SnapGear™ VPN Appliance Family
User Manual

Rev: 1.7.8
May 2nd, 2003

SnapGear, Inc.
7984 South Welby Park Drive #101
Salt Lake City, Utah 84084
Email: support@snapgear.com
Web: www.snapgear.com

Introduction

Table of contents

1. Introduction

This chapter provides an overview of your SnapGear appliance's features and capabilities, and explains how to install and configure your SnapGear appliance.

The SnapGear appliance enables small to medium-sized businesses to securely interconnect computers on your office network to the Internet. The SnapGear appliance has all the features a business needs to take full advantage of the Internet. Regardless of whether you are connecting to the Internet for the first time or looking for a cost-effective and safe VPN solution, the SnapGear appliance will meet your needs.

The SnapGear appliance simply and securely interconnects your network to the Internet using a robust embedded firewall. Shielded behind a NAT gateway, your office computers are protected from outside threats. The SnapGear appliance filters and checks data packets to prevent unauthorized Internet applications accessing your network.

The SnapGear appliance provides your network with a Virtual Private Network (VPN) server. A VPN enables remote workers or branch offices to securely access your company network to send and receive data at a very low cost. With the SnapGear appliance, you can remotely access your office network securely using the Internet. The SnapGear appliance can also connect to external VPNs as a client.

Using your SnapGear appliance, everyone on your office LAN can access the Internet using a single connection. Your entire network can log on to the Internet using only one ISP account through one analog modem, DSL or ISDN line. This eliminates separate connections and ISP charges for each individual user. Using a dial-in modem connected to your SnapGear appliance, your remote staff can also securely access your office network using direct-dial.

This manual describes how to take advantage of the features of your SnapGear appliance, including setting up an Internet connection, a secure firewall and a VPN. It also describes how to set up the SnapGear appliance on your existing or new network using the web configuration interface.

Installing your SnapGear appliance into a well-planned network is quick and easy. Although network planning and design is outside the scope of this manual, please take the time to plan your network prior to installing your SnapGear appliance.

Terminology

This section explains terms that are commonly used in this document.

Term	Meaning
ADSL	Asymmetric Digital Subscriber Line. A technology allowing high-speed data transfer over existing telephone lines. ADSL supports data rates between 1.5 and 9 Mb/s when receiving data and between 16 and 640 Kb/s when sending data.
BOOTP	Bootstrap Protocol. A protocol that allows a network user to automatically receive an IP address and have an operating system boot without user interaction. BOOTP is the basis for the more advanced DHCP.
DHCP	Dynamic Host Configuration Protocol. A communications protocol that assigns IP addresses to computers when they are connected to the network.
DNS	Domain Name System that allocates Internet domain names and translates them into IP addresses. A domain name is a meaningful and easy to remember name for an IP address.
DUN	Dial Up Networking.
Ethernet	A physical layer protocol based upon IEEE standards.
Extranet	A private network that uses the public Internet to securely share business information and operations with suppliers, vendors, partners, customers, or other businesses. Extranets add external parties to a company's intranet.
Failover	A method for detecting that the main Internet connection (usually a broadband connection) has failed and the SnapGear apliance cannot communicate with the Internet. If this occurs, the SnapGear appliance automatically moves to a lower speed, secondary Internet connection.
Fall-forward	A method for shutting down the failover connection when the main Internet connection can be re-established.
Firewall	A network gateway device that protects a private network from users on other networks. A firewall is usually installed to allow users on an intranet access to the public Internet without allowing public Internet users access to the intranet.
Gateway	A machine that provides a route (or pathway) to the outside world.
Hub	A network device that allows more than one computer to be connected as a LAN, usually using UTP cabling.
IDB	Intruder Detection and Blocking. A feature of your SnapGear VPN appliance that detects connection attempts from intruders and can also optionally block all further connection attempts from the intruder's machine.
Internet	A worldwide system of computer networks - a public, cooperative, and self-sustaining network of networks accessible to hundreds of

Term	Meaning
	millions of people worldwide. The Internet is technically distinguished because it uses the TCP/IP set of protocols.
Intranet	A private TCP/IP network within an enterprise.
IPSec	Internet Protocol Security. IPSec provides interoperable, high quality, cryptographically-based security at the IP layer and offers protection for network communications.
LAN	Local Area Network.
LED	Light-Emitting Diode.
MAC address	The hardware address of an Ethernet interface. It is a 48-bit number usually written as a series of 6 hexadecimal octets, e.g. 00:d0:cf:00:5b:da. A SnapGear appliance has a MAC address for each Ethernet interface. These are listed on a label on the underneath of the device.
Masquerade	The process when a gateway on a local network modifies outgoing packets by replacing the source address of the packets with its own IP address. All IP traffic originating from the local network appears to come from the gateway itself and not the machines on the local network.
NAT	Network Address Translation. The translation of an IP address used on one network to an IP address on another network. Masquerading is one particular form of NAT.
Net mask	The way that computers know which part of a TCP/IP address refers to the network, and which part refers to the host range.
NTP	Network Time Protocol (NTP) used to synchronize clock times in a network of computers.
PAT	Port Address Translation. The translation of a port number used on one network to a port number on another network.
PPP	Point-to-Point Protocol. A networking protocol for establishing simple links between two peers.
PPPoE	Point to Point Protocol over Ethernet. A protocol for connecting users on an Ethernet to the Internet using a common broadband medium (e.g. single DSL line, wireless device, cable modem, etc).
PPTP	Point to Point Tunneling Protocol. A protocol developed by Microsoft™ that is popular for VPN applications. Although not considered as secure as IPSec, PPP is considered “good enough” technology. Microsoft has addressed many flaws in the original implementation.
Road warrior	A remote machine with no fixed IP address.
Router	A network device that moves packets of data. A router differs from hubs and switches because it is “intelligent” and can route packets to their final destination.
Subnet mask	See “Net mask”.
Switch	A network device that is similar to a hub, but much smarter. Although

Term	Meaning
	not a full router, a switch partically understands how to route Internet packets. A switch increases LAN efficiency by utilizing bandwidth more effectively.
TCP/IP	Transmission Control Protocol/Internet Protocol. The basic protocol for Internet communication.
TCP/IP address	Fundamental Internet addressing method that uses the form *nnn.nnn.nnn.nnn*.
UTC	Coordinated Universal Time.
UTP	Unshielded Twisted Pair cabling. A type of Ethernet cable that can operate up to 100Mb/s. Also known as Category 5 or CAT 5.
VPN	Virtual Private Networking. When two locations commmunicate securely and effectively across a public network (e.g. the Internet). The three key features of VPN technology are privacy (nobody can see what you are communicating), authentication (you know who you are communicating with), and integrity (nobody can tamper with your messages/data).
WAN	Wide Area Network.
WINS	Windows Internet Naming Service that manages the association of workstation names and locations with IP addresses.

Document conventions

This document uses different fonts and typefaces to show specific actions.

Warning

Warning text like this highlights important issues.

Bold text in procedures indicates text that you type, or the name of a screen object (e.g. a menu or button).

Installing and configuring your SnapGear appliance

This manual contains instructions for installing and configuring your SnapGear appliance on your network. The basic steps and related chapters are:

Step	**Chapter**
1. Interconnect the SnapGear appliance and PCs on a local area network.	Chapter 2, Getting started
2. Connect the telecommunications hardware/modem for dial-in/dial-out Internet access.	Chapter 3, Connecting to the Internet
3. Set up the network IP addresses and firewall.	Chapter 2, Getting started
4. Set up Internet hardware and Internet account and connect to the Internet.	Chapter 3, Connecting to the Internet
5. Set up users' security dial-in/dial-out VPN.	Chapter 4, Dial-in server configuration Chapter 6, Firewall Chapter 7, Virtual Private Networking

Your SnapGear appliance

The following items are included with your SnapGear appliance:

- Power adapter
- Installation CD
- Printed Quick Install guide
- Cabling including
    - 1 normal “straight through” UTP cable (blue color).
    - 1 “cross-over” UTP cable (either gray or red color). If you have the LITE+ or LITE2+ you will receive two straight through cables (blue color).

LEDs

The front and rear panels contain LEDs indicating status. The front panel LEDs are illustrated in the following figure and detailed in the following table.

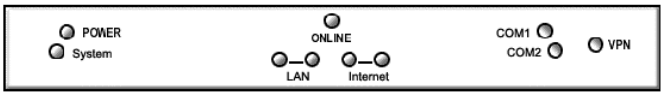


Figure 1.1 SnapGear SOHO+/PRO front panel LEDs

Label	Activity	Description
POWER/PWR	On	Power is supplied to the SnapGear appliance.
System/SYSTEM	Flashing	System flashes once every second when the SnapGear appliance is operating correctly.
	On	If the System LED is on and not flashing, an operating error has occurred. In this situation, the other LEDs form a diagnostic pattern indicating the failure.
Online/ONLINE	On	Indicates a valid Internet connection is present.
COM 1, 2	Flashing	For either of the SnapGear appliance COM ports, these LEDs indicate receive and transmit data.
VPN	On	Virtual Private Networking is enabled.

The rear panel contains the connector ports for the LAN (*LAN*) and modem (*COM1*, *COM2*), LAN 10BaseT status LEDs, WAN 10BaseT status LEDs, the reset button and power inlet.

For units with LAN/Internet status LEDs, one LED represents the *link* condition (upper on SME530, SME550 and PRO+, lower on PRO and SOHO+), where a cable is connected correctly to another device (e.g. a cable modem). The other light represents the *activity* as per the front panel.

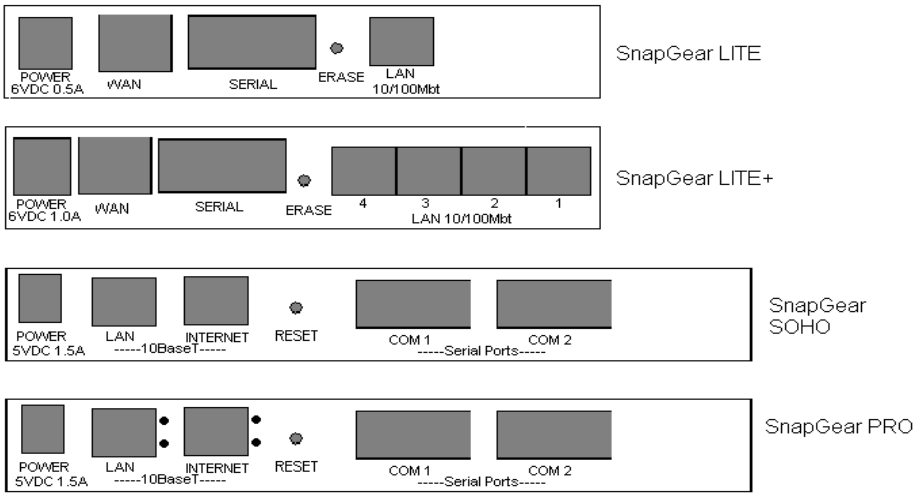


Figure 1.2 SnapGear appliance back panels

The following figure shows how your SnapGear appliance interconnects . If you are using the SnapGear LITE+ or LITE2+, a secondary hub/switch is not required as this unit has a 4-port Ethernet switch.

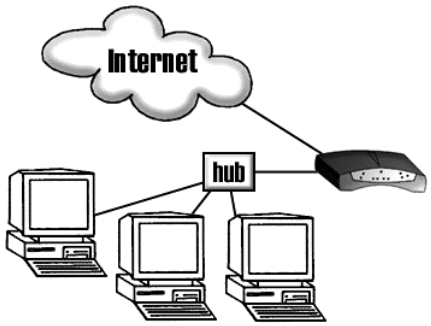


Figure 1.3 Network interconnections

SnapGear appliance features

- Software features

    - Network Address Translation (NAT) firewall that isolates the LAN from the Internet and offers network access control and filtering. Usually a simple form of NAT called *masquerading* is used.

    - DHCP server and client that ensure simple and flexible IP network configuration.

    - PPTP VPN server that provides communications to remote users running standard Windows VPN client software.

    - PAP, CHAP, MSCHAPv2, RADIUS and TACACS+ tunnel authentication (RFC1334, RFC1994).

    - Transparent tunnel support for PPTP. IPSec pass through.

    - Dial-in remote access with PAP, CHAP, MSCHAPv2, RADIUS and TACACS+ authentication.

    - Dial-on-demand for outgoing Internet connections.

    - Wizard setup and browser-based management and configuration.

    - Flash upgradeable firmware that allows you to download and install the latest protocols and security software using the web. This option is not available for the LITE and LITE+ models.

    - Connect Windows PCs, Macintoshes, Linux and Unix workstations - basically anything that talks IP - to the Internet.

Internet link features

- Connect to the Internet using an external cable modem, DSL, dial-up or ISDN modem.
- Serial ports connect to the Internet using an external modem or ISDN T/A. The LITE2, LITE2+, SME530 and SME550 models have a single serial port.
- 10baseT Ethernet port (*Internet*) that connect to the Internet using a cable or ADSL modem.
- Front panel serial status LEDs (for TXD/RXD).
- Online status LEDs (for Internet/VPN).
- Rear panel Ethernet LEDs (Link Transmit/Receive).

LAN link features

- 10/100BaseT LAN port to connect to the local network Ethernet on PRO+, LITE2, LITE2+, SME530 and SME550 models, 10BaseT on other models.
- Rear panel Ethernet LEDs (Link Transmit/Receive) on all models but LITE2 and LITE2+.

Dial-in connection features

If you are using the SnapGear PRO+, PRO, SOHO+, SME530 or SME550, external modems may be attached via serial port for dial-in connections. Additionally, the SnapGear PRO+ has an internal modem that can be used for dial-in connections.

Environmental features

- External power adaptor (voltages/current depend on individual models).
- Front panel status LEDs: Power Test.
- Operating temperature between 0° C and 40° C.
- Storage temperature between -20° C and 70° C.
- Humidity between 0 to 95% (non-condensing).

2. Getting started

Your SnapGear appliance provides a secure, simple gateway to connect PCs and other devices on your local network to the outside world. This chapter provides step-by-step instructions for connecting the SnapGear appliance to your LAN. The procedures in this section expand on the steps in the *SnapGear Quick Install Guide*, which you may prefer to use if you are in a hurry.

If you are connecting the SnapGear appliance to an established LAN, use a standard Ethernet cable to connect the SnapGear LAN port to a spare port on the network's hub. If you are connecting your SnapGear appliance to a single PC, use the provided Ethernet crossover cable to interconnect them directly. In the case of the SnapGear LITE+ and LITE2+, use a standard Ethernet cable to connect any one of its four LAN switch ports to a single PC, or an Ethernet crossover cable to connect to another hub.

The SnapGear appliance comes with an in-built DHCP server that can automatically assign IP addresses to other devices on the network. If you have an existing network, you may already have an active DHCP server and the PCs and devices on the network may already have IP addresses assigned. To simplify the installation in existing networks, the SnapGear appliance ships without an initial IP address and without the DHCP server activated by default.

If your network does not have an active DHCP server, it is recommended that you take advantage of using the SnapGear appliance as a DHCP server and setup the PCs on your network to dynamically receive TCP/IP configuration information.

Static IP reset

Although it is not the default behaviour, it is also possible to boot the SnapGear appliance with an initial, static IP address of **192.168.0.1** (netmask 255.255.255.0). While the SnapGear appliance is running (i.e. *System*/*TST*/*Heart Beat* is blinking), press the black *RESET* button twice within 3 seconds.

Note that this will reset any existing configuration options back to their factory defaults. Additionally, your network must (at least initially) be on the **192.168.0.0**/**255.255.255.0** subnet, as per step 6 of *New Networks*.

Note

The following steps detail the initial setup procedure for networks with at least one Windows workstation. If you wish to perform the setup procedure using a Linux box, skip to the section called later in this chapter.

New Networks

If you do not have an existing LAN, you need to configure one networked PC to get started:

1. Install an Ethernet adapter and software driver in at least one of the PCs to be networked.

2. Assign an IP address for your PC so the SnapGear appliance can be configured on the network. From the Start menu, select Settings, Control Panel, Network and click the Configuration tab (or Protocols if using NT).

3. Ensure that the TCP/IP networking protocol is installed. If not, click Add (then Protocol if using Windows 95/98, Microsoft then TCP/IP). Your PC will then reboot.

4. Highlight TCP/IP (followed by your Ethernet adapter's name if using Windows 95/98) and click Properties.

5. In the IP Address panel, select Specify an IP Address. Private network addresses should be in the ranges:

```
10.0.0.0 - 10.255.255.255  (10/8 prefix)
172.16.0.0 - 172.31.255.255  (172.16/12 prefix)
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)
```

6. If you have chosen to use the static IP reset feature of the SnapGear appliance, choose an address in the range:

   `192.168.0.0 - 192.168.0.255 (192.168.0/24 prefix)`

   Enter the value into the IP Address field followed by a number (1-254) to identify your PC (e.g. *192.168.0.2*). You may have to reboot at this point.

7. Connect the SnapGear appliance and the PC to the hub and continue with the following steps.

Note

Your SnapGear appliance ships with a Windows installation program called the **SnapGear Setup Wizard**. *If you are using statically pre-assigned IP addresses on your network (i.e. there is a static network with no active DHCP server), the Setup Wizard will help assign an IP address to the SnapGear appliance.*

On DHCP enabled (i.e. dynamic) networks, or if you have performed a static IP reset, the Setup Wizard will locate the IP address assigned to your SnapGear appliance. The Setup Wizard will also provide the option to change the SnapGear appliance administrative password.

You can run the Setup Wizard from any PC on the network running Windows 2000, Windows XP, Windows ME, Windows NT 4 or Windows 95/98.

If you are using Windows 95 you must have the MS Dial Up Networking 1.3 update *(**msdun13.exe**) installed.*

If you are using an early version of Windows 95 (i.e. pre-OSR2), you must install the Winsock 2.0 update *(**w95w2setup.exe**). If you are using Windows NT, Windows 2000, or Windows XP Professional you must be logged in as* administrator *to run the Setup Wizard.*

Configuring the SnapGear appliance on your network

Below is an overview of the steps in initial setup of the SnapGear appliance on your network:

1. Apply power to the SnapGear appliance. When the SnapGear appliance is powered on in factory default mode, it has no LAN IP address. This state is indicated by all front panel LEDs except *Power* flashing (except on LITE+ and LITE2+). The LEDs remain flashing until a LAN IP address is acquired.

