

VPN

Описание

VPN - виртуальная частная сеть, позволяющая объединить в единую сеть пользователей, физически находящихся в различных местах. Кроме того, с помощью VPN можно организовать выход компьютеров локальной сети к интернету по логину/паролю.

Обычно VPN используется для организации удалённого доступа к локальной сети: например, в тех случаях, когда пользователю требуется получить доступ к внутренним ресурсам сети предприятия пока он находится в командировке или отпуске.

Создание VPN-сети

Для того, чтобы начать работу с VPN, необходимо создать виртуальную подсеть, в которой будут появляться VPN-пользователи после подключения. Для этого необходимо перейти в раздел «Провайдеры и сети» и выбрать пункт «Добавить» → «VPN-сеть».

Добавление VPN-сети

Название: Новая VPN-сеть

Ip-адрес/префикс: 192.168.1.1/24

Протоколы: PPTP
 L2TP
 L2TP IPsec

Ключ:

PPPoE

Интерфейс: em1

Имя сервиса: test

Использовать NAT:

Разрешить управление ИКС через веб
 Разрешить управление ИКС через SSH

Меньше параметров...

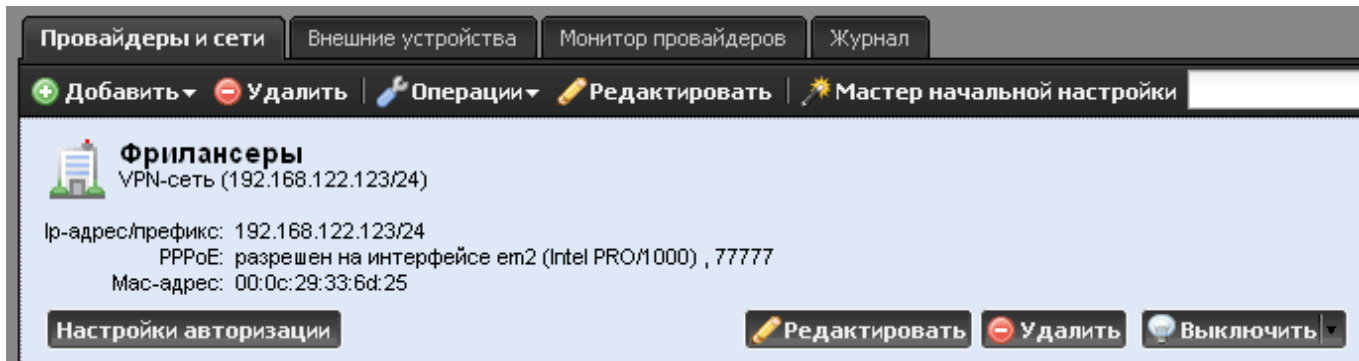
Добавить Отмена

Необходимо указать диапазон адресов для VPN-сети в формате ip-адрес VPN-интерфейса/маска. Адреса из этого диапазона будут выдаваться пользователям, подключающимся через VPN.

Для предоставления пользователям доступа в интернет посредством PPPoE, необходимо

выбрать опцию «PPPoE» и указать сетевой интерфейс, который подключен к сети с пользовательскими компьютерами.

В том случае, если в вашей сети находятся несколько PPPoE-серверов, вы можете идентифицировать сервер ИКС при помощи поля «Имя сервиса», задав в нем произвольное имя.



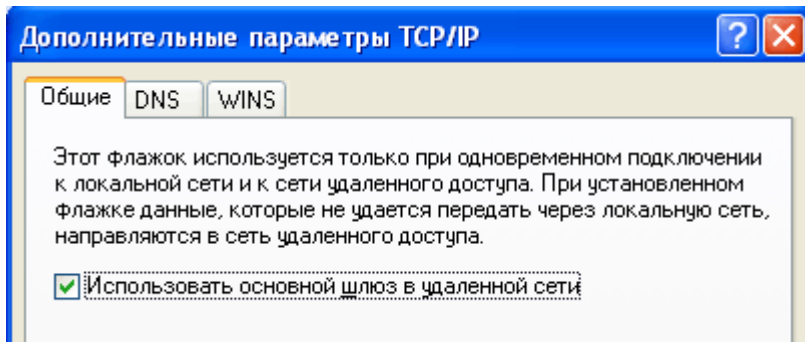
Чтобы сразу перейти к списку пользователей, разрешенных для подключения, нажмите кнопку «Настройки авторизации» на панели созданной VPN-сети.

