

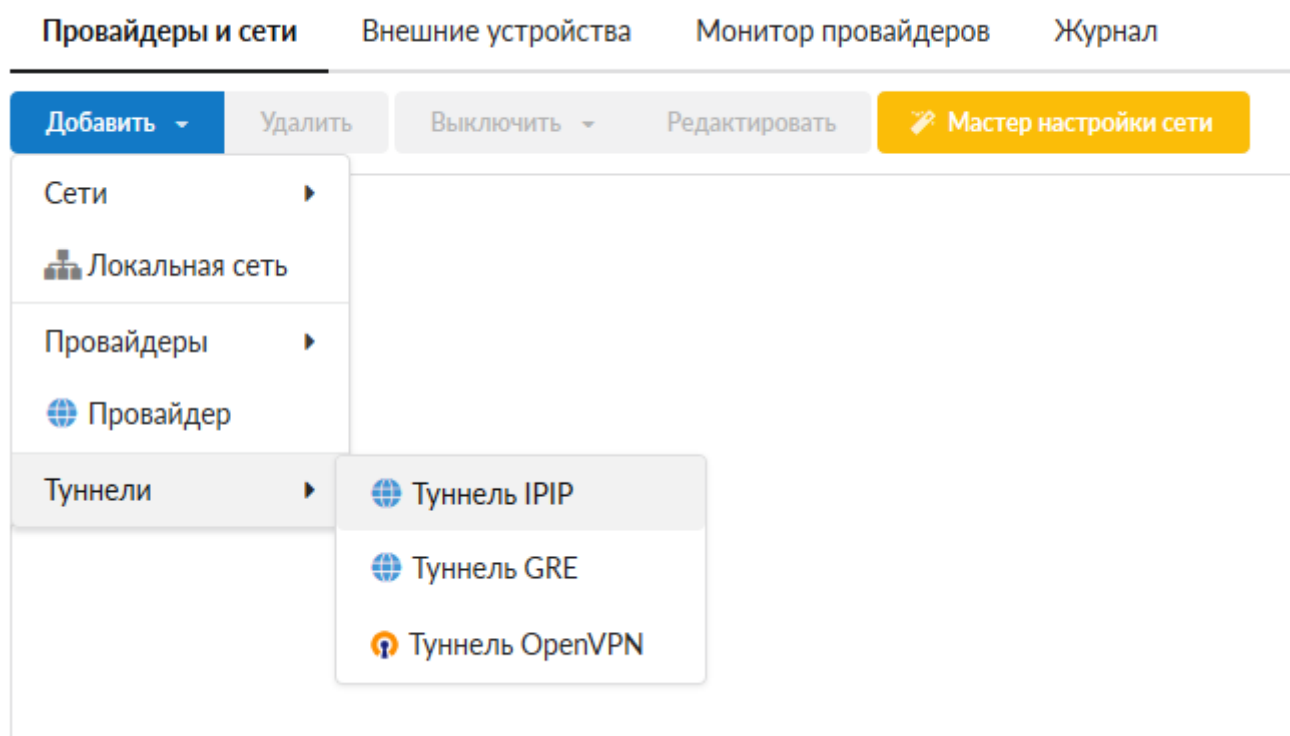
# Туннели

**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.



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

Добавление туннеля IPIP

Общие настройки

Настройки шифрования

Название \*

Ламповый туннель

Внешний интерфейс \*

Мощный провайдер (192.168.170.134/24) x

Внешний ip-адрес удаленного сервера \*

192.168.187.14

Локальный ip-адрес туннеля \*

10.0.0.1

Удаленный ip-адрес туннеля \*

10.0.0.2

Локальные сети

Локальные сети

Удаленные сети

Удаленные сети

MTU

Автоопределение

☐ Автоматически создавать маршрут для удаленных сетей

☐ Использовать NAT

Добавить

Отмена

Добавление туннеля GRE

Общие настройки

Настройки шифрования

Название \*

Классный туннель GRE

Внешний интерфейс \*

Мощный провайдер (192.168.170.134/24) x

Внешний ip-адрес удаленного сервера \*

192.168.187.14

Локальный ip-адрес туннеля \*

10.0.0.1

Удаленный ip-адрес туннеля \*

10.0.0.2

Локальные сети

Локальные сети

Удаленные сети

Удаленные сети

MTU

Автоопределение

☐ Автоматически создавать маршрут для удаленных сетей

☐ Использовать NAT

Ключ GRE

(не использовать)

Добавить

Отмена

Настройки туннелей также не отличаются. Вам необходимо указать, на каком интерфейсе будет настроен данный туннель и прописать параметры маршрутизации:

1. внешний адрес удаленного сервера

2. адрес локальной сети

3. 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.

