ЭЛЕКТРОНИКА

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Настройка туннелей на роутерах iRZ

Содержание

Рисунки

Таблицы

1. Введение

1.1. Описание документа

Данный документ содержит примеры корректной конфигурации сетевой службы OpenVPN, GRE, IPsec 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**	
1.0 (17.07.2017)		Основной документ	
Подготовлено:	Колмак О., Головин В.Н.	**Проверено:**	Колмак О.

1.2. Предупреждение

Отклонение от рекомендованных параметров и настроек может привести к непредсказуемым последствиям и значительным издержкам, как в процессе пуско-наладки вычислительного комплекса, так и во время эксплуатации production-версии вычислительного комплекса в «боевых» 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. Примеры конфигураций OpenVPN

2.1. OpenVPN Layer 2: dev TAP

OpenVPN тоннель бывает двух типов: Ethernet Bridging и Routing. В данном разделе рассматривается тоннель OpenVPN типа Ethernet Bridging.

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

Всего четыре варианта настройки тоннеля, 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 тоннель 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:

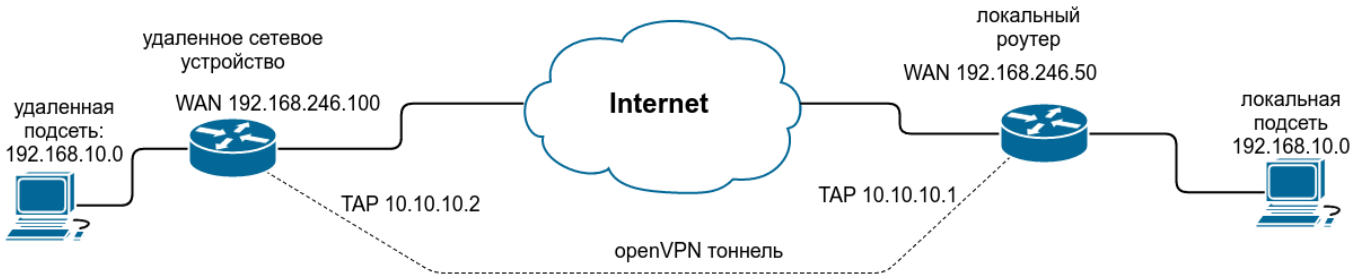

Рис. 2.1. Схема сети

2.1.1. Пример настройки тоннеля без аутентификации (Authentication method: None)

Для настройки OpenVPN-тоннеля 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**;
5. А также настройте остальные параметры на странице в зависимости от требуемой конфигурации (см. таблицы 2.1 и 2.2).

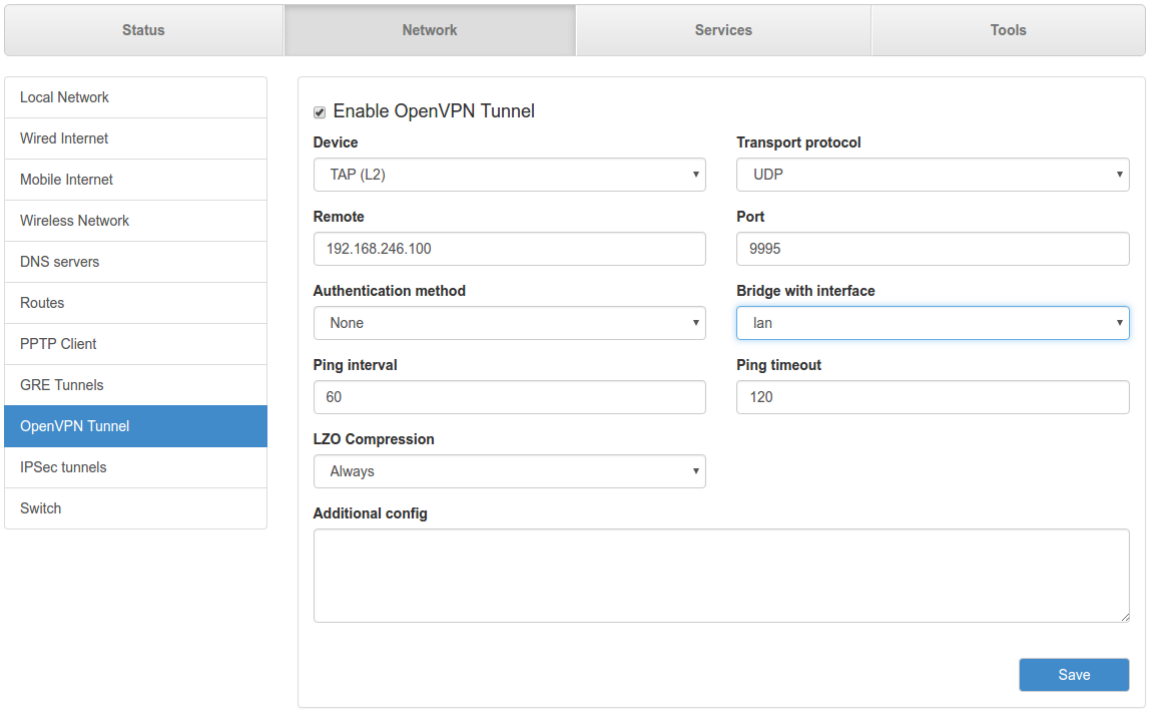

Рис. 2.2. Настройка OpenVPN (без аутентификации), базовая TAP (L2)

Таблица 2.1. 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 тоннель
Authentification Method	Метод авторизации (в данном примере – **None**)
Bridge with Interface	Создание моста с локальными интерфейсами роутера (дополнительные настройки см. в таблице 2.2)
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 тоннеля)
Ping Timeout	Время ожидания в секундах, через которое устройство попытается заново создать OpenVPN-тоннель, если ответ от удаленного устройства не будет получен
LZO Compression	Включение или отключение сжатия данных, проходящих через тоннель

Если создать мост с LAN-портами (**Bridge with Interface** = **LAN**), тогда эти порты будут использоваться как интерфейсы для тоннеля.

Если не создавать мост (**Bridge with Interface** = **None**), тогда в настройках необходимо будет дополнительно указать вручную адреса подсети, маску и шлюз по умолчанию, как показано на Рис. 2.3.

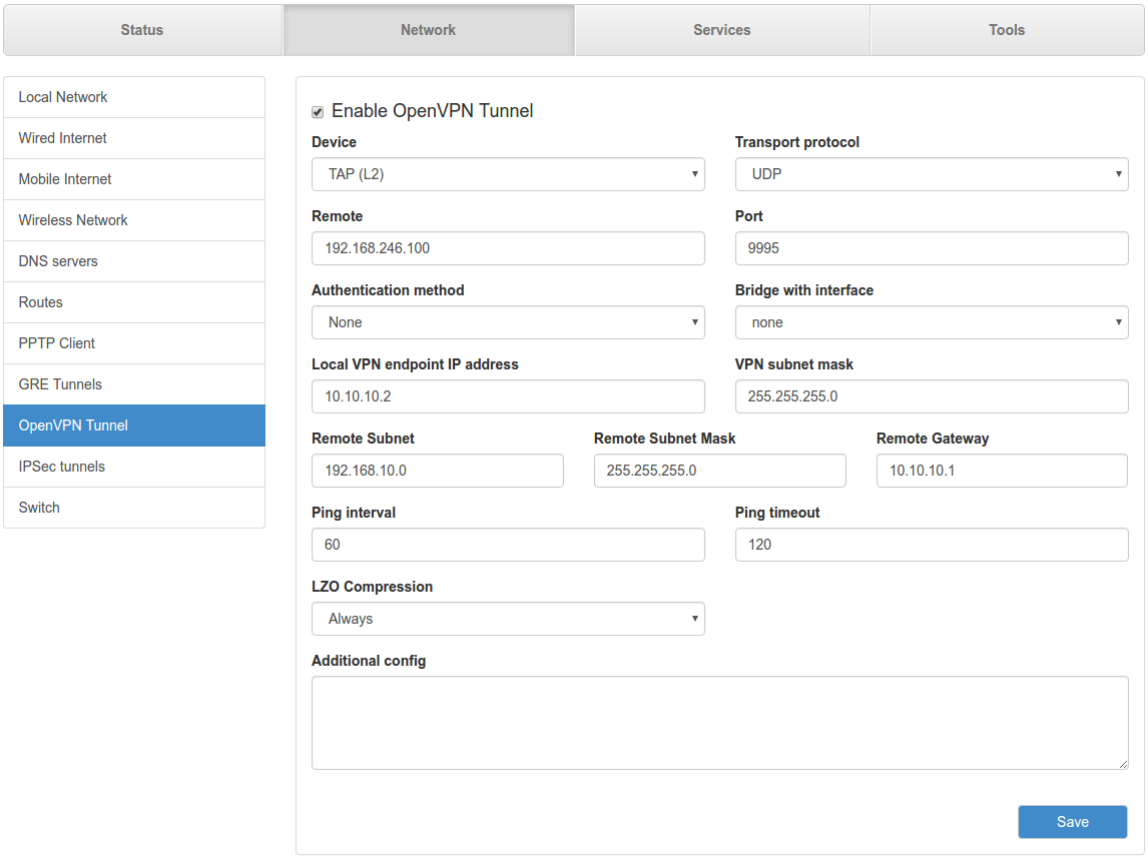

Рис. 2.3. Настройка OpenVPN (без аутентификации), Bridge with Interface = None

Таблица 2.2. Настройки OpenVPN Tunnel → TAP (L2), Bridge with Interface = None

Поле	Описание
Local VPN Endpoint IP Address	IP-адрес тоннеля на данном устройстве
VPN Subnet Mask	Маска IP-адреса тоннеля на данном устройстве
Remote Subnet	IP-адрес удаленной сети (на другом конце тоннеля), который необходим для создания маршрута в таблице маршрутизации
Remote Subnet Mask	Маска удаленной сети (на другом конце тоннеля)
Remote Gateway	Шлюз удаленной сети (на другом конце тоннеля)

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

2.1.2. Пример настройки тоннеля с аутентификацией по ключу (Authentication method: Shared Secret)

Для настройки OpenVPN-тоннеля 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. описание далее);
6. А также настройте остальные параметры на странице в зависимости от требуемой конфигурации (см. таблицы 2.1 и 2.2).

