3COM

OfficeConnect®

VPN Firewall (3CR870-95)

User Guide

3Com Corporation
350 Campus Drive
Marlborough, MA USA 01752-3064

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as “Commercial Computer Software” as defined in DFARS 252.227-7014 (June 1995) or as a “commercial item” as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com’s standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com, the 3Com logo and OfficeConnect are registered trademarks of 3Com Corporation.

Intel and Pentium are registered trademarks of Intel Corporation. Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Novell and NetWare are registered trademarks of Novell, Inc. UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd.

Netscape Navigator is a registered trademark of Netscape Communications.

JavaScript is a trademark of Sun Microsystems

All other company and product names may be trademarks of the respective companies with which they are associated.

ENVIRONMENTAL STATEMENT

It is the policy of 3Com Corporation to be environmentally-friendly in all operations. To uphold our policy, we are committed to:

Establishing environmental performance standards that comply with national legislation and regulations.

Conserving energy, materials and natural resources in all operations.

Reducing the waste generated by all operations. Ensuring that all waste conforms to recognized environmental standards. Maximizing the recyclable and reusable content of all products.

Ensuring that all products can be recycled, reused and disposed of safely.

Ensuring that all products are labelled according to recognized environmental standards.

Improving our environmental record on a continual basis.

End of Life Statement

3Com processes allow for the recovery, reclamation and safe disposal of all end-of-life electronic components.

Regulated Materials Statement

3Com products do not contain any hazardous or ozone-depleting material.

Environmental Statement about the Documentation

The documentation for this product is printed on paper that comes from sustainable, managed forests; it is fully biodegradable and recyclable, and is completely chlorine-free. The varnish is environmentally-friendly, and the inks are vegetable-based with a low heavy-metal content.

CONTENTS

About This Guide

This guide is intended for use by those responsible for installing and setting up network equipment; consequently, it assumes a basic working knowledge of LANs (Local Area Networks) and Internet firewall systems.

ℹ *If a release note is shipped with this OfficeConnect VPN Firewall and contains information that differs from the information in this guide, follow the information in the release note.*

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) on the 3Com World Wide Web site:

`http://www.3com.com`

Naming Convention

Throughout this guide, the *OfficeConnect VPN Firewall* is referred to as the *Firewall*.

Category 3 and Category 5 Twisted Pair Cables are referred to as Twisted Pair Cables throughout this guide.

Conventions

Table 1 and Table 2 list conventions that are used throughout this guide.

Table 1 Notice Icons

Icon	Notice Type	Description
ℹ	Information note	Information that describes important features or instructions
⚠	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device
⚡	Warning	Information that alerts you to potential personal injury

Table 2 Text Conventions

Convention	Description
The words “enter” and “type”	When you see the word “enter” in this guide, you must type something, and then press Return or Enter. Do not press Return or Enter when an instruction simply says “type.”
Keyboard key names	If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press Ctrl+Alt+Del

Table 2 Text Conventions (continued)

Convention	Description
Words in *italics*	Italics are used to: ■ Emphasize a point. ■ Denote a new term at the place where it is defined in the text. ■ Identify menu names, menu commands, and software button names. Examples: From the *Help* menu, select *Contents*. Click *OK*.

Feedback about this User Guide

Your suggestions are very important to us. They will help make our documentation more useful to you. Please e-mail comments about this document to 3Com at:

pddtechpubs_comments@3com.com

Please include the following information when commenting:

- Document title
- Document part number (on the title page)
- Page number (if appropriate)

Example:

- OfficeConnect VPN Firewall User Guide
- Part Number DUA08709-5AAA0x
- Page 24

Do not use this e-mail address for technical support questions. For information about contacting Technical Support, please refer to “Obtaining Support for your Product” *on* page 93.

INTRODUCING THE OFFICECONNECT VPN FIREWALL

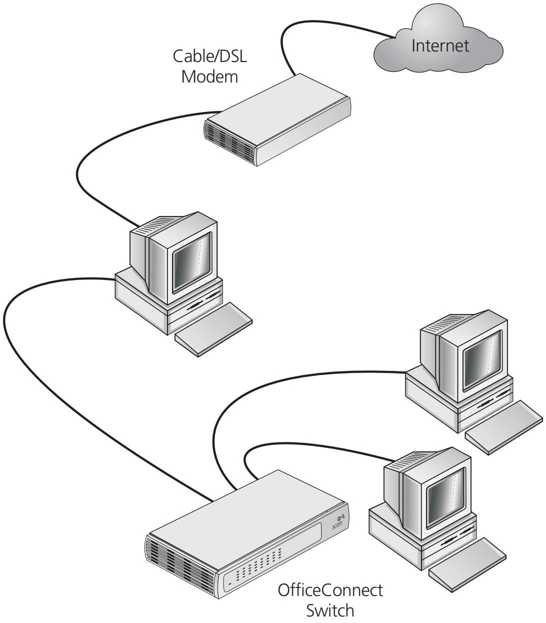
Welcome to the world of networking with 3Com®. In the modern business environment, communication and sharing information is crucial. Computer networks have proved to be one of the fastest modes of communication but, until recently, only large businesses could afford the networking advantage. The OfficeConnect® product range from 3Com has changed all this, bringing networks to the small office.

The products that compose the OfficeConnect line give you, the small office user, the same power, flexibility, and protection that has been available only to large corporations. Now, you can network the computers in your office, connect them all to a single Internet outlet, and harness the combined power of all of your computers.

OfficeConnect VPN Firewall

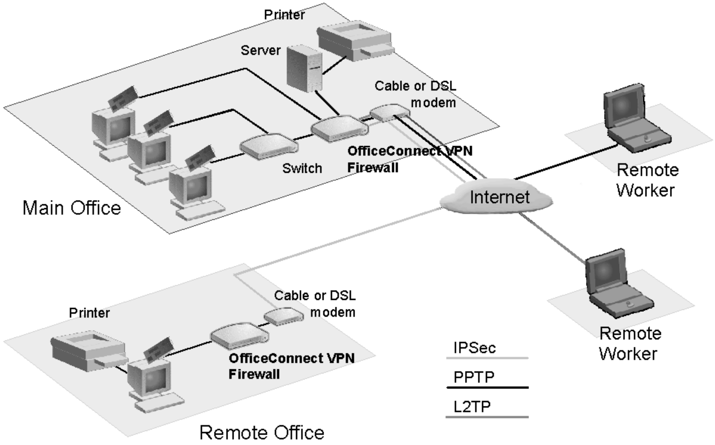
The OfficeConnect VPN Firewall is designed to provide a robust, secure solution for multi-site small businesses. This completely equipped, broadband-capable Virtual Private Network (VPN) firewall prevents unauthorised external access to your network — and by creating Virtual Private Networks (VPNs) — encrypted links to other private networks. The OfficeConnect VPN Firewall also provides Denial of Service (DoS) protection and intrusion detection using Stateful Packet Inspection (SPI), web content filtering, logging and reporting.

Figure 1 Example Network Without a VPN Firewall



When you use the VPN Firewall in your network (Figure 2), it becomes your connection to the Internet. Connections can be made directly to the Device, or through an OfficeConnect Hub or Switch, expanding the number of computers you can have in your network.

Figure 2 Example Network Using a VPN Firewall



VPN Firewall Advantages

The advantages of using the VPN Firewall include:

- Provides firewall protection against Internet hacker attacks.
  - Implements Stateful Packet Inspection (SPI) to block network intrusions.
  - Blocks Denial of Service (DoS) attacks by using pattern detection.
- Supports Virtual Private Networks (VPNs).
  - Initiates and terminates IPSec connections.
  - Terminates PPTP and L2TP over IPSec connections.
  - Provides hardware accelerated encryption for IPSec VPNs, including L2TP over IPSec.
- Shared Internet connection.
- No need for a dedicated, “always on” computer serving as your Internet connection.
- Cross-platform operation for compatibility with Windows, Unix and Macintosh computers.
- Easy-to-use, Web-based setup and configuration.
- Provides centralization of all network address settings (DHCP).
- Provides *Virtual Server* redirection to enable remote access to Web, FTP, and other services on your network
- Supports content filtering service (license sold separately).

Package Contents

The OfficeConnect VPN Firewall kit includes the following items:

- One OfficeConnect VPN Firewall
- One power adapter for use with the Firewall
- Four rubber feet
- One stacking clip
- One Ethernet cable
- One CD-ROM containing
  - the Discovery program
  - this User Guide
  - the license agreement
- One Warranty Flyer
- One License Agreement
- This User Guide

If any of these items are missing or damaged, please contact your retailer.

Minimum System and Component Requirements

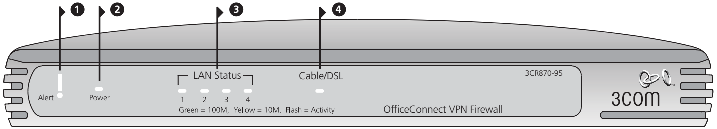
Your OfficeConnect VPN Firewall requires that the computer(s) and components in your network be configured with at least the following:

- A computer with an operating system that supports TCP/IP networking protocols (for example Windows 95/98/NT/Me/2000/XP, Unix, Mac OS 8.5 or higher).
- An Ethernet 10 Mbps or 10/100 Mbps NIC for each computer to be connected to the four-port switch on your Firewall.
- An Internet access device with an Ethernet (RJ-45) port, for example a cable modem or DSL modem.
- An active Internet access account.
- A Web browser program that supports JavaScript, such as Netscape 4.7 or higher or Internet Explorer 5.5 or higher.

Front Panel

The front panel of the VPN Firewall contains a series of indicator lights (LEDs) that help describe the state of various networking and connection operations.

Figure 3 VPN Firewall - Front Panel



1
2
3
4
Alert
Power
LAN Status
1 2 3 4
Green = 100M, Yellow = 10M, Flash = Activity
Cable/DSL
3CR870-95
OfficeConnect VPN Firewall
3com

1 Alert LED (Orange)

Indicates a number of different conditions, as described below.

Off The Firewall is operating normally.

Flashing quickly Indicates one of the following conditions:

- The Firewall has just been started up and is running a self-test routine.

The Alert LED may continue to flash for one minute or longer during self test, depending on your network configuration.

- The system software is in the process of being upgraded.

In each of these cases, wait until the Firewall has completed the current operation and the alert LED is Off.

Flashing slowly The Firmware is corrupt or the Firewall has booted in fail-safe mode. See “Troubleshooting” on page 77.

On for 2 seconds, then off The Firewall has detected and prevented a hacker from attacking your network from the Internet.

Continuously on A fault has been detected with your Firewall during the start-up process. See “Troubleshooting” on page 77.

The Alert LED will be on for a period of between three and five seconds during the power on self test. This is normal and no cause for alarm.

2 Power LED (Green)

Indicates that the Firewall is powered on.

3 Four LAN Status LEDs

Green (100 Mbps link) / Yellow (10 Mbps link)

Indicates a number of different conditions, as described below.

On The link between the port and the next piece of network equipment is OK.

Flashing The link is OK and data is being transmitted or received.

Off Indicates one of the following

- nothing is connected
- the connected device is switched off
- there is a problem with the connection. “Troubleshooting” on page 77.

4 Cable/DSL Status LED

Green (100 Mbps link) / Yellow (10 Mbps link)

Indicates a number of different conditions, as described below.

On The link between the Firewall and the cable or DSL modem is OK.

Flashing The link is OK and data is being transmitted or received.

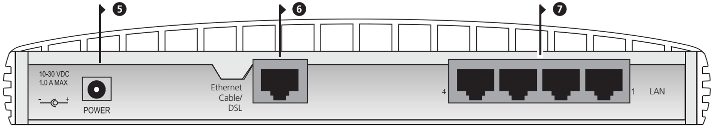
Off Indicates one of the following

- nothing is connected
- the modem is switched off
- there is a problem with the connection. “Troubleshooting” on page 77.

Rear Panel

The rear panel (Figure 4) of the Firewall contains four LAN ports, one Ethernet Cable/DSL port, and a power adapter socket.

Figure 4 VPN Firewall - Rear Panel



5 Power Adapter socket

Only use the power adapter that is supplied with this Firewall. Do not use any other adapter.

6 Ethernet Cable/DSL port

Use the supplied patch cable to connect the Firewall to the 10/100 port on your cable or DSL modem. This port will automatically adjust for the correct speed, duplex and cable type. You can connect your Cable/DSL modem using either straight-through or crossover cables.

7 Four 10/100 LAN ports

Use suitable cable with RJ-45 connectors. You can connect your Firewall to a computer, or to any other piece of equipment that has an Ethernet connection (for example, a hub or a switch). All ports will automatically adjust for the correct speed, duplex and cable type. You can connect your Ethernet devices using either straight-through or crossover cables.

Installing the Firewall

Introduction

This chapter will guide you through a basic installation of the OfficeConnect VPN Firewall, including:

- Connecting the Firewall to the Internet.
- Connecting the Firewall to your network.

Positioning the Firewall

You should place the VPN Firewall in a location that:

- is conveniently located for connection to the cable or DSL modem that will be used to connect to the Internet.
- allows convenient connection to the computers that are to be connected to the four LAN ports on the rear panel.
- allows easy viewing of the front panel LED indicator lights, and access to the rear panel connectors, if necessary.

Safety Information

⚠ ***WARNING:*** *Please read the "Important Safety Information" section before you start.*

⚠ ***VORSICHT:*** *Bitte lesen Sie den Abschnitt "Wichtige Sicherheitsinformationen" sorgfältig durch, bevor Sie das Gerät einschalten.*

⚠ ***AVERTISSEMENT:*** *Veuillez lire attentivement la section "Consignes importantes de sécurité" avant de mettre en route.*

When positioning your Firewall, ensure:

- It is out of direct sunlight and away from sources of heat.
- Cabling is away from power lines, fluorescent lighting fixtures, and sources of electrical noise such as radios, transmitters and broadband amplifiers.
- Water or moisture cannot enter the case of the unit.
- Air flow around the unit and through the vents in the side of the case is not restricted. We recommend you provide a minimum of 25mm (1in.) clearance.

Using the Rubber Feet

Use the four self-adhesive rubber feet to prevent your Firewall from moving around on your desk or when stacking with flat top OfficeConnect units. Only stick the feet to the marked areas at each corner of the underside of your Firewall.

Using the Stacking Clip

The stacking clip allows you to stack your OfficeConnect units together neatly and securely.

⚠ ***CAUTION:*** *You can stack up to a maximum of four units. Smaller units must be stacked above larger units.*

To fit the clip:

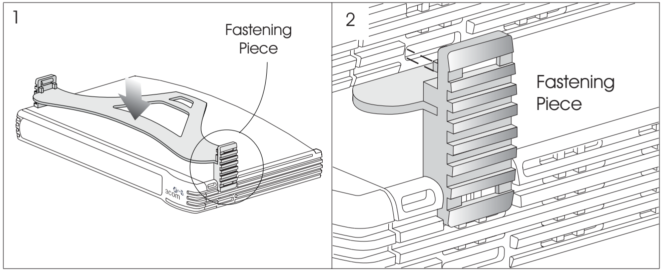
1. Place your unit on a flat surface.
2. Fit the clip across the top of the unit, as shown in Figure 5 (picture 1), ensuring that the longer sections of the fastening pieces are pointing downwards.
3. Align the fastening pieces over the slots found on each side of the unit.

4. Push the clip down gently to secure it, ensuring the fastening pieces snap into the slots on the unit.

To fit another unit:

1. Rest the second unit on top of the clip and align it with the front of the unit below.
2. Press down gently on the unit to secure it onto the clip, ensuring the fastening pieces fit into the slots on the unit below, as shown in Figure 5 (picture 2).

Figure 5 Stacking Your Units Together



To remove the clip:

1. Remove the top unit together with the clip. If you hook a finger around one of the the fastening pieces and then pull it gently from out of the slot, the clip should come away with the upper unit attached to it.
2. Push the clip in the center, so it bends towards the base of the unit, and then separate once the clip is loose.

Before you Install your Firewall

Before you can configure the Firewall you need to know the IP information allocation method used by your ISP. There are four different ways that ISPs allocate IP information, as described below:

Dynamic IP Address (DSL or Cable)

Dynamic IP addressing (or DHCP) automatically assigns the Firewall IP information. This method is popular with Cable providers. This method is also used if your modem has a built in DHCP server.

PPPoE (DSL only)

If the installation instructions that accompany your modem ask you to install a PPPoE client on your PC then select this option. Note that when you install the Firewall, you will not need to use the PPPoE software on your PC. To configure the Firewall you will need to know the following: Username, Password, and Service Name (if required by your ISP).

Static IP Address (DSL or Cable)

The ISP provides the IP addressing information for you to enter manually. To configure the Firewall you will need to know the following: IP Address, Subnet Mask, ISP Gateway Address, and DNS address(es).

PPTP (DSL or Cable)

PPTP is used by some providers, mostly in Europe. If the installation instructions that accompany your modem ask you to setup a dialup connection using a PPTP VPN tunnel then select this option. Note that when you install the Firewall, you will not need to use the dialup VPN on your PC anymore. To configure the Firewall, you need to know the following: Username, Password, and VPN Server Address (usually your modem). You will be asked for the IP Allocation Mode when you run the Setup Wizard.

Powering Up the Firewall

1 Plug the power adapter into the power adapter socket located on the back panel of the Firewall (refer to “Power Adapter socket” on page 13).

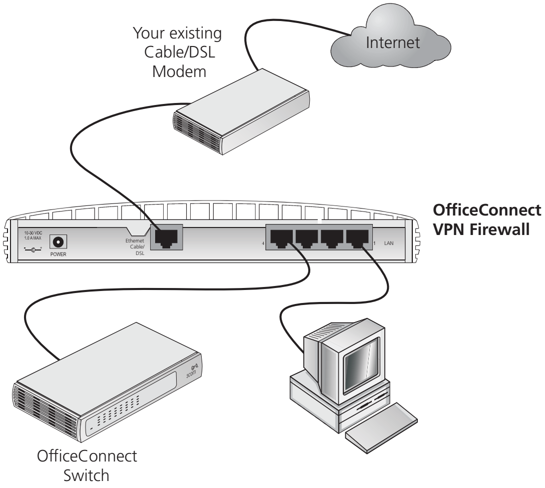
2 Plug the power adapter into a standard electrical wall socket.

Connecting the VPN Firewall

The first step for installing your VPN Firewall is to physically connect it to a cable or DSL modem in order to be able to access the Internet.

:

Figure 6 Connecting the VPN Firewall



To use your VPN Firewall to connect to the Internet through an external cable or DSL modem (Figure 6)

1 Use the supplied cable to connect the Firewall's Ethernet Cable/DSL port to your Cable/DSL modem. Ensure that your modem is connected to the Internet and switched on.

2 Connect your computer to one of the 10/100 LAN ports on the Firewall.

3 Connect the power adaptor to the Firewall and wait for the Alert LED to stop flashing. Check that the Cable/DSL Status LED is illuminated.

4 Switch on your computer. Once your computer is ready to use, check that the LAN Port Status LED on the Firewall is illuminated.

You have now completed the hardware installation of your Firewall. You now need to set up your computers so that they can make use of the Firewall to communicate with the Internet.

SETTING UP YOUR COMPUTERS

The OfficeConnect VPN Firewall has the ability to dynamically allocate network addresses to the computers on your network, using DHCP. However, your computers need to be configured correctly for this to take place. To change the configuration of your computers to allow this, follow the instructions in this chapter.

If your computers are configured with static addresses (also known as fixed addresses) and you do not wish to change this, then you should use the Discovery program on the Firewall CD-ROM to detect and configure your Firewall. Refer to “Using Discovery” on page 81 for information on using the Discovery program.

Obtaining an IP Address Automatically

Windows 2000, XP, 2003 Server

If you are using Windows 2000, Windows XP or Windows 2003 Server, use the following procedure to change your TCP/IP settings (Windows XP and 2003 Server specific instructions in brackets):

1 From the Windows *Start* Menu, select *Settings* > *Control Panel* (select Control Panel directly from the Start menu in Windows XP)

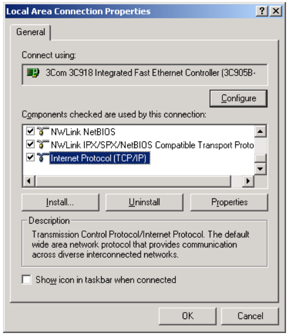
2 Double click on *Network and Dial-Up Connections* (*Network and Internet Connections*). For XP and 2003 Server only — click on *Network Connections*.

3 Double click on *Local Area Connection*.

4 Click on *Properties*.

5 A screen similar to Figure 7 should be displayed. Select *Internet Protocol (TCP/IP)* and click on *Properties*.

Figure 7 Local Area Connection Properties



Local Area Connection Properties

Connect using:
3Com 3C918 Integrated Fast Ethernet Controller (3C905B-

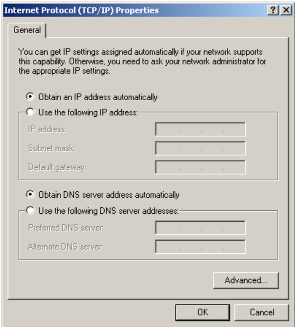
Components checked are used by this connection:
☑ NWLink NetBIOS
☑ NWLink IPX/SPX/NetBIOS Compatible Transport Proto
☑ Internet Protocol (TCP/IP)

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

□ Show icon in taskbar when connected

6 Ensure that the options *Obtain an IP Address automatically*, and *Obtain DNS server address automatically* are both selected as shown in Figure 8. Click *OK*.

Figure 8 Internet Protocol Properties


Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

7 Restart your computer.

Windows 95, 98

1 From the Windows *Start* Menu, select *Settings* > *Control Panel*.

2 Double click on *Network*. Select the *TCP/IP* item for your network card and click on *Properties*.

3 In the TCP/IP dialog, select the *IP Address* tab, and ensure that *Obtain IP address automatically* is selected. Click *OK*.

4 Restart your computer.

Macintosh OS 8.5, 9.x

If you are using a Macintosh computer, use the following procedure to change your TCP/IP settings:

1 From the desktop, select *Apple Menu*, *Control Panels*, and *TCP/IP*.

2 In the *TCP/IP* control panel, set *Connect Via:* to "Ethernet."

3 In the TCP/IP control panel, set *Configure:* to "Using DHCP Server."

4 Close the *TCP/IP* dialog box, and save your changes.

5 Restart your computer.

Disabling PPPoE and PPTP Client Software

If you have PPPoE or PPTP client software installed on your computer, you will need to disable it. To do this:

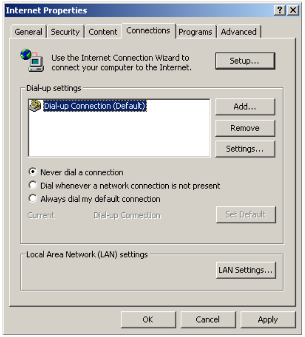
1 From the Windows *Start* menu, select *Settings* > *Control Panel*.

2 Double click on *Internet* Options.

3 Select the *Connections* Tab. A screen similar to Figure 9 should be displayed.

4 Select the *Never Dial a Connection* option and click *OK*.

Figure 9 Internet Properties



Use the Internet Connection Wizard to connect your computer to the Internet.

Dial-up settings

Dial-up Connection (Default)

● Never dial a connection

○ Dial whenever a network connection is not present

○ Always dial my default connection

Current Dial-up Connection

Local Area Network (LAN) settings

You may wish to remove the PPPoE client software from your computer to free resources, as it is not required for use with the Firewall.

Disabling Web Proxy

Ensure that you do not have a web proxy enabled on your computer.

Go to the *Control Panel* and click on *Internet Options*. Select the *Connections* tab and click on *LAN Settings* at the bottom. Make sure that the *Use Proxy Server* option is unchecked.

Running the Setup Wizard

If the Firewall needs to be configured, for example if it has not yet been used or has been reset, it will run the Setup Wizard automatically. This detects some of the settings the Firewall needs to function and asks that you input the others.

Accessing the Wizard

The VPN Firewall Setup Wizard is Web-based, which means that it is accessed through your Web browser (Netscape Navigator or Internet Explorer).

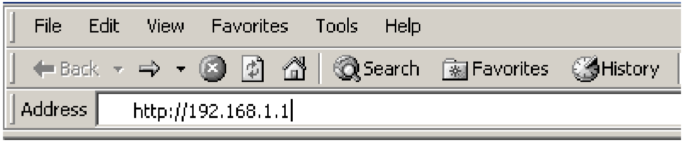
To use the Setup Wizard:

1 Ensure that you have at least one computer connected to the Firewall. See "Installing the Firewall" on page 15.

2 Launch your Web browser on the computer. Enter the URL of your Firewall in to the location or address box of your browser (Figure 10).

*The default URL for the Firewall is **http://192.168.1.1**. If you have changed the IP address of the unit you should substitute this for the default address within the URL.*

Figure 10 Web Browser Location Field (Factory Default)

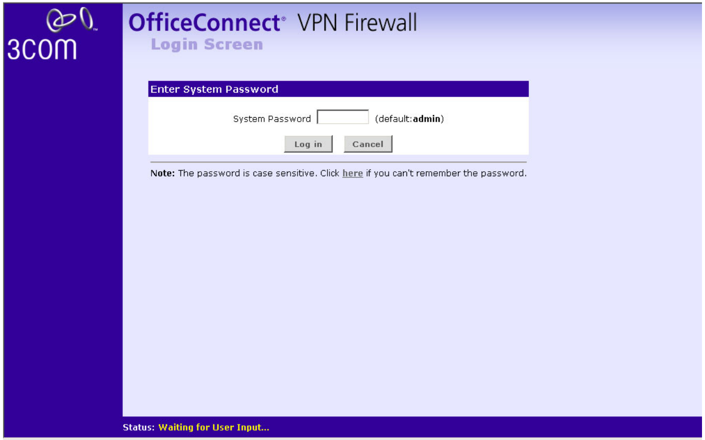


http://192.168.1.1

The *Login* screen, as shown in Figure 11, should appear in your browser. If it does not, refer to "Troubleshooting" on page 77.

3 To log in, enter the password (the default password is *admin*) in the *System Password* field and click *Log in*.

Figure 11 Login Screen



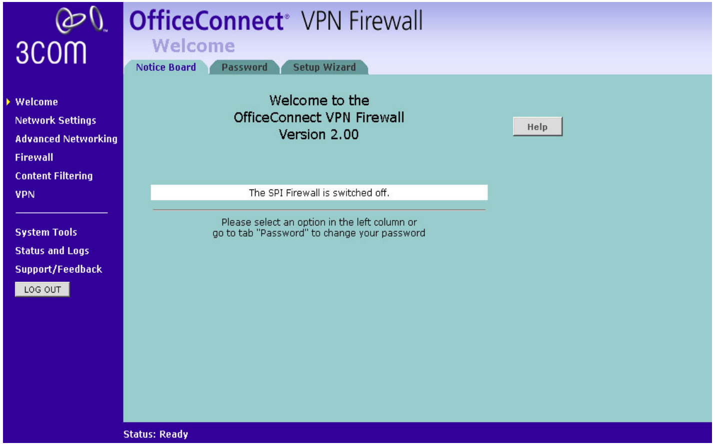
System Password (default:**admin**)

Note: The password is case sensitive. Click here if you can't remember the password.

Status: Waiting for User Input...

