NetComm™

Mobile VPN Firewall

User Guide

VPN100

NetComm™ Broadband Solutions

Legal & Regulatory Information Copyright Information

Customer Information

ACA (Australian Communications Authority) requires you to be aware of the following information and warnings:

(1) This unit shall be connected to the Telecommunication Network through a line cord which neets the requirements of the ACA TS008 Standard.

(2) This equipment has been tested and found to comply with the Standards for C-Tick and or A-Tick as set by the ACA . These standards are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio noise and, if not installed and used in accordance with the instructions detailed within this manual, may cause interference to radio communications. However, there is no guarantee that interference will not occur with the installation of this product in your home or office. If this equipment does cause some degree of interference to radio or television reception, which can be determined by turning the equipment off and on, we encourage the user to try to correct the interference by one or more of the following measures:

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

(3) The power supply that is provided with this unit is only intented for use with this product. Do not use this power supply with any other product or do not use any other power supply that is not approved for use with this product by NetComm. Failure to do so may cause damage to this product, fire or result in personal injury.

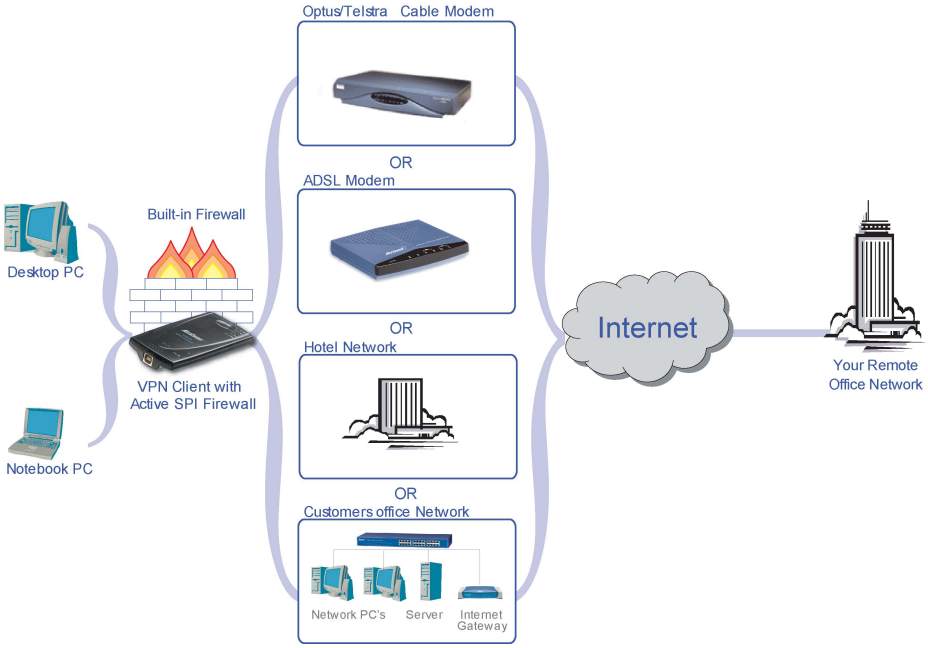
(4) The VPN100 portable VPN adaptor achieved class B compliance when used with a class B compliant PC. Compliance with class B EMI is not assured when the adaptor is used with a non-compliant PC.

Contents

Introduction

Congratulations on your purchase of the NetComm VPN100. The NetComm VPN100 is designed to provide a portable solution for your PC security. This lightweight network interface with advanced security features allows you to connect to the Internet through any broadband connection (such as ADSL, Cable or a hotel's Broadband/Ethernet Internet service).

The NetComm VPN100 protects your PC from most known Internet attacks with a powerful Stateful Packet Inspection firewall. At the same time it can create a secure encrypted VPN Tunnel back to your office Network.



The NetComm VPN100 connects to virtually any PC through the USB port, and requires no external power supply. Once you're connected, you can establish a Virtual Private Network tunnel from your PC to a corporate network using the popular IPSec VPN standard, and your transmitted data will be protected by government-spec DES or Triple-DES encryption. This makes the VPN100 a perfect traveling companion, allowing you to securely connect to your home resources to retrieve files, or check your local email. Once you're connected over VPN, it's just like being part of the remote network.

With a web-based UI (User Interface), this NetComm VPN100 is easy to setup and maintain via web browsers such as Netscape Communicator and Internet Explorer.

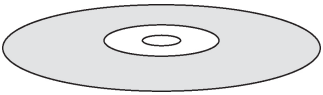
Package Contents

The following items should be contained in your NetComm Personal Firewall VPN Adaptor Package:

- NetComm Personal Firewall VPN Adaptor (VPN100)

- Package Contents Note and Traveller's Guide

- NetComm Driver CD-ROM (including drivers and additional user guide)



- Etherent Network Cable (RJ-45)

- USB Connection Cable

Check the contents of your package and, if any parts are missing or damaged, please contact your Dealer.

Default Settings & Facts

The following lists the default settings of your NetComm VPN100.

Router

LAN IP:	192.168.1.1
Username:	<none>
Password:	admin

Resetting

While using or installing your NetComm VPN100 you may need to utilise the reset feature. There are two types of reset:

Soft

A soft reset will restart the unit and reconnect to the internet using the settings stored previously, none of your settings are deleted. To perform a soft reset briefly press the reset button on the back of the unit.

Hard

A hard reset will return your unit to its factory default setting, meaning that you will loose all configurations and logs set/stored previously. To perform a hard reset, press and hold in the reset button on the back of the unit for 10 seconds. You must have USB connected for at least one minute before performing a reset.

Contact Information

If you have any technical difficulties with your product, please do not hesitate to contact NetComm's Customer Support Department.

Email: support@netcomm.com.au

Fax: (02) 9424-2010

Web: www.netcomm.com.au

Features of the NetComm VPN100

Your NetComm VPN100 contains the following features that make it excellent for the executive on the road.

- A USB-attached network interface.
- Provides network security through a powerful firewall engine.
- Prevents hackers from launching a DoS attack to overwhelm your computer, offering advanced protection with SPI.
- Establishes an IPSec Virtual Private Network tunnel to your corporate network.
- Blocks inappropriate web sites, cookies and Javascript, if required.
- Supports PPPoE to connect via ADSL.
- Built-in web-based user interface for easy configuration and management through common web browsers like Netscape or Internet Explorer.
- Supports DHCP client to receive a dynamic IP Address from your ISP.
- Built-in DHCP server to automatically assign your computer an IP address.
- Allows administrators to block specific LAN users from accessing specified applications or services.
- USB interface -- can be used with a computer that does not have a Network Interface Card (NIC).

Firewall

DoS is the acronym for Denial of Service, which refers to the response when a computer or network is overwhelmed to the point that it can no longer function normally. For example, a hacker may use a fake IP address to build connections to flood the compuer they want to attack. TCP works by sending a SYN packet to the server from the client. After the server receives the SYN packet, a SYN-ACK is sent back to client. The server will then wait for a response to the SYN-ACK. If the hacker sends hundreds of SYN packets to a server with a false address, the server allocates computer and memory resources to establishing a connection - since the server does not know a legitimate SYN message from a false message. By flooding the server with such a large volume of requests, the server's maximum capacity can easily be used by these false attempts to establish a connection - this is what the firewall is designed to prevent.

SPI is the acronym of Stateful Packet Inspection. The SPI engine examines not just the headers of the packet, but also the contents, to determine more about the packet than just its source and destination information. Moreover, stateful inspection firewalls also close off ports until a connection to the specific port is requested.

VPN100 LEDs

The following figure shows the top view of the NetComm VPN100.

The LEDs on the top indicate the status of the unit.

LED	Colour	Description
Session	Orange.	The Session LED indicates a successful VPN Tunnel has been established between two endpoints.
Diag	Red.	The Diag LED lights up when the Adapter goes through its self-diagnosis mode during every boot-up. It will turn off upon successful completion of the diagnosis.
Link/Act	Green.	The Link/Act LED serves two purposes. If the LED is continuously lit, the Adapter is successfully connected. If the LED is flickering, the Adapter is actively sending or receiving data.
Full/Col	Green.	The Full/Col LED also serves two purposes. If this LED is lit up continuously, the connection is running in Full Duplex mode. If the LED flickers, the connection is experiencing collisions. If this LED flickers too often, there may be a problem with your connection. See “Appendix A: Troubleshooting” if you encounter this problem.
100	Orange.	The 100 LED lights up when a successful 100Mbps connection is made. If this LED does not light up, then your connection speed is 10 Mbps.
USB	Green.	The USB LED lights up when the Adapter is connected to a PC and powered on.

Hardware

This chapter provides information about your NetComm VPN100's physical features and gives step-by-step installation instructions.

Connecting your Router

1. Before you begin, make sure that all of your hardware is powered off, including the Adapter, PCs, cable or DSL modem, and/or Router.
2. Connect one end of the USB cable to the USB port on the Adapter and the other end of the USB cable to a USB port on your PC.

3. Connect one end of an Ethernet cable to the Ethernet port on the Adapter, and the other end to an Ethernet port (LAN port) on a Network. If you are not using a Router, you can connect it directly to a Cable or DSL modem.

If the PC is powered up:

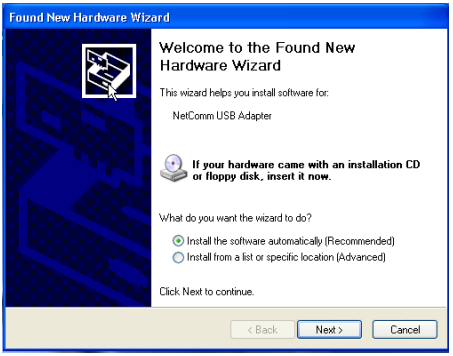
- The USB LED will light up green as soon as the Adapter is connected correctly to the PC.
- The Diag LED will light up red for a few seconds when the Adapter goes through its self-diagnostic test. This LED will turn off when the self-test is complete.

4. Turn on the PC, cable or DSL modem and/or Router.
5. If this is the first time you have connected the VPN100 Adapter to this computer, you will be prompted to install drivers by Windows. Refer to the following section and follow the instructions for the version of Windows you are using.

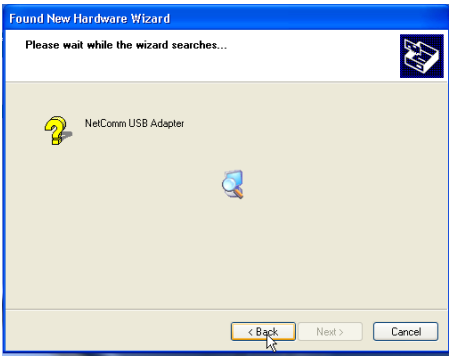
Driver Installation

Windows XP

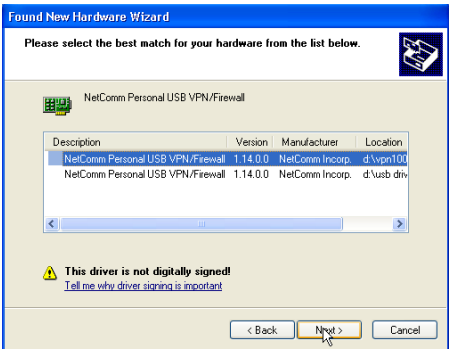
1. Insert the NetComm Driver CD-ROM in your CD-ROM drive and turn on your computer.
2. When prompted by the Found New Hardware Wizard confirm that "**Install the software automatically (Recommended)**" is selected and click on **Next>**.



3. The Found New Hardware Wizard will search for the correct driver.

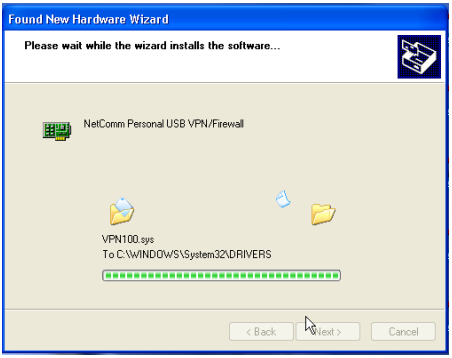


4. Select the NetComm Personal USB VPN/ Firwall and click on Next>.

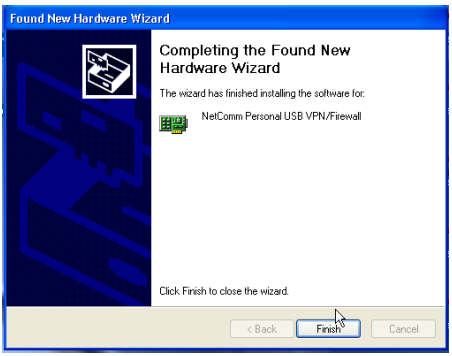


5. If prompted, click on **Continue Anyway** to proceed with the installation.

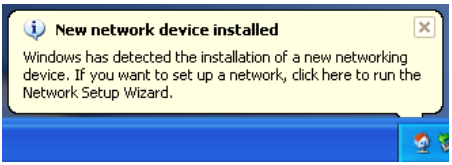
6. Windows will install the driver on your system.



7. Click on **Finish** to complete the installation.

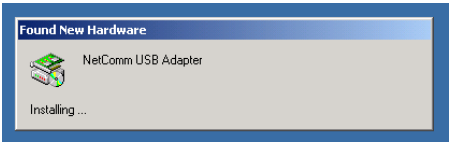


8. Windows XP will advise that a **new network device** has been installed.

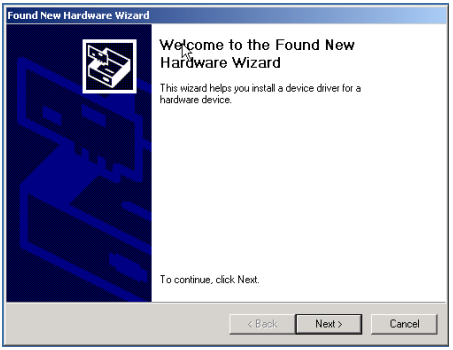


Windows 2000

1. Insert the NetComm Driver CD-ROM in your CD-ROM drive and turn on your computer.
2. The NetComm USB Adaptor will be located.

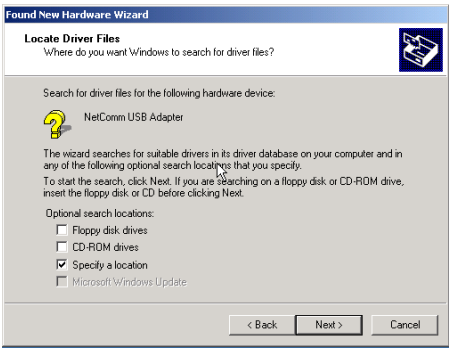


3. The Found New Hardware Wizard will appear. Click **Next>** to continue.

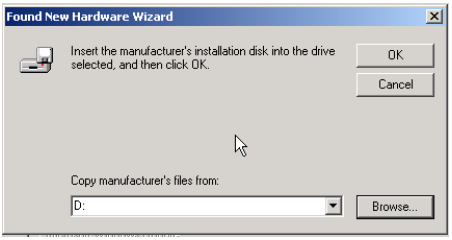


4. Select "**Search for a suitable driver for my device (recommended)**" and click on **Next>**.

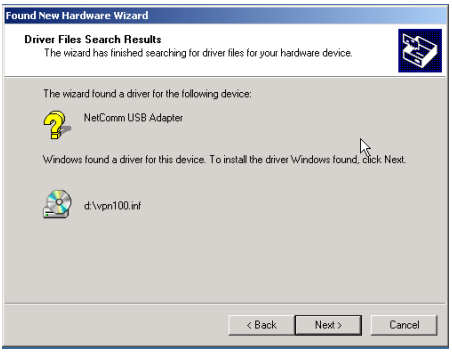
5. Select "**Specify a location**" and click on **Next>**.



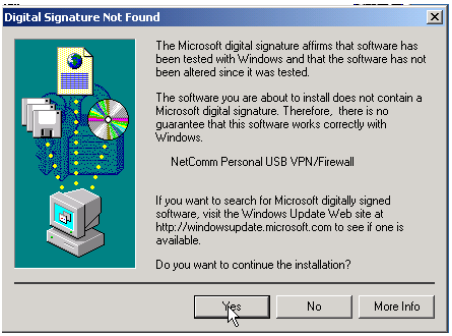
6. The Found New Hardware Wizard will prompt for a location to search for the driver. Type the drive letter of your CD-ROM (ie D:\ where D is the letter of your CD-ROM drive) and click **OK**.



