

IP Tunnel Manager

Copyright © 2003-2009, Pavel Aronovich

<mailto:sales@apbsoft.com>

<http://www.apbsoft.com>

Introduction

The program **IP Tunnel Manager** is used for IP tunneling with the options for compressing and encrypting traffic.

Thus, the program makes it possible to create a secure connection for any application or service using TCP/IP (HTTP, FTP, SMTP, POP, NNTP, SNPP, Telnet, etc.). It is especially important for those TCP/IP services and applications (for example, FTP, Telnet, various DBMS) that transfer passwords openly when establishing a connection between a client and a server. IP Tunnel Manager starts encrypting traffic from the moment when a TCP/IP connection is established, that is why all data transferred between a client and a server are encrypted. Besides, IP Tunnel Manager protects transferred data from being changed by checking the integrity of the transferred data using a 128-bit MAC algorithm.

Data compression provides a significant (not less than 3 times less) decrease in the volume of data transferred via the network.

Multithreaded, highly effective, streaming traffic processing produces practically no negative influence on the channel capacity.

To create a secure connection, the program does not require opening additional ports and it does not transfer keys via the network (as it uses a synchronous algorithm to encrypt traffic). In fact, one and the same password is used to authorize a client and to encrypt data.

IP Tunnel Manager can be used as PROXY (Network Address Translation). As IP Tunnel Manager transfers data "on its own", the server process knows nothing about the client process.

Algorithms for compressing and encrypting data used in the program are among the most fast and effective ones. The **ZLIB** library (Copyright © Base2 Technologies) is used for compressing, the **Blowfish*** algorithm (synchronous, key length - up to 448 bits, library Copyright © Hagen Reddmann, the description of the algorithm can be found here <http://www.schneier.com/blowfish.html>) is used for encrypting and the **Message Digest 5** algorithm (MD5, key length - 128 bits, library Copyright © Hagen Reddmann) is used to ensure the integrity of the transferred data.

At present the program is realized on the Windows platform, including a service application for Windows NT/2000/2003/2008/XP/Vista.

The work of the application is based on the Windows Sockets 2 interface (http://msdn.microsoft.com/library/default.asp?url=/library/en-us/winsock/winsock/windows_sockets_start_page_2.asp).

Read carefully this description before starting the installation of the program

** Another encrypting algorithm can be used depending on your choice.*

Sample use

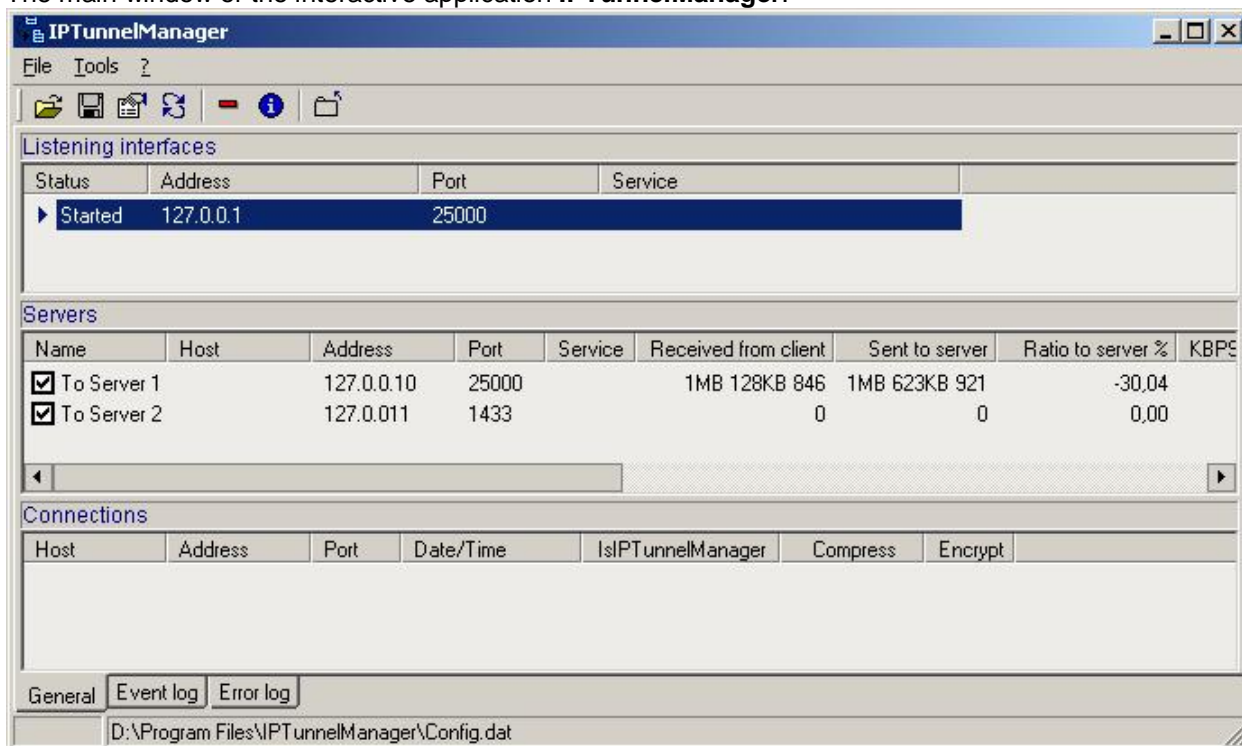
The most common ways of using the program:

1. Client-server application. When an application remotely works with a database server, it is necessary to provide a secure connection with traffic compression. Suppose the database server is located in your head office and client applications work with the database remotely from local branches. Besides, the database server may be inaccessible from the Internet. It can be accessed using IP Tunnel Manager installed on the "gateway" computer that is accessible from the Internet. This kind of applications require an especially secure connection and high data transfer rate. IP Tunnel Manager was originally developed exactly for such applications (for example, for MS SQL Server or Oracle databases) and was successfully tested in practice.
2. Any Internet service (HTTP, FTP, SMTP, POP, NNTP, SNPP, Telnet, etc.). Protection and compression of the transferred data requiring no re-equipment. Moreover, you can use the port that already exists. It is important that data are encrypted from the moment a TCP/IP connection is established.
3. Creating a secure connection with traffic compression between your home and office computers.

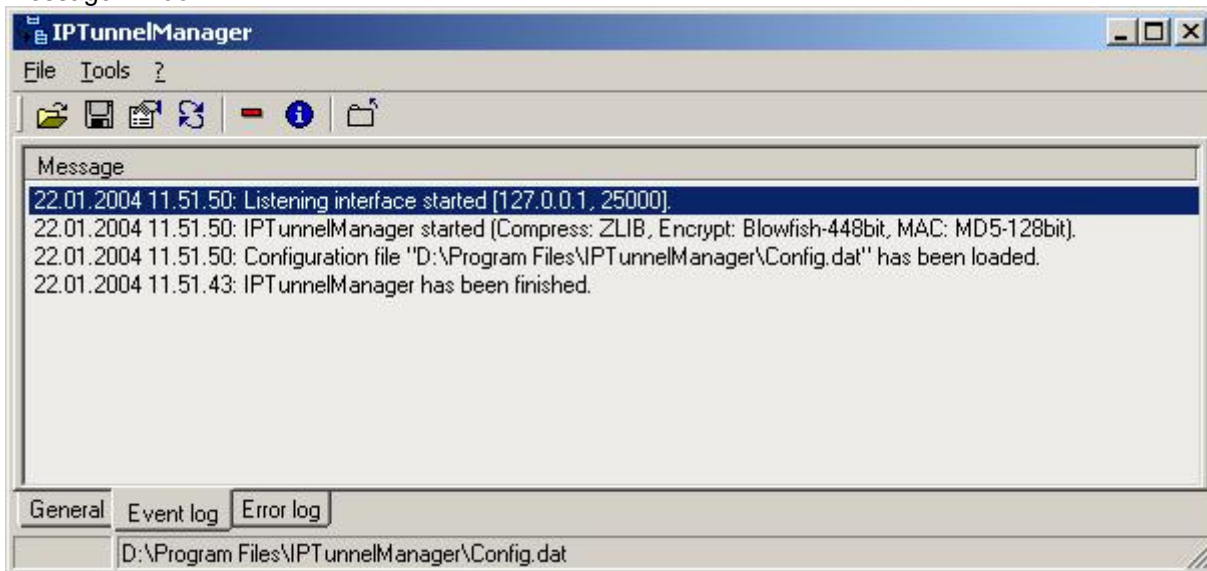
4. Creating a secure connection with traffic compression between your hosting provider and your computer.
5. Using IPTunnelManager as a means of translating network addresses (NAT – Network Address Translation).

Features

The main window of the interactive application **IPTunnelManager**:



Message window:



The main features of IPTunnelManager:

1. Configuring and creating IP tunneling for any number of TCP/IP services (it is possible to listen on several ports).
2. Switching new connections to another server automatically when denial of service occurs on one of the servers.
3. Managing the capacity of one channel (restricting the highest possible number of connected clients).
4. Creating a secure connection.
5. Compressing traffic.
6. Network addresses translating (NAT).