4 If the password is correct, the *OfficeConnect VPN Firewall Welcome* screen, shown in Figure 12, will appear. If your Firewall has not been configured before, the Wizard, shown in Figure 13, will also launch automatically.

Figure 12 Welcome Screen



Welcome to the
OfficeConnect VPN Firewall
Version 2.00

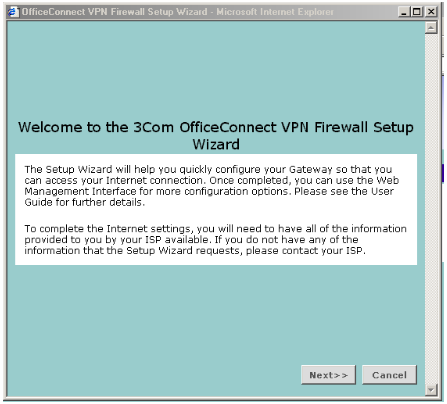
The SPI Firewall is switched off.

Please select an option in the left column or
go to tab "Password" to change your password

If the *Wizard* does not launch automatically (this may occur if the Firewall has been powered up or configured previously) you can launch the *Wizard* manually.

5 To launch the *Wizard* manually click on the *Setup Wizard* tab in the welcome screen followed by the *WIZARD...* button.

Figure 13 Wizard Screen


OfficeConnect VPN Firewall Setup Wizard - Microsoft Internet Explorer
Next>>
Cancel

Welcome to the 3Com OfficeConnect VPN Firewall Setup Wizard

The Setup Wizard will help you quickly configure your Gateway so that you can access your Internet connection. Once completed, you can use the Web Management Interface for more configuration options. Please see the User Guide for further details.

To complete the Internet settings, you will need to have all of the information provided to you by your ISP available. If you do not have any of the information that the Setup Wizard requests, please contact your ISP.

Click *Next* to continue.

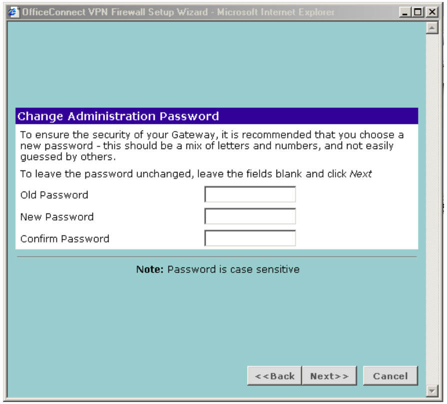
You will now be guided through the setup of your Firewall.

Setting the Password

When the *Change Administration Password* screen (Figure 14) appears, type the *Old Password*, then a new password in both the *New Password* and *Confirm Password* fields.

The default password for the Firewall is 'admin'. It is case sensitive and must be entered as the Old Password the first time you configure the Firewall. 3Com recommends that you change the password from its default value.

Figure 14 Change Administration Password Screen


OfficeConnect VPN Firewall Setup Wizard - Microsoft Internet Explorer

Change Administration Password

To ensure the security of your Gateway, it is recommended that you choose a new password - this should be a mix of letters and numbers, and not easily guessed by others.

To leave the password unchanged, leave the fields blank and click *Next*

Old Password

New Password

Confirm Password

Note: Password is case sensitive

Choose a password that you can remember but that others are unlikely to guess. Remember that the password is case sensitive.

Click *Next* to display the *Time Zone* setup screen (Figure 15).

Setting the Time Zone

The Firewall sets its time automatically when it connects to the Internet. This time is used when recording information log files.

To set the Firewall to your local time:

1 Select your time zone from the drop-down menu.

2 Check the *Enable Daylight Saving* box to automatically adjust the time seasonally.

3 Click *Next* to continue.

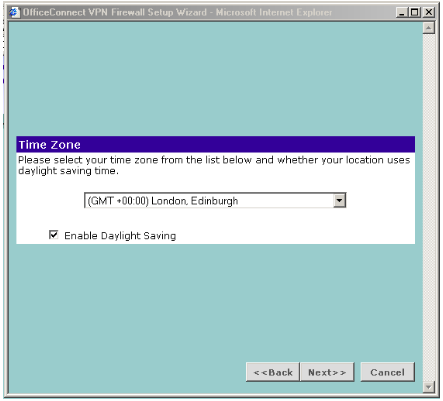
To set the Firewall to World Time (UTC):

1 Select *(GMT) Greenwich Mean Time* from the drop-down menu.

2 Ensure that the *Enable Daylight Saving* box is cleared.

3 Click *Next* to continue.

Figure 15 Time Zone Screen


OfficeConnect VPN Firewall Setup Wizard - Microsoft Internet Explorer

Time Zone

Please select your time zone from the list below and whether your location uses daylight saving time.

(GMT +00:00) London, Edinburgh

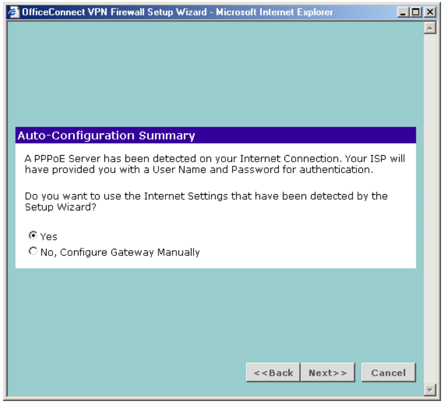
☑ Enable Daylight Saving

The Daylight Savings option automatically adjusts the system clock for summer and winter time. To disable this feature ensure that the Enable Daylight Saving *box is cleared.*

Auto-Configuration Settings

If the Firewall is able to detect a PPPoE or DHCP server on its Ethernet Cable/DSL port then it will offer you the option of configuring its Internet settings automatically. As an example, the *Auto-Configuration* screen for PPPoE is shown in Figure 16 below.

Figure 16 PPPoE Auto-configuration Screen


OfficeConnect VPN Firewall Setup Wizard - Microsoft Internet Explorer
<<Back
Next>>
Cancel

Auto-Configuration Summary

A PPPoE Server has been detected on your Internet Connection. Your ISP will have provided you with a User Name and Password for authentication.

Do you want to use the Internet Settings that have been detected by the Setup Wizard?

● Yes
○ No, Configure Gateway Manually

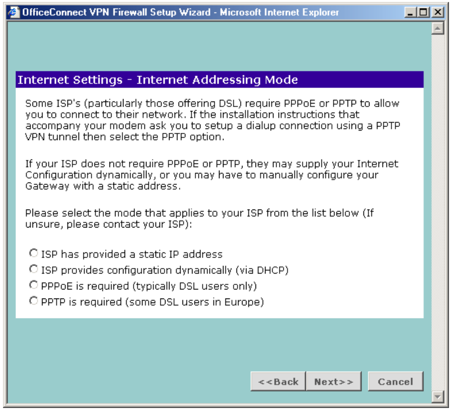
Click *Next* to accept the option you have chosen and continue.

- If the Firewall could not automatically configure your internet settings or if you chose to configure your Internet settings manually, continue at “Internet Settings” below.
- If you chose one of the automatic configuration options continue at “Choosing your LAN Settings” on page 29.

Internet Settings

The *Internet Settings* window allows you to set up the Firewall for the type of Internet connection you have. Before setting up your Internet connection mode, have the modem configuration supplied by your ISP to hand.

Figure 17 Internet Settings Screen


OfficeConnect VPN Firewall Setup Wizard - Microsoft Internet Explorer
<<Back
Next>>
Cancel

Internet Settings - Internet Addressing Mode

Some ISP's (particularly those offering DSL) require PPPoE or PPTP to allow you to connect to their network. If the installation instructions that accompany your modem ask you to setup a dialup connection using a PPTP VPN tunnel then select the PPTP option.

If your ISP does not require PPPoE or PPTP, they may supply your Internet Configuration dynamically, or you may have to manually configure your Gateway with a static address.

Please select the mode that applies to your ISP from the list below (If unsure, please contact your ISP):

○ ISP has provided a static IP address
○ ISP provides configuration dynamically (via DHCP)
○ PPPoE is required (typically DSL users only)
○ PPTP is required (some DSL users in Europe)

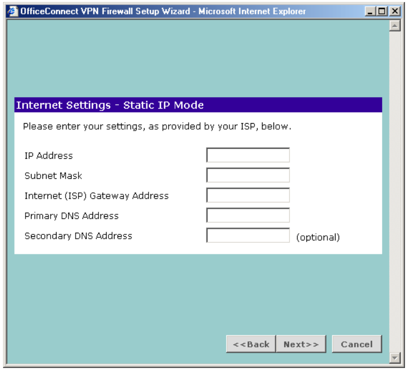
Select the Internet Addressing mode your ISP requires and click *Next*. Depending on your selection, refer to:

- “Static IP Mode” on page 27
- “Dynamic IP Address Mode” on page 27
- “PPPoE Mode” on page 28,
- “PPTP Mode” on page 29.

Static IP Mode

To setup the Firewall for use with a static IP address connection, use the following procedure:

Figure 18 Static IP Mode Screen


OfficeConnect VPN Firewall Setup Wizard - Microsoft Internet Explorer
<<Back
Next>>
Cancel

Internet Settings - Static IP Mode

Please enter your settings, as provided by your ISP, below.

IP Address	
Subnet Mask	
Internet (ISP) Gateway Address	
Primary DNS Address	
Secondary DNS Address	(optional)

1 Enter your IP Address in the *IP Address* text box.

2 Enter your subnet mask in the *Subnet Mask* text box.

3 Enter your ISP Gateway address in the *Internet (ISP) Gateway Address* text box.

4 Enter your primary DNS address in the *Primary DNS Address* text box.

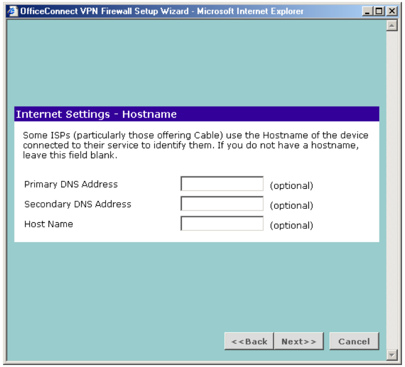
5 If your ISP provides a secondary DNS address, enter it in the *Secondary DNS Address* text box, otherwise leave the box blank.

6 Click *Next* to continue.

Dynamic IP Address Mode

To setup the Firewall for use with a dynamic IP address connection:

Figure 19 Hostname Screen


OfficeConnect VPN Firewall Setup Wizard - Microsoft Internet Explorer
<<Back
Next>>
Cancel

Internet Settings - Hostname

Some ISPs (particularly those offering Cable) use the Hostname of the device connected to their service to identify them. If you do not have a hostname, leave this field blank.

Primary DNS Address	(optional)
Secondary DNS Address	(optional)
Host Name	(optional)

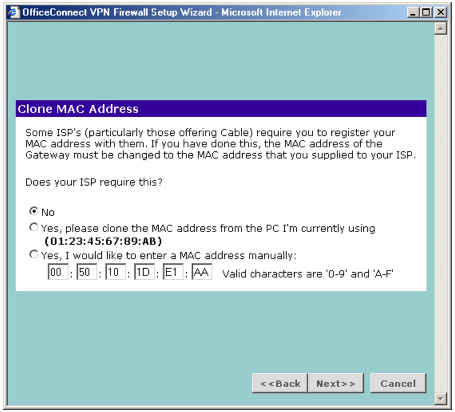
1 If your ISP requires the addresses of a Primary and Secondary DNS Server then enter them in the fields labelled *Primary DNS Address* and *Secondary DNS Address*.

If your ISP does not require one of the fields to be filled in then leave it blank.

2 If your ISP requires you to supply a host name enter it in the *Host Name* box, otherwise leave the box blank.

3 Click Next to continue to the *Clone MAC Address* screen, shown in Figure 20 below.

Figure 20 Clone MAC Address Screen



OfficeConnect VPN Firewall Setup Wizard - Microsoft Internet Explorer

Clone MAC Address

Some ISP's (particularly those offering Cable) require you to register your MAC address with them. If you have done this, the MAC address of the Gateway must be changed to the MAC address that you supplied to your ISP.

Does your ISP require this?

● No

○ Yes, please clone the MAC address from the PC I'm currently using (01:23:45:67:89:AB)

○ Yes, I would like to enter a MAC address manually:

00 : 50 : 10 : 1D : E1 : AA Valid characters are '0-9' and 'A-F'

4 If your ISP requires an assigned MAC address, select the appropriate radio button:

- *Yes, please clone the MAC address from the PC I'm currently using* if the computer you are using now is the one that was previously connected directly to the cable or DSL modem.
- *Yes, I would like to enter a MAC address manually* and manually enter the values for a MAC address if the computer you are using now was **not** previously connected directly to the cable or DSL modem.

Otherwise click *No*.

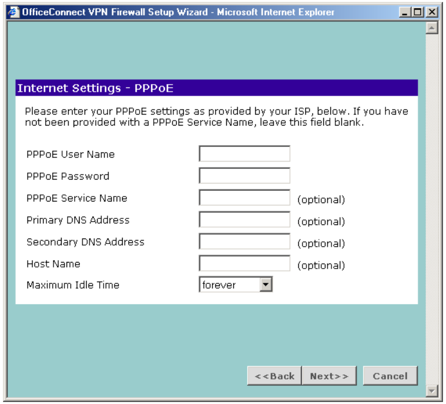
5 Click *Next* to continue

Continue at "Choosing your LAN Settings" on page 30.

PPPoE Mode

To setup the Firewall for use with a PPP over Ethernet (PPPoE) connection, use the following procedure:

Figure 21 PPPoE Screen



OfficeConnect VPN Firewall Setup Wizard - Microsoft Internet Explorer

Internet Settings - PPPoE

Please enter your PPPoE settings as provided by your ISP, below. If you have not been provided with a PPPoE Service Name, leave this field blank.

PPPoE User Name		
PPPoE Password		
PPPoE Service Name		(optional)
Primary DNS Address		(optional)
Secondary DNS Address		(optional)
Host Name		(optional)
Maximum Idle Time	forever	

1 Enter your PPP over Ethernet user name in the *PPPoE User Name* text box.

2 Enter your PPP over Ethernet password in the *PPPoE Password* text box.

If your ISP does not require one of the fields to be filled in then leave it blank.

3 If your ISP requires you to supply a PPPoE service name, enter it in the *PPPoE Service Name* text box.

4 If your ISP requires the addresses of a Primary and Secondary DNS Server then enter them in the fields labelled *Primary DNS Address* and *Secondary DNS Address*.

5 If your ISP requires you to supply a host name enter it in the *Host Name* box, otherwise leave the box blank.

6 If your ISP charges for connection time then you may wish to set the Maximum Idle time to control costs. The Maximum Idle Time is the amount of time without activity before the Firewall terminates the Internet connection. By default the value will be forever.

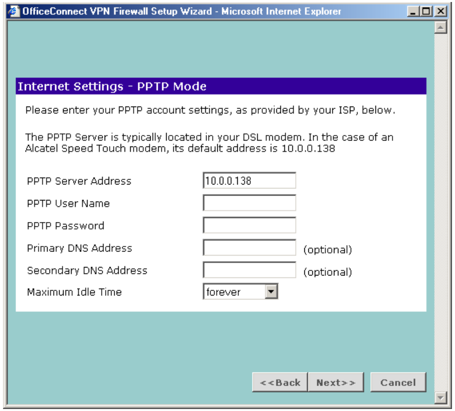
7 Click *Next* to continue.

Continue at "Choosing your LAN Settings" on page 30.

PPTP Mode

To setup the Firewall for use with a PPTP connection, use the following procedure:

Figure 22 PPTP Screen


OfficeConnect VPN Firewall Setup Wizard - Microsoft Internet Explorer
<<Back
Next>>
Cancel

Internet Settings - PPTP Mode

Please enter your PPTP account settings, as provided by your ISP, below.

The PPTP Server is typically located in your DSL modem. In the case of an Alcatel Speed Touch modem, its default address is 10.0.0.138

PPTP Server Address	10.0.0.138	
PPTP User Name		
PPTP Password		
Primary DNS Address		(optional)
Secondary DNS Address		(optional)
Maximum Idle Time	forever	

1 Enter your PPTP server address in the *PPTP Server Address* text box.

2 Enter your PPTP user name in the *PPTP User Name* text box.

3 Enter your PPTP password in the *PPTP Password* text box.

4 If your ISP requires the address of a Primary DNS Server then enter it in the field labelled *Primary DNS Address*.

5 If your ISP requires the address of a Secondary DNS Server then enter it in the field labelled *Secondary DNS Address*, otherwise leave the box blank.

6 If you wish to set maximum idle time enter it in the *Maximum Idle Time* box, otherwise leave the box blank. If your ISP charges for connection time then you may wish to set the Maximum Idle time to control costs. The Maximum Idle Time is the amount of

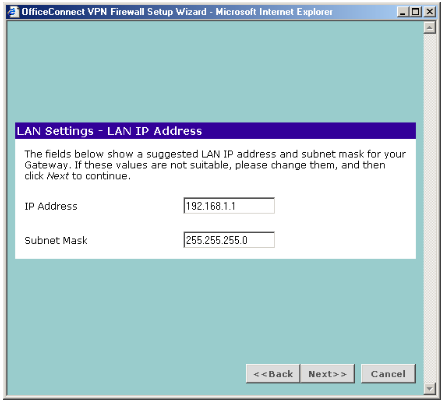
time without activity before the Firewall terminates the Internet connection. By default the value will be forever.

7 Check all your settings, and then click *Next*.

Choosing your LAN Settings

The LAN settings screen, shown in Figure 23 below, displays the Firewall's current IP address and subnet mask. If this is the first time the Wizard has been run it will display the default address and subnet mask.

Figure 23 LAN IP Address Screen


OfficeConnect VPN Firewall Setup Wizard - Microsoft Internet Explorer
<<Back
Next>>
Cancel

LAN Settings - LAN IP Address

The fields below show a suggested LAN IP address and subnet mask for your Gateway. If these values are not suitable, please change them, and then click *Next* to continue.

IP Address 192.168.1.1

Subnet Mask 255.255.255.0

1 Enter your chosen IP address for the Firewall in the *IP Address* field. This should be a private network so that it does not conflict with IP addresses on the Internet. See "Private IP Addresses" on page 85.

3Com recommends that you use the default IP address and subnet mask unless you already have a network that uses different values.

2 Enter your chosen subnet mask in the Subnet Mask field. This should be large enough to contain all your computers and other network devices. The default (255.255.255.0) allows for 254 devices including the Firewall.

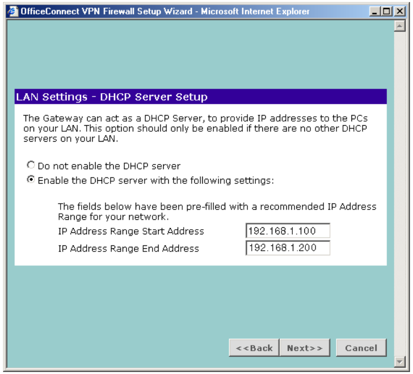
If you are going to set up an IPSec VPN with another Firewall you must set your subnet mask to 255.255.255.0. See "Configuring VPNs" *on* page 61.

Activating DHCP

The Firewall contains a Dynamic Host Configuration (DHCP) server that can automatically configure the TCP/IP settings of every computer on your network. The *DHCP Server Setup* screen is shown below.

If you intend to use the Firewall to control the permissions of individual machines on your network then you must use the Firewall's DHCP server to allocate addresses (or use static addressing). If you use another DHCP server you may get unexpected results. See "PC Privileges" *on* page 51.

Figure 24 DHCP Server Setup Screen


OfficeConnect VPN Firewall Setup Wizard - Microsoft Internet Explorer

LAN Settings - DHCP Server Setup

The Gateway can act as a DHCP Server, to provide IP addresses to the PCs on your LAN. This option should only be enabled if there are no other DHCP servers on your LAN.

○ Do not enable the DHCP server

● Enable the DHCP server with the following settings:

The fields below have been pre-filled with a recommended IP Address Range for your network.

IP Address Range Start Address	192.168.1.100
IP Address Range End Address	192.168.1.200

3Com recommends that you activate the DHCP server and leave it at the default values unless you already have a DHCP Server on your network.

- To activate the DHCP Server option, select *Enable the DHCP server with the following settings:*. The DHCP server will default to the addresses 192.168.1.100 to 192.168.1.200 if the IP address of the Firewall has been left at the default 192.168.1.1.

The Setup Wizard suggests a DHCP server address range that is valid for the LAN settings entered. If the defaults are used it will be 100 - 200. The suggested range will vary depending on the LAN IP Address *screen.*

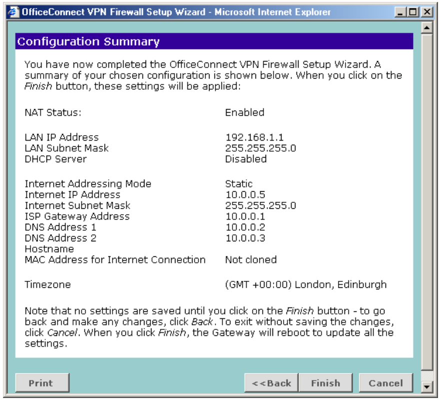
- To disable DHCP, select *Do not enable the DHCP server.*

Click *Next* when you have finished.

Viewing the Summary

When you complete the Setup Wizard, a configuration summary will display. See Figure 25 below. Verify the configuration information of the Firewall and click *Finish* to save your settings and restart the Firewall.

Figure 25 Configuration Summary Screen


OfficeConnect VPN Firewall Setup Wizard - Microsoft Internet Explorer

Configuration Summary

You have now completed the OfficeConnect VPN Firewall Setup Wizard. A summary of your chosen configuration is shown below. When you click on the *Finish* button, these settings will be applied:

NAT Status:	Enabled
LAN IP Address	192.168.1.1
LAN Subnet Mask	255.255.255.0
DHCP Server	Disabled
Internet Addressing Mode	Static
Internet IP Address	10.0.0.5
Internet Subnet Mask	255.255.255.0
ISP Gateway Address	10.0.0.1
DNS Address 1	10.0.0.2
DNS Address 2	10.0.0.3
Hostname	
MAC Address for Internet Connection	Not cloned
Timezone	(GMT +00:00) London, Edinburgh

Note that no settings are saved until you click on the *Finish* button - to go back and make any changes, click *Back*. To exit without saving the changes, click *Cancel*. When you click *Finish*, the Gateway will reboot to update all the settings.

3Com recommends that you print the Configuration Summary screen for your records.

If you have changed the IP address of your Firewall your computer will need to change its IP address to communicate with the Firewall. Reboot your computer once the Firewall has restarted to get a new address.

If want to make changes, click the *Back* button until you reach the screen which contains the settings you want to change and follow the instructions from that point.

Your Firewall is now configured.

You can start using your Firewall straight away or further configure your Firewall (see “Firewall Configuration” on page 33).

FIREWALL CONFIGURATION

This chapter describes all the options available through the Firewall configuration pages, and is provided as a reference.

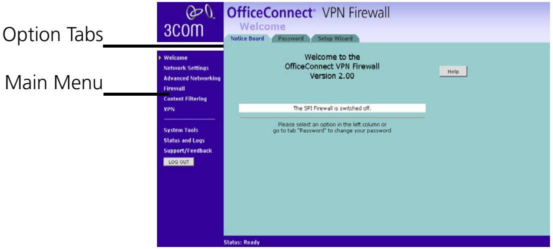
Navigating Through the Firewall Configuration Pages

To get to the configuration pages, browse to the Firewall by entering the URL in the location bar of your browser. The default URL is `http://192.168.1.1`. If you changed the Firewall LAN IP address during initial configuration, use the new IP address instead. When you have browsed to the Firewall, log in using your system password. The default password is ‘admin’.

Main Menu

At the left side of all screens is a main menu, as shown in Figure 26. When you click on a topic from the main menu, that page will appear in the main part of the screen.

Figure 26 OfficeConnect VPN Firewall Screen Layout



Welcome to the
OfficeConnect VPN Firewall
Version 2.00

The SPI Firewall is switched off.

Please select an option in the left column or
go to tab "Password" to change your password

Status: Ready

- Welcome — displays the firmware version of the Firewall and important messages on the Notice Board, allows you to change your password, and launch the Wizard.
- Network Settings — allows you to set up Internet addressing modes such as PPPoE connection, dynamic IP address allocation and static IP address settings. Also allows you to configure LAN IP address and subnet mask information, set up DHCP server parameters, and display the DHCP client list.
- Advanced Networking — allows you to set up Network Address Translation (NAT), static routing, dynamic routing, dynamic DNS and traffic shaping.
- Firewall — allows configuration of the Firewall’s firewall features: Virtual Servers, Special Applications, PC Privileges and other general security options.
- Content Filtering — allows control of access to web sites on the internet.
- VPN — allows the administrator to set up and maintain Virtual Private Network (VPN) connections.
- System Tools — allows the administrator to perform maintenance activities on the Firewall.
- Status and Logs — displays the current status and activity logs of the Firewall.
- Support/Feedback — contains a comprehensive online help system and 3Com contact information.

Option Tabs

Each menu page may also provide sub-sections which are accessed through the use of option tabs (see Figure 26 for example). To access an option, simply click on the required tab.

Getting Help

On every screen, a *Help* button is available that provides access to the context-sensitive online help system. Click this button for further assistance and guidance relating to the current screen.

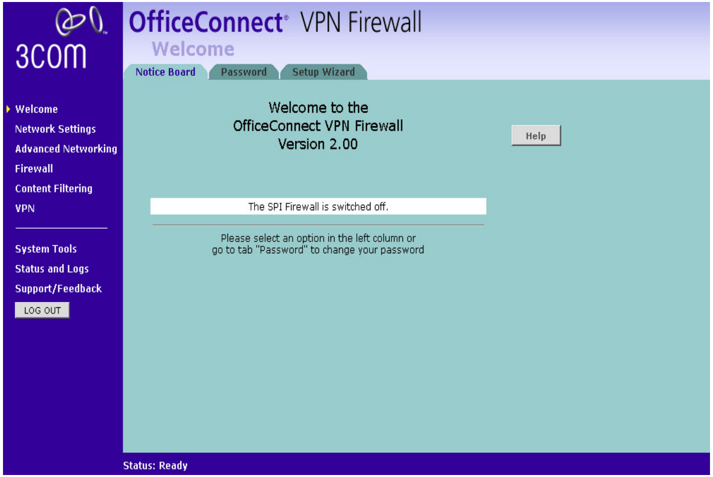
Welcome Screen

The *Welcome* section allows you to view the Notice board and to change your Password. You can also gain access to the Configuration Wizard. See "Accessing the Wizard" on page 23 for details.

Viewing the Notice Board

The Notice Board, shown in Figure 27 below, is used to display important messages. For example, you would be warned if you had disabled the firewall feature or if the LAN and Internet addresses or subnets conflicted.

Figure 27 Notice Board Screen



Welcome to the
OfficeConnect VPN Firewall
Version 2.00

The SPI Firewall is switched off.

