Wireless Data Privacy Configuration Guide

HP ProCurve
Secure Access
700wl Series

www.hp.com/go/hpprocurve

HP PROCURVE

SECURE ACCESS 700WL SERIES

WIRELESS DATA PRIVACY CONFIGURATION GUIDE

Publication Number

5990-5989
July 2003
Edition 1

Applicable Products

HP ProCurve Access Controller 720wl	(J8153A)
HP ProCurve Access Control Server 740wl	(J8154A)
HP ProCurve Integrated Access Manager 760wl	(J8155A)
HP ProCurve 700wl 10/100 Module	(J8156A)
HP ProCurve 700wl Gigabit-SX Module	(J8157A)
HP ProCurve 700wl Gigabit-LX Module	(J8158A)
HP ProCurve 700wl 10/100/1000Base-T	(J8159A)
HP ProCurve 700wl Acceleration Module	(J8160A)

Trademark Credits

Windows NT®, Windows®, and MS Windows® are US registered trademarks of Microsoft Corporation.

Disclaimer

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Warranty

See the Customer Support / Warranty booklet included with the product.

A copy of the specific warranty terms applicable to your Hewlett-Packard products and replacement parts can be obtained from your HP Sales and Service Office or authorized dealer.

CONTENTS

PREFACE

This preface describes the audience, use, and organization of the *HP ProCurve Secure Access 700wl Series Wireless Data Privacy Configuration Guide.* It also outlines the document conventions, related documentation, support information, and revision history.

Audience

The primary audience for this document are network administrators who want to enable their network users to communicate using the 700wl Series system. This document is intended for authorized personnel who have previous experience working with network telecommunications systems or similar equipment. It is assumed that the personnel using this document have the appropriate background and knowledge to complete the procedures described in this document.

How To Use This Document

This document contains procedural information describing how to configure an HP ProCurve Integrated Access Manager 760wl or an HP ProCurve Access Control Server 740wl to provide support for client connections via IPsec, PPTP (Point-to-Point Tunneling Protocol), and L2TP/IPsec (Layer 2 Tunnel Protocol over IPsec). It also describes how to configure the client system to use an IPsec, PPTP, or L2TP/IPsec client for its VPN connection.

Where applicable, navigation aids also refer you to supplemental information such as figures, tables, and other procedures in this document or another document. Main chapters are followed by supplemental information such as appendices and an index.

Organization

This document is organized as follows.

Chapter 1 — Overview of Security Protocols

This chapter provides an overview of the security protocols that can be used with the 700wl Series system.

Chapter 2 — Configuring Security on the 700wl Series

This chapter describes the configuration of the 700wl Series Rights Manager.

Chapter 3 — Client Configuration

This chapter describes client security configuration.

Chapter 4 — Setup Scripts for L2TP/IPSec on Windows 2000 or XP

This chapter describes the use of scripts to setup L2TP/IPSec connections on Windows systems.

Related Documentation

The following lists related documentation:

- *HP ProCurve Secure Access 700wl Series Management and Configuration Guide*
- *HP ProCurve Secure Access 700wl Series Release Notes*

Document Conventions

The following text conventions are used in this document:

Table 1. Text Conventions

Convention	Definition
Boldface Arial	Screen menus that you click to select, commands that you select, or field names are in boldface Arial.
Boldface Italic Palatino	New terms that are introduced are in boldface italic Palatino.
Italic Palatino	Emphasized terms are in italic Palatino.
`Courier`	Filenames and text that you type are in `Courier`.

The following icons are used to alert you to important information.

Table 2. Alert Icons

Icon	Notice Type	Alerts you to...
None	Note	Helpful suggestions or information that is of special importance in certain situations.
None	Caution	Risk of loss of system functionality or loss of data.
	Warning	Risk of personal injury, system damage, or irrecoverable loss of data.

Support Information

See the HP ProCurve Networking web site at `www.hp.com/go/procurve`. Click on **technical support** and select **support services** for a list of available support resources and options for contacting HP.

OVERVIEW OF SECURITY PROTOCOLS 1

This chapter provides an overview of security protocols. It consists of the following sections:

Wireless Data Privacy in the HP ProCurve 700wl Series System

The HP ProCurve Secure Access 700wl Series is used to enhance the security and availability of client connections at the edge of the network. The connections can be made from both wired and wireless networks.

The client must be authenticated by the 700wl Series system before he/she can gain access to the network. The client connection can be secured through a Virtual Private Network (VPN) established between the client system and the 700wl Series system.

This document describes how to configure the HP ProCurve Integrated Access Manager 760wl to provide support for client connections via IPSec, PPTP (Point-to-Point Tunneling Protocol), and L2TP/IPSec (Layer 2 Tunnel Protocol over IPSec). It also describes how to configure the client system to use an IPSec, PPTP, or L2TP/IPSec client for its VPN connection. The client configuration procedures are described based on Windows XP, Windows 2000, Windows 98, and Apple's MacOS 9.

The configuration procedures described in this document are also applicable for a 700wl Series system using a combination of HP ProCurve Access Control Server 740wl and Access Controller 720wl instead of the Integrated Access Manager 760wl.

IPSec

IPSec is a protocol suite that provides security services at the IP layer. IPSec enables a system to select required security protocols, determine the algorithm(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services.

IPSec can be used to protect communications between a pair of security gateways, or between a security gateway and a host. In a 700wl Series system, the Integrated Access Manager and Access Controller are used as the security gateway.

IPSec uses two protocols to provide traffic security: Authentication Header (AH) and Encapsulating Security Payload (ESP). See more details on these two protocols in RFCs 2402[5] and 2406[6], respectively.

The Integrated Access Manager 760wl and Access Controller 720wl only provide support for the IPSec ESP protocol. ESP completely encapsulates user data and provides optional authentication. Cryptographic keys or shared secret values are used for both authentication/integrity and encryption services. IPSec relies on a separate set of mechanisms for putting these keys in place, one of which uses the Internet Key Exchange (IKE) protocol. IKE is used between the client and the security gateway for negotiating what kind of IPSec attributes to use. The attributes are, for example, the encryption algorithm, the authentication algorithm, and the key length, and so on.

This document describes how to configure both the IPSec client and server. Two applications, namely SafeNet SoftRemote and PGPnet, are used as IPSec clients on Windows platforms. PGPnet is also available for Mac OS 9 and is very similar in configuration to the PGPnet for Windows.

PPTP

Point-to-Point Tunneling Protocol (PPTP) is a network protocol used to secure Point-to-Point (PPP) connections by creating a VPN (tunneling) across a public TCP/IP network. The security of a VPN relies on the strength of authentication and encryption protocols used.

This document describes PPTP-based security only on the Microsoft implementation.

Authentication protocols used in Microsoft PPTP include the Microsoft Challenge/Reply Handshake Protocol (MS-CHAP) and its new version MS-CHAPv2.

The encryption protocol used in Microsoft PPTP is Microsoft Point to Point Encryption (MPPE). The minimum encryption key length for PPTP is 40 bits, and the maximum is 128 bits.

Configuration of both the PPTP client and server to use MS-CHAPv2 with the 128-bit encryption key length is described.

L2TP over IPSec

Layer-2 Tunneling Protocol (L2TP) is an extension of PPP similar to PPTP described in the previous section. L2TP tunnels PPP traffic across a public TCP/IP network.

L2TP inherits the authentication, encryption, and compression control protocols from PPP. It also includes support for tunnel authentication, which can be used to mutually authenticate the tunnel endpoints. However, L2TP does not define tunnel protection mechanisms.

The IPSec protocol suite described in Section 2.1 can be used to protect the L2TP traffic over IP networks. The implementation of L2TP using IPSec is referred to as *L2TP over IPSec* (L2TP/IPSec). See more details in RFC 3193[8].

This document describes how to configure both the L2TP/IPSec client and server. Windows XP and Windows 2000 are used as L2TP/IPSec clients.

SSH

Secure Shell (SSH) is a UNIX-based command interface and protocol for users on a local computer (SSH Client) to log into and execute commands on a remote computer (SSH Server).

SSH provides secure encrypted communications between the local and remote computers, which include X11 connections and applications running on arbitrary TCP/IP ports. Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted. SSH uses RSA public key cryptography for both connection and authentication. Encryption algorithms include AES (SSH2 only), Blowfish, 3DES, and DES.

There are two versions of SSH: version 1 (SSH1) and version 2 (SSH2). SSH2, the latest version, is a proposed set of standards from the Internet Engineering Task Force (IETF). The 700wl Series system supports both versions.

SSH is widely used among network administrators to control Web and other application servers remotely. SSH is also available on Microsoft Windows and Apple MacOS platforms.

This document describes how to configure the 700wl Series system to function as the SSH server. A freeware application, named “PuTTY” is used as the SSH client on a Windows platform. User traffic is tunneled through the opened SSH session into the network.

2 CONFIGURING SECURITY ON THE 700WL SERIES

This chapter provides an overview of the HP ProCurve 700wl Series system wireless data privacy configuration. It consists of the following sections:

Configuration Overview

There are two parts to the configuration procedure for each security protocol. The first part is to configure the security protocol for each *Location*, using the Rights Manager interface in either the Access Control Server 740wl or the Integrated Access Manager 760wl. The second is to enable the selected VPN protocols using the Wireless Data Privacy settings through the Administrative Interface. This globally enables these protocols for all Access Controllers in the system.

You may access the Administrative Interface of an Integrated Access Manager either from the secured side of the network, or through a client (downlink) port. You can connect to an Access Control Server only from the network, because the Access Control Server does not have any client ports.

To access the Administrative Interface from the network, point your browser to the IP address or host name of the unit you want to access. The special IP address used for referencing the 700wl Series unit through a downlink port is `42.0.0.1`.

For all examples in this document, the 700wl Series built-in authentication service is assumed as the method used to authenticate users.

IPSec Configuration

This section describes how to configure the HP ProCurve Integrated Access Manager 760wl as the VPN Gateway for IPSec clients. Note that the Integrated Access Manager serves as both the Access Control Server and the Access Controller in one system.

Configuring the Rights Manager for IPSec

Do the following to configure the Rights Manager:

Step 1. To access the Administrative Interface from the network, set your browser to the IP address or hostname of the Integrated Access Manager or Access Control Server. If your system is connected through a downlink port on an Integrated Access Manager, set your browser to `https://42.0.0.1:445`.

Note that if you are connected to the client port and have not logged on to the network, you will see a Logon page on the screen when you first start the web browser. You may ignore the Logon page if you are configuring the Integrated Access Manager and then open the given URL to access the **Main Menu**. If you are configuring the Access Control Server you can either logon to the network as a normal user or access the unit from the secured side of the network. You can find the information on how to create a normal user account in *HP ProCurve 700wl Series Management and Configuration Guide*, accessible through the **HELP** menu.

Step 2. Enter the Administrator username and password in the appropriate fields and click **Login**.

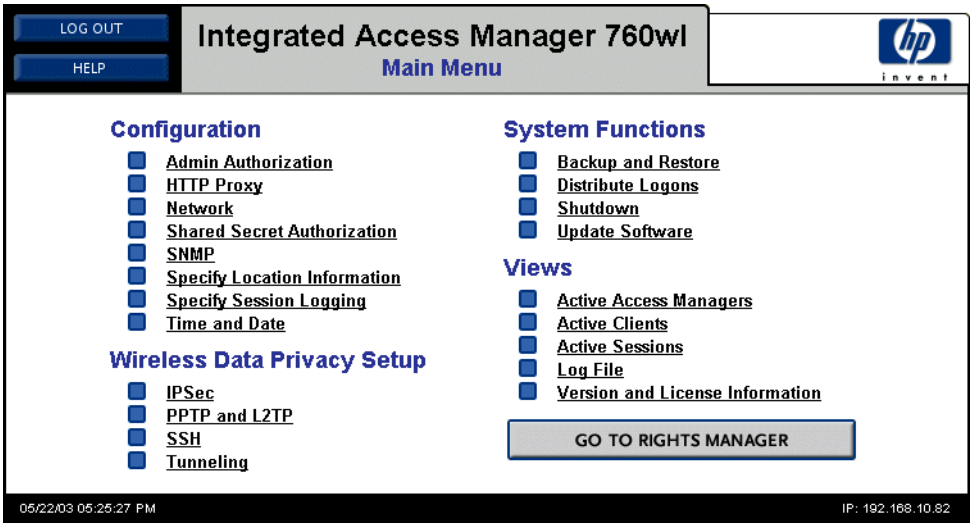

Figure 2-1. Main Menu on an Integrated Access Manager

Step 3. Click the **GOTO RIGHTS MANAGER** button to access the Rights Manager Clients page (see Figure 2-2).

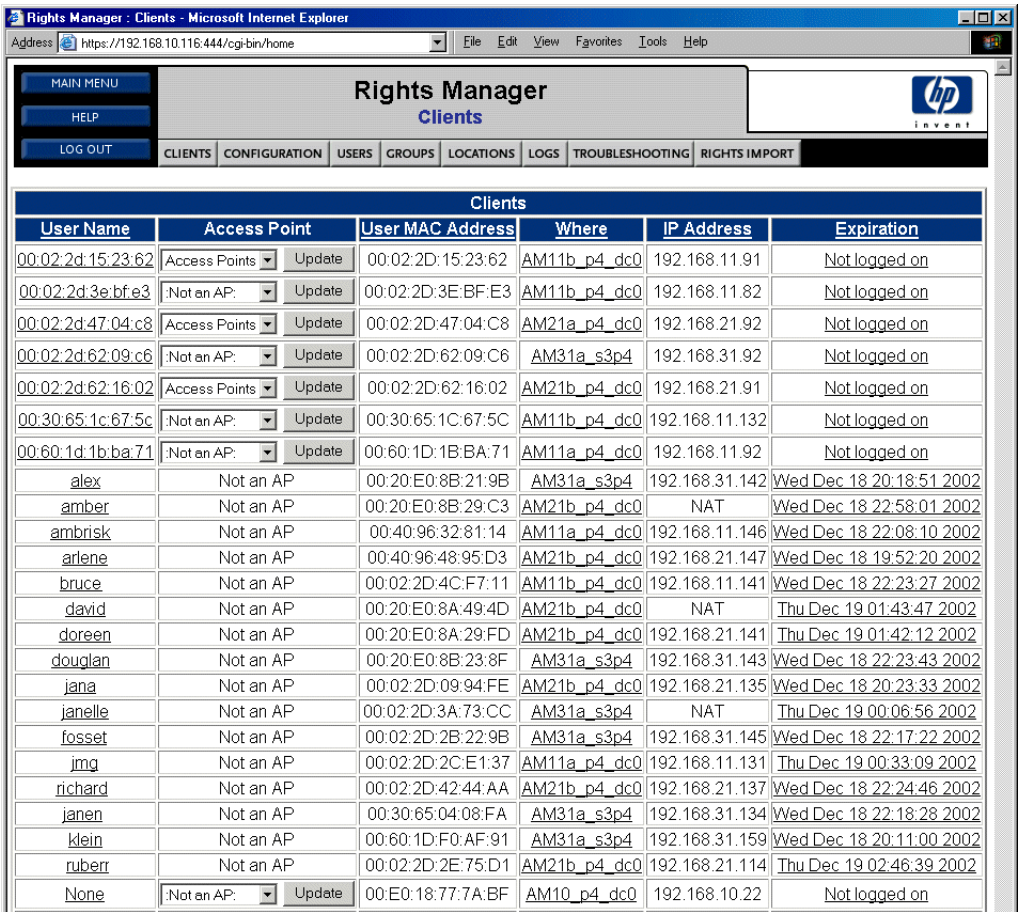

Figure 2-2. Rights Manager Clients page

Step 4. Click **CONFIGURATION** to access the Rights Manager's Configuration page.

Figure 2-3. Rights Manager Configuration Page

Step 5. Click **Encryption/Authentication per Location** in the Wireless Data Privacy Logon section of the **Configuration** Menu

The Encryption / Authentication per Location page appears, as shown in Figure 2-4.

Suppose you want to configure an existing location, named *Finance*, to support IPSec. Note that there is currently no encryption configured for that location.

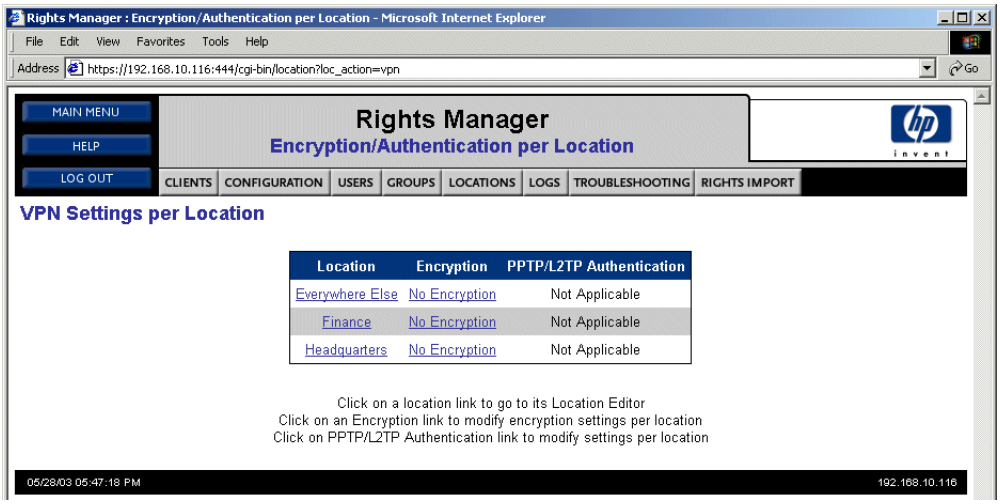

Figure 2-4. VPN Settings per Location table, with default settings

Step 6. Click **No Encryption** in the Finance row.

The Specify Encryption per Location page appears.

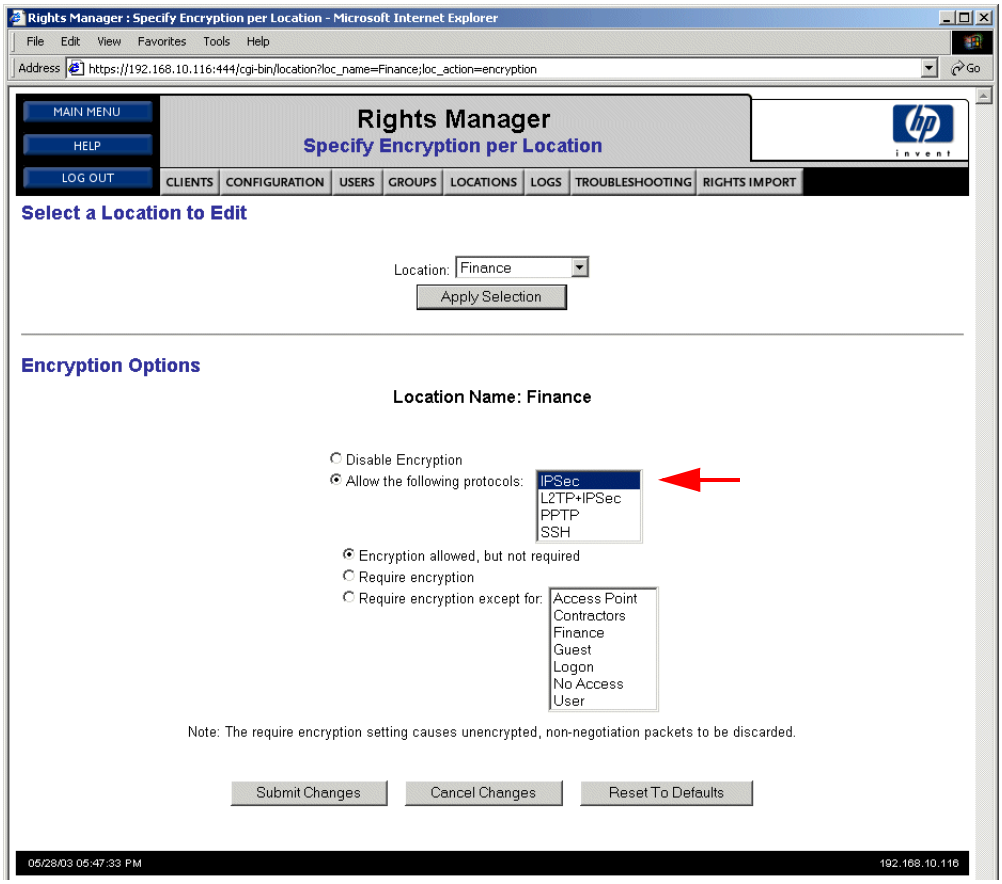

Figure 2-5. Setting IPSec on the Specify Encryption per Location page

Step 7. Select **Allow the following protocols** and then select **IPSec** from the list

If encryption is required for all clients connecting to this location, you must select the **Require encryption** option. Leaving the setting at **Encryption allowed by not required** allows access to unencrypted clients through this location as well.

Step 8. Click the **Submit Changes** button to save the settings.

To verify the new settings in the VPN Settings per Location page, click the Configuration tab and then Encryption / Authentication per Location. The new setting should appear in the VPN Settings per Location page (see Figure 2-6).

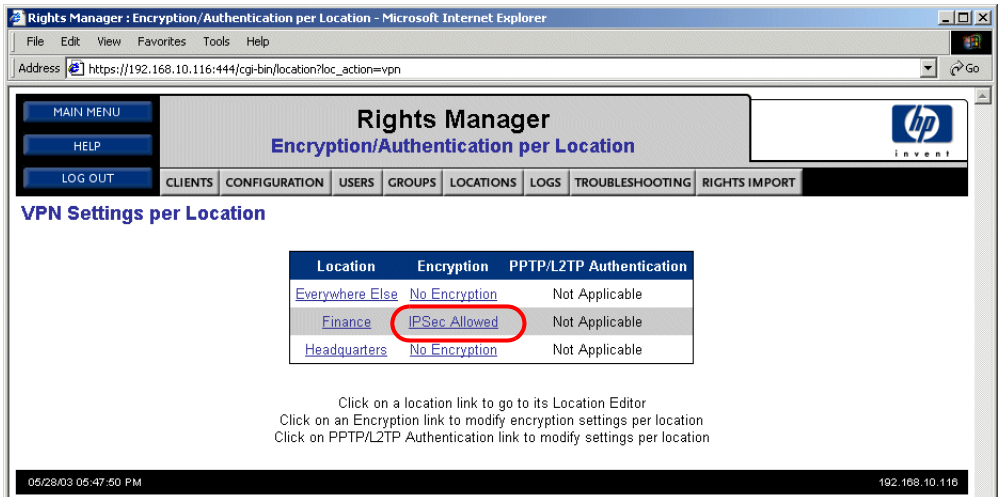

Figure 2-6. VPN Settings per Location table showing IPSec enabled for location Finance

Step 9. Since Finance is an existing location, you should refresh the group's rights in order to apply the new settings to active users.

Click **CLIENTS** at the top of the screen to go to the Rights Manager Clients page. Once the Clients page appears, click the **Refresh every client's rights** to refresh the rights of all users. Note that you may choose to refresh the client's rights on a per-user basis by clicking on each individual user's link in the Clients table.

Enabling IPSec Wireless Data Privacy

Enabling IPSec in the Wireless Data Privacy Setup is a global setting that affects all Access Controllers in the system. The following procedure is also applicable to an Access Control Server.

Do the following to enable IPSec:

Step 1. To access the Administrative Interface from the network, set your browser to the IP address or hostname of the Integrated Access Manager or Access Control Server. If your system is connected through a downlink port on an Integrated Access Manager, set your browser to `https://42.0.0.1:445`.

Step 2. Enter the Administrator username and password in the appropriate fields and click **Login**.

Step 3. Once the **Main** Menu appears, click **IPSec** in the Wireless Data Privacy Setup section of the **Main** Menu.

The IPSec Configuration page appears, as shown in Figure 2-7.

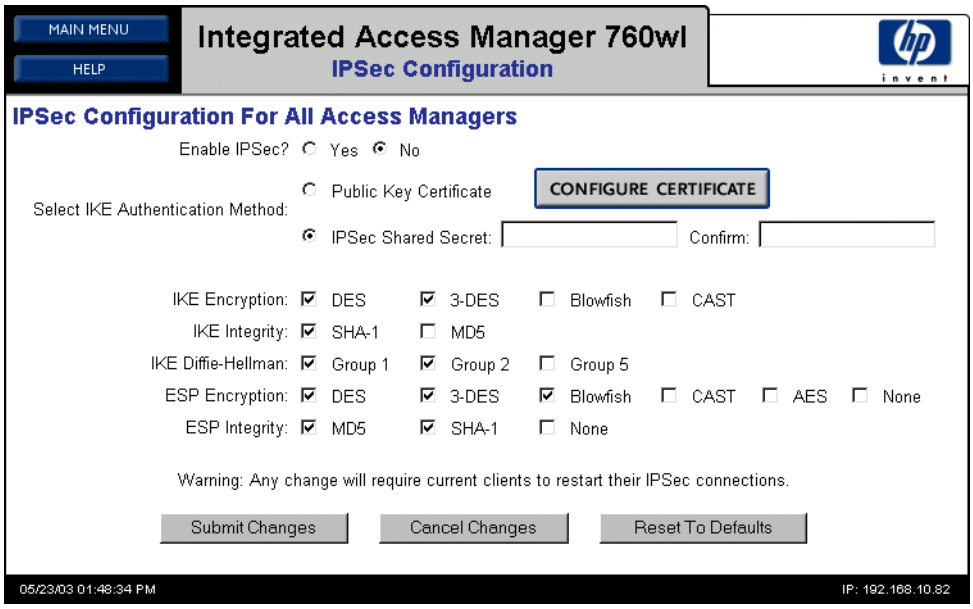

Figure 2-7. IPSec Configuration page

Step 4. Select **Yes** to enable IPSec.

Step 5. To use an IPSec shared secret, enter the secret in the appropriate field and confirm it in the second field.

You can use a Public Key Certificate as the alternative to using the shared secret. Click **CONFIGURE CERTIFICATE** to setup the Public Key Certificate. Make sure that the client uses the same certificate key and certificate authority when making IPSec connection to the Access Controller (please see the *HP ProCurve 700wl Series Management and Configuration Guide* for details).

Step 6. Make any necessary changes to the various settings for IKE Integrity, Encryption, ESP Integrity, Encryption, and so on.

Note: *If you plan to use PGPnet as the IPSec client software, you must enable MD5 for IKE Integrity. If you plan to use SSH Sentinel as the IPSec client software, you should enable AES for ESP Encryption. Otherwise, the client connection will fail.*

Step 7. Click **Submit Changes** to save the modification.

The Integrated Access Manager is now ready for the IPSec clients.

PPTP Configuration

This section describes how to configure the HP ProCurve Integrated Access Manager or Access Control Server as a PPTP server.

Configuring the Rights Manager for PPTP

Do the following to configure the Rights Manager:

Step 1. To access the Administrative Interface from the network, set your browser to the IP address or hostname of the Integrated Access Manager or Access Control Server. If your system is connected through a downlink port on an Integrated Access Manager, set your browser to `https://42.0.0.1:445`.

Step 2. Enter the Administrator username and password in the appropriate fields and click **Login**.

Note that if you are connected to the client port and have not logged on to the network, you will see a Logon page on the screen when you first start the web browser. You may ignore the Logon page if you are configuring the Integrated Access Manager and then open the given URL to access the **Main Menu**. If you are configuring the Access Control Server you can either logon to the network as a normal user or access the unit from the secured side of the network. You can find the information on how to create a normal user account in *HP ProCurve 700wl Series Management and Configuration Guide* accessible through the **HELP** menu.

Step 3. Once the **Main** Menu appears, click the **GOTO RIGHTS MANAGER** button to access the Rights Manager Clients page.

Step 4. Click **CONFIGURATION** to access the Rights Manager's Configuration page, as shown in Figure 2-8.

Figure 2-8. Rights Manager Configuration page

Step 5. Click **Encryption/Authentication per Location** in the Wireless Data Privacy Logon section of the **Configuration** Menu.

The Encryption / Authentication per Location page appears, as shown in Figure 2-9.

Suppose you want to configure an existing location, named *Finance*, to support PPTP encryption. Note that there is currently no encryption configured for that location.

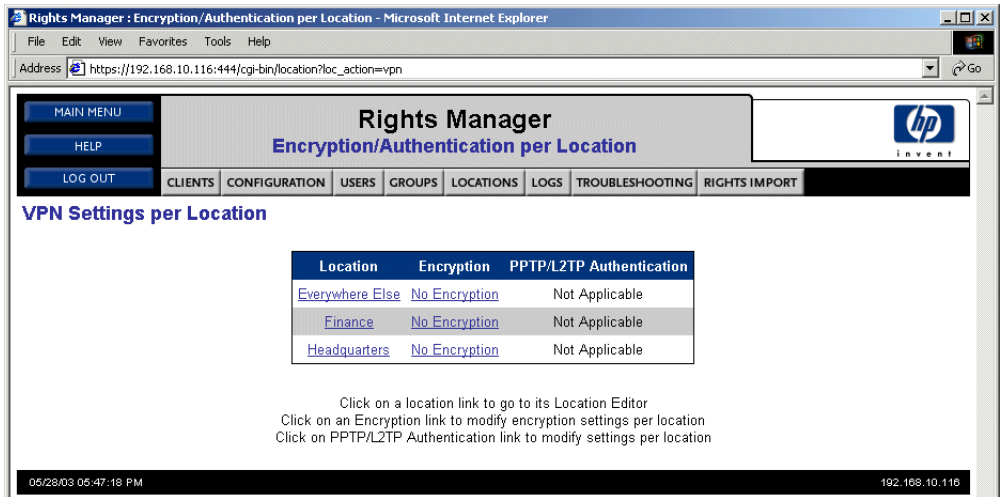

Figure 2-9. Encryption/Authentication per Location page, default settings

Step 6. Click **No Encryption** in the Finance row.

The Specify Encryption per Location page appears.