   Note

   If the LEDs on the front of the unit are not initially flashing, try pressing the Reset/ERASE *button on the back panel of the unit. This does not apply to the LITE+ and LITE2+ models, which do not flash their LEDs. If after doing this all the LEDs on the front on the unit do not flash, then you may need to contact customer support.*

   However, the SnapGear appliance may be acquiring an initial IP address from another DHCP server on the LAN, causing its LEDs to stop flashing soon after booting. In this case, the SnapGear Setup Wizard *will detect this address, as detailed in the following steps.*

2. Insert the *Installation CD* into the CD drive of any Windows PC on your network that meets the system requirements. If the setup program does not run automatically, select **Run** from the **Start** menu and type **`z:\setup`** (where **`z`** is the letter of your CD drive).

3. Select the directory and Start menu group where the software utilities for your SnapGear appliance will be installed.

4. The wizard will search the network for your device. If your SnapGear appliance does not yet have an IP address assigned to it, you will be asked to enter one now. The next section, *Set up an IP address*, describes this scenario in more detail.

Note

The front of the SnapGear appliance contains activity LEDs that vary slightly between models. These provide information on the operating status of your SnapGear appliance. In particular you should note:

The Power/PWR LED is on when power is applied (use only the SnapGear Power Adapter packaged with the unit).

The System/TST/Heart Beat LED blinks when the SnapGear appliance is running.

For all modes except the LITE+ and LITE2+, all LEDs (except Power/PWR) will flash when your SnapGear appliance is powered on for the first time in factory default mode. These LEDs stop flashing when the device has been assigned an IP address, or if a static IP reset is performed.

Set up IP addresses

To communicate on your network the SnapGear appliance will need an IP address. This is accomplished using the *SnapGear Setup Wizard* application that ships with your SnapGear CD. If the SnapGear appliance has already been assigned an IP address

Note

The WAN interface is by factory default inactive in that there are no network services such as DHCP in operation, and no IP address is configured. The LAN interface is set up as a DHCP client, and will not initially have an assigned IP address. This is deliberately set to be passive so as not to interfere with your existing LAN. All of this will be configured later in the installation process but to get you up and running the **setup.exe** *application is simply a miniature DHCP server that will give the SnapGear appliance a known IP address. If you use Linux, Unix, Macintosh or another operating system you may either use a DHCP server application to assign an IP address.*

The *SnapGear Setup Wizard* can be run from any PC on the network that is running Windows. To run SnapGear Setup Wizard:

Insert the *SnapGear Installation CD* into your CD drive.

The Setup Wizard should automatically run, but if not then select **Run** from the **Start** menu and type **z:\setup.exe** (where **z** is the letter of your CD drive), or use Windows Explorer to find the program.

SnapGear Setup Wizard will install some files onto your PC, then attempt to find your SnapGear appliance on the network. At this point, the installation procedure diverges and a popup window will display either **A**, **B** or **C**.

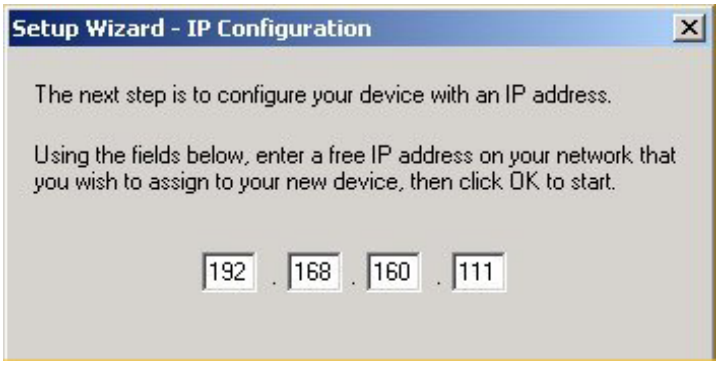
A. Your SnapGear appliance was found on the network.

This means either your network is DHCP enabled and another PC on the network has already given it an IP address, or you have chosen to boot the SnapGear appliance with an initial, static IP address. If this is the case, skip to *Administrative Password* further on in this chapter.

B. Multiple SnapGear appliances were found on the network.

This means your network is DHCP enabled. If this is the case, SnapGear Setup Wizard will prompt you to select which SnapGear VPN Router you wish to configure, based on its LAN port MAC address. The SnapGear Setup Wizard will display each of the different SnapGear VPN Routers that were found on the network. When the appropriate one is displayed, click "Yes" to indicate that this is the unit you want to configure. Your SnapGear VPN Router's LAN port MAC address is printed on its underside of the unit. Make the appropriate selection, then skip to *Administrative Password* further on in this chapter.

C. Your SnapGear appliance needs an IP address.



This means your network is *not* DHCP enabled and you must perform the following steps:

Enter the IP address that you want to assign to your SnapGear appliance. *SnapGear Setup Wizard* will already have auto-completed the IP address. Verify that this address is acceptable and not already in use, and click OK.

SnapGear Setup Wizard will check that the IP address you selected isn't already in use. If it is you will be asked to make a new selection, otherwise it is assigned to your SnapGear appliance. Note that this may take a few seconds.

Your SnapGear VPN Router is now set up with an IP address so all front panel LEDs (except *System/TST/Heart Beat*) will stop flashing.

Administrative password

After an IP address is allocated or the SnapGear appliance has been located, the SnapGear Setup Wizard will prompt you to change the SnapGear appliance administrative password. This password controls access to the *SnapGear Management Console* web administration pages.

SnapGear recommends that you select a new password that is easy for you to remember but difficult for other people to guess. Your password must be kept secret to maintain the security provided by the SnapGear appliance.

SnapGear Management Console web administration pages

Your SnapGear appliance is now configured. The Setup Wizard will prompt you to launch a web browser to open the *SnapGear Management Console* web administration pages.

The *SnapGear Management Console* web administration pages is where you can configure the additional features of your SnapGear appliance.

To access the web administration pages, select **Management Console** under **SnapGear** in the Start menu. Alternately you can point your web browser to the SnapGear appliance's IP address (e.g. **`http://192.168.0.1`**).

If you cannot access the web administration pages, check that your browser proxy settings are correctly configured. In Microsoft's Internet Explorer, the settings are modified in *Tools*, *Internet Options*, *Connection* tab, *LAN settings*.

Initial setup using Linux

By default, your SnapGear appliance as shipped does not have any IP addresses configured. When the SnapGear appliance is powered on, if it has no LAN IP address all the front panel LEDs except *Power* will flash (except on LITE+ and LITE2+). The LEDs remain flashing until a LAN IP address is acquired.

The first setup task is to add an IP address in the SnapGear appliance using either DHCP or BOOTP. You may use an existing local DHCP/BOOTP server, set up a new local DHCP/BOOTP server, or use the **`lin_set_ip`** program on the SnapGear CD in the **`/tools`** directory.

Alternately, you may choose to boot the SnapGear appliance with the initial, static IP address of **192.168.0.1** (netmask 255.255.255.0). Refer to the start of this chapter for details on how to activate this option.

Using *lin_set_ip*

The **`lin_set_ip`** program is a command line tool for assigning an IP address or you SnapGear appliance. Depending on your system configuration, you may need root privileges to run this tool.

You may also need to add an extra static route using:

```
route add –host 255.255.255.255 eth0
```

where **`eth0`** is the name of your LAN interface. You may need to prefix this line with the **`route`** command's directory path (e.g.***`/sbin/route add`***, etc.).

Run **`lin_set_ip`** with the additional arguments of the IP address and netmask for your SnapGear appliance, e.g.:

```
./lin_set_ip 192.168.0.1 255.255.255.0
```

After a short time, the IP address is assigned to the SnapGear appliance and the LEDs will stop flashing.

Using an existing local DHCP or BOOTP server

If your local network is configured with a DHCP server, the SnapGear appliance will automatically acquire an address when attached to the network. Check your local DHCP server logs to find the address assigned to your SnapGear appliance.

If you are unable to access your local DHCP server logs, you can find the assigned address by entering the following commands at a command prompt.

1. **ping –b <subnet broadcast address>**

2. **arp –a**

The output of the '**arp**' command will contain the MAC address of your SnapGear appliance and the corresponding Internet Address. You can find the MAC address printed on the underside of your SnapGear appliance.

If your network has a BOOTP server, it can be used to set up the SnapGear appliance. Edit the BOOTP server file **/etc/bootptab** and add an entry for the SnapGear appliance. Use the Ethernet MAC address printed on a label on the bottom of the SnapGear appliance. Restart bootpd if it is running and connect the SnapGear appliance to the local network.

The SnapGear appliance will accept gateway and DNS server tags from DHCP or BOOTP, and automatically set up the routing tables for the SnapGear appliance.

Configuring a new local DHCP or BOOTP server

If your network has no DHCP or BOOTP server, you can temporarily configure a local Linux system as a bootp server using the following steps:

1. Edit **the /etc/inetd.conf** file.

2. Search for the **bootpd** line. Most distributions ship with this feature disabled (i.e. the line is commented out with "**#**" at the front). Remove the "**#**" from the start of this line.

3. Save and exit the file.

4. Edit the **/etc/bootptab** file. At the bottom of the file, add the following new line:

```
SnapGear appliance:ht=ethernet:ha=00d0cf000101:ip=192.168.0.1
```

   You need to modify the IP address (tag "**ip**") to match the addressing for your local network and use an address in your local subnet.

   You also need to modify the MAC address (tag "**ha**") to match your SnapGear appliance hardware. The MAC address is printed on a label on the underside of the SnapGear appliance. You can optionally include gateway ("**gw**") and DNS ("**ds**" and "**dn**") tags if required. See the manual page for *bootptab* for further information.

5. Save and exit the file.

Restart TCP/IP on your system. If you are unsure how to restart TCP/IP, simply reboot the Linux system. Once the system is running, it will serve the IP address to the SnapGear appliance when it is connected to your network.

After completing the initial network setup, you can use the web pages for the common configuration tasks.

SnapGear Quick Setup

The SnapGear Quick Setup Wizard will guide you through the basic steps for configuring the LAN port for your SnapGear appliance and connecting to the Internet.

To start the wizard, click the **Quick Setup Wizard** link on the **SnapGear Appliance Configuration** page. To modify the configuration, you need to enter the administrator username and password for the SnapGear appliance. The username is *root*, the default factory password is *default*.

LAN port quick setup

The following figure shows the LAN port quick setup:

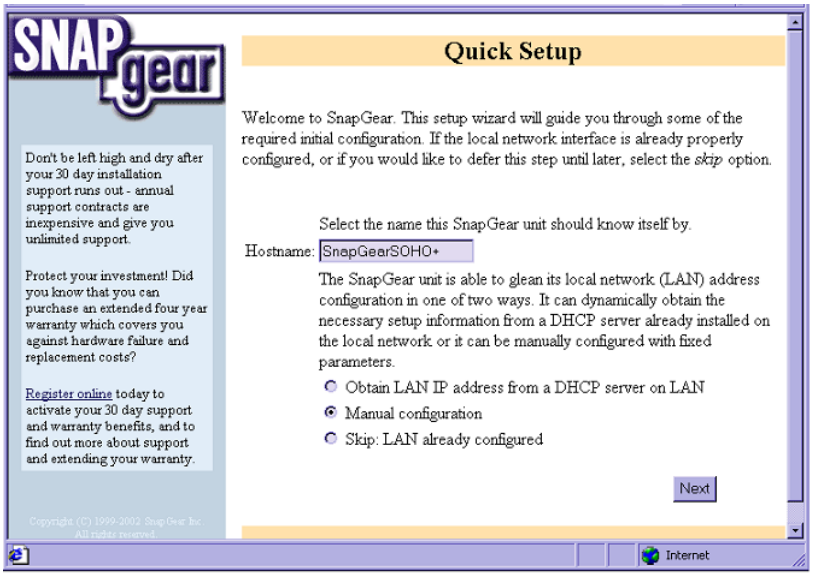


Figure 2.3 LAN port quick setup

1. Enter the name for your SnapGear appliance on the LAN.

2. Select the method for setting the LAN port network address configuration (either DHCP or manual).

3. If you select **DHCP** or **Skip**, the **Next** button will take you to the **ISP Connection** configuration page.

4. If you select **Manual,** the **Next** button shows the **Manual LAN Configuration** page where you must enter an **IP address** and a **Subnet mask** for the SnapGear appliance's LAN port.

ISP connection quick setup

The following figure shows the ISP connection quick setup:

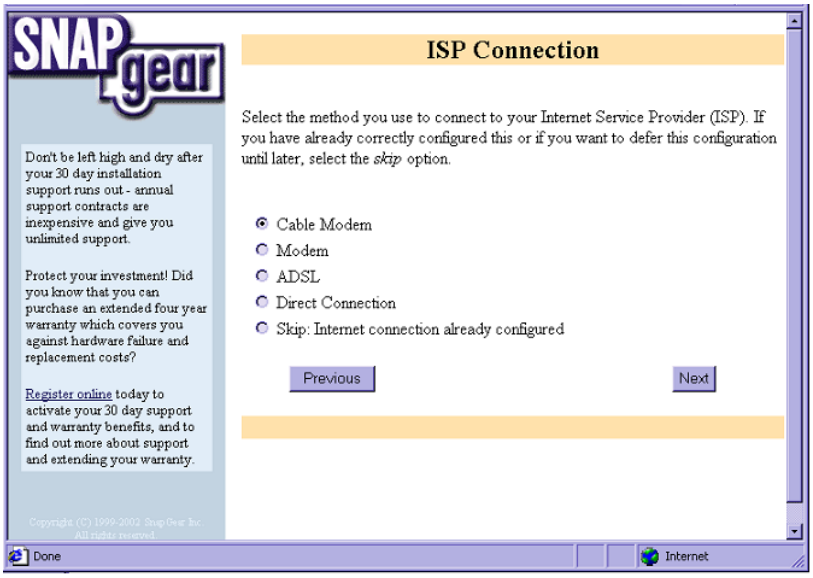


Figure 2.4 ISP connection quick setup

Select **Cable Modem, Modem, ADSL, or Direct** as the method for connecting to your ISP. **Direct connections** are where the SnapGear Internet Port is connected to a LAN with another gateway to the Internet.

For cable modems, you need to enter your Cable Modem Service Provider. This is usually **Generic Cable Modem Provider**.

If you use an external analog modem to connect to your ISP, you must also specify:

- The serial port connected to your modem. The SnapGear SOHO+ and SnapGear PRO have two serial ports; the SnapGear LITE, LITE+, LITE2 and LITE2+ have only one. The SnapGear PRO+ has one integrated modem and one serial port.
- The name of your ISP.
- The phone number used to dial your ISP.
- The username and password for your ISP account.

- The DNS server for your ISP.

If you use ADSL (Asymmetric Digital Subscriber Line) to connect to your ISP, you must specify the ADSL connection type. This can be done in one of the following ways:

- Allow your SnapGear appliance to automatically detect your ADSL connection type. This is the best choice in most cases.

- **Use PPPoE to connect.** Select this option if your ADSL modem communicates using PPPoE, or if your ISP accesses the Internet using username and password authentication. You will also be asked to specify:

    - The username and password for your ADSL connection.

    - If you want to **connect on demand** or stay connected continuously (the best choice in most cases).

    - For **connect on demand** connections, you need to specify the **idle disconnect time** (in minutes).

- **Use DHCP to connect.** DHCP is used if your ISP requires you to get an IP address automatically from a DHCP server over the Internet.

- **Manually assign settings.** Select this option if your ISP provides a fixed IP address and a subnet mask and (optionally) a gateway address and a DNS address to be configured into the computer connecting to the ADSL modem.

- For a **Direct Connection** you must configure the Internet port to either get its address information via DHCP or manually enter static values for **IP Address, Subnet Mask, Gateway Address,** and **DNS Address.** The **Gateway Address** is the address of the host where all Internet network traffic is initially directed for further processing. The **DNS Address** is the address of the host that translates Internet domain names into IP addresses.

Configuring the PCs on your network

To access the Internet, all PCs on your network must have:

- The IP address of the SnapGear appliance defined as their default gateway, and
- Must use the DNS server provided by the ISP or the DNS proxy on the SnapGear appliance.

You can enter these details manually (i.e. statically), or they can be dynamically assigned by a DHCP server each time the PC boots.

To take advantage of the SnapGear appliance's DHCP server (or if you are already using a DHCP server on the network), configure the computers on your network to use DHCP.

If you are using Windows 95/98, click the **Configuration** panel, **TCP/IP-<your network adapter>**, **Properties**, then the **IP Address** panel.

If you are using Windows NT 4, click the **Protocols** panel, **TCP/IP**, **Properties**, and then the **IP Address** panel.

If you are using Windows 2000, click **Start**, **Settings**, **Network and Dial-up Connections**, right-click **Local Area Connection**, click **Properties**, select **Internet Protocol** and then click **Properties** to display the following screen:

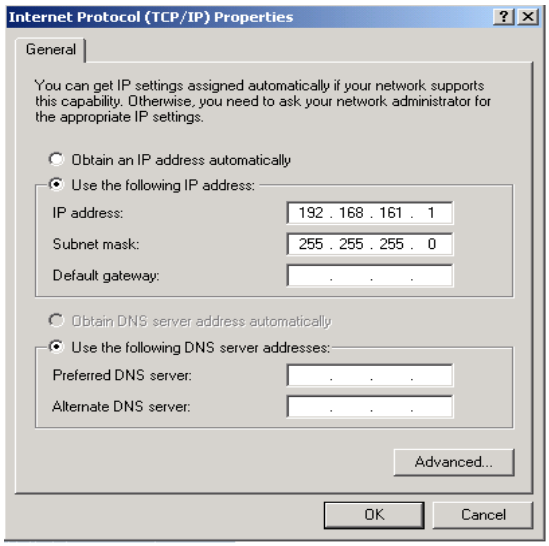


Figure 2.3 TCP/IP properties

You can also manually configure the PCs on your network. For each non-configured Windows 2000 PC on the network, open **TCP/IP Properties** using the above instructions and ensure that **Use the following IP address** is checked and add the following information:

- A unique IP address and appropriate subnet mask.
- The Default Gateway (enter the IP address of the SnapGear appliance).
- In the *DNS* tab, enter the DNS server address(es) provided by your ISP, or the address of the SnapGear appliance if you are using the DNS proxy.

