РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Настройка туннелей на роутерах iRZ

Содержание

Таблицы

Рисунки

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**	
Подготовлено:		**Проверено:**	

1.2. Предупреждение

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.

Внимание! 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. Пример интерфейса представлен на Рис. 1.

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

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

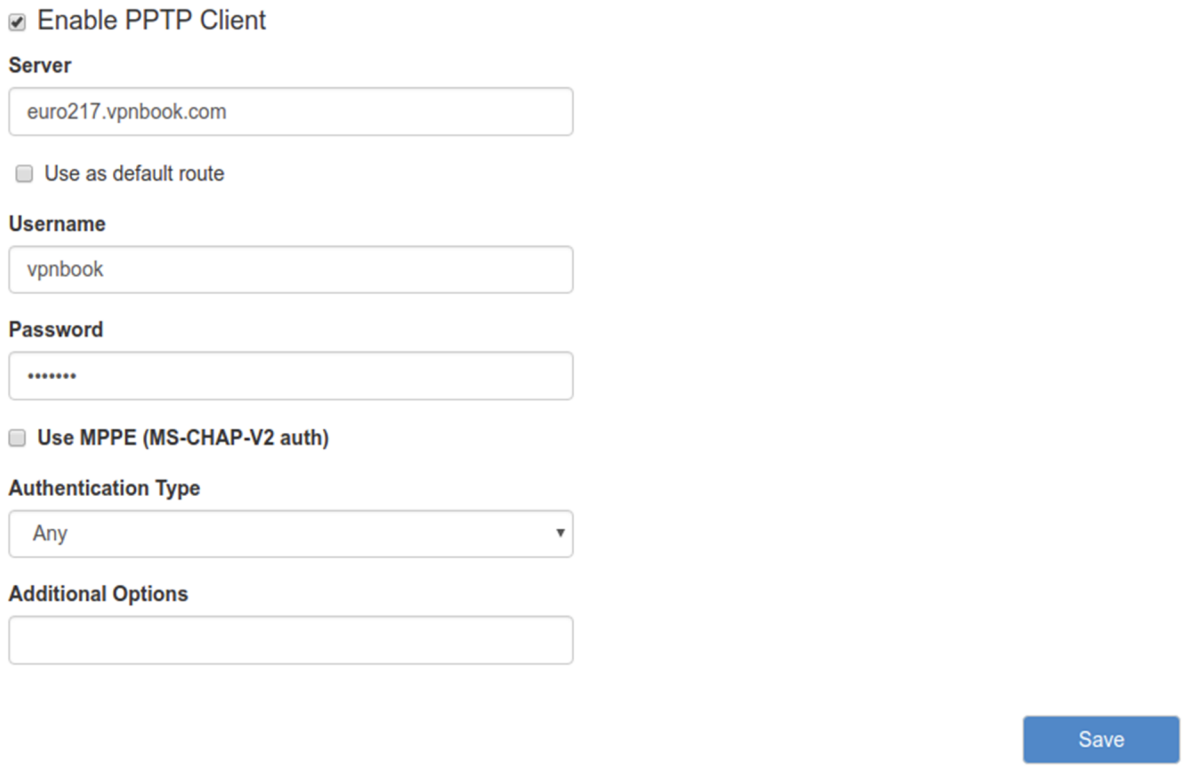

Рис. 1 Пример интерфейса PPTP Client

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.

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.

Чекбокс — Use as default route заставит роутер весь трафик направлять через данный туннель. В этом случае в таблице маршрутизации маршрут через данный туннель будет приоритетнее остальных. 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.

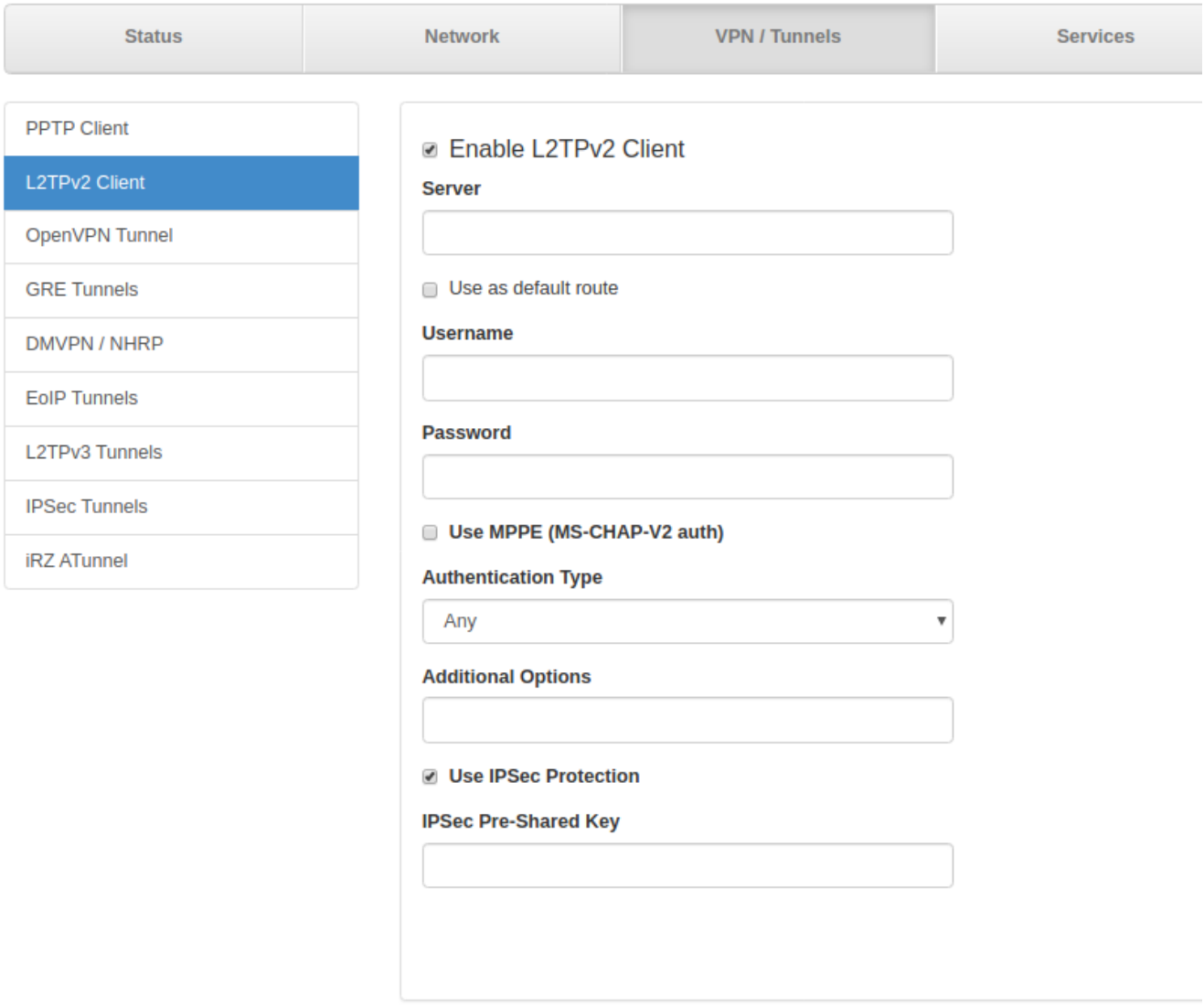

Рис. 2 Пример интерфейса L2TPv2 Client

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.

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**;

Настройте остальные параметры на странице в зависимости от требуемой конфигурации (см. Табл. 4.1, Табл. 4.2).

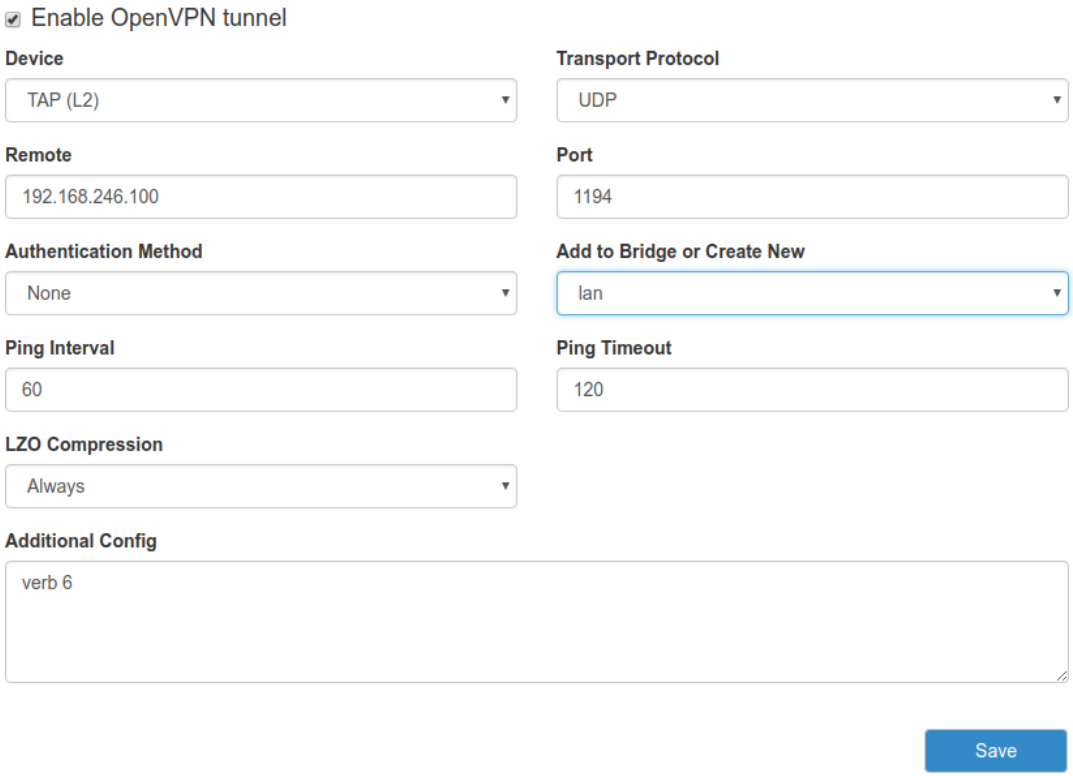

Рис. 4 Примеры конфигураций OpenVPN. Настройка OpenVPN (без аутентификации), базовая TAP (L2)

Табл. 4.1 Примеры конфигураций OpenVPN. Настройки OpenVPN Tunnel → TAP (L2), основные настройки

Поле	Описание
Device	Выбор виртуального интерфейса (в данном примере – **TAP (L2)**)
Transport Protocol	Выбор транспортного протокола: 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
Authentification Method	Метод авторизации (в данном примере – **None**)
Add to Bridge or Create New	Создание моста с локальными интерфейсами роутера (дополнительные настройки см. в таблице 2)
Advanced Settings (нажмите на строчку **Show advanced settings**, чтобы открыть доступ к настройкам):	
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	Режим сжатия данных, проходящих через туннель: 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.