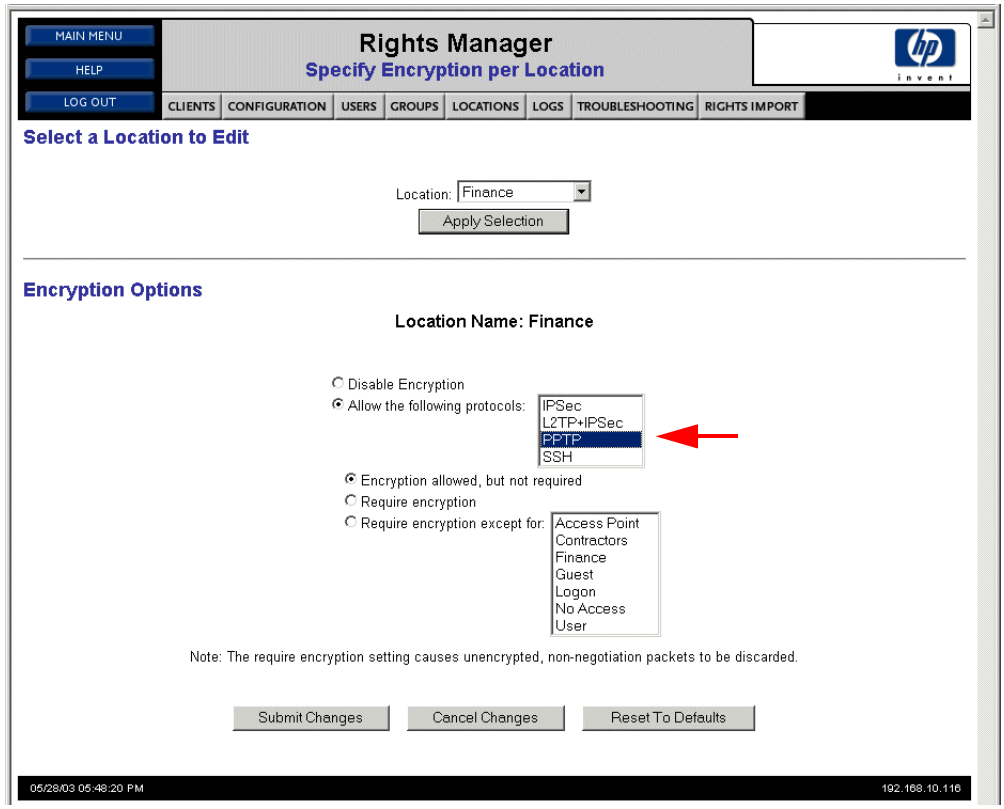

Figure 2-10. Setting PPTP on the Specify Encryption per Location page

Step 7. Select **Allow the following protocols** and then select **PPTP** from the list.

If encryption is required for all clients connecting to this location, select the **Require encryption** option. With this selection, the user must connect to the system using PPTP encryption, or the connecting attempt will fail. Leaving the setting at **Encryption allowed by not required** allows access to unencrypted clients through this location as well.

Step 8. Click **Submit Changes** to save the settings.

The new settings update the VPN Settings per Location table, as shown in Figure 2-11.

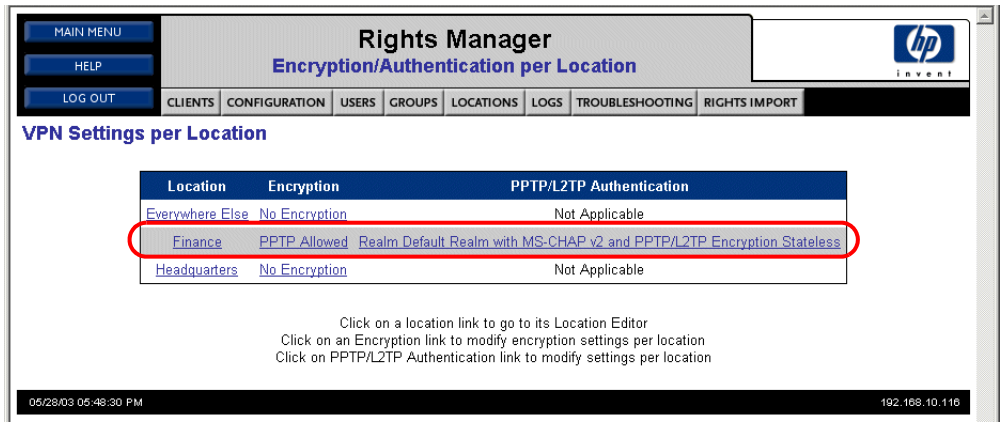

Figure 2-11. VPN Settings per Location table showing PPTP enabled

Step 9. Click **Realm Default Realm with MS-CHAP v2 and PPTP/L2TP Encryption Stateless** in the Finance row under the PPTP/L2TP column. This step is required in order to include an authentication realm in the encryption options.

The Specify PPTP/L2TP per Location page appears, as shown in Figure 2-12.

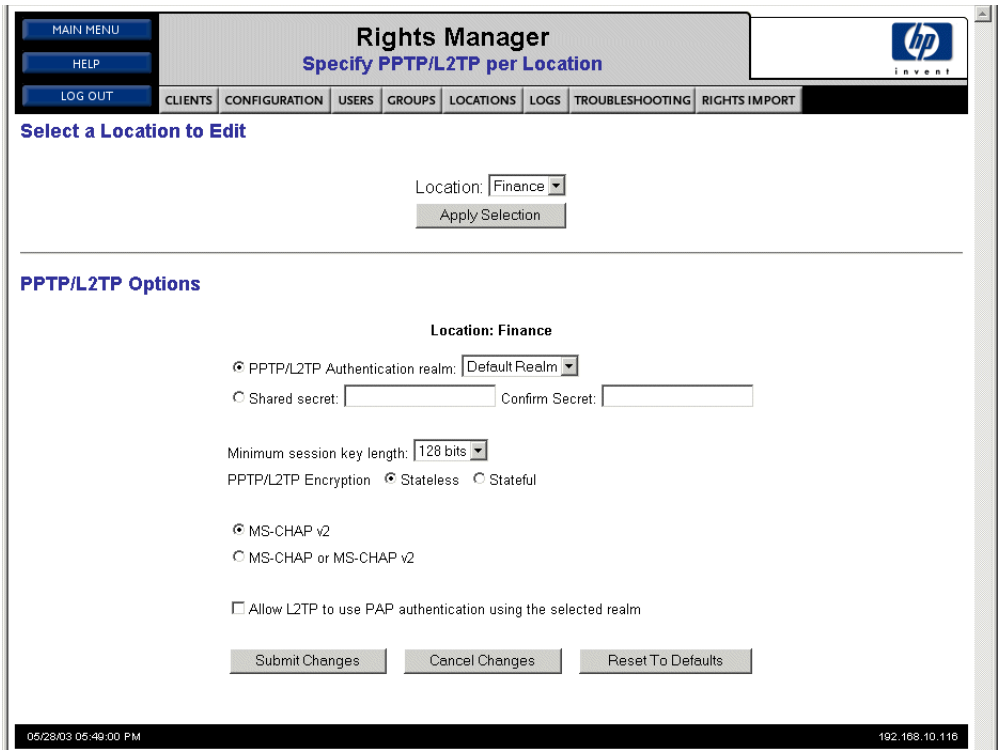

Figure 2-12. PPTP/L2TP Options for PPTP

Step 10. Select a realm to use for authentication or PPTP clients, or leave this set to the Default Realm,

Step 11. Click **Submit Changes** to save the settings.

The new settings update the PPTP / L2TP Authentication column of the VPN Settings per Location table.

Step 12. Since Finance is an existing location, you should refresh the group's rights in order to apply the new settings to active users.

a. Click **CLIENTS** at the top of the screen to go to the Rights Manager clients page.

b. Once, the client page appears, click **Refresh every client's rights** to refresh the rights of all users. You may choose to refresh the client's rights on a per-user basis by clicking on each individual user's link in the Clients table.

Enabling PPTP Wireless Data Privacy

Enabling IPSec in the Wireless Data Privacy Setup is a global setting that affects all Access Controllers in the system. The following procedure is also applicable to an Access Control Server.

Do the following to enable PPTP:

Step 1. To access the Administrative Interface from the network, set your browser to the IP address or hostname of the Integrated Access Manager or Access Control Server. If

your system is connected through a downlink port on an Integrated Access Manager, set your browser to `https://42.0.0.1:445`.

Step 2. You will be prompted for the Administrator username and password. Type the username and password in the appropriate text boxes and then click the **Login** button.

Step 3. Click **PPTP and L2TP** in the Wireless Data Privacy Setup section of the **Main** Menu.

The PPTP and L2TP Configuration page appears.

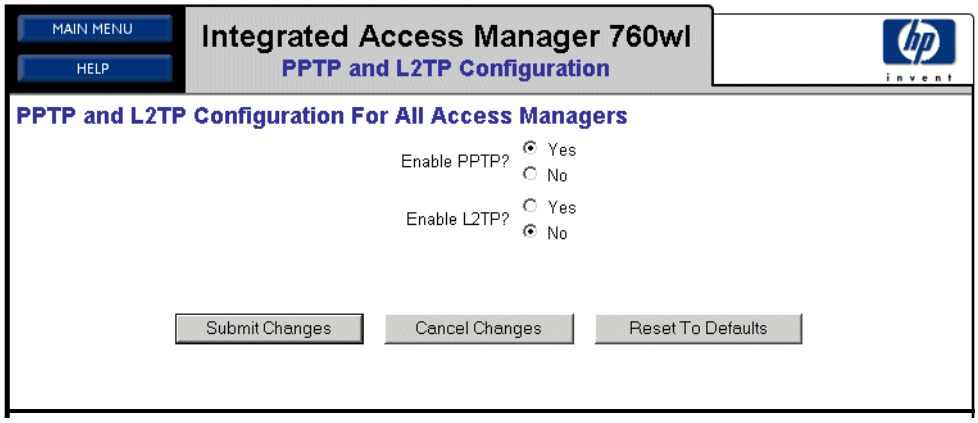

Figure 2-13. Enabling PPTP on the PPTP and L2TP Configuration page

Step 4. Select **Yes** to enable PPTP.

Step 5. Click the **Submit Changes** button to save the settings.

The Integrated Access Manager is now ready for the PPTP clients.

L2TP/IPSec Configuration

This section describes how to configure the Integrated Access Manager or Access Control Server as the L2TP / IPSec server.

Configuring the Rights Manager for L2TP/IPSec

Do the following to configure the Rights Manager:

Step 1. To access the Administrative Interface from the network, set your browser to the IP address or hostname of the Integrated Access Manager or Access Control Server. If your system is connected through a downlink port on an Integrated Access Manager, set your browser to `https://42.0.0.1:445`.

Step 2. Type the Administrator username and password in the appropriate fields and click **Login**.

If you are connected to a client port and have not logged on to the network, you will see a Logon page on the screen when you first start the web browser. You may ignore the Logon page if you are configuring the Integrated Access Manager and then open

the given URL to access the **Main** Menu. If you are configuring the Access Control Server you can either logon to the network as a normal user or access the unit from the secured side of the network. You can find the information on how to create a normal user account in the *HP ProCurve 700wl Series Management and Configuration Guide* accessible through the **HELP** menu.

Step 3. Once the **Main** Menu appears, click the **GOTO RIGHTS MANAGER** button to access the Rights Manager Clients page.

Step 4. Click **CONFIGURATION** to access the Rights Manager's Configuration page, then click **Encryption/Authentication per Location** in the Wireless Data Privacy Logon section of the **Configuration** Menu.

The Encryption / Authentication per Location page appears, as shown in Figure 2-14.

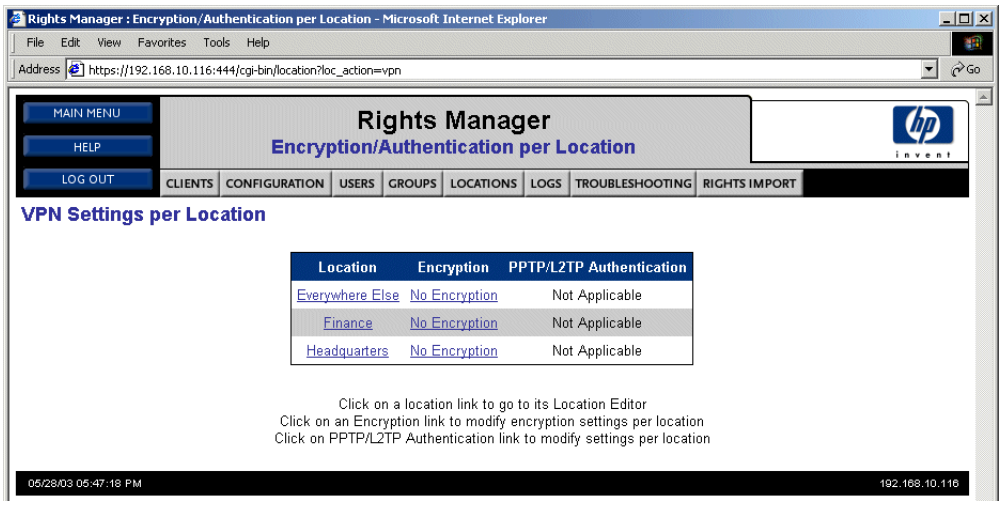

Figure 2-14. Encryption/Authentication per Location page, default settings

Suppose you want to configure an existing location, named *Finance*, to support L2TP / IPSec encryption. Note that there is currently no encryption configured for that location.

Step 5. Click **No Encryption** in the Finance row.

The Specify Encryption per Location page appears, as shown in Figure 2-15.

Figure 2-15. Setting L2TP with IPSec on the Specify Encryption per Location Page

Step 6. Select **Allow the following protocols** and then select **L2TP+IPSec** from the list

If encryption is required for all clients connecting to this location, you must select the **Require encryption** option. With this selection, the user must connect to the system using L2TP / IPSec encryption. Otherwise, the connecting attempt will fail.

Step 7. Click the **Submit Changes** button to save the settings.

The new settings will update the VPN Settings per Location table (Figure 2-16).

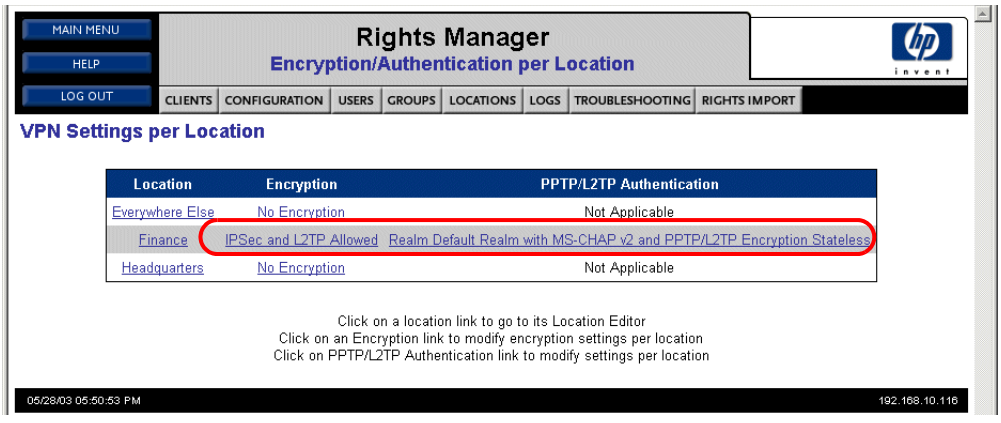

Figure 2-16. VPN Settings per Location table showing L2TP and IPSec enabled

Step 8. Click **Realm Default Realm with MS-CHAP v2 and PPTP/L2TP Encryption Stateless** in the Finance row under the PPTP/L2TP column. This step is required in order to include an authentication realm in the encryption options.

The Specify PPTP/L2TP per Location page appears, as shown in Figure 2-17.

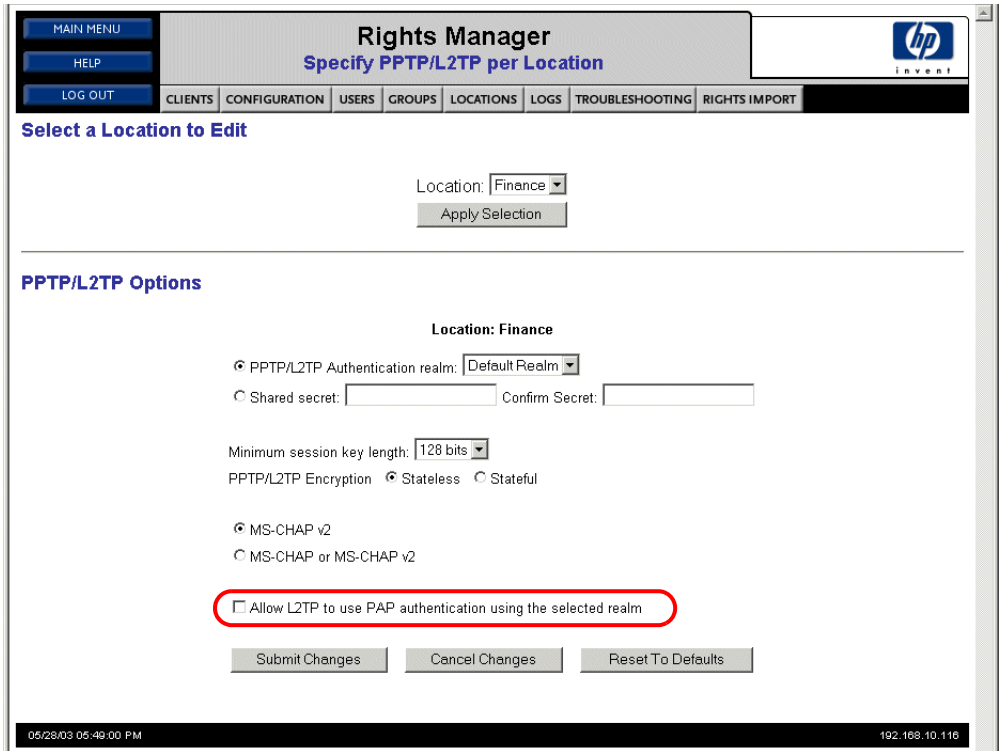

Figure 2-17. PPTP/L2TP Options for L2TP

Step 9. (Optional) If an external LDAP server is used to authenticate the user, selecting the **Allow L2TP to use PAP authentication** option enables the Rights Manager to obtain group information for the client from the LDAP server. This option allows the Rights Manager to assign the appropriate group rights to the user once authenticated. Group information from the LDAP server cannot be obtained through MS-CHAP v2 or MS-CHAP.

Once this option is selected, the user must also customize their L2TP/IPSec connection properties on the Windows client to use PAP as well. Please see details on the client-side configuration in Step 12 and 13 of "Windows XP Clients" and in Step 11 and 12 of "Windows 2000 Clients".

Step 10. Click **Submit Changes** to save the settings

The new settings update the PPTP/L2TP Authentication column of the VPN Settings per Location table.

Step 11. Since Finance is an existing location, you should refresh the group's rights in order to apply the new settings to active users.

a. Click **CLIENTS** at the top of the screen to go to the Rights Manager clients page.

b. Once, the client page appears, click **Refresh every client's rights** to refresh the rights of all users. You may choose to refresh the client's rights on a per-user basis by clicking on each individual user's link in the Clients table.

Enabling L2TP/IPSec Wireless Data Privacy

Enabling L2TP / IPSec in the Wireless Data Privacy settings must be done per Access Controller. The following procedures are also applicable to the Integrated Access Manager.

Since this security protocol is L2TP over IPSec, you are required to enable not only L2TP but also IPSec.

Do the following to enable L2TP / IPSec:

Step 1. To access the Administrative Interface from the network, set your browser to the IP address or hostname of the Integrated Access Manager or Access Control Server. If your system is connected through a downlink port on an Integrated Access Manager, set your browser to `https://42.0.0.1:445`.

Step 2. You will be prompted for the Administrator username and password. Type the username and password in the appropriate text boxes and then click the **Login** button.

Step 3. Click **PPTP and L2TP** in the Wireless Data Privacy Setup section of the **Main** Menu.

The PPTP and L2TP Configuration page appears.

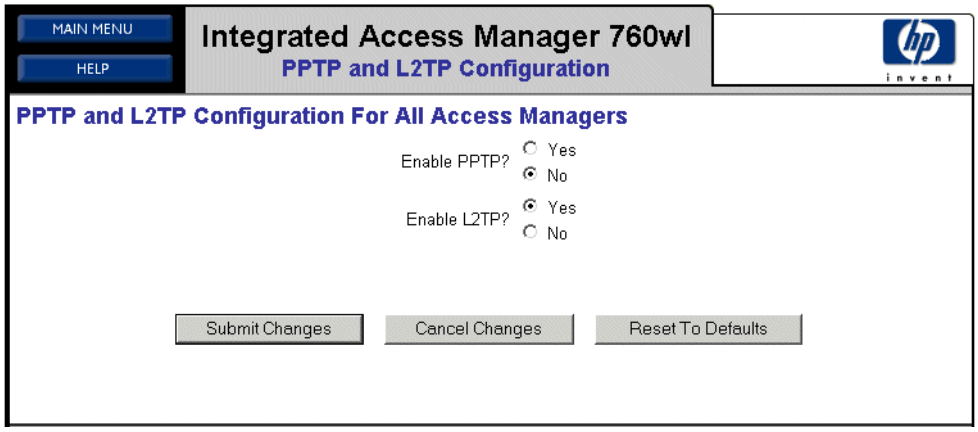

Figure 2-18. Enabling L2TP on the PPTP and L2TP Configuration page

Step 4. Select **Yes** to enable L2TP.

Step 5. Click **Submit Changes** to save the modification.

Step 6. Follow the instructions in "IPSec Configuration" on page 2-1 and "Enabling IPSec Wireless Data Privacy" on page 2-6 to enable IPSec.

The Integrated Access Manager is now ready for the L2TP / IPSec clients.

SSH Configuration

This section describes how to configure the Integrated Access Manager or Access Control Server as the SSH server.

Configuring the Rights Manager for SSH

To configure the Rights Manager to allow SSH, do the following:

Step 1. To access the Administrative Interface from the network, set your browser to the IP address or hostname of the Integrated Access Manager or Access Control Server. If your system is connected through a downlink port on an Integrated Access Manager, set your browser to `https://42.0.0.1:445`.

Step 2. Type the administrator username and password in the appropriate fields and then click the **Login** button.

If you are connected to a client port and have not logged on to the network, you will see a Logon page on the screen when you first start the web browser. You may ignore the Logon page if you are configuring the Integrated Access Manager and then open the given URL to access the **Main** Menu. If you are configuring the Access Control Server you can either logon to the network as a normal user or access the unit from the secured side of the network. You can find the information on how to create a normal user account in the *HP ProCurve 700wl Series Management and Configuration Guide* accessible through the **HELP** menu.

Step 3. From the **Main** Menu click **GOTO RIGHTS MANAGER** to access the Rights Manager Clients page, then click **CONFIGURATION.**

Step 4. Click **Encryption/Authentication per Location** in the Wireless Data Privacy Logon section of the **Configuration** Menu.

The Encryption / Authentication per Location page appears, as shown in Figure 2-19.

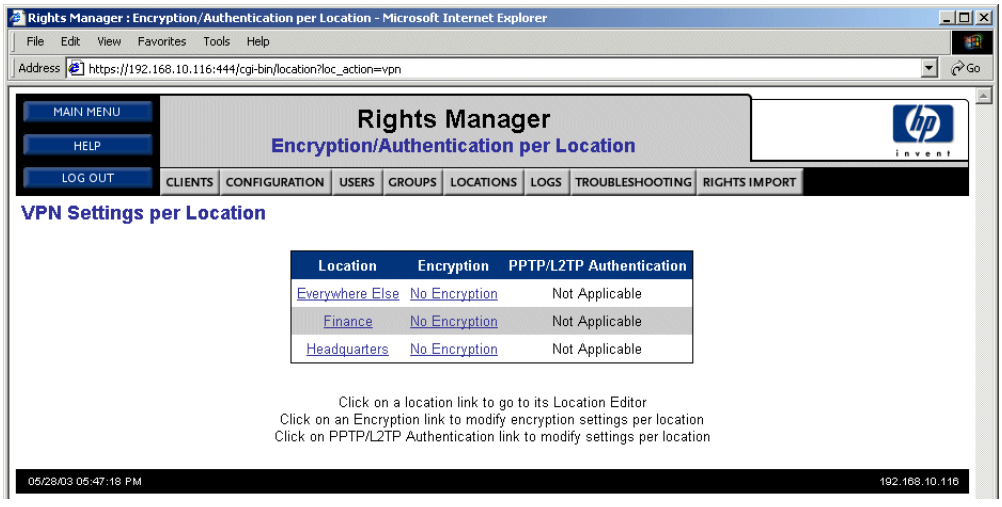

Figure 2-19. Encryption/Authentication per Location page, default settings

Suppose you want to configure the default location, *Everywhere Else*, to support SSH. Note that the IPSec protocol assigned by default to the Everywhere Else location.

Step 5. Click **IPSec Allowed** in the Everywhere Else row.

The Specify Encryption per Location page appears, as shown in Figure 2-20.

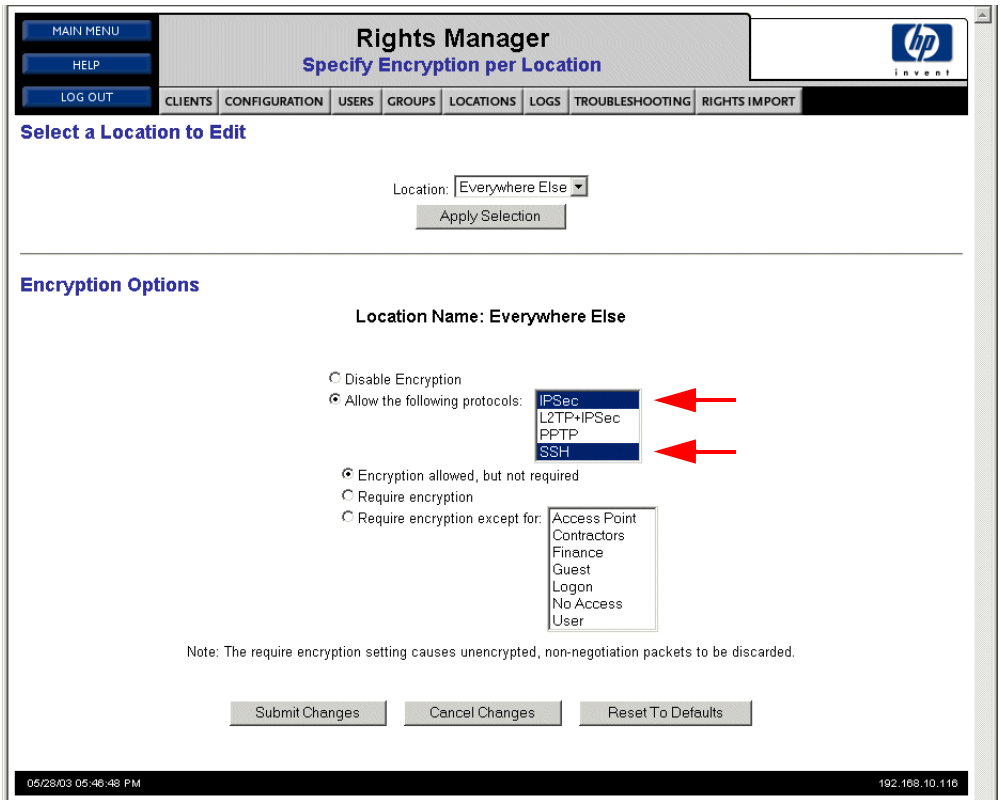

Figure 2-20. Setting IPSec and SSH on the Specify Encryption per Location page

Step 6. Make sure that the **Allow the following protocols** option is selected.

Step 7. Select both SSH and IPSec from the protocol list. To select multiple entries in the panel, press and hold the CTRL key and then click the desired protocols one at a time. This preserves the default setting (IPSec) and adds SSH to it.

If encryption is required for all clients connecting to this location, select the **Require encryption** option. With this selection, the user must connect to the system using the specified protocols. Otherwise, the connecting attempt will fail.

Step 8. Click **Submit Changes** to save the settings.

The new settings will update the VPN Settings per Location table (see below).

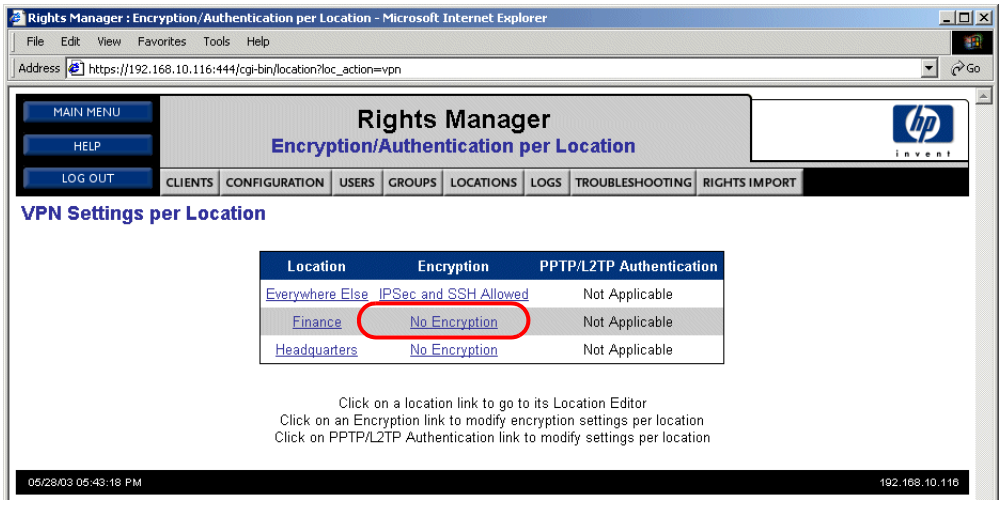

Figure 2-21. VPN Settings per Location Table showing SSH and IPSec enabled

Step 9. Since *Everywhere Else* is an existing location, you should refresh the group's rights in order to apply the new settings to active users.

a. Click **CLIENTS** at the top of the screen to go to the Rights Manager clients page.

b. Once the client page appears, click **Refresh every client's rights** to refresh the rights of all users. You may choose to refresh the client's rights on a per-user basis by clicking on each individual user's link in the Clients table.

Enabling SSH Wireless Data Privacy

Enabling SSH in the Wireless Data Privacy Setup is a global setting that affects all Access Controllers in the system. The following procedure is applicable to both an Integrated Access Manager and an Access Control Server.

To enable SSH, do the following:

Step 1. Start your web browser and open the URL, `https://42.0.0.1:445`, to access the **Main** Menu of the Integrated Access Manager. Use the appropriate IP address instead of `42.0.0.1` if you are accessing the unit via its Uplink port or you are configuring the Access Control Server.

Step 2. Enter the administrator username and password in the appropriate fields and then click the **Login** button.

Step 3. Click **SSH** in the Wireless Data Privacy Setup section of the **Main** Menu.

The SSH Configuration page appears.

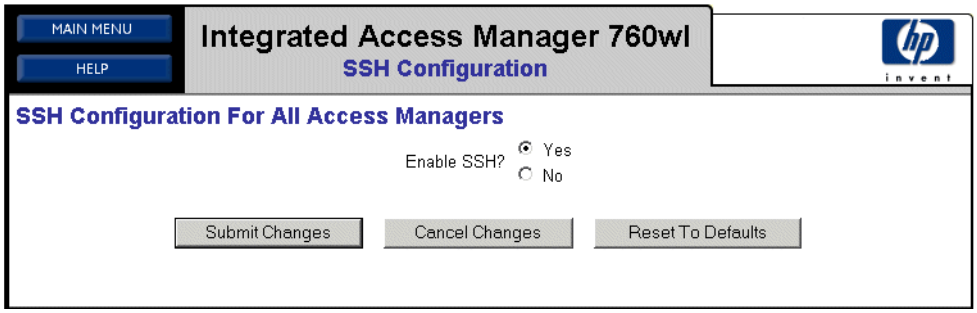

Figure 2-22. Enabling SSH

Step 4. Select **Yes** to enable SSH.