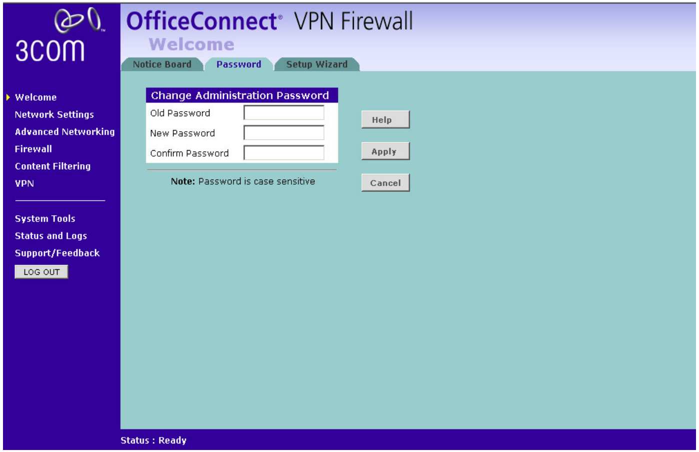
Please select an option in the left column or
go to tab "Password" to change your password

Status: Ready

Changing the Administration Password

You should change the password to prevent unauthorized access to the Administration System.

Figure 28 Password Screen



Change Administration Password

Old Password

New Password

Confirm Password

Note: Password is case sensitive

Status : Ready

To change the password:

1 Enter the current password in the *Old Password* field.

2 Enter the new password in the *New Password* field.

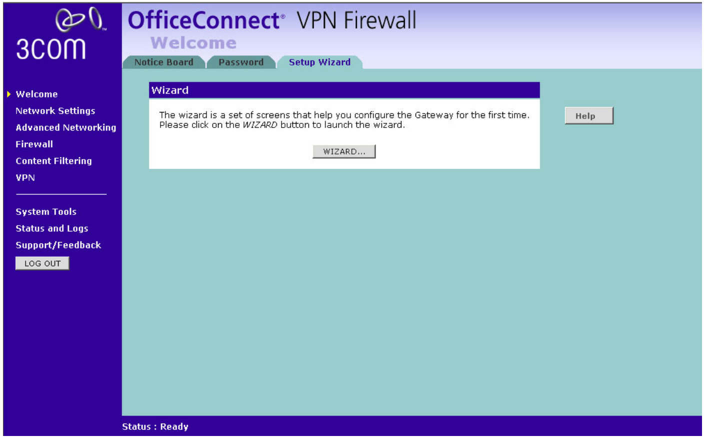
3 Enter the new password again in the *Confirm Password* field.

4 Click *Apply* to save the new password.

The password is case sensitive.

Setup Wizard

Figure 29 Wizard Screen



Wizard

The wizard is a set of screens that help you configure the Gateway for the first time. Please click on the *WIZARD* button to launch the wizard.

Status : Ready

Click the *WIZARD...* button to launch the configuration wizard. Refer to "Running the Setup Wizard" on page 23 for information on how to run the wizard.

Network Settings

The Network Settings menu allows you to view and amend your Firewall's:

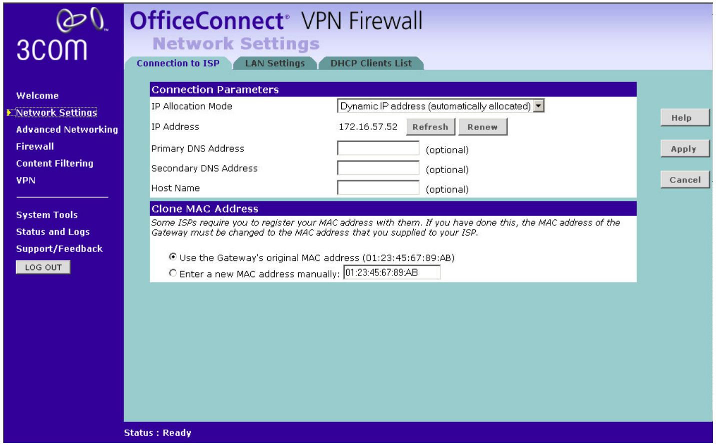
- Connection to ISP.
- LAN settings.
- DHCP Clients list.

Connection to ISP

This option, shown in Figure 30, allows you to change the method your Firewall uses to connect to your ISP. You should only need to change these settings if:

- you change your Internet connection password (PPPoE only), or
- your ISP informs you of a change in their settings or you change ISPs.

Figure 30 Connection to ISP Screen



Connection Parameters

IP Allocation Mode: Dynamic IP address (automatically allocated)

IP Address: 172.16.57.52

Primary DNS Address: (optional)

Secondary DNS Address: (optional)

Host Name: (optional)

Clone MAC Address

Some ISPs require you to register your MAC address with them. If you have done this, the MAC address of the Gateway must be changed to the MAC address that you supplied to your ISP.

● Use the Gateway's original MAC address (01:23:45:67:89:AB)

○ Enter a new MAC address manually: 01:23:45:67:89:AB

Status : Ready

Select the addressing method that your ISP uses to allocate your Firewall's Internet IP address. Choose from the options in the *IP Allocation Mode* drop-down box and the screen will refresh with options relevant to that choice.

- If you select *Static IP address (to be specified manually)* see "Configuring a Static IP Address" on page 37.
- If you select *Dynamic IP address (automatically allocated)* see "Configuring a Dynamic IP Address" on page 38.
- If you select *PPPoE (PPP over Ethernet)* see "Configuring a PPPoE connection" on page 39.
- If you select *PPTP (used by some European providers)* see "Configuring a PPTP connection" on page 40.

If you are using One to One NAT your method of connection will already be fixed to Static. To change to another method of address allocation you must first turn off One to One NAT. See "Setting up NAT" *on* page 44.

Before you can configure the Firewall, you need to know the IP information allocation method used by your ISP. There are four different ways that ISPs can allocate IP information, as described below.

When you install the Firewall, you will not need to use the PPPoE software on your PC.

When you install the Firewall, you will not need to use the dialup VPN on your PC anymore.

The Firewall will automatically 'dial on demand' PPPoE or PPTP and obtain date/time via NTP.

- **Static IP Address (DSL or Cable)**

  The ISP provides the IP addressing information for you to enter manually. To configure the Firewall you will need to know the following:

  - IP address
  - Subnet Mask
  - ISP Gateway address
  - DNS address(es)

- **Dynamic IP Address (DSL or Cable)**

  Dynamic IP addressing (or DHCP) automatically assigns the Firewall IP information. This method is popular with Cable providers. This method is also used if your modem has a built in DHCP server.

- **PPPoE (DSL only)**

  PIf the installation instructions that accompany your modem ask you to install a PPPoE client on your PC, then select this option. To configure the Firewall you will need to know the following:

  - Username
  - Password
  - Service Name (if required by your ISP)

- **PPTP (DSL or Cable)**

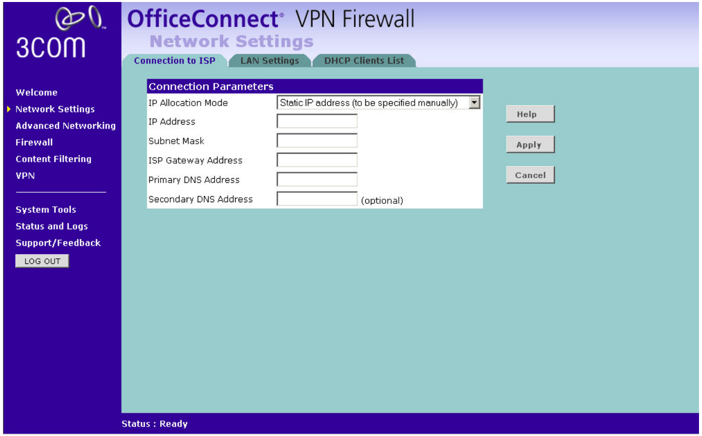
  PPTP is used by some providers, mostly in Europe. If the installation instructions that accompany your modem ask you to setup a dialup connection using a PPTP VPN tunnel then select this option. To configure the Firewall you will need to know the following:

  - Username
  - Password
  - VPN server address (usually your modem).

Configuring a Static IP Address

If your ISP has allocated you one or more static addresses you will have selected *Static IP address (to be specified manually)* as your *IP Allocation Mode*.

Figure 31 Static Address Setup Screen



Connection Parameters

IP Allocation Mode	Static IP address (to be specified manually)
IP Address	
Subnet Mask	
ISP Gateway Address	
Primary DNS Address	
Secondary DNS Address	(optional)

The following settings are required to set up Static IP address connection. Enter the values provided by your ISP:

- *IP Address* — The address allocated by your ISP for this connection.

If you have been allocated a range of IP addresses by your ISP enter the first IP address in the range.

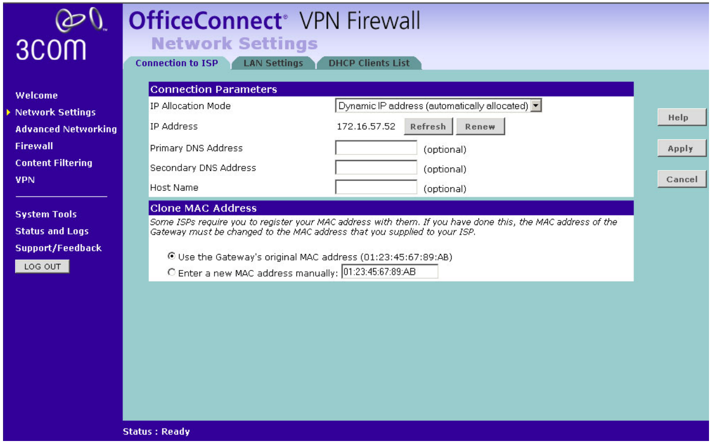
- *Subnet Mask* — The subnet mask supplied by your ISP for this connection.
- *ISP Gateway Address* — The Gateway address from your ISP to the Internet.
- *Primary DNS Address* — The address of your ISP's Domain Name Service server.
- *Secondary DNS Address* — The address of your ISP's secondary Domain Name Service server. The second server is optionally provided by an ISP in case of failure of the primary server.

Click *Apply* to save any changes you have made.

Configuring a Dynamic IP Address

If your ISP has allocated you a dynamic address using DHCP you will have selected *Dynamic IP address (automatically allocated)* as your *IP Allocation Mode*.

Figure 32 Dynamic Address Setup Screen



Connection Parameters

IP Allocation Mode	Dynamic IP address (automatically allocated)	
IP Address	172.16.57.52	
Primary DNS Address		(optional)
Secondary DNS Address		(optional)
Host Name		(optional)

Clone MAC Address

Some ISPs require you to register your MAC address with them. If you have done this, the MAC address of the Gateway must be changed to the MAC address that you supplied to your ISP.

● Use the Gateway's original MAC address (01:23:45:67:89:AB)
○ Enter a new MAC address manually: 01:23:45:67:89:AB

Status : Ready

To setup the Firewall for use with a dynamic IP address connection the following settings are configured:

- *IP Address* — The internet address allocated by your ISP for this connection is automatically configured and is not editable.

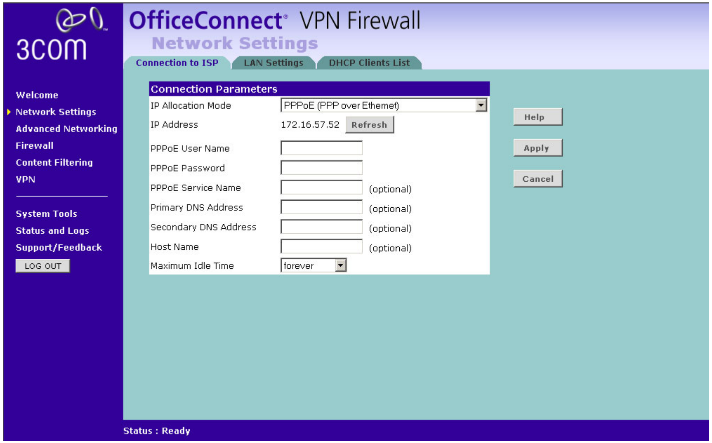
- *Subnet Mask* — The subnet for the address is automatically configured but is not displayed.
- *ISP Gateway Address* — The Gateway address from your ISP to the Internet is automatically configured but is not displayed.
- *Primary DNS Address* — If your ISP requires the address of a Primary DNS Server then enter it in the field labelled *Primary DNS Address*.
- *Secondary DNS Address* — If your ISP requires the address of a Secondary DNS Server then enter it in the field labelled *Secondary DNS Address*, otherwise leave the box blank.
- *Host Name* — The Host Name of your computer may be required by your ISP.
- *Clone MAC Address* — Your ISP may require you to have a particular MAC address. This will be the MAC address of the computer you first used to connect with your ISP.

Click *Apply* to save any changes you have made.

Configuring a PPPoE connection

If your ISP has allocated you a dynamic address using PPPoE you will have selected *PPPoE (PPP over Ethernet)* as your *IP Allocation Mode*.

Figure 33 PPPoE Setup Screen



Connection Parameters

IP Allocation Mode	PPPoE (PPP over Ethernet)	
IP Address	172.16.57.52	
PPPoE User Name		
PPPoE Password		
PPPoE Service Name		(optional)
Primary DNS Address		(optional)
Secondary DNS Address		(optional)
Host Name		(optional)
Maximum Idle Time	forever	

Status : Ready

Your ISP may need you to enter host name or PPPoE settings. To setup the Firewall for use with a PPPoE connection the following fields will need to be completed:

- *IP Address* — The internet address allocated by your ISP for this connection is automatically configured and is not editable.
- *PPPoE User Name* — The user name you use to access your ISP.

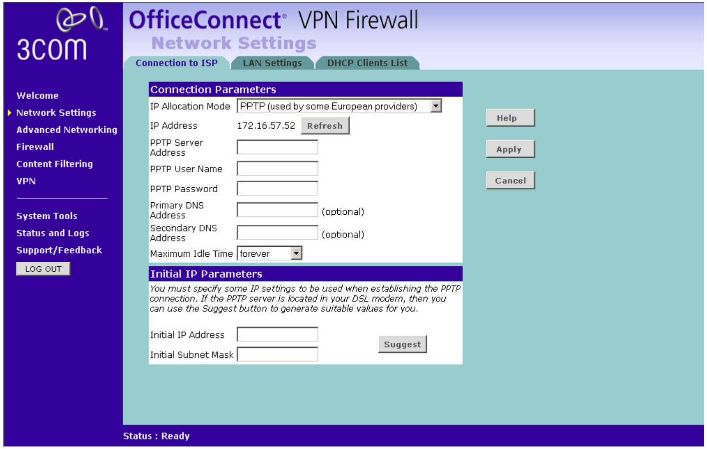
- *PPPoE Password* — The password you use to access your ISP.
- *PPPoE Service Name* — Your ISP may require you to specify a service name for your connection.
- *Primary DNS Address* — If your ISP requires the address of a Primary DNS Server then enter it in the field labelled *Primary DNS Address*.
- *Secondary DNS Address* — If your ISP requires the address of a Secondary DNS Server then enter it in the field labelled *Secondary DNS Address*, otherwise leave the box blank.
- *Host Name* — The Host Name of your computer may be required by your ISP.
- *Maximum Idle Time* — The amount of time without activity before the Firewall terminates the Internet connection.

Since the Firewall firmware contains its own PPPoE client, you no longer need to run PPPoE client software on your computer to access the Internet. You can simply start your browser and connect to the Internet immediately after setting up your cable or DSL modem.

Configuring a PPTP connection

If your ISP has allocated you a dynamic address using PPTP you will have selected *PPTP (used by some European providers)* as your *IP Allocation Mode.*

Figure 34 PPTP Setup Screen



Connection Parameters

IP Allocation Mode	PPTP (used by some European providers)
IP Address	172.16.57.52
PPTP Server Address	
PPTP User Name	
PPTP Password	
Primary DNS Address	(optional)
Secondary DNS Address	(optional)
Maximum Idle Time	forever

Initial IP Parameters

You must specify some IP settings to be used when establishing the PPTP connection. If the PPTP server is located in your DSL modem, then you can use the Suggest button to generate suitable values for you.

Initial IP Address	
Initial Subnet Mask	

Status : Ready

To setup the Firewall for use with a PPTP connection the following fields will need to be completed.

- *IP Address* — The internet address allocated by your ISP for this connection is automatically configured and is not editable.
- *PPTP Server Address* - This is typically the address of your modem.

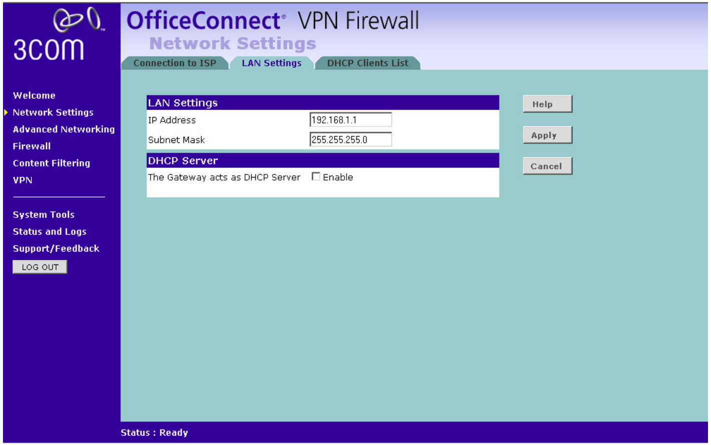
- *PPTP User Name* - The user name you use to access your ISP.
- *PPTP Password* - The password you use to access your ISP.
- *Primary DNS Address* — If your ISP requires the address of a Primary DNS Server then enter it in the field labelled *Primary DNS Address*.
- *Secondary DNS Address* — If your ISP requires the address of a Secondary DNS Server then enter it in the field labelled *Secondary DNS Address*, otherwise leave the box blank.
- *Maximum Idle Time* - The amount of time without activity before the Firewall terminates the Internet connection.

Initial IP Address and *Initial Subnet Mask* - IP settings must be used when establishing a PPTP connection. Alternatively, if the PPTP server is located in your DSL modem, click *Suggest* to select an IP address on the same subnet as the PPTP server.

LAN Settings

The *LAN Settings screen* screen allows you to change the TCP/IP settings of your Firewall and its DHCP server.

Figure 35 Unit Configuration Screen



LAN Settings

IP Address 192.168.1.1

Subnet Mask 255.255.255.0

DHCP Server

The Gateway acts as DHCP Server □ Enable

Status : Ready

Changing the LAN Settings

These settings will have been entered during the set-up wizard when the device is first used. You only need to change these if you reconfigure your network. If you make any changes, click *Apply* to save them to the Firewall.

When changing the IP Address of the Firewall choose an address that will be unique in your network and in your network's subnet. The default IP Address of the Firewall is 192.168.1.1.

When you change the IP Address of the Firewall you must reboot all computers that gain their IP address from the Firewall before they will be able to access the Internet.

If you are using static addresses for your PCs you must alter the network configuration on each PC so that they have an IP address within the same subnet as the Firewall and have their default Gateway set as the Firewall's LAN IP address.

If you reconfigure your network you may need to change your *Subnet Mask*. The *Subnet Mask* detemines how many addresses are available to your network. The default Subnet Mask is 255.255.255.0.

For example if the IP Address of your Firewall is 192.168.1.1 and the Subnet Mask of your network is 255.255.255.0 then your network can have a maximum of 254 addresses from 192.168.1.1 to 192.168.1.254 (192.168.1.0 and 192.168.1.255 are reserved by the subnet and are not available for use).

When you change the IP Address or Subnet Mask of the Firewall you should review the DHCP Server settings as described below.

Changing the DHCP Server Settings

This section allows to you enable, disable and configure the settings of the Firewall's DHCP server.

If you intend to use the Firewall to control the permissions of individual machines on your network then you must use the Firewall's DHCP server to allocate addresses (or use static addressing). If you use another DHCP server you may get unexpected results. See "PC Privileges" *on* page 51*.*

To enable the DHCP Server ensure that the *Enable* check box is ticked. To disable the DHCP Server ensure that the *Enable* check box is cleared. Click *Apply* to validate your changes.

Set the *IP Pool Start Address* and *IP Pool End Address* to the first and last address you want the Firewall to allocate to computers. The IP address pool must be contained within the subnet as defined in "Changing the LAN Settings" on page 41. The default start and end addresses are 192.168.1.100 and 192.168.1.200.

The *Local Domain Server* is set to *Domain* as default.

If you have a WINS Server on your network enter its IP address in the *WINS Server* box. The Firewall will pass this information on to all Windows PCs that obtain an address from its DHCP server.

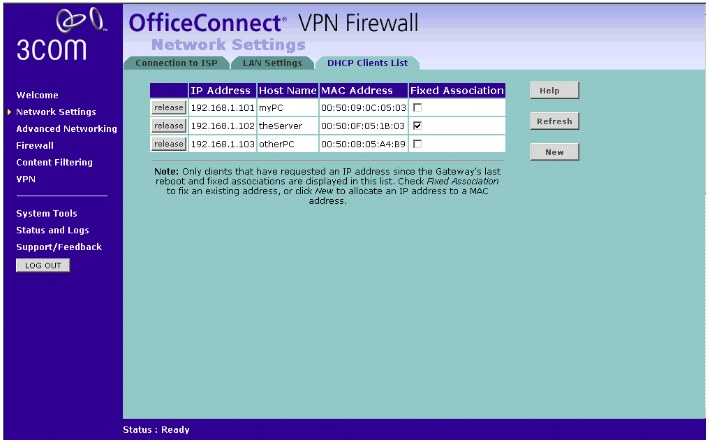
If you have a 3Com NBX Call Processor on your network enter its IP address in the *3Com NBX Call Processor* box. The 3Com NBX Call Processor acts as a switchboard for voice-over-IP phones and the Firewall will pass on this information.

If you will be using One-to-One NAT you must set up a range that is one less than the number of public addresses allocated to you by your ISP. The DHCP range must also be identical to the range specified when you set up One-to-One NAT. See "Setting up One-to-One NAT" *on* page 45*.*

DHCP Clients List

The *DHCP Clients* screen provides details of the devices that have been given IP addresses by the Firewall's DHCP server. For each device that has been granted a lease, the *IP address*, *Host Name* and *MAC address* of that device is displayed.

Figure 36 DHCP Clients Screen



	IP Address	Host Name	MAC Address	Fixed Association
release	192.168.1.101	myPC	00:50:09:0C:05:03	□
release	192.168.1.102	theServer	00:50:0F:05:1B:03	☑
release	192.168.1.103	otherPC	00:50:08:05:A4:B9	□

Note: Only clients that have requested an IP address since the Gateway's last reboot and fixed associations are displayed in this list. Check *Fixed Association* to fix an existing address, or click *New* to allocate an IP address to a MAC address.

Status : Ready

The Firewall grants leases for 7 days. If a computer does not connect for a week, its IP Address may be reused.

The Firewall will attempt to supply a computer the same lease as was issued previously, even if that lease has expired.

Expired leases are only reused when there are no free leases available. When an expired lease is re-issued the oldest lease that is not a fixed association is used.

The *Release* button allows the lease for an IP address that has been issued to a device to be cleared. If you are running short of addresses in the DHCP Pool and you know of computers that are unlikely to connect to your network soon you can release the IP address allowing it to be reallocated to another machine.

If you have spare or expired IP addresses in the pool you will not need to release addresses.

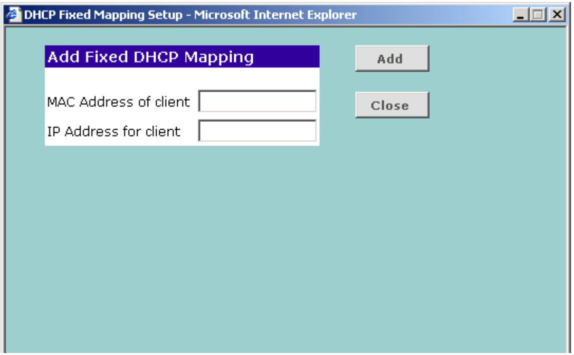
The *IP Address*, *Host Name* and *MAC Address* indicate the address that has been allocated. They identify the machine by name and by the unique number (MAC Address) of the machine's network card.

The *Fixed Association* check box allows you to freeze the relationship between an IP address and a particular machine. If you check the box for one row, that IP address will always be given out to the same machine and will not be allocated to another machine even if the lease has expired. Clear the check box to allow the address to revert back to normal behavior.

Click *Refresh* to save any changes you have made.

Click *New* to allocate an IP address to a MAC address. Click *Add* to save.

Figure 37 Fixed DHCP Mapping Screen



Add Fixed DHCP Mapping

MAC Address of client

IP Address for client

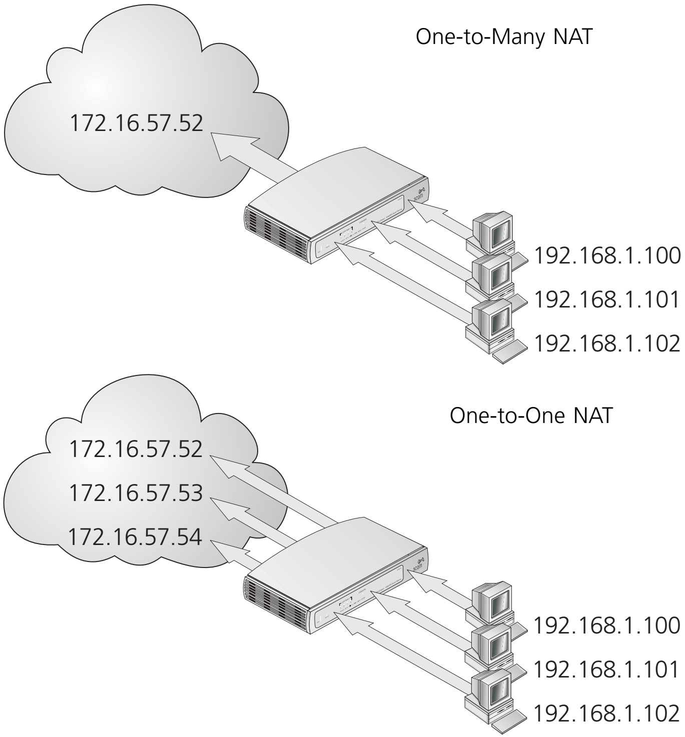
Advanced Networking

Setting up NAT

The Firewall is able to perform Network Address Translation (NAT) in one of two modes as shown in Figure 38:

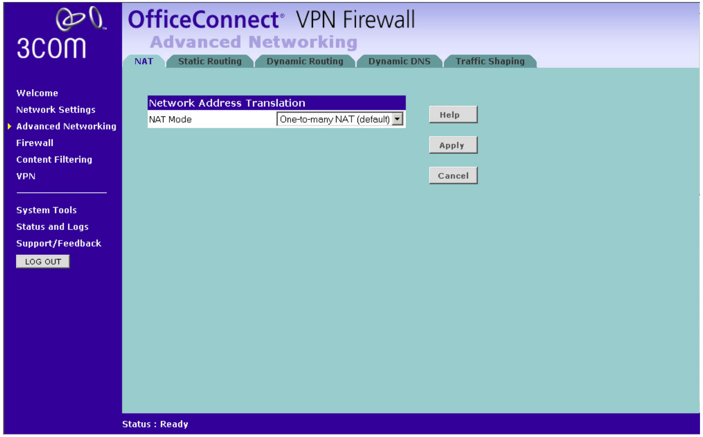
- *One-to-many NAT* — The Firewall shows only one address to the Internet.
- *One-to-one NAT* — Every address on the Internet pool is linked to an address in the LAN pool. The Firewall will respond to all the addresses in the Internet pool.

