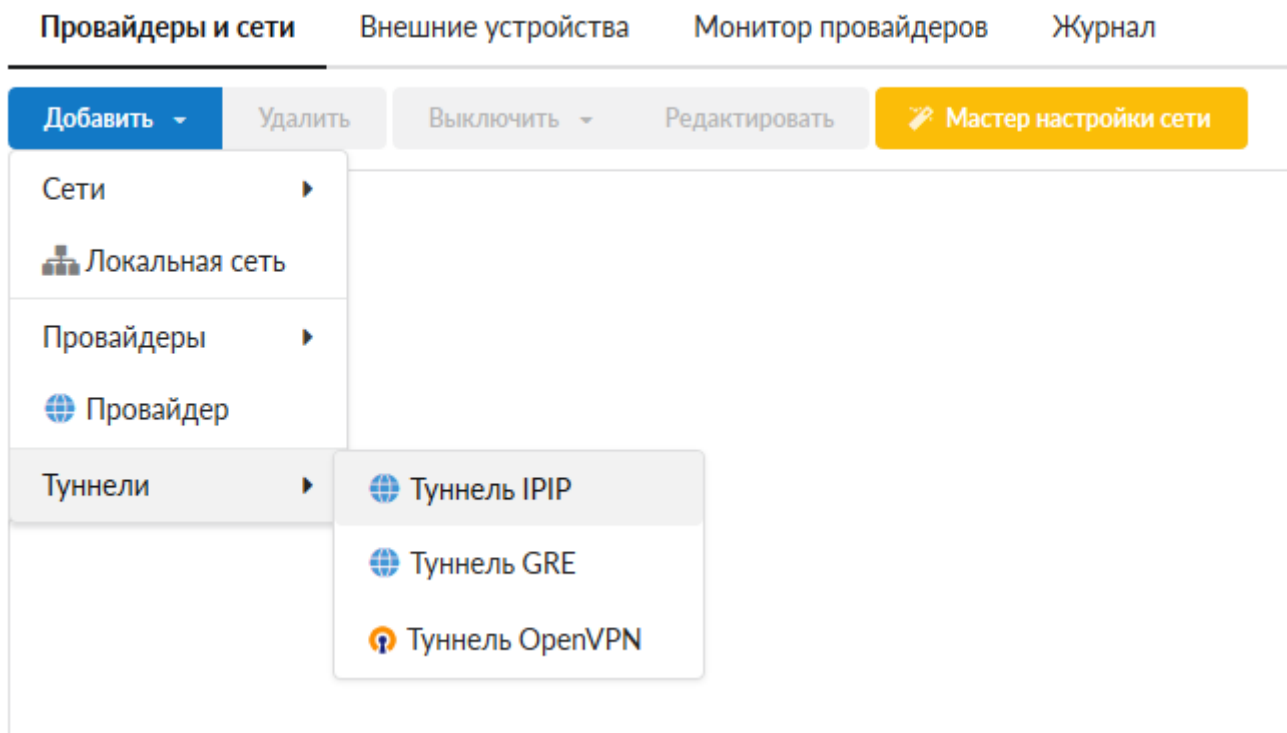


**Туннель** - это механизм позволяющий объединить две удалённые и не связанные физически сети в единую логическую структуру. Статические туннели используются для объединения нескольких локальных сетей в одну: например при объединении нескольких удалённых офисов в одну локальную сеть таким образом, чтобы 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 IP/IP или GRE протоколу.



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

<h3>Добавление туннеля IPIP</h3> <p><b>Общие настройки</b>    Настройки шифрования</p> <p>Название * Ламповый туннель</p> <p>Внешний интерфейс * Мощный провайдер (192.168.170.134/24) ✕</p> <p>Внешний ip-адрес удаленного сервера * 192.168.187.14</p> <p>Локальный ip-адрес туннеля * 10.0.0.1</p> <p>Удаленный ip-адрес туннеля * 10.0.0.2</p> <p>Локальные сети Локальные сети</p> <p>Удаленные сети Удаленные сети</p> <p>MTU Автоопределение</p> <p><input type="checkbox"/> Автоматически создавать маршрут для удаленных сетей</p> <p><input type="checkbox"/> Использовать NAT</p> <p><b>Добавить</b>    Отмена</p>	<h3>Добавление туннеля GRE</h3> <p><b>Общие настройки</b>    Настройки шифрования</p> <p>Название * Классный туннель GRE</p> <p>Внешний интерфейс * Мощный провайдер (192.168.170.134/24) ✕</p> <p>Внешний ip-адрес удаленного сервера * 192.168.187.14</p> <p>Локальный ip-адрес туннеля * 10.0.0.1</p> <p>Удаленный ip-адрес туннеля * 10.0.0.2</p> <p>Локальные сети Локальные сети</p> <p>Удаленные сети Удаленные сети</p> <p>MTU Автоопределение</p> <p><input type="checkbox"/> Автоматически создавать маршрут для удаленных сетей</p> <p><input type="checkbox"/> Использовать NAT</p> <p>Ключ GRE (не использовать)</p> <p><b>Добавить</b>    Отмена</p>
---	--

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 туннеля.

**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 IPsec

Общие настройки

**Настройки шифрования**

Использовать шифрование

Ключ шифрования

Ключ шифрования

Настройки для фазы 1:

Настройки для фазы 2:

Режим работы

main

Протокол

ESP

Алгоритм шифрования

aes256

PFS

15 - modp3072

Алгоритм хеширования

sha2\_384

Алгоритм аутентификации \*

hmac\_sha2\_384 ✕

DH-группа

15 - modp3072

Алгоритм шифрования

aes256 ✕

Время жизни \*

28800

сек.

Время жизни \*

1200

сек.

Добавить

Отмена

Защита передачи данных 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

Название \*

Лучший туннель OpenVPN

Адрес сервера \*

10.100.0.0

Протокол

UDP

Порт сервера \*

1194

Использовать NAT

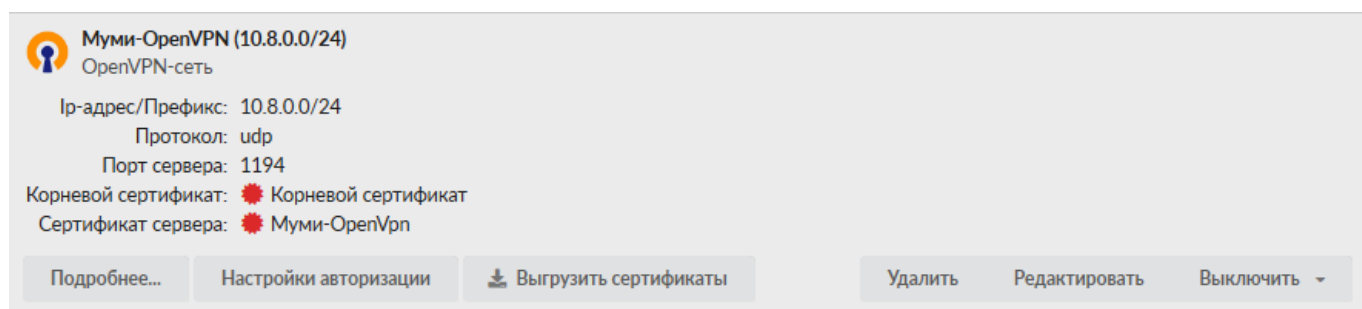
Добавить

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. Разрешить пользователю на сервере использовать 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)

!!!!!!!кртинка сертификаты2

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

Permanent link:  
<https://doc-old.a-real.ru/doku.php?id=ics70:tunnels&rev=1574338231>

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