Step 5. Click the **Submit Changes** button to save the modification.

The Integrated Access Manager is now ready for SSH clients.

CLIENT CONFIGURATION 3

This chapter provides an overview of client configurations. It consists of the following sections:

IPSec Client Configuration

This section describes how to configure computers running Microsoft Windows as IPSec clients.

SafeNet SoftRemote for Windows

The following procedures configures SafeNet SoftRemote for use as an IPSec client.

Note: *This procedure assumes you have already installed the SoftRemote software on your system. SoftRemote should start automatically after the software installation and system reboot.*

The following procedure is based on a Windows XP client. You may follow the same procedure for configuring the software on different Windows platforms.

Step 1. Start the SoftRemote software Security Policy Editor:

- Double-click the **SoftRemote** icon in the desktop taskbar's notification area (lower-right corner) to open the Security Policy Editor window

or

- From the **Start** menu select **Programs**, then **SoftRemote**, then click **Security Policy Editor**.

The Security Policy Editor – SafeNet SoftRemote window appears (Figure 3-1).

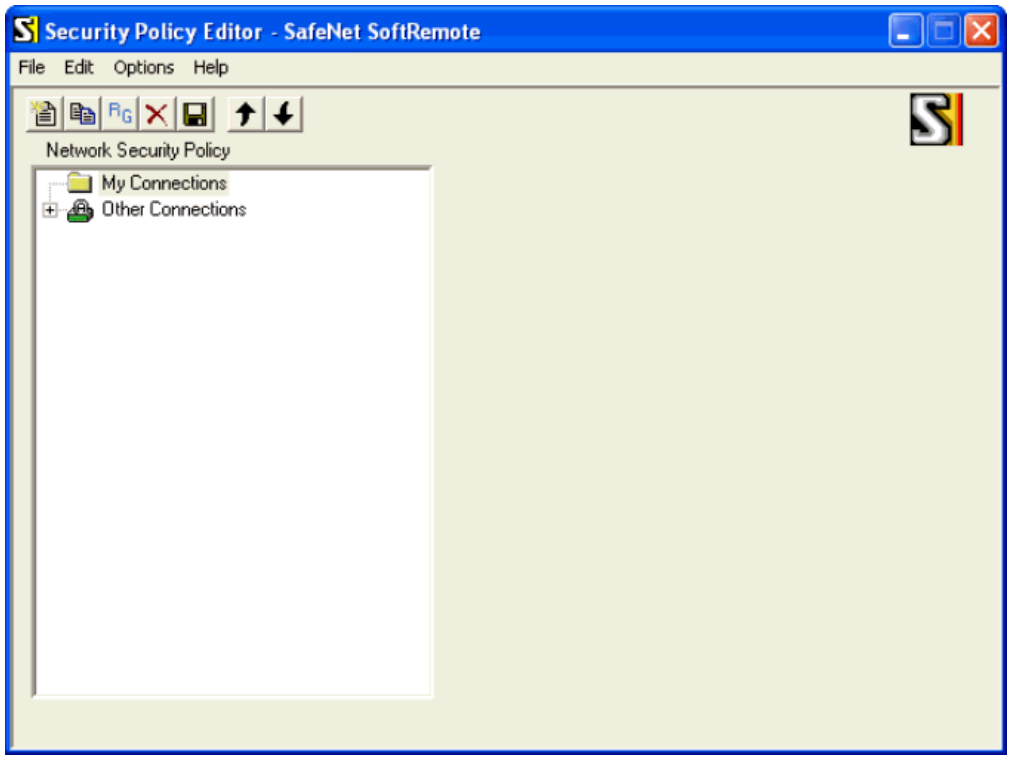

Figure 3-1. Security Policy Editor – SafeNet Remote Window

Step 2. Click **Options** to display the **Options** menu.

Select **Secure** and then select **All Connections**. This will force all network connections through the secure tunnel.

The Connection Security Panel appears (Figure 3-2).

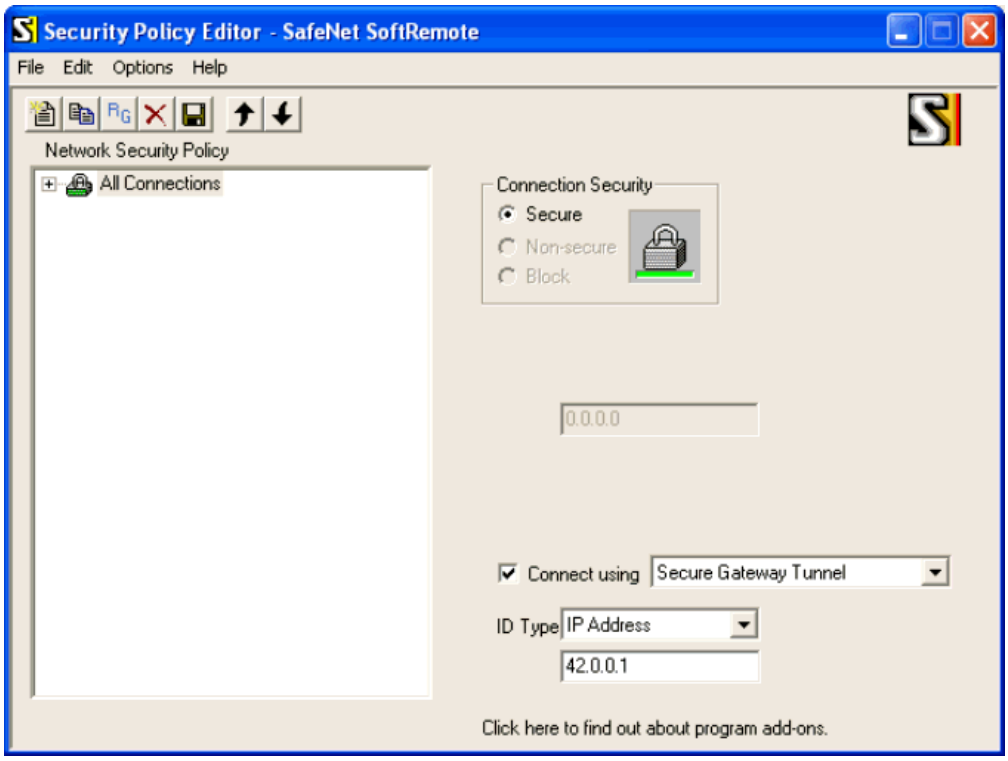

Figure 3-2. Security Policy Editor – SafeNet Remote Window, Connection Security Panel

Step 3. Click to select the **Connect using** checkbox and make sure that **Secure Gateway Tunnel** is selected. Also make sure that **ID Type** is set to **IP Address**. Next, enter `42.0.0.1` in the text box below the **ID Type** menu.

Step 4. Expand **All Connections** in the Network Security Policy panel and select **My Identity**.

The displays the My Identity panel (Figure 3-3).

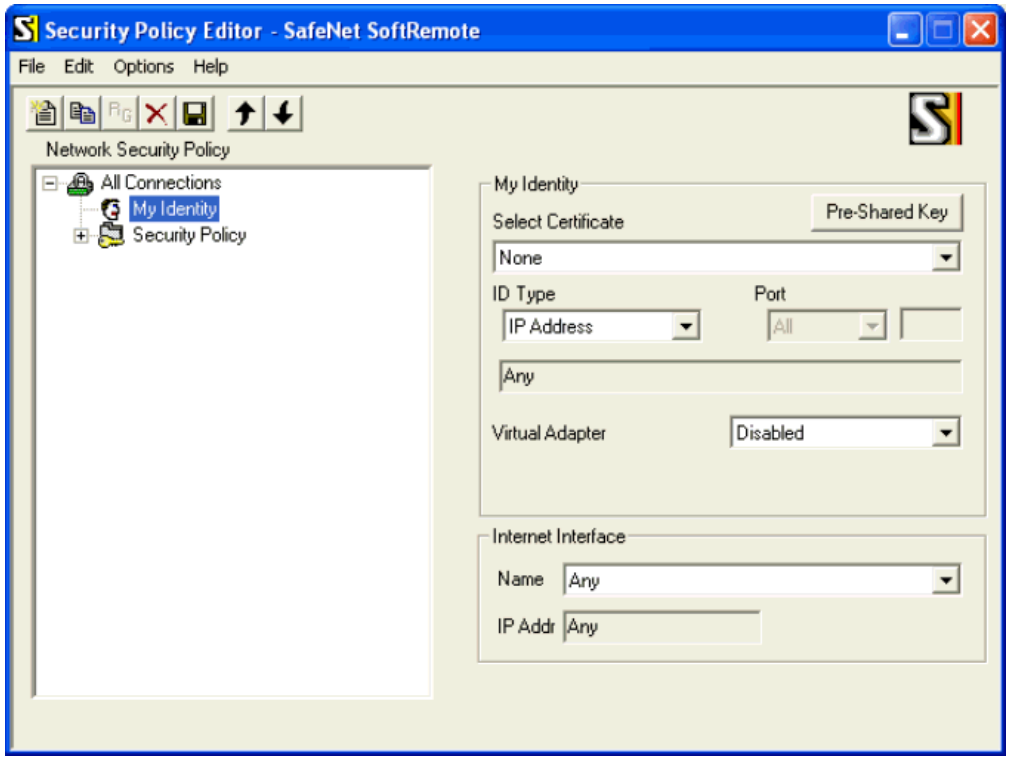

Figure 3-3. Security Policy Editor – SafeNet Remote Window, My Identity Panel

Make sure that **Select Certificate** is set to **None**.

Step 5. Click the **Pre-Shared Key** button. The Pre-Shared Key window appears (Figure 3-4).

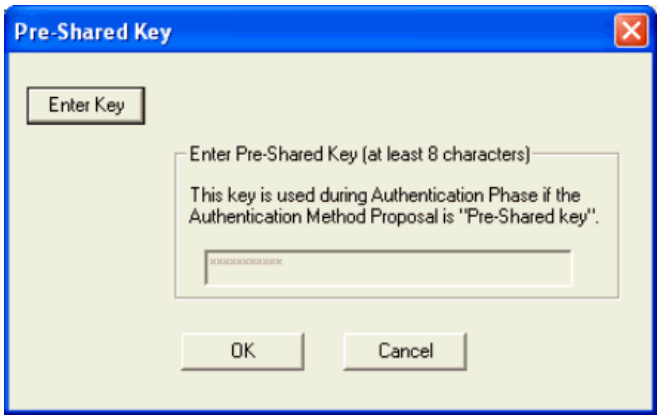

Figure 3-4. Pre-Shared Key Dialog

Step 6. Click the **Enter Key** button and then enter the shared key in the text box. The key must be at least 8 characters long and it must be the same key as you entered when you configured IPSec in the 700wl Series system.

Click **OK**.

Step 7. Expand **Security Policy** in the Network Security Policy panel. Also expand all items below Security Policy, including: **Authentication (Phase 1)** and **Key Exchange (Phase 2)** (see Figure 3-5).

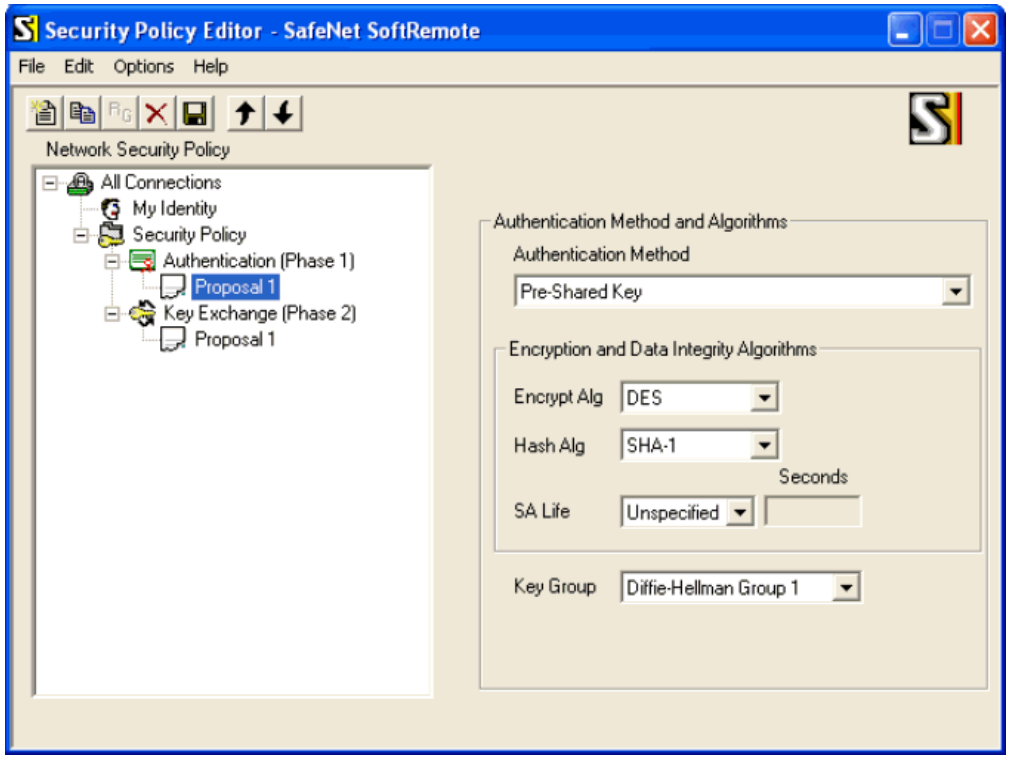

Figure 3-5. Security Policy Editor – SafeNet Remote Window, Authentication Method Panel

Step 8. Setup the authentication method.

Select **Proposal 1** below Authentication (Phase 1). Make sure that the **Authentication Method** is set to **Pre-Shared Key**.

Note the default settings of SafeNet SoftRemote work with the default settings of the 700wl Series system. If a different authentication algorithm is used, make sure that the settings match those configured on the 700wl Series unit.

Step 9. Setup the key exchange protocol.

Select **Proposal 1** below Key Exchange (Phase 2). You may keep the default settings (see Figure 3-6) because they work with the default settings on the 700wl Series unit.

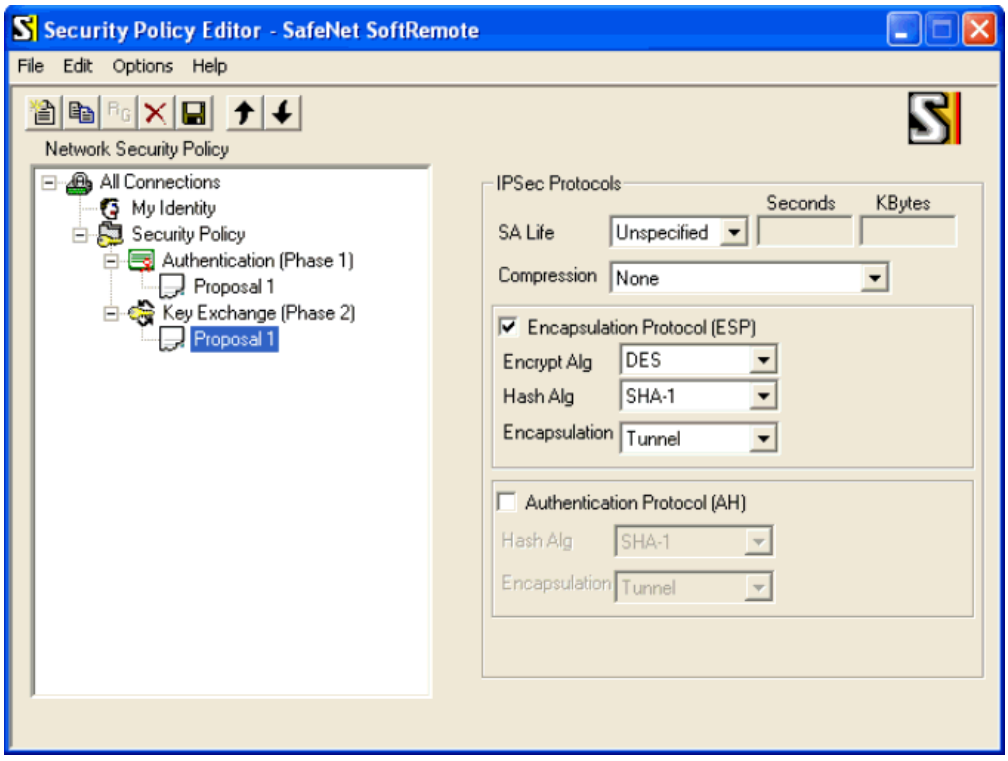

Figure 3-6. Security Policy Editor – SafeNet Remote Window, IPSec Protocols Panel

If a different encapsulation protocol is used, you must modify the settings on the 700wl Series unit accordingly.

Step 10. Pull down the **File** menu and then select **Save Changes**. Next, pull down the **File** menu again, and click **Exit**.

At this point, your system should be able to establish the secured connection with the server. You should see the icon as shown below in the notification area on the lower right corner of the desktop.

Figure 3-7. Connection Icon

If the connection failed, you will not see the yellow key in the icon. In this case, the easiest approach to resolving the problem is by rebooting your system. You must also make sure that the settings on the HP ProCurve Integrated Access Manager or Access Control Server for IPSec match those on your client system.

SSH Sentinel for Windows

This configuration procedure is based on SSH Sentinel version 1.3.2 (build 2) installed on Windows XP Professional. You may follow the same procedures for configuring the software on different Windows platforms.

Note: *This procedure assumes you have already installed the SSH Sentinel software on your system.*

To configure the SSH Sentinel IPSec client, do the following:

Step 1. Start SSH Sentinel Policy Editor:

- From the **Start** menu select **All Programs**, then **SSH Sentinel**, then **SSH Sentinel Policy Editor**

or

- Right click the **Sentinel** icon in the notification area (lower-right corner of the desktop) and then select **Run Policy Editor…**.

Step 2. The SSH Sentinel Policy Editor window appears. Click the **Key Management** tab and then select **My Keys** (Figure 3-8).

Figure 3-8. SSH Sentinel Policy Editor Window, Key Management Tab

Step 3. Click the **Add** button to start the New Authentication Key wizard (Figure 3-9).

Figure 3-9. New Authentication Key Wizard

Step 4. Select the **Create a pre-shared key** option and then click **Next>**.

Step 5. The Create Pre-Shared Key window appears (Figure 3-10).

Figure 3-10. Create Pre-Shared Key window

Step 6. Type the Pre-shared key name, the Shared secret, and Confirm the shared secret in the appropriate fields. Click **Finish**.

The new entry appears in the **My Keys** list.

Step 7. Click the **Security Policy** tab to create a new policy (Figure 3-11).

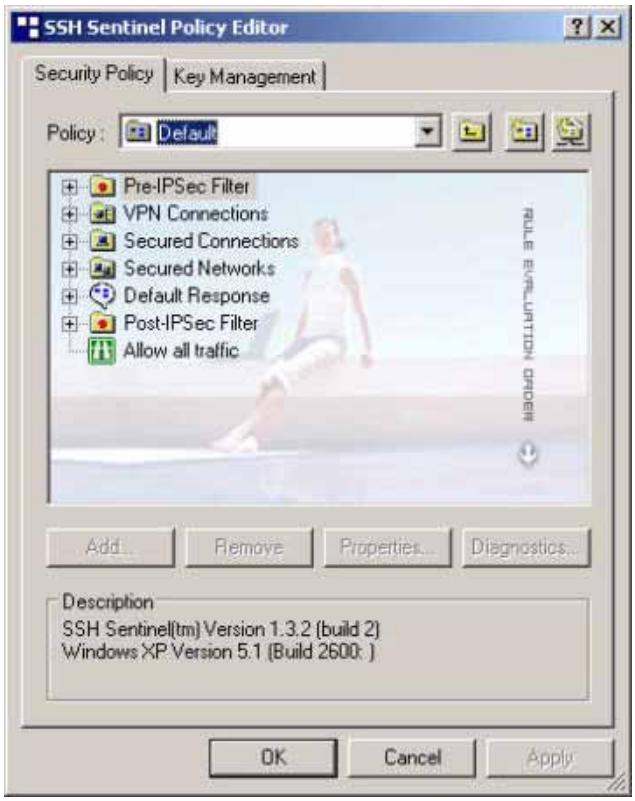

Figure 3-11. SSH Sentinel Policy Editor Window, Security Policy Tab

Step 8. Select **VPN Connections** and then click **Add**.

Step 9. The Add VPN Connection window appears (Figure 3-12).

Figure 3-12. Add VPN Connection Dialog

Step 10. Do the following:

- Enter `42.0.0.1` in the **Gateway name** field.
- Specify the **Remote network** (default is *any* – 0.0.0.0 / 0.0.0.0) that this computer will access through the VPN connection.
- Pull down the **Authentication key** menu and then select the pre-shared key entry created in Step 6.

Step 11. (Optional) Click the **Diagnostics** button to test the connection.

Step 12. Click **OK** to finish the settings.

Step 13. Do the following to establish the VPN connection:

- Right click the **Sentinel** icon in the notification area to display the **SSH Sentinel** menu.
- Move the pointer to the **Select VPN** submenu and then select **42.0.0.1 (any)**, which is the VPN connection created in the previous section.

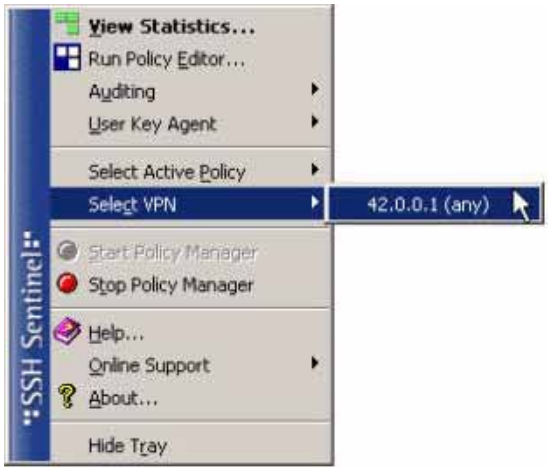

Figure 3-13. Select VPN Submenu

The computer will open the VPN connection to the 700wl Series unit (`42.0.0.1`).

Step 14. Verify the VPN Connection:

Double click the **Sentinel** icon in the notification area to view the statistics of the VPN connection.

Notice that the `42.0.0.1` entry appears in the Security Associations panel along with the detailed information of the encryption protocol (Figure 3-14).

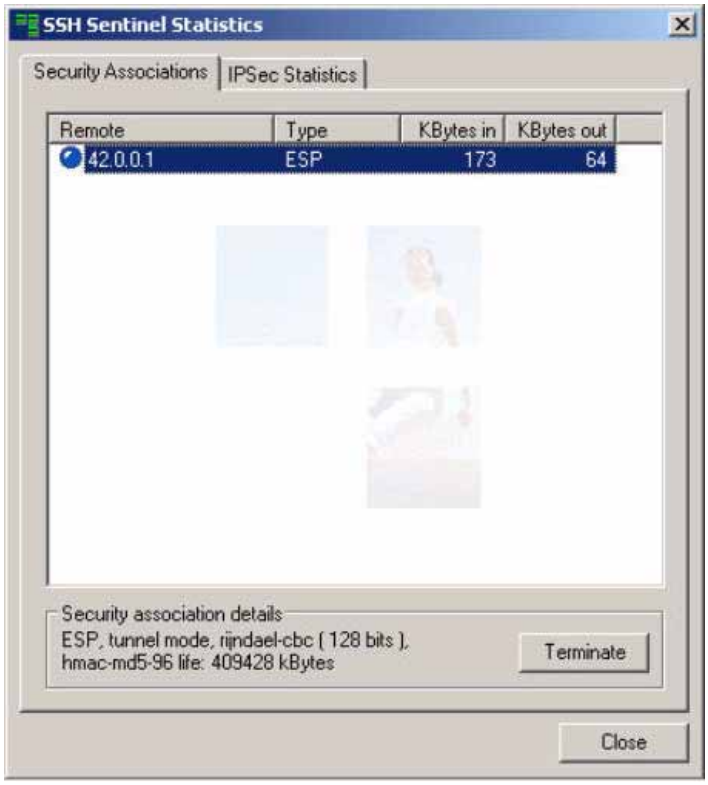

Figure 3-14. SSH Sentinel Statistics Window

PGPnet for Windows

This section describes the procedure for configuring the PGPnet IPSec client software.

Note: *This procedure assumes you have already installed the PgP software on your system. PGPnet should start automatically after the software installation and system reboot.*

The following procedure is based on a Windows 2000 client. You may follow the same procedures for configuring the software on different Windows platforms.

Step 1. Start the PGPnet software:

- From the **Start** menu select **Programs,** then **Pgp**, then click **PGPnet**.

or

- Right click the **PgP** icon in the notification area (lower-right corner of the desktop) and then select **Run Policy Editor…**.

The PGPnet window appears (Figure 3-15).

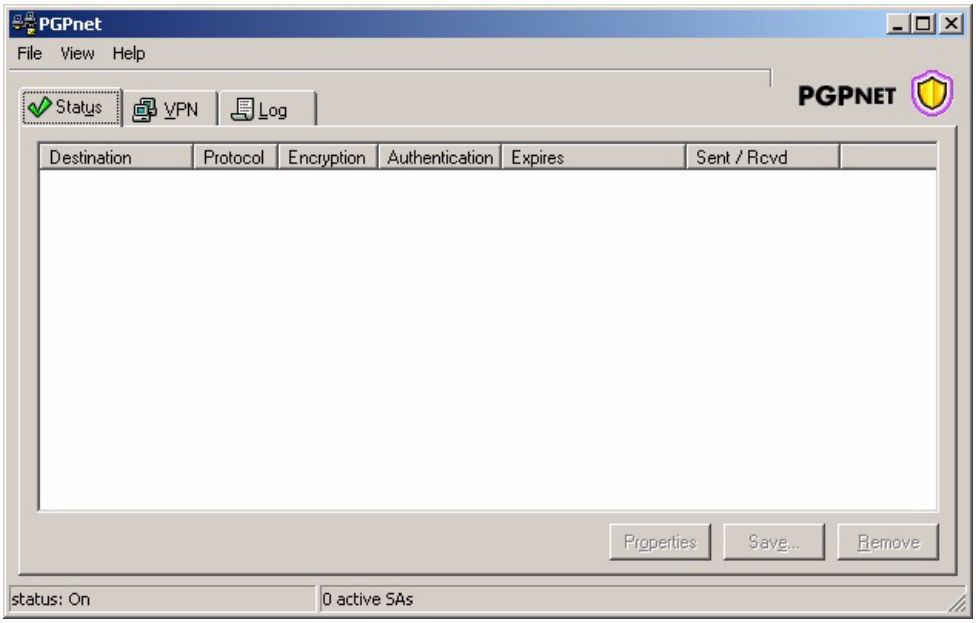

Figure 3-15. PGPnet Window

Step 2. Select the VPN tab and then click the **Add** button. The Host/Gateway window appears.

Step 3. Setup the VPN gateway by entering the desired name and IP address in the appropriate text boxes. Pull-down the menu below **IP Address** and then select **VPN Gateway**. Next, select **Require manual connection** from the Connection Options.

If the button in the Shared Secret section shows **Set Shared Passphrase**, you must click the button to setup the Pre-shared key. On the other hand, if the button shows **Clear Shared Passphrase** but you are not sure that the passphrase is setup correctly, you may click the button to clear the previous setting and then setup a new one.

When you are done, click **OK**.

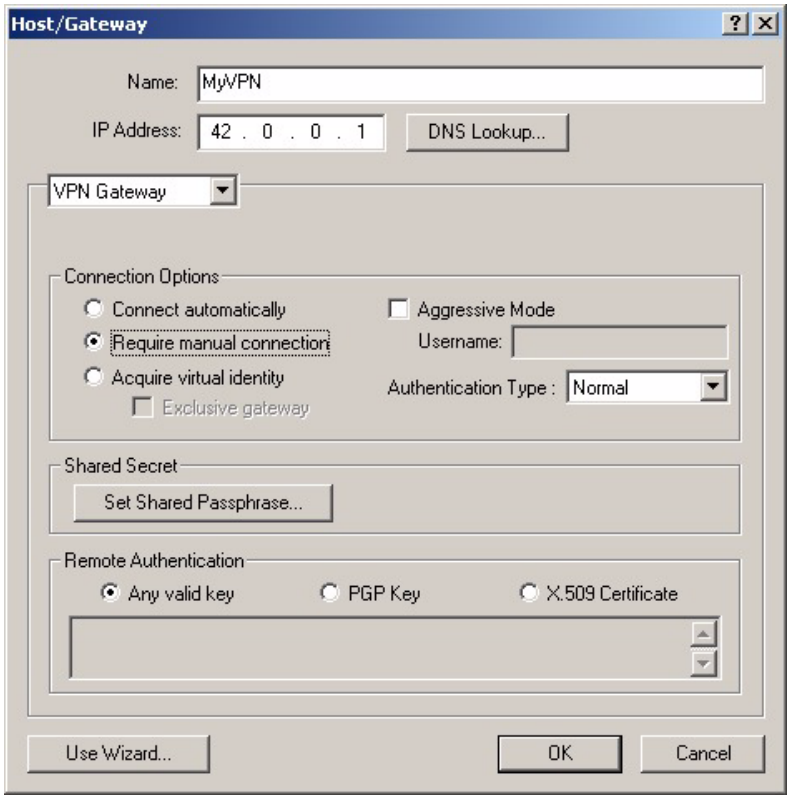

Figure 3-16. Host/Gateway Window

A new entry appears in the PGPnet panel, with the name you entered ("*MyVPN*" in this example).

The following steps show how to create a secured connection to the internal network with the address 192.168.2.0/24 using the VPN gateway created in Step 3.

Step 4. Highlight the entry you created in the previous step and then click **Add**.