Настройка пользователя

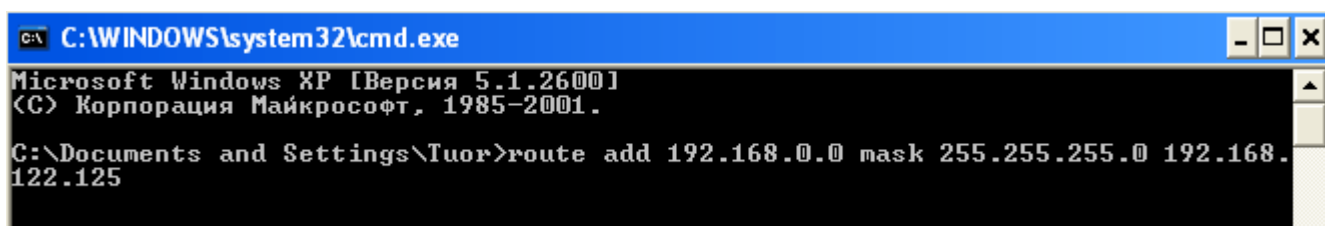
Для того, чтобы пользователь мог подключиться к серверу по VPN, необходимо отметить его флажком в списке пользователей в меню VPN - Пользователи. Также нужно указать ему логин и пароль для подключения.

Имя	Логин	Ip-адреса из Vpn-сетей	Vpn-доступ
Корневая группа			<input type="checkbox"/>
v1	v1	192.168.122.1	<input checked="" type="checkbox"/>
Администратор (недельная квота исчерпана)	root	192.168.122.10	<input checked="" type="checkbox"/>
Новый пользователь (недельная квота исчерпана)	ksu	192.168.122.11	<input checked="" type="checkbox"/>
Новый пользователь1	ksu1		<input type="checkbox"/>

Если пользователь всегда должен получать один и тот же ip-адрес, можно присвоить ему адрес из диапазона VPN-сети во вкладке пользователя «IP-адреса». Этот адрес будет назначаться пользователю при подключении, в противном случае пользователю будет выдаваться первый свободный адрес из VPN-диапазона. Назначение адреса вручную удобно в том случае, если пользователь при подключении не использует ИКС как удаленный шлюз. В таком случае клиенту можно прописать статический маршрут до сетей ИКС. Это делается следующим образом (на примере Windows XP):



В свойствах созданного VPN-подключения во вкладке «Сеть» необходимо выбрать пункт «Протокол интернета TCP/IP», нажать кнопку «Свойства», в открывшемся окне нажать кнопку «Дополнительно» и снять флажок «Использовать основной шлюз в удаленной сети».



После этого пользователю в настройка системы необходимо прописать маршрут вида «Удаленная сеть» → «Выданный VPN-адрес».

Настройка межсетевого экрана

Для того, чтобы удалённые пользователи могли подключаться к ИКС через PPTP VPN, необходимо чтобы в [межсетевом экране](#) были разрешены правила «Доступ к VPN-серверу» (разрешены входящие соединения на порт 1723) и «Доступ к серверу через GRE-туннели» (разрешен GRE-трафик).

Мониторинг подключений

Во вкладке модуля [VPN](#) «Текущие сеансы» можно просмотреть список активных VPN-сессий, имена подключённых пользователей, их ip-адреса и т.д. Любое подключение можно разорвать.

Использование ARP-прокси

Обычно, если при настройке PPTP-подключения не была указана опция «использовать шлюз в удалённой сети», пользователю необходимо вручную указывать маршрут до компьютеров локальной сети. Для того, чтобы обойти это ограничение, используется технология ARP proxy.

В этом случае, при подключении по VPN пользователю выдаётся свободный ip-адрес из общей локальной сети и он может обращаться к ресурсам локальной сети так, как будто он физически находится в ней.

Для того, чтобы использовать ARP-прокси, необходимо в свойствах VPN-сети указать диапазон

адресов из локальной сети, например если используется локальная сеть 192.168.1.0/24, то для VPN можно выделить диапазон 192.168.1.129/28, таким образом VPN-пользователям можно выдать адреса 192.168.1.130-192.168.1.144.

From:

<https://doc.a-real.ru/> - **Документация**

Permanent link:

<https://doc.a-real.ru/doku.php?id=en:vpn>

Last update: **2020/01/27 16:28**

