

Туннель - это механизм позволяющий объединить две удалённые и не связанные физически сети в единую логическую структуру. Статические туннели используются для объединения нескольких локальных сетей в одну: например при объединении нескольких удалённых офисов в одну локальную сеть таким образом, чтобы пользователи одной сети могли обращаться к ресурсам других. Туннели настраиваются на пограничных маршрутизаторах этих сетей и весь промежуточный трафик передаётся через интернет инкапсулированным в IP или GRE-пакеты.

В ИКС вы можете настроить подключение между серверами статическим туннелем по IPIP или GRE протоколу.

The screenshot shows the 'Tunnels' configuration page. At the top, there are tabs: 'Провайдеры и сети' (selected), 'Внешние устройства', 'Монитор провайдеров', and 'Журнал'. Below the tabs are buttons: 'Добавить' (Add), 'Удалить' (Delete), 'Выключить' (Shutdown), 'Редактировать' (Edit), and a yellow 'Мастер настройки сети' (Network Configuration Wizard) button. On the left, a sidebar lists categories: 'Сети' (Networks), 'Локальная сеть' (Local Network), 'Провайдеры' (Providers), 'Провайдер' (Provider), 'Туннели' (Tunnels), and three sub-options under 'Туннели': 'Туннель IPIP', 'Туннель GRE', and 'Туннель OpenVPN'. The 'Туннель IPIP' option is highlighted with a yellow box.

Обычно выбор типа туннеля зависит от промежуточных провайдеров, которые по каким-либо причинам они могут блокировать трафик GRE или IPIP что приводит к невозможности использования какого-то одного типа туннеля. Принципиальной же разницы между этими типами туннелей нет.

Добавление туннеля IPIP		Добавление туннеля GRE	
<input checked="" type="radio"/> Общие настройки <input type="radio"/> Настройки шифрования		<input checked="" type="radio"/> Общие настройки <input type="radio"/> Настройки шифрования	
Название* <input type="text" value="Ламповый туннель"/>		Название* <input type="text" value="Классный туннель GRE"/>	
Внешний интерфейс* <input type="text" value="Мощный провайдер (192.168.170.134/24)"/>	Внешний ip-адрес удаленного сервера* <input type="text" value="192.168.187.14"/>	Внешний интерфейс* <input type="text" value="Мощный провайдер (192.168.170.134/24)"/>	Внешний ip-адрес удаленного сервера* <input type="text" value="192.168.187.14"/>
Локальный ip-адрес туннела* <input type="text" value="10.0.0.1"/>	Удаленный ip-адрес туннела* <input type="text" value="10.0.0.2"/>	Локальный ip-адрес туннела* <input type="text" value="10.0.0.1"/>	Удаленный ip-адрес туннела* <input type="text" value="10.0.0.2"/>
Локальные сети <input type="text" value="Локальные сети"/>	Удаленные сети <input type="text" value="Удаленные сети"/>	Локальные сети <input type="text" value="Локальные сети"/>	Удаленные сети <input type="text" value="Удаленные сети"/>
MTU <input type="text" value="Автоопределение"/>		MTU <input type="text" value="Автоопределение"/>	
<input type="checkbox"/> Автоматически создавать маршрут для удаленных сетей <input type="checkbox"/> Использовать NAT		<input type="checkbox"/> Автоматически создавать маршрут для удаленных сетей <input type="checkbox"/> Использовать NAT	
<input type="button" value="Добавить"/> <input type="button" value="Отмена"/>		<input type="button" value="Добавить"/> <input type="button" value="Отмена"/>	

Настройки туннелей также не отличаются. Вам необходимо указать, на каком интерфейсе будет настроен данный туннель и прописать параметры маршрутизации: внешний адрес удаленного сервера, адрес локальной сети и адрес удаленной сети. Аналогичные настройки необходимо произвести на другом конце тоннеля.

Важно: для того, чтобы туннель работал корректно, необходимо, чтобы в межсетевом экране ИКС был разрешен GRE-трафик, а также разрешены входящие соединения с ip-адреса удаленного сервера.

IPsec (сокращение от IP Security) — набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP, позволяет осуществлять подтверждение подлинности и/или шифрование IP-пакетов.

Добавление туннеля IPiP

Общие настройки

Настройки шифрования

Использовать шифрование

Ключ шифрования

Ключ шифрования

Настройки для фазы 1:

Режим работы

main

Алгоритм шифрования

aes256

DH-группа

15 - modp3072

Время жизни *

28800

Настройки для фазы 2:

Протокол

ESP

PFS

15 - modp3072

Алгоритм аутентификации *

hmac_sha2_384

Алгоритм шифрования

aes256

Время жизни *

1200

Добавить

Отмена

Защита передачи данным по туннелям позволяет избежать многих проблем, связанных с утечкой информации и получения ложных данных. Вы можете защитить туннельный трафик, перейдя на вкладку «Шифрование» и установив флажок «Использовать шифрование». После этого вы можете произвести необходимые настройки параметров. Внимание! Данную процедуру необходимо произвести на обоих концах туннеля, в противном случае передача данных работать не будет.