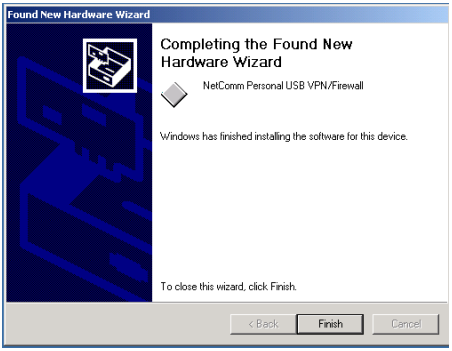
7. The Found New Hardware Wizard will locate the driver on the CD-ROM and display the result. Click **Next>** to continue.



8. If the Digital Signature Not Found window appears, click **Yes** to continue.

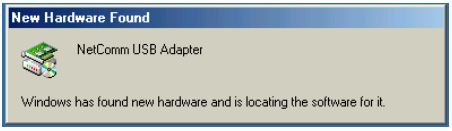


9. The driver will be installed on your system. Click **Finish** to complete the installation.



Windows Me

1. Insert the NetComm Driver CD-ROM in your CD-ROM drive and turn on your computer.

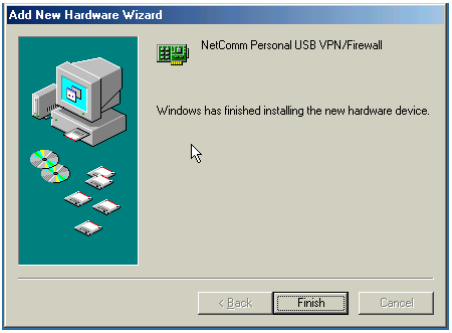


2. The NetComm USB Adaptor will be located.

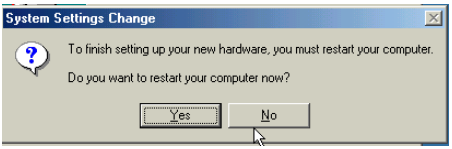
3. The Add New Hardware Wizard will appear. Select "**Automatic search for a better driver [Recommended]**" and click on **Next>**.

4. The Add New Hardware Wizard will search for the driver and display the result. Click **Next>** to continue.

5. After the Add New Hardware Wizard has completed the installation of the driver, click **Finish**.

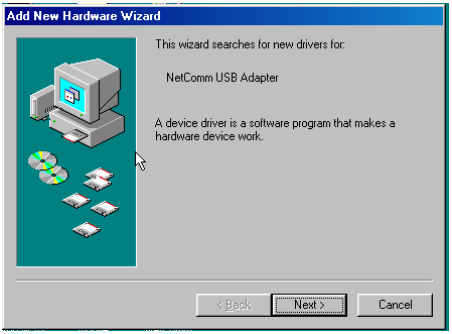


6. You may be prompted to restart your machine. Click on **Yes**.



Windows 98 - USB

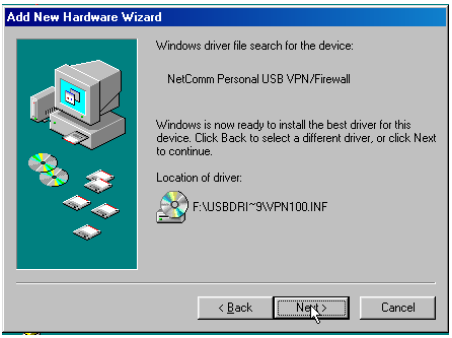
1. Insert the NetComm Driver CD-ROM in your CD-ROM drive and turn on your computer.
2. The NetComm USB Adaptor will be located.



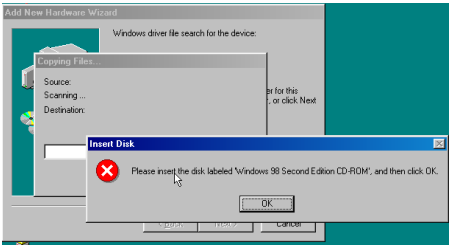
3. The Add New Hardware Wizard will appear. Select "**Search for the best driver for your device [Recommended]**" and click on **Next>**.

4. Select **CD ROM Drive** and click **Next>** to continue.

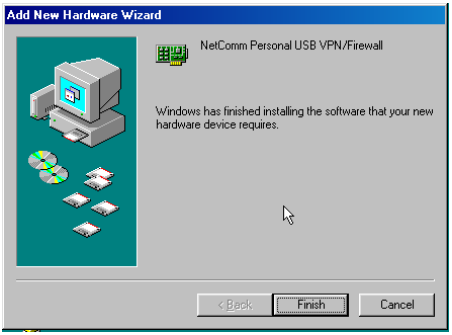
5. The Add New Hardware Wizard will locate the driver for your **NetComm Personal USB VPN/Firewall**. Click **Next>** to continue.



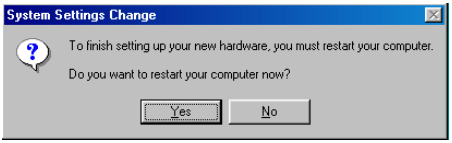
6. You may be prompted to Insert your Windows 98 SE CD-ROM. If so insert this and click **OK** to contiue.

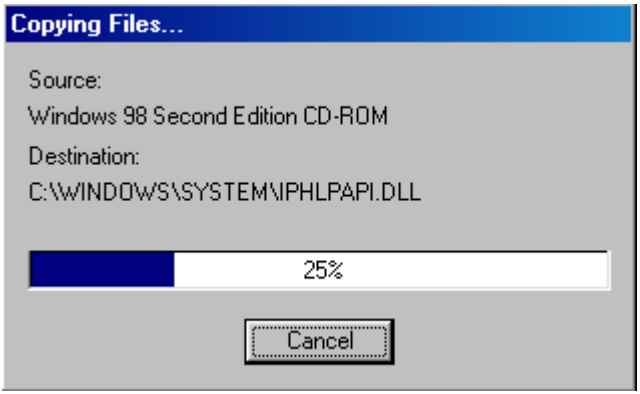


7. The Add New Hardware Wizard will continue with the installation and will advise when it has completed the installation. Click on **Finish**.



8. You may be prompted to restart your machine. Click on **Yes**.





Configuring your VPN100

This chapter describes the procedures necessary to configure the basic functions and to start up your NetComm VPN100. On successful completion of these procedures, you will be able to access the Internet via your NetComm VPN100.

Before you begin

In order to allow a quick reference point when setting up your NetComm VPN100, it is suggested you complete the table below with the necessary information, which should be supplied by your ISP:

Provided by some ISPs (✓ tick indicates common minimal requirements)

Host Name: _____

Domain Name: _____

IP address given by ISP:

✓❒ Obtain IP Address automatically, or

✓❒ Static IP

IP Address (if static): _____._____._____._____

Subnet Mask: _____._____._____._____

Default Gateway: _____._____._____._____

DNS Server Primary: _____._____._____._____

DNS Server Secondary (optional): _____._____._____._____

DNS Server Third (optional): _____._____._____._____

✓**PPP authentication:**

❒ PPPoE

❒ PPTP

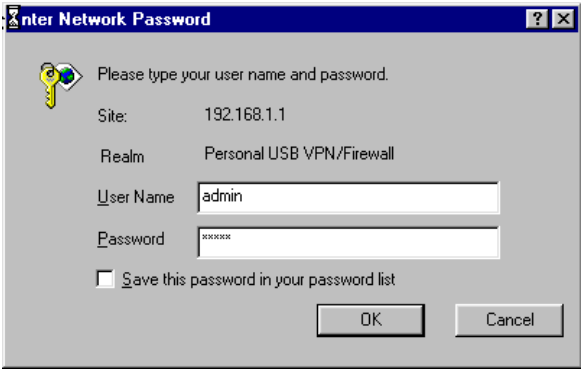
✓User Name: _____

✓Password: _____

Using the Web-based User Interface

The NetComm VPN100 uses a Web-based User Interface for configuration. Start your web browser and type http://192.168.1.1 in the browser's *address box*. This address is the factory default IP Address of your NetComm VPN100. Press "**Enter**".

The **"Username and Password Required"** prompt box will appear. Leave the **"User Name"** empty and type **"admin"** (default password) for the **"Password"**. Click "**OK**". The setup screen will load.

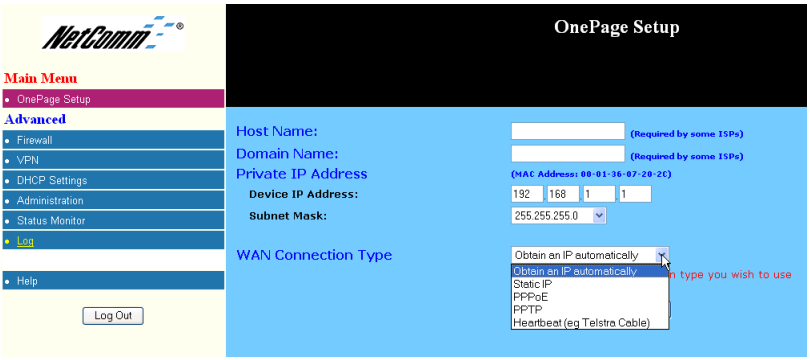


Note: This password should be changed via the Administration page immediately. The password can be reset by restoring the factory defaults with the Reset button.

When making changes to the settings, click on the "Apply" button before moving to another page. The router will reboot and refresh the screen in 5 seconds. Continue the session by selecting more menu items.

One Page Setup

The **"OnePage Setup"** screen is the first screen you will see when you access the VPN100's configuration. If the router has already been successfully installed and set up, this screen's values will already be properly configured. Below is a description of each setting.



- **Host Name** This entry is required by certain ISPs.
- **Domain Name** This entry is required by certain ISPs.
- **Time Zone:** Select your time zone from the pop-down list.
- **Private IP Address** The Device IP Address and Subnet Mask of the router are used by the internal LAN. The default values are 192.168.1.1 for IP Address and 255.255.255.0 for

Subnet Mask.

WAN Connection Type

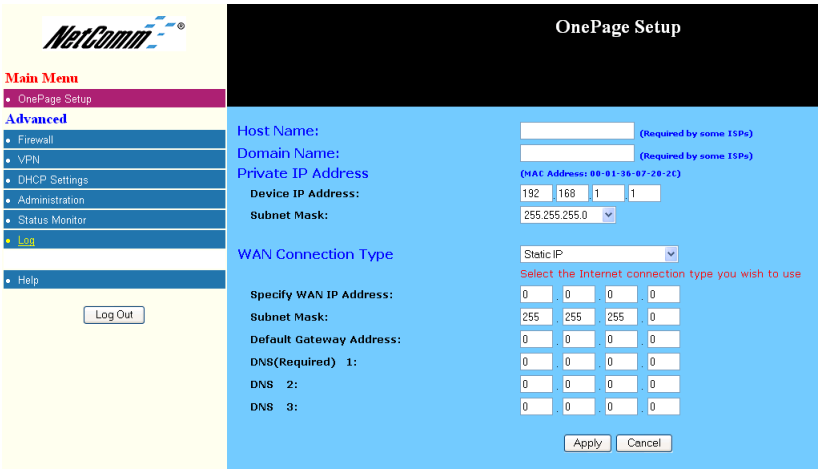
There are a number of options for WAN connection types: **Obtain IP automatically** (eg Optus Cable), **Static IP**, **PPPoE** (ADSL), **HeartBeat** (eg Telstra Cable) and **PPTP**. If you do not know which connection type you currently use, contact your ISP to get the information.

Obtain IP automatically (eg Optus Cable)

Obtain IP automatically is the default option for the router. If your ISP automatically assigns the IP addresses and other values to the NetComm VPN100, use this option. This option is the most commonly used setting for connecting to a corporate LAN.

Static IP

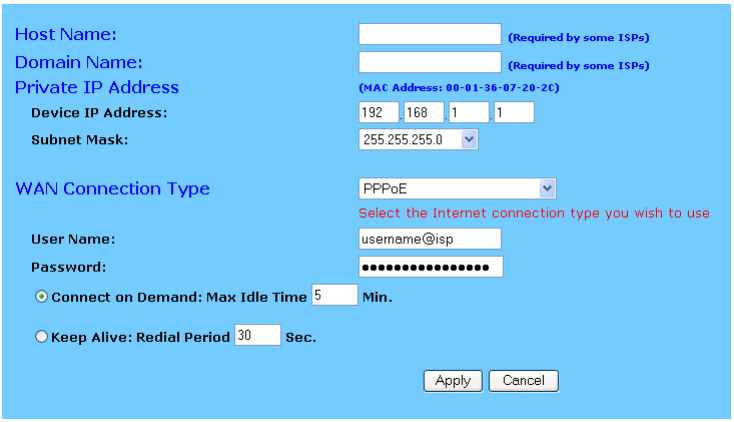
Static IP Addresses are most commonly used when connecting your VPN100 to the ethernet LAN of an office that you are visiting. Using “Obtain IP automatically” or DHCP is preferable but may not be possible if the Local Office LAN doesn’t support DHCP.



- **Specify WAN IP Address** Enter the IP address provided by your ISP.
- **Subnet Mask** Enter the subnet mask values provided by your ISP.
- **Default Gateway IP Address** Your ISP will provide you with the Default Gateway IP Address.
- **Domain Name Server (DNS)** Your ISP will provide you with at least one DNS IP Address. Multiple DNS IP settings are common. The first available DNS entry is used in most cases.

PPPoE

If your ISP provides PPPoE connectivity, choose this item from the drop-down list.

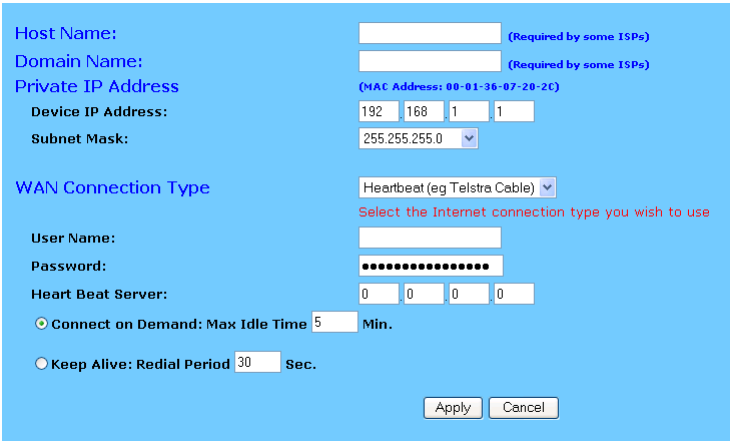


Note: If you select PPPoE, you will no longer need to use any existing PPPoE applications on any computers to connect to the Internet.

- **User Name** Enter the user name as provided by your ISP.
- **Password** Enter the password as provided by your ISP.
- **Connect-on-demand** Is a utility to trigger the PPPoE session to connect if in a disconnected state when Internet access is being attempted. Choose "**Enable**" to make this function active, and enter the number of minutes you wish to wait after network idle time in the "**Max Idle Time"** location. This is the amount of time the router will remain connected after network traffic has ceased. This function is for PPPoE only and is mainly used for security.
- **Keep Alive** This function keeps your PPPoE connection always on even during a period of no WAN activity. In some situations the PPPoE session cannot be restored immediately after disconnection because the ISP's system may need time to restore. Check with your ISP to ascertain how much time is required before the router starts to re-build the PPPoE session and enter this into the "**Redial Period**" field.

HeartBeat

If your ISP provides Heartbeat connectivity, choose this item from the drop-down list.



- **User Name** Enter the user name as provided by your ISP.
- **Password** Enter the password as provided by your ISP.
- **Heart Beat Server** When you select the "HeartBeat (eg Telstra Cable)" option for your WAN connection type in the NetComm router One-Page Setup, you may also need to specify the Heart Beat Server's IP address.

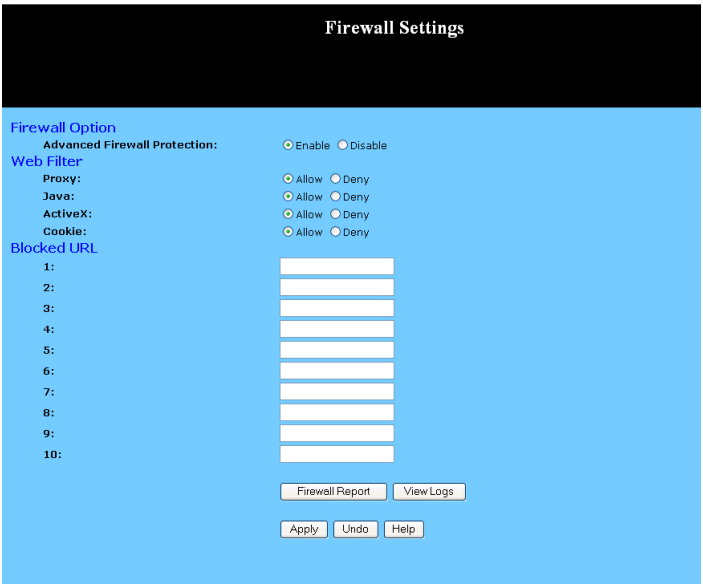
When you have properly configured the Setup page, click "**Apply"**. Your Router will then attempt to connect to the Internet. If you experience problems, please refer to the Trouble Shooting section before contacting NetComm Technical Support.