7. Additional features to increase the security of your network.

Diagram 1. The simplest variant of a tunnel.

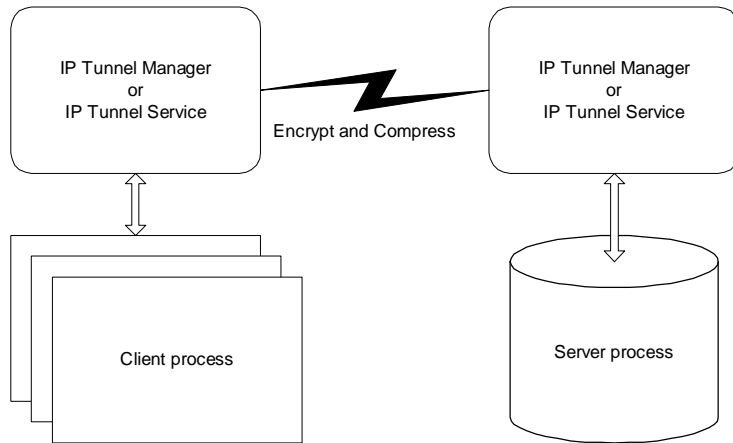
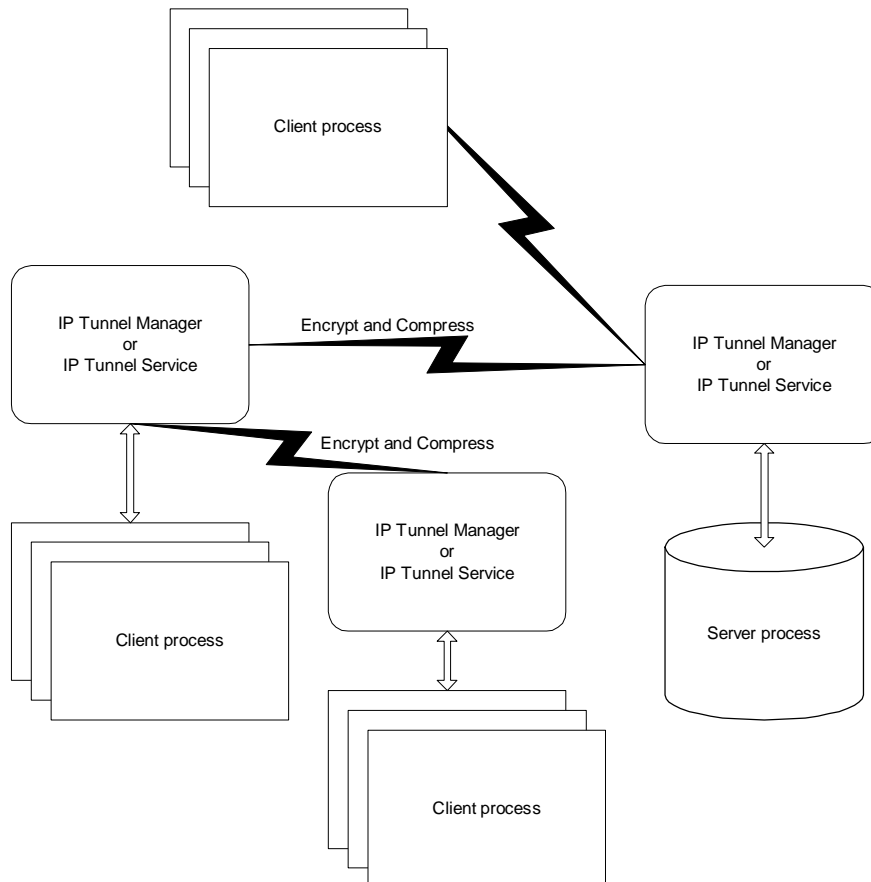


Diagram 2. A more complicated variant of a tunnel.



Additional features:

1. Generating an unique 448-bit key.
2. Saving/restoring the configuration file for configuring the remote applications IPTunnelManager and IPTunnelService.
3. Logging messages and errors.
4. Creating the «Access list» to protect IPTunnelManager against an unauthorized access, as well as to specify that another IPTunnelManager will be a client.
5. Specifying the buffer size and the smallest possible size of a packet to be compressed.
6. Forced client disconnection.
7. Server connection test.

8. Analyzing the amount of transferred data and estimating the data compression rate both for the server and for the client.
9. Showing the data transfer rate (*KBPS, kilobits per second*).
10. Resetting the transferred data counter.