## IP Security

**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.

**Внимание!** При использовании IPsec шифрования в туннелях IPsec и GRE трафик будет проходить через интерфейс **enc0**. Статистика на данном интерфейсе не собирается!

## OpenVPN

**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, в рамках «ИКС» настраивается OpenVPN-сеть; а все остальные - клиентами, в рамках «ИКС» OpenVPN туннели.

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"/>
Туте 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 сертификат в индивидуальном модуле пользователя, с расширением \*.ovpn

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

☐ Передать клиенту маршрут по умолчанию

IP клиента (опционально)

Передать клиентам маршруты до сетей

Передать клиентам маршруты до сетей

Удаленные сети

Удаленные сети

Сертификат клиента \*

Новая OpenVPN-сеть\_Администратор

Сохранить

Обновить

Выгрузить сертификаты

4. Информацию из скаченного файла (\*.ovpn) необходимо разбить на 3 файла (ca.crt, client.crt, client.key). В файл ca.crt поместить информацию содержащуюся между тегами <ca></ca>. Аналогично и для файлов client.crt и client.key помещаем информацию между тегами <cert></cert> и <key></key> соответственно. Далее импортируем корневой сертификат, а затем клиентский с указанием ключа на клиентском сервере.

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

Защита

Антивирус ClamAV

Антивирус Касперского

Антивирус Касперского

Веб-фильтр Касперского

Веб-фильтр SkyDNS

Межсетевой экран

Web Application Firewall

Application Firewall

Детектор атак Suricata

DLP

Контейнт-фильтр

Fail2ban

Сертификаты

IPsec

ООО "Организация" > Сертификаты

Администратор 137

Добавить Удалить Просмотр сертификата Импорт Экспорт

Поиск

Название	Тип сертификата	Закрытый ключ	Создан	Действует до	Имя или адрес хоста
Сертификаты					
Корневой сертификат	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_5dd66238932e16.61893393	Конечный сертификат	не зашифрован	21.11.2019	22.11.2029	ics-mail-server

5. После этого импортированные сертификаты можно будет выбрать на вкладке «Шифрование» при создании туннеля OpenVPN (поле «Ключ TLS авторизации» необходимо заполнить, содержимым файла \*.ovpn, а именно информацией между тегами <tls-auth></tls-auth>)

Добавление туннеля OpenVPN

Основные настройки

Шифрование и сертификаты

Алгоритм шифрования

Алгоритм хеширования

AES-256-CBC

SHA256

☐ Включить сжатие LZO

link-MTU \*

1500

Корневой сертификат

Сертификат клиента

Корневой сертификат

OpenVpnNetwork1\_tunnel

Ключ TLS авторизации

```
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
7dbb7d87c3b7e3b9745211888bcbb9ef
9524ae4cc6876bf37255ef390a339c48
```

