InJoy PPTP 4.0

Configuration Guide

Contents

Part I
Introduction to PPTP

1 Introduction

PPTP is a networking technology that supports multiprotocol VPNs. Using PPTP, remote users can employ point-to-point protocol (PPP)-enabled client systems to dial into a local Internet service provider to connect through secure tunnel to their corporate network via the Internet.

For the end user, there are only a few minor changes from the old dial-up environment. Instead of having the connection automatically occur when your computer boots, the connection and authentication will be established using PPTP client software. Due to the extra PPTP protocol layer, the maximum IP packet size has become smaller. The "Maximum Transmission Unit" section is recommended reading.

1.1. Document Scope

Before reading this document you should be familiar with the InJoy Firewall™ and have basic knowledge of the TCP/IP protocol – i.e. know what an IP address is. Additionally, your LAN adapter should be installed and connected to your ISP hookup.

To ease your navigation, this document has been divided into several distinct parts according to the amount of information different types of readers are likely to need:

Part I.	Introduction to PPTP
Part II.	Setting up PPTP
Part III.	References

Part II by itself contains enough information to successfully install and use the PPTP Plugin. Users who want a better understanding of PPTP can consult the remaining parts for additional information.

2 PPTP Overview

This section gives you an overview of PPTP and its capabilities.

2.1. What is PPTP?

PPTP is a tunnelling protocol that allows remote users access corporate network over the Internet. Another common PPTP appliance is connecting to the Internet Service Provider (ISP) through broadband modems.

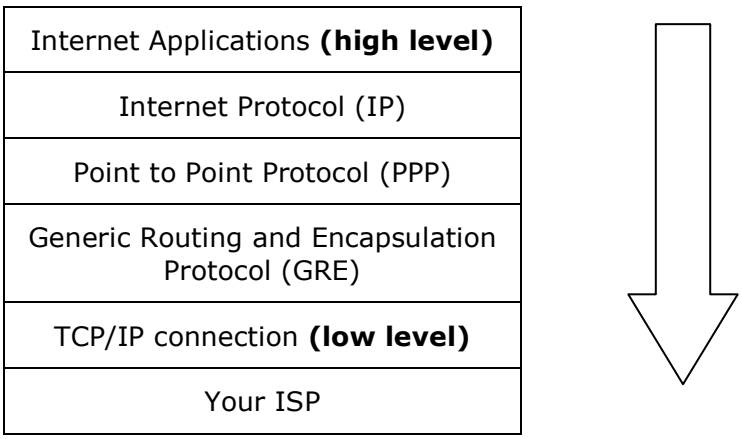
In short, PPTP establishes PPP session and then uses GRE, the Internet Generic Routing and Encapsulation Protocol and encapsulates PPP packets into IP datagrams for transmission over Internet or other TCP/IP based networks. Due to its PPP nature, PPTP itself supports only peer-to-peer connections, thereby disallowing using of multicast and broadcast packets. Another PPTP limitations are its weak security and inability to support more than one tunnel per each user.

PPTP itself was not originally designed to provide LAN-to-LAN tunnelling, but it perfectly handles peer-to-peer or peer-to-LAN connection types. PPTP cannot handle more than one tunnel at a time for each user.

2.2. How PPTP Works

Protocol Stack

PPTP is an encapsulation technique that allows use of the PPP protocol over an existing public TCP/IP connection. After applying PPTP, the layered protocol communications stack looks like this:



PPTP Overview

The PPTP protocol is built upon the widely used protocols of PPP (Point-to-Point Protocol) and TCP/IP.

PPP offers authentication and methods of privacy and compression of data. PPTP allows a PPP session to be tunneled through an existing IP connection, no matter how it was set up. So a VPN are orginized over a public network.

PPTP provides encapsulation by wrapping packets of information (IP, IPX, or NetBEUI) within IP packets for transmission through the Internet such way organizing a tunnel.

Upon receipt, the external IP packets are stripped away, exposing the original packets for delivery. Encapsulation allows the transport of packets that will not otherwise conform to Internet addressing standards.