Advanced Applications

This chapter provides information on how to set up and use the advanced features of your NetComm VPN100.

Firewall

The Firewall setting page allows you to configure advanced Firewall functions to provide superior security for your network environment. You must click **"Apply"** to make any changes active.



- **Firewall Option** Enable this function to prevent DoS (Denial of Service) attacks and to use SPI (Stateful Packet Inspection). SPI function will check the contents of incoming data packets for malicious attacks. Temporarily disable this option if you have a particularly sensitive Internet application that does not funciton through the router.
- **Web Filter** This feature provides the ability to filter potential risks contained in web pages accessed by LAN users.

  Web proxy is a server your device will connect to when you access any web site. Setting a web proxy can save accessing time but may create a security issue by bypassing any URL filters or IP blocking you have configured. For example, if you configure the Broadband Firewall Router to block the access of 216.115.102.76 that is the IP address of www.yahoo.com, it will fail if your browser is using a proxy because the router only sees the connection to the proxy and then the proxy connects to yahoo. If you block the use of proxies then all connections must be made directly through the router.

Java & **Active X** are programming languages for web pages. However, some Trojan programs are also written in these programming languages. If you deny either of these, you may not be able access some parts of web sites.

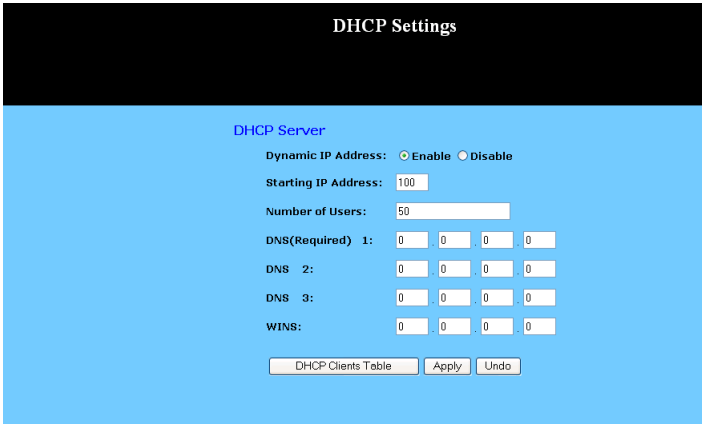
A **cookie** is data stored on your computer, which a web server can retrieve to identify your machine. It is a piece of text with an ID number. Cookies can be blocked by the router if the "Deny" option is selected.

- **Blocked URL** This feature allows you to restrict LAN users to access specific web sites. Enter the keyword text included in the URLs (Internet address) or whole URLs you wish to block in the fields supplied. For example, if you enter "google" then both www.google.com and www.google.co.uk will be blocked.
- **Time Filter** This feature allows you to limit WAN/Internet access according to a time schedule. Check "**Block LAN**" to restrict the connection from your LAN to the WAN/ Internet. Check "**Block WAN**" to restrict the connection from the WAN/Internet to your LAN servers that were set as virtual servers, port forwards or DMZ host. Check "**Block Both**" to restrict both connections. Check "Disable" to turn off this function. Set the time schedule from the drop-down list.

Click **Apply** after making any changes.

DHCP Configuration

A DHCP (Dynamic Host Configuration Protocol) Server can automatically assign IP Addresses and other information to each computer in your network. Unless you already have a DHCP Service on your LAN, it is highly recommended that you set your router to act as a DHCP server.

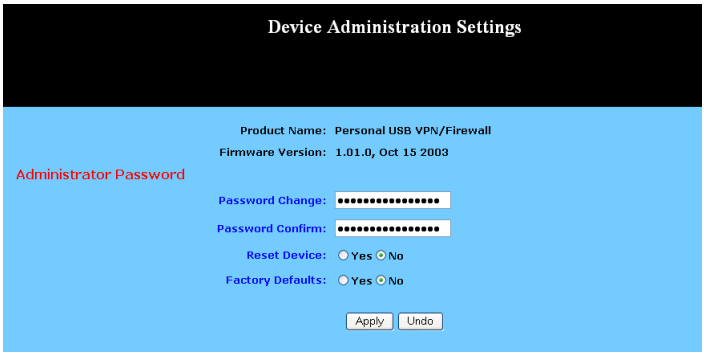


Note: The DHCP Server can support a maximum pool of 253 IP Addresses.

- **Dynamic IP Address** Select **"Enable"** to set your Router to act as a DHCP server. If you already have a DHCP server on your network, set the router's DHCP option to **"Disable"**.
- **Starting IP Address** Enter a numerical value, from 2 to 254, for the DHCP server to start at when assigning IP Addresses.
- **Number of Users** Enter the maximum number of computers that you want the DHCP server to assign IP Addresses to, with the absolute maximum being 253.
- **DNS1, 2, 3** Enter the DNS numbers you wish to be assigned to DHCP clients.
- **WINS** Enter the WINS number you wish to be assigned to DHCP clients.
- **DHCP Clients Table** Click the DHCP Clients Table button to show current DHCP client information.

Administration Settings

This feature allows the administrator to manage the NetComm VPN100 by setting certain parameters. For security reasons, it is strongly recommended that you set a Password and SNMP communities so that only authorized persons are able to manage your NetComm VPN100. If the **"Password"** is left blank, all users on your network can access the router simply by entering the unit's IP Address into their web browser's location window.



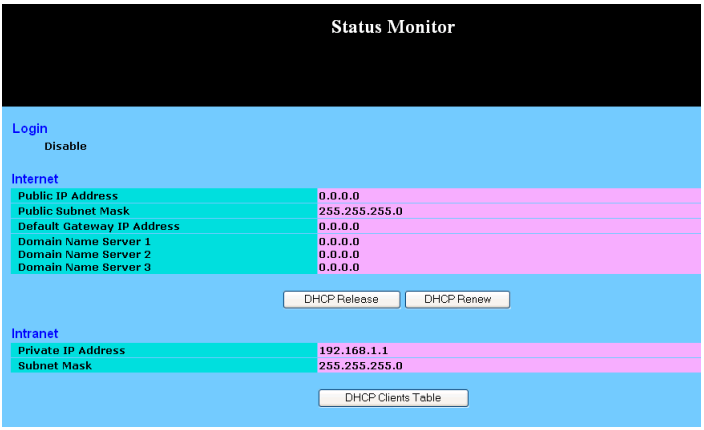
- **Firmware Version** This field shows the installed version of the firmware.
- **Administrator Password** Enter the password you want to use into the **"Password Change"** field and re-enter it into the **"Password Confirm"** field for confirmation. Be sure that the password is less than 64 characters long and without any spaces.
- **Reset Device** Select **"Yes"** if you want to clear connections, reboot, and re-initialize the unit without affecting any of your configuration settings.
- **Factory Defaults** Select **"Yes"** if you want to return all the router's current settings to their factory default settings.

Note: Do not restore to the factory defaults unless it is absolutely necessary.

Click **"Apply"** to make any changes.

Status Monitor

This screen shows the router's current status. All of the information provided is read-only.



- **Login** This column shows the login information of your WAN connection. You can manually initiate a connection or a disconnection by clicking the buttons. However, if you initiate a disconnection here, the "**Connect-on-Demand**" will not function until the connection button is clicked. Note that the Login won't show any information if you select "**Obtain IP automatically**" or "**Static IP**" in the **"OnePage Setup**" page.
- **Internet** This section shows the IP settings status of the router as seen by external users of the Internet. If you select **"Get IP Address Automatically", "PPPoE",** or **"PPTP"** in OnePage Setup, the **" IP Address"**, **"Subnet Mask"**, **"Default Gateway**", and **"Domain Name Server"** (DNS) will show the information received from the DHCP server or ISP currently being used. If you select **" Static IP"** in the **"One Page Setup: Public IP Address**", the information will be the same as your input.

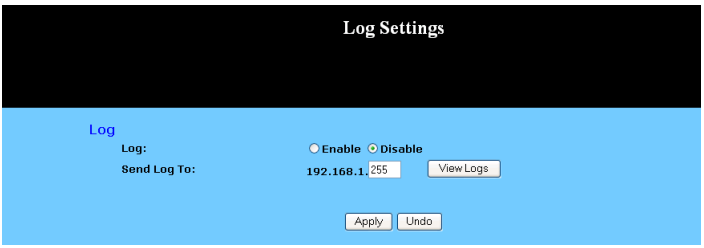
  DHCP Release: Click this button to release the IP address obtained from the ISP's DHCP server.

  DHCP Renew: Click this button to re-acquire an IP address from the ISP's DHCP server.

  Note: The "DHCP Release" and "DHCP Renew" button only show up when you select "Get IP Address Automatically" in the OnePage Setup.
- **Intranet** This section displays the current **"Private IP Address"** and **"Subnet Mask"** of the router, as seen by users of your internal network.
- **DHCP Clients Table** If the router is setup to act as a DHCP server, the LAN side IP Address distribution table will appear when this button is selected.

Log

The Log application allows the administrator to trace Internet access. You can send the record to specific LAN computers for remote monitoring, but can also watch the incoming (WAN to LAN) and outgoing (LAN to WAN) traffic in the **"Log Settings"** page.



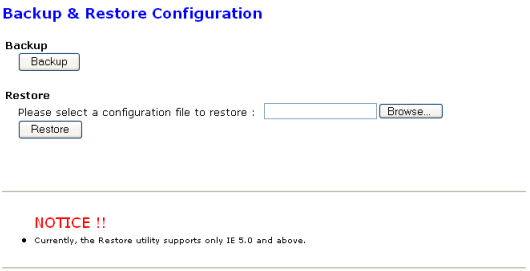
- **Log** Set to **Enable** if you want to activate this function.
- **Send Log To** Enter the IP address of the computer that you want to send the Log information to. Thiscomputer msut run a suitable "syslog" application (a copy of such an application can be downloaded from the NetComm website).

Note: You must enable the log and click apply before you can use the "View Logs" button.

Click **"Apply"** after making any changes.

Back Up and Restore

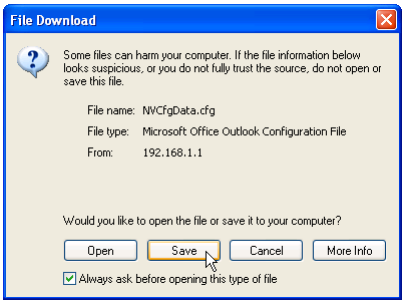
The VPN100 has the ability to store the current configuration to a file. This information can then be restored to the router at a later date.



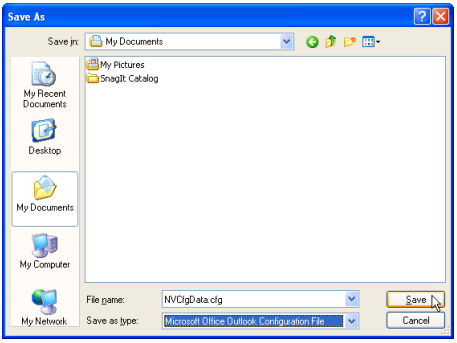
Note: Your configuration should be kept secret and in a secure location to prevent unwanted access to password or network topology information. Currently you should only use Internet Explorer version 5.0 or above to back up your router.

To Back up your router;

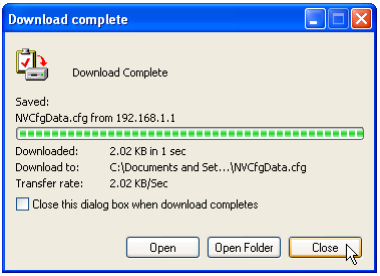
1. Click the **Backup** button. When the **File Download** window opens select **Save this file to disk**. Click **OK**



2. Choose the location where you would like to store the file and enter the file name (leave the .cfg extension). Click **Save**.

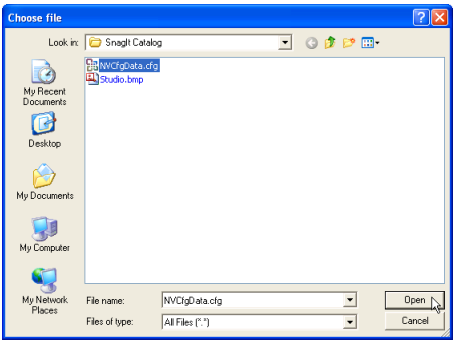


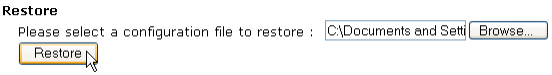
3. If required when the download is complete click the **Close** button.



To Restore your Router's configuration;

1. Log into the router and click the **Backup and Restore** menu item from the left hand menu.
2. Click the **Browse** button to open a Choose file window, search and select your previously backed up file. Click **Open**.





3. When you return to the Backup & Restore screen you should see the file path in the white field. Click the **Restore** button to start the configuration upload.
4. Once the upload is complete the router should reboot and implement the new configuration. The IP address and subnet of the could now be different, perform a "IPconfig Release and renew" to check if the browser menu stops responding.

Note: You may not be able to restore a configuration that was backed up from a different version of firmware. It is strongly advised that you try to match the firmware version in your router to the version from which the backup file was made.

Configuring IPSec/VPN Tunnels

VPN/IPSec Introduction

The VPN Router creates secure communications between sites without the expense of leased site-to-site lines. A VPN tunnel is a combination of authentication, encryption, tunneling and access control technologies used to transport traffic over the Internet or any insecure network. IPSec(Internet Protocol Security) is an industry-standard protocol suite that provides confidentiality, data integrity and authentication at the IP Layer to offer secure communications across a public network like the Internet.

IPSec Components

IPSec contains the following protocols:

- Encapsulating Security Payload (ESP):
  Provides confidentiality, authentication, and integrity.
- Authentication Header (AH):
  Provides authentication and integrity.
- Internet Key Exchange (IKE):
  Provides key management and Security Association (SA)

Security Association (SA)

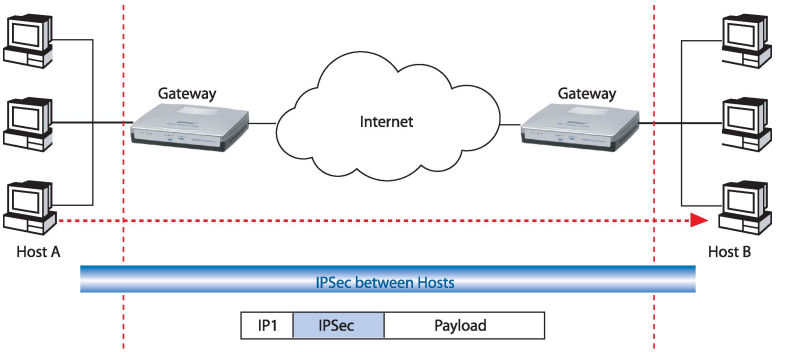
An SA provides data protection for unidirectional traffic as defined in the IPSec protocols. An IPSec tunnel typically consists of two unidirectional SAs, which together provide a protected, full-duplex data channel.

IPSec can be used in tunnel mode or transport mode. Typically, the tunnel mode is used for gateway-to-gateway IPSec tunnel protection, while transport mode is used for host-host IPSec tunnel protection. A gateway is a device that monitors and manages incoming and outgoing network traffic and routes the traffic accordingly. A host is a device that sends and receives network traffic.

Transport Mode

The transport mode IPSec implementation encapsulates only the packet's payload. The IP header is not changed. After the packet is processed with IPSec, the new IP packet contains the old IP header (with the source and destination IP addresses unchanged) and the processed packet payload.

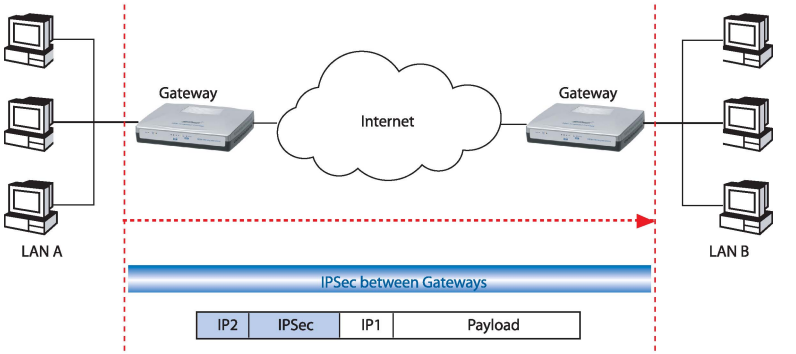
Tunnel Mode



The tunnel mode IPSec implementation encapsulates the entire IP packet.

