

Secure Router User Guide



**Secure Router
User Guide**

Secure Router User Guide

This document is the copyright of Teltronics, Inc. and is intended for exclusive use of Teltronics customers. All rights are reserved. Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Teltronics, Inc.

© 2006 Teltronics, Inc. All rights reserved.

The material in this document has been carefully reviewed; however, Teltronics, Inc. does not guarantee it to be free of all errors or omissions and reserves the right to make corrections, changes, updates, or revisions to the information contained herein.

Other than those held by Teltronics, Inc., any other brand and product names referenced in this manual are trademarks or registered trademarks of their respective holders and are used here for informational purposes only.

Teltronics, Inc.
2150 Whitfield Industrial Way
Sarasota, Florida 34243-4046 USA

Part Number: 610-0000-0514 Rev. B (Feb/06)

Contents

1. Introduction.....	1
NET-PATH Plus Secure Router	1
2. Getting Started.....	3
Secure Router.....	4
3. Network Setup.....	15
Configuring Connections	15
Direct Connection	16
ADSL.....	20
Cable Modem.....	23
Failover, Load Balancing and High Availability	25
Internet Failover.....	25
Internet Load Balancing.....	30
High Availability	31
Bridging	32
GRE Tunnels.....	35
Routes	39
System.....	40
DNS	40
DHCP Server	40
QoS Traffic Shaping	44
4. Firewall.....	47
Incoming Access.....	47
Web Server.....	49
Customizing the Firewall.....	50
Definitions.....	50
Packet Filtering	53
Network Address Translation (NAT)	55
Connection Tracking.....	64
Intrusion Detection.....	65
Basic Intrusion Detection and Blocking (IDB).....	67
Access Control and Content Filtering.....	69

5.	Virtual Private Networking	75
	PPTP and L2TP.....	76
	PPTP VPN Server	76
	L2TP VPN Server	83
	PPTP and L2TP VPN Client.....	90
	IPSec	92
	Set Up the Branch Office.....	92
	Configuring the Headquarters.....	104
	Tunnel List.....	106
	NAT Traversal Support.....	109
	Certificate Management.....	109
	IPSec Troubleshooting.....	114
	Port Tunnels	117
6.	System	121
	Date and Time.....	121
	Backup/Restore Configuration.....	122
	Users	125
	Management.....	128
	Diagnostics.....	131
	Advanced	131
	Reboot and Reset	135
	Flash upgrade	135
	Configuration Files	137
	Support.....	138
	Appendix A – Terminology	141
	Appendix B – System Log.....	147
	Access Logging.....	147
	Creating Custom Log Rules.....	149
	Rate Limiting	152
	Administrative Access Logging.....	153
	Boot Log Messages.....	153
	Appendix C – Firmware Upgrade Practices and Precautions	155
	Appendix D – Recovering From a Failed Upgrade	157

1. Introduction

The NET-PATH Plus introduces the Secure Router component that provides a second Ethernet interface and VPN firewall functions. This manual describes the features and capabilities of the Secure Router and provides you with instructions on how to best take advantage of them.

This includes setting up network connections (in the chapter entitled *Network Connections*), tailoring the firewall to your network (*Firewall*), and establishing a virtual private network (*Virtual Private Networking*). It also guides you through setting up the Secure Router on your existing or new network using the web management console (*Getting Started*).

This chapter provides an overview to familiarize you with the Secure Router's features and capabilities.

NET-PATH Plus Secure Router

The Secure Router range provides Internet security and privacy of communications for small- and medium-sized enterprises and branch offices. It simply and securely connects your office to the Internet, and with its robust stateful firewall, shields your computers from external threats.

With the Secure Router's masquerading firewall, hosts on your LAN (local area network) can see and access resources on the Internet, but all outsiders see is the Secure Router's external address.

You can tailor your Secure Router to disallow access from your LAN to specific Internet sites or categories of content, give priority to specific types of network traffic, and allow controlled access to your LAN from the outside world. You can also enable intrusion detection and prevention services on your Secure Router to further bolster the security of your local network.

The Secure Router lets you establish a virtual private network (VPN). A VPN enables remote workers or branch offices to connect securely to your LAN over the public Internet. The Secure Router can also connect to external VPNs as a client.

You can configure the Secure Router with multiple Internet connections. These auxiliary connections can be kept on stand-by should the primary connection become unavailable, or maintained concurrently with the primary connection for spreading network load.

This page intentionally left blank.

2. Getting Started

Your *NET-PATH Plus Installation and Operation Guide* that shipped with your Secure Router gives you basic setup information for the Secure Router. It is a dedicated programming guide that offers advanced programming information. This chapter provides step-by-step instructions for installing your Secure Router.

These instructions assume you have a PC running Microsoft Windows 2000/XP. You must have an Ethernet network interface card installed. You may need to be logged in with administrator privileges.

Instructions are not given for other operating systems; refer to your operating system documentation on how to configure your PCs' network settings using the examples given for Windows PCs as a guide.

Note

Installing your Secure Router into a well-planned network is easy. However, network planning is outside the scope of this manual. Please take the time to plan your network before installing your Secure Router.

Secure Router

Set up a PC to connect to the web management console

The Secure Router ships with initial, static IP settings of:

IP address:	192.168.0.1
Subnet mask:	255.255.255.0

Your Secure Router needs a suitable IP address before it is connected to your LAN. You may choose to use the Secure Router's initial network settings as a basis for your LAN settings.

1. Connect the supplied power adapter to the NET-PATH Plus.
 - If you are setting up the SECURE ROUTER, attach your PC's network interface card directly to any of NET-PATH Plus LAN switch ports.

Note

*You may attach the Secure Router directly to your LAN at this point; however, **before doing so, it is critical that you ensure there are no other devices or PCs on the LAN with an address of 192.168.0.1.***

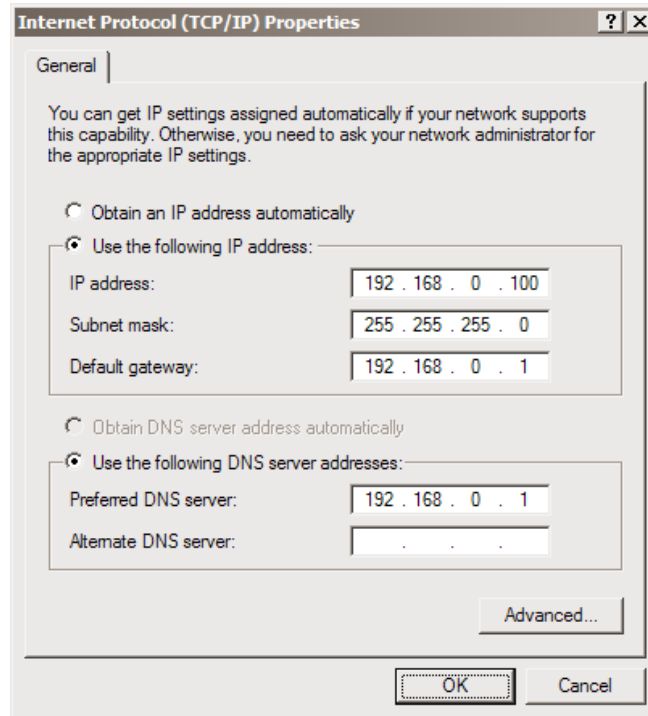
All other network ports are by default inactive, i.e. they are not running any network services such as DHCP, and they are not configured with an IP address.

2. Next, you must modify your PC's network settings to enable it to communicate with the Secure Router.
3. Click **Start** -> (**Settings** ->) **Control Panel** and double click **Network Connections**.
4. Right-click **Local Area Connection**; then, select **Properties**.

Note

If there is more than one existing network connection, select the one corresponding to the network interface card to which the Secure Router is directly attached.

5. Select **Internet Protocol (TCP/IP)** and click **Properties**.



6. Select **Use the following IP address** and enter the following details:

IP address: **192.168.0.100**
Subnet mask: **255.255.255.0**
Default gateway: **192.168.0.1**

7. Select **Use the following DNS server addresses** and enter:

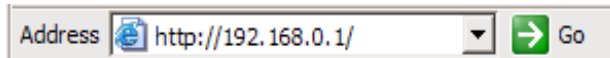
Preferred DNS server: **192.168.0.1**

Note

*If you wish to retain your existing IP settings for this network connection, click **Advanced** and **Add** the secondary IP address of **192.168.0.100**, subnet mask **255.255.255.0**.*

Set up the password and LAN connection settings

1. Launch Internet Explorer (or your preferred web browser) and navigate to **192.168.0.1**.



The web management console displays.

2. Select **Quick Setup Wizard** from the center of the page.

A log in prompt is displayed. Enter the initial user name and password for your Secure Router:

User name:	root
Password:	default

Note

If you are unable to connect to the web management console at 192.168.0.1, or the initial username and password are not accepted; then, this stage of the installation has already been performed. You will need to obtain the username and password, and possibly the IP address, from your system administrator.

3. Enter and confirm a password for your Secure Router. This is the password for the user *root*, the main administrative user account on the Secure Router. It is therefore important that you choose a password that is hard to guess, and keep it safe.

The new password takes effect immediately; you are prompted to enter it upon completing the next step.

The quick setup wizard is displayed.

Quick Setup

LAN -> Internet -> Confirm -> Done

This setup wizard will guide you through some of the required initial configuration. If the local network interface is already properly configured, or if you would like to defer this step until later, select the *skip* option.

Use the NET-PATH Plus embedded name as the Secure Router HOSTNAME.

Hostname

The Secure Router's local IP address (LAN) can be dynamically assigned by an existing DHCP server or configured manually. NET-PATH Plus applications require static IP addresses, which are configured using the manual configuration option.

LAN IP Configuration

- Obtain LAN IP address from a DHCP server on LAN
- Manual configuration
- Skip: LAN already configured

Hostname: Enter the embedded name of the NET-PATH Plus as the hostname. This will be the only reference that links the Secure Router database to the remote agent.

Manual configuration: Select this to manually specify your Secure Router's LAN connection settings.

Skip: LAN already configured: Select this if you wish to use the Secure Router's initial network settings (IP address 192.168.0.1 and subnet mask 255.255.255.0) as a basis for your LAN settings. You may skip to *Set up Internet Connection Settings*.

Obtain LAN IP address from a DHCP server on LAN (not generally recommended): The Secure Router's local IP address (LAN) can be dynamically assigned by an existing DHCP server or configured manually. NET-PATH Plus applications require static IP addresses, which are configured using the manual configuration option.

4. Click **Next**.

Manual LAN Configuration

LAN -> Internet -> Confirm -> Done

Configure the local network (LAN) interface.

Select the address that the Secure Router should use for its LAN network interface. This must be an address that lies within the range of the local network and that is not used by any other host.

IP Address

The subnet mask determines the logical size of the local area network.

Subnet Mask

Select the range of addresses that the DHCP server on this Secure Router unit may assign to other machines on the LAN. (May be left blank to disable the DHCP server)

DHCP Server Address Range

Note

*This page only displays if you previously selected **Manual configuration**. Otherwise skip to **Set up Internet Connection Settings**.*

5. Enter an **IP address** and **Subnet mask** for your Secure Router's LAN connection. You may choose to use the Secure Router's initial network settings if you are sure no other PC or network device already has the address of 192.168.0.1.

The **IP address** can be used as the gateway address for the devices on the LAN. To gain access through this gateway, the devices on the LAN must have an IP address within the bounds of the subnet described by the Secure Router's IP address and subnet mask (e.g. using the Secure Router's initial network settings, 192.168.0.2 – 192.168.0.254).

Take note of this IP address and subnet mask, as you need them later on.

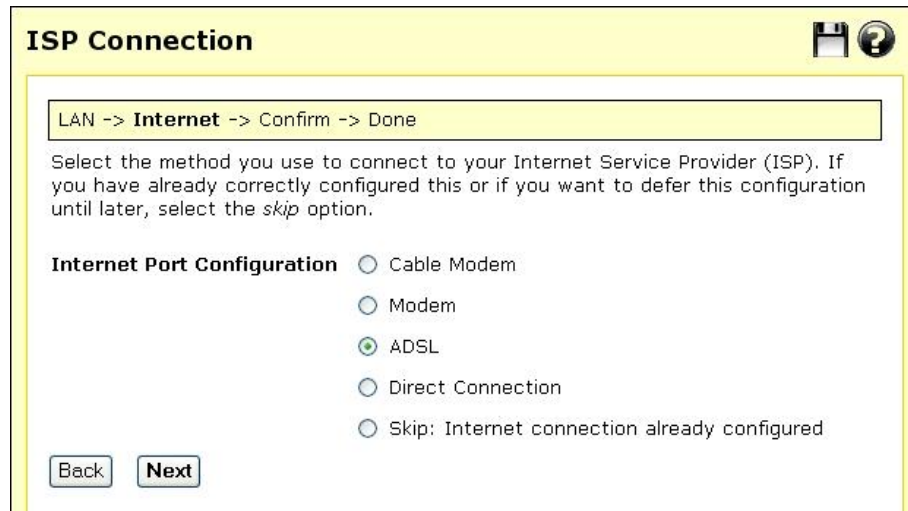
6. Click **Next** to set up your Secure Router's Internet connection settings and connect to the Internet.

Set up Internet connection settings

1. Select your Internet connection type. The Internet connection is made through the port labeled “WAN” on the NET-PATH Plus.

Note

Most applications use Direct Connection.



Cable Modem: If connecting using a cable modem, select the appropriate ISP on the next page. Choose **Generic cable modem provider** if yours does not appear.

Modem: If connecting using a regular analog modem, enter the details provided by your ISP.

ADSL: If connecting using an ADSL modem, select **Auto detect ADSL connection type** and enter the details provided by your ISP. If auto detection fails and you are unsure of your ADSL connection type, contact your ISP.

Direct Connection: If you have a direct connection to the Internet (e.g. a leased line), enter the IP settings provided by your ISP.

Note

For detailed help for each of these options, please refer to the chapter entitled Network Setup.

2. Click **Next**.

Set up the PCs on your LAN to access the Internet

1. Once the Secure Router's Internet connection has been set up, click **Next**; then, select **Finish**.

Note

If you have changed the Secure Router's LAN connection settings, you may not be able to contact it at this point. This step describes how to set up the PCs on your network to access the Secure Router and the Internet.

2. Connect your Secure Router to your LAN if you have not already done so.
3. To set up the Secure Router, connect PCs and your LAN hub directly to the LAN port.
4. Connect your Secure Router's LAN port directly to your LAN hub using the straight through Ethernet cable.
5. To access the Internet, the devices on your network must all be set up to use the Secure Router as their default gateway. This can be done a number of different ways depending on how your LAN is set up.

Note

The NET-PATH Plus application requires static IP addresses. The Secure Router supports a DHCP server for selected applications. Devices monitored by NET-PATH Plus should not use DHCP.

- If your LAN already has a DHCP server (aside from the Secure Router you are setting up), proceed to *LAN with a DHCP server*.
- If your LAN does not have a DHCP server, proceed to *LAN with no DHCP server*.

If you are not sure, you probably want *LAN with no DHCP server*.

LAN with a DHCP server

1. Add a lease to your existing DHCP server to reserve the IP address you chose in **STEP 3** for the Secure Router's LAN connection.

If you chose to set the Secure Router's LAN connection settings using **Manual configuration**, you may simply remove this address from the pool of available addresses.

2. Enter this same IP address as the gateway IP address to be handed out by the DHCP server.

3. Enter this same IP address as the DNS server IP address to be handed out by the DHCP server.
4. Restart all the PCs on the network (this resets their gateway and DNS addresses).

Note

*The purpose of restarting the computers is to force them to gain a new DHCP lease. Alternatively you can use a utility such as **ipconfig** to release then renew a lease, or disable and re-enable the network connection.*

LAN with no DHCP server

A DHCP server allows PCs to automatically obtain network settings when they start up. If your network does not have a DHCP server, you may either manually set up each PC on your network, or set up the Secure Router's DHCP server.

Note

If you only have a few PCs, we suggest manually setting up your network. If you have more PCs, enabling the Secure Router's DHCP server is more scalable.

To manually set up each Windows PC on your network:

1. Click **Start** -> (**Settings** ->) **Control Panel** and double click **Network Connections**.
2. If presented with multiple connections, right-click **Local Area Connection**; then, select **Properties**.
3. Select **Internet Protocol (TCP/IP)** and click **Properties** (or in 95/98/Me, **TCP/IP** -> [**your network card name**] if there are multiple entries).
4. Enter the following details:

IP address is an IP address that is part of the same subnet range as the Secure Router's LAN connection (e.g. if using the default settings, 192.168.0.2 – 192.168.0.254).

- **Subnet mask** is the subnet mask of the Secure Router's LAN connection.
 - **Default gateway** is the IP address of the Secure Router's LAN connection.
 - **Preferred DNS server** is the IP address of your network's domain name server.
5. Click **OK**.
 6. Perform these steps for each PC on your network.

Alternatively, to activate your Secure Router's DHCP server:

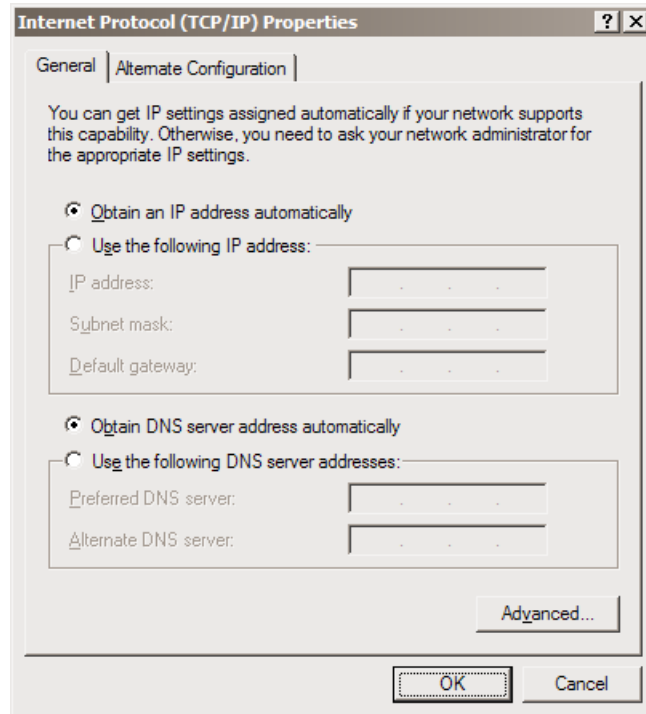
1. Launch Internet Explorer (or your preferred web browser) and navigate to the IP address of the Secure Router's LAN connection.
2. The web management console is displayed.
3. Select **DHCP Server** from the **Network Setup** menu.
4. Select **Server** from the Type drop-box; then, configure the DHCP server with the following details:
 - **Gateway Address** is the IP address of the Secure Router's LAN connection, it may be left blank.
 - **DNS Address** is the IP address of your network's name server. It may be left blank.
 - **Domain Name** (optional) is the name of the domain to be configured on the DHCP client.
 - **WINS Address** (optional) is the IP address of any existing WINS server on your LAN.
 - **Default Lease Time and Maximum Lease Time** should generally be left at their default values.
 - **Address Range** is a range of free IP addresses on your LAN's subnet for the Secure Router to hand out to PCs on your LAN. Use the format "192.168.0.100-150" to specify a range.

Note

For a detailed description of configuring DHCP Server Settings, please refer to the DHCP Server section of the chapter entitled Network Connections.

Each PC on your LAN must now be set up to use DHCP. For each PC on your LAN:

5. Click **Start** -> (**Settings** ->) **Control Panel** and double click **Network Connections**.
6. If presented with multiple connections, right-click **Local Area Connection** (or appropriate network connection); then, select **Properties**.
7. Select **Internet Protocol (TCP/IP)** and click **Properties**.



8. Check **Obtain an IP address automatically**, check **Obtain DNS server address automatically** and click **OK**.

Quick setup is now complete.

This page intentionally left blank.

3. Network Setup

This chapter describes the **Network Setup** sections of the web management console. Here you can configure each of your Secure Router's Ethernet ports. It is accessed by clicking **Network Setup** under the **Network Setup** section of the main web management console menu.

The **QoS Traffic Shaping** section is also described later in this chapter.

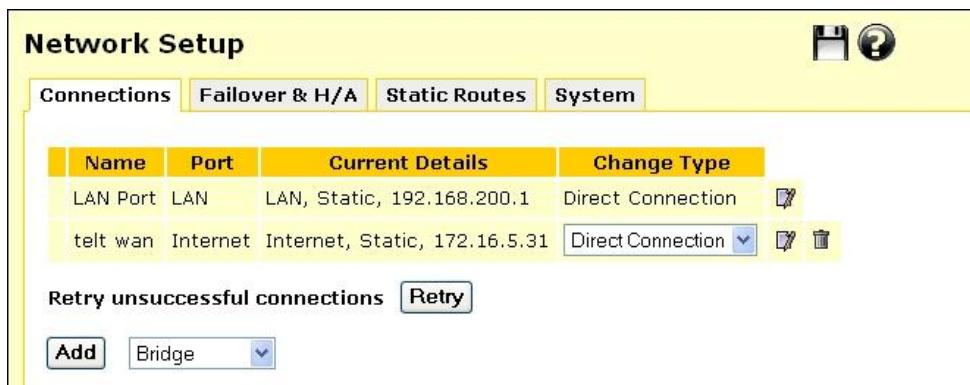
An Ethernet network interface may be configured to connect to your LAN, DMZ, an untrusted LAN, or the Internet as a primary, back-up or load-balancing connection.

If you are using a Secure Router as a primary Internet gateway, the section *Set up the PCs on your LAN to access the Internet* in the chapter entitled *Getting Started* describes how to configure the PCs on your LAN to share the connection once your Internet connection has been established.

Configuring Connections

Under the **Connections** tab, each of your Secure Router's network interfaces is displayed, alongside its physical **Port** name and the **Current Details** of its configuration.

Initially, only one network interface is configured for a single LAN connection on the initial setup port.



Configure a network interface by selecting a connection type from the **Change Type** pull down menu. View or modify the current configuration by clicking the **Edit** icon. Click the **Delete** icon to remove a network interface configuration. The system prompts you to confirm this action.

Direct Connection

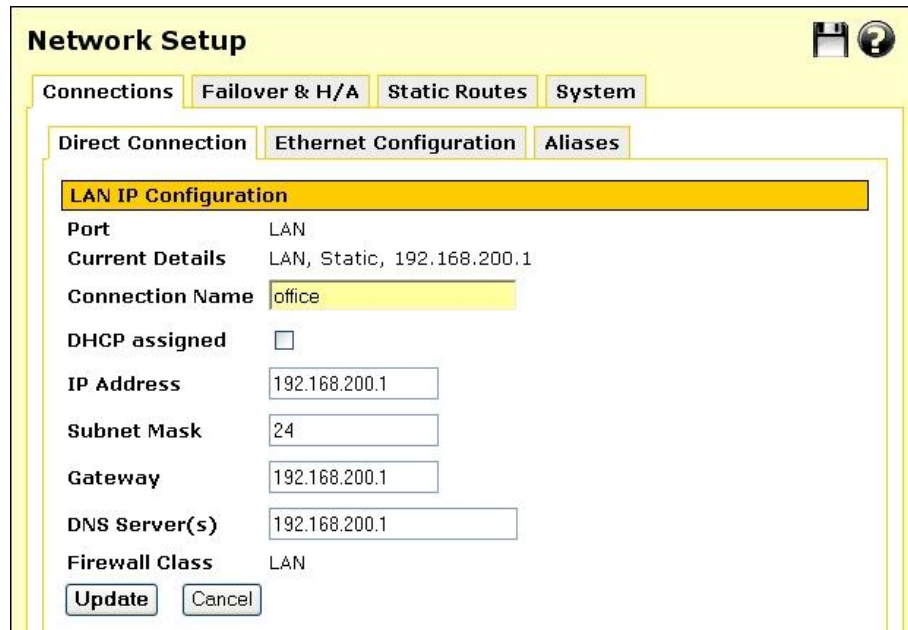
A direct connection is a direct IP connection to a network, i.e. a connection that does not require a modem to be present. This is typically a LAN, DMZ or Guest connection, but may also be an Internet connection. Network settings may be assigned statically or dynamically by a DHCP server; however, NET-PATH Plus must use a static IP.

Note

Direct connections may be added to a network bridge. This is discussed in *Bridging* later in this chapter.

Network settings

1. Click the **Edit** icon of the interface your wish to modify.



Network Setup

Connections | Failover & H/A | Static Routes | System

Direct Connection | Ethernet Configuration | Aliases

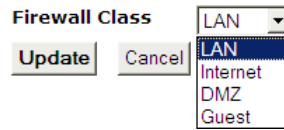
LAN IP Configuration

Port	LAN
Current Details	LAN, Static, 192.168.200.1
Connection Name	office
DHCP assigned	<input type="checkbox"/>
IP Address	192.168.200.1
Subnet Mask	24
Gateway	192.168.200.1
DNS Server(s)	192.168.200.1
Firewall Class	LAN

2. To assign network settings statically, enter an **IP Address** and **Subnet Mask**. If you are using the Secure Router in its default, network address translation mode, (see *Network address translation* in the *Advanced* section of this chapter), this is typically part of a private IP range, such as *192.168.0.1 / 255.255.255.0*. Ensure **DHCP assigned** is unchecked.
3. If required, enter a default **Gateway** to use for outgoing traffic on this connection. For LAN connections, a default gateway is not generally necessary.
4. You may also enter one or more **DNS servers**. Enter multiple servers by separating them with commas. If no LAN DNS servers are available, use the same DNS server address assigned to the WAN interface.

Firewall class

The **Firewall class** setting controls the basic allow/deny policy for this interface. Allowed network traffic is *accepted*, denied network traffic is *dropped*; this means network traffic is denied silently, no response such as “connection refused” is sent back to the originator of the traffic.



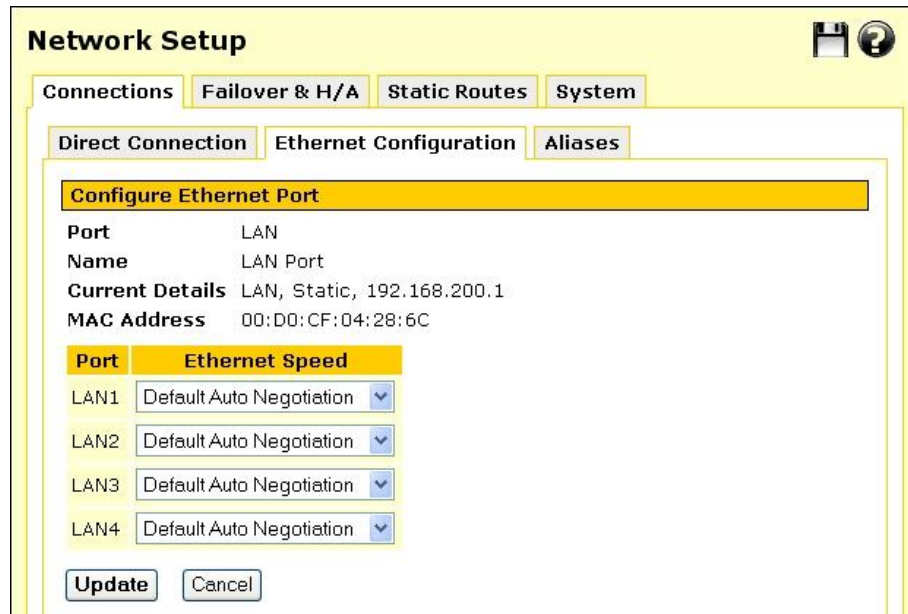
The following table details the policy associated with each firewall class. Note that VPN and Dial-In connections are by default assigned a firewall class of LAN.

Incoming Interface	Outgoing Interface	Action
LAN	Any	Accept
VPN	Any	Accept
Internet	Any	Drop

Click **Update** to apply the new settings.

Ethernet configuration

1. Click the **Ethernet configuration** tab to modify the low level Ethernet configuration settings of an Ethernet network port.



The screenshot shows the 'Network Setup' window with the 'Ethernet Configuration' tab selected. The 'Configure Ethernet Port' section displays the following information:

Port	LAN
Name	LAN Port
Current Details	LAN, Static, 192.168.200.1
MAC Address	00:D0:CF:04:28:6C

Below this, there is a table for 'Ethernet Speed' settings:

Port	Ethernet Speed
LAN1	Default Auto Negotiation
LAN2	Default Auto Negotiation
LAN3	Default Auto Negotiation
LAN4	Default Auto Negotiation

At the bottom of the window are 'Update' and 'Cancel' buttons.

2. If an Ethernet port is experiencing difficulties auto-negotiating with another device, set the **Ethernet Speed** and duplex manually.

Sometimes it may be necessary to change the Ethernet hardware or **MAC Address** of your Secure Router. The MAC address is a globally unique address and is specific to a single Secure Router. It is set by the manufacturer and should not normally be changed. However, you may need to change it if your ISP has configured your ADSL or cable modem to only communicate with a device with a known MAC address.

Note

This address cannot be changed for the LAN port.

Interface aliases

Interface aliases (on the Alias tab) allow the Secure Router to respond to multiple IP addresses on a single network interface. This is useful for when your ISP has assigned you a range of IP addresses to use with your Internet connection, or when you have more than one subnet connected to a single network interface.

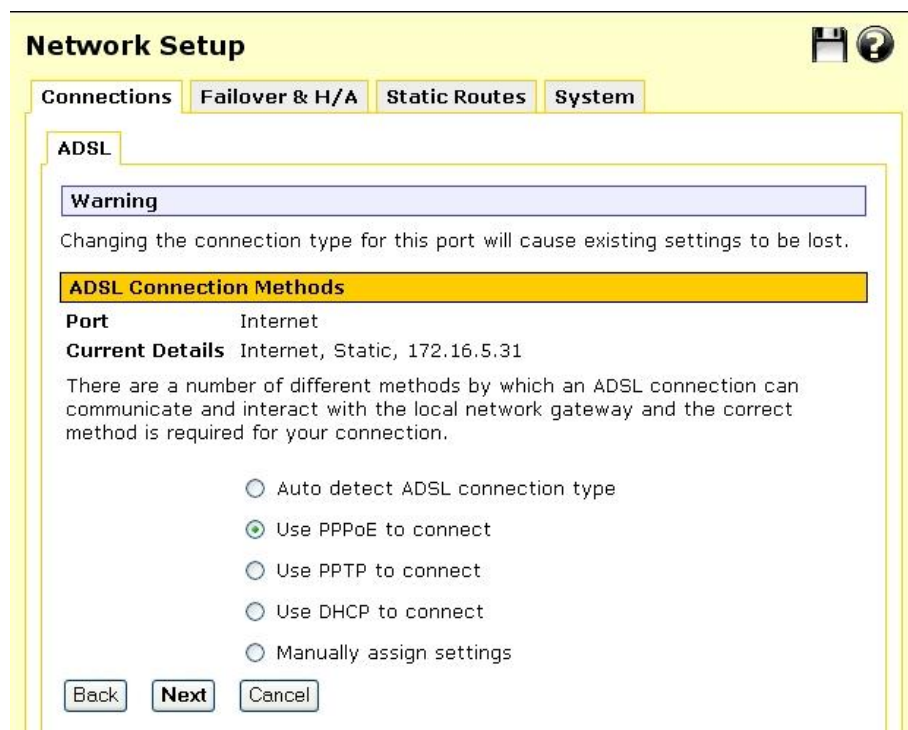
The screenshot shows a 'Network Setup' dialog box with a yellow background. At the top, there are tabs for 'Connections', 'Failover & H/A', 'Static Routes', and 'System'. Below these, there are sub-tabs for 'Direct Connection', 'Ethernet Configuration', and 'Aliases'. The 'Aliases' tab is active, showing a section titled 'Interface Aliases'. Under this section, the 'Name' is 'LAN Port' and 'Current Details' are 'LAN, Static, 192.168.200.1'. There are three buttons: 'Alias IP Address', 'Alias Subnet Mask', and 'Delete'. Below these buttons, it says 'No entries'. At the bottom, there are two input fields: 'Alias IP Address' with the value '192.168.0.1' and 'Alias Subnet Mask' with the value '24'. There are also 'Add' and 'Cancel' buttons at the bottom left.

For aliases on interfaces that have the Internet firewall class, you must also setup appropriate **Packet Filtering** and/or **Port forwarding** rules to allow traffic on these ports to be passed onto the local network. See the chapter entitled *Firewall* for details.

ADSL

1. To connect to the Internet using DSL, select **ADSL** from the **Change Type** pull down menu for the interface that connects to your DSL modem. ADSL connections have the interface firewall class of *Internet*.
2. If you have not already done so, connect the appropriate network port of your Secure Router to your DSL modem. Power on the DSL modem and give it some time to initialize. If fitted, ensure the Ethernet link LEDs are illuminated on both the Secure Router and DSL modem.

Do not continue until it has reached the *line sync* state and is ready to connect.



The screenshot shows the 'Network Setup' window with the 'ADSL' tab selected. A warning message states: 'Changing the connection type for this port will cause existing settings to be lost.' Below this, the 'ADSL Connection Methods' section is highlighted. It shows the 'Port' is 'Internet' and 'Current Details' are 'Internet, Static, 172.16.5.31'. A text block explains that different methods exist for ADSL connections. Five radio button options are listed: 'Auto detect ADSL connection type', 'Use PPPoE to connect' (which is selected), 'Use PPTP to connect', 'Use DHCP to connect', and 'Manually assign settings'. At the bottom are 'Back', 'Next', and 'Cancel' buttons.

3. Select the connection method to use in establishing a connection to your ISP: **PPPoE**, **PPTP**, **DHCP**, or **Manually Assign Settings**.

Note

*Use **PPPoE** if your ISP uses username and password authentication to access the Internet. Use **PPTP** if your ISP has instructed you to make a dial-up VPN connection to the Internet. Use **DHCP** if your ISP does not require a username and password, or your ISP instructed you to obtain an IP address dynamically. If your ISP has given you an IP address or address range, you must **Manually Assign Settings**.*

If you are unsure, let the Secure Router attempt to **Auto detect ADSL connection type**. Note that the Secure Router is unable to detect the **PPTP** connection type.

