

Руководство пользователя

Настройка туннелей на роутерах iRZ



Содержание

| | |
|---|-----------|
| 1. Введение | 3 |
| 1.1. Описание документа | 3 |
| 1.2. Версия встроенного обеспечения | 3 |
| 1.3. Предупреждения | 3 |
| 2. PPTP Client | 4 |
| 3. L2TPv2 Client | 6 |
| 4. OpenVPN туннели | 8 |
| 4.1. OpenVPN Layer 2: dev TAP | 8 |
| 4.1.1. Пример настройки туннеля без аутентификации (Authentication method: None) | 9 |
| 4.1.2. Пример настройки туннеля с аутентификацией по ключу (Authentication method: Shared Secret) | 12 |
| 4.1.3. Пример настройки туннеля с аутентификацией по протоколу TLS, когда роутер выступает в роли сервера OpenVPN | 14 |
| 4.1.4. Пример настройки туннеля с аутентификацией по протоколу TLS, когда роутер выступает в роли клиента OpenVPN | 16 |
| 4.2. OpenVPN Layer 3: dev TUN | 18 |
| 4.2.1. Пример настройки туннеля без аутентификации (Authentication method: None) | 19 |
| 4.2.2. Пример настройки туннеля с аутентификацией по ключу (Authentication method: Shared Secret) | 22 |
| 4.2.3. Пример настройки туннеля с аутентификацией по протоколу TLS, когда роутер выступает в роли сервера OpenVPN | 24 |
| 4.2.4. Пример настройки туннеля с аутентификацией по протоколу TLS, когда роутер выступает в роли клиента OpenVPN | 26 |
| 5. GRE туннели | 28 |
| 5.1. Настройка GRE туннеля уровня L2 | 28 |
| 5.2. Настройка GRE туннеля уровня L3 | 31 |
| 6. IPsec туннели (только для роутеров серии R4, R2) | 34 |
| 7. DMVPN / NHRP туннели (только для роутеров серии R4, R2) | 38 |
| 8. EoIP туннели | 42 |
| 9. L2TPv3 туннели | 44 |
| 10. IRZ Atunnel (только для роутеров серии R4, R2) | 46 |
| 11. Термины и сокращения | 47 |
| 11.1. Сетевые технологии | 47 |
| 11.2. Технология OpenVPN | 49 |
| 12. Контакты | 51 |

1. Введение

1.1. Описание документа

Данный документ содержит примеры корректной конфигурации сетевых служб PPTP Client, L2TPv2 Client, OpenVPN Tunnel, GRE Tunnels, DMVPN/NHRP, EoIP Tunnels, L2TPv3 Tunnels, IPsec Tunnels в решениях, построенных на базе роутеров iRZ. Для получения информации о работе самих устройств смотрите соответствующее руководство пользователя. Для получения информации о веб-интерфейсе роутеров смотрите документ «Руководство пользователя. Средства управления и мониторинга на роутерах iRZ».

| Версия документа | Дата публикации |
|------------------|--|
| 2.1 | 14.03.2019 (Основной документ) |
| 2.2 | 24.12.2019 (Изменения в разделе L2TPv2) |
| 2.3 | 18.06.2021 (Переход на встроенное ПО версии v20.1, изменения в разделах DMVPN/NHRP туннели, IPsec туннели) |
| 2.4 | 26.08.2021 (Проверка состояния соединения для PPTP и L2TPv2 туннелей) |
| 2.5 | 01.09.2021 (Переход на встроенное ПО версии v20.2) |

1.2. Версия встроенного обеспечения

Актуальная (текущая) версия встроенного ПО

- роутеры серии R0: R0-v20.2 (2021-08-23)
- роутеры серии R2: R2-v20.1 (2021-08-23)
- роутеры серии R4: R4-v20.1 (2021-08-23)

1.3. Предупреждения

Отклонение от рекомендованных параметров и настроек может привести к непредсказуемым последствиям и значительным издержкам как в процессе пусконаладки вычислительного комплекса, так и во время эксплуатации production-версии вычислительного комплекса в реальных условиях.



Прежде чем вносить любые изменения в настройки оборудования, устанавливаемого на объекты, настоятельно рекомендуется проверить работоспособность всех параметров новой конфигурации на тестовом стенде. Также не следует ограничиваться синтетическими тестами, а максимально реалистично воспроизвести условия, в которых будет эксплуатироваться оборудование.

2. PPTP Client

Туннель PPTP представлен на роутерах iRZ в виде клиентской части. Для подключения к серверу PPTP необходимо указать адрес сервера в виде IP адреса или его доменного имени, логин и пароль клиентского доступа и выбрать тип аутентификации.

Для сохранения выполненных настроек, используйте кнопку **Save**.



При переходе на другие страницы разделов все выполненные, но не сохраненные настройки будут сброшены!

| Status | Network | VPN / Tunnels | Services |
|--------|---------|---------------|----------|
|--------|---------|---------------|----------|

| |
|--------------------|
| PPTP Client |
| L2TPv2 Client |
| OpenVPN Tunnel |
| GRE Tunnels |
| DMVPN / NHRP |
| EoIP Tunnels |
| L2TPv3 Tunnels |
| IPSec Tunnels |
| iRZ ATunnel |

Enable PPTP Client

Server

Use as default route

Username

Password

Firewall Zone

Use MPPE (MS-CHAP-V2 auth)

Authentication Type

Additional Options

Ping Address

Ping Interval (sec)

Ping Attempts

Рис. 1. Пример интерфейса PPTP Client

Для авторизации на сервере представлены следующие распространенные типы аутентификации для PPTP туннеля: EAP, PAP, CHAP и MPPE (MS-CHAP-V2). Значение Any в поле Authentication Type позволяет договариваться с сервером PPTP о методе аутентификации в автоматическом режиме.

Проверка состояния соединения

Предусмотрена проверка состояния соединения при помощи отправки пакетов (ICMP) на указанный адрес.

В поле **Ping Address** указывается IP-адрес или доменное имя сервера для проверки работы соединения. Можно указать несколько IP-адресов или доменов через пробел. В поле **Ping Interval** задается периодичность запуска пинга (в секундах). В поле **Ping Attempts** указывается количество неудачных попыток подряд, после чего соединение будет считаться деградировавшим.

- Если соединение установлено и передача данных происходит корректно, туннель работает как обычно.
- Если при установленном соединении количество неудачных попыток **Ping Attempts** достигло заданного, роутер инициирует перезагрузку данного интерфейса (туннель будет построен заново).

3. L2TPv2 Client

Туннель L2TP версии 2 на роутерах представлен только в виде клиентской части. Для подключения к удаленному серверу необходимо указать адрес или доменное имя сервера и логин с паролем.

| Status | Network | VPN / Tunnels | Services |
|--------|---------|---------------|----------|
|--------|---------|---------------|----------|

| |
|----------------------|
| PPTP Client |
| L2TPv2 Client |
| OpenVPN Tunnel |
| GRE Tunnels |
| DMVPN / NHRP |
| EoIP Tunnels |
| L2TPv3 Tunnels |
| IPSec Tunnels |
| iRZ ATunnel |

Enable L2TPv2 Client

Server

Use as default route

Username

Password

Firewall Zone

Use MPPE (MS-CHAP-V2 auth)

Authentication Type

Additional Options

Ping Address

Ping Interval (sec)

Ping Attempts

Use IPSec Protection

IPSec Pre-Shared Key

Рис. 2. Пример интерфейса L2TPv2 Client

Чекбокс — Use as default route заставит роутер направлять весь трафик через данный туннель. В этом случае в таблице маршрутизации маршрут через данный туннель будет приоритетным. Таким образом WAN интерфейсы (такие как подключение через сотовую сеть или отдельный WAN порт) станут резервными и переключение с одного WAN порта на другой не будет приводить к разрыву туннеля, то есть его переподключению.

Чекбокс — Use MPPE (MS-CHAP-V2) заставит роутер подключаться к серверу L2TP только по указанному протоколу аутентификации.

Поле Additional Options позволяет прописывать дополнительные опции для работы туннеля.

Чекбокс — Use IPSec Protection — возможность настроить шифрование туннеля с помощью IPSec. Данный функционал разработан для взаимодействия с сетевым оборудованием Mikrotik. В поле IPSec Pre-Shared Key следует вписать ключ.

Проверка состояния соединения

Предусмотрена проверка состояния соединения при помощи отправки пакетов (ICMP) на указанный адрес.

В поле **Ping Address** указывается IP-адрес или доменное имя сервера для проверки работы соединения. Можно указать несколько IP-адресов или доменов через пробел. В поле **Ping Interval** задается периодичность запуска пинга (в секундах). В поле **Ping Attempts** указывается количество неудачных попыток подряд, после чего соединение будет считаться деградировавшим.

- Если соединение установлено и передача данных происходит корректно, туннель работает как обычно.
- Если при установленном соединении количество неудачных попыток **Ping Attempts** достигло заданного, роутер инициирует перезагрузку данного интерфейса (туннель будет построен заново).

4. OpenVPN туннели

4.1. OpenVPN Layer 2: dev TAP

В данном разделе рассматривается туннель OpenVPN типа Ethernet Bridging.

Этот тип туннеля OpenVPN характеризуется общим адресным пространством между устройствами, а маршрутизаторы, на которых создается OpenVPN, прозрачны для остальных сетевых устройств. Данный туннель создаётся на базе виртуального сетевого интерфейса TAP.

