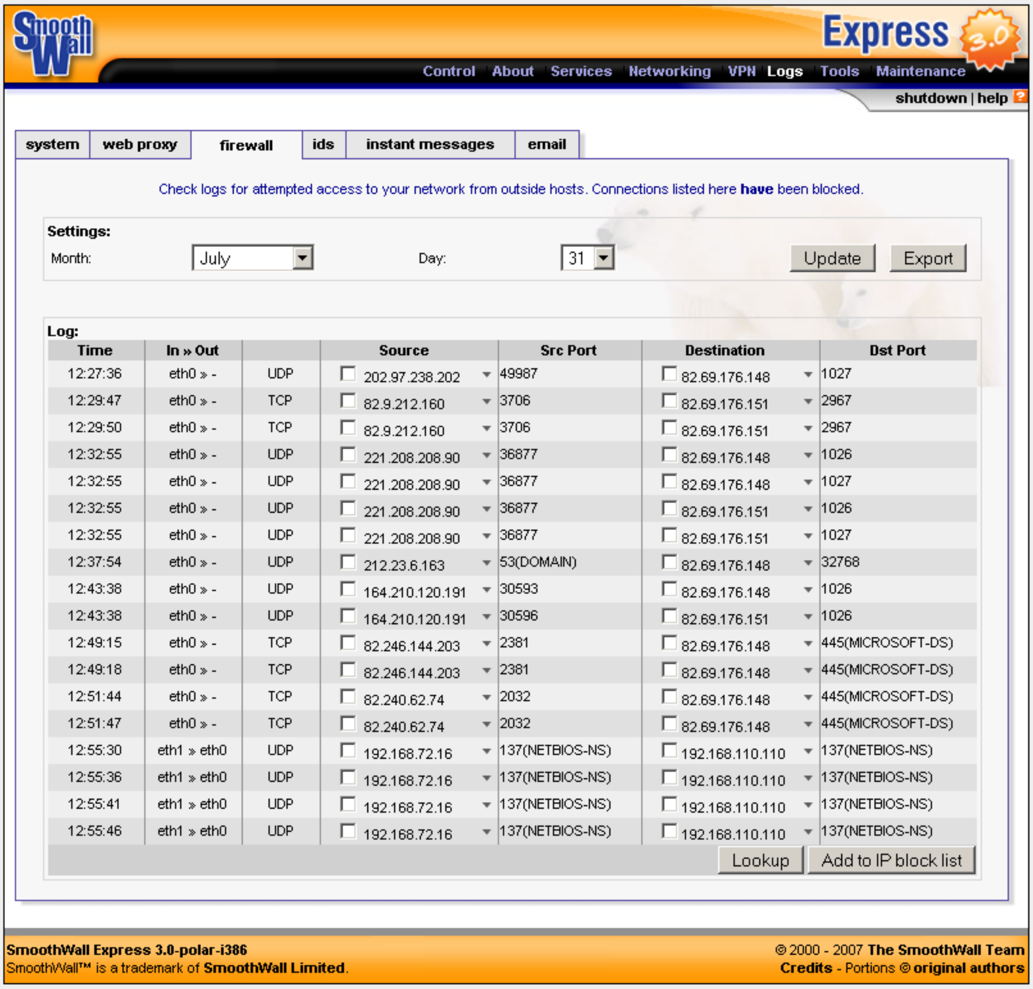
Firewall Logs

Displays a log of packets that were dropped by SmoothWall Express.

Note: Not all denied packets are hostile attempts by crackers to gain access to your network. Connections to the ident/authentication port (113) are common occurrences and can be ignored.

To view the firewall log:

1 Browse to the **Logs > web proxy** page:



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

Settings:
Month: July
Day: 31

Log:

Time	In » Out		Source	Src Port	Destination	Dst Port
12:27:36	eth0 » -	UDP	□ 202.97.238.202	49987	□ 82.69.176.148	1027
12:29:47	eth0 » -	TCP	□ 82.9.212.160	3706	□ 82.69.176.151	2967
12:29:50	eth0 » -	TCP	□ 82.9.212.160	3706	□ 82.69.176.151	2967
12:32:55	eth0 » -	UDP	□ 221.208.208.90	36877	□ 82.69.176.148	1026
12:32:55	eth0 » -	UDP	□ 221.208.208.90	36877	□ 82.69.176.148	1027
12:32:55	eth0 » -	UDP	□ 221.208.208.90	36877	□ 82.69.176.151	1026
12:32:55	eth0 » -	UDP	□ 221.208.208.90	36877	□ 82.69.176.151	1027
12:37:54	eth0 » -	UDP	□ 212.23.6.163	53(DOMAIN)	□ 82.69.176.148	32768
12:43:38	eth0 » -	UDP	□ 164.210.120.191	30593	□ 82.69.176.148	1026
12:43:38	eth0 » -	UDP	□ 164.210.120.191	30596	□ 82.69.176.151	1026
12:49:15	eth0 » -	TCP	□ 82.246.144.203	2381	□ 82.69.176.148	445(MICROSOFT-DS)
12:49:18	eth0 » -	TCP	□ 82.246.144.203	2381	□ 82.69.176.148	445(MICROSOFT-DS)
12:51:44	eth0 » -	TCP	□ 82.240.62.74	2032	□ 82.69.176.148	445(MICROSOFT-DS)
12:51:47	eth0 » -	TCP	□ 82.240.62.74	2032	□ 82.69.176.148	445(MICROSOFT-DS)
12:55:30	eth1 » eth0	UDP	□ 192.168.72.16	137(NETBIOS-NS)	□ 192.168.110.110	137(NETBIOS-NS)
12:55:36	eth1 » eth0	UDP	□ 192.168.72.16	137(NETBIOS-NS)	□ 192.168.110.110	137(NETBIOS-NS)
12:55:41	eth1 » eth0	UDP	□ 192.168.72.16	137(NETBIOS-NS)	□ 192.168.110.110	137(NETBIOS-NS)
12:55:46	eth1 » eth0	UDP	□ 192.168.72.16	137(NETBIOS-NS)	□ 192.168.110.110	137(NETBIOS-NS)

SmoothWall Express 3.0-polar-i386
SmoothWall™ is a trademark of SmoothWall Limited.

© 2000 - 2007 The SmoothWall Team
Credits - Portions © original authors

2 Select the month and day and click **Update** to see the logs.

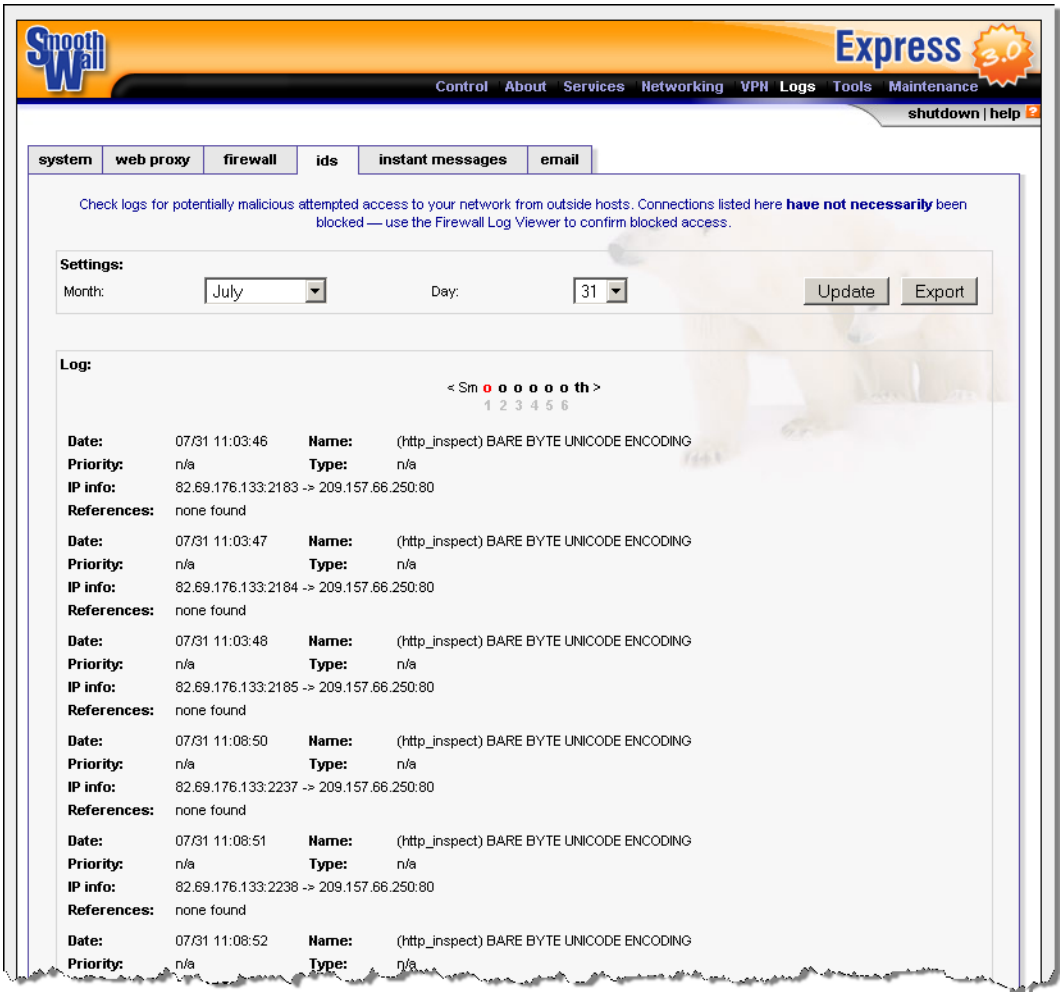
Tip: Every IP address has a small arrow and a checkbox. Click the arrow to perform whois look-ups and IP blocks from within the firewall log viewer itself. Use the checkboxes to select multiple entries. The whois function is useful for determining who is scanning your SmoothWall.