При выборе данного метода аутентификации, все настройки в окне интерфейса такие же, как в разделе 2.1.2, к ним прибавляется лишь поле **Shared Secret**, в котором указывается общий ключ. Сам ключ необходимо заранее сгенерировать и распространить на устройствах участниках (см. рис. 2.4).

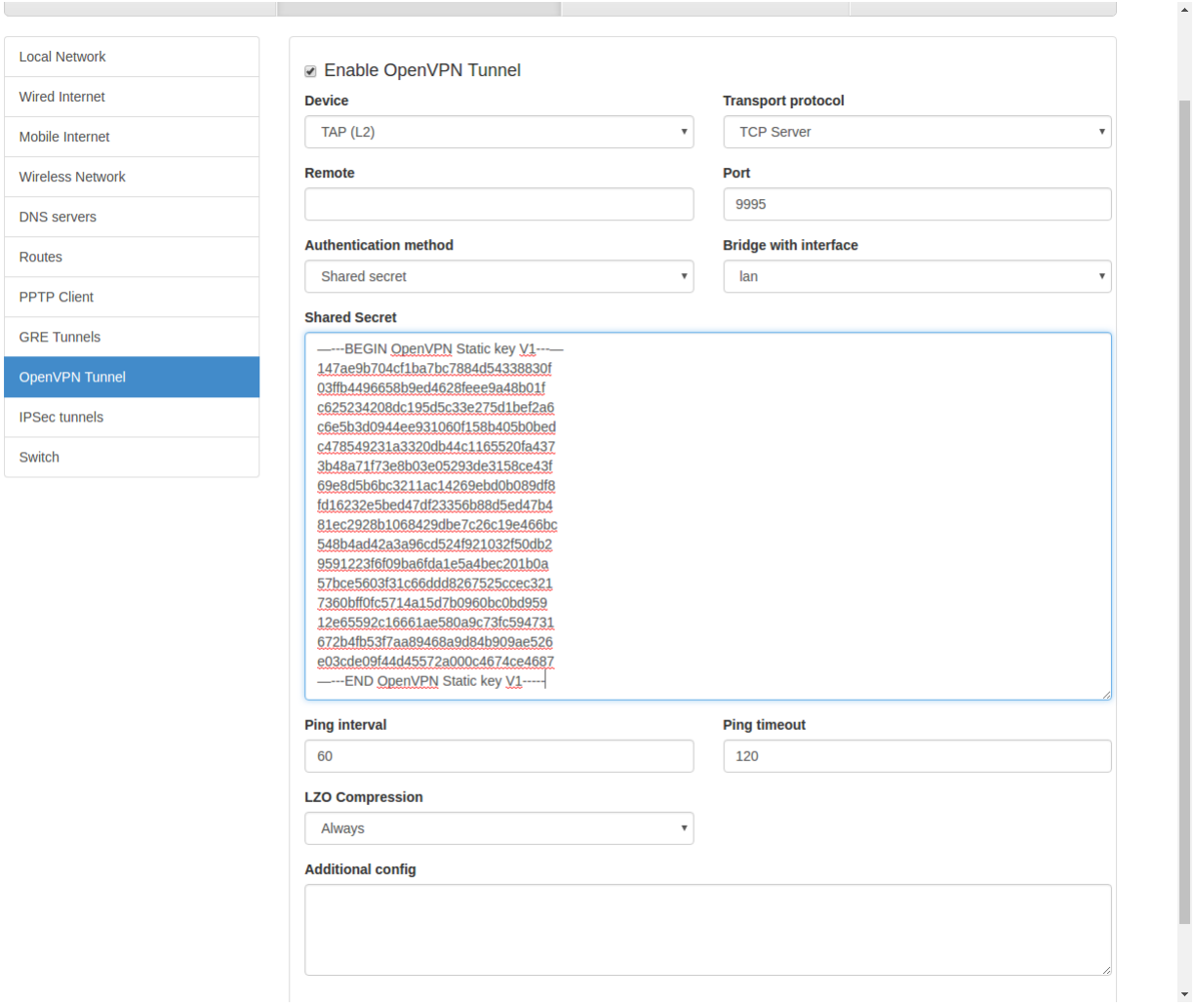

Рис. 2.4. Настройка OpenVPN (с аутентификацией по ключу)

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

Для настройки OpenVPN-тоннеля 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);
6. А также настройте остальные параметры на странице в зависимости от требуемой конфигурации (см. таблицы 2.1 и 2.2).

При выборе данного метода аутентификации, все настройки в окне интерфейса такие же, как в разделе 2.1.2, к ним прибавляется 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 тоннеля понадобятся файлы, указанные в таблице 2.3.

Таблица 2.3. Ключи и сертификаты для аутентификации по протоколу TLS

Поле	Файл	Описание
CA Certificate	ca.crt	Сертификат удостоверяющего центра
DH Parameter	dh1024.pem	Файл 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

Из полученных файлов необходимо будет скопировать зашифрованные данные, которые начинаются строкой “BEGIN CERTIFICATE”, а заканчиваются “END CERTIFICATE”, и вставить текст в соответствующие поля согласно таблице 2.3. Пример настройки показан на рис. 2.5.

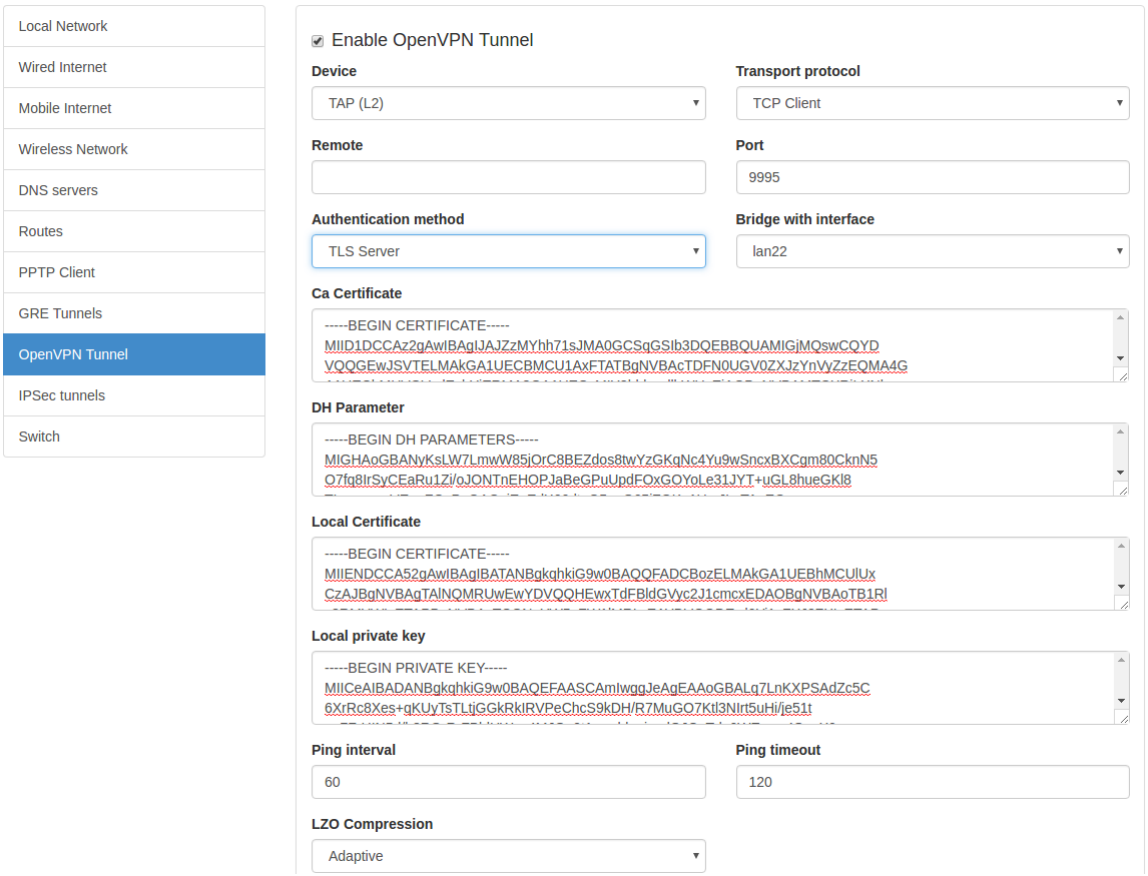

Рис. 2.5. Настройка OpenVPN (с аутентификацией по протоколу TLS), роутер – сервер

При выборе протокола передачи данных в поле **Transport Protocol** следует учитывать, что по протоколу UDP тоннель 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.

