IP Tunnel Manager

mailto:sales@apbsoft.com
http://www.apbsoft.com

Введение

Программа **IPTunnelManager** предназначена для организации IP-туннеля (IP tunneling) с возможностью сжатия и криптования трафика.

Таким образом, программа позволяет, без какого либо переоснащения сетевой инфраструктуры, организовать защищенное соединение для абсолютно любых приложений и сервисов, использующих TCP/IP (HTTP, FTP, SMTP, POP, NNTP, SNPP, Telnet и т.д.). Это особенно важно для тех TCP/IP сервисов и приложений (например, FTP, Telnet, различные СУБД), которые передают в открытом виде пароли при соединении клиента с сервером. **IPTunnelManager** начинает шифровать трафик с момента установления TCP/IP соединения, поэтому шифруются абсолютно все данные, передаваемые от клиента к серверу и обратно. Кроме того, **IPTunnelManager** защищает передаваемые данные от подмены, проверяя целостность переданных данных с помощью 128 битного MAC-алгоритма.

Сжатие данных позволяет значительно (не менее чем в 3 раза) снизить объем передаваемых по сети данных.

Многопоточная высокоэффективная потоковая обработка трафика практически не оказывает отрицательного влияния на производительность канала передачи данных.

Для организации защищенного соединения программа не требует открытия дополнительных портов и не передает по сети ключи (поскольку для шифрования трафика используется синхронный алгоритм). Фактически для авторизации клиента используется тот же пароль, что и для шифрования данных.

В программе применены одни из самых быстрых и эффективных алгоритмов криптования и сжатия данных. Для сжатия используется библиотека **ZLIB** (Copyright © Base2 Technologies), для криптования данных алгоритм **Blowfish*** (синхронный, длина ключа до 448 бит, библиотека Copyright © Hagen Reddmann, описание алгоритма здесь: http://www.schneier.com/blowfish.html), для подтверждения целостности переданных данных алгоритм **Message Digest 5** (MD5, длина ключа 128 бит, библиотека Copyright © Hagen Reddmann).

На данный момент существует реализация программы для Windows платформы, в т.ч. в виде сервиса (Service application) для Windows NT/2000/2003/2008/XP/Vista.

Работа приложения основана на интерфейсах Windows Sockets 2 (http://msdn.microsoft.com/library/default.asp?url=/library/en-us/winsock/winsock/windows_sockets_start_page_2.asp).

Перед началом установки программы внимательно прочитайте данное описание

** По вашему желанию может быть реализован другой алгоритм шифрования.*

Примеры использования

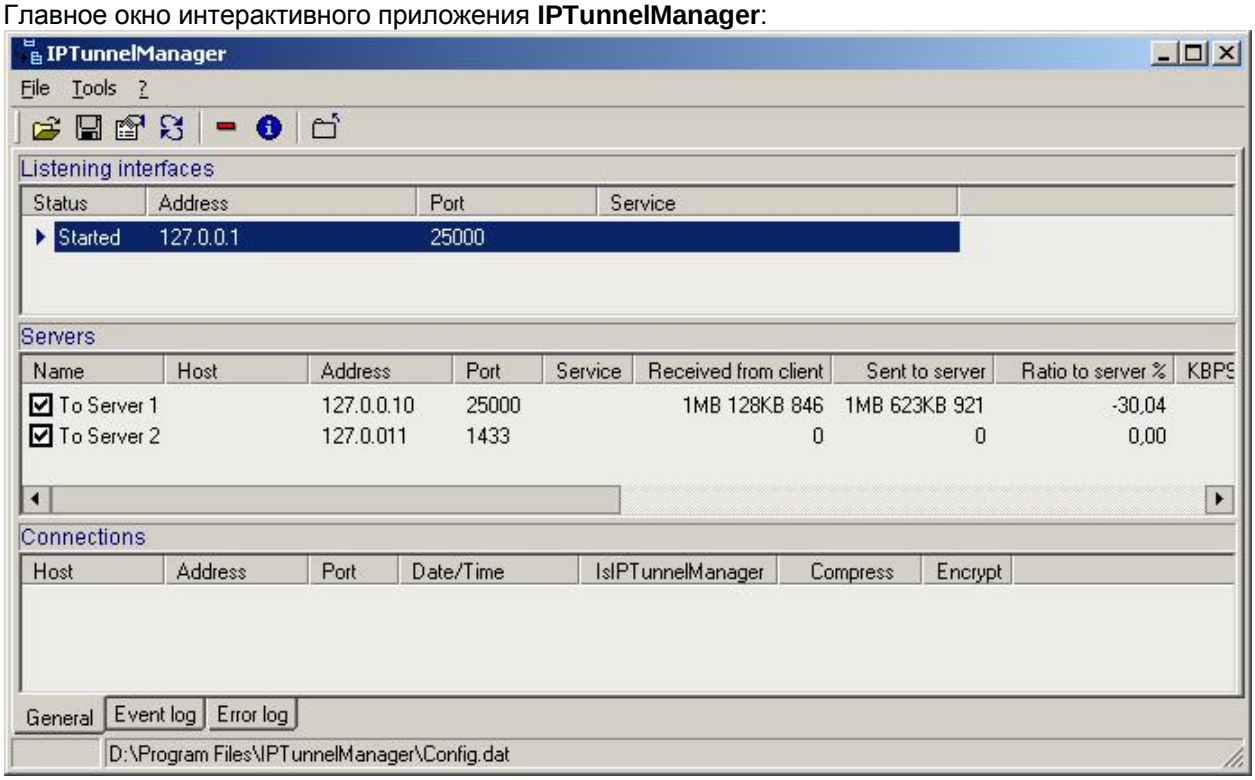
Наиболее часто встречающиеся примеры использования программы:

