eicon networks

Shiva VPN Gateway

Model 500 and 1100

System Administrator's Guide

Connecting People to Information

Second Edition (March 2005) *206-463-02*

Copyright © 2005 Eicon Networks Corporation. All Rights Reserved. You may not reproduce this document in whole or in part without permission in writing from Eicon Networks Corporation.

All contents of this document are subject to change without notice and do not represent a commitment on the part of Eicon Networks Corporation. Reasonable effort is made to ensure the accuracy of the information contained in the document. However, due to ongoing product improvements and revisions, Eicon Networks Corporation does not warrant the accuracy of this information and cannot accept responsibility for errors or omissions that may be contained in this document. It is possible that the use or implementation of any one of the concepts, applications, or ideas described in this document, in marketing collateral produced by or on web pages maintained by Eicon Networks Corporation or its subsidiaries may infringe one or more patents or other intellectual property rights owned by third parties. Eicon Networks Corporation does not provide any intellectual property licenses with the sale of Eicon products other then a license to use such product in accordance with intellectual property owned or validly licensed by Eicon Networks Corporation or its subsidiaries. More detailed information about such intellectual property is available from Eicon Networks Corporation's legal department at 9800 Cavendish Blvd., Montreal, Quebec, Canada H4M 2V9. Eicon Networks Corporation encourages all users of its products to procure all necessary intellectual property licenses required to implement any concepts or applications and does not condone or encourage any intellectual property infringement and disclaims any responsibility related thereto. These intellectual property licenses may differ from country to country and it is the responsibility of those who develop the concepts or applications to be aware of and comply with different national license requirements. The software referred to in this document is provided under a Software License Agreement. Refer to the Software License Agreement for complete details governing the use of the software.

All names, products, and services mentioned herein are the trademarks or registered trademarks of their respective organizations and are the sole property of their respective owners. Eicon, Eicon Networks, Shiva, and Connecting People to Information are registered trademarks or trademarks of Eicon Networks Corporation or its subsidiaries.

To contact Eicon Customer Support, refer to the 'Customer Services' section in the printed guide that came with the Eicon product which you purchased or visit our web site at www.eicon.com.

Contents

Chapter 1 Introduction 7

Getting started 8

Overview 9
- Package contents 10

Document conventions 11
- Formatting conventions 11
- Specifying IP addresses 11

Status lights 13

Ports/connectors 14

Chapter 2 Network connections 15

Connections tab 16

LAN port settings 17
- Direct LAN 17
- Bridged LAN 17

Internet port settings 18
- Connecting a modem 18
- Setting up an Internet connection 18

COM port settings 21
- Connecting a modem 21
- Setting up a dial out Internet connection 21

Wireless port settings 24
- Wireless network performance 24
- Setting up the wireless network 24
- Setting up an ACL 26
- Advanced wireless settings 27

Bridging 29
- Bridging between network ports 29
- Bridging across a VPN connection 29

Internet failover 30
- Enable the primary connection for failover 30
- Set up a secondary backup Internet connection 31

Routes 32
- Additional routes 32
- Route management 32

Interface aliases 33
- LAN port alias 33
- Internet port alias 33

Changing the MAC address 34

Advanced network settings 35
Hostname 35
DNS Proxy 35
Network address translation (NAT/masquerading) 36
Dynamic DNS 36

QoS traffic shaping 37

Chapter 3 DHCP services 39

DHCP server configuration 40
To configure the DHCP server 40

DHCP relay 43

Chapter 4 Firewall 45

Incoming access 46
Administration services 46
Shiva web server. 47

Packet filtering. 49
Service groups 50
Addresses 51
Rules 52
NAT 53

Connection tracking 57

Rules 58

Intrusion detection. 59
Setting up intrusion detection and blocking. 59

Universal plug and play gateway 61
Configuring the UPnP gateway 61

Access control. 62
User authentication 62
IP lists 64
Web lists 65

Chapter 5 Virtual private networking 67

Overview 68

VPN client 69
PPTP client 69
L2TP client 70

VPN server 71
PPTP server 71
L2TP server. 74

IPSec. 75
Scenario 75
Set up the branch office 75
Set up the head office 84
Tunnel List. 86
Connection 87
Remote party. 87
Status 87
NAT traversal support 90
Dynamic DNS Support 90
Troubleshooting 90

Certificate management 94
Adding certificates. 94
Adding a CA or CRL certificate 94
Adding a local certificate 95

GRE 96
Setting up a GRE tunnel 96

Port Tunnels 98
Setting up a port tunnel. 98

Chapter 6 Management. 101

Setting the date and time 102
Locality 103

User list 104
Adding a user 104
Administrator password security 106

Management settings 107
Management configuration 107
Local names 108

Diagnostics 109
Diagnostics 109
Network tests 110

System log 111
Access logging 112
Creating custom log rules 113
Rate Limiting 115
Administrative Access Logging 115
Boot Log Messages 116

Configuration files 117

Flash upgrade 118
Before upgrading. 118
Upgrade procedure 118

Reboot. 120
Reset button 120

Technical Support. 121

Chapter 7 Terminology 123

Chapter 8 International Regulatory Information 133

Shiva 500 VPN Gateway 134
Regulatory information for the USA 134
Regulatory information for Canada. 134
Regulatory information for Europe 135

Shiva 1100 VPN Gateway 136
Information for the user 136
Regulatory information 139

Chapter 1

Introduction

This manual describes how to take advantage of the features of your Shiva VPN Gateway, including setting up network connections, a secure firewall, and a VPN.

This chapter provides an overview of your Shiva VPN Gateway's features and capabilities.

Getting started

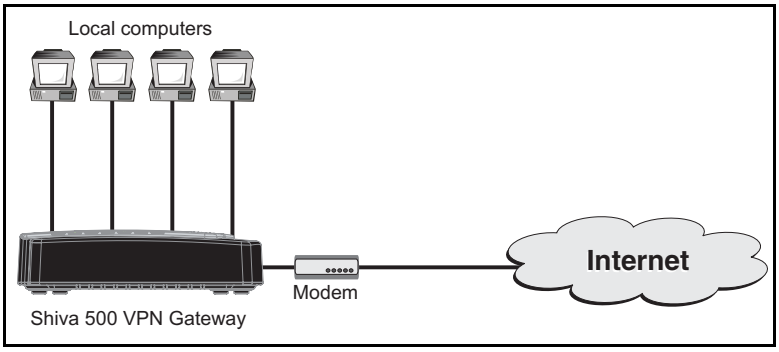
To get started with the Shiva VPN Gateway refer to the printed Quick Start guide.

Once your Shiva VPN Gateway is operational you can customize its settings as described in this document.

Chapter	Description
Chapter 2	This chapter describes the Network Setup section of the Web Management Console. Here you can configure each of your Shiva VPN Gateway's network ports (Ethernet, serial). Network ports may be configured for Internet connection, LAN connection, remote dial-in access or Internet failover.
Chapter 3	The Shiva 500 VPN Gateway enables remote and secure access to your office network. This chapter shows how to set up the dial-in features.
Chapter 3	The Shiva VPN Gateway can act as a DHCP server for machines on your local network. To configure your Shiva VPN Gateway as a DHCP server, you must set a static IP address and netmask on the LAN port.
Chapter 4	The Shiva VPN Gateway is equipped with a fully featured, stateful firewall. The firewall allows you to control both incoming and outgoing access, so that computers on the LAN can have tailored Internet access facilities and are shielded from malicious attacks. By default the firewall is active, and allows all outgoing connections and blocks all incoming connections.
Chapter 5	This chapter details how to configure the PPTP client, how to establish an IPSec tunnel, and also provides an overview of GRE and L2TP VPN tunneling.
Chapter 6	This chapter describes how to configure various management options such as date and time, users, administrator settings, and diagnostics.
Chapter 7	This chapter describes terms that are commonly used in this document.
Chapter 8	This chapter provides regulatory information for all regions.

Overview

The Shiva VPN Gateway provides Internet security and privacy of communications for small and medium enterprises. It simply and securely connects your office to the Internet, and with its robust stateful firewall, shields your computers from outside threats. The Shiva VPN Gateway checks and filters data packets to prevent unauthorized intruders gaining access.



new picture for the 1100 when graphics become available

The Shiva VPN Gateway is a price/performance leader designed for securing small offices and remote workers. The Shiva VPN Gateway makes it simple and easy to set up and secure a small or home office that connects to a corporate network over the Internet via broadband connections like ADSL or cable. For optimum security, the Shiva VPN Gateway has a powerful stateful inspection firewall with service-based intrusion detection to help protecting the remote PCs or offices. This, combined with support for industry-standard VPN and authentication protocols, makes the Shiva VPN Gateway a fully featured security device that will also help maximize productivity by assuring uninterrupted connectivity, or high availability, through the combination of WAN and serial ports.

The Shiva VPN Gateway enables you to significantly cut the telecommunications costs associated with dial-up, leased-line, and frame relay connections by leveraging the Internet to securely provide remote access, LAN-to-LAN, and Extranet connectivity. By including the Shiva CMS with your purchase (please refer to the *Shiva CMS System Administrator's Guide* on the Shiva VPN Gateway CD for more information), Eicon significantly reduces the initial deployment and maintenance costs involved with rolling out your networks and provides you with one of the most complete solutions available on the market today.

Package contents

The following items are included with your Shiva VPN Gateway gateway:

- Power adapter
- Installation CD
- Quick Install guide
- Install Map
- Two six-foot straight-through Ethernet cables

Document conventions

The following conventions are used in this guide.

Formatting conventions

This manual uses the following formatting conventions.

Example	Description
Network or **mkdir rootCA**	When referring to the web-based management console, items in bold type identify menu commands or input fields. They are presented exactly as they appear on screen. Bold text is also used to present command line output or program listings.
Network Setup > Routes	When referring to the web-based management console, submenus and tabs are indicated using the ‘>’ sign. The example refers to the Routes tab, which is found after selecting the Network Setup option.

Specifying IP addresses

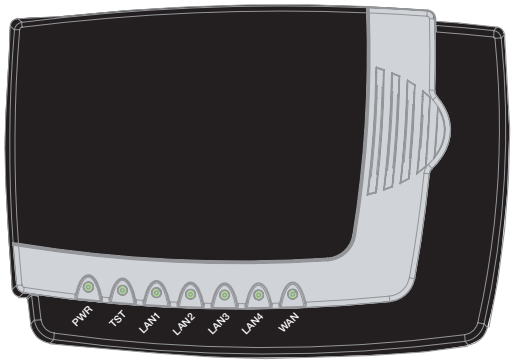
When using the web-based management console to configure the Shiva VPN Gateway, you will need to specify IP addresses and address ranges. The following syntax conventions are used to do this:

Syntax	Description
a.b.c.d	Use this form to specify a single IP address. Replace each letter by a digit in the range 0 to 255.
a.b.c.d-e	Use this form to specify an IP address range, where a.b.c.d specifies the starting address and a.b.c.e specifies the ending address. The start and end addresses are included in the range.
a.b.c.d-e.f.g.h	Use this form to specify an IP address range, where a.b.c.d specifies the starting address and e.f.g.h specifies the ending address. The start and end addresses are included in the range.

Syntax	Description
a.b.c.d/e	Use this form to specify an IP address range that covers an entire subnet. The value of e specifies the number of bits in the IP address range. For example: • a.b.c.d/24 covers the entire C class network/subnet a.b.c.0 and is equivalent to specifying the range as a.b.c.0-255. • a.b.c.d/32 is equivalent to the single IP address a.b.c.d. • 192.168.12.150/26 is equivalent to the range 192.168.12.128-191 and it includes 64 IP addresses.

Status lights

The Shiva VPN Gateway provides the following status lights on its top panel.



1100 tba

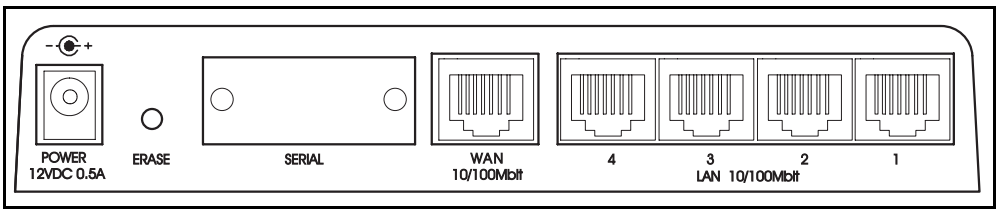
.

Label	State	Description
PWR	On	Power is supplied to the Shiva VPN Gateway.
TST	Flashing	The Shiva VPN Gateway is operating correctly.
	On	The unit is restarting or an operating error has occurred.
LAN1 LAN2 LAN3 LAN4	Flashing	Traffic is being sent or received on the indicated LAN port.
WAN	Flashing	Traffic is being sent or received on the WAN port.

Ports/connectors

The rear panel contains the following connector:

1100 tba



Label	Description
POWER	Connect the power adapter here.
ERASE	Details ?????.
SERIAL	Serial port with DB-9 connector supporting speeds up to 115200.
WAN	10/100 auto-sensing Ethernet port.
LAN1 LAN2 LAN3 LAN4	10/100 auto-sensing Ethernet ports.
ANT1 ANT2	Shiva 1100 VPN Gateway only. Details ?????.

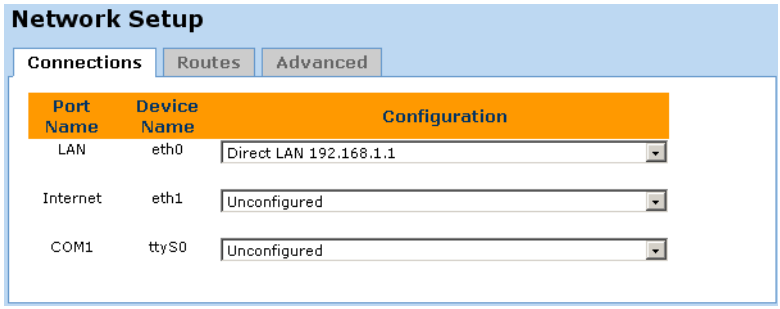
Chapter 2

Network connections

This chapter describes the Network Setup section of the Web Management Console. Here you can configure each of your Shiva VPN Gateway's network ports (Ethernet, serial). Network ports may be configured for Internet connection, LAN connection, remote dial-in access or Internet failover.

Connections tab

The **Connections** tab displays each network port on the Shiva VPN Gateway along with its **Device Name** and current **Configuration**. Initially, all network ports are unconfigured, aside from the LAN port.



Port configuration

- To change the configuration of a port, select a new setting in the **Configuration** column. This will automatically display additional configuration pages.
- To edit an existing configuration, select **Edit current settings** in the **Configuration** column. This will automatically display additional configuration pages that are described later in this chapter.
- If a port is experiencing difficulties auto-negotiating with another device, Ethernet speed and duplex may be set manually by selecting **Edit Ethernet configuration**.

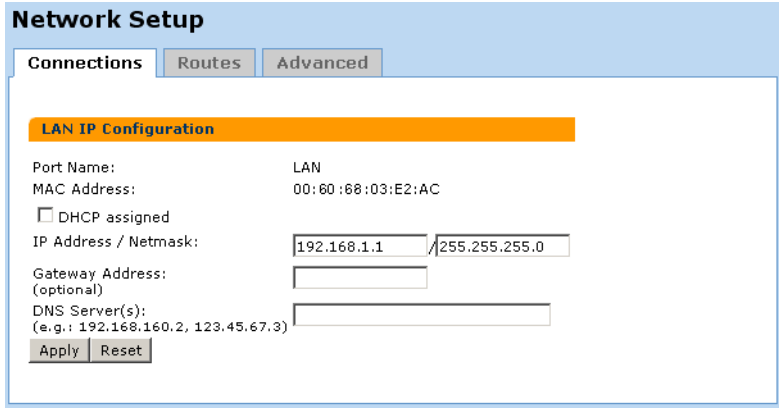
LAN port settings

Network settings for the LAN port can be assigned statically, or dynamically by a DHCP server (Direct LAN). Alternatively you may choose to configure the LAN port as a bridge (Bridged LAN).

Direct LAN

1 Click **Network Setup** on the main menu.

2. Select **Direct LAN** in for the LAN port.



3. Enter an **IP Address** and **Netmask** for the LAN network port. If you are using the Shiva VPN Gateway in its default, network address translation mode, (“Network address translation (NAT/masquerading)” on page 36), this will typically be part of a private IP range, such as 192.168.1.1 / 255.255.255.0. Ensure DHCP assigned is unchecked.

   If you want to have your Shiva VPN Gateway obtain its LAN network settings from an active DHCP server on your local network, check **DHCP** assigned then **Apply**. Note that anything in the IP Address and Netmask fields will be ignored.

   You may also enter one or more DNS servers. Multiple servers may be entered separated by commas.

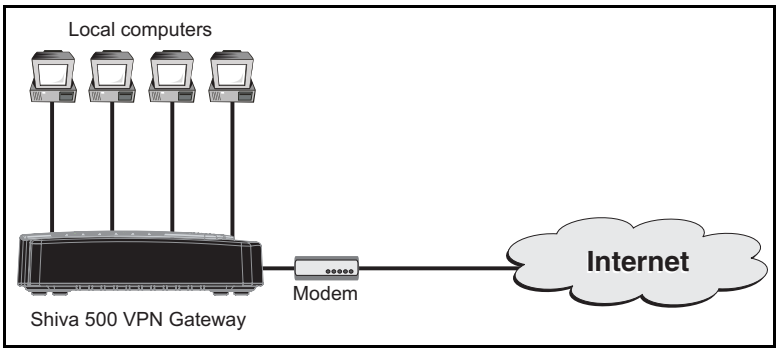
4. Click **Apply**.

Bridged LAN

For details, see “Bridging” on page 29.

Internet port settings

The Shiva VPN Gateway can connect to the Internet using an external dialup analog modem, an ISDN modem, a permanent analog modem, a cable modem or DSL link.



Connecting a modem

The first step in connecting your office network to the Internet is to physically attach your Shiva VPN Gateway to the modem device.

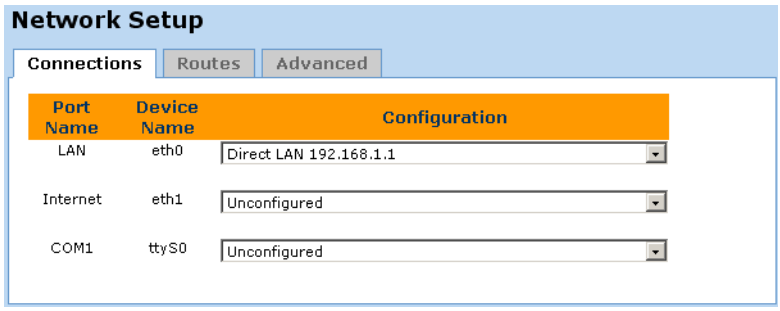
If you are configuring an analog modem or ISDN connection as your primary Internet connection, see the section “COM port settings” on page 21.

Connect your Shiva VPN Gateway's Internet port to the modem device using a straight through Ethernet cable. Apply power to the modem and give it some time to power up. Ensure that the Ethernet link LEDs are illuminated on both the Shiva VPN Gateway and modem device.

Setting up an Internet connection

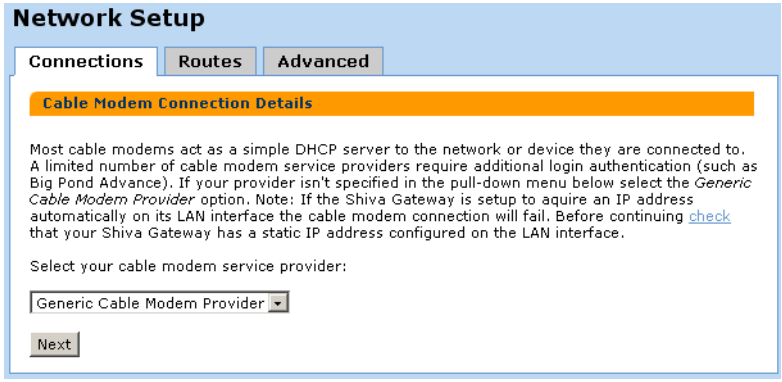
1 Click **Network Setup** on the main menu.

2. Select a connection type (all options are detailed below) for the Internet port. A configuration page for the connection type will open.



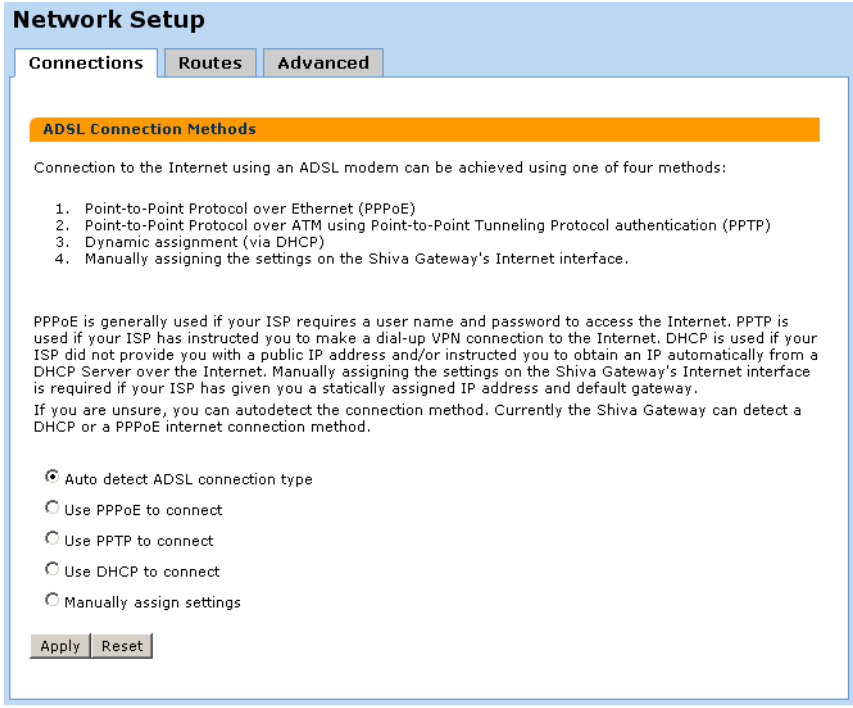
Cable Internet

Select your cable ISP from the list and click **Next**. If your provider does not appear, select **Generic Cable Modem Provider**. For cable modem providers other than Generic, enter your user name and password and click **Finish**. You are now ready to connect. Click the **Reboot** button to save your configuration and reboot your Shiva VPN Gateway.



ADSL Internet

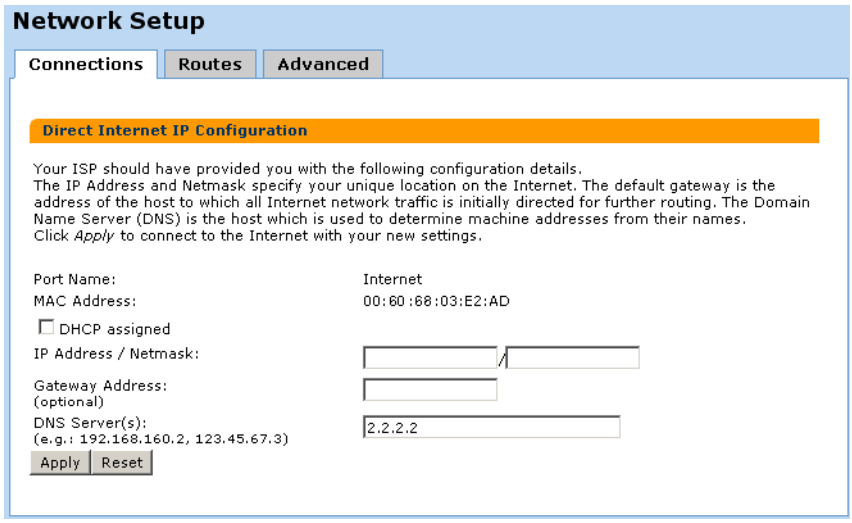
If you are connecting to the Internet using ADSL, you may select the connection method PPPoE, DHCP, or Manually Assign Settings. If you are unsure, you can let the Shiva VPN Gateway attempt to Auto detect ADSL connection type. Click **Apply** to continue.



Direct Internet

If you have a direct connection to the Internet, select this option. Typically your ISP will have provided you with network settings (possibly a range of IP addresses), or asked you to auto-configure using DHCP.

To use DHCP, check the **DHCP Assigned** check box. You may also enter one or more DNS Server(s), however any DNS server addresses allocated by your ISP will take precedence over these.



To manually configure your Internet network settings, enter the **IP Address, Netmask, Internet Gateway** and **DNS Server(s)** supplied by your ISP. If you have been given a range of IP addresses, they may be added as **Interface Aliases**. For details, see “Interface aliases” on page 33.

Reboot your Shiva VPN Gateway to establish your Internet connection.

Bridged Internet

For details, see “Bridging” on page 29.

Failover direct/Cable/ADSL Internet

For details, see “Internet failover” on page 30.

COM port settings

With a modem attached, the COM (serial) port can be configured as:

- a primary Dialout Internet connection to provide dial-in Access for remote users
- a secondary Failover Dialout Internet connection that will be activated when your primary Internet connection becomes unavailable (e.g. ISP equipment or the telecommunications network may temporarily fail).