IDS Logs

Displays potentially malicious, attempted access to your network from outside hosts. Connections listed here have not necessarily been blocked. Use the firewall log to confirm blocked access.

To access IDS logs:

1 Browse to the **Logs > ids** page:



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: July
Day: 31

Log:

```
Date:        07/31 11:03:46                      Name:   (http_inspect) BARE BYTE UNICODE ENCODING
Priority:    n/a                                 Type:   n/a
IP info:     82.69.176.133:2183 -> 209.157.66.250:80
References:  none found

Date:        07/31 11:03:47                      Name:   (http_inspect) BARE BYTE UNICODE ENCODING
Priority:    n/a                                 Type:   n/a
IP info:     82.69.176.133:2184 -> 209.157.66.250:80
References:  none found

Date:        07/31 11:03:48                      Name:   (http_inspect) BARE BYTE UNICODE ENCODING
Priority:    n/a                                 Type:   n/a
IP info:     82.69.176.133:2185 -> 209.157.66.250:80
References:  none found

Date:        07/31 11:08:50                      Name:   (http_inspect) BARE BYTE UNICODE ENCODING
Priority:    n/a                                 Type:   n/a
IP info:     82.69.176.133:2237 -> 209.157.66.250:80
References:  none found

Date:        07/31 11:08:51                      Name:   (http_inspect) BARE BYTE UNICODE ENCODING
Priority:    n/a                                 Type:   n/a
IP info:     82.69.176.133:2238 -> 209.157.66.250:80
References:  none found

Date:        07/31 11:08:52                      Name:   (http_inspect) BARE BYTE UNICODE ENCODING
Priority:    n/a                                 Type:   n/a
```

Note: Unfortunately, we have had to crop this screenshot – it's too long to fit.