1. Клиент-серверное приложение. При удаленной работе приложения с сервером базы данных необходимо организовать защищенное соединение с сжатием трафика. Допустим, сервер базы данных находится в вашем центральном офисе, а клиентские приложения работают с базой данных удаленно в филиалах. Причем сервер базы данных может быть недоступен из Интернет. Доступ к нему осуществляется с помощью IPTunnelManager, установленного на шлюзовом компьютере, который доступен из Интернет. Такого рода приложения особо требовательны к надежности соединения и высокой скорости передачи данных. IPTunnelManager изначально создавался именно для таких приложений (например, для баз данных MS SQL Server, Oracle) и успешно прошел испытания на практике.
2. Любые Интернет-сервисы (HTTP, FTP, SMTP, POP, NNTP, SNPP, Telnet и т.д.). Защита и сжатие передаваемых данных от сервера к клиенту не требующее переоснащения. Важно то, что данные шифруются с момента установления TCP/IP соединения.

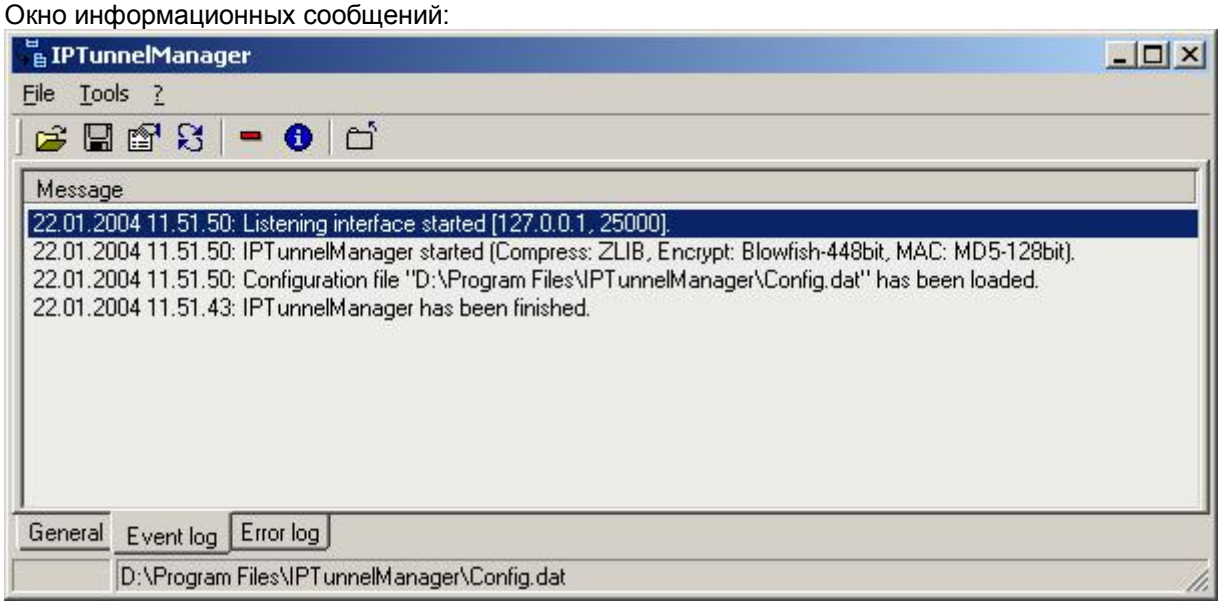
3. Организация защищенного соединения с сжатием трафика между домашним компьютером и офисом.
4. Организация защищенного соединения с сжатием трафика между хостером и вашим компьютером.
5. Использование IPTunnelManager как средства для трансляции сетевых адресов (NAT – Network Address Translation).

Функции

Главное окно интерактивного приложения **IPTunnelManager**:



Окно информационных сообщений:



Основные функции программы IPTunnelManager:

1. Настройка и организация IP tunneling для любого количества TCP/IP сервисов (возможно «прослушивание» множества портов).
2. Автоматическое переключение новых соединений на другой сервер при отказе в обслуживании одним из серверов.
3. Управление нагрузкой на один канал (ограничение максимального количества подключенных клиентов).
4. Организация защищенного соединения.
5. Организация сжатия трафика.