Installation

1. Install the program on your computer (setup.exe).
2. Select the installation type from the following options.
 - 2.1. More details about «**IP Tunnel Manager for Windows 95/98/Me**»:
 - 2.1.1. Installing «IP Tunnel Manager» and «IP Tunnel Service».
 - 2.1.2. Installing «IP Tunnel Manager Users Guide».
 - 2.1.3. Adding icons for «IP Tunnel Manager» to the «Startup» folder and to the «Desktop».
 - 2.2. More details about «**IP Tunnel Manager for Windows NT/2000/2003/XP**»:
 - 2.2.1. Installing «IP Tunnel Manager» and «IP Tunnel Service».
 - 2.2.2. Installing «IP Tunnel Manager Users Guide».
 - 2.2.3. Adding icons for «IP Tunnel Manager» to the «Desktop».
 - 2.2.4. Adding the icons «Install IP Tunnel Service» and «Uninstall IP Tunnel Service» to the program folder.
3. After the installation is complete, launch the program (the installation program will prompt you to do it).
4. The interactive program is added to the autostart programs of the operating system and to the system tray for quick access.
5. Install the service «IP Tunnel Service», if necessary (see below). Configure the tunnel using the interactive application.
6. You can uninstall the program from your computer using the standard Windows feature (Start/Settings/Control Panel/Add|Remove Programs).

Before uninstalling the program from the computer you stop the service «IP Tunnel Service» using «Uninstall IP Tunnel Service»

Working with the program

Creating a tunnel (See Diagram 1):

1. Install the program on a server (it can be a "gateway" computer accessible from the Internet that redirects the data to the computer with a server application).
2. Install the program on a client (it can be a separate computer to which all client applications connect).
3. Configure the programs:
 - 3.1. On the server
 - 3.1.1. Add a «Listening interface» (see Fig. 2), specify any port number (for example, 25000). One IP Tunnel Manager can work with any number of «Listening interfaces». But each «Listening interface» must have an unique port number (the limitations are connected only with your license).
 - 3.1.2. Specify the address of a client computer in the «Access list». It can be either another IP Tunnel Manager (in this case the checkbox «Is IP Tunnel Manager» must be marked) or a usual client (in this case the checkbox «Is IP Tunnel Manager» must be unmarked). Set the rest of the checkboxes and password to fit your needs (see Fig. 3). You can specify any number of addresses in the «Access list».
 - 3.1.3. Add a «Server description» (see Fig. 4) by specifying the address of the computer where the server application is running and the number of the port (for example, 1433 for MS SQL Server) listening for this application (consult the documentation for the corresponding software). The «Is IP Tunnel Manager» checkbox must be unmarked if it is not another IP Tunnel Manager that is connected.
 - 3.2. On the client
 - 3.2.1. Add a «Listening interface» (see Fig. 2), specify any port number (for example, 25000). One IP Tunnel Manager can work with any number of «Listening interfaces». The «Is IP Tunnel Manager» checkbox must be unmarked.
 - 3.2.2. Either enumerate all the addresses of client computers in the «Access list» or leave it empty to allow all computers to access IP Tunnel Manager.
 - 3.2.3. Add a «Server description» (see Fig. 4) by specifying the address of the computer where the server IP Tunnel Manager is installed and the number of the port that is specified in its «Listening interfaces» list (for example, 25000). You must mark the «Is IP Tunnel Manager» checkbox, set the rest of the checkboxes and password to fit your need. You can add any number of «Server descriptions» as alternative connection.

- 3.2.4. You should configure the client application in such a way that it would not connect directly to its server but to client IPTunnelManager. To do that, as a rule, you will have to change the settings of your software (consult the documentation for the corresponding software) specifying the address of client IPTunnelManager and the number of the port specified in it for listening.

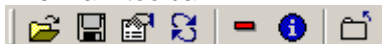
Sample configuration:

To connect a client application to Microsoft SQL Server:

1. Install IPTunnelManager on the server and the client.
2. On the server:
 - 2.1. "Listening interface" – port number 25000, the address of the client computer is in the «Access list», the «IsIPTunnelManager» checkbox is marked. To create a secure connection, you should turn on the "Encrypt" option and specify a password in the «Password» field.
 - 2.2. "Server description" – MS SQL Server address, port number 1433, the «IsIPTunnelManager» checkbox is unmarked.
3. On the client:
 - 3.1. "Listening interface" – port number 25000, the address of the client computer can in the «Access list», or the list can be empty, «IsIPTunnelManager» checkbox is unmarked.
 - 3.2. "Server description" – the address of server IPTunnelManager, port number 25000, «IsIPTunnelManager» checkbox is unmarked. To create a secure connection, you should turn on the "Encrypt" option and specify a password in the «Password» field.
 - 3.3. You should launch the «Client network utility» from the «Microsoft SQL Server» package on client computers. Add an «Alias» specifying the «TCP/IP» protocol, the IP address of client IPTunnelManager and port number 25000.