PPTP uses an enhanced Generic Routing Encapsulation (GRE) protocol in transporting PPP packets.

The PPTP protocol has two basic parts:

- Control Connection
- PPTP Tunnel

The control connection is used for establishment, management, and release of sessions carried through the tunnel.

The control connection is a standard TCP session over which PPTP call control and management information is passed.

PPTP tunnel is used to transfer the data packets which contain the user data that must be sent to or received from the LAN or WAN.

Data packets are PPP packets encapsulated using the Internet Generic Routing Encapsulation Protocol Version 2 (GRE V2).

PPTP Standard

Additional information about the PPTP protocol is available in the following RFCs:

- RFC 1661 “The Point-to-Point Protocol”
- RFC 1662 “PPP in HDLC-like Framing”
- RFC 1701 “Generic Routing Encapsulation (GRE)”
- RFC 2637 “Point-to-Point Tunnelling Protocol (PPTP)”.

2.3. InJoy PPTP Features

This section covers details of the InJoy PPTP implementation.

Installation	• Installed seamlessly as part of the InJoy Firewall™ software. • Similar operation on all supported operating systems. • Plugs into the InJoy Firewall™ as a loadable module, maintaining the Firewall's superior speed and efficiency.
Configuration	• Multiple ISP profiles and an easy to use GUI. • For the experts (and for easy scripting), all configuration attributes are also directly editable in a plain-text file.
Performance	• Allows sustained utilization of all network bandwidth. • Adjustable priority allows user control of CPU utilization.
Connection	• Connect at start-up. • Connect on demand. • Connect manually. • Idle disconnect. • Manual disconnect. • Session timeout disconnect. • Connection loss detection. • Auto re-connect.
Diagnostics	• Message log. • Screen output. • On OS/2, system tools “iptrace” and “ipformat” are fully supported.
Line Sharing	• The gateway (NAT) capability in the InJoy Firewall™ allows for sharing the PPTP connections.
Security	• All the filtering and firewall capabilities of the InJoy Firewall™ are available.
VPN Support	• PPTP is one of the Microsoft standards to build VPN.
Documentation	• Complete with instructions to help both beginners and advanced users.

