Wireless solutions
for M2M world

Создание виртуальных сетей и туннелей средствами OpenVPN для роутеров iRZ

RUH, RUH2, RUH2b, RUH3, RCA

Содержание

Рисунки

Таблицы

1. Введение

1.1. Описание документа

Данный документ является частью «Пакета инструкций по обслуживанию роутера iRZ» и содержит примеры корректной конфигурации сетевой службы OpenVPN в решениях, построенных на базе роутеров iRZ. Для получения более подробной информации см. раздел 1.2.

Версия документа		**Дата публикации**	
1.0		2013-07-31	
Подготовлено:	Афанасьев Д.С., Головин В.Н.	**Проверено:**	Коробань Д.С.

1.2. Обзор пакета инструкций

Вся документация на русском языке по продукции iRZ доступна на официальном сайте группы компаний «Радиофид» (www.radiofid.ru) в разделе «Поддержка».

Содержание «Пакета инструкций по обслуживанию роутера iRZ»:

- Руководство по эксплуатации роутера iRZ;
- Описание средств управления и мониторинга роутера iRZ;
- Диагностика и методы устранения неисправностей роутера iRZ;
- Руководство по настройке роутера iRZ с помощью USB-накопителя;
- Примеры рабочих конфигураций роутера iRZ:
  - **Создание виртуальных сетей и туннелей средствами OpenVPN;**
  - Удалённый доступ к COM-порту роутера;
  - Защита передаваемых данных средствами IPSec;
  - DynDNS и обход ограничений внешнего динамического IP-адреса;
  - Объединение сетей с помощью виртуальных GRE-туннелей;
  - Сбоеустойчивость уровня сети средствами VRRP;
  - Обеспечение доступа к внутрисетевым службам средствами PortForwarding;
  - Защита локальной сети и сервисов средствами встроенного Firewall;
- Технические условия (ТУ);
- Протокол температурных испытаний;
- Декларация о соответствии.

1.3. 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. Конфигурация

«OpenVPN Server ← RXX. Точка - многоточка. Незащищённая»

Данная конфигурация позволяет организовать частную OpenVPN-сеть между роутерами и операционным центром по принципу «точка-многоточка» без использования средств защиты передаваемой информации. Связь между узлами может быть установлена через Интернет-соединение, либо с использованием выделенного канала, предоставленного оператором сотовой связи. Схема соединения узлов приведена на рис. 2.1.