Всего четыре варианта настройки туннеля, различающиеся по методу аутентификации:

- без аутентификации (Authentication method: None);
- с аутентификацией по общему ключу (Authentication method: Shared secret);
- в роли сервера OpenVPN (Authentication method: TLS Server);
- в роли клиента OpenVPN (Authentication method: TLS Client).

При этом необходимо учитывать, что туннель может работать по двум сетевым протоколам: UDP и TCP. Для протокола TCP есть возможность работать по методу сервера, когда роутер ожидает подключения извне, так и по методу клиента, когда роутер инициирует подключение с другим сетевым устройством.

В примерах настройки используется следующая схема сети:



Рис. 3. Примеры конфигураций OpenVPN. Схема сети

4.1.1. Пример настройки туннеля без аутентификации (Authentication method: None)

Для настройки OpenVPN-туннеля с TAP (Layer 2) без аутентификации между сетевыми устройствами, в веб-интерфейсе роутера:

1. Зайдите в раздел **Network** → **OpenVPN Tunnel**;
2. Поставьте галочку напротив пункта **Enable OpenVPN tunnel**;
3. Выберите в поле **Device** значение **TAP (L2)**;
4. В поле **Authentication Method** выберите значение **None**.

Enable OpenVPN tunnel

| | |
|------------------------------|------------------------------------|
| Device | Transport Protocol |
| TAP (L2) ▼ | UDP ▼ |
| Remote | Port |
| 192.168.246.100 | 1194 |
| Authentication Method | Add to Bridge or Create New |
| None ▼ | lan ▼ |
| Ping Interval | Ping Timeout |
| 60 | 120 |
| LZO Compression | |
| Always ▼ | |
| Additional Config | |
| verb 6 | |

Save

Рис. 4. Примеры конфигураций OpenVPN. Настройка OpenVPN (без аутентификации), базовая TAP (L2)

Настройте остальные параметры на странице в зависимости от требуемой конфигурации (см. таблицы ниже).

Таблица 1. Настройки OpenVPN Tunnel → TAP (L2), основные настройки

| Поля | Описание |
|-----------------------------|---|
| Device | Выбор виртуального интерфейса (в данном примере – TAP (L2)) |
| Transport Protocol | <p>Выбор транспортного протокола:</p> <ul style="list-style-type: none"> • UDP; • TCP Server; • TCP Client. |
| Remote | IP-адрес удаленного сетевого устройства (указывается если Transport Protocol = UDP или TCP Client) |
| Port | Номер порта, через который будет работать туннель |
| Authentication Method | Метод авторизации (в данном примере – None) |
| Add to Bridge or Create New | Создание моста с локальными интерфейсами роутера (дополнительные настройки см. в таблице Примеры конфигураций OpenVPN. Настройки OpenVPN Tunnel → TAP (L2), Bridge with Interface = None) |
| Advanced Settings: | <i>Нажмите на строчку Show advanced settings, чтобы открыть доступ к настройкам</i> |
| Ping Interval | Время в секундах, через которое будут отсылаться ICMP-пакеты для проверки доступности удаленного сетевого устройства (и соответственно работы туннеля) |
| Ping Timeout | Время ожидания в секундах, через которое устройство попытается заново создать OpenVPN-туннель, если ответ от удаленного устройства не будет получен |
| LZO Compression | <p>Режим сжатия данных, проходящих через туннель:</p> <ul style="list-style-type: none"> • No- отсутствие сжатия данных • Always — всегда сжимать данные • Adaptive — адаптивное сжатие данных |

Если создать мост с LAN-портами (**Bridge with Interface = LAN**), тогда эти порты будут использоваться как интерфейсы для туннеля. Если не создавать мост (**Add to Bridge or Create New = None**), тогда в настройках необходимо будет дополнительно указать вручную адрес подсети, маску и шлюз по умолчанию, как показано на [рис. 5](#).

Таблица 2. Настройки OpenVPN Tunnel → TAP (L2), Bridge with Interface = None

| Поля | Описание |
|--------------------|--|
| Tunnel IP | IP-адрес туннеля на данном устройстве |
| Tunnel Mask | Маска IP-адреса туннеля на данном устройстве |
| Remote Subnet | IP-адрес удаленной сети (на другом конце туннеля), который необходим для создания маршрута в таблице маршрутизации |
| Remote Subnet Mask | Маска удаленной сети (на другом конце туннеля) |
| Remote Gateway | Шлюз удаленной сети (на другом конце туннеля) |

Поле **Additional Config** позволяет указывать дополнительные параметры для создания туннеля. Пункты и их расшифровка, которые указываются в данном поле, можно посмотреть на официальном сайте OpenVPN по адресу: <https://openvpn.net/index.php/open-source/documentation/howto.html#server>.

Enable OpenVPN tunnel

| | | |
|--|--|-----------------------|
| Device TAP (L2) ▼ | Transport Protocol UDP ▼ | |
| Remote 192.168.246.100 | Port 1194 | |
| Authentication Method None ▼ | Add to Bridge or Create New none ▼ | |
| Tunnel IP 10.10.10.1 | Tunnel Mask 10.10.10.2 | |
| Remote Subnet 192.168.2.0 | Remote Subnet Mask 255.255.255.0 | Remote Gateway |
| Ping Interval 60 | Ping Timeout 120 | |
| LZO Compression Always ▼ | | |
| Additional Config verb 6 | | |

Save

Рис. 5. Примеры конфигураций OpenVPN. Настройка OpenVPN (без аутентификации), Bridge with Interface = None

4.1.2. Пример настройки туннеля с аутентификацией по ключу (Authentication method: Shared Secret)

Для настройки OpenVPN-туннеля с TAP (Layer 2) с аутентификацией по общему ключу между сетевыми устройствами, в веб-интерфейсе роутера:

1. Зайдите в раздел **Network** → **OpenVPN Tunnel**;
2. Поставьте галочку напротив пункта **Enable OpenVPN tunnel**;
3. Выберите в поле **Device** значение **TAP (L2)**;
4. В поле **Authentication Method** выберите значение **Shared Secret**;
5. Добавьте заранее сгенерированный ключ в поле **Shared Secret** (см. далее).

Настройте остальные параметры на странице в зависимости от требуемой конфигурации (см. раздел [Пример настройки туннеля без аутентификации \(Authentication method: None\)](#)).

При выборе данного метода аутентификации, все настройки в окне интерфейса такие же, как в разделе [Пример настройки туннеля без аутентификации \(Authentication method: None\)](#), к ним прибавляется лишь поле **Shared Secret**, в котором указывается общий ключ. Сам ключ необходимо заранее сгенерировать и распространить на устройствах участниках (см. рисунок ниже).

Enable OpenVPN tunnel

Device
TAP (L2) ▼

Transport Protocol
UDP ▼

Remote
192.168.246.100

Port
1194

Authentication Method
Shared secret ▼

Add to Bridge or Create New
none ▼

Tunnel IP
10.10.10.1

Tunnel Mask
10.10.10.2

Shared Secret
Upload

Remote Subnet
192.168.2.0

Remote Subnet Mask
255.255.255.0

Remote Gateway

Ping Interval
60

Ping Timeout
120

LZO Compression
Always ▼

Additional Config
verb 6

Save

Рис. 6. Примеры конфигураций OpenVPN. Настройка OpenVPN (с аутентификацией по ключу)

4.1.3. Пример настройки туннеля с аутентификацией по протоколу TLS, когда роутер выступает в роли сервера OpenVPN

Для настройки OpenVPN-туннеля с TAP (Layer 2) с аутентификацией по протоколу TLS между сетевыми устройствами, при этом роутер выступает в роли OpenVPN-сервера, в веб-интерфейсе роутера:

1. Зайдите в раздел **Network** → **OpenVPN Tunnel**;
2. Поставьте галочку напротив пункта **Enable OpenVPN tunnel**;
3. Выберите в поле **Device** значение **TAP (L2)**;
4. В поле **Authentication Method** выберите значение **TLS Server**;
5. Добавьте необходимые сертификаты и ключи в поля: **CA Certificate**, **DH Parameter**, **Local Certificate**, **Local Private Key** (см. далее).

Настройте остальные параметры на странице в зависимости от требуемой конфигурации (см. раздел [Пример настройки туннеля без аутентификации \(Authentication method: None\)](#)).

При выборе данного метода аутентификации, все настройки в окне интерфейса такие же, как в разделе

[Пример настройки туннеля без аутентификации \(Authentication method: None\)](#), к ним добавляются лишь поля для указания сертификатов и ключей: **CA Certificate**, **DH Parameter**, **Local Certificate**, **Local Private Key**. Ключи и сертификаты необходимо получить либо от сертификационного центра, либо создать свой собственный сертификационный центр и создать на его основе требуемые ключи и сертификаты.

Для работы туннеля понадобятся файлы, указанные в следующей таблице.

Таблица 3. Ключи и сертификаты для аутентификации по протоколу TLS

| Поля | Файл | Описание |
|-------------------|------------|---|
| CA Certificate | ca.crt | Сертификат удостоверяющего центра |
| DH Parameter | dh1024.pem | Файл с ключом для алгоритма Диффи-Хелмана для защиты передаваемых данных от расшифровки |
| Local Certificate | server.crt | Сертификат сервера OpenVPN |
| Local Private Key | server.key | Приватный ключ сервера OpenVPN, секретный |
| TLS Auth Key | ta.key | Предустановленный ключ клиента OpenVPN, используется всеми участниками туннеля |

Полученные файлы сертификатов необходимо загрузить на роутер по кнопке Upload в соответствии с указанными в таблице полями. Пример настройки показан на рисунке ниже.

