

---

The logo for eSoft, consisting of the word "eSoft" in white serif font on a blue square background, with a registered trademark symbol (®) to the right.

---

# InstaGate PPTP VPN



Configuration of PPTP Server and Clients

## COPYRIGHT NOTICES

©eSoft Inc. 2008. eSoft, InstaGate, and ThreatWall are registered trademarks, and SoftPak and SoftPak Director are trademarks of eSoft, Inc. Microsoft and Windows are registered trademarks of Microsoft Corporation. Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corporation. Adobe, the Adobe logo, and Acrobat are registered trademarks of Adobe Systems Inc. UNIX is a registered trademark of UNIX Systems Laboratories, Inc. All other brand and/or product names are the property of their respective holders.

Portions of this software are covered under the GNU General Public License. You may freely obtain source code versions of the software covered by the GNU General Public License through the Internet at <http://www.redhat.com>. However, some applications remain the property of their owners, and require their permission to redistribute. For more information, access the eSoft web site at <http://www.esoft.com>.

Portions of this software are Copyright © The Regents of the University of California. A complete copy of the copyright notice follows:

Copyright © The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistribution of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistribution in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

All advertising materials mentioning features or use of this software must display the following acknowledgment:

“This product includes software developed by the University of California, Berkeley and its contributors.”

Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions of this software are Copyright © The Apache Group. A complete copy of the copyright notice follows:

Copyright © 1995-1997 The Apache Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

All advertising materials mentioning features or use of this software must display the following acknowledgment:

“This product includes software developed by the Apache Group for use in the Apache HTTP server project (<http://www.apache.org/>).”

The names “Apache Server” and “Apache Group” must not be used to endorse or promote products derived from this software without prior written permission.

Redistributions of any form whatsoever must retain the following acknowledgment:

“This product includes software developed by the Apache Group for use in the Apache HTTP server project (<http://www.apache.org/>).”

## INTRODUCTION

PPTP (*Point-to-Point Tunneling Protocol*) VPN connections allow remote users to securely connect to an InstaGate firewall by creating an encrypted ‘tunnel’ over the Internet. This allows access to resources on the local area network (LAN) as if the user were directly connected to the network. PPTP client applications are built into most major operating systems, offering the simplest method for deploying secure remote connections to an office network.

InstaGate firewalls use PPP (*Point-to-Point Protocol*) and MS-CHAPv2 (*Microsoft Challenge-handshake Authentication Protocol*) to establish and authenticate PPTP VPN client connections. The following document will detail how to setup the InstaGate to accept these connections, and how to configure PPTP clients on computers using Windows operating systems. Configuration on Windows 98 SP2 through Windows Vista is nearly identical. Earlier versions of Windows may need to obtain a separate PPTP client application.

## PART ONE – INSTAGATE CONFIGURATION

### 1.1 Access the PPTP VPN Menu

The PPTP VPN settings are available in the InstaGate user interface under the Firewall menu. Select the menu option for PPTP VPN here. The option ‘Server’ is used to configure the InstaGate unit to accept PPTP connections directly. If you have an internal PPTP VPN solution, you may also select ‘Passthrough to Internal Server’ and specify that server’s local IP address to pass PPTP traffic to the internal device.

### 1.2 PPTP VPN Server Settings – IP Address Pool

With the ‘Server’ option selected, you will be presented with a Server Settings prompt, asking for the IP address range to use. Generally you will specify a range of IP addresses from the same subnet as your LAN. The range of IP addresses assigned to clients will extend inclusively from the First IP Address to the Last IP Address. Note that this range of IP addresses also determines how many PPTP clients are able to connect at one time – specifying a range of 5 IP addresses would allow only 5 PPTP connections, since there would be no further addresses to assign to new clients.