3. Connecting to the Internet

This chapter provides step-by-step instructions for connecting your SnapGear appliance to your Internet Service Provider (ISP).

The SnapGear appliance provides secure Internet access using its robust embedded firewall. The SnapGear appliance has an IP masquerading feature, which means that users on your local network can see the outside world; however the outside world cannot see inside your local network. This shields your network from intruders and also allows you to filter packets (see *Chapter 6, Firewall*) to prevent unwanted traffic to/from your network.

The SnapGear appliance can connect to the Internet using an external dialup analog modem, an ISDN modem, a permanent analog modem, a cable modem or DSL link as shown in the following figure:

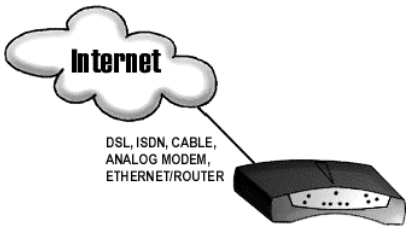


Figure 3.1 Internet connection

Physically connect modem device

The first step in connecting your office network to the Internet is to physically attach your SnapGear appliance to the modem device. For analog modems, attach the modem serial cable to one of the SnapGear appliance's serial ports (i.e. *COM1*, *COM2*). For digital connections (e.g. cable, DSL), plug the cable into the *Internet* port.

Warning

To connect to an ISDN line, the SnapGear appliance requires an intermediate device called a Terminal Adapter (TA). A TA connects into your ISDN line and has either a serial or Ethernet interface that is connected to your SnapGear appliance. Do NOT plug an ISDN connection directly in to your SnapGear appliance.

Select Internet connection

The next step is to select the method for connecting your SnapGear appliance to the Internet. From the **SnapGear appliance Config Pages,** in the **Networking** menu, select **Connect to Internet** and select the method to connect to your local ISP. You can connect using a cable, ISDN, DSL or analog modem connection. Select the connection type and click **Continue**.

Connect to Internet – cable modem

If you are connecting to the Internet using a cable modem, select a cable connection, select your cable ISP from the list and click **Next**. If your provider does not appear, select *Generic Cable Modem Provider.* For cable modem providers other than Generic, enter your username and password and click **Finish**. You are now ready to connect. Click the **Reboot** button to save your configuration and reboot your SnapGear appliance.

Connect to Internet – ADSL

If you are connecting to the Internet using ADSL, you must select the connection method **PPPoE, DHCP,** or **Manually Assign Settings.** Alternatively, the SnapGear appliance can determine the connection method automatically.

Use PPPoE if your ISP uses username and password authentication to access the Internet. Use DHCP if your ISP does not require a username and password, or if your ISP instructed you to obtain an IP address dynamically. If your ISP has given you an IP address, you must manually assign the settings on the SnapGear appliance's Internet interface. Select the appropriate method and click **Apply.**

For PPPoE, enter the username and password for your ISP account. By default, your SnapGear appliance maintains the ADSL connection continuously; however you can change this if required to **Connect on Demand**. For on demand connections, enter an **Idle Disconnect Time**. This is the time (in minutes) that the SnapGear appliance will wait before disconnecting if the line is idle.

DHCP connections also require a host name for your SnapGear appliance. Select **Manually Assign Settings** and enter the **IP Address** and **Netmask** and optionally the **Gateway** and the **DNS Address** if provided by your ISP. Reboot the SnapGear appliance for the new configuration to take effect.

If you are unsure of the **ADSL Connection Method**, select **Autodetect connection type** and your SnapGear appliance will attempt to automatically determine the connection method.

Connect to Internet – direct

Choosing **Direct Connection** to the Internet shows the **IP Configuration** page. See the section called *IP configuration.*

Connect to Internet – modem

The following figure shows the Setup modem Internet connection:

Figure 3.2 Setup modem Internet connection

If you are connecting to the Internet using a modem, the system displays the **Connect to Internet via a Modem** screen. The following table describes the fields and explains how to configure the dial up connection to your ISP.

Field	Description
Serial port to dial-out on	Select the SnapGear appliance COM (serial) port you will use for the modem that will dial your ISP. This port will be dedicated for the Internet connection; any attempt to dial-in using this COM port will be blocked. Note: If a port was previously setup for dial-in and is later enabled for Internet access, the dial-in function is automatically disabled.
Name of Internet provider	Enter the name of your ISP.
Phone number to dial	Enter the number to dial to reach your ISP. If you are behind a PABX that requires you to dial a prefix for an outside line (e.g. 0 or 9) ensure you enter the appropriate prefix.
ISP DNS Server	Enter the DNS server address supplied by your ISP.
Username and password	Enter the unique username and password allocated by your ISP. The **Password** and **Confirm Password** fields must match.

Click **Advanced** to configure the following options.

Field	Description
Idle timeout	By default, the SnapGear appliance dials-on-demand (i.e. when there is traffic trying to reach the Internet) and disconnects if the connection is inactive (i.e. when there is no traffic to/from the Internet) for 15 minutes. If using dial-on-demand, this value can be set from 0 to 99 minutes. Selecting **Stay Connected** will disable the idle timeout.
Redial setup	If the dial up connection to the Internet fails, **Max Connection Attempts** specifies the number of redial attempts to make before discontinuing . **Time Between Redials** specifies the number of seconds to wait between redial attempts.
Statically assigned IP address	The majority of ISPs dynamically assign an IP address to your connection when you dial-in. However some ISPs use pre-assigned static addresses. If your ISP has given you a static IP address, enter it in **Local IP Address** and enter the address of the ISP gateway in **Remote IP Address**.

Internet failover

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

Failover provides the ability to use a low-speed connection when the high-speed connection fails to allow services to continue operating. When the main Internet connection fails and the backup connection (or failover) is started, VPN connections are restarted and dynamic DNS services are advised of the new IP address.

Internet failover is currently only available in the SnapGearSOHO+, SnapGearPRO, and SnapGearPRO+ appliances. After configuring a normal Internet connection, a link to the Internet failover page allows you to configure failover support. You can also access the failover page by clicking Connect To Internet in the Networking menu.

The following figure shows the advanced configuration options:

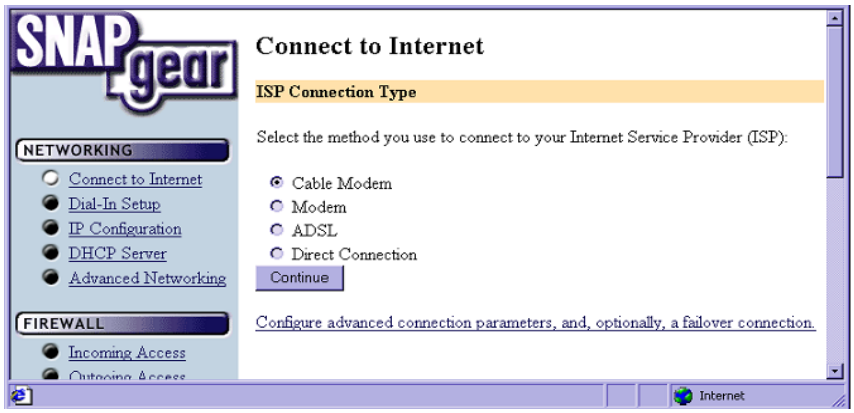


Figure 3.3 Advanced configuration option

The following figure shows the failover configuration screen:

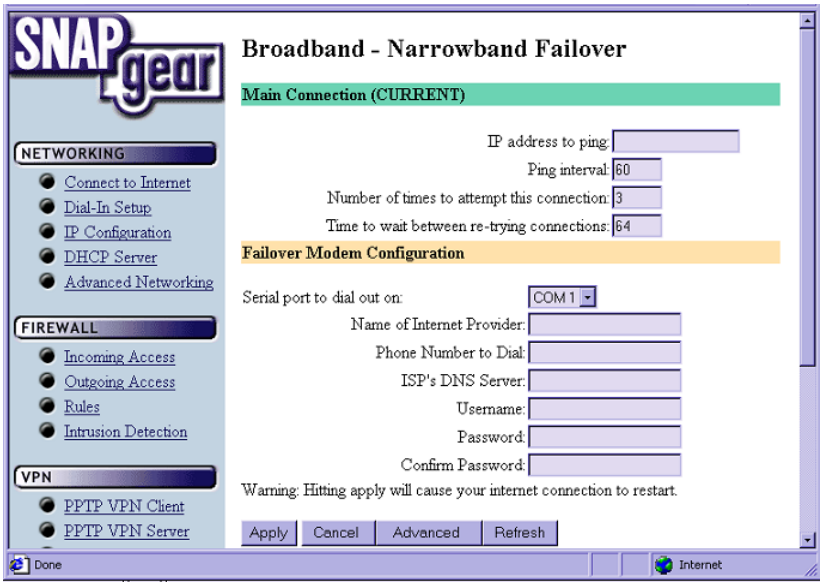


Figure 3.4 Failover configuration screen

The following fields can be configured for the failover connection.

Field	Description
IP Address to ping	IP address the SnapGear appliance will ping to determine if the Internet connection is up or down.
Ping Interval	How often to ping the remote machine to determine if the Internet connection is up or down.
Number of times to attempt this connection	Number of times to attempt the connection before the SnapGear appliance moves to the failover connection.
Time to wait between re-trying connections	The Internet connection fails immediately when the password is wrong, or if the SnapGear appliance is unable to contact an ADSL modem to make a connection. Specify the time to wait between retrying this connection after detecting the initial failure.
Fall forward. This option is only available after configuring the failover connection.	Allow the SnapGear appliance to continue trying the main Internet connection until the connection is established. At this point the SnapGear appliance disconnects the backup Internet connection and continues using the main Internet connection.
Enable failover. This option is only available after configuring the failover connection.	Checking this box indicates you want the SnapGear appliance to use the backup Internet connection if the SnapGear appliance detects that the main Internet connection has failed.

Failed connection

An Internet connection is considered failed if the SnapGear appliance tests the Internet connection the specified number of times, and fails each time. The SnapGear appliance can test the Internet connection by ensuring that the physical connection was made correctly (i.e. an IP address was received from the ISP), and then pinging a remote host.

For some Internet connections (e.g. PPPoE ADSL) you may need to ping a remote host to determine if the Internet connection is up or down. The SnapGear appliance will usually detect if a PPPoE ADSL Internet connection is down.

For Internet connection types that require you to specify a static IP address or use DHCP, the SnapGear appliance cannot usually detect if the Internet connection is down. To ensure that the Internet connection is up, enter a host for the SnapGear appliance to ping.

If the Internet connection fails, the SnapGear appliance will attempt to reconnect to the Internet using the main connection for the number of specified times. After each failed attempt, the SnapGear appliance will wait the number of seconds specified.

For PPPoE and dial-up connections, the SnapGear appliance sends an echo request and the remote machine responds with an echo reply. The main connection is considered down if more than three echo replies do not appear.

Warning

You currently cannot failover for an ADSL demand dial-internet connection, or for any type of analog modem connection.

Configure PCs to use SnapGear appliance Internet gateway

The PCs on your network must be configured to use the SnapGear appliance as the default gateway for Internet access. See the section called *Configuring the PCs on your network* for more information.

Establishing the connection

If you are connecting to your ISP using a modem or ISDN connection, the SnapGear appliance will automatically place a call when an application requires access to the Internet (e.g. sending e-mail, browsing the web, etc).

To establish the connection:

1. From any PC on the network, launch a browser application (e.g. Internet Explorer or Netscape Navigator).

2. The SnapGear appliance will dial the ISP and log in. On the front panel, the *COM* LED will flash when establishing the connection.

3. The *ONLINE* LED will light when the Internet link is created and your browser will display the default home page.

4. If *Dial-on-demand/Idle time* is enabled, the SnapGear appliance will also disconnect from the Internet when the connection is idle for the specified period.

Internet access is automatic if you are using a permanent connection device (e.g. cable modem) or if you are using ADSL or an analog modem configured to stay connected.

4. Dial-in server configuration

SnapGear appliance enables remote and secure access to your office network. This chapter shows how to set up the dial-in features.

Your SnapGear appliance can be configured to receive dial-in calls from remote users/sites. Remote users are individual users (e.g. telecommuters) who connect directly from their client workstations to dial into modems connected to the serial ports on the SnapGear appliance. Remote site dial-in connections can be LAN-to-LAN connections, where a router at a remote site establishes a dial-in link using a modem connected to the SnapGear appliance.

The SnapGear appliance's dial-in facility establishes a PPP connection to the remote user or site. Dial-in requests are authenticated by usernames and passwords verified by the SnapGear appliance. Once authenticated, remote users and sites are connected and have the same access to the LAN resources as a local user.

Note

Not all SnapGear appliances support the RAS (Remote Access Server) functions in this section.

The SnapGear appliance Models SOHO+, PRO and PRO+ support up to two dial-in connections. The SnapGear appliance models LITE2, LITE2+, SME530 and SME550 support a single dial-in connection.

To configure the SnapGear appliance for a dial-in connection:

1. Attach external modems to the relevant SnapGear appliance serial ports. Refer to Chapter 7, *Serial Ports and Modem Devices* for modem configuration details.

2. Enable and configure the selected SnapGear appliance COM port for dial-in as detailed in *Dial-in Setup*.

3. Set up and configure user dial-in accounts for each person or site requiring dial-in access.

You can also apply filtering to dial-in connections, as detailed in Chapter 6, *Firewall.*

Dial-in setup

The following figure shows the dial-in setup:

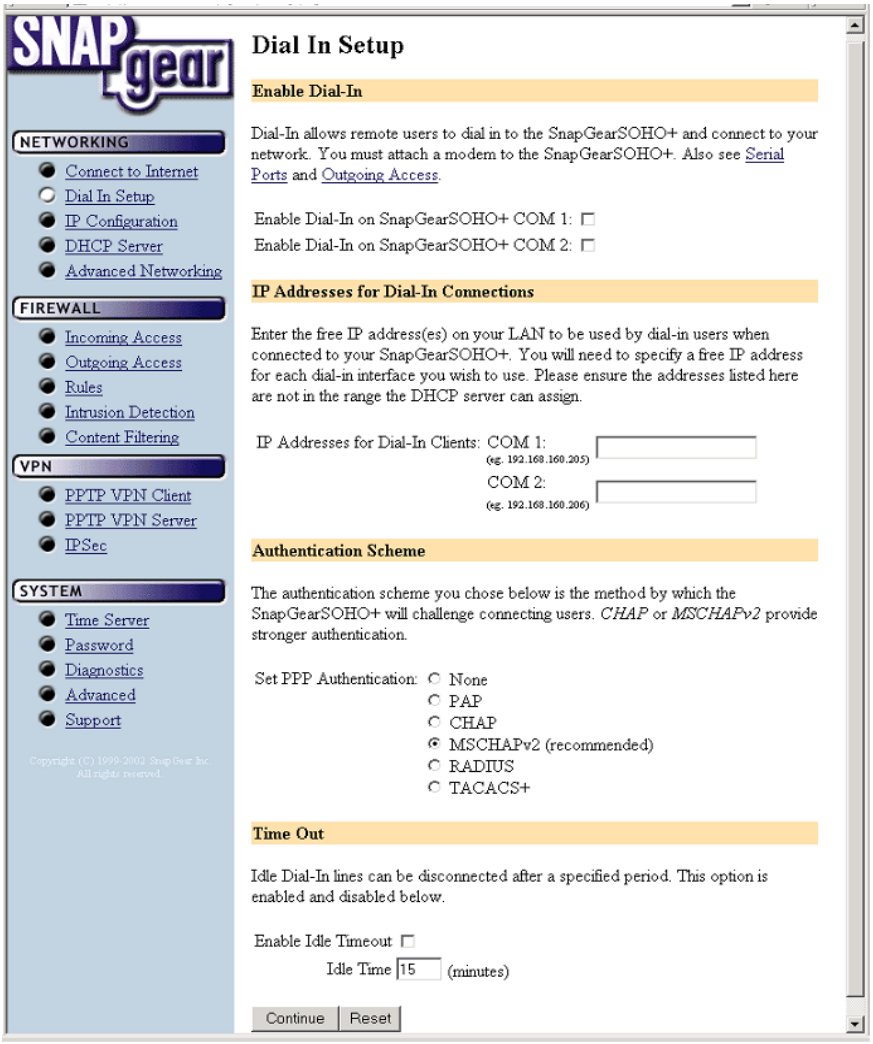


Figure 4.1 Dial-in setup

To enable and configure Dial-In server for the SnapGear appliance, select **Dial-In Setup** from the **Networking** menu. The following table describes the fields in the **Dial-In Setup** screen and explains how to enable and configure dial-in access on a SnapGear appliance COM port.

Field	Description
Enable Dial-in	To enable and configure dial-in, check the relevant COM port box. The selected port is now available for dial-in access. If no COM port is selected, all dial-in attempts will be blocked. The current dial-in status of all COM ports is displayed. If dial-in is already enabled, the checkbox displays a bold or shaded check mark. If dial-in is not enabled, the checkbox is clear Note: A port enabled for dial-in cannot be used simultaneously for dial-out activities (e.g. dial-on-demand Internet connection). If a port was previously set up for Internet access and is later enabled for dial-in, the Internet access function is disabled.
IP Addresses for Dial-in users	Dial-in users must be assigned local IP addresses to access the local network. Specify a free IP address from your local network that each dial-up client will use when connecting to the SnapGear appliance.
Authentication Scheme	The authentication scheme is the method the SnapGear appliance uses to challenge users dialing into the network. Dial-in clients must be configured to use the selected authentication scheme which may be one of: • *MSCHAPv2* is the most secure. • *CHAP* is less secure, and *PAP* (although more common) is even less secure. If you select **None**, no username/password authentication is done on dial-in. • *RADIUS* and *TACACS+* use a remote authentication server on the local network. When selected, you must enter the IP address of a server setup to use this scheme.
Idle Timeout	If a dial-in connection remains inactive, it can be automatically disconnected after a specified time period. Selecting **Enable idle timeout** will disconnect idle connections after 5 minutes. **Idle time** can be set between 0 – 99 minutes.

After enabling and configuring the selected SnapGear appliance COM ports to support dial-in, click **Continue** to create and configure the dial-in user accounts.