Note

If autodetection fails, it may also be because your DSL modem is misconfigured for your connection type, or your DSL service has not yet been provisioned by your telco.

4. Click **Next** to continue.

PPPoE

To configure a **PPPoE** connection, enter the user name and password provided by your ISP. You may also enter a descriptive **Connection Name** if you wish. Click **Finish**.

The screenshot shows a web-based configuration interface titled "Network Setup". It has four tabs: "Connections", "Failover & H/A", "Static Routes", and "System". The "Connections" tab is active. Underneath, there is a sub-tab for "ADSL". A yellow banner reads "ADSL PPPoE Configuration". Below this, the "Port" is set to "Internet" and "Current Details" are "Internet, Static, 172.16.5.31". A text block explains: "Configure your PPPoE ADSL Internet connection. Your service provider should have supplied you with a username and password to use to connect to the Internet." There are four input fields: "Connection Name" (containing "Main DSL"), "Username" (containing "Administrator"), "Password" (masked with dots), and "Confirm Password" (masked with dots). At the bottom are three buttons: "Back", "Finish", and "Cancel".

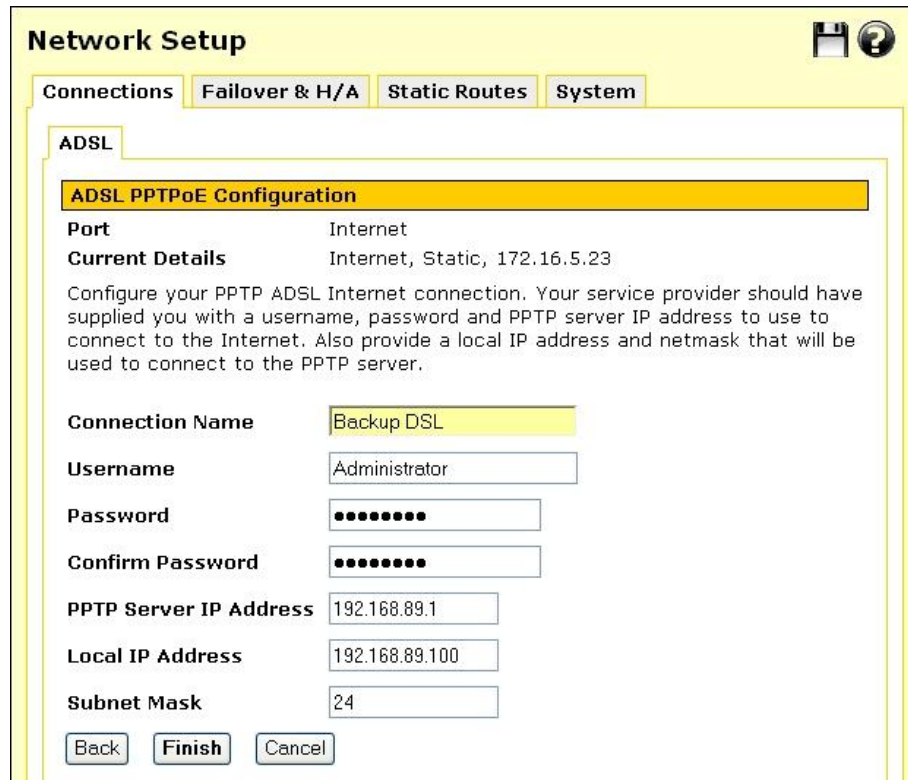
Note

For PPPoE connections, ensure your DSL modem is set to operate in bridged mode. Typically, for PPPoE connections, your DSL modem must be set to use LLC multiplexing/encapsulation.

By default, PPPoE connections are treated as “always on” and are kept up continuously. Alternatively, you may choose to only bring the connection up when PCs on the LAN, DMZ or Guest network (via a VPN tunnel) are trying to reach the Internet. For instructions, refer to the section entitled *Dial on Demand* further on in this chapter. As DSL connections are not generally metered by time, this is not generally necessary.

PPTP

1. To configure a **PPTP** connection to your ISP, enter the **PPTP Server IP Address** and a **Local IP Address** and **Netmask** for the Secure Router network port through which you are connecting to the Internet.



The screenshot shows a web-based configuration interface titled "Network Setup". It has four tabs: "Connections", "Failover & H/A", "Static Routes", and "System". The "Connections" tab is selected. Underneath, there is a sub-tab for "ADSL". A yellow header bar reads "ADSL PPTPoE Configuration". Below this, the "Port" is set to "Internet" and "Current Details" are "Internet, Static, 172.16.5.23". A paragraph of text explains the configuration: "Configure your PPTP ADSL Internet connection. Your service provider should have supplied you with a username, password and PPTP server IP address to use to connect to the Internet. Also provide a local IP address and netmask that will be used to connect to the PPTP server." The form fields are: "Connection Name" (Backup DSL), "Username" (Administrator), "Password" (masked with dots), "Confirm Password" (masked with dots), "PPTP Server IP Address" (192.168.89.1), "Local IP Address" (192.168.89.100), and "Subnet Mask" (24). At the bottom are "Back", "Finish", and "Cancel" buttons.

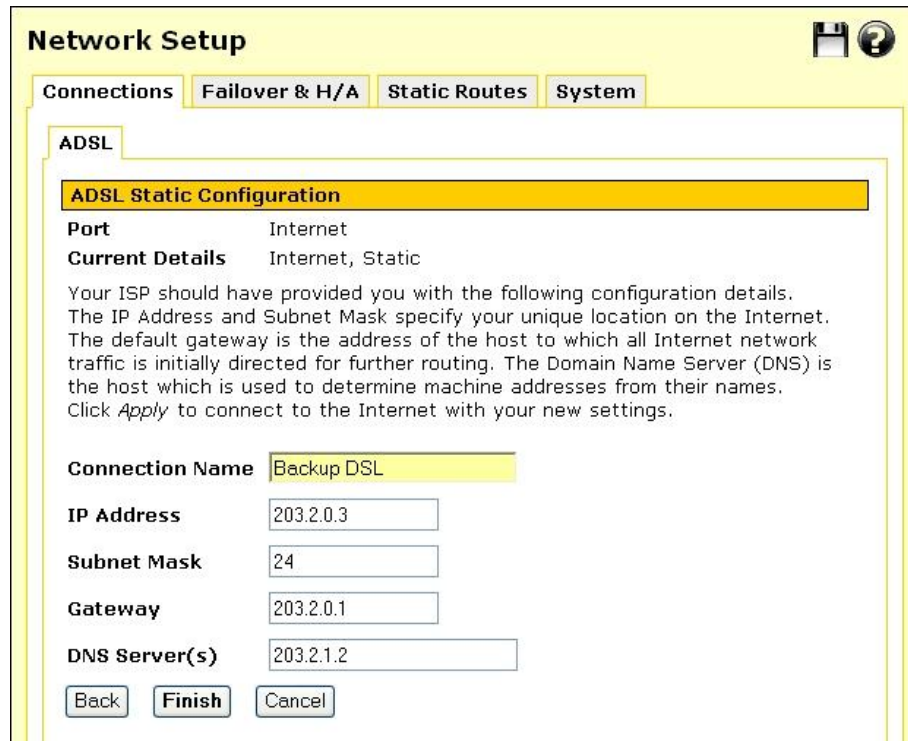
2. The **Local IP address** is used to connect to the PPTP server and is not typically your real Internet IP address. You may also enter a descriptive **Connection Name** if you wish.
3. Click **Finish** or **Update**.

DHCP

DHCP connections may require a **Hostname** to be specified, but otherwise all settings are assigned automatically by your ISP. You may also enter a descriptive **Connection Name** if you wish. Click **Finish** or **Update**.

Manually assign settings

For **Manually Assign Settings** connections, enter the **IP Address**, **Subnet mask**, the **Gateway** and the **DNS Address** provided by your ISP.



Network Setup

Connections | **Failover & H/A** | Static Routes | System

ADSL

ADSL Static Configuration

Port Internet
Current Details Internet, Static

Your ISP should have provided you with the following configuration details. The IP Address and Subnet Mask specify your unique location on the Internet. The default gateway is the address of the host to which all Internet network traffic is initially directed for further routing. The Domain Name Server (DNS) is the host which is used to determine machine addresses from their names. Click *Apply* to connect to the Internet with your new settings.

Connection Name Backup DSL

IP Address 203.2.0.3

Subnet Mask 24

Gateway 203.2.0.1

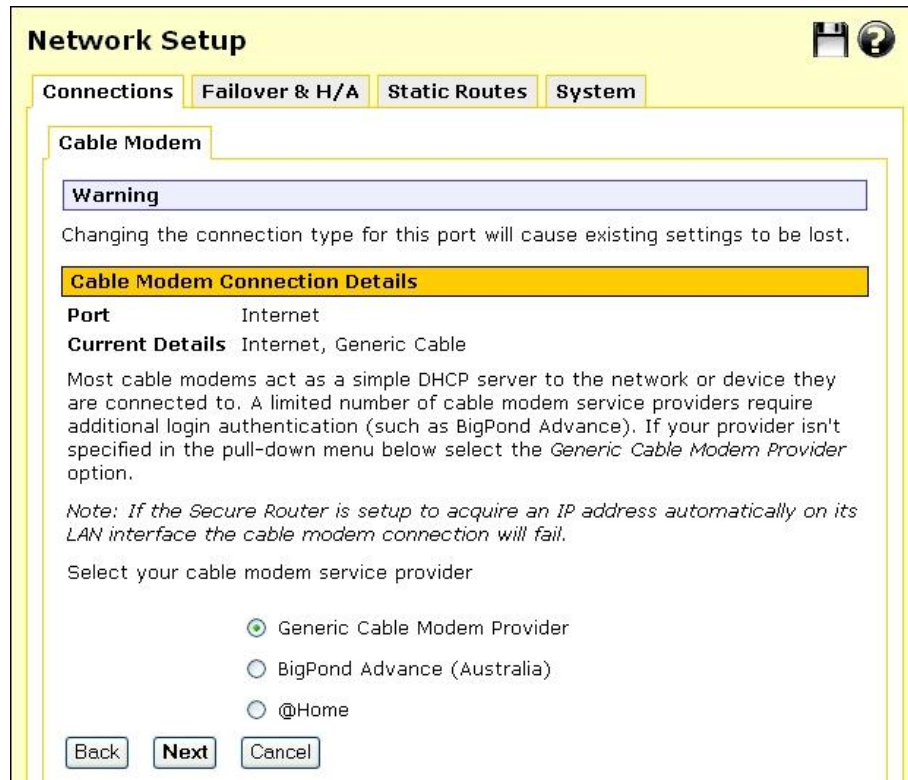
DNS Server(s) 203.2.1.2

Back Finish Cancel

The latter two settings are optional, but are generally required for normal operation. Multiple DNS addresses may be entered separated by commas. You may also enter a descriptive **Connection Name** if you wish. Click **Finish** or **Update**.

Cable Modem

1. To connect to the Internet using a cable Internet service, select **Cable Modem** from the **Change Type** pull down menu for the interface that connects to your cable modem. Cable Modem connections have the interface firewall class of *Internet*.
2. If you have not already done so, connect the appropriate network port of your Secure Router to your cable modem. Power on the cable modem and give it some time to initialize. If fitted, ensure the Ethernet link LEDs are illuminated on both the Secure Router and cable modem.



3. Select your cable ISP from the list and click **Next**. If your provider does not appear, select **Generic Cable Modem Provider**. You may enter a descriptive **Connection Name** if you wish. For cable modem providers other than **Generic**, enter your user name and password or hostname. Click **Finish** or **Update**.

Ethernet configuration

See the section entitled *Ethernet configuration* under *Direct Connection*.

Aliases

See the section entitled *Aliases* under *Direct Connection*.

Failover, Load Balancing and High Availability

The Secure Router supports a wide range of configurations through which you can use multiple Internet connections, and even multiple Secure Routers, to ensure Internet availability in the event of service outage or heavy network load.

The following Internet availability services are provided by the Secure Router. They may be configured individually, or in combination.

- *Internet Failover*: configuring a back up Internet connection (or connections) that is only established should the primary link lose connectivity
- *Load Balancing*: establishing another Internet connection (or connections) concurrently with the primary link, for spreading network load over multiple connections
- *High Availability*: installing a back up Secure Router to monitor the status of the primary unit, coming online and becoming the Internet gateway for your network should the primary Secure Router fail

Note

The Secure Router is limited to Internet availability configurations using a single broadband Internet connection and a single dialout or ISDN connection.

Configure Internet connections

Configure all Internet connections to use in conjunction with the Secure Router's Internet availability services. Secondary and tertiary Internet connections are configured in the same manner as the primary Internet connection, as detailed in the sections entitled *Direction Connection, ADSL, Cable Modem, and Dialout/ISDN* earlier in this chapter.

Once the Internet connections have been configured, specify the conditions under which the Internet connections are established.

Internet Failover

Secure Routers support three connection levels. A *connection level* consists of one or more Internet connections. When all primary connections are functioning as expected, the primary connection level is deemed to be up.

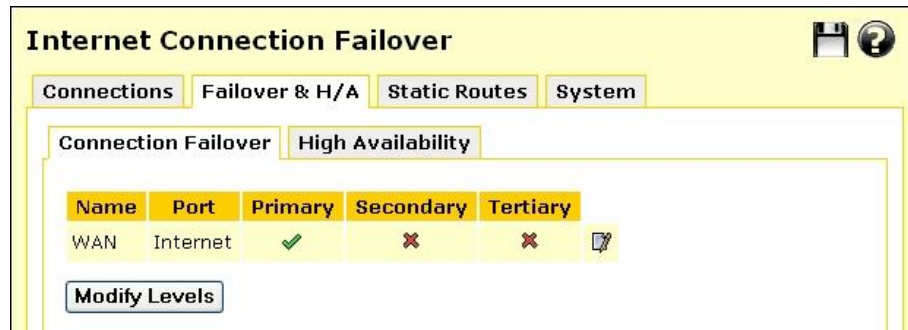
If one or more of the primary connections should fail, the Secure Router drops back to the secondary connection level. This typically involves bringing up a secondary Internet connection, until the primary Internet connection or connections become available again.

You may also optionally configure the tertiary failover level. If one or more of the secondary connections should fail, the Secure Router drops back to the tertiary connection level. This is typically a “last resort” dialup link to the Internet, but may be any kind of network connection. The primary connection level and secondary connection level are tested in turn, until one becomes available.

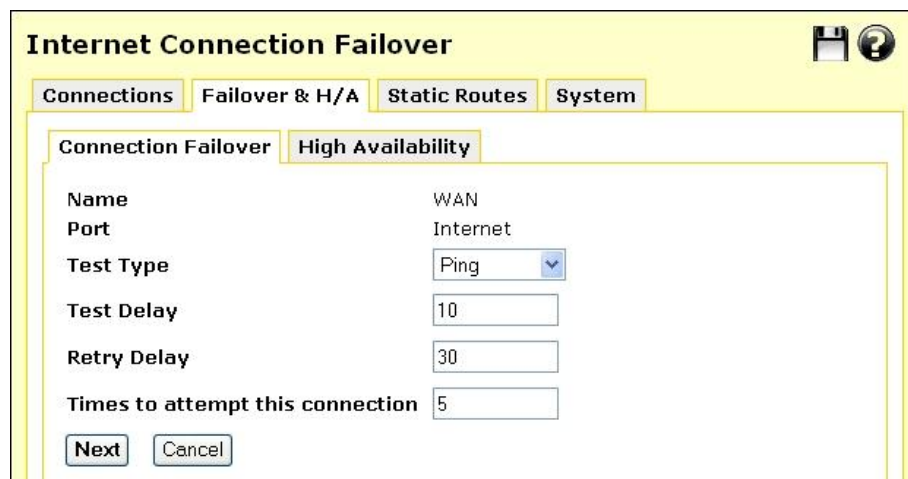
Edit connection parameters

To configure failover is to set failover parameters for each connection. These parameters specify how to test whether a connection is up and functioning correctly.

1. On the **Network Setup** page, click the **Failover & H/A** tab. A list of the connections that you have configured is displayed under the **Connection Failover** tab, alongside ticks and crosses. The ticks and crosses indicate how the connection behaves at each failover level, this is discussed further in the section entitled *Modify failover levels (primary, secondary, tertiary)*.



2. Click the **Edit** icon next to the connection to edit its failover parameters. The **Name** and **Port** of this connection is displayed, along with several options.



3. Select a **Test Type**. The **Ping** test is usually appropriate.

- **Ping** sends network traffic to a remote host at regular intervals, if a reply is received the connection is deemed to be up.
- **Custom** (*advanced users only*) allows you to enter a custom console command to run to determine whether the connection is up. This is typically a script you have written and uploaded to the Secure Router.
- **Always Up** means no test is performed, and Internet failover is disabled for this connection.

If you wish, you may fine tune the timeouts for the failover test, however the defaults are usually suitable.

- **Test Delay** is the number of seconds to wait after starting this connection before testing whether it is functioning correctly, a longer delay is used for connection types that are slow to establish, such as dialout.
- **Retry Delay** is the number of seconds to wait after a connection test fails before re-attempting the test.
- **Times to attempt this connection** is the number of times to try a connection before giving up. Once the Secure Router has given up trying this connection, manual intervention is required to re-establish it.

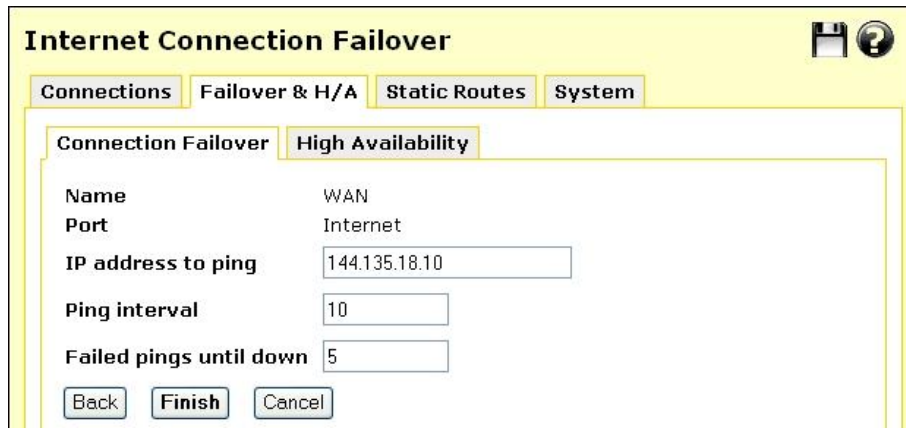
4. Click **Next** to configure settings specific to the **Test Type**.

- If you selected a **Test Type** of **Always Up**, no further configuration is required. Skip ahead to *Modify failover levels (primary, secondary, tertiary)*.
- If you selected **Custom**, enter the custom **Test Command** that is used to test the connection, e.g.: `myscript 5 10 ping -c 1 -I $if_netdev 15.1.2.3`

Note

*If the **Test Command** exits with a return code of zero (0), the test is deemed to have passed and the connection is considered up. Otherwise, the connection is considered down. Also note that `$if_netdev` is replaced with the name of the network interface on which the test is being run, e.g. `ppp0`.*

- If you selected **Ping**, enter an **IP Address to Ping**. Ensure you choose a host on the Internet that can be contacted reliably and responds to pings. You can check whether you can ping a host under **Diagnostics** -> **Network Tests** -> **Ping Test**.



Ping Interval is the time to wait in between sending each ping, **Failed Pings** is the number of missed ping replies before this connection attempt is deemed to have failed.

5. Click **Finish**.

Modify failover levels (primary, secondary, tertiary)

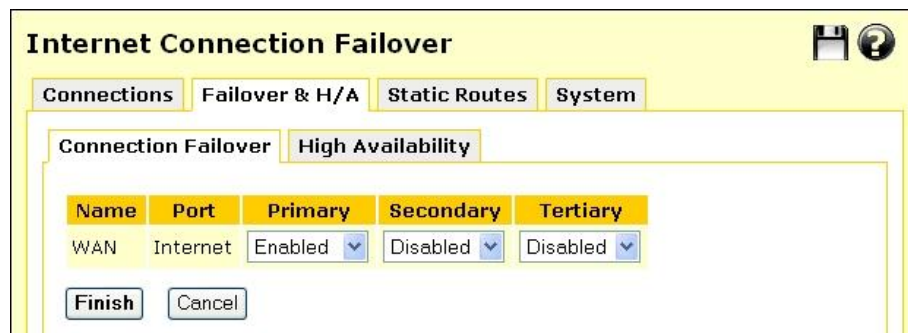
The second and final step of configured Internet failover is associating Internet connections with and primary, secondary and optionally tertiary connection levels.

Recall that a connection level is one or more connections. These connections may be marked as **Required** or **Enabled**. Internet connections that are marked **Disabled** are not part of this connection level. A connection level is deemed to be up when all connections marked **Required** at that level are up, and at least one connection (marked **Required** or **Enabled**) at that level is up.

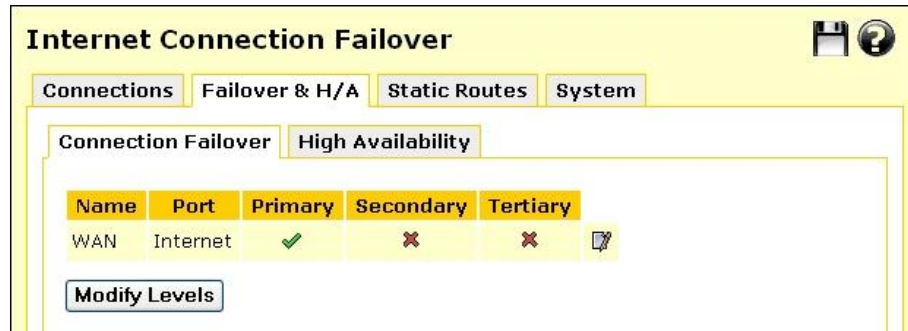
1. On the **Network Setup** page, click the **Failover & H/A** tab, then **Modify Levels**. A table is displayed listing each of the connections alongside a drop down box for each connection level.

Note

If a connection is marked <Always Up>, you must edit its connection parameters as described by the previous section before it can be associated with a connection level.



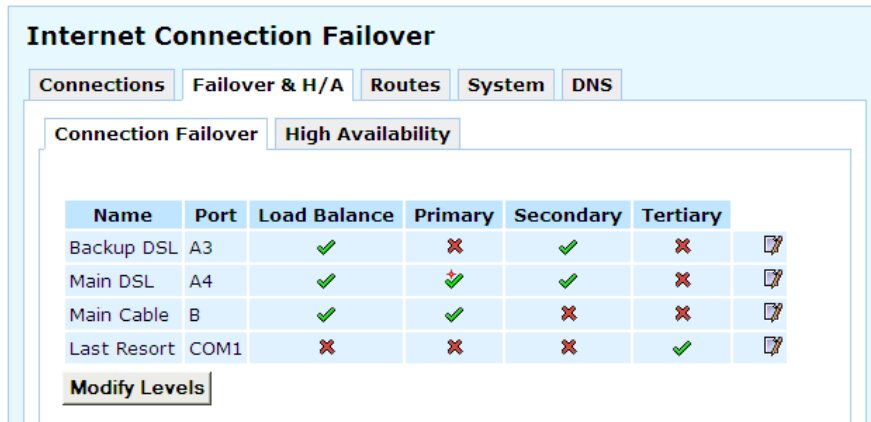
2. Configure the **Primary** connection level. If you have a single Internet connection only, setting it to **Enabled** or **Required** has the same effect. For failover to occur, you must then configure at least the secondary connection level.
3. Click **Finish**.



This returns you to the main **Connection Failover** page. You'll notice that ticks and crosses are display alongside each connection, describing how they are configured for each connection level. A red cross means **Disabled**, a green tick means **Enabled** and a green tick with a small red plus means **Required**,

Internet Load Balancing

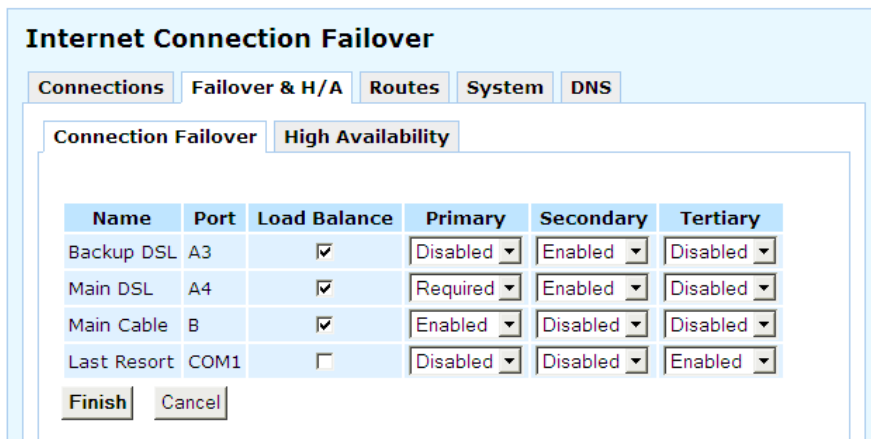
Once you have configured two or more Internet connections, you may enable Internet load balancing. Load balancing may be used in conjunction with Internet failover, or on its own.



The Internet connections need not be the same, e.g. you can perform load balancing between a PPPoE ADSL connection on one network port, and a Cable Internet connection on the other.

Enabling load balancing

1. Under the **Failover & H/A** tab, click **Modify Levels**.



2. Check **Load Balance** for each connection to enable for load balancing. Click **Finish**.

Note

Load balancing settings are not specified for each failover level; load balancing occurs when any two or more load balancing connections are up.

Limitations of load balancing

Load balancing works by alternating outgoing traffic across Internet connections in a round robin manner. It does not bond both connections together to work as one link, e.g. it does not bond two 512 kbit/s links to function as a single 1 mbit/s link.

Total bandwidth and available bandwidth are *not* taken into account when choosing a connection on which to send outgoing traffic.

When an internal client makes a connection to a server on the Internet, this and subsequent connections between the the internal client and remote server are confined to the one Internet connection to ensure connections are not broken.

If a second internal client makes a connection to the same remote server, it may or may not go across the same link, depending on which Internet connection is next to be selected in the round robin process.

VPN connections such as IPSec or PPTP tunnels are confined to a single Internet connection, as they are a single connection (that encapsulate other connections).

Load balancing is not performed for incoming traffic. This scenario can be addressed using other solutions such as round robin DNS to alternate incoming connections between the two links.

High Availability

If you have two Secure Routers on the same LAN segment, you may configure a *shared LAN IP address* which is assigned to one or the other device (as an Ethernet alias address) depending upon which one is available.

The device which currently has the address is termed the *master* while the other device is termed the *slave*.

You may use either the supplied script, */bin/highavaild*, to manage the shared address, or you may write your own script.

Enabling high availability

On each of the devices, select the **Failover & H/A**, then the **High Availability** tab.

If you are using the supplied `/bin/highavaild` script, enter a command similar to the following as the **Start Command** on both devices. **Stop Command** and **Test Command** are not required.

```
exec /bin/highavaild ipaddr &
```

Note

Enter the shared LAN IP address in the place of ipaddr. You do not need to manually configure this IP address on either unit, the /bin/highavaild script handles this internally.

Limitations of high availability

Currently `/bin/highavaild` only supports managing an IP address on eth0. To manage an IP address on a different interface, open a telnet or ssh connection to the Secure Router and complete the following commands:

1. `cp /bin/highavaild /etc/config`
2. `chmod 755 /etc/config/highavaild`
3. Modify the script appropriately
4. use this new script as your **Start Command**

Bridging

The Secure Router may be configured to bridge between network interfaces. When two or more network interfaces are bridged, the Secure Router learns and keeps track of which hosts are reside on either side of the bridge, and automatically directs network traffic appropriately.

One advantage of bridging network interfaces is that hosts on either side of the bridge can communicate with hosts on the other side without having to specify a route to the other network via the Secure Router.

Another advantage is that network traffic not usually routed by unbridged interface, such as broadcast packets, multicast packets, and any non-IP protocols such as IPv6, IPX or Appletalk pass over the bridge to their destination host.

Bridging network interfaces involves creating, then associating existing network interfaces with a **Bridge** interface.

Warning

You must trust all devices that are directly connected to bridged interfaces. This is because the firewall does not know which IP addresses for the bridged network belong on which interface. This means it is easy for a directly connected device to spoof an IP address. You can manually add Packet Filter rules to prevent spoofing.

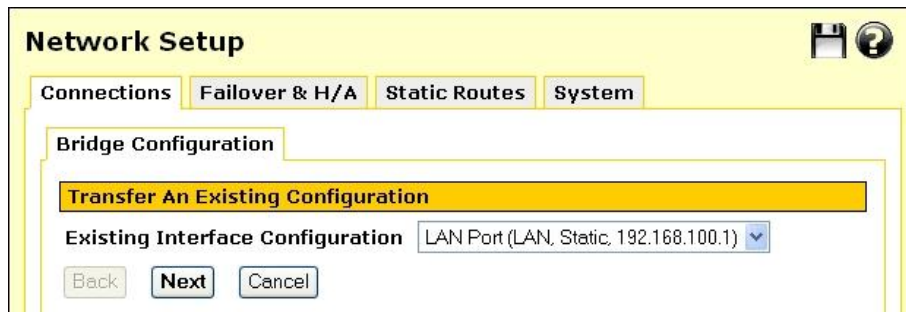
Furthermore, non-IP protocols are not restricted by the firewall. You should not bridge between interfaces with different firewall classes if you are using non-IP protocols.

Adding a bridge interface

1. From below the main **Connections** table, select **Bridge** from the pull down menu and click **Add**.

Once you add this bridge interface, it appears on the **Network Setup** page under the **Connections** tab, along with the Secure Router's other network interfaces.

When network interfaces are bridged, they all share a common configuration for the network connection. This means that a single IP address is used on all of the network interfaces.



2. If you wish to transfer the IP address settings of an existing network connection to the bridge interface, select it from the **Existing Interface Configuration** pull down menu.
3. Click **Next**.

Note

As the Secure Router automatically directs network traffic, hosts on either side do not need to specify this IP address as a gateway to the networks connected to the bridge.

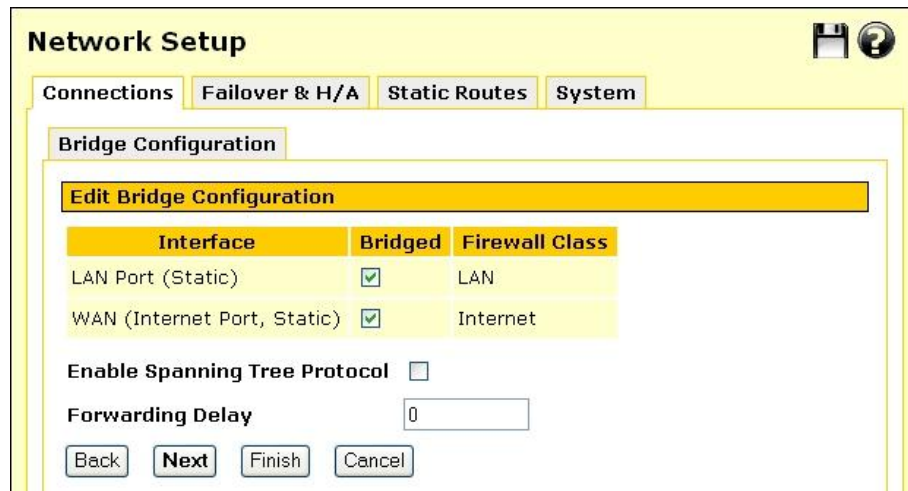
So in reality, it is not so important which IP address you choose to assign to the bridge interface. It is primarily used by hosts on either side of the bridge only to connect to the Secure Router's web management console. Specific routes are still required to reach networks that are not being bridged.

Edit bridge configuration

1. For each network interface that you wish to bridge, select **Bridged**. Also ensure its **Firewall Class** is set appropriately; this setting is discussed in the *Direct Connection* section towards the beginning of this chapter.

Note

Bridging only supports ethernet and GRE network interfaces, and can only be configured as a Direct Connection. This means you cannot bridge a PPPoE connection.



You may want to **Enable Spanning Tree Protocol** if you have multiple bridges on your network. It allows the bridges to exchange information, helping eliminate loops and find the optimal path for network traffic.

Forwarding Delay is the time in seconds between when the bridge interface comes online and when it begins forwarding packets. This usually only occurs when the unit first boots, or the bridge configuration is modified. This delay allows the Secure Router's bridge to begin learning which hosts are connected to each of the bridge's interfaces, rather than blindly sending network traffic out all network interfaces.

2. Click **Next** to review or change IP address information for the bridge interface, otherwise click **Finish**.

Bridging across a VPN connection

Bridging across a VPN connection is useful for:

- Sending IPX/SPX over a VPN, something that is not supported by other VPN vendors
- Serving DHCP addresses to remote sites to ensure that they are under better control
- It allows users to make use of protocols that do not work well in a WAN environment (e.g. *netbios*)

A guide to bridging across an IPSec tunnel using GRE is provided in the section entitled *GRE over IPSec* in the *Virtual Private Networking* chapter.

GRE Tunnels

The GRE configuration of the Secure Router allows you to build GRE tunnels to other devices that support the *Generic Routing Encapsulating* protocol. You can build GRE tunnels to other Secure Routers that support GRE, or to other devices such as Cisco equipment.

GRE tunnels are useful for redistributing IPv6 or broadcast and multicast traffic across a VPN connection. It is also useful for carrying unsupported protocols such as IPX or Appletalk between remote IP networks.