Табл. 4.2 Примеры конфигураций OpenVPN. Настройки OpenVPN Tunnel → TAP (L2), Bridge with Interface = None

Поле	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

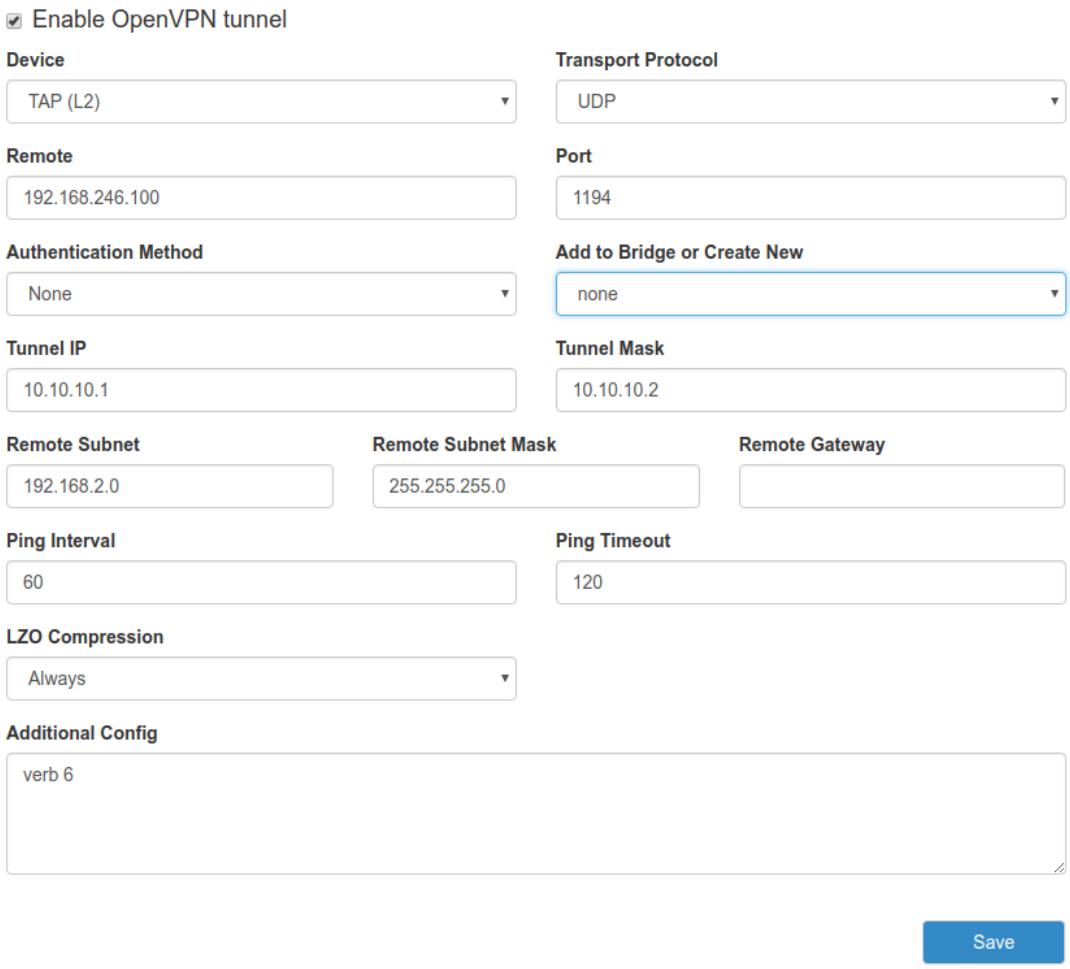

Рис. 5 Примеры конфигураций OpenVPN. Настройка OpenVPN (без аутентификации), Bridge with Interface = None

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. Табл. 4.1, Табл. 4.2)

При выборе данного метода аутентификации, все настройки в окне интерфейса такие же, как в разделе 4.1.1, к ним прибавляется лишь поле **Shared Secret**, в котором указывается общий ключ. Сам ключ необходимо заранее сгенерировать и распространить на устройствах участниках (см. Рис. 6).

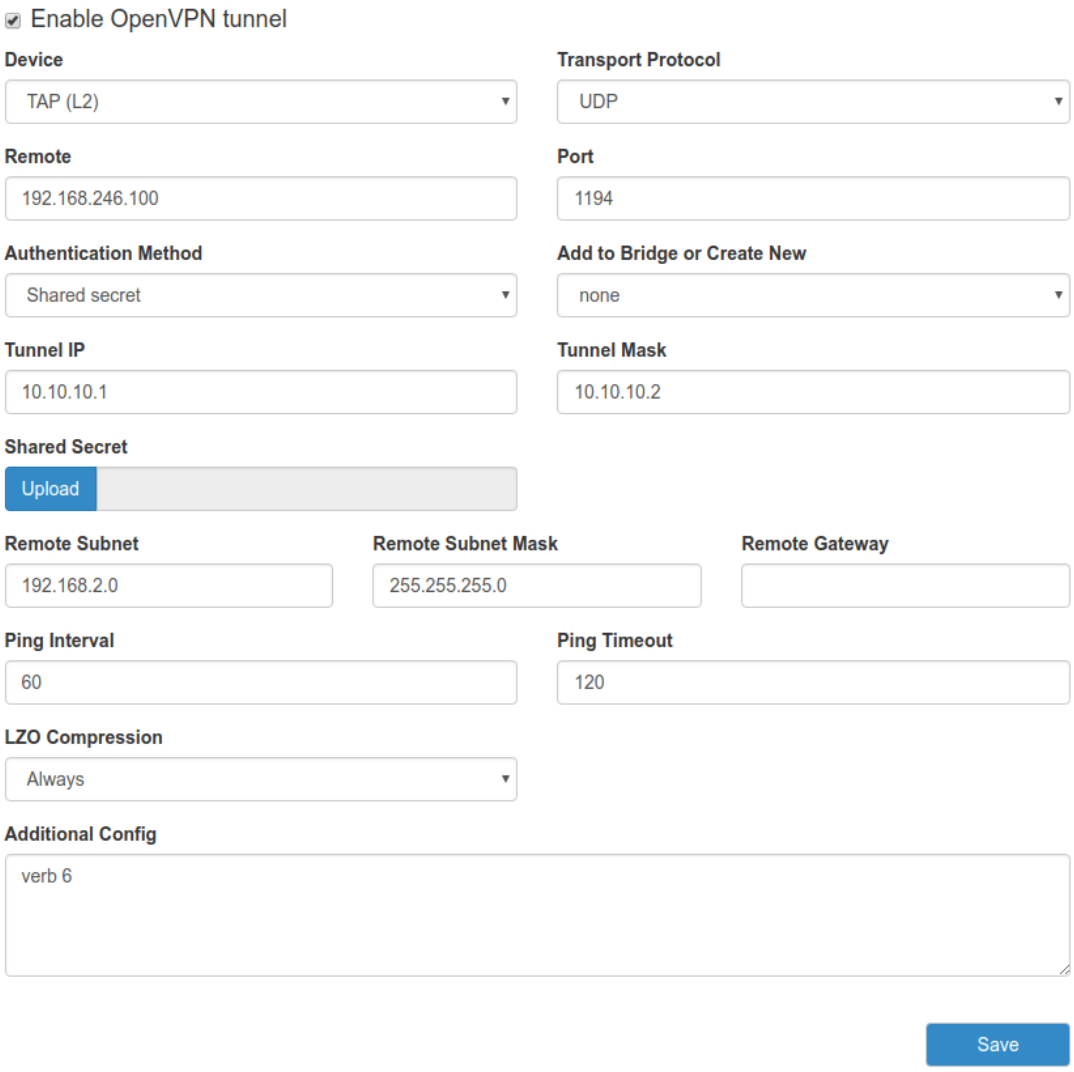

Рис. 6 Примеры конфигураций OpenVPN. Настройка OpenVPN (с аутентификацией по ключу)

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 описание);

Настройте остальные параметры на странице в зависимости от требуемой конфигурации (см. Табл. 4.1, Табл. 4.2).

При выборе данного метода аутентификации, все настройки в окне интерфейса такие же, как в разделе 4.1.2, 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 Табл. 4.3

Табл. 4.3 Примеры конфигураций OpenVPN. Ключи и сертификаты для аутентификации по протоколу TLS

Поле	Файл	Описание
CA Certificate	ca.crt	Сертификат удостоверяющего центра
DH Parameter	dh1024.pem	Файл с ключом для алгоритма Диффи-Хелманадля 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 полями согласно Табл. 4.3. Пример настройки показан на Рис. 7.