Interactive program IPTunnelManager:

The main toolbar:



The description of commands from left to right:

1. «Open configuration file» - Load the configuration file. You can change the configuration file you use. On exit the program saves the name of the configuration file that is used so that IPTunnelService could use the same file when it is launched the next time.
2. «Save configuration file as» - Save the configuration file for another IPTunnelManager or IPTunnelService. IPTunnelManager automatically saves all changes in the current file (its name is displayed on the application status bar), that is why the user does not need to save the file manually. By default, the "Config.dat" file is used. It is stored in one folder with IPTunnelManager or IPTunnelService.
3. «Options» - General settings
4. «Refresh» - Refresh lists
5. «Hide» - Hide the program
6. «About» - Information about the program
7. «Exit» - Close the program

Program windows:

The «General» tab

1. **Listening interfaces** – the list of the interfaces being listened to (ip/port).
2. **Servers** – all server descriptions for the selected «Listening interface».
3. **Connections** – all current client connections for the selected «Server description».

The «Event log» tab

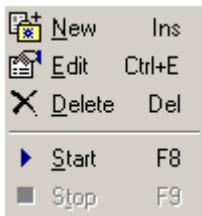
The history of messages.

The «Error log» tab

The history of error messages.

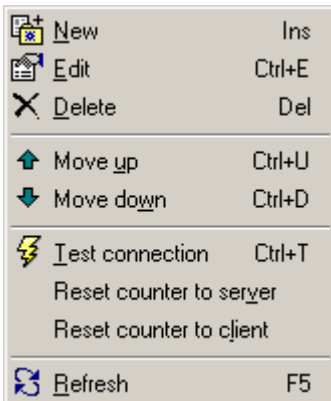
Context menu:

1. The menu of the «Listening interfaces» list



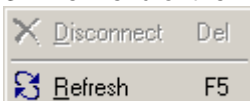
- Add a new «Listening interface»
- Edit the selected «Listening interface»
- Delete the selected «Listening interface»
- Start the selected «Listening interface»
- Stop the selected «Listening interface»

2. The menu of the «Servers» list



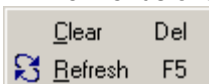
- Add a new «Server description»
- Edit the selected «Server description»
- Delete the selected «Server description»
- Move the selected «Server description» one position up
- Move the selected «Server description» one position down
- Test the connection to the server
- Reset the counter to the server
- Reset the counter to the client
- Refresh data from the list

3. The menu of the «Connections» list



- Disconnect the client
- Refresh data from the list

4. The menus of the «Event log» list and the «Error log» list



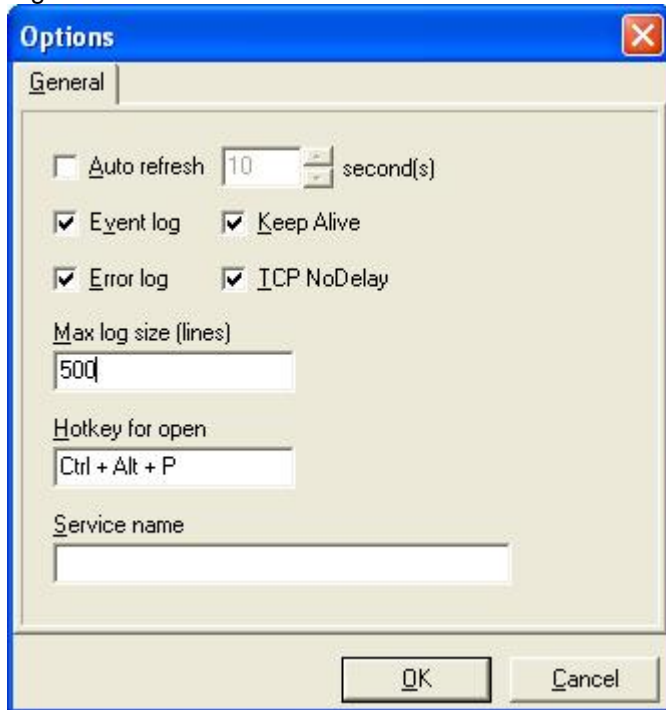
- Clear the list
- Refresh data from the list

Program options window (a button on the main toolbar).