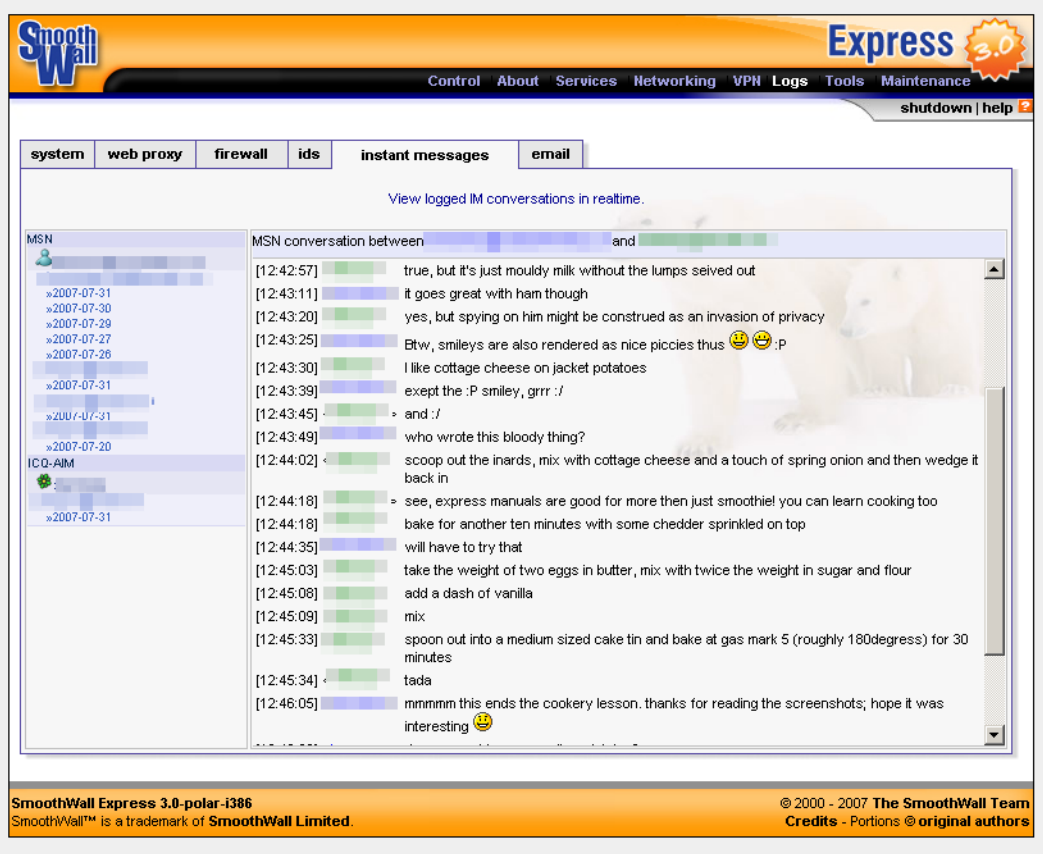
2 Select the month and day and click **Update** to see the logs.

Instant Messages Logs

Displays near-realtime information on instant messages.

To review the instant message logs:

1 Browse to the Logs > instant messages page:



View logged IM conversations in realtime.

MSN conversation between and

```
[12:42:57]  true, but it's just mouldy milk without the lumps seived out
[12:43:11]  it goes great with ham though
[12:43:20]  yes, but spying on him might be construed as an invasion of privacy
[12:43:25]  Btw, smileys are also rendered as nice piccies thus 😃 😃 :P
[12:43:30]  I like cottage cheese on jacket potatoes
[12:43:39]  exept the :P smiley, grrr :/
[12:43:45]  and :/
[12:43:49]  who wrote this bloody thing?
[12:44:02]  scoop out the inards, mix with cottage cheese and a touch of spring onion and then wedge it
            back in
[12:44:18]  see, express manuals are good for more then just smoothie! you can learn cooking too
[12:44:18]  bake for another ten minutes with some chedder sprinkled on top
[12:44:35]  will have to try that
[12:45:03]  take the weight of two eggs in butter, mix with twice the weight in sugar and flour
[12:45:08]  add a dash of vanilla
[12:45:09]  mix
[12:45:33]  spoon out into a medium sized cake tin and bake at gas mark 5 (roughly 180degress) for 30
            minutes
[12:45:34]  tada
[12:46:05]  mmmmm this ends the cookery lesson. thanks for reading the screenshots; hope it was
            interesting 😃
```

SmoothWall Express 3.0-polar-i386
SmoothWall™ is a trademark of SmoothWall Limited.

© 2000 - 2007 The SmoothWall Team
Credits - Portions © original authors

Note: Some information has been pixelated for privacy reasons.