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

Для настройки OpenVPN-тоннеля 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** (см. далее описание);
6. А также настройте остальные параметры на странице в зависимости от требуемой конфигурации (см. таблицы 2.1 и 2.2).

При выборе данного метода аутентификации, все настройки в окне интерфейса такие же, как в разделе 2.1.2, к ним прибавляется лишь поля для указания сертификатов и ключей: **CA Certificate**, **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 тоннеля понадобятся файлы, указанные в таблице 2.3, кроме файла Диффи-Хелмана. Пример настройки показан на рис. 2.6.

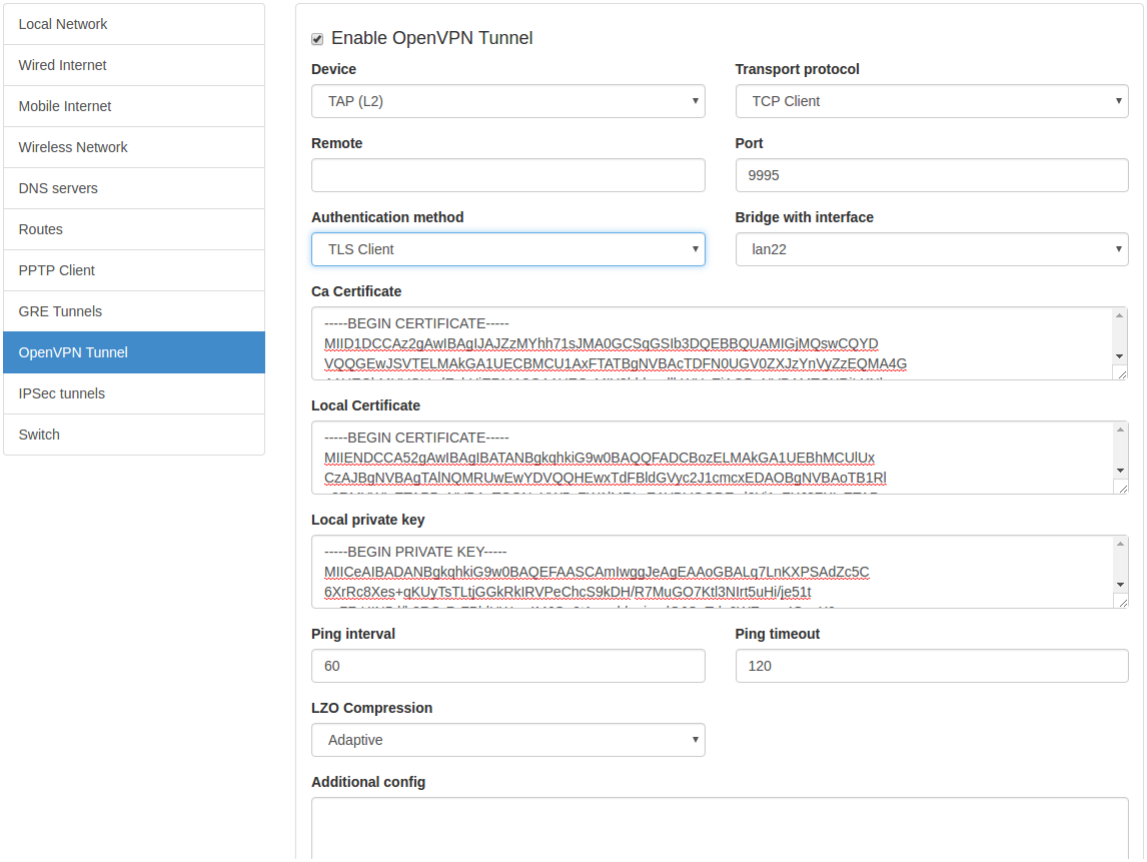

Рис. 2.6. Настройка OpenVPN (с аутентификацией по протоколу TLS), роутер – клиент

2.2. OpenVPN Layer 3: dev TUN

OpenVPN тоннель бывает двух типов: Ethernet Bridging и Routing. В данном разделе рассматривается тоннель OpenVPN типа Routing.

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

Всего четыре варианта настройки тоннеля, 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 тоннель 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:

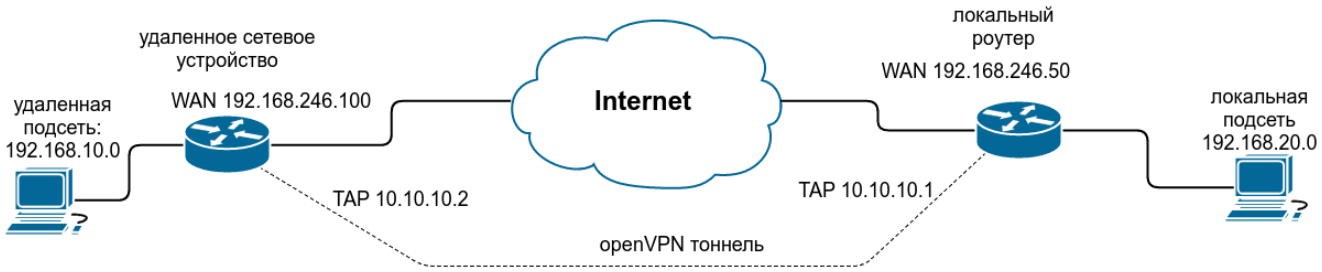

Рис. 2.7. Схема сети

2.2.1. Пример настройки тоннеля без аутентификации (Authentication method: None)

Для настройки OpenVPN-тоннеля 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**;
5. А также настройте остальные параметры на странице в зависимости от требуемой конфигурации (см. таблицы 2.4 и 2.5).

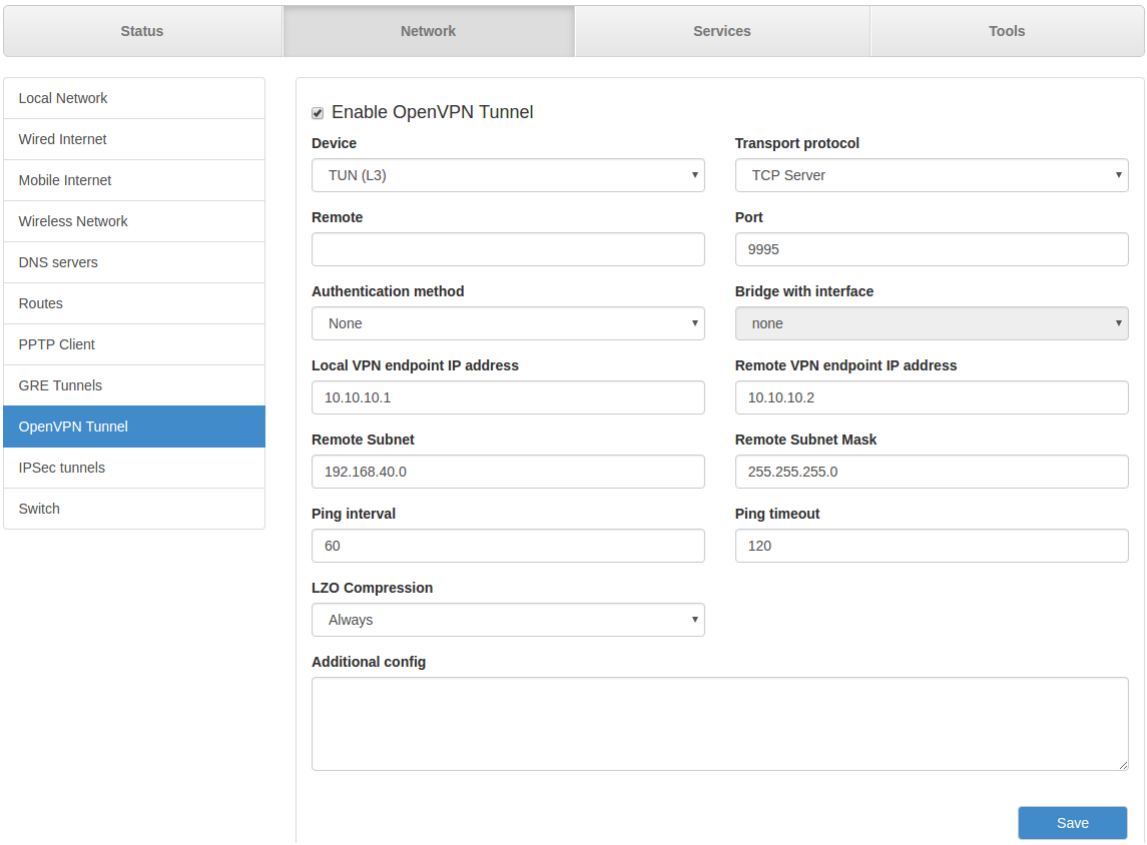

Рис. 2.8. Настройка OpenVPN (без аутентификации), базовая TUN (L3)

Таблица 2.4. 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 тоннель
Authentification Method	Метод авторизации (в данном примере – **None**)
Bridge with Interface	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 тоннеля)
Ping Timeout	Время ожидания в секундах, через которое устройство попытается заново создать OpenVPN-тоннель, если ответ от удаленного устройства не будет получен
LZO Compression	Включение или отключение сжатия данных, проходящих через тоннель

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

Таблица 2.5. Настройки OpenVPN Tunnel → TUN (L3), Bridge with Interface = None

Поле	Описание
Local VPN Endpoint IP Address	IP-адрес тоннеля на данном устройстве*
Remote VPN Endpoint IP Address	Удаленный IP-адрес тоннеля (устройство на другом конце тоннеля)*
Remote Subnet	IP-адрес удаленной сети (на другом конце тоннеля), который необходим для создания маршрута в таблице маршрутизации
Remote Subnet Mask	Маска удаленной сети (на другом конце тоннеля)
Remote Gateway	Шлюз удаленной сети (на другом конце тоннеля)

***** Так как тоннель OpenVPN с маршрутизацией является тоннелем по типу point-to-point, поэтому адреса в этих полях должны указываться с учётом маски сети /32 (255.255.255.255) и не должны совпадать с адресами локальных сетей на концах тоннеля.