Enable OpenVPN tunnel

Device
TAP (L2) ▾

Remote
192.168.246.100

Authentication Method
TLS Server ▾

CA Certificate
Upload [x]

DH Parameter
Upload [x]

Local Certificate
Upload [x]

Local Private Key
Upload [x]

Ping Interval
60

Ping Timeout
120

LZO Compression
Always ▾

Additional Config
verb 6

Transport Protocol
UDP ▾

Port
1194

Add to Bridge or Create New
lan ▾

Save

Рис. 7. Примеры конфигураций OpenVPN. Настройка OpenVPN (с аутентификацией по протоколу TLS), роутер – сервер

При выборе протокола передачи данных в поле **Transport Protocol** следует учитывать, что по протоколу UDP туннель будет работать быстрее всего, так как при использовании протокола TCP Server роутер будет ожидать установления соединения от удаленного устройства. При выборе TCP Client (необходимо будет указать в поле **Remote** – адрес устройства) – роутер будет сам инициировать соединение с удалённым устройством.

4.1.4. Пример настройки туннеля с аутентификацией по протоколу TLS, когда роутер выступает в роли клиента OpenVPN

Для настройки OpenVPN-туннеля с TAP (Layer 2) с аутентификацией по протоколу TLS между сетевыми устройствами, при этом роутер выступает в роли OpenVPN-клиента, в веб-интерфейсе роутера:

1. Зайдите в раздел **Network** → **OpenVPN Tunnel**;
2. Поставьте галочку напротив пункта **Enable OpenVPN tunnel**;
3. Выберите в поле **Device** значение **TAP (L2)**;
4. В поле **Authentication Method** выберите значение **TLS Client**;
5. Добавьте необходимые сертификаты и ключи в поля: **CA Certificate**, **Local Certificate**, **Local Private Key**, при необходимости двойной аутентификации и наличии ta.key файла добавьте ключ в поле **TLS Auth Key** и/или укажите логин и пароль. (см. далее).

Настройте остальные параметры на странице в зависимости от требуемой конфигурации (см. раздел [Пример настройки туннеля без аутентификации \(Authentication method: None\)](#)).

При выборе данного метода аутентификации все настройки в окне интерфейса идентичны разделу [Пример настройки туннеля с аутентификацией по ключу \(Authentication method: Shared Secret\)](#), к ним прибавляются только поля для указания сертификатов и ключей: **CA Certificate**, **Local Certificate**, **Local Private Key**, при необходимости **TLS Auth Key** и/или логин и пароль. Ключи, сертификаты и логины/пароли необходимо получить либо от сертификационного центра, либо создать свой собственный сертификационный центр и создать на его основе требуемые ключи и сертификаты. Для работы туннеля понадобятся файлы, указанные в разделе [Пример настройки туннеля с аутентификацией по протоколу TLS, когда роутер выступает в роли сервера OpenVPN](#)), кроме файла с ключом для алгоритма Диффи-Хелмана. Пример настройки показан на рисунке ниже.

Enable OpenVPN tunnel

| | |
|--|--|
| Device <input type="text" value="TAP (L2)"/> | Transport Protocol <input type="text" value="UDP"/> |
| Remote <input type="text"/> | Port <input type="text" value="1194"/> |
| Authentication Method <input type="text" value="TLS Client"/> | Add to Bridge or Create New <input type="text" value="lan"/> |
| CA Certificate <input type="text" value="Upload"/> <input type="button" value="X"/> | |
| Local Certificate <input type="text" value="Upload"/> <input type="button" value="X"/> | |
| Local Private Key <input type="text" value="Upload"/> <input type="button" value="X"/> | |
| TLS Auth Key <input type="text" value="Upload"/> <input type="button" value="X"/> | |
| Username <input type="text"/> | Password <input type="text"/> |
| Ping Interval <input type="text" value="60"/> | Ping Timeout <input type="text" value="120"/> |
| LZO Compression <input type="text" value="Always"/> | |
| Additional Config <input type="text" value="verb 6"/> | |

Рис. 8. Примеры конфигураций OpenVPN. Настройка OpenVPN (с аутентификацией по протоколу TLS), роутер – клиент

4.2. OpenVPN Layer 3: dev TUN

В данном разделе рассматривается туннель OpenVPN типа Routing.

Данный тип туннеля OpenVPN характеризуется маршрутизацией пакетов между сетями на разных концах туннеля, находящимися за сетевыми устройствами, и устанавливающими туннель между собой. Данный вид туннеля создается на базе виртуального сетевого интерфейса TUN.

Всего четыре варианта настройки туннеля, различающиеся по методу аутентификации:

- без аутентификации (Authentication method: None);
- с аутентификацией по общему ключу (Authentication method: Shared secret);
- в роли сервера OpenVPN (Authentication method: TLS Server);
- в роли клиента OpenVPN (Authentication method: TLS Client).

При этом необходимо учитывать, что туннель может работать по двум сетевым протоколам: UDP и TCP. Для протокола TCP есть возможность работать по методу сервера, когда роутер ожидает подключения извне, так и по методу клиента, когда роутер инициирует подключение с другим сетевым устройством.

В примерах настройки используется следующая схема сети:



Рис. 9. Примеры конфигураций OpenVPN. Схема сети

4.2.1. Пример настройки туннеля без аутентификации (Authentication method: None)

Для настройки OpenVPN-туннеля с TUN (Layer 3) без аутентификации между сетевыми устройствами, в веб-интерфейсе роутера:

1. Зайдите в раздел Network → OpenVPN Tunnel;
2. Поставьте галочку напротив пункта Enable OpenVPN tunnel;
3. Выберите в поле Device значение TUN (L3);
4. В поле Authentication Method выберите значение None.

Enable OpenVPN tunnel

| | | | |
|------------------------------|-------------------------------------|------------------------------------|---------------|
| Device | TUN (L3) ▼ | Transport Protocol | UDP ▼ |
| Remote | <input type="text"/> | Port | 1194 |
| Authentication Method | None ▼ | Add to Bridge or Create New | lan ▼ |
| Tunnel IP | 10.10.10.1 | Remote Tunnel IP | 10.10.10.2 |
| Remote Subnet | 192.168.40.0 | Remote Subnet Mask | 255.255.255.0 |
| Ping Interval | 60 | Ping Timeout | 120 |
| LZO Compression | Always ▼ | | |
| Additional Config | <input type="text" value="verb 6"/> | | |

Save

Рис. 10. Примеры конфигураций OpenVPN. Настройка OpenVPN (без аутентификации), TUN (L3)

Настройте остальные параметры на странице в зависимости от требуемой конфигурации в соответствии с таблицами, приведенными ниже.

Таблица 4. Настройки OpenVPN Tunnel → TUN (L3), основные настройки

| Поля | Описание |
|-----------------------------|---|
| Device | Выбор виртуального интерфейса (в данном примере – TUN (L3)) |
| Transport Protocol | <p>Выбор транспортного протокола:</p> <ul style="list-style-type: none"> • UDP; • TCP Server; • TCP Client. |
| Remote | IP-адрес удаленного сетевого устройства (указывается если Transport Protocol = UDP или TCP Client) |
| Port | Номер порта, через который будет работать туннель |
| Authentication Method | Метод авторизации (в данном примере – None) |
| Add to Bridge or Create New | Создание моста с локальными интерфейсами роутера (в данном примере неактивно) |
| Advanced Settings: | <i>Нажмите на строчку Show advanced settings, чтобы открыть доступ к настройкам</i> |
| Ping Interval | Время в секундах, через которое будут отсылаться ICMP-пакеты для проверки доступности удаленного сетевого устройства (и соответственно работы туннеля) |
| Ping Timeout | Время ожидания в секундах, через которое устройство попытается заново создать OpenVPN-туннель, если ответ от удаленного устройства не будет получен |
| LZO Compression | <p>Режим сжатия данных, проходящих через туннель:</p> <ul style="list-style-type: none"> • No- отсутствие сжатия данных • Always — всегда сжимать данные • Adaptive — адаптивное сжатие данных |

Поле **Bridge with Interface** не активно в данной конфигурации, из-за типа туннеля OpenVPN с маршрутизацией.

Таблица 5. Настройки OpenVPN Tunnel → TUN (L3), Bridge with Interface = None

| Поля | Описание |
|--------------------|--|
| Tunnel IP | IP-адрес туннеля на данном устройстве * |
| Remote Tunnel IP | Удаленный IP-адрес туннеля (устройство на другом конце туннеля)* |
| Remote Subnet | IP-адрес удаленной сети (на другом конце туннеля), который необходим для создания маршрута в таблице маршрутизации |
| Remote Subnet Mask | Маска удаленной сети (на другом конце туннеля) |



* Так как туннель OpenVPN с маршрутизацией является туннелем по типу point-to-point, поэтому адреса в этих полях должны указываться с учётом маски сети /30 (255.255.255.252) и не должны совпадать с адресами локальных сетей на концах туннеля.

Поле **Additional Config** позволяет указывать конфигурационные параметры, которые роутер будет передавать, подключаясь к нему сетевому устройству. Пункты и их расшифровка, которые указываются в данном поле, можно посмотреть на официальном сайте OpenVPN по адресу: <https://openvpn.net/index.php/open-source/documentation/howto.html#server>.