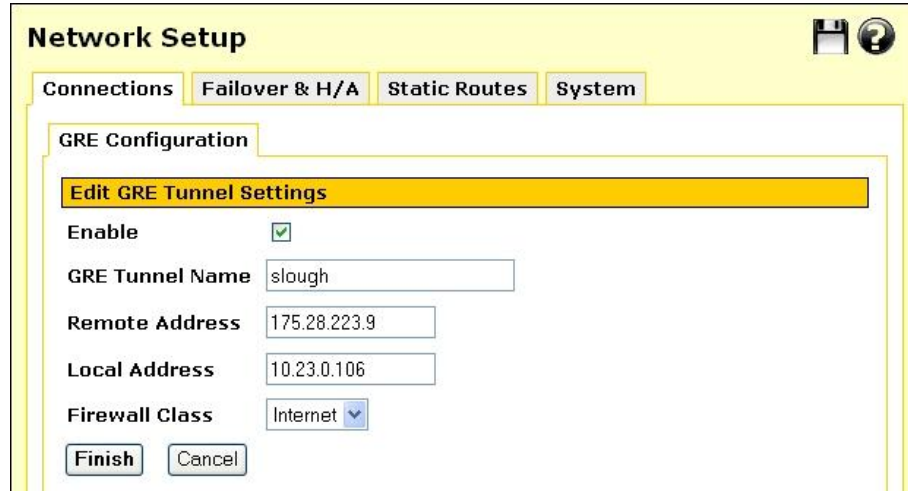
Warning

GRE tunnels are not secure unless they are run over another secure protocol. Using a GRE tunnel that runs over the Internet, it is possible for an attacker to put packets onto your network. If you want a tunneling mechanism to securely connect to networks, then you should use IPSec, or tunnel GRE over either IPSec or PPTP tunnels.

An example setup that describes using GRE to bridge a network over an IPSec tunnel is described in GRE over IPSec.

Adding a GRE interface

1. Under the **Network Setup** -> **Connections** table, select **GRE Tunnel** and click **Add**.



The screenshot shows the 'Network Setup' dialog box with the 'Connections' tab selected. The 'GRE Configuration' section is active, and the 'Edit GRE Tunnel Settings' sub-section is highlighted. The settings are as follows:

Field	Value
Enable	<input checked="" type="checkbox"/>
GRE Tunnel Name	slough
Remote Address	175.28.223.9
Local Address	10.23.0.106
Firewall Class	Internet

Buttons for 'Finish' and 'Cancel' are visible at the bottom.

2. Ensure **Enable** is checked and enter a descriptive **GRE Tunnel Name** for this tunnel.
3. Enter the address of the remote GRE endpoint in **Remote Address**, e.g. the Internet IP address of a remote Secure Router.
4. Enter the address of the local GRE endpoint in **Local Address**. This is typically a free address on your main LAN. If your LAN connection has an alias address, it may also be a free address on the alias network.
5. Select a **Firewall Class** for the GRE interface, this setting is discussed in the *Direct Connection* section towards the beginning of this chapter.
6. Click **Finish**.

The GRE interface now appears in the main **Network Setup** table.

GRE over IPSec

The basic steps to set up GRE over IPSec are:

1. Use the same network for the primary IP addresses of the LAN interfaces at both ends of the tunnel.
2. Assign unused alias IP addresses to the LAN interfaces at both ends of the tunnel.

3. Create an IPsec tunnel between the alias IP addresses.
4. Create a GRE tunnel between the alias IP addresses.
5. Create bridges between the LAN interfaces and the GRE tunnel.
6. Modify the firewall.

In this example we use a dummy alias network of 10.254.0.0 / 255.255.0.0 to bridge two example local networks, one at Brisbane and one at Slough. These steps must be repeated for either end of the tunnel.

Note that the two locations are using the same subnet.

Secure Router in Brisbane

Internet address: 203.23.45.6
LAN address: 192.168.1.1
LAN alias: 10.254.0.1
LAN: 192.168.1.0 / 24

Secure Router in Slough

Internet address: 195.45.67.8
LAN address: 192.168.1.2
LAN alias: 10.254.0.2
LAN: 192.168.1.0 / 24

1. Add the LAN connection to a bridge, as described in the section entitled *Bridging* earlier in this chapter.
2. Give the LAN interface bridge a secondary address that is part of the network we want bridged across the tunnel. Adding an alias is described in *Aliases* in the section entitled *Direction Connection* earlier in this chapter. In this example, the Brisbane end uses an alias address of 10.254.0.1, the Slough end uses and alias address of 10.254.0.2.
3. Ensure the alias address is *not* part of the network to bridge across the tunnel (in this example, it mustn't be part of 192.168.0.0 / 24), and *not* on the same network as any of the Secure Router's other interfaces.

Note

The alias IP addresses are essentially dummy addresses and can be anything that does not conflict with your existing network infrastructure.

4. Create an IPsec tunnel between Brisbane and Slough. Select **IPsec** from the **VPN** section of the main menu and click **New**. For a complete overview of all available options when setting up an IPsec tunnel, please refer to the *IPsec* section earlier in this chapter.

Take note of the following important settings:

1. Set the **local party** as a **single network behind this appliance**. Set the **remote party** as **single network behind a gateway**.
2. For the Slough end's **Phase 2 Settings**, specify the **Local Network** as *10.254.0.1 / 255.255.255.255* and the **Remote Network** as *10.254.0.2 / 255.255.255.255*. For the Brisbane end's **Phase 2 Settings**, specify the **Local Network** as *10.254.0.2 / 255.255.255.255* and the **Remote Network** as *10.254.0.1 / 255.255.255.255*. Note the 32 bit netmasks (255.255.255.255) being used.
3. Create the GRE tunnel. Under the main **Network Setup** table, select **GRE Tunnel** and click **Add**. For the Slough end, enter:

GRE Tunnel Name: *to_bris*
Remote Address: *10.254.0.2*
Local Address: *10.254.0.1*
Firewall Class: *LAN*

4. For the Brisbane end, enter:

GRE Tunnel Name: *to_slough*
Remote External Address: *10.254.0.1*
Local External Address: *10.254.0.2*
Firewall Class: *LAN*

5. Click **Finish** to add the interface. **Edit** the bridge interface that you added at the beginning of these steps. Check **Bridged** for the GRE interface you have just added, and select a **Firewall Class** of **LAN**. Click **Finish**.
6. At the Slough end, click **Packet Filtering**, the **Custom Firewall Rules** tab and add this custom firewall rule:

```
iptables -I OUTPUT ! -o ipsec+ -d 10.254.0.2 -j DROP
```

7. Click **Update**.

- At the Brisbane end, click **Packet Filtering**, the **Custom Firewall Rules** tab and add this custom firewall rule:

```
iptables -I OUTPUT ! -o ipsec+ -d 10.254.0.1 -j DROP
```

- Click **Update**.

GRE troubleshooting

- Symptom:** Cannot ping a host on the other side of the GRE tunnel.
Ensure that there is a route set up on the GRE tunnel to the remote network.
Ensure that there is a route on the remote GRE endpoint to the network at this end of the GRE tunnel.
Check that there is a GRE interface created on the device. To do this, go into *Advanced Networking* and scroll to the bottom. There should be an interface called **greX** created. **greX** is the same as the **Interface Name** specified in the table of current GRE tunnels.
Also ensure that the required routes have been set up on the GRE interface. This might not occur if you have the same route specified on different GRE tunnels, or on different network interfaces.
Ensure that the remote GRE endpoint is reachable. Do this by using the ping utility on the *Advanced Networking* page.
- Symptom:** Cannot ping the remote GRE end point.
Ensure that the remote GRE end point responds to pings. Note that by default no packets are routed across the GRE tunnel unless there is a route setup on the GRE tunnel.

Routes

To configure the Secure Router's advanced routing features, click the **Static Routes** tab on the **Network Setup** page.

Here you may add additional static routes for the Secure Router. These routes are additional to those created automatically by the Secure Router configuration scripts.

Click **New** to add a static route. **Target Address** and **Subnet mask** identify the destination network or host. You may also specify an **Interface** out which the network traffic should be routed, a **Gateway Address** through which the network traffic should be routed, and a **Metric** for this route.

System

To configure the Secure Router's network system settings, click the **System** tab on the **Network Setup** page. These settings control the Secure Router's identity on the network.

Hostname

The **Hostname** is a descriptive name for the Secure Router on the network. It is also used as the SNMP *sysName* field. By default, this is set to the model name of your Secure Router and should be changed to the embedded IP of the NET-PATH Plus.

Administrative contact

You may enter the email address of the local administrator of the Secure Router for use as the SNMP *sysContact* field. *(not required)*

Device location

You may also enter a short description of the physical location of the Secure Router for use as the SNMP *sysLocation* field. *(not required)*

DNS

To configure the Secure Router's DNS settings, click the **DNS** tab on the **Network Setup** page. These settings control the Secure Router's network name services.

DHCP Server

Note

To configure your Secure Router as a DHCP server, you must set a static IP address and netmask on the network interface on which you want the DHCP server to run; see the Direct Connection section of the chapter entitled Network Connections.

To begin configuring the Secure Router's DHCP server, select **DHCP Server** from the **Network Setup** section of the web management console's main menu.

DHCP configuration

1. Click the **Edit** icon next to the network interface on which you wish to edit or enable a DHCP server.

DHCP Server Configuration

DHCP Server

DHCP Configuration

Server Configuration

Interface	LAN Port
Subnet	10.23.0.106/16
Enable DHCP Server for this Subnet	<input checked="" type="checkbox"/>
Gateway Address	<input type="text"/>
DNS Address	<input type="text"/>
Domain Name	Main
WINS Address	10.23.1.1
Default Lease Time (s)	86400
Maximum Lease Time (s)	172800
Address Range	10.23.0.100-200

2. To configure the DHCP server, follow these instructions.

- Check the **Enable DHCP Server for this Subnet** checkbox.
- Enter the **Gateway Address** to issue the DHCP clients. If this field is left blank, the Secure Router's IP address is used.
- Enter the **DNS Address** to issue the DHCP clients. If this field is left blank, the Secure Router's IP address is used. Leave this field blank for automatic DNS server assignment. If your Secure Router is configured for DNS masquerading, you should either leave this field blank, or enter the IP address of the LAN port of the Secure Router.
- Optionally enter a **Domain Name** suffix to issue DHCP clients.
- Optionally enter IP address of the WINS server to be distributed to DHCP clients in the **WINS Address** field.
- Enter the **Default Lease Time** and **Maximum Lease Time** in seconds. The lease time is the time that a dynamically assigned IP address is valid before the client must re-request it.
- Enter the IP address or range of IP addresses (see the appendix entitled *IP Address Ranges*) to be issued to DHCP clients in the **Address Range** field.

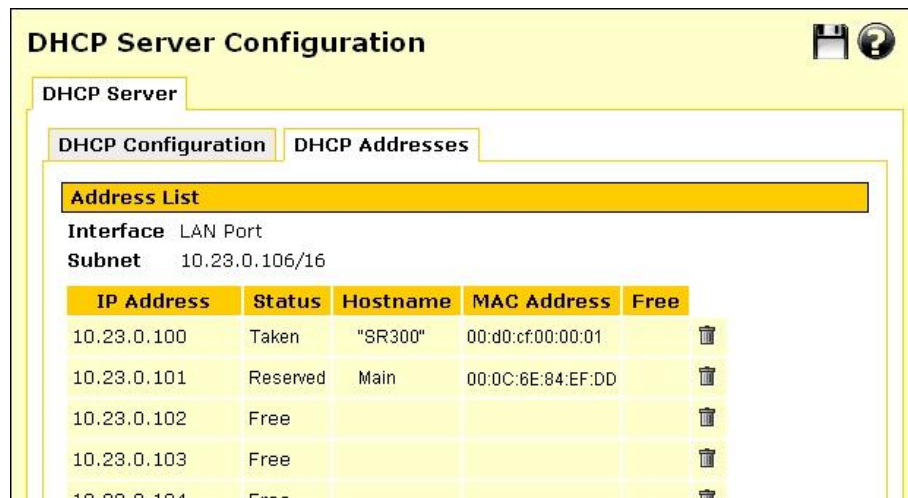
3. Click **Finish**.

DHCP addresses

To view the status of the IP address the DHCP server is configured to distribute, click the **Edit** icon next to the appropriate network interface, then click the **DHCP Addresses** tab.

Address list

For each **IP Address** that the DHCP server is managing, the **Status**, **Hostname**, **MAC Address** is displayed.



IP Address	Status	Hostname	MAC Address	Free
10.23.0.100	Taken	"SR300"	00:d0:cf:00:00:01	<input type="checkbox"/>
10.23.0.101	Reserved	Main	00:0C:6E:84:EF:DD	<input type="checkbox"/>
10.23.0.102	Free			<input type="checkbox"/>
10.23.0.103	Free			<input type="checkbox"/>
10.23.0.104	Free			<input type="checkbox"/>

There is an icon to **Delete** the address from the list of addresses to manage. You may also **Free** addresses that have been leased by hosts on your network, this causes the lease to expire immediately, leaving the address available for the next host that requests IP configuration.

The **Status** field displays one of three states:

- **Reserved:** the address is reserved for the particular host defined by hostname and MAC address
- **Free:** the address is available to be handed out to any DHCP client host
- **Taken:** the address has been issued to a host

Adding and removing addresses

1. Under **Add/Remove Dynamic IP Addresses**, enter the IP address or IP address range and click **Add** or **Remove**.

Add/Remove Dynamic IP Addresses

You may add or remove dynamic IP addresses for the DHCP server by specifying those addresses below. (Note: The IP address field will accept a range or a single IP address as input. For example: 192.168.0.234-238 or 192.168.0.1).

IP Address

2. To remove an address, you may also click its **Delete** icon under the **Address List**.

Reserving IP addresses

You may also reserve IP addresses for particular hosts, identifying them by hostname and MAC address.

Add Reserved IP Addresses

You may add reserved IP addresses for the DHCP server by specifying their details below. Please enter in the MAC Address in the form AB:CD:EF:12:34:56.

Hostname

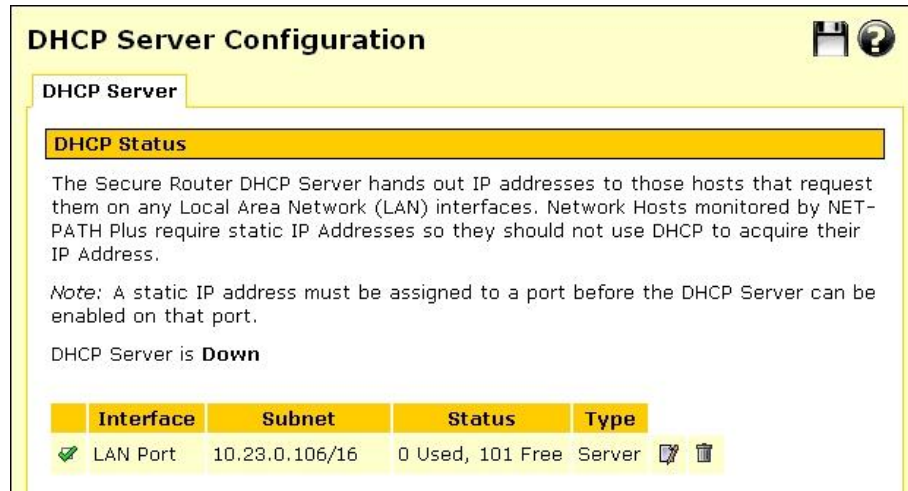
MAC Address

IP Address

1. To reserve an IP address for a certain host, enter the following in the **Add reserved IP address** section.
 - Enter the **Hostname** of the DHCP client.
 - Enter the **MAC address** of the DHCP client.
 - Enter the reserved **IP address** for the DHCP client.
2. Click **Submit**.

DHCP status

This main DHCP server page displays the status for each interface on which the DHCP server is running. There are **Edit**, **Delete** and **Enable/Disable** icons displayed for each Interface.



DHCP Server Configuration

DHCP Server

DHCP Status

The Secure Router DHCP Server hands out IP addresses to those hosts that request them on any Local Area Network (LAN) interfaces. Network Hosts monitored by NET-PATH Plus require static IP Addresses so they should not use DHCP to acquire their IP Address.

Note: A static IP address must be assigned to a port before the DHCP Server can be enabled on that port.

DHCP Server is **Down**

Interface	Subnet	Status	Type
LAN Port	10.23.0.106/16	0 Used, 101 Free	Server

The **Subnet** is the network on which DHCP server is handing out addresses. **Free Addresses** displays the number of remaining available IP addresses that can be distributed. You may need to increase the number of IP addresses to hand out if this value is 0.

DHCP Proxy

The DHCP proxy allows the Secure Router to forward DHCP requests from the LAN to an external server for resolution. This allows both static and dynamic addresses to be given out on the LAN just as running a DHCP server would.

To enable this feature, specify the server which is to receive the forwarded requests in **Relay Host**. This server must also be configured to know and accept requests from the Secure Router's LAN. Then check **Enable DHCP Relay** and click **Apply**.

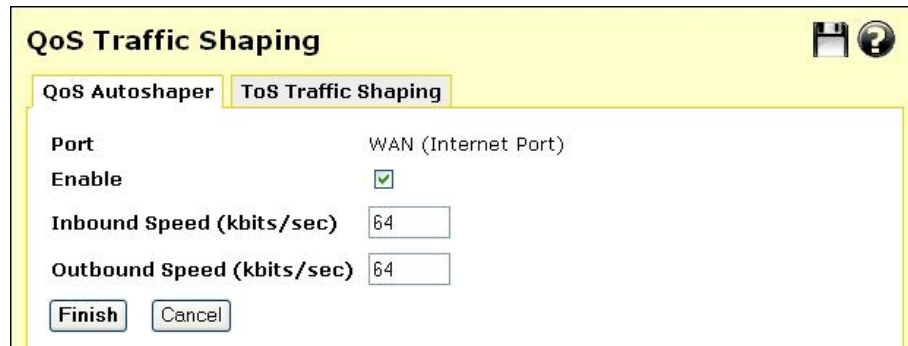
QoS Traffic Shaping

This advanced feature is provided for expert users to fine tune their network connections. Traffic shaping allows you to give preference to certain types of network traffic to maintain quality of service when a network connection is under heavy load.

QoS autoshaper

The **Auto Traffic Shaper** uses a set of inbuilt traffic shaping rules to attempt to ensure low latency on interactive connections, while maintaining fast throughput on bulk transfers.

1. Click **Edit** next to the network interface on which you wish to enable the autoshaper.



QoS Traffic Shaping

QoS Autosshaper | **ToS Traffic Shaping**

Port: WAN (Internet Port)

Enable:

Inbound Speed (kbits/sec): 64

Outbound Speed (kbits/sec): 64

Finish Cancel

2. Click **Enable** and enter the **Outbound Speed** (upstream speed) of this interface's network connection in megabits per second. Click **Finish**.

Note

If you have a PPTP or PPPoE connection to the Internet, enter approximately 80 – 90% of the speed that the ISP supplied to account for protocol overheads.

ToS traffic shaping

Traffic shaping provides a level of control over the relative performance of various types of IP traffic. The traffic shaping feature of your Secure Router allows you to allocate **High**, **Medium**, or **Low** priority to the following services such as **domain (tcp)**, **domain (udp)**, **ftp**, **ftp-data**, **http**, **https**, **imap**, **irc**, **nntp**, **ntp**, **pop3**, **smtp**, **ssh**, and **telnet**.



QoS Traffic Shaping

QoS Autosshaper | **ToS Traffic Shaping**

Enable Traffic Shaping:

Default priority: Medium

Submit

Services	Priority		
SSH	High		
Telnet	Low		
FTP Data	Low		

New

1. Check **Enable Traffic Shaping**, select a **Default priority** and click **Submit** to enable this feature. The **Default priority** is assigned to all network services other than those specifically added below.
2. To add a service, click **New** then **New** again. Select the **Protocol** and **Port** on which this service runs. Select **Priority** for this service click **Finish**.

4. Firewall

The Secure Router is equipped with a fully featured, stateful firewall. The firewall allows you to control both incoming and outgoing access, so that PCs on local networks can have tailored Internet access facilities while being shielded from malicious attacks from external networks.

The Secure Router's stateful firewall keeps track of outgoing connections (e.g. a PC on your LAN requesting content from a server on the Internet) and only allows corresponding incoming traffic (e.g. the server on the Internet sending the requested content to the PC).

By default, your Secure Router allows network traffic as shown in the following table:

Incoming Interface	Outgoing Interface	Action
LAN	Any	Accept
VPN	Any	Accept
Internet	Any	Drop

Sometimes it is useful to allow some incoming connections, e.g. if you have a mail or web server on your LAN or DMZ that you want to be accessible from the Internet. This is accomplished using a combination of NAT and packet filter rules.



The Secure Router web management console provides a powerful interface for tailoring your firewall to your network. For details, refer to the Customizing your Firewall section later in this chapter.

Incoming Access

The **Incoming Access** section allows you to control access to the Secure Router itself, e.g. for remote administration. Click **Incoming Access** under **Firewall** on the main menu to display the **Incoming Access** configuration page.

Administration services

The following figure shows **the Administration Services** page:

Administration Services  

Administration Services **Web Server**

Administration Services

By default the Secure Router runs a web administration service and a telnet service. You can enable these services on specific interface types by checking the boxes below.

Warning: Disabling **all** of the services will make future configuration changes to the unit impossible without a factory reset.

	Telnet	SSH	Web (HTTP)	SSL Web (HTTPS)
LAN interfaces	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Internet interfaces	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

ICMP messages relating to existing connections are always accepted. You can also choose to accept ICMP echo request messages on Internet interfaces.

Accept echo request (incoming ping)

By default the Secure Router runs a web administration server, a Telnet and an SSH service. Access to these services can be restricted to specific interfaces.

Typically, access to the web management console (**Web/SSL Web**) is restricted to hosts on your local network (**LAN Interfaces**).

Disallowing all services is not recommended, as this makes future configuration changes impossible unless your Secure Router is reset to the factory default settings.

Warning

*If you do want to allow administrative access on interfaces other than **LAN Interfaces**, there are several security precautions you should take. See the note in the next section for details. Also consider remote administration using a VPN connection as an alternative to opening a hole in the firewall, PPTP in particular is well suited to this task.*

You can also select to **Accept echo request (incoming port)** on Internet interfaces. The default is to disallow echo requests, so your Secure Router does not respond to pings on its Internet interfaces. This may make it more difficult for external attackers scanning for hosts to discover your Secure Router. Destination unreachable ICMP messages are always accepted.

Web Server

Click the **Web Server** tab to configure the Secure Router's administrative web server. This web server is responsible for running the web management console.

Here you can change the port on which the server runs. Most Secure Routers support enabling SSL encryption for establishing secure connections to the web management console from SSL enabled browsers.

The screenshot shows the 'Web Server' configuration page. At the top, there are tabs for 'Administration Services' and 'Web Server'. Under 'Web Server', there are sub-tabs for 'Web Server', 'Upload SSL Certificates', and 'Create SSL Certificates'. The 'Web Server' sub-tab is active. The page contains a text block explaining that the router can be configured to run on a port other than the default HTTP port (80). Below this is a 'Web server port' input field with the value '80' and a 'Submit' button. A section titled 'Secure Router SSL/HTTPS Web Server Support' contains a message: 'A valid SSL certificate has been installed'. It explains that the URL becomes 'https://' instead of 'http://'. Below this, it states that the web server can be configured in one of three ways: 'Normal (HTTP) and SSL (HTTPS) web server access' (selected), 'Disable SSL (HTTPS) web server access', and 'Disable normal (HTTP) web server access'. A 'Submit' button is at the bottom.

Note

Changing the web server port number is recommended if you are allowing Internet access to the Management Console. This may help hide the web management console from casual web surfers who type your Secure Router's Internet IP address into a web browser.

Ideally, you should use packet filter rules (see the Packet Filtering section later in this chapter) to restrict who has access for remote administration (i.e. allow connections on the administrative web server port from trusted originating IP addresses only).

By default, the web management console runs on the default HTTP port (i.e. 80).

After changing the web server port number, you must include the new port number in the URL to access the pages. For example, if you change the web administration to port number 88, the URL to access the web administration is similar to: <http://192.168.0.1:88>

Customizing the Firewall

The majority of firewall customization is typically accomplished by creating **Packet Filter** and network address translation (**NAT**) rules.

Packet filter rules match network packets based on a combination of incoming and outgoing interface, source and destination address and destination port and protocol. Once a packet is matched, it can be allowed or disallowed.

NAT rules match packets in a similar manner. However, instead of simply allowing or disallowing traffic, you may alter the source or destination address and/or port of the packet as it passes through the firewall.

A typical use of NAT rules is to forward packets destined for your Internet IP address to an internal web server or email server on your LAN. This is known as a port forward, or destination NAT as it alters the destination address of the packet.

The first step in creating packet filter or NAT rules, is to define services (such as web or email) and addresses (such as your internal web server, or a trusted external host) under **Definitions**.

Definitions

Before creating packet filter or NAT rules, it is useful to define services or groups of services, addresses and interfaces to be used to match packets.

Definitions need not be created for simple rules that only specify a single service, address or interface, as these can be entered while creating the rule.

If a rule specifies groups of services, addresses or interfaces, then you must create definitions for these groups before creating the rule.

Service groups

A network service is defined by a protocol and port. Protocol may be either TCP, UDP, ICMP or IP, and port may be any valid network port number (i.e. 1 and 65535), e.g. HTTP (web) uses the TCP protocol, with a default port of 80. Network packets may be matched by destination service.

Click the **Service Groups** tab. Any services that have already been defined are displayed. Click **New** to add a new service group, or select an existing service group and click **Modify**.

Adding or modifying a service group is shown in the following figure:

The screenshot shows a window titled "Service Groups" with three tabs: "Service Groups", "Addresses", and "Interfaces". The "Service Groups" tab is active, and a "Modify Service Group" dialog is open. The dialog has a yellow header bar with the title "Modify Service Group". Below the header, the "Name" field contains "Domain (TCP)". A list of services follows, each with a checkbox: "Domain (UDP)" (unchecked), "Domain (TCP)" (checked), "FTP" (unchecked), "HTTP (Web)" (unchecked), "HTTPS" (unchecked), "IMAP4 (E-Mail)" (unchecked), "IRC" (unchecked), "NNTP (News)" (unchecked), "NTP (Time)" (unchecked), "POP3 (E-Mail)" (unchecked), "SMTP" (unchecked), "SNMP" (unchecked), "SSH" (unchecked), and "Telnet" (unchecked). Below the list are four input fields: "Other TCP Ports", "Other UDP Ports", "IP Protocols", and "ICMP Types". At the bottom of the dialog are "Finish" and "Cancel" buttons.

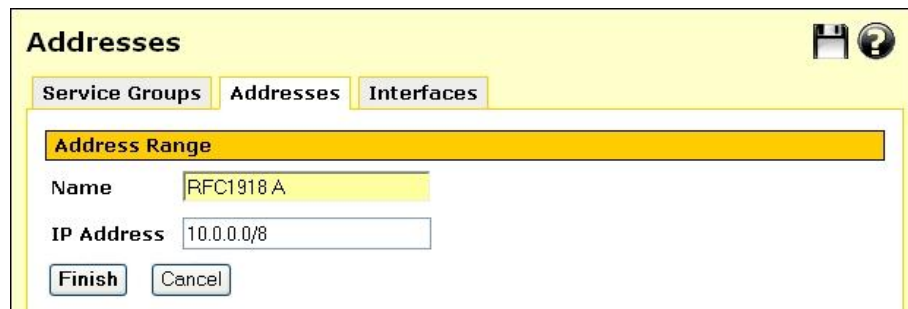
A service group can be used to group together similar services. For example, you can create a group of services that you wish to allow, and then use a single rule to allow them all at once. Select the services from the list of predefined services, or enter the port number to define a custom TCP, UDP, ICMP or IP service. A service may belong to multiple service groups.

Addresses

Addresses are a single IP address, or range of IP addresses, or a DNS hostname. Network packets may be matched by source or destination address.

1. Click the **Addresses** tab. Any addresses that have already been defined are displayed.
2. Click **New** to add a new address, or select an existing address and click **Modify**. There is no need to add addresses for the Secure Router's interfaces, these are predefined.

Adding or modifying an address is shown in the following figure:



You may either add a **Single Address or Range** or **DNS Hostname**. You may also group previously added addresses together by defining an **Address Group** to simplify your firewall ruleset.

3. Select how you would like to add the address or addresses, and click **New**. Enter the DNS **Hostname**, the **IP Address**, or address range and an optional descriptive **Name**, or select the addresses to group and enter a descriptive **Name**.
4. Click **Finish**.

Warning

DNS hostnames are not generally recommended for enforcing security policies. They are unreliable, and may cause significant delays in updating the firewall rules.

Interfaces

Packets may also be matched by incoming and outgoing **Interface**.

You may group the Secure Router network interfaces into **Interface Groups**, to simplify your firewall ruleset. Select the interfaces to group and enter a descriptive **Name** (required). Click **Finish**.

Packet Filtering

Packet filter rules match traffic based on a combination of the source and destination address, incoming and outgoing interface, and destination service. Matched packets may be allowed or disallowed.

Packet filter rules

1. Click **Packet Filter Rules**.

			Descriptive Name	Action	Incoming Interface	Outgoing Interface	Source Address	Destination Address	Services		
<input checked="" type="checkbox"/>	↓	↑	Drop Windows Networking	Accept	Any	Any Internet interface	Any	Any	Windows Networking		
<input type="checkbox"/>	↑	↓	Drop RFC1918 Incoming	Drop	Any Internet interface	Any	RFC1918	Any	Any		
<input type="checkbox"/>	↑	↑	Drop RFC1918 Outgoing	Drop	Any	Any Internet interface	Any	RFC1918	Any		

2. Click **New** to add a new filter rule.

Any rules that have already been defined are displayed, you may **Edit** or **Disable/Enable** these rules by clicking the appropriate icon.

You may also add a new rule above an existing one by clicking the **Add Above** icon.

Note

The first matching rule determines the action for the network traffic, so the order of the rules is important. You can use the **Move Up** and **Move Down** icons to change the order. The rules are evaluated top to bottom as displayed on screen.

Adding or modifying a rule is shown in the following figure:



The **Action** specifies what to do if the rule matches.

- **Accept** means to allow the traffic.
- **Drop** means to disallow the traffic.
- **Reject** means to disallow the traffic, but also send an ICMP port unreachable message to the source IP address.
- **None** means to perform no action for this rule. This is useful for a rule that logs packets, but performs no other action.

The **Incoming Interface** is the interface/network port that the Secure Router received the network traffic on. Set this to **None** to match traffic destined for the Secure Router itself.

The **Outgoing Interface** is the interface/network port that the Secure Router routes the network traffic out. Set this to **None** to match traffic originating from the Secure Router itself.

The **Source Address** is the address that the traffic is arriving from.

The **Destination Address** is the address that the traffic destined to.

Warning

*The previous four fields may be set to **Any**. **Any** does not match traffic sent or received by the Secure Router itself, only traffic passing through it.*

The four fields above may also be set to **None** or **Any**. **None** matches requests originating from the Cyber

None matches network traffic that is destined for the Secure Router itself. This is useful for controlling access to services provided by the Secure Router, such as the web management console.

Note

*When adding a rule, you may either use **Predefined** addresses or services that have been added under **Definitions**, or click **New** to manually enter an address or service.*

The **Log** option controls whether to log the first packet of the connection to the Secure Router's system log. You may enter a **Log Prefix** to make it easier to identify which rules are being matched when inspecting the system log.

Custom firewall rules

The **Custom Firewall Rules** and **Custom IPv6 Firewall Rules** tabs allow firewall experts to view the current firewall rules and add custom *iptables* firewall rules.

Note

*Only experts on firewalls and *iptables* are able to add effective custom firewall rules.*

*Configuring the Secure Router's firewall via the **Incoming Access** and **Outgoing Access** and **Packet Filtering** configuration pages is adequate for most applications.*

Refer to *Appendix C – System Log* for details on creating custom log rules using *iptables*.

Network Address Translation (NAT)

Network address translation (NAT) modifies the IP address and/or port of traffic traversing the Secure Router. The Secure Router supports several types of network address translation.

The most common of these is **Port Forwarding** (also known as port address translation, PAT or destination NAT, DNAT). This is typically used to alter the destination address (and possibly port) of matched packets arriving on the Secure Router Internet interface to the address of a host on the LAN. This is the most common way for internal, masqueraded servers to offer services to the outside world.

Source NAT rules are useful for masquerading one or more IP addresses behind a single other IP address. This is the type of NAT used by the Secure Router to masquerade your private network behind its public IP address.

To a server on the Internet, requests originating from the hosts behind masqueraded interface appear to originate from the Secure Router, as matched packets have their source address altered. You may enable or disable source NAT between interfaces under **Masquerading**, and fine tune source NAT rules under **Source NAT**.

1-to-1 NAT is a combination of destination NAT and source NAT. Both destination NAT and source NAT rules are created for full IP address translation in both directions. This can be useful if you have a range of IP addresses that have been added as interface aliases on the Secure Router's WAN interface, and want to associate one of these external alias IP addresses with a single internal, masqueraded computer. This effectively allocates the internal computer its own real world IP address, also known as a *virtual DMZ*.

Port forwarding

Port forwarding rules alter the destination address and optionally the destination port of packets received by the Secure Router.

Port forwarding allows controlled access to services provided by machines on your private network to users on the Internet by forwarding requests for a specific service coming into one of the Secure Router's interfaces (typically the WAN interface) to a machine on your LAN, which services the request.

1. Click **Port Forwarding**. Any rules that have already been defined are displayed, you may **Edit** or **Disable/Enable** these rules by clicking the appropriate icon.
2. Click **New** to add a new rule.

You may also add a new rule above an existing one by clicking the **Add Above** icon, or below with **Add Below**.

Note

*The first matching rule determines the action for the network traffic, so the order of the rules is important. You can use the **Move Up** and **Move Down** icons to change the order. The rules are evaluated top to bottom as displayed on screen.*

Note

The example shown in the screenshot above forwards the SSH (secure shell) protocol to an internal server (barry’s server). SSH allows encrypted remote access, typically to a server running Linux, BSD or another Unix-like operating system.