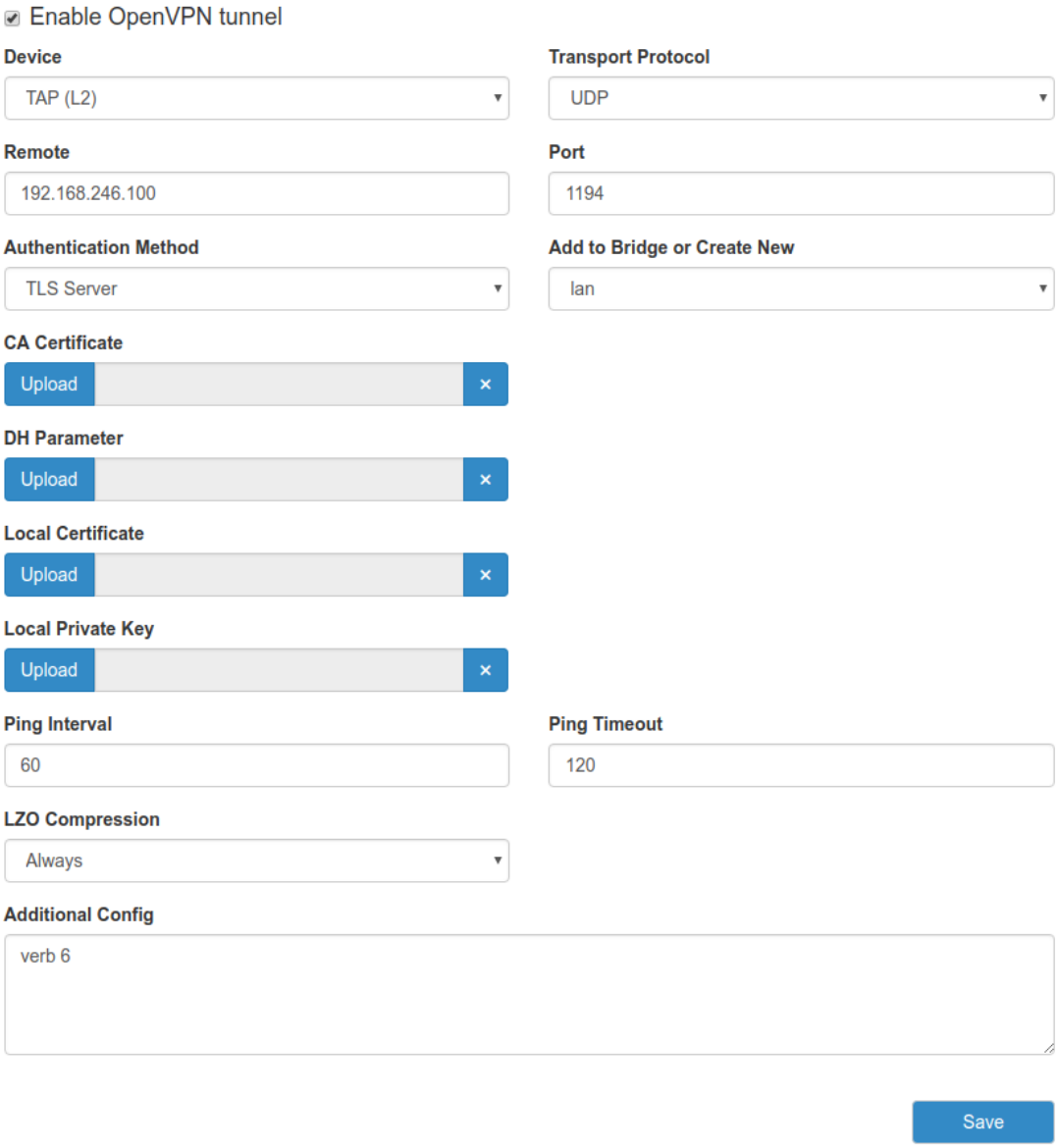

Рис. 7 Примеры конфигураций OpenVPN. Настройка OpenVPN (с аутентификацией по протоколу TLS), роутер – сервер

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 наличиии ta.key файла добавьте ключ в поле **TLS Auth Key** и/или укажите логин и пароль. (см. далее описание);

Настройте остальные параметры на странице в зависимости от требуемой конфигурации (см. Табл. 4.1, Табл. 4.2).

При выборе данного метода аутентификации все настройки в окне интерфейса идентичны разделу 4.1.2, 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 Табл. 4.3, кроме файла с ключом для алгоритма Диффи-Хелмана. Пример настройки показан на Рис. 8

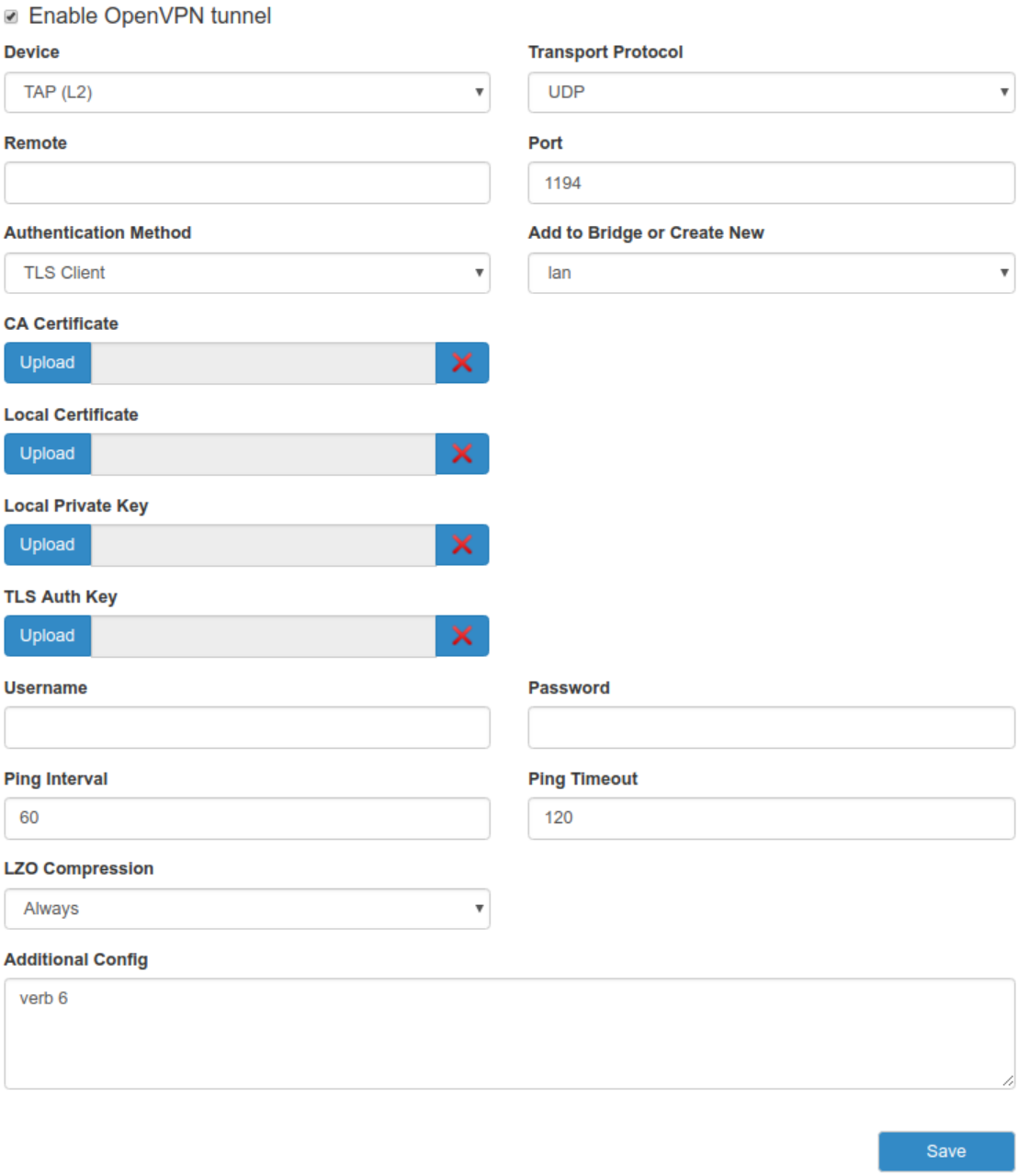

Рис. 8 Примеры конфигураций OpenVPN. Настройка OpenVPN (с аутентификацией по протоколу TLS), роутер – клиент

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:

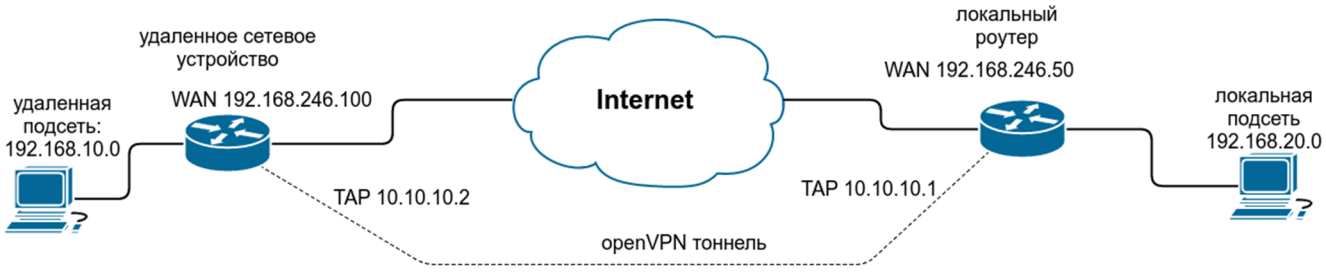

Рис. 9 Примеры конфигураций OpenVPN. Схема сети

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**;

Настройте остальные параметры на странице в зависимости от требуемой конфигурации (см. Табл. 4.4, Табл. 4.5).