Dial-in user accounts

User accounts must be set up before remote users can dial-into the SnapGear appliance. The following figure shows the Dial-in user account creation:

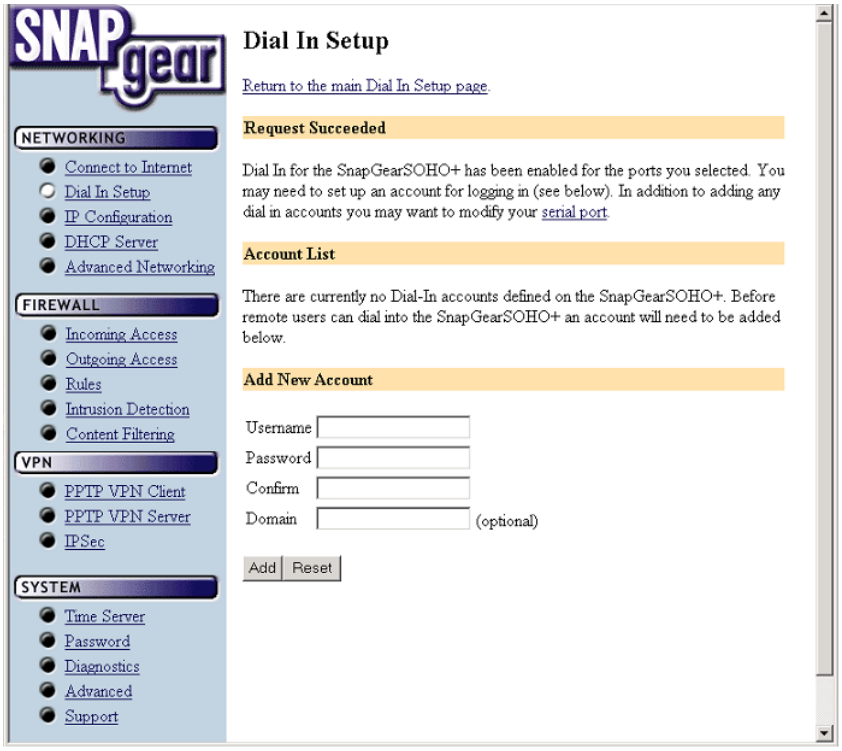


Figure 4.2 Dial-in user account creation

The field options in *Add New Account* are shown in the following table:

Field	Description
Username	Username for dial-in authentication only. The name is case-sensitive (e.g. *Jimsmith* is different to *jimsmith*).
Password	Password for the remote dial-in user.
Confirm	Re-enter the password to confirm.
Domain	If your network has a Windows NT server, you can attach a domain name to your dial-in remote user accounts. This field is optional and can be left blank.

The following figure shows the user maintenance screen:

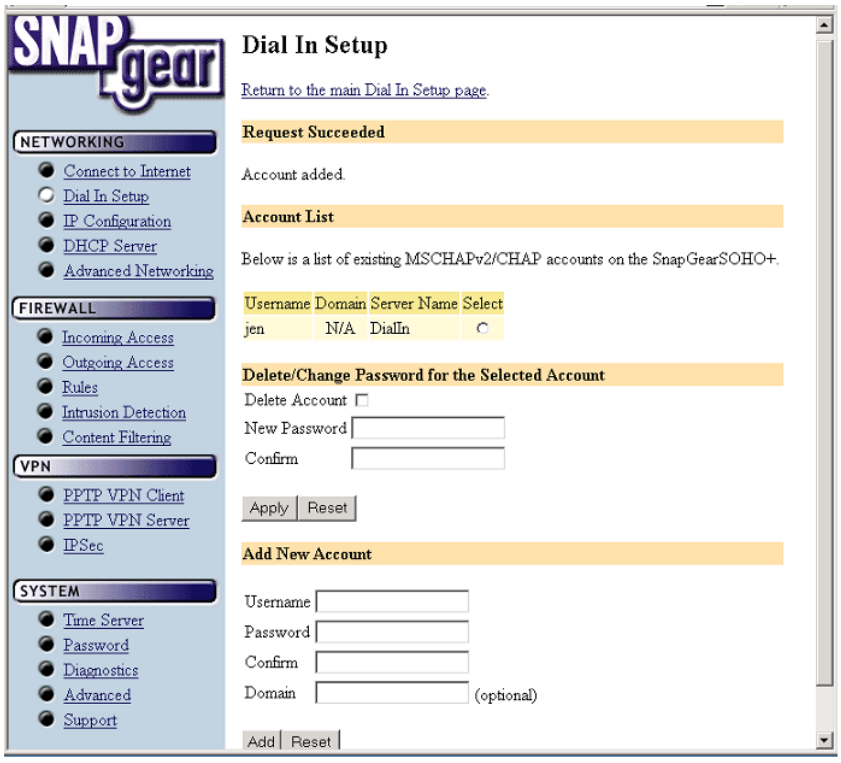


Figure 4.3 User maintenance screen

Account list

As new dial-in user accounts are added, they are displayed on the updated Account List. To modify a password for an existing account, select the account in the Account List and enter the new password in the **New Password** and **Confirm** fields. Click **Apply** under the **Delete or Change Password for the Selected Account** heading, or click **Reset** if you make a mistake.

To delete an existing account, select the account in the **Account List** and check **Delete** under the **Delete or Change Password for the Selected Account** heading. If changes to the user account are successful, the change is shown on the **Dial-in Setup** screen . If the change is unsuccessful, an error is reported as shown in the following figure:

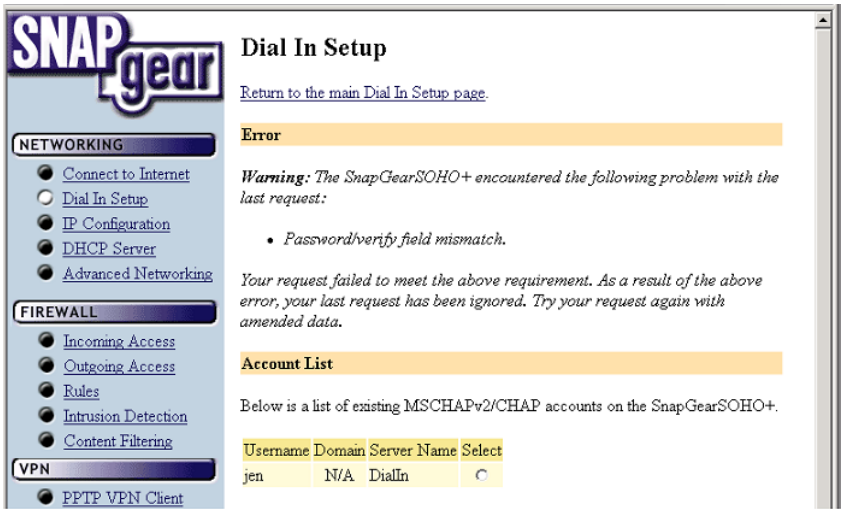


Figure 4.4 Dial-in password error

When you have finished adding and modifying user account details, you can configure other SnapGear appliance functions by selecting the appropriate item from the **Network** or **System** menus. You can also apply packet filtering to the dial-in service as detailed in Chapter 6, *Firewall*.

Warning

If you have enabled a SnapGear appliance COM port for dial-in, this port cannot be used simultaneously for dial-out activities (e.g. dial-on-demand Internet connection). If a port is set-up for Internet access, and is later enabled for dial-in, the Internet access function is automatically disabled.

Remote user configuration

Remote users can dial-in using the SnapGear appliance using the standard Windows **Dial-Up Networking** software. Set up a new dial-out connection on the remote PC to dial the phone number of the modem connected to the SnapGear appliance COM port. After the dial-in is connected, users can access all network resources as if they were a local user.

For Windows 95 and Windows 98:

From the **Dial-Up Networking** folder, double-click **Make New Connection** and enter the ***Connection Name*** for your new dial-in connection as shown in the following figure:

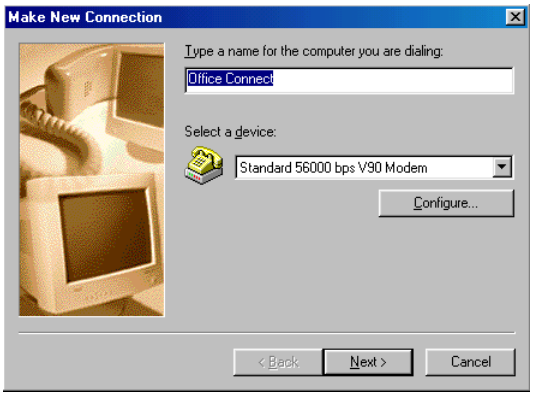


Figure 4.5 Make new connection screen

Select the modem to use from the **Select a device** pull down menu.

Click **Next** and enter the phone number of the modem connected to the SnapGear appliance.

Click **Finish**.

An icon is displayed in Dial-Up Networking with your Connection Name. Right click the icon once, and then click **File** and **Properties** and click the **Server Types** tab as shown in the following figure:

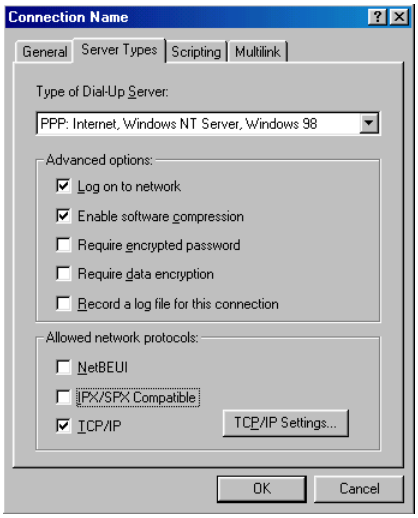


Figure 4.6 Server types

Check the **Log on to network** and **Enable software compression** checkboxes. If your SnapGear appliance dial-in server requires *MSCHAP-2* authentication, you also need to check the **Require encrypted password** checkbox. Leave all other **Advanced Options** unchecked.

Select the **TCP/IP** network protocols from the **Allowed network protocols** list.

Warning

Do not select NetBEUI or IPX. If an unsupported protocol is selected, an error message is returned when attempting to connect.

Click **TCP/IP Settings** and confirm that the **Server Assigned IP Address**, **Server Assigned Name**, **Server Address**, **Use IP Header Compression** and **Use Default Gateway on Remote Network** are all checked and click **OK**.

Dial-in and log on to the remote SnapGear appliance by double-clicking the *Connection Name* icon. You need to enter the **Username** and the **Password** that was set up for the SnapGear appliance dial-in account as shown in the following figure:

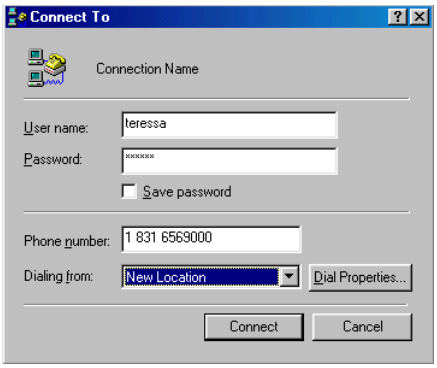


Figure 4.7 Connect to dialogue box

Windows 2000

To configure a remote access connection on a Windows 2000 computer, click **Start**, **Settings**, **Network and Dial-up Connections** and select **Make New Connection.**

The network connection wizard will guide you through setting up a remote access connection:

Figure 4.8 Network connection wizard

Click **Next** to continue.

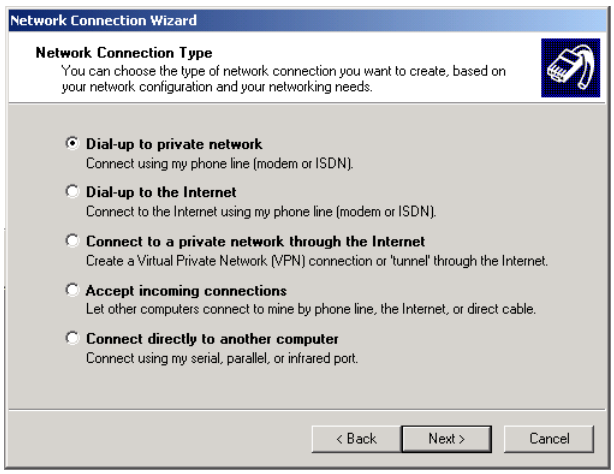


Figure 4.9 Connection type

Select **Dial-up to private network** as the connection type and click **Next** to continue.

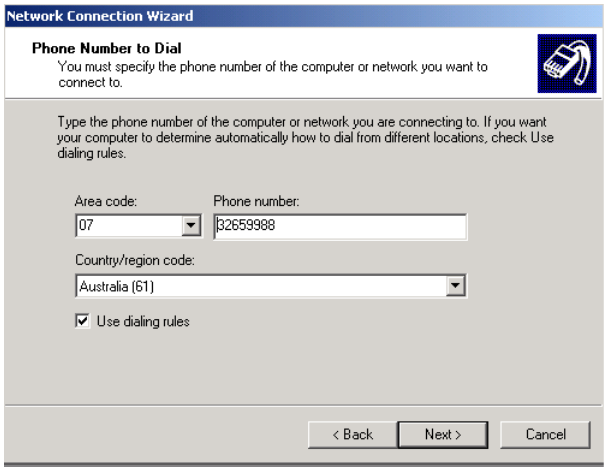


Figure 4.10 Phone number to dial

Tick **Use dialing rules** to enable you to select a country code and area code. This feature is useful when using remote access in another area code or overseas.

Click **Next** to continue.

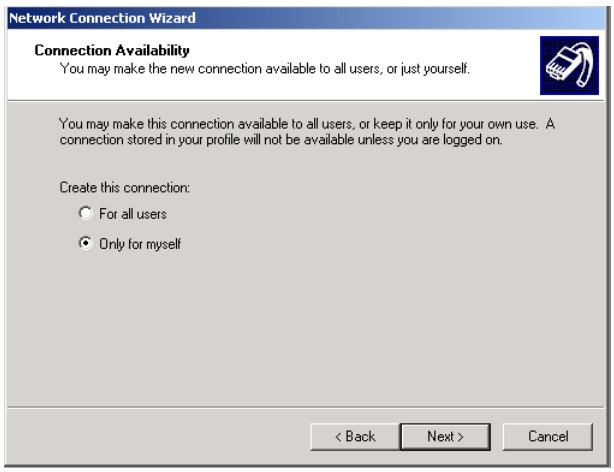


Figure 4.11 Connection availability

Select the option **Only for myself** to make the connection only available for you. This is a security feature that will not allow any other users who log onto your machine to use this remote access connection:

Figure 4.12 Connection name

Enter a name for the connection and click **Finish** to complete the configuration. By ticking **Add a shortcut to my desktop,** an icon for the remote connection will appear on the desktop.

To launch the new connection, double-click on the new icon on the desktop, and the remote access login screen will appear as in the next figure. If you did not create a desktop icon, click **Start, Settings, Network and Dial-up Connections** and select the appropriate connection and enter the username and password set up for the SnapGear appliance dial-in account.

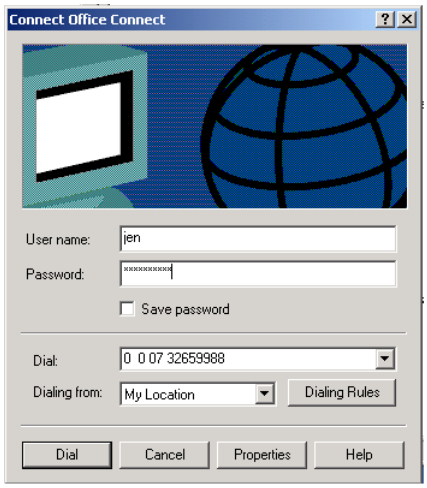


Figure 4.13 Remote access login screen

5. Network configuration

IP configuration

Users can set the IP address configuration for both the LAN and Internet interfaces by selecting **IP Configuration** from the **Networking** menu as shown in the following figure:

Figure 5.1 IP configuration

To configure the LAN Interface of the SnapGear appliance, select either a dynamically or statically assigned IP address. If the LAN interface of your SnapGear appliance gets its IP address from a DHCP server on your local network, then check **DHCP assigned**.

For a static IP address on the LAN interface, enter the **IP Address** and **Netmask** in the fields provided. You must enter a static IP address if the SnapGear appliance will act as the DHCP server on your local network.

If your SnapGear appliance is configured for a **Direct Connection** to the Internet, you must also set the IP address for the Internet Interface. Check **DHCP assigned** if the IP address of the Internet Interface is set via a DHCP server, or enter the **IP Address** and **Netmask** if you have a static address for the Internet interface.

Enter the IP address of default gateway in the **Internet Gateway** field. The SnapGear appliance will send all packets not destined for the local network to this machine.

Enter the IP address of the DNS Server that the SnapGear appliance will use to resolve domain names in the **Domain Name Server** field. This is only required if the SnapGear appliance is configured with a static IP address on the Internet interface and does not automatically get its DNS server address.