6. Трансляция сетевых адресов (NAT).
7. Дополнительные возможности для увеличения безопасности ваших сетей.

Схема 1. Простейший вариант туннеля.

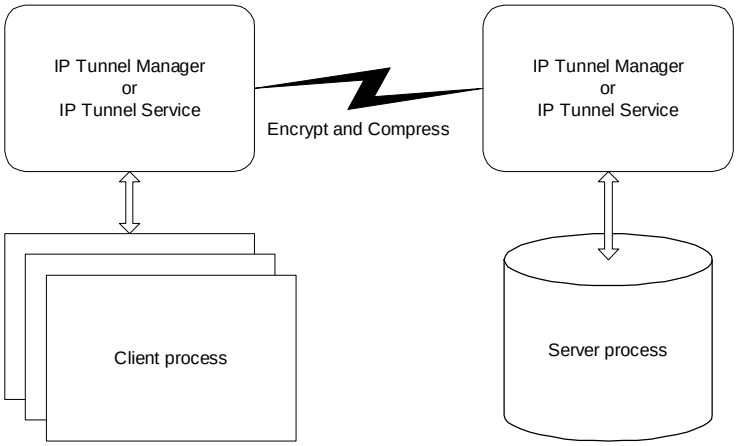
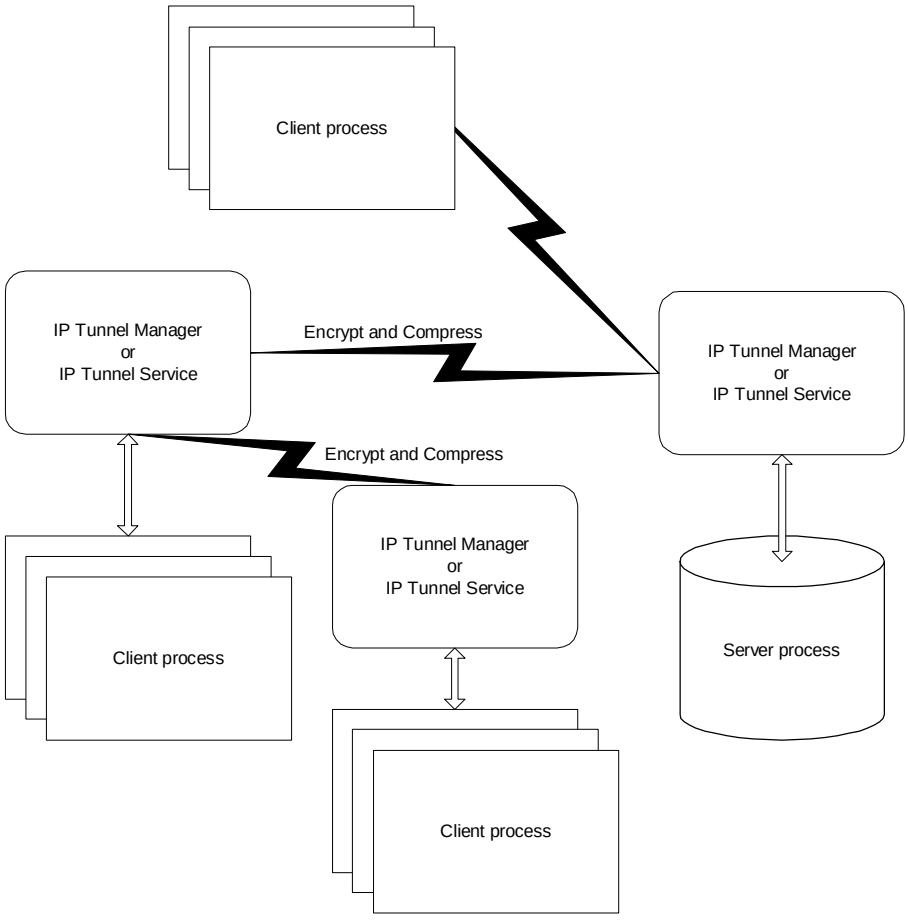


Схема 2. Более сложный вариант туннеля.



Дополнительные функции:

1. Генерация уникального ключа длиной 448 бит.
2. Сохранение/восстановление конфигурационного файла для настройки удаленных приложений IPTunnelManager и IPTunnelService.
3. Ведение журнала сообщений и ошибок.
4. Создание «Access list» для защиты от несанкционированного доступа к IPTunnelManager, а также для указания, что клиентом будет другой IPTunnelManager.
5. Настройка размера буфера и минимального размера пакета данных для сжатия.
6. Принудительное отсоединение клиента.
7. Тестирование соединения с сервером.

8. Подсчет передаваемых данных и расчет процента сжатия данных в сторону сервера и клиента.
9. Отображение скорости передачи данных (*KBPS, kilobits per second*).
10. Сброс счетчиков переданных данных.