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

2.2.2. Пример настройки тоннеля с аутентификацией по ключу (Authentication method: Shared Secret)

Для настройки OpenVPN-тоннеля 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);
6. А также настройте остальные параметры на странице в зависимости от требуемой конфигурации (см. таблицы 2.4 и 2.5).

При выборе данного метода аутентификации, большинство настроек в окне интерфейса такие же, как в разделе 2.2.1, к ним прибавляется лишь поле **Shared Secret**, в котором указывается общий ключ. Сам ключ необходимо заранее сгенерировать и распространить на устройствах участниках (см. рис. 2.4).

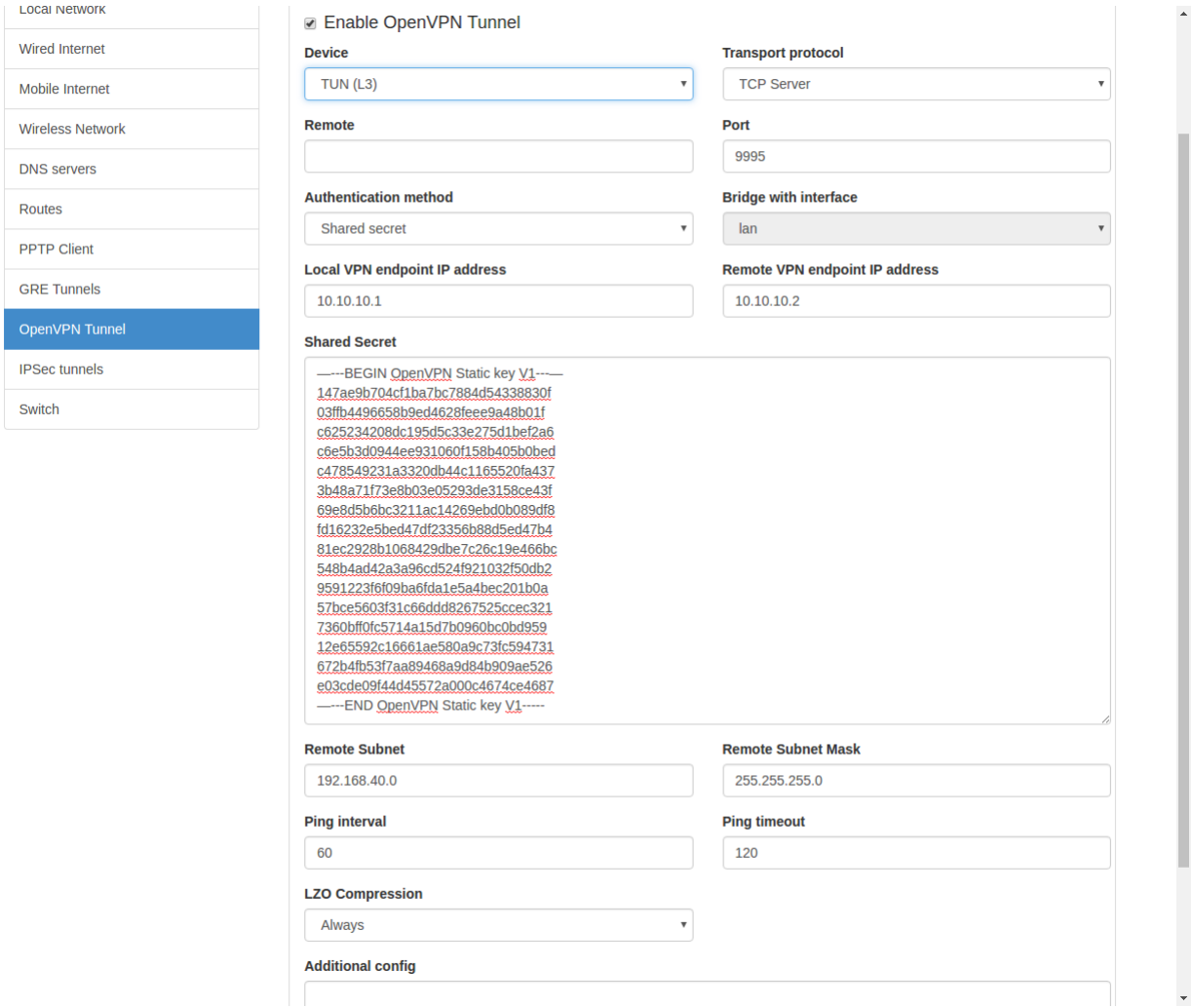

Рис. 2.9. Настройка OpenVPN (с аутентификацией по ключу)

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

Для настройки OpenVPN-тоннеля 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);
6. А также настройте остальные параметры на странице в зависимости от требуемой конфигурации (см. таблицы 2.4 и 2.5).

При выборе данного метода аутентификации, все настройки в окне интерфейса такие же, как в разделе 2.2.1, к ним прибавляется лишь поля для указания сертификатов и ключей: **CA Certificate**, **DH Parameter**, **Local Certificate**, **Local Private Key**. Необходимые 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 тоннеля понадобятся файлы, указанные в таблице 2.6.

Таблица 2.6. Ключи и сертификаты для аутентификации по протоколу TLS

Поле	Файл	Описание
CA Certificate	ca.crt	Сертификат удостоверяющего центра
DH Parameter	dh1024.pem	Файл 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

Из полученных файлов необходимо будет скопировать зашифрованные данные, которые начинаются строкой “BEGIN CERTIFICATE”, а заканчиваются “END CERTIFICATE”, и вставить текст в соответствующие поля согласно таблице 2.6. Пример настройки показан на рис. 2.10.