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

Advanced IP configuration

The following figure shows the advanced IP configuration:

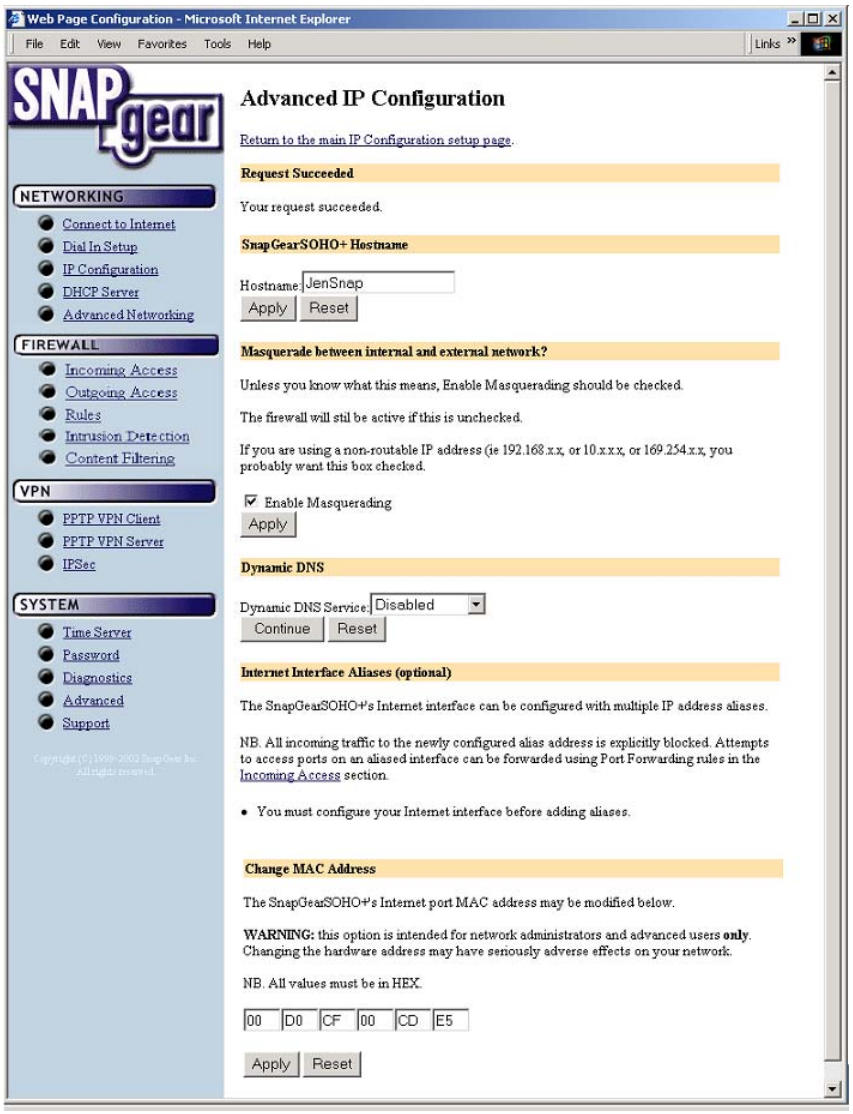


Figure 5.2 Advanced IP configuration

The **Hostname** is a descriptive name for the SnapGear appliance on the network.

The SnapGear appliance can utilize IP **Masquerading** (a simple form of Network Address Translation, or NAT) where users on the local network effectively share a single external IP address. Masquerading allows insiders to get out, without allowing outsiders in. By default, the Internet interface is setup to Masquerade.

Masquerading has the following advantages:

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

SnapGear recommends setting **Masquerade** on the Internet interface.

Internet Interface Aliases allows the SnapGear appliance to respond to multiple IP addresses on the Internet interface. You must also setup appropriate **Incoming Access** rules to allow traffic sent to the additional (i.e. aliased) IP addresses to be passed to the local network.

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

DHCP server

The following figure shows the DHCP server configuration:

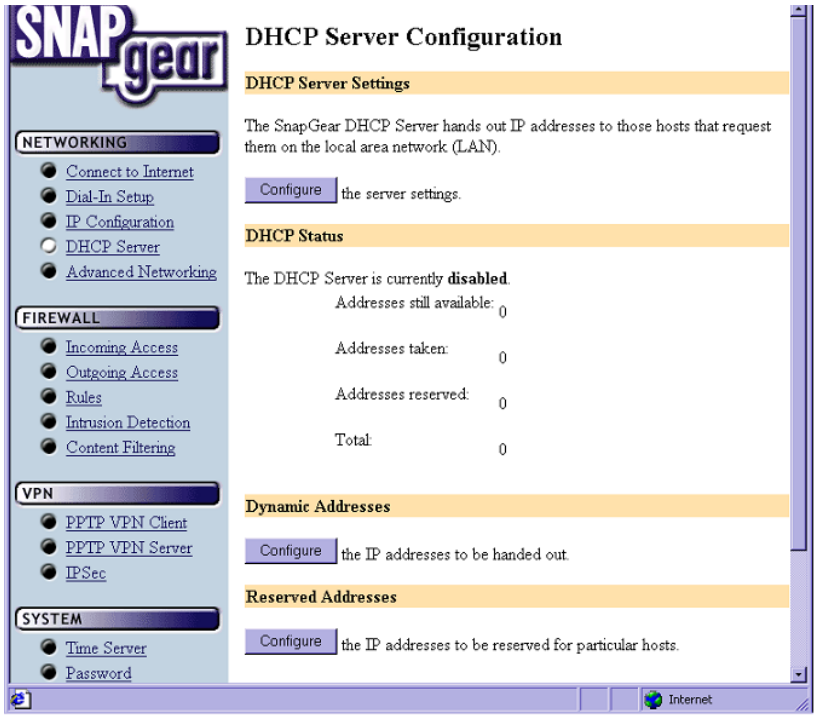


Figure 5.3 DHCP server configuration

To help keep your network design as simple as possible, your SnapGear appliance can act as a DHCP server for machines on your local network. To configure your SnapGear appliance as a DHCP server, you must set a static IP address and netmask on the LAN Interface (see the section called *IP configuration*).

Click **Configure the server settings** on the **DHCP Server Configuration** screen to:

- Check the **Enable DHCP server** checkbox.
- Enter the **Gateway Address** to be distributed to DHCP clients. This is normally the IP address of the LAN interface of the SnapGear appliance.
- Enter the **DNS Address** to be distributed to DHCP clients. Leave this field blank for automatic DNS server assignment. If your SnapGear appliance is configured for DNS masquerading, you should either leave this field blank, or enter the IP address of the LAN interface of the SnapGear appliance.
- Enter IP address of the WINS server to be distributed to DHCP clients in the **WINS Address** field.
- Enter the **Default Lease Time** and **Maximum Lease Time** in seconds. The lease time is the time that a dynamically assigned IP address is valid.
- Click **Configure the IP addresses to be handed out** to enter the addresses from where the DHCP server will allocate IP addresses to machines on the local network.

To reserve a particular IP address for a specific machine click **Configure the IP addresses to be reserved for particular hosts.** For each reserved IP address, you must enter the **Hostname and MAC Address** of the machine as well as the **IP Address** that will be allocated to the machine.

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

Advanced networking

Users can perform the following diagnostic tasks on the **Advanced Networking** screen:

- Perform a Ping Test.
- Perform a Trace Route Test (not available on LITE and LITE+ due to memory constraints).
- View the Interface Configuration.
- View the Kernel Route Table.

The advanced networking configuration tasks **Traffic Shaping** and **Additional Routes** are also accessed using the **Advanced Networking** page.

Traffic shaping

The **Traffic Shaping** feature of your SnapGear appliance allows you to allocate **High, Medium,** or **Low** priority to the following services: domain (tcp), domain (udp), ftp, ftp-data, http, https, imap, irc, nntp, ntp, pop3, smtp, ssh, and telnet.

Traffic Shaping provides a level of control over the relative performance of various types of IP traffic. This advanced feature is provided for expert users to fine tune their networks.

Additional routes

The **Additional routes** feature allows expert users to add additional static routes for the SnapGear appliance. These routes are additional to those created automatically by the SnapGear appliance configuration scripts.

6. Firewall

The SnapGear appliance has a fully featured, stateful firewall. The firewall allows you to control both incoming and outgoing access and to detect intrusion attempts, so that PCs on the office network can have tailored Internet access facilities and be shielded from malicious attacks.

The SnapGear Firewall filters packets at the network layer, determines whether the session packets are legitimate and evaluates the contents of packets at the application layer to provide maximum protection for your private network.

Incoming access

Click **Incoming Access** on the **Firewall** menu to show the **Incoming Access** configuration page to configure the firewall to:

- Control external access to services provided by the SnapGear appliance itself
- Control services provided by machines on your local network.

Incoming access – administration services

The following figure shows the incoming access configuration page:

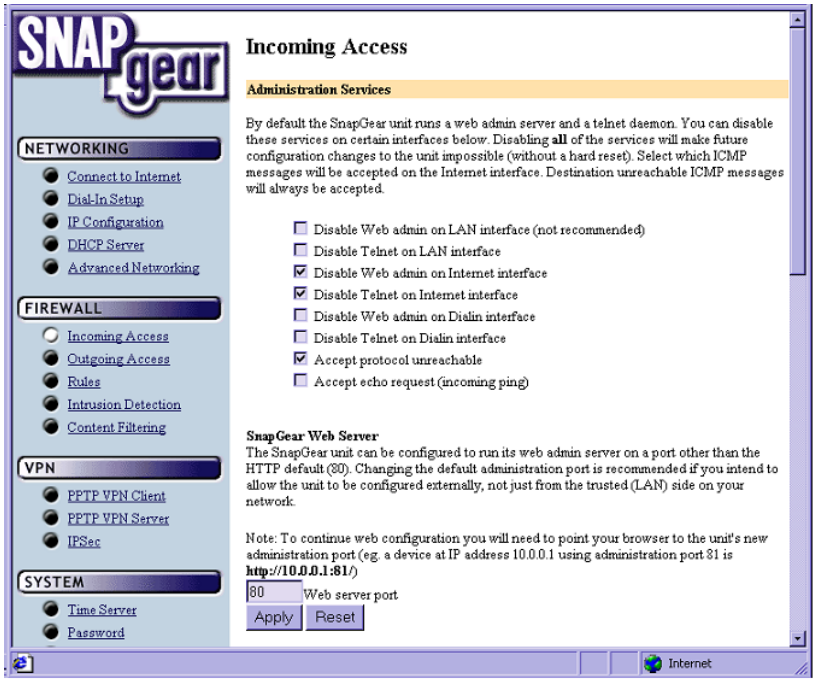


Figure 6.1 Incoming access configuration

By default the SnapGear appliance runs a web administration server and a telnet service. Access to these services can be restricted to specific interfaces. For example, you may want to restrict access to the SnapGear appliance's configuration web pages (**Web Admin)** to machines on your local network. SnapGear does not recommend disallowing all services, as this will make future configuration changes impossible unless your SnapGear appliance is reset to the factory default settings.

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

The SnapGear appliance's Web Admin pages are usually accessed on the default HTTP port (i.e. port 80). Change the port number if you are allowing Internet access to the web administration page. This will hide your web administration pages from casual web surfers who finds your SnapGear appliance on the Internet. After changing the web server port number, you must include the new port number in the URL to access the pages. For example, if you change the web administration to port number 88, the URL to access the web administration will be similar to http://192.168.22.1:88.

External access to services

The following figure shows how to configure external access to services:

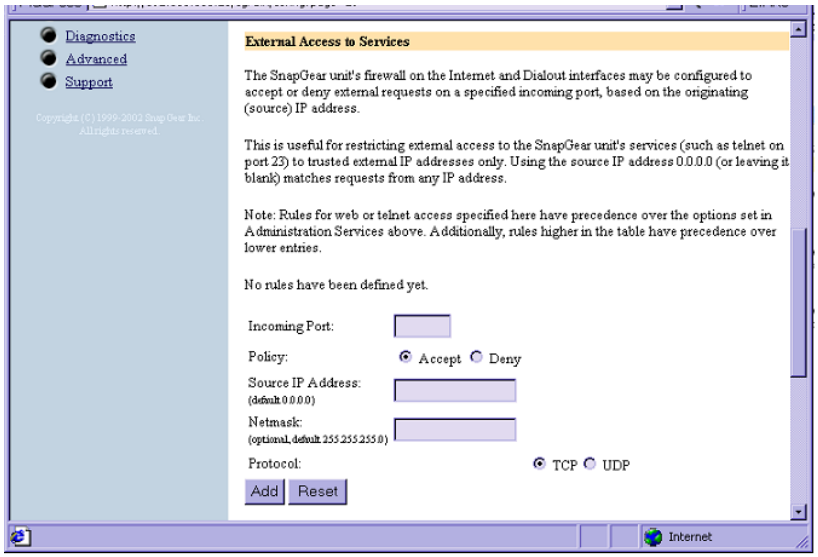


Figure 6.2 Configure external access to services

The SnapGear appliance firewall on the Internet interface can be configured to accept or deny external requests on a specified incoming port, based on the originating (i.e. source) IP address.

This is useful for restricting external access to the SnapGear appliance's services (e.g. telnet on port 23) to trusted external IP addresses only. The options specified in the **Administration Services** section for disabling web or telnet access on the Internet interface have lower priority than any rules you specify for web or telnet access in this section.

Port forwarding

The following figure shows the port forwarding configuration:

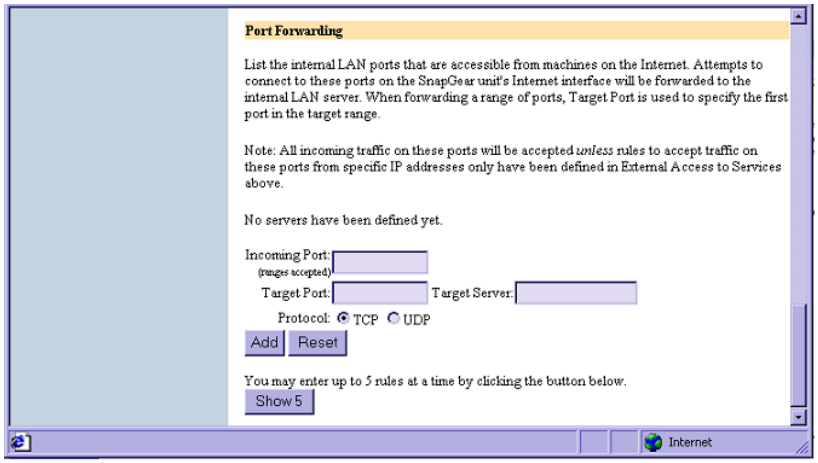


Figure 6.3 Port forwarding configuration

Port forwarding allows the SnapGear appliance to control access to services provided by machines on your private network from users on the Internet. Requests coming into the SnapGear appliance on the specified **Incoming Port(s)** are forwarded to the **Target Port** on the **Target Server**.

Outgoing access

Your SnapGear appliance can be configured to restrict network traffic going out the Internet interface. These restrictions can be applied to specific hosts or networks (defined by IP address), or globally across all hosts on your internal LAN.

Outgoing Access restrictions are applied by denying a group of services (e.g. web and email) from specific hosts or networks or globally across all hosts.

Your SnapGear appliance's Outgoing Access Restrictions are configured using security group classes. Click the **security group classes** link on the **Outgoing Access Configuration** page to set the restrictions for each security group class. Each security group class can be configured to restrict certain TCP/IP application protocols or to block specified TCP and UDP ports as shown in the following figure:

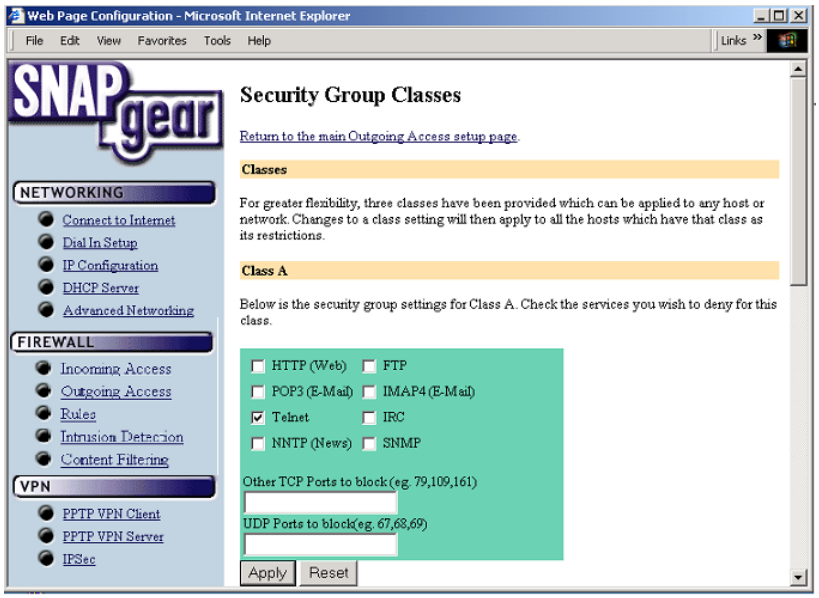


Figure 6.4 Security group classes configuration

You can specify the restrictions for each security group class to impose, and apply the restrictions globally to all machines on your local network or to specific machines or networks.

Use the **Add Hosts** *or* **Networks** section to specify the specific machines or networks to restrict outgoing access as shown in the following figure:

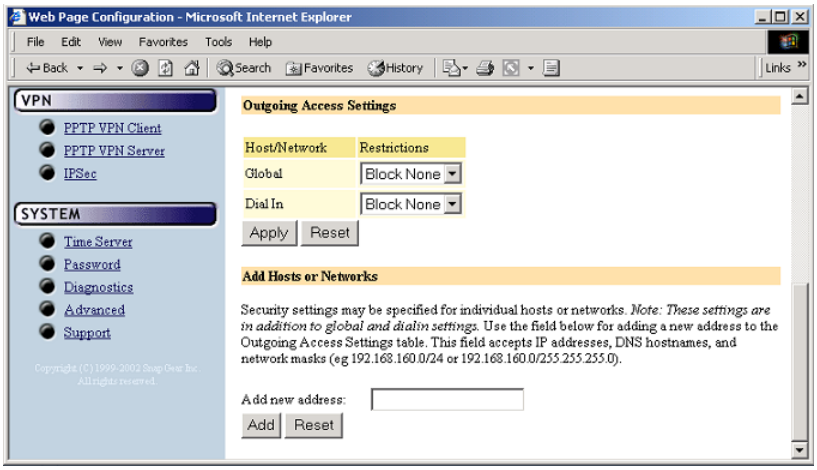


Figure 6.5 Outgoing access settings

Firewall rules

The **Firewall Rules** configuration page allows firewall experts to view the current firewall rules and add custom firewall rules.

To access this page, click **Rules** in the **Firewall** menu. Only experts on firewalls and **iptables** rules will be able to add effective custom firewall rules. Configuring the SnapGear firewall via the **Incoming Access** and **Outgoing Access** configuration pages is adequate for most applications.