Figure 38 One-to-Many and One-to-One NAT



Setting up One-to-Many NAT

Figure 39 Network Address Translation Screen



Network Address Translation

NAT Mode: One-to-many NAT (default)

This is very easy to set up and is the Firewall's default mode. It works with any IP Allocation Mode and will map all the addresses on your LAN to the Internet address of your Firewall. To set up One-to-Many NAT:

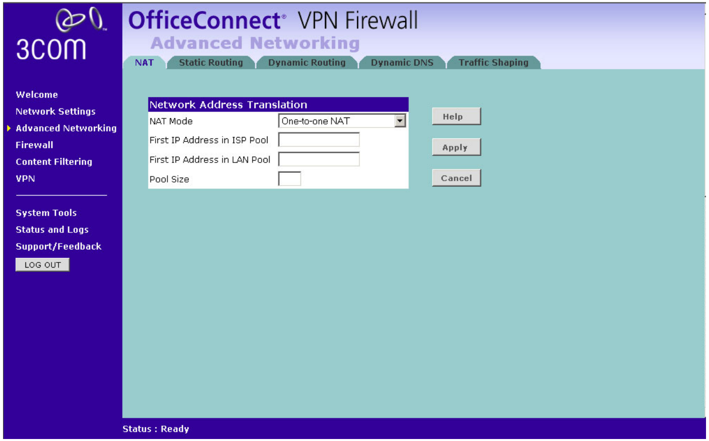
1. Select *One-to-Many NAT* from the *NAT Mode* drop-down box.
2. Click *Apply* to save your changes.

Setting up One-to-One NAT

The following criteria must be met to be able to use One-to-One NAT:

- You must have a static Internet IP address for every computer on your network plus one for the Firewall itself.
- The addresses must be in one continuous block in the same subnet
- You must have selected *Static IP Address* as your *IP Allocation Mode* and have given your Firewall the first of the Internet addresses allocated by your ISP.

Figure 40 One-to-One NAT Screen



Network Address Translation

NAT Mode: One-to-one NAT

First IP Address in ISP Pool:

First IP Address in LAN Pool:

Pool Size:

To set up One-to-One NAT:

1. Select *One-to-One NAT* from the *NAT Mode* drop-down box.
2. Enter the second address of your Internet range of addresses in the *First IP Address in ISP Pool* field.
3. Enter the first address in your LAN range of addresses to which you want to map this range in the *First IP Address in LAN Pool* field.

3Com recommends that you set your DHCP pool to the same as the range of LAN addresses used as your LAN pool.

4. Enter the number of addresses in the range into the *Pool Size* field.
5. Click *Apply* to save your changes.

Static Routing

Setting up Static Routing

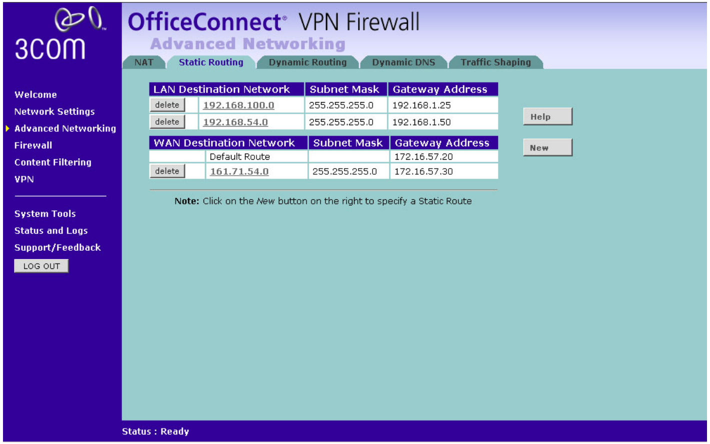
The Firewall supports up to 10 static routes in total, shared between LAN and WAN interfaces. WAN side static routes are only available if the mode of connection to your ISP is Static or Dynamic (DHCP Client mode).

To set up Static Routing:

1. Select *New* on the right side of the screen to open the Static Routing configuration dialogue box.
2. Enter the IP address of the Destination Network (e.g. 192.168.20.0).
3. Enter the IP address of the Subnet Mask (e.g. 255.255.255.0).
4. Enter the IP address of the Gateway Address (e.g. 192.168.1.25).
5. Select the location of the Destination Network in relation to the Firewall (either LAN or WAN) from the Location drop down box.
6. Click *Apply* to save your changes.

The list of all routes (static and dynamic) are listed in the Status and Logs section.

Figure 41 Static Routing Screen



	LAN Destination Network	Subnet Mask	Gateway Address
delete	192.168.100.0	255.255.255.0	192.168.1.25
delete	192.168.54.0	255.255.255.0	192.168.1.50

	WAN Destination Network	Subnet Mask	Gateway Address
	Default Route		172.16.57.20
delete	161.71.54.0	255.255.255.0	172.16.57.30

Note: Click on the *New* button on the right to specify a Static Route

Status : Ready

Dynamic Routing

The Firewall provides support for RIPv1, RIPv2 or both for each interface, for sending and receiving data, LAN routes are sent on the LAN subnet, and WAN routes are sent on the WAN subnet.

From the Dynamic Routing screen you can enable the Firewall to automatically adjust to physical changes in the networks layout. Using the RIP protocols, the Firewall determines the network packets' route based on the fewest number of hops between the source and the destination. The RIP protocol regularly broadcasts routing information to other devices on the network.

Setting up Dynamic Routing

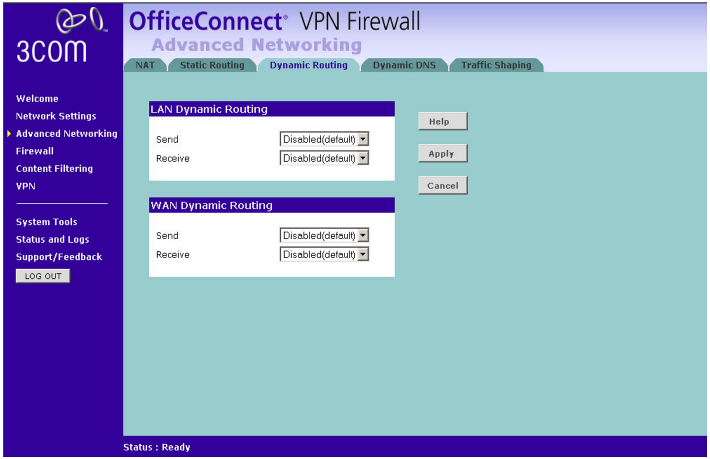
To set up Dynamic Routing:

1 Select a Service from the pull-down list.

2 Click *Apply* to save your changes.

The list of all routes (static and dynamic) are listed in the Status and Logs section.

Figure 42 Dynamic Routing Screen



LAN Dynamic Routing

Send: Disabled(default)
Receive: Disabled(default)

WAN Dynamic Routing

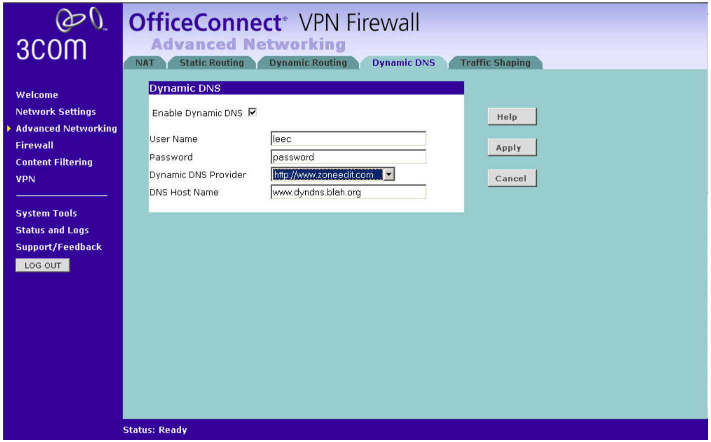
Send: Disabled(default)
Receive: Disabled(default)

Status : Ready

Dynamic DNS

The Firewall provides a list of dynamic DNS providers for you to choose from. Dynamic DNS is disabled by default.

Figure 43 Dynamic DNS Screen



Dynamic DNS

Enable Dynamic DNS ☑

User Name	leec
Password	password
Dynamic DNS Provider	http://www.zoneedit.com
DNS Host Name	www.dyndns.blah.org

Status: Ready

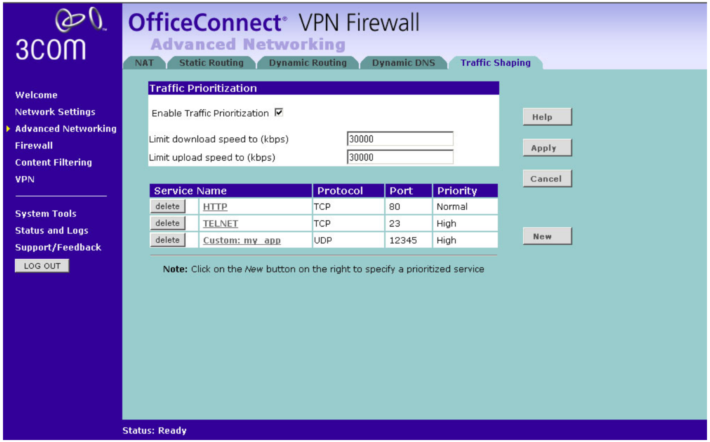
Setting up Dynamic DNS

To set up Dynamic DNS:

1. Check the Enable Dynamic DNS box to open the Dynamic DNS settings screen.
2. Enter your Username and password.
3. Select a Dynamic DNS provider from the pull-down list.
4. Enter the DNS Host name.
5. Click *Apply* to save your changes.

Traffic Shaping

Figure 44 Traffic Shaping Screen



Traffic Prioritization

Enable Traffic Prioritization ☑

Limit download speed to (kbps)	30000
Limit upload speed to (kbps)	30000

	Service Name	Protocol	Port	Priority
delete	HTTP	TCP	80	Normal
delete	TELNET	TCP	23	High
delete	Custom: my_app	UDP	12345	High

Note: Click on the *New* button on the right to specify a prioritized service

Status: Ready

Setting up Traffic Shaping

To set up Traffic Shaping:

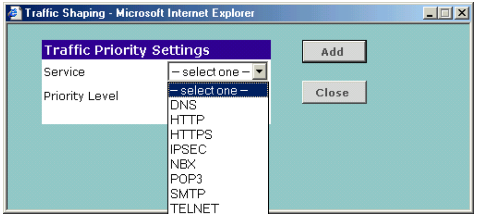
1. Check the Enable Traffic Prioritization box to display the Traffic Shaping options.
2. Check that the figure in the *Limit upload speed to (kbps)* field is slightly lower than your broadband upload and download speed. This information is supplied by your ISP.

Setting the value too low will reduce your Firewall's throughput. However if it is set higher than your connection speed, the feature will have no noticeable effect.

3 Select a Service Name or click *New* to open the Traffic Priority settings screen. (Figure 45).

4 Select a *Service* from the pull-down list.

Figure 45 Traffic Priority Settings screen



Traffic Shaping - Microsoft Internet Explorer

Traffic Priority Settings

Service: – select one –

Priority Level

If you select *Custom* in the Service box, the screen shown in Figure 46 displays. Steps 5 to 7 apply only if you select the *Custom* Service.

5 Enter a name for the custom service in the *Custom Service Name* box.

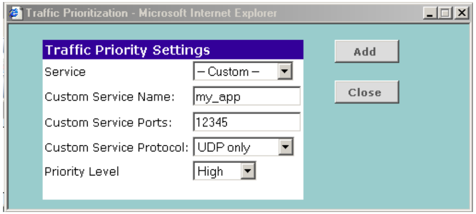
6 Enter a single port number in the *Custom Service Ports* box.

7 Select a *Custom Service Protocol* from the pull-down list.

8 Select a *Priority Level* from the pull-down list.

9 If you are adding a new service, click *Add*, or if you are editing an existing service click *Apply* to save your changes and return to the Traffic Shaping screen.

Figure 46 Custom Traffic Priority settings screen



Traffic Prioritization - Microsoft Internet Explorer

Traffic Priority Settings

Service: – Custom –

Custom Service Name: my_app

Custom Service Ports: 12345

Custom Service Protocol: UDP only

Priority Level: High

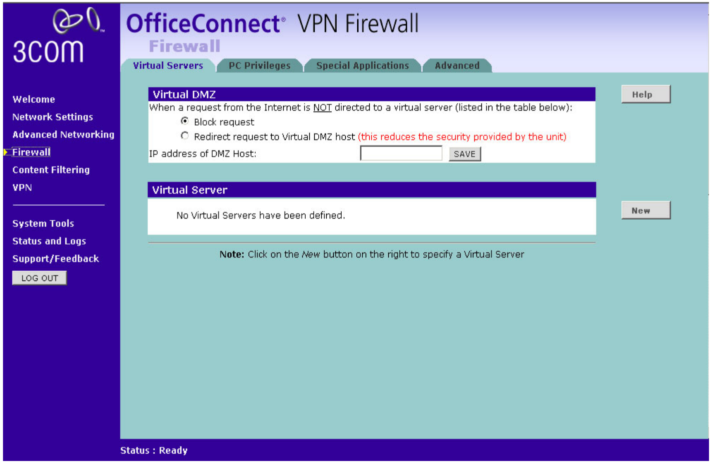
Configuring the Firewall

On the main frame of the *Firewall* setup screen is a menu with four tabs: *Virtual Servers*, *PC Privileges*, *Special Applications*, and *Advanced*. These enable you to set the access to and security of your network.

The Virtual Servers Menu

Selecting the *Firewall* option on the main menu displays the *Virtual Servers* screen. (Figure 47)

Figure 47 Virtual Servers Screen



Virtual DMZ

When a request from the Internet is NOT directed to a virtual server (listed in the table below):

● Block request

○ Redirect request to Virtual DMZ host (this reduces the security provided by the unit)

IP address of DMZ Host: ________

Virtual Server

No Virtual Servers have been defined.

Note: Click on the *New* button on the right to specify a Virtual Server

Status : Ready

Creating a Virtual DMZ

A virtual DMZ (De-Militarized Zone) Host is a computer on your network with reduced protection provided by the firewall. This feature allows a single computer to be exposed to 2-way communication from outside of your network in One-to-Many NAT mode. The PC is still protected against DoS and hacker attacks.

CAUTION: *This feature should be used only if the Virtual Server or Special Applications options do not provide the level of access needed for certain applications.*

To specify one of your computers as a DMZ host, select *Redirect Request to Virtual DMZ Host* and enter the IP address of the computer in the *IP Address of DMZ Host* text box, and then click *SAVE*.

Creating a Virtual Server

Activating and configuring a virtual server allows one or more of the computers on your network to function as an Internet service host. For example, one of your computers could be configured as an FTP host, allowing others outside of your office network to download files of your choosing. Or, if you have created a Web site, you can configure one of your computers as a Web server, so that others can view your Web site.

If you are using One-to-Many NAT you can only have one server of each type on your network. To have more than one server of a type (for example more than one web server) visible to the Internet you must be using One-to-One NAT.

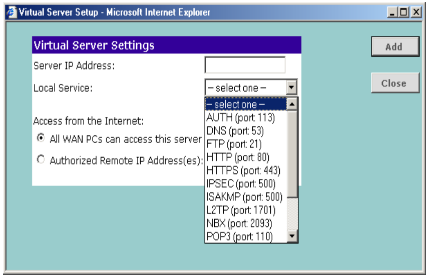
To configure a virtual server:

1 Click *New* on the right side of the screen to open the *Virtual Server Settings* dialogue box. (Figure 47)

2 Enter the IP address of the computer in the *Server IP Address* text box.

3 Select the Service from the pull-down list. (Figure 48)

Figure 48 Virtual Servers Settings Screen



Virtual Server Setup - Microsoft Internet Explorer

Virtual Server Settings

Server IP Address:

Local Service: – select one –

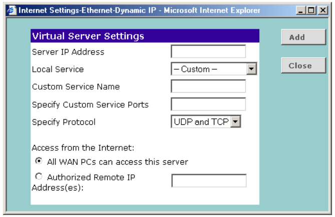
Access from the Internet:

● All WAN PCs can access this server

○ Authorized Remote IP Address(es):

If you select *Custom,* the screen shown in Figure 49 displays. Specify a suitable name for the service and then enter the port numbers required for that service. If a service requires more than one port number enter the multiple ports as a comma separated list or a range e.g. 51,52,54-59.

Figure 49 Custom Setup Screen



Internet Settings-Ethernet-Dynamic IP - Microsoft Internet Explorer

Virtual Server Settings

Server IP Address

Local Service – Custom –

Custom Service Name

Specify Custom Service Ports

Specify Protocol UDP and TCP

Access from the Internet:

● All WAN PCs can access this server

○ Authorized Remote IP Address(es):

4 Select either *All WAN PCs can access this server*, or *Authorized Remote IP Address(es)*. If you select *Authorized Remote IP Address(es),* you must specify an IP address or a range of addresses. For example, 162.223.41.12-162.223.41.15 gives access to all IP addresses in this range.

5 Click *Add* to save the settings.

PC Privileges

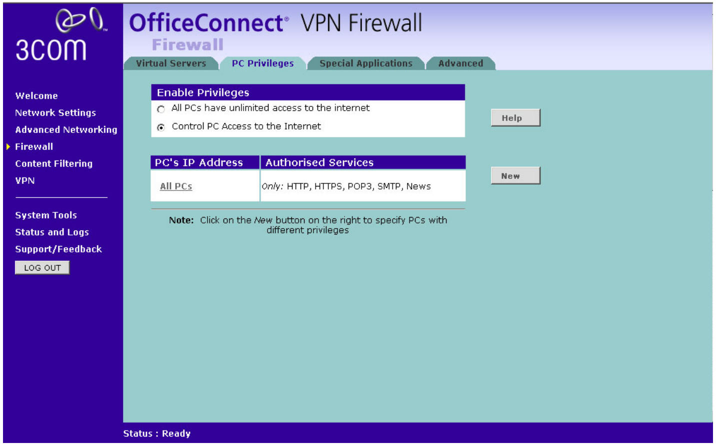
Access from the local network to the Internet can be controlled on a PC-by-PC basis. In the default configuration the Firewall will allow all connected PCs unlimited access to the Internet.

PC Privileges allows you to assign different access rights for different computers on your network, restricting this access and controlling your users' access to outside resources.

Select *PC Privileges* to display the PC Privileges setup screen. This is shown in Figure 50 below.

The Firewall's DHCP server has been enhanced to support PC Privileges. If you want to control access to the Internet on a user by user basis then you should either use the Firewall's DHCP server or static addressing.

Figure 50 PC Privileges Screen



Enable Privileges

○ All PCs have unlimited access to the internet

● Control PC Access to the Internet

PC's IP Address	Authorised Services
All PCs	*Only:* HTTP, HTTPS, POP3, SMTP, News

Note: Click on the *New* button on the right to specify PCs with different privileges

Status : Ready

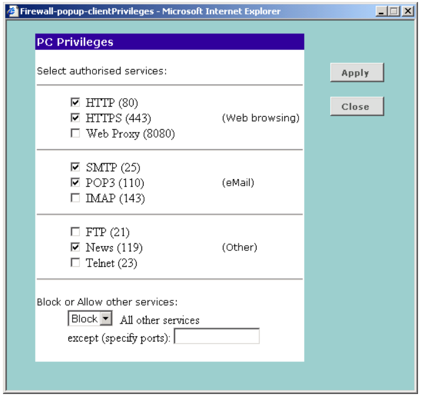
To use access control for all computers:

1 Click the *Control PC Access to the Internet* radio button.

2 Click on *All PCs* to setup the access rights for all computers connected to the Firewall.

3 Check the box of a service to authorize it. Clear the box to deny the service. See Figure 51.

Figure 51 All PCs Setup Screen


Firewall-popup-clientPrivileges - Microsoft Internet Explorer
Apply
Close

PC Privileges

Select authorised services:

☑ HTTP (80)
☑ HTTPS (443) (Web browsing)
☐ Web Proxy (8080)

☑ SMTP (25)
☑ POP3 (110) (eMail)
☐ IMAP (143)

☐ FTP (21)
☑ News (119) (Other)
☐ Telnet (23)

Block or Allow other services:

Block All other services

except (specify ports):

4 Either:

- Enter the additional services that you wish to allow in the *except (specify ports)* box and set the drop down box to *Allow*.
- Enter the services that you wish to deny in the *except (specify ports)* box and set the drop down box to *Deny*.

Enter multiple ports as either a comma separated list e.g. 101, 105, 107, or as a range, e.g. 101-107.

5 Click *Apply* to save the settings.

To assign different access rights for different computers:

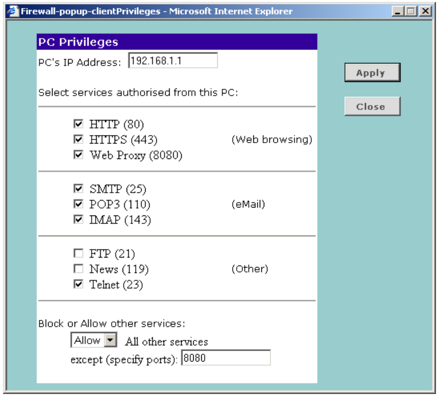
1 Click the *Control PC Access to the Internet* radio button.

2 Click *New* to display the *PC Privileges* setting screen.

3 Enter the IP address of the computer in the *PC's IP Address* text box.

4 Check the box of a service to authorize it. Clear the box to deny the service. See Figure 52.

Figure 52 PC Privileges Setup Screen



Firewall-popup-clientPrivileges - Microsoft Internet Explorer

PC Privileges

PC's IP Address: 192.168.1.1

Select services authorised from this PC:

☑ HTTP (80)
☑ HTTPS (443) (Web browsing)
☑ Web Proxy (8080)

☑ SMTP (25)
☑ POP3 (110) (eMail)
☑ IMAP (143)

□ FTP (21)
□ News (119) (Other)
☑ Telnet (23)

Block or Allow other services:
Allow All other services
except (specify ports): 8080

5 Either:

- Enter the additional services that you wish to allow in the *except (specify ports)* box and set the drop down box to *Allow*.
- Enter the services that you wish to deny in the *except (specify ports)* box and set the drop down box to *Deny*.

Enter multiple ports as either a comma separated list e.g. 101, 105, 107, or as a range, e.g. 101-107.

6 Click *Apply* to save the settings.

Example: Allowing only web and E-mail access.

To allow web and E-mail access and block all other services across the Firewall's firewall:

- Ensure that the *Control PC Access to the Internet* radio button is selected.
- Click on *All PCs* to pop up the *PC Privileges* window.
- Ensure that the *Email (110,25)* and *Web (80)* boxes are checked and that other check-boxes are left cleared.
- Set the *Block or Allow other services:* drop-down box to *Block* other services.

For the purposes of this example, your users also need to access a test server on port 8000. To allow this:

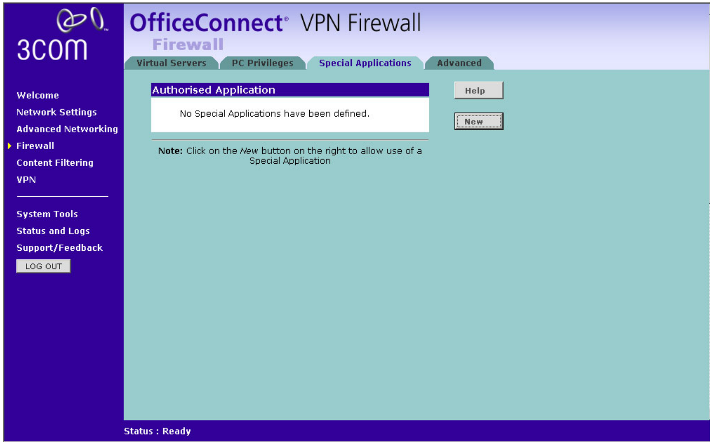
- Enter the number *8000* in the *except (specify ports):* box.
- Click *Apply* to save your changes and close the *PC Privileges* window.

VPN connections to other networks are unaffected by settings in PC Privileges. To allow or deny VPN connections to other networks see "Configuring VPNs" *on* page 61.

Special Applications

Select *Special Applications* tab to display the *Authorized Application* setup screen. See Figure 53 below.

Figure 53 Special Applications Screen



Authorised Application

No Special Applications have been defined.

Note: Click on the *New* button on the right to allow use of a Special Application

Status : Ready

Some software applications need a connection to be started from the Internet — an act that is usually blocked by the Firewall's firewall.

So that these special applications can work properly and are not blocked, the firewall needs to be told about them. In each instance there will be an outgoing trigger which tells the Firewall's firewall that the application has started and to allow the incoming connections.

Each defined Special Application only supports a single computer user and any incoming ports opened by a Special Application trigger will be closed after 20 minutes of inactivity for TCP/IP connections or 10 for UDP/IP connections.

For each special application configured by the Firewall, a row is added to the table. Each row contains the following items:

- *Delete* button — Deletes the special application on that row. This will prevent the Firewall's firewall from opening to that connection.
- *Name* — Each special application is named. This name is not used by the Firewall and is only to enable you to identify the connection. Clicking the name of a connection displays the *Special Application Setup* screen. See "Adding and Editing Special Applications" below.
- *Trigger Port* — This is the TCP/IP port number that the Firewall uses to recognize that the application has started.

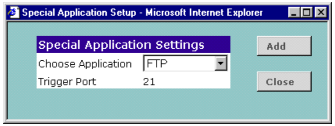
Additionally there are two buttons outside the table:

- *Help* — displays the online help page for this screen.
- *New* — creates a new special application. See "Adding and Editing Special Applications" below.

Adding and Editing Special Applications

1. Click on the *New* button to create a new special application or on the name of a special application to edit the settings for that application.

Figure 54 Special Application Settings Screen



Special Application Setup - Microsoft Internet Explorer

Special Application Settings

Choose Application: FTP

Trigger Port: 21

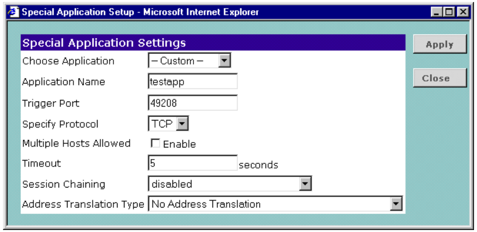
2. Select the applications from the *Choose Application* drop-down box. See Figure 54. If the application you want to define is not in the list select *Custom* and see "Creating Custom Special Applications" below.
3. Click *Add* to add the special application to the list of protocols or *Close* to abort your selection and return to the *Special Applications* screen.

Depending on the settings you have made in PC Privileges the Special Application you have defined may not be allowed across the Firewall. See "PC Privileges" *on* page 51.

Creating Custom Special Applications

If your special application is not listed in the *Choose Application* drop-down box you can still configure it manually. Select Custom from the *Choose Application* drop-down box and the Special Application Setup Screen gains the extra fields needed to describe a custom special application. These are shown in Figure 55 below.