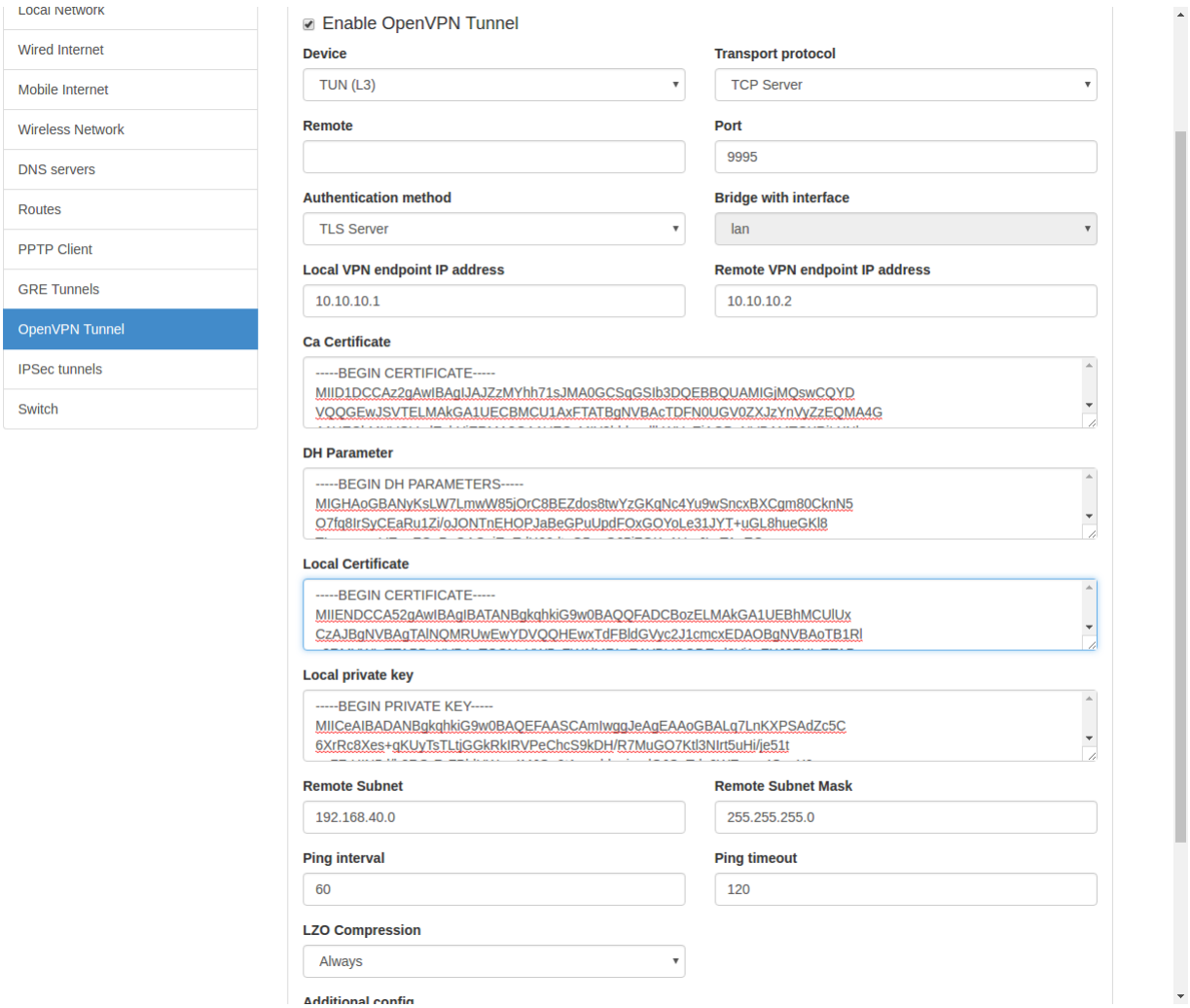

Рис. 2.10. Настройка OpenVPN (с аутентификацией по протоколу TLS), роутер – сервер

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

Для настройки OpenVPN-тоннеля 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** (см. далее описание);
6. А также настройте остальные параметры на странице в зависимости от требуемой конфигурации (см. таблицы 2.1 и 2.2).

При выборе данного метода аутентификации, все настройки в окне интерфейса такие же, как в разделе 2.2.1, к ним прибавляется лишь поля для указания сертификатов и ключей: **CA Certificate**,

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 тоннеля понадобятся файлы, указанные в таблице 2.6, кроме файла Диффи-Хелмана. Пример настройки показан на рис. 2.11.

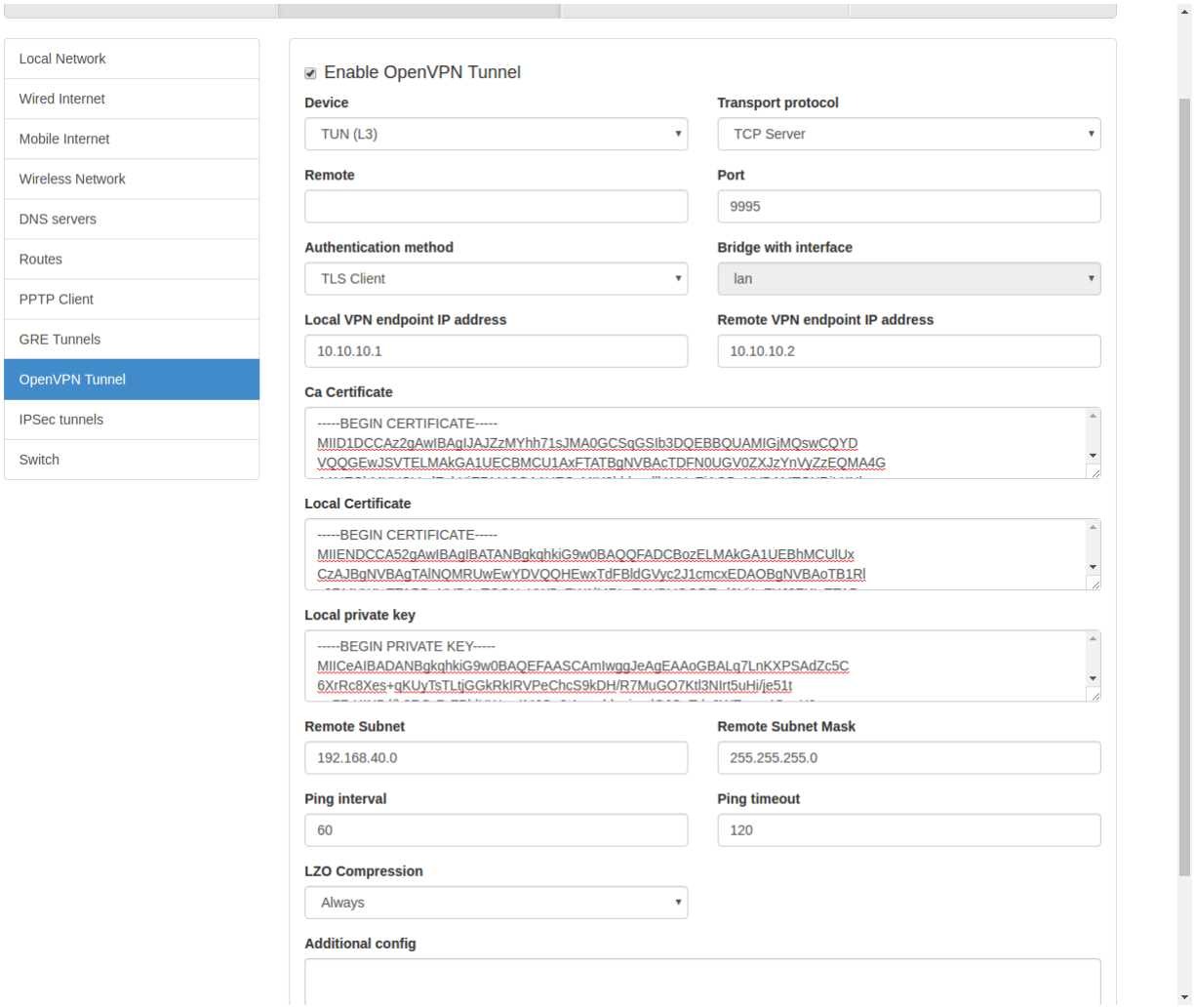

Рис. 2.11. Настройка OpenVPN (с аутентификацией по протоколу TLS), роутер – клиент

2.3. Инструкция по настройке тоннеля GRE (на примере роутеров iRZ R4)

2.3.1. Настройка GRE-тоннеля уровня L2 (на примере двух роутеров RU41)

В примерах настройки используется следующая схема сети:

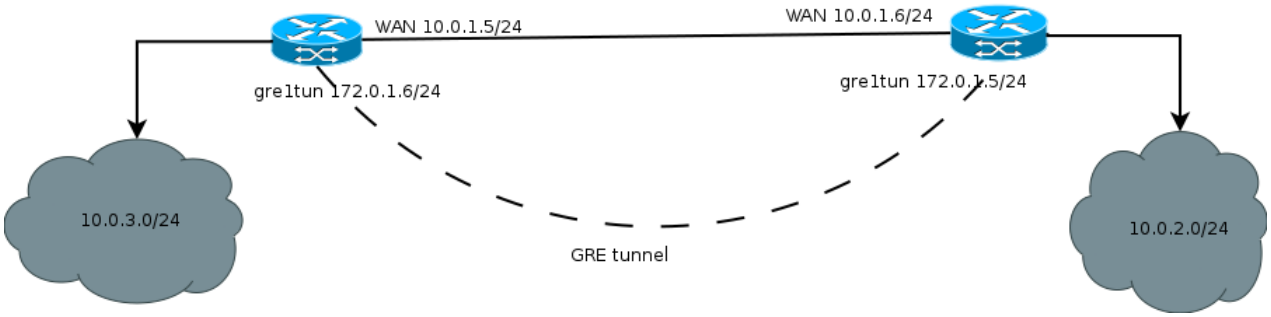

Рис. 2.12. Схема сети

Для настройки GRE-тоннеля уровня L2, в веб-интерфейсе роутера (см. рис. 2.13):

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

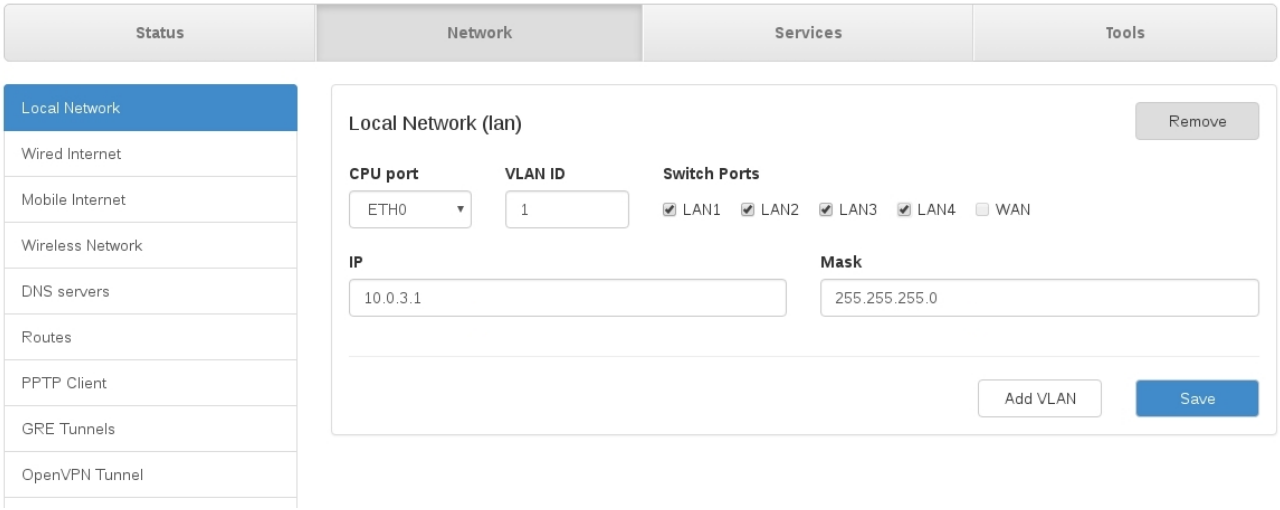

Рис. 2.13. Настройка локальной сети

Далее необходимо настроить WAN-порт роутера (см. рис. 2.14):