Connecting a modem

Use a serial cable to connect the Shiva VPN Gateway's serial port (COM1) to a modem.

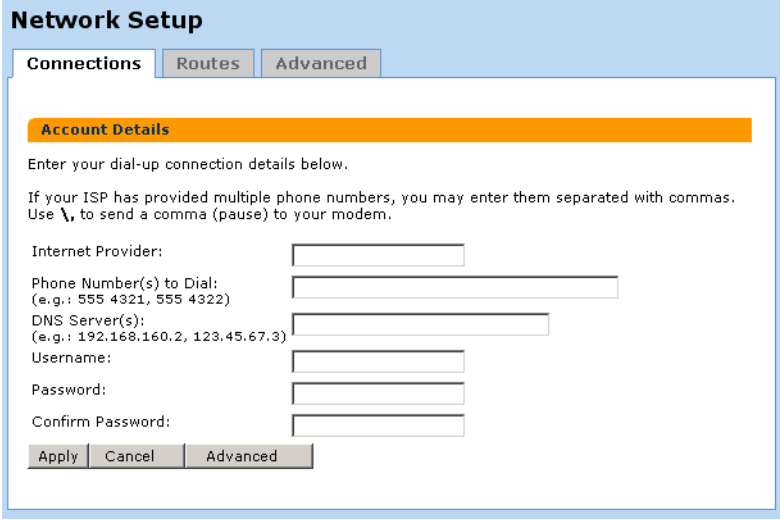
Note: *To connect to an ISDN line, the* Shiva VPN Gateway *requires an intermediate device called a Terminal Adapter (TA). A TA connects into your ISDN line and has either a serial or Ethernet port that is connected to your* Shiva VPN Gateway*. Do not plug an ISDN connection directly in to your* Shiva VPN Gateway*.*

Setting up a dial out Internet connection

1 Click **Network Setup** on the main menu.

2. Select **Dialout Internet** in for the COM1 port.

3. Configure parameters as required by your ISP.

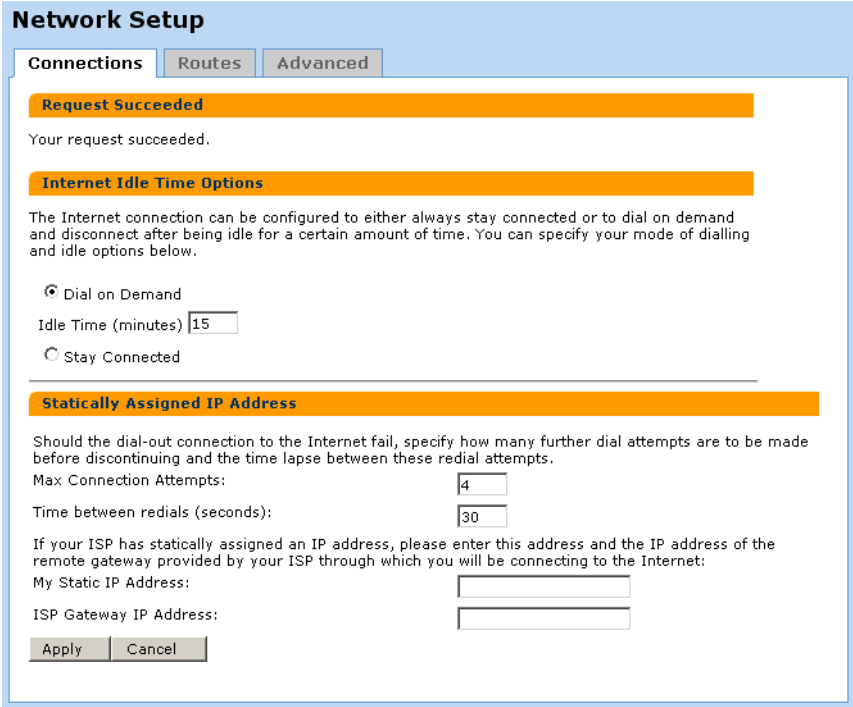


- Internet Provider: Enter the name of your ISP.
- Phone Number(s) to Dial: Enter the number to dial to reach your ISP. If you are behind a PABX that requires you to dial a prefix for an outside line (e.g. 0 or 9) ensure you enter the appropriate prefix. If your ISP has provided you with multiple phone numbers, you may enter them separated with commas.
- DNS Server(s) (optional): Enter the DNS server address supplied by your ISP. Multiple DNS addresses may be entered separated by commas. Note

that any DNS addresses automatically handed out by your ISP will take precedence over the addresses specified here.

- Username
  Password: Enter the unique username and password allocated by your ISP. The Password and Confirm Password fields must match.

4. If required, additional parameters can be configured by clicking the **Advanced** button.



- Dial on Demand: When enabled, the Shiva VPN Gateway establishes the connection only when there is traffic trying to reach the Internet and disconnects if the connection is inactive (i.e. when there is no traffic to/from the Internet) for the time specified by Idle Timer.
- Idle Time: Specifies how long the connection can be idle before it is dropped when Dial on Demand is active. Selecting **Stay Connected** will disable the idle timeout.
- Max Connection Attempts: Specifies the number of redial attempts to make before discontinuing.
- Time Between Redials: Specifies the number of seconds to wait between redial attempts
- My Static IP Address
  ISP Gateway IP Address: The majority of ISPs dynamically assign an IP address to your connection when you dial-in. However some ISPs use pre-assigned static addresses. If your ISP has given you a static IP address, enter it in Local IP Address and enter the address of the ISP gateway in ISP Gateway IP Address.

- If a dial on demand connection has been set up, **Connect Now/Disconnect Now** buttons will be displayed. These make the Shiva VPN Gateway dial or hang up the modem connection immediately.

5. Click **Apply**.

Wireless port settings

Note: *This feature is only supported on the Shiva 1100 VPN Gateway.*

The Shiva VPN Gateway can create a wireless network for connection of client computers that have wireless network cards. The Shiva VPN Gateway supports both the 802.11b and 802.11g standards.

An important note about wireless security

The wireless network created by the Shiva VPN Gateway may extend beyond the physical boundaries of your location. Therefore, it is important to properly secure access to the wireless network and to enable protection for all wireless transmissions using the Shiva VPN Gateway's wireless security features. This will ensure that rouge users are uanble to compromise your network or spy on its transmissions.

Wireless network performance

The Shiva VPN Gateway can create a wireless network (called a cell) in a radius of up to 300 feet. The quality of the wireless signal in this cell is governed by a number of factors, including:

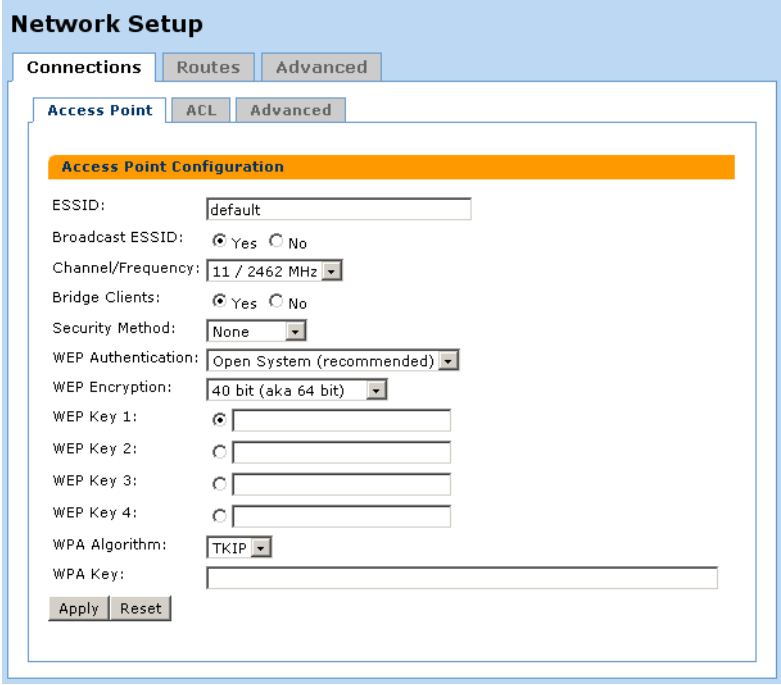
- **Intervening obstructions:** Each obstruction between the Shiva VPN Gateway and a wireless client station will reduce the signal strength. Some materials, (wood and plaster) have less of an effect than others (concrete, brick). Metal creates the most trouble for wireless signals (metal doors, reinforced concete walls, elevator shafts).
- **Electircal devices:** Any device that generates RF noise (electric motors, microwaves, monitors, power supplies) can affect wireless performance. For maximum performance it is best to install the Shiva VPN Gateway at least 5 feet away from these types of devices.
- **2.4 GHz devices:** Other device using the 2.4 GHz frequency band can dramatically interfere with wireless operation. This includes other wireless access points, security systems, and wireless phones. If other wireless access points are operating in the area, you can adjust the operating channel of the Shiva VPN Gateway to minimize interference.

Setting up the wireless network

1 Click **Network Setup** on the main menu.

2. Select **Edit Wireless configuration** in for the Wireless port.

3. Configure wireless settings as required and then click **Apply**.



- ESSID: Specify the name of the wireless network. Client stations will need to supply this name to associate with the Shiva VPN Gateway. You can use the same network name for multiple wireless access points. Normally a client station can specify the network name 'ANY' to access any wireless network within range that does not require encryption. However, by default the Shiva VPN Gateway ignores requests for the 'ANY' network.
- The ESSID can contain up to 32 alphanueric characters and is case sensitive, meaning 'MYNETWORK' and 'mynetwork' are two different network names.
- Broadcast ESSID: Enable this option to have the Shiva VPN Gateway broadcast the ESSID in the wireless beacom. This makes the Shiva VPN Gateway visible to all wireless client stations.
- Channel/Frequency: Select the operating channel for the wireless network. To avoid interference with other 2.4GHz devices, select a channel number that differs from the one used by the other device by at least 5 channels. For example, if another wireless access point is operating on channel 6, you could select either channel 1 or 11.

  Note: Channels availablility is subject to government regulation. You are responsible for making sure that the channel you select conforms to local regulations. As a result, in some areas it may not be possible to choose two channels that have the necessary seperation to reduce interference.
- Bridge Clients: Enable this option to allow wireless client stations to communicate with each other. When disabled, client-to-client communication is blocked.

  Note: If this option is enabled it can create a serious security risk if network access is not properly secured.
- Bridge Clients: Enable this option to allow wireless client stations to communicate with each other.

- Security: This option enables the wireless security option that protects the network. Two options are available:
  - WEP: Provides encryption of the wireless data stream using a set of predefined keys for all stations.
  - WPA-PSK: WPA with pre-shared key. Provides encryption of the wireless data stream using either TKIP or AES. More secure than WEP.
- WEP Authentication: Sets the type of authentication method to use for WEP.
  - Open system: ?????
  - Shared Key: ?????
- WEP encyrption: Sets the number of bits to use for the WEP key.
- WEP Key 1 to 4: WEP supports up to four keys. Encryption keys can be either 5 (40-bit) or 13 (104-bit) ASCII characters in length. Hexadecimal keys are not supported. To function properly, all wireless stations have identical key lists. If you define only one encryption key, it must be entered in the first key field. If you configure one key only in fields 2, 3, or 4, you may not be able to access your wireless network, even if you have configured your wireless computer card in the same manner.
- WPA Algorithm: Sets the algorithm that is used to generate user-specific keys based on the master WPA key.
- WPA Key: Sets the master WPA key that is used to generate user-specific keys. AES specifies three master key sizes: 128, 192 and 256 bits. TKIP ????

Setting up an ACL

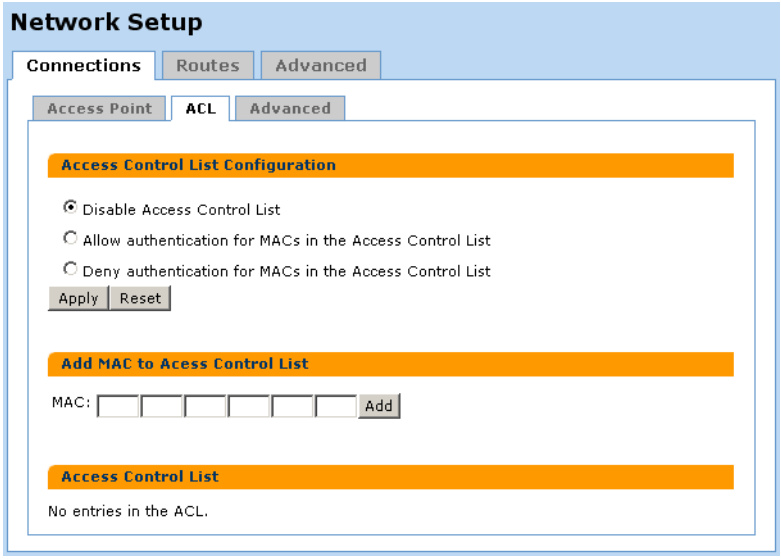
The ACL (access controll list) that enables the Shiva VPN Gateway to permit or deny access to wireless client stations based on their MAC addresses. This is an effective way to protect access to the wireless network.

To activate the ACL:

1 Click **Network Setup** on the main menu.

2. Select **Edit Wireless configuration** in for the Wireless port.

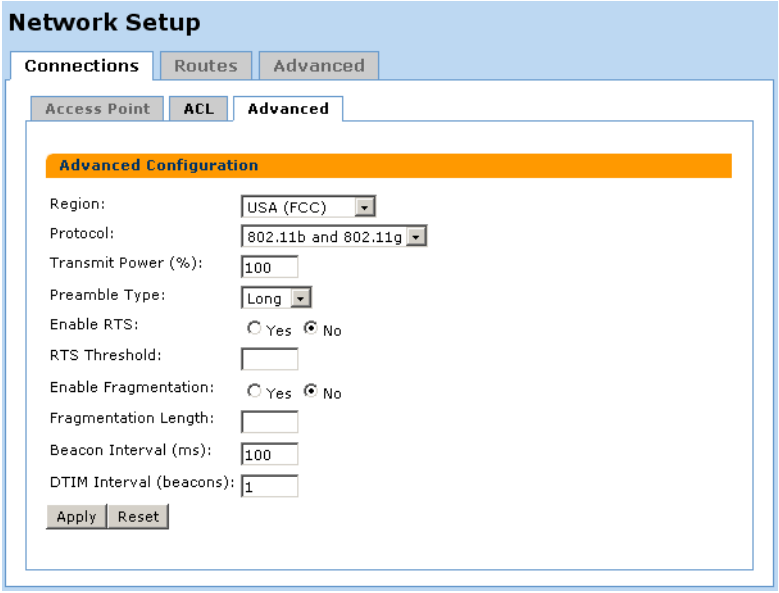
3. Click the ACL tab.



4. Determine if you want to allow or deny access based on MAC addreses and enable the appropriate option.
5. Specify a MAC address and click the **Add** button.

Advanced wireless settings

The Advanced tab gives you access to a number of settings that can be used to fine tune the operation of the wireless network.



Region

Select the geographical region that the Shiva VPN Gateway is operating in.

Protocol

Select the wireless protocol the radio will operate using.

Transmit power

Specifies the transmit power as a percentage. Can be used to reduce the wireleess cell size to avoid interference with neighboring wireless networks.

Peramble Type

???

- Long: ???
- Short: ???

RTS Threshold

???

Enable Fragmentation

???

Fragmentation Length

???

Beacon Interval

???

DTIM Interval

???

Bridging

The Shiva VPN Gateway may be configured as a network bridge. You may bridge between network ports (e.g. Internet - LAN) or enable bridging on a single port (typically LAN) for bridging across a VPN connection.

When bridging has been enabled, a Bridge / br0 port will appear in the Connections menu. It will be allocated the IP address of the port on which bridging was enabled. This IP address will be used primarily for accessing the Shiva VPN Gateway management console, and does not have to be part of the networks that the Shiva VPN Gateway is bridging.

Bridging between network ports

Select Bridged (Internet/LAN) on the two ports to create a bridge between them. The Shiva VPN Gateway will learn which computers or devices are present on either side of the bridge and direct traffic appropriately.

Note: *When the* Shiva VPN Gateway *is bridging between LAN and Internet, it will not be performing NAT/masquerading. computers will typically use an IP address on the network connected to the* Shiva VPN Gateway*'s Internet port as their gateway, rather than the* Shiva VPN Gateway *itself.*

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).

Warning: *The unit may take up to 30 seconds longer than normal to reboot after bridging has been enabled.*

Internet failover

Shiva VPN Gateways are designed with the real Internet in mind, which may mean downtime due to ISP equipment or telecommunications network failure. Failures can be caused by removing the wrong plug from the wall, typing in the wrong ISP password or many other reasons. Regardless of the cause of a failure, it can potentially be very expensive.

When the main Internet connection fails and the backup connection (failover connection) is started, VPN connections are restarted and dynamic DNS services are advised of the new IP address.

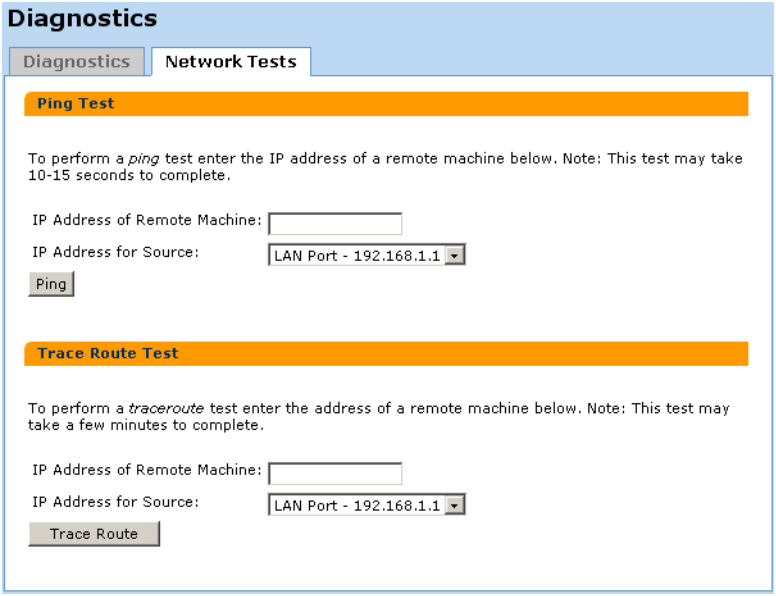
To utilize the failover capabilities of your Shiva VPN Gateway, you must:

- Enable your primary Internet connection for failover.
- Set up a secondary backup Internet connection.

Enable the primary connection for failover

Set up your primary broadband Internet connection as described in the Internet section of this chapter. From the **Connections** menu, select **Edit failover parameters** from the **Configuration** pull down box.

The Shiva VPN Gateway determines whether an Internet connection is up by listening for responses to ping (ICMP echo request) packets sent to a host on the Internet. 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**.



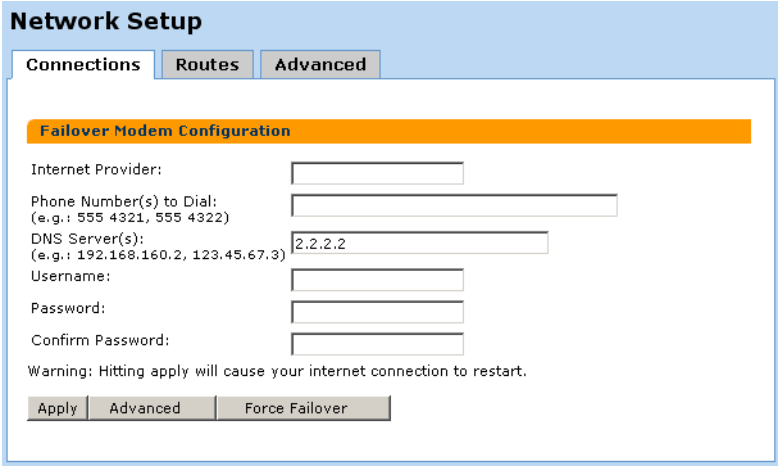
- IP Address of Remote Machine: Enter the IP address of the host.
- IP Address for the Source: Select the port the ping will be sent on.

Set up a secondary backup Internet connection

To switch to a dialout Internet connection when your primary broadband Internet connection is unavailable, from the **Connections** menu select the appropriate Failover Internet configuration for the COM port.

Note: *The Failover Cable/DSL/Direct/Dialout Internet option will not appear as an available Configuration until a primary Internet connection has been configured.*

Refer to “Enable the primary connection for failover” on page 30 for details on enabling your primary broadband Internet connection for failover.



Next, configure the failover connection as you would a normal Internet connection.

- See “Setting up a dial out Internet connection” on page 21 for a description of the fields on the Failover Modem Configuration page.
- See “Internet port settings” on page 18 for a description of how to configure a broadband Internet connection.

Routes

Additional routes

The Additional routes feature allows expert users to add additional static routes for the Shiva VPN Gateway. These routes are additional to those created automatically by the Shiva VPN Gateway configuration scripts.

Route management

Your Shiva VPN Gateway can be configured to automatically exchange routing information with other routers. Note that this feature is intended for network administrators adept at configuring route management services.

Check **Enable route management**, select the Protocol you wish to use to exchange routes and click **Apply**. Once enabled, the routing manager can be configured by editing zebra.conf and protocold.conf (e.g. bgpd.conf) through **Advanced > Configuration Files**.

For more information on configuring route management, refer to: http://www.zebra.org/

Interface aliases

Interface aliases allow the Shiva VPN Gateway to respond to multiple IP addresses on its LAN and Internet ports.

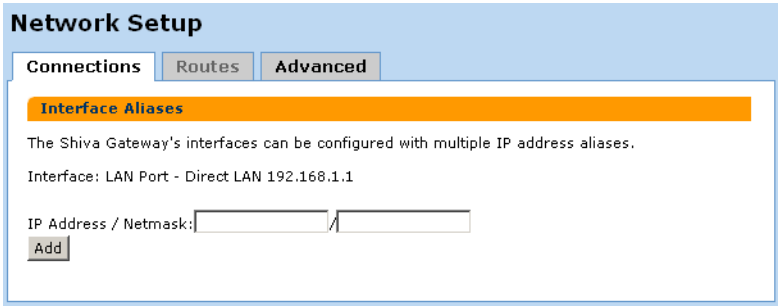
LAN port alias

To define a LAN port interface alias, do the following:

1 Click **Network Setup**.

2. Select **Edit alias configuration** for the LAN port.

3. Specify an **IP address** and **Netmask** and click **Add**.



Internet port alias

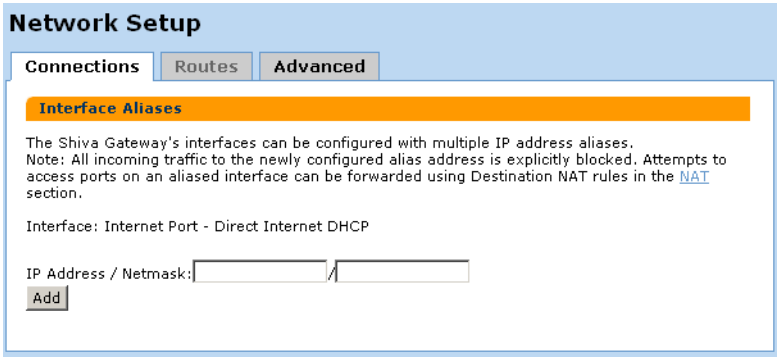
Note: *For Internet aliased ports, you must also setup appropriate Packet Filtering and/or Port forwarding rules to allow traffic on these ports to be passed onto the local network.*

To define an Internet port interface alias, do the following:

1 Click **Network Setup**.

2. Select **Edit alias configuration** for the Internet port.

3. Specify an **IP address** and **Netmask** and click **Add**.



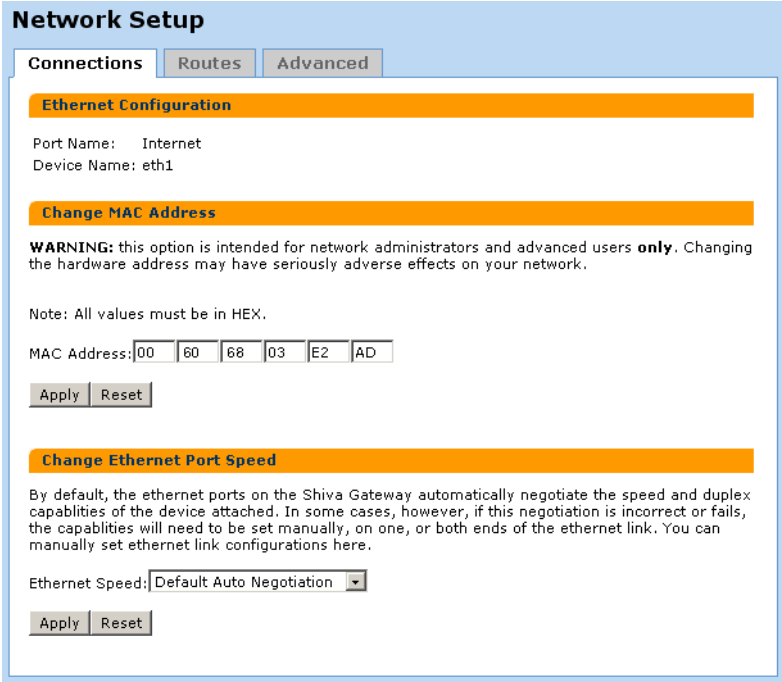
Changing the MAC address

On rare occasions it may be necessary to change the Ethernet hardware or MAC Address of your Shiva VPN Gateway's Internet port. The MAC address is a globally unique address and is specific to a single Shiva VPN Gateway. 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.