4.2.2. Пример настройки туннеля с аутентификацией по ключу (Authentication method: Shared Secret)

Для настройки OpenVPN-туннеля с TUN (Layer 3) с аутентификацией по общему ключу между сетевыми устройствами, в веб-интерфейсе роутера:

1. Зайдите в раздел **Network** → **OpenVPN Tunnel**;
2. Поставьте галочку напротив пункта **Enable OpenVPN tunnel**;
3. Выберите в поле **Device** значение **TUN (L3)**;
4. В поле **Authentication Method** выберите значение **Shared Secret**;
5. Добавьте заранее сгенерированный ключ в поле **Shared Secret** (см. описание далее).

Настройте остальные параметры на странице в зависимости от требуемой конфигурации (см. раздел [Пример настройки туннеля без аутентификации \(Authentication method: None\)](#)).

При выборе данного метода аутентификации, большинство настроек в окне интерфейса такие же, как в разделе [Пример настройки туннеля без аутентификации \(Authentication method: None\)](#), к ним прибавляется поле **Shared Secret**, в котором указывается общий ключ. Сам ключ необходимо заранее сгенерировать и распространить на устройствах участниках (см. рисунок ниже).

Enable OpenVPN tunnel

| | |
|---|--|
| Device TUN (L3) ▼ | Transport Protocol UDP ▼ |
| Remote 192.168.246.100 | Port 1194 |
| Authentication Method Shared secret ▼ | Add to Bridge or Create New none ▼ |
| Tunnel IP 10.10.10.1 | Remote Tunnel IP 10.10.10.2 |
| Shared Secret Upload | |
| Remote Subnet 192.168.20inta.0 | Remote Subnet Mask 255.255.255.0 |
| Ping Interval 60 | Ping Timeout 120 |
| LZO Compression Always ▼ | |
| Additional Config verb 6 | |

Save

Рис. 11. Примеры конфигураций OpenVPN. Настройка OpenVPN (с аутентификацией по ключу)

4.2.3. Пример настройки туннеля с аутентификацией по протоколу TLS, когда роутер выступает в роли сервера OpenVPN

Для настройки OpenVPN-туннеля с TUN (Layer 3) с аутентификацией по протоколу TLS между сетевыми устройствами, при этом роутер выступает в роли OpenVPN-сервера, в веб-интерфейсе роутера:

1. Зайдите в раздел **Network** → **OpenVPN Tunnel**;
2. Поставьте галочку напротив пункта **Enable OpenVPN tunnel**;
3. Выберите в поле **Device** значение **TUN (L3)**;
4. В поле **Authentication Method** выберите значение **TLS Server**;
5. Добавьте необходимые сертификаты и ключи в поля: **CA Certificate**, **DH Parameter**, **Local Certificate**, **Local Private Key** (см. далее).

Настройте остальные параметры на странице в зависимости от требуемой конфигурации (см. раздел [Пример настройки туннеля без аутентификации \(Authentication method: None\)](#)).

При выборе данного метода аутентификации, большинство настроек в окне интерфейса такие же, как в разделе [Пример настройки туннеля без аутентификации \(Authentication method: None\)](#), к ним прибавляются поля для указания сертификатов и ключей: **CA Certificate**, **DH Parameter**, **Local Certificate**, **Local Private Key**. Необходимые ключи и сертификаты следует получить либо от сертификационного центра, либо создать свой собственный сертификационный центр и создать на его основе требуемые ключи и сертификаты.

Для работы туннеля понадобятся файлы, указанные в таблице приведенной ниже.

Таблица 6. Ключи и сертификаты для аутентификации по протоколу TLS

| Поля | Файл | Описание |
|-------------------|------------|---|
| CA Certificate | ca.crt | Сертификат удостоверяющего центра |
| DH Parameter | dh1024.pem | Файл с ключом для алгоритма Диффи-Хелмана для защиты передаваемых данных от расшифровки |
| Local Certificate | server.crt | Сертификат сервера OpenVPN |
| Local Private Key | server.key | Приватный ключ сервера OpenVPN, секретный |

Полученные файлы сертификатов необходимо загрузить на роутер по кнопке Upload в соответствии с указанными в таблице полями. Пример настройки показан на рисунке ниже.

Enable OpenVPN tunnel

| | |
|--|--|
| Device TUN (L3) ▾ | Transport Protocol UDP ▾ |
| Remote 192.168.246.100 | Port 1194 |
| Authentication Method TLS Server ▾ | Add to Bridge or Create New none ▾ |
| Tunnel IP 10.10.10.1 | Remote Tunnel IP 10.10.10.2 |
| CA Certificate Upload [x] | |
| DH Parameter Upload [x] | |
| Local Certificate Upload [x] | |
| Local Private Key Upload [x] | |
| Remote Subnet 192.168.20.0 | Remote Subnet Mask 255.255.255.0 |
| Ping Interval 60 | Ping Timeout 120 |
| LZO Compression Always ▾ | |
| Additional Config verb 6 | |

Save

Рис. 12. Примеры конфигураций OpenVPN. Настройка OpenVPN (с аутентификацией по протоколу TLS), роутер – сервер

4.2.4. Пример настройки туннеля с аутентификацией по протоколу TLS, когда роутер выступает в роли клиента OpenVPN

Для настройки OpenVPN-туннеля с TUN (Layer 3) с аутентификацией по протоколу TLS между сетевыми устройствами, при этом роутер выступает в роли OpenVPN-клиента, в веб-интерфейсе роутера:

1. Зайдите в раздел **Network** → **OpenVPN Tunnel**;
2. Поставьте галочку напротив пункта **Enable OpenVPN tunnel**;
3. Выберите в поле **Device** значение **TUN (L3)**;
4. В поле **Authentication Method** выберите значение **TLS Client**;
5. Добавьте необходимые сертификаты и ключи в поля: **CA Certificate**, **Local Certificate**, **Local Private Key**, а при необходимости двойной аутентификации и наличии ta.key файла, добавьте ключ в поле **TLS Auth Key** и/или укажите логин и пароль.

Настройте остальные параметры на странице в зависимости от требуемой конфигурации (см. раздел [Пример настройки туннеля без аутентификации \(Authentication method: None\)](#)).

При выборе данного метода аутентификации, большинство настроек в окне интерфейса такие же, как в разделе [Пример настройки туннеля без аутентификации \(Authentication method: None\)](#), к ним прибавляются лишь поля для указания сертификатов и ключей: **CA Certificate**, **Local Certificate**, **Local Private Key**, при необходимости **TLS Auth Key** и/или логин и пароль. Ключи, сертификаты, логины/пароли необходимо получить либо от сертификационного центра, либо создать свой собственный сертификационный центр и создать на его основе требуемые ключи и сертификаты. Для работы туннеля понадобятся файлы, указанные в разделе [Пример настройки туннеля с аутентификацией по протоколу TLS, когда роутер выступает в роли сервера OpenVPN](#)), кроме файла с ключом для алгоритма Диффи-Хелмана. Пример настройки показан на рисунке ниже.

Enable OpenVPN tunnel

| | |
|--|---|
| Device <input type="text" value="TUN (L3)"/> | Transport Protocol <input type="text" value="UDP"/> |
| Remote <input type="text" value="192.168.246.100"/> | Port <input type="text" value="1194"/> |
| Authentication Method <input type="text" value="TLS Client"/> | Add to Bridge or Create New <input type="text" value="lan"/> |
| Tunnel IP <input type="text" value="10.10.10.1"/> | Remote Tunnel IP <input type="text" value="10.10.10.2"/> |
| CA Certificate <input type="text" value="Upload"/> <input type="button" value="X"/> | |
| Local Certificate <input type="text" value="Upload"/> <input type="button" value="X"/> | |
| Local Private Key <input type="text" value="Upload"/> <input type="button" value="X"/> | |
| TLS Auth Key <input type="text" value="Upload"/> <input type="button" value="X"/> | |
| Username <input type="text" value="test"/> | Password <input type="text" value="...."/> |
| Remote Subnet <input type="text" value="192.168.20.0"/> | Remote Subnet Mask <input type="text" value="255.255.255.0"/> |
| Ping Interval <input type="text" value="60"/> | Ping Timeout <input type="text" value="120"/> |
| LZO Compression <input type="text" value="Always"/> | |
| Additional Config <input type="text" value="verb 6"/> | |

Рис. 13. Примеры конфигураций OpenVPN. Настройка OpenVPN (с аутентификацией по протоколу TLS), роутер – клиент

5. GRE туннели

5.1. Настройка GRE туннеля уровня L2

В примерах настройки используется следующая схема сети:

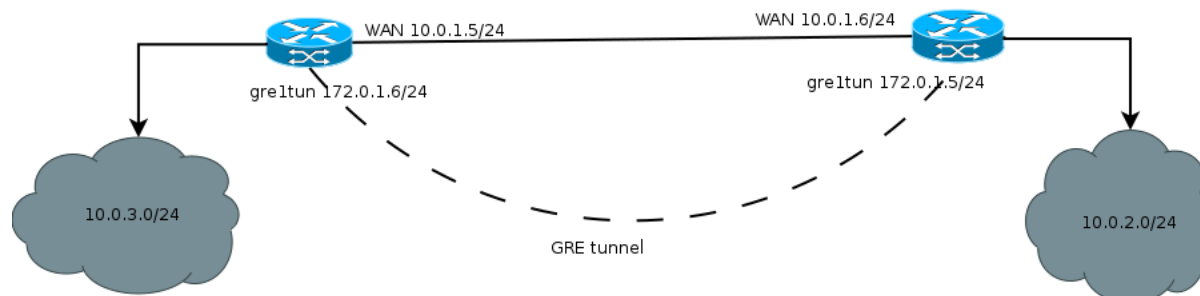


Рис. 14. Примеры конфигураций GRE. Схема сети

Для настройки GRE-туннеля уровня L2, в веб-интерфейсе роутера (см. рисунок ниже):