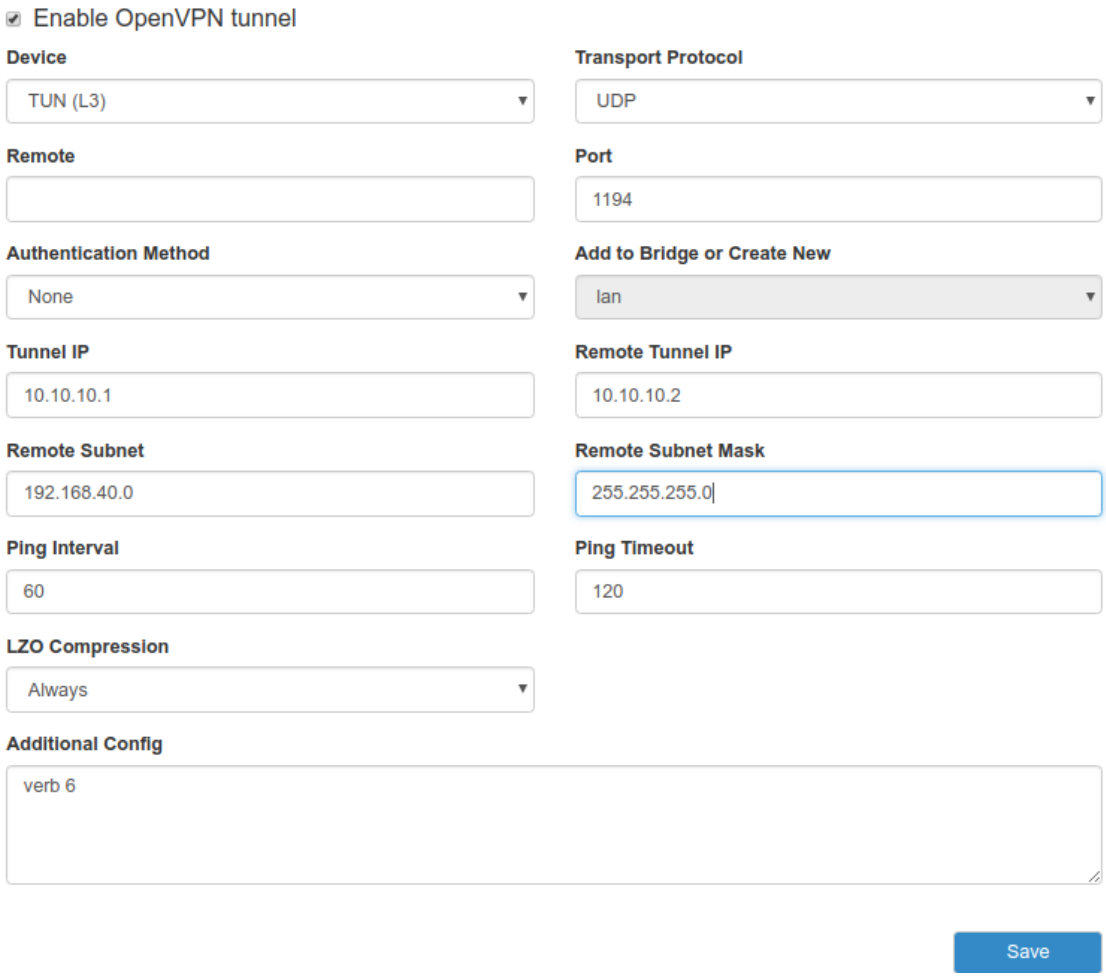

Рис. 10 Примеры конфигураций OpenVPN. Настройка OpenVPN (без аутентификации), TUN (L3)

Табл. 4.4 Примеры конфигураций OpenVPN. Настройки OpenVPN Tunnel → TUN (L3), основные настройки

Поле	Описание
Device	Выбор виртуального интерфейса (в данном примере – **TUN (L3)**)
Transport Protocol	Выбор транспортного протокола: □ 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
Authentification 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 (нажмите на строчку **Show advanced settings**, чтобы открыть доступ к настройкам):	
Ping Interval	Время в секундах, через которое будут отсылаться ICMP-пакеты для проверки доступности удаленного сетевого устройства (и соответственно работы туннеля)

Поле	Описание
Ping Timeout	Время ожидания в секундах, через которое устройство попытается заново создать OpenVPN-туннель, если ответ от удаленного устройства не будет получен
LZO Compression	Режим сжатия данных, проходящих через туннель: 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.

Табл. 4.5 Примеры конфигураций OpenVPN. Настройки OpenVPN Tunnel → TUN (L3), Bridge with Interface = None

Поле	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, подключающемуся 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. Табл. 4.4, Табл. 4.5).

При выборе данного метода аутентификации, большинство настроек в окне интерфейса такие же, как в разделе 4.2.1, к ним прибавляется поле **Shared Secret**, в котором указывается общий ключ. Сам ключ необходимо заранее сгенерировать и распространить на устройствах участниках (см. Рис. 11).

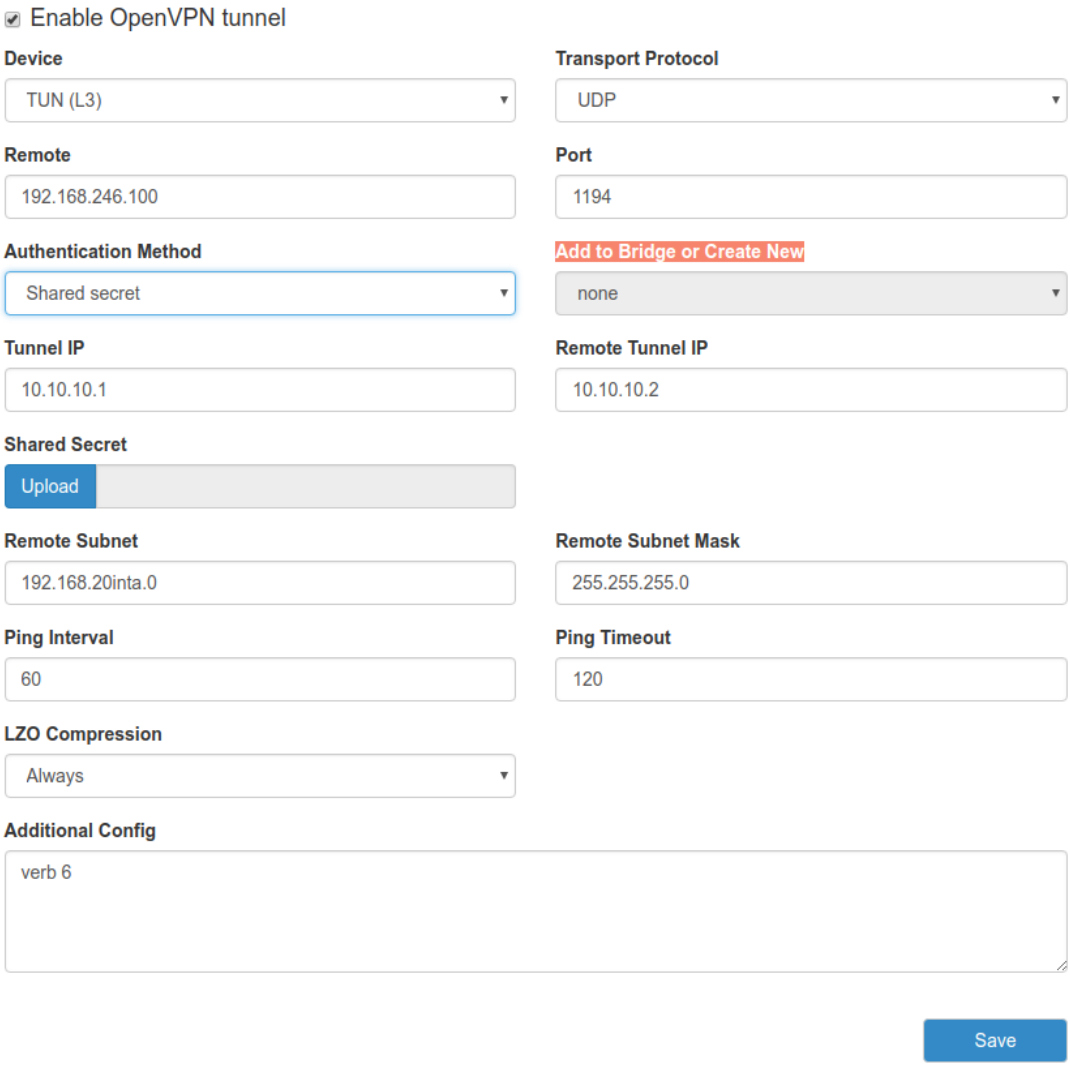

Рис. 11 Примеры конфигураций OpenVPN. Настройка OpenVPN (с аутентификацией по ключу)

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 описание);

Настройте остальные параметры на странице в зависимости от требуемой конфигурации (см. Табл. 4.4, Табл. 4.5).

При выборе данного метода аутентификации, все настройки в окне интерфейса такие же, как в разделе 4.2.1, 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 Табл. 4.6

Табл. 4.6 Примеры конфигураций OpenVPN. Ключи и сертификаты для аутентификации по протоколу TLS

Поле	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 необходимо будет загрузить посредством кнопок **Upload** в соответствующие поля согласно Табл. 4.6. Пример настройки показан на Рис. 12.