To change the MAC address:

1 Click **Network Setup**.

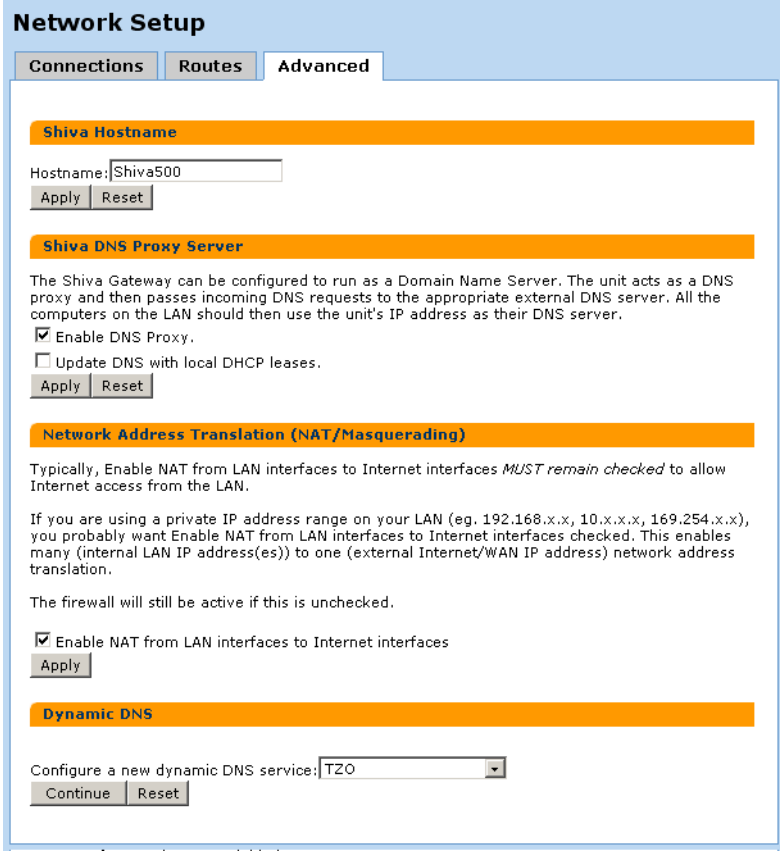
2. Select **Edit Ethernet configuration** for the **Internet** port.



3. Specify the new **MAC address** and click **Apply**.

Advanced network settings

The following figure shows the options available on the **Network Setup > Advanced** tab.



Hostname

The Hostname is a descriptive name for the Shiva VPN Gateway on the network.

DNS Proxy

The Shiva VPN Gateway can also be configured to run as a Domain Name Server. The Shiva VPN Gateway acts as a DNS Proxy and passes incoming DNS requests to the appropriate external DNS server. If this is enabled, all the computers on the LAN should specify the IP address of the Shiva VPN Gateway as their DNS server.

Network address translation (NAT/masquerading)

The Shiva VPN Gateway can utilize IP Masquerading (a simple form of Network Address Translation, or NAT) where computers on the local network effectively share a single external IP address. Masquerading allows insiders to get out, without allowing outsiders in. By default, the Internet port is setup to masquerade.

Masquerading has the following advantages:

- Added security because machines outside the local network only know the gateway address.
- 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.

Note: *It is strongly recommended that you leave Enable NAT on Internet Interface checked.*

Dynamic DNS

A dynamic DNS service is useful when you don't have a static Internet IP address, but need to remain contactable by hosts on the Internet. Dynamic DNS service providers such as TZO.com and dyndns.org can register an Internet domain name that will point to your Internet IP address no matter how often it changes.

Whenever its Internet IP address changes, the Shiva VPN Gateway will alert the dynamic DNS service provider so the domain name records can be updated appropriately.

First, create an account with the dynamic DNS service provider of your choice.

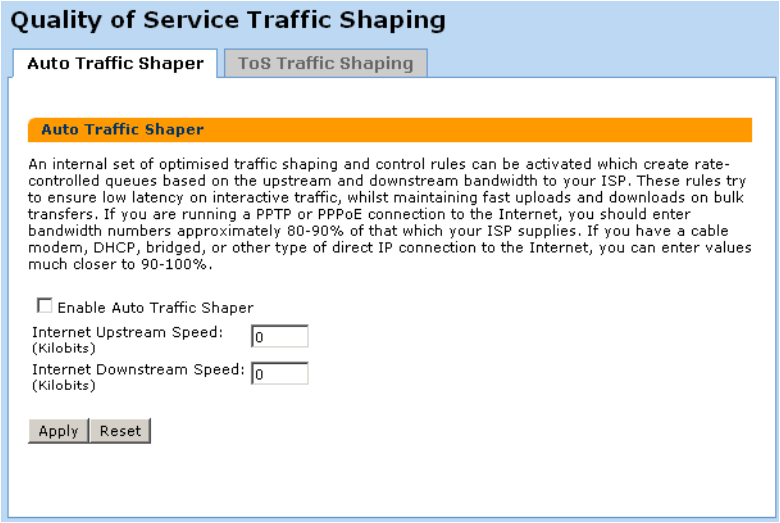
Next, select your chosen Dynamic DNS service and click **Continue**. Select which interface/connection's IP address you want associated with your newly created DNS name from Internet Connection. Enter the details provided by your dynamic DNS service provider and click **Apply** to enable.

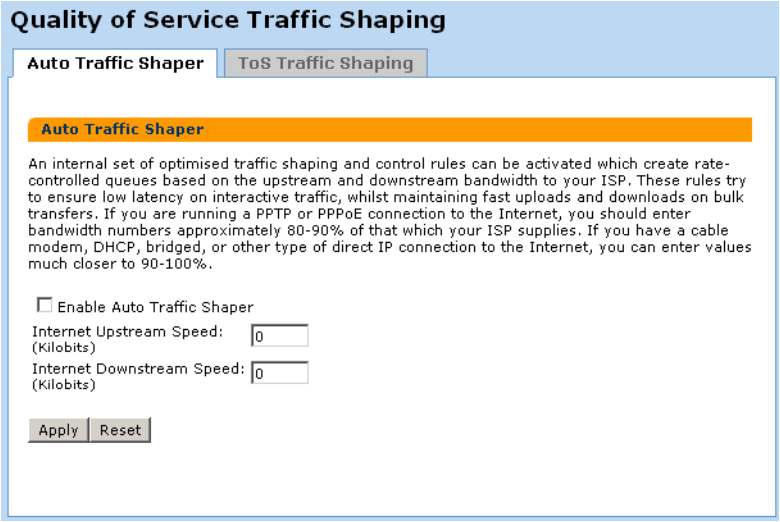
QoS traffic shaping

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

This advanced feature is provided for expert users to fine tune their networks. 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. The Upstream and Downstream Speed should. 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.

The following option are supported:





Chapter 3

DHCP services

The Shiva VPN Gateway can act as a DHCP server for machines on your local network. To configure your Shiva VPN Gateway as a DHCP server, you must set a static IP address and netmask on the LAN port.

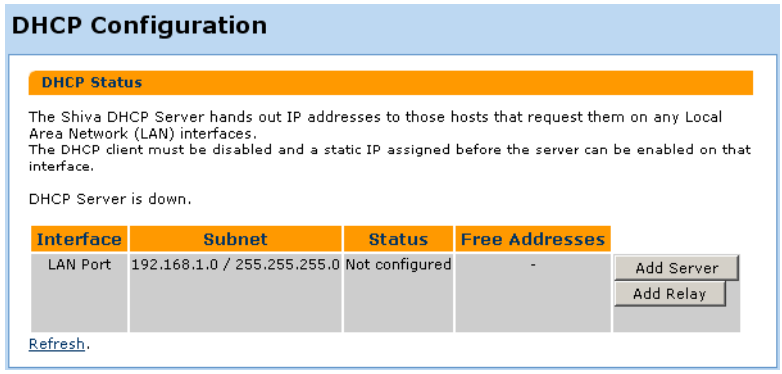
DHCP server configuration

The DHCP server allows the automatic distribution of IP, gateway, DNS and WINS addresses to hosts running DHCP clients on the LAN ports.

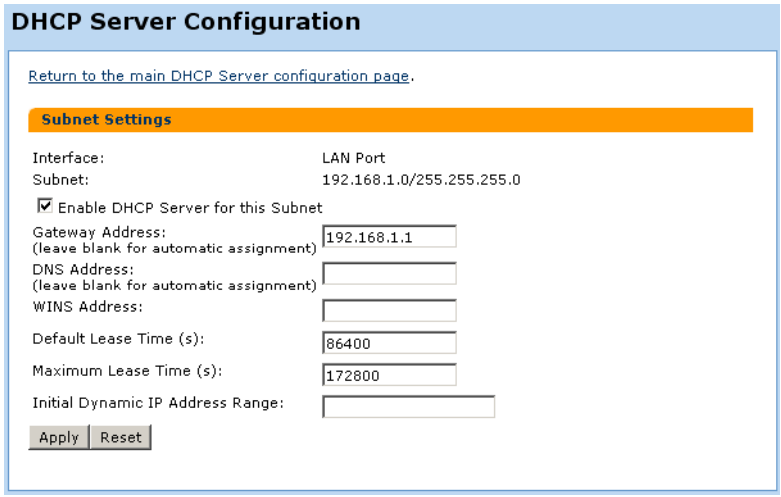
To configure the DHCP server

1 Click the **DHCP Server** link in the **Networking** section of the menu bar.

2. Click **Add Server**.



3. Configure the DHCP server settings and click **Apply**.

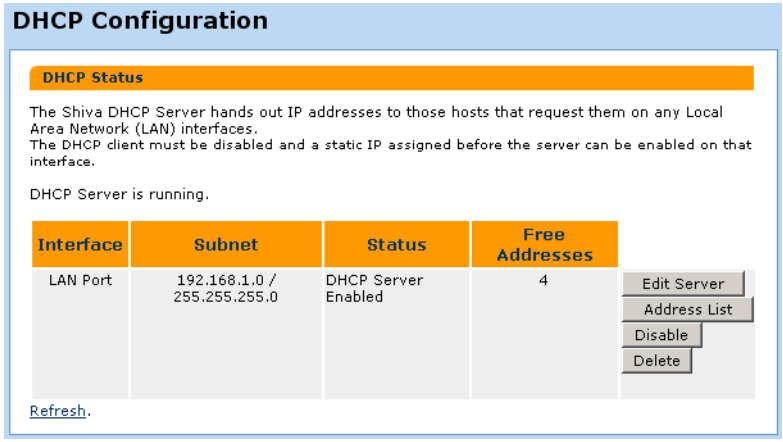


- Enter the **Subnet** and netmask of the IP addresses to be distributed.
- Enter the **Gateway Address** that the DHCP clients will be issued with. If this field is left blank, the Shiva VPN Gateway's IP address will be used.
- Enter the **DNS Address** that the DHCP clients will be issued with. If this field is left blank, the Shiva VPN Gateway's IP address will be used. Leave this field blank for automatic DNS server assignment. If your Shiva VPN Gateway is configured for DNS masquerading, you should either leave this field blank, or enter the IP address of the LAN port of the Shiva VPN Gateway.

- 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.
- Enter the IP address or range of IP addresses to be issued to DHCP clients in the **Initial Dynamic IP Address Range** field.

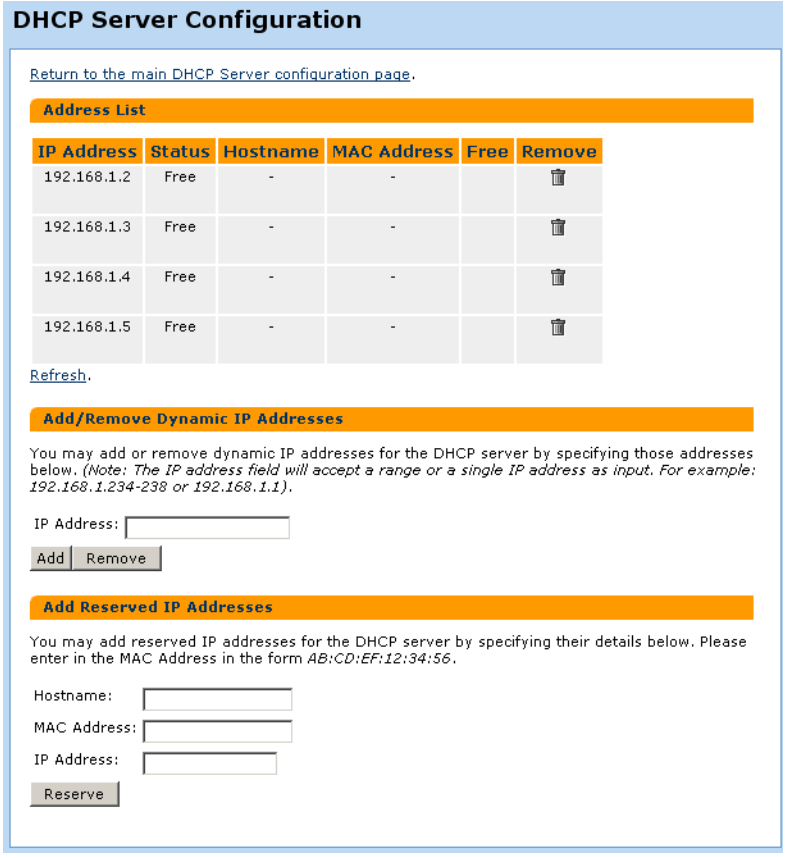
To take advantage of the Shiva VPN Gateway's DHCP server functionality, you should configure the other machines on your local network to get their IP addresses dynamically from the Shiva VPN Gateway. Please refer the documentation for the other machines for instructions on how to configure the local network port.

4. Click **Apply** to save these settings. A page similar to the following will be displayed.



- Interface: Once a subnet has been configured, the port which the IP addresses will be issued from will be shown in the Interface field.
- Subnet: The value shown in this field is the subnet for which the IP addresses distributed will use.
- Free Addresses: This field will contain 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.
- Enable/Disable: Each subnet can be enabled or disabled by clicking on the Enable or Disable button under the Enable/Disable heading.
- Edit: The settings for each subnet can be modified by clicking the Edit button. You will also have the option to add more IP addresses that can be handed out and add reserved IP addresses as well.
- Delete: The settings for the subnet can be removed by clicking the Delete button.

- Address List: Click this button to display a page similar to the following.



DHCP Server Configuration

Return to the main DHCP Server configuration page.

Address List

IP Address	Status	Hostname	MAC Address	Free	Remove
192.168.1.2	Free	-	-		
192.168.1.3	Free	-	-		
192.168.1.4	Free	-	-		
192.168.1.5	Free	-	-		

Refresh.

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: 192.168.1.234-238 or 192.168.1.1).*

IP Address:

Add Remove

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:

Reserve

For each IP address that the DHCP server services, the Status, Hostname, MAC Address will be shown. There is also be an option to Remove the address and for reserved IP addresses, the added option to Unreserve the address. Unreserving the address will allow it to be handed out to any host. The Status field will have three possible states. These include:

- 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.

DHCP relay

The DHCP proxy allows the Shiva VPN Gateway 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 Shiva VPN Gateway's LAN. Then check Enable DHCP Relay and click Apply.

Chapter 4

Firewall

The Shiva VPN Gateway is equipped with a fully featured, stateful firewall. The firewall allows you to control both incoming and outgoing access, so that computers on the LAN can have tailored Internet access facilities and are shielded from malicious attacks. By default the firewall is active, and allows all outgoing connections and blocks all incoming connections.

The Shiva VPN Gateway's stateful firewall keeps track of outgoing connections (e.g. a computer 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 computer).

Sometimes it may be useful to allow some incoming connections, e.g. if you have a mail or web server on your LAN that you want to be accessible from the Internet. These situations are catered for by configuring Packet Filtering rules.

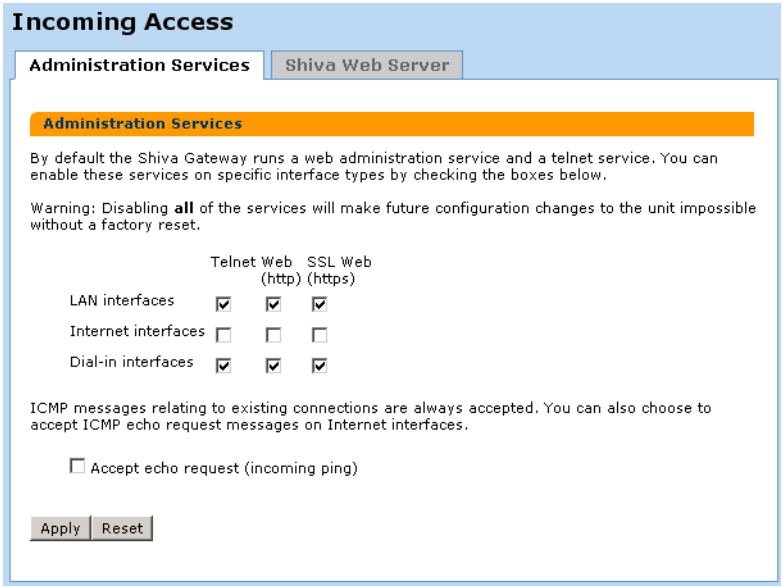
Generally, the majority of customizations to the default firewall rule set will be done through Packet Filtering (page 49).

Incoming access

The Incoming Access section allows you to control access to the Shiva VPN Gateway itself, e.g. for remote administration. Click **Incoming Access** on the **Firewall** menu to show the Incoming Access configuration page which has two tabs: Administration Services and Shiva Web Server.

Administration services

The following figure shows the Administration Services page:



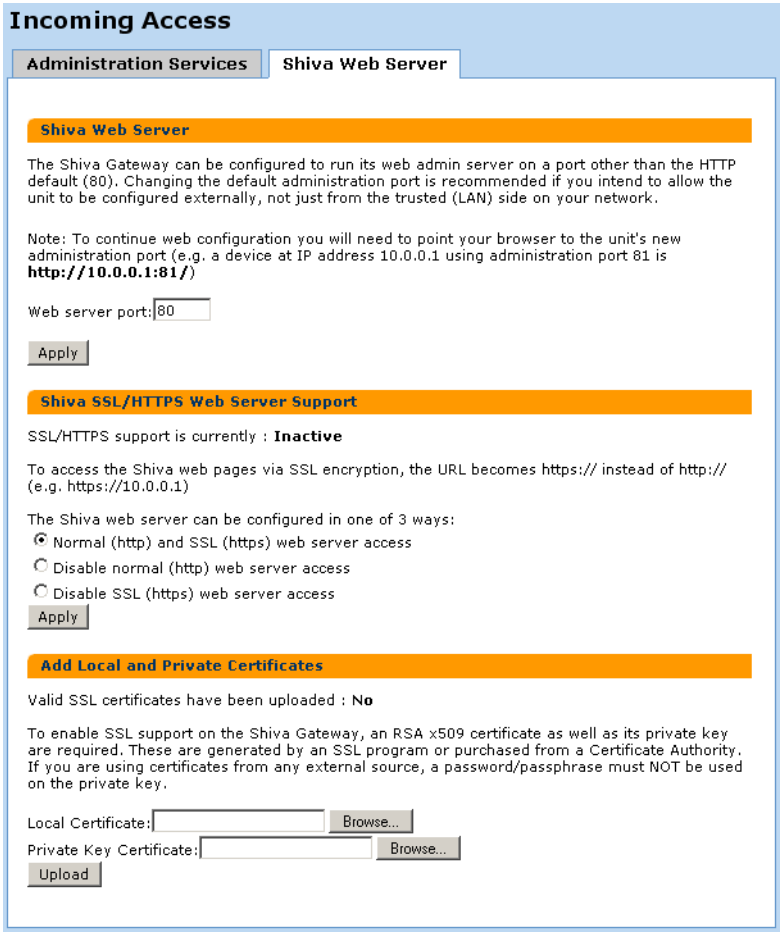
By default the Shiva VPN Gateway runs a web administration server and a telnet service. Access to these services can be restricted to specific interfaces. For example, you generally want to restrict access to the Web Management Console web administration pages (Web Admin) to machines on your local network. Disallowing all services is not recommended, as this will make future configuration changes impossible unless your Shiva VPN Gateway is reset to the factory default settings.

Warning: *If you do want to allow administrative access on interfaces other than the LAN, there are several security precautions you should take. See the note in the next section for details.*

You can also select to accept ICMP messages on the Internet port. For example, if you disallow echo requests (the default for increased security), your Shiva VPN Gateway will not respond to pings on its Internet port. Destination unreachable ICMP messages are always accepted.

Shiva web server

Clicking the Shiva VPN Gateway Web Server tab takes you to the page to configure the administrative web server. This web server is responsible for running the web-based management console.



Note: *Changing the web server port number is strongly recommended if you are allowing Internet access to the management console. This will help hide the Management Console from casual web surfers who type your Shiva VPN Gateway's Internet IP address into a web browser. Ideally, you should use Packet Filtering 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).*

The web-based management console is usually accessed 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 will be similar to: http://192.168.1.1:88

SSL/HTTPS web server support

Once valid SSL certificates have been uploaded, the Shiva VPN Gateway administrative web server can operate in one of one of 3 different modes.

- Both normal and SSL web access (both HTTP/HTTPS).
- Disable normal access (HTTPS only).
- Disable SSL access (HTTP only).

To access the web-based management console administrative web pages securely using SSL encryption, the URL becomes https:// instead of http:// (e.g. https://10.0.0.1).

Add local and private certificates

Valid SSL certificates have been uploaded indicates whether valid certificates are present on the Shiva VPN Gateway (Yes/No).

If you have purchased or created SSL certificates for a web server, you can upload them to the Shiva VPN Gateway by clicking Upload.

Alternately, you can create self-signed certificates internally on the Shiva VPN Gateway by following the link to the SSL Certificate page.

Packet filtering

By default, your Shiva VPN Gateway allows network traffic as follows:

Incoming Interface	Outgoing Interface	Action
LAN/VPN/Dial-In	Any	Accept
WAN	Any	Drop

You can configure your Shiva VPN Gateway with additional filter rules to allow or restrict network traffic. These rules can match traffic based on the source and destination address, the incoming and outgoing network port, and/or the services.

You can also configure your Shiva VPN Gateway to perform network address translation (NAT). This may be in the form of source address NAT, destination address NAT, or 1-to-1 NAT. Network address translation modifies the IP address and/or port of traffic traversing the Shiva VPN Gateway.

The most common use of this is for port forwarding (aka PAT/Port Address Translation) from ports on the Shiva VPN Gateway's WAN interface to ports on machines on the LAN. This is the most common way for internal, masqueraded servers to offer services to the outside world. Destination NAT rules are used for port forwarding.

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 Shiva VPN Gateway to masquerade your private network behind its public IP address.

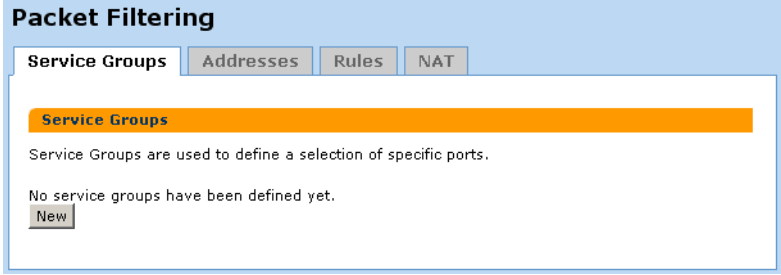
1-to-1 NAT creates both Destination NAT and Source NAT rules for full IP address translation in both directions. This can be useful if you have a range of IP addresses that have been added as interface aliases on the Shiva VPN Gateway's WAN interface, and want to associate one of these external alias 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.