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

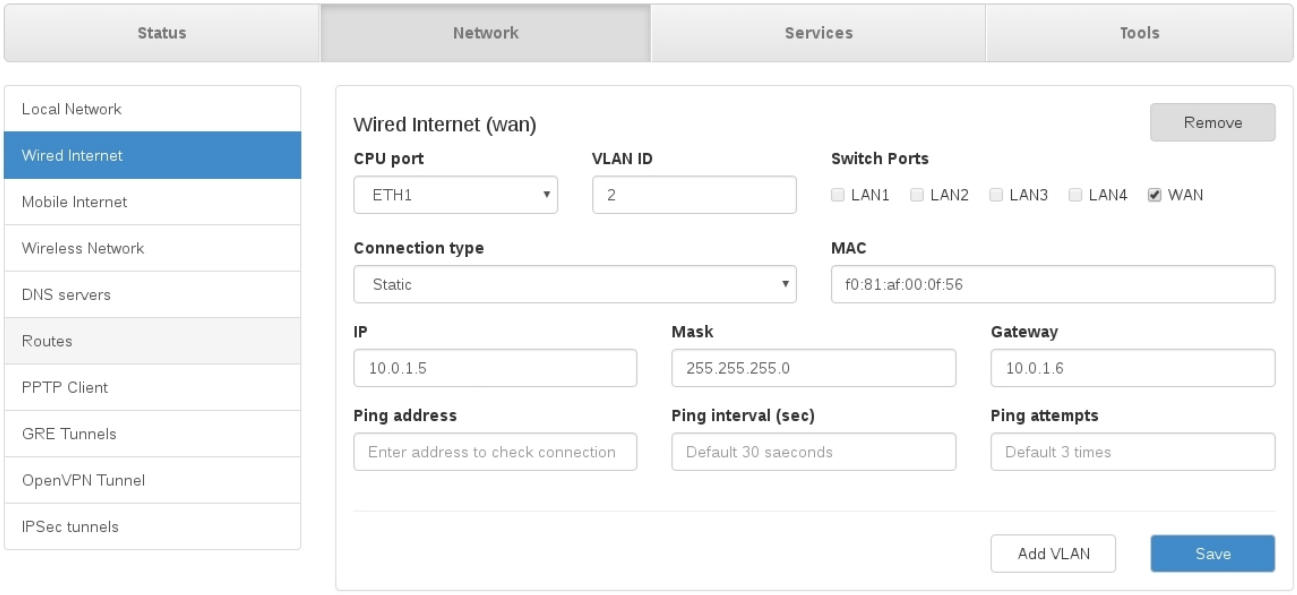

Рис. 2.14. Настройка WAN

Далее необходимо настроить GRE-тоннель (см. рис. 2.15):

6. Зайдите в раздел **Network** → **GRE Tunnels**;
7. Добавьте новый тоннель, нажав на кнопку **Add Tunnel**;
8. Введите имя тоннеля (на выбор пользователя) в поле **Name**;
9. Выберите локальный интерфейс, через который будет работать тоннель в поле **Local Address** (поскольку в данном примере показана настройка через WAN-порт, то соответственно – **WAN**);
10. Укажите IP-адрес порта удаленного устройства, с которым будет построен тоннель, в поле **Remote Address**;
11. Выберите на каком уровне будет работать тоннель в поле **Network Type** (в данном примере рассматривается **L2**);
12. Выберите в каком интерфейсе будет работать GRE-тоннель, выбрав значение в поле **Interface** (если **Interface** = **LAN** или **WAN**, то дополнительных настроек не требуется, если **Interface** = **<Custom Network>** [пользовательская сеть], то необходимо будет указать IP-адрес пользовательского интерфейса в поле **Tunnel IP** и маску сети в поле **Tunnel Mask**);
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**.

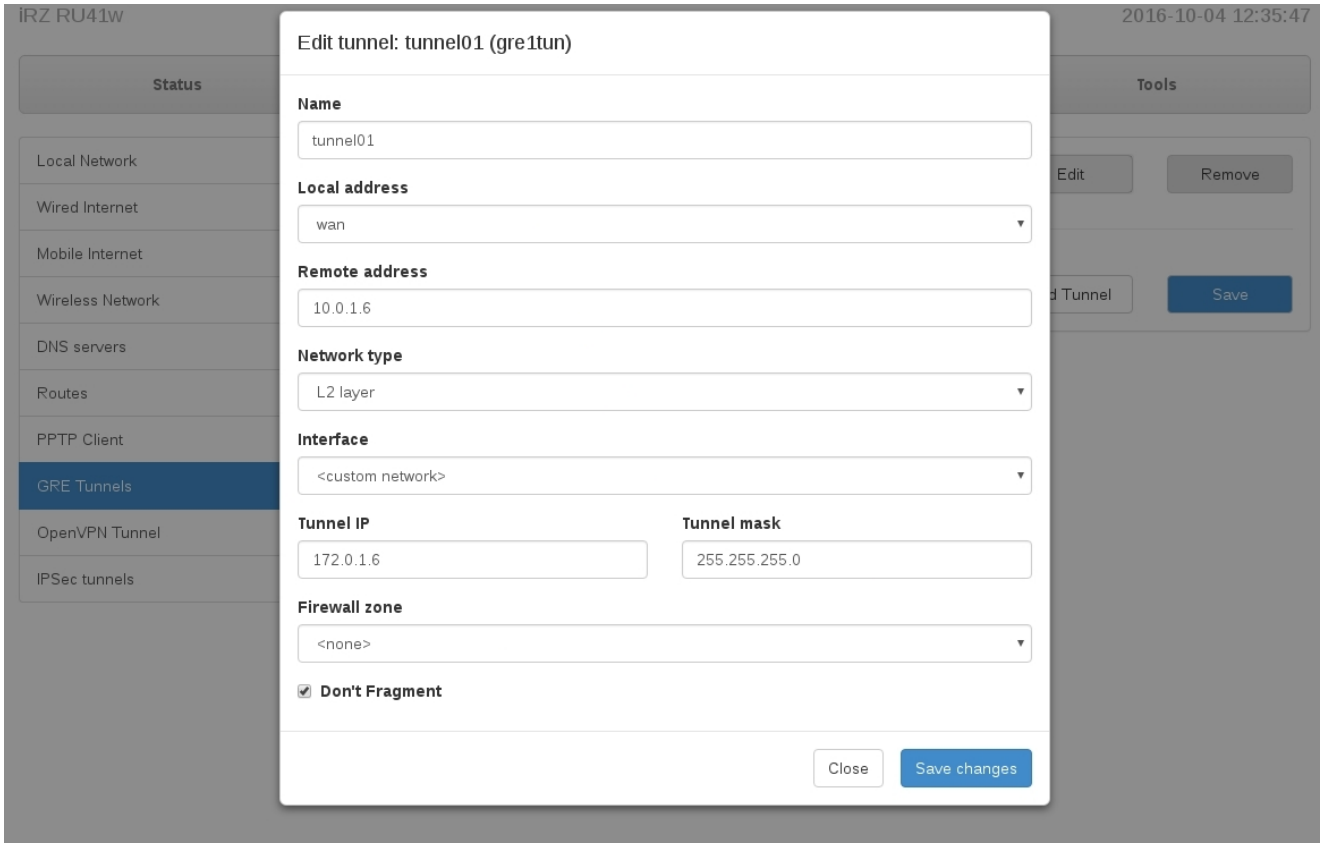

Рис. 2.15. Настройка GRE-тоннеля

2.3.2. Настройка GRE-тоннеля уровня L3 (на примере двух роутеров RU41)

В примерах настройки используется следующая схема сети:

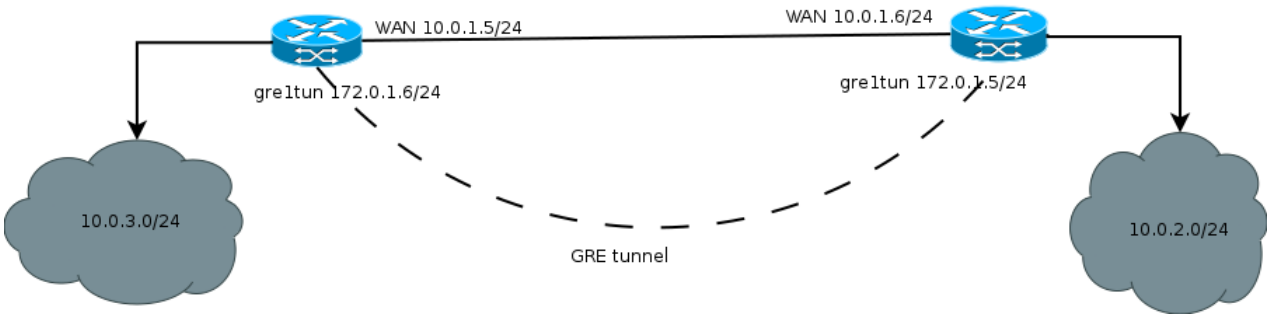

Рис. 2.16. Схема сети

Для настройки GRE-тоннеля уровня L3, в веб-интерфейсе роутера (см. рис. 2.17):