The entire packet becomes the payload of the packet that is processed with IPSec. A new IP header is created that contains the two IPSec gateway addresses. The gateways perform the encapsulation/decapsulation on behalf of the hosts. Tunnel mode ESP prevents an attacker from analyzing the data and deciphering it, as well as knowing who the packet is from and where it is going.

Key Management

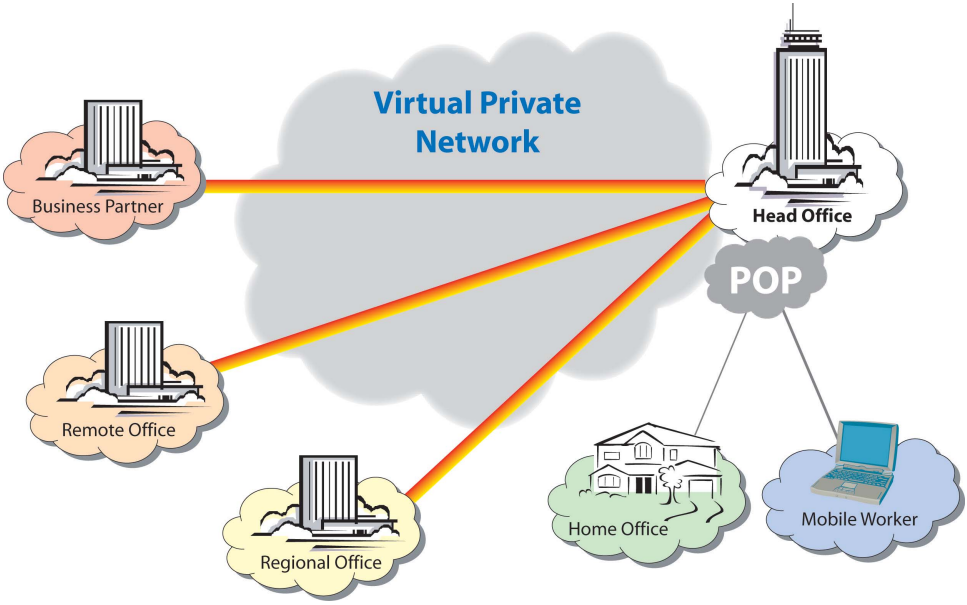


IPSec uses the Internet Key Exchange (IKE) protocol to facilitate and automate the SA setup and the exchange of keys between parties transferring data. IPSec requires that keys be re-created, or refreshed, frequently so that the parties can communicate securely with each other. IKE manages the process of refreshing keys; however, a user can control the key strength and the refresh frequency. Refreshing keys on a regular basis ensures data confidentiality between sender and receiver.

VPN Application Types

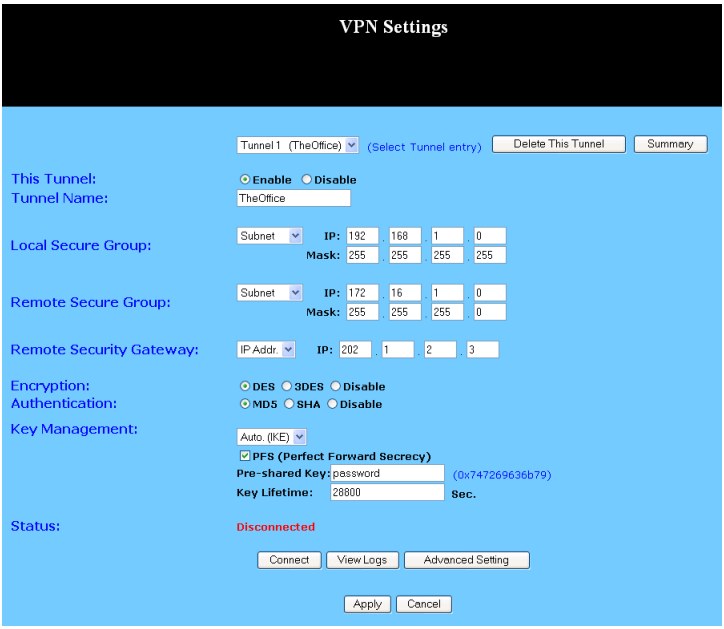
VPNs address the following applications

- Provide telecommuting workers with access to central office resources.
- Interconnect branch offices to enable corporate intranets.
- Connect business partners over the Internet with significant cost savings.



VPN / IPSec Setup

1. Select the tunnel you wish to create in the **Select Tunnel Entry** drop-down box. It is possible to create up to 5 simultaneous tunnels with the VPN100.

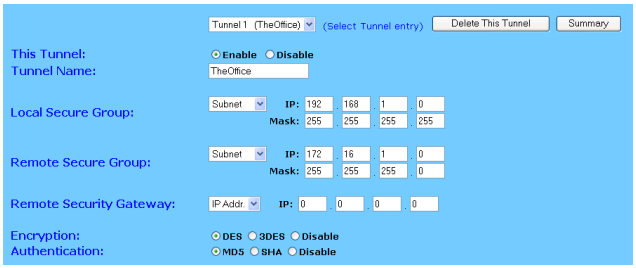


Then select **Enable** to enable the tunnel.

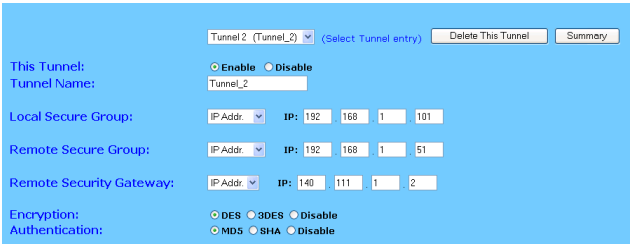
Once the tunnel is enabled, enter the name of the tunnel in the **Tunnel Name** field. This is to allow you to identify multiple tunnels and does not have to match the name used at the other end of the tunnel.

2. Under **Local Secure Group** and **Remote Secure Group**, you may choose one of five options:

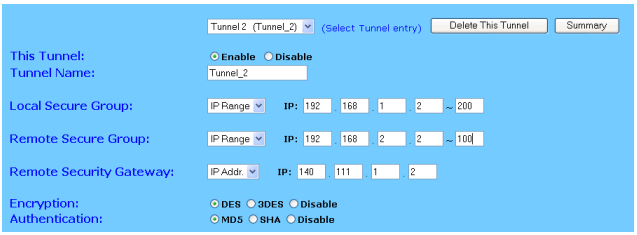
   - **Subnet -** If you select Subnet (which is the default), this will allow all computers on the local subnet to access the tunnel. In the example shown below, all Local Secure Group computers with IP Addresses 192.168.1.xxx will be able to access the tunnel. All Remote Secure Group computers with IP Addresses 192.168.2.xxx will be able to access the tunnel.



When using the Subnet setting, the default value of 0 should remain in the last octet of the **IP** and **Mask** fields.

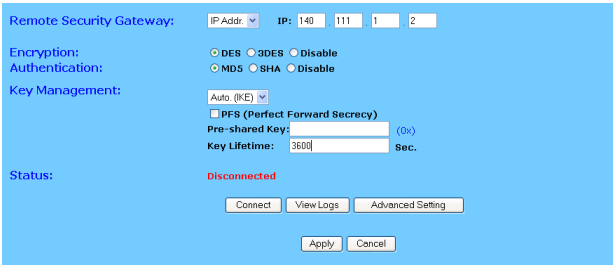


- **IP Address -** If you select IP Address, only the computer with the specific IP Address that you enter will be able to access the tunnel. In the example shown below, only the computer with IP Address 192.168.1.101 can access the tunnel from this end. Only the computer with IP Address 192.168.2.51 can access the tunnel from the remote end.
- **IP Range -** If you select IP Range, it will be a sort of combination of Subnet and IP Address. You can specify a range of IP Addresses on the Subnet which will have access to the tunnel. In the example shown below, all computers on this end of the tunnel with IP Addresses between 192.168.1.2 and 192.168.1.200 can access the tunnel from the local end. Only computers assigned an IP Address between 192.168.2.2 and 192.168.2.100 can access the tunnel from the remote end.
- **Host** – If you select Host, the value should be set the same as the Remote Security Gateway setting
- **Any** – When this option is selected, this Gateway accepts requests from any IP address such as remote users, mobile users or telecommutors using dynamic IP.

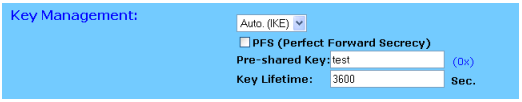


3. Under Remote Security Gateway, enter the *Public* IP Address of the VPN device at the other end of the tunnel. The remote VPN device can be another VPN Router, a VPN Server, or a host with VPN software. In the example shown above, the IP Address of the Remote Security Gateway is 140.111.1.2. This IP Address may either be **static** or **dynamic,** depending on the settings of the remote VPN device. When connecting between two routers the remote security gateway will be the public (WAN) IP address of the remote router as given on the status page or by the remote ISP.

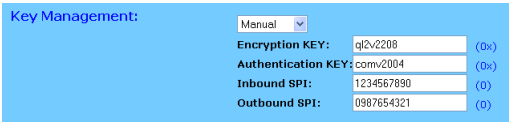
4. Using **Encryption** also helps make your connection more secure. There are two different types of encryption: **DES** or **3DES**. You may choose either of these, but it must be the same type of encryption that is being used by the VPN device at the other end of the tunnel. Or, you may choose not to encrypt by selecting **Disable**. In our example shown below, DES (which is the default) has been selected.
5. **Authentication** acts as another level of security. There are two types of authentication: **MD5** and **SHA**. As with encryption, either of these may be selected, provided that the VPN device at the other end of the tunnel is using the same type of authentication. Or, both ends of the tunnel may choose to **Disable** authentication. In the screen below, MD5 (the default) has been selected.



6. In order for any encryption to occur, the two ends of the tunnel must agree on the type of encryption and the way the data will be decrypted. This is done by sharing a “key” to the encryption code. Under Key Management, you may choose Auto (IKE) and enter a series of numbers or letters in the Pre-shared Key field. In the example shown below, the word Test is used. Based on this word (which MUST be entered at both ends of the tunnel) a code is generated to scramble (encrypt) the data being transmitted over the tunnel, where it is unscrambled (decrypted). You may use any combination of up to 23 numbers or letters in this field. No special characters or spaces are allowed. In the Key Lifetime field, you may optionally select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you’d like the key to be used, or leave it blank for the key to last indefinitely.



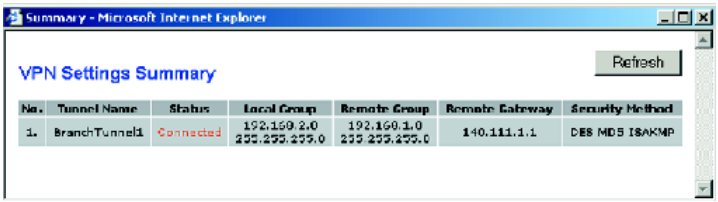
Similarly, you may choose Manual Keying, which allows you to generate the code yourself. Enter your code into the Encryption KEY field. Then enter an Authentication KEY into that field. These fields must both match the information that is being entered in the fields at the other end of the tunnel. The example shown below displays some sample entries for both the Encryption and Authentication Key fields. Again, up to 23 alphanumeric characters are allowed to create this key.



The Inbound SPI and Outbound SPI fields are different, however. The Inbound SPI value set here must match the Outbound SPI value at the other end of the tunnel. The Outbound SPI here must match the Inbound SPI value at the other end of the tunnel. In the example (see above), the Inbound SPI and Outbound SPI values shown would be opposite on the other end of the tunnel. Only numeric characters can be used in these fields.

Once you are satisfied with all your settings, click the Apply button. If you make any mistakes, clicking the Cancel button will exit the screen without saving any changes, provided that you have not already clicked the Apply button.

After the VPN device is set up at the other end of the tunnel, you may click the Connect button to use the tunnel. This assumes that both ends of the tunnel have a physical connection to each other (e.g., over the Internet, physical wiring, etc.). After clicking the Connect button, click the Summary button. If the connection is made, the screen shown below will appear:



Under Status, the word Connected should appear if the connection is successful. The other fields reflect the information that you entered on the VPN screen to make the connection. If Disconnected appears under Status, some problem exists that prevents the creation of the tunnel.

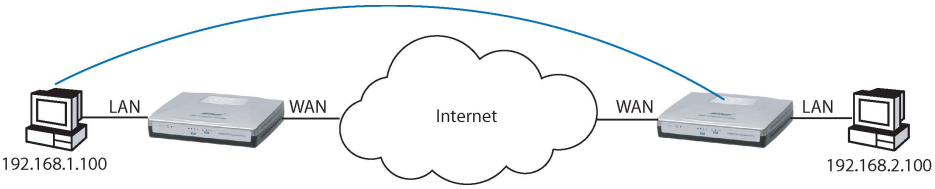
- Double-check all the values you entered on the VPN screen to make sure they are correct.
- Check the status page of both the local router and the remote device and ensure the public IP addresses are the same as entered for the remote security gateway.

If, for any reason, you experience a temporary disconnection, the connection will be re-established as long as the settings on both ends of the tunnel stay the same.

To get more details concerning your tunnel connection, click the View Log button.

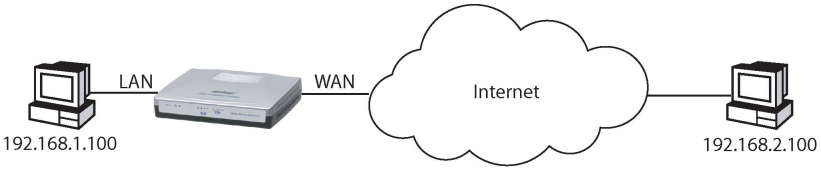
The VPN Log screen displays successful connections, transmissions and receptions, and the types of encryptions used. Once you no longer have need of the tunnel, simply click the Disconnect button on the bottom of the VPN page.

Example1: Tunnel between Two VPN Routers



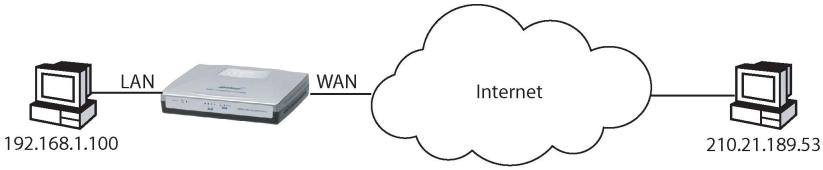
	VPN Router #1	VPN Router #2
LAN IP:	92.168.1.1	192.168.2.1
WAN IP:	210.241.239.77	211.21.189.53
Default Gateway:	210.241.239.73	211.21.189.49
	Tunnel 1	Tunnel 1
This Tunnel:	Enable	Enable
Local Secure Group:	Subnet 192.168.1.0, 255.255.255.0	Subnet 192.168.2.0, 255.255.255.0
Remote Secure Group:	Subnet 192.168.2.0, 255.255.255.0	Subnet 192.168.1.0, 255.255.255.0
Remote Security Gateway:	211.21.189.53	210.241.239.77
Encryption:	DES	DES
Authentication:	MD5	MD5
IPSec:	ISAKMP	ISAKMP
PFS:	Off	Off
IKE Pre-share KEY:	MyTest	MyTest

Example2: Tunnel between VPN Router-and-VPN Client with Fix IP



	VPN Router #1		
LAN IP:	192.168.1.1		
WAN IP:	210.241.239.77	IP:	140.111.1.2
Default Gateway:	210.241.239.73		140.111.1.1
	Tunnel 1		Tunnel 1
This Tunnel:	Enable		Enable
Local Secure Group:	Subnet 192.168.1.0, 255.255.255.0	IP:	140.111.1.2
Remote Secure Group:	IP: 140.111.1.2	Subnet 192.168.1.0, 255.255.255.0	
Remote Security Gateway:	140.111.1.2	140.111.1.1	
Encryption:	DES	DES	
Authentication:	MD5	MD5	
IPSec:	ISAKMP	ISAKMP	
PFS:	Off	Off	
IKE Pre-share KEY:	MyTest	MyTest	

Example3: Tunnel between VPN Router-and-VPN Client with dynamic IP



	VPN Router #1	Win2000 Professional Safenet Cisco VPN Client
LAN IP:	192.168.1.1	
WAN IP:	210.241.239.77	IP: 210.21.189.53
Default Gateway:	210.241.239.73	210.21.189.49
	Tunnel 1	Tunnel 1
This Tunnel:	Enable	Enable
Local Secure Group:	Subnet 192.168.1.0, 255.255.255.0	IP: 211.21.189.53
Remote Secure Group:	IP: Any	Subnet 192.168.1.0, 255.255.255.0
Remote Security Gateway:	Any	210.241.239.77
Encryption:	DES	DES
Authentication:	MD5	MD5
IPSec:	ISAKMP	ISAKMP
PFS:	Off	Off
IKE Pre-share KEY:	MyTest	MyTest

Configuring IPSec on Windows 2000/XP

This chapter illustrates the steps of Microsoft Windows 2000/XP computer to establish a secure IPsec tunnel with the Cable/DSL Firewall Router. You can find detailed information on configuring the Microsoft Windows 2000 server at the Microsoft website:

Microsoft KB Q252735 - How to Configure IPSec Tunneling in Windows 2000
http://support.microsoft.com/support/kb/articles/Q252/7/35.asp

Microsoft KB Q257225 - Basic IPSec Troubleshooting in Windows 2000
http://support.microsoft.com/support/kb/articles/Q257/2/25.asp

Environment

Windows XP or Windows 2000Server

IP Address: 140.111.1.2 (Note: ISP provided IP Address; this is only an example.)