### 1.3 PPTP VPN Server Settings – Require Strong Encryption

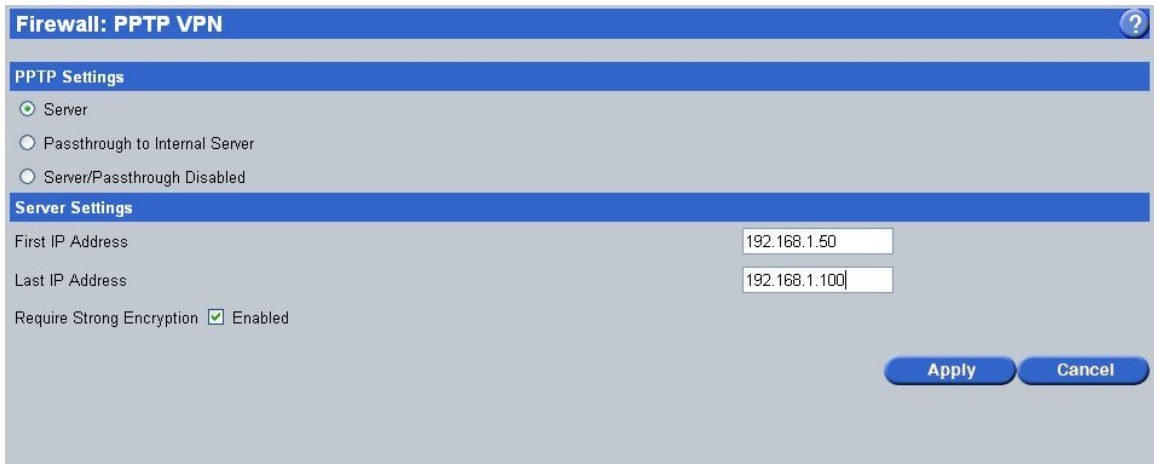
---

The option ‘Require Strong Encryption’ determines the cipher strength (the level of encryption) required for clients to establish a PPTP connection. If this option is enabled, the InstaGate will require 128-bit encryption on the PPTP tunnel. For best security, we recommend enabling this option unless you have PPTP clients that cannot support 128-bit encryption. When this option is disabled, both 128-bit and 40-bit encrypted tunnels will be accepted, allowing for compatibility with older PPTP clients. The InstaGate will always try to negotiate the most secure connection when possible.

### 1.4 Final Configuration

---

The screenshot below shows our final InstaGate configuration.



The screenshot displays the configuration interface for the Firewall: PPTP VPN. It is divided into two main sections: PPTP Settings and Server Settings. In the PPTP Settings section, the 'Server' option is selected with a radio button. The Server Settings section includes two text input fields: 'First IP Address' with the value '192.168.1.50' and 'Last IP Address' with the value '192.168.1.100'. Below these fields, the 'Require Strong Encryption' checkbox is checked and labeled 'Enabled'. At the bottom right of the configuration area, there are two buttons: 'Apply' and 'Cancel'.

## PART TWO – MICROSOFT WINDOWS PPTP CLIENT CONFIGURATION

### 2.1 Windows PPTP VPN Client

---

Microsoft Windows has included native support for PPTP VPN connections beginning with Windows 98, as part of the Dialup Networking protocol and driver suite. Configuration of the client has changed very little since its inception, so we will be using Windows XP as an example for configuring PPTP VPN connections in this document. Previous and more recent versions of Windows will be basically identical. Users of Windows versions older than Windows 98 may need to obtain a third-party PPTP VPN client.

### 2.2 Create a New Connection

---

The easiest method for creating a PPTP VPN connection is by using the ‘New Connection Wizard’. Select the Start Menu, and browse to Control Panel. Within Control Panel, select Network Connections. In the Network Connections menu, select ‘File’ in the toolbar, and browse down to ‘New Connection...’ This will spawn the New Connection Wizard.



Select the ‘Next’ button to continue.

## 2.3 Create a New PPTP VPN Connection

---

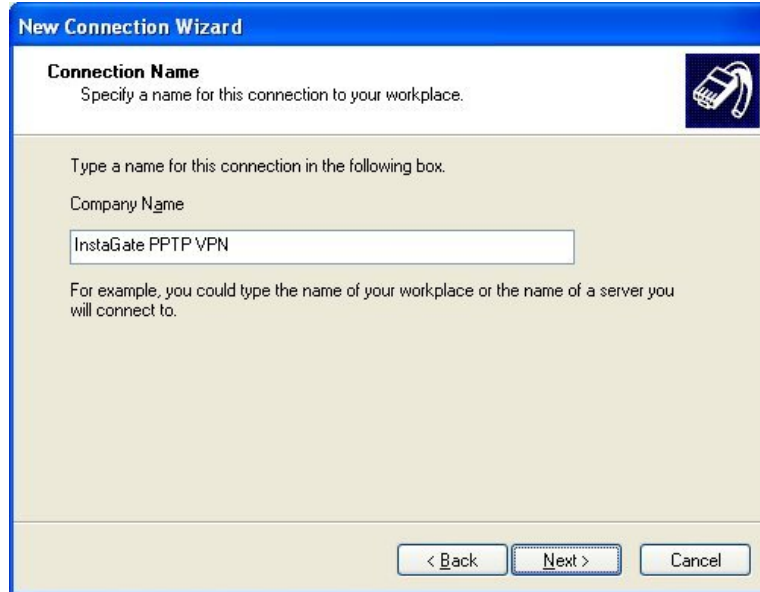
The next page of the wizard will present you with several choices. To create a PPTP VPN Connection, you should select 'Connect to the network at my workplace'.