1. Зайдите в раздел **Network** → **Local Network**;
2. Укажите IP-адрес локального пользователя в поле **IP**;
3. Укажите маску сети в поле **Mask**;

| | | |
|---|----------------|--|
| Local Network (lan) Remove | | |
| CPU port | VLAN ID | Switch Ports |
| ETH0 | 1 | <input checked="" type="checkbox"/> PORT1 <input checked="" type="checkbox"/> PORT2 <input checked="" type="checkbox"/> PORT3 <input type="checkbox"/> PORT4 |
| IP | Mask | MAC |
| 10.0.3.1 | 255.255.255.0 | f0:81:af:00:8f:64 |
| | | Add VLAN Save |

Рис. 15. Примеры конфигураций Local Network. Настройка локальной сети

Далее необходимо настроить WAN-порт роутера (см. следующий рисунок):

4. Зайдите в раздел **Network** → **Wired Internet**;
5. Укажите тип подключения в поле **Connection Type** (**Static** – статический адрес, **DHCP** – адрес

Wired Internet (wan66) Remove

| | | |
|--|--|--|
| CPU Port | VLAN ID | Switch Ports |
| <input type="text" value="ETH0"/> | <input type="text" value="66"/> | <input type="checkbox"/> PORT1 <input type="checkbox"/> PORT2 <input type="checkbox"/> PORT3 <input checked="" type="checkbox"/> PORT4 |
| Connection Type | MAC | |
| <input type="text" value="Static"/> | <input type="text" value="Leave blank to use hardware default"/> | |
| IP | Mask | Gateway |
| <input type="text" value="10.0.1.5"/> | <input type="text" value="255.255.252.0"/> | <input type="text" value="10.0.1.6"/> |
| Ping Address | Ping Interval (sec) | Ping Attempts |
| <input type="text" value="Enter address to check connection"/> | <input type="text" value="Default 30 seconds"/> | <input type="text" value="Default 3 times"/> |

Рис. 16. Примеры конфигураций Wired Internet. Настройка WAN

Далее необходимо настроить GRE-туннель (см. следующий рисунок):

6. Зайдите в раздел **VPN/Tunnels** → **GRE Tunnels**;
7. Добавьте новый туннель, нажав на кнопку **Add Tunnel**;
8. Введите имя туннеля (на выбор пользователя) в поле **Name**;
9. Выберите локальный интерфейс, через который будет работать туннель в поле **Local Address**;
10. Укажите IP-адрес порта удаленного устройства, с которым будет построен туннель, в поле **Remote Address**;
11. Выберите на каком уровне будет работать туннель в поле **Network Type** (в данном примере рассматривается **L2**);
12. Выберите с каким **LAN** интерфейсом будет создан bridge или задайте отдельную сеть для GRE-туннеля, выбрав значение в поле **Add to Bridge or Create New** (если значение = **LAN**, то дополнительных настроек не требуется, если значение = **<new network>**, то необходимо будет указать IP-адрес пользовательского интерфейса в поле **Tunnel IP** и маску сети в поле **Tunnel Mask**);
13. Выберите к какой зоне **Firewall** необходимо отнести туннель (к зоне **Lan** или зоне **WAN**), выбрав значение в поле **Firewall Zone** (правила можно настроить вручную в разделе **Services** → **Firewall**);
14. При необходимости укажите ключ туннеля — **GRE key** (данный пункт чаще всего необходим если вы устанавливаете несколько таких туннелей с одним удаленным узлом).
15. При необходимости поставьте устройству запрет на фрагментацию (разделение) пакета на маршруте следования, поставив галочку напротив пункта **Don't fragment**.

Create new GRE

Name

Local Address

Remote Address

Network Type

Add to Bridge or Create New

Tunnel IP

Tunnel Mask

GRE key

Firewall Zone

Don't Fragment packets

Рис. 17. Примеры конфигураций GRE. Настройка GRE-туннеля

5.2. Настройка GRE туннеля уровня L3

В примерах настройки используется следующая схема сети:

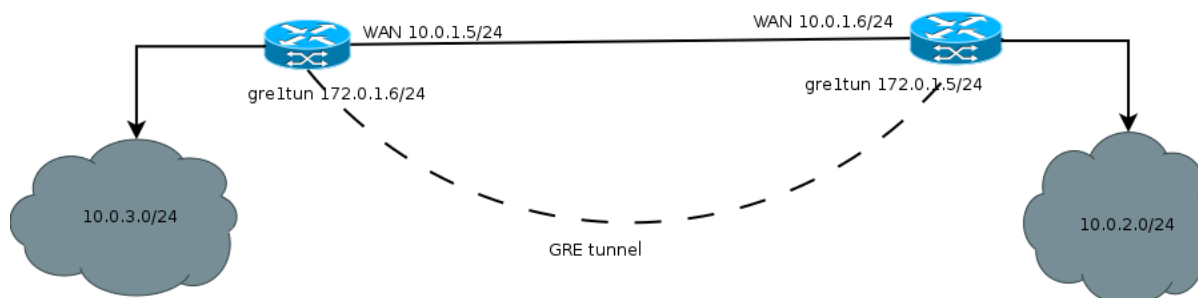


Рис. 18. Примеры конфигураций GRE. Схема сети

Для настройки GRE-туннеля уровня L3, в веб-интерфейсе роутера (см. рисунок ниже):

1. Зайдите в раздел Network → Local Network;
2. Укажите IP-адрес локального пользователя в поле IP;
3. Укажите маску сети в поле Mask;

Local Network (lan) Remove

| | | |
|-----------------|----------------|--|
| CPU port | VLAN ID | Switch Ports |
| ETH0 | 1 | <input checked="" type="checkbox"/> PORT1 <input checked="" type="checkbox"/> PORT2 <input checked="" type="checkbox"/> PORT3 <input type="checkbox"/> PORT4 |
| IP | Mask | MAC |
| 10.0.3.1 | 255.255.255.0 | f0:81:af:00:8f:64 |

Add VLAN Save

Рис. 19. Примеры конфигураций GRE. Настройка локальной сети

Далее необходимо настроить WAN-порт роутера (см. рисунок ниже):

4. Зайдите в раздел Network → Wired Internet;
5. Укажите тип подключения в поле Connection Type (Static – статический адрес, DHCP – адрес получаемый по DHCP);

Wired Internet (wan66) Remove

| | | |
|--|--|--|
| CPU Port | VLAN ID | Switch Ports |
| <input type="text" value="ETH0"/> | <input type="text" value="66"/> | <input type="checkbox"/> PORT1 <input type="checkbox"/> PORT2 <input type="checkbox"/> PORT3 <input checked="" type="checkbox"/> PORT4 |
| Connection Type | MAC | |
| <input type="text" value="Static"/> | <input type="text" value="Leave blank to use hardware default"/> | |
| IP | Mask | Gateway |
| <input type="text" value="10.0.1.5"/> | <input type="text" value="255.255.252.0"/> | <input type="text" value="10.0.1.6"/> |
| Ping Address | Ping Interval (sec) | Ping Attempts |
| <input type="text" value="Enter address to check connection"/> | <input type="text" value="Default 30 seconds"/> | <input type="text" value="Default 3 times"/> |

Рис. 20. Примеры конфигураций GRE. Настройка WAN

Далее необходимо настроить GRE-туннель (см. рисунок ниже):

6. Зайдите в раздел **VPN/Tunnels** → **GRE Tunnels**;
7. Добавьте новый туннель, нажав на кнопку **Add Tunnel**;
8. Введите имя туннеля (на выбор пользователя) в поле **Name**;
9. Выберите интерфейс, через который будет работать туннель в поле **Local Address**;
10. Укажите IP-адрес порта удаленного устройства, с которым будет построен туннель, в поле **Remote Address**;
11. Выберите на каком уровне будет работать туннель в поле **Network Type** (в данном примере рассматривается L3);
12. Укажите IP-адрес интерфейса в поле **Tunnel IP**; а также его маску в поле **Tunnel Mask** при необходимости, если не указывать — маска будет назначена автоматически и будет равна /32.
13. Выберите правило работы межсетевого экрана (firewall), если необходимо, выбрав значение в поле **Firewall Zone** (правила можно настроить вручную в разделе **Services** → **Firewall**);
14. При необходимости, поставьте устройству запрет на фрагментацию (разделение) пакета на маршруте следования, поставив галочку напротив пункта **Don't fragment**.