Subnet Mask: 255.255.255.0

Cable/DSL Firewall Router

WAN

IP Address: 140.111.1.1 (Note: ISP provided IP Address, this is only an example.)

Subnet Mask: 255.255.255.0

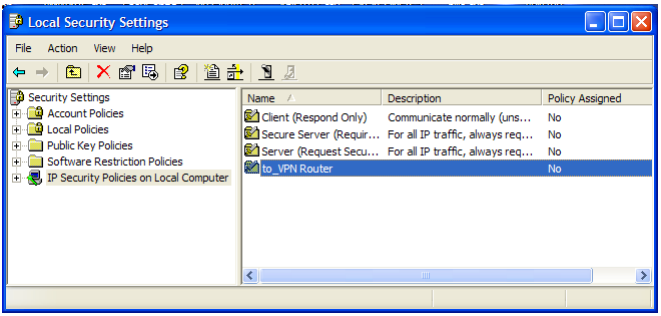
LAN

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Create IPSec Policy

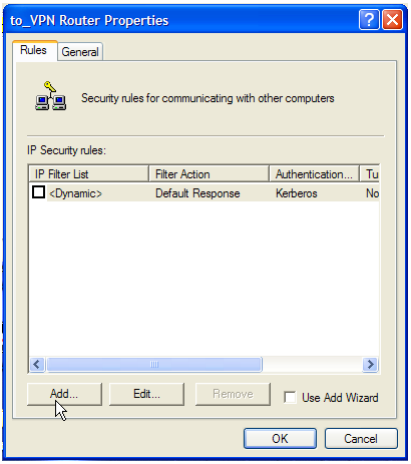
1. Click **Start** button, select **Run**, and type **secpol.msc** in the open field.
2. Right-click **IP Security Policies on Local Computer**, and then click **Create IP Security Policy**.
3. Click **Next**, and then type a name for your policy (for example, "**to_VPNRouter**").



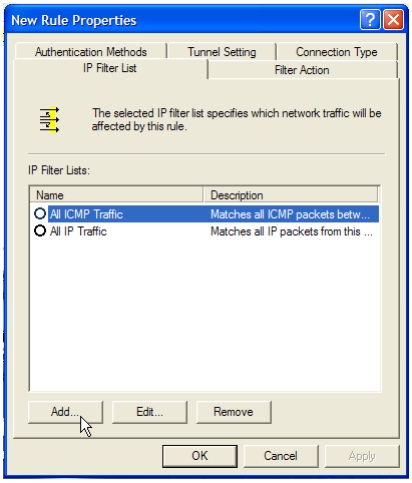
4. Deselect the **Activate the default response rule** check box, and then click **Next** button.
5. Click the **Finish** button, making sure the **Edit** check box is checked.

Build 2 Filter Lists: “WinXP to Cable/DSL Firewall Router” and “Cable/DSL Firewall Router to WinXP”.

[Filter List 1] WinXP to Cable/DSL Firewall Router

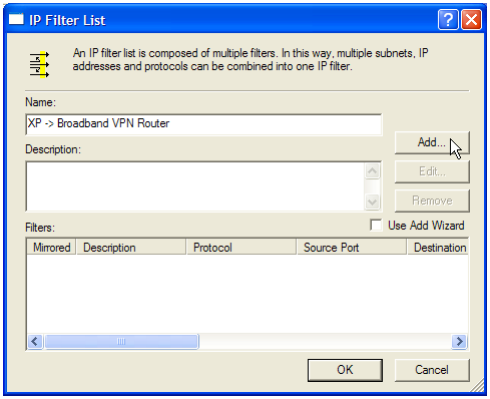


1. In the **to_VPNRouter Properties**, deselect the **Use Add Wizard** check box, and then click **Add** button to create a new rule.

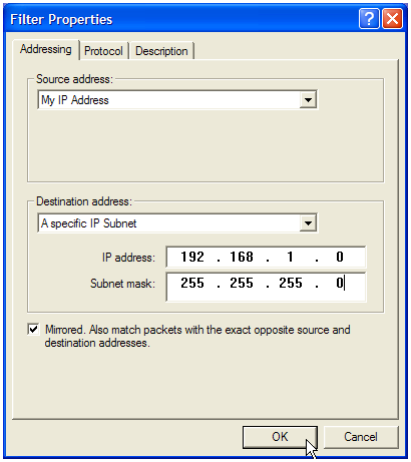


2. From the **IP Filter List** tab, click the **Add** button.

3. Type an appropriate name **"XP→Cable/DSL Firewall Router"** for the filter list, deselect the **Use Add Wizard** check box, and then click **Add** button.



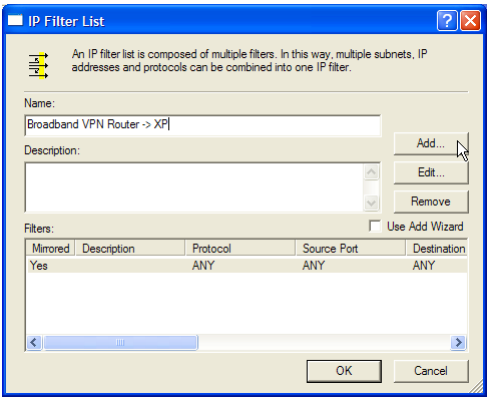
4. In the **Source address** area, click **My IP Address**.
5. In the **Destination address** field, select **A specific IP Subnet**, and fill in the **IP Address "192.168.1.0"** and **Subnet mask "255.255.255.0"**.
6. If you want to type a description for your filter, click the **Description** tab.



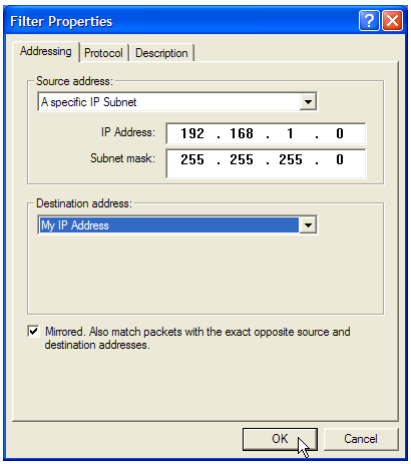
7. Click **OK** button. Then click **OK**(for WinXP) or **Close** (for Win2000) button on the **IP Filter List** window.

[Filter List 2] Cable/DSL Firewall Router to WinXP

8. On the **IP Filter List** tab, click the **Add** button.
9. Type an appropriate name **"Cable/DSL Firewall Router→XP"** for the filter list, click to clear the **Use Add Wizard** check box, and then click **Add**.



10. In the **Source address** area, click **A specific IP Subnet**, and fill in the **IP Address "192.168.1.0"** and **Subnet mask "255.255.255.0"**.
11. In the **Destination address** area, click **My IP Address**.
12. If you want to type a description for your filter, click the **Description** tab.

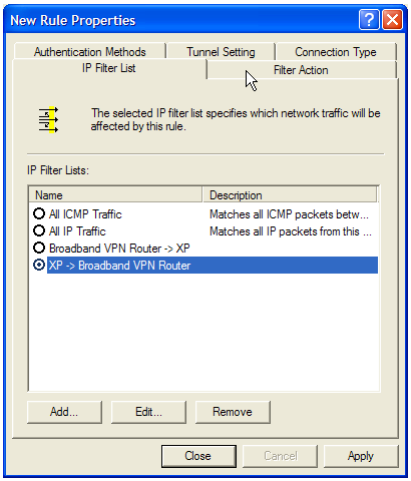


13. Click **OK**, and then click **OK**.

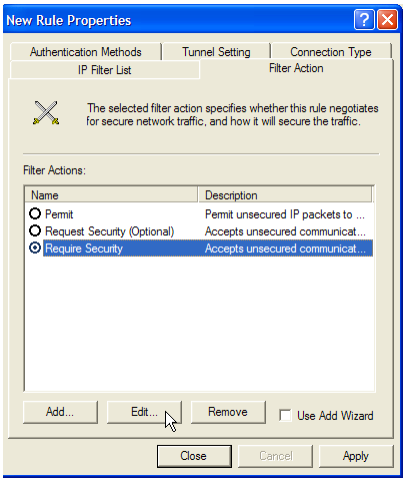
Configure Individual Rule of 2 Tunnels

[Tunnel 1] WinXP to Cable/DSL Firewall Router

1. From the **IP Filter List** tab, click the filter list **"XP→Cable/DSL Firewall Router"**.

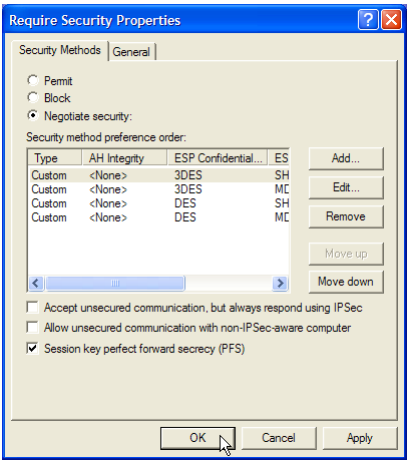


2. From the **Filter Action** tab, click the filter action **"Require Security"**, and click the **Edit** button.

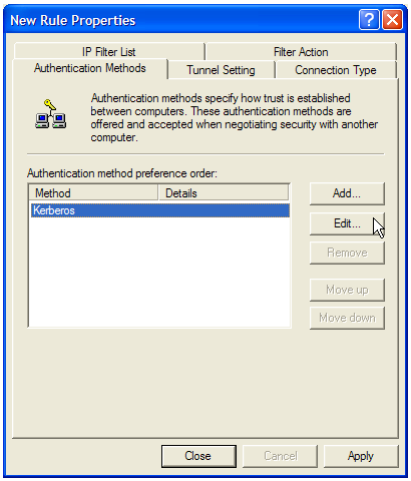


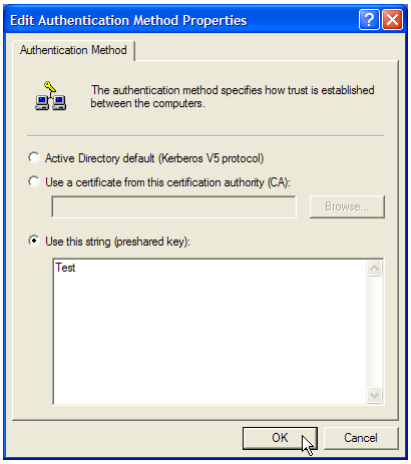
3. Check that the **Negotiate security** option is enabled, and deselect the **Accept unsecured communication, but always respond using IPsec** check box.

4. Select the **Session key Perfect Forward Secrecy (PFS)** and remember to check the **PFS** option on the Cable/DSL Firewall Router, and then click the **OK** button.

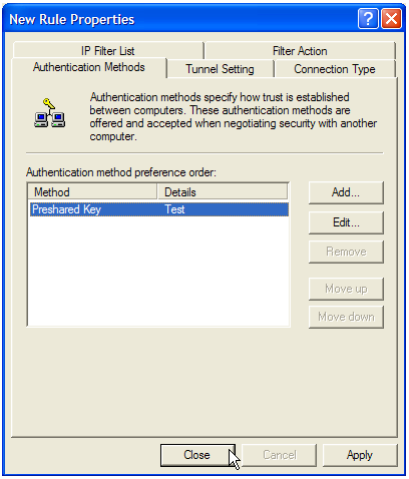


5. From the **Authentication Methods** tab, click the **Edit** button.



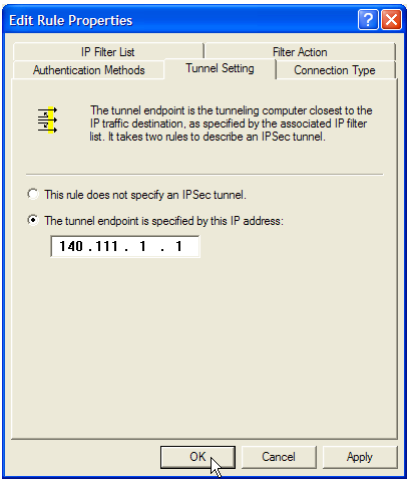


6. Change the authentication method to **"Use this string (preshared key)"**, enter the string **"Test"**, and then click the **OK** button.

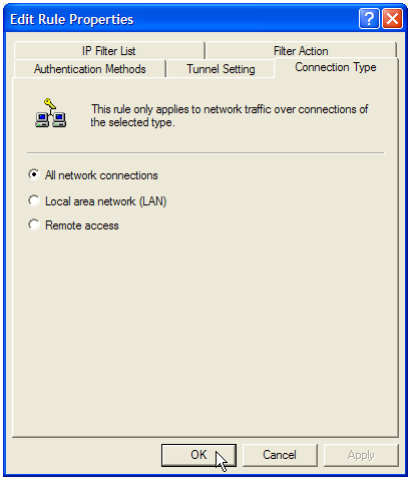


This new Preshared key will be displayed in Authentication method preference order. Click the **OK** button to continue.

7. From the **Tunnel Setting** tab, click **The tunnel endpoint is specified by this IP Address** box, and then type the **WAN IP Address "140.111.1.1"** (Note: Use your ISP provided IP Address; this is only an example.) of Cable/DSL Firewall Router.

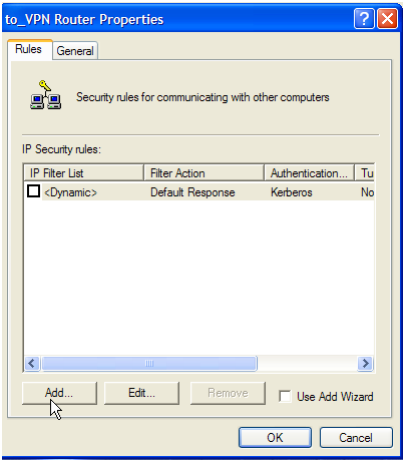


8. From the **Connection Type** tab, select **All network connections**, and then click the **OK** or **Close** button to finish this rule.

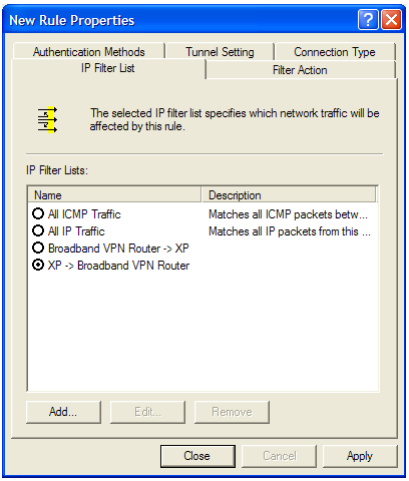


[Tunnel 2] Cable/DSL Firewall Router to WinXP

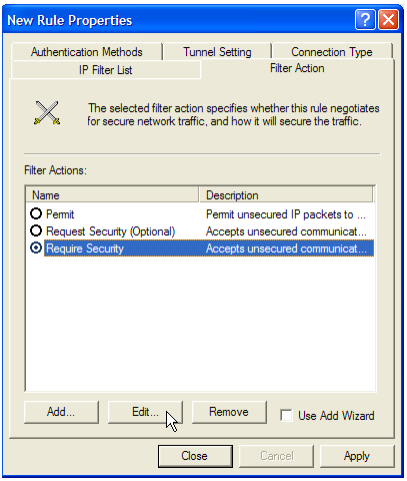
9. In the **to_VPNRouter Properties**, deselect the **Use Add Wizard** check box, and then click the **Add** button to create the second IP Filter.