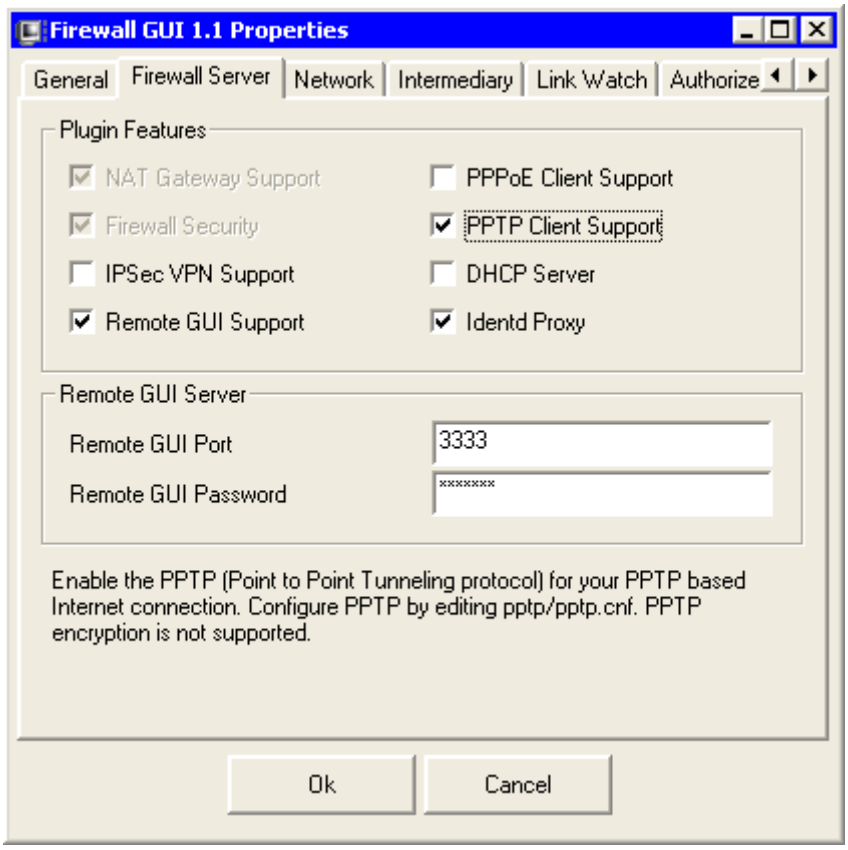
Part II
Setting up PPTP

3 Configuring PPTP

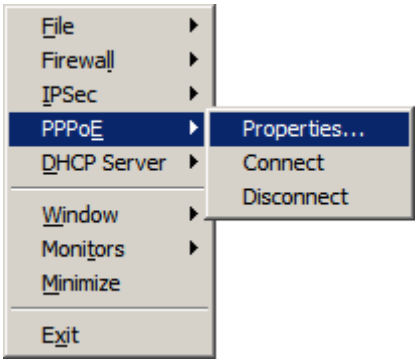
3.1. Enabling PPTP

The PPTP Plugin is seamlessly installed with the InJoy Firewall™ product and can be activated, if supported by the registration key.

To enable the PPTP Plugin, go into the Firewall GUI Properties and enable the "PPTP Client Support" checkbox - as shown below:



Press the **OK** button and restart the InJoy Firewall™ as directed. After restarting the Firewall, the Firewall GUI pop-up menu should include a PPTP submenu, as shown below:



3.2. Configuring PPTP

The PPTP configuration is divided into ISP profiles that can be edited by using a simple plain-text editor (the configuration is stored in PPTP\PPTP.CNF).

4 PPTP Operation

4.1. Managing PPTP Connections

The Connection

PPTP transforms a physical LAN-2-LAN connection into a logical connection scenario.

Once "connected" using a PPTP client, your connection will look the same as your current TCP/IP connection. When you are finished, or when you've been idle for a period of time, the client will typically be disconnected and you will need to reconnect to use the Internet again. InJoy PPTP can monitor the link, and automatically reconnect. It is your choice whether this is immediately, or on demand. In NAT environments, this interruption is transparent.

Connecting

A connection can be triggered manually, automatically or on demand.

Using the Firewall GUI, you can manually trigger a connection by selecting "**PPTP | Connect**" from the RMB (Right Mouse Button) pop-up menu.

Disconnecting

Disconnections can be triggered manually, by timers or by the ISP.

Using the Firewall GUI, you can manually disconnect by selecting "**PPTP | Disconnect**" from the RMB (Right Mouse Button) pop-up menu.

Reconnecting

As previously mentioned in the configuration section, the re-connect flag allows you to determine when, how and if a PPTP connection is to be reconnected at connection loss.

If you wish to maintain a full time PPTP connection, then set the re-connect flag to "auto" and InJoy will automatically reconnect when the connection loss is detected. This makes InJoy the perfect choice for keeping a connection alive 24 hours a day.

Setting the re-connect flag to "demand" allows for automatic reconnects when your TCP/IP applications require Internet connectivity.

Connection details

When a PPTP connection has been successfully established, the file CONNECT.TXT is immediately created. This file includes characteristics about your current connection. The following is an example of the contents of a typical CONNECT.TXT file:

```
194.234.160.52
194.234.160.8
Host.........: Sympatico
Modem connect.: void
Line speed....: unknown
DNS (Primary).: 194.234.160.2
DNS (Backup)..: 194.234.160.3
```

CONNECT.TXT is not a semaphore file, so don't use it to determine if you are connected at any moment.

This file is also found in the InJoy Dialer™ product and the same file format is maintained between products.

4.2. Applying Configuration Changes

At start-up and with each connect attempt, the ISP profiles are automatically scanned for the active profile. Once found, the active profile is read and the new settings are put into action. There is no need to manually re-load the configuration each time it is changed (unlike the IPSec and DHCP Server Plugins).