Сохранить

Отмена

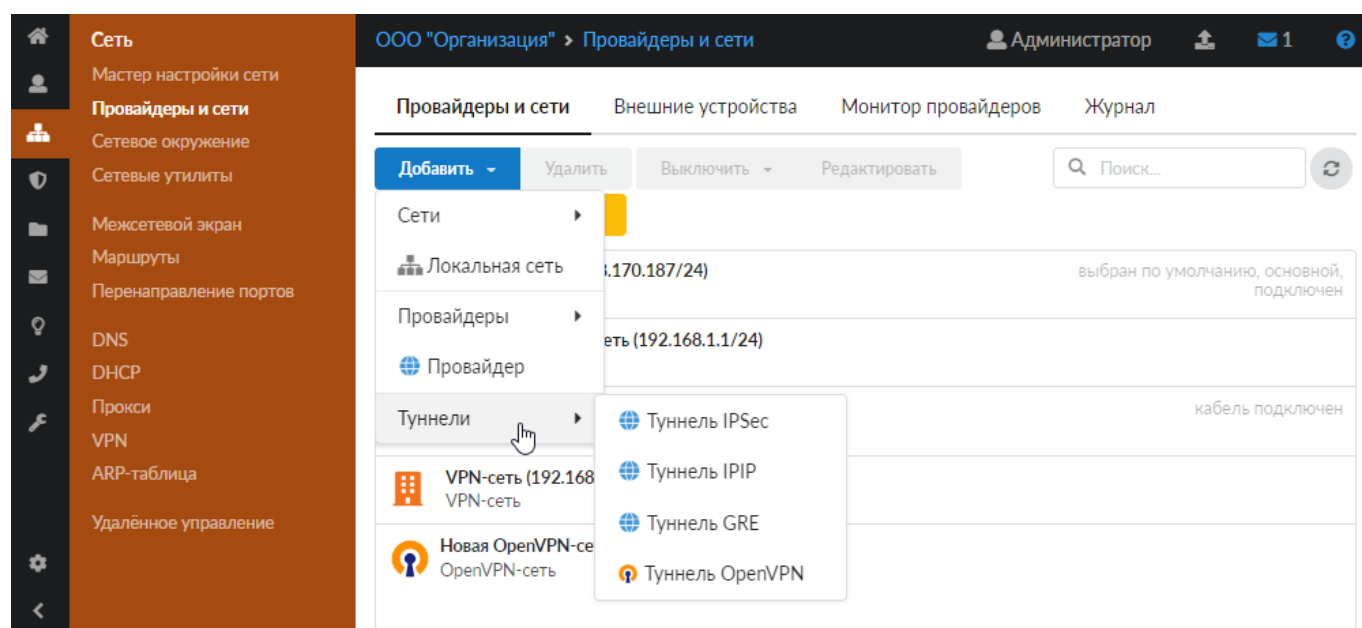
## Туннель IPsec

В ИКС можно настроить подключение между серверами IPsec-туннелем, в котором IPsec

работает в туннельном режиме. Особенностью данного туннеля является то, что он считается активным только до тех пор, пока между локальными и удаленными сетями туннеля происходит обмен трафиком. При отсутствии такого трафика в течение 8 часов туннель объявляется неактивным, с соответствующим статусом туннеля (время можно задать в настройках шифрования).

Чтобы добавить туннель IPsec, выполните следующие действия:

1. Нажмите кнопку **«Добавить»** и выберите **«Сети > Туннели > Туннель IPsec»**.



2. На вкладке **«Общие настройки»** введите **название** туннеля.
3. Выберите **внешний интерфейс**.
4. Введите в соответствующих полях следующие **адреса**: внешний IP-адрес удаленного сервера, локальные сети, удаленные сети.

## Добавление туннеля IPSec

Общие настройки


Настройки шифрования

Настройки мониторинга

Название \*

Новый туннель IPSec

Внешний интерфейс \*

 Новый провайдер (192.168.17.108/24) ✕

Внешний ip-адрес удаленного сервера \*

192.168.1.1

Локальные сети \*

192.168.17.187 ✕

Удаленные сети \*

192.168.17.108/24 ✕

Добавить

Отмена

5. На вкладке «**Настройки шифрования**» можно установить параметры шифрования IPSec.

**Внимание!** Данную процедуру необходимо произвести на обоих концах туннеля, в противном случае передача данных работать не будет.



## Добавление туннеля IPSec

Общие настройки

Настройки шифрования

Настройки мониторинга

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

6. На вкладке «**Настройки мониторинга**» можно установить **флаги**:
- «Проверять наличие пинга внешнего IP-адреса удаленного сервера» — проверка, отвечает ли на ICMP-запросы внешний адрес удаленного сервера, который указан в общих настройках туннеля. Если пинг не будет проходить, в статусе туннеля отобразится соответствующее уведомление;
  - «Проверять наличие пинга удаленной сети» — позволяет задать пинг до IP-адреса в удаленной сети с указанием в качестве источника IP-адрес ИКС из локальной сети. Таким образом, если пинг будет проходить успешно, статус туннеля всегда будет «Подключен». При установке флага выберите локальную сеть и введите IP-адрес удаленной локальной сети;
  - «Проверять доступность серверов» — при установке флага укажите серверы, доступность которых будет проверяться.

По умолчанию все флаги сняты.

## Добавление туннеля IPSec

Общие настройки

Настройки шифрования

Настройки мониторинга

☒ Проверять наличие пинга внешнего ip-адреса удаленного сервера☐ Проверять наличие пинга удаленной сети

Локальная сеть \*

Ip-адрес удаленной локальной сети \*

☐ Проверять доступность серверов

Добавить

Отмена

7. Нажмите «**Добавить**» — новый туннель появится в списке.

8. Аналогичные настройки необходимо произвести на другом конце туннеля.

**Внимание!** Для корректной работы туннеля необходимо, чтобы в межсетевом экране ИКС был разрешен трафик от внешнего удаленного адреса, а также разрешен трафик от локальных удаленных сетей, если это необходимо.

**Важно!** Удаленный сервер, с которым ИКС устанавливает соединение, не должен находиться за NAT, иначе соединение не будет работать. Данное ограничение будет устранено в ИКС версии 7.2.

From:

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

Permanent link:

<https://doc-old.a-real.ru/doku.php?id=ics70:tunnels>

Last update: 2020/07/23 12:47