Установка

1. Установите программу на компьютер (setup.exe).
2. Выберите тип установки из предложенных.
   2.1. Подробнее о «**IPTunnelManager for Windows 95/98/Me**»:
      2.1.1. Устанавливаются программы «IPTunnelManager» и «IPTunnelService».
      2.1.2. Устанавливается документ «IPTunnelManager Users Guide».
      2.1.3. Добавляется ярлык на «IPTunnelManager» в папку «Startup» и на «Desktop».
   2.2. Подробнее о «**IPTunnelManager for Windows NT/2000/2003/XP**»:
      2.2.1. Устанавливаются программы «IPTunnelManager» и «IPTunnelService».
      2.2.2. Устанавливается документ «IPTunnelManager Users Guide».
      2.2.3. Добавляется ярлык на «IPTunnelManager» на «Desktop».
      2.2.4. Добавляются в папку программы ярлыки «Install IPTunnelService» и «Uninstall IPTunnelService».
3. После завершения установки (установщик предложит это в самом конце) запустите программу.
4. Интерактивная программа помещается в автоматически запускаемые приложения операционной системы и в панель задач (system tray) для быстрого доступа.
5. Если необходимо установите сервис «IPTunnelService» (см. ниже). Настройку туннеля произведите с помощью интерактивного приложения.
6. Удаление программы с компьютера осуществляется с помощью стандартной возможности Windows (Start/Settings/Control Panel/Add|Remove Programs).

Перед удалением программы с компьютера остановите сервис «IPTunnelService» выполнив «Uninstall IPTunnelService»

Работа с программой

Организация туннеля (см. Схему 1):

1. Установите программу на серверный компьютер (это может быть «шлюзовой» компьютер, который доступен из Интернет, с которого происходит переадресация на компьютер с серверным приложением).
2. Установите программу на компьютер клиента (это может быть один выделенный компьютер, к которому подключаются все клиентские приложения).
3. Выполните настройку программ:
   3.1. <u>На сервере</u>
      3.1.1. Добавьте «Listening interface» (см. рис. 2), укажите произвольный номер порта (например, 25000). Одна программа IPTunnelManager может работать с любым количеством «Listening interface» (ограничения связаны только с вашей лицензией). Но каждый «Listening interface» должен иметь уникальный номер порта.
      3.1.2. В списке «Access list» укажите адрес клиентского компьютера. Это может быть как другой IPTunnelManager, тогда флажок «IsIPTunnelManager» должен быть включен, так и обычный клиент, тогда флажок «IsIPTunnelManager» должен быть выключен. Остальные флажки и пароль установите по необходимости (см. рис. 3). В списке «Access list» вы можете указать любое количество адресов.
      3.1.3. Для нового «Listening interface» добавьте «Server description» (см. рис. 4), указав адрес компьютера, на котором функционирует серверное приложение и номер порта (например, 1433 для MS SQL Server), который «слушает» это приложение (обратитесь к документации на соответствующее программное обеспечение). Флажок «IsIPTunnelManager» обязательно должен быть выключен, если обращение осуществляется не к другому IPTunnelManager.
   3.2. <u>На клиенте</u>
      3.2.1. Добавьте «Listening interface» (см. рис. 2), укажите произвольный номер порта (например, 25000). Одна программа IPTunnelManager может работать с любым количеством «Listening interface». Флажок «IsIPTunnelManager» обязательно должен быть выключен.
      3.2.2. В списке «Access list» либо перечислите все адреса клиентских компьютеров, либо оставьте его пустым и тогда всем компьютерам будет разрешен доступ к IPTunnelManager.

3.2.3. Добавьте «Server description» (см. рис. 4), указав адрес компьютера, на котором установлен серверный IPTunnelManager и номер порта, который указан в его списке «Listening interfaces» (например, 25000). Обязательно установите флажок «IsIPTunnelManager», остальные флажки и пароль по необходимости. Вы можете добавить любое количество «Server description» для альтернативного подключения.

3.2.4. Необходимо настроить клиентское приложение, таким образом, чтобы оно обращалось не напрямую к своему серверу, а к клиентскому IPTunnelManager. Для этого, как правило, необходимо изменить настройки программного обеспечения (см. документацию по соответствующему программному обеспечению), указав адрес клиентского IPTunnelManager и номер порта, который указан в нем для прослушивания.