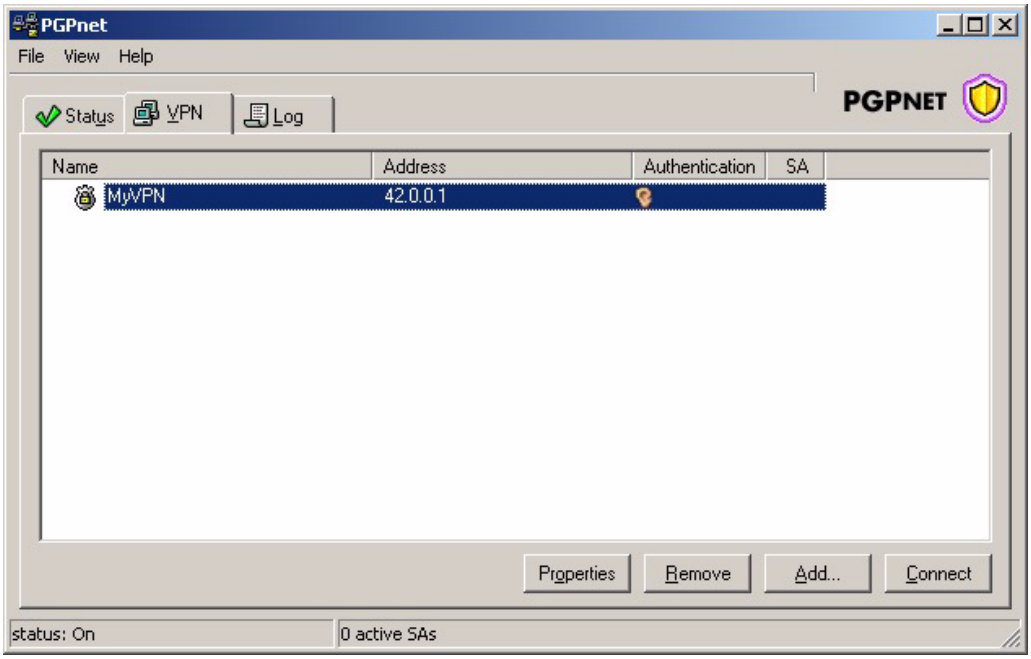

Figure 3-17. PGPnet Window, VPN Panel

You will be prompted with the following window. Click **Yes**.

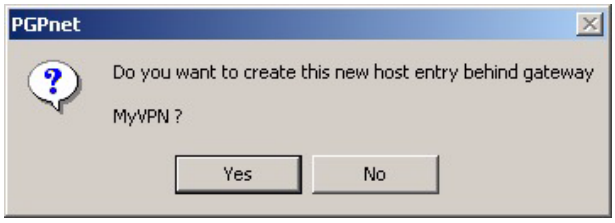

Figure 3-18. PGPnet Create Host Entry Confirmation

The Host/Gateway window appears.

Step 5. Enter the desired name and IP address in the appropriate text boxes. Pull down the menu below **IP Address** and then select **Subnet**. The Host/Gateway window will be reduced to that shown below. Make sure that the Subnet Mask value is 255.255.255.0 (/24). Click **OK**.

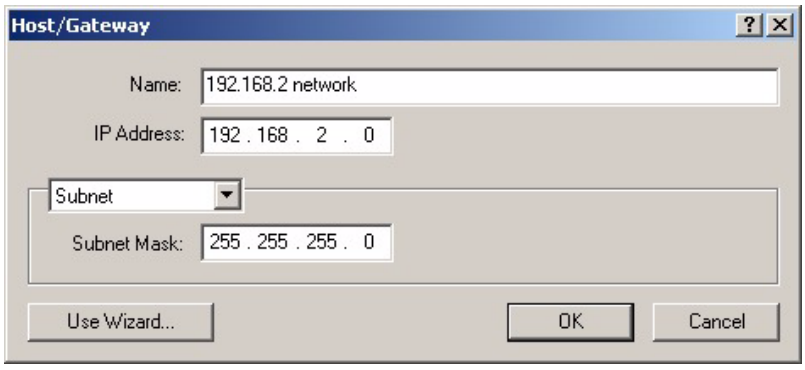

Figure 3-19. Host/Gateway Window, Reduced

Note that based on the above settings, all traffic going to this subnet will be encrypted.

A new entry appears below the *MyVPN* entry (you must expand the *MyVPN* entry to see it) as shown below.

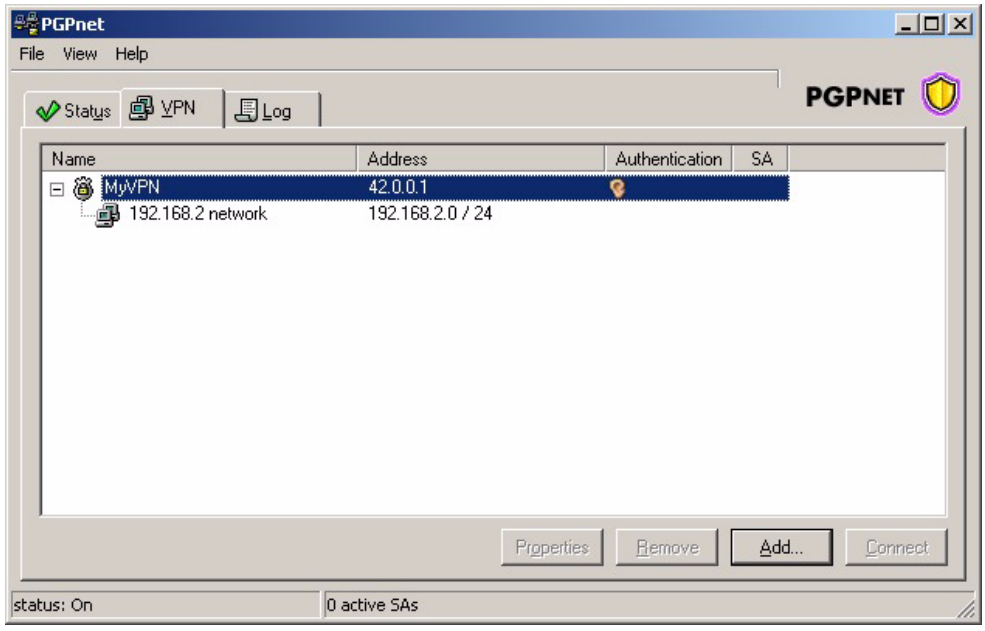

Figure 3-20. PGPnet Window, VPN Panel

Repeat Steps 4 and 5 to create additional subnet/host entries to which your system will encrypt the traffic and send it through the VPN gateway.

Note: *If you plan to encrypt all IP traffic through the VPN gateway, you must create the following subnet entries:*

0.0.0.1 /1 (covers 0.0.0.1 – 127.255.255.255)

128.0.0.0 /1 (covers 128.0.0.0 – 255.255.255.255)

Step 6. The last configuration step is to change the order of how the PGPnet client attempts to connect to the VPN gateway.

Pull down the **View** menu and then select **Options**. The PGP Options window appears. Next, click the VPN Advanced tab. In the **Proposals** section, highlight the **Shared Key MD5 TripleDES 1024** in the IKE panel. Click **Move Up** repeatedly until the entry is at the top of the panel. Furthermore, highlight the **None MD5, TripleDES None** entry in the IPSec panel and then move the entry up to the top of the panel. The final settings are shown in the picture below.

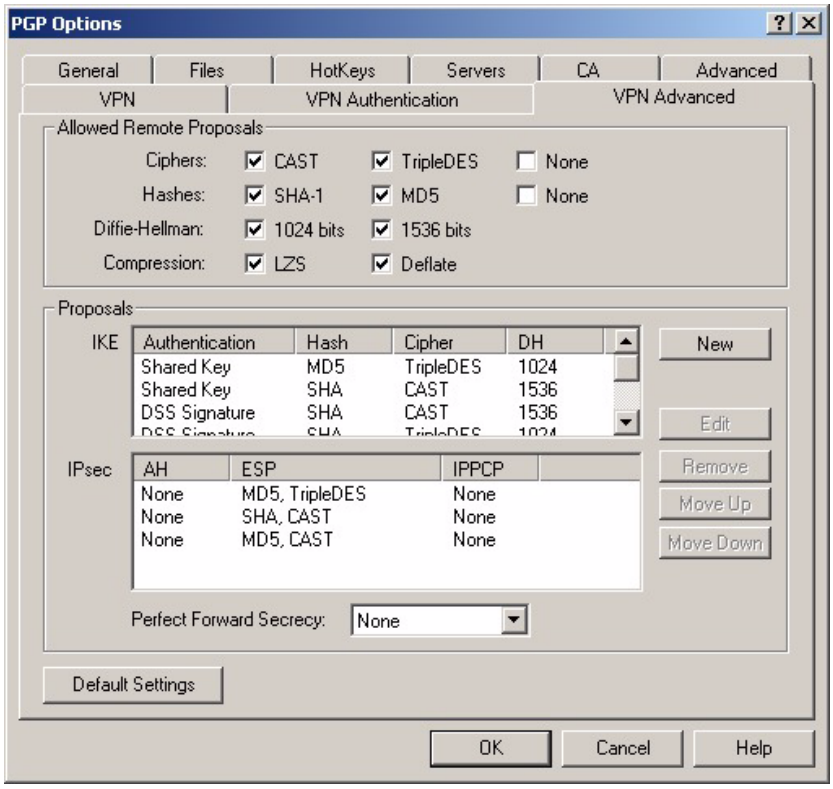

Figure 3-21. PGP Options Window

At this point, PGPnet should be ready for connecting to the IPSec server.

Step 7. Highlight the VPN gateway (*MyVPN* in this example) and then click **Connect**.

After the VPN connection has been made, you will see a green icon on the SA column of each entry. Otherwise, you will get a red icon indicating that the VPN connection has failed.

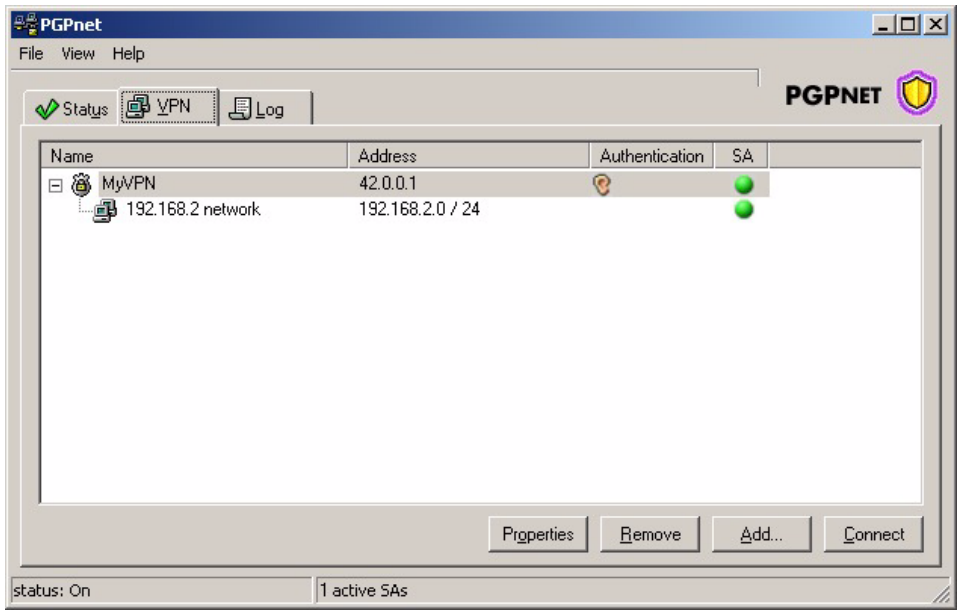

Figure 3-22. PGPnet Window, VPN Panel

If you have problems connecting to the VPN server, you can click the Log tab for information. You may also view additional information from the Log File on the 700wl Series unit.

When you click the Status tab, you should see the Sent/Rcvd values increase every time traffic is generated to your defined subnets.

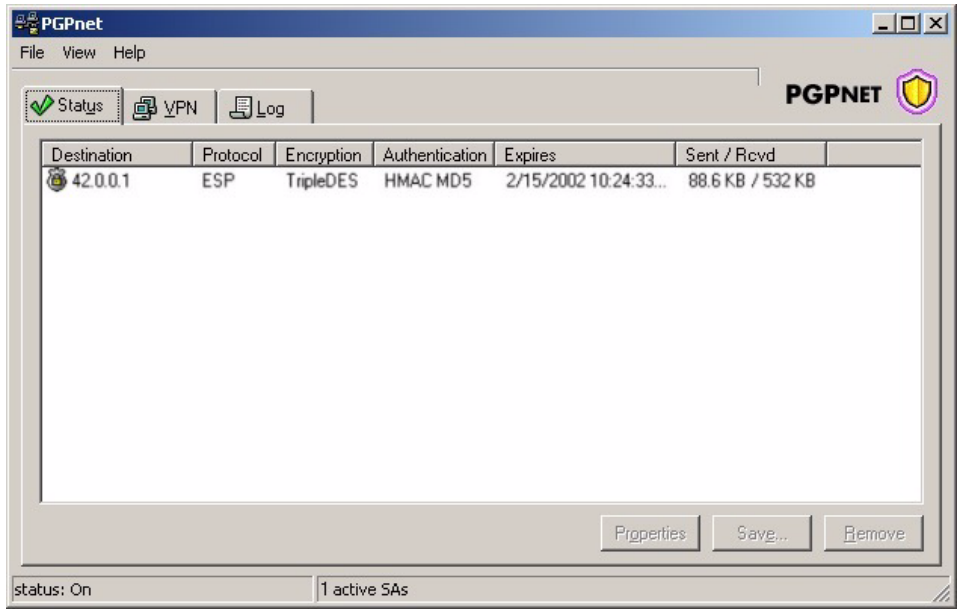

Figure 3-23. PGPnet Window, Status Panel

PGPnet for Mac OS 9.x

In this section, the procedures for configuring PGPnet 7.1 on Apple Mac OS 9.x are described.

The following procedures are created based on Mac OS 9.2.2. You may follow the same procedures for configuring the software on different Mac OS versions.

Step 1. After the installation and system restart, PGPnet is started automatically. Click the **PGPnet** icon on the upper-right corner of the desktop (left of Finder) and then select **PGPnet**.

The PGPnet window appears.

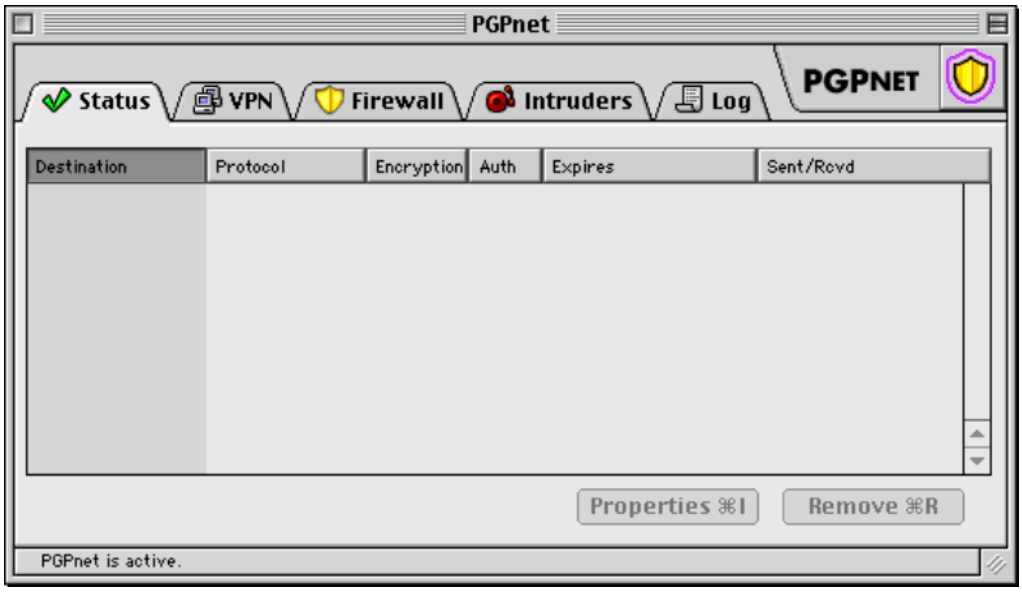

Figure 3-24. PGPnet Window, Status Tab

Step 2. Select the VPN tab and then click the **Add** button. The Host/Gateway window appears.

Step 3. Setup the VPN gateway by entering the desired name and IP address in the appropriate text boxes. Pull-down the menu below **IP Address** and then select **VPN Gateway**. Next, select **Require manual connection** from the Connection Options.

If the button in the **Shared Secret** section shows **Set Shared Passphrase**, you must click the button to setup the Pre-shared key. On the other hand, if the button shows **Clear Shared Passphrase** but you are not sure that the passphrase is setup correctly, you may click the button to clear the previous setting and then setup a new one.

Click **OK** when you are done.

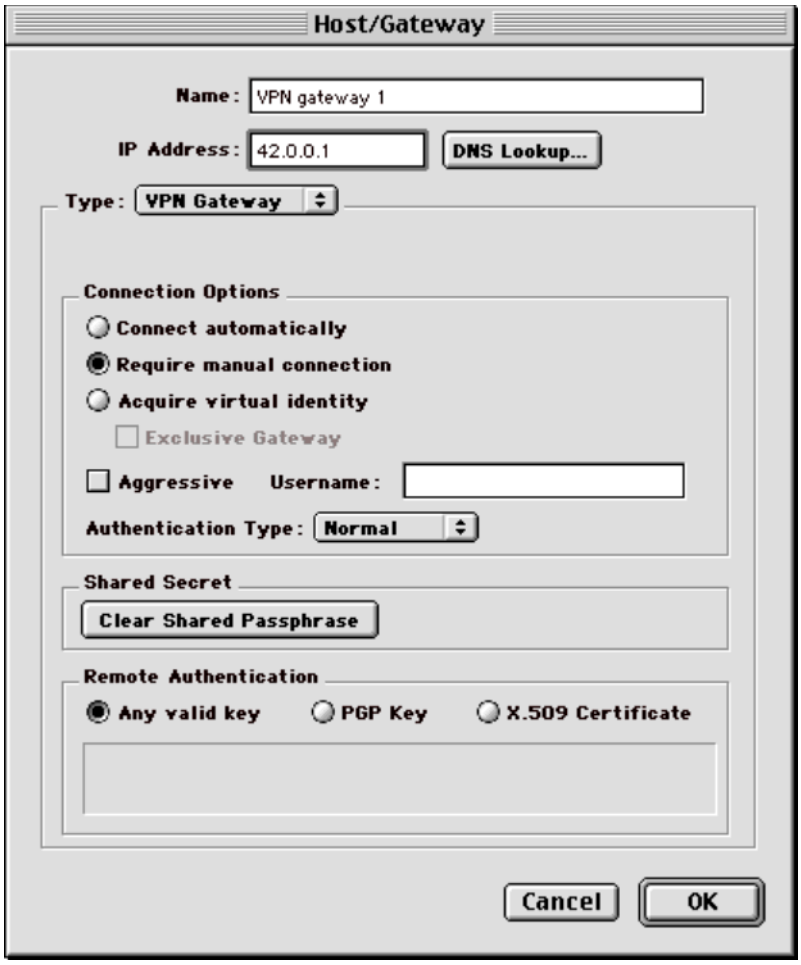

Figure 3-25. Host/Gateway Window

Based on the above settings a new entry named *VPN gateway 1*, appears in the PGPnet panel.

The following shows how to create a secured connection to the internal network with the address 192.168.0.0 /16 using the VPN gateway created in Step 3.

Step 4. Highlight the entry you created in the previous step and then click **Add**.

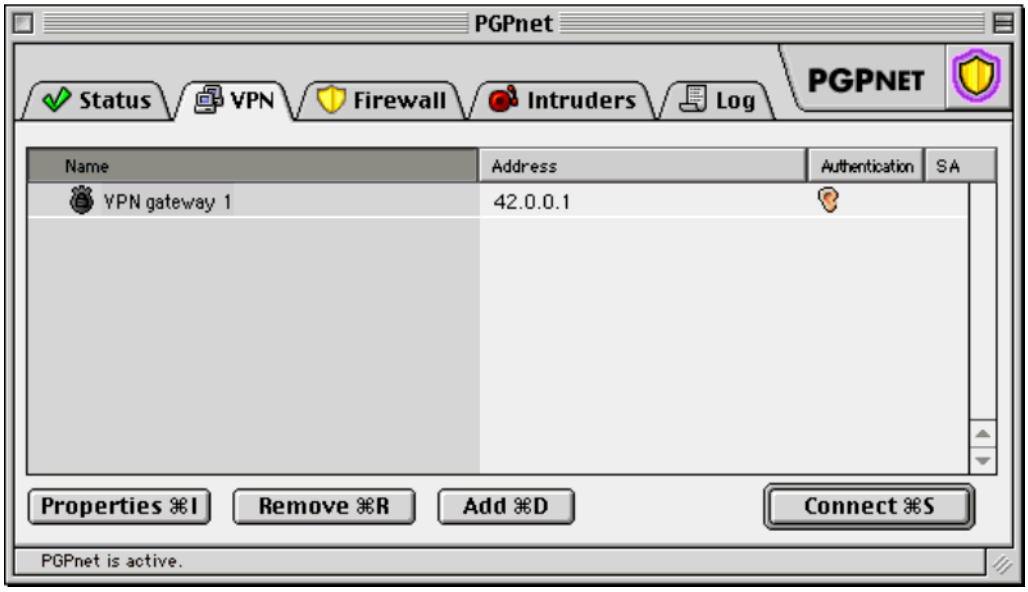

Figure 3-26. PGPnet Window, VPN Panel

The Host/Gateway window appears.

Step 5. Enter the desired name and IP address in the appropriate text boxes. Pull down the menu below **IP Address** and then select **Subnet**. The Host/Gateway window will be reduced to that shown below. Make sure that the Subnet Mask value is 255.255.0.0 (/16). Click **OK**.

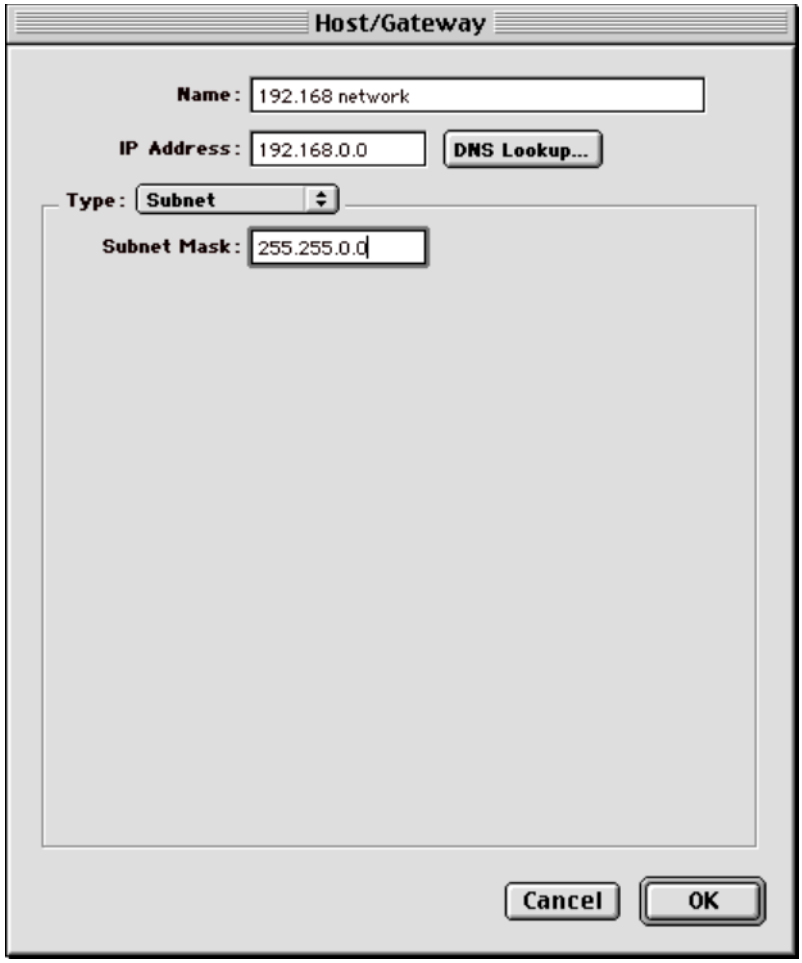

Figure 3-27. Host/Gateway Window

Note that based on the above settings, all traffic going to this subnet will be encrypted.

A new entry appears below the **VPN gateway 1** entry (you must expand the **VPN gateway 1** entry to see it) as shown below.

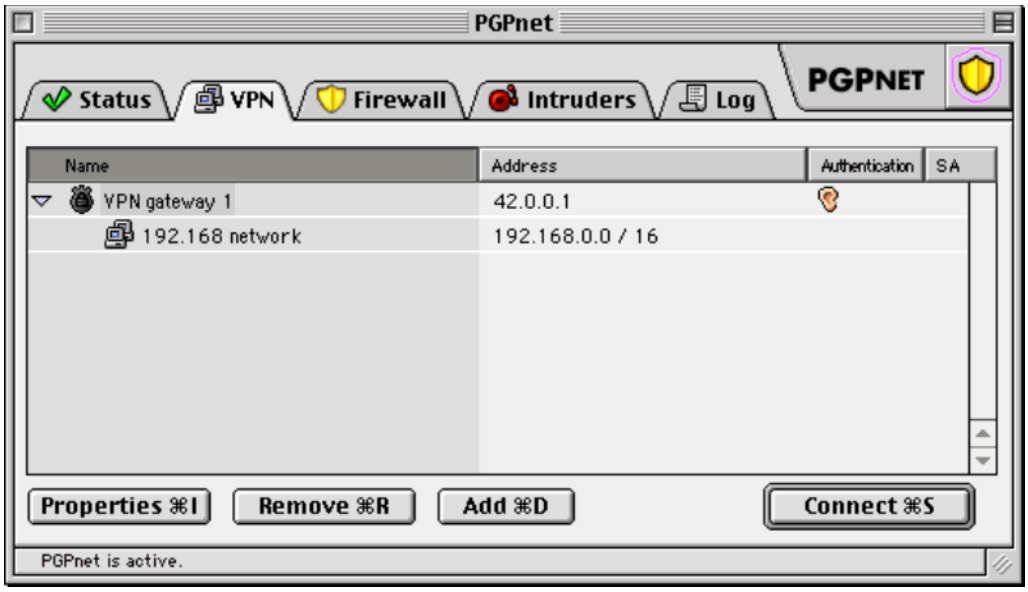

Figure 3-28. PGPnet Window, VPN Panel

Step 6. Repeat Steps 4 and 5 to create additional subnet/host entries to which your system will encrypt the traffic and send it through the VPN gateway.

Note: *If you plan to encrypt all IP traffic through the VPN gateway, you must create the following subnet entries:*

0.0.0.1 /1 (covers 0.0.0.1 – 127.255.255.255)

128.0.0.0 /1 (covers 128.0.0.0 – 255.255.255.255)

Step 7. The last configuration step is to change the order of how the PGPnet client attempts to connect to the VPN gateway.

a. Pull down the **Edit** menu and then select **Preferences...**. The PGP Preferences window appears.

b. Select **VPN Advanced** from the Preference Panels

c. In the **Proposals** section, highlight the **Shared Key MD5 TripleDES 1024 bits** in the IKE panel and then click **Move Up** repeatedly until the entry is at the top of the panel.

d. Highlight the **None MD5,TripleDES None** entry in the IPSec panel and then move the entry up to the top of the panel.

The final settings are shown in the picture below.

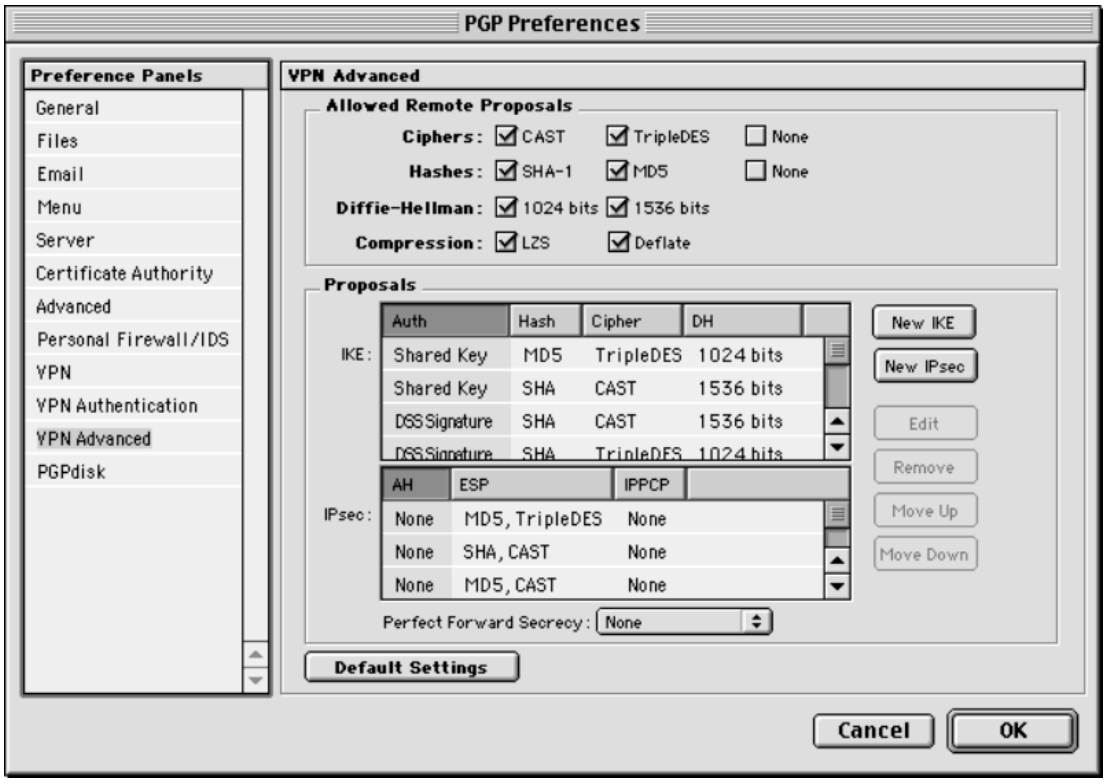

Figure 3-29. PGP Preferences Settings

e. Click **OK**.

At this point, PGPnet is ready for connecting to the IPSec gateway.

Step 8. Highlight the VPN gateway (in this example – **VPN gateway 1**) and then click **Connect**.

After the VPN connection has been made, you will see a green icon on the SA column of each entry. Otherwise, you will get a red icon indicating that the VPN connection has failed.