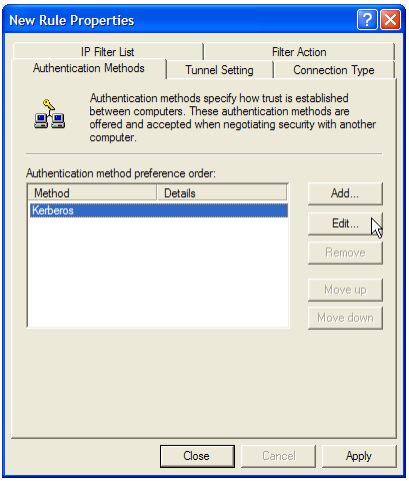
10. On the **IP Filter List** tab, click the filter list **"Cable/DSL Firewall Router→XP"**.



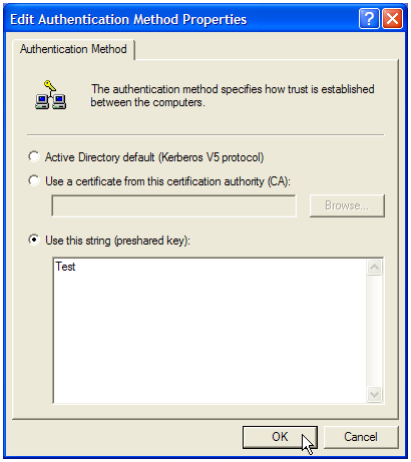
11. From the **Filter Action** tab, click the filter action **"Require Security"**.



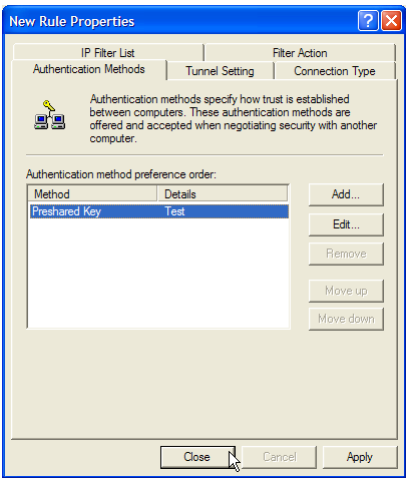
12. From the **Authentication Methods** tab, click the **Edit** button.



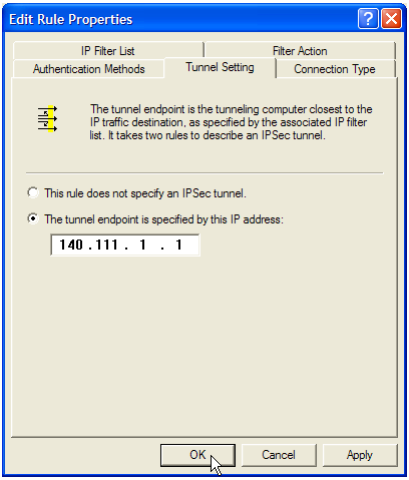
13. Change the authentication method to **"Use this string (preshared key)"**, enter the string **"Test"**, and then click the **OK** button.



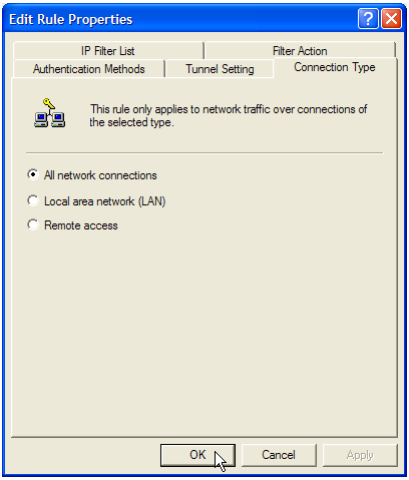
This new Preshared key will be displayed in Authentication method preference order. Click the **OK** button to continue.



14. From the **Tunnel Setting** tab, click **The tunnel endpoint is specified by this IP Address** box, and then type the **Windows 2000/XP IP Address "140.111.1.2"**.



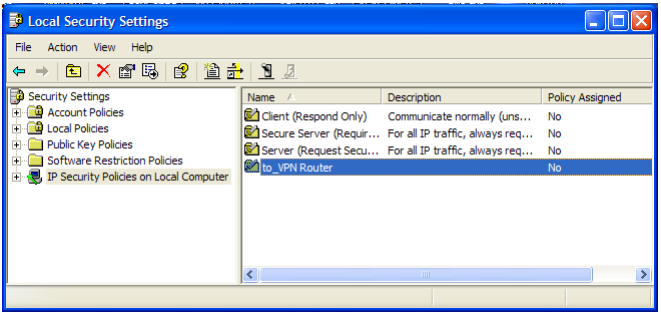
15. From the **Connection Type** tab, select **All network connections**, and then click the **OK**(for WinXP) or **Close**(for Win2000) button to finish.



16. From the **Rules** tab, click the **OK** button to back to the **secpol** screen.

Assign New IPsec Policy

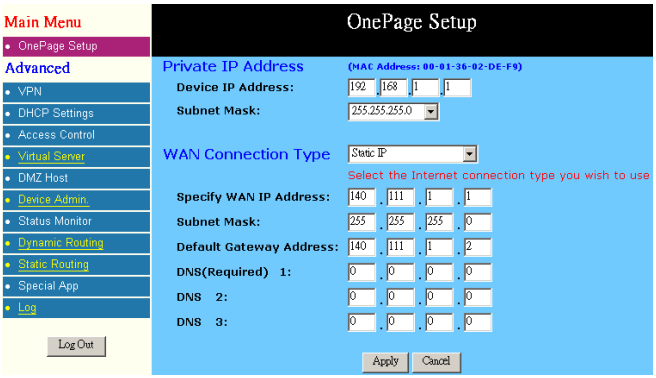
1. In the **IP Security Policies on Local Computer MMC** snap-in, right-click policy named **"to_VPNRouter"**, and then click **Assign**. A green arrow appears in the folder icon.



Steps in Cable/DSL Firewall Router

OnePage Setup Screen

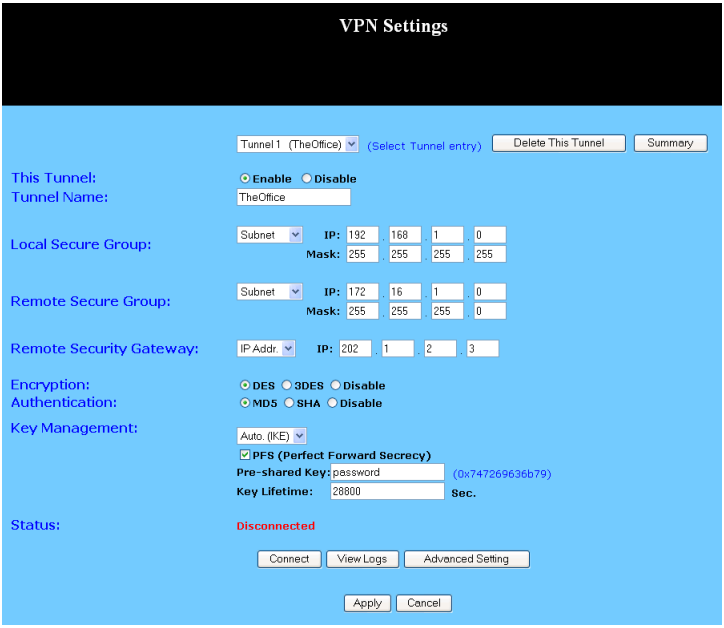
1. Open your web browser and enter **192.168.1.1** in the **Address** field and press the **Enter** key.
2. When the **User Name** and **Password** field appears, skip the user name and enter the default password admin and press the **Enter** key.



3. Click the **OnePage Setup** tab to set the configuration as shown below.

VPN Screen

The following Figure is a sample configuration for the Router's VPN tab.



Once all these have been entered, click the Connect button to establish a VPN connection. The Status should indicate that the Router is Connected.

Network Administrator's Guide

This chapter is designed to assist you in demonstrating how the VPN100 can be configured to create an IPsec VPN tunnel back to a Head office. Of course you can configure more than one tunnel in your VPN100 and allow the end user access to the Head office as well as their home office. The VPN100 can work with many types of NetComm routers as well as virtually any other VPN router that supports 'IPSec using Preshared key', even Windows servers can be configured to use this sort of VPN tunnel.

IP Addresses and Subnets

Because the VPN100 is primarily a NAT router there must be a logical difference between the LAN side of the router and the WAN side of each VPN100 used in your network. The key element to designing how you want your VPN100 units to be configured is to ensure that each independent "Mini LAN" that is created behind each VPN100 in your fleet must be on a different subnet. For this reason the subnets used should be small such as 255.255.255.248. You will also want to stagger your DHCP server pool to hand out an appropriately Unique IP address.

The factory default LAN IP and subnet of the VPN100 is 192.168.1.1 / 255.255.255.0 and the VPN100 DHCP server pool starts at 192.168.1.100 and normally will continue to 192.168.1.149. You should design each VPN100 "Mini LAN" to be unique and small within your overall companies WAN.

Multi-routed Head Offices

If your Head office LAN involves more than one Gateway or router you will need to use a dynamic routing protocol (such as RIP1 or RIP2) to ensure the route back to all the "Mini LANs" points to the Head office VPN router. Alternatively, if you keep all your "Mini-LANs" together in smaller consecutive subnets you can manually correct the route by redirecting the return path to the "Mini-LANs" together as one subnet.

Configuring the VPN tunnel

The IPSec VPN endpoints in the VPN100 must be configured with correlating details at both ends of the tunnel (in both the VPN100 and the remote VPN Router/Gateway). It is also possible toconfigure two VPN100 units to create a VPN tunnel between themselves. To create a VPN tunnel at least one of the VPN devices must have a fixed Public (WAN) IP address, because the VPN100 is designed for travel it is most likely to be assigned a different Public IP address. For the purposes of this manual it will always be assumed that the Head Office uses a fixed IP address.

Local Secure group

The Local Secure Group setting designates which IP addresses in the local LAN ("Mini-LAN") can communicate through the VPN tunnel. The Local Secure group can be an IP subnet (e.g. 192.168.1.0 / 255.255.255.0) or it can be an IP range within a subnet (e.g. 192.168.1.100 ~ 149) or it can be narrowed down to one single IP address (e.g. 192.168.1.100).

The VPN100 can only service one computer on it's LAN side (because it connects via USB) - when using the default settings your computer is usually going to be assigned 192.168.1.100. You may wish to differentiate each VPN100 by changing the next octet in the Device IP address (e.g. 192.168.xxx.0 / 255.255.255.0). It is important that the 'Local Secure Group' in your VPN100 has exactly the same settings as the 'Remote Secure Group' in the equivalent tunnel setting at the remote VPN device.

Remote Secure Group

The Remote Secure Group setting designates which IP addresses in the Remote LAN (the Head Office) can communicate through the VPN tunnel. The Remote Secure Group can be specified as a Any (which negates the need to match the remote end setting), Subnet, IP range, a specific Host or IP address. The Remote Security Group must match the 'Local Secure Group' specification given by the remote VPN device. The Remote security group can be used to limit an end user's access to specific Servers, Printers etc via the VPN tunnel.

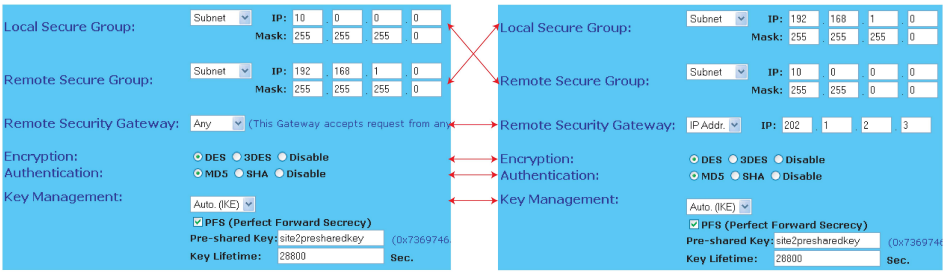
Remote Security Gateway

The Remote Security Gateway setting designates the Public (Internet) IP address that should be contacted to create the VPN tunnel. So In your VPN100 you would specify the Public IP (WAN) address of the Head Office VPN device as the Remote Security Gateway.

Note: *The Remote Security Gateway Setting for the VPN device at the Head Office will usually be set to 'Any' to allow the VPN tunnel to be created from any Public IP address (because the VPN100 is roaming and will not have a fixed IP address). However for extra security you can specify the Remote Security Gateway setting in the Head Office VPN device if the VPN100 is always using the same Internet connection and Public IP address.*

Preshared Key

The Preshared Key is the initial Authentication key (or password) used to confirm the tunnel originator is a authorised user. Preshared Keys must match exactly for both VPN devices wishing to create the VPN tunnel to each other. It is recommended that you use different Preshared keys for each tunnel that you configure.



Head Office VPN device tunnel setting
E.g. NetComm NB5580

VPN100 at site 2 VPN tunnel setting

Manual or Automatic 'keep alive' tunnels

The VPN tunnels in the VPN100 can be configured to automatically connect when the VPN100 has an Internet connection. This is a recommended practice as it will reduce the need for the end user to log into the VPN100 to manually connect the VPN tunnel. The option for 'Keep Alive' is in the 'Advanced Setting' options of the tunnel.

File Sharing over VPN

Once you have your VPN tunnel connected you may wish to allow your end user access to files. This can be done in several ways depending on your Network operating system and architecture. The most simple example for Windows users is to use 'mapped network drives' remember to do this you must either map the drive via an IP address (e.g.\\10.0.2.10\sharename) or Map it via a UNC pathname (e.g. \\fps1\sharename). However if you wish to use full UNC path names to your network drives you should ensure that your DNS service will connect through your VPN tunnel or edit the Host file on the end user's computer.

Email over VPN

Similar to file sharing it is best to ensure that your DNS will resolve via the Head Office DNS server. Then you can configure your end user's mail client to use the mail server's name instead of it's IP address. Email client applications should be configured the same as if they were connected locally in the Head office.

Windows Authentication via VPN

If you wish to have the End user log into the Windows domain via the VPN tunnel you may need to ensure your MTU in the VPN100 is set to 1492 or less. Also it is strongly advisable to set the VPN100 to 'Keep Alive' the VPN tunnel so that the tunnel is created whilst the computer is booting – and therefore ready for the Windows log-in to pass through it. If the end user is using Windows 2000, Windows XP or greater you may also need to force the use of TCP for packets for Kerberos authentication. This can be done by adding the following registry key to the end user's computer.