Пример настройки:

Для соединения клиентского приложения с Microsoft SQL Server:

1. Установите IPTunnelManager на сервер и клиент.
2. На сервере:
   2.1. “Listening interface” – номер порта 25000, в «Access list» адрес клиентского компьютера, флажок «IsIPTunnelManager» включен. Для установки защищенного соединения необходимо включить опцию “Encrypt” и указать пароль в поле «Password».
   2.2. “Server description” – адрес MS SQL Server, номер порта 1433, флажок «IsIPTunnelManager» выключен.
3. На клиенте:
   3.1. “Listening interface” – номер порта 25000, в «Access list» адрес клиентского компьютера или список может быть пустой, флажок «IsIPTunnelManager» выключен.
   3.2. “Server description” – адрес серверного IPTunnelManager, номер порта 25000, флажок «IsIPTunnelManager» включен. Для установки защищенного соединения необходимо включить опцию “Encrypt” и указать пароль в поле «Password».
   3.3. На клиентских компьютерах необходимо запустить программу «Client network utility» из комплекта «Microsoft SQL Server». Добавить «Alias» с указанием протокола «TCP/IP», IP-адреса клиентского IPTunnelManager и номером порта 25000.

Интерактивная программа IPTunnelManager:

Главная панель инструментов:

Описание команд по порядку слева направо:

1. «Open configuration file» - Загрузить файл настроек. Вы можете заменить используемый файл настроек приложения на другой. Программа сохраняет при выходе имя используемого файла настроек для следующего сеанса работы, и этот же файл будет использоваться программой IPTunnelService при ее запуске.
2. «Save configuration file as» - Сохранить файл настроек для другого IPTunnelManager или IPTunnelService. IPTunnelManager автоматически сохраняет все изменения в текущем файле (его имя отображается в панели состояния приложения), поэтому нет необходимости пользователю сохранять файл вручную. По умолчанию используется файл “Config.dat” находящийся в том же каталоге, что и приложение IPTunnelManager или IPTunnelService.
3. «Options» - Общие настройки
4. «Refresh» - Обновить списки
5. «Hide» - Скрыть программу
6. «About» - Информация о программе
7. «Exit» - Закрыть программу

Окна программы:

Закладка «General»

1. **Listening interfaces** – список прослушиваемых интерфейсов (ip/port).
2. **Servers** – для выделенного «Listening interface» перечислены все описания серверов.
3. **Connections** - для выделенного «Server description» перечислены все текущие клиентские соединения.

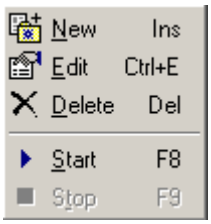
Закладка «Event log»

История информационных сообщений.

Закладка «Error log»
История сообщений об ошибках.

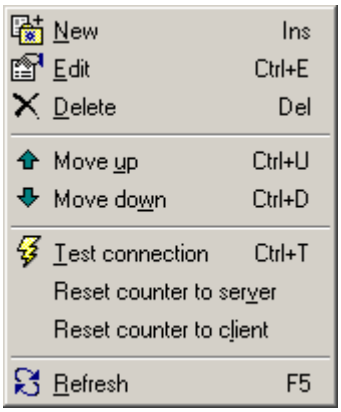
Контекстное (выпадающее) меню:

1. Меню списка «Listening interfaces»



- Добавить новый «Listening interface»
- Изменить выбранный «Listening interface»
- Удалить выбранный «Listening interface»
- Запустить выбранный «Listening interface»
- Остановить выбранный «Listening interface»

2. Меню списка «Servers»

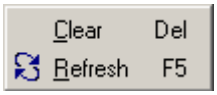


- Добавить новый «Server description»
- Изменить выбранный «Server description»
- Удалить выбранный «Server description»
- Переместить выбранный «Server description» на одну позицию наверх
- Переместить выбранный «Server description» на одну позицию вниз
- Выполнить тестирование соединения с сервером
- Обнулить счетчик в сторону сервера
- Обнулить счетчик в сторону клиента
- Обновить данные списка

3. Меню списка «Connections»

- Отсоединить клиента
- Обновить данные списка

4. Меню списков «Event log» и «Error log»

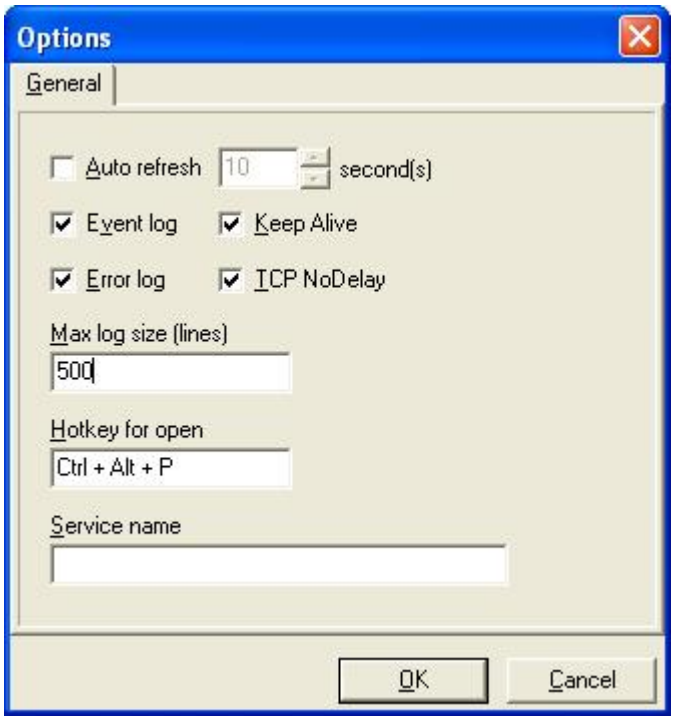


- Очистить список
- Обновить данные списка

Окно настройки программы (кнопка на главной панели инструментов).