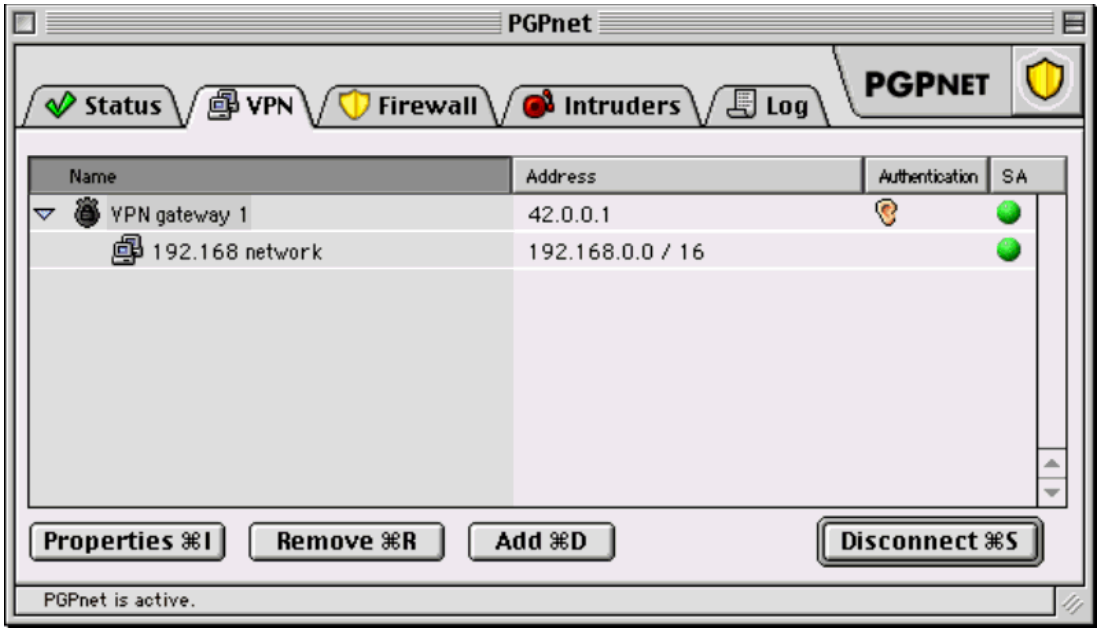

Figure 3-30. PGPnet Window, VPN Panel

If you have problems connecting to the VPN server, you can click the Log tab for information. You may also view additional information from the Log File on the 700wl Series unit.

When you click the Status tab, you should see the Sent/Rcvd values increase every time traffic is generated to your defined subnets.

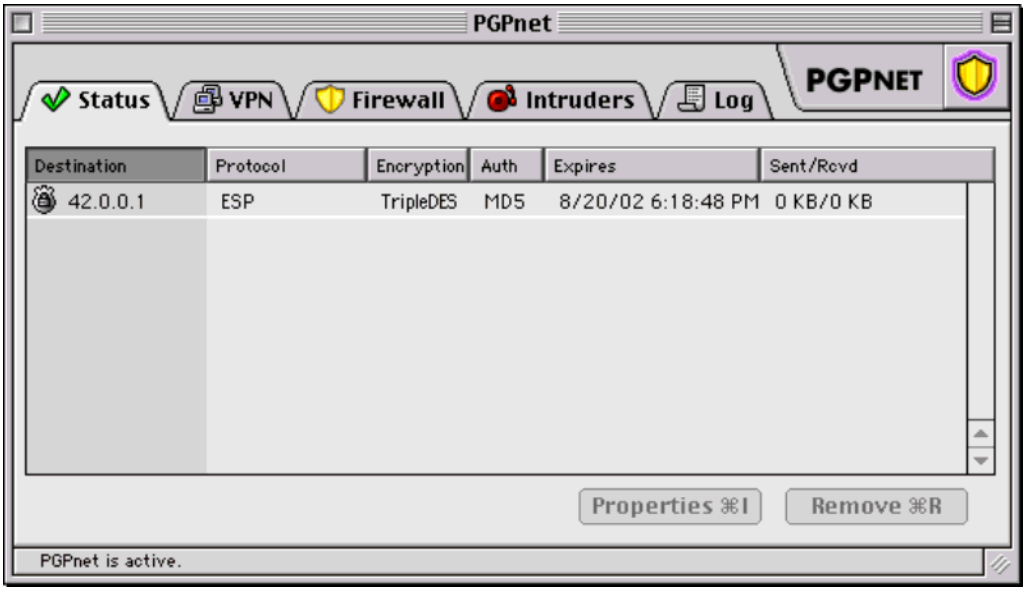

Figure 3-31. PGPnet Window, Status Panel

PPTP Client Configuration

This section describes how to configure computers running Windows XP, 2000, and 98SE as PPTP clients.

Windows XP Clients

Do the following to configure the Windows XP client:

Step 1. Open the Network Connections window:

Click the **Start** button and then move the pointer to **My Network Places**. Right-click My Network Places to display the pop-up menu and then select **Properties**.

The Network Connections window appears.

Step 2. Click the **Create a new connection** link on the **Network Tasks** panel.

The New Connection Wizard window appears.

Step 3. Click the **Next>** button to go to the Network Connection Type page.

Figure 3-32. New Connection Wizard

Step 4. Select the **Connect to the network at my workplace** option and then click the **Next>** Button.

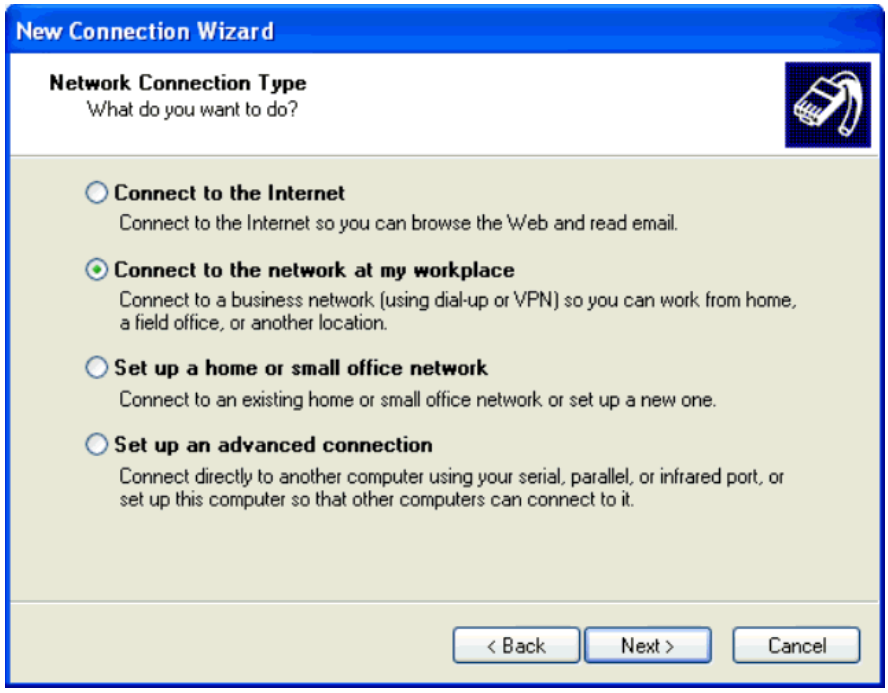

Figure 3-33. Network Connection Type Window

Step 5. Select the **Virtual Private Network connection** option. Click **Next>.**

Figure 3-34. Network Connection Window

Step 6. Enter the desired connection name in the **Company Name** text box. Click **Next>**.

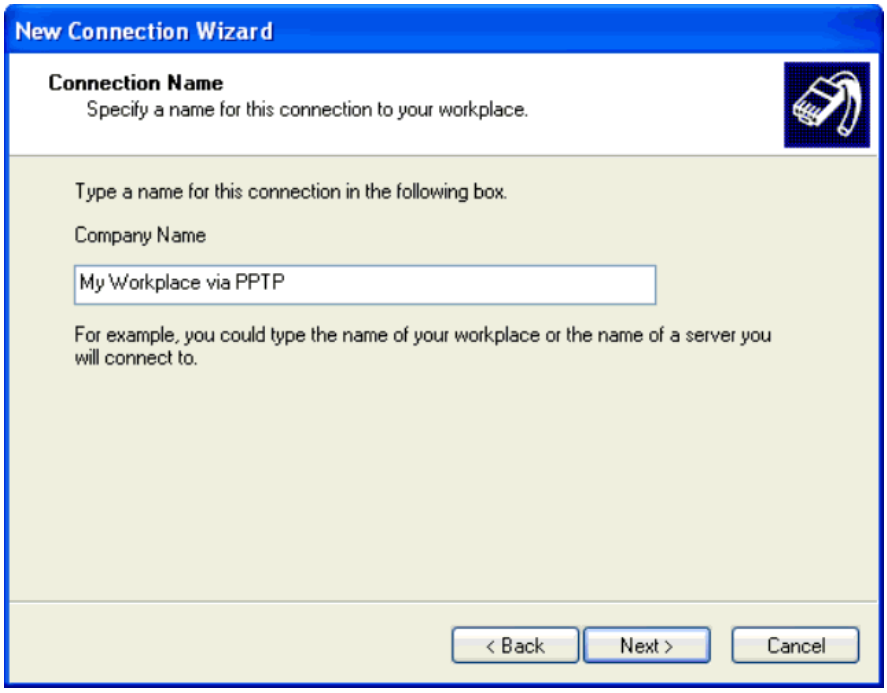

Figure 3-35. Connection Name Window

Step 7. Enter the IP address of the VPN server in the **Host name or IP address** text box. In this case, the internal address `42.0.0.1` of the 700wl Series unit (either the Integrated Access Manager or Access Controller) is used. Click **Next>**.

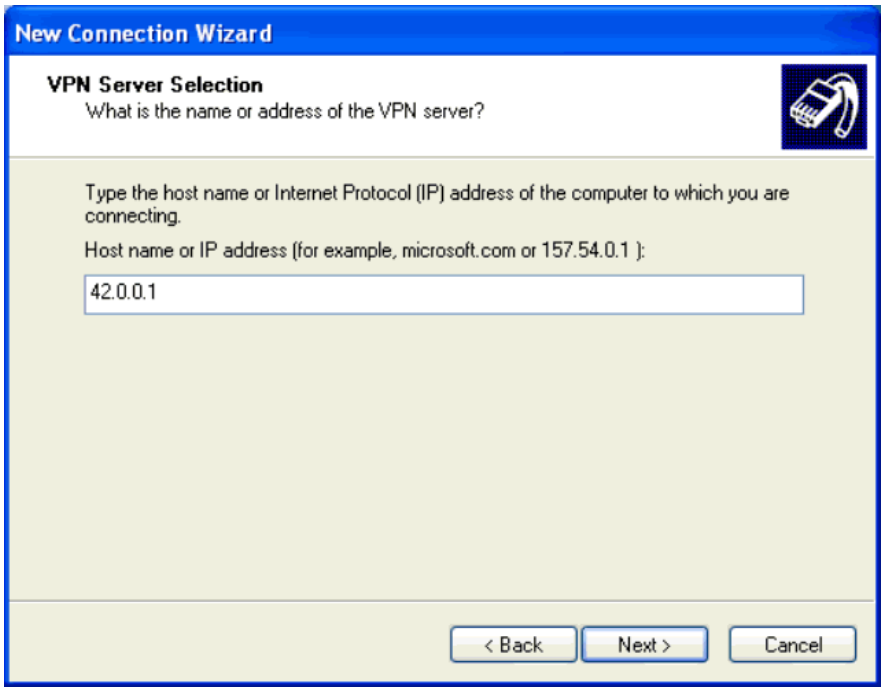

Figure 3-36. VPN Server Selection Window

The Completing the New Connection Wizard page appears.

Step 8. Click the **Finish** button. You may choose to add a shortcut to this connection to the desktop before clicking the **Finish** button.

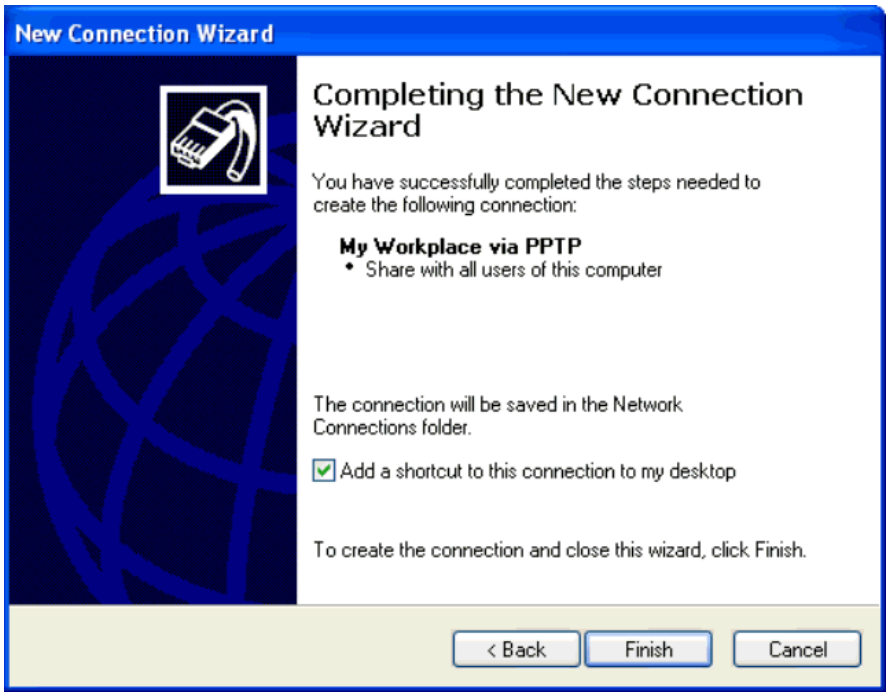

Figure 3-37. New Connection Wizard Completion Window

At this point, an icon representing the new connection appears in the Network Connections window under the **Virtual Private Network** section. In the meantime, the Sign-on window should appear on the screen; otherwise, double-click the new connection icon.

Figure 3-38. Sign-on Window

Step 9. You need to customize the properties of your connection to use PPTP and match the settings of the 700wl Series unit. Click the **Properties** button to open the connection's properties window.

Figure 3-39. PPTP Properties Window, General Tab

Step 10. Click the Networking tab to specify the type of VPN.

Pull down the **Type of VPN** menu and select **PPTP VPN**. Make sure that **Internet Protocol (TCP/IP)** is selected.

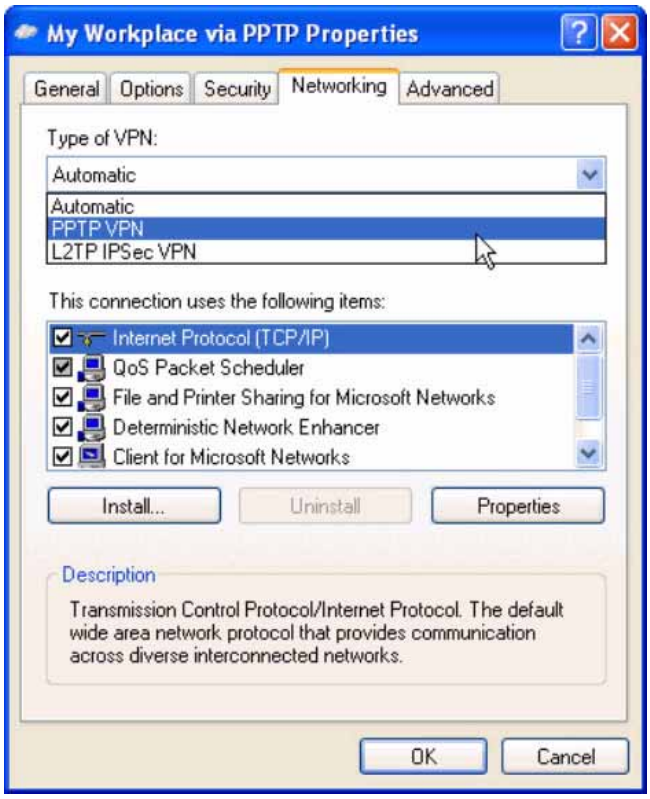

Figure 3-40. PPTP Properties Window, Networking Tab

Step 11. Click the Security tab to customize the security protocols.

Select **Advanced (custom settings)** and then click the **Settings** button.

The Advanced Security Settings window appears.

Step 12. Make sure that **Microsoft CHAP (MS-CHAP)** is *not* selected. Note that this protocol is selected by default. You must deselect this option so that only MS-CHAP v2 is used.

Step 13. Pull down the **Data Encryption** menu and select **Maximum strength encryption (disconnect if server declines)**. This will set the length of the encryption key to 128 bits.

Step 14. Click **OK** to go back to the connection's properties window.

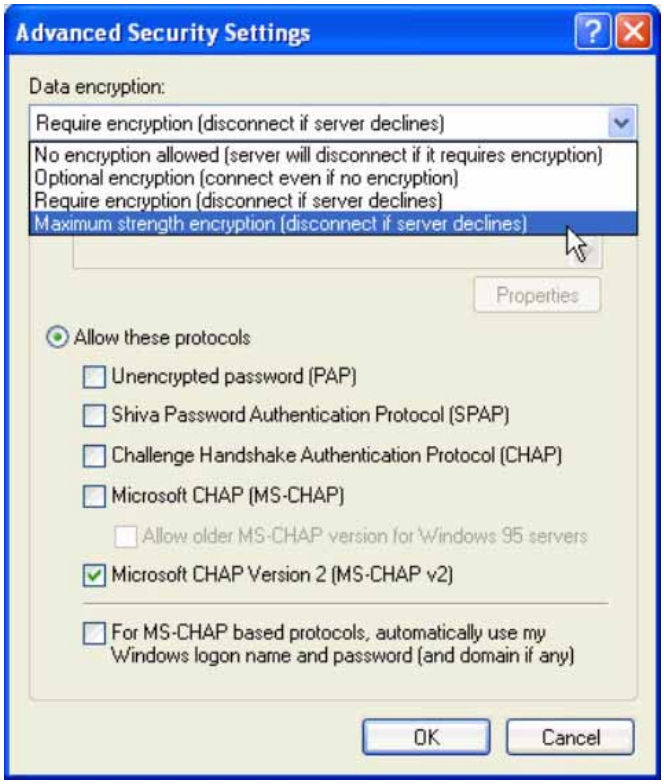

Figure 3-41. Advanced Security Settings Window

Step 15. Click **OK** to go back to the Sign-on window.

Before starting the VPN connection, you must make sure your system has established the network connection with the server, and the server has assigned an IP address to your system.

Step 16. Enter your username and password in the appropriate boxes and then click the **Connect** button to connect to the server. You may choose to save this username and password for future uses before clicking the **Connect** button.

Figure 3-42. Sign-on Window

After the connection is made, the connection icon appears in the notification area on the lower-right corner of the screen as shown below.

Figure 3-43. Connection Icon

You may double-click the icon to display the status of the connection.

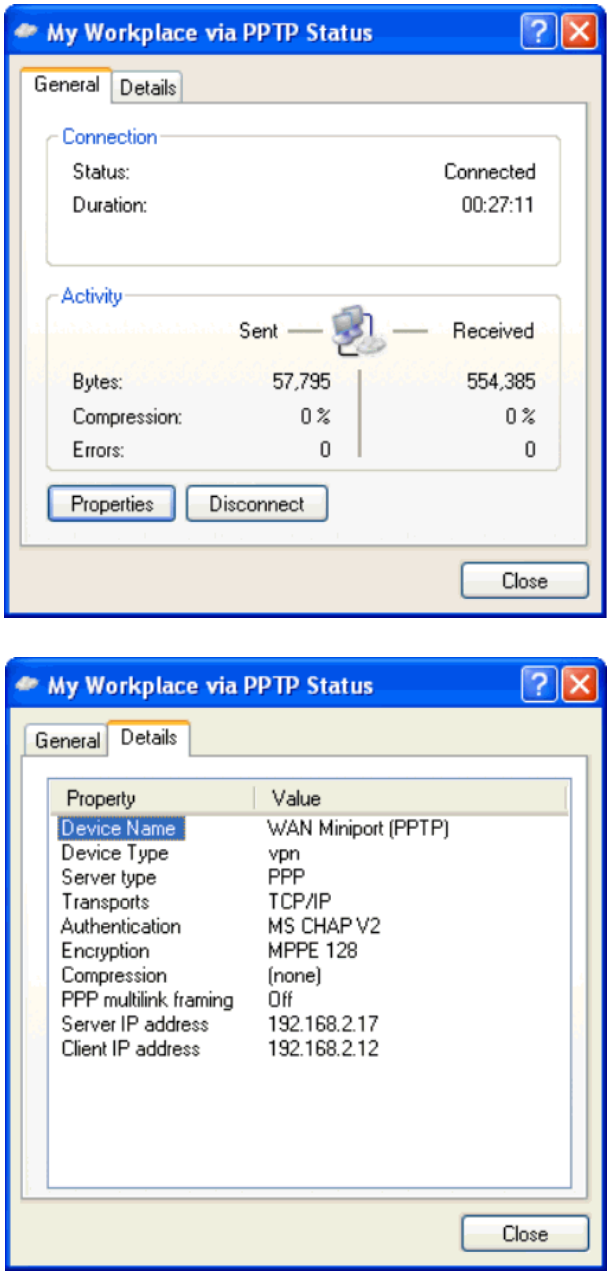

Figure 3-44. Connection Status Windows

Notice that your system is now connected to the server via the VPN device using PPTP protocol with 128-bit session key and MS CHAP v2 authentication.

Windows 2000/NT Clients

In this section, the procedures for configuring a PPTP connection on Windows 2000/NT are described.

The following procedures are created based on a Windows 2000 client. You may follow similar procedures for configuring PPTP on Windows NT (RAS).

Step 1. Open the Network and Dial-up Connections window:

Click the **Start** button. Move the pointer to and select **Programs**, **Accessories**, and **Communications**, respectively. Click **Network and Dial-up Connections** on the **Communications** menu.

The Network and Dial-up Connections window appears.

Step 2. Double-click the **Make new connection** icon.

The Network Connection Wizard window appears.

Figure 3-45. Network Connection Wizard

Step 3. Click the **Next>** button to go to the Network Connection Type page. Select the **Connect to a private network through the Internet** option and then click the **Next>** button.

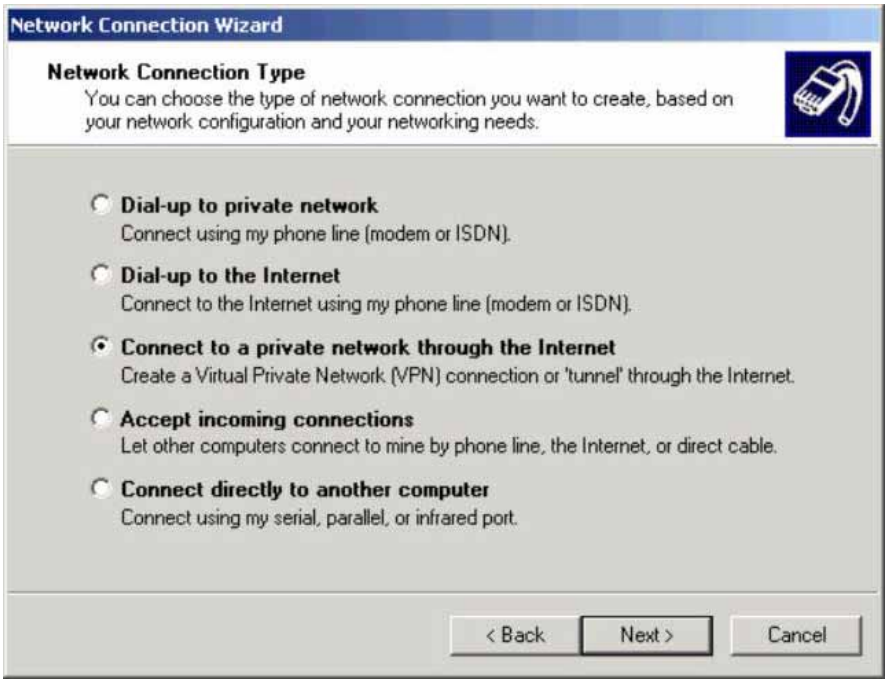

Figure 3-46. Network Connection Type Window

Step 4. Enter the destination address in the **Host name or IP address** text box. In this case, the internal address `42.0.0.1` of the 700wl Series unit (either Integrated Access Manager or Access Controller) is used. Click **Next>**.

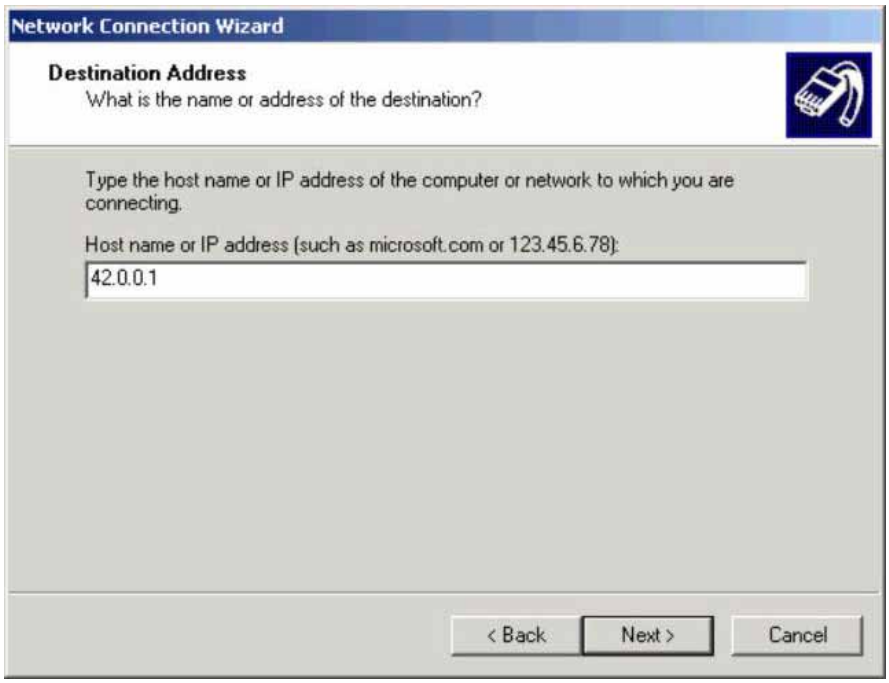

Figure 3-47. Destination Address Window

Step 5. The network connection wizard will display the Public Network screen if other dial-up connections exist. Select the **Do not dial the initial connection** option and then click **Next>**.

If no other dial-up connection is previously created, the Connection Availability window shown in Step 6 is displayed.

Step 6. Select the desired Connection Availability option, e.g., **Only for myself**. Click **Next>**.

Figure 3-48. Connection Availability Window

Step 7. Click the **Finish** button. You may choose to add a shortcut to this connection to the desktop before clicking the **Finish** button.

Figure 3-49. Network Connection Wizard Completion Window

At this point, an icon, named **Virtual Private Network**, representing the new connection appears in the Network and Dial-up Connections window. In the meantime, the Sign-on window should appear on the screen; otherwise, double-click the new connection icon.

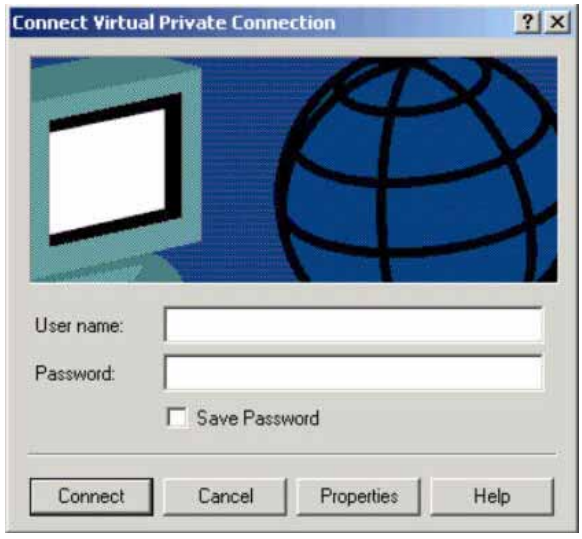

Figure 3-50. Sign-on Window

Step 8. You need to customize the properties of your connection to use PPTP and match the settings of the 700wl Series unit. Click the **Properties** button to open the connection's properties window.

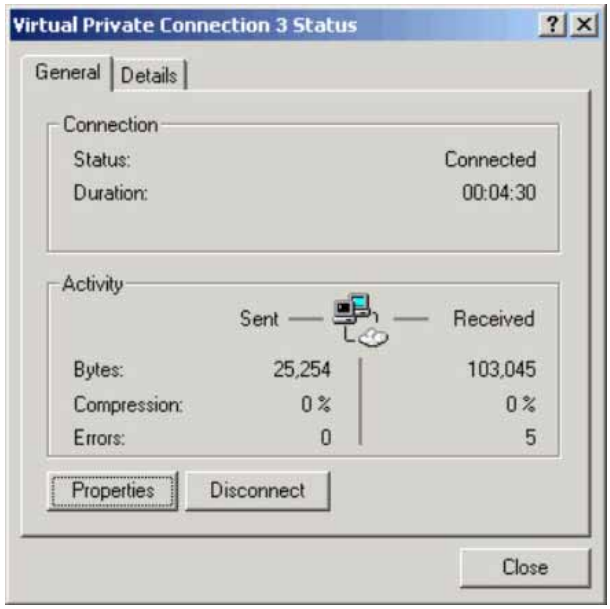

Figure 3-51. Virtual Private Connection Window, General Tab

Step 9. Click the Networking tab to specify the type of VPN. Next, pull down the **Type of VPN** menu and select **PPTP**. Make sure that **Internet Protocol (TCP/IP)** is selected.

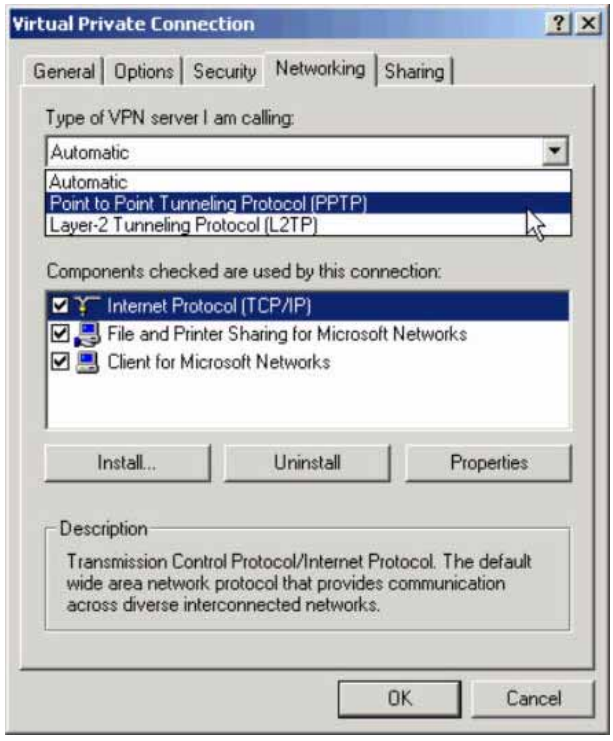

Figure 3-52. Virtual Private Connection Window, Networking Tab

Step 10. Click the Security tab to customize the security protocols. Next, select **Advanced (custom settings)** and then click the **Settings** button.

Figure 3-53. Virtual Private Connection Window, Security Tab

The Advanced Security Settings window appears.

Step 11. Make sure that **Microsoft CHAP (MS-CHAP)** is *not* selected. Note that this protocol is selected by default. You must deselect this option so that only MS-CHAP v2 is used.

Step 12. Pull down the **Data Encryption** menu and select **Maximum strength encryption (disconnect if server declines)**. This will set the length of the encryption key to 128 bits.