Function	NAT Method
Port forwarding (PAT)	Destination NAT
Masquerading	Source NAT
Virtual DMZ	1-to-1 NAT

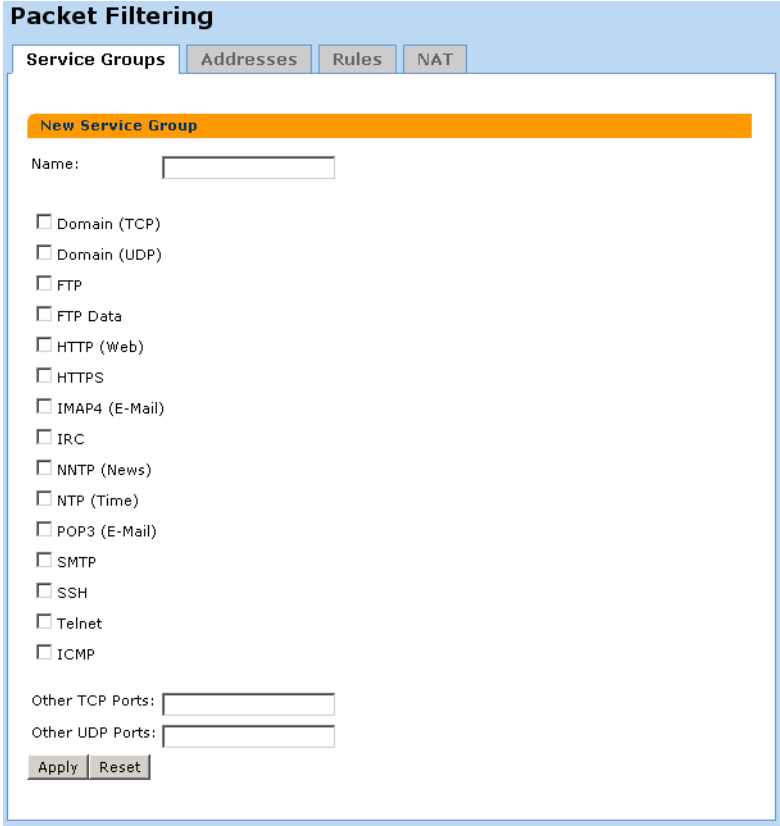
Before configuring a filter or NAT rule, you need to define the addresses and service groups.

Service groups

Click the **Service Groups** tab. Any groups that have already been defined are displayed.



Click **New** to add a new service groups, or select an existing address and click **Modify**.

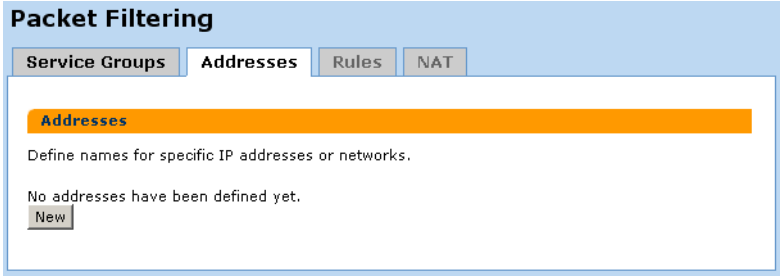


A service group can be used to group together similar services. For example, you can create a group of services that you wish to allow, and then use a single rule to allow them all at once. Select the services from the list of predefined services, or enter the port number to define a custom TCP or UDP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

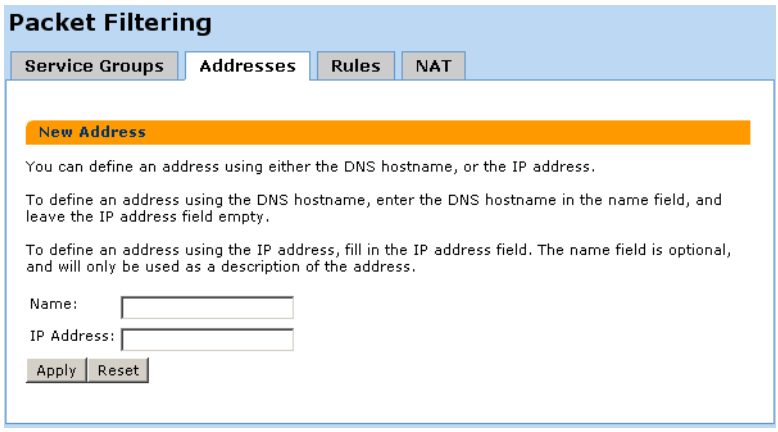
Addresses

This tab enables you to define the address aliases that must be created for any internal server to map services to such as FTP, HTTP.

Any addresses that have already been defined will be displayed.



Click **New** to add a new address, or select an existing address and click **Modify**. There is no need to add addresses for the Shiva VPN Gateway's interfaces, these are predefined.



You can define an address using either the DNS hostname, or the IP address.

To define an address using the DNS hostname, enter the DNS hostname in the Name field, and leave the IP Address field empty. The Shiva VPN Gateway will perform a DNS lookup, and fill in the IP Address field. If the DNS hostname is invalid, you may need to wait while the DNS lookup times out.

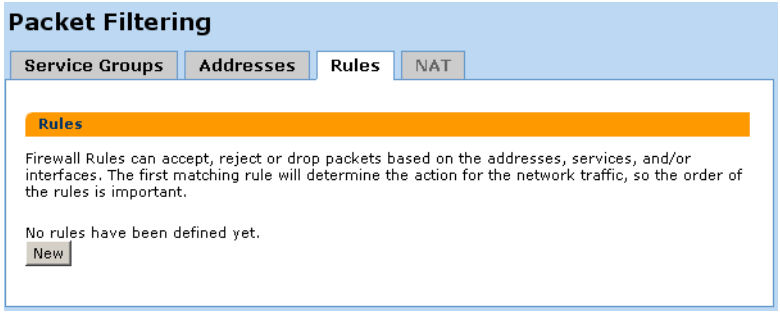
Warning: *The DNS lookup is only performed once, when you enter it. If the IP address corresponding to the DNS hostname ever changes, you will need to delete the IP address to force the Shiva VPN Gateway to perform another DNS lookup. This means that this option is not suitable for use with dynamic DNS.*

Additionally, some DNS hostnames resolve to several IP addresses (e.g. www.cnn.com). In this case, you must create an address entry and rule for each of these IP addresses.

To define an address using the IP address, fill in the IP Address field. The Name field is optional, and will only be used as a description of the address. Entering a description will make the rules easier to read.

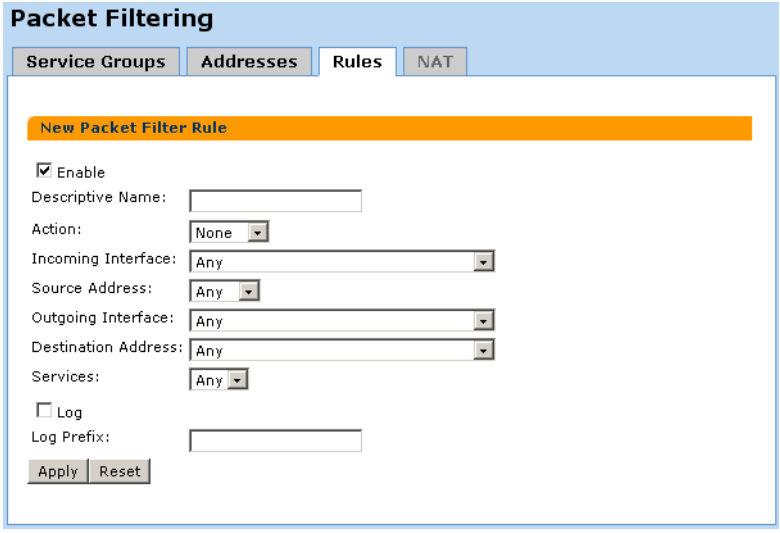
Rules

Once addresses and services have been defined, you can create filter rules. Click **Rules**. Any rules that have already been defined will be displayed.



Click **New** to add a new filter rule, or select an existing rule and click **Modify**.

Note: *The first matching rule will determine the action for the network traffic, so the order of the rules is important. You can use the buttons on the Packet Filtering page to change the order. The rules are evaluated top to bottom as displayed on the Packet Filtering page.*



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. It can also be used to temporarily disable a rule.

Incoming Interface

The interface/network port that the Shiva VPN Gateway received the network traffic on.

Source Address

Always set to **Any**.

Outgoing Interface

The interface/network port that the Shiva VPN Gateway will route the network traffic out. None will match network traffic that is destined for the Shiva VPN Gateway itself. This is useful for controlling access to services provided by the Shiva VPN Gateway, such as the Web Management Console.

Destination address

Always set to **Any**.

Log option

Controls whether to log the first packet of the connection. You may enter a Log Prefix to make it easier to identify which rules are being matched when inspecting the system log.

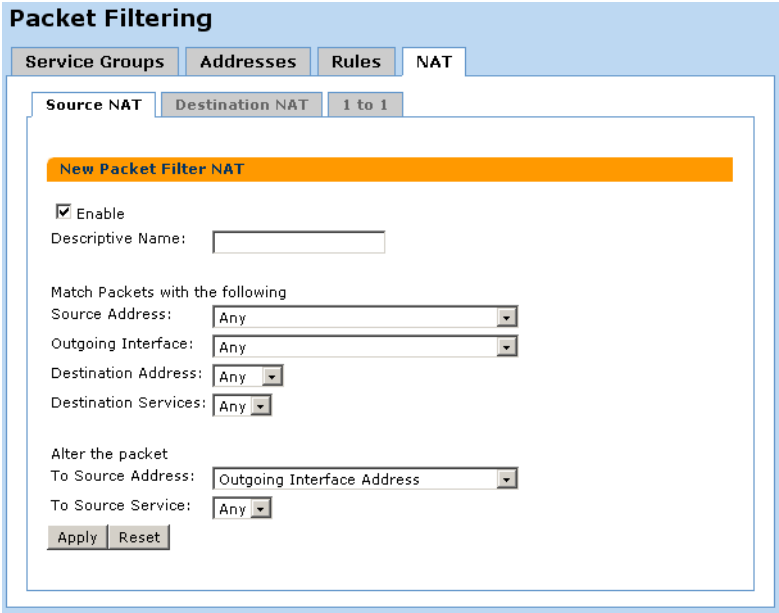
NAT

Once appropriate addresses (and perhaps service groups) have been defined, you can add 1-to-1 and Destination NAT rules. Source NAT rules may be added at any time, as these may apply solely between the interfaces of the Shiva VPN Gateway itself.

By default, the Shiva VPN Gateway performs Source NAT on traffic where the incoming interface is LAN and the outgoing interface is WAN. See the Advanced section of the chapter entitled Network Connections for information on configuring the basic masquerading (Source NAT) relationships between your Shiva VPN Gateway's interfaces.

Source NAT

Source NAT alters the source address and optionally the source port of packets received by the Shiva VPN Gateway. This is typically used for masquerading.



You can use the Source NAT functionality of Packet Filtering to tweak your Shiva VPN Gateway's masquerading behavior.

See “Network address translation (NAT/masquerading)” on page 36 for information on configuring the basic masquerading (Source NAT) relationships between your Shiva VPN Gateway's interfaces.

Enable

Uncheck to temporarily disable this rule

Descriptive Name

An arbitrary name for this rule.

Match Packets with the following

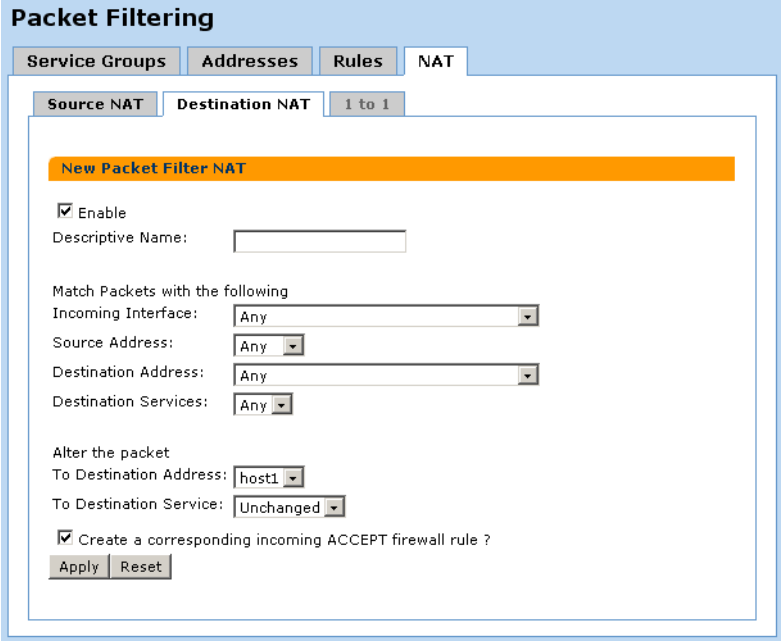
- Source Address: The address from which the request originated (for masquerading this will typically be a private LAN or DMZ address)
- Outgoing Interface: The interface that receives the request (for masquerading this will typically be private interface, i.e. LAN or DMZ)
- Destination Address: The destination address of the request
- Destination Services: The destination service(s) (port(s)) of the request

After the packet

- To Source Address: The address to replace the Source Address (for masquerading this will typically be a public address of the Shiva VPN Gateway, i.e. WAN/Internet)
- To Source Service: The service to replace Source Services, this need not be the same as the Source Service used to match the packet, but often will be

Destination NAT/port forwarding

Destination NAT alters the destination address and optionally the destination port of packets received by the Shiva VPN Gateway. Typically this is used for port forwarding.



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 Shiva VPN Gateway's interfaces (typically the WAN interface) to a machine on your LAN, which services the request.

Enable

Uncheck to temporarily disable this rule

Descriptive Name

An arbitrary name for this rule.

Match Packets with the following

- Incoming Interface: The interface that receives the request (for port forwarding will typically be set to WAN/Internet)
- 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)
- Destination Address: The destination address of the request, this is the address that will be altered
- Destination Services: The destination service(s) (port(s)) of the request, many public ports may be forwarded to a single internal port

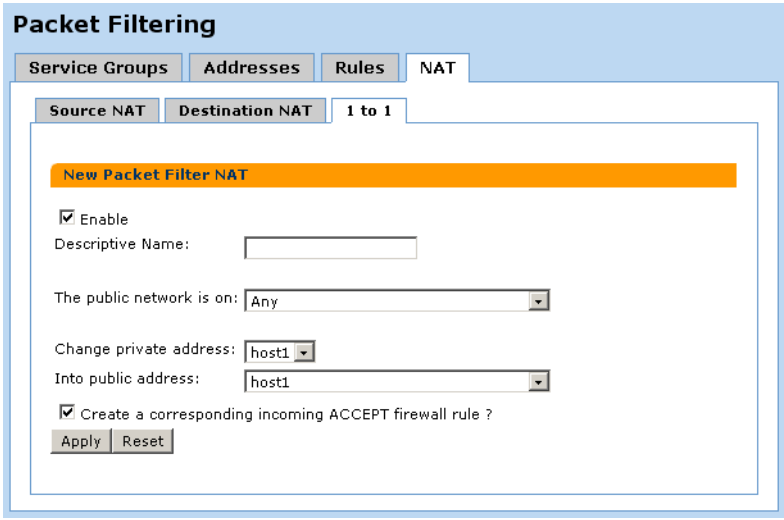
After the packet

- To Destination Address: The address to replace the Destination Address (for port forwarding this will typically be the private address of an internal machine)
- To Destination Service: The address to replace Destination Services, this need not be the same as the Destination Service used to match the packet, but often will be

Generally leave Create a corresponding ACCEPT firewall rule checked unless you want to manually create a more restrictive filter rule through Rules.

1-to-1 NAT

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



Enable

Uncheck to temporarily disable this rule.

Descriptive Name

An arbitrary name for this rule.

The public network is on

Select the interface on which the public address resides, this will typically be a WAN or Internet port.

Change private address

The private address to change.

Into public address

The public address, typically a WAN interface alias.

Create a corresponding ACCEPT firewall rule

Leave checked to create a virtual DMZ type scenario, where the machine at the private address will be effectively unfirewalled.

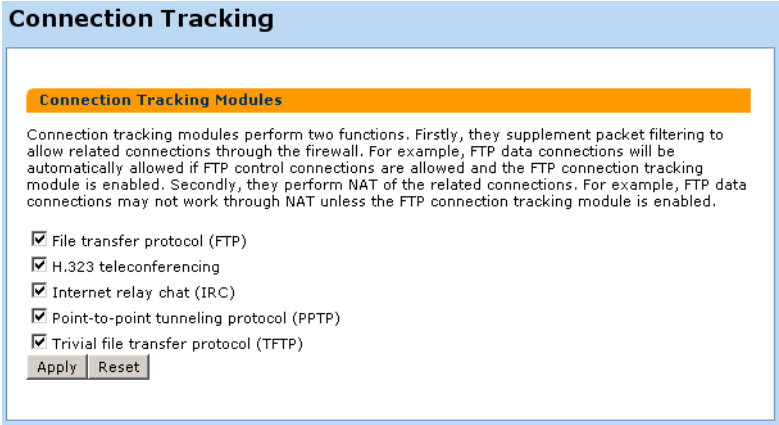
Warning: *Leaving Create a corresponding ACCEPT firewall rule will allow all traffic into and out from the specified private address, i.e. the private address will no longer be shielded by your Shiva VPN Gateway's firewall.*

Connection tracking

Connection tracking provides support for the listed services by creating a proxy for the service.

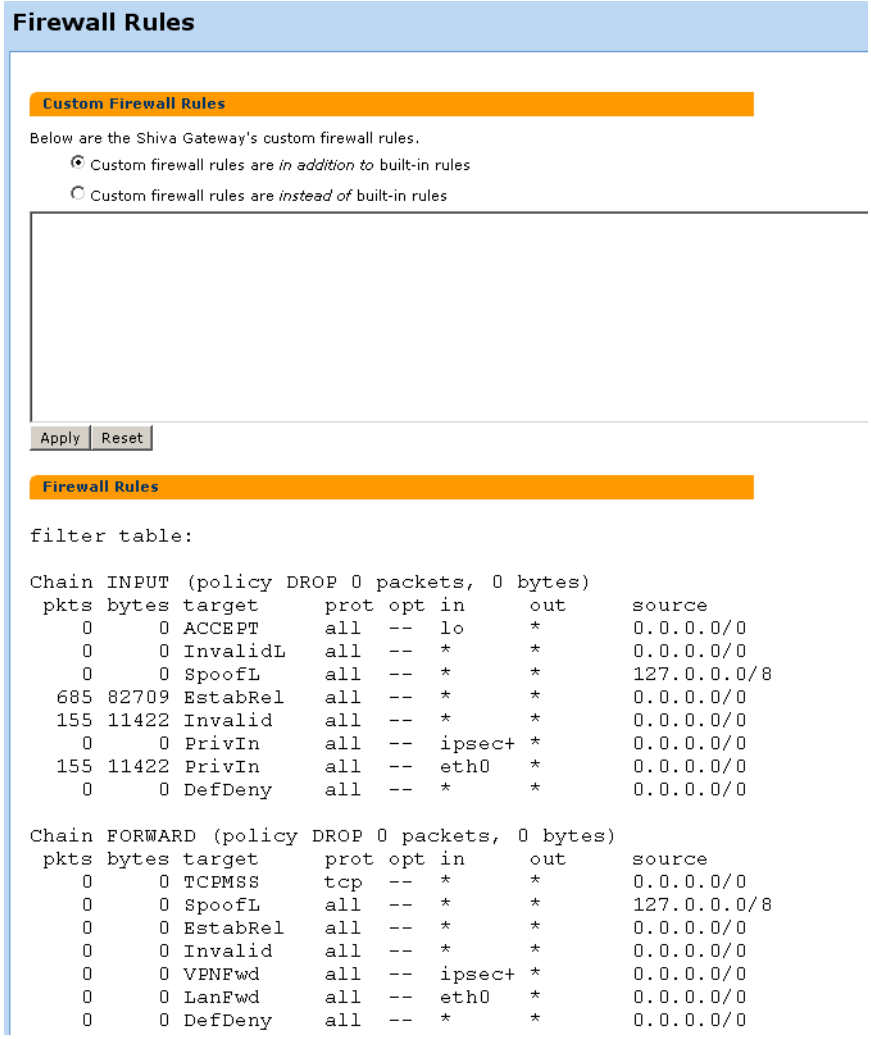
Supported services include:

- File transfer protocol (FTP)
- H.323 teleconferencing
- Internet relay chat (IRC)
- Point-to-point tunneling protocol (PPTP)
- Trivial file transfer protocol (TFTP)



Rules

The Rules configuration page allows firewall experts to view the current firewall rules and add custom iptables firewall rules. To access this page, click **Rules** in the **Firewall** menu.



Warning: *Only experts on firewalls and iptables will be able to add effective custom firewall rules (for more information see http://www.netfilter.org/documentation/).*

Configuring the Shiva VPN Gateway's firewall via the Incoming Access and Outgoing Access and Packet Filtering configuration pages is adequate for most applications.

Refer to “Creating custom log rules” on page 113 for details on creating log rules using iptables.

Intrusion detection

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 behavior 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 using an intrusion detection system (IDS). The IDS logs information and sends alerts, so that administrators may be able to contain and recover from any harm caused.

Setting up intrusion detection and blocking

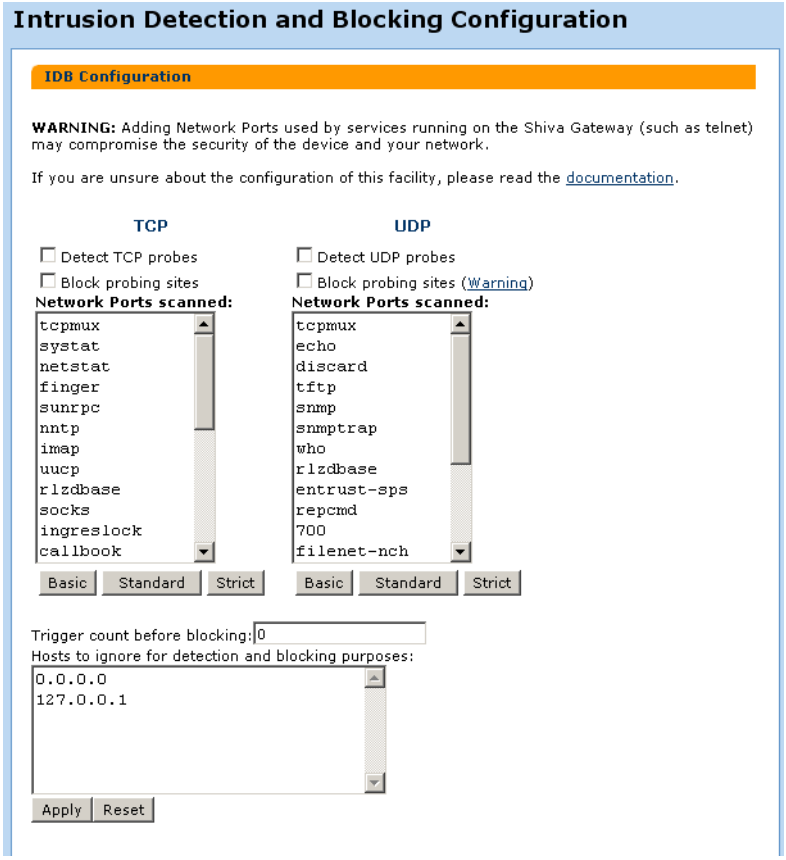
IDB operates by offering a number of services to the outside world that are monitored for connection attempts. Remote machines attempting to connect to these services generate a system log entry providing details of the access attempt, and the access attempt is denied.

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.

Several 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 Shiva unit (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.*

The following figure shows the Intrusion Detection and Blocking (IDB) configuration page:



The trigger count 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 (o 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 will reduce the number of false positives.

The ignore list contains a list of host IP addresses which the IDB will ignore for detection and blocking purposes. 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.

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 will significantly reduce this risk.*

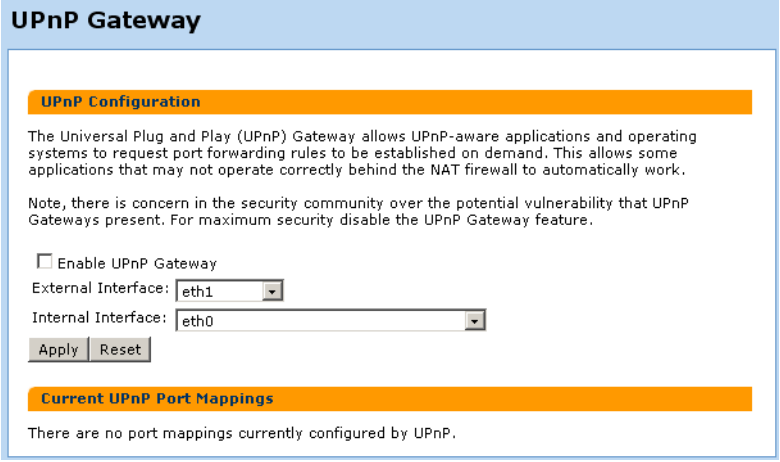
Universal plug and play gateway

The Universal Plug and Play (UPnP) Gateway allows UPnP capable applications and devices to request port forwarding rules to be established on demand. This allows some applications and devices that may not operate correctly behind the NAT firewall to automatically work.

Warning: *There is concern in the security community over the potential vulnerability that UPnP gateways present. For maximum security disable the UPnP Gateway feature.*

Configuring the UPnP gateway

The UPnP Gateway needs to be run on a pair of interfaces, the external interface and the internal interface.



The UPnP Gateway will send out notifications on the internal interface, advertising its presence on the network. Any UPnP capable applications or devices that you require to make use of the UPnP Gateway need to be connected to the Shiva VPN Gateway via this interface. The UPnP Gateway will listen on this interface to requests from UPnP capable applications and devices to establish port forwarding rules.

In response to these requests, the UPnP Gateway will establish port forwarding rules to allow matching packets to be forwarded from the configured external interface through to the internal interface.