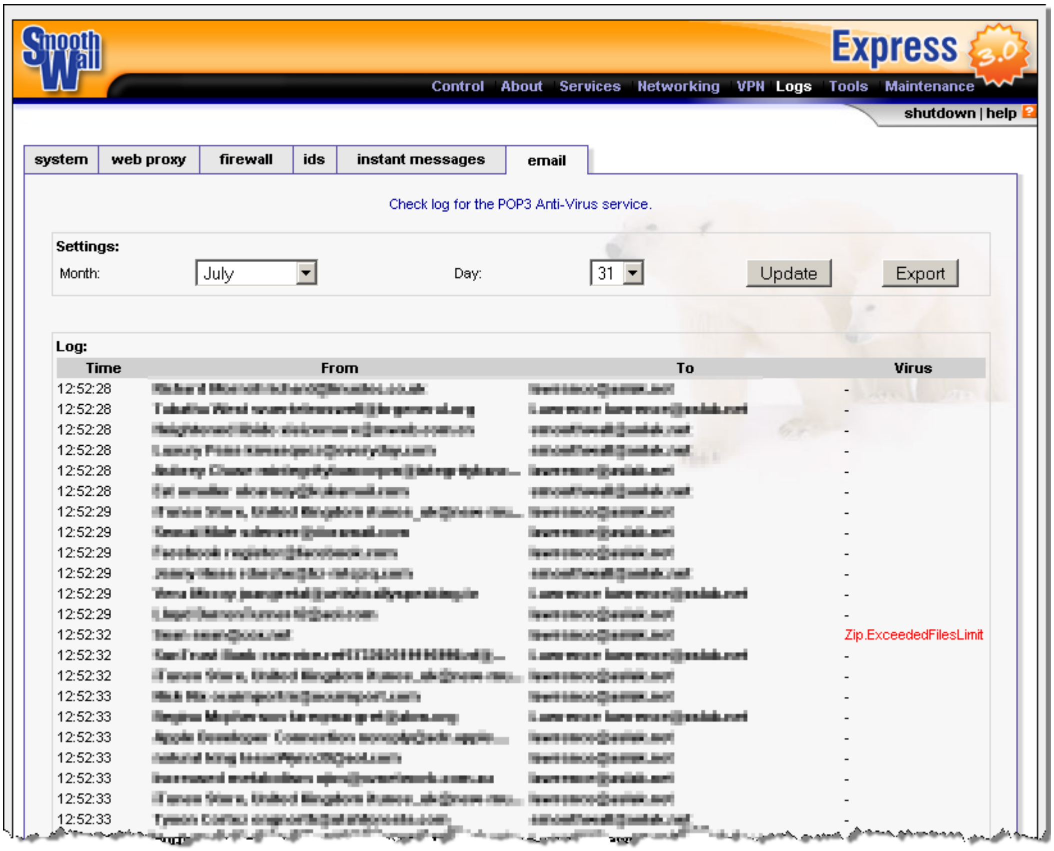
2 Select the date of the log you want to read. The right hand portion of the screen updates to show the chat transcript. It will also periodically refresh, enabling you to view the selected conversation in near-realtime.

Email Logs

Displays a log of all emails passing though the POP3 proxy and anti-virus engine. Viruses are shown in highlighted text.

To access email logs:

1 Browse to the **Logs > email** page:



Check log for the POP3 Anti-Virus service.

Settings:

Month: July

Day: 31

Update

Export

Log:

Time	From	To	Virus
12:52:28	[redacted]	[redacted]	-
12:52:28	[redacted]	[redacted]	-
12:52:28	[redacted]	[redacted]	-
12:52:28	[redacted]	[redacted]	-
12:52:28	[redacted]	[redacted]	-
12:52:28	[redacted]	[redacted]	-
12:52:29	[redacted]	[redacted]	-
12:52:29	[redacted]	[redacted]	-
12:52:29	[redacted]	[redacted]	-
12:52:29	[redacted]	[redacted]	-
12:52:29	[redacted]	[redacted]	-
12:52:29	[redacted]	[redacted]	-
12:52:32	[redacted]	[redacted]	Zip.ExceededFilesLimit
12:52:32	[redacted]	[redacted]	-
12:52:32	[redacted]	[redacted]	-
12:52:33	[redacted]	[redacted]	-
12:52:33	[redacted]	[redacted]	-
12:52:33	[redacted]	[redacted]	-
12:52:33	[redacted]	[redacted]	-
12:52:33	[redacted]	[redacted]	-
12:52:33	[redacted]	[redacted]	-
12:52:33	[redacted]	[redacted]	-

2 Select the month and day and click **Update** to see the logs.

Note: Unfortunately, we have had to crop this screenshot – it's too long to fit. Email addresses have been pixelated for privacy reasons.

Index