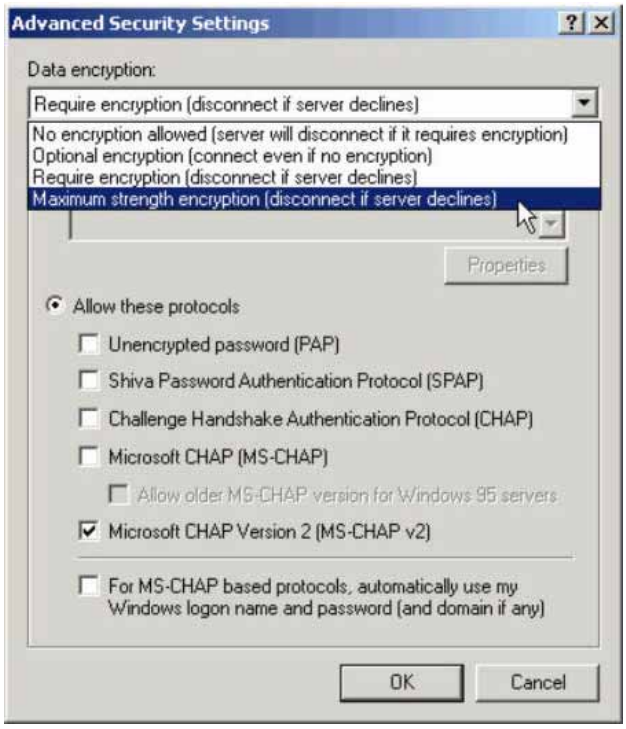

Figure 3-54. Advanced Security Settings Window

Step 13. Click **OK** to go back to the connection's properties window.

Step 14. Click **OK** to go back to the Sign-on window.

Before starting the VPN connection, you must make sure your system has established the network connection with the server, and the server has assigned an IP address to your system.

Step 15. Enter your username and password in the appropriate boxes and then click the **Connect** button to connect to the server. You may choose to save this username and password for future uses before clicking the **Connect** button.

Figure 3-55. Sign-on Window

After the connection is made, the connection icon appears in the notification area on the lower-right corner of the screen as shown below

Figure 3-56. Connection Icon

You may double-click the icon to display the status of the connection.

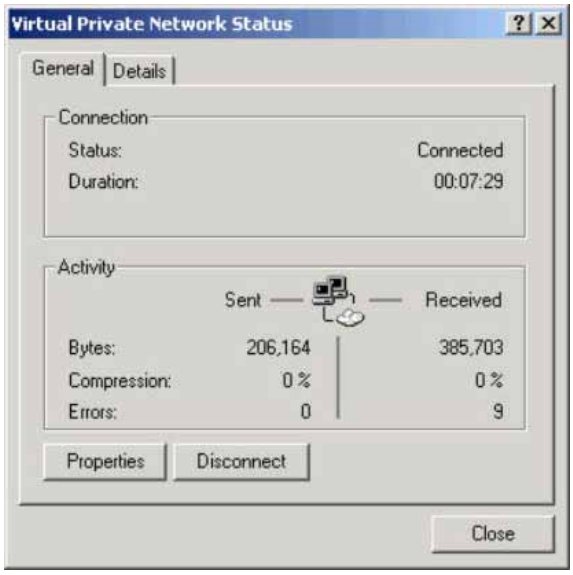

Figure 3-57. Virtual Private Network Status Window, General Tab

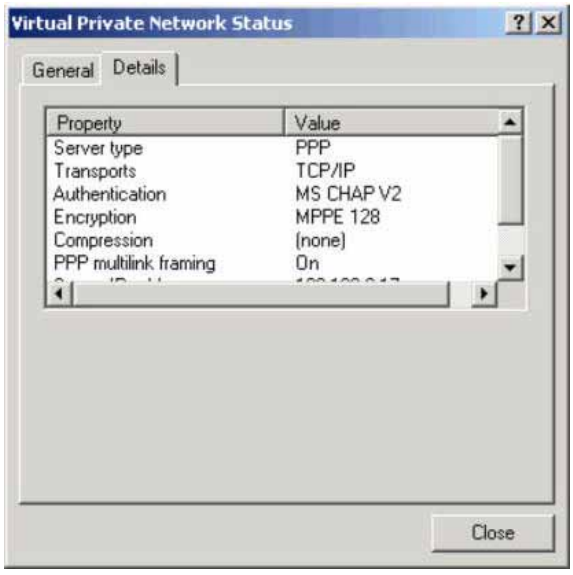

Figure 3-58. Virtual Private Network Status Window, Details Tab

Notice that your system is now connected to the server via PPP using 128-bit encryption and MS CHAP v2 authentication.

Windows 98/95/ME Clients

This section describes the procedures for configuring a PPTP connection on Windows 98/95/ME.

For Windows 95, make sure that Dial-up Networking has been updated to version 1.3 and Virtual Private Networking for Windows 95 has been installed.

For Windows 98, make sure that the Virtual Private Networking has been updated. You should read Article Q237691 at http://www.microsoft.com prior to updating the software.

The software updates for both Windows 95 and 98 can be found at the Microsoft web site. The easiest approach to find all the information at once is by searching for the keyword "DUN" at the web site.

The following procedures are created based on a Windows 98 client. You may follow similar procedures for configuring PPTP on Windows 95 and ME.

Step 1. Open the Dial-Up Networking window:

Move the pointer to the **My Computer** icon on the desktop. Right-click the icon to display the pop-up menu and then select **Explore**.

The Exploring - My Computer window appears.

Double-click the **Dial-Up Networking** link on the **Network Tasks** panel.

The New Connection Wizard window appears.

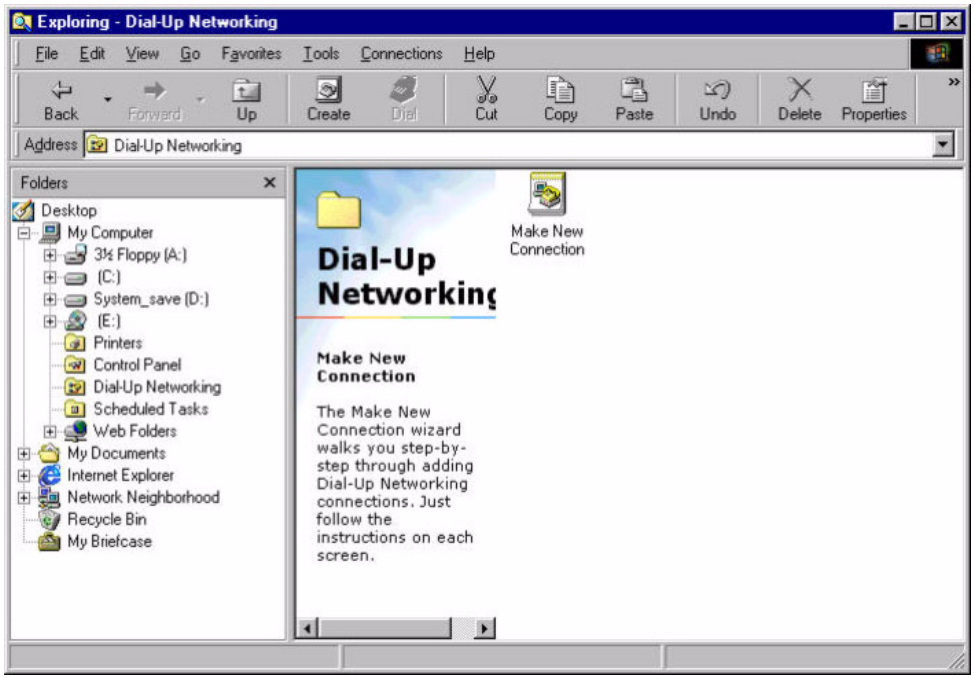

Figure 3-59. New Connection Wizard Window

Step 2. Double-click the **Make New Connection** icon to start the Make New Connection wizard (see Figure 3-60). Enter the desired connection name in the text box. Pull-down the **Select a device** menu and then select **Microsoft VPN Adapter**. Click **Next>**.

Figure 3-60. Make New Connection Window, selecting a device

Note that if **Microsoft VPN Adapter** does not appear on the menu, you must cancel the Make New Connection activities and add the VPN adapter to the Network's Properties.

Step 3. Enter the IP address of the VPN server in the **Host name or IP address** text box. In this case, the internal address `42.0.0.1` of the 700wl Series unit (either Access Controller or Integrated Access Manager) is used. Click **Next>**.

Figure 3-61. Make New Connection Window, VPN server address

Step 4. Click the **Finish** button to complete the process.

Figure 3-62. Make New Connection Window, Final Screen

At this point, an icon representing the new connection appears in the Dial-Up Networking window as shown below.

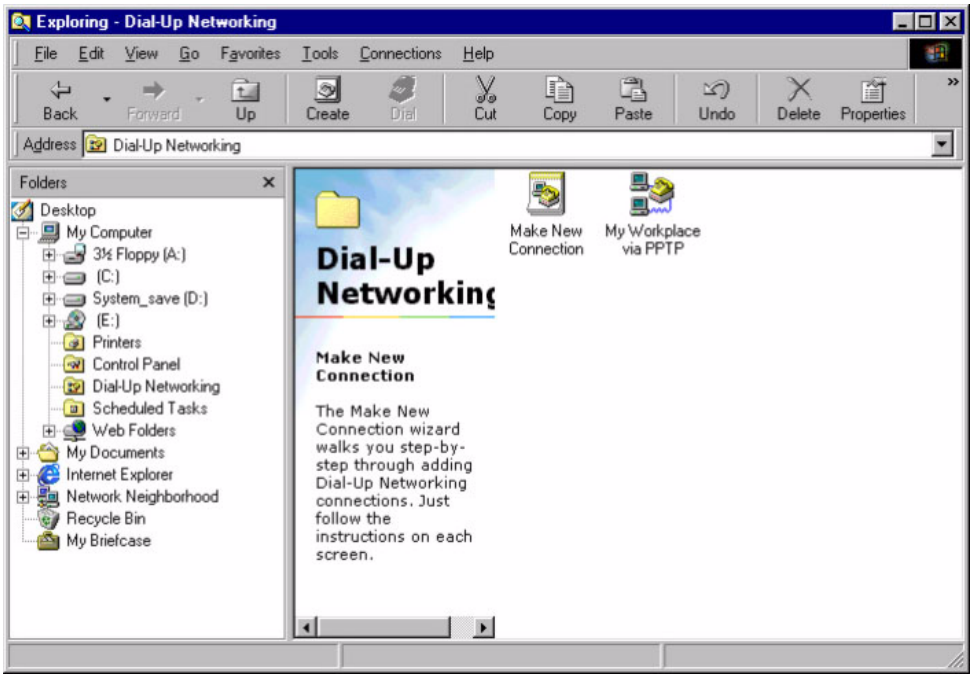

Figure 3-63. Dial-up Networking Window with new connection icon

Step 5. To set the default gateway for the remote network, right-click the new connection icon, and select **Properties** from the pop-up menu.

Go to the Server Types tab and click the **TCP/IP Settings...** button. The TCP/IP Settings window appears (see Figure 3-64).

Check the box for **Use default gateway on remote network** at the bottom of the window.

Click **OK** to close the window, and **OK** in the Properties window.

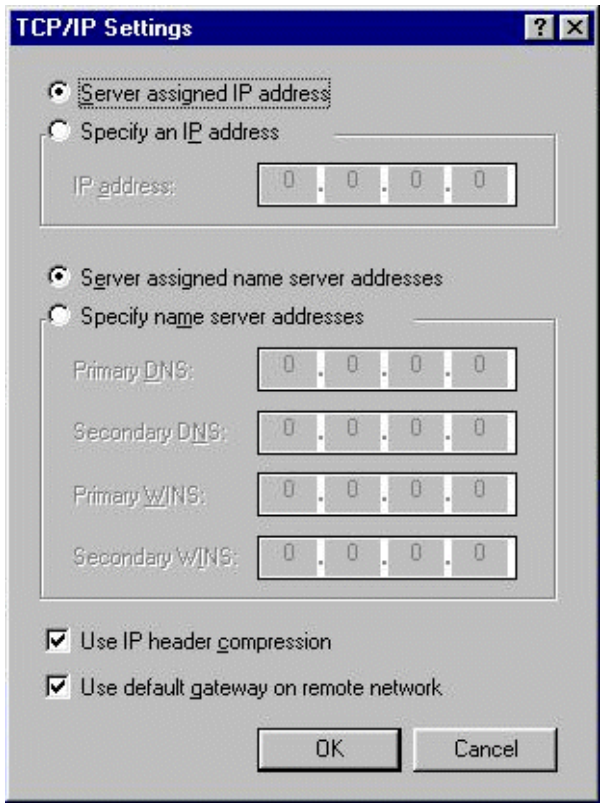

Figure 3-64. TCP/IP Settings window

Before starting the VPN connection, you must make sure your system has established the network connection with the server, and the server has assigned an IP address to your system.

Step 6. Double-click the new connection icon to start connecting. The Connect To window appears. Enter your username and password in the appropriate boxes and then click the **Connect** button to connect to the server. You may choose to save this username and password for future uses before clicking the **Connect** button.

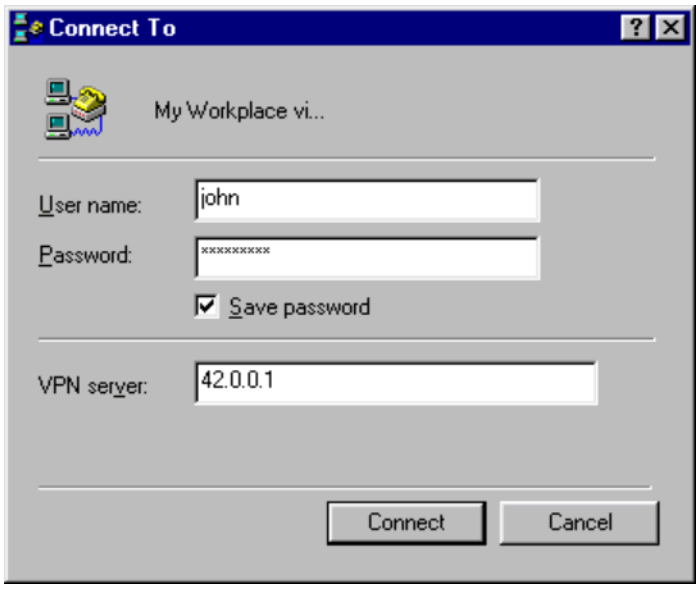

Figure 3-65. Connect To Window

After the connection is made, the connection icon appears in the notification area on the lower-right corner of the screen as shown below.

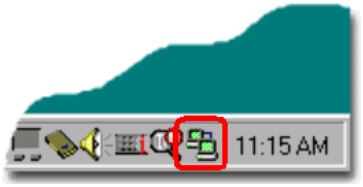

Figure 3-66. Connection Icon

You may double-click the icon to display the status of the connection.

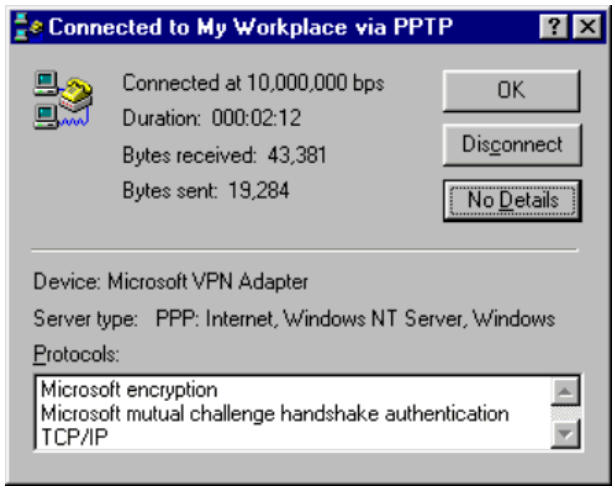

Figure 3-67. Connection Status Window

Notice that your system is now connected to the server via PPP using Microsoft encryption and Microsoft mutual challenge handshake (MS CHAP) authentication. This PPP connection is certainly using a 128-bit encryption key and MS CHAP v2 authentication because the server is configured to accept only this type of the connection.

Note: *If the server rejects the connection, it is highly likely that the 128-bit encryption key does not work.*

You need to access the Rights Manager to modify the Location's properties to lower the minimum encryption key length to 40 bits (see "Configuring the Rights Manager for PPTP" on page 2-8).

LAN Tunnel Builder (PPTP) for Mac OS 9

In this section, the procedures for configuring LAN Tunnel Builder, which is a PPTP client software for Mac OS 9, are described.

Step 1. Configure Tunnel Builder in the TCP/IP control panel.

Select **LAN TunnelBuilder** from the **Connect via** menu and **Using PPP Server** from the **Configure** menu. Next, enter the DNS server address in the **Name server addr.** text box.

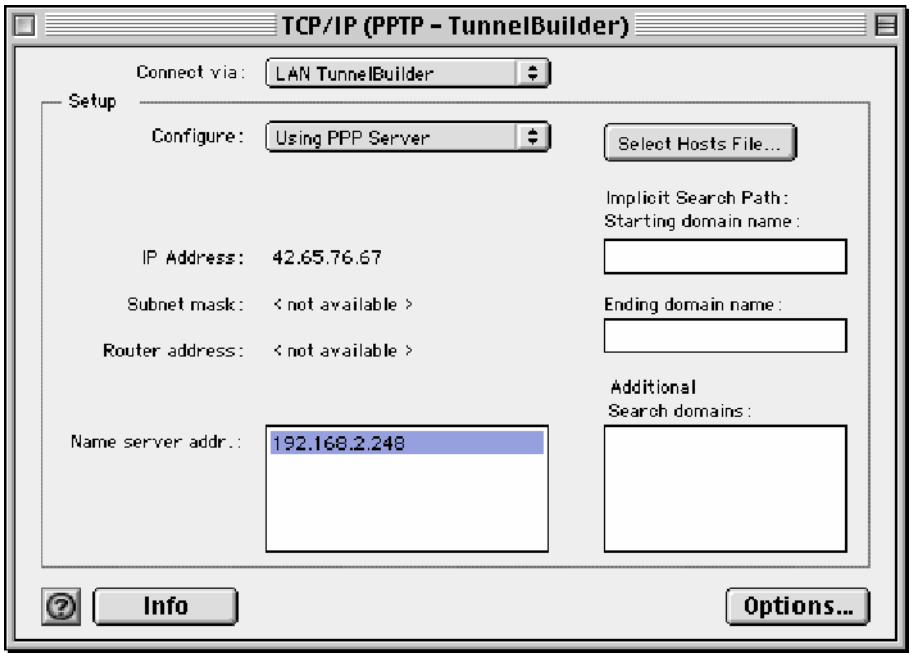

Figure 3-68. TCP/IP (PPTP - TunnelBuilder) Dialog

Step 2. Double-click the **LAN TunnelBuilder Settings** icon to start the application.

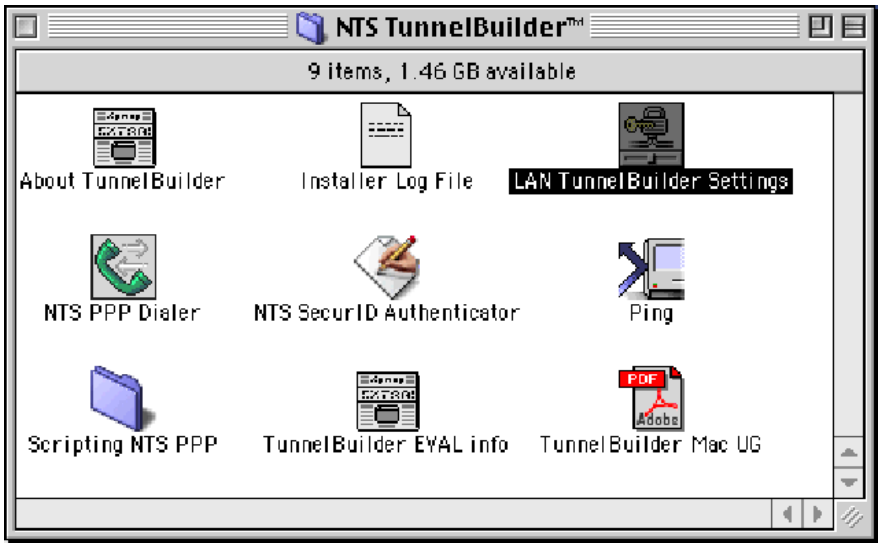

Figure 3-69. TunnelBuilder Settings Icon

Step 3. Once the LAN TunnelBuilder window appears, do the following to configure the application:

a. Select **Airport** from the **Connect via** menu

b. Select **Using DHCP Server** from the **Configure** menu

c. Select **PPTP** from the **VPN Protocol** menu

d. Enter the desired username in the **VPN Username** text box

e. Enter the corresponding password in the **VPN Password** text box

f. Enter `42.0.0.1` in the **VPN Server Address** text box

g. Select **MPPE** from the **Encryption** menu

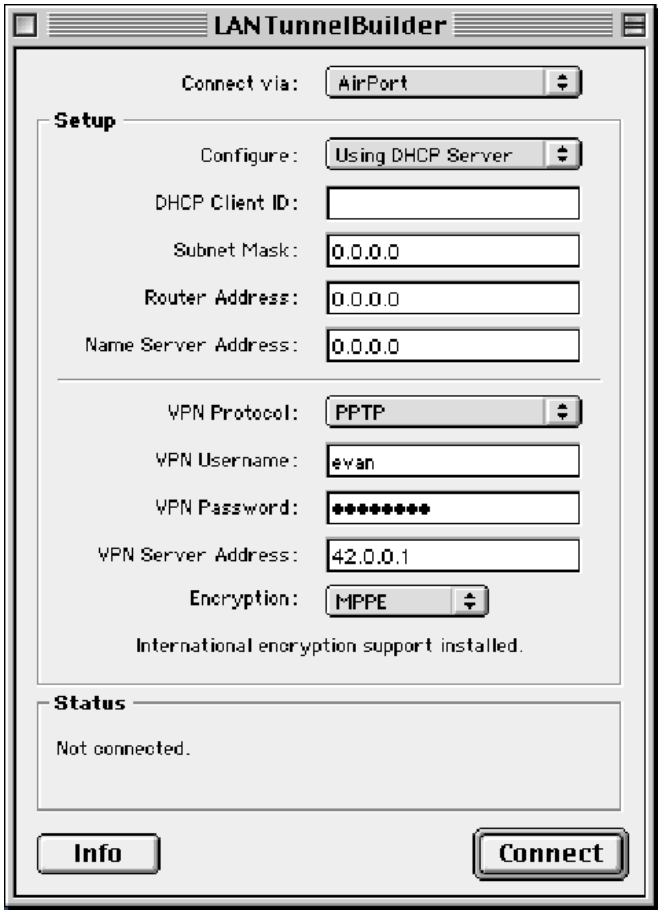

Figure 3-70. LAN TunnelBuilder Window

Step 4. Click the **Connect** button to initiate a PPTP tunnel.

After a successful connection, the status section in the LAN TunnelBuilder window is updated with the connection information.

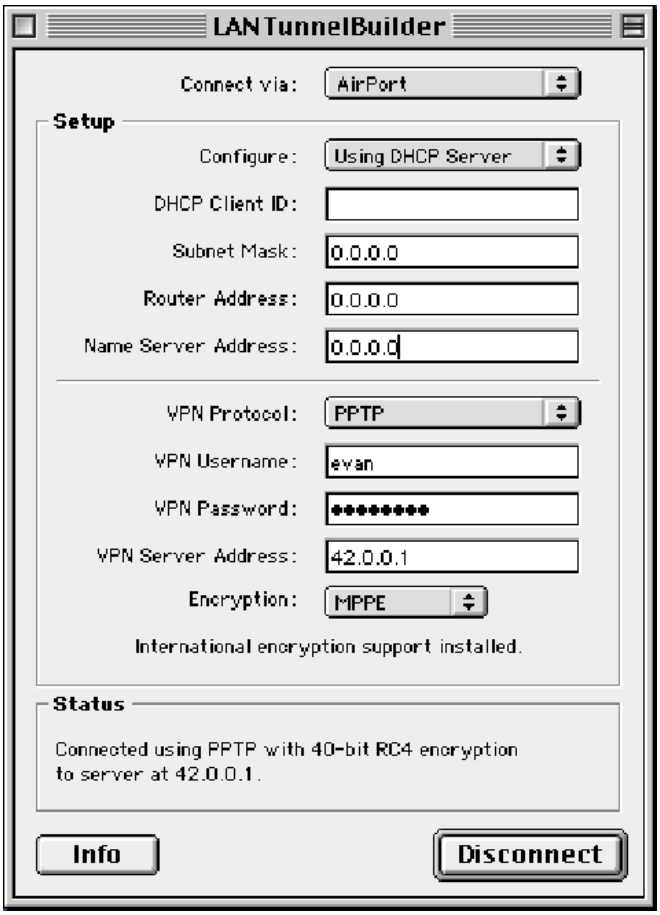

Figure 3-71. LAN TunnelBuilder Window

Note: *Tunnel Builder will not work with the default settings of the 700wl Series system.*

You need to go to the Rights Manager to modify the Location's properties to lower the Minimum encryption key length to 40 bits and select MS-CHAP or MS-CHAP v2 (See "Configuring the Rights Manager for PPTP" on page 2-8).

L2TP/IPSec Client Configuration

This section describes how to configure computers running Windows XP and Windows 2000 as L2TP / IPSec clients.

Windows XP Clients

Before configuring the L2TP / IPSec client, please read Chapter 4 "Setup Scripts for L2TP / IPSec on Windows 2000 or XP". The instructions in Chapter 4 will guide you through the uses of Microsoft Connection Manager Administration Kit to create a script for setting up an L2TP / IPSec connection on Windows XP. If you use the script, you do not need to use the procedure described here.

Do the following to configure the Windows XP client:

Step 1. Open the Network Connections window:

Click the **Start** button and then move the pointer to **My Network Places**. Right-click **My Network Places** to display the pop-up menu and then select **Properties**.

The Network Connections window appears.

Step 2. Click the **Create a new connection** link on the **Network Tasks** panel.

The New Connection Wizard window appears.

Step 3. Click the **Next>** button to go to the Network Connection Type page.

Figure 3-72. New Connection Wizard

Step 4. Select the **Connect to the network at my workplace** option and then click the **Next>** button.

Figure 3-73. Network Connection Type Window

Step 5. Select the **Virtual Private Network connection** option. Click **Next>**.

Figure 3-74. Network Connection Window

Step 6. Enter the desired connection name in the **Company Name** text box. Click **Next>**.

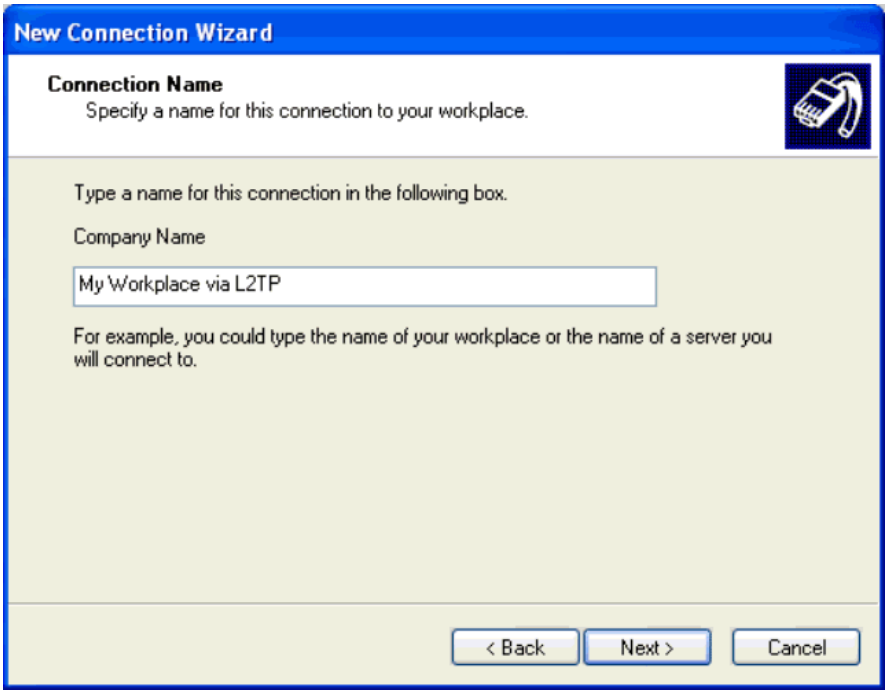

Figure 3-75. Connection Name Window

Step 7. Enter the IP address of the VPN server in the **Host name or IP address** text box. In this case, the internal address `42.0.0.1` of the 700wl Series unit (either Access Controller or Integrated Access Manager) is used. Click **Next>**.

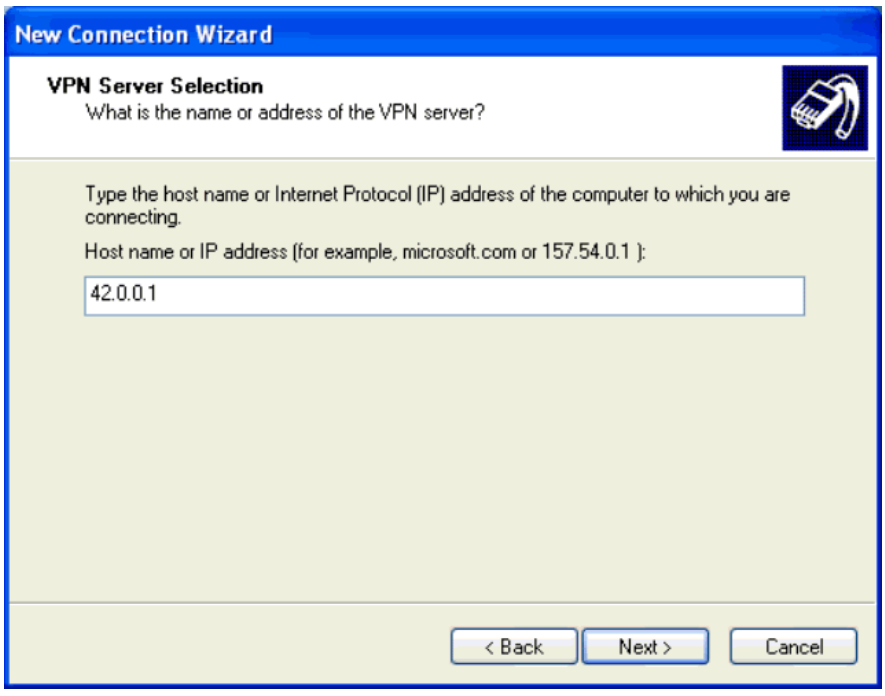

Figure 3-76. VPN Server Selection Window

The Completing the New Connection Wizard page appears.

Step 8. Click the **Finish** button. You may choose to add a shortcut to this connection to the desktop before clicking the **Finish** button.