1. **AutoRefresh** – refresh information in the active window automatically (General, Event log, Error log, only the active window is refreshed!). The time for autorefreshing is specified in seconds. When the program is hidden, data in windows are not refreshed. “Listening interface” and “Server” must be selected for the main window to be refreshed.
2. **Event log** – add messages to the «Event log».
3. **Error log** - add error messages to the «Error log».
4. **Max log size** – the largest allowed size (number of lines) for the «Event log» and the «Error log». When the specified number of lines is exceeded, the oldest line is deleted.
5. **Hotkey for open** – a keyboard shortcut used to open the main window of IPTunnelManager that stays in the system tray.
6. **Keep Alive** - Sends keep-alives. Not supported on ATM sockets (results in an error).

7. **TCP NoDelay** - Disables the Nagle algorithm for send coalescing.

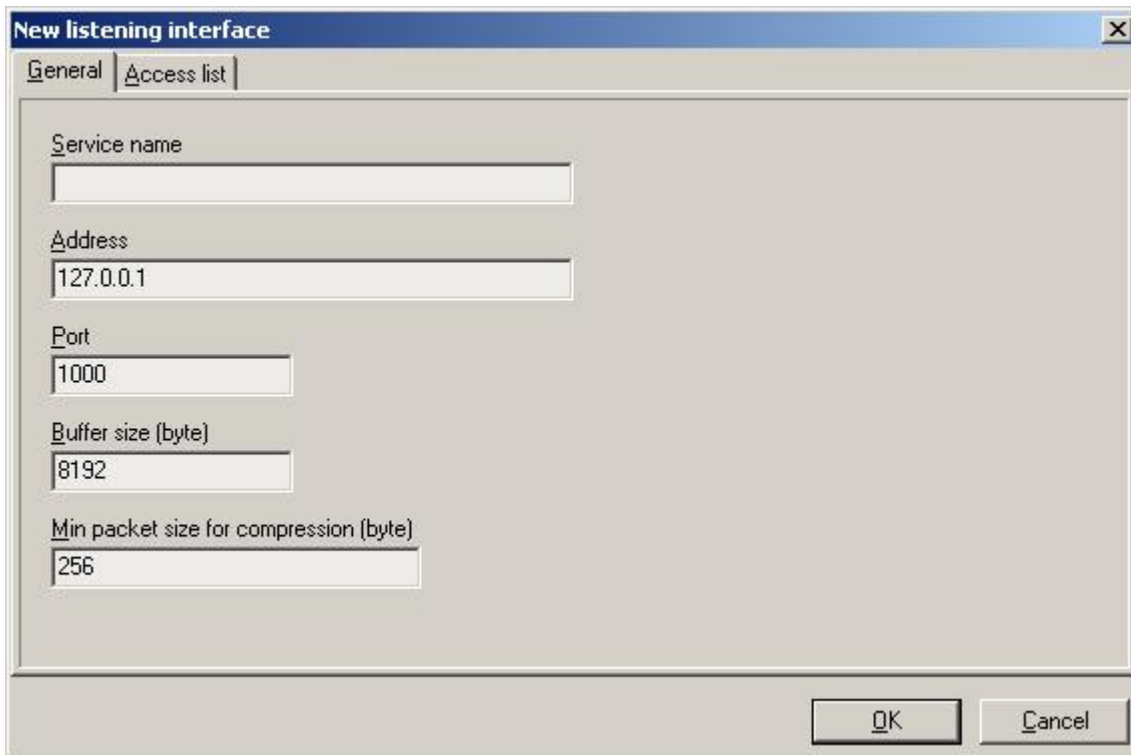
Fig. 1.



Window for adding/editing a “Listening interface”.

1. **Service name** – service name (see more details below)
2. **Address** – the IP address of the interface (by default 127.0.0.1)
3. **Port** – port number
4. **Buffer size** – the size of the buffer for sending/receiving data in bytes. The slower the network is, the smaller the buffer should be (the optimal size for a network with the capacity of 256Kbit/sec is not more than 8Kbyte, the buffer size can be more than 16Kbyte for 10Mbit networks). Specify the same buffer size in your client and server applications (consult the documentation for the corresponding software). The optimal value is determined experimentally.
5. **Min packet size for compression** – the smallest possible size of a packet (in bytes) to be compressed. As the compression algorithm adds its service information to the transferred data, it is not effective to compress small data packets for their size will increase compared with the original size. The smallest recommended size for a packet to be compressed is 128 bytes. The bigger the size of the packet being compressed, the higher the compression rate is.