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

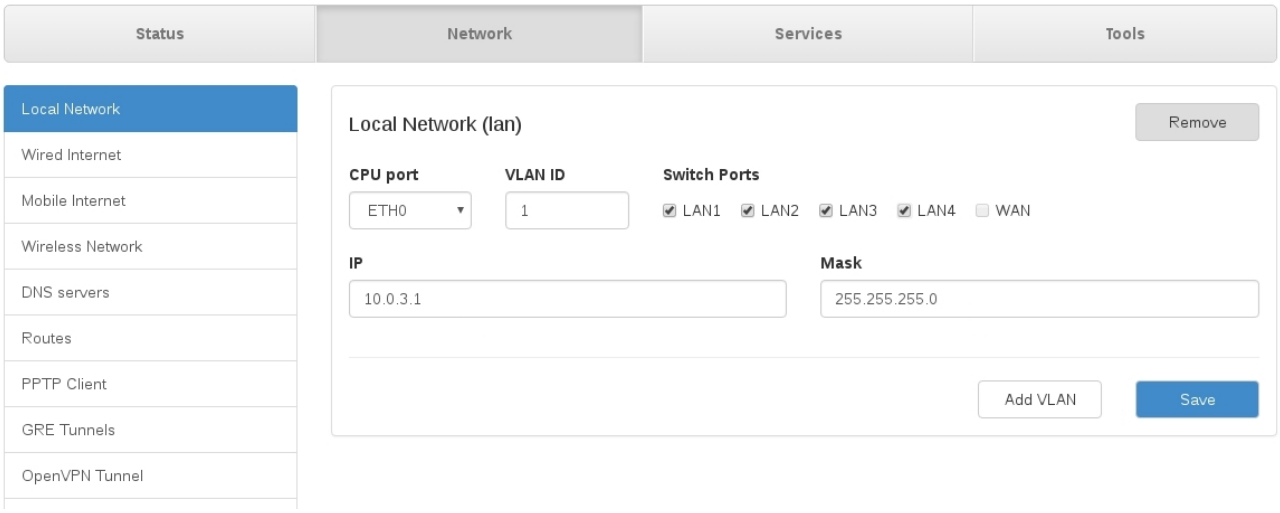

Рис. 2.17. Настройка локальной сети

Далее необходимо настроить WAN-порт роутера (см. рис. 2.18):

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

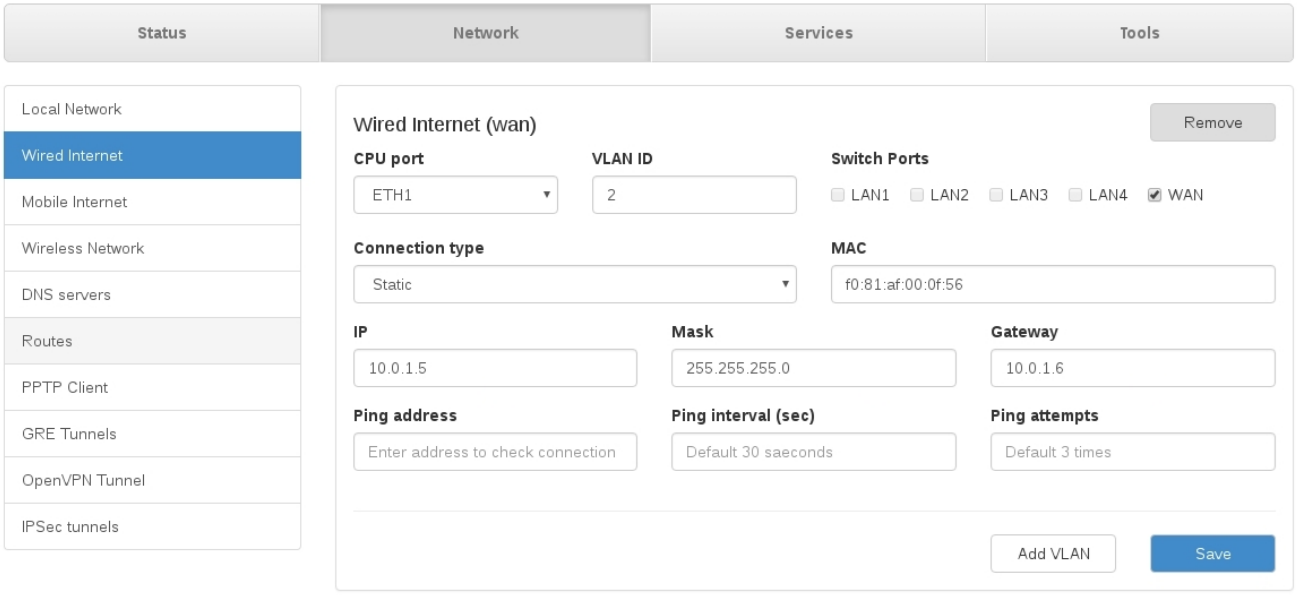

Рис. 2.18. Настройка WAN

Далее необходимо настроить GRE-тоннель (см. рис. 2.15):

6. Зайдите в раздел **Network** → **GRE Tunnels**;
7. Добавьте новый тоннель, нажав на кнопку **Add Tunnel**;
8. Введите имя тоннеля (на выбор пользователя) в поле **Name**;
9. Выберите локальный интерфейс, через который будет работать тоннель в поле **Local Address** (поскольку в данном примере показана настройка через WAN-порт, то соответственно – **WAN**);
10. Укажите IP-адрес порта удаленного устройства, с которым будет построен тоннель, в поле **Remote Address**;
11. Выберите на каком уровне будет работать тоннель в поле **Network Type** (в данном примере рассматривается **L3**);
12. Укажите IP-адрес интерфейса в поле **Tunnel IP**;
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**.

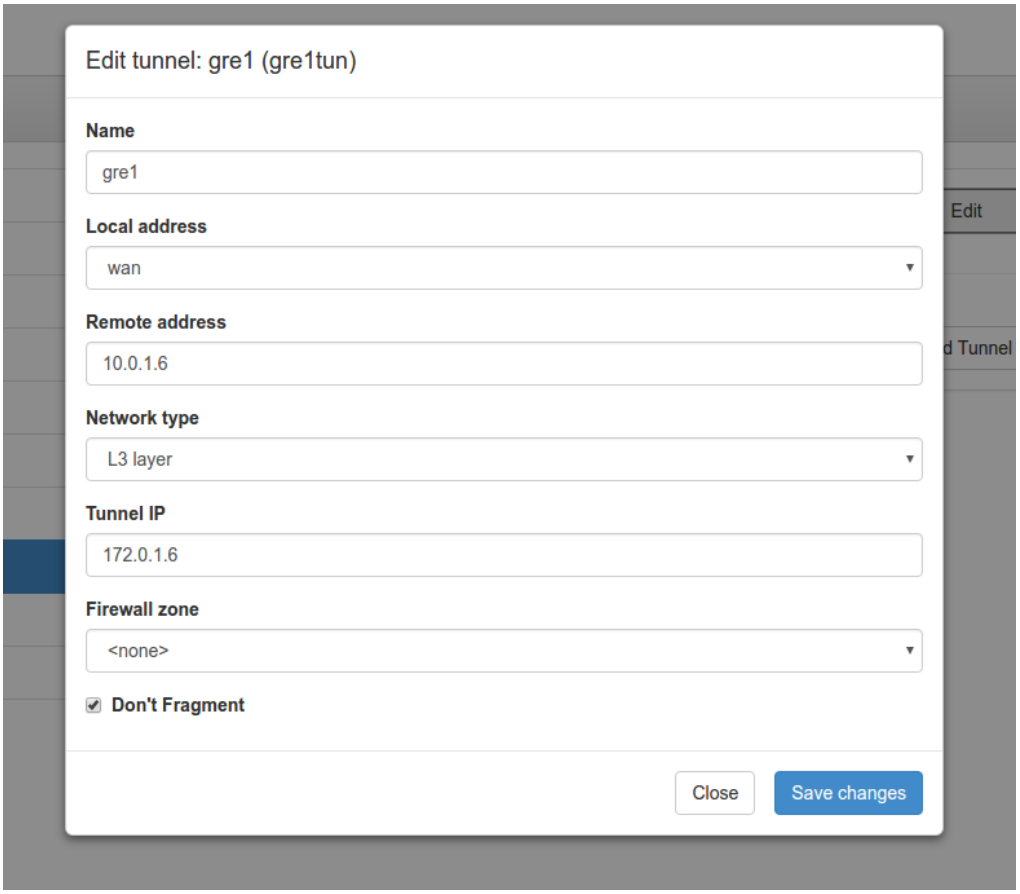

Рис. 2.19. Настройка GRE-туннеля

2.4. Создание IPsec-тоннеля (на роутерах серии R4, R1)

Для создания IPsec-тоннеля на роутере должна быть настроена локальная сеть и порты WAN, затем в веб-интерфейсе роутера (см. рис. 2.20):

1. Зайдите в раздел **Network → IPsec Tunnels**;

В данном разделе в полях **Port** и **NAT-T Port** уже занесены значения, чаще всего используемые при создании тоннелей по стандартам IPsec. Поле **Port** указывает на порт, через который будут работать тоннели, если настраиваемый роутер имеет внешний «белый» IP-адрес. А поле **NAT-T Port** указывает тоннелю через какой порт будет осуществляться связь в случае, если роутер находится в зоне NAT.