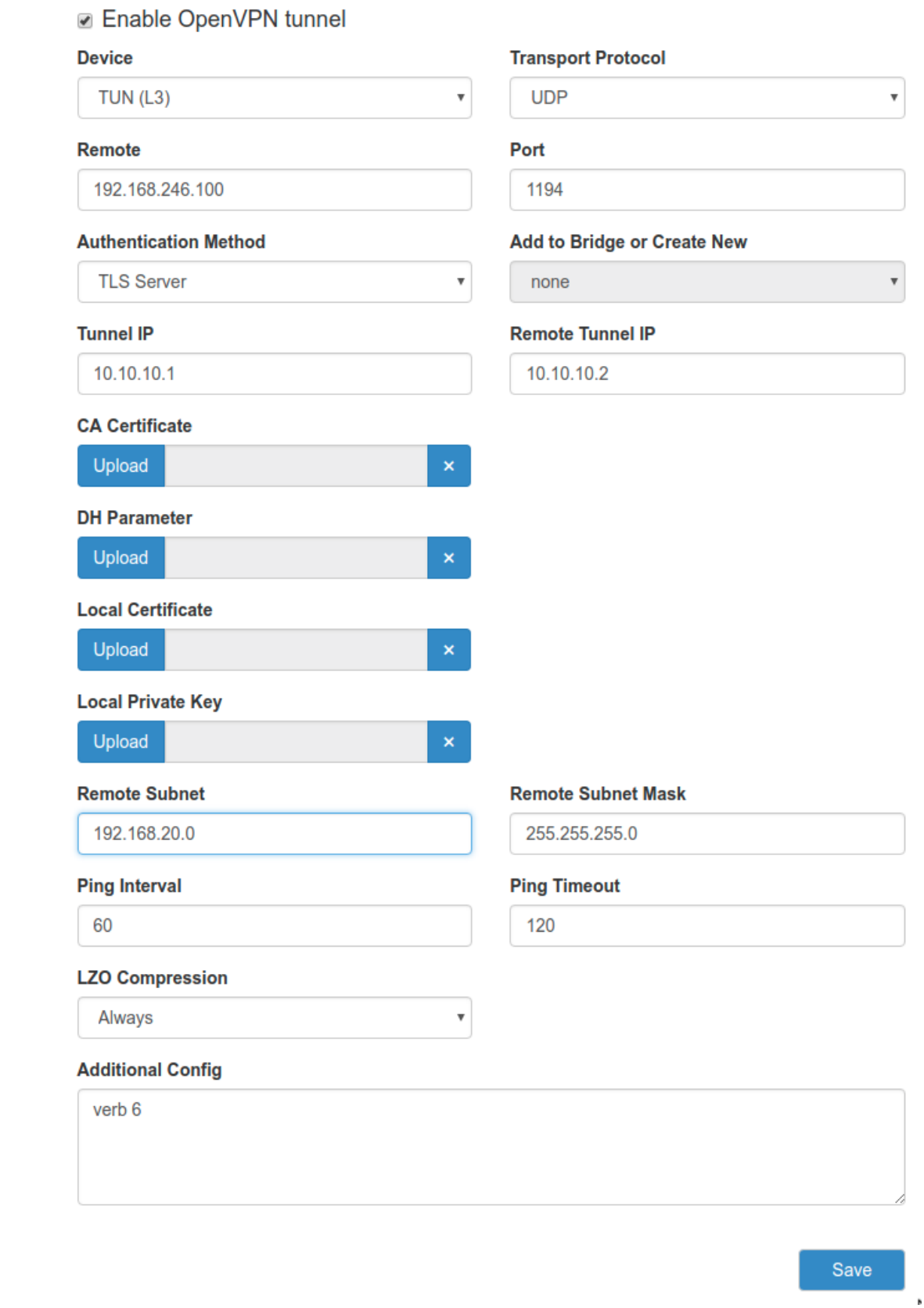

Рис. 12 Примеры конфигураций OpenVPN. Настройка OpenVPN (с аутентификацией по протоколу TLS), роутер – сервер

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 ниличиии 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. Табл. 4.4, Табл. 4.5).

При выборе данного метода аутентификации, все настройки в окне интерфейса такие же, как в разделе 4.2.1, 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 Табл. 4.6, кроме файла с ключом для алгоритма Диффи-Хелмана. Пример настройки показан на Рис. 13.

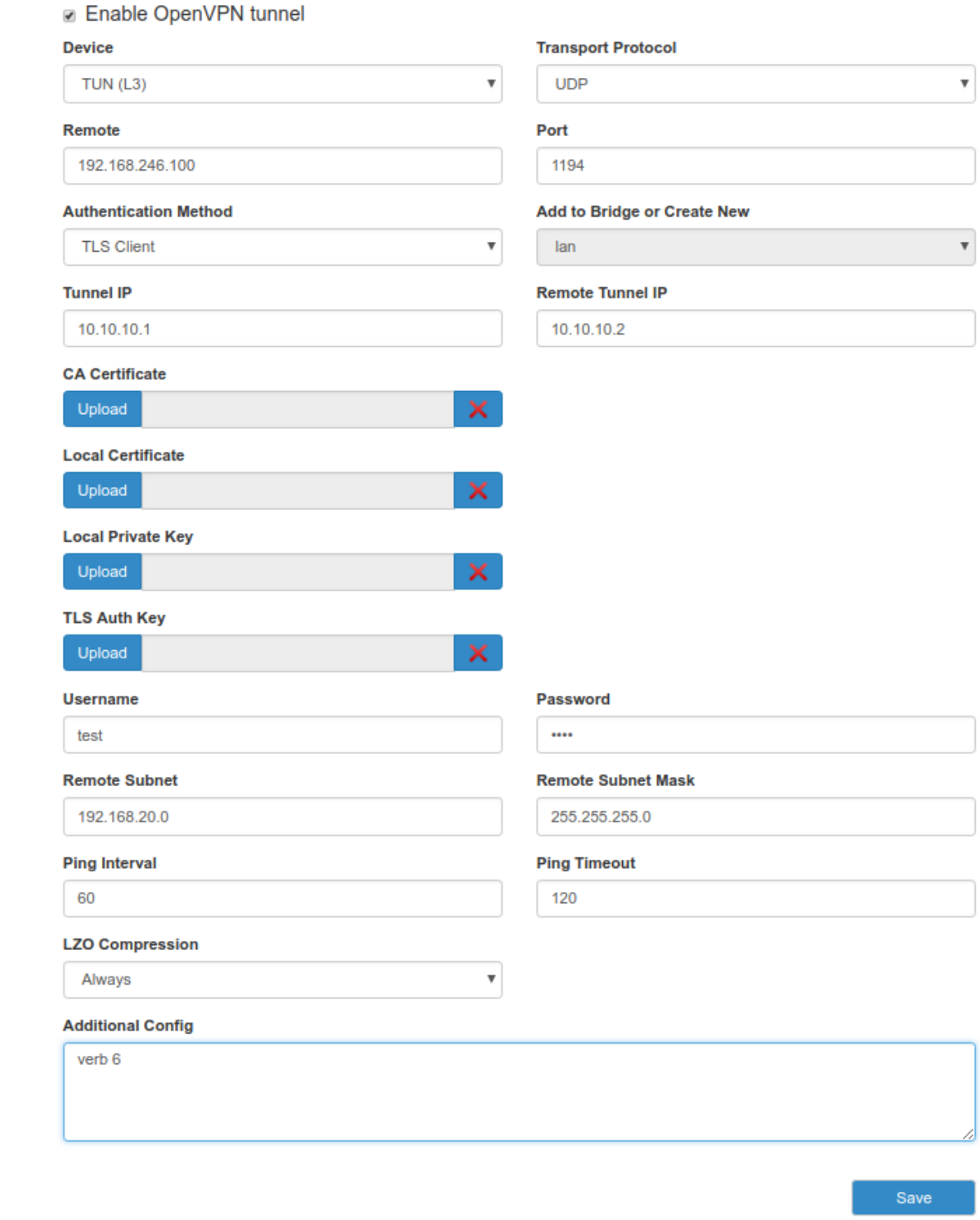

Рис. 13 Примеры конфигураций OpenVPN. Настройка OpenVPN (с аутентификацией по протоколу TLS), роутер – клиент

5. GRE туннели

5.1.1. Настройка GRE туннеля уровня L2

В примерах настройки используется следующая схема сети:

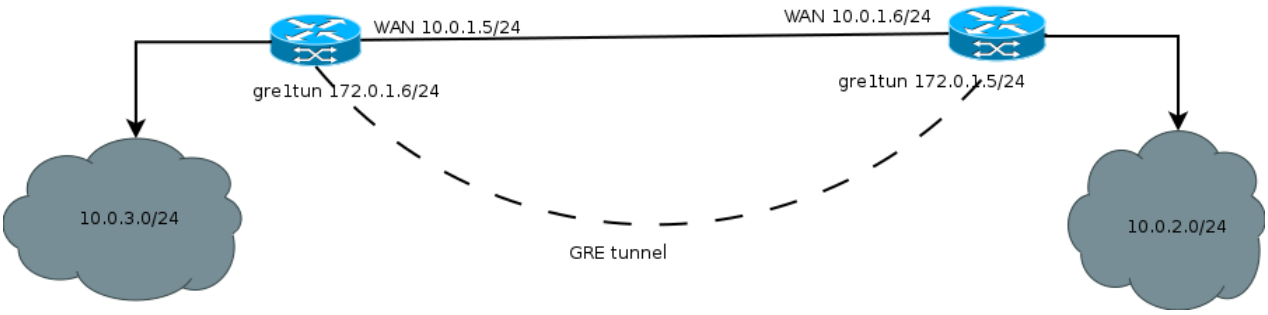

Рис. 14 Примеры конфигураций GRE. **Схема сети**

Для настройки GRE-туннеля уровня L2, в веб-интерфейсе роутера (см. Рис. 15):

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

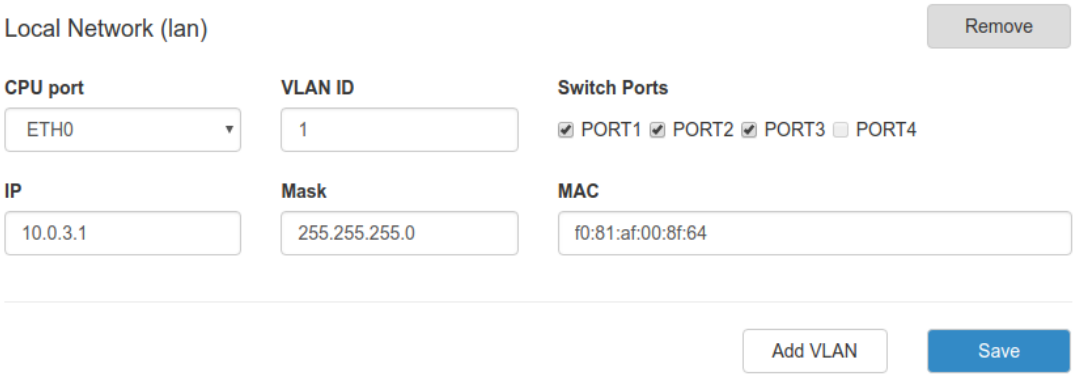

Рис. 15 Примеры конфигураций Local Network. Настройка локальной сети

Далее необходимо настроить WAN-порт роутера (см. Рис. 16):

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

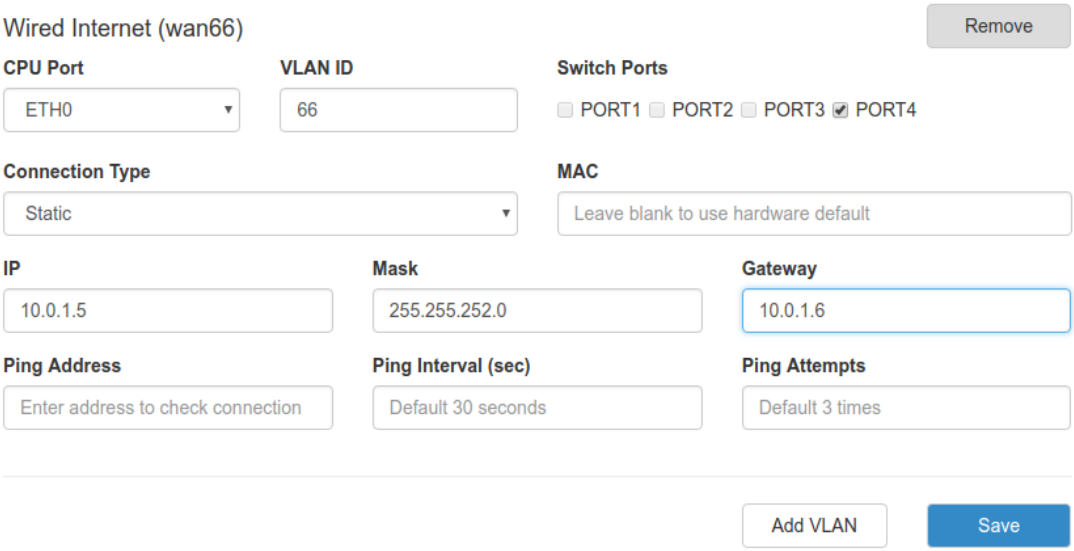

Рис. 16 Примеры конфигураций Wired Internet. Настройка WAN

Далее необходимо настроить GRE-туннель (см. Рис. 17):

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**.