Note: *The port forwarding rules set up via the UPnP Gateway are temporary. Power cycling the Shiva VPN Gateway will clear the list of configured UPnP port forwarding rules, as will the event of either the internal or external interfaces becoming unavailable.*

The UPnP Gateway is intended for transitory application port forwarding, such as those established by some versions of Microsoft Messenger for file transfers. For long term port forwarding, we recommend configuring the necessary rules via the Destination NAT features in Packet Filtering.

Should there be a conflict, rules established via Packet Filtering will have priority over those established via the UPnP Gateway.

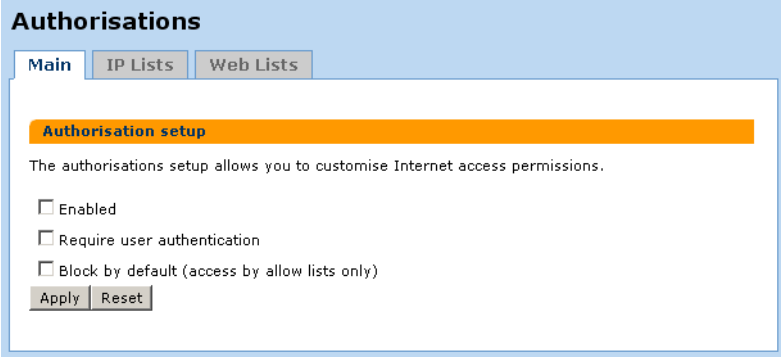
Otherwise, you may manually create filter rules through Rules.

Access control

Inappropriate Internet use during work hours can have a serious effect on productivity. With the Shiva VPN Gateway Access Control web proxy, you can 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).

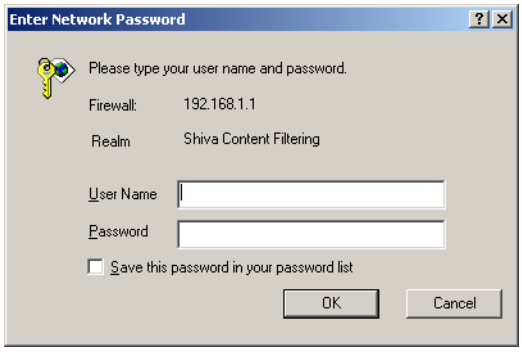
Additionally, you can set up global block/allow lists for web sites that you always want to be accessible/inaccessible (Web Lists), or force users to have a personal firewall installed before accessing the Internet (ZoneAlarm).

To enable any of these access controls or content filtering, select **Access Control**, then under the **Main** tab check **Enabled** and click **Apply**.



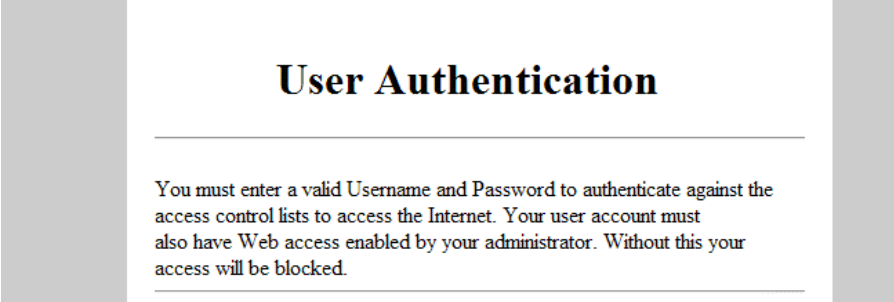
User authentication

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 will display a dialog similar to the following:



Web proxy user accounts are added and removed through **Users** under the **System** menu. Web proxy users should generally have only Internet Access (via. Access Controls) checked, with all other access permissions unchecked. See “User list” on page 104 for further details on adding user accounts.

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



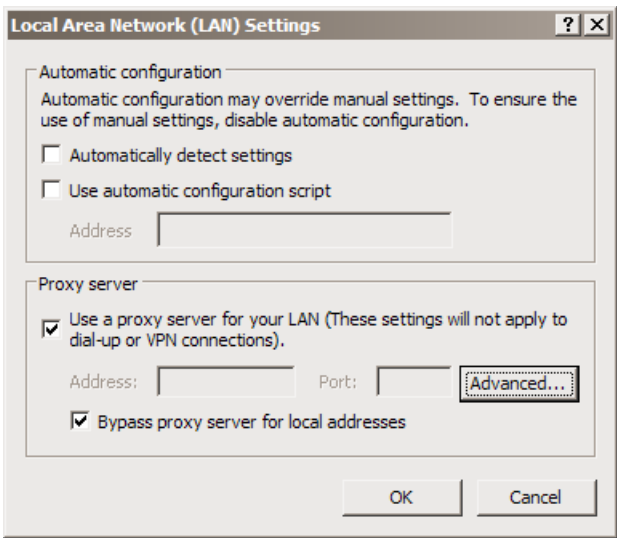
Note: *Each browser on the LAN will now have to be set up to use the Shiva VPN Gateway's web proxy.*

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.

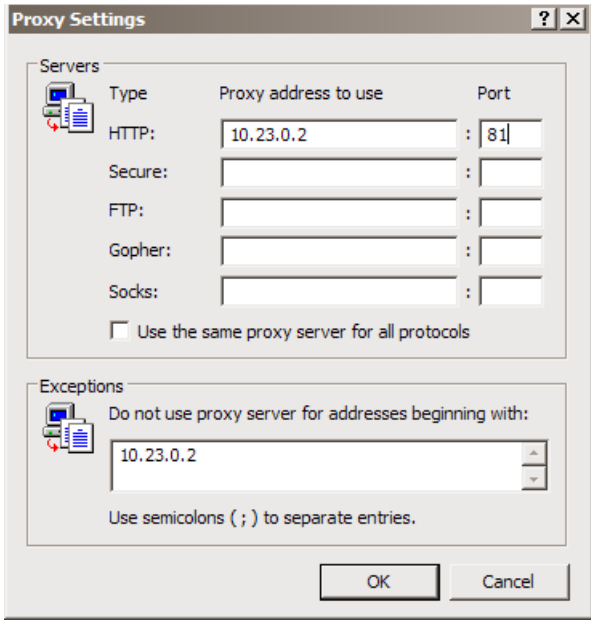
1 On the **Internet Options** menu, select **Tools**.

2. On the **Connections** tab, click the **LAN Settings** button.



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

4. Click **Advanced**.



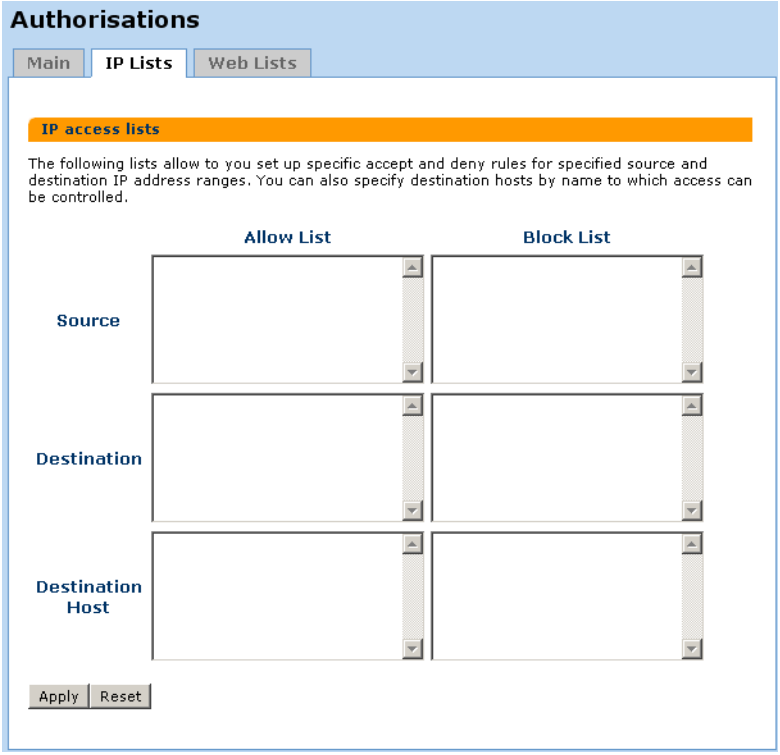
5. In the row labeled **HTTP**, enter your Shiva VPN Gateway's LAN IP address in the **Proxy address to use** column, and **81** in the **Port** column. Leave the other rows blank.
6. In the **Exceptions** box, enter your Shiva VPN Gateway's LAN IP address.
7. Click **OK**, **OK,** and **OK** again.

IP lists

Internet 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. See Appendix A for more information on IP address ranges.

Note: *All Internet traffic, not just web traffic, is affected by the IP Lists.*

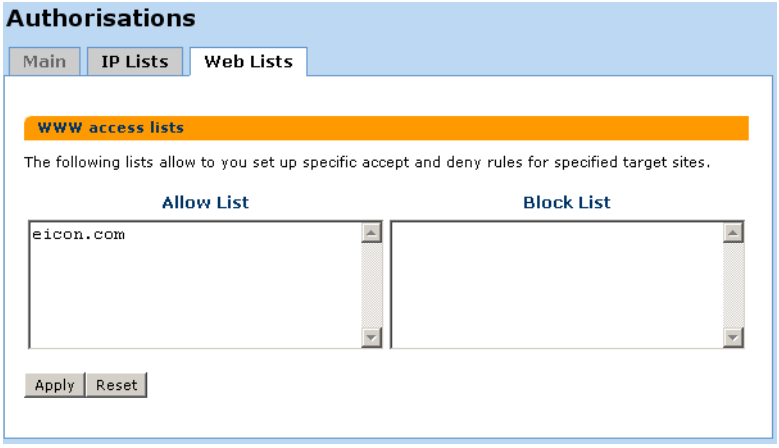
Allow entries have preference over Block entries, e.g. if www.kernel.org is in the Destination Host Allow list and 192.168.1.100 is in the Source Block list, access to www.kernel.org (and www.kernel.org only) from 192.168.1.100 will be granted.



Web lists

Access will be denied to any web address (URL) that contains text entered in the **Block List**, e.g. entering xxx will block any URL containing xxx, including http://xxx.example.com or www.test.com/xxx/index.html.

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



Chapter 5

Virtual private networking

This chapter details how to configure the PPTP client, how to establish an IPSec tunnel, and also provides an overview of GRE and L2TP VPN tunneling.

Overview

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:

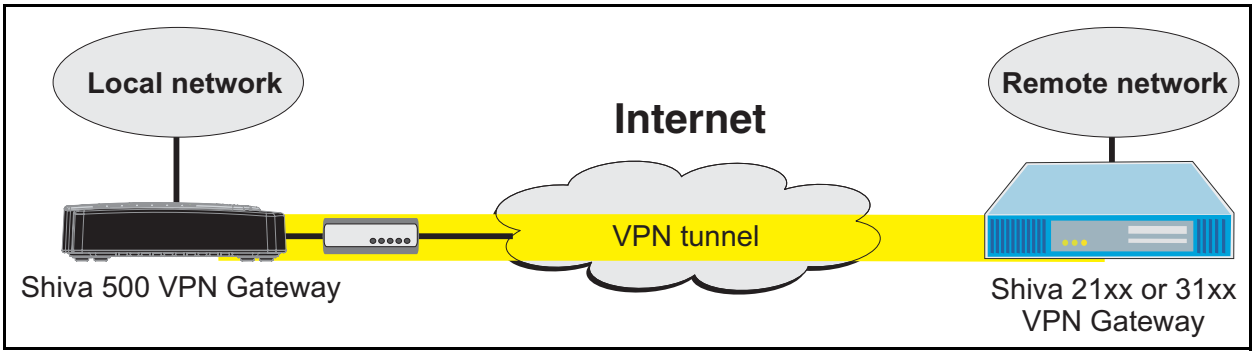
- Privacy - no one else can see what you are communicating
- Authentication - you know who you are communicating with
- Integrity - no one else can tamper with your messages/data

Using VPN, you can access the office network securely across the Internet using Point-to-Point Tunneling Protocol (PPTP), IPSec, GRE 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 Shiva VPN Gateway you can establish a VPN tunnel over the Internet using either PPTP, IPSec, GRE or L2TP. IPSec provides the best security; however PPTP is the preferred protocol for integrating with existing Microsoft infrastructure. GRE and L2TP VPNs will generally be used for specialized purposes only.

Using the Shiva VPN Gateway's PPTP client or IPSec you can also connect your office network to one or more remote networks.



The Shiva 1100 VPN Gateway provides both a PPTP and L2TP servers which enable remote Windows clients to securely access your office network.

(new picture needed here when updated graphics become available)

VPN client

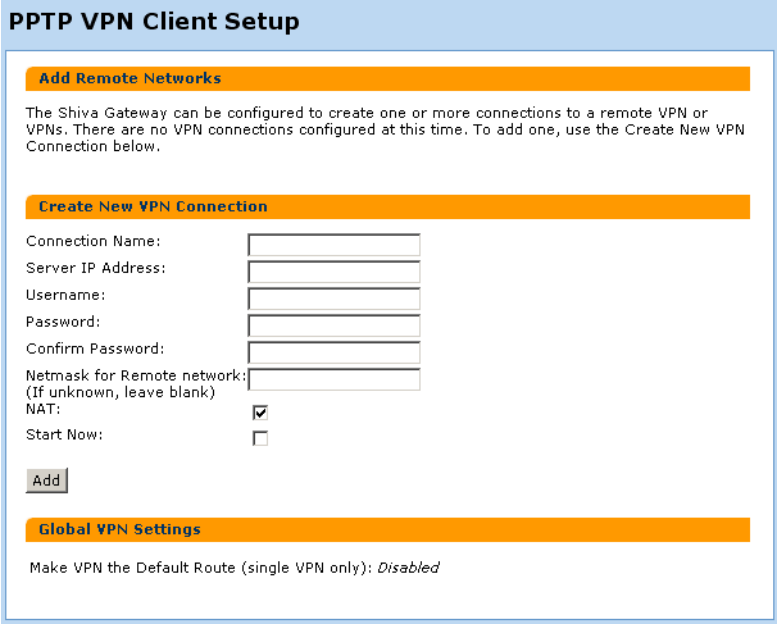
The Shiva VPN Gateway provides both a PPTP and L2TP VPN client.

PPTP client

The PPTP client enables the Shiva VPN Gateway to establish a VPN to a remote network running a PPTP server (usually a Microsoft Windows server).

To create a PPTP client connection:

1 Select **PPTP VPN Client** from the **VPN** menu.



2. Specify the following settings and then click **Add**:
   - A descriptive name for the VPN connection. This may describe the purpose for the connection.
   - The remote PPTP 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 and,
   - Optionally, the remote network's netmask. This is used to determine which packets should go the remote network.
   - If the remote VPN is already up and running, check **Start Now** to establish the connection immediately.

The Shiva VPN Gateway supports multiple VPN client connections. Additional connections can be added by following these steps. To set a VPN connection as the default route for all network traffic, check the **Make VPN the Default Route** checkbox and click **Apply**. This option is only available when the Shiva VPN Gateway is configured with a single VPN connection only. After adding a new VPN, two new

tables are displayed in the PPTP VPN Client menu. VPN Connection Status provides information about the State of the VPN (i.e. enabled or disabled) and the Status of the connection (i.e. up or down).

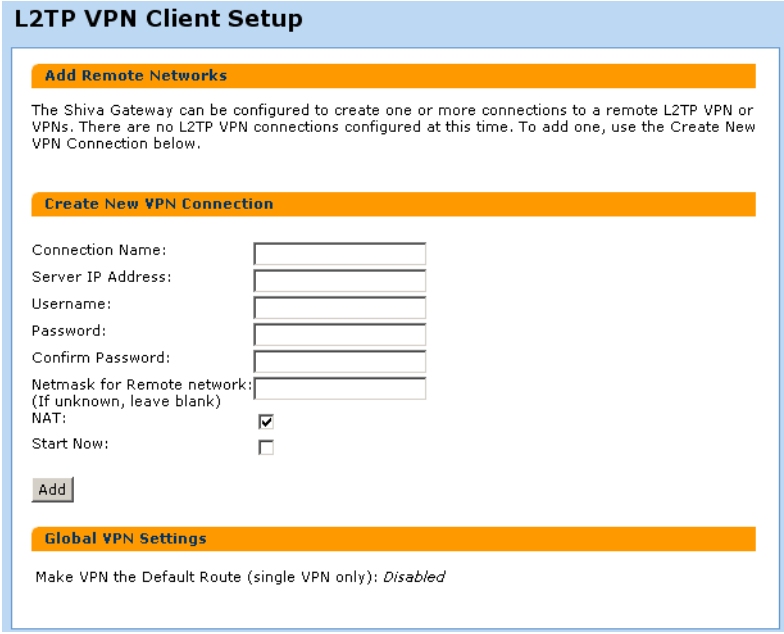
The VPN Configuration table provides the ability to enable/disable the VPN, edit the VPN configuration, delete the VPN entry and edit the advanced routing information.

L2TP client

The Layer Two Tunneling Protocol was developed by Microsoft and Cisco as a multi-purpose network transport protocol.

Many DSL ISPs use L2TP over ATM to create tunnels across the Internet backbone. The Shiva VPN Gateway L2TP implementation can only run L2TP over Ethernet since it doesn't have an ATM adapter. L2TP packets are encapsulated in UDP packets on port 1701 and sent over Ethernet to the L2TP server.

The Shiva VPN Gateway L2TP VPN client is configured and operates in a similar way to the PPTP VPN Client.



VPN server

Note: *This feature is only supported on the Shiva 1100 VPN Gateway.*

The Shiva VPN Gateway provides both a PPTP and L2TP VPN server.

PPTP server

The Shiva VPN Gateway includes a PPTP Server, a virtual private network server that supports up to forty simultaneous VPN tunnels (depending on your Shiva VPN Gateway model). The Shiva VPN Gateway PPTP Server allows remote Windows clients to securely connect to the local network.

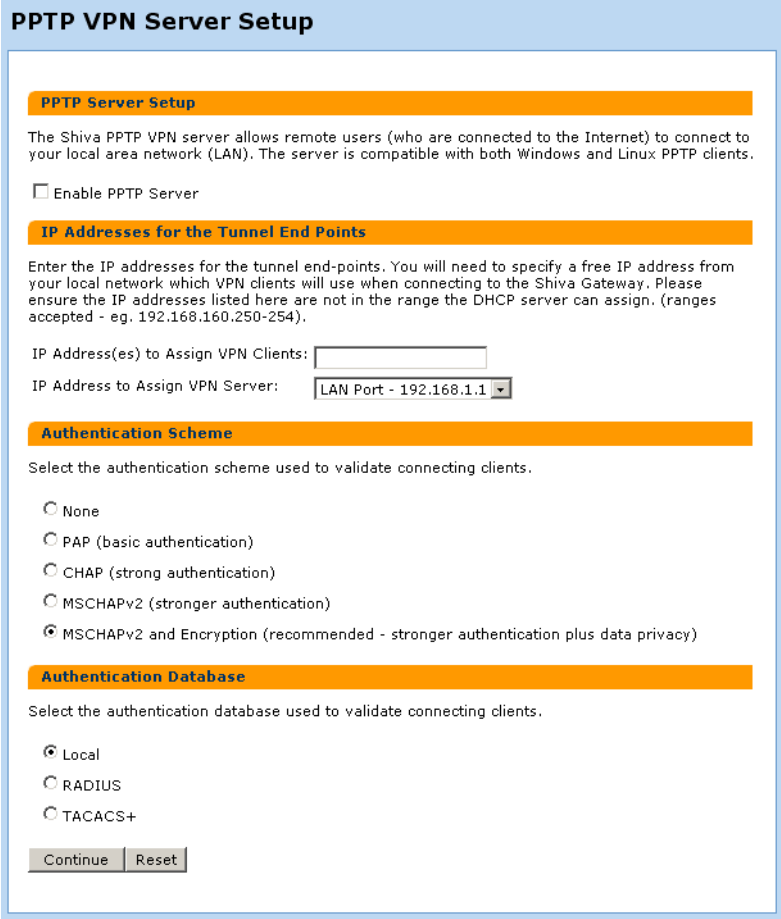
To setup a VPN connection:

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

Configuring the PPTP VPN server

1 Select **PPTP VPN Server** from the **VPN** menu.

2. Configure the appropriate settings.

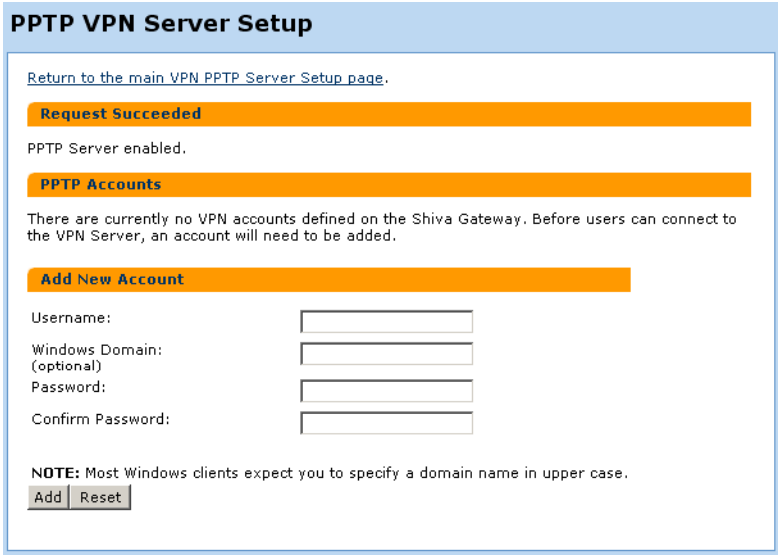


- Enable PPTP Server: Enables the PPTP server.
- IP Addresses to Assign to VPN Clients: Enter the IP addresses for the tunnel end-points. You need to specify a free IP address on your local network that each VPN client will use when connecting to the Shiva VPN Gateway. Please ensure that the IP addresses listed here are not in the range the DHCP server can assign. Ranges are accepted, for example 192.168.160.250-254.
- IP Addresses to Assign to VPN Server: Select the port that the VPN tunnel will be created on.
- Authentication Scheme: PPTP provides an authenticated tunnel between a client and a gateway by using a user ID and password. The authentication scheme is the method the Shiva VPN Gateway uses to challenge users wanting to establish a PPTP connection to the network. The remote client must be set up to use the selected authentication scheme.·
    - MSCHAPv2 is the most secure option. MSCHAPv2 plus data encryption is strongly recommended. This keeps your data private as well as providing secure authentication.
    - CHAP is less secure·
    - PAP (although more common) is even less secure.·

    - None means that no username/password authentication is required (not recommended).
  - Authentication Database: The authentication database is used to verify the username and password received from the dial-in client.·
    - Local means the PPTP user accounts created on the Shiva VPN Gateway. You will need to created user accounts as described below. This can be used with any authentication scheme.·
    - RADIUS means an external RADIUS server. You will be prompted to enter the server IP address and password. This can be used with any authentication scheme, provided that the RADIUS server also supports it.·
    - TACACS+ means an external TACACS+ server. You will be prompted to enter the server IP address and password. This can only be used with the PAP authentication scheme.

3. Click **Continue.**
4. Configure user account settings. PPTP Accounts are distinct from those added through **Users** on the **System** menu and those added through **L2TP Server** and **Dial-in Access**. It is possible, however, to create any of these three accounts sharing the one username and password combination. This may be easier than remembering two or three separate usernames and/or passwords.

   For security reasons, it is recommended that you do not use your ISP username and password for these accounts.



- Username: Username for VPN authentication only. The name selected is case-sensitive (e.g. Jimsmith is different to jimsmith). Username can be the same as, or different to, the name set for dial-in access.
- Windows Domain: Most Windows clients expect you to specify a domain name in upper case. This field is optional.
- Password: Enter the password for the remote VPN user.

  As new VPN user accounts are added, they are displayed on the updated **Account List**.

To modify the password of an existing account, Select the account in the Account List and then enter New Password and Confirm in the Delete or Change Password for the Selected Account field.

To delete an existing account, Select the account in the Account List and then check Delete in the Delete or Change Password for the Selected Account field.

If a requested change to a user account is successful, the PPTP VPN Setup screen is shown with the change noted. An error is displayed if the change request is unsuccessful.

Configuring remote VPN clients

The remote VPN clients can now be configured to securely access the local network. You need to enter the a PPTP Account username and password that you added in the previous section, and the IP address of the Shiva VPN Gateway PPTP VPN server.

The Shiva VPN Gateway PPTP VPN server IP address is displayed on the Diagnostics page. This will generally be the same as the IP address of your main Internet connection.

Note the current IP address of the Shiva VPN Gateway PPTP server. This address may change if your ISP has not allocated you a static IP address. One solution to this is to set up a Dynamic DNS service for use by your Shiva VPN Gateway (see Dynamic DNS in the Network Connections section).

Ensure the remote VPN client computer 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.

Ensure that both the VPN and Dial Up Networking (DUN) software is installed on the remote computer. If you are using Windows 95 or an older version of Windows 98 (first edition), install the Microsoft DUN update (available on the Shiva VPN Gateway Installation CD) and VPN Client update.

Your Shiva VPN Gateway's PPTP server will operate with the standard Windows PPTP clients in all current versions of Windows.