In this example, port 2222 is used rather than the standard SSH port of 22, this is to allow remote access using SSH to the Secure Router itself, which runs an SSH server on port 22. So a remote user connects to port 2222 on Secure Router’s Internet address in order to access port 22 of Barry’s server.

The following fields are displayed:

- Descriptive Name** An arbitrary name for this rule
- Enable** Uncheck to temporarily disable this rule
- Create Packet Filter Rule** Create a corresponding packet filter rule to accept NATED packets, generally leave this checked unless you want to manually create a more restrictive filter rule through **Rules**

This rule is applied to packets that match the criteria described by the next four fields.

- Destination Address** The destination address of the request, this is the address that is altered
- Protocol** The protocol of the packet

Ports The destination service port or ports of the request, note that many public ports may be forwarded to a single internal port

The next two fields describe how matching packets should be altered.

To Destination Address The address to replace the **Destination Address** (this is typically the private address of a host on the LAN)

Optional To Ports The port to replace **Ports**, if you leave this blank the port remains unchanged, otherwise enter the port on the host at **To Destination Address** to service the request

3. Click **Advanced** if you want to specify the incoming interface and source address, otherwise this rule is applied to all WAN interfaces and all source addresses are matched.

Incoming Interface The interface that receives the request

Source Address The address from which the request originated (for port forwarding you may specify this to restrict the internal service to be only accessible from a specific remote location)

Note

*When adding a rule, you may either use **Predefined** addresses or services that have been added under **Definitions**, or click **New** to manually enter an address or service.*

Port forwarding to an internal mail server

The following is an example of using port forwarding to allow hosts on the Internet to send and receive mail using a mail server on your LAN.

Warning

Precautions must be taken when configuring the mail server, otherwise you become susceptible to such abuse as unauthorized relaying of unsolicited email (spam) using your server. Configuration of the email server is outside the scope of this manual.

Where possible, add packet filter rules to restrict access to the internal email server to trusted external hosts only.

Add a service group to group email services (SMTP, POP3 and IMAP).

1. Click **Definitions**, the **Service Groups** tab; then, **New**.

2. Enter *E-Mail* in **Name**.

Service Groups

Service Groups | Addresses | Interfaces

Modify Service Group

Name	POP3 (E-Mail)
Domain (UDP)	<input type="checkbox"/>
Domain (TCP)	<input type="checkbox"/>
FTP	<input type="checkbox"/>
HTTP (Web)	<input type="checkbox"/>
HTTPS	<input type="checkbox"/>
IMAP4 (E-Mail)	<input checked="" type="checkbox"/>
IRC	<input type="checkbox"/>
NNTP (News)	<input type="checkbox"/>
NTP (Time)	<input type="checkbox"/>
POP3 (E-Mail)	<input checked="" type="checkbox"/>

3. Check one or both of **IMAP4 (E-Mail)** if your server supports IMAP mail retrieval and **POP3 (E-Mail)** if your server supports POP3 mail retrieval.

Other TCP Ports: 25

Other UDP Ports:

IP Protocols:

ICMP Types:

Finish Cancel

4. Enter *smtp* in **Other TCP Ports**. This is the protocol remote clients use for sending mail via the server.

5. Click **Finish**.

6. Click **NAT**, the **Port Forwarding** tab; then click **New**.

Modify Port Forwarding.

1. Click **Advanced** at the bottom of the page.

Port Forwarding

Port Forwarding | Source NAT | 1 to 1 NAT | Masquerading | UPnP Gateway

Modify Port Forward

Descriptive Name: Mail server

Enable:

Create Packet Filter Rule:

Match packet fields:

Incoming Interface: Any

Source Address: Any [New]

Destination Address: Internet via mlh (Port B, 10.23.0.106) [New]

2. Enter *Mail server* In **Descriptive Name**.
3. Leave **Enable** and **Create Packet Filter Rule** checked.
4. Leave **Incoming Interface** and **Source Address** as **Any**.
5. Select your Internet connection in **Destination Address**.
6. Click **Predefined** next to **Services**.

Services E-Mail [Ports]

Translate packet fields:

To Destination Address 192.168.0.200 [Predefined]

[Finish] [Cancel] [Advanced]

7. Select **E-Mail** from **Services**.
8. Enter your internal email server's IP address in **To Destination Address**.
9. Click **Finish**.

Configure mail clients on the Internet with the Secure Router's Internet IP address as the server to use for sending (SMTP) and receiving (POP3 or IMAP) mail.

Source NAT

Source NAT alters the source address of packets received by the Secure Router. This is typically used for fine tuning the Secure Router's masquerading behaviour.

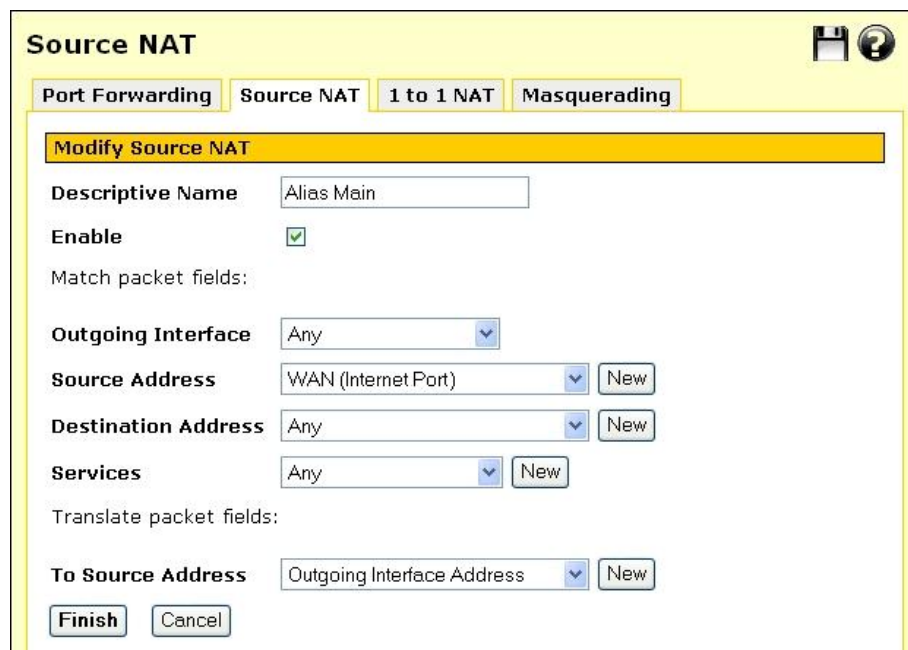
See the *Masquerading* section later in this chapter for information on altering the basic masquerading relationships between your Secure Router's interfaces.

Click **Source NAT**. Any rules that have already been defined are displayed, you may **Edit** or **Disable/Enable** these rules by clicking the appropriate icon. Click **New** to add a new rule.

You may also add a new rule above an existing one by clicking the **Add Above** icon, or below with **Add Below**.

Note

*The first matching rule determines the action for the network traffic, so the order of the rules is important. You can use the **Move Up** and **Move Down** icons to change the order. The rules are evaluated top to bottom as displayed on screen.*



The screenshot shows a web-based configuration interface for 'Source NAT'. At the top, there are tabs for 'Port Forwarding', 'Source NAT', '1 to 1 NAT', and 'Masquerading'. The 'Source NAT' tab is active. Below the tabs is a yellow header bar that says 'Modify Source NAT'. The main configuration area contains several fields: 'Descriptive Name' (text input with 'Alias Main'), 'Enable' (checkbox checked), 'Match packet fields:' section with 'Outgoing Interface' (dropdown 'Any'), 'Source Address' (dropdown 'WAN (Internet Port)' with a 'New' button), 'Destination Address' (dropdown 'Any' with a 'New' button), and 'Services' (dropdown 'Any' with a 'New' button). Below this is the 'Translate packet fields:' section with 'To Source Address' (dropdown 'Outgoing Interface Address' with a 'New' button'). At the bottom are 'Finish' and 'Cancel' buttons. In the top right corner of the window, there are icons for a floppy disk and a question mark.

The following fields are displayed:

- | | |
|-------------------------|--|
| Enable | Uncheck to temporarily disable this rule |
| Descriptive Name | An arbitrary name for this rule |

This rule is applied to packets that match the criteria described by the next four fields.

Outgoing Interface	The interface that the packet to masquerade behind, typically Internet
Source Address	The address from which the request originated, typically be a private address on the LAN or DMZ
Destination Address	The destination address of the request
Services	The destination service port or ports of the request

The next field describes how matching packets should be altered.

To Source Address	The address to replace the Source Address , this is typically a public address of the Secure Router, i.e. Internet or Outgoing Interface Address
--------------------------	---

Note

*When adding a rule, you may either use **Predefined** addresses or services that have been added under **Definitions**, or click **New** to manually enter an address or service.*

1-to-1 NAT

This creates both a source NAT and destination NAT rule for mapping all services on an internal, private address to an external, public address.

Note

After adding a 1-to-1 NAT rule, you must manually create packet filter rules to allow incoming packets on the public address.

Click **Source NAT**. Any rules that have already been defined are displayed, you may **Edit** or **Disable/Enable** these rules by clicking the appropriate icon. Click **New** to add a new rule.

You may also add a new rule above an existing one by clicking the **Add Above** icon, or below with **Add Below**.

Note

*The first matching rule determines the action for the network traffic, so the order of the rules is important. You can use the **Move Up** and **Move Down** icons to change the order. The rules are evaluated top to bottom as displayed on screen.*

The following fields are displayed:

Descriptive Name	An arbitrary name for this rule
Enable	Uncheck to temporarily disable this rule
Private Address	The private address to change
Public Address	The public address, typically a WAN interface alias
Public Interface	Select the interface on which the public address resides, this is typically Internet

Note

When adding a rule, you may either use **Predefined** addresses that have been added under **Definitions**, or click **New** to manually enter an address.

Masquerading

Masquerading is a form of source network address translation (NAT). It translates many addresses (such as private LAN IP addresses) into a single address (such as the external Internet IP address).

Masquerading has the following advantages:

- All machines on the local network can access the Internet using a single ISP account.
- Only one public IP address is used and is shared by all machines on the local network. Each machine has its own private IP address.

The firewall remains active when masquerading is disabled.

Note

The displayed options apply to the firewall classes, not to the ports with these names. That is, the LAN interface options apply to all interfaces that are configured with a LAN connection type, not just to the port labelled as LAN.

*It is strongly recommended that you leave **Enable NAT from LAN/VPN interfaces to Internet interfaces** checked. Typically, this is required to allow Internet access from the LAN.*

Connection Tracking

Connection tracking keeps a record of what packets have passed through the unit, and how they relate to each other. A sequence of related packets is called a connection. This is required for stateful packet filtering and network address translation (NAT).

Most packets are correctly handled by generic support for protocols such as TCP and UDP. However, some protocols are more complicated and require specific connection tracking modules in order to record the state correctly. For example, FTP requires additional connections for data transfer, and also transmits IP addresses and ports within the data portion of packets.

Configuring connection tracking

You can select which connection tracking modules are used by checking the **Enabled** option. Since connection tracking modules can allow additional connections through the firewall, you should disable modules that you do not need.

Connection Tracking

Connection Tracking

Enabled	Module	Description
<input checked="" type="checkbox"/>	ftp	File transfer protocol (FTP)
<input checked="" type="checkbox"/>	h323	H.323 teleconferencing
<input checked="" type="checkbox"/>	irc	Internet relay chat (IRC)
<input checked="" type="checkbox"/>	pptp	Point-to-point tunneling protocol (PPTP)
<input checked="" type="checkbox"/>	tftp	Trivial file transfer protocol (TFTP)

Enable Connection Logging
 Enable Flood Rate Limiting
Flood Rate Limit (per second)

Note

Implementations of protocols such as H.323 can vary, so if you are experiencing problems then you can try disabling the module.

Check **Enable Connection Logging** to log connections to the system log as they are established and expire, however this may result in a lot of log messages if you have a large or busy network.

Intrusion Detection

Note

The SECURE ROUTER provides Basic Intrusion Detection and Blocking only.

The Secure Router provides two intrusion detection systems (IDS): the lightweight and simple-to-configure *Basic Intrusion Detection and Blocking*, and the industrial strength *Advanced Intrusion Detection and Prevention*.

These two systems take quite different approaches. Basic Intrusion Detection offers a number of dummy services to the outside world, which are monitored for connection attempts. Clients attempting to connect to these dummy services can be blocked. *Advanced* Intrusion Detection uses complex rulesets to detect known methods used by intruders to circumvent network security measures, which it either blocks, or logs to a remote database for analysis.

Read on to find out how using an IDS can benefit your network's security, or skip ahead to the *Basic* or *Advanced Intrusion Detection* section for an explanation of configuration options.

The benefits of using an IDS

External attackers attempting to access desktops and servers on the private network from the Internet are the largest source of intrusions. Attackers exploiting known flaws in operating systems, networking software and applications, compromise many systems through the Internet.

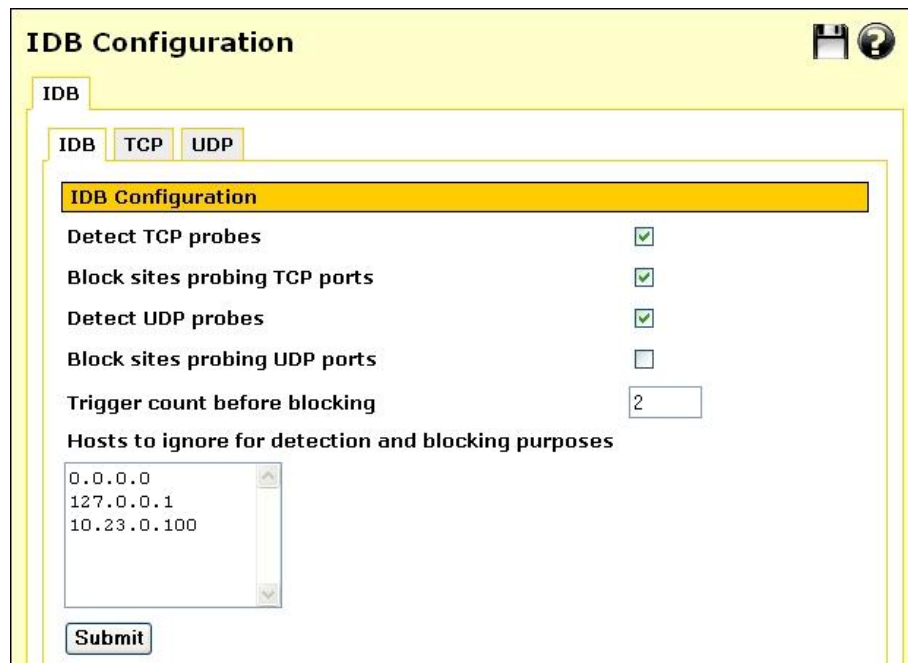
Generally firewalls are not granular enough to identify specific packet contents that signal an attack based on a known system exploit. They act as a barrier analogous to a security guard screening anyone attempting to enter and dismissing those deemed unsuitable, based on criteria such as identification. However identification may be forged. On the other hand intrusion detection systems are more like security systems with motion sensors and video cameras. Video screens can be monitored to identify suspect behaviour and help to deal with intruders.

Firewalls are often easily by-passed through well-known attacks. The most problematic types of attacks are tunnelling-based and application-based. The former occurs when an attacker masks traffic that should be normally screened by the firewall rules by encapsulating it within packets corresponding to another network protocol. Application-based attacks occur when vulnerabilities in applications can be exploited by sending suspect packets directly with those applications.

These attacks can potentially be detected and prevented using an intrusion detection system.

Basic Intrusion Detection and Blocking (IDB)

Click the **IDB** tab to configure basic Intrusion Detection and Blocking (IDB).



The screenshot shows the 'IDB Configuration' web interface. At the top, there are tabs for 'IDB', 'TCP', and 'UDP', with 'IDB' selected. Below the tabs, there is a section titled 'IDB Configuration' with the following settings:

- Detect TCP probes**:
- Block sites probing TCP ports**:
- Detect UDP probes**:
- Block sites probing UDP ports**:
- Trigger count before blocking**:
- Hosts to ignore for detection and blocking purposes**:
 -
 -
 -

A 'Submit' button is located at the bottom of the configuration area.

IDB operates by offering a number of services to the outside world that are monitored for connection attempts. Remote machines attempting to connect to these services generate a system log entry providing details of the access attempt, and the access attempt is denied.

Because network scans often occur before an attempt to compromise a host, you can also deny all access from hosts that have attempted to scan monitored ports. To enable this facility, select one or both of the block options and these hosts are automatically blocked once detected.

IDB Configuration

Detect TCP probes monitors dummy TCP services, **Detect UDP probes** monitors dummy UDP services. **Block sites probing TCP ports** and **Block sites probing UDP ports** blocks hosts attempting to connect to these services from all access to the Secure Router. Connection attempts are logged under **Scanning Hosts**.

Warning

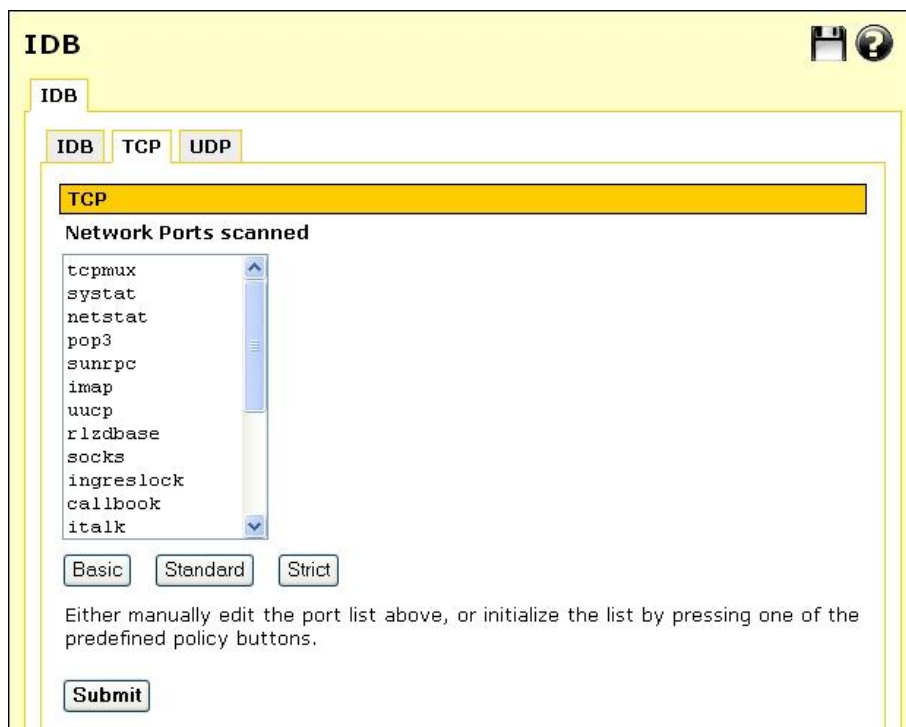
A word of caution regarding automatically blocking UDP requests. Because an attacker can easily forge the source address of these requests, a host that automatically blocks UDP probes can be tricked into restricting access from legitimate services. Proper firewall rules and ignored hosts lists significantly reduces this risk.

Trigger count before blocking specifies the number of times a host is permitted to attempt to connect to a monitored service before being blocked. This option only takes effect when one of the previous blocking options is enabled. The trigger count value should be between 0 and 2 (0 represents an immediate blocking of probing hosts). Larger settings mean more attempts are permitted before blocking and although allowing the attacker more latitude, these settings reduce the number of false positives.

Hosts to ignore for detection and block purposes is a list of host IP addresses which the IDB ignores. This list may be freely edited so trusted servers and hosts are not blocked. The two addresses *0.0.0.0* and *127.0.0.1* cannot be removed from the ignore list because they represent the IDB host. You may enter the IP addresses as a range, see the IP address ranges section further on for more information.

Dummy services

Specify the dummy services to monitor under the **TDP** and **UDP** tabs. Shortcut buttons also provide pre-defined lists of services to monitor.



The **Basic** button installs a bare bones selection of ports to monitor while still providing sufficient coverage to detect many intruder scans. The **Standard** option extends this coverage by introducing additional monitored ports for early detection of intruder scans. The **Strict** button installs a comprehensive selection of ports to monitor and should be sufficient to detect most scans.

Warning

The list of network ports can be freely edited, however adding network ports used by services running on the Secure Router (such as telnet) may compromise the security of the device and your network. It is strongly recommended that you use the pre-defined lists of network ports only.

Access Control and Content Filtering

The access control web proxy allows you to control access to the Internet based on the type of web content being accessed (**Content**), and which user or workstation is accessing the Internet content (**Require user authentication, IP Lists**). This is useful to minimize inappropriate Internet use.

Additionally, you can set up global block/allow lists for web sites that you always want to be accessible/inaccessible (**Web Lists**), or force users to have a personal firewall installed (**ZoneAlarm**) or ensure they are not running network services that may be exploited (**Policy**) before accessing the Internet.

Access control options operate in the following order for web access:

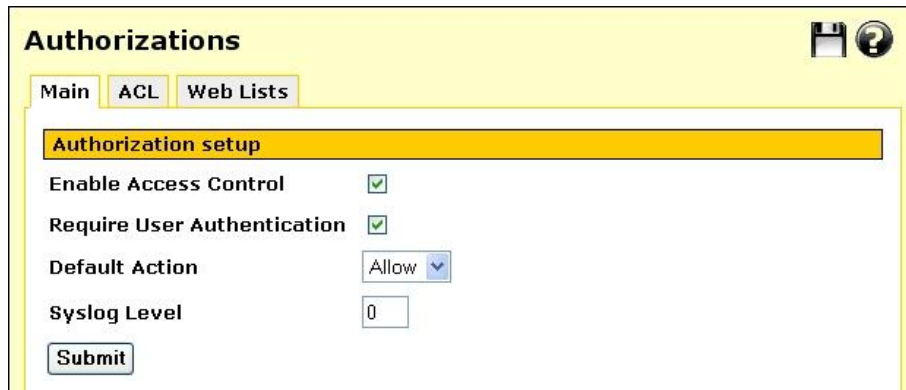
1. **Web Lists** allow
2. **Web Lists** deny
3. Security **Policy** enforcement
4. **ACL** allow
5. **ACL** block

Access control options operate in the following order for all other Internet access:

1. Security **Policy** enforcement
2. **ACL** allow
3. **ACL** block

Enabling access control

Select **Access Control** from the main menu, then the **Main** tab.



The **Enable Access Control** checkbox enables/disables the entire access control subsystem. This box must be checked for *any* access control operation to take place.

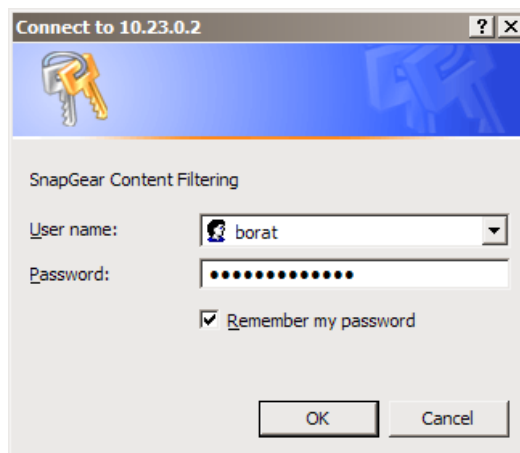
The **Default Action** field defines the behaviour when none of the myriad of settings positively allow or block access. If changed to *block by default*, some definitions must be created elsewhere in access control to allow some network traffic or no access is possible.

The **Require user authentication** checkbox determines if users are asked for a username and password when attempting to access the web through the Secure Router.

The **Syslog level** controls the level of debug output that is logged to the system log. The higher this is set to, the more verbose the output. For normal operation, this should be set to **0** or very large logs and a noticeable system slow down might result. For normal debugging, set this to **1**. Higher levels need only be turned on when so directed by Secure Router support.

User authentication

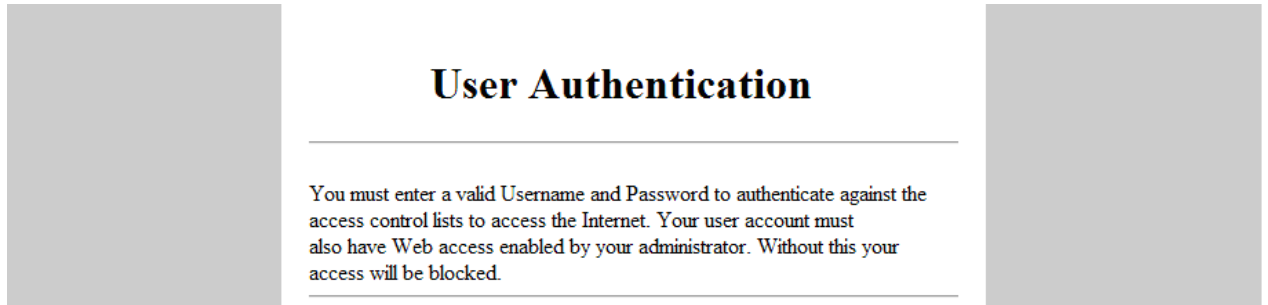
Check **Require user authentication** if you want to require users to authenticate themselves before browsing the web. When attempting to access a web site on the Internet, their browser displays a dialog similar to the following:



Note

To add or remove access controls user accounts, select **Users** from the main menu and click the **Local Users** tab. Access controls users should generally have only **Internet Access (via. Access Controls)** checked, with all other access permissions unchecked. See the *Users* section in the chapter entitled *System* for further details on adding user accounts.

Users without web proxy access see a screen similar to the figure below when attempting to access external web content.



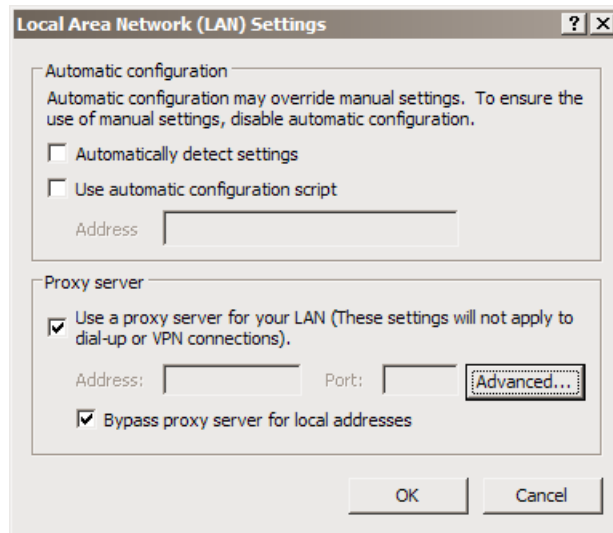
Note

Each browser on the LAN now has to be set up to use the Secure Router's web proxy.

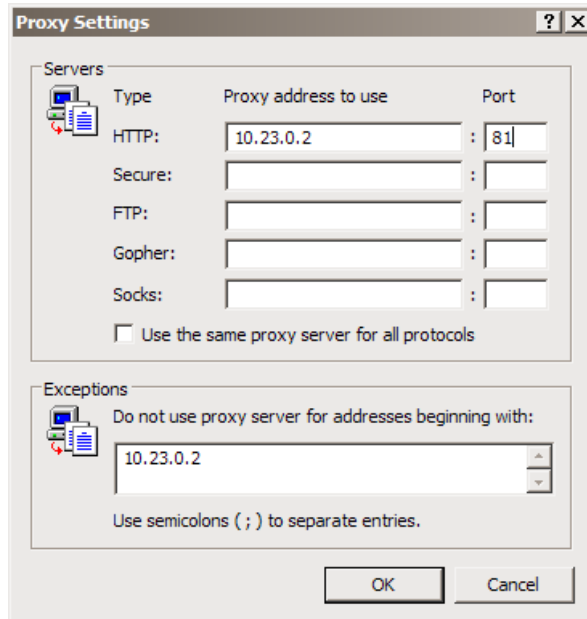
Browser setup

The example given is for Microsoft Internet Explorer 6. Instructions for other browsers should be similar, refer to their user documentation for details on using a web proxy.

1. From the **Internet Options** menu, select **Tools**. From the **LAN Settings** tab, select **LAN Settings**.



2. Check **Use a proxy server for your LAN...** and **Bypass proxy server for local address**. All other options should remain unchecked.
3. Click **Advanced**.



4. In the row labeled **HTTP**, enter your Secure Router's LAN IP address in the **Proxy address to use** column, and *81* in the **Port** column. Leave the other rows blank.
5. In the **Exceptions** text box, enter your Secure Router's LAN IP address.
6. Click **OK**, **OK** and **OK** again.

ACL

Access may be **Blocked** or **Allowed** by the **Source** (LAN) IP address or address range, the **Destination** (Internet) host's IP address or address range, or the **Destination Host**'s name.

Addresses are added through **Definitions** -> **Addresses**, refer to the *Definitions* section earlier in this chapter for further detail.

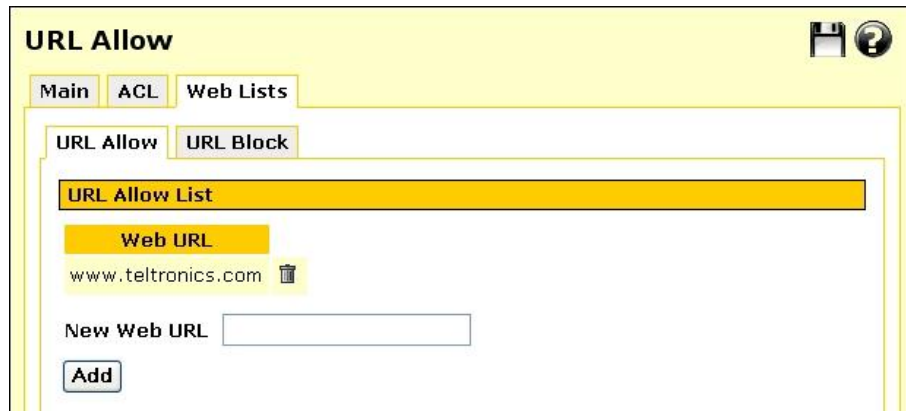
Note

All Internet traffic, not just web traffic, is affected by ACL.

Web lists

Access is be denied to any web address (URL) that contains text **Added** under **URL Block List**, e.g. entering *xxx* blocks access to any URL containing *xxx*, e.g.: <http://www.xxx.com>, <http://xxx.example.com> or www.test.com/xxx/index.html

The **Allow List** also enables access to URLs containing the specified text.



Note

Defining large numbers of URL fragments to match against can result in a significant slowing down of WWW accesses. Defining overly short URL fragments can result in many sites matching and being allowed or denied erroneously.

5. Virtual Private Networking

Virtual Private Networking (VPN) enables two or more locations to communicate securely and effectively, usually across a public network (e.g. the Internet) and has the following key traits:

- **Privacy** - no one else can see what you are communicating
- **Authentication** - you know who you are communicating with
- **Integrity** - no one else can tamper with your messages/data

Using VPN, you can access the NET-PATH Plus network securely across the Internet using Point-to-Point Tunneling Protocol (PPTP), IPSec or L2TP.

VPN technology can also be deployed as a low cost way of securely linking two or more networks, such as a headquarters LAN to the branch office(s). IPSec is generally the most suitable choice in this scenario.

With the Secure Router you can establish a VPN tunnel over the Internet using either PPTP, IPSec or L2TP. IPSec provides enterprise-grade security, and is generally used for connecting two or more networks, such as a branch office to a head office.

PPTP's strength is its ease of configuration and integration into existing Microsoft infrastructure. It is generally used for connecting single remote Windows clients.

L2TP combines elements of IPSec and PPTP. It is generally used as a relatively easy to configure way to bolster a PPTP-style connection from a remote Windows XP client with IPSec security.

This chapter details how to configure the L2TP and PPTP servers and clients, how to configure a remote client to connect, how to establish an IPSec tunnel, and also provides an overview of L2TP VPN tunneling.

PPTP and L2TP

The Secure Router includes a PPTP and an L2TP VPN server. These allow remote Windows clients to securely connect to the local network.

PPTP or L2TP are also commonly used to secure connections from a Guest network; see the *Guest Network* section in the chapter entitled *Network Setup*.

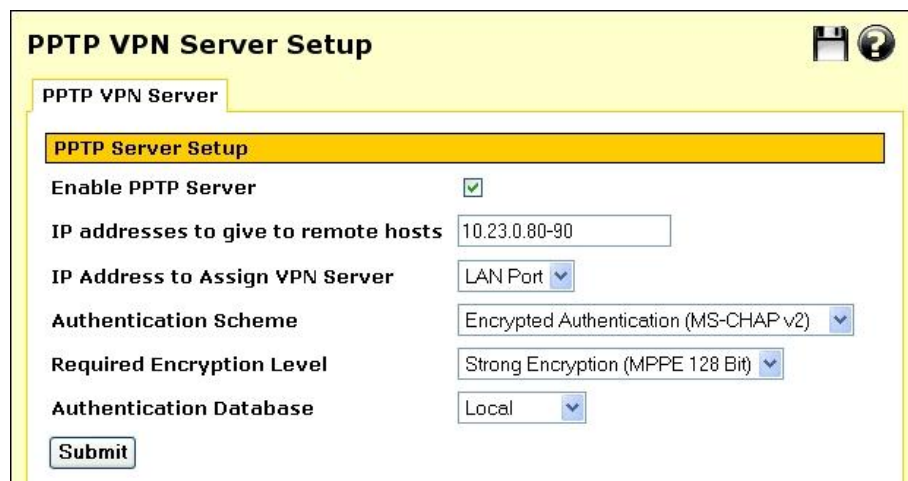
PPTP VPN Server

To setup a PPTP connection from a remote Windows client to your Secure Router and local network:

- Enable and configure the PPTP VPN server.
- Set up VPN user accounts on the Secure Router and enable the appropriate authentication security.
- Configure the VPN clients at the remote sites. The client does not require special software, the Secure Router PPTP Server supports the standard PPTP client software included with Windows 95/98, Windows ME, Windows XP, WinNT and Windows 2000. The Secure Router PPTP server is also compatible with Unix PPTP client software.
- Connect the remote VPN client.