On the following page, select 'Virtual Private Network Connection' as the connection type, and select Next.

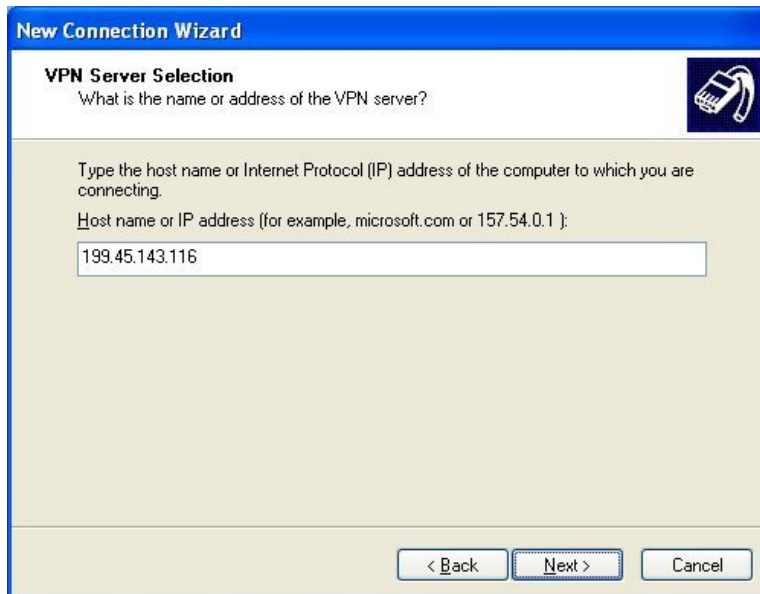


The name you provide for the VPN connection can be anything you wish, but we recommend setting this to something memorable, especially in the case when you have multiple PPTP VPN connections.



The screenshot shows a Windows-style dialog box titled "New Connection Wizard". The main heading is "Connection Name" with a sub-instruction: "Specify a name for this connection to your workplace." Below this, there is a text input field containing "InstaGate PPTP VPN". The dialog also includes a "Company Name" label above the input field and a small icon of a mobile phone in the top right corner. At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

On the following screen, enter the Public IP Address (WAN IP) of your InstaGate. You may also use a FQDN (fully qualified domain name) which resolves to the IP address of your InstaGate if available.



The screenshot shows the next step in the "New Connection Wizard" dialog box, titled "VPN Server Selection". The instruction reads: "What is the name or address of the VPN server?". Below this, there is a text input field containing the IP address "199.45.143.116". The dialog also includes a small icon of a mobile phone in the top right corner and a label "Host name or IP address (for example, microsoft.com or 157.54.0.1 ):" above the input field. At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

To finalize the settings and create your PPTP VPN Connection, simply select 'Finish'. You may also create a shortcut to this VPN connection on your desktop if you wish.



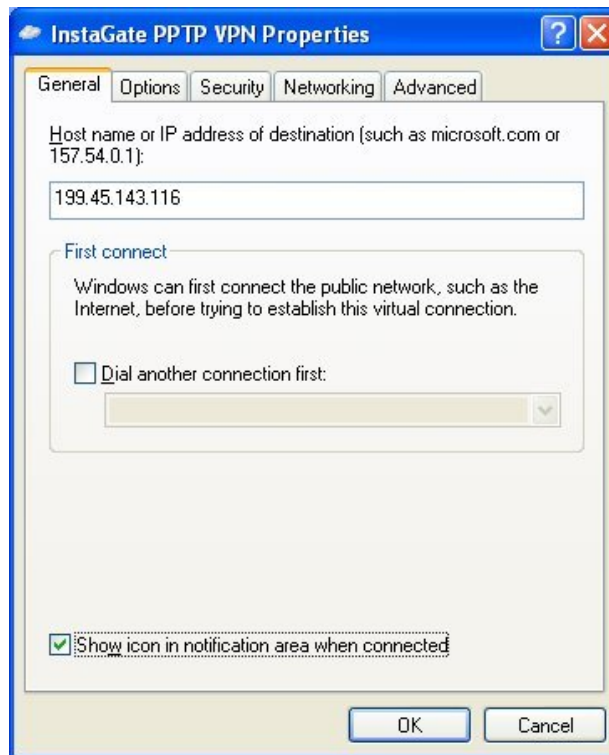
At this point you should have a functional PPTP VPN connection. When you open your newly created connection, you will be prompted for a username and password. The credentials you use here must match a user account configured to allow Remote Access on your InstaGate product.