Figure 3-77. New Connection Wizard, Completion Window

At this point, an icon representing the new connection appears in the Network Connections window under the **Virtual Private Network** section. In the meantime, the Sign-on window should appear on the screen; otherwise, double-click the new connection icon.

Figure 3-78. Sign-on Window

Step 9. You need to customize the properties of your connection to use L2TP/IPSec and match the settings of the 700wl Series unit. Click the **Properties** button to open the connection's properties window.

Step 10. Click the Networking tab to specify the type of VPN.

Pull down the **Type of VPN** menu and select **L2TP IPSec VPN**. Make sure that **Internet Protocol (TCP/IP)** is selected.

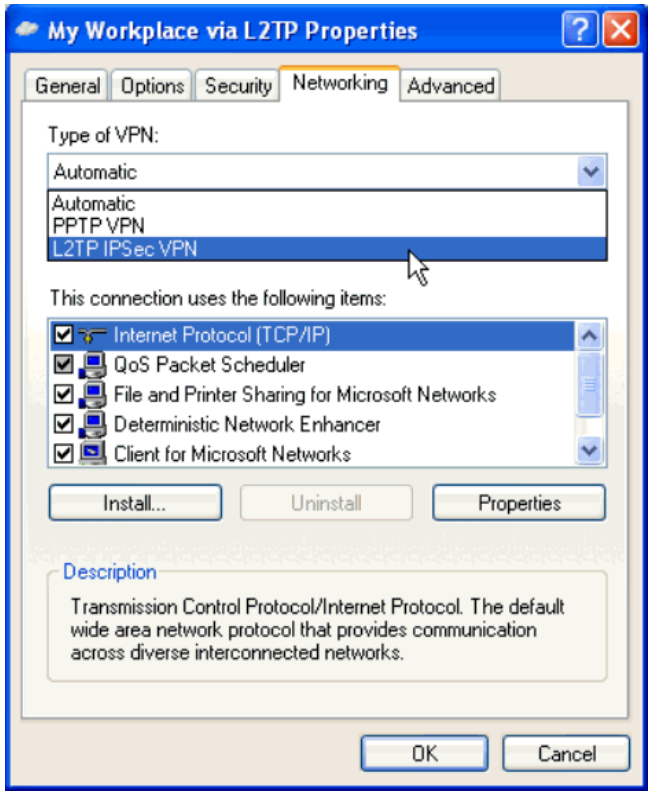

Figure 3-79. L2TP Properties Window, Networking Tab

Step 11. Click the Security tab to customize the security protocols.

Select **Advanced (custom settings)** and then click the **Settings** button.

The Advanced Security Settings window appears.

Step 12. Make sure that **Microsoft CHAP (MS-CHAP)** is *not* selected. Note that this protocol is selected by default. You must clear the selection so that only MS-CHAP v2 is used.

If an external LDAP server is used for user authentication with PAP (an Option in the Location properties), then make sure that only **Unencrypted password (PAP)** is selected.

Step 13. Pull down the **Data Encryption** menu and select **Maximum strength encryption (disconnect if server declines)**. This will set the length of the encryption key to 128 bits.

If an external LDAP server is used for user authentication with PAP, then select **Optional encryption (connect even if no encryption)** from the **Data encryption** menu.

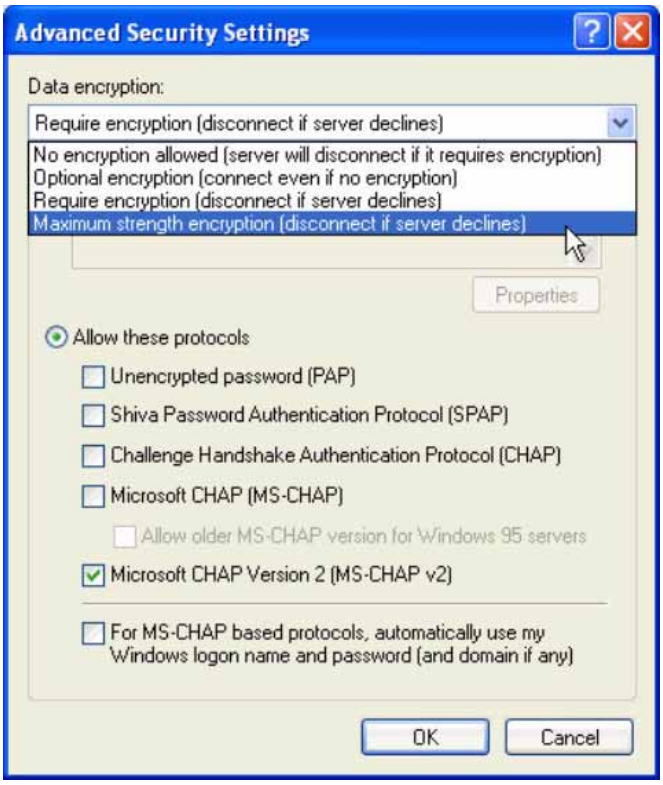

Figure 3-80. Advanced Security Settings Window

Step 14. Click **OK** to return to the Security tab.

Step 15. Click the **IPSec Settings** button.

The IPSec Settings window appears.

Step 16. Enter the appropriate pre-shared key in the **Key** text box. Click **OK**.

Figure 3-81. IPSec Settings Authentication Window

Step 17. Click **OK** to go back to the Sign-on window.

Before starting the VPN connection, you must make sure your system has established the network connection with the server, and the server has assigned an IP address to your system.

Step 18. Enter your username and password in the appropriate boxes and then click the **Connect** button to connect to the server. You may choose to save this username and password for future uses before clicking the **Connect** button.

Figure 3-82. Sign-on Window

After the connection is made, the connection icon appears in the notification area on the lower-right corner of the screen as shown below.

Figure 3-83. Connection Icon

You may double-click the icon to display the status of the connection.

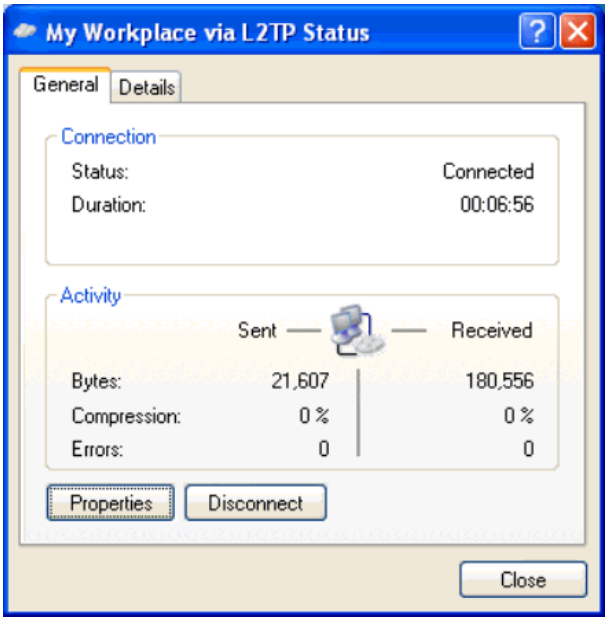

Figure 3-84. Connection Status Window, General Tab

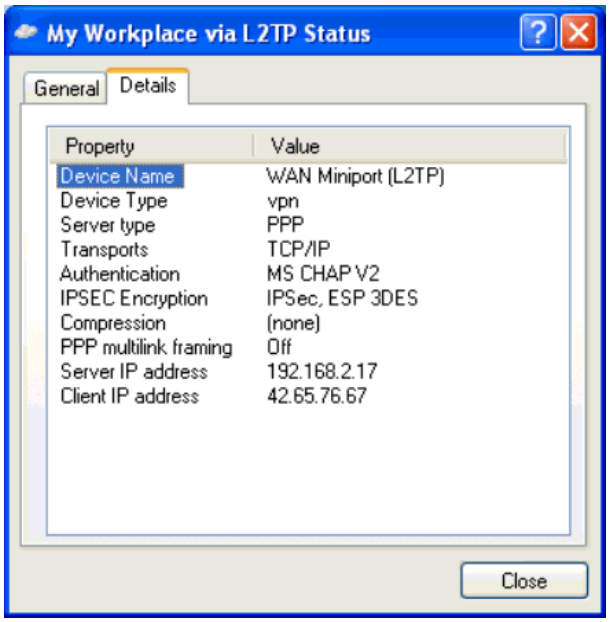

Figure 3-85. Connection Status Window, Details Tab

Notice that your system is now connected to the server via IPSec using 3DES (168-bit) encryption and MS CHAP v2 authentication.

Windows 2000 Clients

Before configuring the L2TP / IPSec client, please read Chapter 4 “Setup Scripts for L2TP / IPSec on Windows 2000 or XP”. The instructions in Chapter 4 will guide you through the uses of Microsoft Connection Manager Administration Kit to create a script for setting up an L2TP / IPSec connection on Windows 2000. If the script is used, it is not required to follow the instructions described below.

Do the following to configure the L2TP / IPSec connection on Windows 2000:

Step 1. Open the Network and Dial-up Connections window:

Click the **Start** button. Move the pointer to and select **Programs**, **Accessories**, and **Communications**, respectively. Click **Network and Dial-up Connections** on the **Communications** menu.

The Network and Dial-up Connections window appears.

Step 2. Double-click the **Make new connection** icon.

The Network Connection Wizard window appears.

Figure 3-86. Network Connection Wizard

Step 3. Click the **Next>** button to go to the Network Connection Type page.

Step 4. Select the **Connect to a private network through the Internet** option and then click the **Next>** button.

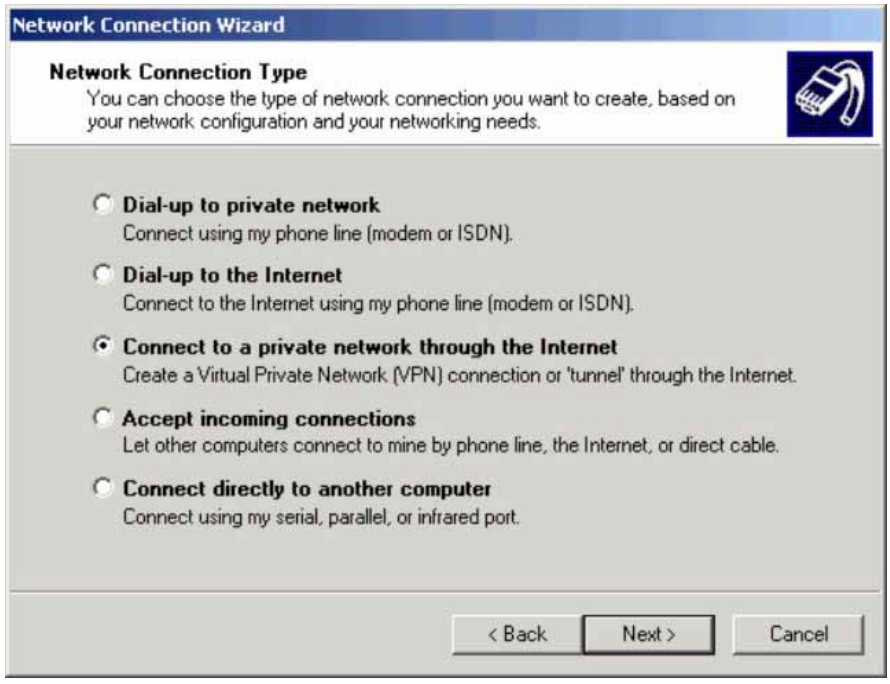

Figure 3-87. Network Connection Type Window

Step 5. Enter the destination address in the **Host name or IP address** text box. In this case, the internal address `42.0.0.1` of the 700wl Series unit (either Access Controller or Integrated Access Manager) is used. Click **Next>**.

Figure 3-88. Destination Address Window

Step 6. The network connection wizard will display the Public Network screen if other dial-up connections exist. Select the **Do not dial the initial connection** option and then click **Next>**.

If no other dial-up connection is previously created, the Connection Availability window shown in Step 6 is displayed.

Step 7. Select the desired Connection Availability option, e.g., **Only for myself**. Click **Next>**.

Figure 3-89. Connection Availability Window

Step 8. Enter the desired name for this connection in the text box and then click the **Finish** button. You may choose to add a shortcut to this connection to the desktop before clicking the **Finish** button.

Figure 3-90. Network Connection Wizard, Completion Window

At this point, an icon, named **Virtual Private Network**, representing the new connection appears in the Network and Dial-up Connections window. In the meantime, the Sign-on window should appear on the screen; otherwise, double-click the new connection icon.

Figure 3-91. Sign-on Window

Step 9. You need to customize the properties of your connection to use L2TP over IPSec and match the settings of the 700wl Series unit. Click the **Properties** button to open the connection's properties window.

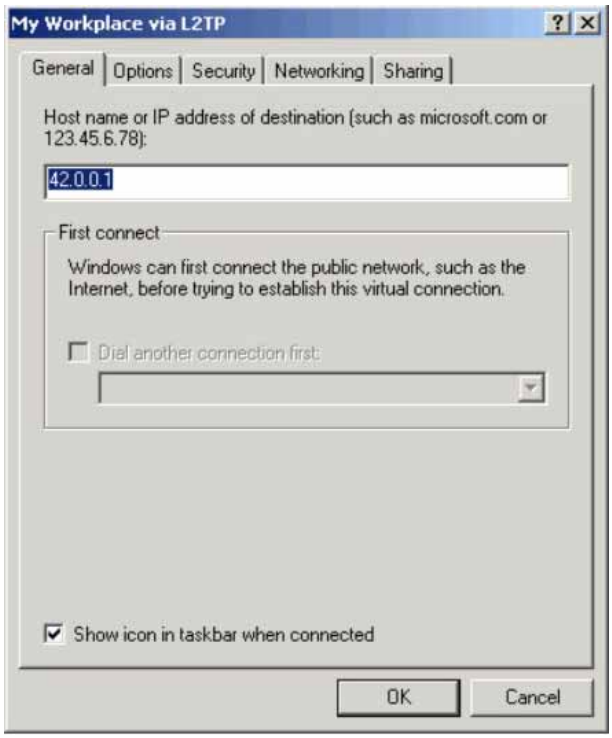

Figure 3-92. L2TP Connection Properties Window, General Tab

Step 10. Click the Networking tab to specify the type of VPN. Next, pull down the **Type of VPN** menu and select **L2TP**. Make sure that **Internet Protocol (TCP/IP)** is selected.

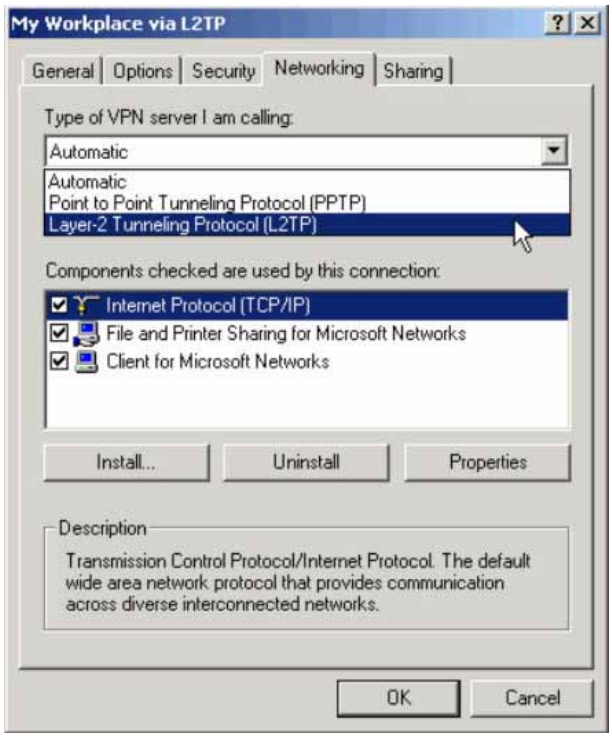

Figure 3-93. L2TP Connection Properties Window, Networking Tab

Step 11. Click the Security tab to customize the security protocols. Next, select **Advanced (custom settings)** and then click the **Settings** button.

Figure 3-94. Virtual Private Connection Window, Security Tab

The Advanced Security Settings window appears.

Step 12. Make sure that **Microsoft CHAP (MS-CHAP)** is *not* selected. Note that this protocol is selected by default. You must deselect this option so that only MS-CHAP v2 is used.

If an external LDAP server is used for user authentication with PAP (an Option in the Location properties), then make sure that only **Unencrypted password (PAP)** is selected.

Step 13. Pull down the **Data Encryption** menu and select **Maximum strength encryption (disconnect if server declines)**. This will set the length of the encryption key to 128 bits.

If an external LDAP server is used for user authentication with PAP, then select **Optional encryption (connect even if no encryption)** from the **Data encryption** menu.

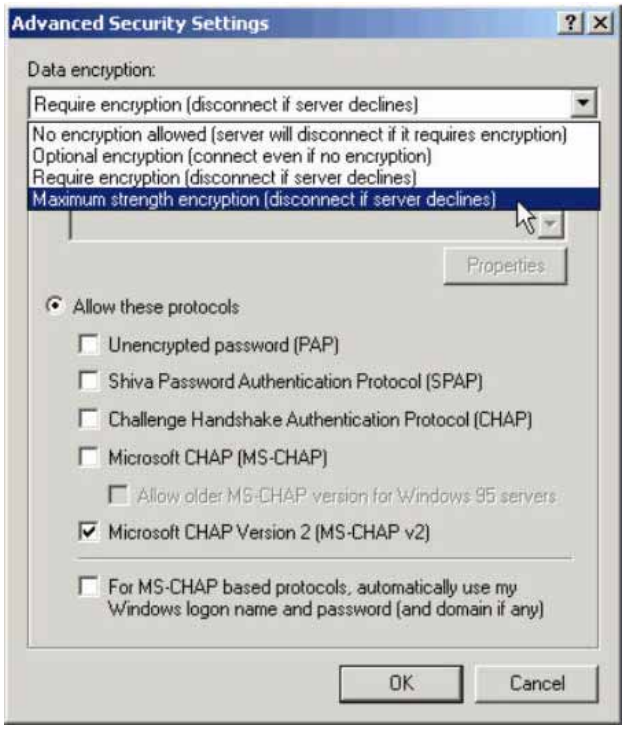

Figure 3-95. Advanced Security Settings Window

Step 14. Click **OK** to go back to the connection's properties window.

Step 15. Click **OK** to go back to the Sign-on window

Before starting the VPN connection, you must make sure your system has established the network connection with the server, and the server has assigned an IP address to your system.

Step 16. Enter your username and password in the appropriate boxes and then click the **Connect** button to connect to the server. You may choose to save this username and password for future uses before clicking the **Connect** button.

Figure 3-96. Sign-on Window

After the connection is made, the connection icon appears in the notification area on the lower-right corner of the screen as shown below.

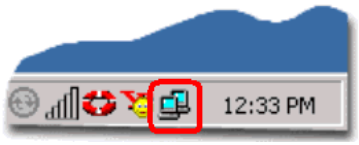

Figure 3-97. Connection Icon

You may double-click the icon to display the status of the connection.

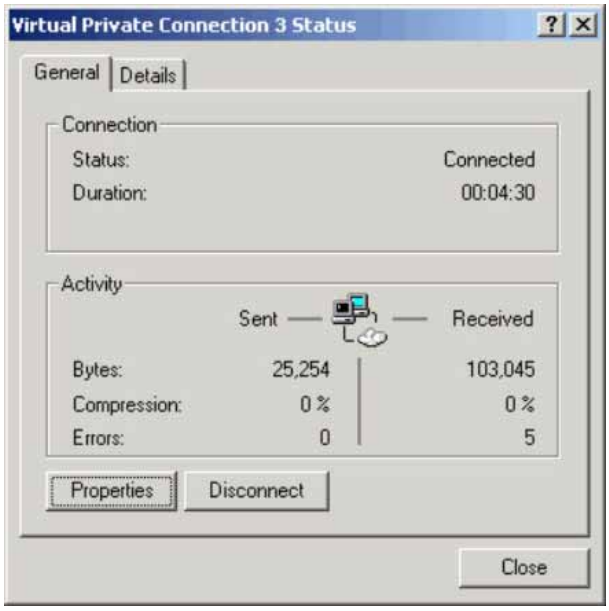

Figure 3-98. Virtual Private Connection Status Window, General Tab

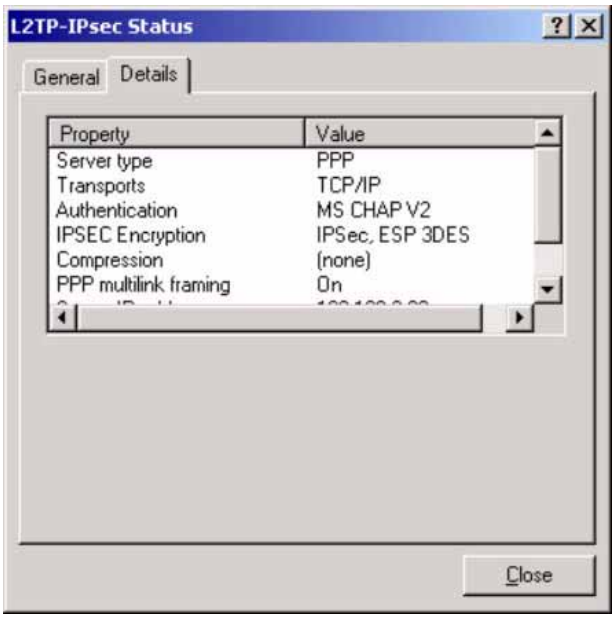

Figure 3-99. L2TP-IPSec Status Window, Details Tab

Notice that your system is now connected to the server via IPSec using 3DES (168-bit) encryption and MS CHAP v2 authentication.

SSH Client Configuration

There are many Windows-based SSH client programs available for download on the Internet. One popular freeware is “PuTTY” which can be obtained from:

http://www.chiark.greenend.org.uk/~sgtatham/ putty/download.html.

This section describes how to configure a computer running Microsoft Windows as an SSH client using PuTTY.

PuTTY for Windows

The following procedure is based on a Windows XP client. You may follow the same procedures for configuring the software on different Windows platforms.

Step 1. Start “putty.exe” from the location where you stored the downloaded file

Figure 3-100. The PuTTY desktop icon

Step 2. The PuTTY Configuration window appears.

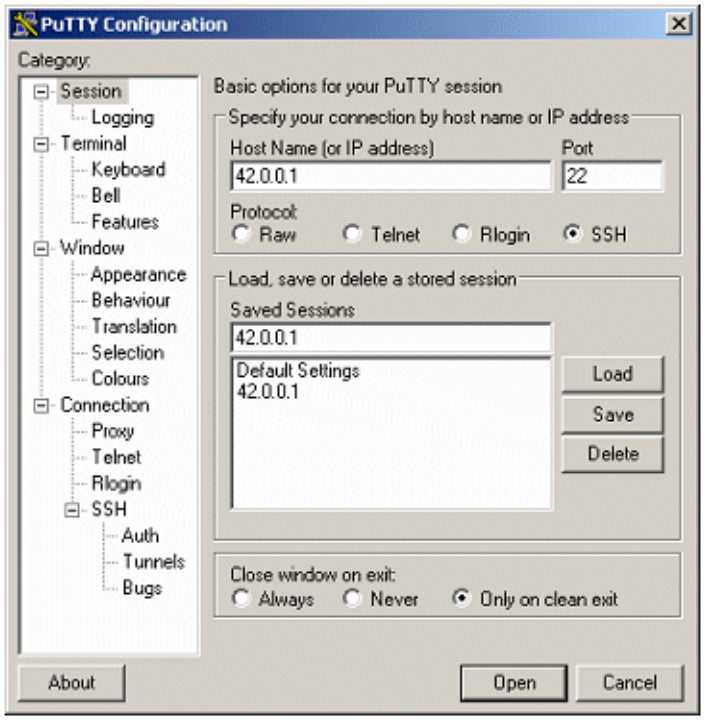

Figure 3-101. The PuTTY Configuration window

Step 3. Enter `42.0.0.1` in the **Host Name (or IP address)** field and then select **SSH** for Protocol. Note that once SSH has been selected the Port field is automatically updated to "22".

Step 4. (Optional) Enter `42.0.0.1` in the **Saved Sessions** field and then click **Save** to store the setting so that it can be reused in the next logon attempt.

Step 5. (Optional) Configure port forwarding tunnels to encrypt application data such as SMTP, POP3, and IMAP via the SSH session to the appropriate servers inside the network

a. Click **Tunnels** in the Category panel. The window displays tunneling configuration options (Figure 3-102).

b. Type the **Source port** and **Destination** address in the appropriate fields.

c. Click **Add.**

d. Repeat the above steps to include all desired applications. In the example shown in Figure 3-102, the Forwarded ports include SMTP, Proxy, POP3, and IMAP.

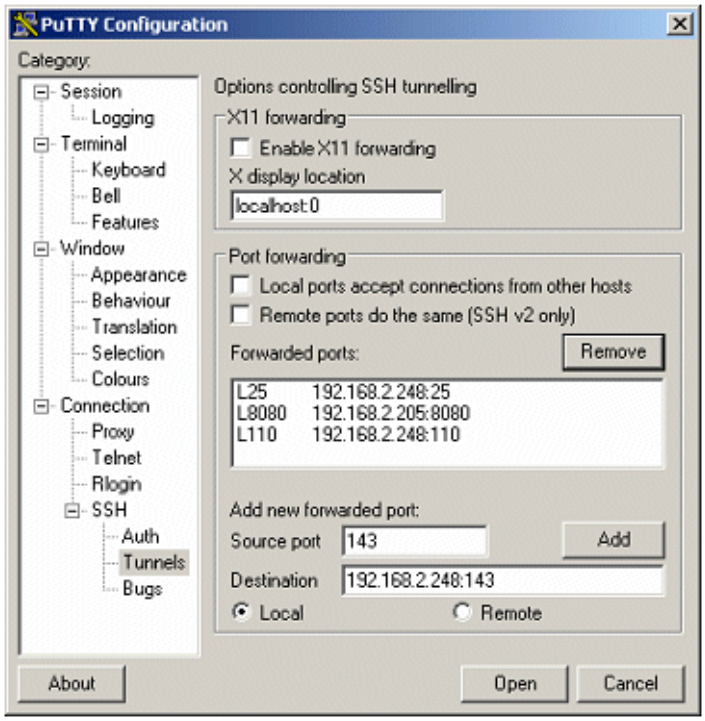

Figure 3-102. SSH Tunneling options

Note that, in changing the configuration, you are required to save the settings again so that the parameters can be reused.

When applicable, clients that use port forwarding must be reconfigured to use localhost or 127.0.0.1 (Loopback) as the server address.

Step 6. Click **Open**.

Step 7. If the client connects to the Integrated Access Manager / Access Controller for the first time, you will be prompted to save the server's digital certificate. Select **Yes** or **Save**.

Step 8. The PuTTY window displaying the login prompt appears (Figure 3-103).

Step 9. Type the username and press ENTER.

Step 10. Type the password and then press ENTER. You will not see anything you've typed for password.

At this point, you should be able to access the network normally. Please make sure to leave the PuTTY window open to stay connected.

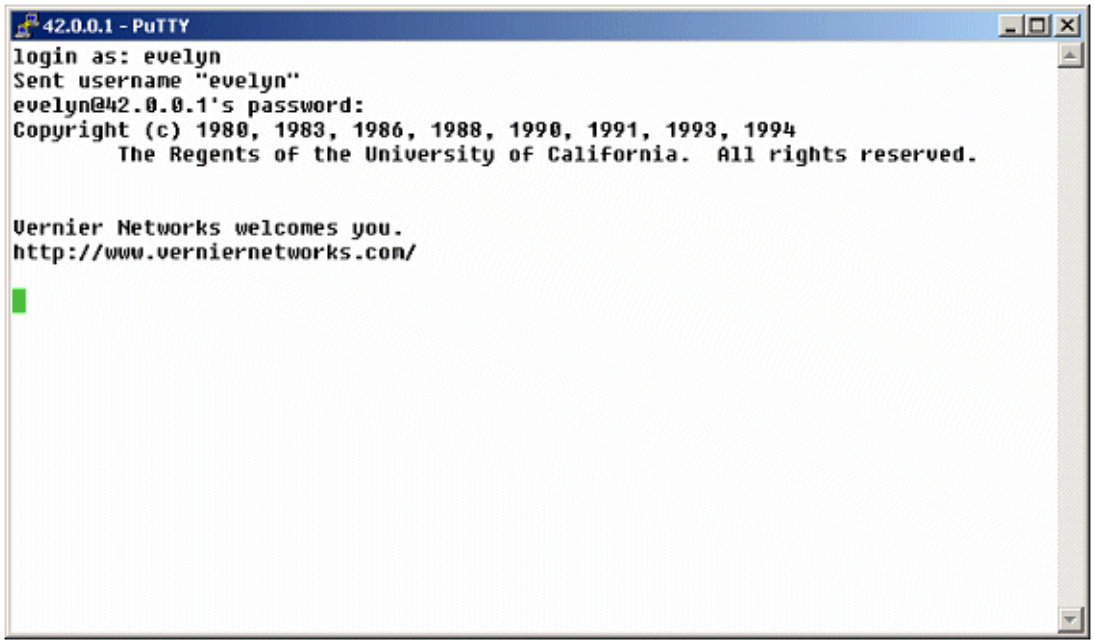

Figure 3-103. PuTTY login window

You may logoff the network by selecting the PuTTY window and then typing CTRL-D (CTRL and D keys together).

4 SETUP SCRIPTS FOR L2TP/IPSEC ON WINDOWS 2000 OR XP

This chapter describes the setup of L2TP / IPSec connections on Windows systems. It includes the following sections:

The information described in this section is intended for use by an administrator.

Scripts Overview

This section describes how to setup an L2TP / IPSec connection to the 700wl Series system on Windows 2000 and Windows XP.

Two scripts, one for Windows 2000 and the other for Windows XP, are used to streamline the setup process. Both scripts make use of Microsoft's CMAK (Connection Manager Administration Kit), which allows you to build a client connection installation package that reflects customer's settings. In addition to CMAK, the script for Windows 2000 makes use of Microsoft **ipsecpol.exe** command line program, which is a tool for configuring Internet Protocol Security (IPSec) policies on the computer.

Note: *The CMAK package is part of the adminpak that is found on the Windows 2000 Server distribution and Windows XP Professional. One can download the Beta 1.3 Distribution from the Microsoft download site (search for adminpak).*

The ipsecpol tool for Windows 2000 can also be downloaded from the Microsoft download site (search for ipsecpol).

It should be noted that without the two scripts, you still can create a new L2TP / IPSec connection using New Connection Wizard available by default on both Windows 2000 and Windows XP. See Chapter 3, "Client Configuration" for instructions.

What's in the Package?

The package contains two important subdirectories, including **win2k** and **winxp**. The list of files in each subdirectory is shown in Table 4-1.