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters\
MaxPacketSize(DWORD)=1
```

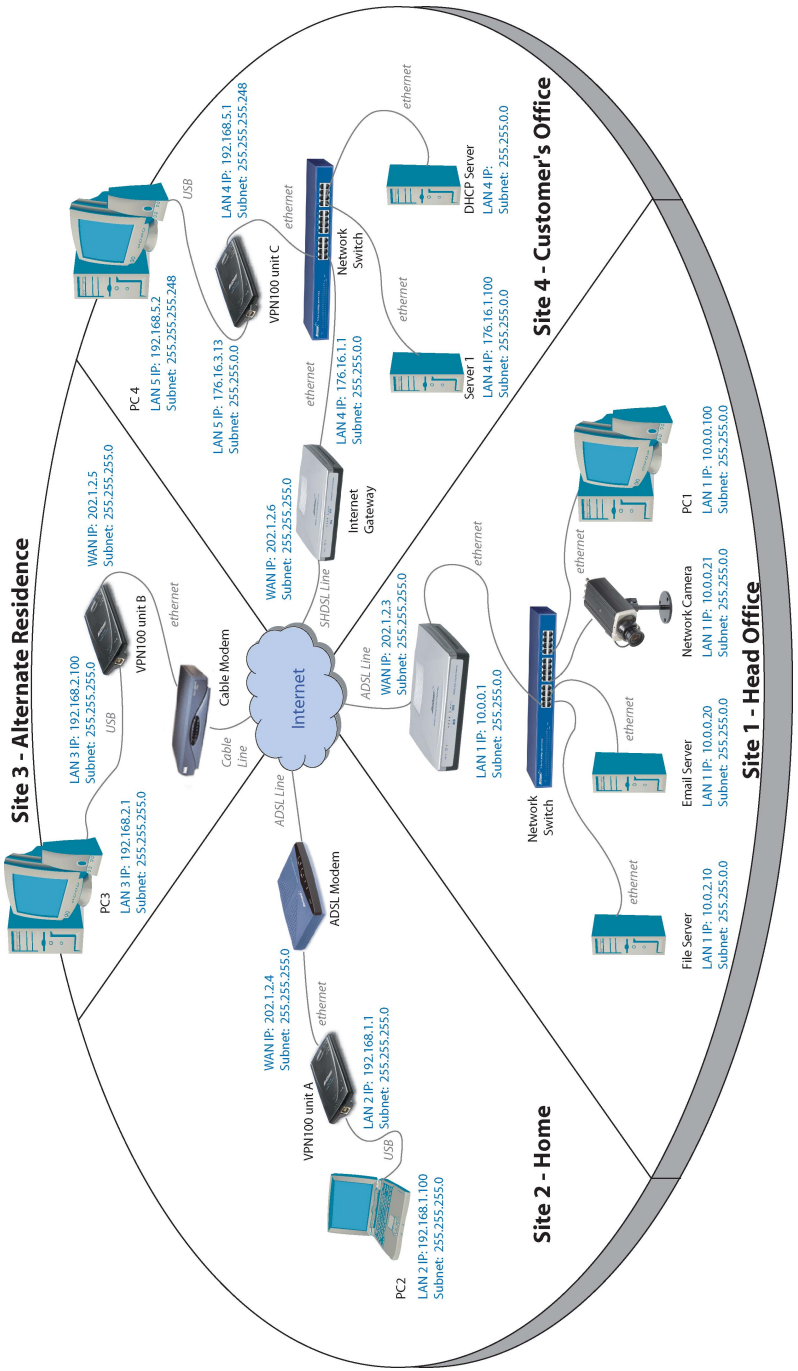
VPN Passthrough

The VPN100 will allow the end user's computer to create a VPN tunnel through the router (via PPTP or IPSec) and out to a remote VPN device. This is because the VPN100 supports 'VPN Pass-Through' or 'NAT traversal' to allow other VPN clients (such as Native Windows VPN client) to be used instead of the built-in VPN endpoints.

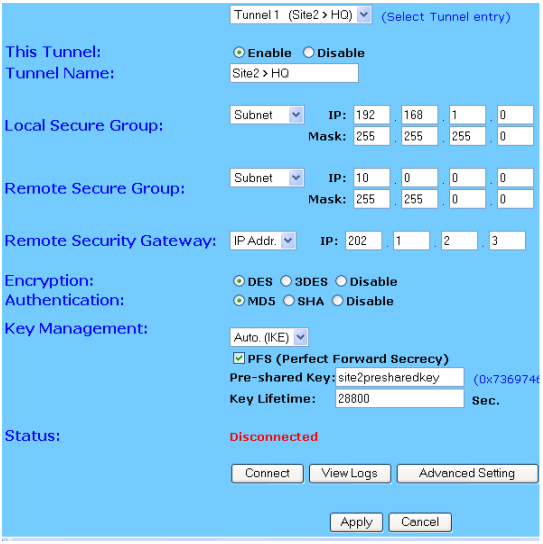
If the End user wishes to use the VPN100 at a customer's office which uses a NAT router or Internet Gateway to share their Internet connection the Internet Gateway must allow VPN Pass through in order for the VPN100 to be able to create a connection to the Head Office.

Multiple VPN100s connected to one Head Office Example

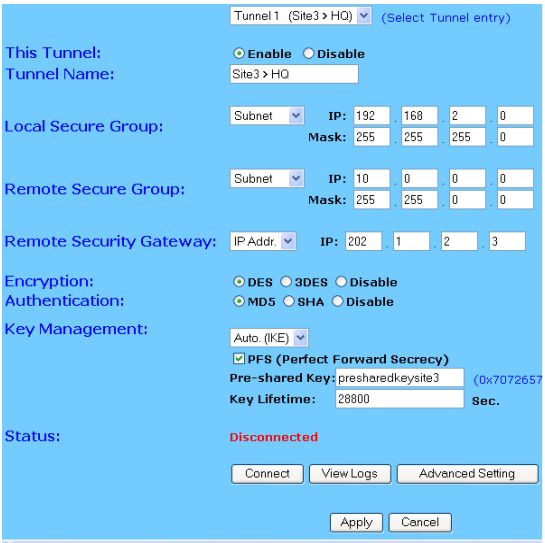
The example diagram and configuration screens on the following pages demonstrate three different VPN100 devices connecting in three different 'Wan Type' methods and also showing each device creating a unique VPN tunnel simultaneously coming from each different site. The equipment used at the Head Office is a NetComm NB5580 which is an ADSL Integrated gateway that currently supports up to 10 IPsec VPN tunnels. When the VPN tunnels are connected in any of the VPN100 units shown the end users of those VPN100s will be able to access the File Server, the Email Server, PC1 and the Network Camera at the head office.


Site 3 - Alternate Residence
Site 4 - Customer's Office
Site 1 - Head Office
Site 2 - Home
Internet
Cable Modem
Cable Line
ADSL Modem
ADSL Line
SHDSL Line
Internet Gateway
WAN IP: 202.1.2.6
Subnet: 255.255.255.0
LAN 4 IP: 176.16.1.1
Subnet: 255.255.0.0
VPN100 unit C
LAN 5 IP: 176.16.3.13
Subnet: 255.255.0.0
LAN 4 IP: 192.168.5.1
Subnet: 255.255.255.248
PC 4
LAN 5 IP: 192.168.5.2
Subnet: 255.255.255.248
Network Switch
DHCP Server
LAN 4 IP:
Subnet: 255.255.0.0
Server 1
LAN 4 IP: 176.16.1.100
Subnet: 255.255.0.0
WAN IP: 202.1.2.5
Subnet: 255.255.255.0
VPN100 unit B
LAN 3 IP: 192.168.2.100
Subnet: 255.255.255.0
PC3
LAN 3 IP: 192.168.2.1
Subnet: 255.255.255.0
WAN IP: 202.1.2.3
Subnet: 255.255.255.0
LAN 1 IP: 10.0.0.1
Subnet: 255.255.0.0
Network Switch
PC1
LAN 1 IP: 10.0.0.100
Subnet: 255.255.0.0
Network Camera
LAN 1 IP: 10.0.0.21
Subnet: 255.255.0.0
Email Server
LAN 1 IP: 10.0.0.20
Subnet: 255.255.0.0
File Server
LAN 1 IP: 10.0.2.10
Subnet: 255.255.0.0
WAN IP: 202.1.2.4
Subnet: 255.255.255.0
VPN100 unit A
LAN 2 IP: 192.168.1.1
Subnet: 255.255.255.0
PC2
LAN 2 IP: 192.168.1.100
Subnet: 255.255.255.0
USB
ethernet

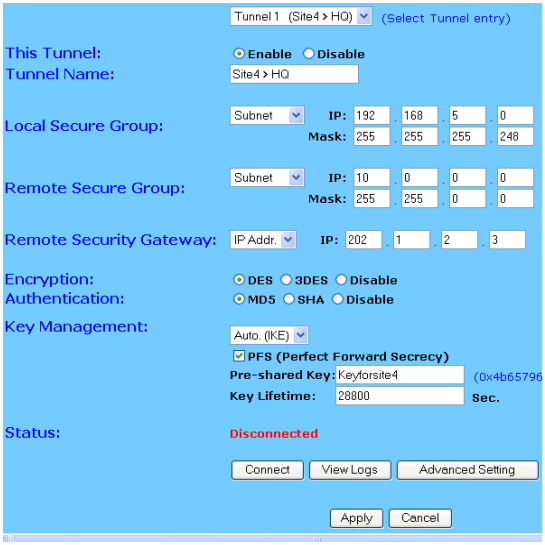
The following are screen captures of the VPN configurations of the Head Office router and the VPN100s at Sites 2, 3 & 4. These are shown to help you understand how you would configure each VPN100 to work with the NB5580 (Head office or Remote VPN device).



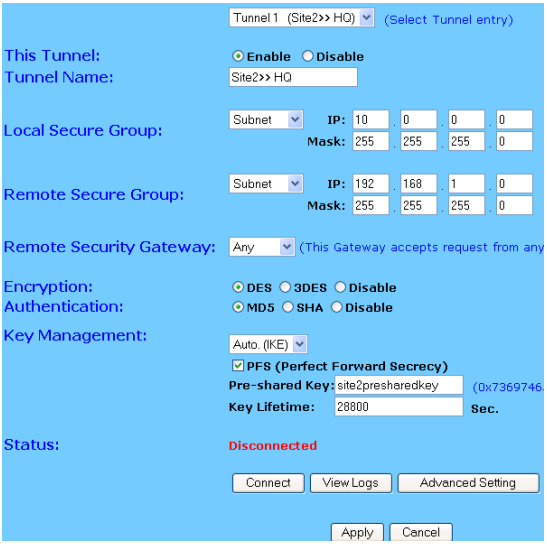
VPN100 at site 2 VPN screen shot



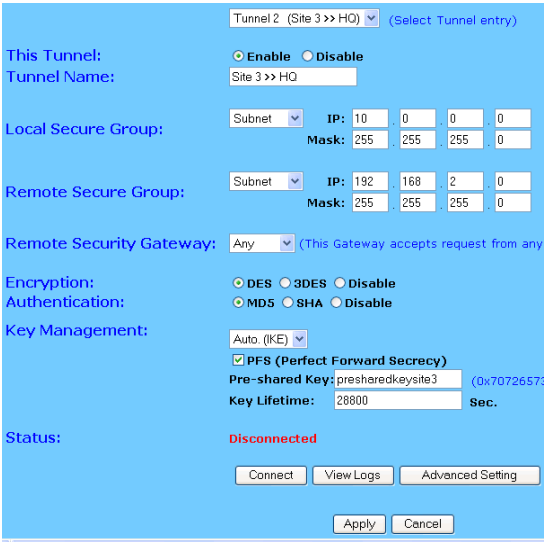
VPN100 at site 3 VPN screen shot



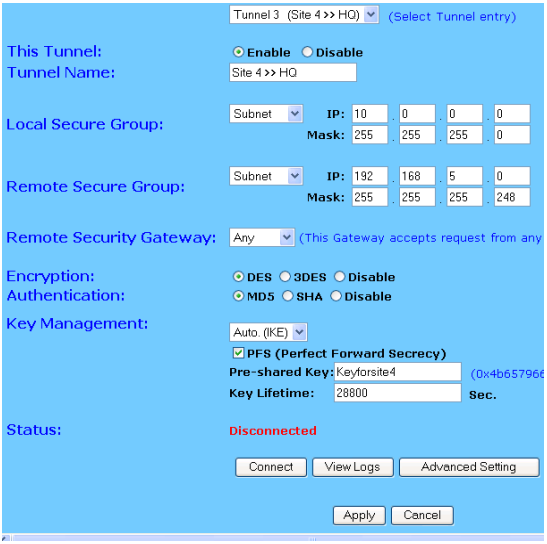
VPN100 at site 4 VPN screen shot



NB5580 VPN config screen shot for tunnel from VPN100 unit A (site 2)



NB5580 VPN config screen shot for tunnel from VPN100 unit B (site 3)



NB5580 VPN config screen shot for tunnel from VPN100 unit C (site 4)

Appendix A: Trouble Shooting

This chapter provides solutions to problems you may encounter during installation and operation of your NetComm VPN100.

Hardware

T: The Power LED is off.

Check the USB cable is properly connected to the NetComm VPN100 and that your computer's USB socket is functional.

T: The Link LED is off.

Check the hub, switch or modem is properly connected to the ethernet socket of the NetComm VPN100.

Check the computer is using an IP address in the range of 192.168.1.2 ~ 192.168.1.254 and is therefore compatible with the Cable/DSL Firewall Router's default IP address of 192.168.1.1 Check also the Subnet Mask is set to 255.255.255.0

T: The DIAG LED stays lit.

The DIAG LED should light up when the device is first powered up to indicate it is checking for proper operation. After a few seconds, the LED should go off. If it stays on, the device is experiencing a problem. Try unplugging the USB cabel and then reconnecting it.

T: Why can't I configure the NetComm VPN100?

First, check whether the NetComm VPN100 is properly installed..

Next, check the IP configuration of your computer :

- For Windows 95/98 users: run **Winipcfg.exe** or **Winipcfg** from **"Run"** on the **"Start"** menu. If there are no IP addresses, click **"Release All"** and then click **"Renew All"** to get an IP address.

For Windows NT 4.0/2000/XP users: Open a command prompt and run **IpConfig**.

- Ensure that your computer and the NetComm VPN100 are on the same network segment. If you are not sure, initiate the DHCP function and let the computer get an IP address automatically from the router.
- Ensure that your computer is using an IP Address within the range 192.168.1.2 to 192.168.1.253 and thus compatible with the NetComm VPN100's default IP address of 192.168.1.1
- Finally, use *Ping* command in MS-DOS mode to verify the network connection:
  - *Ping* 127.0.0.1 to check the TCP/IP stack of your computer.
  - *Ping* the Router's IP address (Default: 192.168.1.1) to check for IP connectivity between your computer and the Router.

Note: If you are not able to get to the web configuration screen for the NetComm VPN100, make sure that you disable the proxy setting within your Internet browser and set your browser to access the Internet via the LAN.

T: What can I do if I have forgotten the password for NetComm VPN100?

You have to reset the Router back to its factory default setting by pushing the Reset button for over 3 seconds.

Note: You will lose all previous settings.

T: I cannot access my ISP's home page, why?

Some ISPs (such as Telstra BigPond) require their host name be specifically configured into your computer before you can surf their local web pages. If you are unable to access your ISP's home page, enter your ISP's Domain Name into the One Page Setup to enable all computers in your LAN to access it. If you only want to allow computers to access these home pages, open the TCP/IP Properties window on these computers, click open the **"DNS Configuration"** tab and enter your ISP's Domain Name in the **"Domain Name Search Suffix"** location.

Client Side (Computers)

T: I can't browse the Internet via the NetComm VPN100

Ensure your computer can ping or access the Router. See the previous section entitled **"Why can't I configure the NetComm VPN100"** for more information.

Check the status page of the Router to ensure connection to your ISP has been established.

T: I get a time out error when I enter a URL or IP address.

Check if other computers on the LAN are experiencing the same problem. If not, ensure the computer's IP settings are correct (IP Address, Subnet Mask, Gateway IP Address and DNS).

Check the NetComm VPN100's settings are correct.

Appendix B: Frequently Asked Questions

Q: What is the maximum number of IP Addresses the NetComm VPN100 can support?

The DHCP Server in the NetComm VPN100 can support up to 50 IP Addresses usually in the range of 192.168.1.100~192.168.1.150 but, because it connects via USB, it is usually only possible to support one PC.

Q: Does the NetComm VPN100 support 100Mb Ethernet?

Yes, the NetComm VPN100 supports both 10Mb & 100Mb Ethernet on the WAN side, but only 10Mb on the LAN side, which runs over USB.

Q: What is "NAT" and what is it used for?

The Network Address Translation (NAT) Protocol translates multiple IP Addresses on a private LAN into a single public IP Address that is accessible to the Internet. NAT not only provides the basis for multiple IP Address sharing but also provides security, since the multiple IP Addresses of LAN computers are never transmitted directly to the Internet.

Q: What operating systems does NetComm VPN100 series support?

Windows 98, Windows ME, Windows 2000, Windows XP, or greater

Q: Can I use multiple E-mail accounts if I use NetComm VPN100?

Yes, you can. Some people think having one Internet account means that they can have only one E-mail account. However, E-mail is set by mailbox accounts and different to the account you use to connect to your ISP. If you want more E-mail accounts, you can contact your ISP or you can browse the Internet to apply for free E-mail account.

Q: Does the NetComm VPN100 support PPTP of VPN packets pass through?

Yes. The NetComm VPN100 supports PPTP pass through.

Q: Does the NetComm VPN100 series support IPsec?

Yes. The NetComm VPN100 supports IPsec pass through or has its own IPsec tunnels to use as an alternative.

Appendix C: Glossary

10Base-T / 100Base-T

The adaptation of the Ethernet standard for Local Area Networks (LANs). 10Base-T uses a twisted pair cable with maximum lengths of 100 meters and transmits data at 10Mbps maximum. 100Base-T is similar, but uses two different twisted pair configurations and transmits at 100Mbps maximum.

Ad-hoc Network

Also known as the peer-to-peer network, an ad-hoc network allows all computers participating in a wireless network to communicate each other without an AccessPoint.

Adapter

A device that makes the connection to a network segment, such as Ethernet and modem cards.

ADSL

Asymmetric Digital Subscriber Line (ADSL), as its name indicates, is an asymmetrical data transmission technology with higher traffic rate downstream and lower traffic rate upstream. ADSL technology satisfies the bandwidth requirements of applications which demand “asymmetric” traffic, such as web surfing, file downloads, and telecommuting.

Bandwidth

The amount of data that can be transmitted in a fixed amount of time.

Browser

A software application used to locate and display Web pages. Examples include Netscape Navigator and Microsoft Internet Explorer.

BSS

BSS is the acronym of Basic Service Set that consists of a wireless access point and a group of wireless client computers.

Communications Protocols

Communication between devices requires they agree on the format in which the data is to be transmitted, sent and received. The communications protocols are a set of rules that define the data format.

Cookie

Cookie is data stored on your computer, which a web server can retrieve, to identify your machine. It is a piece of text with an ID number.

DHCP

DHCP, short for Dynamic Host Configuration Protocol, is a protocol for assigning dynamic IP Addresses to devices on a network. Dynamic Addressing means that a device can have a different IP Address each time it connects to the network.

Domain Name

A name that identifies one or more IP Addresses. For example, the domain name microsoft.com represents about a dozen IP Addresses. Domain names are used in URLs to identify particular Web pages. For example, in the URL http://www.pcwebopedia.com/index.html, the domain name is pcwebopedia.com.

DoS

DoS is the acronym for Denial of Service. This is the result when a computer or network is overwhelmed to the point that it can no longer function normally.

DNS

Short for Domain Name Server, translates domain names into IP Addresses. To help us recognize and remember domain names they are alphabetic in form, however, the Internet actually runs on numbered IP Addresses. DNS servers translate domain names into their respective IP Addresses.

DSSS

Also known as Direct Sequence Spread Spectrum, it is a radio transmission method that continuously changes frequencies.

Ethernet

One of the most common Local Area Network (LAN) standards. Ethernet uses a bus topology which supports a data transfer rate of 10 or 100 Mbps.

ESS

ESS is the acronym of Extend Service Set that consists of several BSS.

Firewall

A security system used to enforce an access control policy between an organisation's networks and the Internet.

IEEE

Short for Institute of Electrical and Electronics Engineers, an organization best known for developing standards for the computer and electronics industry.

Internet

A global network connecting millions of computers for the exchange of data, news and opinions.

Intranet

A network based on TCP/IP Protocol belonging to an organization, and accessible only by that organization's members, employees, or others with authorization.

Infrastructure Network

Unlike an ad-hoc network (where users on a wireless LAN send data to each other directly), users on an infrastructure network send data through a dedicated access point. Additionally, the access point enables users on a wireless LAN to access an existing wired network to take advantage of sharing the wired network's resources, such as files, printers, and Internet access.

IP Address

An identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP Protocol route messages based on the IP Address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be from zero to 255.

IPSec

Internet Protocol Security is a security standard for network transmission, which is often used for VPN connections. It provides authentication and packet encryption over the Internet.

ISP

Short for Internet Service Provider, a company that provides access to the Internet for a fee.

Local Area Network (LAN)

A computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings. However, one LAN can be connected to other LANs over any distance. A system of LANs connected in this way is called a wide area network (WAN)

MAC Address

Short for Media Access Control Address, a hardware address that uniquely identifies each node of a network.