Figure 55 Custom Special Applications Setup Screen



Special Application Setup - Microsoft Internet Explorer

Special Application Settings

Choose Application: – Custom –

Application Name: testapp

Trigger Port: 49208

Specify Protocol: TCP

Multiple Hosts Allowed: □ Enable

Timeout: 5 seconds

Session Chaining: disabled

Address Translation Type: No Address Translation

- *Application Name* — Each special application is named and will detect the ports that need to be opened so you do not need to specify them. This name is not used by the Firewall and is only to enable you to identify the connection.
- *Trigger Port* — This is the TCP/IP port number that the Firewall uses to recognize the outgoing packet that starts special application session. Your application provider can provide you with this information.

The Firewall allows Trigger Ports that are a single value or a range of values but not a list. So '6599' and '6577-6587' are both valid but '6577, 6579, 6582' is not.

- *Specify Protocol* — Select the protocol (TCP or UDP) that your special application uses. Your application provider can provide you with this information.
- *Multiple Hosts Allowed* — If your application provider uses more that one IP address during a session or responds from an address different to the one you use to start the special application then you must ensure that the *Multiple Hosts Allowed* box is checked. Otherwise leave it clear. Your application provider can provide you with this information.

CAUTION: *Selecting* Multiple Hosts Allowed *weakens the security that your Firewall's firewall is able to provide and should only be used if the special application requires it.*

- *Timeout* — Enter the number of seconds the Firewall should wait for the first reply from the special application server before it abandons the connection.

The default Timeout is three seconds. If you find that connections are being dropped enter a higher value.

- *Session Chaining* — Some special applications need to take control of a session. If the special application you wish to run requires this, ensure that *Session Chaining* is enabled, otherwise ensure that it is disabled.

CAUTION: *Allowing* Session Chaining *weakens the security that your Firewall is able to provide and should only be used if the special application requires it.*

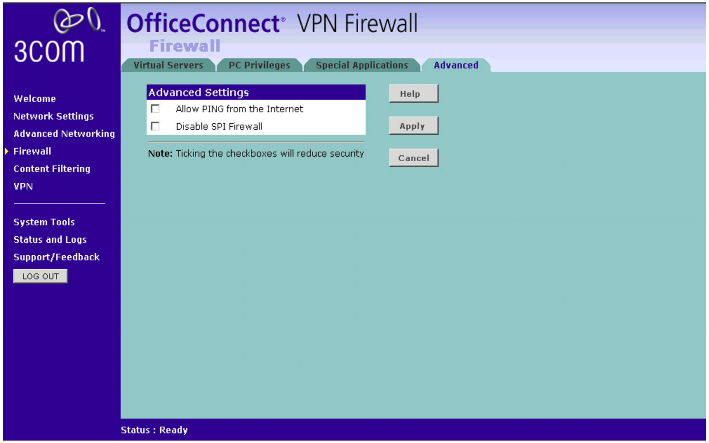
- *Address Translation Type* — If your special application provider embeds IP addresses in TCP or UDP packets you will have to enable address translation on the appropriate protocol type. Your application provider can provide you with this information.

When you have configured your special application click *Add* to save your changes or *Close* to quit without making any changes.

Advanced

Select *Advanced* to display the Advanced Settings screen. See Figure 56 below.

Figure 56 Advanced Settings Screen



Advanced Settings

☐ Allow PING from the Internet

☐ Disable SPI Firewall

Note: Ticking the checkboxes will reduce security

Status : Ready

The Internet connects millions of computer users throughout the world. The vast majority of the computer users on the Internet are friendly and have no intention of breaking into, stealing from, or damaging your network. However, there are hackers who may try to break into your network.

The options on this screen enable you to allow PING from the internet and to disable the firewall as shown below:

- *Allow PING from the Internet* — PING is a utility, which is used to determine whether a device is active at the specified IP address. PING is normally used to test the physical connection between two devices, to ensure that everything is working correctly.

  By default the Firewall has PING disabled so that it does not respond to PING requests. This makes the device more difficult to find on the Internet and less prone to attack.

  This feature is enabled by clicking on the check box so that a tick can be seen and then selecting *Apply*.

3Com recommends that you leave Allow PING from the Internet disabled as this provides greater security.

- *Disable SPI Firewall* — The firewall feature detects attack patterns used by hackers on the Internet and once detected will block their access to your network. The firewall feature is disabled by clicking on the check box so that a tick can be seen and then clicking *Apply*.

3Com recommends that you leave the firewall feature enabled (checkbox cleared) for normal use. You may wish to turn it off for diagnostic purposes.

Content Filtering

The Content Filtering menu allows you to control access to web sites on the internet. You can do this using one or a combination of the following:

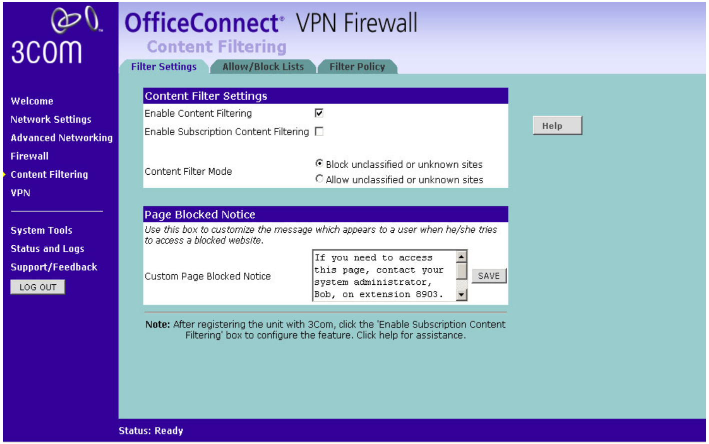
- Local Content Filtering — You can enter the URLs, IP addresses or keywords of sites that are allowed to be viewed or blocked.
- Subscription Content Filtering — You can choose which sites are allowed to be viewed or blocked depending on their content. This is a subscription-based service which requires registration of your unit on the 3Com website; contact your supplier for more information, or visit:

  `http://www.3com.com`
- Filter Policy — You can exclude certain PCs on the LAN from content filtering by specifying their IP addresses.

Filter Settings

Check *Enable Content Filtering* to display the *Filter Settings* tab. See Figure 57 below.

Figure 57 Filter Settings screen



Content Filter Settings

Enable Content Filtering ☑

Enable Subscription Content Filtering □

Content Filter Mode ● Block unclassified or unknown sites ○ Allow unclassified or unknown sites

Page Blocked Notice

Use this box to customize the message which appears to a user when he/she tries to access a blocked website.

Custom Page Blocked Notice

```
If you need to access
this page, contact your
system administrator,
Bob, on extension 8903.
```

SAVE

Note: After registering the unit with 3Com, click the 'Enable Subscription Content Filtering' box to configure the feature. Click help for assistance.

Status: Ready

Using the Filter Settings screen, you can:

- Check *Enable Subscription Content Filtering* to display the *Subscription Filtering* menu tab. Refer to "Subscription Filtering" on page 58.
- Select the content filter mode by checking *Block unclassified or unknown sites* or *Allow unclassified or unknown sites*. When the content filter mode is set to *Block unclassified or unknown sites* only allowed sites can be viewed.
- Customize the message which appears to a user when he/she tries to access a blocked website by typing it in the *Custom Page Blocked Notice* field. Click *Save* to save your changes.

Subscription Filtering

Subscription filtering allows you to choose which sites are viewed or blocked depending on their content. This is a subscription-based service which requires registration of your unit on the 3Com website. Contact your supplier for more information, or visit:

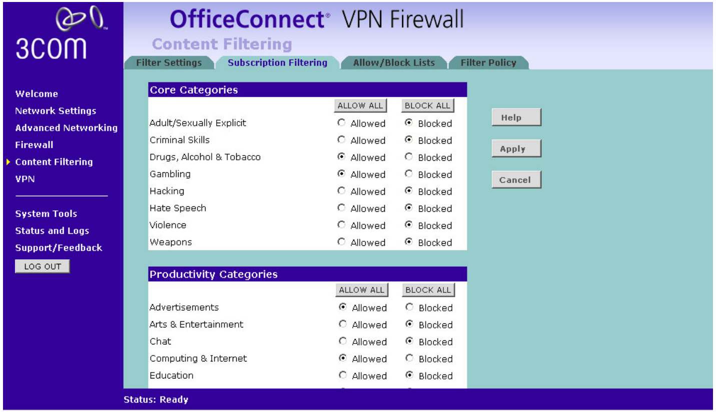
`http://www.3com.com`

To enable subscription filtering, check *Enable Content Filtering* on the *Filter Settings* screen and then check *Enable Subscription Content Filtering*.

To configure Subscription Filtering, select the *Subscription Filtering* tab to display the *Subscription Filtering* screen. See Figure 58 below.

If the Subscription Filtering tab is not displayed, check Enable Content Filtering on the Filter Settings screen, and then check Enable Subscription Content Filtering.

Figure 58 Subscription Filtering Screen



Core Categories

	ALLOW ALL	BLOCK ALL
Adult/Sexually Explicit	○ Allowed	● Blocked
Criminal Skills	○ Allowed	● Blocked
Drugs, Alcohol & Tobacco	● Allowed	○ Blocked
Gambling	● Allowed	○ Blocked
Hacking	○ Allowed	● Blocked
Hate Speech	○ Allowed	● Blocked
Violence	○ Allowed	● Blocked
Weapons	○ Allowed	● Blocked

Productivity Categories

	ALLOW ALL	BLOCK ALL
Advertisements	● Allowed	○ Blocked
Arts & Entertainment	○ Allowed	● Blocked
Chat	○ Allowed	● Blocked
Computing & Internet	● Allowed	○ Blocked
Education	○ Allowed	● Blocked

Status: Ready

To allow or block categories:

1 Either:

- Check the *Allowed* or *Blocked* box against each Core and Productivity category as required.

or:

- Click *Allow All* to set all categories to Allowed, or *Block All* to set all categories to Blocked.

2 Click *Apply* to save your changes.

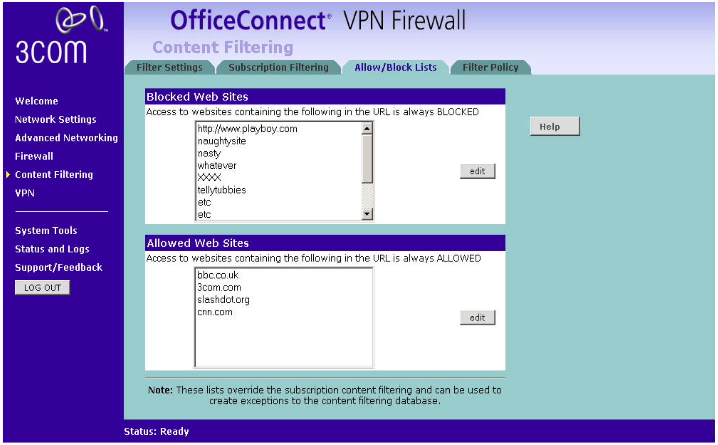
The list of websites on the Allow/Block Lists screen override any choices made on the Subscription Filtering screen.

Allow/Block Lists

To set Allow/Block lists, check *Enable Content Filtering* on the *Filter Settings* screen and check the required content filter mode. Select the *Allow/Block Lists* tab to display the *Allow/Block Lists* screen.

If *Enable Subscription Content Filtering* is checked on the *Filter Settings* screen, the screen shown in Figure 59 below is displayed.

Figure 59 Allow/Block Lists screen



Blocked Web Sites

Access to websites containing the following in the URL is always BLOCKED

http://www.playboy.com
naughtysite
nasty
whatever
xxxx
tellytubbies
etc
etc

Allowed Web Sites

Access to websites containing the following in the URL is always ALLOWED

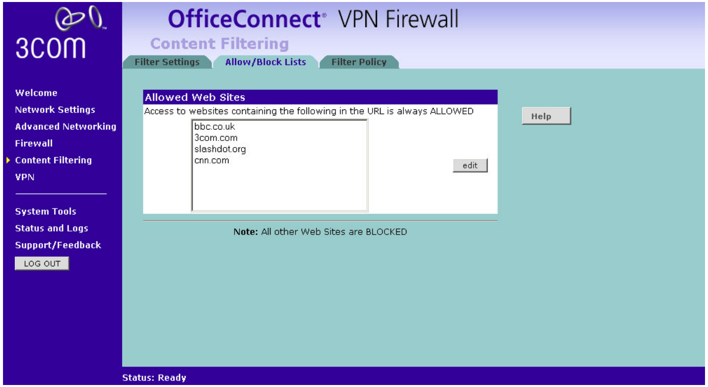
bbc.co.uk
3com.com
slashdot.org
cnn.com

Note: These lists override the subscription content filtering and can be used to create exceptions to the content filtering database.

Status: Ready

If *Enable Subscription Content Filtering* is not checked on the *Filter Settings* screen, the screen shown in Figure 60 below is displayed.

Figure 60 Allow/Block Lists screen



Allowed Web Sites

Access to websites containing the following in the URL is always ALLOWED

bbc.co.uk
3com.com
slashdot.org
cnn.com

Note: All other Web Sites are BLOCKED

To set up a list of sites:

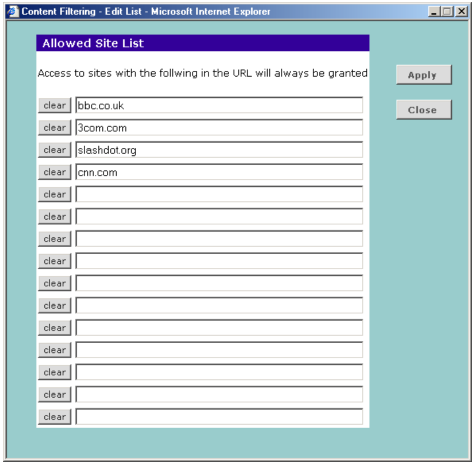
1 Click *Edit* to display the *Content Filtering Edit List* screen. See Figure 61 below.

2 Enter the URLs, IP addresses or keywords of sites that are allowed to be viewed or blocked depending on the chosen content filtering mode.

3 Click *Apply* to save your changes.

The list of websites on the Allow/Block Lists screen override any choices made on the Subscription Filtering screen.

Figure 61 Content Filtering Edit List Screen



Allowed Site List

Access to sites with the follwing in the URL will always be granted

bbc.co.uk
3com.com
slashdot.org
cnn.com

Filter Policy

To set up Filter Policy, check *Enable Content Filtering* on the *Filter Settings* screen. Select the *Filter Policy* tab to display the *Filter Policy* screen. See Figure 62 below.

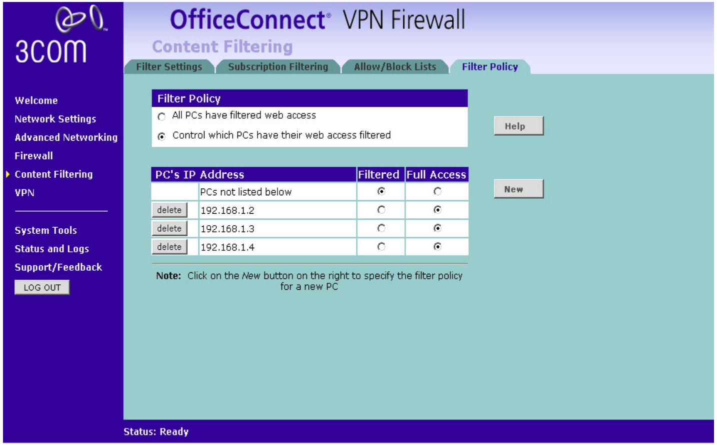
To set up the same content filtering policy for all PCs on the network, check the *All PCs have filtered web access* box.

To set up which PCs have the content filtered:

1 Check the *Control which PCs have their web access filtered* box.

2 Check the *filtered* or *full access* box against each PC as required. See Figure 62 below.

Figure 62 Filter Policy Settings Screen



Filter Policy

○ All PCs have filtered web access

● Control which PCs have their web access filtered

	PC's IP Address	Filtered	Full Access
	PCs not listed below	●	○
delete	192.168.1.2	○	●
delete	192.168.1.3	○	●
delete	192.168.1.4	○	●

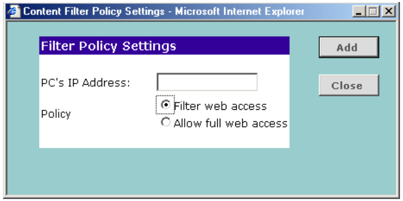
Note: Click on the *New* button on the right to specify the filter policy for a new PC

Status: Ready

To set up a New Filter Policy:

1. Click *New* to open the *Content Filter Policy Settings* screen.
2. Enter the PC's IP address.
3. Check a Policy for that PC.
4. Click *Add* to set up the new filter.

Figure 63 Content Filter Policy Settings Screen


Content Filter Policy Settings - Microsoft Internet Explorer
Add
Close

Filter Policy Settings

PC's IP Address:

Policy ● Filter web access
○ Allow full web access

Configuring VPNs

Virtual private networks (VPN) provide an encrypted connection (or tunnel) between networks or between a network and a user over a public network (such as the Internet). Instead of using a dedicated, real-world connection such as leased line, a VPN uses virtual connections through the public network. The VPN Firewall supports both network to network connections and network to remote client connections.

There are two modes of operation, pass-through and server. The Firewall supports IPSec tunnels, L2TP over IPSec, and PPTP connections and allows VPN pass-through to enable other secure devices on your network to set up their own secure connections.

Your Cable/DSL modem and your ISP must support IPSec pass-through, L2TP over IPSec pass-through or PPTP pass-through for you to be able to use these protocols.

To allow VPN pass-through, you must configure a virtual server. See "The Virtual Servers Menu" on page 49 for details of how to configure pass-through protocols.

Setting the VPN Mode

The Firewall supports three modes of VPN operation:

- *IPSec Enabled* — IPSec (Internet Protocol Security) is a complex secure protocol with a variety of different encryption methods. When setting up an IPSec connection between two devices they must support the same encryption method.
- *L2TP over IPSec Enabled* — L2TP over IPSec is a combination of two protocols. A user is authenticated (using L2TP) and encrypts data (using IPSec). See “L2TP Configuration” on page 63. L2TP does not support gateway to gateway connections and is only suitable for connecting remote users
- *PPTP Server Enabled* — PPTP (Point-to-Point Tunnelling Protocol) is an encrypted VPN protocol like IPSec. It is not as secure as IPSec but is easy to administrate. PPTP does not support gateway to gateway connections and is only suitable for connecting remote users.

Enabling IPSec VPN will disable pass-through to IPSec and L2TP/IPSec Virtual Servers on the LAN. Enabling L2TP over IPSec will disable pass-through to IPSec and L2TP/IPSec Virtual Servers on the LAN. Enabling the PPTP server will disable PPTP pass-through to a Virtual Server on the LAN. Pass-through outbound from clients on the LAN to servers on the internet is unaffected.

A VPN Tunnel needs the same protocol on both sides of the connection. If you are trying to establish an IPSec connection with another Firewall or with a user the other Firewall must support IPSec or the user must have software installed that supports IPSec VPN.

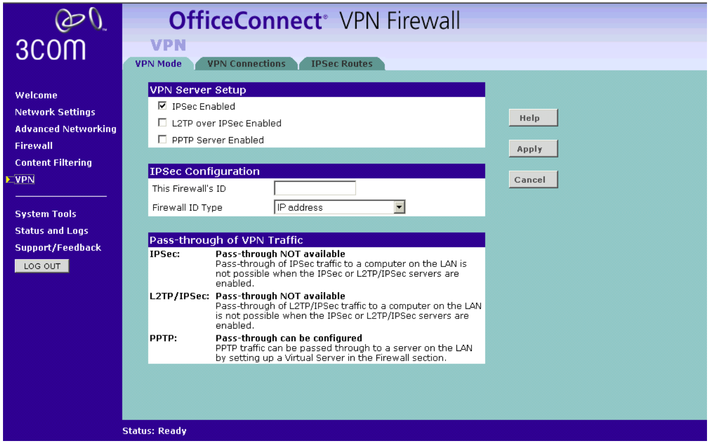
The VPN Mode menu is shown in Figure 64 below. Choose from the options by clicking in the appropriate radio button under *VPN Server Setup*.

IPSec Configuration

In the *IPSec Configuration* field, enter *This Firewall’s ID* as an Internet IP address or name of the Firewall that you are configuring. This value is common across all IPSec connections but does not apply to PPTP connections. If PPTP only is enabled, *This Firewall’s ID* field does not appear.

If you require main mode IPSec connections then this value must be the public IP address of the Firewall.

Figure 64 VPN Mode Screen



VPN Server Setup

☑ IPSec Enabled

☐ L2TP over IPSec Enabled

☐ PPTP Server Enabled

IPSec Configuration

This Firewall's ID:

Firewall ID Type: IP address

Pass-through of VPN Traffic

IPSec:	**Pass-through NOT available** Pass-through of IPSec traffic to a computer on the LAN is not possible when the IPSec or L2TP/IPSec servers are enabled.
L2TP/IPSec:	**Pass-through NOT available** Pass-through of L2TP/IPSec traffic to a computer on the LAN is not possible when the IPSec or L2TP/IPSec servers are enabled.
PPTP:	**Pass-through can be configured** PPTP traffic can be passed through to a server on the LAN by setting up a Virtual Server in the Firewall section.

Status: Ready

L2TP Configuration

If you have enabled L2TP over IPSec you must enter the following items:

1. In the *IPSec Configuration* field, enter *This Firewall's ID* as an Internet IP address, the DNS address of the unit or the name of the Firewall that you are configuring. This value is common across all IPSec connections but does not apply to PPTP connections. If PPTP only is enabled, *This Firewall's ID* field disappears.
2. In the *Firewall ID type* field, Select one of the following:
   - *IP address* (default). This should be the public WAN address of the Firewall.
   - The *DNS address of this unit.*
   - A *name for this unit*. Used when it is not possible to use one of the other modes, for example, if the IP address keeps changing.
3. In the *L2TP Configuration* field, enter:
   - the *Domain Name* as an IP address. A Domain Name locates a website on the Internet.
   - The *IPSec Shared Key*. This is the key for the connection and is a combination of letters, numbers and punctuation and can be up to 64 characters in length. 3Com recommends that the key and password are not the same. The user will need to know the IPSec Shared Key to enable connection.
   - In the *Encryption Level* field, choose the encryption type from DES, 3DES or AES. 3DES is more secure than DES but may take longer to encrypt and decrypt. AES provides the highest security but will take longer than 3DES to encrypt and decrypt.

3DES and AES are not shipped with the Firewall as standard due to international restrictions on encryption. If your country permits their use they can be downloaded from the 3Com web site at **`http://www.3com.com/`**

4. To set up the Firewall for L2TP over IPSec you must allocate IP addresses from the Firewall's LAN for use with L2TP over IPSec. The connections made by L2TP over IPSec will appear to come from these addresses. The addresses must be in a continuous range.

   In the *Address Pool for PPTP and L2TP clients* field enter:
   - The first LAN address you wish to reserve for L2TP over IPSec in the *First Remote IP Address* field.
   - The last LAN address you wish to reserve for L2TP over IPSec in the *Last Remote IP Address* field.

   If both PPTP and L2TP over IPSec modes are selected, then the Address Pool is the same for both clients.

These addresses must be within the Firewall's LAN subnet and must not form part of the DHCP pool.

5. Click *Apply* to save your changes.

PPTP Configuration

To set up the Firewall for PPTP you must allocate IP addresses from the Firewall's LAN for use with PPTP. The connections made by PPTP will appear to come from these addresses. The addresses must be in a continuous range.

In the *Address Pool for PPTP and L2TP clients* field enter:

- The first LAN address you wish to reserve for PPTP clients in the *First Remote IP Address* field.

  and

- The last LAN address you wish to reserve for PPTP clients in the *Last Remote IP Address* field.

If both PPTP and L2TP over IPSec modes are selected, then the Address Pool is the same for both clients..

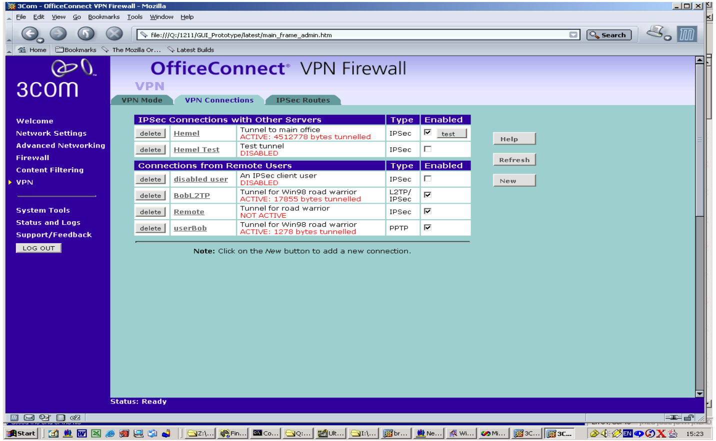
These addresses must be within the Firewall's LAN subnet and must not form part of the DHCP pool.

Click *Apply* to save your changes.

Viewing VPN Connections

The VPN Connections Screen shows information about the IPSec, L2TP over IPSec, and PPTP connections made by the Firewall. It also allows you to add, delete, edit and temporarily disable these connections.

Figure 65 VPN Connections Screen



IPSec Connections with Other Servers			Type	Enabled
delete	Hemel	Tunnel to main office ACTIVE: 4512778 bytes tunnelled	IPSec	☑ test
delete	Hemel Test	Test tunnel DISABLED	IPSec	☐
Connections from Remote Users			**Type**	**Enabled**
delete	disabled user	An IPSec client user DISABLED	IPSec	☐
delete	BobL2TP	Tunnel for Win98 road warrior ACTIVE: 17855 bytes tunnelled	L2TP/ IPSec	☑
delete	Remote	Tunnel for road warrior NOT ACTIVE	IPSec	☑
delete	userBob	Tunnel for Win98 road warrior ACTIVE: 1278 bytes tunnelled	PPTP	☑

Note: Click on the *New* button to add a new connection.

For each connection configured for the Firewall, a row is added to the table. Each row contains the following items:

- *Delete* button — deletes the VPN connection on that row. This will prevent the device or user from establishing a secure connection with the Firewall in future.
- *Name* — Identifies the tunnel. Clicking the name of a connection displays the *Edit VPN Connection* screen. See "Adding and Editing VPN Connections" below.
- *Description* — A text description that enables you to identify a connection. This field in the table additionally displays whether the connection is currently active.
- *Type* — Indicates the type of connection.

- *Enabled* — This check box allows you to enable or disable a connection without deleting it and thus losing the connection details. Check this box to enable a connection. Clear this box to disable the connection. If the connection is active it will be disconnected.
- *Test* — attempts to establish a connection (in Gateway to Gateway mode only).

Additionally there are three buttons outside the table:

- *Help* — displays the online help page for this screen.
- *Refresh* — updates the contents of the window allowing you to see the current status of connections.
- *New* — creates a new VPN connection. See "Adding and Editing VPN Connections" below.

Adding and Editing VPN Connections

This screen also allows you to add new IPSec, L2TP over IPSec and PPTP connections and to edit existing ones. When adding or amending values on this screen remember that both sides of an IPSec, L2TP over IPSec or PPTP connection must contain the same information.

An IPSec, L2TP over IPSec or PPTP connection cannot therefore be activated until both ends of the tunnel have been configured.