Part III
References

5 Maximum Transmission Unit

This section provides you with the background information to understand and solve the MTU issues that arise from using the PPTP protocol.

The problems are likely to be of different importance in various organizations and there is no single perfect work-around available. As a general approach, it is recommended that you start out by using the MSS fix described below and only continue to update the MTU on internal machines if it proves absolutely required.

While this section delivers a comprehensive introduction to the possible MTU issues, a complete description of the MTU is beyond the scope of this document. Please check back for more deployment examples in the future.

5.1. Solving the PPTP MTU Implications

Understanding the PPTP MTU Problem

Typically, packets on your network have a maximum size of 1500 bytes, which is the default MTU (Maximum Transmission Unit) on Ethernet.

Packets of 1500 bytes are larger than the maximum possible PPTP packet size and therefore it is typically recommended that all machines which send data over the PPTP connection MUST have their MTU set to a smaller value (for example 1492 bytes, which is 1500 bytes less the 8 bytes PPTP header).

On a larger network with many different OS platforms, it can however be a resource demanding task to change the MTU on all internal PCs. Adding to this complexity are other protocols, such as IPSec, which also enlarges IP packets.

The TCP/IP protocol includes its own technology to allow big packets to traverse smaller pipes. This technology is known as packet fragmentation and it is supported by the InJoy Firewall™.

Packet fragmentation splits up big packets into several small packet fragments and once the fragments arrive at their final destination, they are defragmented into a complete packet. The packet fragmentation can somewhat solve the PPTP MTU problem, however, it introduces an extra hit on performance and even worse, certain applications require packets to reach their destination without the use of fragmentation.

Identifying MTU problems

MTU problems are quite distinct and easy to detect.

If you have an MTU misconfiguration, you will experience problems especially when you download large web pages or e-mails. Very small e-mails and certain web pages may download just fine, while others just seem to stall.

Maximum Segment Size (MSS) - A Quick Fix

The Maximum Segment Size is the maximum portion of data (in a single IP packet) that can pass over a TCP connection. By default, the MSS is automatically set by the TCP/IP stack, based on the interface MTU. For example, if the MTU is 1500 bytes, the MSS is typically 1460 bytes – calculated as 1500 minus the 40 bytes used by the TCP/IP headers.

The InJoy Firewall™ has a feature to automatically change the MSS value for every new TCP connection, thereby tricking the opposite end of the connection to send smaller packets. In practice, this effectively solves the MTU problems for all TCP connections (but not for UDP, ICMP and other protocols).

When using PPTP, it is recommended that you start by setting the MSS-Adjust value in the InJoy Firewall™, "**File | Properties | Intermediary**" to a low value – for example in the range 1000-1200 (1200 is the default and it should be okay).

You can read more about the MSS-Adjust feature in the InJoy Firewall™ "Getting Started" documentation.

5.2. Setting the MTU Value

On different Operating Systems, different ways exist to edit the MTU values of network interfaces.

It is often a complicated procedure to adjust the MTU values and whenever possible, it is recommended that you use the MSS-Adjust feature to solve the PPTP inflicted MTU problems.

If you however find that you must update the MTU values to ensure proper operation, you will find the procedure to edit the MTU on OS/2, eComStation, Windows 2000/XP and RedHat Linux 7.2+ below:

Setting the MTU on OS/2 and eComStation

There are several ways to change to the MTU in OS/2, but they all evaluate to a simple parameter to the ifconfig statements in:

\MPTN\BIN\SETUP.CMD

Example:

```
route -fh
arp -f
ifconfig lo 127.0.0.1 mtu 1492
ifconfig lan0 192.168.1.1 netmask 255.255.255.0 mtu 1492
...
```

TCP/IP 4.1 has been known to ignore MTU values at the end of ifconfig lines. The solution is to set the MTU on separate lines.

Example:

```
route -fh
arp -f
ifconfig lo 127.0.0.1
ifconfig lo mtu 1492
ifconfig lan0 192.168.1.1 netmask 255.255.255.0
ifconfig lan0 mtu 1492
...
```

Reboot the OS/2 Machine.