1. **AutoRefresh** – включить/выключить автоматическое обновление информации в текущем окне (General, Event log, Error log, обновляется только текущее окно !). Время обновления задается в секундах. Когда программа невидима, обновление данных в окнах не происходит. Для обновление главного окна необходимо чтобы были выбраны “Listening interface” и “Server”.
2. **Event log** – включить/выключить добавление информационных сообщений программы в список «Event log».
3. **Error log** - включить/выключить добавление сообщений об ошибках в список «Error log».
4. **Max log size** – максимальное количество строк для «Event log» и «Error log». При превышении указанного количества строк происходит вытеснение первой строки.
5. **Hotkey for open** – горячая комбинация клавиш для открытия главного окна приложения IPTunnelManager, которое находится в system tray.
6. **Keep Alive –** измените этот параметр если программа работает в вашей сети не стабильно.
7. **TCP NoDelay** – измените этот параметр если программа работает в вашей сети не стабильно.

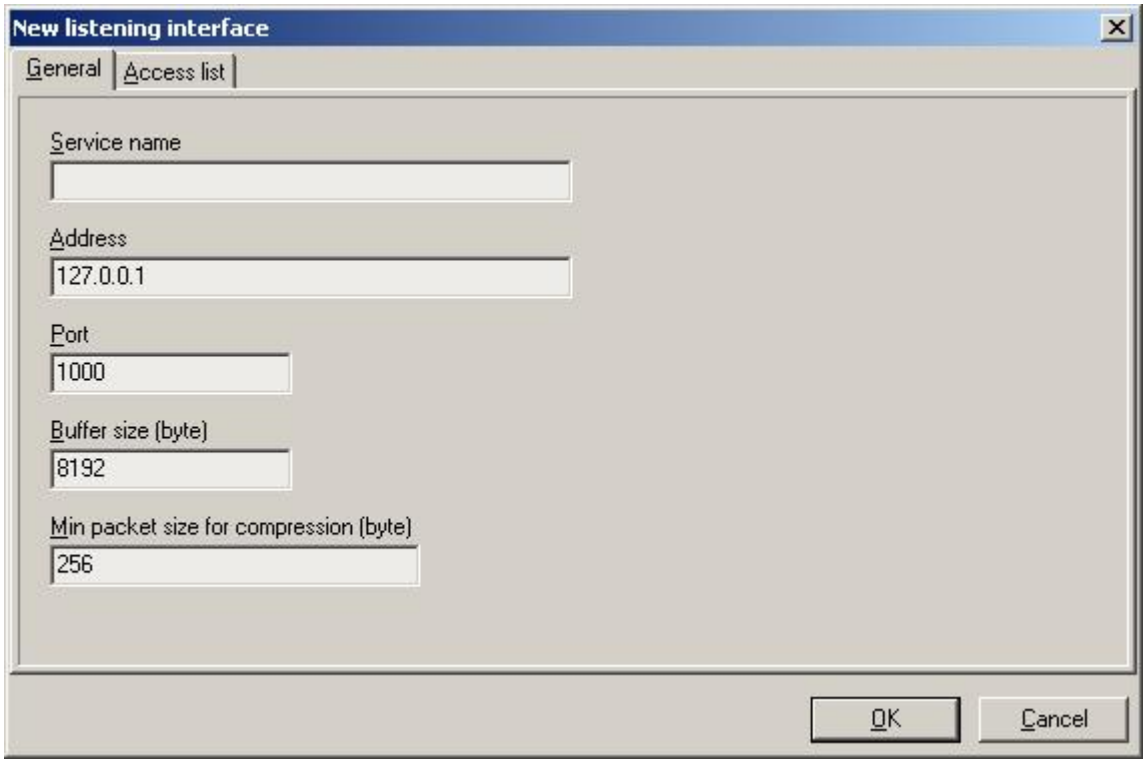
Рис. 1.



Окно для добавления, изменения “Listening interface”.