Intrusion detection and blocking

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

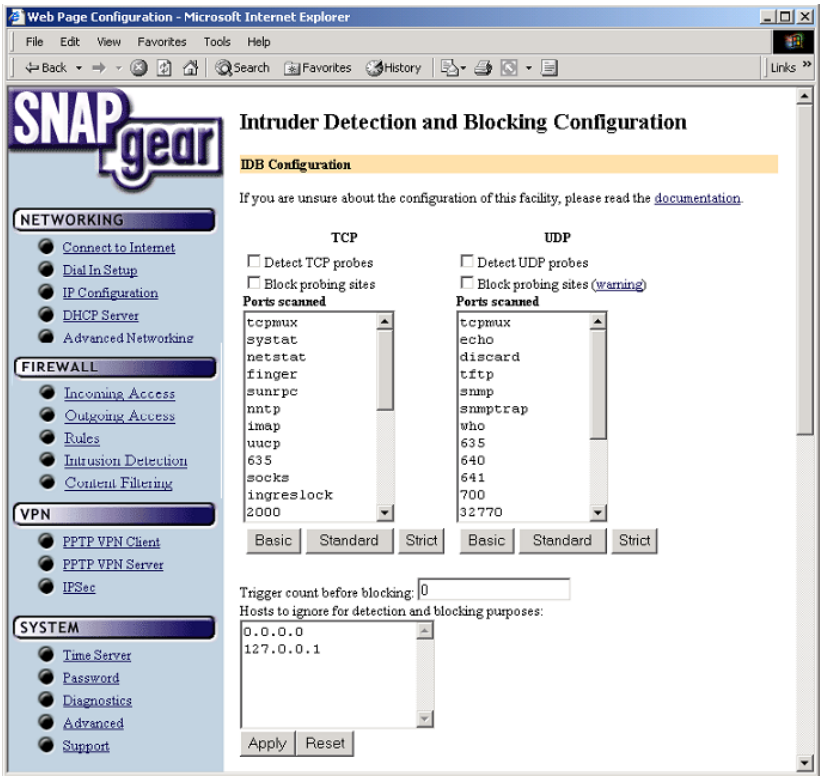


Figure 6.6 Intrusion detection and blocking configuration

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

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

The list of monitored network ports can be freely edited. Several shortcut buttons also provide pre-selected lists of services to monitor. The **basic** button installs a bare bones selection of ports to monitor while still providing sufficient coverage to detect many intruder scans. The **standard** option extends this coverage by introducing additional monitored ports for early detection of intruder scans. The **strict** button installs a comprehensive selection of ports to monitor and should be sufficient to detect most scans.

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

The ignore list contains a list of host IP addresses which the IDB will ignore for detection and blocking purposes. This list may be freely edited so trusted servers and hosts are not blocked. The two addresses **0.0.0.0** and **127.0.0.1** cannot be removed from the ignore list because they represent the IDB host.

Warning

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

Content filtering

The SnapGear Content Filtering system limits the types of web-based content accessed. Web-based content featuring profanity, sexually explicit or other objectionable material can be limited or blocked from the following screens. The following figure shows content filtering:

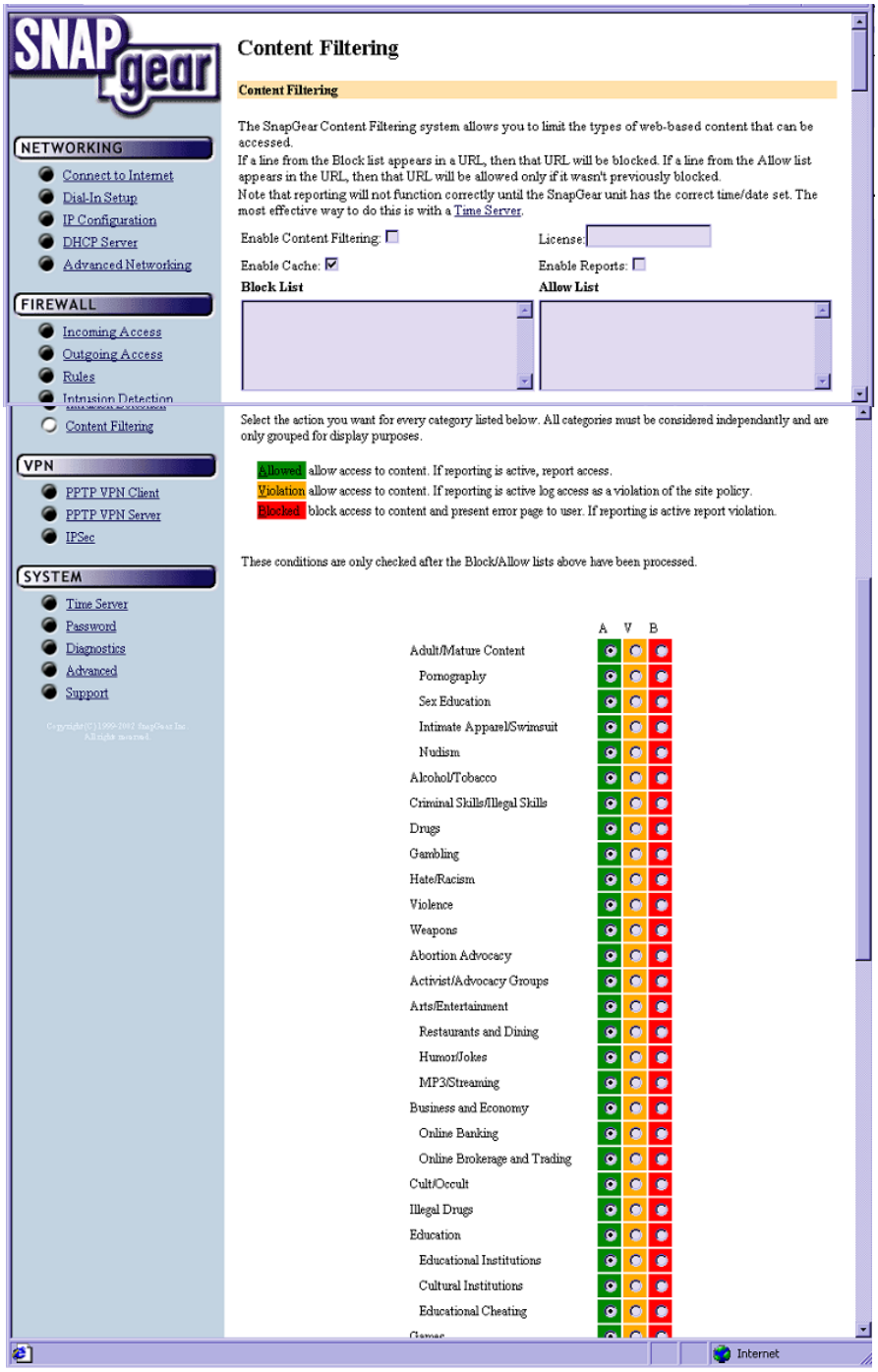


Figure 6.7 Content filtering

In the **Block List**, specify text that will block access to any URL containing that text. For example, if access to websites containing references to “widgets” is a violation, entering that text will block any URL containing “widgets” including http://www.widgets.example.com or www.test.com/widgets/index.html.

Warning

This list only refers to the URL; it will not search and block on content.

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

Filtering levels and reporting

The SnapGear **Content Filtering** screen allows you to select filtering levels based on green, yellow, and red color codes. You can select from some commonly blocked content and set the filtering levels according to your requirements.

Reporting contains the following filtering levels:

Filtering Level	Description
Green (Allowed)	Access to content is allowed. If reporting is active, report the access.
Yellow (Violation)	Access to content is allowed. If reporting is active, log the access as a violation of the site policy.
Red (Blocked)	Access to content is blocked. Show the error page to the user. If reporting is active, log the access as a violation.

An activity report is available by ticking the **Enable Reports** box.

Warning

The correct time/date must be set on your SnapGear appliance for Reporting to work. The most effective way to do this is by using a time server.

The filtering and reporting can only be activated after visiting the **Registration** page.

7. Virtual Private Networking

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

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

Using VPN, you can access the office network securely across the Internet using Point-to-Point Tunneling Protocol (PPTP) or IPSec. If you take your portable computer on a business trip, you can dial a local number to connect to your Internet access provider and then create a second connection (called a "tunnel") into your office network across the Internet and have the same access to your corporate network as if you were connected directly from your office. Similarly, telecommuters can also set up a VPN tunnel over their cable modem or DSL links to their local ISP.

With the SnapGear appliance you can establish a secure VPN over the Internet using either PPTP or IPSec. IPSec provides better security; however PPTP is the preferred protocol for integrating with existing Microsoft infrastructure. The SnapGear appliance provides a PPTP server to enable remote Windows clients to securely access your office network. Using the SnapGear appliance's PPTP client or IPSec you can also connect your office network to one or more remote networks.

This chapter explains how to configure the PPTP server and client, as well as IPSec, in your SnapGear appliance and how to set up remote clients to connect to your VPN tunnel as shown in the following figure:

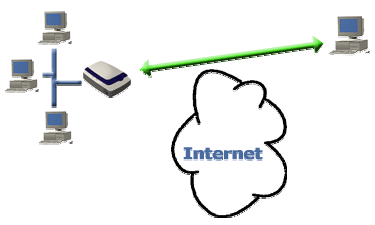


Figure 7.1VPN tunneling using the PPTP server

PPTP client setup

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

To set up a SnapGear PPTP VPN Client, select **PPTP VPN Client** from the **VPN** menu and create a new VPN connection by entering:

- A descriptive **name** for the VPN connection. This may describe the purpose for the connection.
- The remote PPTP **server IP address** to connect to.
- A **username** and **password** to use when logging in to the remote VPN. You may need to obtain this information from the system administrator of the remote PPTP server and,
- Optionally, the remote network's **netmask**. This is used to determine which packets should go the remote network.
- Click **Add**.

Warning

If you are using Windows 98, you must ensure that Dial Up Networking has been upgraded to version 1.4 otherwise you will be unable to use MS-CHAPv2 authentication (the recommended method).

If the remote VPN is already up and running, check **Start Now** to establish the connection immediately as shown in the following figure:

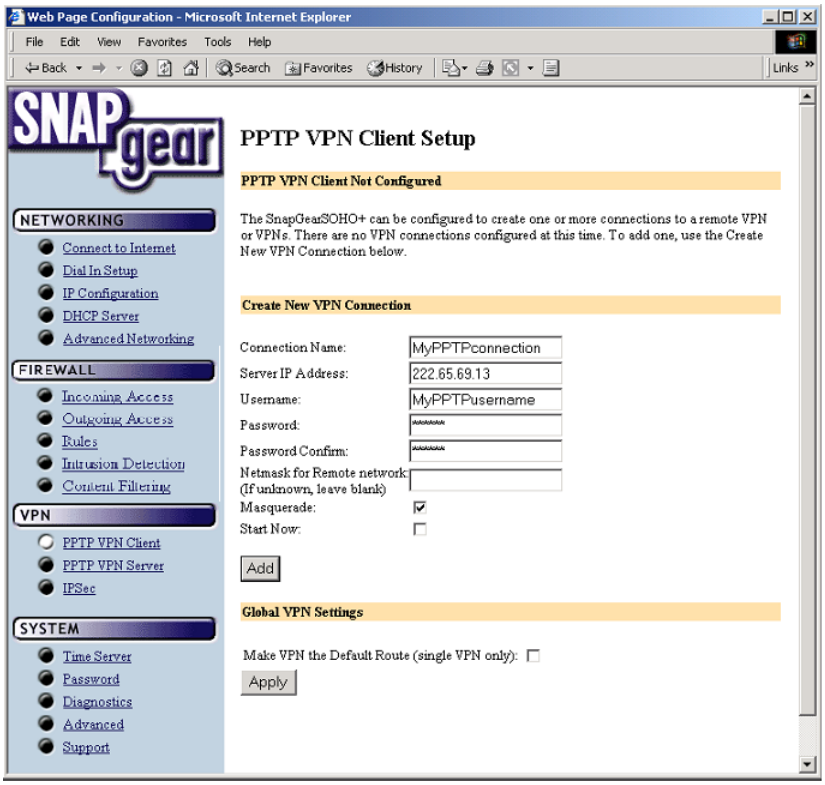


Figure 7.2 PPTP client configuration

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

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

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

PPTP server setup

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

To setup a VPN connection:

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

The following sections provide additional detailed instructions.

Enable and configure the PPTP VPN server

The following figure shows the PPTP server setup:

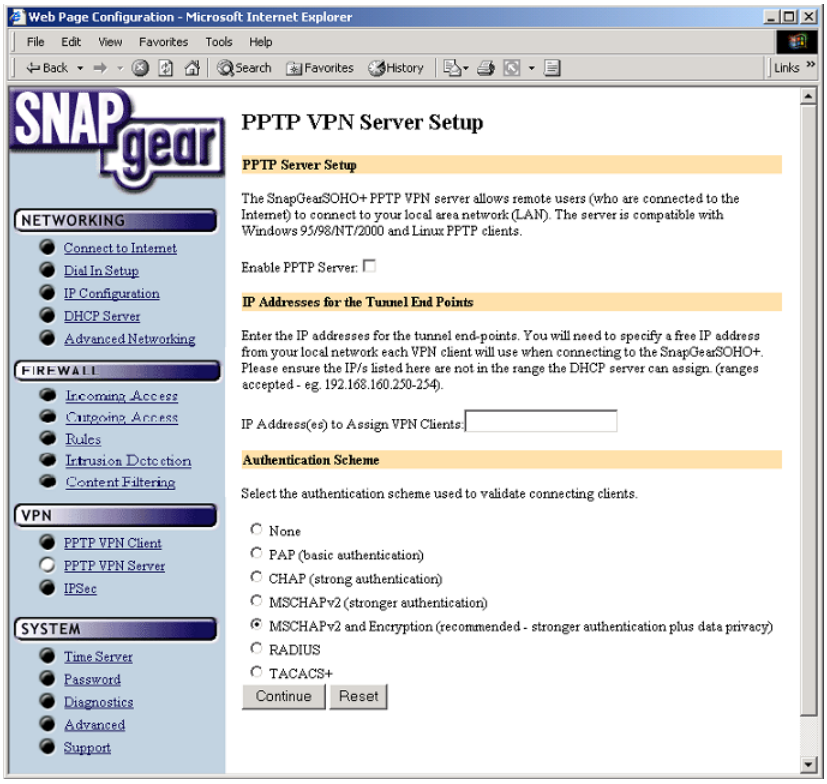


Figure 7.3 PPTP server setup

To enable and configure your SnapGear appliance's VPN server, select **PPTP VPN Server** from the **VPN** menu in the **SnapGear appliance Config Pages**.

The following table describes the fields in the VPN Setup screen and the options available when enabling and configuring VPN access.

Field	Description
Enable PPTP Server	Check this box to enable PPTP connections to be established to your SnapGear appliance.
IP Addresses for the Tunnel End Points	Enter the IP addresses for the tunnel end-points. You need to specify a free IP address on your local network that each VPN client will use when connecting to the SnapGear appliance. Please ensure that the IP addresses listed here are not in the range the DHCP server can assign. Ranges are accepted; for example 192.168.160.250-254.
Authentication scheme	PPTP provides an authenticated communication tunnel between a client and a gateway by using a user ID and password. The authentication scheme is the method the SnapGear appliance uses to challenge users wanting to establish a PPTP connection to the network. The remote client must be set up to use the selected authentication scheme. • *MSCHAPv2* is the most secure. It uses encrypted passwords. SnapGear recommends the use of MSCHAPv2 plus data encryption as this keeps your data private as well as providing secure authentication. • *CHAP* is less secure, and similarly *PAP* is even less secure, but more common. • *RADIUS* and *TACACS+* make use of a remote authentication server on the local network. You must enter the IP address of a server setup to use this scheme.

Configuring user accounts for VPN server

After setting up the VPN server, select **Continue** and to show the *PPTP VPN Server Accounts* screen as shown in the following figure:

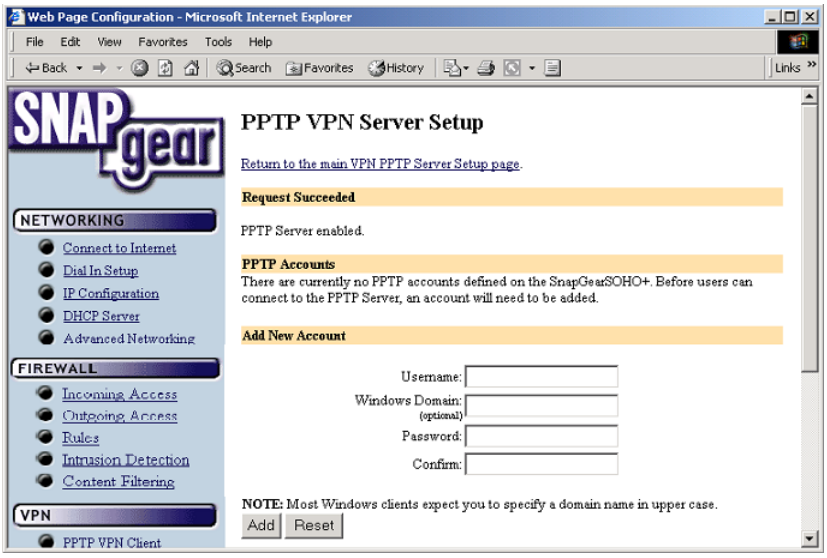


Figure 7.4PPTP VPN server accounts screen

Before remote users can set up a VPN tunnel to the SnapGear appliance PPTP server, they must have a user accounts set up. The field options in the **Add New Account** are detailed in the following table.

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

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

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

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

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

Configuring the remote VPN client

After setting up the SnapGear PPTP VPN server, the remote VPN clients can be configured to securely access the local network. You need to enter the VPN client username and password that your remote users will use to access the SnapGear PPTP VPN from the remote site.

The names may or may not be the same as your normal network username and password, and should be different from the username and password used by your remote users use to access their local ISP.