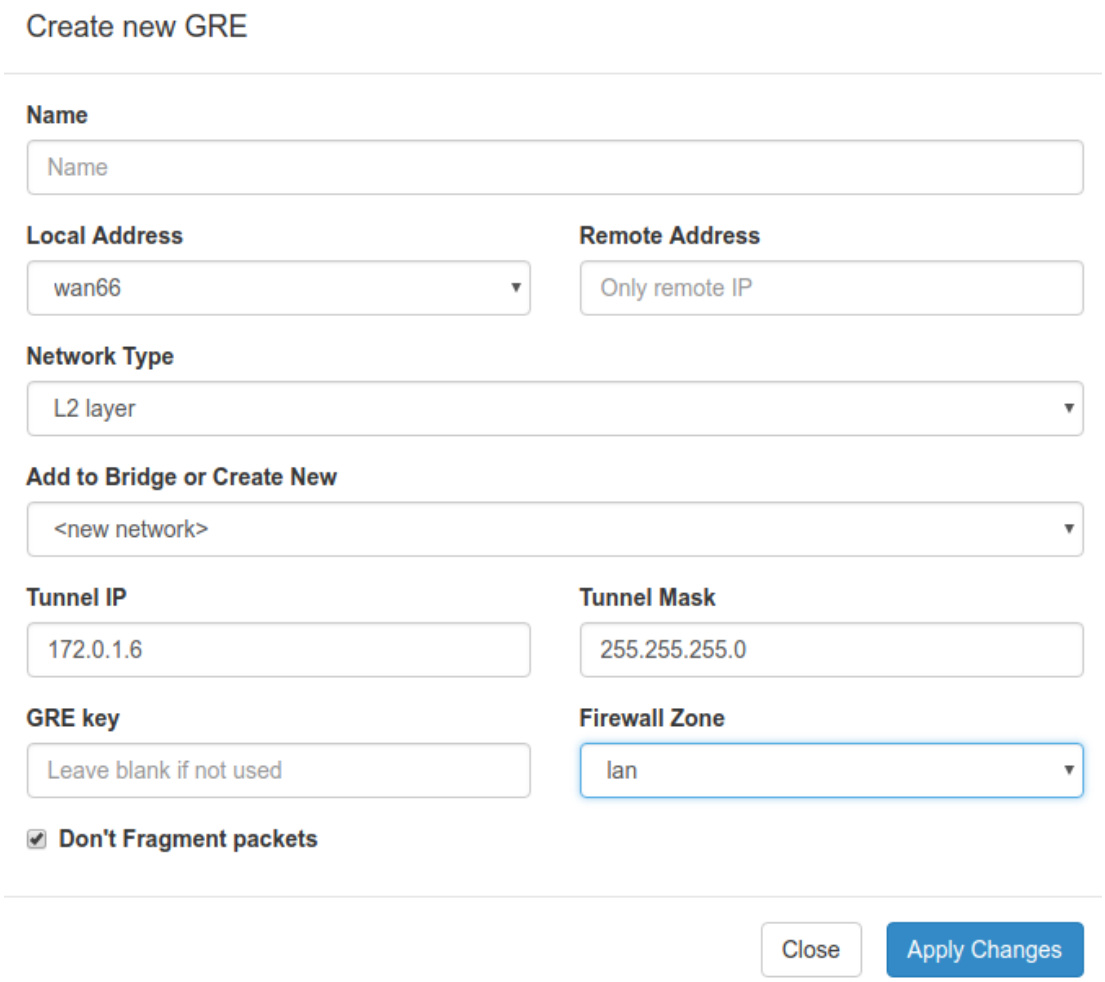

Рис. 17 Примеры конфигураций GRE. Настройка GRE-туннеля

5.1.2. Настройка GRE туннеля уровня L3

В примерах настройки используется следующая схема сети:

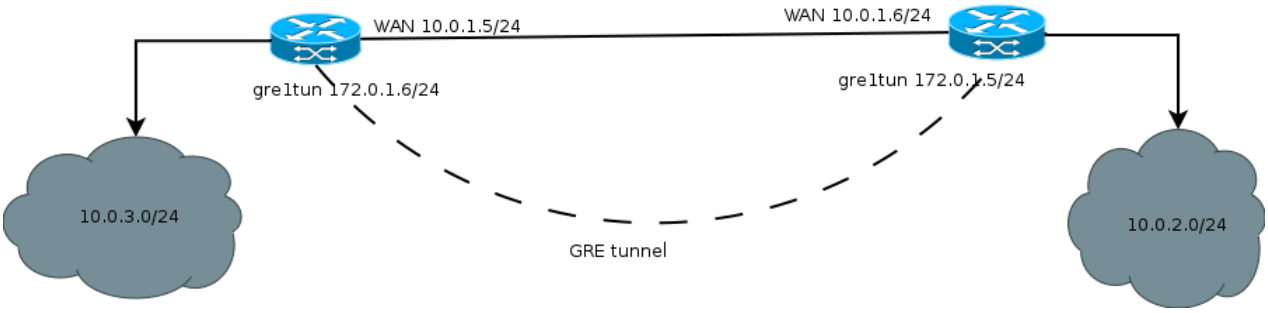

Рис. 18. Примеры конфигураций GRE. **Схема сети**

Для настройки GRE-туннеля уровня L3, в веб-интерфейсе роутера (см. Рис. 19):

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

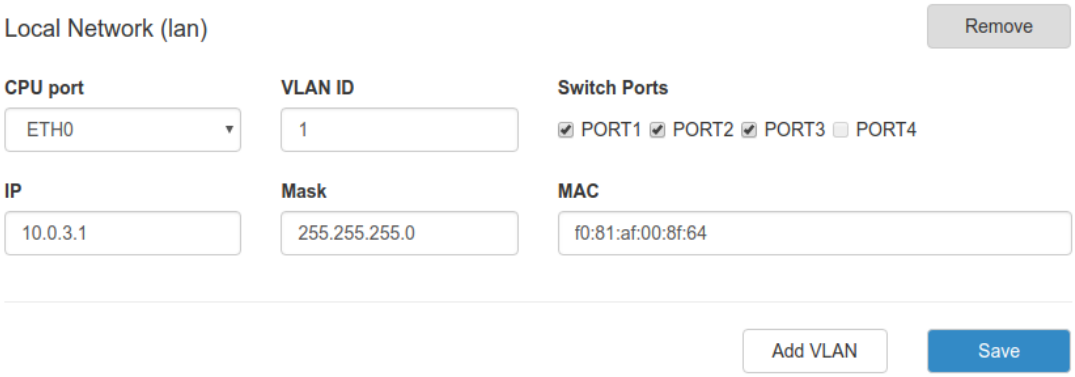

Рис. 19. Примеры конфигураций GRE. **Настройка локальной сети**

Далее необходимо настроить WAN-порт роутера (см. Рис. 20):

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

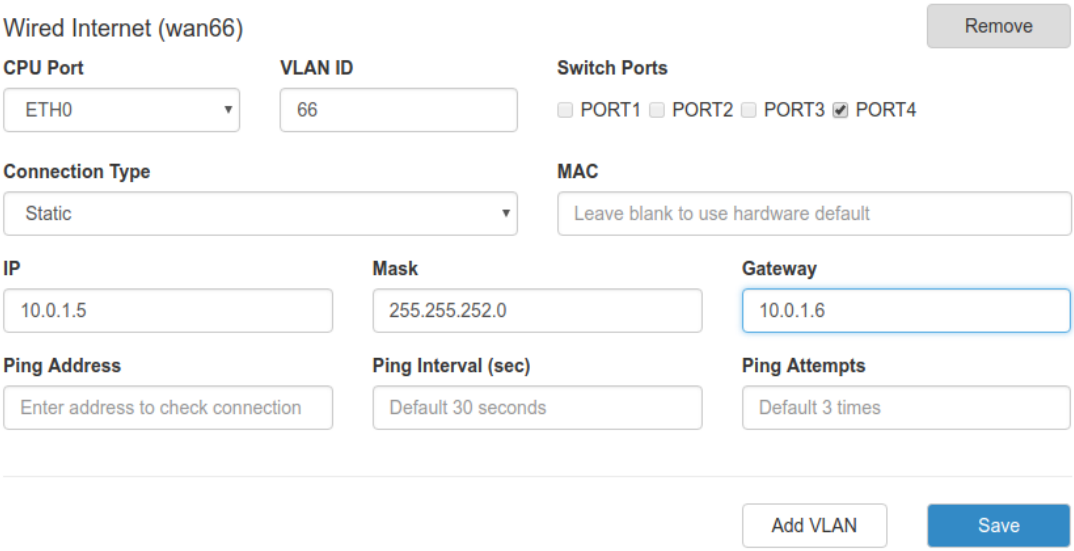

Рис. 20 Примеры конфигураций GRE. Настройка WAN

Далее необходимо настроить GRE-туннель (см. Рис. 21):

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**.