- *Connection Type* — choose either *Gateway to Gateway* (only available with IPSec) to connect to another Gateway, Firewall or Router or *Remote User Access* to create a connection for a remote computer.
- *Tunnel Type* — Choose either IPSec (either Remote User Access or Gateway to Gateway), L2TP over IPSec or PPTP.
- *Description* — a description of the connection. This can be different on each Firewall as it is not used in the connection.

ℹ *If the remote site has another Gateway, Firewall or Router with an established IPSec, L2TP over IPSec or PPTP connection then there is no need to create a connection for a remote user on that site.*

ℹ *If you configure an IPSec connection for a remote computer then that computer will require software that supports IPSec. If you configure an L2TP over IPSec or PPTP connection for a remote computer then you should contact Microsoft for information on whether an upgrade is required.*

Depending on which Tunnel Type you have selected, choose from the following to edit or add the remaining fields:

- "IPSec Connections using Remote User Access" on page 65
- "IPSec Connections using Gateway to Gateway" on page 66
- "L2TP over IPSec Connections" on page 69
- "PPTP Connections" on page 69

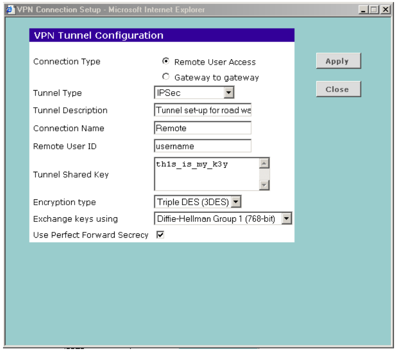
IPSec Connections using Remote User Access

If you have selected IPSec as a Tunnel Type and Remote User Access as a Connection Type, enter the following values:

- *Connection Name* — Enter a descriptive name for the connection.
- *Remote User ID* — Enter the Remote User ID. This must be entered identically on the IPSec software installed on the client's machine.

- *Tunnel Shared Key* — this is the password for the connection and is a combination of letters, numbers and punctuation and can be up to 64 characters in length.

Figure 66 IPSec Connection - Remote User Access



VPN Connection Setup - Microsoft Internet Explorer

VPN Tunnel Configuration

Connection Type	● Remote User Access ○ Gateway to gateway
Tunnel Type	IPSec
Tunnel Description	Tunnel set-up for road wa
Connection Name	Remote
Remote User ID	username
Tunnel Shared Key	th1s_is_my_k3y
Encryption type	Triple DES (3DES)
Exchange keys using	Diffie-Hellman Group 1 (768-bit)
Use Perfect Forward Secrecy	☑

- *Encryption type* — choose the encryption type from DES, 3DES or AES. 3DES is more secure than DES but may take longer to encrypt and decrypt. AES provides the highest security but will take longer than 3DES to encrypt and decrypt.

3DES and AES are not shipped with the Firewall as standard due to international restrictions on encryption. If your country permits their use they can be downloaded from the 3Com web site at **`http://www.3com.com/`**

- *Exchange keys using* — choose the encryption method used to exchange shared keys. *Diffie-Hellman Group 5 and Diffie-Hellman Group 2* are more secure but less common than *Diffie-Hellman Group 1*.
- *Use Perfect Forward Secrecy* — Choose whether to use perfect forward secrecy. Using perfect forward secrecy will change the encryption keys during the course of a connection making the tunnel more secure but slowing data transfer. To enable perfect forward secrecy ensure that the *Use Perfect Forward Secrecy* box is checked. To keep the same key for the length of a connection leave the box unchecked.

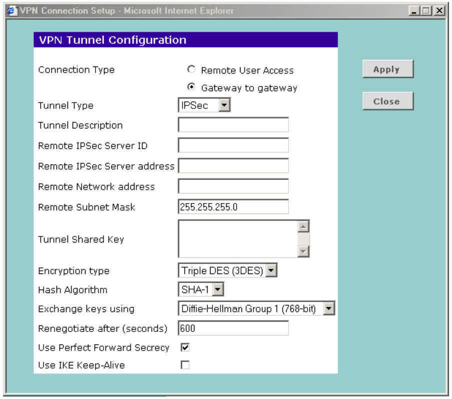
Click *Apply* to save your changes or *Close* to return without saving.

IPSec Connections using Gateway to Gateway

If you have selected IPSec as a Tunnel Type and Gateway to Gateway as a Connection Type, enter the following values:

- *Remote IPSec Server ID* — The ID of the remote server. In the case of another 3Com VPN Firewall this is the *This Firewall's ID* field on the VPN Mode page.
- *Remote IPSec Server Address* — enter the Internet IP address or DNS name of the remote device (Figure 67). A DNS name may only be entered if it is the same as the Remote IPSec Server ID in the box above.
- *Remote Network address* — enter the LAN IP address of the remote network. This is the first IP address of a subnet, one below the first address available for use.

Figure 67 IPSec Connection - Gateway to Gateway



VPN Tunnel Configuration

Connection Type ○ Remote User Access ● Gateway to gateway

Tunnel Type: IPSec

Tunnel Description:

Remote IPSec Server ID:

Remote IPSec Server address:

Remote Network address:

Remote Subnet Mask: 255.255.255.0

Tunnel Shared Key:

Encryption type: Triple DES (3DES)

Hash Algorithm: SHA-1

Exchange keys using: Diffie-Hellman Group 1 (768-bit)

Renegotiate after (seconds): 600

Use Perfect Forward Secrecy ☑

Use IKE Keep-Alive □

If the remote device has a LAN IP address of 192.168.1.1 and a subnet mask of 255.255.255.0 then the LAN IP address of the remote subnet is 192.168.1.0.

The devices must be configured with LAN IP address ranges that do not overlap.

- *Remote Subnet Mask* — this is set as *255.255.255.0* as default.
- *Tunnel Shared Key* — this is the password for the connection and is a combination of letters, numbers and punctuation and can be up to 64 characters in length.

If you are creating a Gateway to Gateway connection you have no need to remember the Tunnel Shared Key once the tunnel is established and do not have to make the key a memorable password.

- *Encryption type* — choose the encryption type from DES, 3DES or AES. 3DES is more secure than DES but may take longer to encrypt and decrypt. AES offers the highest security but will take longer than 3DES to encrypt and decrypt.

3DES and AES are not shipped with the Firewall as standard due to international restrictions on encryption. If your country permits their use they can be downloaded from the 3Com web site at **`http://www.3com.com/`**

- *Hash Algorithm* — choose either SHA-1 or MD5 from the drop-down list. Both ends of the connection must use the same value.
- *Exchange keys using* — choose the encryption method used to exchange shared keys. *Diffie-Hellman Group 5 and Diffie-Hellman Group 2* are more secure but less common than *Diffie-Hellman Group 1*.
- *Renegotiate after (seconds)* — this controls how often the connection will be renegotiated (and the encryption key changed). Longer periods are less secure but may be useful for connections to older equipment which does not have the processing power to negotiate frequently. The default value is 600 seconds (10 minutes).
- *Use Perfect Forward Secrecy* — Choose whether to use perfect forward secrecy. Using perfect forward secrecy will change the encryption keys during the course of a connection making the tunnel more secure but slowing data transfer. To enable perfect forward secrecy ensure that the *Use Perfect Forward Secrecy* box is checked. To keep the same key for the length of a connection leave the box unchecked.

- *Use IKE keep-alive* — when checked the gateway will attempt to ensure that this tunnel remains operational once it has been established, even if there is no traffic on it. This is useful for tunnels where only one end can establish the connection (eg one end of the tunnel is on a dynamic IP address, in this case set *IKE keep-alive* on the 'dynamic' end of the tunnel).

Example: Setting up an IPSec connection between two VPN Firewalls.

VPN Firewall One is located at the head office and is configured with the following settings:

- Internet IP address: 174.19.201.162
- LAN IP address: 192.168.1.1
- LAN Subnet Mask: 255.255.255.0

VPN Firewall Two is located at the sales office and is configured with the following settings:

- Internet IP address: 172.27.34.202
- LAN IP address: 192.168.2.1
- Remote Subnet Mask: 255.255.255.0

The remote VPN Firewall used in this example could be any other IPSec-terminating VPN enabled device, e.g. a 3Com SuperStack 3 Firewall.

To set up an IPSec Connection between the two VPN Firewalls, do the following on each device:

1 Select IPSec Enabled from the VPN Mode screen.

2 Enter the Internet IP address of the Firewall you are configuring in the *This Firewalls ID* field.

a Enter 174.19.201.162 on Firewall One.

b Enter 172.27.34.202 on Firewall Two.

3 Switch to the *VPN Connections* screen and click New.

4 Ensure that the *Gateway to Gateway* radio button is selected.

5 Check that *IPSec* is selected as the *Tunnel Type*.

6 In the *Tunnel Description* field enter: Connection from head office to sales office.

7 In the *Remote IPSec Server ID* field enter the ID of the REMOTE firewall.

a Enter 172.27.34.202. on Firewall One

b Enter 174.19.201.162 on Firewall Two

8 Enter the Internet IP address of the other VPN Firewall in the Remote IPSec Server Address field.

a Enter 172.27.34.202 on Firewall One.

b Enter 174.19.201.162 on Firewall Two.

9 Enter the IP address of the other LAN subnet in the Remote Network address field.

a Enter 192.168.2.0 on Firewall One.

b Enter 192.168.1.0 on Firewall Two.

10 In this example, the Remote Subnet Mask is a default setting of 255.255.255.0; this is the subnet mask on the LANs of the two devices.

11 Enter a password in the Tunnel Shared Key field in both Gateways e.g. TYP0249//23b.

12 Choose *3DES* as the Encryption Type.

13 Choose *SHA-1* as the Hash Algorithm.

14 Choose Diffie-Hellman Group 2 (1024- bit) in the Exchange Keys Using drop-down box.

15 Set *Renegotiate After* (seconds) to 600.

16 Ensure that the *Use Perfect Forward Secrecy* box is checked

17 Leave the *Use IKE Keep-Alive* box unchecked

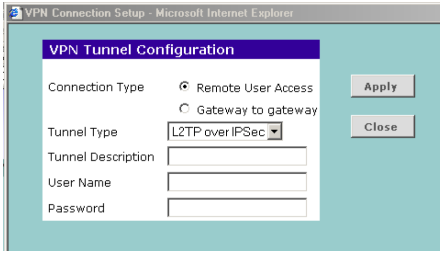
18 Click *Add* to save your new connection or Close to return without saving.

L2TP over IPSec Connections

If you have selected L2TP over IPSec as your Tunnel Type, enter the following values. See Figure 68:

- *Username* — This is the username that the remote VPN client will use to connect.
- *Password* — The password that will need to be supplied to connect.

Figure 68 L2TP over IPSec Connections



VPN Tunnel Configuration

Connection Type ● Remote User Access ○ Gateway to gateway

Tunnel Type L2TP over IPSec

Tunnel Description

User Name

Password

Click *Apply* to save your changes or *Close* to return without saving. When you have created a user account the user will need to know in order to enable connection.

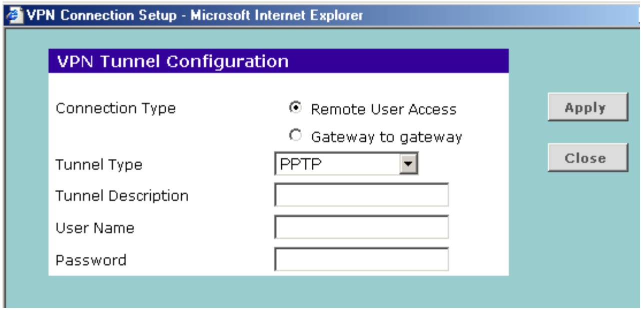
PPTP Connections

If you have selected PPTP as a Tunnel Type, enter the following:

- *Username* — This is the username that the remote VPN client will use to connect.
- *Password* — The Password that the user will need to supply to connect. (Figure 69)

When you have created a user account the user will need to know the User Name and Password you have given them.

Figure 69 PPTP Connections



VPN Tunnel Configuration

Connection Type	● Remote User Access ○ Gateway to gateway
Tunnel Type	PPTP
Tunnel Description	
User Name	
Password	

The screens to edit and add a PPTP user contain the same fields.

Click *Apply* to save your changes or *Close* to return without saving.

Editing IPSec Routes

The IPSec Routes tab is only displayed when IPSec Enabled is selected on the VPN Mode screen. This screen allows you to add and replace networks in the existing IPSec Route. See Figure 70

To do this:

1 Select *edit* to display the *Edit Route* screen. (Figure 71).

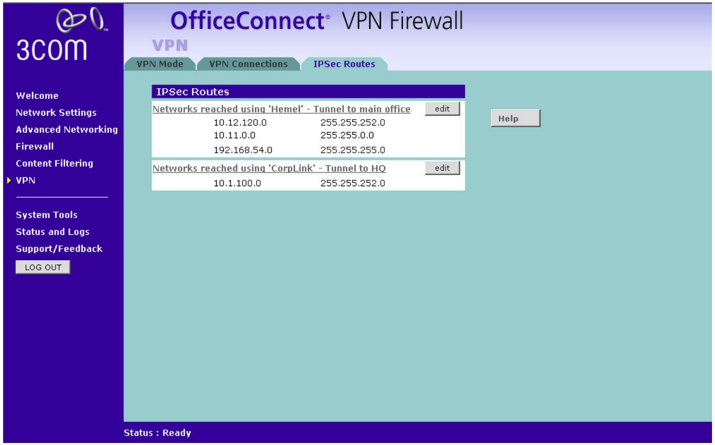
2 Click in the table and add a new *Network* and *Subnet Mask* entry.

3 Leave the *Negotiate all subnets whenever tunnel is triggered* check box blank, unless the remote subnet cannot open the connection, and needs to try more than one subnet.

4 Click *Apply* to save your changes or *Close* to return without saving.

The gateway for a remote network must also be set to use the VPN tunnel to access your local network. Therefore, if you include a subnet for a remote network in your IPSec route then the remote network must also include your subnet in its IPSec route also.

Figure 70 IPSec Routes



IPSec Routes

Networks reached using 'Hemel' - Tunnel to main office

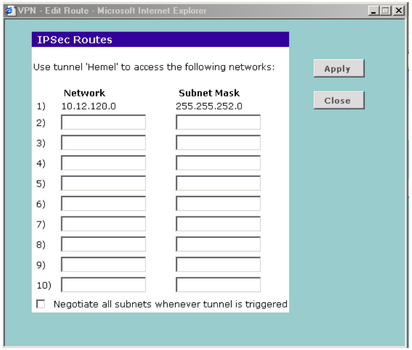
10.12.120.0	255.255.252.0
10.11.0.0	255.255.0.0
192.168.54.0	255.255.255.0

Networks reached using 'CorpLink' - Tunnel to HQ

10.1.100.0	255.255.252.0

Status : Ready

Figure 71 Edit Route



IPSec Routes

Use tunnel 'Hemel' to access the following networks:

	Network	Subnet Mask
1)	10.12.120.0	255.255.252.0
2)		
3)		
4)		
5)		
6)		
7)		
8)		
9)		
10)		

□ Negotiate all subnets whenever tunnel is triggered

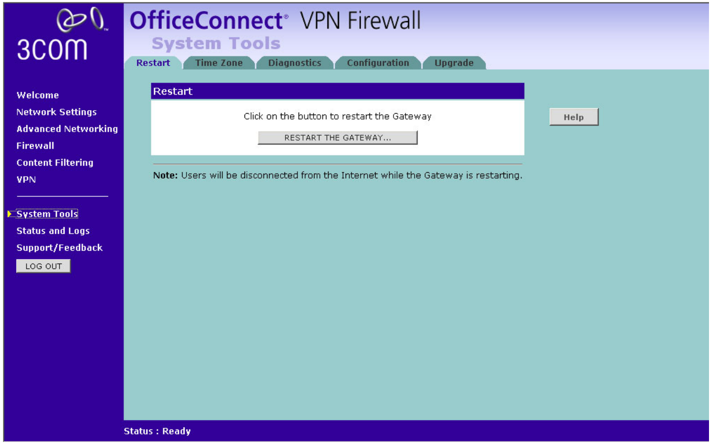
Accessing the System Tools

The System Tools menu includes four administration items: *Restart, Diagnostics, Time Zone, Configuration,* and *Upgrade*. See Figure 72.

Restart

Pressing the *Restart the Gateway* button has the same effect as power cycling the unit. No configuration information will be lost but the log files will be erased. This function may be of use if you are experiencing problems and you wish to re-establish your Internet connection.

Figure 72 Restart Screen



Restart

Click on the button to restart the Gateway

Note: Users will be disconnected from the Internet while the Gateway is restarting.

Status : Ready

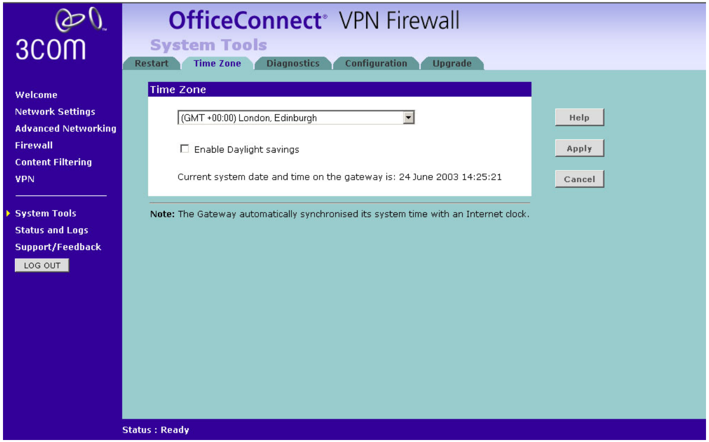
Any network users who are currently accessing the Internet will have their access interrupted whilst the restart takes place, and they may need to reboot their computers when the restart has completed and the Firewall is operational again.

Time Zone

Choose the time zone that is closest to your actual location. The time zone setting is used by the system clock when displaying the correct time in the log files.

If you use Daylight saving tick the Enable Daylight savings box, and then click *Apply*. (Figure 73)

Figure 73 Time Zone Screen



Time Zone

(GMT +00:00) London, Edinburgh

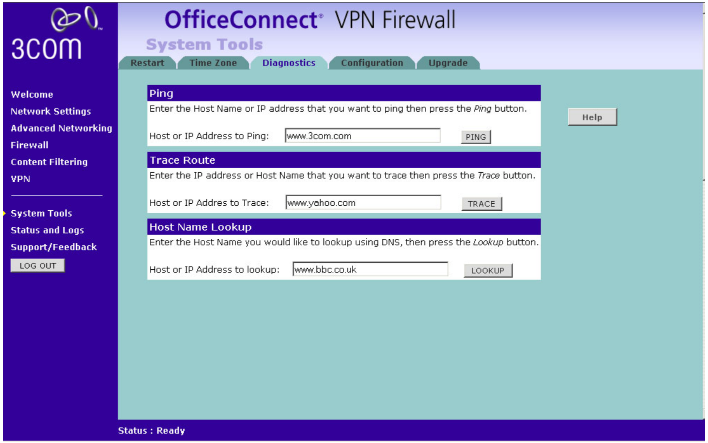
□ Enable Daylight savings

Current system date and time on the gateway is: 24 June 2003 14:25:21

Note: The Gateway automatically synchronised its system time with an Internet clock.

Status : Ready

Figure 74 Diagnostics Screen



Ping

Enter the Host Name or IP address that you want to ping then press the *Ping* button.

Host or IP Address to Ping: www.3com.com

Trace Route

Enter the IP address or Host Name that you want to trace then press the *Trace* button.

Host or IP Addres to Trace: www.yahoo.com

Host Name Lookup

Enter the Host Name you would like to lookup using DNS, then press the *Lookup* button.

Host or IP Address to lookup: www.bbc.co.uk

Status : Ready

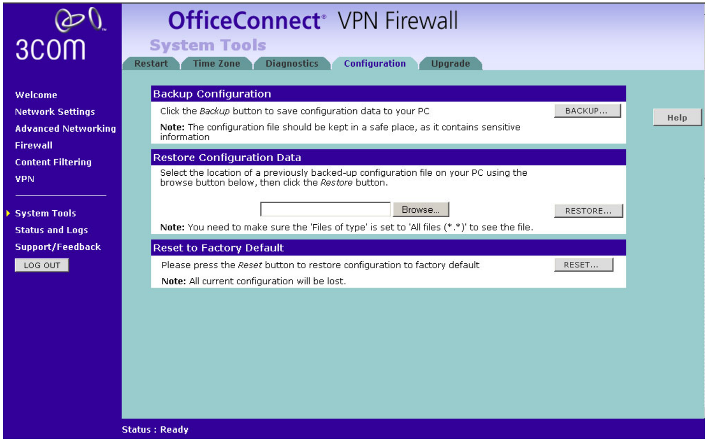
The Firewall reads the correct time from NTP servers on the Internet and sets its system clock accordingly. The Daylight Savings option automatically adjusts the clock to daylight savings time as appropriate to your time zone.

Diagnostics

This screen provides *Ping, Trace Route* and *Host Name Lookup* facilities.

Loading and Saving the Firewall Configuration

Figure 75 Configuration Screen



Backup Configuration

Click the *Backup* button to save configuration data to your PC

Note: The configuration file should be kept in a safe place, as it contains sensitive information

Restore Configuration Data

Select the location of a previously backed-up configuration file on your PC using the browse button below, then click the *Restore* button.

Note: You need to make sure the 'Files of type' is set to 'All files (*.*)' to see the file.

Reset to Factory Default

Please press the *Reset* button to restore configuration to factory default

Note: All current configuration will be lost.

Select the *Configuration* tab to display the *Configuration* screen (Figure 75).

- Click *BACKUP* to save the current configurations of the OfficeConnect VPN Firewall. You will be prompted to download and save a file to disk.
- If you want to reinstate the configuration settings previously saved to a file, click *Browse* to locate the backup file on your computer, and then *RESTORE* to copy the configuration back to the Firewall.

For security purposes restoring the configuration does not change the password.

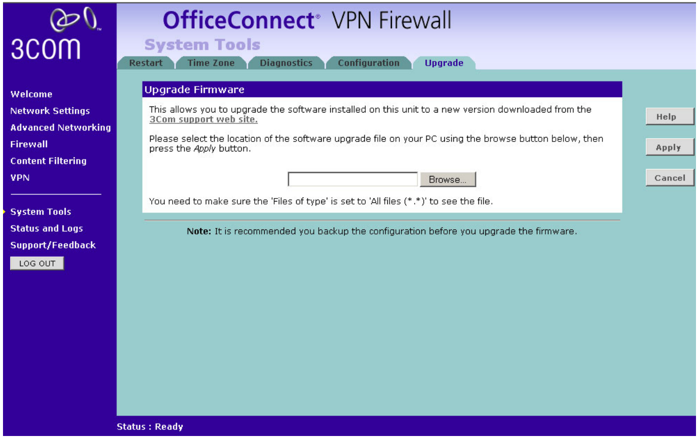
- If you want to reset the settings on your Firewall to those that were loaded at the factory, click *RESET*. You will lose all your configuration changes. The Firewall LAN IP address will revert to 192.168.1.1, and the DHCP server on the LAN will be enabled. You may need to reconfigure and restart your computer to re-establish communication with the Firewall.

Upgrading the Firmware of your Firewall

The Upgrade facility allows you to install on the Firewall any new releases of system software that 3Com may make available.

3DES and AES encryption are not shipped with the Firewall as standard due to international restrictions on encryption. If your country permits their use they can be downloaded from the 3Com web site at **`http://www.3com.com/`**

Figure 76 Upgrade Screen



Upgrade Firmware

This allows you to upgrade the software installed on this unit to a new version downloaded from the 3Com support web site.

Please select the location of the software upgrade file on your PC using the browse button below, then press the *Apply* button.

You need to make sure the 'Files of type' is set to 'All files (*.*)' to see the file.

Note: It is recommended you backup the configuration before you upgrade the firmware.

Once you have downloaded the software, use the *Browse* button to locate the file on your computer, and then click on *Apply*.

*You may need to change the file type in the dialog box displayed by your web browser to *.* to be able to see the file.*

The file will be copied to the Firewall, and once this has completed, the Firewall will restart. Although the upgrade process has been designed to preserve your configuration settings, 3Com recommends that you make a backup of the configuration beforehand, in case the upgrade process fails for any reason (for example, the connection between the computer and the Firewall is lost while the new software is being copied to the Firewall).

The upgrade procedure can take a few minutes, and is complete when the Alert LED has stopped flashing and is permanently off. Make sure that you do not interrupt power to the Firewall during the upgrade procedure; if you do, the software may be corrupted and the Firewall may not start up properly afterwards. If the Alert LED comes on continuously or flashing slowly after a failed upgrade, refer to “Troubleshooting” on page 77.

Viewing Status and Logs

Selecting *Status and Logs* from the Main menu displays the *Status* and *Logs* screens in your Web browser. The *Status* and *Logs* screen displays a tabular representation of your network and Internet connection.

Status — to display the current unit status, including a summary of the configuration. See Figure 77.

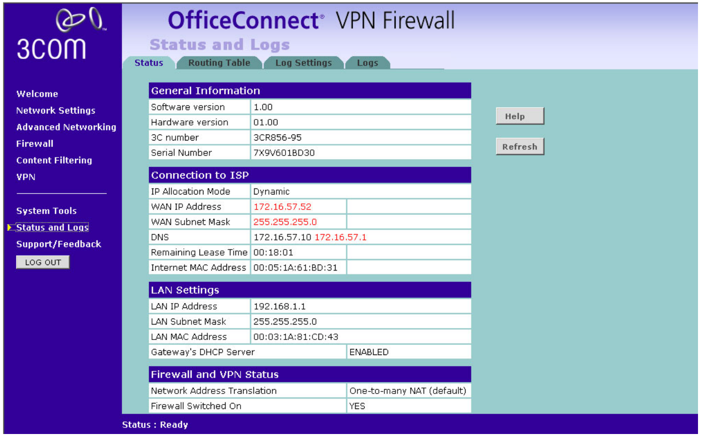
Routing Table— to display the configured static and dynamic routings. See Figure 78

Log Settings — to choose whether to store the log on the Firewall or to send to the remote user or both and to choose to to enable or disable some log entries. See Figure 79.

If you choose the option to store the log on the Firewall the log file will be overwritten when it is full. If you choose the option to send logs to a remote server then you will need to specify the IP address of the remote server. The IP address must be within the LAN subnet and a syslog server must be installed on the remote server.

Logs — to view both the normal events, and security threats logged by the Firewall

Figure 77 Status Screen



General Information	
Software version	1.00
Hardware version	01.00
3C number	3CR856-95
Serial Number	7X9V601BD30

Connection to ISP		
IP Allocation Mode	Dynamic	
WAN IP Address	172.16.57.52	
WAN Subnet Mask	255.255.255.0	
DNS	172.16.57.10 172.16.57.1	
Remaining Lease Time	00:18:01	
Internet MAC Address	00:05:1A:61:BD:31	

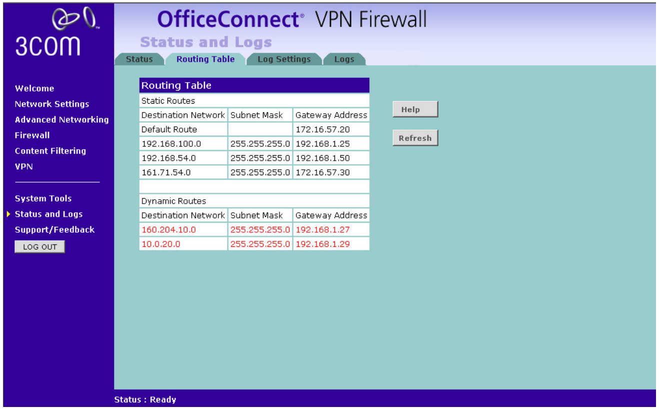
LAN Settings	
LAN IP Address	192.168.1.1
LAN Subnet Mask	255.255.255.0
LAN MAC Address	00:03:1A:81:CD:43
Gateway's DHCP Server	ENABLED

Firewall and VPN Status	
Network Address Translation	One-to-many NAT (default)
Firewall Switched On	YES

Status : Ready

You may be asked to refer to the information on the Status screen if you contact your supplier for technical support.