The following figure shows the VPN PPTP IP address:

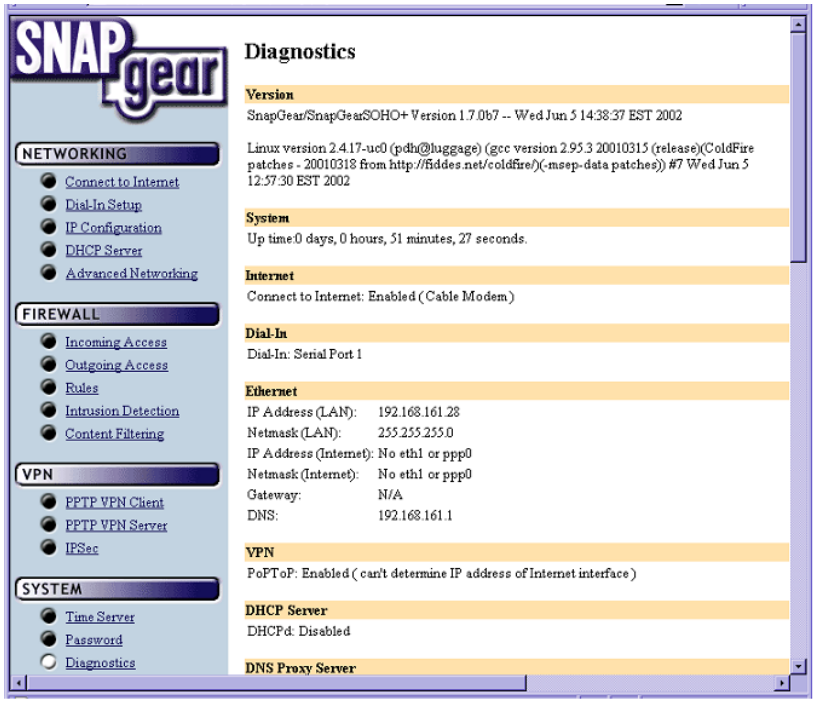


Figure 7.5 VPN PPTP IP address

Obtain the current IP address of the SnapGear appliance PPTP server. This address may change if your office network has an external DHCP server (i.e. your ISP dynamically assigns your an IP address).

To determine the current SnapGear appliance's PPTP server IP address, select **Diagnostics** from the **System** menu in the main menu bar. The IP address is displayed in the **VPN** field. Your remote users must know this **PPTP IP address** to setup a VPN tunnel to the SnapGear appliance.

Check that the remote PC has a modem installed and that you have a local ISP account, (i.e. an ISP phone number and a username and password to log in to the ISP). Although users are often connected to the Internet using a dial-out modem, VPN connection can also be set up using a cable modem, ADSL, ISDN or other Internet link.

Ensure that both the VPN and Dial Up Networking (DUN) software is installed on the remote PC. If necessary, install the *Microsoft DUN update* (available on the SnapGear Installation CD) and *VPN Client update.*

To create a VPN connection across the Internet, you must set up two networking connections. One connection is for the Internet access provider, and the other connection is for the VPN tunnel to your office network. Verify that a networking connection is established for the link to your local ISP.

Set up a new connection for the VPN connection. Your SnapGear appliance's PPTP server will operate with the standard Windows PPTP clients in all versions of Windows.

The following sections provide details for client setup in Windows 95/98, Windows NT, and Windows 2000. Setup instructions for Windows ME and Windows XP can be deduced from this information and the Microsoft Windows documentation.

Windows 95 and Windows 98

From the Dial-Up Networking folder, double-click **Make New Connection**. Type **SnapGear appliance** or a similar descriptive name for your new VPN connection.

From the **Select a device** drop-down menu, select the **Microsoft VPN Adapter** and click **Next**. Enter the PPTP IP address of the SnapGear appliance VPN server in the **VPN Server** field. This may change if your ISP uses dynamic IP assignment. Click **OK** and then click **Finish**.

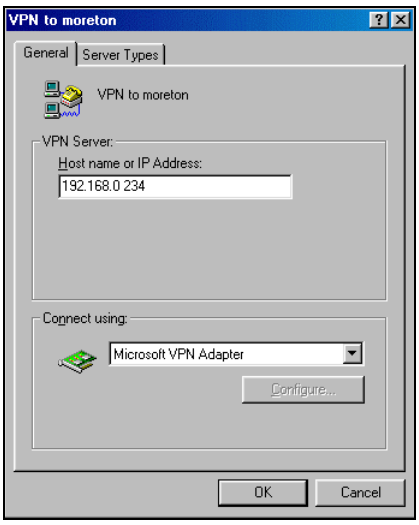


Figure 7.6 VPN client setup

Right-click the new icon and select **Properties**.

Select the **Server Types** tab and check the **Log on to network**, **Enable software compression**, and **Require encrypted password** checkboxes. Leave the other ***Advanced Options*** unchecked.

Select the **TCP/IP** network protocols from the **Allowed network protocols** list.

Warning

Do not select NetBEUI or IPX. If an unsupported protocol is selected, an error message is returned.

Click ***TCP/IP Settings***. Confirm that the **Server Assigned IP Address**, **Server Assigned Name Server Address**, **Use IP Header Compression** and **Use Default Gateway on Remote Network** are all selected and click **OK**.

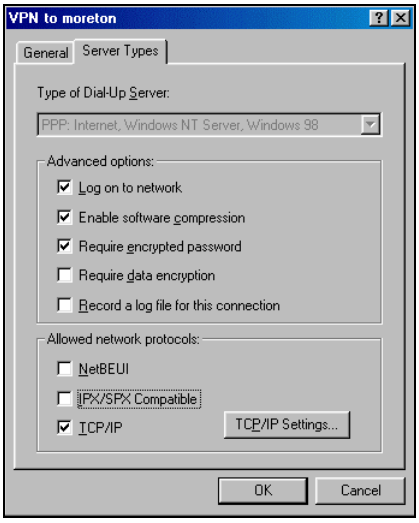


Figure 7.7 VPN client server settings

Your VPN client is now set up correctly.

Windows NT

From the **Dial-Up Networking** dialog, click **New** and select the **Basic** tab.

In the **Entry name** field, enter **SnapGear appliance** or a similar descriptive name and click **Next**.

Enter the SnapGear appliance's *PPTP IP address* into the **Phone Number** field.

Warning

Note that this IP address may change if your ISP uses dynamic IP assignment.

In the **Dial Using** dialog box, select **RASSPPTPM (VPN1)** and click **Next**.

Click **More** and select **Edit entry** then **Modem properties** from the menu.

Select the **Server** tab.

Select **TCP/IP** only.

Warning

Do not select NetBEUI or IPX. If an unsupported protocol is selected, an error message is returned.

Select the **Security** tab and select **Accept only Microsoft encrypted authentication**. Click **OK**.

Your VPN client is now set up correctly.

Windows 2000

To set up VPN access, first setup a Dial Up Networking account to access the Internet. Once you have done this, you are ready to begin.

The first thing you need to do is log in as Administrator on your PC. After logging in, from the **Start** menu, select **Settings** and then **Network and Dial-up Connections** as shown in the following figure:

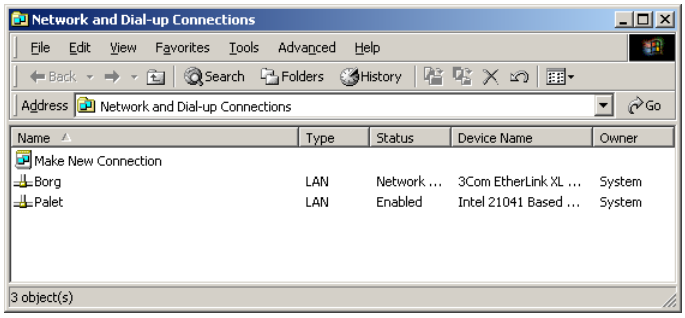


Figure 7.8 Network and dial-up connections

To set up your VPN account, double-click **Make New Connection** and then click **Next** to show the **Network Connection Type** window:

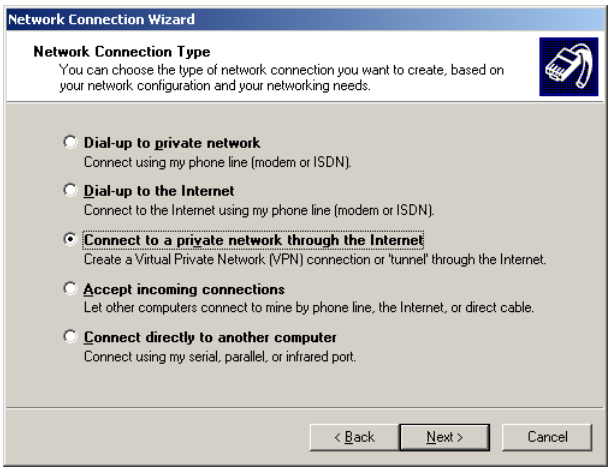


Figure 7.9 Network connection type

Select **Connect to a private network through the Internet** and click **Next**.

This displays the **Destination Address** window:

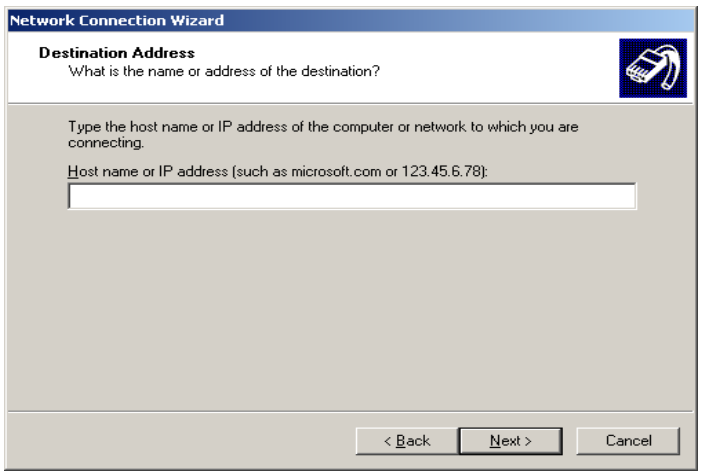


Figure 7.10 Destination address

Enter the SnapGear PPTP server's IP address and click **Next**. Select the **Connection Availability** you require on the next window and click **Next** to display the final window:

Figure 7.11 Completing the network connection wizard

Enter an appropriate name for your connection and click **Finish**.

Your VPN client is now set up correctly.

Connecting the remote VPN client

Firstly, connect to the Internet using the network connection to your ISP.

After authenticating the connection to your ISP, select the connection for the SnapGear appliance VPN.

For *Windows 95/98/2000*, enter the username and password allocated by your SnapGear appliance's VPN administrator and click **Connect**.

For *Windows NT*, click **Dial** and enter the username and password *allocated* by your SnapGear appliance's VPN administrator.

After you are authenticated to the network, you can check your e-mail, use the office printer, access shared files and browse the network as if you were physically on the LAN.

To disconnect the VPN tunnel connection to the remote SnapGear appliance:

- On the desktop, double-click **My Computer** then **Dial-Up Networking** and select the phonebook entry for the SnapGear appliance VPN.
- For *Windows 95/98/2000*, click the **Disconnect** button
- For *Windows NT*, click the **Hang up** button

You can then disconnect from the Internet.

IPSec setup

The SnapGear appliance supports IPSec tunnels as well as PPTP tunnels. To setup your VPN using IPSec, select IPSec from the VPN menu to display the following screen:

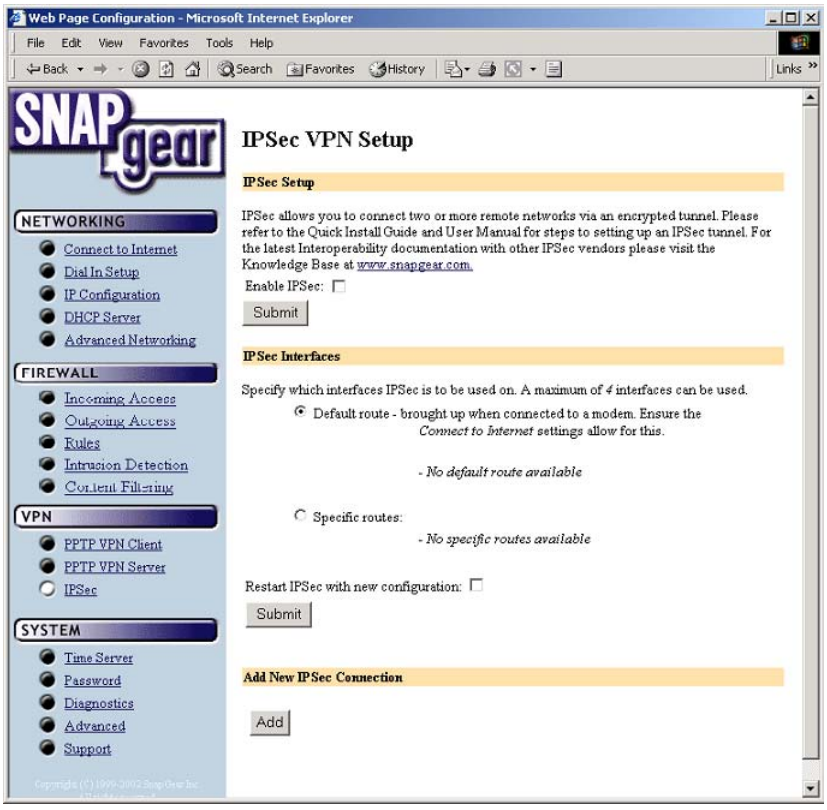


Figure 7.12 IPSec setup

Enable IPSec by clicking the **Enable IPSec** box underneath the **IPSec Setup** title and then click **Submit**.

Enable the interface where you want to use IPSec. This may be the default gateway or a PPP interface for ADSL and cable modems, or **eth1** if the SnapGear appliance is connected to a router before connecting to the Internet and then click **Submit**.

To add a new IPSec connection click on **Add** under **Add New IPSec Connection** to show the following screen:

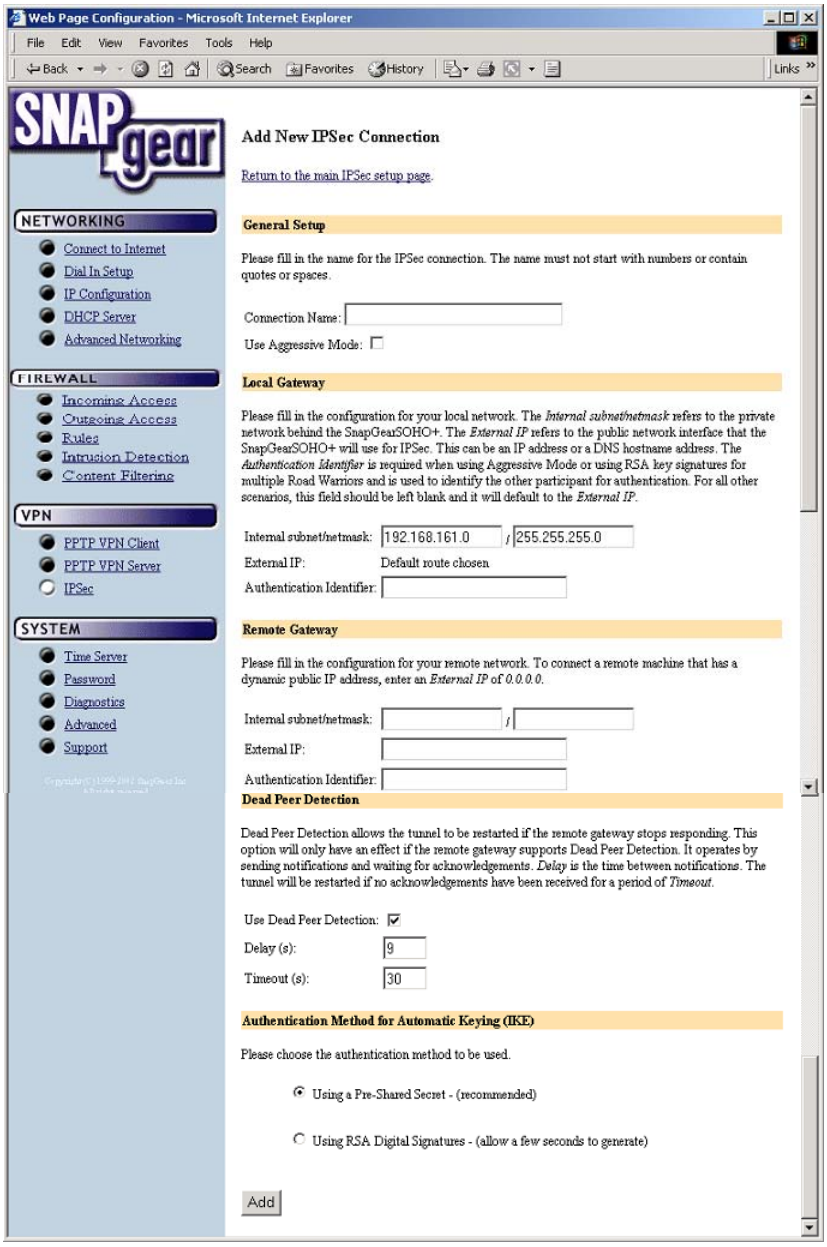


Figure 7.13 Add new IPSec connection

Enter a descriptive name for the connection in the **Connection Name** field.

Choosing to connect with **Aggressive Mode** increases interoperability with third party IPSec servers that only support aggressive mode connections.

Enter the local gateway settings. **Internal subnet/netmask** is the private network behind the SnapGear appliance. **External IP** is the public-network interface that the SnapGear appliance will use for IPSec.

The **Authentication Identifier** is required when using RSA key signatures for multiple Road Warriors and is used to identify the other participant during authentication. If this field is blank, the Authentication Identifier defaults to the External IP.

Nexthop refers to the next-hop gateway IP address to the public network this field is not normally required and can be left blank. This option is only available if you have chosen a specific route; SnapGear recommends that you use the default route. Enter the remote gateway settings. To connect to/from a remote machine that does not have a fixed IP address (e.g. a Road Warrior), enter an External IP of 0.0.0.0 only.

Dead Peer Detection allows the tunnel to be restarted if the remote gateway stops responding. This option is only used if the remote gateway supports Dead Peer Detection. It operates by sending notifications and waiting for acknowledgements. **Delay** is the time between notifications. The tunnel will be restarted if no acknowledgements have been received for a period of **Timeout**.

The recommended keying used in IPSec is **Automatic Keying (IKE)**. The default and recommended method of authentication is using a **Pre-Shared secret** that should be at least 24 characters long. This should be a phrase that you can remember easily but is difficult for others to guess. You can also authenticate using RSA digital signatures.