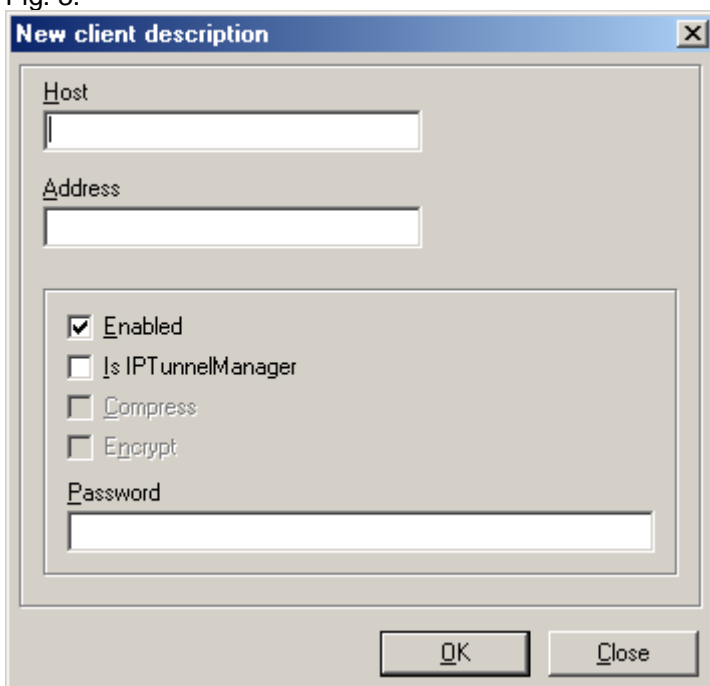
Fig. 2.



Window for editing the «Access list».

1. **Host** – the name of the client host (either Host or Address should be specified). Host is the name of the system that is running the application that uses the Windows socket. Host is a string containing the domain name and service of the local socket endpoint, such as «<http://www.wsite.com/>». Most Intranets provide host names for the IP addresses of systems on the net. On Windows 95 and NT machines, if a host name is not available, create one for the local IP address by entering the name into the HOSTS file. See the Microsoft documentation on Windows sockets for more information on the HOSTS file.
2. **Address** – the IP address of the client (either Host or Address should be specified).
3. **Enabled** – on/off.
4. **Is IPTunnelManager** – the corresponding client is another IPTunnelManager.
5. **Compress** – compress traffic.
6. **Encrypt** – encrypt traffic.
7. **Password** – password (it must be that same as on corresponding IPTunnelManager). Password is used to decrypt data received from the client (if Encrypt is on).

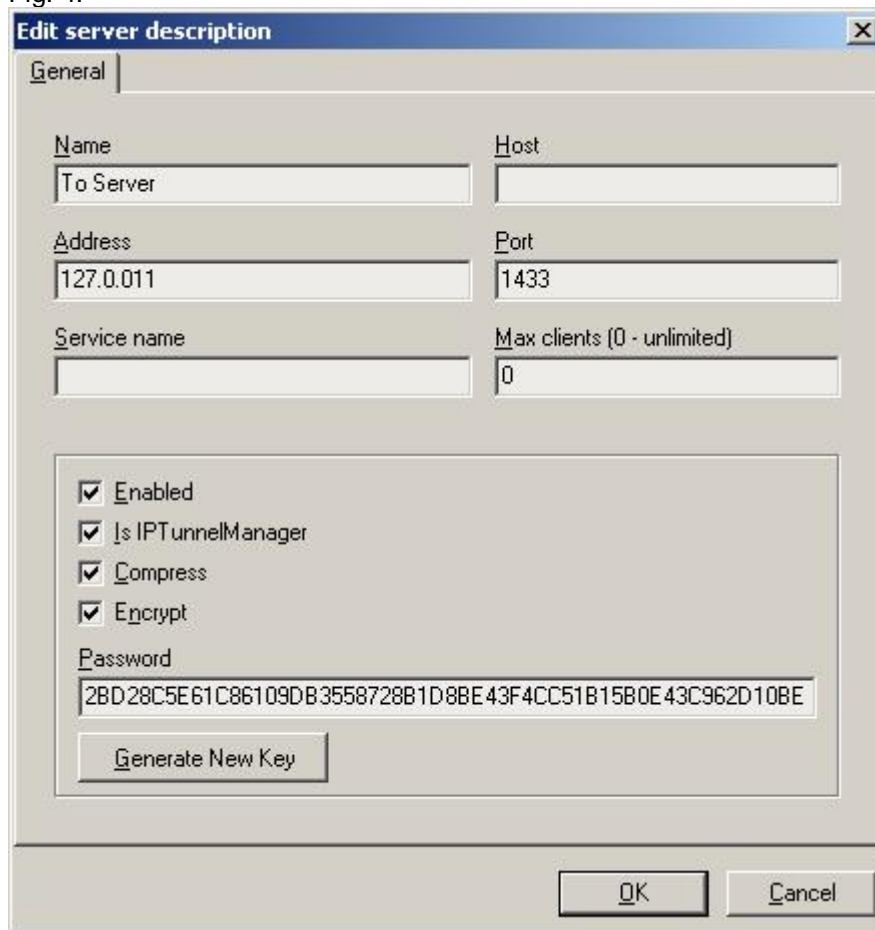
Fig. 3.