Enable the PPTP server

1. Select **PPTP VPN Server** from the **VPN** section of the main menu.



The screenshot shows the 'PPTP VPN Server Setup' window. It has a yellow header with a floppy disk icon and a help icon. Below the header is a tab labeled 'PPTP VPN Server'. Underneath is a sub-section titled 'PPTP Server Setup' with a yellow background. The configuration options are as follows:

Enable PPTP Server	<input checked="" type="checkbox"/>
IP addresses to give to remote hosts	<input type="text" value="10.23.0.80-90"/>
IP Address to Assign VPN Server	<input type="text" value="LAN Port"/>
Authentication Scheme	<input type="text" value="Encrypted Authentication (MS-CHAP v2)"/>
Required Encryption Level	<input type="text" value="Strong Encryption (MPPE 128 Bit)"/>
Authentication Database	<input type="text" value="Local"/>

At the bottom left of the form is a 'Submit' button.

2. Check **Enable PPTP Server**.

3. Enter the **IP Addresses to give to remote hosts**, this must be a free IP address, or range of free IP addresses, from the network (typically the LAN) that the remote users are assigned while connected to the Secure Router.
4. If you have configured several network connections, select the one that you want to connect remote users to from the **IP Address to Assign VPN Server** pull down menu. This is typically a LAN interface or alias.
5. Select the weakest **Authentication Scheme** to accept, access is denied to remote users attempting to connect using an authentication scheme weaker than this. They are described below, from strongest to weakest.
 - **Encrypted Authentication (MS-CHAP v2):** The strongest type of authentication to use. This is the recommended option.
 - **Encrypted Authentication (MS-CHAP):** This is not a recommended encryption type and should only be used for older dialin clients that do not support MS-CHAP v2.
 - **Weakly Encrypted Authentication (CHAP):** This is the weakest type of encrypted password authentication to use. It is not recommended that clients connect using this as it provides very little password protection. Also note that clients connecting using CHAP are unable to encrypt traffic.
 - **Unencrypted Authentication (PAP):** This is plain text password authentication. When using this type of authentication, the client passwords is transmitted un-encrypted.
6. Select the **Required Encryption Level**, access is denied to remote users attempting to connect not using this encryption level. Using **Strong Encryption (MPPE 128 Bit)** is recommended.
7. Select the **Authentication Database**. This allows you to indicate where the list of valid clients can be found. You can select from the following options:
 - **Local:** Use the local database defined on the **Local Users** tab of the **Users** page. You must enable the **Dialin Access** option for the individual users that are allowed dialin access.
 - **RADIUS:** Use an external RADIUS server as defined on the **RADIUS** tab of the **Users** page.
 - **TACACS+:** Use an external TACACS+ server as defined on the **TACACS+** tab of the **Users** page.

Note

See the Users section of the chapter entitled System for details on adding user accounts for PPTP access, and configuring the Secure Router to enable authentication against a RADIUS or TACACS+ server.

Add a PPTP user account

Select **Users** under **System** from the main menu, click **Local Users** and a **New** user with **PPTP Access**. Keep note of the **Username** and **Password**, as these are required in configuring the remote PPTP client.

Refer to the the *Users* section of the chapter entitled *System* for a more detailed account of adding a new local user.

Setup the remote PPTP client

To connect remote VPN clients to the local network, you need to know the username and password for the PPTP account you added, as well as the Secure Router's Internet IP address.

Your Internet IP address is displayed on the **Network Setup** page.

Ensure the remote VPN client PC has Internet connectivity. To create a VPN connection across the Internet, you must set up two networking connections. One connection is for ISP, and the other connection is for the VPN tunnel to your office network.

Note

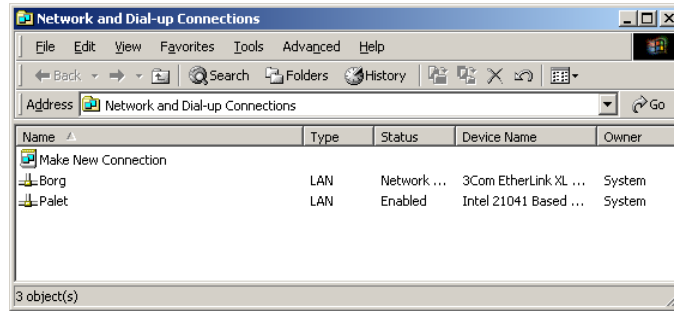
If you are using Windows 95 or an older version of Windows 98 (first edition), install the Microsoft DUN update and VPN Client update, available from the Microsoft website.

Your Secure Router's PPTP server interoperates with the standard Windows PPTP clients in all current versions of Windows.

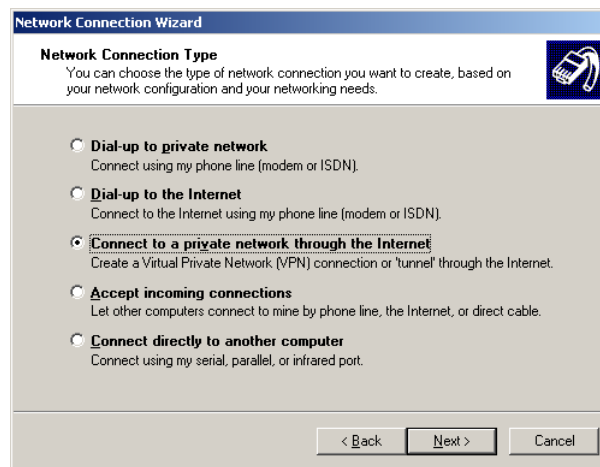
The following sections provide details for client setup in Windows 2000 and Windows XP. More detailed instructions are available in the Windows product documentation, and from the Microsoft website.

Windows 2000 PPTP client setup

1. Log in as *Administrator* or with Administrator privileges. From the **Start** menu, select **Settings** and then **Network and Dial-up Connections**. A window similar to the following is displayed.

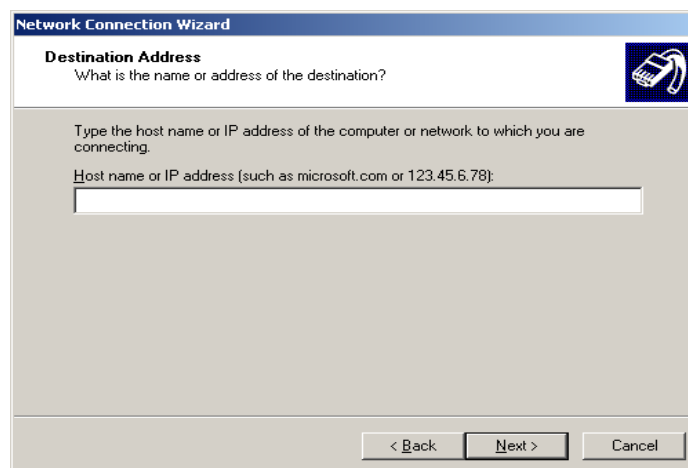


2. Double-click **Make New Connection** from the main windows. Click **Next** to show the **Network Connection Type** window:



3. Select **Connect to a private network through the Internet**.
4. Click **Next**.

This displays the **Destination Address** window:



5. Enter the Secure Router's Internet IP address or fully qualified domain name and click **Next**. Select the **Connection Availability** you require on the next window and click **Next** to display the final window:

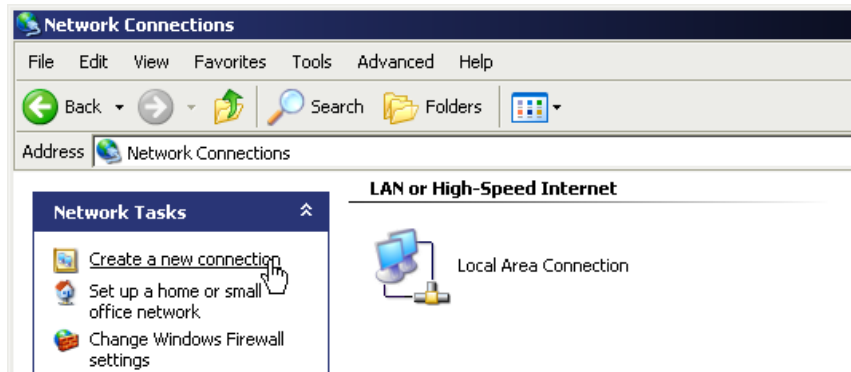


6. Enter an appropriate name for your connection.
7. Click **Finish**.

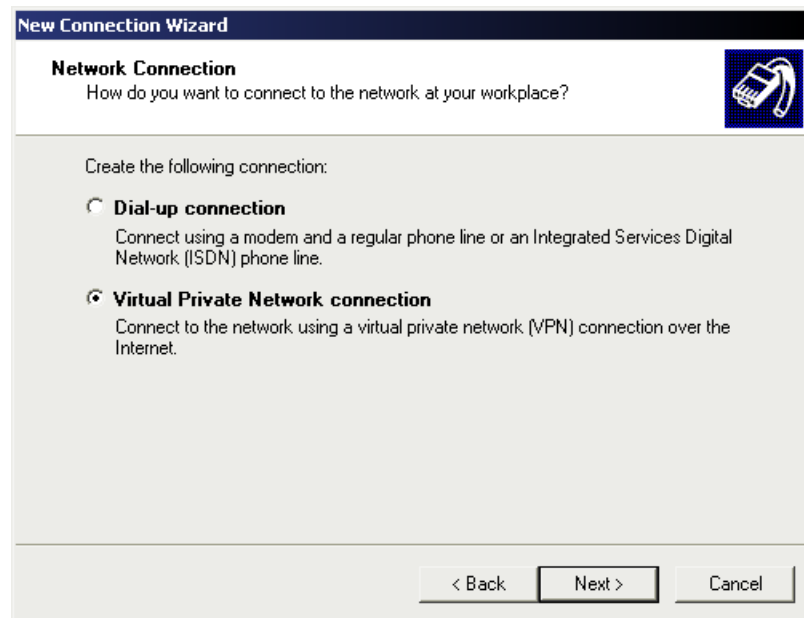
Your VPN client is now set up and ready to connect.

Windows XP PPTP client setup

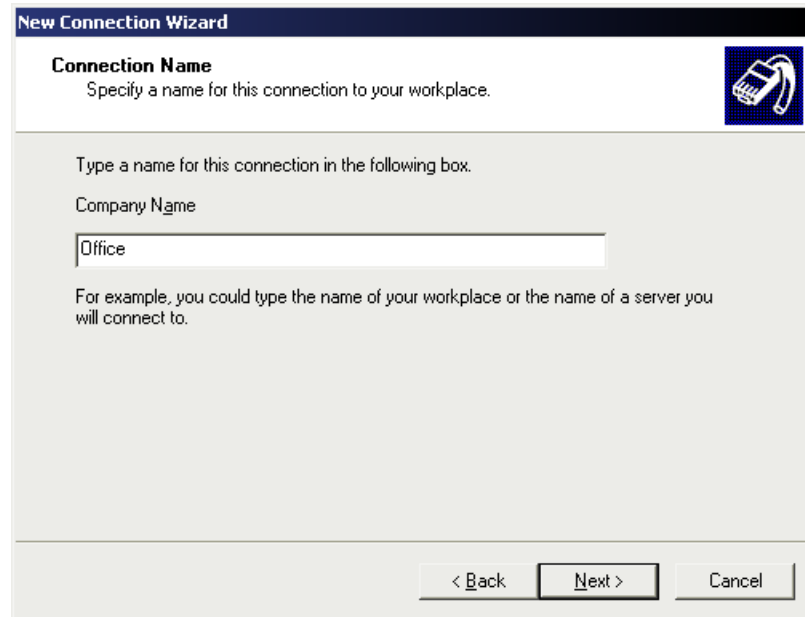
1. Log in as *Administrator* or with Administrator privileges. From the **Start** menu, select **Settings** and then **Network Connections**.



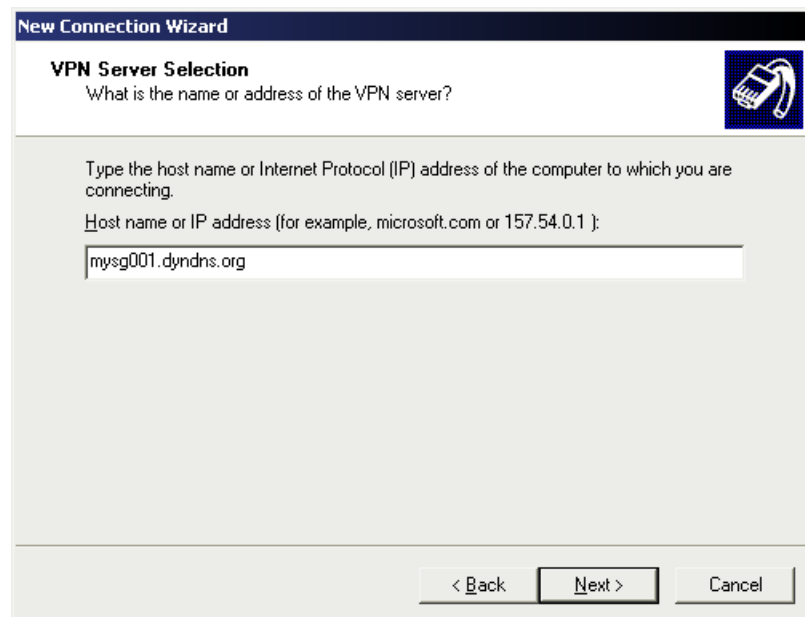
2. Click **Create New Connection** from the **Network Tasks** menu to the left.



3. Select **Connect to the network at my workplace** and click **Next**. Select **Virtual Private Network connection** and click **Next**.



4. Choose a **Connection Name** for the VPN connection, such as your company name or simply *Office*. Click **Next**.
5. If you have set up your computer to connect to your ISP using dial up, select **Automatically dial this initial connection** and your dial up account from the pull down menu. If not, or you wish to manually establish your ISP connection before the VPN connection, select **Do not dial the initial connection**. Click **Next**.

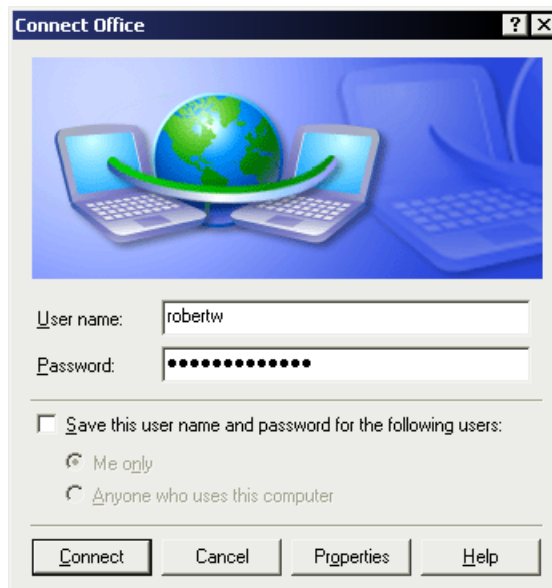


6. Enter the Secure Router PPTP appliance's Internet IP address or fully qualified domain name and click **Next**. Select whether you wish make this connect available to all users and whether you wish to add a shortcut to your desktop and click **Finish**.

Your VPN client is now set up and ready to connect.

Connect the remote VPN client

1. Verify that you are connected to the Internet, or have set up your VPN connection to automatically establish an initial Internet connection.
2. Select the connection for the Secure Router VPN.



3. Enter a username and password added in the *Configuring user accounts for VPN server* section and click **Connect**.

L2TP VPN Server

To setup an L2TP/IPSec connection from a remote Windows XP client to your Secure Router and local network:

- Enable and configure the L2TP VPN server.
- Configure IPSec tunnel settings.
- Set up VPN user accounts on the Secure Router and enable the appropriate authentication security.

- Configure the VPN clients at the remote sites. The client does not require special software, the Secure Router L2TP Server supports the standard L2TP and IPSec client software included with Windows XP.
- Connect the remote VPN client.

L2TP server setup

1. Select **L2TP VPN Server** from the **VPN** section of the main menu.

2. Check **Enable L2TP Server**.
3. Enter the **IP Addresses to give to remote hosts**, this must be a free IP address, or range of free IP addresses, from the network (typically the LAN) that the remote users are assigned while connected to the Secure Router.
4. If you have configured several network connections, select the one that you want to connect remote users to from the **IP Address to Assign VPN Server** pull down menu. This is typically a LAN interface or alias.
5. Select the weakest **Authentication Scheme** to accept, access is denied to remote users attempting to connect using an authentication scheme weaker than this. They are described below, from strongest to weakest.
 - **Encrypted Authentication (MS-CHAP v2):** The strongest type of authentication to use. This is the recommended option.
 - **Encrypted Authentication (MS-CHAP):** This is not a recommended encryption type and should only be used for older dialin clients that do not support MS-CHAP v2.

- **Weakly Encrypted Authentication (CHAP):** This is the weakest type of encrypted password authentication to use. It is not recommended that clients connect using this as it provides very little password protection. Also note that clients connecting using CHAP are unable to encrypt traffic.
 - **Unencrypted Authentication (PAP):** This is plain text password authentication. When using this type of authentication, the client passwords is transmitted un-encrypted.
6. Select the **Required Encryption Level**, access is denied to remote users attempting to connect not using this encryption level. Using **Strong Encryption (MPPE 128 Bit)** is recommended.
 7. Select the **Authentication Database**. This allows you to indicate where the list of valid clients can be found. You can select from the following options:
 - **Local:** Use the local database defined on the **Local Users** tab of the **Users** page. You must enable the **Dialin Access** option for the individual users that are allowed dialin access.
 - **RADIUS:** Use an external RADIUS server as defined on the **RADIUS** tab of the **Users** page.
 - **TACACS+:** Use an external TACACS+ server as defined on the **TACACS+** tab of the **Users** page.

Note

See the Users section of the chapter entitled System for details on adding user accounts for PPTP access, and configuring the Secure Router to enable authentication against a RADIUS or TACACS+ server.

8. Click **Submit**.

Add an IPSec tunnel

1. Select **L2TP VPN Server** from the **VPN** section of the main menu and click the **L2TP IPSec Configuration** tab. Any existing L2TP IPSec tunnels are displayed, alongside icons to **Modify** and **Delete** them.

Authentication is performed using x.509 certificates or a pre-shared secret. You may add a single shared secret tunnel for *all* remote clients authenticating using shared secrets, an x.509 certificate tunnel for *each* remote client authenticating using certificates, or both.

- Select **Shared Secret Tunnel** to use a common secret (passphrase) that is shared between the Secure Router and the remote client. This authentication method is relatively simple to configure, and relatively secure.

Note

Only one shared secret tunnel may be added. The one shared secret is used by all remote clients to authenticate.

- Select **x.509 Certificate Tunnel** to use x.509 certificates to authenticate the remote client against a Certificate Authority's (CA) certificate. The CA certificate must have signed the local certificates that are used for tunnel authentication. Certificates need to be uploaded to the Secure Router before a tunnel can be configured to use them (see *Certificate Management* in the *IPSec* section later in this chapter). This authentication method is more difficult to configure, but very secure.

Creating and adding x.509 certificates is detailed in *Certificate Management* in the *IPSec* section later in this chapter.

Note

Multiple x.509 certificate tunnels may be added. A separate x.509 certificate tunnel is required for each remote client to authenticate.

2. Click **New**.

The screenshot shows a web configuration page titled "L2TP IPsec Configuration". It has two tabs: "L2TP VPN Server" and "L2TP IPsec Configuration". The second tab is selected. Below the tabs, there is a section titled "L2TP Server IPsec x509 Certificate Configuration" with a yellow background. This section contains three input fields: "Tunnel Name" with the value "dave_l2tp", "Local Certificate" with a dropdown menu showing "cert1_public", and "Client Distinguished Name" with the value "C=US, ST=Illinois, L=Chicago, O=CyberGuar". At the bottom of the form are "Submit" and "Cancel" buttons.

3. Enter a **Tunnel Name** to identify this connection. It may not be the same as any other L2TP/IPsec or regular IPsec tunnel names.
4. If adding a **Shared Secret Tunnel**, enter the **Shared Secret**. Ensure it is something hard to guess. Keep note of the shared secret, as it will be used in configuring the remote client.
5. If adding an **x.509 Certificate Tunnel**, select the **Local Certificate** that you have uploaded to the Secure Router. Enter the **Client Distinguished Name**; it must match exactly the distinguished name of the remote party's local certificate to successfully authenticate the tunnel. Distinguished name fields are listed.

Note

Certificates need to be uploaded to the Secure Router before a tunnel can be configured to use them (see Certificate Management in the IPSec section later in this chapter).

Add an L2TP user account

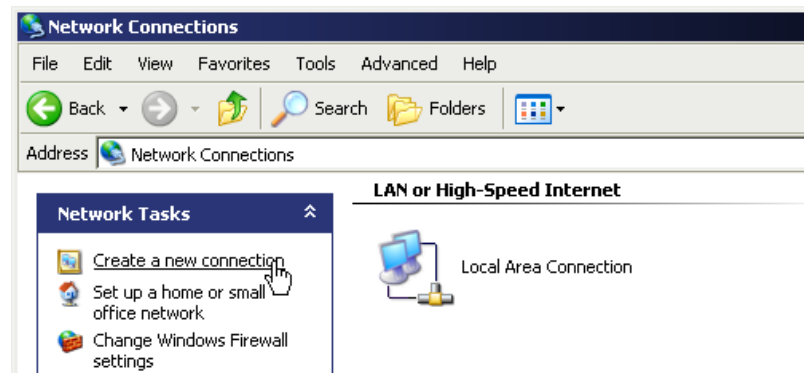
Select **Users** under **System** from the main menu, click **Local Users** and a **New** user with **PPTP Access**. Keep note of the **Username** and **Password**, as these are required in configuring the remote PPTP client.

Refer to the the *Users* section of the chapter entitled *System* for a more detailed account of adding a new local user.

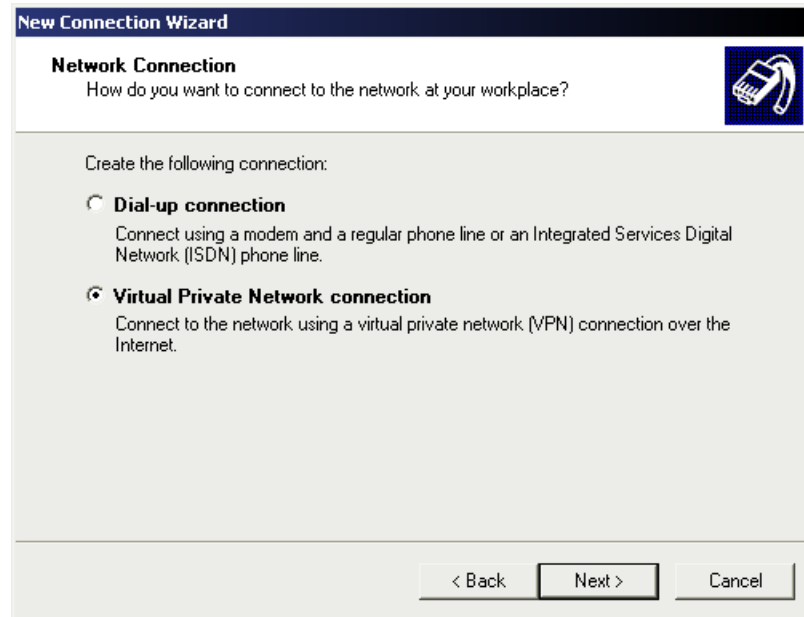
Configure the remote L2TP client

The following instructions are for Windows XP.

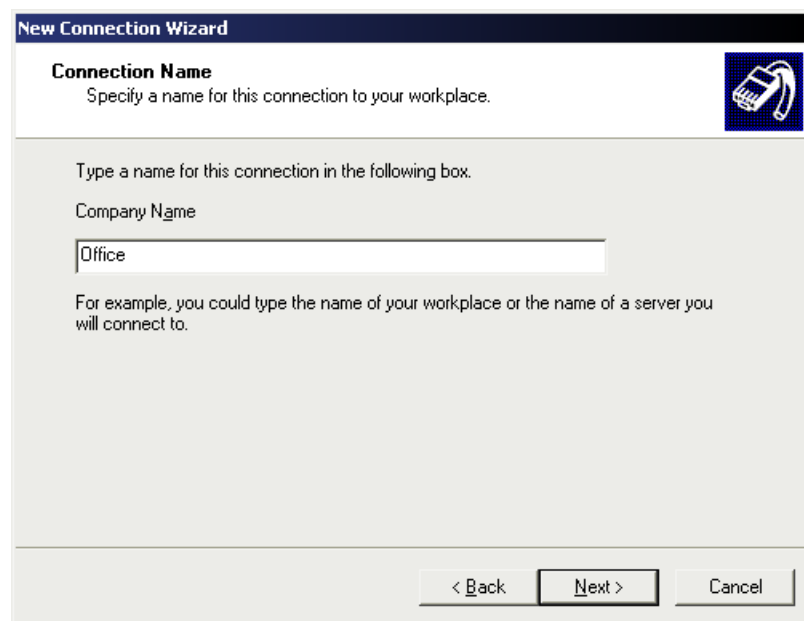
1. Log in as *Administrator* or with Administrator privileges. From the **Start** menu, select **Settings** and then **Network Connections**.



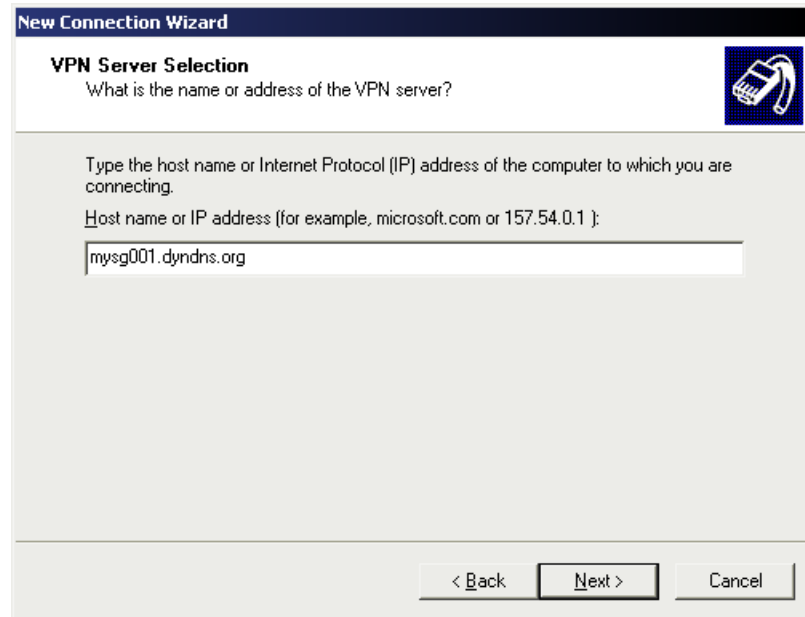
2. Click **Create New Connection** from the **Network Tasks** menu to the left.



3. Select **Connect to the network at my workplace** and click **Next**. Select **Virtual Private Network connection** and click **Next**.

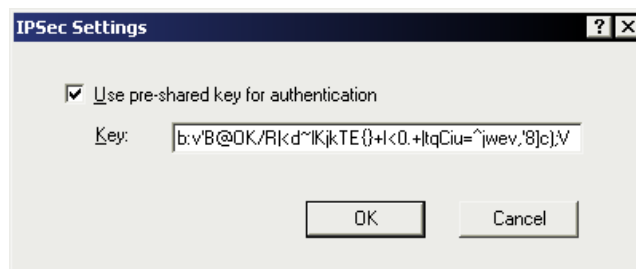


4. Choose a **Connection Name** for the VPN connection, such as your company name or simply *Office*. Click **Next**.
5. If you have set up your computer to connect to your ISP using dial up, select **Automatically dial this initial connection** and your dial up account from the pull down menu. If not, or you wish to manually establish your ISP connection before the VPN connection, select **Do not dial the initial connection**. Click **Next**.



6. Enter the Secure Router PPTP appliance's Internet IP address or fully qualified domain name and click **Next**. Select whether you wish make this connect available to all users and whether you wish to add a shortcut to your desktop and click **Finish**.

- To authenticate using a **Shared Secret Tunnel**, click **Properties** on the **Connect Connection Name** dialog.



7. Click **Security** -> **IPSec Settings**, check **Use pre-shared key for authenticate** and in **Key** enter the **Shared Secret** you selected when configuring the shared secret tunnel on the Secure Router.

- To authenticate using an **x.509 Certificate Tunnel**, you must first install the local certificate. The distinguished name of this local certificate must match that entered in **Client Distinguished Name** when configuring the x.509 certificate tunnel on the Secure Router.

See *Certificate Management* and *Using certificates with Windows IPSec* in the *IPSec* section later in this chapter for details on creating, packaging and adding certificates for use by Windows IPSec.

Note

Once a certificate added, Windows IPSec will automatically use it to attempt to authenticate the connection. If more than one certificate is installed, it will try each of them in turn.

Authentication will not succeed if the Windows client's certificate and the Secure Router's certificate are not signed by the same certificate authority.

Your VPN client is now set up and ready to connect.

Connect the remote VPN client

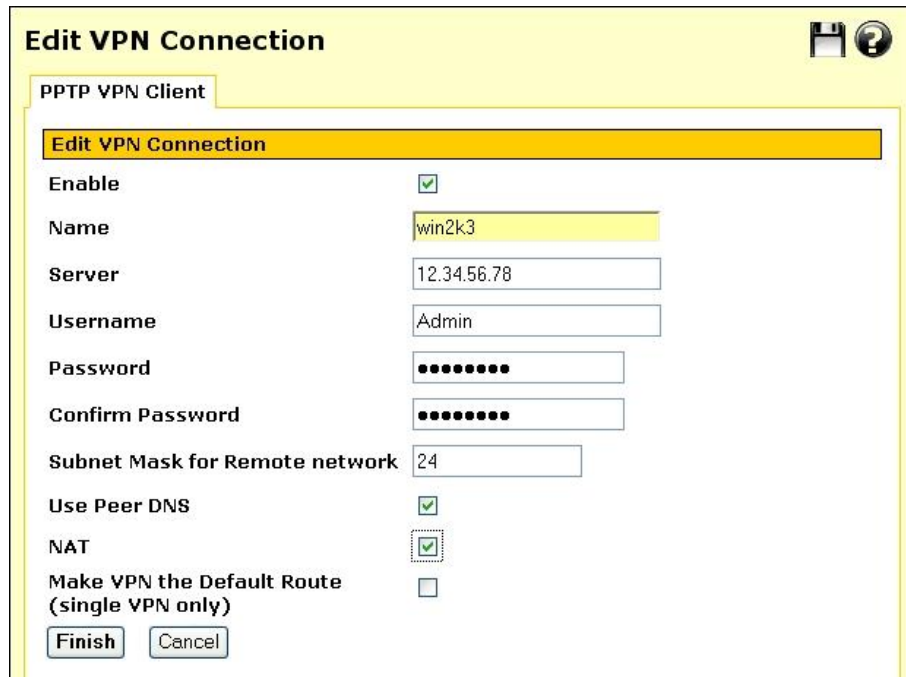
1. Verify that you are connected to the Internet, or have set up your VPN connection to automatically establish an initial Internet connection.
2. Select the connection for the Secure Router VPN.
3. Enter a username and password added in the *Configuring user accounts for VPN server* section and click **Connect**.

PPTP and L2TP VPN Client

The PPTP and L2TP client enables the Secure Router to establish a VPN to a remote network running a PPTP or L2TP server (usually a Microsoft Windows server).

Although the VPN protocols are different, configuration of client tunnels is exactly the same.

1. Select **PPTP VPN Client** or **L2TP VPN Client** from the **VPN** section of the main menu. Any existing client tunnels are displayed alongside icons to **Enable/Disable**, **Delete**, and **Edit** them.
2. To add a new tunnel, click **New**.



3. Ensure **Enable** is checked, and enter:

- A descriptive **Name** for the VPN connection. This may describe the purpose for the connection.
- The remote PPTP or L2TP **Server** IP address to connect to.
- A **Username** and **Password** to use when logging in to the remote VPN. You may need to obtain this information from the system administrator of the remote PPTP server.
- Optionally, the **Subnet Mask for Remote network**. This is used to determine which packets should go the remote network.
- Check **NAT** to masquerade your local network behind the IP address on the remote network that the remote PPTP or L2TP server allocates the Secure Router.
- Check **Make VPN the default route (single VPN only)** if you have a single VPN and want traffic from your local network to be routed through the tunnel instead of straight out onto the Internet.

4. Click **Finish**.

A PPTP status icon appears in the system tray on the bottom right hand side of your computer, informing you that you are connected.

You can now check your e-mail, use the office printer, access shared files and and computers on the network as if you were physically on the LAN.

Note

Depending on how your remote network is set up, some additional configuration may be required to enable browsing the network (aka **Network Neighborhood** or **My Network Places**).

To disconnect, right-click the PPTP Status system tray icon; then, select **Disconnect**.

You can then disconnect from the Internet if you wish.

IPSec

Secure Router to Secure Router

There are many possible configurations in creating an IPSec tunnel. The most common and simplest is described in this section. Additional options are also explained throughout this example, should it become necessary to configure the tunnel with those settings. For most applications to connect two offices together, a network similar to the following is used.

To combine the Headquarters and Branch Office networks together, an IPSec tunnel must be configured on both Secure Routers.

Set Up the Branch Office

Enable IPSec

1. Select **IPSec** from the **VPN** section of the main menu. A page similar to the following is displayed.

IPSec VPN Setup [Save] [Help]

IPSec | Certificate Lists

IPSec General Settings

Enable IPSec

IPSec MTU

Submit

Tunnel List

Connection	Remote Party	Status
No entries		

Refresh New

2. Check the **Enable IPSec** checkbox.

The Maximum Transmission Unit (**MTU**) of the IPSec interface can be configured filling in the desired MTU value in **IPSec MTU**. For most applications this need not be configured, however if it is set, the MTU value should be between 1400 and 1500. In this example leave the checkbox unchecked. Click the **Submit** button to save the changes.