Edit tunnel: Unnamed (gre1)

Name

Name

Local Address

wan

Remote Address

10.0.1.6

Network Type

L3 layer

Tunnel IP

172.0.1.6

Tunnel Mask

Netmask

GRE key

Leave blank if not used

Firewall Zone

lan

Don't Fragment packets

Close

Apply Changes

Рис. 21. Примеры конфигураций GRE. Настройка GRE-туннеля

6. IPsec туннели (только для роутеров серии R4, R2)

Для создания IPsec-туннеля на роутере должна быть настроена локальная сеть и порты WAN, затем в веб-интерфейсе роутера (см. рисунок ниже):

1. Добавьте новый IPsec-туннель, нажав на кнопку **Add Tunnel**;

IPSec tunnels



Рис. 22. Примеры конфигураций IPsec. Настройка IPsec-туннеля

2. Далее необходимо настроить параметры туннеля (см. далее);
3. Введите описание туннеля (на выбор пользователя) в поле **Description**;
4. Выберите физический интерфейс, через который будет работать туннель, выбрав значение в поле **Source Address (Default** – через интерфейс, являющийся на данный момент активным WAN-портом, или через другие интерфейсы: **SIM1, SIM2, WAN**);
5. Укажите IP-адрес порта удаленного устройства, с которым будет построен туннель, в поле Remote Address;
6. Укажите интервал в секундах, через который будет определяться доступность узла на противоположном конце туннеля, указав значение в поле **Dead Peer Detect (0** – отключение данной функции);
7. Укажите локальный идентификатор и идентификатор удаленной стороны в полях **Local Identifier** и **Remote Identifier** соответственно;
8. Поле **Key Exchange Mode** предназначено для переключения между первой и второй версиями обмена ключей при установлении туннеля;

Create new IPsec tunnel (ipsec1)

Description

Description

Source Address

<default route>

Remote Address

IP or domain name

DPD Delay (sec)

0

Local Identifier

Remote Identifier

Key Exchange Mode

ikev2

Local Subnets

| | |
|--|---|
| <input data-bbox="293 779 336 824" type="button" value="+"/> | <input data-bbox="363 779 774 824" type="text" value="Subnet Address"/> |
|--|---|

Remote Subnets

| | |
|--|--|
| <input data-bbox="849 779 892 824" type="button" value="+"/> | <input data-bbox="924 779 1334 824" type="text" value="Subnet Address"/> |
|--|--|

Phase #1

Lifetime

28800

IKE Encryption

aes256

IKE Hash

sha256

DH Group

14

Phase #2

Lifetime

3600

ESP Encryption

aes256

ESP Hash

sha1

PFS Group

Authentication Method

psk

Pre-Shared Key

Password

Close

Apply changes

Рис. 23. Примеры конфигураций IPsec. Параметры туннеля

9. Выберите режим установления соединения между участниками туннеля, выбрав значение в поле **Exchange Mode** (**Main** – основной, **Aggressive** – более активный [быстрый], но без обеспечения защиты подлинности на данном этапе). Выбор доступен только при условии **Key Exchange Mode** версии 1;
10. Настройте параметры **SAinfo** для работы IPsec SA, заполнив поля **Local Subnets** и **Remote Subnets**. В столбцах **Local Subnets** и **Remote Subnets** добавляем нужное количество адресов сетей, между которыми устанавливается туннель. Сети записываются в поля в формате CIDR.
11. Настройте фазу 1 и фазу 2, заполнив соответствующие поля в блоках **Phase #1** и **Phase #2** (см. таблицы ниже).
12. Выберите способ аутентификации узлов туннеля (см. рисунок далее), выбрав значение в поле **Authentication Method** (**psk** – по общему ключу, **pubkey** – по сертификату и ключу RSA);

Таблица 7. Параметры Phase #1 и Phase #2

Phase #1 (фаза 1)

| Поля | Описание |
|----------------|---|
| Lifetime | Время жизни ключа в секундах, создаваемого на этапе фазы. Рекомендуется устанавливать значение минимум в два раза больше, чем у фазы 2 (например, 24 часа или 86400 секунд). |
| IKE Encryption | Выбор алгоритма шифрования: AES 128, AES 192, AES 256, 3DES. |
| IKE Hash | Выбор алгоритма для проверки целостности данных: SHA-1, SHA-256, SHA-512, SHA-384, MD5. |
| DH Group | Выбор криптографического алгоритма, который позволяет двум точкам обмениваться ключами через незащищенный канал. Числа – обозначают сложность ключа, чем выше, тем надежнее ключ. |

Phase #2 (фаза 2)

| Поля | Описание |
|----------------|--|
| Lifetime | Время жизни ключа в секундах, создаваемого на этапе фазы. Рекомендуется устанавливать значение меньше, чем у фазы 1 (например, 1 час или 3600 секунд). |
| ESP Encryption | Выбор алгоритма шифрования: AES 128, AES 192, AES 256, 3DES. |
| ESP Hash | Выбор алгоритма для проверки целостности данных: SHA-1, SHA-256, SHA-384, SHA-512, MD5. |
| PFS Group | Выбор криптографического алгоритма, который удостоверяет, что ключи, используемые в фазе 2 не получены от фазы 1. Числа – обозначают сложность ключа, чем выше, тем надежнее ключ. |

Authentication Method

pubkey

CA Certificate

Upload

CA PEM certificate



Download

Local Certificate

Upload

PEM certificate



Download

Key

Upload

PEM key



Download

Рис. 24. Способ аутентификации pubkey



На оборудовании iRZ в целях безопасности для входящих подключений запрещено использование функции IPsec с параметрами: KeyExchangeMode = ikev1, Agressive mode=yes, Authentication Method = PSK.

7. DMVPN / NHRP туннели (только для роутеров серии R4, R2)

Dynamic Multipoint VPN (DMVPN) — виртуальная частная сеть с возможностью динамического создания туннелей между узлами. Роутеры iRZ для данного туннеля могут выступать только в роли Spoke- маршрутизатора.

Для создания данного туннеля необходимо в разделе **VPN/Tunnels** → **DMVPN/NHRP** нажать кнопку **Add Tunnel** и на открывшейся странице настроек (см. рисунок ниже) заполнить поля согласно таблице приведенной далее.

| | | |
|--|--|--|
| Description | Local NBMA Address | Remote NBMA Address |
| <input type="text"/> | <input type="text" value="<default>"/> | <input type="text" value="IP or domain name"/> |
| Local Tunnel Address | HUB Tunnel Address | Tunnel Netmask |
| <input type="text" value="IP address"/> | <input type="text" value="IP address"/> | <input type="text" value="ex. 255.255.255.0"/> |
| GRE key | Holding Time (sec.) | Firewall Zone |
| <input type="text" value="Leave blank if not used"/> | <input type="text" value="default 7200 sec."/> | <input type="text" value="<none>"/> |
| Ping Address | Ping Interval (sec) | Ping Attempts |
| <input type="text" value="IP address to check"/> | <input type="text" value="Default 30"/> | <input type="text" value="Default 3"/> |
| <input type="checkbox"/> No Caching <input type="checkbox"/> Allow Shortcuts | | |
| <input type="checkbox"/> HUB is Cisco | | |

Рис. 25. Страница настроек DMVPN/NHRP

Таблица 8. Настройки DMVPN/NHRP

| Поля | Описание |
|---------------------|--|
| Description | Описание или название туннеля. |
| Local NBMA Address | Локальный адрес сети - NBMA(Non Broadcast Multiple Access), необходимо выбрать один из интерфейсов роутера; значение <default> означает использование интерфейса с маршрутом по умолчанию. |
| Remote NBMA Address | Удаленный адрес NBMA — указывается только IP адрес. |
| HUB Tunnel Address | Туннельный IP адрес HUBа к которому происходит подключение. |
| Tunnel Mask | Маска сети туннеля. |

Таблица 8. Настройки DMVPN/NHRP

| | |
|----------------------|---|
| Holding Time (sec.) | Время (в секундах) в течение которого информация о соседнем NBMA хосте считается действительной. |
| Local Tunnel IP | Туннельный IP адрес данного роутера. |
| GRE key | Идентификационный ключ GRE туннеля в случае если данный функционал используется в конфигурации. |
| Firewall Zone | Зона в которой будет находится туннель и соответственно политики фаервола, которые будут применяться к данному туннелю. |
| Ping Address | Адрес проверки работоспособности туннеля (проверка доступности туннеля ICMP пакетами). |
| Ping Interval (sec) | Интервал проверки. |
| Ping Attempts | Количество попыток, по истечении которых роутер попытается переустановить туннель. |
| No Caching | Отключает кэширование информации о пирах из пересылаемых пакетов ответа на разрешение NHRP. Это можно использовать для уменьшения потребления памяти в больших подсетях NBMA. |
| Allow Shortcuts | Разрешает помещение в таблицу маршрутизации только тех префиксов, которые реально используются в данный момент времени. |
| HUB is Cisco | Данная настройка позволяет ввести ключ аутентификации в случае если хабом является оборудование компании Cisco. |
| No Unique | Флаг неуникальности ip-адреса туннеля в базе nhrp на hub-маршрутизаторе (см. рис. 26). |
| Allow Redirects | Разрешает направлять трафик напрямую между spoke маршрутизаторами в обход хаба (см. рис. 26). |
| Use IPsec Protection | Данная настройка откроет дополнительное поле с возможностью настроить шифрование туннеля с помощью IPsec туннеля (см. таблицу Настройка шифрования туннеля с помощью IPsec). |