1. **Service name** – имя сервиса (более подробно см. ниже)
2. **Address** – IP адрес интерфейса (по умолчанию 127.0.0.1)
3. **Port** – номер порта
4. **Buffer size** – размер буфера передачи/получения данных в байтах. Чем медленнее сеть, тем меньше должен быть буфер (для сети с пропускной способностью 256Кбит/сек оптимальный размер не более 8Кбайт, для 10Мбит сетей размер буфера может быть более 16Кбайт). Установите такой же размер буфера в вашем клиентском и серверном приложении (см. документацию на соответствующее программное обеспечение). Оптимальное значение подбирается экспериментально.
5. **Min packet size for compression** – минимальный размер пакета в байтах, который будет сжиматься. Поскольку алгоритм сжатия добавляет в передаваемые данные свою служебную информацию неэффективно сжимать маленькие пакеты данных, они наоборот будут увеличиваться относительно первоначального размера. Минимальный рекомендуемый размер сжимаемого пакета 128 байт. Чем больше размер сжимаемого пакета, тем большая эффективность сжатия.

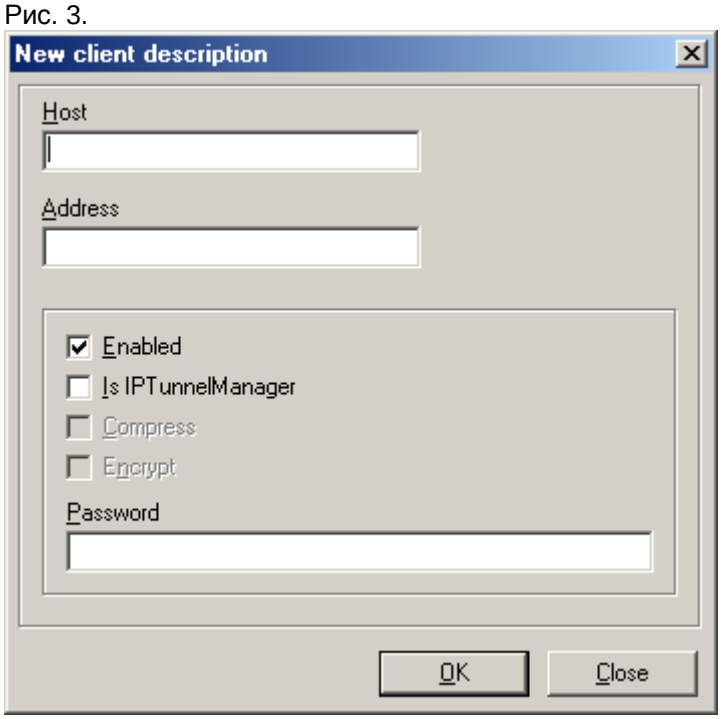
Рис. 2.



Окно для редактирования «Access list».

1. **Host** – имя клиентского хоста (необходимо указывать Host или Address). Host - 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** – клиентский IP адрес (необходимо указывать Host или Address).
3. **Enabled** – включить/выключить.
4. **Is IPTunnelManager** – соответствующий клиент - это другой IPTunnelManager.
5. **Compress** – сжимается ли трафик.
6. **Encrypt** – шифруется ли трафик.
7. **Password** – пароль (должен быть таким же как и на подключаемом IPTunnelManager). Пароль используется для дешифрования (если включен Encrypt) пришедших от клиента данных.

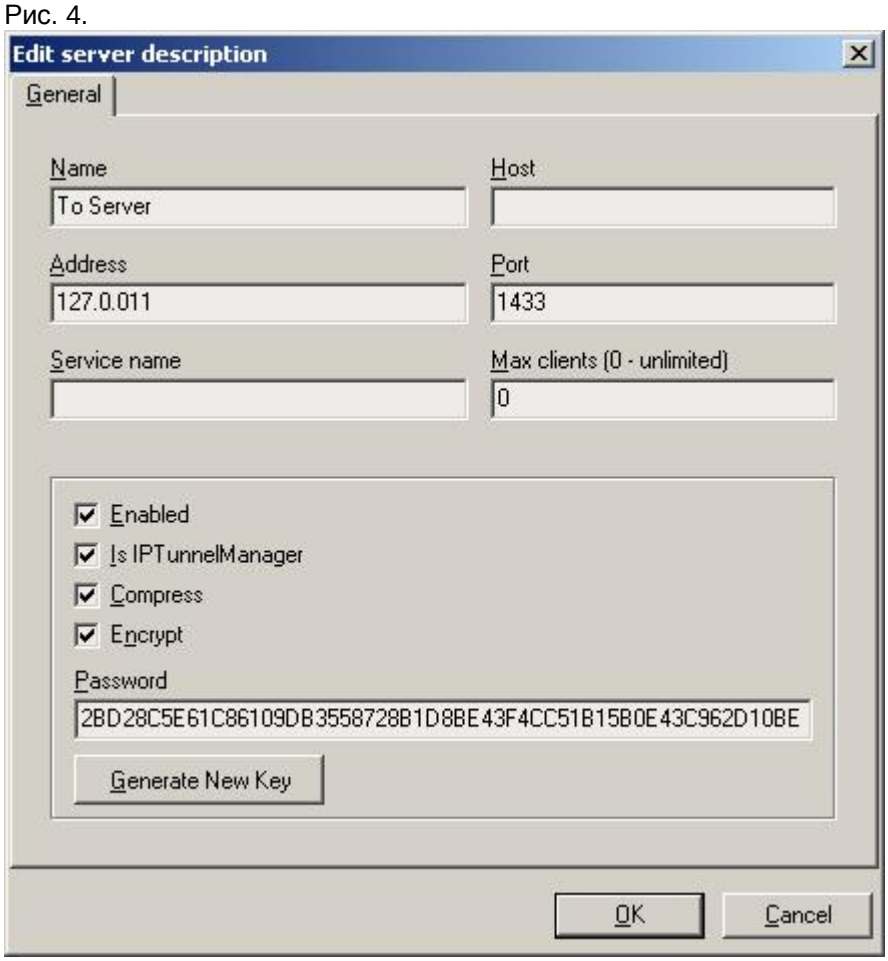
Рис. 3.