## PART THREE: ADVANCED PPTP CONFIGURATION

The default configuration provided when you create a new PPTP VPN connection should work in most circumstances. Both the Windows client and your InstaGate will default to the most secure connection available, so you generally do not need to change advanced settings. Any advanced settings not covered in this document should be left at their default configuration to ensure a reliable connection. The following screenshots are a reference guide, if you must change these settings for your particular configuration.

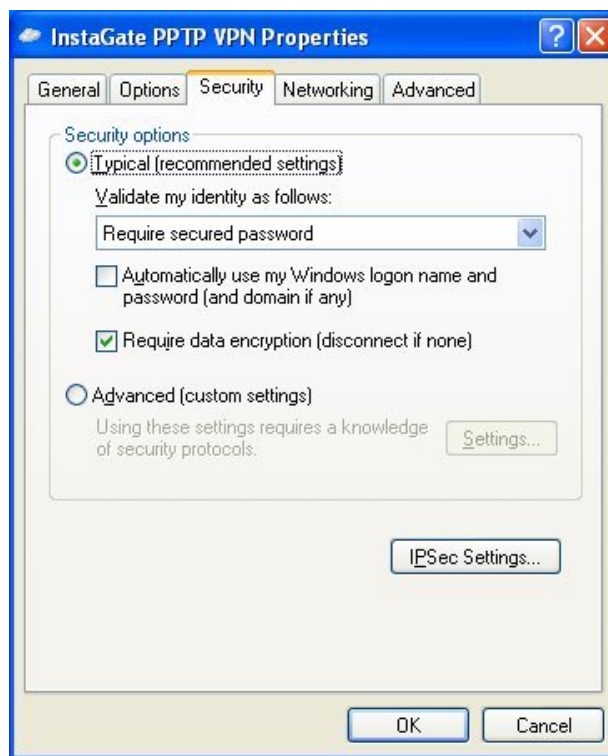
To access the advanced settings for the connection, go to the Start Menu, select Control Panel, and browse to Network Connections. Here you should find the icon for the PPTP VPN Connection you created. Right-Click this icon and select 'Properties', and you will be presented with the following screen:



- If you use a transitory Internet connection (for example, dialup or PPPoE), check 'Dial another connection first' and select it from the dropdown list.
- The Hostname or IP address shown here should match the IP address of your InstaGate. You may also use a domain name that resolves your InstaGate's IP address if available.

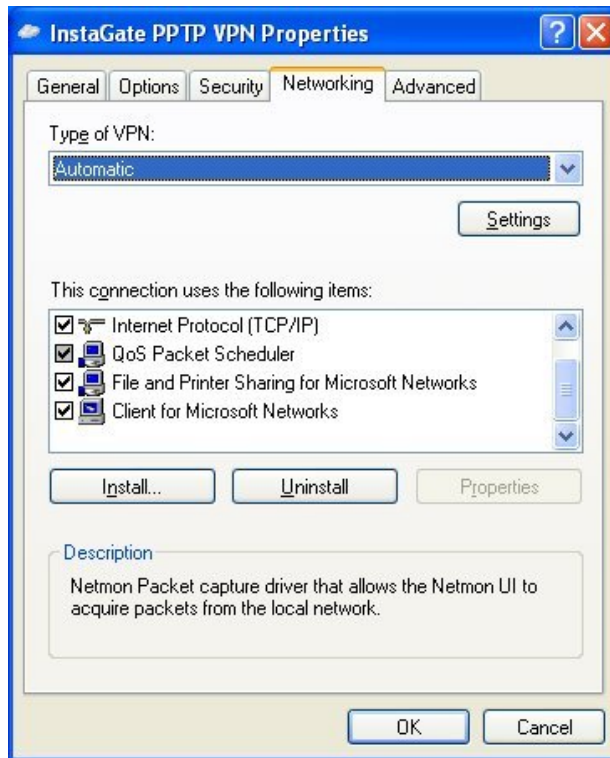
The Options tab of the Properties window contains personal preference options for your PPTP VPN connection, which do not affect your connection, and will not be covered in this document. You may change settings such as automatic 'redialing' on the Options tab.