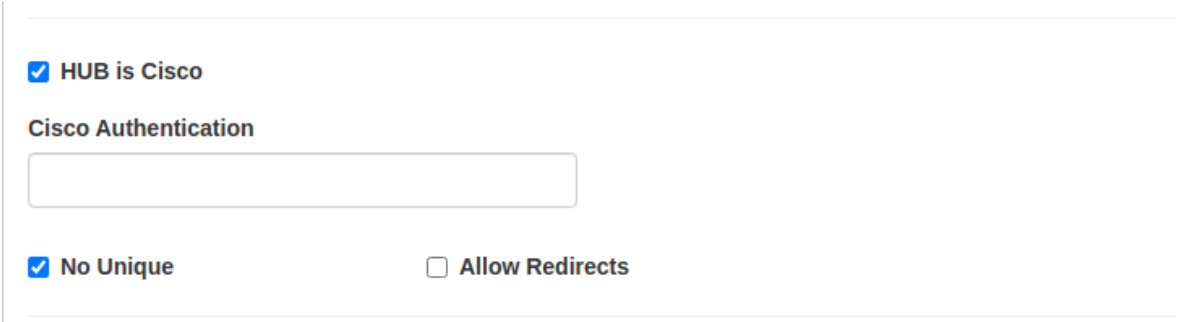


Рис. 26. Поле ввода ключа аутентификации для оборудования Cisco

Таблица 9. Настройка шифрования туннеля с помощью IPSec

| Поля | Описание |
|-----------------------|---|
| Local Identifier | Локальный идентификатор. |
| Remote Identifier | Идентификатор удаленной стороны. |
| Key Exchange Mode | Предназначено для переключения между первой и второй версиями обмена ключей. |
| Authentication Method | Способ аутентификации узлов туннеля: psk – по общему ключу, rsasig – по сертификату и ключу RSA (то же что и pubkey). |
| DPD Delay (sec.) | Интервал отправки DPD и keepalive пакетов. |
| DPD Timeout (sec.)* | Интервал по которому рвётся соединение. |
| Aggressive Mode* | Включение/отключение более активного [быстрого] режима (без обеспечения защиты подлинности). |



Редактирование DPD Timeout и Aggressive Mode возможно только в режиме IKEv1 для Key Exchange Mode.

В случае использования шифрования туннеля с помощью технологии IPSec необходимо настроить соответствующие параметры туннеля. Подробная информация о каждом параметре приведена в разделе [IPsec туннели \(только для роутеров серии R4, R2\)](#).

Use IPSec Protection

| | | | |
|---|---|------------------------------------|---------------------------------|
| Local Identifier | Remote Identifier | Key Exchange Mode | |
| <input type="text" value="IPSec identifier"/> | <input type="text" value="IPSec identifier"/> | <input type="text" value="IKEv1"/> | |
| Authentication Method | DPD Delay (sec.) | DPD Timeout (sec.) | Aggressive Mode |
| <input type="text" value="rsasig"/> | <input type="text" value="30"/> | <input type="text" value="150"/> | <input type="text" value="No"/> |

CA Certificate

Certificate

Key

| | | | |
|-------------------------------------|-----------------------------------|---|------------------------------------|
| IKE Encryption | IKE Hash | DH Group | IKE Lifetime (sec.) |
| <input type="text" value="aes128"/> | <input type="text" value="sha1"/> | <input type="text" value="1"/> | <input type="text" value="28800"/> |
| ESP Encryption | ESP Hash | PFS Group | ESP Lifetime (sec.) |
| <input type="text" value="aes128"/> | <input type="text" value="sha1"/> | <input type="text" value="<none>"/> | <input type="text" value="3600"/> |

Рис. 27. Поле настройки шифрования туннеля с помощью IPSec

Use IPSec Protection

| | | | |
|---|---|------------------------------------|---------------------------------|
| Local Identifier | Remote Identifier | Key Exchange Mode | |
| <input type="text" value="IPSec identifier"/> | <input type="text" value="IPSec identifier"/> | <input type="text" value="IKEv1"/> | |
| Authentication Method | DPD Delay (sec.) | DPD Timeout (sec.) | Aggressive Mode |
| <input type="text" value="psk"/> | <input type="text" value="30"/> | <input type="text" value="150"/> | <input type="text" value="No"/> |

Pre-Shared Key

| | | | |
|-------------------------------------|-----------------------------------|---|------------------------------------|
| IKE Encryption | IKE Hash | DH Group | IKE Lifetime (sec.) |
| <input type="text" value="aes128"/> | <input type="text" value="sha1"/> | <input type="text" value="1"/> | <input type="text" value="28800"/> |
| ESP Encryption | ESP Hash | PFS Group | ESP Lifetime (sec.) |
| <input type="text" value="aes128"/> | <input type="text" value="sha1"/> | <input type="text" value="<none>"/> | <input type="text" value="3600"/> |

Рис. 28. Поле настройки шифрования туннеля с помощью IPSec

8. EoIP туннели

Ethernet over IP (EoIP) — тип туннеля, разработанный компанией MikroTik, представляет собой Ethernet туннель точка-точка поверх IP подключения. Данный туннель создает мост между двумя роутерами как будто эти роутеры подключены друг к другу напрямую через физические ethernet порты. Такой туннель можно создавать поверх любого другого туннеля или подключения, умеющего транспортировать протокол IP. Пример настроек туннеля приведен на рисунке ниже.

Create new EoIP

The screenshot shows the 'Create new EoIP' configuration window. It contains the following fields and options:

- Name:** A text input field with the placeholder 'Name'.
- Local Address:** A dropdown menu currently showing 'loopback'.
- Remote Address:** A dropdown menu currently showing 'Only remote IP'.
- Add to Bridge or Create New:** A dropdown menu currently showing '<new network>'. Below this dropdown is a text input field for a specific address.
- Tunnel IP:** A text input field with the placeholder 'Local IP address for tunnel'.
- Tunnel Mask:** A text input field with the placeholder 'Netmask'.
- Tunnel ID:** An empty text input field.
- Firewall Zone:** A dropdown menu currently showing '<none>'.

At the bottom right, there are two buttons: 'Close' and 'Apply Changes'.

Рис. 29. Настройка EoIP-туннеля

Для создания туннеля необходимо проделать следующие шаги:

1. Зайдите в раздел **VPN / Tunnels** → **EoIP Tunnels** и создайте новый туннель кнопкой **Add Tunnel**.
2. В открывшихся настройках туннеля (см. [рис. 29](#) Настройка EoIP-туннеля) укажите имя туннеля в поле **Name**, если требуется.
3. В поле **Local Address** укажите интерфейс через который будет работать туннель.
4. В поле **Remote Address** необходимо указать адрес удаленной точки туннеля.
5. В поле **Add to Bridge or Create New** необходимо выбрать локальную сеть с которой будет создан мост или же задать отдельный адрес туннельного интерфейса.
6. В случае если в предыдущем пункте выбран вариант задания отдельного адреса для интерфейса туннеля необходимо в полях **Tunnel IP** и **Tunnel Mask** указать IP адрес и маску

сети для интерфейса туннеля.

7. Поле **Tunnel ID** предназначено для задания идентификационного номера туннеля, в случае если создается несколько туннелей с терминованием на одной удаленной точке, для того чтобы текущий роутер и удаленный могли различать пакеты разных туннелей. В случае одного туннеля данное поле можно не заполнять.
8. Поле **Firewall Zone** предназначено для ассоциации туннеля с одной из зон фаервола.

9. L2TPv3 туннели

L2TPv3 (англ. Layer 2 Tunneling Protocol — протокол туннелирования второго уровня версия 3) — в компьютерных сетях туннельный протокол, использующийся для поддержки виртуальных частных сетей.

Для настройки туннеля необходимо зайти в раздел VPN/Tunnels → L2TPv3 и добавить новый туннель по кнопке Add Tunnel.

В открывшемся окне настроек (см. рисунок ниже) заполнить поля согласно таблице приведенной далее.

Create new L2TP

Name

Local Address **Remote Address**
Add to Bridge or Create New
Tunnel IP **Tunnel Mask**
Tunnel ID **Session ID**
Firewall Zone

Рис. 30. Настройка L2TP3-туннеля

Таблица 10. Настройки L2TP3

| Поля | Описание |
|-----------------------------|--|
| Name | Название туннеля. |
| Local Address | Локальный интерфейс на роутере через который будет устанавливаться соединение. |
| Remote Address | IP-адрес удаленной сети, участвующей в туннеле. |
| Add to Bridge or Create New | Установление моста с каким-то из локальных интерфейсов (lan) роутера или создание отдельного интерфейса со своей подсетью - <new network>. |
| Tunnel IP | IP адрес туннельного интерфейса. |
| Tunnel Mask | Маска сети туннельного интерфейса. |
| Tunnel ID | ID — идентификатор туннеля. |
| Session ID | ID — идентификатор сессии. |
| Firewall Zone | Включение туннельного интерфейса в одну из зон фаервола. |

10. IRZ Atunnel (только для роутеров серии R4, R2)

Данный раздел предназначен для настройки работы роутера с iRZ SD-WAN. Более подробную информацию можно прочитать в документе «**РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ iRZ SD-WAN**» на сайте www.radiofid.ru

11. Термины и сокращения

11.1. Сетевые технологии

GSM – стандарт сотовой связи («СПС-900» в РФ);

GPRS – стандарт передачи данных в сетях операторов сотовой связи «поколения 2.5G» основанный на пакетной коммутации (до 56 Кбит/с);

EDGE – преемник стандарта GPRS, представитель «поколения 2.75G», основанный на пакетной коммутации (до 180 Кбит/с);