Setting the MTU on Windows 2000/XP

Changing the MTU in Windows requires use of the registry editor.

START > RUN > type **regedit** and press Enter.

Export your current registry to back it up into a temporary directory.

Then add these registry keys in the following sections (if they are not there already). If they are already present, then modify them to these values:

```
HKEY_LOCAL_MACHINE
\SYSTEM\CurrentControlSet\Services\<Adapter Name>\Parameters\Tcpip
MTU="1492"
```

(Make sure MTU is a DWORD VAR and NOT a STRING)

Windows 2000/XP has a registry setting at the TCP/IP level that tells TCP/IP to ignore explicit NIC MTU values and instead rely on detection of the maximum packet size. The settings that turn this on are presented below:

```
HKEY_LOCAL_MACHINE\
SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
"TcpWindowSize"="63990" (DWORD VAR)
DefaultTTL="128" (DWORD VAR)
EnablePMTUDiscovery="1" (DWORD VAR)
EnablePMTUBHDetect="0" (DWORD VAR)
```

Setting the MTU on Windows 98

Changing the MTU in Windows requires use of the registry editor.

START > RUN > type **regedit** and hit Enter.

Export your current registry to back it up into a temporary directory.

Then add these registry keys in the following sections (if they are not there already). If they are already present, then modify them to the new values.

The following keys should be set for your Ethernet adapter. When you go to the registry and look through the 000n folders in Nettrans (as shown below) you will know you found the right folder when you find the IP address of the Win95 client. In that 000n device folder add this:

```
HKEY_LOCAL_MACHINE\
System\CurrentControlSet\Services\Class\NetTrans\000n

MaxMTU="1492" (STRING VAR)
```

The following keys are also recommended, but only the PMTUDiscovery is mandatory for the PPTP operation.

```
DefaultRcvWindow="362610" (FOR WIN98 USERS ONLY, STRING VAR)
DefaultTTL="128" (STRING VAR)
PMTUDiscovery="0" (DWORD)
PMTUBlackHoleDetect="0" (DWORD )
```

Reboot the Win98 Machine.

Setting the MTU on Windows 95

Changing the MTU in Windows requires use of the registry editor.

START > RUN > type **regedit** and hit Enter.

Export your current registry to back it up into a temporary directory.

Then add these registry keys in the following sections (if they are not there already). If they are already present, then modify them to the new values.

The following keys should be set for your Ethernet adapter. When you go to the registry and look through the 000n folders in Nettrans (as shown below) you will know you found the right folder when you find the IP address of the Win95 client. In that 000n device folder add this:

```
HKEY_LOCAL_MACHINE\
System\CurrentControlSet\Services\Class\NetTrans\000n

MaxMTU="1492" (STRING VAR)

HKEY_LOCAL_MACHINE\
System\CurrentControlSet\Services\VxD\MSTCP

DefaultRcvWindow="63990" (STRING VAR)
DefaultTTL="128" (STRING VAR)
PMTUDiscovery="0" (DWORD VAR),
PMTUBlackHoleDetect="0" (DWORD VAR)
```

Reboot the Win95 Machine.

Setting the MTU on Windows NT

Changing the MTU in Windows requires use of the registry editor.

START > RUN > type **regedit** and hit Enter.

Export your current registry to back it up into a temporary directory.

Then add these registry keys in the following sections (if they are not there already). If they are already present, then modify them to these values:

```
HKEY_LOCAL_MACHINE
\SYSTEM\CurrentControlSet\Services\<Adapter Name>\Parameters\Tcpip

MTU="1492" (Make sure it's a DWORD VAR and NOT a STRING)
```

Now add:

```
HKEY_LOCAL_MACHINE\
SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

DefaultTTL="128" (DWORD VAR)
EnablePMTUDiscovery="0" (DWORD VAR)
EnablePMTUBHDetect="0" (DWORD VAR)
```

Reboot the NT Machine.