Warning

It may be necessary to reduce the MTU of the IPSec interface if large packets of data are not being transmitted.

Configure a tunnel to connect to the headquarters office

To create an IPSec tunnel, click the **IPSec** link on the left side of the web management console and then click the **New** button under **Tunnel List**. A window similar to the following is displayed.



Tunnel settings page

1. Fill in the **Tunnel name** field with an apt description for the tunnel. The name must not contain spaces or start with a number. In this example, enter *Headquarters*.
2. Leave the **Enable this tunnel** checkbox checked.
3. Select the interface the IPSec tunnel is to go out on. The options depend on what is currently configured on the Secure Router. For the vast majority of setups, this is the **default gateway interface** to the Internet. In this example, select the **default gateway interface** option.

Note

Select an interface other than the default gateway when you have more than one Internet connection or have configured aliased Internet interfaces, and require the IPSec tunnel to run on an interface other than the default gateway.

4. Select the type of keying for the tunnel to use. The Secure Router supports the following types of keying:

- **Main Mode** automatically exchanges encryption and authentication keys and protects the identities of the parties attempting to establish the tunnel.

This mode is the most secure, but difficult to configure in environments where one end has a dynamic Internet IP address.

- **Aggressive Mode** automatically exchanges encryption and authentication keys and uses less messages in the exchange when compared to main mode.

Aggressive mode is typically used to allow parties that are configured with a dynamic IP address and a preshared secret to connect or if the Secure Router or the remote party is behind a NAT device.

This mode is less secure than main mode, but much easier to configure in environments where one end has a dynamic Internet IP address. When using this mode, ensure to use a long and particularly hard to guess preshared secret.

- **Manual Keying** requires the encryption and authentication keys to be specified. This mode is not recommended unless connecting to a legacy device that does not support main or aggressive modes.

It is hard to identify problems Manual keying requires regular user intervention in the form of manual key changes, and it is hard to identify

In this example, select the **Aggressive Mode** option.

An IPSec tunnel connects two endpoints. These endpoints may be of different types; however, some configurations are preferable to others with regards to ease of configuration and security (i.e. main vs. aggressive mode) and robustness (i.e. relying on an external DNS server). The following is a list of configurations, from most to least preferable:

1. **static IP address to static IP address**
2. **dynamic IP address to static IP address** (as detailed in this example)
3. **DNS hostname address to static IP address**
4. **DNS hostname address to DNS hostname address**
5. **DNS hostname address to dynamic IP address**

6. Select the type of IPSec endpoint this Secure Router has on the interface on which the tunnel is going out. The Secure Router can either have a **static IP**, **dynamic IP** or **DNS hostname address**.
7. Select the type of IPSec endpoint the remote party has. The remote endpoint can have a **static IP address**, **dynamic IP address** or a **DNS hostname address**. In this example, select the **static IP address** option.
8. Select the type of authentication for the tunnel to use. The Secure Router supports the following types of authentication:
 - **Preshared Secret** is a common secret (passphrase) that is shared between the Secure Router and the remote party.

This authentication method is widely supported, relatively simple to configure, and relatively secure, although it is somewhat less secure when used with aggressive mode keying.
 - **RSA Digital Signatures** uses a public/private RSA key pair for authentication. The Secure Router can generate these key pairs. The public keys need to be exchanged between the Secure Router and the remote party in order to configure the tunnel.

This authentication method is not widely support, but is relatively secure and allows dynamic endpoints to be used with main mode keying.
 - **x.509 Certificates** are used to authenticate the remote party against a Certificate Authority's (CA) certificate. The CA certificate must have signed the local certificates that are used for tunnel authentication. Certificates need to be uploaded to the Secure Router before a tunnel can be configured to use them (see *Certificate Management*).

This authentication method is widely supported and very secure, however differering terminology between vendors can make it difficult to set up a tunnel between a Secure Router and an appliance from another vendor. This authentication method allows dynamic endpoints to be used with main mode keying.
 - **Manual Keys** establishes the tunnel using predetermined encryption and authentication keys.

This authentication method is no longer widely used. It is not very secure as changing keys requires user intervention, and consequently keys are not changed very often. Using manual keys is not recommended.
9. In this example, select the **Preshared Secret** option.
10. Click the **Next** button to configure the **Local Endpoint Settings**.

Local endpoint settings

The screenshot shows the 'IPsec VPN Setup' dialog box with the 'Local Endpoint Settings' tab selected. The settings are as follows:

Setting	Value
Tunnel name	Headquarters
Initiate Tunnel Negotiation	<input checked="" type="checkbox"/>
Optional Endpoint ID	branch@office
IP Payload Compression	<input type="checkbox"/>
Dead Peer Detection	<input checked="" type="checkbox"/>
Delay (sec)	9
Timeout (sec)	30
Initiate Phase 1 & 2 rekeying	<input checked="" type="checkbox"/>

Buttons: Back, Next, Cancel

1. Leave the **Initiate the tunnel from this end** checkbox checked.

Note

This option is not be available when the Secure Router has a static IP address and the remote party has a dynamic IP address.

2. Enter the **Required Endpoint ID** of the Secure Router. This ID is used to authenticate the Secure Router to the remote party. It is required because the Secure Router in this example has a dynamic IP address. This field is also required if RSA Digital Signatures are used for authentication.

It becomes optional if the Secure Router has a static IP address and is using Preshared Secrets for authentication. If it is optional and the field is left blank, the **Endpoint ID** defaults to the static IP address.

Note

*If the remote party is a Secure Router, the ID must have the form abcd@efgh. If the remote party is not a Secure Router, refer the interoperability documents on the Secure Router Knowledge Base to determine what form it must take. In this example, enter: **branch@office***

3. Leave the **Enable IP Payload Compression** checkbox unchecked. If compression is selected, *IPComp* compression is applied before encryption.
4. Check the **Enable Dead Peer Detection** checkbox. This allows the tunnel to be restarted if the remote party stops responding. This option is only used if the remote party supports Dead Peer Detection. It operates by sending notifications and waiting for acknowledgements.

5. Enter the **Delay** and **Timeout** values for Dead Peer Detection. The default times for the delay and timeout options are 9 and 30 seconds respectively. This means that a Dead Peer Detection notification is sent every 9 seconds (**Delay**) and if no response is received in 30 seconds (**Timeout**) then the Secure Router attempts to restart the tunnel. In this example, leave the delay and timeout as their default values.
6. Leave the **Enable Phase 1 & 2 rekeying to be initiated from my end** checkbox checked. This enables automatic renegotiation of the tunnel when the keys are about to expire.
7. Click the **Next** button to configure the **Remote Endpoint Settings**.

Other options

The following options become available on this page depending on what has been configured previously:

- **Route to remote endpoint** is the next gateway IP address or *nexthop* along the previously selected IPSec interface. This field becomes available if an interface other than the default gateway was selected for the tunnel to go out on.
- **SPI Number** is the *Security Parameters Index*. It is a hexadecimal value and must be unique. It is used to establish and uniquely identify the tunnel. The SPI is used to determine which key is used to encrypt and decrypt the packets. It must be of the form *0xhex*, where *hex* is one or more hexadecimal digits and be in the range of *0x100-0xfff*. This field appears when **Manual Keying** has been selected.
- **Authentication Key** is the *ESP Authentication Key*. It must be of the form *0xhex*, where *hex* is one or more hexadecimal digits. The *hex* part must be exactly 32 characters long when using MD5 or 40 characters long when using SHA1 (excluding any underscore characters). This field appears when **Manual Keying** has been selected.
- **Encryption Key** is the *ESP Encryption Key*. It must be of the form *0xhex*, where *hex* is one or more hexadecimal digits. The *hex* part must be exactly 16 characters long when using DES or 48 characters long when using 3DES (excluding any underscore characters). This field appears when **Manual Keying** has been selected.
- **Cipher and Hash** pull down menu contains the ESP encryption/authentication algorithms that can be used for the tunnel. The option selected must correspond to the encryption and authentication keys used. This pull down menu appears when **Manual Keying** has been selected. The options include the following:
 - **3des-md5-96** uses the encryption transform following the Triple-DES standard in Cipher-Block-Chaining mode with authentication provided by HMAC and MD5 (96-bit authenticator). It uses a 192-bit 3DES encryption key and a 128-bit HMAC-MD5 authentication key.

- **3des-sha1-96** uses the encryption transform following the Triple-DES standard in Cipher-Block-Chaining mode with authentication provided by HMAC and SHA1 (96-bit authenticator). It uses a 192-bit 3DES encryption key and a 160-bit HMAC-SHA1 authentication key.
- **des-md5-96** uses the encryption transform following the DES standard in Cipher-Block-Chaining mode with authentication provided by HMAC and MD5 (96-bit authenticator). It uses a 56-bit 3DES encryption key and a 128-bit HMAC-MD5 authentication key.
- **des-sha1-96** uses the encryption transform following the DES standard in Cipher-Block-Chaining mode with authentication provided by HMAC and SHA1 (96-bit authenticator). It uses a 56-bit DES encryption key and a 160-bit HMAC-SHA1 authentication key.
- **Local Network** is the network behind the local Secure Router. This field appears when **Manual Keying** has been selected.

The screenshot shows the 'IPsec VPN Setup' dialog box with the 'Certificate Lists' tab selected. Under the 'Remote Endpoint Settings' section, the following fields are visible:

Tunnel name	Headquarters
The remote party's IP address	209.0.0.1
Optional Endpoint ID	

At the bottom of the dialog, there are three buttons: 'Back', 'Next', and 'Cancel'.

1. Enter the Internet IP address of the remote party in **The remote party's IP address** field. In this example, enter: **209.0.0.1**

The **Endpoint ID** is used to authenticate the remote party to the Secure Router. The remote party's ID is optional if it has a static IP address and uses Preshared Secrets for authentication. It becomes a required field if the remote party has a dynamic IP or DNS hostname address or if RSA Digital Key Signatures are used for authentication. It is optional in this example, because the remote party has a static IP address. If the remote party is a Secure Router, it must have the form *abcd@efgh*. If the remote party is not a Secure Router, refer the interoperability documents on the Secure Router Knowledge Base to determine what form it must take. In this example leave the field blank.

2. Click the **Next** button to configure the **Phase 1 Settings**.

Other options

The following options become available on this page depending on what has been configured previously:

- **The remote party's DNS hostname address** field is the DNS hostname address of the Internet interface of the remote party. This option becomes available if the remote party has been configured to have a DNS hostname address.
- **Distinguished Name** field is the list of attribute/value pairs contained in the certificate. The list of attributes supported are as follows:

C	Country
ST	State or province
L	Locality or town
O	Organization
OU	Organizational Unit
CN	Common Name
N	Name
G	Given name
S	Surname
I	Initials
T	Personal title
E	E-mail
Email	E-mail
SN	Serial number
D	Description
TCGID	[Siemens] Trust Center Global ID

The attribute/value pairs must be of the form *attribute=value* and be separated by commas. For example : C=US, ST=Illinois, L=Chicago, O=Secure Router, OU=Sales, CN=SECURE ROUTER. It must match exactly the **Distinguished Name** of the remote party's local certificate to successfully authenticate the tunnel. This field appears when **x.509 Certificates** has been selected.

- **RSA Key Length** pull down menu allows the length of the Secure Router generated RSA public/private key pair to be specified. The options include 512, 1024, 1536 and 2048 bits. The greater the key pair length, the longer the time required to generate the keys. It may take up to 20 minutes for a 2048 bit RSA key to be generated. This option appears when RSA Digital Key Signatures has been selected.
- **SPI Number** field is the *Security Parameters Index*. However, this applies to the remote party. It is a hexadecimal value and must be unique. It is used to establish and uniquely identify the tunnel. It must be of the form *0xhex*, where *hex* is one or more hexadecimal digits and be in the range of *0x100-0xffff*. This field appears when **Manual Keying** has been selected.
- **Authentication Key** field is the ESP Authentication Key. However, this applies to the remote party. It must be of the form *0xhex*, where *hex* is one or more hexadecimal digits. The *hex* part must be exactly 32 characters long when using MD5 or 40 characters long when using SHA1 (excluding any underscore characters). It must use the same hash as the Secure Router's authentication key. This field appears when **Manual Keying** has been selected.
- **Encryption Key** field is the ESP Encryption Key. However, this applies to the remote party. It must be of the form *0xhex*, where *hex* is one or more hexadecimal digits. The *hex* part must be exactly 16 characters long when using DES or 48 characters long when using 3DES (excluding any underscore characters). It must use the same cipher as the Secure Router's encryption key. This field appears when **Manual Keying** has been selected.
- **Remote Network** is the network behind the remote party. This field appears when **Manual Keying** has been selected.

Phase 1 settings

The screenshot shows the 'IPSec VPN Setup' dialog box with the 'Certificate Lists' tab selected. The 'Phase 1 Settings' section is highlighted in yellow. The settings are as follows:

Field	Value
Tunnel name	Headquarters
Key lifetime (sec)	3600
Rekey margin (sec)	600
Rekey fuzz (%)	100
Preshared Secret	keep confidential
Phase 1 Proposal	3DES-SHA-Diffie Hellman Group 2 (1024bit)

Buttons: Back, Next, Cancel

1. Set the length of time before Phase 1 is renegotiated in the **Key lifetime (s)** field. The length may vary between 60 and 86400 minutes. Shorter values offer higher security at the expense of the computational overhead required to calculate new keys. For most applications 3600 seconds is recommended. In this example, leave the **Key Lifetime** as the default value of 3600 seconds.

A new Phase 1 key can be renegotiated before the current one expires. The time for when this new key is negotiated before the current key expires can be set in the **Rekeymargin (s)** field. In this example, leave the **Rekeymargin** as the default value of 600 seconds.

The **Rekeyfuzz** value refers to the maximum percentage by which the **Rekeymargin** should be randomly increased to randomize rekeying intervals. The **Key lifetimes** for both Phase 1 and Phase 2 are dependent on these values and must be greater than the value of "**Rekeymargin x (100 + Rekeyfuzz) / 100.**" In this example, leave the **Rekeyfuzz** as the default value of 100%.

2. Enter a secret in the **Preshared Secret** field. Keep a record of this secret as it is used to configure the remote party's secret. In this example, enter: **This secret must be kept confidential.**

Warning

The secret must be entered identically at each end of the tunnel. The tunnel fails to connect if the secret is not identical at both ends. The secret is a highly sensitive piece of information. It is essential to keep this information confidential. Communications over the IPsec tunnel may be compromised if this information is divulged.

3. Select a **Phase 1 Proposal**. Any combination of the ciphers, hashes and Diffie Hellman groups that the Secure Router supports can be selected. The supported ciphers are *DES* (56 bits), *3DES* (168 bits) and *AES* (128, 196 and 256 bits). The supported hashes are *MD5* and *SHA* and the supported Diffie Hellman groups are *1* (768 bit), *2* (1024 bit) and *5* (1536 bits). The Secure Router also supports extensions to the Diffie Hellman groups to include 2048, 3072 and 4096 bit Oakley groups. In this example, select the **3DES-SHA-Diffie Hellman Group 2 (1024 bit)** option. Click the **Next** button to configure the **Phase 2 Settings**.

Other options

The following options become available on this page depending on what has been configured previously:

- **Local Public Key** field is the public part of the RSA key generated for RSA Digital Signatures authentication. These fields are automatically populated and do not need to be modified unless a different RSA key is to be used. This key must be entered in the Remote Public Key field of the remote party's tunnel configuration. This field appears when **RSA Digital Signatures** has been selected.
- **Remote Public Key** field is the public part of the remote party's RSA Key generated for RSA Digital Key authentication. This field must be populated with the remote party's public RSA key. This field appears when **RSA Digital Signatures** has been selected.
- **Local Certificate** pull down menu contains a list of the local certificates that have been uploaded for x.509 authentication. Select the required certificate to be used to negotiate the tunnel. This field appears when **x.509 Certificates** has been selected.

Phase 2 settings page

The screenshot shows the 'IPsec VPN Setup' window with the 'Certificate Lists' tab selected. The 'Phase 2 Settings' section is highlighted. The 'Tunnel name' is 'Headquarters'. Under 'Local Network' and 'Remote Network', there are dropdown menus and 'Custom' buttons. The 'Local Network' dropdown is set to 'Network of LAN Port' and the 'Remote Network' dropdown is set to 'Remote Endpoint'. There is an 'Add' button below these. The 'Key lifetime (sec)' is set to '3600'. The 'Phase 2 Proposal' is set to '3DES-SHA-Diffie Hellman Group 2 (1024bit)'. At the bottom are 'Back', 'Finish', and 'Cancel' buttons.

1. Specify the **Local Networks** and **Remote Networks** to link together with the IPsec tunnel. For the **Local Network**, you may use a **Predefined** network, or enter a **Custom** network address. You must **Add** at least one local and one remote network.

Note

Only network traffic that is coming from a **Local Network** and is destined for a **Remote Network** is allowed across the tunnel. IPsec uses its own routing mechanisms, and disregards the main routing table.

For this example, select **Network of LAN** for the **Local Network**, and enter **192.168.1.0/24** for the **Remote Network** and click **Add**.

2. Set the length of time before Phase 2 is renegotiated in the **Key lifetime (s)** field. The length may vary between 1 and 86400 seconds. For most applications 3600 seconds is recommended. In this example, leave the **Key Lifetime** as the default value of 3600 seconds.
3. Select a **Phase 2 Proposal**. Any combination of the ciphers, hashes and Diffie Hellman groups that the Secure Router supports can be selected. The supported ciphers are *DES*, *3DES* and *AES* (128, 196 and 256 bits). The supported hashes are *MD5* and *SHA* and the supported Diffie Hellman group are *1* (768 bit), *2* (1024 bit) and *5* (1536 bits). The Secure Router also supports extensions to the Diffie Hellman groups to include 2048, 3072 and 4096 bit Oakley groups. *Perfect Forward Secrecy* is enabled if a Diffie-Hellman group or an extension is chosen. Phase 2 can also have the option to not select a Diffie Hellman Group, in this case *Perfect Forward Secrecy* is not enabled. *Perfect Forward Secrecy* of keys provides greater security and is the recommended setting. In this example, select the **3DES-SHA-Diffie Hellman Group 2** (1024 bit) option.

4. Click the **Finish** button to save the tunnel configuration.

Configuring the Headquarters

Enable IPSec

1. Click the **IPSec** link on the left side of the web management console.
2. Check the **Enable IPSec** checkbox.
3. Select the type of IPSec endpoint the Secure Router has on its Internet interface. In this example, select **static IP address**. Leave the **IPSec MTU** unchanged.
4. Click the **Apply** button to save the changes.

Configure a tunnel to accept connections from the branch office

To create an IPSec tunnel, click the **IPSec** link on the left side of the web management console; then, click **New**. Many of the settings such as the **Preshared Secret**, **Phase 1 and 2 Proposals** and **Key Lifetimes** are the same as the branch office.

Tunnel settings page

1. Fill in the **Tunnel name** field with an apt description of the tunnel. The name must not contain spaces or start with a number. In this example, enter: *Branch_Office*
2. Leave checked the **Enable this tunnel** checkbox.
3. Select the Internet interface the IPSec tunnel is to go out on. In this example, select **default gateway interface** option.
4. Select the type of keying for the tunnel to use. In this example, select the **Aggressive mode with Automatic Keying (IKE)** option.
5. Select the type of IPSec endpoint this Secure Router has. In this example, select the **static IP address** option.
6. Select the type of IPSec endpoint the remote party has. In this example, select the **dynamic IP address** option.
7. Select the type of authentication for the tunnel to use. In this example, select the **Preshared Secret** option.

8. Click the **Next** button to configure the **Local Endpoint Settings**.

Local endpoint settings page

1. Leave the **Optional Endpoint ID** field blank in this example. It is optional because this Secure Router has a static IP address. If the remote party is a Secure Router and an Endpoint ID is used, it must have the form *abcd@efgh*. If the remote party is not a Secure Router refer the interoperability documents on the Secure Router Knowledge Base to determine what form it must take.
2. Leave the **Enable IP Payload Compression** checkbox unchecked.
3. Leave the **Enable Phase 1 & 2 rekeying to be initiated from my end** checkbox checked.
4. Click the **Next** button to configure the **Remote Endpoint Settings**.

Remote endpoint settings page

1. Enter the **Required Endpoint ID** of the remote party. In this example, enter the **Local Endpoint ID** at the Branch Office which was: **branch@office**
2. Click the **Next** button to configure the **Phase 1 Settings**.

Phase 1 settings page

1. Set the length of time before Phase 1 is renegotiated in the **Key lifetime (s)** field. In this example, leave the **Key Lifetime** as the default value of 3600 minutes.
2. Set the time for when the new key is negotiated before the current key expires in the **Rekeymargin** field. In this example, leave the **Rekeymargin** as the default value of 600 seconds.
3. Set the maximum percentage by which the **Rekeymargin** should be randomly increased to randomize rekeying intervals in the **Rekeyfuzz** field. The **Key lifetimes** for both Phase 1 and Phase 2 are dependent on these values and must be greater than the value of “**Rekeymargin x (100 + Rekeyfuzz) / 100**.” In this example, leave the **Rekeyfuzz** as the default value of 100%.
4. Enter a secret in the **Preshared Secret** field. This must remain confidential. In this example, enter the Preshared Secret used at the branch office Secure Router, which was: **This secret must be kept confidential**
5. Select a **Phase 1 Proposal**. In this example, select the **3DES-SHA-Diffie Hellman Group 2 (1024 bit)** option (same as the Branch Office **Phase 1 Proposal**).

6. Click the **Next** button to configure the **Phase 2 Settings**.

Phase 2 settings page

1. Select **Network of LAN (Switch A)** for the **Local Network**, enter **192.168.2.0/24** for the **Remote Network** and click **Add**.
2. Set the length of time before Phase 2 is renegotiated in the **Key lifetime (s)** field. In this example, leave the **Key Lifetime** as the default value of 600 seconds.
3. Select a **Phase 2 Proposal**. In this example, select the **3DES-SHA-Diffie Hellman Group 2 (1024 bit)** option (same as the Branch Office **Phase 2 Proposal**).
4. Click the **Apply** button to save the tunnel configuration.

Tunnel List



The screenshot displays the 'IPsec VPN Setup' interface. At the top, there are tabs for 'IPsec' and 'Certificate Lists'. Below these, the 'IPsec General Settings' section includes a checked 'Enable IPsec' checkbox and an empty 'IPsec MTU' input field, with a 'Submit' button below. The 'Tunnel List' section features a table with columns for 'Connection', 'Remote Party', and 'Status'. A single entry is shown: 'Headquarters' with '209.0.0.1' as the remote party and 'Running' as the status. Below the table are 'Refresh' and 'New' buttons.

Connection	Remote Party	Status
✓ Headquarters	209.0.0.1	Running  

Connection

Once a tunnel has been configured, an entry with the tunnel name in the **Connection** field is shown.

Note

You may modify, delete or disable/enable a tunnel by clicking on the corresponding **Edit**, **Delete** or **Enable/Disable** icon.

Remote party

The **Remote Party** which the tunnel is configured to connect to is defined either by its Endpoint ID, IP Address or Distinguished Name.

Click **Remote Party** to sort the tunnel list by the remote party ID/name/address.

Status

Tunnels that use *Automatic Keying (IKE)* display one of four states in the **Status** field. The states include the following:

- **Down** indicates that the tunnel is not being negotiated. This may be due to the following reasons:
 - IPsec is disabled.
 - The tunnel is disabled.
 - The tunnel could not be loaded due to misconfiguration.
- **Negotiating Phase 1** indicates that IPsec is negotiating Phase 1 to establish the tunnel. Aggressive or Main mode packets (depending on tunnel configuration) are transmitted during this stage of the negotiation process.
- **Negotiating Phase 2** indicates that IPsec is negotiating Phase 2 to establish the tunnel. Quick mode packets are transmitted during this stage of the negotiation process.
- **Running** indicates that the tunnel has been established.

Tunnels that use *Manual Keying* are in either a **Down** or **Running** state.

For tunnels that use *Automatic Keying*, further negotiation details can be seen by clicking on the status. A window similar to the following is displayed.

```

Interfaces Loaded
000 interface ipsec0/eth1 209.0.0.2
000 interface ipsec0/eth1 209.0.0.2

Phase 2 Ciphers Loaded
000 algorithm ESP encrypt: id=2, name=ESP_DES, ivlen=64, keysize=64, keysize=168
000 algorithm ESP encrypt: id=3, name=ESP_3DES, ivlen=64, keysize=168, keysize=168
000 algorithm ESP encrypt: id=12, name=ESP_AES, ivlen=128, keysize=128, keysize=256

Phase 2 Hashes Loaded
000 algorithm ESP auth attr: id=1, name=AUTH_ALGORITHM_HMAC_MD5, keysize=128, keysize=128
000 algorithm ESP auth attr: id=2, name=AUTH_ALGORITHM_HMAC_SHA1, keysize=160, keysize=160

Phase 1 Ciphers Loaded
000 algorithm IKE encrypt: id=7, name=OAKLEY_AES_CBC, blocksize=16, keydeflen=128
000 algorithm IKE encrypt: id=5, name=OAKLEY_3DES_CBC, blocksize=8, keydeflen=192
000 algorithm IKE encrypt: id=1, name=OAKLEY_DES_CBC, blocksize=8, keydeflen=64

```

Interfaces Loaded lists the Secure Router's interfaces which IPsec is using.

Phase 2 Ciphers Loaded lists the encryption ciphers that tunnels can be configured with for Phase 2 negotiations. This includes DES, 3DES and AES.

Phase 2 Hashes Loaded lists the authentication hashes that tunnels can be configured with for Phase 2 negotiations. This includes MD5 and SHA1 (otherwise known as SHA).

Phase 1 Ciphers Loaded lists the encryption ciphers that tunnels can be configured with for Phase 1 negotiations. This includes DES, 3DES and AES.

Phase 1 Hashes Loaded lists the authentication hashes that tunnels can be configured with for Phase 1 negotiations. This includes MD5 and SHA.

Diffie Hellman Groups Loaded lists the Diffie Hellman groups and Oakley group extensions that can be configured for both Phase 1 and Phase 2 negotiations.

Connection Details lists an overview of the tunnel's configuration. It contains the following information:

- An outline of the tunnel's network setup. In this example, it is `192.168.2.0/24===209.0.0.2(branch@office)...209.0.0.1===192.168.1.0/24`
- Phase 1 and Phase 2 key lifetimes (**ike_life** and **ipsec_life** respectively). In this example, they are both `3600s`.
- Type of automatic (IKE) keying. In this example, the **policy** line displays `AGGRESSIVE`. For Main mode, it displays `MAIN`.
- Type of authentication used. In this example, the **policy** line displays `PSK` (Preshared Key). For RSA Digital Signatures or x.509 certificates, it displays `RSA`.
- Whether Perfect Forward Secrecy is used. In this example, the **policy** line has the `PFS` keyword. If PFS is disabled, the keyword does not appear.

- Whether IP Payload Compression is used. In this example, the **policy** line does not have the *COMPRESS* keyword since it has not been enabled.
- The interface on which the tunnel is going out. In this example, the **interface** line has *eth1*, which is the Internet interface.
- The current Phase 1 key. This is the number that corresponds to the **newest ISAKMP SA** field. In this example, phase 1 has not been successfully negotiated, so there is no key yet.
- The current Phase 2 key. This is the number that corresponds to the **newest IPsec SA** field. In this example, phase 1 has not been successfully negotiated, so there is no key yet.
- The Phase 1 proposal wanted. The line **IKE algorithms wanted** reads *5_000-2-2*. The *5_000* refers to cipher 3DES (where 3DES has an id of 5, see Phase 1 Ciphers Loaded), the first *2* refer to hash SHA (where SHA has an id of 2, see Phase 1 Hashes Loaded) and the second *2* refer to the Diffie Hellman Group 2 (where Diffie Hellman Group 2 has an id of 2).
- The Phase 2 proposal wanted. The line **ESP algorithms wanted** reads *3_000-2; pfsgroup=2*. The *3_000* refers to cipher 3DES (where 3DES has an id of 3, see Phase 2 Ciphers Loaded), the *2* refers to hash SHA1 or SHA (where SHA1 has an id of 2, see Phase 2 Hashes Loaded) and *pfsgroup=2* refers to the Diffie Hellman Group 2 for Perfect Forward Secrecy (where Diffie Hellman Group 2 has an id of 2).

Negotiation State reports what stage of the negotiation process the tunnel is in. In this example it has *initiated* and sent the first aggressive mode packet (*AII*) and is expecting its *response* (*ARI*) in the line *STATE_AGGR_II (sent AII, expecting ARI)*. Once the Phase 1 has been successfully negotiated, the status displays *ISAKMP SA established*. Once the Phase 2 has been successfully negotiated, the status displays *IPsec SA established*. The tunnel is then established and running.

NAT Traversal Support

NAT Traversal allows tunnels to be established when the IPsec endpoints reside behind NAT devices. If any NAT devices are detected, the NAT Traversal feature is automatically used. It cannot be configured manually on the Secure Router.

Certificate Management

The x.509 certificates can be used to authenticate IPsec endpoints during tunnel negotiation for Automatic Keying. The other methods are *Preshared Secrets* and *RSA Digital Signatures*.

Certificates need to be uploaded to the Secure Router before they can be used in a tunnel. Certificates have time durations in which they are valid. Ensure that the certificates uploaded are valid and that the **Date and Time** settings have been set correctly on the Secure Router.

The Secure Router only supports certificates in *base64 PEM* or *binary DER* format.

Some certificate authorities (CA) distribute certificates in a *PKCS12* format file. This format combines the CA certificate, local public certificate and local private key certificate into one file. These certificates must be extracted before uploading them to the Secure Router; see *Extracting certificates* further on.

If you do not have access to certificates issued by a certificate authority (CA), you may create self-signed certificates; see *Creating certificates* further on.

The OpenSSL application

The remainder of this section requires OpenSSL application, run from a Windows command prompt (**Start** -> **Run** -> type **cmd**) or Linux shell prompt.

A Windows version of OpenSSL is provided in the *openssl* directory of the Secure Router CD. Ensure that this directory is in your execution path, or copy all files from this directory into a working directory on your hard drive.

Extracting certificates

1. To extract the CA certificate, run:

```
openssl pkcs12 -nomacver -cacerts -nokeys -in pkcs12_file -out  
ca_certificate.pem
```

where: **pkcs12_file** is the PKCS12 file issued by the CA and **ca_certificate.pem** is the CA certificate to be uploaded into the Secure Router.

2. When the application prompts you to **Enter Import Password**, enter the password used to create the certificate. If none was used simply press enter.
3. To extract the local public key certificate type, enter the following at the Windows command prompt:

```
openssl pkcs12 -nomacver -clcerts -nokeys -in pkcs12_file -out  
local_certificate.pem
```

where: **pkcs12_file** is the PKCS12 file issued by the CA and **local_certificate.pem** is the local public key certificate to be uploaded into the Secure Router.

4. When the application prompts you to **Enter Import Password**, enter the password used to create the certificate. If none was used simply press enter.

5. To extract the local private key certificate type, enter the following at the Windows command prompt:

```
openssl pkcs12 -nomacver -nocerts -in pkcs12_file -out
local_private_key.pem
```

where: **pkcs12_file** is the PKCS12 file issued by the CA and **local_private_key.pem** is the local private key certificate to be uploaded into the Secure Router.

6. When the application prompts you to **Enter Import Password**, enter the password used to create the certificate. If none was used simply press enter. When the application prompts you to **Enter PEM pass phrase**, choose a secure pass phrase that is greater than 4 characters long. This is the pass phrase used to secure the private key file, and is the same pass phrase you enter when uploading the private key certificate into the Secure Router. Verify the pass phrase by typing it in again.

The Secure Router also supports *Certificate Revocation List* (CRL) files. A CRL is a list of certificates that have been revoked by the CA before they have expired. This may be necessary if the private key certificate has been compromised or if the holder of the certificate is to be denied the ability to establish a tunnel to the Secure Router.

Creating certificates

There are two steps to create self-signed certificates. First, create a single CA certificate, second, create one or more local certificate pairs and sign them with the CA certificate.

Create a CA certificate

1. Create the CA directory:

```
mkdir rootCA
```

2. Create the serial number for the first certificate:

```
echo 01 > rootCA/serial
```

3. Create an empty CA database file under Windows:

```
type nul > rootCA/index.txt
```

or under Linux:

```
touch rootCA/index.txt
```

4. Create the CA certificate, omit the `-nodes` option if you want to use a password to secure the CA key:

```
openssl req -config openssl.cnf -new -x509 -keyout
rootCA/ca.key -out rootCA/ca.pem -days DAYS_VALID -nodes
```

where: `DAYS_VALID` is the number of days the root CA is valid for.

Create local certificate pairs

For each local certificate you wish to create, there are two steps.

1. Create the certificate request:

```
openssl req -config openssl.cnf -new -keyout cert1.key -out
cert1.req
```

2. Enter a PEM pass phrase (this is the same pass phrase required when you upload the key to the Secure Router) and then the certificate details. All but the **Common Name** are optional and may be omitted.

3. Sign the certificate request with the CA:

```
openssl ca -config openssl.cnf -out cert1.pem -notext -infile
cert1.req
```

You now have a local certificate pair, the local public certificate `cert1.pem` and the local private key certificate `cert1.key`, ready to use in the Secure Router.

4. For each certificate required, change the `cert1.*` filenames appropriately.

Using certificates with Windows IPsec

1. To create certificates to use with IPsec on a Windows system, first follow the previous instructions in *Creating a CA certificate* and *Creating local certificate pairs*.

Windows IPsec requires the certificates to be in a PKCS12 format file. This format combines the CA certificate, local public certificate and local private key certificate into one file.

```
openssl pkcs12 -export -inkey cert1.key -in cert1.pem -certfile
rootCA/ca.pem -out cert1.p12 -name "Certificate 1"
```

2. To install the new PCKS12 file, `cert1.p12`, on Windows XP, open up the *Microsoft Management Console* (**Start** -> **Run** -> then type `mmc`).