HSPA (HSDPA, HSUPA) – технология беспроводной широкополосной радиосвязи, использующая пакетную передачу данных и являющаяся надстройкой к мобильным сетям WCDMA/UMTS, представитель «поколения 3G» (HSUPA - до 3,75 Мбит/с, HSDPA - до 7,2 Мбит/с);

WCDMA – стандарт беспроводной сотовой связи;

3G - общее описание набора стандартов, описывающих работу в широкополосных мобильных сетях UMTS и GSM: GPRS, EDGE, HSPA;

IP-сеть – компьютерная сеть, основанная на протоколе IPv4 (Internet Protocol) - межсетевой протокол 4 версии. IP-сеть позволяет объединить для взаимодействия и передачи данных различные виды устройств (роутеры, компьютеры, сервера, а так же различное узкоспециализированное оборудование);

IP-адрес – адрес узла (компьютера, роутера, сервера) в IP-сети;

Внешний IP-адрес – IP-адрес в сети Интернет, предоставленный провайдером услуг связи в пользование клиенту на своём/его оборудовании для обеспечения прямой связи с оборудованием клиента через сеть Интернет;

Фиксированный внешний IP-адрес – внешний IP-адрес, который не может измениться ни при каких условиях (смена типа оборудования клиента и др.) или событиях (переподключение к сети провайдера и др.); единственной возможностью сменить фиксированный IP-адрес является обращение к провайдеру;

Динамический IP-адрес – IP-адрес, который может меняться при каждом новом подключении к сети;

Динамический внешний IP-адрес – внешний IP-адрес в сети Интернет, изменяющийся, как правило, в одном из следующих случаев:

- при каждом новом подключении к Интернет;
- по истечении срока аренды клиентского локального IP-адреса;
- через заданный промежуток времени;
- в соответствии с другой политикой клиентской адресации провайдера;

Локальный IP-адрес:

- IP-адрес, назначенный локальному интерфейсу роутера, как правило локальный IP-адрес должен находиться в адресном пространстве обслуживаемой роутером сети;

IP-адрес, присвоенный оборудованием Интернет-провайдера клиентскому устройству в момент подключения к Интернет; данный IP-адрес не может быть использован для получения доступа к клиентскому устройству из вне (через сеть Интернет), он позволяет только пользоваться доступом в Интернет;

Серый/частный/приватный IP-адрес – см. определение для термина "**локальный IP-адрес**";

Узел сети – объект сети (компьютерной/сотовой), способный получать от других узлов сети и передавать этим узлам служебную и пользовательскую информацию;

Клиент/клиентский узел/удаленный узел/удалённое устройство – устройство, территориально удалённое от места, либо объекта/узла, обсуждаемого в конкретно взятом контексте;

Сетевой экран (firewall) – программный аппаратный комплекс, призванный выполнять задачи защиты обслуживаемой роутером сети, её узлов, а так же самого роутера от: нежелательного трафика, несанкционированного доступа, нарушения их работы, а так же обеспечения целостности и конфиденциальности передаваемой информации на основе predetermined администратором сети правил и политик обработки трафика в обоих направлениях;

(Удалённая) командная строка, (удалённая) консоль роутера – совокупность программных средств (серверная и клиентская программы Telnet/SSH), позволяющая осуществлять управление роутером посредством консольных команд при отсутствии физического доступа к устройству;

Служебный трафик – трафик, содержащий в себе служебную информацию, предназначенную для контроля работы сети, поддержания целостности передаваемых пользовательских данных и взаимодействия сетевых служб двух и более узлов между собой;

Пользовательские данные (в сети) – информация, создаваемая или используемая оборудованием в сети пользователя, для передачи, обработки и хранения которой было разработано техническое решение;

Нежелательный трафик – трафик, не несущий полезной нагрузки, который тем не менее генерируется одним или несколькими узлами сети, тем самым создавая паразитную нагрузку на сеть;

Сетевая служба – служба, обеспечивающая решения вопросов обработки, хранения и/или передачи информации в компьютерной сети;

Сервер – этот термин может быть использован в качестве обозначения для:

- серверной части программного пакета используемого в вычислительном комплексе;
- роли компонента, либо объекта в структурно-функциональной схеме технического решения, развёртываемого с использованием роутера iRZ;
- компьютера, предоставляющего те или иные сервисы (сетевые службы, службы обработки и хранения данных и прочие);

Провайдер – организация, предоставляющая доступ в сеть Интернет;

Оператор сотовой связи – организация, оказывающая услуги передачи голоса и данных, доступа в Интернет и обслуживания виртуальных частных выделенных сетей (VPN) в рамках емкости своей сотовой сети;

Относительный URL-путь – часть строки web-адреса в адресной строке браузера, находящаяся после доменного имени или IP-адреса удалённого узла, и начинающаяся с символа косой черты (символ «/»), пример:

Исходный web-адрес: <http://192.168.1.1/index.php>

Относительный путь: /index.php

"Crossover"-патчкорд – сетевой кабель, проводники которого обжаты таким образом, что его можно использовать для прямого подключения роутера к компьютеру без необходимости использования коммутационного оборудования;

Учётная запись, аккаунт – другое название "личного кабинета" пользователя Интернет-сайта, позволяющего вносить и редактировать его личные данные, настройки;

USB-накопитель – запоминающее устройство, подключаемое к роутеру через USB-интерфейс, и используемое для сохранения/считывания служебной информации роутера; может быть использовано для резервирования настроек роутера, их восстановления, а так же для автоматической конфигурации службы OpenVPN (не сервера OpenVPN).

11.2. Технология OpenVPN

Сертификат – электронный или печатный документ, выпущенный удостоверяющим центром, для подтверждения принадлежности владельцу открытого ключа или каких-либо атрибутов;

Корневой сертификат – сертификат выданный и подписанный одним и тем же центром сертификации;

Ключ сервера – блок криптографической информации, позволяющий серверу OpenVPN подтвердить свою подлинность в момент попытки получения доступа клиентом к сети, обслуживаемой данным сервером;

Ключ клиента/пользователя – блок криптографической информации, позволяющий пользователю, либо клиентскому узлу идентифицировать себя в системе, к которой он осуществляет попытку доступа;

Топология сети – термин, позволяющий описать конфигурацию сети на разных уровнях взаимодействия информационных систем. Как правило, топология сети формируется администратором/архитектором сети исходя из поставленных задач, решаемых техническим решением, основная идея которого реализуется данной сетью;

Сетевой интерфейс – данный термин имеет несколько определений:

- Аппаратная часть роутера, позволяющая осуществлять на низких уровнях взаимодействия связь с удалёнными узлами, а так же обмениваться с ними информацией;
- Программный виртуальный объект ОС, позволяющий определить правила и порядок следования и обмена информацией между узлами компьютерной сети;

OpenVPN – открытый бесплатный программный продукт, позволяющий создать защищённую виртуальную среду передачи данных внутри IP-сети. Поскольку OpenVPN представляет из себя многофункциональный программный пакет, в различном контексте термин «OpenVPN» может иметь различные значения, самые распространённые из которых: «сервер доступа к сети OpenVPN», «клиент, позволяющий подключиться к OpenVPN-сети», «сеть, либо сектор/уровень/слой сети, подразумевающий использование ПО OpenVPN»;

OpenVPN-сеть – IP-сеть, построенная на базе сети, созданной ПО OpenVPN;

(Виртуальное) адресное пространство OpenVPN-сети – адресное пространство IP-сети OpenVPN, призванное добавить сегмент в совокупность всех сетей на пути следования пользовательских данных, то есть обеспечить чёткую декомпозицию маршрута, тем самым упрощая проектирование и обслуживание всего вычислительного комплекса, построенного на базе ПО OpenVPN в целом;

OpenVPN-клиент – см. клиентский узел;

Туннель – виртуальная сущность/технология/объект, позволяющая логически выделить конкретно взятый поток данных между двумя узлами, заключая его в отдельное от общего адресное пространство; Авторизация – процедура предоставления надлежащих прав субъекту (пользователю/участнику/клиенту/клиентскому узлу) системы после получения от него запроса на доступ к системе и прохождения проверки его подлинности (аутентификации);

Аутентификация – процедура проверки подлинности субъекта (пользователя/участника/клиента/ клиентского узла) системы путём сравнения предоставленных им на момент подключения реквизитов с реквизитами, соотнесёнными с указанным именем пользователя/логином в базе данных.

12. Контакты

Новые версии прошивок, документации и сопутствующего программного обеспечения можно получить, обратившись по следующим контактам:

Санкт-Петербург

| | |
|---------------------------|--|
| сайт компании в Интернете | www.radiofid.ru |
| тел. в Санкт-Петербурге | +7 (812) 318 18 19 |
| e-mail | support@radiofid.ru |

Наши специалисты всегда готовы ответить на все Ваши вопросы, помочь в установке, настройке и устранении проблемных ситуаций при эксплуатации оборудования.

В случае возникновения проблемной ситуации, при обращении в техническую поддержку, следует указывать версию программного обеспечения, используемого в роутере. Так же рекомендуется к письму прикрепить журналы запуска проблемных сервисов, снимки экранов настроек и любую другую полезную информацию. Чем больше информации будет предоставлено сотруднику технической поддержки, тем быстрее он сможет разобраться в сложившейся ситуации.



Перед обращением в техническую поддержку настоятельно рекомендуется обновить программное обеспечение роутера до актуальной версии.



Нарушение условий эксплуатации (ненадлежащее использование роутера) лишает владельца устройства права на гарантийное обслуживание.