L2TP server

The L2TP Server runs in a similar way to the PPTP Server. A range of IP addresses is allocated, and then username and password pairs are created to allow users to log on.

Note: *To increase security, L2TP VPN connections from Windows computers are also run through an IPSec tunnel. This means an IPSec connection must be configured and enabled as well as the L2TP server before Windows clients can connect.*

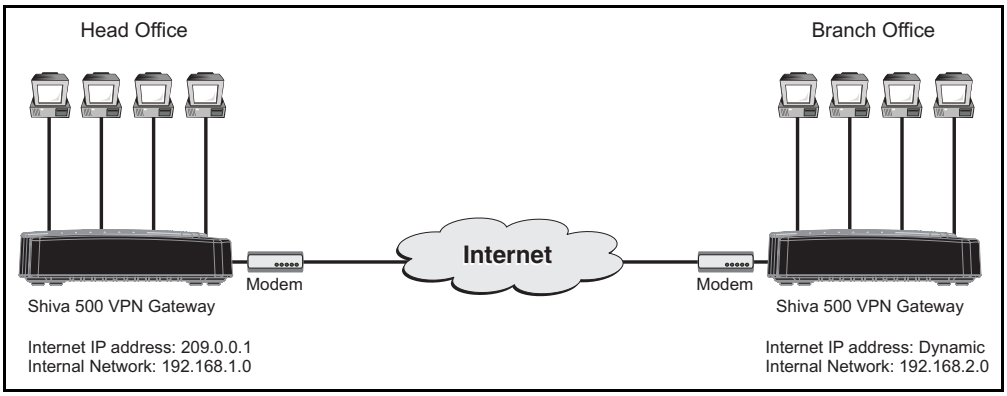
The default way for the IPSec connection to be authenticated is to use x.509/RSA certificates. The Shiva VPN Gateway therefore needs to have IPSec configured with both a CA and local certificate before connections can be established. The Windows machine needs to have a copy of the CA certificate used to sign the Shiva VPN Gateway local certificate, and similarly, the Shiva VPN Gateway needs a copy of the CA of the Windows certificate.

IPSec

There are many possible scenarios for making use of IPSec. The most common is described in this section. Additional options are also be explained throughout this example, should it become necessary to configure the tunnel with those settings.

Scenario

This scenario demonstrates how to link two offices via the Internet using IPSec. This provides a secure tunnel through which users on both networks can share data and resources.

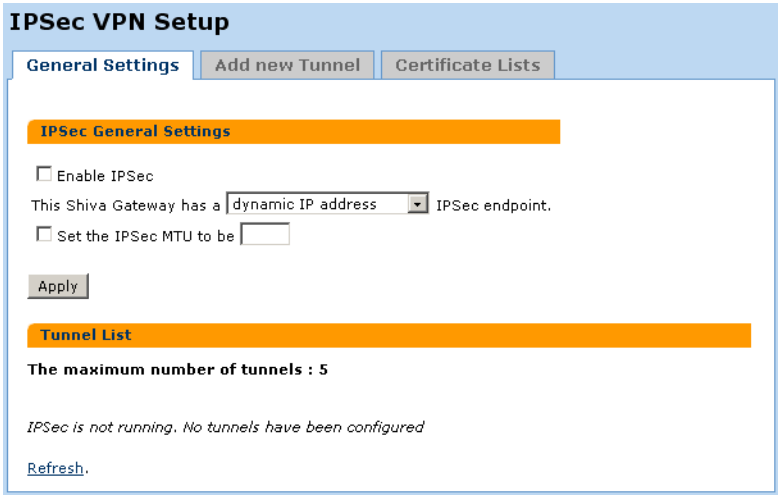


To combine the Headquarters and Branch Office networks together, an IPSec tunnel must be configured on both Shiva VPN Gateways.

Set up the branch office

Enable IPSec

1 Click the **IPSec** link on the left side of the web-based management console.

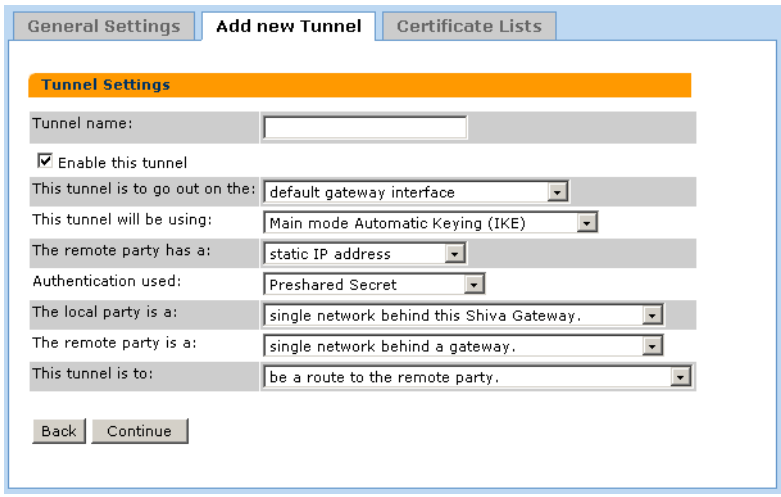


2. Select the **Enable IPSec** option.
3. Select the type of IPSec endpoint the Shiva VPN Gateway will create on the Internet port. The Shiva VPN Gateway can either have a static IP, dynamic IP or DNS hostname address. If a dynamic DNS service is to be used or there is a DNS hostname that resolves to the IP address on the Internet port, then the DNS hostname address option should be selected. For this example, select **dynamic IP address**.
4. The Maximum Transmission Unit (MTU) of the IPSec interface can be configured by selecting the **Set the IPSec MTU to be** option and filling in the desired MTU value. For most applications this does not need to be configured. However, if set, the MTU value should be between 1400 and 1500.
5. Click the **Apply** 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.*

Create a tunnel to connect to the head office network

1 Click the **Add New Tunnel** tab.



2. Assign a name to the tunnel. The name must not contain spaces or start with a number. For this example specify **Headquarters**.
3. Leave the **Enable this tunnel** checkbox checked.
4. Select the Internet port the IPSec tunnel is to go out on. The options will depend on what is currently configured on the Shiva VPN Gateway. For the vast majority of setups, this will be the default gateway interface to the Internet. For this example, select the **default gateway interface** option.

   Note: *You may want to select an interface other than the default gateway when you have configured aliased Internet interfaces and require the IPSec tunnel to run on an interface other than the default gateway.*

5. Select the type of keying the tunnel will use. The Shiva VPN Gateway supports the following types of keying:
   - Main mode with Automatic Keying (IKE) automatically exchanges encryption and authentication keys and protects the identities of the parties attempting to establish the tunnel.
   - Aggressive mode with Automatic Keying (IKE) automatically exchanges encryption and authentication keys and uses less messages in the exchange when compared to Main mode. Aggressive mode is must be used to allow parties that are configured with a dynamic IP address and a preshared secret to connect or if the Shiva VPN Gateway or the remote party is behind a NAT device.
   - Manual Keying requires the encryption and authentication keys to be specified.

   For this example, select the **Aggressive mode with Automatic Keying** option.
6. 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. For this example, select the static IP address option.
7. Select the type of authentication the tunnel will use. The Shiva VPN Gateway supports the following types of authentication:
   - Preshared Secret is a common secret (passphrase) that is shared between the Shiva VPN Gateway and the remote party.
   - RSA Digital Signatures uses a public/private RSA key pair for authentication. The Shiva VPN Gateway can generate these key pairs. The public keys need to be exchanged between the Shiva VPN Gateway and the remote party in order to configure the tunnel.
   - 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 Shiva VPN Gateway before a tunnel can be configured to use them (see Certificate Management).
   - Manual Keys establishes the tunnel using predetermined encryption and authentication keys.

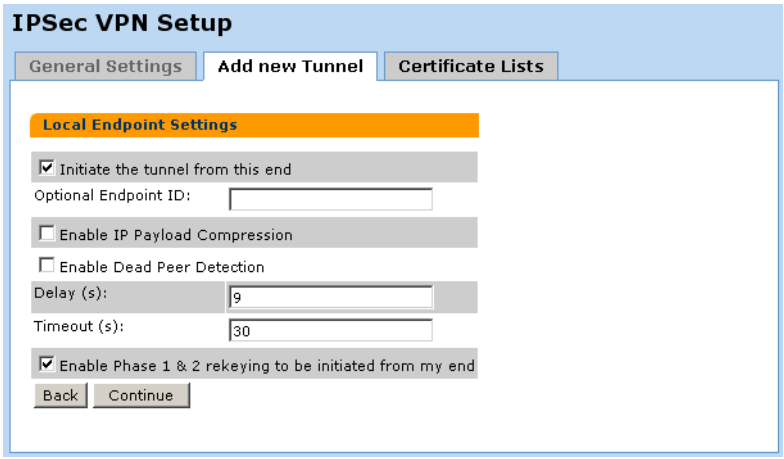
   For this example, select the **Preshared Secret** option.
8. Select the type of private network that is behind the Shiva VPN Gateway. The following types of networks are supported:
   - Single network is selected when a single subnet resides behind the Shiva VPN Gateway that the remote party will have access to.
   - Multiple networks is selected when multiple subnets reside behind the Shiva VPN Gateway that the remote party will have access to.
   - Masqueraded network is selected when all traffic behind the Shiva VPN Gateway is seen as originating from its Internet IP address by the remote party. The remote party will not have any access to the network behind the Shiva VPN Gateway.

   For this example, select the **single network behind this Shiva Gateway** option.

9. Select whether the remote party is a single host or whether it is a gateway that has a single network or has multiple networks behind it. For this example, select the **single network behind a gateway** option.
10. Select in which way the tunnel should be utilized to route traffic. The Shiva VPN Gateway can support following types of routing:
    - Be a route to the remote party is selected when the tunnel sets up a route to the remote party's subnet(s).
    - Be this's default gateway for all traffic is selected when the tunnel will be the default gateway for all traffic to the remote party.
    - Be the remote party's default gateway for all traffic is selected when the tunnel will be the default gateway for all traffic from the remote party.

    For this example, select the **be a route to the remote party** option.
11. Click the **Continue** button to configure the Local Endpoint Settings.

Define local endpoint settings



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

Note: *This option will not be available when the Shiva VPN Gateway has a static IP address and the remote party has a dynamic IP address.*

2. Enter the **Required Endpoint ID** of the Shiva VPN Gateway. This ID is used to authenticate the Shiva VPN Gateway to the remote party. It is required because the Shiva VPN Gateway For this example has a dynamic IP address. This field will also be required if RSA Digital Signatures are used for authentication.

   It becomes optional if the Shiva VPN Gateway 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. If the remote party is a Shiva VPN Gateway, the ID must have the form abcd@efgh.
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 will be sent every 9 seconds (Delay) and if no response is received in 30 seconds (Timeout) then the Shiva VPN Gateway will attempt to restart the tunnel. For 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 **Continue** button to configure the Remote Endpoint Settings.

Other options

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

- The next IP address on the interface the tunnel is to go on field is the next gateway IP address or nexthop along the previously selected IPSec interface. This field will become available if an interface other than the default gateway was selected for the tunnel to go out on.
- SPI Number field 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 field 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 field 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 field is the network behind the local Shiva VPN Gateway. This field appears when **Manual Keying** has been selected.

Define remote endpoint settings

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

The Endpoint ID is used to authenticate the remote party to the Shiva VPN Gateway. 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 For this example, because the remote party has a static IP address. If the remote party is a Shiva VPN Gateway, it must have the form abcd@efgh. For this example leave the field blank.

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

Other options

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

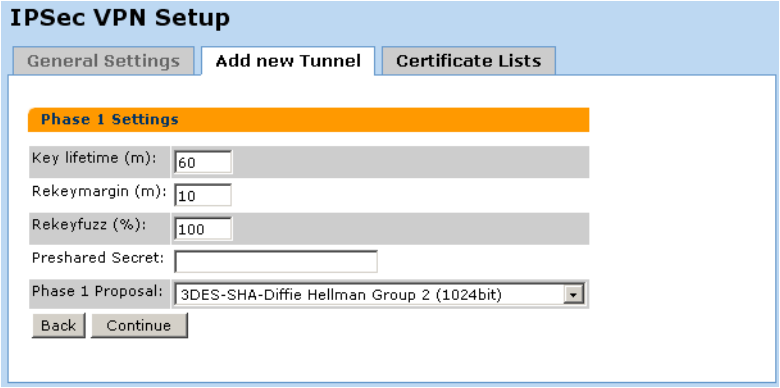
- The remote party's DNS hostname address field is the DNS hostname address of the Internet interface of the remote party. This option will become available if the remote party has been configured to have a DNS hostname address.
- Distinguished Name field is the list of attribute/value pairs contained 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=Shiva, OU=Sales, CN=SG550. 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.

- Generate an RSA key of pull down menu allows the length of the Shiva VPN Gateway 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 0x100-0xfff. 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 Shiva VPN Gateway'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 Shiva VPN Gateway'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.

Define phase 1 settings



Set the length of time before Phase 1 is renegotiated in the **Key lifetime (m)** field. The length may vary between 1 and 1440 minutes. Shorter values offer higher security at the expense of the computational overhead required to calculate new keys. For most applications 60 minutes is recommended. For this example, leave the **Key Lifetime** as the default value of 60 minutes.

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 field. For this example, leave the **Rekeymargin** as the default value of 10 minutes.

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 that the value of "Rekeymargin x (100 + Rekeyfuzz) / 100." For this example, leave the Rekeyfuzz as the default value of 100%.

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

Note: *The secret must be entered identically at each end of the tunnel. The tunnel will fail 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.*

Select a **Phase 1 Proposal**. Any combination of the ciphers, hashes and Diffie Hellman groups that the Shiva VPN Gateway 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 Shiva VPN Gateway also supports extensions to the Diffie Hellman groups to include 2048, 3072 and 4096 bit Oakley groups. For this example, select the 3DES-SHA-Diffie Hellman Group 2 (1024 bit) option.

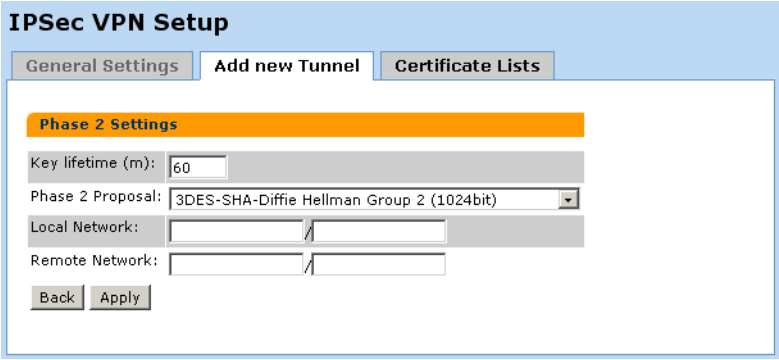
Click the **Continue** button to configure the Phase 2 Settings.

Other options

The following options will 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.
- Modulus, Public Exponent, Private Exponent, Prime1, Prime2, Exponent1, Exponent2 and Coefficient fields constitute the private part of the RSA key. These fields are automatically populated and do not need to be modified unless a different RSA key is to be used. 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.

Define phase 2 settings page



1 Set the length of time before Phase 2 is renegotiated in the **Key lifetime (m)** field. The length may vary between 1 and 1440 minutes. For most applications 60 minutes is recommended. For this example, leave the Key Lifetime as the default value of 60 minutes.

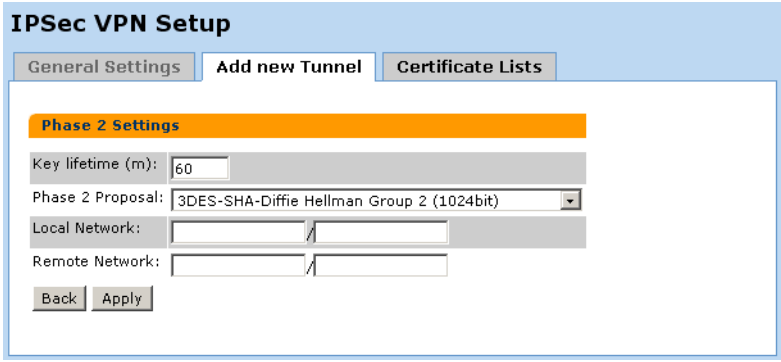
2. Select a **Phase 2 Proposal**. Any combination of the ciphers, hashes and Diffie Hellman groups that the Shiva VPN Gateway supports can be selected. The supported ciphers are DES, 3DES and AES (128, 196 and 256 bits). The supported hashes are MD5 and SHA and the supported Diffie Hellman group are 1 (768 bit), 2 (1024 bit) and 5 (1536 bits). The Shiva VPN Gateway 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. For this example, select the 3DES-SHA-Diffie Hellman Group 2 (1024 bit) option.

3. Define the **Local Network** behind the Shiva VPN Gateway that is to have access through the tunnel. For this example, enter 192.168.2.0 / 255.255.255.0 in the field.
4. Define the **Remote Network** behind the remote party that is to have access through the tunnel. For this example, enter 192.168.1.0 / 255.255.255.0 in the field.
5. Click the **Apply** button to save the tunnel configuration.

Other options

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

A separate section may appear to enter multiple Local Networks or Remote Networks or both. In the case where both local and remote parties have been configured to have multiple subnets behind them.



In the **Subnet Settings** section, a local and remote network combination can be added one at a time by entering subnets into the **Add Local Network** and **Add Remote Network** fields and then clicking **Apply**. Configured local and remote network combinations can be deleted by clicking the **Delete** checkbox for the appropriate combination and then clicking **Apply**. Once the required networks have been added, configure the Phase 2 Settings section.

Set up the head office

Enable IPSec

1 Click the **IPSec** link on the left side of the web-based management console.
2. Check the **Enable IPSec** checkbox.
3. Select the type of IPSec endpoint the Shiva VPN Gateway has on its Internet interface. For this example, select static IP address.
4. Leave the **Set the IPSec MTU to be** checkbox unchecked.
5. Click the **Apply** button to save the changes.

Setup a tunnel to accept connections from the branch office

1 Click the **IPSec** link on the left side of the web-based management console.
2. Click the **Add New Tunnel** tab. Many of the settings such as the Preshared Secret, Phase 1 and 2 Proposals and Key Lifetimes will be 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. For this example, enter: Branch_Office

2. Select **Enable this tunnel**.

3. Select the Internet interface the IPSec tunnel is to go out on. For this example, select **default gateway interface** option.

4. Select the type of keying the tunnel will use. For this example, select the **Aggressive mode with Automatic Keying (IKE)** option. This is required when dynamic addressing is used.

5. Select the type of IPSec endpoint the remote party has. For this example, select the **dynamic IP address** option.

6. Select the type of authentication the tunnel will use. For this example, select the Preshared Secret option.

7. Select the type of private network that is behind the Shiva VPN Gateway. For this example the Headquarters has a single network, so select the **single network behind this Shiva Gateway** option.

8. Select whether the remote party is a single host or whether it is a gateway that has a single or has multiple networks behind it. For this example the Branch Office has single network, so select the **single network behind a gateway** option.

9. Select the type of routing the tunnel will be used as. For this example, select the **be a route to the remote party** option.

10. Click the **Continue** button to configure the Local Endpoint Settings.

Define local endpoint settings

1 Leave the Optional Endpoint ID field blank For this example. It is optional because the Shiva VPN Gateway has a static IP address. If the remote party is a Shiva VPN Gateway and an Endpoint ID is used, it must have the form abcd@efgh.

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 Continue button to configure the Remote Endpoint Settings.

Define remote endpoint settings

1 Enter the Required Endpoint ID of the remote party. For this example, enter the Local Endpoint ID at the Branch Office which was: branch@office

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

Define phase 1 settings

1 Set the length of time before Phase 1 is renegotiated in the Key lifetime (m) field. For this example, leave the Key Lifetime as the default value of 60 minutes.

2. Set the time for when the new key is negotiated before the current key expires in the Rekeymargin field. For this example, leave the Rekeymargin as the default value of 10 minutes.

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 that the value of "Rekeymargin x (100 + Rekeyfuzz) / 100." For this example, leave the Rekeyfuzz as the default value of 100%.
4. Enter a secret in the Preshared Secret field. This must remain confidential. For this example, enter the Preshared Secret used at the branch office Shiva VPN Gateway, which was: This secret must be kept confidential.
5. Select a Phase 1 Proposal. For this example, select the 3DES-SHA-Diffie Hellman Group 2 (1024 bit) option (same as the Branch Office Phase 1 Proposal).
6. Click the **Continue** button to configure the Phase 2 Settings.

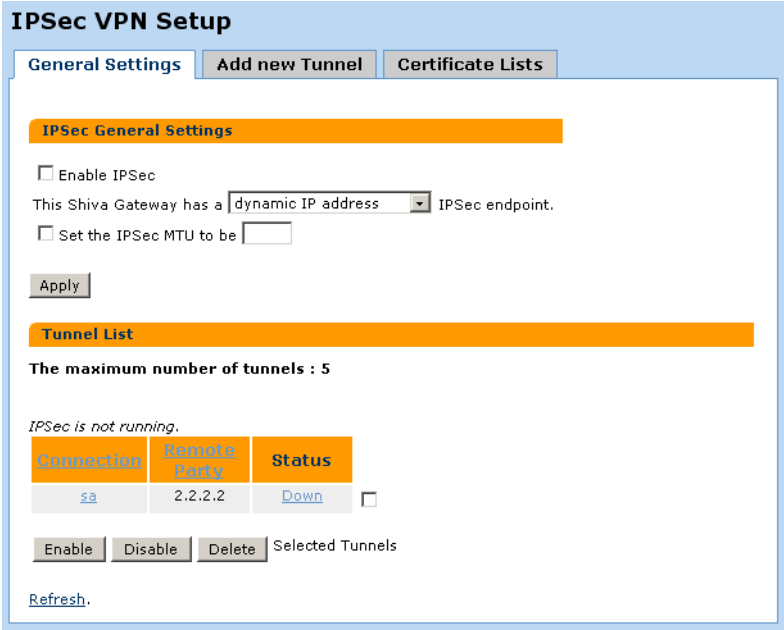
Define phase 2 settings

1 Set the length of time before Phase 2 is renegotiated in the **Key lifetime (m)** field. For this example, leave the Key Lifetime as the default value of 60 minutes.

2. Select a **Phase 2 Proposal**. For this example, select the **3DES-SHA-Diffie Hellman Group 2 (1024 bit)** option (same as the Branch Office Phase 2 Proposal).
3. Define the **Local Network** behind the Shiva VPN Gateway that is to have access through the tunnel. For this example, enter 192.168.1.0 / 255.255.255.0 in the field.
4. Define the Remote Network behind the remote party that is to have access through the tunnel. For this example, enter 192.168.2.0 / 255.255.255.0 in the field.
5. Click the **Apply** button to save the tunnel configuration.

Tunnel List

The tunnel list shows all current configured tunnels and their status (enabled/disabled and if they are established or not).



Connection

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

Note: *You may modify a tunnel's settings by clicking on its connection name.*

Click Connection to sort the tunnel list alphabetically by connection name.

Remote party

The Remote Party which the tunnel is configured to connect to will be 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) will have 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. Aggressive mode must be set when dynamic addressing is used.