3. Add the *Certificate Snap-in* (**File** -> **Add/Remove Snap-in** -> **Add** -> select **Certificates** -> **Add** -> select the account level you want the certificates installed for (i.e. current user vs. all users) (-> **Local Computer**) -> **Close** -> **OK**.
4. Double click **Certificates** to open the store.
5. Select the **Personal** store.
6. Import new certificate (**Action** -> **All Tasks** -> **Import**).
7. Locate *cert1.p12*.
8. Type in the **Export Password** if you used one.
9. Select **Automatically select the certificate store based on the type of certificate**.

Add certificates

1. To add certificates to the Secure Router, select **IPSec** from the **VPN** section of the main menu and then click the **Certificate Lists** tab at the top of the window. Any previously uploaded certificates are displayed, and may be removed by clicking the corresponding **Delete** icon.



2. Select the certificate type click **New**. You may add a **CA Certificate** (Certificate Authority), **CRL Certificate** (Certificate Revocation List) or **Local Certificate**.
3. Click **Browse** to locate the certificate file or files.
4. If you are adding a **Local Certificate**, enter the *Public Key certificate* in **Local Certificate** the *Local Private Key certificate* in **Private Key Certificate**, and the passphrase to unlock the private key certificate in **Private Key Certificate Passphrase**. The certificate must be in *PEM* or *DER* format.
5. Certificates have time durations in which they are valid. Ensure that the certificates uploaded are valid and that the **Date and Time** settings have been set correctly on the Secure Router.

IPSec Troubleshooting

- **Symptom:** IPSec is not running and is enabled.
Possible Cause: The Secure Router has not been assigned a default gateway.
Solution: Ensure the Secure Router has a default gateway by configuring the Internet connection on the Connect to Internet page or assigning a default gateway on the IP Configuration page.
- **Symptom:** Tunnel is always down even though IPSec is running and the tunnel is enabled.
Possible Cause: The tunnel is using Manual Keying and the encryption and/or authentication keys are incorrect.
The tunnel is using Manual Keying and the Secure Router's and/or remote party's keys do not correspond to the Cipher and Hash specified.
Solution: Configure a correct set of encryption and/or authentication keys. Select the appropriate Cipher and Hash that the key have been generated from, or change the keys used to use the selected Cipher and Hash.
- **Symptom:** Tunnel is always Negotiating Phase 1.
Possible Cause: The remote party does not have an Internet IP address (a *No route to host* message is reported in the system log).
The remote party has IPSec disabled (a *Connection refused* message is reported in the system log).
The remote party does not have a tunnel configured correctly because:
 - The tunnel has not been configured.
 - The Phase 1 proposals do not match.
 - The secrets do not match.
 - The RSA key signatures have been incorrectly configured.
 - The Distinguished Name of the remote party has not be configured correctly.
 - The Endpoint IDs do not match.
 - The remote IP address or DNS hostname has been incorrectly entered.
 - The certificates do not authenticate correctly against the CA certificate.**Solution:** Ensure that the tunnel settings for the Secure Router and the remote party are configured correctly. Also ensure that both have IPSec enabled and have Internet IP addresses. Check that the CA has signed the certificates.
- **Symptom:** Tunnel is always Negotiating Phase 2
Possible Cause: The Phase 2 proposals set for the Secure Router and the remote party do not match.
The local and remote subnets do not match.
Solution: Ensure that the tunnel settings for the Secure Router and the remote party are configured correctly.

- **Symptom:** The tunnel appears to be up and I can ping across it, but HTTP, FTP, SSH, telnet, etc. don't work
Possible Cause: The MTU of the IPSec interface is too large.
Solution: Reduce the MTU of the IPSec interface.

- **Symptom:** Tunnel goes down after a while
Possible Cause: The remote party has gone down.
 - The remote party has disabled IPSec.
 - The remote party has disabled the tunnel.
 - The tunnel on the Secure Router has been configured not to rekey the tunnel.
 - The remote party is not rekeying correctly with the Secure Router.**Solution:** Confirm that the remote party has IPSec and the tunnel enabled and has an Internet IP address. Ensure that the Secure Router has rekeying enabled. If the tunnel still goes down after a period of time, it may be due to the Secure Router and remote party not recognising the need to renegotiate the tunnel. This situation arises when the remote party is configured to accept incoming tunnel connections (as opposed to initiate tunnel connections) and reboots. The tunnel has no ability to let the other party know that a tunnel renegotiation is required. This is an inherent drawback to the IPSec protocol. Different vendors have implemented their own proprietary method to support the ability to detect whether to renegotiate the tunnel. Dead peer detection has been implemented based on the draft produced by Cisco Systems (*draft-ietf-ipsec-dpd-00.txt*). Unfortunately, unless the remote party implements this draft, the only method to renegotiate the tunnel is to reduce the key lifetimes for Phase 1 and Phase 2 for Automatic Keying (IKE). This does not occur for Manual Keying.

- **Symptom:** Dead Peer Detection does not seem to be working
Possible Cause: The tunnel has Dead Peer Detection disabled.
The remote party does not support Dead Peer Detection according to *draft-ietf-ipsec-dpd-00.txt*
Solution: Enable Dead Peer Detection support for the tunnel. Do not use Dead Peer Detection if the remote party does not support *draft-ietf-ipsec-dpd-00.txt*.

- **Symptom:** Tunnels using x.509 certificate authentication do not work
Possible Cause: The date and time settings on the Secure Router has not been configured correctly.
 - The certificates have expired.
 - The Distinguished Name of the remote party has not be configured correctly on the Secure Router's tunnel.
 - The certificates do not authenticate correctly against the CA certificate.

- The remote party's settings are incorrect.

Solution: Confirm that the certificates are valid. Confirm also that the remote party's tunnel settings are correct. Check the Distinguished Name entry in the the Secure Router's tunnel configuration is correct.

- **Symptom:** Remote hosts can be accessed using IP address but not by name

Possible cause: Windows network browsing broadcasts are not being transmitted through the tunnel.

Solution: Set up a WINS server and use it to have the remote hosts resolve names to IP addresses.

Set up LMHOSTS files on remote hosts to resolve names to IP addresses.

- **Symptom:** Tunnel comes up but the application does not work across the tunnel.

Possible cause: There may be a firewall device blocking IPSec packets.

- The MTU of the IPSec interface may be too large.
- The application uses broadcasts packets to work.

Solution: Confirm that the problem is the VPN tunnel and not the application being run. These are the steps you can try to find where the problem is (it is assumed that a network to network VPN is being used):

- Ping from your PC to the Internet IP address of the remote party (it assumed that the remote party is configured to accept incoming pings)
- Ping from your PC to the LAN IP address of the remote party.
- Ping from your PC to a PC on the LAN behind the remote party that the tunnel has been configured to combine.

If you cannot ping the Internet IP address of the remote party, either the remote party is not online or your computer does not have its default gateway as the Secure Router. If you can ping the Internet IP address of the remote party but not the LAN IP address, then the remote party's LAN IP address or its default gateway has not been configured properly. Also check your network configuration for any devices filtering IPSec packets (protocol 50) and whether your Internet Service Provider is filtering IPSec packets. If you can ping the LAN IP address of the remote party but not a host on the remote network, then either the local and/or remote subnets of the tunnel settings have been misconfigured or the remote host does not have its default gateway as the remote party.

If you can ping across the tunnel, then check if the MTU of the IPSec interface is allowing packets to go through. Reduce the MTU if large packets are not being sent through the tunnel.

If the application is still not working across the tunnel, then the problem is with the application. Check that the application uses IP and does not use broadcast packets since these are not sent across the IPSec tunnels. You should contact the producer of the application for support.

Port Tunnels

Port tunnels are point to point tunnels similar to regular VPNs, but only offer transport for a TCP service from one end of the tunnel to the other. This allows you to “wrap” a TCP service, such as telnet or mail retrieval (POP3), in an HTTP or SSL connection. Note that a single port tunnel may transport a single TCP port only.

The Secure Router supports two kinds of port tunnels.

HTTP Tunnels are port tunnels that send data using the HTTP protocol, and are not encrypted. HTTP tunnels are *not* encrypted. They can be useful when the Secure Router is behind a firewall that only allows outgoing HTTP connections and blocks all other traffic.

SSL Tunnels are port tunnels that send data using an encrypted SSL pipe. In order to use an SSL tunnel, you must first install an SSL certificate using the **Upload SSL Certificates** page or the **Create SSL Certificates** page; see the *Upload SSL certificates* and *Create SSL certificates* sections of the chapter entitled *Firewall*. SSL tunnels can be useful for encrypting TCP services that are by themselves unencrypted, such as a telnet or FTP session.

The end of the port tunnel that is offering the TCP service (such as a telnet or FTP server) must be configured as a **Tunnel Server**. The end of the port tunnel that is accessing the TCP service must be configured as a **Tunnel Client**.

Tunnel server

A tunnel server accepts connections on **Tunnel Port** from a host on the Internet, and forwards them over the **Data Port** to the **Data Server**.

1. Click **Port Tunnels** from the **VPN** section of the main menu. Select either **HTTP Tunnel Server** or **SSL Tunnel Server** and click **Add**.
2. Enter a descriptive **Name** for this tunnel server. Check **Enable**.
3. In **Data Server**, enter the IP address of the local server that is offering the TCP service, such as a local mail or FTP server. In **Data Port**, enter the port on which the TCP service is running. Incoming requests from hosts on the remote end of the tunnel are forwarded to this IP address and port.
4. In **Tunnel Port**, Enter the TCP port on which to listen for connections from the client. This must match the tunnel client's **Tunnel Port**.

The following fields are displayed for **HTTP Tunnel Server** only:

If necessary, you may specify the **Content Length** to use in HTTP PUT requests. You may also set **Strict Content Length** to force this **Content Length** for all requests.

You may specify a **Maximum Age** for connections, after which the connection is closed, and a **Keep Alive** interval, the interval at which to send keep alive bytes to keep the connection open.

The following field is displayed for **SSL Tunnel Server** only:

You may specify the **Protocol** to use when negotiating the SSL connection. Leave this set to **Raw** when incoming connections are from a tunnel client. Setting **Protocol** to another value allows the tunnel server to accept connections directly from an SSL client other than a tunnel client, e.g. a mail client configured to use **POP3** over SSL.

Tunnel client

A tunnel client accepts connections on **Data Port** from a host on the local network, and forwards them over the **Tunnel Port** to the **Tunnel Server**.

1. Click **Port Tunnels** from the **VPN** section of the main menu. Select either **HTTP Tunnel Client** or **SSL Tunnel Client** and click **Add**.
2. Enter a descriptive **Name** for this tunnel client. Check **Enable**.
3. In **Data Port**, enter the TCP port on which to listen for connections from local hosts to forward across the tunnel. It is not necessary for this to match the tunnel server's **Data Port**, but it often will.
4. Enter the publically accessible IP address of the remote **Tunnel Server**, and in **Tunnel Port**, enter the TCP port on which the tunnel server is listening for connections. This must match the tunnel server's **Tunnel Port**.
5. The following fields are displayed for **HTTP Tunnel Client** only:

If necessary, you may specify the **Content Length** to use in HTTP PUT requests. You may also set **Strict Content Length** to force this **Content Length** for all requests.

You may specify a **Maximum Age** for connections, after which the connection is closed, and a **Keep Alive** interval, the interval at which to send keep alive bytes to keep the connection open.

You may disregard the remaining fields if you are not connecting to the HTTP tunnel server via an **HTTP Proxy Server**.

Otherwise, either the **Proxy Server** IP address and the **Proxy Port**. If the proxy server requires authentication, enter the details in **Proxy Username** and **Proxy Password**.

If the proxy accepts connects from clients with a specific User Agent field only, enter it in **Proxy User Agent**.

If the HTTP proxy is a buffering proxy, then enter the **Proxy Buffer Size**. Otherwise set this field to 0. You may also specify the timeout before sending padding to fill up the buffer size in **Proxy Padding Timeout**.

6. The following field is displayed for **SSL Tunnel Server** only:

You may specify the **Protocol** to use when negotiating the SSL connection. Leave this set to **Raw** connecting to a tunnel server. Setting **Protocol** to another value allows the tunnel client to connect directly to an SSL server other than a tunnel server, e.g. a mail server configured to use **POP3** over SSL.

This page intentionally left blank.

6. System

Date and Time

We recommend setting the Secure Router's clock to the correct date and time, otherwise system log message time stamps do not match the time of the event. If you are using certificates for SSL or IPSec, it is especially important that you set the date and time correctly, as all certificates include an expiry date after which they do not function.

Set date and time

If you have a Javascript enabled web browser, click the top **Set Date and Time** button to synchronize the time on the Secure Router with that of your PC.

You may also set the date and time manually by selecting the **Year, Month, Date, Hour** and **Minute** and clicking the bottom **Set Date and Time** button.

NTP time server

The Secure Router can synchronize its system time with a remote time server using the Network Time Protocol (NTP). Configuring the NTP time server ensures that the Secure Router's clock is accurate soon after the Internet connection is established.

To set the system time using NTP, select the **Set Time** checkbox on the **NTP Server Configuration** page and enter the IP address of the time server in the **Remote NTP Server** field.

Date and Time Configuration

Set Date and Time
NTP Time Server
Locality

NTP Time Server

The Secure Router network time (NTP) server sets the system time so that it is synchronized with a remote time server. This ensures that the Secure Router's clock (in UTC) will be accurate soon after the Internet connection is established. Without a time server running, the unit's clock will be randomly set at startup. If the *set time* checkbox is selected, attempts will be made to synchronize the local clock with the time server specified.

The Secure Router NTP server can also act as a local time server which allows other hosts on the local network to synchronize their clocks with the Secure Router's clock. Select the *local NTP server* checkbox to allow this mode of operation.

Local NTP Server

Set Time

Remote NTP Server

Note

*When synchronizing with an NTP server, the date and time is displayed in UTC. To display local time, you must set the **Locality** appropriately.*

Locality

Select your local **Region** and click **Submit**. The system clock subsequently displays local time. By default, the system clock displays UTC.

Backup/Restore Configuration

In the unlikely event that your Secure Router should lose its configuration, or if it should require a factory reset, configuration stored on a PC, USB storage device, or some other safe place can be restored to minimize downtime.

After configuring your Secure Router it is strongly recommended that you back up your configuration. It is good practice to back up your configuration regularly.

Secure Router configuration is backed up to and restored from a single, password protected file, or a single, unsecured text file.

Select **Backup/Restore** from the **System** section of the main menu, or the black backup/restore icon at the top right hand side of the screen.

Backup/Restore

1. Click the **Backup/Restore** tab.



The screenshot shows a web interface titled "Remote Configuration Backup/Restore". It has three tabs: "Remote Backup/Restore", "Local Backup/Restore", and "Text Save/Restore". The "Remote Backup/Restore" tab is selected. Below the tabs, there is a paragraph of text explaining the backup and restore process. There are two main sections: "Save Configuration" and "Restore Configuration". The "Save Configuration" section has a "Submit" button. The "Restore Configuration" section has a "Restore from file" label, a text input field, a "Browse..." button, and a "Submit" button.

Remote Configuration Backup/Restore

Remote Backup/Restore Local Backup/Restore Text Save/Restore

The Secure Router provides a method to backup and restore the entire configuration in a secure manner to your computer's hard drive or another remote location. All the unit's configuration will be saved to or restored from a single file that contains cryptographic protection and integrity checking.

Save Configuration

Backup the entire configuration of this Secure Router as a file on your computer.

Submit

Restore Configuration

Select the file which you'd like to restore from.

Restore from file **Browse...**

Submit

2. To back up your configuration, click **Submit**.
3. To restore configuration, click **Browse** to locate the `.sgc` configuration file you previously backed up, click **Submit**.

Local Backup/Restore

You can store a copy of your Secure Router database in a Flash file on the Secure Router.

1. Click the **Local Backup/Restore** tab.

Local Configuration Backup/Restore

Remote Backup/Restore | **Local Backup/Restore** | Text Save/Restore

Save Configuration

Store a snapshot of the current configuration on the Secure Router itself.

Description:

Restore or Delete Configuration

Select a configuration to restore or delete.

Date	Time	Description		
20051115	13:50:34	Teltronics-SecureRouter		
20051109	10:02:48	pre upgrade to later firmware		
20051004	01:37:52	Teltronics-dingle		

2. To back up your configuration, click **Submit**.
3. To restore configuration, click **Browse** to locate the file you previously backed up, click **Submit**.

Text Save/Restore

1. Click the **Text Save/Restore** tab.
2. Copy and paste the configuration files to and from a plain text file stored on a PC for backup purposes. Click **Submit** and **Reboot** to apply any changes.

Warning

Passwords are stored unencrypted, and plain text files are prone to undetected corruption. It is therefore preferable to use Backup/Restore for regular backups.

Users

This section details adding administrative users, as well as local users for PPTP, L2TP or dialin access, or access through the access control web proxy (see the *Access Control* section in the chapter entitled *Firewall*).

Administrative users

Administrative user accounts on a Secure Router allow administrative duties to be spread amongst a number of different people according to their level of competence and trust.

Each administrative user has a password that they use to authenticate when connecting to the web management console, or via telnet or ssh. They also have a number of access controls that modify what they can and cannot do via the web management console

There is one special user, *root*, who has the role of the final administrative user, or super user. The access privileges for this user may not be lowered, and this user may not be deleted or disabled. You may disallow telnet or ssh connections using the root account however.

1. Select **Users** under the **System** section in the main menu. Existing users are displayed alongside **Delete**, **Edit**, and **Enable/Disable** icons.
2. Click **New** to add a new user. Enter a **Username** (login name), an optional **Description**, and enter and confirm a **Password**.

3. You may specify the following access controls for each administrative user.

- The **Login** control provides the user with telnet and ssh access to the command-line administration interface of the Secure Router.
- The **Administration** control provides the user with the ability to make changes to the Secure Router's configuration via the web-based administration interface. This should only be provided to trusted users who are permitted to configure and reconfigure the unit.
- The **Diagnostic** control provides the user with the ability to view restricted diagnostic information via the web-based administration interface. This access control may be given to technical support users so they can attempt to diagnose but not fix any problems which occur.
- The **Encrypted save / restore all** control provides the user with the ability to save and restore the configuration of the Secure Router via the **Save/Restore** page (see the *Save/Restore* section earlier in this chapter). This access control may be given to a technician whom you want to be able to restore the unit to a known good configuration but to whom you do not wish to grant full administration rights.

Warning A user with **Encrypted save / restore all** access can conceivably create an encrypted config file with an arbitrary root password that they can restore, thus granting them Administration privileges. Therefore, grant **Encrypted save / restore all** only to users that you trust with **Administration** access.

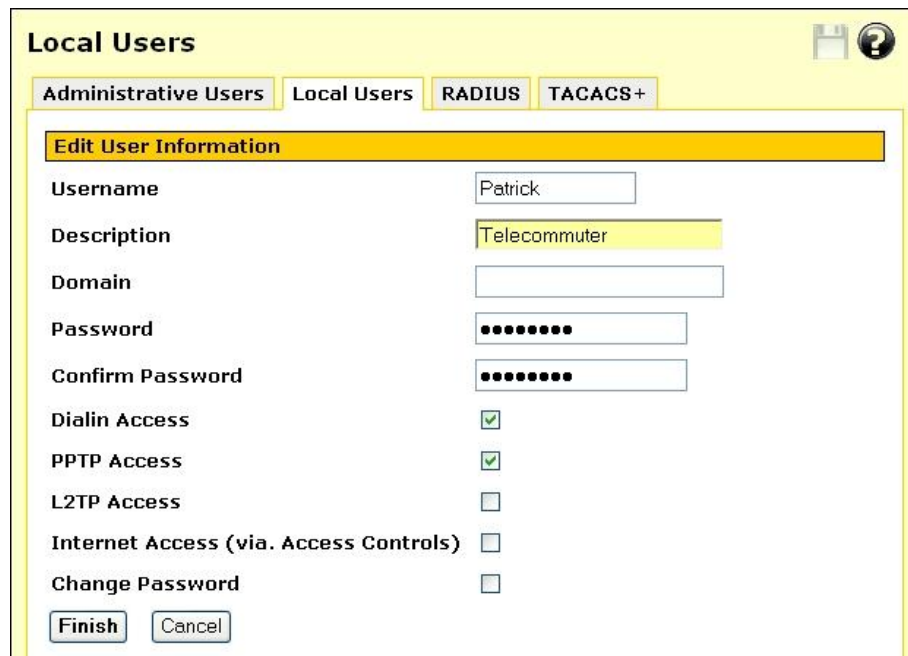
- The **Change Password** control lets users change their password.

4. Click **Finish** to apply your changes.

Local Users

Local users accounts are used to grant PPTP, L2TP or dialin access, and access through the access control web proxy (see the *Access Control* section in the chapter entitled *Firewall*).

1. Select **Users** under the **System** section in the main menu and click the **Local Users** tab. Existing users are displayed alongside **Delete**, **Edit**, and **Enable/Disable** icons.
2. Click **New** to add a new user.



The screenshot shows a web-based configuration interface titled "Local Users". It has four tabs: "Administrative Users", "Local Users", "RADIUS", and "TACACS+". The "Local Users" tab is active. Below the tabs is a section titled "Edit User Information" with the following fields and options:

Username	Patrick
Description	Telecommuter
Domain	
Password	••••••••
Confirm Password	••••••••
Dialin Access	<input checked="" type="checkbox"/>
PPTP Access	<input checked="" type="checkbox"/>
L2TP Access	<input type="checkbox"/>
Internet Access (via. Access Controls)	<input type="checkbox"/>
Change Password	<input type="checkbox"/>

At the bottom of the form are two buttons: "Finish" and "Cancel".

3. Enter a **Username** (login name), an optional **Description**, and enter and confirm a **Password**.
4. For dial-in, PPTP and L2TP users, you may also optionally enter a **Domain** name if your network has a Windows domain server.
5. You may specify the following access controls for each local user.
 - The **Dialin Access** control provides the user with the authority to connect to the Secure Router's dialin server.
 - The **PPTP Access** control provides the user with the authority to connect to the Secure Router's PPTP VPN server (see the *PPTP VPN Server* section of the chapter entitled *VPN*).
 - The **L2TP Access** control provides the user with the authority to connect to the Secure Router's L2TP server (see the *L2TP VPN Server* section of the chapter entitled *VPN*).

- The **Internet Access (via. Access Controls)** control provides the user with the authority to connect to the Internet, subject to the restrictions defined on the **Access Control** page (see the *Access Control* section of the chapter entitled *Firewall*).
 - The **Change Password** control provides the user with the ability to change their password.
6. Click **Finish** to apply your changes.

RADIUS

The Secure Router may be configured to access a central repository of users and passwords on a RADIUS server to authenticate dial-in, PPTP VPN server and L2TP VPN server connections.

1. Enter the **RADIUS Server** address from which to obtain client authentication information.
2. Enter the **RADIUS Server Port**. This is usually port 1812, however some older RADIUS servers use port 1645.
3. Enter and confirm the **RADIUS Secret** used to access the RADIUS server.
4. Click **Submit** to apply your changes.

TACACS+

The Secure Router may be configured to access a central repository of users and passwords on a TACACS+ server to authenticate dial-in, PPTP VPN server and L2TP VPN server connections.

1. Enter the **TACACS+ Server** address from which to obtain client authentication information.
2. Enter and confirm the **TACACS+ Secret** used to access the TACACS+ server.
3. Click **Submit** to apply your changes.

Management

The Secure Router may be management remotely using Secure Router Centralized Management Server (CMS) or Simple Network Management Protocol (SNMP).

CMS

1. To enable remote management by a Secure Router Centralized Management Server, check **Enable Central Management**.

Centralized Management Settings

CMS Management | **SNMP**

Centralized Management Configuration

These settings are used to allow this device to report information to a non-IRISnGEN management server. Several options are available that include periodic ICMP ping, delivery of SNMP traps, and reporting events to a remote SYSLOG server.

Enable Central Management

IP Address of CMS

Authentication Key

Back-to-base ping interval (s)

Local SNMP port

SNMP trap port on CMS

Administrative Contact

Device Location

Syslog Remote Port

Syslog Filter

2. In **IP Address of CMS**, enter the IP address of the host on which Secure Router CMS is running.
3. Specify the shared **Authentication Key** with which to authenticate this device against the CMS. This must be the same as the *snmp_community* configuration setting for CMS. It should be something hard to guess.

When configured for centralized management, the device periodically sends a "ping" (SNMP trap) back to the CMS to indicate that it is alive. **Back-to-base ping interval (s)** specifies the interval in seconds between these pings. This must be less than the *max_alive_interval* configuration setting for CMS.

4. Specify the **Local SNMP Port** on which the management agent listens for requests.

Note

Local SNMP Port should be changed if you have enabled the SNMP agent under Management -> SNMP.

Administrative Contact is the SNMP *sysContact* field. Any value may be specified, but a good choice is contact information for the local administrator.

Device Location is the SNMP *sysLocation* field. Any value may be specified, but a good choice is a short description of the physical location of the device.

5. Enter the **Syslog Remote Port** to which to send syslog messages. This must be the same as the `syslog_port` configuration setting for CMS

Syslog Filter allows setting of a filter for syslog message which are sent to CMS. **Absolutely Everything** sends all messages, including debug messages. This may result in many messages being sent to CMS. **Log Nothing** sends no messages, which can make troubleshooting more difficult. Typically, a setting somewhere between the two is appropriate.

6. Click **Submit** to apply your changes.

SNMP

1. To allow external SNMP management software to query this device for management information, check **Enable SNMP Agent**.
2. Enter the name of a community that is allowed read-only access in **Read-Only Community**. You may optionally include an IP address or network to restrict who is allowed access. You may optionally include an OID to restrict the fields that are accessible.
3. Enter the name of a community that is allowed read-write access in **Read-Write Community**. You may optionally include an IP address or network to restrict who is allowed access. You may optionally include an OID to restrict the fields that are accessible.

Warning

The community name is equivalent to a password, and is sent in plain text in every SNMP packet. Anyone who knows the community name is able to modify settings on this device. It is highly recommended that you do not allow read-write access, or that you take additional steps to secure the connection.

4. In **Local SNMP Port**, specify the endpoints on which the SNMP agent accepts requests. An endpoint consists of an optional transport, an optional address, and a port, separated by : (colon) characters. The default transport is UDP, and the default address is any address. For example: **1161**, **tcp:161**, **10.0.0.1:1161**, or **tcp:10.0.0.1:1161**.

Administrative Contact is the SNMP `sysContact` field. Any value may be specified, but a good choice is contact information for the local administrator.

Device Location is the SNMP `sysLocation` field. Any value may be specified, but a good choice is a short description of the physical location of the device.

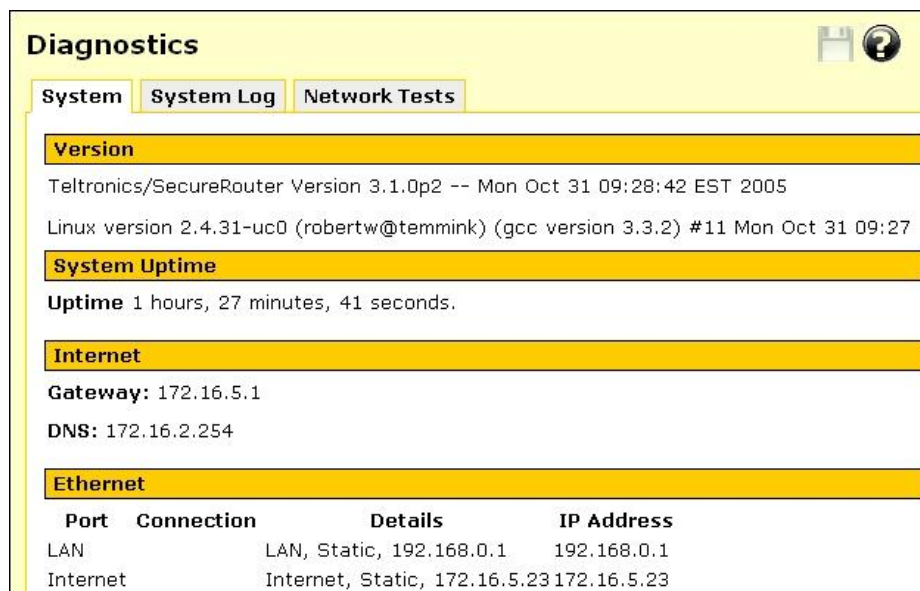
5. Click **Submit** to apply your changes.

Diagnostics

Low-level diagnostic information and network tests are provided to assist you in diagnosing network problems.

Diagnostics

To access this diagnostic information, select **Diagnostics** under the **System** section of the main menu. This page displays information including the current firmware version, network settings and the status of Internet and VPN connections.



Port	Connection	Details	IP Address
LAN		LAN, Static, 192.168.0.1	192.168.0.1
Internet		Internet, Static, 172.16.5.23	172.16.5.23

Network tests

Basic network diagnostic tests (*ping*, *traceroute*) can be accessed by clicking the **Network Tests** tab at the top of the **Diagnostics** page.

Advanced

The following options are intended for network administrators and advanced users *only*.

Warning

Altering the advanced configuration settings may render your Secure Router inoperable.

System log

The system log contains debugging information that may be useful in determining whether all services for your Secure Router are operating correctly.

Log output is color coded by output type. General information and debug output is black, warnings and notices are blue, and errors are red.

The **Display** pull down menu underneath the log output allows you to filter the log output to display, based on output type.

Appendix B contains for details on interpreting log output and configuring advanced log rules.

Local syslog

By default all messages are recorded in the System Log. **Filter Level** allows you to control which classes of messages are recorded in the system log.

Every message recorded in the System Log includes a basic time stamp.

1. Check **Include extended ISO date** to force a more precise and standardized timestamp to be included with every message.
2. Click **Submit** to apply your changes.

Remote syslog

System log messages may be sent to a remote syslog server. This allows you to keep system log messages persistently.

1. Once you have set up a remote syslog server, check **Enable Remote Logging**.

Diagnostics

System System Log Network Tests

View Log Local Syslog Remote Syslog Email Delivery

Remote System Log Delivery

You may redirect the Secure Router's system log to a remote machine by entering the remote machines IP address below.

Enable Remote Logging

Remote Host

Remote Port

Filter Level

Include extended ISO date

Submit

2. Enter the IP address or DNS hostname for the remote syslog server in **Remote Host**.
3. Enter the **Remote Port** on which the remote syslog server is listening for syslog messages. Typically, the default is correct.
4. Set the **Filter Level** to only send syslog messages at this level or above.
5. You may also **Include extended ISO date**, which is prepended to syslog messages before being sent.
6. Click **Submit** to save your changes.

Email delivery

Syslog log messages may be sent to an email account. This allows you to keep system log messages persistently.

1. Check **Enable Email Logging**.

Diagnostics

System System Log Network Tests

View Log Local Syslog Remote Syslog Email Delivery

Email System Log Delivery

You may redirect the Secure Router's system log to an email account by filling in the details below.

Enable Email Logging

Email Server

Email Address(es)

Sender Email

Filter Level

Delay to Send (s)

Messages per Email

2. Enter the address of an **Email Server** (SMTP server) that accepts email for forwarding.
3. Enter the **Email Address(es)** to which to send the system log messages.
4. The **Sender Email** address that System Log messages are sent from.
5. Set the **Filter Level** to only send syslog messages at this level or above.
6. Specify the number of seconds to wait after receiving a system log message before sending the an email in **Delay to Send (s)**. This allows multiple system log messages to accumulate before sending an email containing them all.

Messages per Email is the maximum number of system log messages that are allowed to accumulate before sending the email. The default setting of 0 means unlimited, and is typically appropriate for all systems but those that experience heavy traffic.

7. Click **Submit** to apply your changes.

Reboot and Reset

Rebooting does not erase your Secure Router's configuration, however network connections such as your Internet connection, VPN tunnels, etc. are terminated and re-established when the device is up and running again.

Warning

Before restoring your Secure Router to its default factory settings via the web management console or reset button, it is strongly recommended that you create a back up of your configuration. Refer to the Save/Restore section earlier in this chapter for details.

Reboot device

Click **Reboot Now** to have the Secure Router to perform a soft reboot. It usually takes around 10 seconds before it is up and running again.

If you have enabled bridging, the Secure Router may take up to 30 seconds to reboot. Any shared printers take 30 seconds to become available, during which time print jobs are not accepted.

Erase configuration

To erase your Secure Router's configuration and return to the factory default settings, click **Erase Configuration**. This is useful if you want to reconfigure the device from scratch after an upgrade, or want to redeploy the device into a different environment.

Flash upgrade

Periodically, Secure Router may release new versions of firmware for your Secure Router. If a new version fixes an issue you've been experiencing, or contains a new feature you wish to utilize, contact Secure Router technical support for information on obtaining the latest firmware. You can then load the new firmware with a flash upgrade.

Note

Please read the appendix entitled Firmware Upgrade Practices and Precautions before attempting a firmware upgrade.

There are two primary methods available for performing a flash upgrade, *Netflash* and *Flash upgrade via HTTP*. Remote upgrades may also be performed using TFTP if you have a TFTP server at the remote site, see *Flash upgrade via TFTP*.

During the upgrade, the front panel LEDs on the Secure Router flash in an in-and-out pattern. The Secure Router retains its configuration information with the new firmware.

Warning

If the flash upgrade is interrupted (e.g. power down), the Secure Router stops functioning and becomes unusable until its flash is reprogrammed at the factory or a recovery boot is performed. User care is advised.

For instructions on performing a recovery boot, refer to Appendix D, Recovering From a Failed Upgrade.

Netflash

The first is to download the *netflash.exe* for the appropriate model and version to which you are upgrading. This is a Windows program that automates the upgrade procedure. Be sure to read the release notes before attempting the upgrade.