Figure 78 Routing Table screen



Routing Table

Static Routes

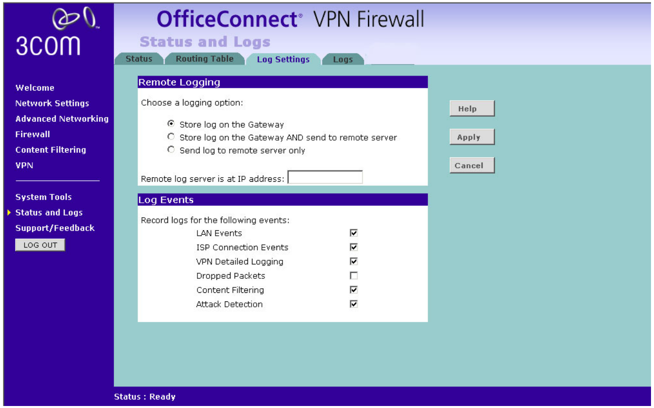
Destination Network	Subnet Mask	Gateway Address
Default Route		172.16.57.20
192.168.100.0	255.255.255.0	192.168.1.25
192.168.54.0	255.255.255.0	192.168.1.50
161.71.54.0	255.255.255.0	172.16.57.30

Dynamic Routes

Destination Network	Subnet Mask	Gateway Address
160.204.10.0	255.255.255.0	192.168.1.27
10.0.20.0	255.255.255.0	192.168.1.29

Status : Ready

Figure 79 Log Settings Screen



Remote Logging

Choose a logging option:

● Store log on the Gateway
○ Store log on the Gateway AND send to remote server
○ Send log to remote server only

Remote log server is at IP address: ____

Log Events

Record logs for the following events:

LAN Events	☑
ISP Connection Events	☑
VPN Detailed Logging	☑
Dropped Packets	□
Content Filtering	☑
Attack Detection	☑

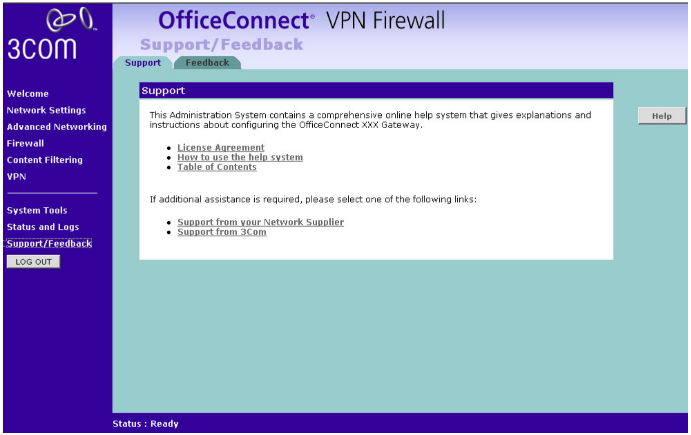
Status : Ready

Obtaining Support and Feedback for your Firewall

Selecting *Support/Feedback* on the main menu generates both:

- The support links screen, which contains a list of Internet links that provide information and support concerning the Firewall. (Figure 80)

Figure 80 Support Screen



Support

This Administration System contains a comprehensive online help system that gives explanations and instructions about configuring the OfficeConnect XXX Gateway.

- License Agreement
- How to use the help system
- Table of Contents

If additional assistance is required, please select one of the following links:

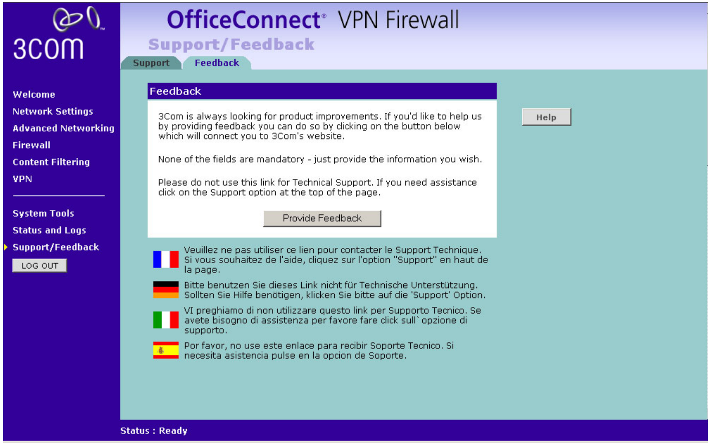
- Support from your Network Supplier
- Support from 3Com

Status : Ready

- The feedback links screen, which contains an Internet link to the 3Com website so that you can provide feedback on the product. (Figure 81)

- 3Com is always looking for product improvements. If you would like to help us by providing feedback please do so by clicking on the *Provide Feedback* button on the Support/Feedback screen which will connect you to 3Com's website.

Figure 81 Feedback Screen



Feedback

3Com is always looking for product improvements. If you'd like to help us by providing feedback you can do so by clicking on the button below which will connect you to 3Com's website.

None of the fields are mandatory - just provide the information you wish.

Please do not use this link for Technical Support. If you need assistance click on the Support option at the top of the page.

Veuillez ne pas utiliser ce lien pour contacter le Support Technique. Si vous souhaitez de l'aide, cliquez sur l'option "Support" en haut de la page.

Bitte benutzen Sie dieses Link nicht für Technische Unterstützung. Sollten Sie Hilfe benötigen, klicken Sie bitte auf die 'Support' Option.

VI preghiamo di non utilizzare questo link per Supporto Tecnico. Se avete bisogno di assistenza per favore fare click sull` opzione di supporto.

Por favor, no use este enlace para recibir Soporte Tecnico. Si necesita asistencia pulse en la opcion de Soporte.

Status : Ready

TROUBLESHOOTING

Basic Connection Checks

- Check that the Firewall is connected to your computers and to the Cable/DSL modem, and that all the equipment is powered on. Check that the LAN and Cable/DSL port link status LEDs on the Firewall are illuminated, and that any corresponding LEDs on the Cable/DSL modem and the NIC are also illuminated.
- Ensure that the computers have completed their start-up procedure and are ready for use. Some network interfaces may not be correctly initialized until the start-up procedure has completed.
- Ensure that the Firewall has completed its power on self test. Refer to "Alert LED" on page 79 for details.
- If the link status LED does not illuminate for a port that is connected, check that you do not have a faulty cable. Try a different cable.

Browsing to the Firewall Configuration Screens

If you have connected your Firewall and computers together but cannot browse to the Firewall configuration screens, check the following:

- Confirm that the physical connection between your computer and the Firewall is OK, and that the link status LEDs on the Firewall and NIC are illuminated and indicating the same speed (10Mbps or 100Mbps). Some NICs do not have status LEDs, in which case a diagnostic program may be available that can give you this information. Refer to the documentation supplied with your NIC for details.
- Ensure that you have configured your computer as described in "Setting Up Your Computers" on page 19. Restart your computer while it is connected to the Firewall to ensure that your computer receives an IP address.
- When entering the address of the Firewall into your web browser, ensure that you include the full URL including the http:// prefix. (e.g. `http://192.168.1.1`)
- If you cannot browse to the Firewall, use the *winipcfg* utility in Windows 95/98/ME to verify that your computer has received the correct address information from the Firewall. From the *Start* menu, choose *Run* and then enter **winipcfg**. Check that the computer has an IP address of the form 192.168.1.xxx (where xxx is in the range 2-254), the subnet mask is 255.255.255.0, and the default Firewall is 192.168.1.1 (the address of the Firewall). If these are not correct, use the *Release* and *Renew* functions to obtain a new IP address from the Firewall. Under Windows NT/2000/XP, use the *ipconfig* command-line utility to perform the same functions.
- If you still cannot browse to the Firewall, then use the Discovery program on the accompanying CD-ROM as described in "Using Discovery" on page 81.

Connecting to the Internet

If you can browse to the Firewall configuration screens but cannot access sites on the Internet, check the following:

- Confirm that the physical connection between the Firewall and the Cable/DSL modem is OK, and that the link status LEDs on both Firewall and modem are illuminated.
- Confirm that the connection between the modem and the Cable/DSL interface is OK.
- Ensure that you have entered the correct information into the Firewall configuration screens as required by your Internet Service Provider. Use the "Internet Settings" screen to verify this.
- For DSL users, check that the PPPoE or PPTP user name, password and service name are correct, if these are required. Only enter a PPPoE service name if your ISP requires one.
- For cable users, check whether your ISP requires a fixed MAC (Ethernet) address. If so, use the *Clone MAC Address* feature in the Firewall to ensure that the correct MAC address is presented, as described in "Configuring a Dynamic IP Address" on page 38.
- Ensure that your computers are not configured to use a Web proxy. On Windows computers, this can be found under *Control Panel* > *Internet Options* > *Connections*.
- Check PC Privileges to see if you have allowed your PCs to connect to the Internet. See "PC Privileges" on page 51.

Forgotten Password

If you can browse to the Firewall configuration screen but cannot log on because you do not know or have forgotten the password, follow the steps below to reset the Firewall to it's factory default configuration. **Warning: all your configuration changes will be lost, and you will need to run the configuration wizard again before you can re-establish your Firewall connection to the Internet.** Also, other computer users will lose their network connections whilst this process is taking place, so choose a time when this would be convenient.

1. Remove power from the Firewall.
2. Disconnect all your computers and the cable/DSL modem from the Firewall.
3. Using an Ethernet cable, connect the Ethernet Cable/DSL port on the rear of the Firewall to any one of the LAN ports.
4. Re-apply power to the Firewall. The Alert LED will flash as the Firewall starts up, and after approximately 30 seconds will start to flash more slowly (typically 2 seconds on, 2 seconds off). Once the Alert LED has started to flash slowly, remove power from the Firewall.
5. Remove the cable connecting the Cable/DSL port to the LAN port, and reconnect one of your computers to one of the Firewall LAN ports.

6 Re-apply power to the Firewall, and when the start-up sequence has completed, browse to:

`http://192.168.1.1`

and run the configuration wizard. You may need to restart your computer before you attempt this.

7 When the configuration wizard has completed, you may reconnect your network as it was before.

Alert LED

When the Firewall is first powered on, the Alert LED will be on for between three and five seconds, and then start to flash while the system software checks the hardware for proper operation. The Alert LED may continue to flash for one minute or longer, depending on your network configuration. Once the Firewall has started normal operation, the Alert LED will go out.

- If the Alert LED does not go out following start up, but illuminates continuously, this indicates that the software has detected a possible fault with the hardware. If the Alert LED is flashing slowly this indicates a firmware failure. Remove power from the Firewall, wait 10 seconds and then re-apply power. If the Alert LED comes on continuously again, then a fault has been detected, refer to "Recovering from Corrupted Software" below. If this does not fix the problem, contact your supplier for further advice.
- During normal operation, you may notice the Alert LED lighting briefly from time to time. This indicates that the Firewall has detected a hacker attack from the Internet and has prevented it from harming your network. You need take no specific action on this, unless you decide that these attacks are happening frequently in which case you may wish to discuss this with your ISP. The Firewall logs such attacks, and this information is available through the configuration screens.

Recovering from Corrupted Software

If the Alert LED flashes slowly on and off following power-up, it is possible that the system software has become corrupted. In this condition, the Firewall will enter a fail-safe state; DHCP is disabled, and the LAN IP address is set to 192.168.1.1. Follow the instructions below to upload a new copy of the system software to a Firewall unit in this state.

Ensure that one of your computers has a copy of the new software image file stored on its hard disk. If not contact 3Com by visiting:

`http://www.3com.com`

1 Remove power from the Firewall and disconnect the Cable/DSL modem and all your computers, except for the one computer with the software image.

2 You will need to reconfigure this computer with the following static IP address information:

- IP address: 192.168.1.2
- Subnet mask: 255.255.255.0
- Default Gateway address: 192.168.1.1

3 Restart the computer, and re-apply power to the Firewall.

4 Using the Web browser on the computer, enter the following URL in the location bar:

`http://192.168.1.1`

This will connect you to the fail-safe mode of the Firewall.

5 Follow the on-screen instructions. Enter the path and filename of the software image file.

6 When the upload has completed, the Firewall will restart, run the self-test and, if successful, resume normal operation. The Alert LED will go out.

7 Reconnect your Firewall to the Cable/DSL modem and the computers in your network. Do not forget to reconfigure the computer you used for the software upload.

If the Firewall does not resume normal operation following the upload, it may be faulty. Contact your supplier for advice.

Frequently Asked Questions

How many computers on the LAN does the VPN Firewall support?

A maximum of 253 computers on the LAN are supported.

There are only 4 LAN ports on the Firewall. How are additional computers connected?

You can expand the number of connections available on your LAN by using hubs and switches connected to the Firewall. 3Com OfficeConnect hubs and switches provide a simple, reliable means of expanding your network; contact your supplier for more information, or visit:

`http://www.3com.com`.

Does the Firewall support virtual private networks (VPNs)?

The Firewall fully supports VPNs It is capable of:

- Initiating and terminating IPSec connections.
- Terminating L2TP over IPSec and PPTP connections.
- Providing hardware accelerated encryption for IPSec VPNs and IPSec VPNs within L2TP over IPSec.
- Providing VPN pass-through.
- Configuring of up to 50 VPN Tunnels.

Where can I download software upgrades for the Firewall?

Upgrades to the VPN Firewall software are posted on the 3Com support web site, accessible by visiting:

`http://www.3com.com`

What other online resources are there?

The 3Com Knowledgebase at:

`http://knowledgebase.3com.com`

is a database of technical information covering all 3Com products. It is updated daily with information from 3Com technical support services, and it is available 24 hours a day, 7 days a week.

USING DISCOVERY

Running the Discovery Application

3Com provides a user-friendly Discovery application for detecting the OfficeConnect VPN Firewall on the network.

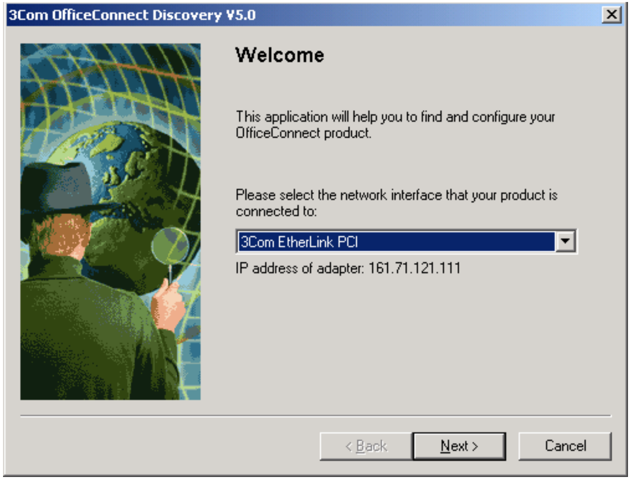
If your computers are configured with static addresses (also known as fixed addresses) and you do not wish to change this, then you should use the Discovery program on the Firewall CD-ROM to detect and configure your Firewall.

Windows Installation (95/98/XP/2000/2003 Server/NT)

1 Insert the Firewall CD-ROM in the CD-ROM drive on your computer. A menu will appear; select *Gateway Discovery*.

Discovery will find the Firewall even if it is unconfigured or misconfigured.

Figure 82 Discovery Welcome Screen



This application will help you to find and configure your OfficeConnect product.

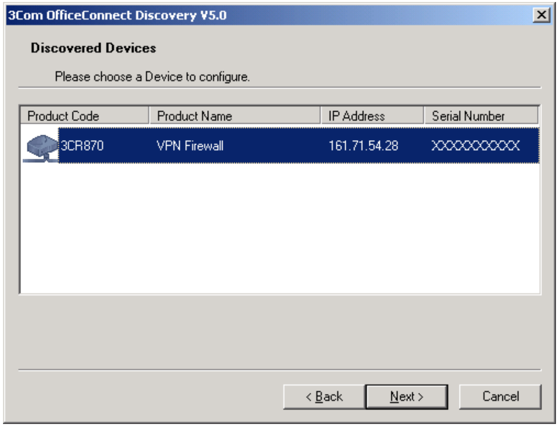
Please select the network interface that your product is connected to:

3Com EtherLink PCI

IP address of adapter: 161.71.121.111

2 When the *Welcome* screen is displayed click on *Next* and wait until the application discovers the Firewalls connected to your LAN.

Figure 83 Discovered Firewall



3Com OfficeConnect Discovery V5.0

Discovered Devices

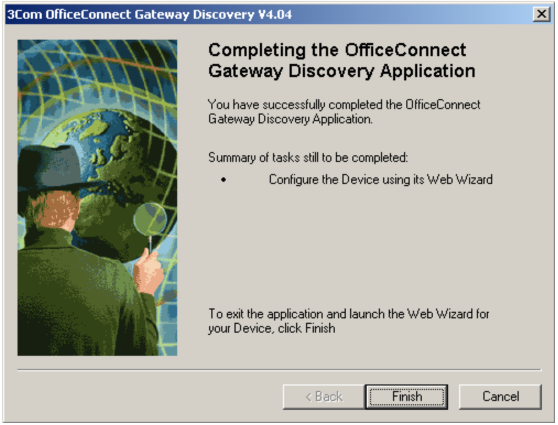
Please choose a Device to configure.

Product Code	Product Name	IP Address	Serial Number
3CR870	VPN Firewall	161.71.54.28	XXXXXXXXXX

In Figure 83 the serial number of the unit has been replaced with XXXXXXXXXX.

3 Figure 83 shows an example Discovered Devices screen. Highlight the VPN Firewall by clicking on it, and press *Next*.

Figure 84 Discovery Finish Screen



3Com OfficeConnect Gateway Discovery V4.04

Completing the OfficeConnect Gateway Discovery Application

You have successfully completed the OfficeConnect Gateway Discovery Application.

Summary of tasks still to be completed:

- Configure the Device using its Web Wizard

To exit the application and launch the Web Wizard for your Device, click Finish

4 Click on *Finish* to launch a web browser and display the login page for the Firewall.

IP ADDRESSING

The Internet Protocol Suite

The Internet protocol suite consists of a well-defined set of communications protocols and several standard application protocols. Transmission Control Protocol/Internet Protocol (TCP/IP) is probably the most widely known and is a combination of two of the protocols (IP and TCP) working together. TCP/IP is an internationally adopted and supported networking standard that provides connectivity between equipment from many vendors over a wide variety of networking technologies.

IP Addresses and Subnet Masks

Each device on your network must have a unique IP address to operate correctly. An IP address identifies the address of the device to which data is being sent and the address of the destination network. IP addresses have the format n.n.n.x where n is a decimal number between 0 and 255 and x is a number between 1 and 254 inclusive.

However, an IP Address alone is not enough to make your device operate. In addition to the IP address, you need to set a subnet mask. All networks are divided into smaller sub-networks and a subnet mask is a number that enables a device to identify the sub-network to which it is connected.

For your network to work correctly, all devices on the network must have:

- The same sub-network address.
- The same subnet mask.

The only value that will be different is the specific host device number. This value must always be unique.

An example IP address is '192.168.100.8'. However, the size of the network determines the structure of this IP Address. In using the Firewall, you will probably only encounter two types of IP Address and subnet mask structures.

Type One

In a small network, the IP address of '192.168.100.8' is split into two parts:

- Part one ('192.168.100') identifies the network on which the device resides.
- Part two ('.8') identifies the device within the network.

This type of IP Address operates on a subnet mask of '255.255.255.0'.

See Table 3 for an example about how a network with three PCs and a VPN Firewall might be configured.

Table 3 IP Addressing and Subnet Masking in a Small Network

Device	IP Address	Subnet Mask
PC 1	192.168.100.8	255.255.255.0
PC 2	192.168.100.33	255.255.255.0
PC 3	192.168.100.188	255.255.255.0
VPN Firewall	192.168.100.72	255.255.255.0

Type Two

In larger networks, where there are more devices, the IP address of ‘192.168.100.8’ is, again, split into two parts but is structured differently:

- Part one (‘192.168’) identifies the network on which the device resides.
- Part two (‘.100.8’) identifies the device within the network.

This type of IP Address operates on a subnet mask of ‘255.255.0.0’.

See Table 4 for an example about how a network (only four PCs represented) and a VPN Firewall might be configured.

Table 4 IP Addressing and Subnet Masking in a Large Network

Device	IP Address	Subnet Mask
PC 1	192.168.100.8	255.255.0.0
PC 2	192.168.201.30	255.255.0.0
PC 3	192.168.113.155	255.255.0.0
PC 4	192.168.2.230	255.255.0.0
VPN Firewall	192.168.2.72	255.255.0.0

How does a Device Obtain an IP Address and Subnet Mask?

There are three different ways to obtain an IP address and the subnet mask. These are:

- Dynamic Host Configuration Protocol (DHCP) Addressing
- Static Addressing
- Automatic Addressing (Auto-IP Addressing)

DHCP Addressing

The VPN Firewall contains a DHCP server, which allows computers on your network to obtain an IP address and subnet mask automatically. DHCP assigns a temporary IP address and subnet mask which gets reallocated once you disconnect from the network.

DHCP will work on any client Operating System such as Windows® XP, Windows 98 or Windows NT 4.0. Also, using DHCP means that the same IP address and subnet mask will never be duplicated for devices on the network. DHCP is particularly useful for networks with large numbers of users on them.

Static Addressing

You must enter an IP Address and the subnet mask manually on every device. Using a static IP and subnet mask means the address is permanently fixed.

Auto-IP Addressing

Network devices use automatic IP addressing if they are configured to acquire an address using DHCP but are unable to contact a DHCP server. Automatic IP addressing is a scheme where devices allocate themselves an IP address at random from the industry standard subnet of 169.254.x.x (with a subnet mask of 255.255.0.0). If two devices allocate themselves the same address, the conflict is detected and one of the devices allocates itself a new address.

Automatic IP addressing support was introduced by Microsoft in the Windows 98 operating system and is also supported in Windows 2000/XP/NT.

Private IP Addresses

The following address ranges have been reserved by the Internet Engineering Task Force (IETF) for private use:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

The Firewall has a default subnet of 192.168.1.0 – 192.168.1.255. 3Com recommends that you use this subnet for the LAN addresses of your first Device and subsequent ranges (192.168.2.0 – 192.168.2.255) for the LAN range of other Devices that you will connect to by VPN.

TECHNICAL SPECIFICATIONS

This section lists the technical specifications for the OfficeConnect VPN Firewall.

Interfaces

Cable or DSL modem connection - one 10/100 Mbps Ethernet port (10BASE-T/100BASE-TX) with Auto-MDI/MDIX.

LAN connection - four 10/100 Mbps Ethernet ports (10BASE-T/100BASE-TX) with Auto-MDI/MDIX.

Operating Temperature

0 °C to 40 °C (32 °F to 105 °F)

Power

7 W power dissipated

Humidity

0 % to 90 % (non-condensing) humidity

Dimensions

Width = 220 mm (8.7 in.)

Depth = 135 mm (5.3 in.)

Height = 36 mm (1.4 in.)

Weight

Approximately 537 g (1.18 lbs)

VPN Tunnels

Fifty

Standards

Functional:ISO 8802/3
IEEE 802.3

Safety:UL 60950, EN 60950
CSA 22.2 #60950
IEC 60950

EMC:EN 55022 Class B[†]
EN 55024
AS/NZS 3548 B[†]
FCC Part 15 Class B[†]*
ICES-003 Class B[†]
VCCI Class B[†]
CNS 13438 Class A

Environmental:EN 60068 (IEC 68)

[†] Category 5 screened cables must be used to ensure compliance with the Class B requirements of this standard. The use of unscreened cables (Category 3 or Category 5) complies with the Class A requirements.

Category 5 cables must be used if you are connecting to 100 Mbps devices.

*See “Safety Information” on page 89 for conditions of operation.

System Requirements

Operating Systems

The VPN Firewall will support the following Operating Systems:

- Windows 95, 98, Me
- Windows NT 4.0
- Windows 2000
- Windows XP
- Windows 2003 Server
- Mac OS 8.5 or higher
- Unix

Ethernet Performance

The VPN Firewall complies with the IEEE 802.3i, u and x specifications.

Cable Specifications

The VPN Firewall supports the following cable types and maximum lengths:

- Category 3 (Ethernet) or Category 5 (Fast Ethernet or Dual Speed Ethernet) Twisted Pair — shielded and unshielded cable types.
- Maximum cable length of 100m (327.86 ft).

Category 5 cables are required for a 100BASE-TX connection.