OpenVPN - свободная реализация технологии VPN с открытым исходным кодом для создания зашифрованных каналов типа точка-точка или сервер-клиенты между компьютерами. Она позволяет устанавливать соединения между компьютерами, находящимися за NAT-firewall, без необходимости изменения их настроек.

Добавление туннеля OpenVPN

Основные настройки	Шифрование и сертификаты
<hr/>	
Название *	Адрес сервера *
<input type="text" value="Лучший туннель OpenVPN"/>	<input type="text" value="10.100.0.0"/>
Протокол	Порт сервера *
<input type="text" value="UDP"/>	<input type="text" value="1194"/>
<input type="checkbox"/> Использовать NAT	
<input style="background-color: green; color: white; padding: 5px 10px; border-radius: 5px; border: none; font-weight: bold; margin-right: 10px;" type="button" value="Добавить"/> <input style="border: 1px solid #ccc; padding: 5px 10px; border-radius: 5px; font-weight: bold;" type="button" value="Отмена"/>	

Система туннелей OpenVPN построена таким образом, что одна из машин выбирается сервером, а все остальные - клиентами. На сервере прописывается адресация пространства внутри openVPN-сети (рекомендуется оставить значение по умолчанию) и размещаются SSL-сертификаты, а на клиентах указывается внешний ip-адрес сервера. Также, указывается порт обмена данными, что позволяет подключаться к серверу, который находится за межсетевым экраном или NAT, при помощи перенаправления портов .

Чтобы прописать необходимые сертификаты от сервера клиентам, сделайте следующее:

1. На сервере необходимо создать [OpenVPN-сеть](#)

Муми-OpenVPN (10.8.0.0/24)

OpenVPN-сеть

Ip-адрес/Префикс: 10.8.0.0/24
 Протокол: udp
 Порт сервера: 1194
 Корневой сертификат: Корневой сертификат
 Сертификат сервера: Муми-OpenVpn

[Подробнее...](#)
[Настройки авторизации](#)
 [Выгрузить сертификаты](#)
Удалить
Редактировать
Выключить ▾

2. Создать пользователя для подключения и открыть ему доступ в модуле OpenVPN

VPN-сервер	Настройки	Пользователи	Текущие сеансы	События	Журнал
		Добавить	Удалить	Выключить	Редактировать
Имя	Логин	Ip-адреса из Vpn-сетей	Vpn-доступ	OpenVPN-доступ	
Корневая группа			<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Семья			<input type="checkbox"/>	<input type="checkbox"/>	
Долина			<input type="checkbox"/>	<input type="checkbox"/>	
Друзья			<input type="checkbox"/>	<input type="checkbox"/>	
Туве Янссон	root		<input type="checkbox"/>	<input type="checkbox"/>	
Муми-туннель	tunnel		<input type="checkbox"/>	<input checked="" type="checkbox"/> Муми-OpenVPN (10.8.0.0/24)	

3. Выгрузить сертификаты в индивидуальном модуле пользователя

Состояние Сводный отчет IP/MAC-адреса Правила и ограничения Почта и телефония Перенаправления OpenVPN Приложения Статистика >

OpenVPN-доступ для пользователя включен в Муми-OpenVPN (10.8.0.0/24)

Передать клиенту маршрут по умолчанию

Передать клиентам маршруты до сетей Удаленные сети

Передать клиентам маршруты до сетей Удаленные сети

Сертификат клиента *

Муми-OpenVPN_Муми-туннель

Сохранить Обновить Выгрузить сертификаты

4. Загрузить сертификаты на клиент

ООО "Организация" > Сертификаты						
Добавить Удалить Просмотр сертификата Импорт Экспорт		Поиск				
Название	Тип сертификата	Закрытый ключ	Создан	Действует до	Имя или адрес хоста	
Сертификаты						
Корневой сертификат [зашифрован]	CA	зашифрован	21.11.2019	21.11.2020	test.ru	
OpenVpnNetwork1_tunnel	Конечный сертификат	не зашифрован	21.11.2019	21.11.2020	tunnel	
Autogenerated Asterisk_5dd662397b8cd0.69169904	Конечный сертификат	не зашифрован	21.11.2019	22.11.2029	ics-asterisk	
Autogenerated GUI_5dd6623855b1d3.90975404	Конечный сертификат	не зашифрован	21.11.2019	22.11.2029	ics-gui	
Autogenerated MailServer_5dd66238932e16.6189339	Конечный сертификат	не зашифрован	21.11.2019	22.11.2029	ics-mail-server	