- 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 will either be in 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 will be 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, keysizemin=64, keysizemax=168
000 algorithm ESP encrypt: id=3, name=ESP_3DES, ivlen=64, keysizemin=168, keysizemax=168
000 algorithm ESP encrypt: id=12, name=ESP_AES, ivlen=128, keysizemin=128, keysizemax=256
```

Phase 2 Hashes Loaded

```
000 algorithm ESP auth attr: id=1, name=AUTH_ALGORITHM_HMAC_MD5, keysizemin=128, keysizemax=128
000 algorithm ESP auth attr: id=2, name=AUTH_ALGORITHM_HMAC_SHA1, keysizemin=160, keysizemax=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
```

Phase 1 Hashes Loaded

```
000 algorithm IKE hash: id=2, name=OAKLEY_SHA, hashsize=20
000 algorithm IKE hash: id=1, name=OAKLEY_MD5, hashsize=16
```

Diffie Hellman Groups Loaded

```
000 algorithm IKE dh group: id=1, name=OAKLEY_GROUP_MODP768, bits=768
000 algorithm IKE dh group: id=2, name=OAKLEY_GROUP_MODP1024, bits=1024
000 algorithm IKE dh group: id=5, name=OAKLEY_GROUP_MODP1536 (extension), bits=1536
000 algorithm IKE dh group: id=42048, name=OAKLEY_GROUP_MODP2048 (extension), bits=2048
000 algorithm IKE dh group: id=43072, name=OAKLEY_GROUP_MODP3072 (extension), bits=3072
000 algorithm IKE dh group: id=44096, name=OAKLEY_GROUP_MODP4096 (extension), bits=4096
```

Connection Details

```
000 "Headquarters": 192.168.2.0/24===209.0.0.2[branch@office]...209.0.0.1===192.168.1.0/24
000 "Headquarters":   ike_life: 3600s; ipsec_life: 3600s; rekey_margin: 600s; rekey_fuzz: 100%; keyingtries: 0
000 "Headquarters":   policy: AGGRESSIVE+PSK+ENCRYPT+TUNNEL+PFS; interface: eth1; unrouted
000 "Headquarters":   newest ISAKMP SA: #0; newest IPsec SA: #0; eroute owner: #0
000 "Headquarters":   IKE algorithms wanted: 5_000-2-2, flags=-strict
000 "Headquarters":   IKE algorithms found:  5_192-2_160-2,
000 "Headquarters":   ESP algorithms wanted: 3_000-2, ; pfsgroup=2; flags=-strict
000 "Headquarters":   ESP algorithms loaded: 3/168-2/160,
```

Negotiation State