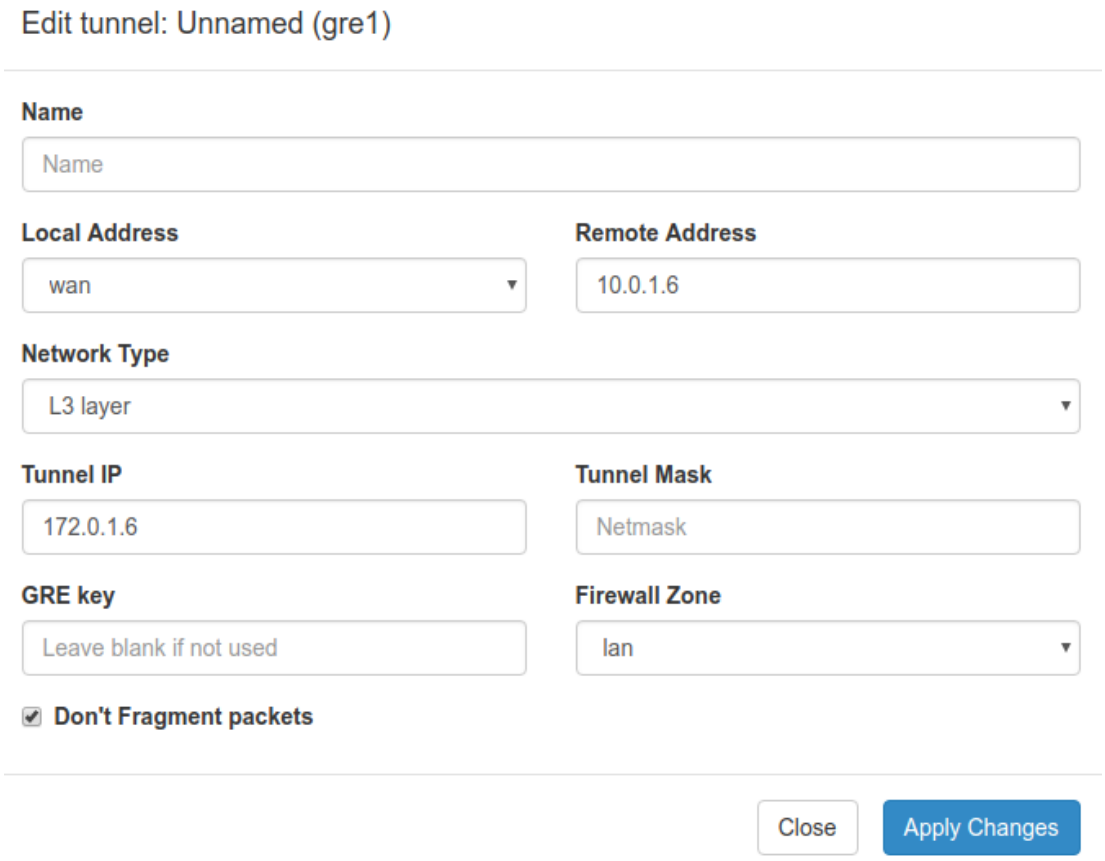

Рис. 21 Примеры конфигураций GRE. Настройка GRE-туннеля

6. 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. Рис. 22) заполнить поля согласно Табл. 6.1

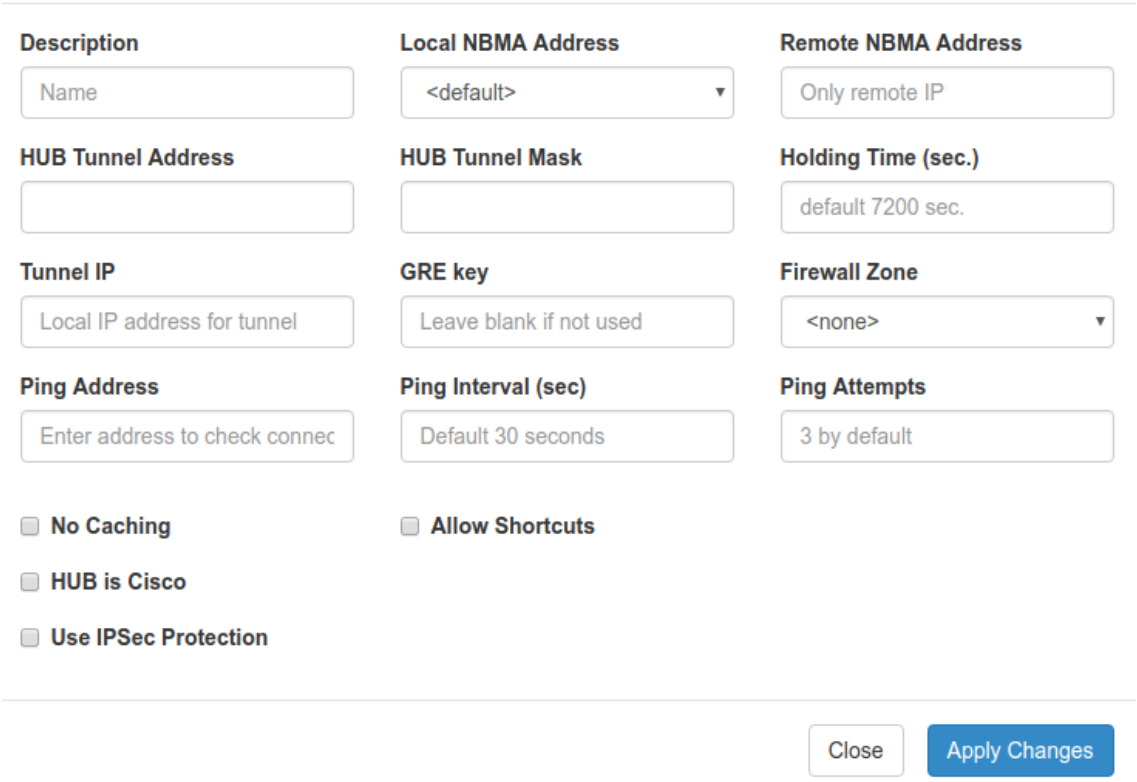

Рис. 22 Страница настроек DMVPN/NHRP

Табл. 6.1 Настройки DMVPN/NHRP

DMVPN/NHRP	
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 HUBa к которому происходит подключение.
HUB Tunnel Mask	Маска сети туннеля.
Holding Time (sec.)	Время (в секундах) в течение которого информация о соседнем NBMA хосте считается действительной.
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 Attemts	Количество попыток, по истечении которых роутер попытается переустановить туннель.
No Caching	
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
Use IPSec Protection	Данная настройка откроет дополнительное поле с возможностью настроить шифрование туннеля с помощью IPSec туннеля
Allow Shortcuts	Разрешает помещение в таблицу маршрутизации только тех префиксов, которые реально используются в данный момент времени
Allow Redirects	Разрешает направлять трафик напрямую между spoke маршрутизаторами в обход хаба

В случае использования шифрования туннеля с помощью технологии IPSec необходимо настроить соответствующие параметры туннеля. Более подробно о каждом параметре можно прочитать в разделе IPsec туннели (только для роутеров серии R4, R2).

7. 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 другу напрямую через физические ethernet порты. Такой туннель можно создавать поверх любого другого туннеля или подключения, умеющего транспортировать протокол IP. Пример настроек туннеля приведет на Рис. 23

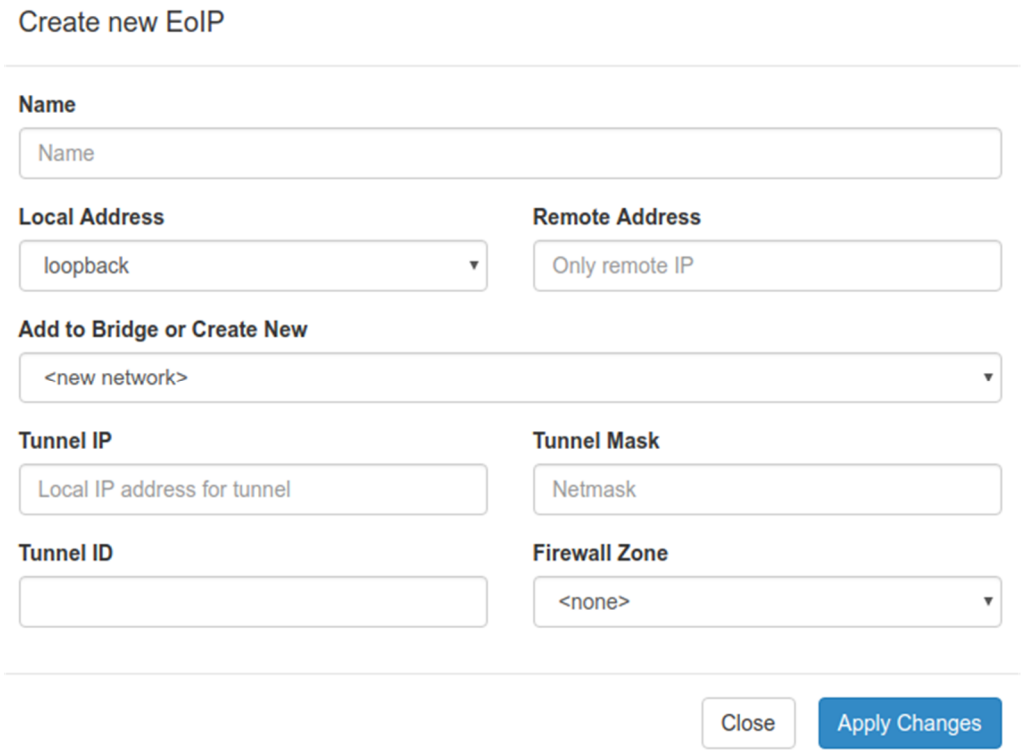

Рис. 23 Настройка EoIP-туннеля

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. 23 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 терминированием 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.

8. 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. Рис. 24) заполнить поля согласно Табл. 8.1.