Window for adding/editing a «Server description».

1. **Name** – internal server name (used only to distinguish between server descriptions).
2. **Host** – server host name (either Host or Address should be specified).
3. **Address** – the IP address of the server (either Host or Address should be specified).
4. **Port** – port number (a whole number).
5. **Service name** – service name (Use Service to identify the use of the connection. Windows provides a number of standard service names such as ftp, http, finger, and time. Servers can specify additional services and their associated ports in the SERVICES file. For more information, see the Microsoft documentation for Windows sockets. Certain port numbers are reserved for specific values of service. Thus, Service provides a more meaningful way to specify the server Port to use for the socket connection. For server sockets, using Service rather than Port ensures that the server will listen for TCP/IP requests on the appropriate port.)
6. **Max clients** – the largest allowed number of connected clients (if the value is «0», the number of clients is not limited).
8. **Is IPTunnelManager** – the server is another IPTunnelManager.
9. **Compress** – compress traffic.
10. **Encrypt** – encrypt traffic.
7. **Password** – password (the same password should be specified in the Access list on the server). Password is used to encrypt data sent to server IPTunnelManager (if Encrypt is on).
8. **Generate New Key** – generate an unique 448-bit key.

Fig. 4.



Service application IPTunnelService:

The service application uses the same configuration file as the interactive application for its work.

Create the configuration file for the service application using the interactive application IPTunnelManager, close the program (the Exit command).

To change the configuration, launch IPTunnelManager, it will ask you to stop the service. You will have to do it to make changes in the configuration. Make the necessary changes and close IPTunnelManager. Before closing, it will ask if you want to restart the service.

To make the configuration of the service easier, we are planning to implement the remote service administration feature.

Service installation (for Windows NT/2000/2003/XP)

There is the «Install IPTunnelService» file in the program folder.
Launch it.

The service will automatically start after the installation.

Uninstalling the service

There is the «Uninstall IPTunnelService» file in the program folder.
Launch it.

Controlling the service

Open the Services window on your computer:
«Start\Settings\Control Panel\Administrative Tools\Services».

Find the service named «IPTunnelService» in the service list.

Using the standard «Start» and «Stop» commands to control services, you can start and stop it.

The files «Eventlog.txt» and «Errorlog.txt» can be viewed only when the service is stopped and the application IPTunnelManager is closed

User Support

The developer provides users' support during the entire period of using the registered software product.

You can send your suggestions and comments to <mailto:support@apbsoft.com>.

A person from the support service will reply to you within not more than one working day.

Before contacting the support service, see F.A.Q. at <http://www.apbsoft.com>.

Pricelist

Number of clients *	Up to 300	Unlimited
Number of «Listening interfaces»	Up to 20	Unlimited
Price, USD	19	29

If you have any questions concerning the pricelist, products or licensing, you can contact us at sales@apbsoft.com.

** The overall number of connected clients for all servers and «Listening interfaces». The price of a license for the entire number of clients.*

Version update

Bug fixes are done free of charge. Version updates are performed at special prices.
Update terms are published at <http://www.apbsoft.com>.

Port number for TCP/IP services

Service name	Port number
HTTP	80
FTP	21
SMTP	25

POP	110
NNTP	119
SNPP	444
IMAP	143
LDAP	389
Telnet	23

Shareware

IP Tunnel Manager/IP Tunnel Service is shareware. If you are using the demo version of **IP Tunnel Manager** (the trial period is limited to **30 days**) and you would like to purchase the full version, you should click the **<Buy now>** button in the **About** program window or at <http://www.apbsoft.com> web site (to do it, you should be connected to the Internet). Follow the instructions at the site further on.