```
000 #7: "Headquarters" STATE_AGGR_I1 (sent AI1, expecting AR1); EVENT_RETRANSMIT in 8s
```

Back

- Interfaces Loaded lists the Shiva VPN Gateway's interfaces which IPSec will use.
- Phase 2 Ciphers Loaded lists the encryption ciphers that tunnels can be configured with for Phase 2 negotiations. This will include DES, 3DES and AES.
- Phase 2 Hashes Loaded lists the authentication hashes that tunnels can be configured with for Phase 2 negotiations. This will include 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 will include DES, 3DES and AES.
- Phase 1 Hashes Loaded lists the authentication hashes that tunnels can be configured with for Phase 1 negotiations. This will include 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. For 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). For this example, they are both 3600s.
  - Type of automatic (IKE) keying. For this example, the policy line has: AGGRESSIVE. For Main mode, it will read MAIN.
- Type of authentication used. For this example, the policy line has: PSK (Preshared Key). For RSA Digital Signatures or X.509 certificates, it will read RSA.
- Whether Perfect Forward Secrecy is used. For this example, the policy line has the PFS keyword. If PFS is disabled, then the keyword will not appear.
- Whether IP Payload Compression is used. For 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. For 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. For this example, phase 1 has not be 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. For this example, phase 1 has not be 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. For this example it has initiated and sent the first aggressive mode packet (AI1) and is expecting its response (AR1) in the line STATE_AGGR_I1 (sent AI1, expecting AR1). Once the Phase 1 has been successfully negotiated, the status will have the line ISAKMP SA established. Once the Phase 2 has been successfully negotiated, the status will read IPSec SA established. The tunnel will then be established and running.

Enable/disable

One or more tunnel can be enabled or disabled by checking the checkbox to the right of the tunnel, and clicking Enable or Disable under the Tunnel List menu.

Delete

One or more tunnel can be enabled or disabled by checking the checkbox to the right of the tunnel, and clicking Delete under the Tunnel List menu.

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 Shiva VPN Gateway.

Dynamic DNS Support

Internet Service Providers generally charge higher fees for static IP addresses than for dynamic IP addresses when connecting to the Internet. The Shiva VPN Gateway can reduce costs since it allows tunnels to be established with both IPSec endpoints having dynamic IP addresses. The two endpoints must, however, be Shiva VPN Gateways and at least one end must have dynamic DNS enabled. The Shiva VPN Gateway supports a number of dynamic DNS providers. When configuring the tunnel, select the DNS hostname address type for the IPSec endpoint that has dynamic DNS supported and enable Dead Peer Detection. If the IP address of the Shiva VPN Gateway's DNS hostname changes, the tunnel will automatically renegotiate and establish the tunnel.

Troubleshooting

Symptom: IPSec is not running and is enabled.

Possible Cause: The Shiva VPN Gateway has not been assigned a default gateway.

Solution: Ensure the Shiva VPN Gateway 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 Shiva VPN Gateway'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 Shiva VPN Gateway 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 Shiva VPN Gateway and the remote party do not match.

The local and remote subnets do not match.

Solution: Ensure that the tunnel settings for the Shiva VPN Gateway and the remote party are configured correctly.

Symptom: Large packets don't seem to get transmitted

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 Shiva VPN Gateway has been configured not to rekey the tunnel.

The remote party is not rekeying correctly with the Shiva VPN Gateway.

Solution: Confirm that the remote party has IPSec and the tunnel enabled and has an Internet IP address. Ensure that the Shiva VPN Gateway has rekeying enabled. If the tunnel still goes down after a period of time, it may be due to the Shiva VPN Gateway and remote party not recognizing 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. Unless the remote party supports draft-ietf-ipsec-dpd-00.txt, Dead Peer Detection will not be used.

Symptom: Tunnels using X.509 certificate authentication do not work

Possible Cause: The date and time settings on the Shiva VPN Gateway has not been configured correctly.

The certificates have expired.

The Distinguished Name of the remote party has not be configured correctly on the Shiva VPN Gateway'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 Shiva VPN Gateway'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 LMHOST 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 computer to the Internet IP address of the remote party (it assumed that the remote party is configured to accept incoming pings)

Ping from your computer to the LAN IP address of the remote party.

Ping from your computer to a computer 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 Shiva VPN Gateway. 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 will not be sent through the Shiva VPN Gateway. You should contact the producer of the application for support.

Certificate management

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 Shiva VPN Gateway 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 Shiva VPN Gateway.

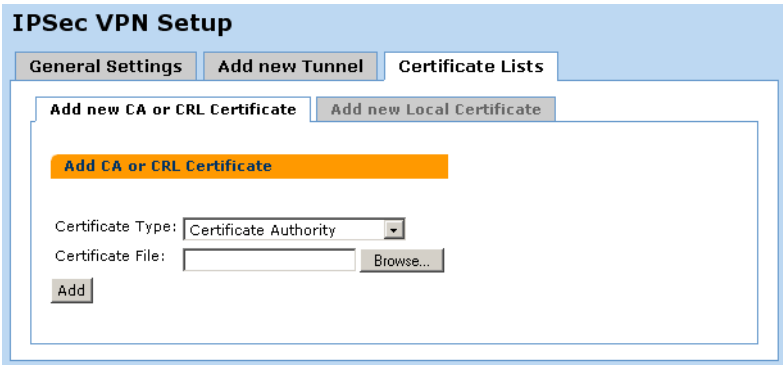
The Shiva VPN Gateway only supports certificates in base64 PEM or binary DER format. Some Certificate Authorities (CA) distribute certificates in a PKCS#12 format file and the CA, local public key and private key certificates must be extracted or created before uploading them into the Shiva VPN Gateway.

Adding certificates

To add certificates to the Shiva VPN Gateway, click the **IPSec** link on the left side of the web-based management console and then click the **Certificate Lists** tab. A window similar to the following will be displayed.

Adding a CA or CRL certificate

1 Click the **Add new CA or CRL Certificate** tab. A window similar to the following will be displayed.



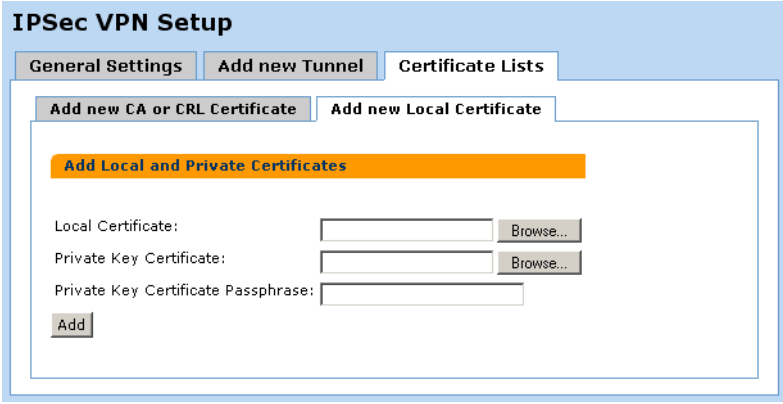
2. Select whether a **Certificate Authority** or **Certificate Revocation List** certificate is to be uploaded from the **Certificate Type** box.
3. Enter the Certificate Authority's Public Key certificate or CRL file in the **Certificate File** field. Click the **Browse** button to select the file from the host computer. CA Certificates have time durations in which they are valid. Ensure

that the certificates uploaded are valid and that the Date and Time has been set correctly on the Shiva VPN Gateway. Also ensure that the certificate is in PEM or DER format.

4. Click the **Add** button to upload the file.

Adding a local certificate

1 Click the **Add new Local Certificate** tab. A window similar to the following will be displayed.



2. Enter the Local Public Key certificate in the **Local Certificate** field. Click the **Browse** button to select the file from the host computer. 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 Shiva VPN Gateway. Also ensure that the certificate is in PEM or DER format.
3. Enter the **Local Private Key certificate** in the **Private Key Certificate** field. Click the **Browse** button to select the file from the host computer. Ensure the certificate is the private key for the above public key certificate. Also ensure that the certificate is in PEM or DER format.
4. Enter the passphrase to unlock the private key certificate in the **Private Key Certificate Passphrase** field.
5. Click the **Add** button to upload the certificates and passphrase.

GRE

The GRE configuration of the Shiva VPN Gateway allows you to build GRE tunnels to other devices that support the Generic Routing Encapsulating protocol. You can build GRE tunnels to other Shiva VPN Gateways 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.

Setting up a GRE tunnel

For this example we will connect two office networks using a GRE tunnel between two Shiva VPN Gateways. One is located in Brisbane, the other in Slough. The two networks have the following configuration:

Shiva VPN Gateway in Brisbane

- Internet address: 203.23.45.6
- LAN address: 192.168.1.1
- LAN: 192.168.1.0 / 255.255.255.0

Shiva VPN Gateway in Slough

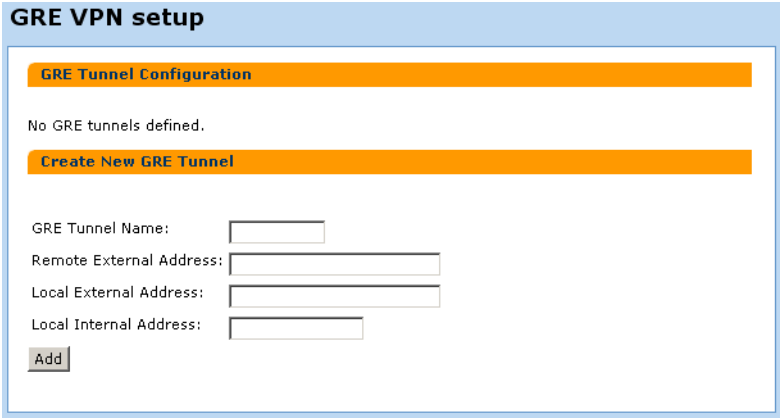
- Internet address: 195.45.67.8
- LAN address: 10.1.0.1
- LAN: 10.1.0.0 / 255.255.0.0

1 On the Brisbane end, click **GRE Tunnels** from the VPN menu. Enter the following details:
   - GRE Tunnel Name: to_slough
   - Remote External Address: 195.45.67.8
   - Local External Address: 203.23.45.6
   - Local Internal Address: 192.168.1.1

2. Click **Add**.
3. Click **Add/Remove** under **Remote Networks** and enter:

   Remote subnet/netmask: 10.1.0.0 /255.255.0.0

4. Click **Add**. The Brisbane end is now set up.



5. On the Slough end, click **GRE Tunnels** from the **VPN** menu. Enter the following details:
   - GRE Tunnel Name: to_bris
   - Remote External Address: 203.23.45.6
   - Local External Address: 195.45.67.8
   - Local Internal Address: 10.1.0.1
6. Click **Add**.
7. Click **Add/Remove** under **Remote Networks** and enter:

   Remote subnet/netmask: 192.168.1.0 /255.255.255.0
8. Click **Add**. The GRE tunnel between the two networks is now set up. Tunnels may be Disabled, Deleted or Edited from the main table of GRE tunnels. A few further things of note are:
   - GRE Tunnel Name: The name is arbitrary.
   - Remote External Address: This may also be in the form of a DNS name, e.g. a dynamic DNS name.
   - Local External Address: This may also be an Internet port alias address.
   - Remote subnet/netmask: Multiple networks can be routed through a single GRE tunnel. Add them through Add/Remove under Remote Networks.

Port Tunnels

Note: *This feature is only supported on the Shiva 1100 VPN Gateway.*

Port tunnels are point-to-point tunnels that are similar in many ways to port forwards. The Shiva VPN Gateway supports two distinct kinds of port tunnels:

- httptunnel which tunnels traffic using the HTTP protocol. httptunnel based tunnels are not encrypted. They are, however, rather good for penetrating zealous firewalls.
- stunnel which tunnels traffic using SSL

In both cases there are two distincts parts to a tunnel, the source and the destination. The source listens for network connections from behind the firewall and when a connection occurs, forwards all traffic to the destination. The destination accepts incoming network traffic and forwards it to a specified destination host and port.

Note: *It is possible to, for example, to create an stunnel port tunnel with a localhost destination (127.0.0.1) and to then have an httptunnel listening on that port which forwards to a remote httptunnel which in turn loops back to a remote stunnel which in turn forwards the network traffic to the desired destination. In this manner, it is possible to create a secure tunnel over HTTP.*

stunnel configuration is essentially the same for both source and destination and the only form field that should be noted here is the Protocol. This allows stunnel to create a link to a non-stunnel server using SSL, e.g. if your POP3 server only accepts SSL conections and your mail client doesn't support these, install a stunnel in the middle using the POP3 protocol.

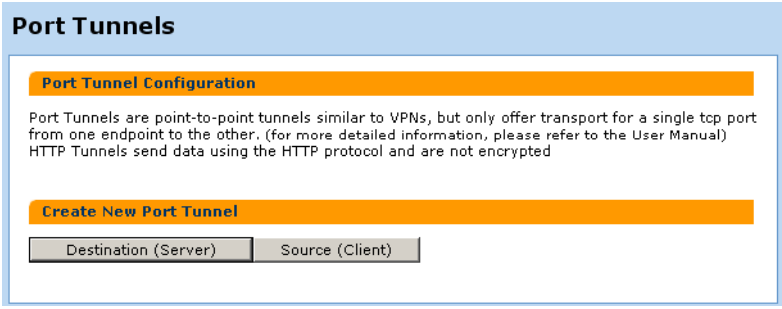
httptunnel has quite different configurations for the two ends and in particular the source side can specify a number of proxy settings to allow it to traverse a proxying firewall.

Setting up a port tunnel

To create a port tunnel, do the following:

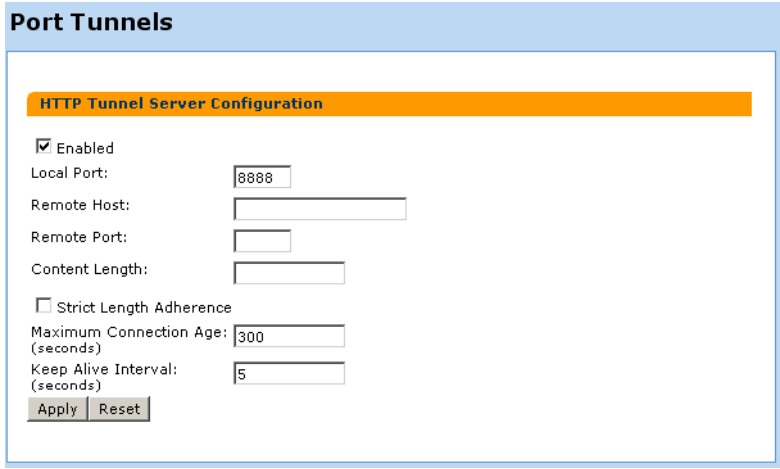
1 Click **Port Tunnels** on the main menu.

2. Select **Destination (Server)** or **Source (Client)**.



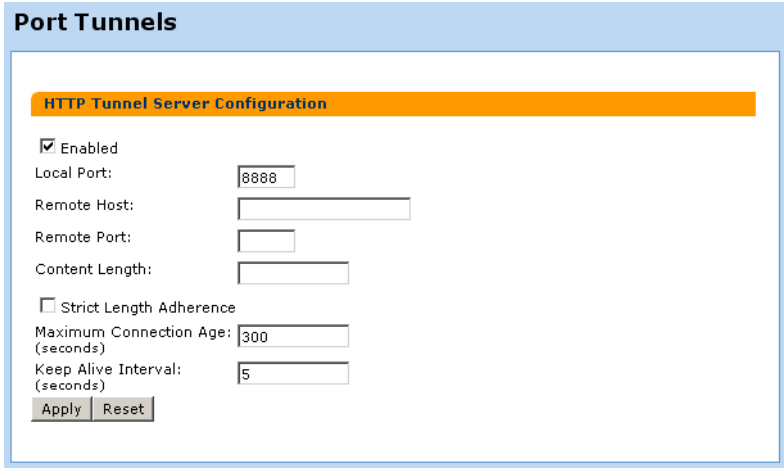
3. Configure tunnel settings as required and then click **Apply**.

Destination (Server) settings



- Enabled: Enables the tunnel.
- Local Port: ????
- Remote Host: ????
- Remote Port: ????
- Content Length: ????
- Strict Length Adherence: ????
- Maximum Connection Age: ????
- Keep Alive Interval: ????

Source (Client) settings



- Enabled: Enables the tunnel.
- Local Port: ????
- Remote Host: ????
- Remote Port: ????
- Content Length:

- Strict Length Adherence: ????
- Maximum Connection Age: ????
- Keep Alive Interval: ????
- Proxy: ????
- Username: ????
- Password: ????
- Port: ????
- Proxy Buffer Size: ????
- User Agent: ????
- Padding Timeout: ????

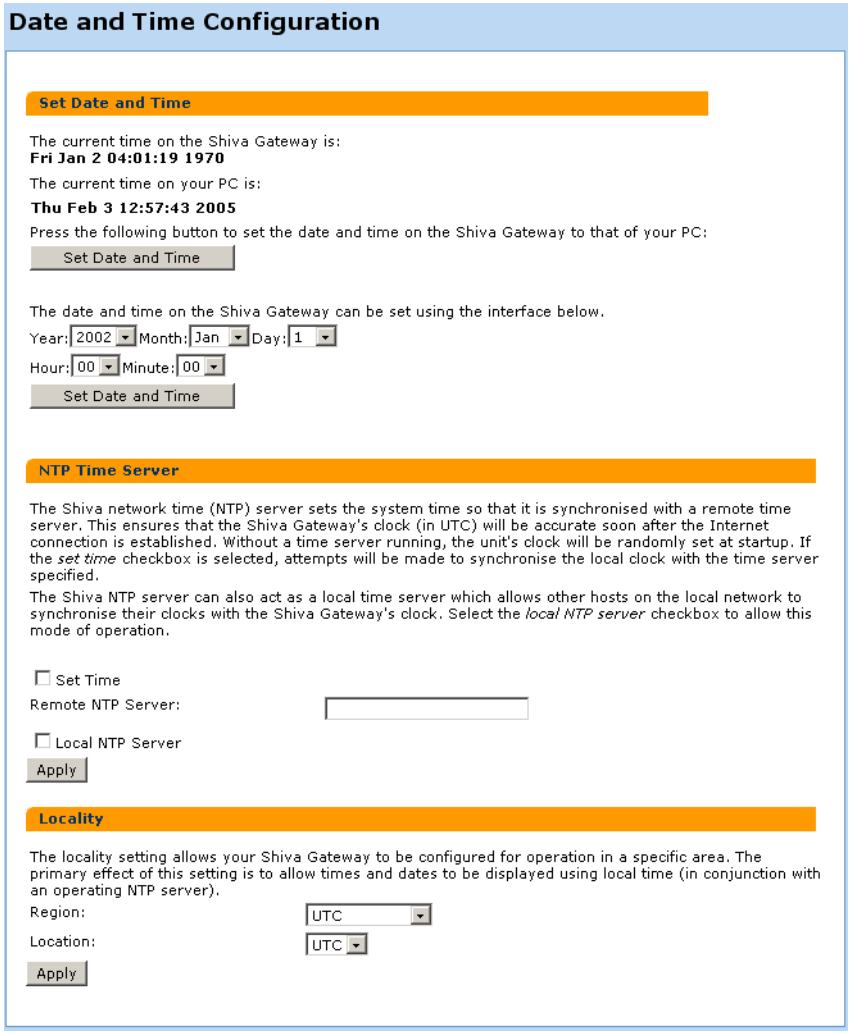
Chapter 6

Management

This chapter describes how to configure various management options such as date and time, users, administrator settings, and diagnostics.

Setting the date and time

To reach this page click **Data and Time** under **System** on the left menu.



Set date and time

If you have a Javascript enabled web browser, you will be able to click the top **Set Date and Time** button to synchronize the time on the Shiva VPN Gateway with that of your computer.

Alternately, you can manually set the Year, Month, Date, Hour and Minute using the selection boxes to set the date and time on the Shiva VPN Gateway.

NTP time server

The Shiva VPN Gateway can synchronize its system time with a remote time server using the Network Time Protocol (NTP). Configuring the NTP time server ensures that the Shiva VPN Gateway's clock (in UTC) will be accurate soon after the Internet connection is established. If NTP is not used, the system clock will be set randomly when the Shiva VPN Gateway starts up.

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

Locality

Select your region then select your location within said region. The system clock will subsequently show local time. Without setting this, the system clock will show UTP. Setting a time zone is only relevant if you are synchronizing with an NTP server or your Shiva VPN Gateway has a real time clock. Without either of these, the Shiva VPN Gateway's clock is set randomly at startup.

User list

User accounts on a Shiva VPN Gateway allow administrative duties to be spread amongst a number of different people according to their level of competence and trust. Each user on the Shiva VPN Gateway has a password that they use to authenticate themselves to the unit's web pages. They also have a number of access controls that modify what they can and cannot do via the web interface, and whether they can access the Internet via the Shiva VPN Gateway's web proxy.

There is one special user, root, who has the role of the final administrative user. This user has extra capabilities beyond any other user.

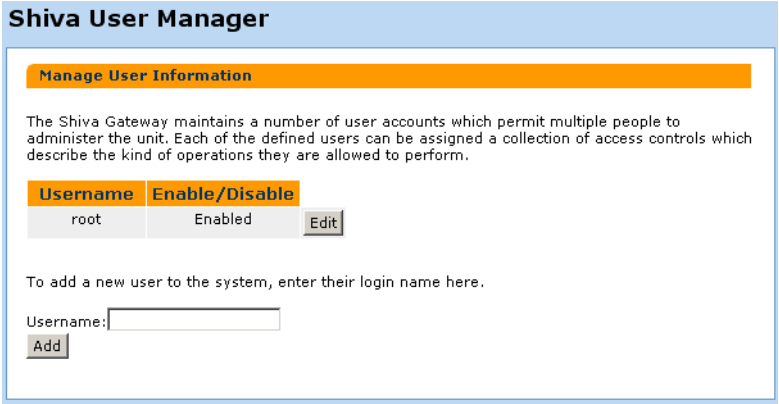
Note: *The root user is the only user permitted to telnet to a Shiva VPN Gateway.*

Web administration access controls are grouped into four broad categories: Administration, Diagnostic, Encrypted save/restore all and User settings. The root administrative user by default has permission to perform any action on the Shiva VPN Gateway. Other users default to no permission. All users can have their access controls modified (including root). To fully utilize access controls, the root user should have their access controls turned off and other users create to handle the day to day administrative duties.

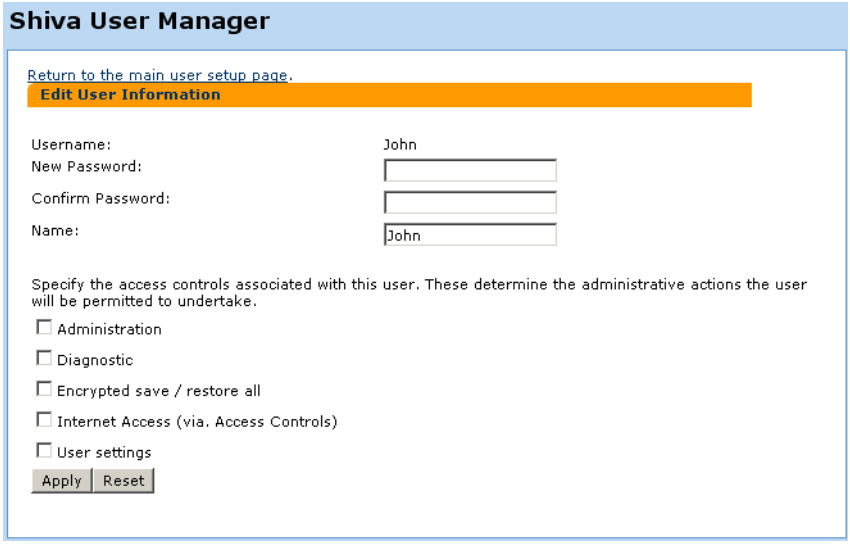
There is a fifth access control, Internet Access (via. Access Controls), that permits users web access through the Shiva VPN Gateway's web proxy.

Adding a user

1 Click **Users** under **System** on the left menu.



2. Specify a **Username** and click **Add**.



3. Configure the following settings.
   - Administration: A user with the administration access control is permitted to edit any configuration file on the Shiva VPN Gateway. It should be given to trusted users who are permitted to configure and reconfigure the unit.
   - Diagnostic: The diagnostic access control allows a user to view status reports, the technical support report, the system log and other read only pages. No capability is granted to allow such a user to edit any of the configuration on the Shiva VPN Gateway. This access control can be granted to technical support users so they can attempt to diagnose but not fix any problems which occur.
   - Encrypted save/restore all: A user with this access control can dump and restore the entire Shiva VPN Gateway's configuration via the encrypted save and restore option on the Advanced page. Such a user cannot edit the configuration nor even see the configuration files themselves. This access control can be allocated to a technician whom you want to be able to restore units to a known good configuration but to whom you do not wish to grant full administration rights.
   - Internet access (via access controls): A user with this access control is permitted controlled access to the web through the Shiva VPN Gateway's web proxy. See “Access control” on page 62 for details on controlling LAN users' web access.
   - User settings: A user with this access control can edit users' login information, create new users and modify access controls for other users. Without this access control, users can only change their own passwords. Because this access control allows a user to edit their own permissions, it is best left such that only the root user has it.

The root user is special. This user alone has one access control which cannot be removed. The root user is always able to edit user settings and thus they can grant themselves any access control if need be. The root user also has the capability to set User ID and Group ID when editing or creating users. It is best to leave these fields blank when creating a new user as this lets the Shiva VPN Gateway automatically allocate and manage them.

4. Click **Apply**

If somebody with the user settings access control attempts to edit the root user (apart from root themselves), they must enter the administrative password (i.e. the password for the root account).

Administrator password security

The Shiva VPN Gateway's administrative (root) password is used to restrict access to the Web Management Console web administration pages (Web Admin) and the Shiva VPN Gateway itself. The Shiva VPN Gateway administrative password is the 'key' to the security of your network and must be kept secret. It is recommended that you choose a password that is easy for you to remember but hard for unauthorized people to guess.

A potential security issue may be introduced by having a network-connected Shiva VPN Gateway accessible, using the factory default password. To prevent this, the password for the Shiva VPN Gateway should be changed when Setup Wizard is run or the Web Management Console web administration pages are accessed for the first time.

The Shiva VPN Gateway administrative password can be changed at any time using the Web Management Console web administration pages by clicking Password in the System menu.

The password is limited to 8 characters.

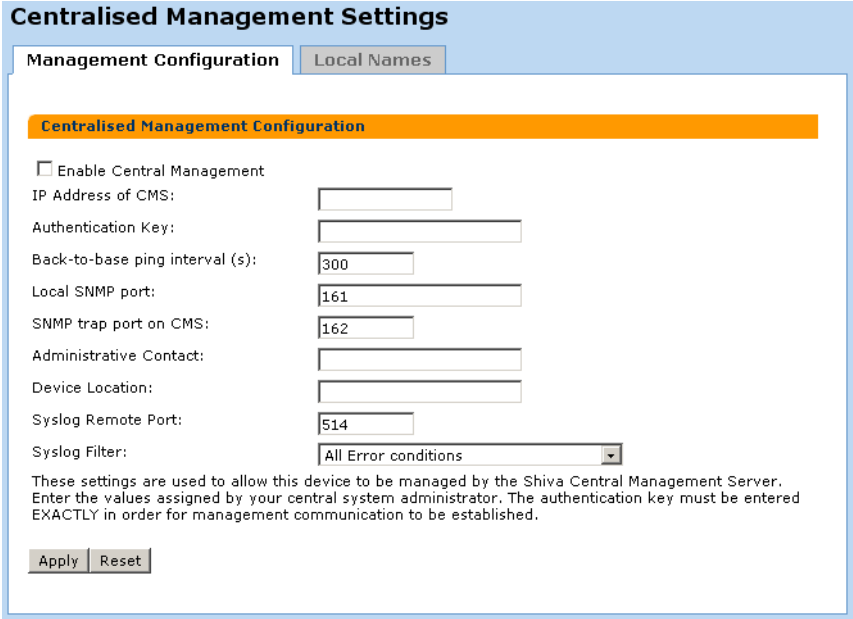
Note: *The username is root. The factory default Shiva VPN Gateway administrative password is default.*

Management settings

This tab enables the centralized policy based management of Shiva units.

Management configuration

To reach this page click **Management** under **System** on the left menu.



Enable Central Management

Enable centralized management.

IP Address of CMS

IP address of the Centralized Management System.

Authentication Key

Specifies a secret key that CMS uses to authenticate devices. This value must be the same as the value configured in CMS.

Back-to-base ping interval

Specifies the time (in seconds) between ALIVE traps sent to CMS.

Local SNMP port

The port on which the devices listen for SNMP from CMS.

Note: *This is not configured on the CMS -- each device sends the port on which it is listening to CMS in its regular trap.*

SNMP trap port on CMS

Specifies the local port to which devices send SNMP traps. The default value (162) is the standard SNMP trap port, however there may be reasons to use a different port, in which case the same value must be specified in the CMS configuration.

Administrative Contact

Can be any text value. This value will be shown under "Administrative contact" in the CMS.

Device Location

Can be any text value. This value will be shown under "Device Location" in the CMS.

Syslog Remote Port

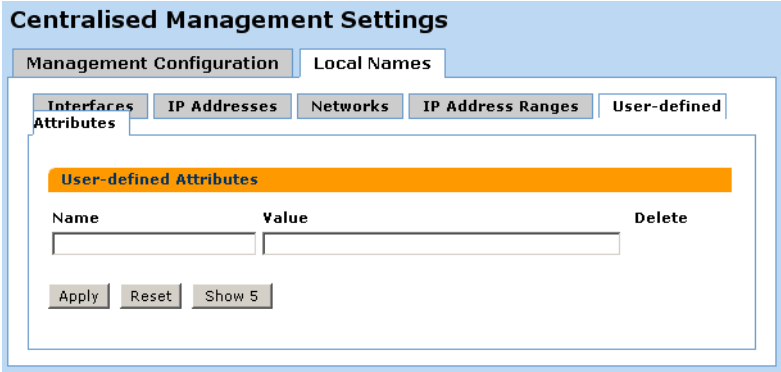
Specifies the port on which to listen for syslog messages. The default value (514) is the standard syslog port, however there may be reasons to use a different port, in which case the same value must be specified in the CMS configuration.

Syslog Filter

Choose the type of messages that will be logged.

Local names

To reach this page click **Management** under **System** on the left menu, the click the **Local Names** tab.

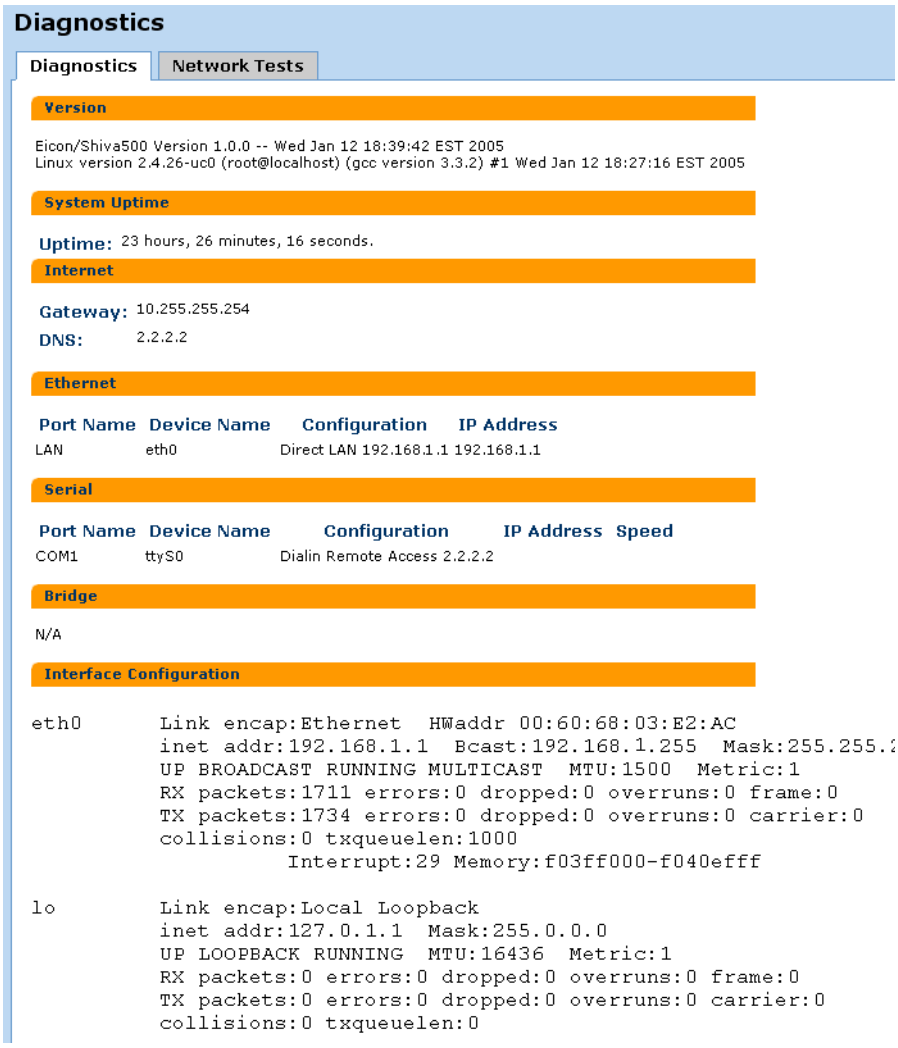


Diagnostics

Diagnostic information and tests are provided through the Web Management Console web administration pages.

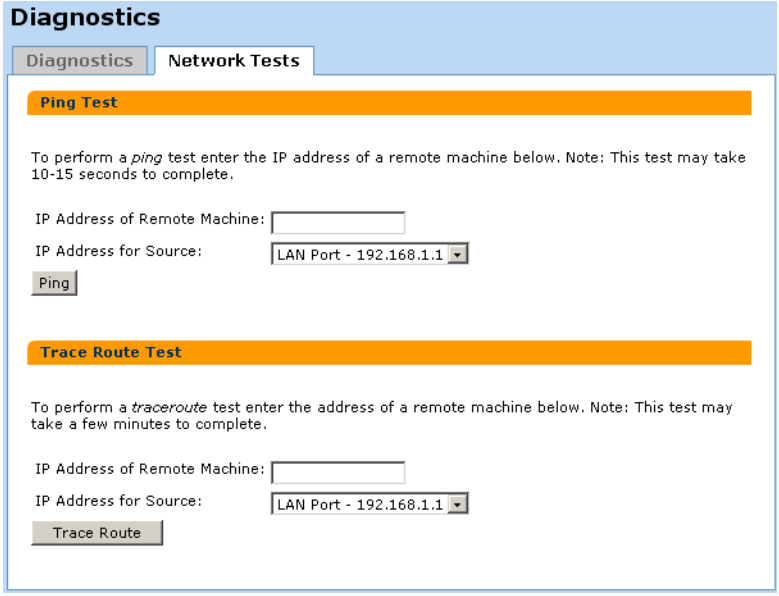
Diagnostics

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



Network tests

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

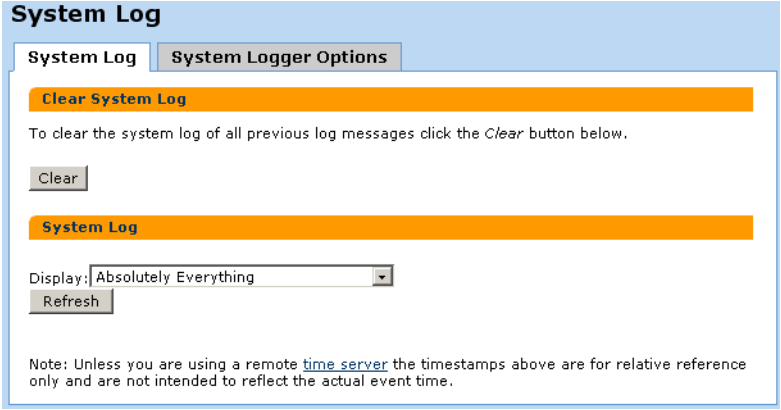


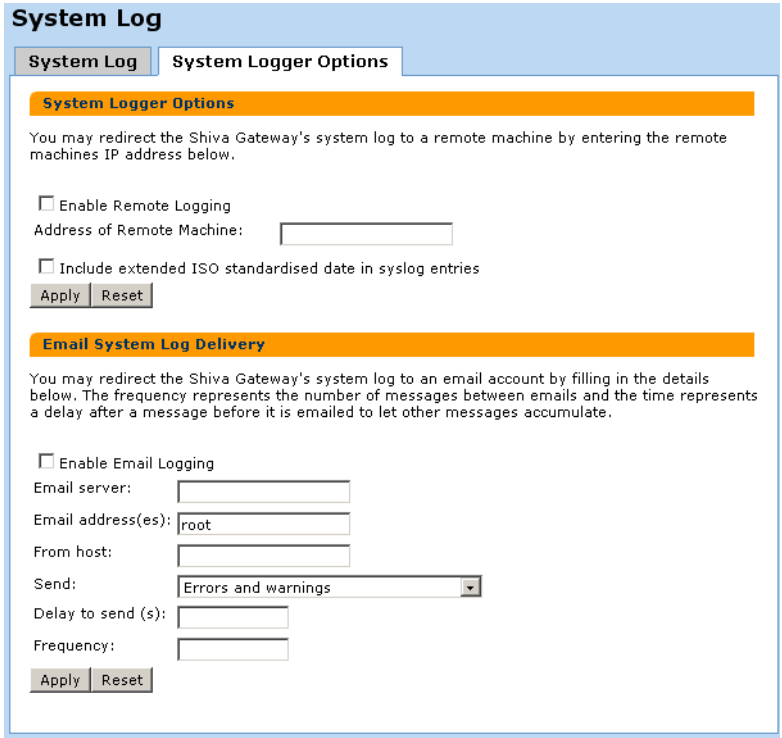
System log

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

The Shiva VPN Gateway also provides the option of re-directing log output to a remote machine using the syslog protocol. Enable this option by selecting Enable Remote Logging, entering the IP address of the remote machine and clicking Apply.

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





Access logging

It is possible to log any traffic that arrives at or traverses the Shiva VPN Gateway. 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 Shiva VPN Gateway 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>	will be empty, or one of eth0, eth1 and 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. ppp0 or ppp1 - a PPP session
ipsecX	e.g. ipsec0, 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: will thus look similar to the following:

Mar 27 09:31:19 2003 klogd: Default deny: IN=eth1 OUT=MAC=00:60:68:00: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 Shiva VPN Gateway 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 Shiva VPN Gateway to a server on the private network, the outgoing interface will be 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 Shiva VPN Gateway 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 web administration pages. 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 Shiva VPN Gateway, 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 will log 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 Shiva VPN Gateway (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 Shiva VPN Gateway'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=00:60:68:00:07:03:00:50: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 Shiva VPN Gateway, rather than attempting to pass through it.

A very similar scenario occurs for logging access requests that are attempting to pass through the Shiva VPN Gateway. It merely requires replacing the INPUT keyword with FORWARD.

Thus, to log permitted inbound requests to services hosted on a server behind the Shiva VPN Gateway, 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 will result in log output something like this:

<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 will use 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. If the name ends in a +, then any interface which begins with this name will match. e.g.

iptables -I FORWARD -j LOG -i eth0 -p tcp ...

This rule will log 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 will log 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 web administration pages, 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 Shiva VPN Gateway'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.

Configuration files

Clicking Configuration Files allows you to select and edit the Shiva VPN Gateway's configuration files manually. Generally, this should only be done at the request of customer support.

The Shiva VPN Gateway's entire configuration may be backed up remotely. Doing this is highly recommended as to minimize downtime in the event of a configuration loss. The configuration may be backed up in plain text, or encrypted with a password.

To backup to a plain text file, click store/restore and copy and paste the configuration into a text editor on the remote machine. Restoring is simply a matter of copying and pasting the configuration from the text file back into the same field on the Shiva VPN Gateway and clicking Submit.

You may also upload additional configuration files from your computer to the Shiva VPN Gateway under Upload file.

To backup to an encrypted file, click save and restore, enter a password and click Save under Save Configuration. To restore from this file, browse for the backup configuration file, enter the password you used to save it and click Restore under Restore configuration.

Flash upgrade

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

Before upgrading

Prior performing any firmware upgrade, it is important that you save a back up of your existing configuration (**Advanced > Store/restore** all configuration files) to a local file.

While we make every effort to ensure your existing configuration will work with the new firmware, sometimes compatibility problems will arise. You should be particularly aware of this possibility when performing a major upgrade.

Note: *An upgrade where the minor and/or major revision number is incremented is considered a major upgrade, e.g. 1.8.5 -> 1.9.2, or 1.9.2 -> 2.0.0, whereas a patch upgrade increments the patch revision number only, e.g. 1.9.0 -> 1.9.1, or 1.9.0 -> 1.9.2.*

Warning: *If the flash upgrade is interrupted (e.g. power down), the Shiva VPN Gateway will stop functioning and will be 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 Shiva VPN Gateway 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.*

Upgrade procedure

1 Download the appropriate flash upgrade file (*.eic) from the Eicon Networks web.

2. Open the **Advanced > Flash Upgrade** page.

3. In the **Flash Upgrade by HTTP** section, click the **Browse** button and select the firmware upgrade file from your hard drive.

4. Click **Upgrade**.

During the upgrade, the front panel lights on the Shiva VPN Gateway will flash more slowly than normal. At the end of the upgrade, all the lights will flash briefly then return to their normal state.

Warning: *If the flash upgrade is interrupted (e.g. power down), the Shiva VPN Gateway will stop functioning and will be unusable until its flash is reprogrammed at the factory or a recovery boot is performed. User care is advised.*

Reboot

Clicking this link will cause the Shiva VPN Gateway to perform a soft reboot. It will usually take around 10 seconds before it is up and running again. Note that if you have enabled bridging, the Shiva VPN Gateway may take up to 30 seconds to reboot.

Reset button

The simplest method to clear the Shiva VPN Gateway's stored configuration information is by pushing the reset button on the back panel of the Shiva VPN Gateway twice within two seconds. A bent paper clip is a suitable tool for performing this procedure.

Pushing the reset button twice clears all stored configuration information, reverts all settings to the factory defaults, and reboots the Shiva VPN Gateway.

Note: *When the Shiva VPN Gateway reboots, it will be configured with the IP address of 192.168.1.1, netmask 255.255.255.0.*

Technical Support

The System menu contains an option detailing support information for your Shiva VPN Gateway.

The Technical Support Report is an invaluable resource for the Shiva VPN Gateway technical support team to analyze problems with your Shiva VPN Gateway. The report gives the support team important information about any problems you may be experiencing.

If you experience a fault with your Shiva VPN Gateway and have to contact the technical support team, ensure that you include the Technical Support Report with your support request. The Technical Support Report should be generated just after the issue has occurred with the Shiva VPN Gateway, and should be supplied in plain text format.

Chapter 7

Terminology

This chapter describes terms that are commonly used in this document.

Term	Description
ADSL	Asymmetric Digital Subscriber Line. A technology allowing high-speed data transfer over existing telephone lines. ADSL supports data rates between 128 kbps to 8 Mbps when receiving data and between 64 kbps to 768 kbps 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 must be used to allow parties that are configured with a dynamic IP address and a preshared secret to connect or if the Shiva VPN Gateway 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.

Term	Description
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 Shiva VPN Gateway.
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 Shiva VPN Gateway, it must conform to the draft draft-ietf-ipsec-dpd-00.txt

Term	Description
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 Shiva VPN Gateway cannot communicate with the Internet. If this occurs, the Shiva VPN Gateway automatically moves to a lower speed, secondary Internet connection.

Term	Description
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 Shiva VPN Gateway 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.

Term	Description
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.
IPSec with Dynamic DNS	Dynamic DNS can be run on the IPSec endpoints thereby creating an IPSec tunnel using dynamic IP addresses.
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 that will be used. The traffic to which the policies will 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 Shiva VPN Gateway. The passphrase is a key that can be used to lock and unlock the information in the private key certificate.
Local Public Key Certificate	The public part of the public/private key pair of the certificate resides on the Shiva VPN Gateway 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 Shiva VPN Gateway has a MAC address for each Ethernet interface. These are listed on a label on the underneath of the device.

Term	Description
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.

Term	Description
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.

Term	Description
RSA Digital Signatures	A public/private RSA key pair used for authentication. The Shiva VPN Gateway 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.

Term	Description
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 Shiva VPN Gateway before a tunnel can be configured to use them (see Certificate Management).

Chapter 8

International Regulatory Information

This chapter provides regulatory information for all regions.

Shiva 500 / Shiva 1100 VPN Gateway

Regulatory information for the USA

WARNING. Changes or modifications to this unit not expressly approved by Eicon Networks Corporation could void the user's authority to operate the equipment.

Declaration of Conformity
We:

Eicon Networks
Parkway Centre II
2805 N. Dallas Parkway
Suite 200
Plano, TX 75093
(972) 473-4500
Fax:(972) 473-4510

Declare under our sole legal responsibility that the products listed below to which this declaration relates, are in conformity with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) This device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

RF Exposure Statement
IMPORTANT NOTE: To comply with FCC RF exposure compliance requirements, the antenna used for this transmitter must be installed to provide a separation distance of at least 20cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

Regulatory information for Canada

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference, including interference that may cause undesired operation of the device.

Antenna Statements

This device has been designed to operate with an antenna having a maximum gain of 1.46dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to others, the antenna type and its gain should be so chosen that the equivalent isotropic radiated power (EIRP) is not more than that required for successful communication.

RF Exposure Statement

The installer of this radio equipment must ensure that the antenna is located or pointed such that it does not emit RF fields in excess of Health Canada limits for the general population; consult safety code 6, obtainable from Health Canada's website www.hc-sc.gc.ca/rpb.

Regulatory information for Europe

CE EU Declaration of Conformity

Eicon Network Corporation declares that this equipement is in compliance with the Electromagnetic Compatibility Directive 89/336/EEC and the Low Voltage Directive 73/23/EEC.

A detailed declaration of conformity for this product can be found: http://www.eicon.com/worldwide/about/declarations/default.htm.

Radio Approvals

To determine whether you are allowed to use this wireless device, check the list below for restrictions on use, if any, in the intended country of use.

Country	Radio Transmitter	Approval refreence	Restrictions
Austria	WMIR-103G	CE Alert, R&TTE Directive 1999/5/EC	
Belgium	WMIR-103G	CE Alert, R&TTE Directive 1999/5/EC	For outdoor useage only channel 10 (2457MHz) and 11 (2462MHz) is allowed. For private useage outside buildings across public grounds over less than 300m no special registration with IBPT/BIPT is required. Registration to IBPT/BIPT is required for private useage outside buildings across public grounds over more than 300m. An IBPT/BIPT licence is required for public useage outside buildings. For registration and licence please contact IBPT/BIPT.
Cyprus	WMIR-103G	CE Alert, R&TTE Directive 1999/5/EC	
Czech Republic	WMIR-103G	CE Alert, R&TTE Directive 1999/5/EC	
Denmark	WMIR-103G	CE Alert, R&TTE Directive 1999/5/EC	
Estonia	WMIR-103G	CE Alert, R&TTE Directive 1999/5/EC	
Finland	WMIR-103G	CE Alert, R&TTE Directive 1999/5/EC	
France	WMIR-103G	CE Alert, R&TTE Directive 1999/5/EC	Restricted frequency band: When operating this device on French territory, you may only do so, using the channels 10 and 11 (2457MHz and 2462MHz respectively). It is not allowed to operate the device at any other channel as supported by the device. Licence required for every indoor installation (please contact ART for procedure to follow). Use outdoors is not allowed.
Germany	WMIR-103G	CE Alert, R&TTE Directive 1999/5/EC	Licence required for outdor installations. Check with reseller for procedure to follow.
Greece	WMIR-103G	CE Alert, R&TTE Directive 1999/5/EC	
Hungary	WMIR-103G	CE Alert, R&TTE Directive 1999/5/EC	
Iceland	WMIR-103G	CE Alert, R&TTE Directive 1999/5/EC	
Ireland	WMIR-103G	CE Alert, R&TTE Directive 1999/5/EC	
Italy	WMIR-103G	CE Alert, R&TTE Directive 1999/5/EC	Licence required for indoor use. Use with outdor installations not allowed.
Latvia	WMIR-103G	CE Alert, R&TTE Directive 1999/5/EC	
Lithuania	WMIR-103G	CE Alert, R&TTE Directive 1999/5/EC	
Luxembourg	WMIR-103G	CE Alert, R&TTE Directive 1999/5/EC	
Malta	WMIR-103G	CE Alert, R&TTE Directive 1999/5/EC	
Netherlands	WMIR-103G	CE Alert, R&TTE Directive 1999/5/EC	Licence required for outdor installations. Check with reseller for procedure to follow.
Poland	WMIR-103G	CE Alert, R&TTE Directive 1999/5/EC	
Portugal	WMIR-103G	CE Alert, R&TTE Directive 1999/5/EC	
Slovak Republic	WMIR-103G	CE Alert, R&TTE Directive 1999/5/EC	
Slovenia	WMIR-103G	CE Alert, R&TTE Directive 1999/5/EC	
Spain	WMIR-103G	CE Alert, R&TTE Directive 1999/5/EC	
Sweeden	WMIR-103G	CE Alert, R&TTE Directive 1999/5/EC	
United Kingdom	WMIR-103G	CE Alert, R&TTE Directive 1999/5/EC	