Flash upgrade via HTTP

The second is to download the binary image file (*.sgu*). Contact Secure Router technical support for instructions on obtaining this file.

1. Select **Advanced** from the **System** section of the main menu and click the **Flash Upgrade** tab. Click **Browse** to locate the *.sgu* file on your local PC and click **Upgrade**.
2. Enter **Extra Parameters** only at the request of Secure Router technical support staff.

Flash upgrade via TFTP

An alternative method is to install and configure a TFTP server. The majority of Linux distributions include a TFTP server, Windows users can download one from:
<http://www.snapgear.com/ftp/tools/tftpd32j.zip>

Note

Although we recommend it, this program is not supported by Secure Router.

Download the binary image file (*.sgu*). Contact Secure Router technical support for instructions on obtaining this file. Place this file in the directory your TFTP is serving files from, usually:
/tftpboot/

Establish a telnet or ssh connection to the Secure Router. Login and run the command:

```
flash image <TFTP server address> <image.sgu>
```

where: *<TFTP server address>* is the address of your TFTP server, and *<image.sgu>* is the binary image filename. Your telnet or ssh connection is terminated once the upgrade commences.

Configuration Files

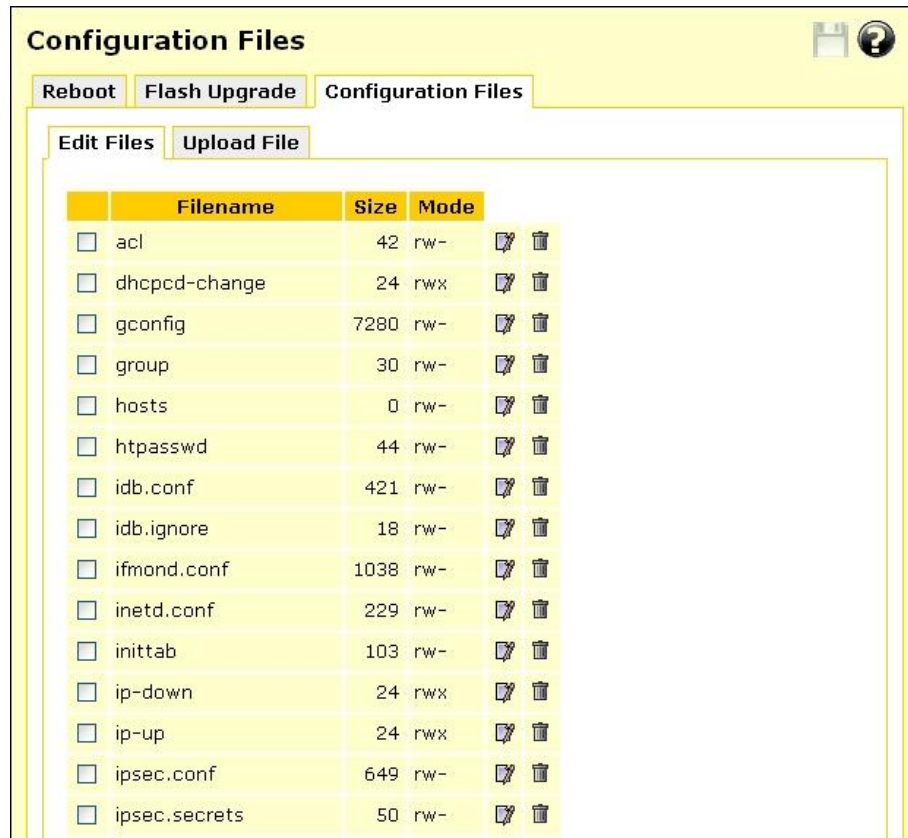
To manually edit, view, or upload new configuration files, select **Advanced** from the **System** section of the main menu and click the **Configuration Files** tab.

Warning

Manually modifying or deleting your Secure Router's configuration files may render the unit inoperable until a factory reset has been performed.

Edit files

1. To modify multiple files at once, check the **Filenames** and click **Modify**. To edit a single file, click its **Edit** icon.



2. You may also create a new file by clicking **New**.

Upload file

Click **Browse** to locate the file on your local PC that you want to upload. You may upload it to an alternative file name on the Secure Router by specifying a **Destination File Name**. Click **Submit** to begin the upload.

Warning

Any existing file with the same name is overwritten.

Support

For information on obtaining support for your Secure Router, select **Support** from the **System** section of the main menu.

This page provides basic troubleshooting tips, contact details for Secure Router technical support, and links to the Secure Router Knowledge Base as shown in the following figure:

Technical Support

Support

Here are some easy options for gaining technical support:

- Please read the NET-PATH Plus Installation and Operations Guide.
- Please read the NET-PATH Plus Secure Router Programmers Guide.
- Please visit the [Technical Support](#) page for steps on how to acquire additional support and information.

Please attach the Secure Router's [Technical Support Report](#) to any support submission.

Technical support report

The **Technical Support Report** page is an invaluable resource for the Secure Router technical support team to analyze problems with your Secure Router. The information on this page gives the support team important information about any problems you may be experiencing.

Note

*If you experience a fault with your Secure Router and have to contact the Secure Router technical support team, **ensure you include the Technical Support Report with your support request.** The Technical Support Report should be generated when the issue is occurring on each of the appliances involved, and attached in plain text format. Otherwise, the Secure Router technical support staff are unlikely to have enough information to assist you.*

This page intentionally left blank.

Appendix A – Terminology

This section explains some of the terms that are commonly used in this document.

Term	Meaning
ADSL	Asymmetric Digital Subscriber Line. A technology allowing high-speed data transfer over existing telephone lines. ADSL supports data rates between 1.5 and 9 Mb/s when receiving data and between 16 and 640 Kb/s when sending data.
Advanced Encryption Standard (AES)	The Advanced Encryption Standard is a new block cipher standard to replace DES, developed by NIST, the US National Institute of Standards and Technology. AES ciphers use a 128-bit block and 128, 192 or 256-bit keys. The larger block size helps resist birthday attacks while the large key size prevents brute force attacks.
Aggressive Mode	This Phase 1 keying mode automatically exchanges encryption and authentication keys and uses less messages in the exchange when compared to Main mode. Aggressive mode is typically used to allow parties that are configured with a dynamic IP address and a preshared secret to connect or if the Secure Router or the remote party is behind a NAT device.
Authentication	Authentication is the technique by which a process verifies that its communication partner is who it is supposed to be and not an imposter. Authentication confirms that data is sent to the intended recipient and assures the recipient that the data originated from the expected sender and has not been altered on route.
Automatic Keying, Internet Key Exchange (IKE)	This type of keying automatically exchanges encryption and authentication keys and replaces them periodically.
Block cipher	A method of encrypting text (to produce ciphertext) in which a cryptographic key and algorithm are applied to a block of data (for example, 64 contiguous bits) at once as a group rather than to one bit at a time. DES, 3DES and AES are all block ciphers.
BOOTP	Bootstrap Protocol. A protocol that allows a network user to automatically receive an IP address and have an operating system boot without user interaction. BOOTP is the basis for the more advanced DHCP.
CA Certificate	A self-signed certification authority (CA) certificate that identifies a CA. It is called a CA certificate because it is the certificate for the root CA.
Certificates	A digitally signed statement that contains information about an entity and the entity's public key, thus binding these two pieces of information together. A certificate is issued by a trusted organization (or entity) called a Certification Authority (CA) after the CA has verified that the entity is who it says it is.
Certificate Authority	A Certificate Authority is a trusted third party, which certifies public key's to truly belong to their claimed owners. It is a key part of any Public Key Infrastructure, since it allows users to trust that a given public key is the one they wish to use, either to send a private message to its owner or to verify the

	signature on a message sent by that owner.
Certificate Revocation List	A list of certificates that have been revoked by the CA before they expired. This may be necessary if the private key certificate has been compromised or if the holder of the certificate is to be denied the ability to establish a tunnel to the Secure Router.
Data Encryption Standard (DES)	The Data Encryption Standard is a block cipher with 64-bit blocks and a 56-bit key.
Dead Peer Detection	The method of detecting if the remote party has a stale set of keys and if the tunnel requires rekeying. To interoperate with the Secure Router, it must conform to the draft draft-ietf-ipsec-dpd-00.txt
DHCP	Dynamic Host Configuration Protocol. A communications protocol that assigns IP addresses to computers when they are connected to the network.
Diffie-Hellman Group or Oakley Group	The groups used as the basis of Diffie-Hellman key exchange in the Oakley protocol, and in IKE.
Diffie-Hellman Key Exchange	A protocol that allows two parties without any initial shared secret to create one in a manner immune to eavesdropping. Once they have done this, they can communicate privately by using that shared secret as a key for a block cipher or as the basis for key exchange.
Distinguished Name	A list of attributes that defines the description of the certificate. These attributes include: country, state, locality, organization, organizational unit and common name.
DNS	Domain Name System that allocates Internet domain names and translates them into IP addresses. A domain name is a meaningful and easy to remember name for an IP address.
DUN	Dial Up Networking.
Encapsulating Security Payload (ESP)	Encapsulated Security Payload is the IPSec protocol which provides encryption and can also provide authentication service.
Encryption	The technique for converting a readable message (plaintext) into apparently random material (ciphertext) which cannot be read if intercepted. The proper decryption key is required to read the message.
Ethernet	A physical layer protocol based upon IEEE standards.
Extranet	A private network that uses the public Internet to securely share business information and operations with suppliers, vendors, partners, customers, or other businesses. Extranets add external parties to a company's intranet.
Failover	A method for detecting that the main Internet connection (usually a broadband connection) has failed and the Secure Router appliance cannot communicate with the Internet. If this occurs, the Secure Router automatically moves to a lower speed, secondary Internet connection.
Fall-forward	A method for shutting down the failover connection when the main Internet connection can be re-established.
Firewall	A network gateway device that protects a private network from users on other networks. A firewall is usually installed to allow users on an intranet access to the public Internet without allowing public Internet users access to the intranet.

Gateway	A machine that provides a route (or pathway) to the outside world.
Hashes	A code, calculated based on the contents of a message. This code should have the property that it is extremely difficult to construct a message so that its Hash comes to a specific value. Hashes are useful because they can be attached to a message, and demonstrate that it has not been modified. If a message were to be modified, then its hash would have changed, and would no longer match the original hash value.
Hub	A network device that allows more than one computer to be connected as a LAN, usually using UTP cabling.
IDB	Intruder Detection and Blocking. A feature of your Secure Router that detects connection attempts from intruders and can also optionally block all further connection attempts from the intruder's machine.
Internet	A worldwide system of computer networks. A public, cooperative, and self-sustaining network of networks accessible to hundreds of millions of people worldwide. The Internet is technically distinguished because it uses the TCP/IP set of protocols.
Intranet	A private TCP/IP network within an enterprise.
IP Compression	A good encryption algorithm produces ciphertext that is evenly distributed. This makes it difficult to compress. If one wishes to compress the data it must be done prior to encrypting. The IPcomp header provides for this. One of the problems of tunnel mode is that it adds 20 bytes of IP header, plus 28 bytes of ESP overhead to each packet. This can cause large packets to be fragmented. Compressing the packet first may make it small enough to avoid this fragmentation.
IPSec	Internet Protocol Security. IPSec provides interoperable, high quality, cryptographically-based security at the IP layer and offers protection for network communications.
IPSec tunnel	The IPSec connection to securely link two private parties across insecure and public channels.
IKE	IKE is a profile of ISAKMP that is for use by IPsec. It is often called simply IKE. IKE creates a private, authenticated key management channel. Using that channel, two peers can communicate, arranging for sessions keys to be generated for AH, ESP or IPcomp. The channel is used for the peers to agree on the encryption, authentication and compression algorithms to be used. The traffic to which the policies are applied is also agreed upon.
ISAKMP	ISAKMP is a framework for doing Security Association Key Management. It can, in theory, be used to produce session keys for many different systems, not just IPsec.
Key lifetimes	The length of time before keys are renegotiated.
LAN	Local Area Network.
LED	Light-Emitting Diode.
Local Private Key Certificate & Passphrase	The private part of the public/private key pair of the certificate resides on the Secure Router. The passphrase is a key that can be used to lock and unlock the information in the private key certificate.
Local Public Key	The public part of the public/private key pair of the certificate resides on the

Certificate	Secure Router and is used to authenticate against the CA certificate.
MAC address	The hardware address of an Ethernet interface. It is a 48-bit number usually written as a series of 6 hexadecimal octets, e.g. 00:d0:cf:00:5b:da. A Secure Router has a MAC address for each Ethernet interface. These are listed on a label on the underneath of the device.
Main Mode	This Phase 1 keying mode automatically exchanges encryption and authentication keys and protects the identities of the parties attempting to establish the tunnel.
Manual Keying	This type of keying requires the encryption and authentication keys to be specified.
Manual Keys	Predetermined encryption and authentication keys used to establish the tunnel.
Masquerade	The process when a gateway on a local network modifies outgoing packets by replacing the source address of the packets with its own IP address. All IP traffic originating from the local network appears to come from the gateway itself and not the machines on the local network.
MD5	Message Digest Algorithm Five is a 128 bit hash. It is one of two message digest algorithms available in IPSec.
NAT	Network Address Translation. The translation of an IP address used on one network to an IP address on another network. Masquerading is one particular form of NAT.
Net mask	The way that computers know which part of a TCP/IP address refers to the network, and which part refers to the host range.
NTP	Network Time Protocol (NTP) used to synchronize clock times in a network of computers.
Oakley Group	See Diffie-Hellman Group or Oakley Group.
PAT	Port Address Translation. The translation of a port number used on one network to a port number on another network.
PEM, DER, PCKS#12 PCKS#07	These are all certificate formats.

Perfect Forward Secrecy	A property of systems such as Diffie-Hellman key exchange which use a long-term key (such as the shared secret in IKE) and generate short-term keys as required. If an attacker who acquires the long-term key provably can neither read previous messages which he may have archived nor read future messages without performing additional successful attacks then the system has PFS. The attacker needs the short-term keys in order to read the traffic and merely having the long-term key does not allow him to infer those. Of course, it may allow him to conduct another attack (such as man-in-the-middle) which gives him some short-term keys, but he does not automatically get them just by acquiring the long-term key.
Phase 1	Sets up a secure communications channel to establish the encrypted tunnel in IPSec.
Phase 2	Sets up the encrypted tunnel in IPSec.
PPP	Point-to-Point Protocol. A networking protocol for establishing simple links between two peers.
PPPoE	Point to Point Protocol over Ethernet. A protocol for connecting users on an Ethernet to the Internet using a common broadband medium (e.g. single DSL line, wireless device, cable modem, etc).
PPTP	Point to Point Tunneling Protocol. A protocol developed by Microsoft™ that is popular for VPN applications. Although not considered as secure as IPSec, PPP is considered "good enough" technology. Microsoft has addressed many flaws in the original implementation.
Preshared secret	A common secret (passphrase) that is shared between the two parties.
Quick Mode	This Phase 2 keying mode automatically exchanges encryption and authentication keys that actually establishes the encrypted tunnel.
Rekeying	The process of renegotiating a new set of keys for encryption and authentication.
Road warrior	A remote machine with no fixed IP address.
Router	A network device that moves packets of data. A router differs from hubs and switches because it is "intelligent" and can route packets to their final destination.
RSA Digital Signatures	A public/private RSA key pair used for authentication. The Secure Router can generate these key pairs. The public keys need to be exchanged between the two parties in order to configure the tunnel.
SHA	Secure Hash Algorithm, a 160 bit hash. It is one of two message digest algorithms available in IPSec.
Security Parameter Index (SPI)	Security Parameter Index, an index used within IPsec to keep connections distinct. Without the SPI, two connections to the same gateway using the same protocol could not be distinguished.
Subnet mask	See "Net mask".
Switch	A network device that is similar to a hub, but much smarter. Although not a full router, a switch partially understands how to route Internet packets. A switch increases LAN efficiency by utilizing bandwidth more effectively.
TCP/IP	Transmission Control Protocol/Internet Protocol. The basic protocol for Internet communication.

TCP/IP address	Fundamental Internet addressing method that uses the form nnn.nnn.nnn.nnn.
TripleDES (3DES)	Using three DES encryptions on a single data block, with at least two different keys, to get higher security than is available from a single DES pass.
UTC	Coordinated Universal Time.
UTP	Unshielded Twisted Pair cabling. A type of Ethernet cable that can operate up to 100Mb/s. Also known as Category 5 or CAT 5.
VPN	Virtual Private Networking. When two locations communicate securely and effectively across a public network (e.g. the Internet). The three key features of VPN technology are privacy (nobody can see what you are communicating), authentication (you know who you are communicating with), and integrity (nobody can tamper with your messages/data).
WAN	Wide Area Network.
WINS	Windows Internet Naming Service that manages the association of workstation names and locations with IP addresses.
x.509 Certificates	An x.509 certificate includes the format of the certificate, the serial number of the certificate, the algorithm used to sign the certificate, the name of the CA that issued the certificate, the name and public key of the entity requesting the certificate, and the CA's signature.x.509 certificates are used to authenticate the remote party against a Certificate Authority's (CA) certificate. The CA certificate must have signed the local certificates that are used for tunnel authentication. Certificates need to be uploaded into the Secure Router before a tunnel can be configured to use them (see Certificate Management).

Appendix B – System Log

Access Logging

It is possible to log any traffic that arrives at or traverses the Secure Router. The only logging that is enabled by default is to take note of packets that were dropped. While it is possible to specifically log exactly which rule led to such a drop, this is not configured by default. All rules in the default security policy drop packets. They never reject them. That is, the packets are simply ignored, and have no responses at all returned to the sender. It is possible to configure reject rules if so desired.

All traffic logging performed on the Secure Router creates entries in the syslog (*/var/log/messages* or external syslog server) of the following format:

```
<Date/Time> klogd: <prefix> IN=<incoming interface>  
OUT=<outgoing interface> MAC=<dst/src MAC addresses>  
SRC=<source IP> DST=<destination IP> SPT=<source port>  
DPT=<destination port> <additional packet info>
```

Where:

<prefix>	if non-empty, hints at cause for log entry
<incoming interface>	empty, or one of eth0, eth1 or similar
<outgoing interface>	as per incoming interface
<dst/src MAC addresses>	MAC addresses associated with the packet
<source IP>	packet claims it came from this IP address
<destination IP>	packet claims it should go to this IP address
<source port>	packet claims it came from this TCP port
<destination port>	packet wants to go to this TCP port

Depending on the type of packet and logging performed some of the fields may not appear.

Commonly used interfaces are:

eth0	the LAN port
eth1	the WAN/Internet port
pppX	e.g. <i>ppp0</i> or <i>ppp1</i> , a PPP session
ipsecX	e.g. <i>ipsec0</i> , an IPSec interface

The firewall rules deny all packets arriving from the WAN port by default. There are a few ports open to deal with traffic such as DHCP, VPN services and similar. Any traffic that does not match the exceptions however is dropped.

There are also some specific rules to detect various attacks (smurf, teardrop, etc.).

When outbound traffic (from LAN to WAN) is blocked by custom rules configured in the GUI, the resultant dropped packets are also logged.

The *<prefix>* for all these rules is varied according to their type.

Currently used prefixes for traffic arriving:

Default Deny	Packet didn't match any rule, drop it
Invalid	Invalid packet format detected
Smurf	Smurf attack detected
Spoof	Invalid IP address detected
SynFlood	SynFlood attack detected
Custom	Custom rule dropped outbound packet

A typical *Default Deny*: looks similar to the following:

```
Mar 27 09:31:19 2003 klogd: Default deny: IN=eth1
OUT=MAC=00:d0:cf:00:ff:01:00:e0:29:65:af:e9:08:00
SRC=140.103.74.181 DST=12.16.16.36 LEN=60 TOS=0x10 PREC=0x00
TTL=64 ID=46341 DF PROTO=TCP SPT=46111 DPT=139 WINDOW=5840
RES=0x00 SYN URGP=0
```

That is, a packet arriving from the WAN (*IN=eth1*) and bound for the Secure Router itself (*OUT=<nothing>*) from IP address 140.103.74.181 (*SRC=140.103.74.181*), attempting to go to port 139 (*DPT=139*, Windows file sharing) was dropped.

If the packet is traversing the Secure Router to a server on the private network, the outgoing interface is eth0, e.g.:

```
Mar 27 09:52:59 2003 klogd: IN=eth1 OUT=eth0
SRC=140.103.74.181 DST=10.0.0.2 LEN=60 TOS=0x10 PREC=0x00
TTL=62 ID=51683 DF PROTO=TCP SPT=47044 DPT=22 WINDOW=5840
RES=0x00 SYN URGP=0
```

Packets going from the private network to the public come in eth0, and out eth1, e.g.:

```
Mar 27 10:02:51 2003 klogd: IN=eth0 OUT=eth1 SRC=10.0.0.2
DST=140.103.74.181 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=62830 DF
PROTO=TCP SPT=46486 DPT=22 WINDOW=5840 RES=0x00 SYN URGP=0
```

Creating Custom Log Rules

Additional log rules can be configured to provide more detail if desired. For example, by analyzing the rules in the **Rules** menu, it is possible to provide additional log messages with configurable prefixes (i.e. other than *Default Deny*;) for some allowed or denied protocols.

Depending on how the *LOG* rules are constructed it may be possible to differentiate between inbound (from WAN to LAN) and outbound (from LAN to WAN) traffic. Similarly, traffic attempting to access services on the Secure Router itself can be differentiated from traffic trying to pass through it.

The examples below can be entered on the Command Line Interface (telnet), or into the **Rules** web management console. Rules entered on the CLI are not permanent however, so while it may be useful for some quick testing, it is something to be wary of.

To log permitted inbound access requests to services hosted on the Secure Router, the rule should look something like this:

```
iptables -I INPUT -j LOG -p tcp --syn -s <X.X.X.X/XX> -d
<Y.Y.Y.Y/YY> --dport <Z> --log-prefix <prefix>
```

This logs any TCP (*-p tcp*) session initiations (*--syn*) that arrive from the IP address/netmask *X.X.X.X/XX* (*-s ...*) and are going to *Y.Y.Y.Y/YY*, destination port *Z* (*--dport*).

For example, to log all inbound access requests from anywhere on the Internet (0.0.0.0/0) to the PPTP service (port 1723) on the Secure Router (IP address 1.2.3.4):

```
iptables -I INPUT -j LOG -p tcp --syn -s 0.0.0.0/0 -d 1.2.3.4 -
-dport 1723 --log-prefix "Internet PPTP access: "
```

To find the resultant log entry in the logs, simply search for the prefix, in this instance *"Internet PPTP access: "*.

If for example site 192.0.1.2 attempted to access the Secure Router's PPTP port, the resultant log message would look something like this:

```
<12> Jan 24 17:19:17 2000 klogd: Internet PPTP access: IN=eth0
OUT= MAC=00:d0:cf:00:07:03:00:50:bf:20:66:4d:08:00 SRC=
DST=1.2.3.4 LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=43470 DF
PROTO=TCP SPT=4508 DPT=1723 WINDOW=64240 RES=0x00 SYN URGP=0
```

Note how *OUT* is set to nothing. This indicates that the packet was attempting to reach a service on the Secure Router, rather than attempting to pass through it.

A very similar scenario occurs for logging access requests that are attempting to pass through the Secure Router. It merely requires replacing the *INPUT* keyword with *FORWARD*.

Thus, to log permitted inbound requests to services hosted on a server behind the Secure Router, or outbound requests to services on a public network server, use:

```
iptables -I FORWARD -j LOG -p tcp --syn -s <X.X.X.X/XX> -d
<Y.Y.Y.Y/YY> --dport <Z> --log-prefix <prefix>
```

For example, to log all inbound requests from the IP address 5.6.7.8 to the mail server (port 25) on the machine *flubber* on the LAN with address 192.168.1.1:

```
iptables -I FORWARD -j LOG -p tcp --syn -s 5.6.7.8/32 -d
192.168.1.1 --dport 25 --log-prefix "Mail for flubber: "
```

This results in log output similar to:

```
<12> Jan 24 18:17:19 2000 klogd: Mail for flubber: IN=eth1
OUT=eth0 SRC=5.6.7.8 DST=192.168.1.1 LEN=48 TOS=0x00 PREC=0x00
TTL=126 ID=45507 DF PROTO=TCP SPT=4088 DPT=25 WINDOW=64240
RES=0x00 SYN URGP=0
```

Note how the *OUT* value has now changed to show which interface the access attempt used to reach the internal host. As this request arrived on eth1 and was destined for eth0, we can determine that it was an *inbound* request, since eth0 is the LAN port, and eth1 is usually the WAN port.

An *outbound* request would have *IN=eth0* and *OUT=eth1*.

It is possible to use the *-i* and *-o* arguments to specify the interface that are to be considered for *IN* and *OUT* respectively. When the *!* argument is used before the interface name, the sense is inverted. A name ending in a *+* matches any interface that begins with the name. e.g.

```
iptables -I FORWARD -j LOG -i eth0 -p tcp ...
```

This rule logs outbound from the LAN (eth0) only. We could limit that further by specifying which interface it is outbound to, by using the *-o* option.

```
iptables -I FORWARD -j LOG -i eth0 -o eth1 -p tcp ...
```

This logs LAN traffic destined for the WAN, but won't log LAN traffic destined for a PPP or perhaps IPsec link.

Similarly, we could construct a rule that looks at all inbound/outbound traffic, but excludes VPN traffic, thus:

```
iptables -I FORWARD -j LOG -i eth+ -o eth+ -p tcp ...
```

If we just wanted to look at traffic that went out to the IPsec world, we could use:

```
iptables -I FORWARD -j LOG -o ipsec+
```

Clearly there are many more combinations possible.

It is therefore possible to write rules that log inbound and outbound traffic, or to construct several rules that differentiate between the two.

Rate Limiting

iptables has the facility for rate-limiting the log messages that are generated, in order to avoid denial of service issues arising out of logging these access attempts. To achieve this, use the following option:

```
--limit rate
```

rate is the maximum average matching rate, specified as a number with an optional */second*, */minute*, */hour*, or */day* suffix. The default is *3/hour*.

```
--limit-burst number
```

number is the maximum initial number of packets to match. This number gets recharged by one every time the limit specified above is not reached, up to this number. The default is 5.

iptables has many more options. Perform a web search for *manpage iptables* to find the relevant documentation.

The *LOG* rules configured by default (e.g. *Default Deny*;) are all limited to:

```
--limit 3/hour --limit-burst 5
```

Administrative Access Logging

When a user tries to log onto the web management console, one of the following log messages appears:

```
Jan 30 03:00:18 2000 boa: Authentication successful for root  
from 10.0.0.2
```

```
Jan 30 03:00:14 2000 boa: Authentication attempt failed for  
root from 10.0.0.2
```

This message shows the date/time, whether the authentication succeeded or failed, the user attempting authentication (in this case *root*) and the IP address from which the attempt was made.

Telnet (Command Line Interface) login attempts appear as:

```
Jan 30 03:18:37 2000 login: Authentication attempt failed for  
root from 10.0.0.2
```

```
Jan 30 03:18:40 2000 login: Authentication successful for root  
from 10.0.0.2
```

Once again, showing the same information as a web login attempt.

Boot Log Messages

The Secure Router's startup boot time messages are identified by log messages similar to the following:

```
klogd: Linux version 2.4.20-uc0 (jamma@daniel) (gcc version  
3.0.4) #4 Mon Feb 3 15:17:50 EST 2003
```

This also shows the version of the operating system (linux), and the build date and time.

This page intentionally left blank.

Appendix C – Firmware Upgrade Practices and Precautions

Prior performing any firmware upgrade, it is important that you save a back up of your existing configuration (see the *Save/Restore* section in the chapter entitled *System*) to a local file.

While we make every effort to ensure your existing configuration continues working after minor and patch revision upgrades, sometimes compatibility problems may arise.

For major upgrades, existing configuration is not maintained. A factory reset must be performed and the Secure Router reconfigured from scratch.

Note

Secure Router firmware revision numbers have the form a.b.c, where a is the major revision number, b is the minor revision number, and c is the patch revision number.

An upgrade where the major revision number is incremented is considered a major upgrade, e.g. 2.1.5 -> 3.0.0. An upgrade where the minor revision number is incremented is considered a minor upgrade, e.g. 3.0.2 -> 3.1.0. An upgrade where the patch revision is incremented is considered a patch upgrade, e.g. 3.0.0 -> 3.0.1.

Warning

If the flash upgrade is interrupted (e.g. power down), the Secure Router stops functioning and becomes unusable until its flash is reprogrammed at the factory or a recovery boot is performed. User care is advised.

After the upgrade has completed successfully and the Secure Router is back up and running with the new firmware, run through a few tests.

Ensure that Internet connectivity and any VPN connections can be established and pass traffic, and that any configured services such as **DHCP Server**, **Access Control** or **Packet Filtering** are functioning as expected.

If you encounter any problems, reset the device to its factory default settings and reconfigure. You may wish to use your backed up old configuration as a guide in this process, but *do not* restore it directly.

If you are upgrading a device that you do not normally have physical access to, e.g. at a remote or client's site, we strongly recommend that following the upgrade, you reset the device to its factory default configuration and reconfigure as a matter of course.

Note

To restore factory default settings, press the black Reset / Erase button on the rear panel twice.

Appendix D – Recovering From a Failed Upgrade

If the *Heart beat* (or *H/B*) LED is not flashing 20 – 30 seconds after power is supplied, the Secure Router unit is unable to boot correctly. This is usually because the firmware inside the Secure Router unit has been written incorrectly or incompletely, or in rare cases it may have become corrupted.

In this situation, a *recovery boot* reprograms the Secure Router to bring it back to a usable state. This can be done using the Netflash executable if you are running Windows, otherwise you have to set up a BOOTP (DHCP) server.

Both procedures are outlined below.

Note

A Netflash that contains the firmware that shipped with your unit is located in the \firmware directory on the SG CD. A Netflash containing the latest firmware for your SG unit can be obtained from SG customer support.

Always attempt a recovery boot before requesting an RMA from customer support.

Recovery using Netflash

The following details the steps required to perform a recovery boot using the Netflash program on a Windows PC.

1. Attach the Secure Router unit's LAN port or switch directly to your PC using a crossover cable.

Note

If you are using an older LITE(2)/LITE(2)+, you may have to attach the unit's WAN port directly to your PC using a crossover cable for the first stage of the recovery procedure. The Netflash program prompts you to switch the cable to the LAN port/switch using a straight through for the second stage of the recovery procedure.

2. Log in to your PC with administrator privileges (2000/XP/NT4 only).
3. Ensure there are no DHCP server programs or services (**Start -> Run -> Open: services.msc**) running on your PC.
4. Disable the inbuilt Windows firewall (**Control Panel -> Windows Firewall**), and any third party firewall or antivirus software.
5. Hold in the **Reset/Erase** button while applying power, keep it held in for 3 seconds.
6. Double click on Netflash to launch it.
7. Click **Recover** and select **Network Recovery**.
8. Click **Recover Device**.
9. Enter an address in the same network range as your PC and click **OK**.

Note

If the recovery procedure fails at or after Assigning IP address..., but the Heart Beat/H/B light is flashing, the unit may have become uncontactable due to bad configuration. If this is the case, press the Reset/Erase button twice within 2 seconds to restore factory default configuration, power off the unit and restart the recovery procedure from the beginning.

10. If prompted, select your Secure Router unit from the list displayed.
11. Enter your Secure Router unit's password and click **OK**.
12. If prompted, enter your Secure Router unit's web administration port.
13. Wait for the recovery procedure to complete and the Secure Router unit to finish reprogramming.

Note

It takes a few minutes for your Secure Router to finish reprogramming. After it has finished it reboots automatically with its old configuration intact. If it is uncontactable after rebooting, press the Reset/Erase button twice within 2 seconds to restore factory default configuration, then follow the instructions in the chapter entitled Getting Started to begin reconfiguration of your unit.

Recovery using a BOOTP server

The following is a brief guide to performing a recovery boot when you are unable to access either Netflash or a Windows PC on which to run it. More comprehensive instructions are not given, as they vary depending on your operating system and server software packages.

The recovery procedure involves network booting the unit using a BOOTP server with access to a Secure Router firmware image file, then upgrading the network as per a normal flash upgrade to reprogram its flash to a usable state.

Note

To perform the recovery boot, you must have a firmware image for your Secure Router unit. The firmware that shipped with your unit is located in the \firmware directory on the SG CD. The latest firmware for your SG unit can be obtained from SG customer support

Firmware files have the format Model_Version_Date.sgu or Model_Version_Date_.sgu.*

1. Log in to your PC with sufficient permissions to edit the server configuration files, and stop and start the servers.
2. Place the firmware file in your BOOTP server's path, e.g.: `/tftpboot/`
3. Edit your BOOTP server configuration to contain an entry for the Secure Router unit. Specify the firmware file as the file to boot, e.g.:

```
filename "SECURE_ROUTER_v2.1.3_20041213.sgu";
```

4. (Re)start the BOOTP server.
5. Attach the Secure Router unit's LAN port or switch directly to your PC using a crossover cable.

Note

If you are using an older LITE(2)/LITE(2)+, you may have to attach the unit's WAN port directly to your PC using a crossover cable for the first stage of the recovery procedure.

Accordingly, your BOOTP server requires an entry specifying the Secure Router unit's WAN port MAC address.

6. Hold in the **Reset/Erase** button while applying power, keep it held in for 3 seconds.

After 20 – 30 seconds, the Secure Router unit loads the file from the DHCP/BOOTP server and the *Heart Beat/H/B* light begins flashing.

7. Browse or telnet/ssh to your Secure Router unit and perform a flash upgrade as per usual to reprogram its flash.

Note

If the Secure Router unit is uncontactable, but the Heart Beat/H/B light is flashing, it may be due to bad configuration. If this is the case, press the Reset/Erase button twice within 2 seconds to restore factory default configuration, and perform the network boot again.

Secure Router User Guide



TELTRONICS

Teltronics, Inc.
2150 Whitfield Industrial Way
Sarasota, FL 34243
941.753.5000

Part Number 610-0000-0514 Rev B