NAT

Short for Network Address Translation, a routing protocol that allows global IP Addresses to be translated into multiple private IP Addresses for use on internal LAN networks. The explosion in the use of the Internet has created a critical problem for the Internet Assigned Numbers Authority (IANA) which is in charge of assigning IP Addresses to Internet users, ISPs etc. NAT is a technology that has been introduced to help maximize the utilization of assigned IANA and global IP Addresses.

Network Protocol

Network protocols encapsulate and forward data packets from one interface to another.

PAP/CHAP

Short for Password Authentication Protocol and Challenge Handshake Authentication Protocol. Most ISPs use either one for user identification. If your ISP doesn't support these two protocols, contact them for an authentication script.

PPP

Short for Point-to-Point Protocol, a communications protocol for transmitting information over standard telephone lines between devices from different manufacturers.

PPPoE

Short for PPP over Ethernet, relying on two widely accepted standards, Ethernet and the Point-to-Point Protocol. PPPoE is a communications protocol for transmitting information over the Ethernet between devices from different manufacturers.

PPTP

The acronym of Point to Point Tunnelling Protocol, PPTP encapsulates the packet for transmission over the Internet. It creates a private "tunnel" through the large public network to have similar security of private network without actually leasing a private line. PPTP is normally used for VPN connections.

Protocol

An agreed format for transmitting, sending and receiving data between two devices.

Roaming

The ability for a wireless device to move from one access point's range to another without losing the connection.

Router

An Internet device that routes requests for information to other routers until the information's location is found and the data can be transmitted back to the origin of the request.

TCP/IP

Short for Transmission Control Protocol and Internet Protocol, the suite of communications protocols that enable hosts on the Internet to connect and exchange streams of data.

VPN

The acronym for Virtual Private Network. Via access control and encryption, VPNs bring security to the data transmission through the Internet as it is transmitted through a private network. It not only takes advantage of economies of scale but also provides a high level of security while the packet is sent over a large public network.

Wide Area Network (WAN)

A system of LANs being connected by telephone lines and radio waves. Although some WANs may be privately owned, they are usually considered a means of public access.

WEP

The acronym for Wired Equivalent Privacy. It is an encryption mechanism used to protect your wireless data communications. WEP uses a combination of 64-bit/128-bit keys to encrypt data that is transmitted between all points in a wireless network to ensure data security. It is described in the IEEE 802.11 standard.

Appendix D: Updating your Firmware

Firmware is the programming that is 'Hard coded' into your router, as newer developments in technology and general product improvements are written your router can be updated to take advantage of this newer programming.

The VPN100 incorporates the TFTP protocol to reliably upload new firmware. These updates are either posted on the NetComm website (www.netcomm.com.au) or Emailed via NetComm's technical staff. You can check your current firmware version in the Administration page.

To upload your firmware you should run the Executable program that is provided and specify the current LAN IP address of the router as well as the router's password. Then click Upgrade.

After the upgrade is complete wait a minute for the router to reboot before continuing use.

Note: ***It is recommended that you reset your router to factory defaults before upgrading. Previous router configuration backups may not work on different firmware versions.***

Appendix E: Cable Connections

This cable information is provided for your reference only. Please ensure you only connect the appropriate cable into the correct socket on either this product or your computer.

If you are unsure about which cable to use or which socket to connect it to, please refer to the hardware installation section in this manual. If you are still not sure about cable connections, please contact a professional computer technician or NetComm for further advice.

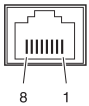
RJ-45 Network Ports

RJ-45 Network Ports can connect any networking devices that use a standard LAN interface, such as a Hub/Switch Hub or Router. Use unshielded twisted-pair (UTP) or shield twisted-pair (STP) cable to connect the networking device to the RJ-45 Ethernet port. Depending on the type of connection, 10Mbps or 100Mbps, use the following Ethernet cable, as prescribed.

10Mbps: Use EIA/TIA-568-100-Category 3, 4 or 5 cable.

100Mbps: Use EIA/TIA-568-100-Category 5 cable.

Note: ***To prevent loss of signal, make sure that the length of any twisted-pair connection does not exceed 100 metres.***



RJ-45 Connector Pin Assignment	Normal Assignment
1	Input Receive Data +
2	Input Receive Data -
3	Output Transmit Data +
6	Output Transmit Data -
4,5,7,8	Not used

Figure 1

Twisted pair cables

Figures 1 and 2 illustrate the use of straight-through and crossover twisted pair cables along with the connector.

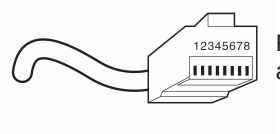


Figure 2

Straight and crossover cable configuration

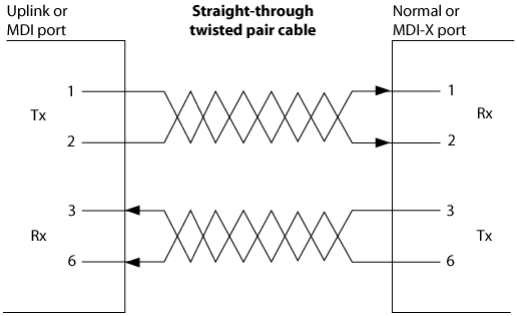


Figure 3

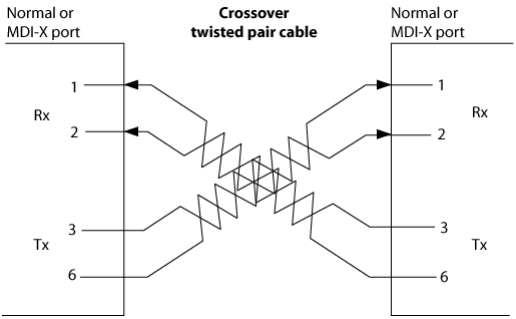


Figure 4

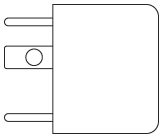
RJ11 connector and cable

An RJ-11 connector is the small, modular plug used for most analog telephones. It has six pin slots in the head, but usually only two or four of them are used.

RJ-11 Connector Pin Assignment	Normal Assignment
1	Signal Ground
2	CTS
3	RXD
4	TXD
5	+5 Volts In
6	Signal Ground

Figure 5

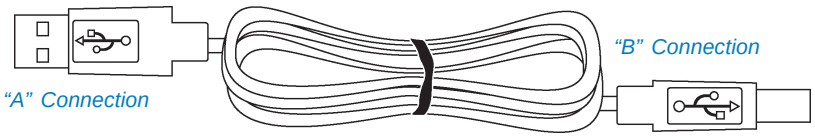
605 to RJ-11 adapter



The 605 to RJ-11 adaptor is provided to comply with the older 610 Telstra wall socket. The 605 to RJ-11 adapter may be used to convert the supplied RJ-11 cable, if the older connection is required.

USB cable

A typical USB cord has an "A" connection (“upstream” to plug into the computer) and a “B” connection (“downstream” to plug into the device).

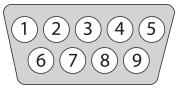


By using different connectors on the upstream and downstream ends, cable connection is simplified. The “B” connection will fit a into the “B” socket of any USB device. Similarly, any "A" connector can be plugged into any "A" socket, such as on a computer.

If it is a new device, the operating system auto-detects it and asks for the driver disk. If the device has already been installed, the computer activates it and starts talking to it. USB devices can be connected and disconnected at any time.

9 Pin (RS-232) Serial Cable

A 9 Pin (RS-232) Serial Cable may be used to connect to a serial console terminal or a PC running a terminal emulation program, such as Hyper Terminal.



Male Connector

Pin No	Name	Notes/Description No.
1	DCD	Data Carrier Detect
2	RD	Receive Data (a.k.a RxD, Rx)
3	TD	Transmit Data (a.k.a TxD, Tx)
4	DTR	Data Terminal Ready
5	SGND	Ground
6	DSR	Data Set Ready
7	RTS	Request To Send
8	CTS	Clear To Send
9	RI	Ring Indicator

Appendix F: Registering your NetComm Product

All NetComm Limited ("NetComm") products have a standard 12 month warranty from date of purchase against defects in manufacturing and that the products will operate in accordance with the specifications outlined in the User Guide. However some products have an extended warranty option (please refer to packaging). To be eligible for the extended warranty you must supply the requested warranty information to NetComm within 30 days of the original purchase by registering on-line via the NetComm web site at:

www.netcomm.com.au

Contact Information

If you have any technical difficulties with your product, please do not hesitate to contact NetComm's Customer Support Department.

Email: support@netcomm.com.au

Fax: (+612) 9424-2010

Web: www.netcomm.com.au

Trade marks and Notices

"NetComm" is a trade mark of NetComm. Windows® is a registered trade mark of Microsoft Corporation. Other brand and product names are trade marks or registered trade marks of their respective holders. Information is subject to change without notice. All rights reserved.

Please note that the images used in this document may vary slightly from those of the actual product. Specifications are accurate at the time of the preparation of this document but are subject to change without notice.

Warranty

Where the Customer (you) is a consumer as defined by any relevant law such as the Trade Practices Act 1974 (Commonwealth) and similar State laws, certain conditions and warranties ("the consumer warranties") cannot be excluded, restricted or modified. You then have the benefit of both the consumer warranties and any other warranty that may be provided by the Company or by the manufacturer of the goods. To the extent permitted by Law, all implied warranties and conditions are excluded.

All NetComm products have a standard 12 months warranty from date of purchase. However some products have an extended warranty option (refer to packaging). To be eligible for the extended warranty you must supply the requested warranty information to NetComm within 30 days of the original purchase by registering on-line via the NetComm web site at www.netcomm.com.au.

To the extent permitted by the consumer warranties, in relation to your product and any other materials provided with the product ("the Goods") the liability of NetComm under the Relevant Acts is limited at the option of NetComm to:

- replace the Goods; or
- repair of the Goods; or
- pay for the cost to replace the Goods; or
- pay for the cost to repair the Goods.

Conditions and exclusions:

The warranty is granted on the following conditions:

1. This warranty extends to the original retail Customer (you) and is not transferable;
2. This warranty does not apply to software programs, batteries, power supplies, cables or other accessories supplied in or with the product;
3. You must comply with all of the terms of any relevant agreement with NetComm and any other reasonable requirements of NetComm including producing such evidence of purchase as NetComm may require;
4. The cost of transporting the product under a claim based on this warranty to and from NetComm's nominated premises is your responsibility; and
5. NetComm does not have any liability or responsibility under this warranty where any cost, loss, injury or damage of any kind, whether direct, indirect, consequential, incidental or otherwise arises out of events beyond NetComm's reasonable control. This includes but is not limited to: acts of God, war, riot, embargoes, acts of civil or military authorities, fire, floods, electricity outages, lightning, power surges, or shortages of materials or labour.
6. You are responsible for the security of your computer and network at all times. Security features may be disabled within the factory default settings. NetComm recommends that you enable these features to enhance your security.

The warranty is void if:

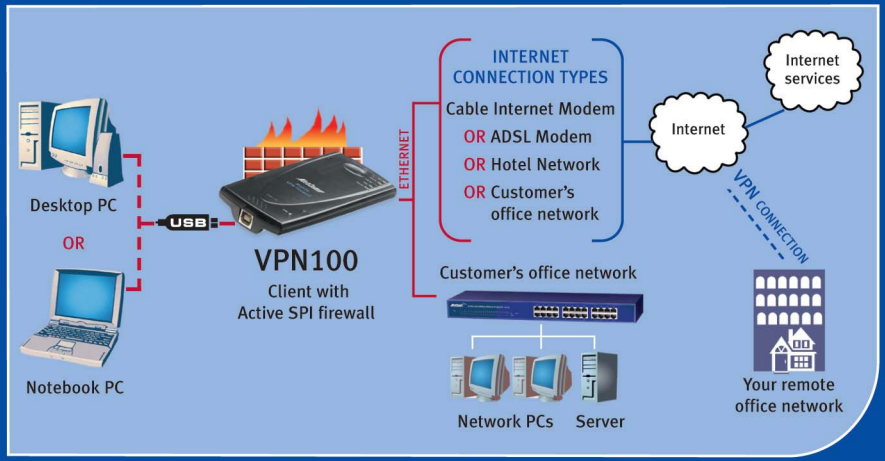
1. You, or someone else, use the product, or attempt to use it, other than as specified by NetComm;
2. The fault or defect in your product is the result of a voltage surge subjected to the product either by the way of power supply or communication line, whether caused by thunderstorm activity or any other cause(s);
3. The fault is the result of accidental damage or damage in transit, including but not limited to liquid spillage;
4. Your product has been used for any purposes other than that for which it is sold, or in any way other than in strict accordance with the user manual supplied;
5. Your product has been repaired or modified or attempted to be repaired or modified, other than by a qualified person at a service center authorised by NetComm; and,
6. The serial number has been defaced or altered in any way or if the serial number plate has been removed.

The only travelling companion for secure communications

Access your corporate or home network from wherever you are in the world with the NetComm Mobile VPN100. Advanced security features such as an active SPI firewall also ensure that you are protected from hackers.

Simple to install and configure, this small and lightweight device is perfect for any travelling executive. Just connect the NetComm Mobile VPN100 Firewall to your Notebook's USB port and access your network resources remotely from a hotel or another office via the Internet.

It's an essential travelling companion for every business executive.



KEY FEATURES

- Connects via PPPoE ADSL, LAN (DHCP) or Cable Internet
- Built-in IPsec VPN end-points with strong DES/3DES encryption
- Active hardware SPI firewall checks all incoming data
- Works with almost any Windows PC
- USB powered (no power pack required)
- Supports URL filtering – blocks; Java, ActiveX, Proxy & Cookies
- Network Address Translation hides PC from outsiders
- Easy to configure via your PC's web browser
- Back up and restore the device configuration

NetComm™

NetComm Limited, ABN 85 002 490 486 • PO Box 1200, Lane Cove NSW 2066 Australia. **PHONE** (02) 9424 2070 • **FAX** (02) 9424 2010 • **EMAIL** sales@netcomm.com.au
 Product Code: VPN100