Окно для добавления, редактирования «Server description».

1. **Name** – внутреннее имя сервера (используется только для отличия описаний серверов).
2. **Host** – имя серверного хоста (необходимо указывать Host или Address).
3. **Address** – серверный IP адрес (необходимо указывать Host или Address).
4. **Port** – номер порта (целое число).
5. **Service name** – имя сервиса (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 a 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** – максимальное количество подключаемых клиентов (если «0» – количество клиентов не ограничено).
8. **Is IPTunnelManager** – сервер – это другой IPTunnelManager.
9. **Compress** – сжимать ли трафик.
10. **Encrypt** – шифровать ли трафик.
7. **Password** – пароль (такой же пароль необходимо указать в Access list на серверной стороне). Пароль используется для шифрования (если включен Encrypt) передаваемых на серверный IPTunnelManager данных.
8. **Generate New Key** – сгенерировать уникальный ключ длиной 448 бит.

Рис. 4.



Приложение-сервис IPTunnelService:

Для своей работы приложение-сервис использует тот же файл настроек, что и интерактивное приложение.

Сформируйте для приложения-сервиса файл настроек интерактивным приложением IPTunnelManager.

Для того чтобы произвести настройку запустите IPTunnelManager, он предложит остановить сервис. Для выполнения настройки необходимо с этим согласиться. Выполните настройку и закройте IPTunnelManager. Перед закрытием он предложит запустить сервис заново.

Для упрощения настройки сервиса мы в ближайшее время планируем реализовать функцию удаленного администрирования сервиса.

Установка сервиса (для Windows NT/2000/2003/XP)

В папке программы находится файл **«Install IPTunnelService».**
Запустите его.

После установки сервис автоматически стартует.

Удаление сервиса

В папке программы находится файл **«Uninstall IPTunnelService».**
Запустите его.

Управление сервисом

Откройте окно управления сервисами на компьютере:
«Start\Settings\Control Panel\Administrative Tools\Services».

Найдите в списке сервисов сервис с именем **«IPTunnelService»**.

Используя стандартные команды «**Start»** и «**Stop**» управления сервисами, вы можете запускать и останавливать его.

Просматривать файлы «Eventlog.txt» и «Errorlog.txt» можно только при остановленном сервисе и закрытом приложении IPTunnelManager

Поддержка пользователей

Поддержка пользователей осуществляется разработчиком в течении всего срока эксплуатации зарегистрированного программного продукта.

Ваши предложения и замечания Вы можете направлять на адрес электронной почты mailto:support@apbsoft.com.

В течении не более чем одного рабочего дня Вам ответит сотрудник службы поддержки.

Перед тем как обратиться в службу поддержки изучите раздел **F.A.Q.** на веб-сайте http://www.apbsoft.com.

Прайс

Количество клиентов *	**До 300**	**Unlimited**
Количество «Listening interface»	До 20	Unlimited
Цена, USD	19	29

Если у вас есть вопросы по прайсу, продуктам или лицензированию вы можете обратиться по адресу mailto:sales@apbsoft.com.

** Общее количество подключаемых клиентов для всех серверов и «Listening interface». Цена указана за лицензию на все количество клиентов.*

Обновление версий

Исправление ошибок осуществляется бесплатно. Обновление версий осуществляется по специальным ценам.
Условия обновления версий публикуются на веб-сайте http://www.apbsoft.com.

Номера портов для сервисов TCP/IP

Название сервиса	Номер порта
HTTP	80
FTP	21
SMTP	25
POP	110
NNTP	119
SNPP	444
IMAP	143
LDAP	389
Telnet	23

Shareware

Программа **IPTunnelManager/IPTunnelService** относится к условно бесплатным программам (Shareware). Если вы используете ограниченную версию программы **IPTunnelManager** (evaluation, ограничена использованием в течении **30 дней**) и хотите приобрести полную версию вам необходимо щелкнуть на кнопке **<Buy now>** в окне программы **About** или на веб-сайте http://www.apbsoft.com (до этого необходимо подключиться к сети Интернет). Далее действуйте согласно инструкции на сайте.