Setting the MTU on Linux Red Hat 7.2+

On Linux systems there are few ways to change the MTU, but the most widely used is to set it at start-up. This can be achieved by editing the file **/etc/sysconfig/network-scripts/ifcfg-XXXX**, where XXXX is interface name.

The setting that controls the MTU size is called "MTU" and it is represented in bytes. An example of valid **ifcfg-fx0** file is below:

```
DEVICE=fx0
ONBOOT=yes
MTU=1492
```

Another way to change the MTU value on-the-fly is to issue the following command:

```
ifconfig XXXX mtu 1492
```

Where XXXX is the interface name (e.g. fx0).

6 Configuration Files

The PPTP Plugin uses the following configuration files:

- PPTP/PPTP.CNF – ISP profiles and their parameters
- TEMPLATE/PPTP.CNF – default values for PPTP configuration file. It is recommended that you do not edit this file!

The following section is divided into two parts. The first part deals with those parameters that MUST be entered in order for PPTP to function. The second part deals with parameters for which the defaults should be sufficient. However, please review these parameters to ensure that possible ISP specific ISP parameters are not overlooked.

For parameters that are not already in PPTP/PPTP.CNF, simply copy & paste from PPTP.CNF in the TEMPLATE directory.

Characters following '#' and ';' are comments and are ignored by the PPTP Plugin.

The sample PPTP/PPTP.CNF file below illustrates the format of the configuration file:

```
# Real ISP profile
#
Real     Description = "Real ISP server",
         PPTP-Server = "10.11.1.1",
         User-Id = "test",
         Password = "test",
         Netmask = "255.255.255.255",
         PPP-MRU = 1400,
         Trace = No,
         DNS-1 = "213.80.144.36",
         DNS-2 = "194.84.12.71",
```

For more details about the individual configuration attributes, please refer to the tables below.

6.1. PPTP Mandatory Parameters

The following parameters should be defined by the user, as defaults values may not work.

Parameter	Permissible Values	Description
PPTP-Server	Valid TCP/IP address	Defines the address of PPTP

		Server (PNS). DEFAULT : “” Enclosed in quotation marks.
Domain-Name	String	This is the domain name of your ISP. DEFAULT : "[domain.com]" Enclosed in quotation marks e.g. "Sympatico.ca".
Password	String	This is the password provided by your ISP. DEFAULT : "" Enclosed in quotation marks e.g. "xyz123abc"
User-Id	String	This is the User-ID provided by your ISP. DEFAULT : "[user@isp.com]" Enclosed in quotation marks e.g. "joe@sympatico.ca"

6.2. PPTP Optional Parameters

The following parameters are optional, defaults should function.

Parameter	Permissible Values	Description
Phone-Number	String	The number to be dialed to establish the outgoing session. Currently rarely used. If your ISP requires you to specify additional information in the server location field (separated by space), add this information to Phone-Number. Example: “**10.11.1.1 pc1**”: PPTP-Server = “**10.11.1.1**”, Phone-Number = “**pc1**”,

		DEFAULT : ”” Enclosed in quotation marks.
Subaddress	String	Field used to specify additional dialing information. Currently rarely used. However, usage will increase in future as more PPTP servers are deployed. Change ONLY if specifically instructed by your ISP. DEFAULT : ”” Enclosed in quotation marks.
Connect	Auto Demand Manual	This defines how the initial connection is to be initiated. **Auto** The connection will be made using the ACTIVE ISP profile when the InJoy Firewall is executed. **Demand** (a.k.a. DOD) Connect the ACTIVE profile when a system process (Application or NAT LAN) requests and close connection when process ends (using the Idle Timer). **Manual** Connect using the mouse RMB in the Firewall GUI environment. DEFAULT : Manual Quotation marks not used.
DNS-1 DNS-2	Valid TCP/IP address	These are provided by your ISP. If your ISP supports server assigned DNS addresses per RFC 1877, then enable the negotiation by entering 0.0.0.0 in these fields. Change ONLY if specifically instructed by your ISP.