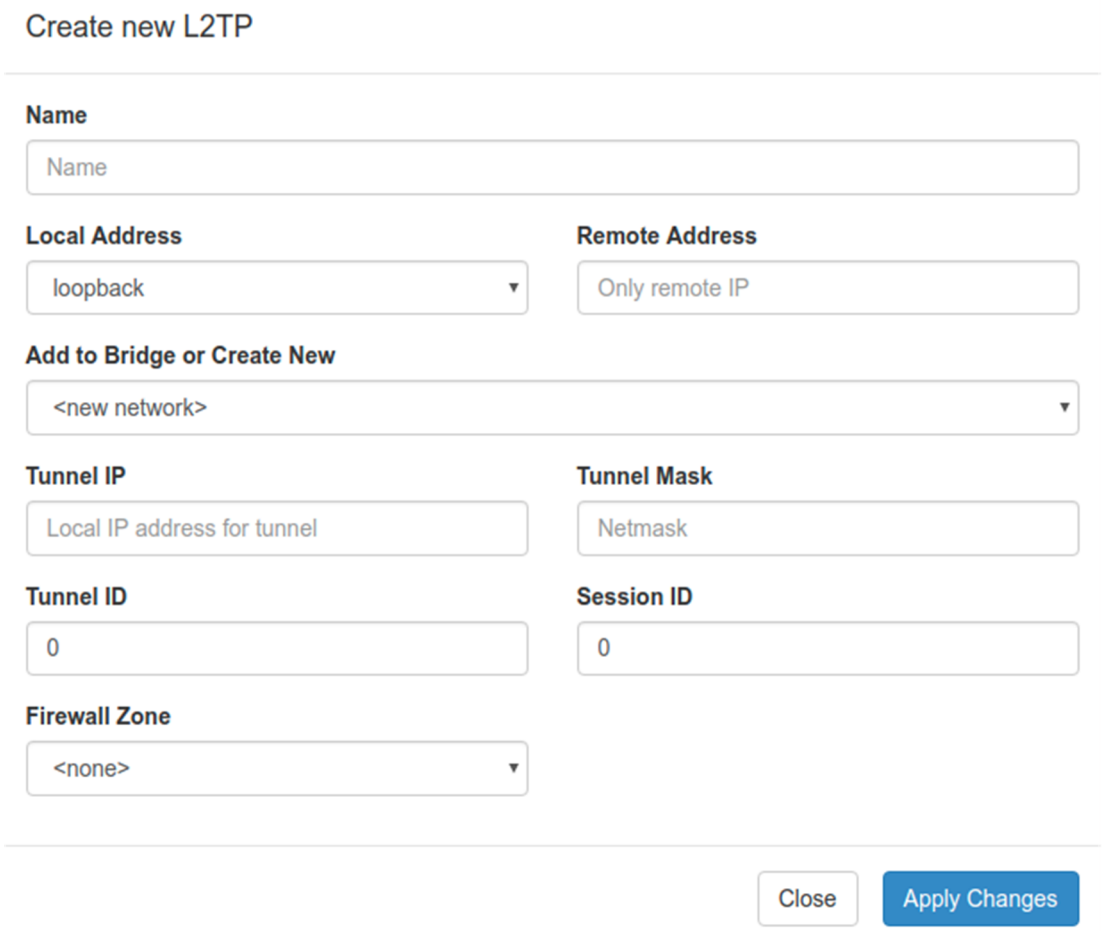

Рис. 24 Настройка L2TP3-туннеля

Табл. 8.1 Настройки L2TP3

L2TPv3	
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 адресс 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

9. 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. Рис. 25):

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

Рис. 25. Примеры конфигураций IPsec. Настройка IPsec-туннеля

Далее необходимо настроить параметры туннеля (см. Рис. 26):

2. Введите описание туннеля (на выбор пользователя) в поле **Description**;
3. 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**);
4. Укажите IP-адрес порта удаленного устройства, с которым будет построен туннель, в поле **Remote Address**;
5. 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);
6. Укажите локальный идентификатор и идентификатор удаленной стороны в полях **Local Identifer** и **Remote Identifer** соответственно;
7. Поле **Key Exchange Mode** предназначено для переключения между первой и второй версиями обмена ключей при установлении тоннеля

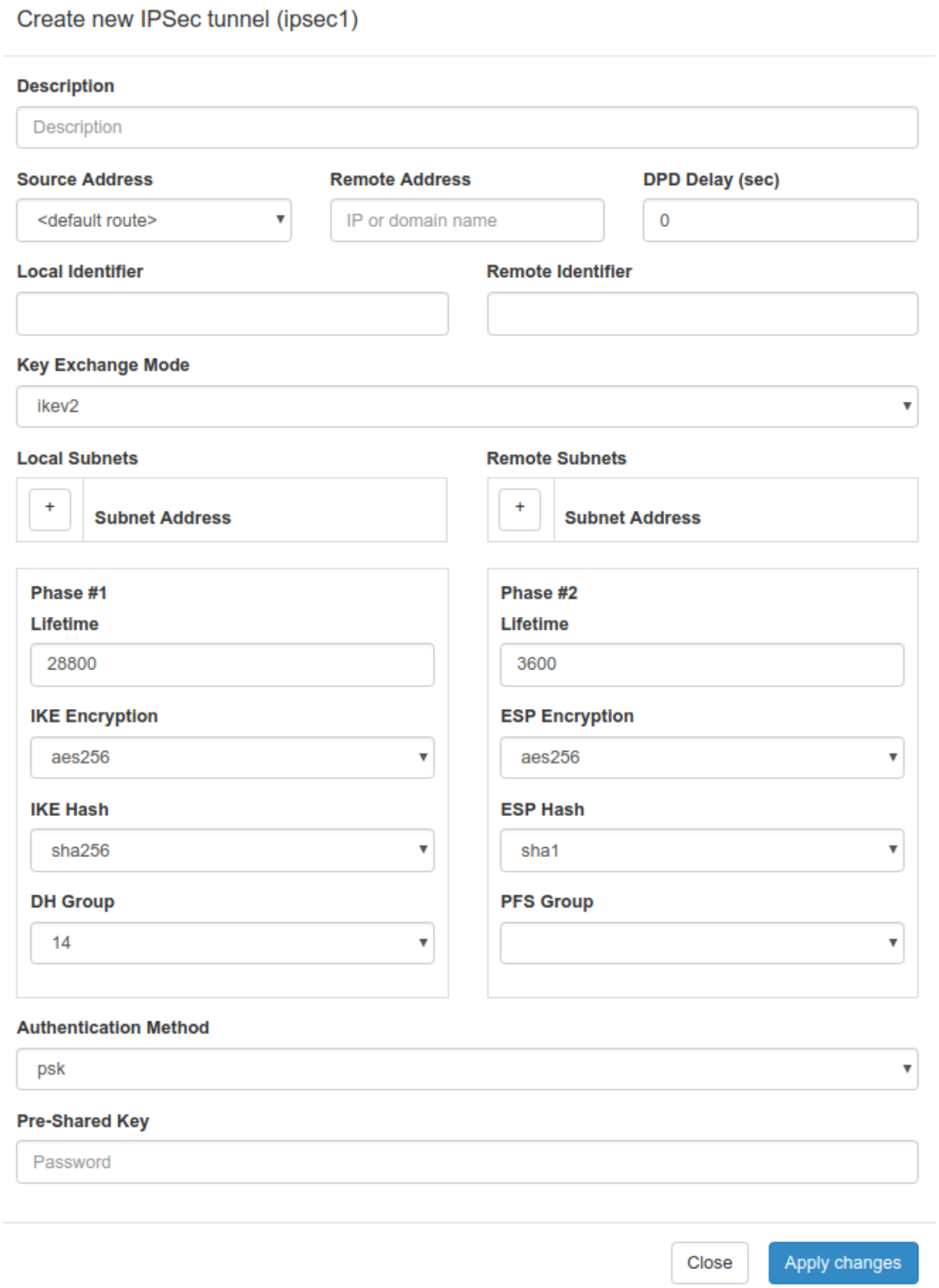

Рис. 26 Примеры конфигураций IPsec. Параметры туннеля

8. 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;
9. 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 тоннель. Сети записываются в поля в формате CIDR.
10. Настройте фазу 1 и фазу 2, заполнив соответствующие поля в блоках **Phase #1** и **Phase #2**:

Табл. 9.1 Параметры Phase #1 и Phase #2

Phase #1 (фаза 1)	
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)	
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.

11. Выберите способ аутентификации узлов туннеля, выбрав значение в поле **Authentication Method** (**psk** – по общему ключу, **pubkey** – по сертификату и ключу RSA);

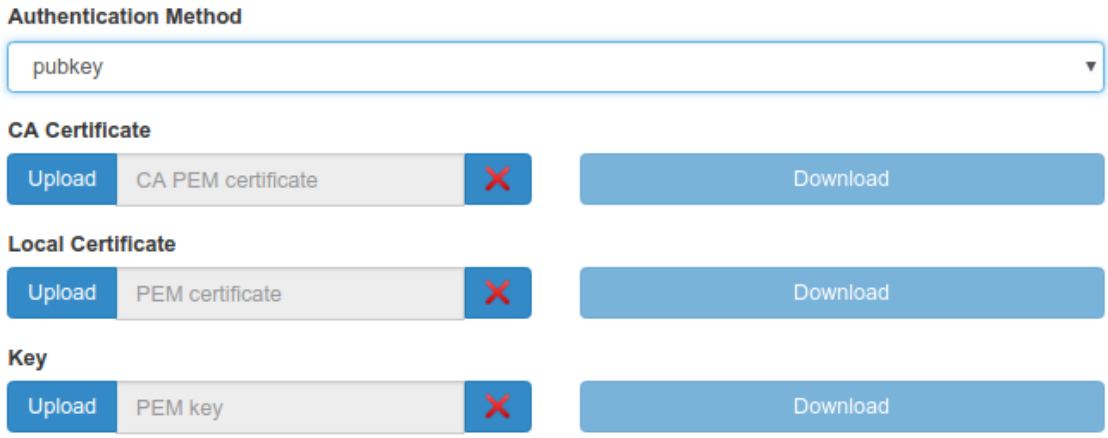

Рис. 27 Способ аутентификации pubkey

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

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**»

11. Термины и сокращения

Сетевые технологии

GSM – стандарт сотовой связи ;

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 2 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 предопределённых 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).

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, позволющая 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.