SAFETY INFORMATION

Important Safety Information

***WARNING**: Warnings contain directions that you must follow for your personal safety. Follow all directions carefully.*
You must read the following safety information carefully before you install or remove the unit:

***WARNING**: Exceptional care must be taken during installation and removal of the unit.*

***WARNING**: Only stack the Firewall with other OfficeConnect units.*

***WARNING**: To ensure compliance with international safety standards, only use the power adapter that is supplied with the unit.*

***WARNING**: The socket outlet must be near to the unit and easily accessible. You can only remove power from the unit by disconnecting the power cord from the outlet.*

***WARNING**: This unit operates under SELV (Safety Extra Low Voltage) conditions according to IEC 60950. The conditions are only maintained if the equipment to which it is connected also operates under SELV conditions.*

***WARNING**: There are no user-replaceable fuses or user-serviceable parts inside the Firewall. If you have a physical problem with the unit that cannot be solved with problem solving actions in this guide, contact your supplier.*

***WARNING**: Disconnect the power adapter before moving the unit.*

***WARNING: RJ-45 ports.** These are shielded RJ-45 data sockets. They cannot be used as telephone sockets. Only connect RJ-45 data connectors to these sockets.*

Wichtige Sicherheitshinweise

***VORSICHT:** Warnhinweise enthalten Anweisungen, die Sie zu Ihrer eigenen Sicherheit befolgen müssen. Alle Anweisungen sind sorgfältig zu befolgen.*
Sie müssen die folgenden Sicherheitsinformationen sorgfältig durchlesen, bevor Sie das Geräts installieren oder ausbauen:

***VORSICHT:** Bei der Installation und beim Ausbau des Geräts ist mit höchster Vorsicht vorzugehen.*

***VORSICHT:** Stapeln Sie das Geräts nur mit anderen OfficeConnect Gerätes zusammen.*

***VORSICHT:** Aufgrund von internationalen Sicherheitsnormen darf das Gerät nur mit dem mitgelieferten Netzadapter verwendet werden.*

VORSICHT: *Die Netzsteckdose muß in der Nähe des Geräts und leicht zugänglich sein. Die Stromversorgung des Geräts kann nur durch Herausziehen des Gerätenetzkabels aus der Netzsteckdose unterbrochen werden.*

VORSICHT: *Der Betrieb dieses Geräts erfolgt unter den SELV-Bedingungen (Sicherheitskleinstspannung) gemäß IEC 60950. Diese Bedingungen sind nur gegeben, wenn auch die an das Gerät angeschlossenen Geräte unter SELV-Bedingungen betrieben werden.*

VORSICHT: *Es sind keine von dem Benutzer zu ersetzende oder zu wartende Teile in dem Gerät vorhanden. Wenn Sie ein Problem mit dem Firewall haben, das nicht mittels der Fehleranalyse in dieser Anleitung behoben werden kann, setzen Sie sich mit Ihrem Lieferanten in Verbindung.*

VORSICHT: *Vor dem Ausbau des Geräts das Netzadapterkabel herausziehen.*

VORSICHT: RJ-45-Anschlüsse. *Dies sind abgeschirmte RJ-45-Datenbuchsen. Sie können nicht als Telefonanschlußbuchsen verwendet werden. An diesen Buchsen dürfen nur RJ-45-Datenstecker angeschlossen werden.*

Consignes importantes de sécurité

AVERTISSEMENT: *Les avertissements présentent des consignes que vous devez respecter pour garantir votre sécurité personnelle. Vous devez respecter attentivement toutes les consignes.*
Nous vous demandons de lire attentivement les consignes de sécurité ci-après avant d'installer ou de désinstaller l'appareil:

AVERTISSEMENT: *Faites très attention lors de l'installation et de la désinstallation de l'appareil.*

AVERTISSEMENT: *L'appareil ne doit être empilé qu'avec d'autres produits OfficeConnect.*

AVERTISSEMENT: *Pour garantir le respect des normes internationales de sécurité, utilisez uniquement l'adaptateur électrique remis avec cet appareil.*

AVERTISSEMENT: *La prise secteur doit se trouver à proximité de l'appareil et son accès doit être facile. Vous ne pouvez mettre l'appareil hors circuit qu'en débranchant son cordon électrique au niveau de la prise.*

AVERTISSEMENT: *L'appareil fonctionne à une tension de sécurité extrêmement basse, conformément à la norme CEI 60950. La conformité à cette norme n'est maintenue* *que si l'équipement auquel il est raccordé fonctionne également dans des conditions conformes à cette norme.*

⚠ ***AVERTISSEMENT:*** *Il n'y a pas d'élément remplaçable ou réparable par l'utilisateur à l'intérieur de l'appareil. Si vous rencontrez avec cet appareil un problème ne pouvant être résolu par les actions de résolution de problèmes présentés dans ce manuel, veuillez contacter votre fournisseur.*

⚠ ***AVERTISSEMENT:*** *Débranchez l'adaptateur électrique avant de désinstaller cet appareil.*

⚠ ***AVERTISSEMENT: Ports RJ-45.*** *Il s'agit de prises de données femelles blindées RJ-45. Vous ne pouvez pas les utiliser comme prise de téléphone. Branchez uniquement des connecteurs de données RJ-45 dans ces prises femelles.*

OBTAINING SUPPORT FOR YOUR PRODUCT

Register Your Product to Gain Service Benefits

To take advantage of warranty and other service benefits, you must first register your product at **`http://eSupport.3com.com/`**.

3Com eSupport services are based on accounts that you create or have authorization to access. First time users must apply for a user name and password that provides access to a number of eSupport features including Product Registration, Repair Services, and Service Request.

Purchase Value-Added Services

To enhance response times or extend warranty benefits, contact 3Com or your authorized 3Com reseller. Value-added services can include 24x7 telephone technical support, software upgrades, onsite assistance or advance hardware replacement. Experienced engineers are available to manage your installation with minimal disruption to your network. Expert assessment and implementation services are offered to fill resource gaps and ensure the success of your networking projects. More information on 3Com Extended Warranty and Professional Services is available at **`http://www.3com.com/`**Contact your authorized 3Com reseller or 3Com for additional product and support information.

Troubleshoot Online

You will find support tools posted on the 3Com web site at **`http://www.3com.com/`**

- **3Com Knowledgebase** helps you troubleshoot 3Com products. This query-based interactive tool is located at **`http://knowledgebase.3com.com`** and contains thousands of technical solutions written by 3Com support engineers.
- **Connection Assistant** helps you install, configure and troubleshoot 3Com desktop and server NICs, wireless cards and Bluetooth devices. This diagnostic software is located at: **`http://www.3com.com/prodforms/software/connection_assistant/ca_thankyou.html`**

Access Software Downloads

Software Updates are the bug fix / maintenance releases for the version of software initially purchased with the product. In order to access these Software Updates you must first register your product on the 3Com web site at **`http://eSupport.3com.com/`**.

First time users will need to apply for a user name and password. A link to software downloads can be found at **`http://eSupport.3com.com/`**, or under the Product Support heading at **`http://www.3com.com/`**

Software Upgrades are the software releases that follow the software version included with your original product. In order to access upgrades and related documentation you must first purchase a service contract from 3Com or your reseller.

Contact Us

3Com offers telephone, e-mail and internet access to technical support and repair services. To access these services for your region, use the appropriate telephone number, URL or e-mail address from the list below. You will find a current directory of support telephone numbers posted on the 3Com web site at **http://csoweb4.3com.com/contactus/**

Telephone Technical Support and Repair

To obtain telephone support as part of your warranty and other service benefits, you must first register your product at **http://eSupport.3com.com/**

When you contact 3Com for assistance, please have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision level
- Diagnostic error messages
- Details about recent configuration changes, if applicable

To send a product directly to 3Com for repair, you must first obtain a return authorization number (RMA). Products sent to 3Com, without authorization numbers clearly marked on the outside of the package, will be returned to the sender unopened, at the sender's expense. If your product is registered and under warranty, you can obtain an RMA number online at **http://eSupport.3com.com/**. First time users will need to apply for a user name and password.

Telephone numbers are correct at the time of publication. Find a current directory of support telephone numbers posted on the 3Com web site at **http://csoweb4.3com.com/contactus/**

Country	Telephone Number
Asia, Pacific Rim Telephone Technical Support and Repair	
Australia	1 800 678 515
Hong Kong	800 933 486
India	+61 2 9424 5179 or 000800 6501111
Indonesia	001 803 61 009
Japan	00531 616 439 or 03 5977 7991
Malaysia	1800 801 777
New Zealand	0800 446 398
Pakistan	+61 2 9937 5083
Philippines	1235 61 266 2602 or 1800 1 888 9469
P.R. of China	10800 61 00137 or 021 6350 1590 or 00800 0638 3266
Singapore	800 6161 463
S. Korea	080 333 3308
Taiwan	00801 611 261
Thailand	001 800 611 2000

You can also obtain support in this region using the following e-mail: **apr_technical_support@3com.com**

Or request a repair authorization number (RMA) by fax using this number: +65 543 6348

Country	Telephone Number
Europe, Middle East, and Africa Telephone Technical Support and Repair	
From anywhere in these regions, call:	+44 (0)1442 435529

From the following countries, you may use the numbers shown:

Austria	01 7956 7124
Belgium	070 700 770
Denmark	7010 7289
Finland	01080 2783
France	0825 809 622
Germany	01805 404 747
Hungary	06800 12813
Ireland	01407 3387
Israel	1800 945 3794
Italy	199 161346
Luxembourg	342 0808128
Netherlands	0900 777 7737
Norway	815 33 047
Poland	00800 441 1357
Portugal	707 200 123
South Africa	0800 995 014
Spain	9 021 60455
Sweden	07711 14453
Switzerland	08488 50112
U.K.	0870 909 3266

You can also obtain support in this region using the following URL: **`http://emea.3com.com/support/email.html`**

Country	Telephone Number
Latin America Telephone Technical Support and Repair	

From the Caribbean, Central and South America, call:

Antigua	1 800 988 2112
Argentina	0 810 444 3COM
Aruba	1 800 998 2112
Bahamas	1 800 998 2112
Barbados	1 800 998 2112
Belize	52 5 201 0010
Bermuda	1 800 998 2112
Bonaire	1 800 998 2112
Brazil	0800 13 3COM
Cayman	1 800 998 2112
Chile	AT&T +800 998 2112
Colombia	AT&T +800 998 2112
Costa Rica	AT&T +800 998 2112
Curacao	1 800 998 2112
Ecuador	AT&T +800 998 2112
Dominican Republic	AT&T +800 998 2112
Guatemala	AT&T +800 998 2112
Haiti	57 1 657 0888
Honduras	AT&T +800 998 2112
Jamaica	1 800 998 2112
Martinique	571 657 0888
Mexico	01 800 849CARE
Nicaragua	AT&T +800 998 2112
Panama	AT&T +800 998 2112
Paraguay	54 11 4894 1888
Peru	AT&T +800 998 2112
Puerto Rico	1 800 998 2112
Salvador	AT&T +800 998 2112
Trinidad and Tobago	1 800 998 2112
Uruguay	AT&T +800 998 2112
Venezuela	AT&T +800 998 2112
Virgin Islands	57 1 657 0888

Country	Telephone Number
You can also obtain support in this region using the following: Spanish speakers, enter the URL: **`http://lat.3com.com/lat/support/form.html`** Portuguese speakers, enter the URL: **`http://lat.3com.com/br/support/form.html`** English speakers in Latin America should send e-mail to: **`lat_support_anc@3com.com`**	
US and Canada Telephone Technical Support and Repair	
	1 800 876 3266

END USER SOFTWARE LICENCE AGREEMENT

3Com Corporation
END USER SOFTWARE LICENSE AGREEMENT

YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE DOWNLOADING, INSTALLING AND USING THIS PRODUCT, THE USE OF WHICH IS LICENSED BY 3COM CORPORATION ("3COM") TO ITS CUSTOMERS FOR THEIR USE ONLY AS SET FORTH BELOW. DOWNLOADING, INSTALLING OR OTHERWISE USING ANY PART OF THE SOFTWARE OR DOCUMENTATION INDICATES THAT YOU ACCEPT THESE TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT DOWNLOAD, INSTALL OR OTHERWISE USE THE SOFTWARE OR DOCUMENTATION, DO NOT CLICK ON THE "I AGREE" OR SIMILAR BUTTON. AND IF YOU HAVE RECEIVED THE SOFTWARE AND DOCUMENTATION ON PHYSICAL MEDIA, RETURN THE ENTIRE PRODUCT WITH THE SOFTWARE AND DOCUMENTATION UNUSED TO THE SUPPLIER WHERE YOU OBTAINED IT.

LICENSE: 3Com grants you a nonexclusive, nontransferable (except as specified herein) license to use the accompanying software program(s) in executable form (the "Software") and accompanying documentation (the "Documentation"), subject to the terms and restrictions set forth in this Agreement. You are not permitted to lease, rent, distribute or sublicense (except as specified herein) the Software or Documentation or to use the Software or Documentation in a time-sharing arrangement or in any other unauthorized manner. Further, no license is granted to you in the human readable code of the Software (source code). Except as provided below, this Agreement does not grant you any rights to patents, copyrights, trade secrets, trademarks, or any other rights with respect to the Software or Documentation.

Subject to the restrictions set forth herein, the Software is licensed to be used on any workstation or any network server owned by or leased to you, for your internal use, provided that the Software is used only in connection with this 3Com product. You may reproduce and provide one (1) copy of the Software and Documentation for each such workstation or network server on which the Software is used as permitted hereunder. Otherwise, the Software and Documentation may be copied only as essential for backup or archive purposes in support of your use of the Software as permitted hereunder. Each copy of the Software and Documentation must contain 3Com's and its licensors' proprietary rights and copyright notices in the same form as on the original. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation delivered to you under this Agreement.

ASSIGNMENT; NO REVERSE ENGINEERING: You may transfer the Software, Documentation and the licenses granted herein to another party in the same country in which you obtained the Software and Documentation if the other party agrees in writing to accept and be bound by the terms and conditions of this Agreement. If you transfer the Software and Documentation, you must at the same time either transfer all copies of the Software and Documentation to the party or you must destroy any copies not transferred. Except as set forth above, you may not assign or transfer your rights under this Agreement.

Modification, reverse engineering, reverse compiling, or disassembly of the Software is expressly prohibited. However, if you are a European Union ("EU") resident, information necessary to achieve interoperability of the Software with other programs within the meaning of the EU Directive on the Legal Protection of Computer Programs is available to you from 3Com upon written request.

EXPORT RESTRICTIONS: The Software, including the Documentation and all related technical data (and any copies thereof) (collectively "Technical Data"), is subject to United States Export control laws and may be subject to export or import regulations in other countries. In addition, the Technical Data covered by this Agreement may contain data encryption code which is unlawful to export or transfer from the United States or country where you legally obtained it without an approved U.S. Department of Commerce export license and appropriate foreign export or import license, as required. You agree that you will not export or re-export the Technical Data (or any copies thereof) or any products utilizing the Technical Data in violation of any applicable laws or regulations of the United States or the country where you legally obtained it. You are responsible for obtaining any licenses to export, re-export or import the Technical Data.

In addition to the above, the Product may not be used, exported or re-exported (i) into or to a national or resident of any country to which the U.S. has embargoed; or (ii) to any one on the U.S. Commerce Department's Table of Denial Orders or the U.S. Treasury Department's list of Specially Designated Nationals.

TRADE SECRETS; TITLE: You acknowledge and agree that the structure, sequence and organization of the Software are the valuable trade secrets of 3Com and its suppliers. You agree to hold such trade secrets in confidence. You further acknowledge and agree that ownership of, and title to, the Software and Documentation and all subsequent copies thereof regardless of the form or media are held by 3Com and its suppliers.

UNITED STATES GOVERNMENT LEGENDS: The Software, Documentation and any other technical data provided hereunder is commercial in nature and developed solely at private expense. The Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a commercial item as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in this Agreement, which is 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov. 1995) or FAR 52.227-14 (June 1987), whichever is applicable.

TERM AND TERMINATION: The licenses granted hereunder are perpetual unless terminated earlier as specified below. You may terminate the licenses and this Agreement at any time by destroying the Software and Documentation together with all copies and merged portions in any form. The licenses and this Agreement will also terminate immediately if you fail to comply with any term or condition of this Agreement. Upon such termination you agree to destroy the Software and Documentation, together with all copies and merged portions in any form.

LIMITED WARRANTIES AND LIMITATION OF LIABILITY: All warranties and limitations of liability applicable to the Software are as stated on the Limited Warranty Card or in the product manual, whether in paper or electronic form, accompanying the Software. Such warranties and limitations of liability are incorporated herein in their entirety by this reference.

GOVERNING LAW: This Agreement shall be governed by the laws of the State of California, U.S.A. excluding its conflicts of laws principles and excluding the United Nations Convention on Contracts for the International Sale of Goods.

SEVERABILITY: In the event any provision of this Agreement is found to be invalid, illegal or unenforceable, the validity, legality and enforceability of any of the remaining provisions shall not in any way be affected or impaired and a valid, legal and enforceable provision of similar intent and economic impact shall be substituted therefor.

ENTIRE AGREEMENT: This Agreement sets forth the entire understanding and agreement between you and 3Com and supersedes all prior agreements, whether written or oral, with respect to the Software and Documentation, and may be amended only in a writing signed by both parties.

Should you have any questions concerning this Agreement or if you desire to contact 3Com for any reason, please contact the 3Com subsidiary serving your country, or write:

3Com Corporation, 350 Campus Drive, Marlborough, MA USA 01752-3064

This product contains encryption and may require U.S. and/or local government authorisation prior to export or import to another country.

ISP INFORMATION

Information Regarding Popular ISPs

Internet Connection Types	Characteristics	Popular ISPs
Dynamic IP (Clone MAC)	Cable modem ISP, non-hostname based. Need to clone MAC in the DHCP page of router.	MediaOne, RoadRunner, Optimum Online, Time Warner, Charter and Adelphia, Metrocast, RCN
Dynamic IP (Hostname)	Cable ISP, Requires Hostname to authenticate i.e. cx213818-B. Need to enter the hostname in the DHCP page of the router, exactly as it appears in your documentation.	@Home Network, Cogoco, ComCast, Cox, Excite, Rogers, Shaw, Insight, Videotron
PPPoE (DSL)	Usually special software installed on PC, MacPOET/WinPOET, EnterNet 300. The VPN Firewall has this software built in and you can safely remove it from your PC. You will need to enter the account name and password that your ISP provided to you in the PPPoE page of the Firewall. Leave the service name blank unless your ISP requires it.	Bell*, Century Tel, Citizens, Primus, Prodigy, Snet, Sprint FC, Verizon, First World, Brightnet, Earthlink, Ameritech, Covad, Mindspring, Sympatico DSL, USwest, Qwest, SNet

Internet Connection Types	Characteristics	Popular ISPs
PPTP	Cable or DSL, always on. Some European ISPs require a PPTP tunnel to authenticate their network.	KPN (Netherlands), Austria Telecom
Static (DSL)	DSL Modem, always on. Need to enter ALL IP information from ISP in the "Static IP" section of the Firewall.	CableSpeed, Cnet, Direct Link, Drizzle, DSL Extreme, Earthlink Wireless, Fast Point, Flashcom, GTE-WhirlWind, Heavenet, HSA Corp, I-55, InterAccess, LinkLine, Mission, Nauticom, NAS, Omitel, Onterra, Phatpipe, Rhythms, Speakeasy, Sterling, XO, Zyan
Static (Cable)	Cable Modem, Always on, ISP assigns specific IP information which needs to be entered on the "Static IP" page of the Firewall.	Cox Cable, Sprint, US Cable, Cable-Cable
* Bell includes Bell Advantage, Bell Canada, Bell South, PacBell and Southwestern Bell		

GLOSSARY

10BASE-T

The IEEE specification for 10 Mbps Ethernet over Category 3, 4 or 5 twisted pair cable.

100BASE-TX

The IEEE specification for 100 Mbps Fast Ethernet over Category 5 twisted-pair cable.

3DES

Triple DES (See DES). 3DES is an extremely secure 168 bit encryption system that works by applying the DES encryption system three times on the same message using different keys. It is typically used in military applications where it is expected that the VPN traffic will be intercepted and an effort made to decode it.

AES

Advanced Encryption Standard. A 256 bit FIPS-approved symmetric encryption algorithm that may be used by U.S. Government organizations (and others) to protect sensitive information. AES provides much higher security than 3DES.

Auto-negotiation

Some devices in the OfficeConnect range support auto-negotiation. Auto-negotiation is where two devices sharing a link, automatically configure to use the best common speed. The order of preference (best first) is: 100BASE-TX full duplex, 100BASE-TX half duplex, 10BASE-T full duplex, and 10BASE-T half duplex. Auto-negotiation is defined in the IEEE 802.3 standard for Ethernet and is an operation that takes place in a few milliseconds.

Bandwidth

The information capacity, measured in bits per second, that a channel can transmit. The bandwidth of Ethernet is 10 Mbps, the bandwidth of Fast Ethernet is 100 Mbps.

Category 3 Cables

One of five grades of Twisted Pair (TP) cabling defined by the EIA/TIA-586 standard. Category 3 is voice grade cable and can only be used in Ethernet networks (10BASE-T) to transmit data at speeds of up to 10 Mbps.

Category 5 Cables

One of five grades of Twisted Pair (TP) cabling defined by the EIA/TIA-586 standard. Category 5 can be used in Ethernet (10BASE-T) and Fast Ethernet networks (100BASE-TX) and can transmit data up to speeds of 100 Mbps. Category 5 cabling is better to use for network cabling than Category 3, because it supports both Ethernet (10 Mbps) and Fast Ethernet (100 Mbps) speeds.

Client

The term used to described the desktop PC that is connected to your network.

DES

Data Encryption Standard. DES is one of the encryption protocols that can be used by an IPSec Virtual Private Network. It is a strong encryption standard only currently exceeded in security by 3DES.

DHCP

Dynamic Host Configuration Protocol. This protocol automatically assigns an IP address for every computer on your network. Windows 95, Windows 98 and Windows NT 4.0 contain software that assigns IP addresses to workstations on a network. These assignments are made by the DHCP server software that runs on Windows NT Server, and Windows 95 and Windows 98 will call the server to obtain the address. Windows 98 will allocate itself an address if no DHCP server can be found.

DNS

Domain Name System. DNS allows Internet host computers to have a domain name (such as 3com.com) and one or more IP addresses (such as 192.34.45.8). A DNS server keeps a database of host computers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing "3com.com" into your Internet browser), the user is sent to the proper IP address. The DNS server address used by the computers on your home network is the location of the DNS server your ISP has assigned.

DSL modem

Digital Subscriber Line. A DSL modem uses your existing phone lines to send and receive data at high speeds.

Ethernet

A LAN specification developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks use CSMA/CD to transmit packets at a rate of 10 Mbps over a variety of cables.

Ethernet Address

See MAC address.

Fast Ethernet

An Ethernet system that is designed to operate at 100 Mbps.

Firewall

Electronic protection that prevents anyone outside of your network from seeing your files or damaging your computers.

Full Duplex

A system that allows packets to be transmitted and received at the same time and, in effect, doubles the potential throughput of a link.

Gateway

A device that acts as a central hub by connecting to each computer's network interface card and managing the data traffic between the local network and the Internet.

Half Duplex

A system that allows packets to transmitted and received, but not at the same time. Contrast with full duplex.

Hub

A device that regenerates LAN traffic so that the transmission distance of that signal can be extended. Hubs are similar to repeaters, in that they connect LANs of the same type; however they connect more LANs than a repeater and are generally more sophisticated.

IEEE

Institute of Electrical and Electronics Engineers. This American organization was founded in 1963 and sets standards for computers and communications.

IETF

Internet Engineering Task Force. An organization responsible for providing engineering solutions for TCP/IP networks. In the network management area, this group is responsible for the development of the SNMP protocol.

IP

Internet Protocol. IP is a layer 3 network protocol that is the standard for sending data through a network. IP is part of the TCP/IP set of protocols that describe the routing of packets to addressed devices. An IP address consists of 32 bits divided into two or three fields: a network number and a host number or a network number, a subnet number, and a host number.

IP Address

Internet Protocol Address. A unique identifier for a device attached to a network using TCP/IP. The address is written as four octets separated with periods (full-stops), and is made up of a network section, an optional subnet section and a host section.

IPSec

IPSec (**Internet Protocol Security**) is a VPN encryption protocol based on TCP/IP. It is a flexible protocol with a wide range of encryption options. IPSec is commonly used for both connections between separate private networks and for connections between remote PCs and private networks.

ISP

Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

LAN

Local Area Network. A network of end stations (such as PCs, printers, servers) and network devices (hubs and switches) that cover a relatively small geographic area (usually not larger than a floor or building). LANs are characterized by high transmission speeds over short distances (up to 1000 metres).

L2TP over IPSec

L2TP over IPSec is a combination of protocols commonly used to authenticate a user (L2TP) and encrypt data (using IPSec).

MAC

Media Access Control. A protocol specified by the IEEE for determining which devices have access to a network at any one time.

MAC Address

Media Access Control Address. Also called the hardware, physical or Ethernet address. A layer 2 address associated with a particular network device. Most devices that connect to a LAN have a MAC address assigned to them as they are used to identify other devices in a network. MAC addresses are 6 bytes long.

NAT

Network Address Translation. NAT enables all the computers on your network to share one IP address. The NAT capability of the Firewall allows you to access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.

Network

A Network is a collection of computers and other computer equipment that are connected for the purpose of exchanging information or sharing resources. Networks vary in size, some are within a single room, others span continents.

Network Interface Card (NIC)

A circuit board installed into a piece of computing equipment, for example, a computer, that enables you to connect it to the network. A NIC is also known as an adapter or adapter card.

Ping

Packet **In**ternet **G**roper. An internet utility used to determine whether a particular IP address is online. It is used to test and debug a network by sending out a packet and waiting for a response.

Protocol

A set of rules for communication between devices on a network. The rules dictate format, timing, sequencing and error control.

PPPoE

Point-to-Point Protocol over Ethernet. Point-to-Point Protocol is a method of secure data transmission originally created for dial-up connections; PPPoE is for Ethernet connections.

PPTP

Point-to-Point Tunnelling Protocol. PPTP is a simple VPN encryption protocol based on the Point to Point protocol. It is most frequently used to connect remote PCs to private networks.

RIP

Routing Information Protocol. A simple routing protocol that is part of the TCP/IP protocol suite. It determines a route based on the smallest hop count between source and destination. RIP is a distance vector protocol that routinely broadcasts routing information to its neighbouring routers.

Router

Protocol dependant device that connects subnetworks together. Routers are useful in breaking down a very large network into smaller subnetworks, they introduce longer delays and typically have much lower throughput rates than bridges.

RJ-45

A standard connector used to connect Ethernet networks. The "RJ" stands for "registered jack".

Server

A computer in a network that is shared by multiple end stations. Servers provide end stations with access to shared network services such as computer files and printer queues.

SPI

Stateful Packet Inspection. This feature requires the firewall to remember what outgoing requests have been sent and only allow responses to those requests back through the firewall. This way, un-requested attempts to access the network will be denied.

Subnet Address

An extension of the IP addressing scheme that allows a site to use a single IP network address for multiple physical networks.

Subnet mask

A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet, which must assigned by InterNIC).

Subnets

A network that is a component of a larger network.

Switch

A device that interconnects several LANs to form a single logical LAN that comprises of several LAN segments. Switches are similar to bridges, in that they connect LANs of a different type; however they connect more LANs than a bridge and are generally more sophisticated.

TCP/IP

Transmission Control Protocol/Internet Protocol. This is the name for two of the most well-known protocols developed for the interconnection of networks. Originally a UNIX standard, TCP/IP is now supported on almost all platforms, and is the protocol of the Internet.

TCP relates to the content of the data travelling through a network — ensuring that the information sent arrives in one piece when it reaches its destination. IP relates to the address of the end station to which data is being sent, as well as the address of the destination network.

Traffic

The movement of data packets on a network.

VPN

Virtual Private Network. A VPN is a private network where the data is passed across a public network infrastructure such as the Internet. The data is kept private by using encryption.

WAN

Wide Area Network. A network that connects computers located in geographically separate areas (for example, different buildings, cities, or countries). The Internet is an example of a wide area network.

Wizard

A Windows application that automates a procedure such as installation or configuration.

INDEX

Regulatory Notices

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules, and the Canadian Department of Communications Equipment Standards entitled, "Digital Apparatus," ICES-003. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

Information to the User

If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient the receiving antenna.
- Relocate the equipment with respect to the receiver.
- Move the equipment away from the receiver.
- Plug the equipment into a different outlet so that equipment and receiver are on different branch circuits.
- Consult the dealer or an experienced radio/television technician for help.

The user may find the following booklet prepared by the Federal Communications Commission helpful:

How to Identify and Resolve Radio-TV Interference Problems

This booklet is available from the U.S. Government Printing Office, Washington, DC 20402, Stock No. 004-000-00345-4. In order to meet FCC emissions limits, this equipment must be used only with cables which comply with IEEE 802.3.

CE Statement (Europe)

This product complies with the European Low Voltage Directive 73/23/EEC and EMC Directive 89/336/EEC as amended by European Directive 93/68/EEC.

CSA Statement

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

VCCI Statement

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい。

DUA08709-5AAA03
Published January 2004