2. Добавьте новый IPsec-тоннель, нажав на кнопку **Add Tunnel**;

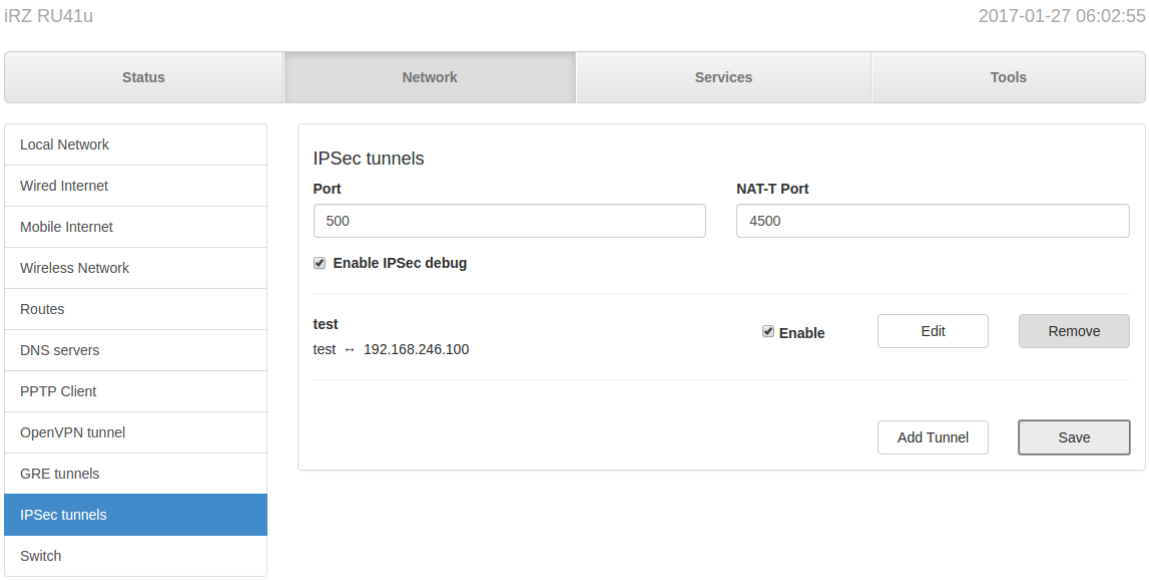

Рис. 2.20. Настройка IPsec-тоннеля

Далее необходимо настроить параметры тоннеля (см. рис. 2.21):

3. Введите имя тоннеля (на выбор пользователя) в поле **Name**;
4. Выберите физический порт, через который будет работать тоннель, выбрав значение в поле **Source Address** (**Default** – через порт, 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 тоннель, в поле **Remote Address**;
6. Укажите интервал в секундах, через который будет определяться доступность узла на противоположном конце тоннеля, указав значение в поле **Dead Peer Detect** (**0** – отключение данной функции);
7. Выберите режим установления соединения между участниками тоннеля, выбрав значение в поле **Exchange Mode** (**Main** – основной, **Aggressive** – более активный [быстрый], но без обеспечения защиты подлинности);
8. Настройте параметры **SA Info**, для работы IPsec SA:

SAInfo	
Local Address	IP-адрес локальной сети, участвующей в тоннеле
Local Netmask	Сетевая маска локальной сети, участвующей в тоннеле
Remote Address	IP-адрес удаленной сети, участвующей в тоннеле
Remote Netmask	Сетевая маска удаленной сети, участвующей в тоннеле

9. Настройте фазу 1 и фазу 2, заполнив соответствующие поля в блоках **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)
Encryption Algorithm	Выбор алгоритма шифрования: **AES**, **AES 128**, **AES 192**, **AES 256**, **DES**, **3DES**.
Hash Algorithm	Выбор алгоритма для проверки целостности данных: **SHA-1**, **SHA-256**, **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)
Encryption Algorithm	Выбор алгоритма шифрования: **AES**, **AES 128**, **AES 192**, **AES 256**, **DES**, **3DES**.
Authentication Algorithm	Выбор алгоритма для проверки целостности данных: **HMAC SHA-1**, **HMAC SHA-256**, **HMAC SHA-384**, **HMAC 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.

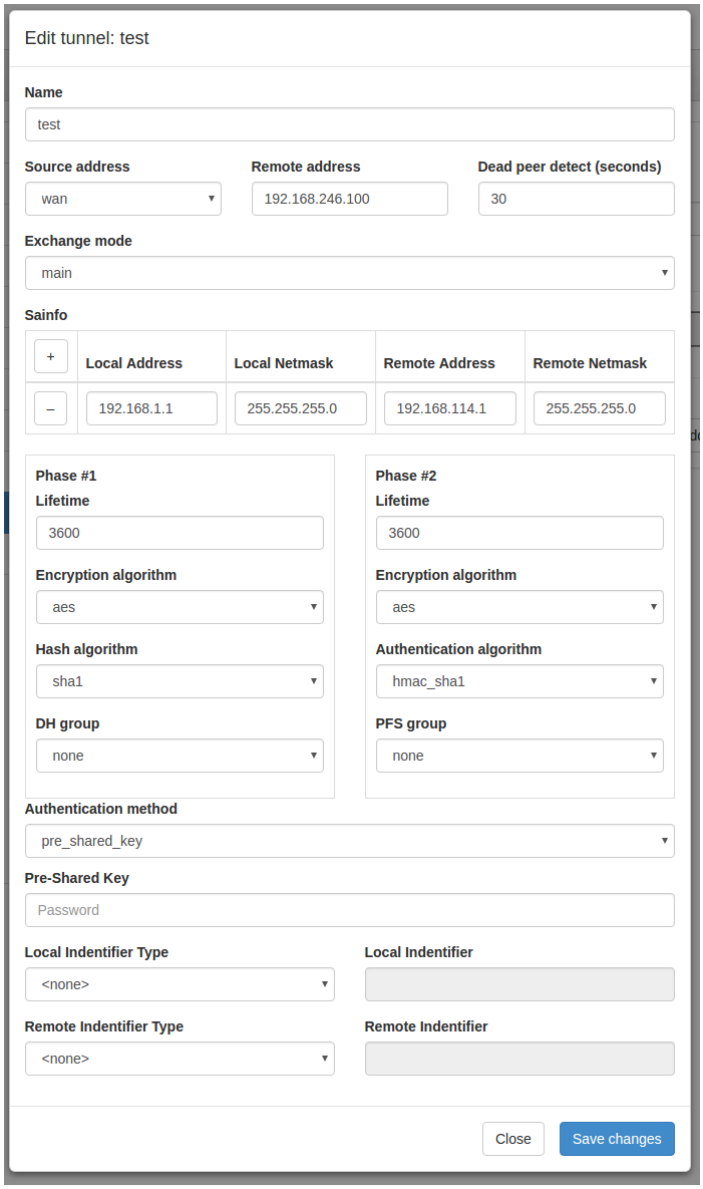

Рис. 2.21. Параметры туннеля

10. Выберите способ аутентификации узлов тоннеля, выбрав значение в поле **Authentication Method** (**pre-shared key** – по общему ключу, **rsasig** – по сертификату и ключу RSA);

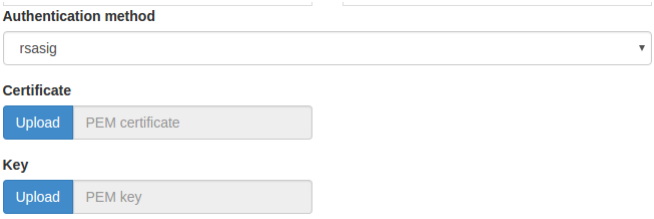

Рис. 2.22. Параметр Authentication Method

Сертификат и ключ необходимо получить от сертификационного центра (CA) и распространить среди участников тоннеля.

11. Выберите признаки идентификации ключей:

Local Identifier Type	Тип локального идентификатора
Remote Identifier Type	Тип удаленного идентификатора
Local Identifier	Значение локального идентификатора
Remote Identifier	Значение удаленного идентификатора

Значения идентификаторов могут быть в виде:

None – без идентификатора;

IP Address – IP-адрес;

FQDN – FQDN-адрес (полный доменный адрес, например, irz.net);

User FQDN – пользовательский FQDN-адрес (например, sales@irz.net);

ASN1DN – известное имя в формате описания ASN.1 (ASN.1 Distinguished Name).

3. Термины и сокращения

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 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.

4. Контакты и поддержка

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. Также 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.

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

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