Click **Add** to complete the IKE setup as shown in the following screen:

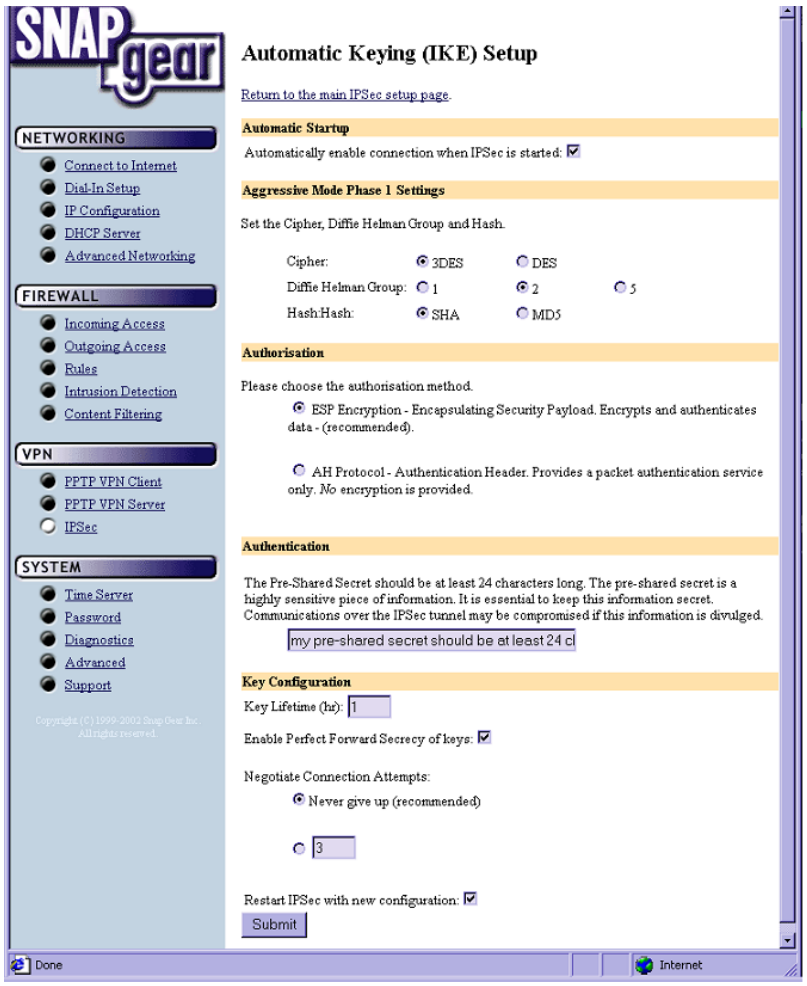


Figure 7.14 Automatic keying setup

Click **Submit** to add the new IPSec tunnel after selecting the appropriate **Automatic Startup**, **Authorization**, **Authentication**, and **Key Configuration**.

Warning

The pre-shared secret must be entered identically at each end of the tunnel. The IPSec tunnel will fail to connect if the pre-shared secret is not identical at both ends.

The pre-shared secret is a highly sensitive piece of information. It is essential to keep this information secret. Communications over the IPSec tunnel may be compromised if this information is divulged.

Aggressive mode phase 1 settings

IPSec combines a number of cryptographic techniques:

Technique	Description
Block ciphers	A symmetric cipher that operates on fixed-size blocks of plaintext, giving a block of ciphertext for each.
Hash functions	A complex operation that uses both a hashing algorithm (MD5 or SHA) and a key.
Diffie-Hellman	The Diffie-Hellman key agreement protocol allows two parties (A and B) to agree on a key in such a way that an eavesdropper who intercepts the entire conversation cannot learn the key. The protocol is based on the discrete logarithm problem and is considered to be secure.

Automatic keying provides a mechanism for regularly changing the cryptographic keys used by the IPSec tunnel. This regular key change results in enhanced security; if a third party gets one key, only the messages between the previous re-keying and the next are exposed.

Key Lifetime is the time between consecutive re-keying events (i.e. the lifetime of a key). Shorter values offer higher security at the expense of the computational overhead required to calculate the new keys. SnapGear recommends a default value of 1 hour.

Checking the **Enable Perfect Forward Secrecy of keys** checkbox means that an attacker who acquires the SnapGear appliance's long-term key (i.e. the *pre-shared secret* or *RSA Signature Key Private Section*) cannot:

- Read previous messages which they may have archived, or
- Read future messages without performing additional successful attacks

Perfect forward secrecy of keys provides the maximum security and is the recommended setting.

IPSec interoperability

Please see the Support Knowledge Base (http://www.SnapGear.com/knowledgebase.html) on the SnapGear Web Site (http://www.SnapGear.com/) for detailed information on successfully establishing IPSec tunnels between your SnapGear appliance and equipment from other vendors.

8. System

Time server

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

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

Password

The SnapGear appliance's password is used to restrict access to the SnapGear appliance's configuration web pages (**WebAdmin**) and the SnapGear appliance itself. The SnapGear appliance password is the 'key' to the security of your network and must be kept secret. SnapGear recommends choosing a password that is easy for you to remember but hard for unauthorized people to guess.

A potential security issue may be introduced by having a network-connected SnapGear appliance accessible, using the factory default password. To prevent this, the password for the SnapGear appliance should be changed when Setup Wizard is run or the Configuration web pages are accessed for the first time.

The SnapGear appliance password can be changed at any time using the configuration web pages by clicking **Password** in the **System** menu.

Warning

Enter **root** *in the username field. The SnapGear appliance factory default password is* **default**.

Diagnostics

If you are experiencing problems with your SnapGear appliance, diagnostic information is provided on the SnapGear appliance's Configuration web pages.

To access this information, from the **System** menu, click **Diagnostics**. Advanced network diagnostics can be viewed by selecting the **Networking** menu, then **Advanced Networking**.

Advanced

The options on the **Advanced** page are intended for network administrators and advanced users **only**.

Warning

Altering the advanced configuration settings may render your SnapGear appliance inoperable.

The **System Log** contains debugging information that may be useful in determining whether all services for your SnapGear appliance are operating correctly. See *Appendix B – System Log* for further details.

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

Flash upgrade

The SnapGear appliance firmware can be updated with newer versions available from the SnapGear web site (http://www.SnapGear.com/downloads.html). The firmware is in binary image files (*.bin*) that can be transferred from a PC on the local network directly into the SnapGear appliance's flash memory. To perform flash upgrades, the SnapGear appliance must be configured on the local network with an IP address.

Flash upgrades can be performed using the configuration web pages. To do this, click **Advanced** then **Flash Upgrade** and enter the IP address of the PC with the binary image and the appropriate filename. A TFTP server must be running on the machine hosting the file.

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

***Warning**:*

If the flash upgrade is interrupted (e.g. power down), the SnapGear appliance will stop functioning and will be unusable until its flash is reprogrammed at the factory. User care is advised.

RESET button

The simplest method to clear the SnapGear appliance's stored configuration information is by pushing the reset button on the back of the SnapGear appliance box. The reset button is the small hole between the serial ports and Ethernet ports. A bent paper clip is a suitable tool for performing this procedure.

Pushing the reset button clears all stored configuration information, reverts all settings to the factory defaults, and reboots the SnapGear appliance.

9. Technical support

The System menu contains an option detailing support information for your SnapGear appliance.

This page provides basic troubleshooting tips, contact details for SnapGear Support, and links to the SnapGear Knowledge Base as shown in the following figure:

Figure 9.1 Technical support

The **Technical Support Report** page is an invaluable resource for the SnapGear Technical Support Staff to analyze problems with your SnapGear appliance. The information on this page gives the Support Staff important information about any problems you may be experiencing.

If you experience a fault with your SnapGear appliance, please attach the **Technical Support Report** to your support request.

Appendix A – LED status patterns

The following table shows the different LED illumination combinations that can indicate possible error conditions.

In each case, the LEDs indicated will be on and steady, unless otherwise noted, and all other LEDs will be off. The Power and System LEDs are not part of the LEDs indicating status. Where the action indicates that you should contact your dealer, please note the LED pattern to assist with faster response and recovery action.

LED Pattern	**Status**	**Action**
VPN	Memory failure.	Please contact your dealer.
COM2	Console device cannot initialize.	Please contact your dealer.
All LEDs on	In recovery mode, usually from a bad Flash image. While the reset button is held in this will be the LED pattern.	
VPN &and Internet Link	Cannot load static data into memory, probably memory and/or Flash problem.	Please contact your dealer.
COM2 and Internet Link	Cannot load SBSS, probably memory and/or Flash problem.	Please contact your dealer.
Online	Memory exception.	Please contact your dealer.

Appendix B – System Log

Access Logging

It is possible to log any traffic that arrives at or traverses the SnapGear appliance. The only logging that is enabled by default is to take note of packets that were dropped. While it is possible to specifically log exactly which rule led to such a drop, this is not configured by default. All rules in the default security policy drop packets. They never reject them. That is, the packets are simply ignored, and have no responses at all returned to the sender. It is possible to configure reject rules if so desired.

All traffic logging performed on the SnapGear appliance creates entries in the syslog (*/var/log/messages* - or external syslog server) of the following format:

<Date/Time> **klogd:** *<prefix>* **IN=***<incoming interface>* **OUT=***<outgoing interface>* **MAC=***<dst/src MAC addresses>* **SRC=***<source IP>* **DST=***<destination IP>* **SPT=***<source port>* **DPT=***<destination port>* *<additional packet info>*

Where:

<prefix>	if non-empty, hints at cause for log entry
<incoming interface>	will be empty, or one of eth0, eth1 and similar
<outgoing interface>	as per incoming interface
<dst/src MAC addresses>	MAC addresses associated with the packet
<source IP>	packet claims it came from this IP address
<destination IP>	packet claims it should go to this IP address
<source port>	packet claims it came from this TCP port
<destination port>	packet wants to go to this TCP port

Depending on the type of packet and logging performed some of the fields may not appear.

Commonly used interfaces are:

eth0	the LAN port
eth1	the WAN/Internet port
ppp*X*	eg. *ppp0* or *ppp1* – a PPP session
ipsec*X*	eg. *ipsec0*, an IPSec interface

The firewall rules deny all packets arriving from the WAN port by default. There are a few ports open to deal with traffic such as DHCP, VPN services and similar. Any traffic that does not match the exceptions however is dropped.

There are also some specific rules to detect various attacks (smurf, teardrop, etc.).

When outbound traffic (from LAN to WAN) is blocked by custom rules configured in the GUI, the resultant dropped packets are also logged.

The <*prefix*> for all these rules is varied according to their type.

Currently used prefixes for traffic arriving:

Default Deny	Packet didn't match any rule – drop it
Invalid	Invalid packet format detected
Smurf	Smurf attack detected
Spoof	Invalid IP address detected
SynFlood	SynFlood attack detected
Custom	Custom rule dropped outbound packet

A typical *Default Deny:* will thus look similar to the following:

```
Mar 27 09:31:19 2003 klogd: Default deny: IN=eth1
OUT=MAC=00:d0:cf:00:ff:01:00:e0:29:65:af:e9:08:00
SRC=140.103.74.181 DST=12.16.16.36 LEN=60 TOS=0x10 PREC=0x00
TTL=64 ID=46341 DF PROTO=TCP SPT=46111 DPT=139 WINDOW=5840
RES=0x00 SYN URGP=0
```

That is, a packet arriving from the WAN (*IN=eth1*) and bound for the SnapGear appliance itself (*OUT=<nothing>*) from IP address 140.103.74.181 (*SRC=140.103.74.181*), attempting to go to port 139 (*DPT=139*, Windows file sharing) was dropped.

If the packet is traversing the SnapGear appliance to a server on the private network, the outgoing interface will be eth0, e.g.:

```
Mar 27 09:52:59 2003 klogd: IN=eth1 OUT=eth0 SRC=140.103.74.181
DST=10.0.0.2 LEN=60 TOS=0x10 PREC=0x00 TTL=62 ID=51683 DF
PROTO=TCP SPT=47044 DPT=22 WINDOW=5840 RES=0x00 SYN URGP=0
```

Packets going from the private network to the public come in eth0, and out eth1, e.g.:

```
Mar 27 10:02:51 2003 klogd: IN=eth0 OUT=eth1 SRC=10.0.0.2
DST=140.103.74.181 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=62830 DF
PROTO=TCP SPT=46486 DPT=22 WINDOW=5840 RES=0x00 SYN URGP=0
```

Creating Custom Log Rules

Additional log rules can be configured to provide more detail if desired. For example, by analysing the rules in the **Rules** menu, it is possible to provide additional log messages with configurable prefixes (i.e. other than *Default Deny:*) for some allowed or denied protocols.

Depending on how the *LOG* rules are constructed it may be possible to differentiate between inbound (from WAN to LAN) and outbound (from LAN to WAN) traffic. Similarly, traffic attempting to access services on the SnapGear appliance itself can be differentiated from traffic trying to pass through it.

The examples below can be entered on the Command Line Interface (telnet), or into the **Rules** SnapGear Management Console web administration pages. Rules entered on the CLI are not permanent however, so while it may be useful for some quick testing, it is something to be wary of.

To log permitted inbound access requests to services hosted on the SnapGear appliance, the rule should look something like this:

iptables -I INPUT -j LOG -p tcp --syn -s *<X.X.X.X/XX>* **-d** *<Y.Y.Y.Y/YY>* **--dport** *<Z>* **--log-prefix** *<prefix>*

This will log any TCP (*-p tcp*) session initiations (*--syn*) that arrive from the IP address/netmask *X.X.X.X/XX* (*-s ...*) and are going to *Y.Y.Y.Y/YY*, destination port Z (*--dport*).

For example, to log all inbound access requests from anywhere on the Internet (0.0.0.0/0) to the PPTP service (port 1723) on the SnapGear appliance (IP address 1.2.3.4):

```
iptables -I INPUT -j LOG -p tcp --syn -s 0.0.0.0/0 -d 1.2.3.4
--dport 1723 --log-prefix "Internet PPTP access: "
```

To find the resultant log entry in the logs, simply search for the prefix, in this instance *"Internet PPTP access: "*.

If for example site 192.0.1.2 attempted to access the SnapGear appliance's PPTP port, the resultant log message would look something like this:

```
<12> Jan 24 17:19:17 2000 klogd: Internet PPTP access: IN=eth0
OUT= MAC=00:d0:cf:00:07:03:00:50:bf:20:66:4d:08:00 SRC=
DST=1.2.3.4 LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=43470 DF
PROTO=TCP SPT=4508 DPT=1723 WINDOW=64240 RES=0x00 SYN URGP=0
```

Note how *OUT* is set to nothing. This indicates that the packet was attempting to reach a service on the SnapGear appliance, rather than attempting to pass through it.

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

Thus, to log permitted inbound requests to services hosted on a server behind the SnapGear appliance, or outbound requests to services on a public network server, use:

iptables -I FORWARD -j LOG -p tcp --syn -s *<X.X.X.X/XX>* **-d** *<Y.Y.Y.Y/YY>* **--dport** *<Z>* **--log-prefix** *<prefix>*

For example, to log all inbound requests from the IP address 5.6.7.8 to the mail server (port 25) on the machine *flubber* on the LAN with address 192.168.1.1:

```
iptables -I FORWARD -j LOG -p tcp --syn -s 5.6.7.8/32 -d
192.168.1.1 --dport 25 --log-prefix "Mail for flubber: "
```

This will result in log output something like this:

```
<12> Jan 24 18:17:19 2000 klogd: Mail for flubber: IN=eth1
OUT=eth0 SRC=5.6.7.8 DST=192.168.1.1 LEN=48 TOS=0x00 PREC=0x00
TTL=126 ID=45507 DF PROTO=TCP SPT=4088 DPT=25 WINDOW=64240
RES=0x00 SYN URGP=0
```

Note how the *OUT* value has now changed to show which interface the access attempt will use to reach the internal host. As this request arrived on eth1 and was destined for eth0, we can determine that it was an *inbound* request, since eth0 is the LAN port, and eth1 is usually the WAN port.

An *outbound* request would have *IN=eth0* and *OUT=eth1*.

It is possible to use the *-i* and *-o* arguments to specify the interface that are to be considered for *IN* and *OUT* respectively. When the *!* argument is used before the interface name, the sense is inverted. If the name ends in a +, then any interface which begins with this name will match. e.g.

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

This rule will log outbound from the LAN (eth0) only. We could limit that further by specifying which interface it is outbound to, by using the *-o* option.

```
iptables -I FORWARD -j LOG -i eth0 -o eth1 -p tcp ...
```

This will log LAN traffic destined for the WAN – but won't log LAN traffic destined for a PPP or perhaps IPSec link.

Similarly, we could construct a rule that looks at all inbound/outbound traffic, but excludes VPN traffic, thus:

```
iptables -I FORWARD -j LOG -i eth+ -o eth+ -p tcp ...
```

If we just wanted to look at traffic which went out to the IPSec world, we could use:

```
iptables -I FORWARD -j LOG -o ipsec+
```

Clearly there are many more combinations possible.

It is therefore possible to write rules which log inbound and outbound traffic, or to construct several rules which differentiate between the two.

Rate Limiting

iptables has the facility for rate-limiting the log messages that are generated, in order to avoid denial of service issues arising out of logging these access attempts. To achieve this, use the following option:

--limit *rate*

> *rate* is the maximum average matching rate, specified as a number with an optional */second*, */minute*, */hour*, or */day* suffix. The default is *3/hour*.

--limit-burst *number*

> *number* is the maximum initial number of packets to match. This number gets recharged by one every time the limit specified above is not reached, up to this number. The default is *5*.

iptables has many more options. Perform a web search for *manpage iptables* to find the relevant documentation.

The *LOG* rules configured by default (e.g. *Default Deny:*) are all limited to:

```
--limit 3/hour --limit-burst 5
```

Administrative Access Logging

When a user tries to log onto the SnapGear Management Console web administration pages, one of the following log messages appears:

```
Jan 30 03:00:18 2000 boa: Authentication successful for root from
10.0.0.2
```

```
Jan 30 03:00:14 2000 boa: Authentication attempt failed for root
from 10.0.0.2
```

This message shows the date/time, whether the authentication succeeded or failed, the user attempting authentication (in this case *root*) and the IP address from which the attempt was made.

Telnet (Command Line Interface) login attempts appear as:

```
Jan 30 03:18:37 2000 login: Authentication attempt failed for
root from 10.0.0.2
```

```
Jan 30 03:18:40 2000 login: Authentication successful for root
from 10.0.0.2
```

Once again, showing the same information as a web login attempt.

Boot Log Messages

The SnapGear appliance's startup boot time messages are identified by log messages similar to the following:

```
klogd: Linux version 2.4.20-uc0 (jamma@daniel) (gcc version
3.0.4) #4 Mon Feb 3 15:17:50 EST 2003
```

This also shows the version of the operating system (linux), and the build date and time.