Table 4-1. Files Contained In Package Subdirectories

Platform	Subdirectory	Files
Windows 2000	win2k	IPSECPOL.EXE
		IPSECUTIL.DLL
		prohibitIPSec.reg
		setupL2TP.cmd
		TEXT2POL.DLL
		uninstallL2Tp.cmd
		u_prohibitIPSec.reg
		MyL2TP.txt
		MyL2TP.exe
		MyL2TP.inf
		[MyL2TP_PAP]
		[MyL2TP_STD]
Windows XP	winxp	**setupl2tp_XP.cmd**
		uninstalll2tp_XP.cmd
		MyL2TP.exe
		MyL2TP.inf
		[MyL2TP_PAP]
		[MYL2TP_STD]

Note: *[*MyL2TP*_PAP] is the subdirectory containing files for setting up an L2TP connection that uses PAP (clear text) for authentication. If PAP is required, e.g. L2TP/IPSec via LDAP authentication, then copy all files in this subdirectory and place them in the win2k directory. This will overwrite the existing files.*

*[*MyL2TP*_STD] is the subdirectory containing files for setting up the L2TP connection that uses MS-CHAP v2 for authentication. This is the default set of files. All files in this subdirectory are only used for restoration purposes.*

Setting Up Windows 2000

Do the following to install and configure a new L2TP / IPSec connection on Windows 2000.

Step 1. Download the supplied ZIP package, **WIN2K_SETUP.zip**, from the 700wl Series system. This ZIP package is also available on the documentation CD.

Step 2. Extract the ZIP package to a directory, then go to the **win2k** subdirectory.

Step 3. To setup your IPSec shared secret, use a text editor, such as Notepad, to edit the file, **MyL2TP.txt**, and then replace the default shared secret, “mysecret” (see the figure below), with the one that is set on the 700wl Series system.

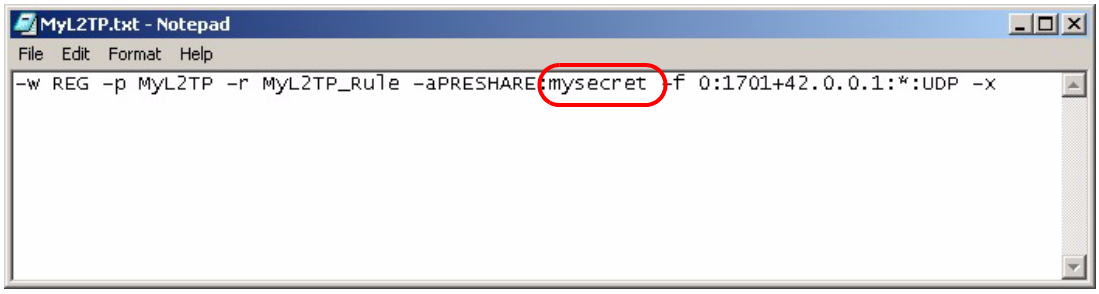

Figure 4-1. Editing MyL2TP.txt File

Step 4. Run **setupL2TP.cmd**. The script will modify the system's registry to allow the uses of shared secret and create the MMC IPSec policy, named *My_L2TP*. In addition, a new Network Connection shortcut, **Shortcut to My L2TP**, is created on the desktop.

Figure 4-2. Desktop Shortcut

Step 5. Reboot the system.

Note: *Without rebooting, any attempt to make the L2TP connection will fail.*

Step 6. Double-click the **Shortcut to My L2TP** icon. The My L2TP connection window appears.

Step 7. Enter the User name and Password information in the appropriate textboxes. If required, enter the **Logon domain** information in the third text box. You may select the **Save password** and / or **Connect automatically** options by clicking the appropriate checkboxes.

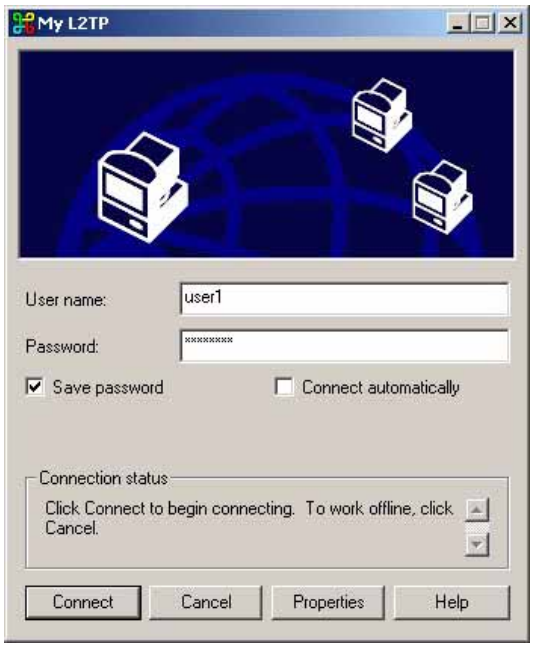

Figure 4-3. My L2TP Connection Window

Step 8. (Optional) Click the **Properties** button to modify the number of **Redial attempts** and the minutes of **Idle time before disconnecting**. After finishing the modification, click **OK**.

Step 9. Click the **Connect** button to make the VPN connection to the HP ProCurve 700wl Series system.

Once the connection is made, you will see a new connection icon appeared in the notification tray (lower-right corner of your desktop). You may click the icon to view the connection status.

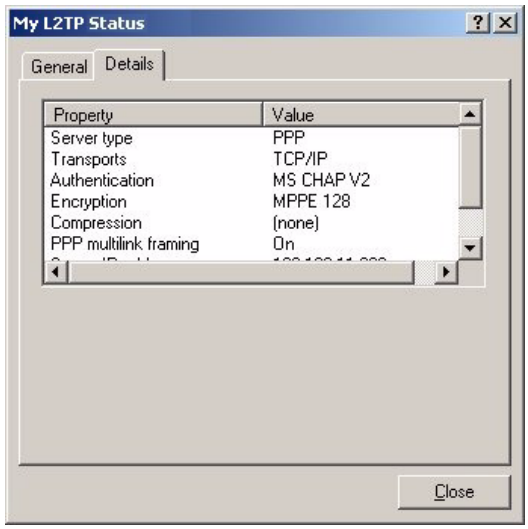

Figure 4-4. My L2TP Status Window, General Tab

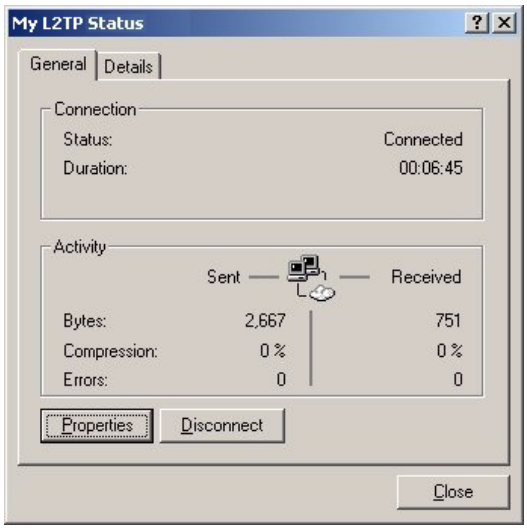

Figure 4-5. My L2TP Status Window, Details Tab

Setting Up Windows XP

Do the following to install and configure a new L2TP/IPSec connection on Windows XP.

Step 1. Download the supplied ZIP package, **WIN2K_SETUP.zip**, from the 700wl Series system. This ZIP package is also available on the documentation CD.

Step 2. Extract the ZIP package to a directory, then go to the **winxp** subdirectory.

Step 3. Run **setupl2tp_XP.cmd**.

Step 4. You will be prompted to enter the PIN for pre-shared key. Enter the PIN and then click **OK**. See details in "How to Rebuild a CMAK Package" on how to rebuild the CMAK package which includes the information on how to setup the PIN and the pre-shared key.

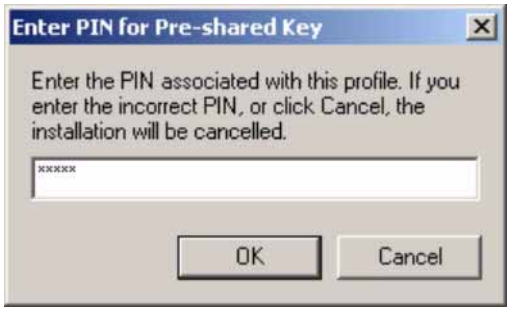

Figure 4-6. PIN Entry Dialog

Step 5. A new Network Connection shortcut, **Shortcut to My L2TP**, is created on the desktop.

Figure 4-7. Desktop Shortcut

Step 6. Double-click the **Shortcut to My L2TP** icon. The My L2TP connection window appears.

Step 7. Enter the User name and Password information in the appropriate textboxes. You may select the **Save password** and / or **Connect automatically** options by clicking the appropriate checkboxes.

Figure 4-8. Sign-on Window

Step 8. (Optional) Click the **Properties** button to modify the number of **Redial attempts** and the minutes of **Idle time before disconnecting.** The Advanced tab is used to enable packet filtering for this connection. Click **OK** to save the settings.

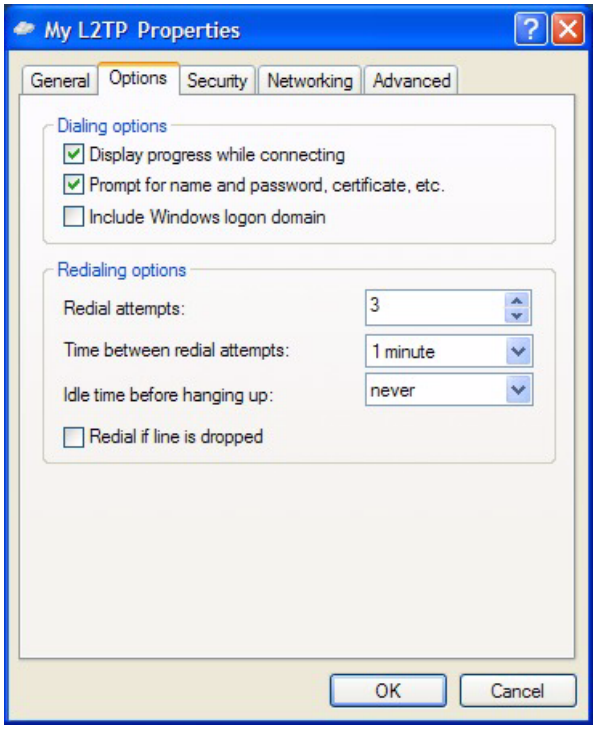

Figure 4-9. My L2TP Properties Window, Options Tab

Step 9. Click the **Connect** button to make the VPN connection to the HP ProCurve 700wl Series system.

Step 10. Once the connection is made, you will see a new connection icon appeared in the notification tray (lower-right corner of your desktop). You may click the icon to view the connection status.

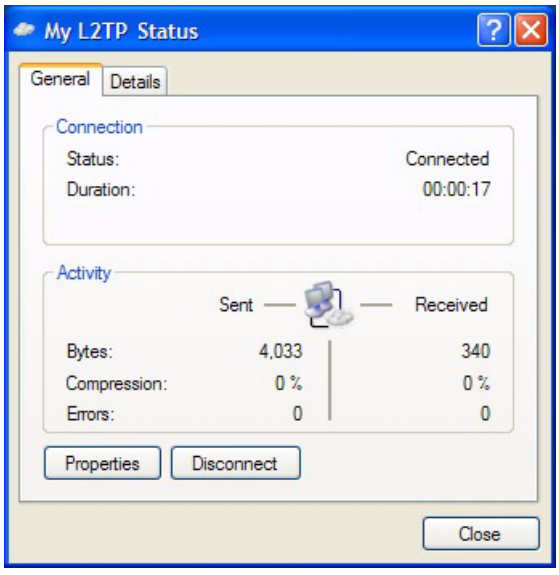

Figure 4-10. My L2TP Status Window, General Tab

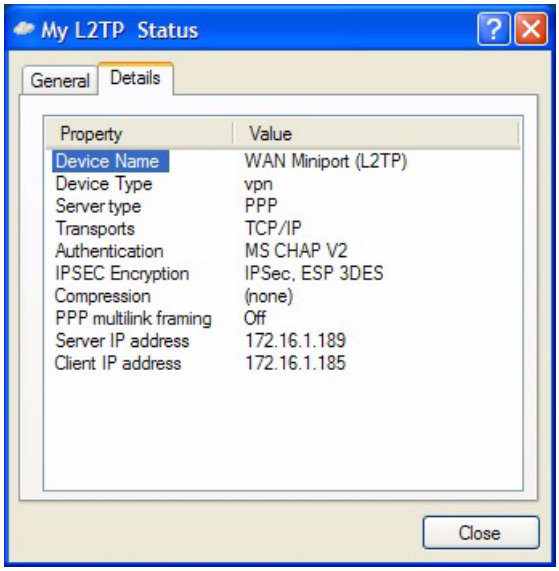

Figure 4-11. My L2TP Status Window, Details Tab

Note: *Both PIN and IPSec shared secret are embedded into the CMAK package. The only method to change either PIN or IPSec shared secret is to rebuild the CMAK package.*

See "How to Rebuild a CMAK Package" for instructions on how to rebuild a CMAK package.

How to Rebuild a CMAK Package

Step 1. Start the CMAK Wizard

Start → **Run...** → Enter "cmak" in the **Open** text box → **OK**

The Welcome screen of the CMAK Wizard appears. Click **Next>**.

Figure 4-12. Connection Manager Administration Kit Wizard

Step 2. The Service Profile Selection screen appears. Make sure that **New profile** is selected and then click **Next>**.

Step 3. The Service and File Names screen appears. Enter the Service name and File name in the appropriate textboxes. Click **Next>**.

Step 4. The Realm Name screen appears. Make sure that **Do not add a realm name to the user name** is selected. Click **Next>**.

Step 5. The Merging Profile Information screen appears. Click **Next>**.

Step 6. Select **Phone book from this profile**. Enter `42.0.0.1` in the **Always use the same VPN server** text box and then check **Use the same user name and password for VPN and dial-up connections**. Click **Next>**.

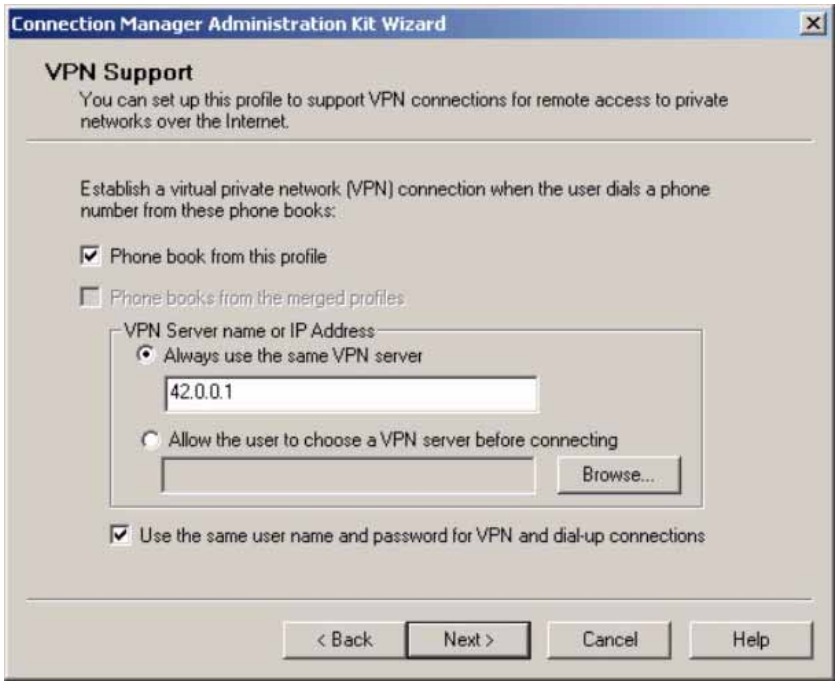

Figure 4-13. VPN Support Screen

Step 7. The VPN Entries screen appears. Select the entry you just created (named after the Service name specify in Step 3) and then click **Edit**.

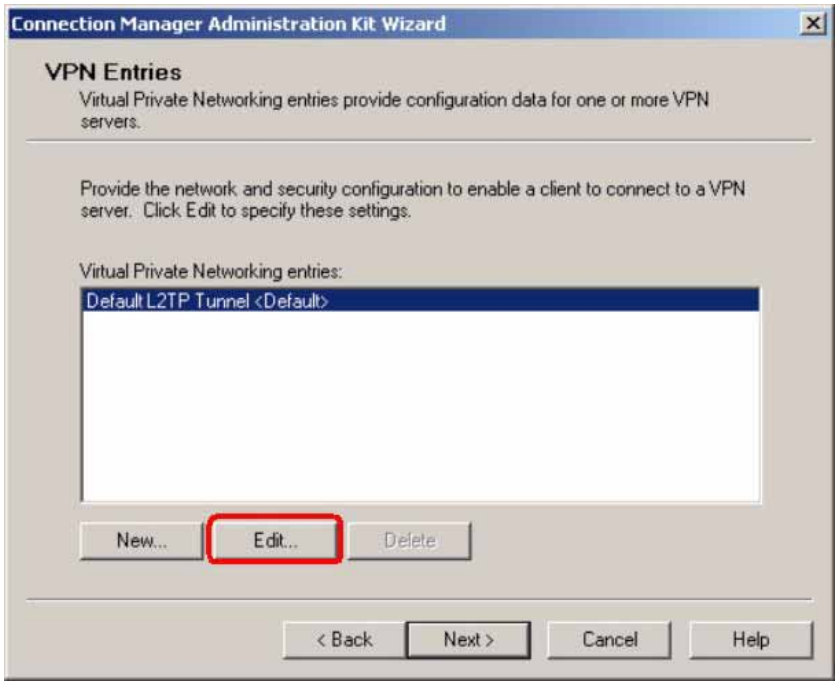

Figure 4-14. VPN Entries Screen

Step 8. The Edit Virtual Private Networking Entry window appears. Click the Security tab and then click the **Configure...** button.

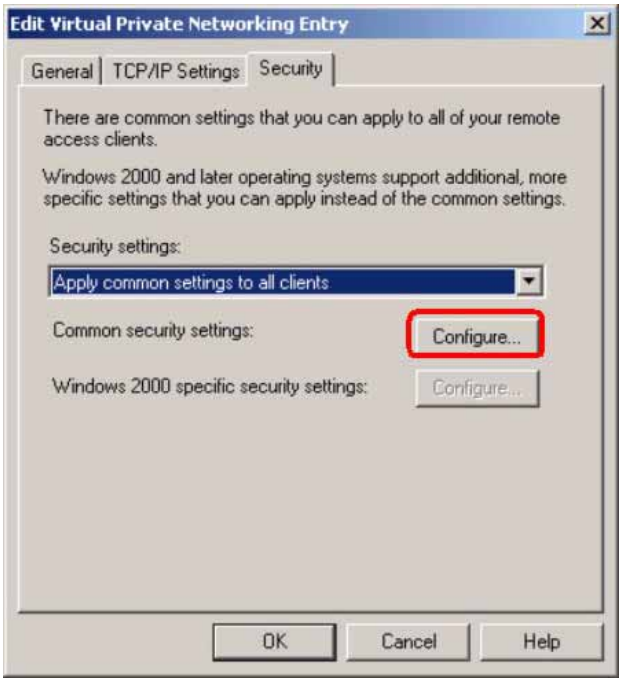

Figure 4-15. Edit Virtual Private Networking Entry Window

Step 9. The Security Settings window appears. Select **Use L2TP/IPSec if available** and then select the **Use a pre-shared key when using L2TP/IPSec** option. Click **OK**.

Figure 4-16. Security Settings Window

Step 10. Click **OK** to return to the VPN Entries screen. Click **Next>**.

Step 11. The Pre-shared Key screen appears. Enter your shared secret in the **Enter key** field and then enter the PIN and the confirmation in the appropriate textboxes. Note that you must enter a PIN; otherwise, the system does not use a shared secret. Click **Next>**.

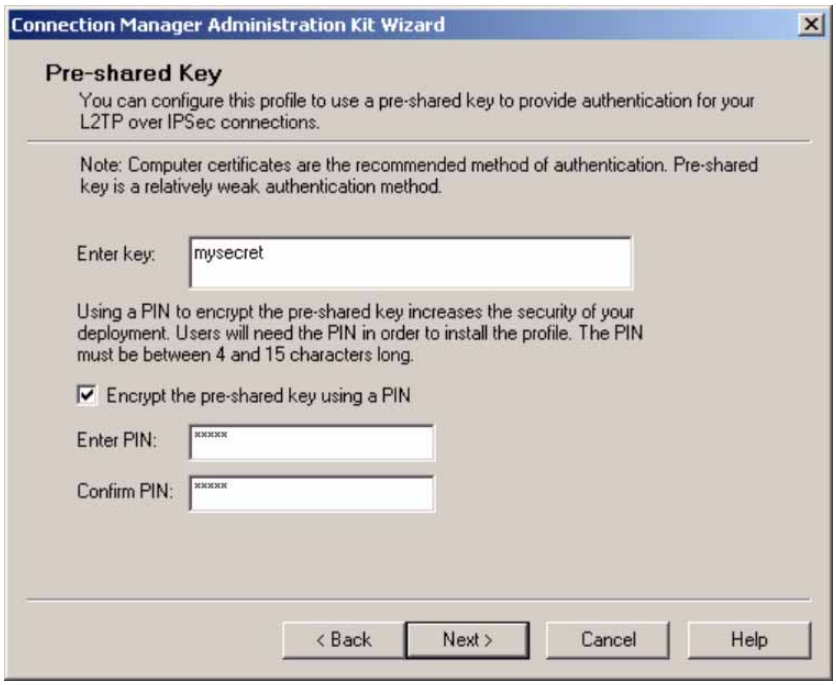

Figure 4-17. Pre-Shared Key Screen

Step 12. The Phone Book screen appears. Make sure that the **Automatically download phone book updates** option is *cleared*. Click **Next>**.

Step 13. The Dial-up Networking Entries screen appears. Select the entry, which is named after the Service name defined in Step 3 and then click **Next>**.

Step 14. The Routing Table Update screen appears. Click **Next>**.

Step 15. The Automatic Proxy Configuration screen appears. Click **Next>**.

Note: *Note that if the Proxy support is required, you must create a PAC file, which contains the proxy information. However, this is beyond the scopes of this document. The detailed information is not provided.*

Step 16. The Custom Actions screen appears. Click **Next>**.

Step 17. The Logon Bitmap screen appears. Click **Next>**.

Step 18. The Phone Book Bitmap screen appears. Click **Next>**.

Step 19. The Icons screen appears. Click **Next>**.

Step 20. The **Notification Area Shortcut** Menu screen appears. Click **Next>**.

Step 21. The Help File screen appears. Click **Next>**.

Step 22. The Support Information screen appears. Click **Next>**.

Step 23. The Connection Manager Software screen appears. Click **Next>**.

Step 24. The License Agreement screen appears. Click **Next>**.

Step 25. The Additional Files screen appears. Click **Next>**.

Step 26. The Ready to Build the Service Profile screen appears. Select **Advanced customization**. Click **Next>**.

Step 27. The Advanced Customization screen appears.

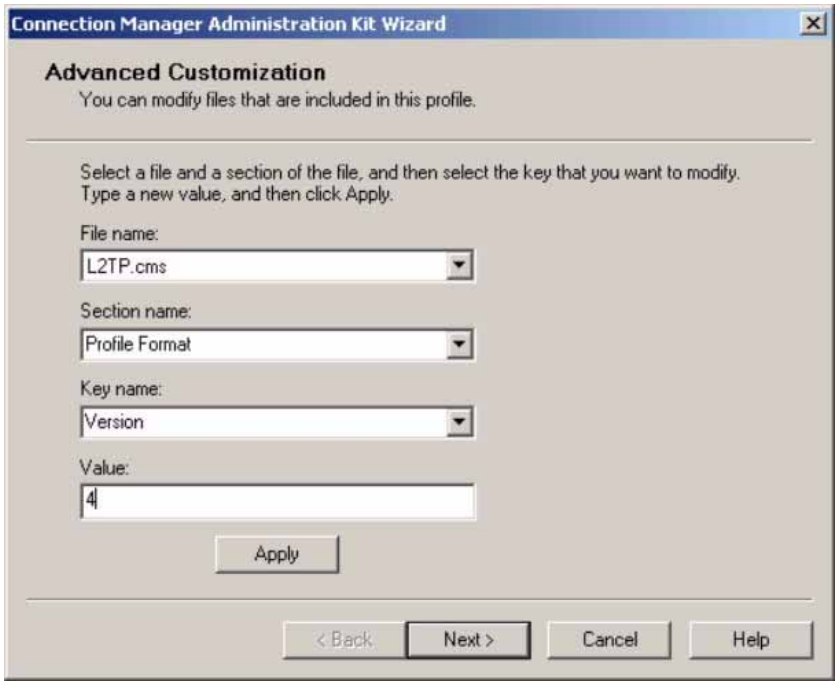

Figure 4-18. Advanced Customization Screen

Make the following modifications (click **Apply** after each change):

a. Select **Connection Manager** from the **Section name** menu. Select **Dialup** from the **Key name** menu. Enter `0` in the **Value** field. Click **Apply**.

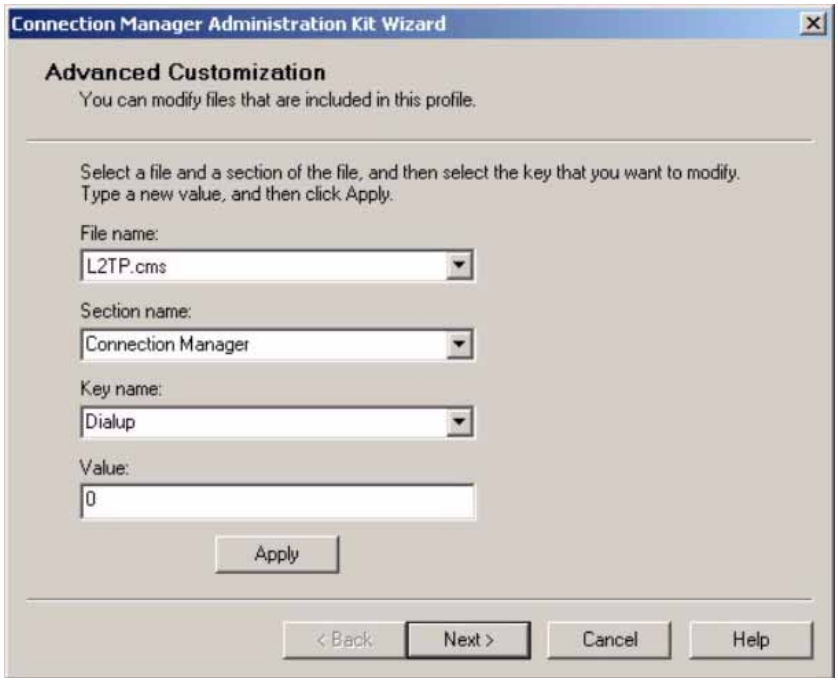

Figure 4-19. Advanced Customization Screen

b. Select **Networking&Default L2TP Tunnel** from the **Section name** menu. Select **VpnStrategy** from the **Key name** menu. Enter 3 in the **Value** field. Click **Apply** and then click **Next>**.

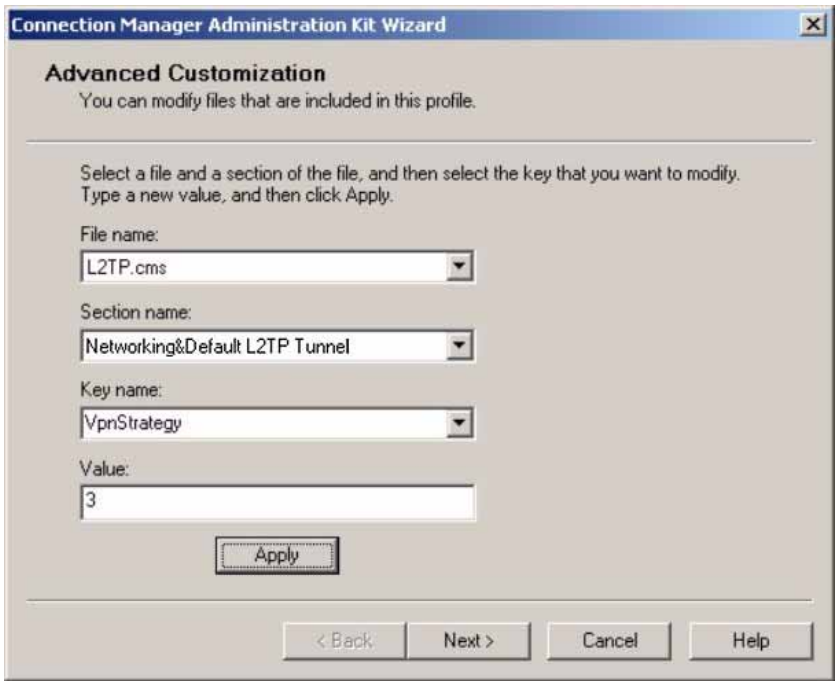

Figure 4-20. Advanced Customization Screen

This will build your files.

Figure 4-21. Connection Manager Administration Kit Wizard, Completion Window

Step 28. Click Finish.

You are now ready to install this connection on a client device. Copy the output files, e.g., **L2TP.exe** and **L2TP.inf** files from **C:\Program Files\CMAK\Profile\L2TP** to any target directory.

To install, use the following command:

```
l2tp /q:a /c:“cmstp.exe l2tp.inf /u /s”
l2tp /q:a /c:“cmstp.exe l2tp.inf /s”
```

The first line will uninstall this connection if it exists and the second line will install the connection.

REFERENCES

1. Microsoft On-line documents, http://www.microsoft.com/ntserver/commserv/deployment/moreinfo/pptpfaq.asp
2. B. Schneier and Mudge, “Cryptanalysis of Microsoft’s Point-to-Point Tunneling Protocol (PPTP)” http://www.counterpane.com/pptp.pdf
3. B. Schneier, D. Wagner, and Mudge, “Cryptanalysis of Microsoft’s PPTP Authentication Extensions (MS-CHAP v2)” http://www.counterpane.com/pptpv2.pdf
4. S. Kent and R. Atkinson, “Security Architecture for the Internet Protocol”, RFC 2401, November 1998
5. S. Kent and R. Atkinson, “IP Authentication Header”, RFC 2402, November 1998
6. S. Kent and R. Atkinson, “IP Encapsulating Security Payload (ESP)”, RFC 2406, November 1998
7. R. Thayer, N. Doraswamy, and R. Glenn, “IP Security Document Roadmap”, RFC 2411, November 1998
8. B. Patel, B. Aboba, W. Dixon, G. Zorn, and S. Booth, “Securing L2TP using IPsec”, RFC 3193, November 2001
9. “HP ProCurve 700wl Series Management and Configuration Guide” v 3.1
10. *Michael Moy* created the scripts and compiled them in ZIP packages.

INDEX

S

W

Edition 1, July 2003

Manual Part Number
5990-5989