The following screenshot outlines the recommended Security properties for InstaGate PPTP VPN connections. Using the settings shown below ensures the most secure connection to your InstaGate, and altering them may cause you to be unable to establish a connection.



- Require Secured Password is necessary for InstaGate VPN connections – the InstaGate will not allow you to authenticate using a 'plain-text' password.
- Selecting the 'Require data encryption' option will ensure the best available encryption method is used. This setting is not usually necessary, as the client and InstaGate will always try to negotiate the most secure connection.

The Networking tab provides advanced options to configure how your data is handled after establishing a PPTP VPN connection. You can specify what protocols are allowed to pass over your VPN tunnel, such as File and Print Sharing to access file shares or print documents in your office.



- Type of VPN should always be set to either Automatic or PPTP VPN. InstaGate firewalls do not currently support L2TP (certificate based) VPN connections.
- Internet Protocol (TCP/IP) must be selected in order to transmit and receive data over your VPN tunnel. Advanced properties for this option will be covered below.
- To access computers and printers on the remote network, you will need to have at least Client for Microsoft Networks enabled. Depending on your configuration, File and Printer Sharing is not necessary unless computers on the remote network need to access your client computer.

Highlight the option 'Internet Protocol (TCP/IP)' and select Properties to see advanced TCP/IP options for your VPN connection.



- You should not specify an IP address in this window. Your InstaGate will be configured to provide an IP address to the connecting client, and specifying one here may cause the connection to fail.
- You may specify an alternate DNS server or servers if required, however it is recommended you allow the InstaGate to provide DNS settings dynamically for your PPTP VPN connection.
- Select 'Advanced' here to see more options.

The Advanced TCP/IP settings allow you to specify specific DNS and WINS servers on your network if necessary. This will allow you to access servers and computers on your remote connection by domain or host name rather than IP address, assuming a properly configured WINS / DNS server exists on the remote network.



- Setting the 'Use default gateway' option will force all of your network traffic through your VPN connection, including browsing and e-mail. We recommend disabling this option over slower or busy Internet connections

## TROUBLESHOOTING

Generally PPTP connections are used to provide a simple, easy to deploy method for establishing a secure tunnel. InstaGate PPTP connections will usually work with no modifications to the default settings of the Windows PPTP client. In some situations, especially when the PPTP client is modified frequently, the connection may suddenly fail. In this case, the first step should be to remove and recreate the PPTP connection. This will also ensure the proper settings are in place, and give a good basis to begin further troubleshooting.

The following common error codes may give you an insight to the specific problem affecting your client if you are still unable to connect.

<b>Error Code</b>	<b>Common Issues</b>
Error 691	Authentication Failure. This error indicates the username or password supplied was invalid or mistyped. Try retyping the username or password. Check with your InstaGate administrator or Technical Support if you believe you have the proper credentials but still obtain this error.
Error 678 or 718	PPP protocol failure. This error indicates that the remote server is not responding properly to your authentication request.  This error is can be caused by several issues: 1) Your router/firewall is blocking VPN connectivity, contact your router/firewall vendor for help with this problem.  2) The GRE protocol ( protocol 47 ) is not allowed to pass over your Internet connection. It may be blocked by your firewall, or your ISP may not allow this traffic.  3) There are too many active connections, and the InstaGate has run out of IP addresses to assign. Try increasing the IP address range supplied in the PPTP VPN configuration.  If these steps do not resolve the issue, contact your administrator or Technical Support.
Error 800	Connection timeout. This error usually means the remote PPTP server is not responding. This could mean your Internet connection is not active, or that the remote PPTP server has been disabled.

Troubleshooting VPN connectivity problems can often be very complex. If you are unable to connect please open a ticket with eSoft Technical Support at 877-754-2986 or through online support at <http://support.esoft.com>.