		DEFAULT : "0.0.0.0" Enclosed in quotation marks.
Idle-Timeout	Seconds (0-99999)	Speicifies how long the connection may remain idle (i.e. nothing being RECEIVED) before automatically disconnecting. 0 – disables the feature. DEFAULT : 0 Quotation marks not used.
LCP-Echo	Seconds (0-99999)	This will trigger the echo packets to be sent at the specified interval in order to detect connection loss. Incoming IP packets reset the timer. When a lost connection is detected, PPTP will respond according to the **Re-connect** setting for the profile. 0 – disables the feature. DEFAULT : 10 Quotation marks not used.
LCP-Consecutive-Errors	Counter (0-99999)	Packets can be lost on a PPTP link without that being critical to the connection. However, if several packets in sequence are lost, then it is normally a sign that the logical PPTP connection is lost. This option allows you to specify the number of consecutive lost packets that are required in order to declare the connection lost. PPTP will respond according to the **Re-connect** setting for the profile. 0 – disables the feature. DEFAULT : 3

		Quotation marks not used.
Local-IP	Valid TCP/IP Address	This is the Internet Protocol (IP) address that your computer will use throughout the current session. The value 0.0.0.0 means that PPTP should obtain the actual IP address from the ISP server during log on negotiation. This is the normal mode used by PPTP. Change ONLY if specifically instructed by your ISP. DEFAULT : "0.0.0.0" Enclosed in quotation marks e.g. "0.0.0.0"
Netmask	Valid TCP/IP Address	If you did not receive an assigned netmask from your ISP then use the netmask 255.255.255.255. DEFAULT : "255.255.255.255" Enclosed in quotation marks.
Peer-IP	Valid TCP/IP Address	This address is normally assigned by the ISP during the log on process. However, some providers specify a fixed IP address that you should enter here. Change ONLY if specifically instructed by your ISP. DEFAULT : "0.0.0.0" Enclosed in quotation marks.
PPP-MRU	Packet Size (1-1500)	This is the size of the Ethernet packets the connection will use. Ethernet has a Max packet size of 1500 bytes, of which 8 bytes are required for the packet

		header. Therefore, unless directed by your ISP, you should use 1492. DEFAULT : 1492 Quotation marks not used.
Re-connect	Auto Demand Manual	This defines what is to happen if a connection is lost. **Auto** Attempt re-connection using the ACTIVE profile automatically. **Demand** Attempt to re-connect when a system process (Applications or NAT LAN) requests. **Manual** Do not attempt a re-connect. DEFAULT : Auto Quotation marks not used.
Restart-Timer	mSec (1/1000th of Sec) 0-99999	This is ONLY used in the opening PPTP negotiation, and resends requests at the specified interval until negotiation is successful. If the opening negotiation seems slow adjust this setting. Note that too small a value can also slow the process down as the server needs time to respond. Note that this only applies to the initial login, once the connection is established this timer is dormant. The smaller you can set this timer and still reliably login, the faster PPTP negotiates. DEFAULT : 300

		Quotations marks not used.
Restart-Timer-Aut	mSec (1/1000th of Sec) 0-99999	This is ONLY used in the opening PPTP negotiation, specifically the user/password authentication process and resends blocks at the specified interval until authentication is successful. If the opening negotiation seems slow, adjust this setting. Note that too small a value can also slow the process down as the server needs time to respond. Note that this is only applies to the initial login, once the connection is established this timer is dormant. DEFAULT : 1000 Quotation marks not used.
Session-Timeout	Seconds (0-99999)	Specifies how long the connection may remain active, irrespective of activity, before automatically disconnecting. 0 – disable the feature. DEFAULT : 0 Quotation marks not used.
Default-Route	Yes No	Signifies whether to create default route record along with the interface route. Change ONLY if specifically instructed by your ISP. DEFAULT : Yes Quotation marks not used.
Trace	Yes	Enable this option if you need

	No	to trace a PPTP connection. The trace information is written to the file "PPTP.TRC" in the home directory. It is recommended to disable trace, unless troubleshooting, as it significantly reduces performance. DEFAULT : No Quotation marks not used.