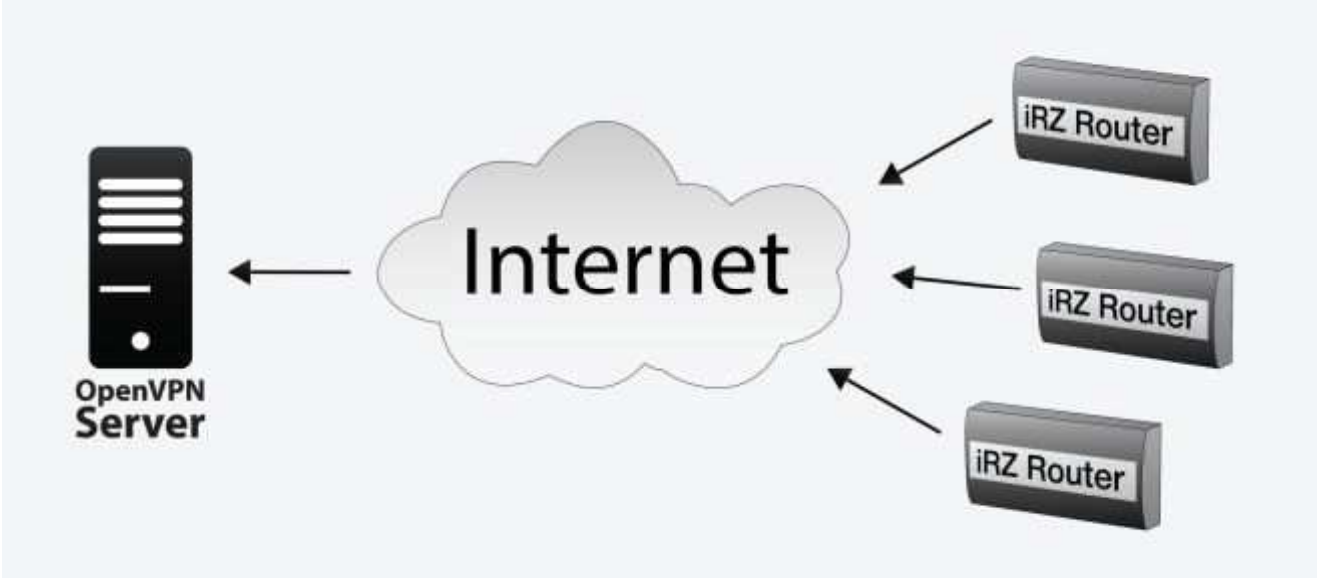

Рис. 2.1. Схема соединения «OpenVPN-сервер – роутеры iRZ (незащищенная)»

2.1.1. Подготовка к настройке

Процесс проектирования и развертывания OpenVPN-сети состоит из следующих этапов:

- определение правил именования/нумерации устройств в соответствии с порядком их географического распределения;
- определение диапазона адресного пространства и правил адресации узлов сети;
- формирование базы данных, содержащей информацию об устройствах:
  - географическое местоположение устройства;
  - порядковый номер/название;
  - виртуальный IP-адрес в будущей OpenVPN-сети (либо диапазон IP-адресов для каждой группы устройств);
- установка программного пакета OpenVPN на компьютер операционного/диспетчерского центра;
- генерирование сертификатов и ключей сервера;
- формирование файла конфигурации сервера OpenVPN;
- формирование набора файлов конфигурации клиентов;
- формирование базы данных аутентификации клиентских узлов;
- запуск сервера OpenVPN;
- настройка Интернет-подключения на роутерах;
- настройка OpenVPN-клиента на роутерах;
- проверка подключения нескольких настроенных узлов к серверу OpenVPN.

Описание процесса проектирования развёртываемой сети, а также настройки интернет-подключения на роутерах выходит за рамки данного документа. Для получения рекомендаций по проектированию следует обратиться к документу «**Руководство по развёртыванию решений на базе роутера iRZ**». Описание настройки Интернет-подключения на роутерах представлено в документе «**Руководство по эксплуатации роутеров iRZ**» (см. разд. «Интернет соединение по GSM-каналу»).

Ниже представлен процесс настройки OpenVPN-сервера. К настройке OpenVPN-сервера следует приступать, когда комплект подготовительной информации уже сформирован техническим персоналом компании-заказчика.

2.1.2. Создание сертификатов и ключей сервера

После установки программного пакета OpenVPN необходимо создать файлы корневого и серверных сертификатов, а также ключ сервера. Это обязательное требование к любым видам сетей на базе OpenVPN, независимо от поставленных задач и топологии связей между узлами.

Генерирование необходимых файлов представляет из себя стандартную процедуру и не требует серьёзных знаний в области шифрования.

Минимальный набор файлов необходимых для подсистемы авторизации и шифрования OpenVPN включает в себя:

- корневой сертификат должен использоваться на всех серверах компании (файл **“ca.crt”**);
- сертификат сервера (файл **“my-server.crt”**);
- криптографический ключ сервера (файл **“my-server.key”**);
- файл энтропии Diffie-Hellmann’a (файл **“dh1024.pem”**).

Для создания файлов необходимо выполнить следующие действия:

1. Откройте командную строку ОС Windows;
   («Пуск» → «Выполнить» → ввести «cmd» → [Enter])
2. Перейдите в каталог OpenVPN с набором утилит «EasyRSA»;
   (команда «cd /d “%programfiles%\OpenVPN\easy-rsa”», [Enter])
3. Введите команду «init-config», [Enter];
4. При необходимости отредактируйте файл “vars.bat”;
   (данный файл предназначен для установки информации об организации, выпускающей сертификаты и ключи)
5. Введите команды:
   - “vars”, [Enter]
   - “clean-all”, [Enter]
6. Запустите генерацию корневого сертификата вводом команды «build-ca», [Enter];
   (нажимать [Enter], до появления запроса Common Name)
7. Введите любое значение Common Name: «my-server», [Enter];
8. Запустите генерацию ключа сервера вводом команды «build-key-server [server-name]»;
   (где server-name – любое имя сервера, в этом примере – «my-server»)
9. Запустите генерацию файла «Diffie-Hellman» вводом команды «build-dh».

После выполнения указанных действий в каталоге **“[диск]:\Program Files\OpenVPN\easy-rsa”** должны появится следующие файлы:

- “ca.crt”;
- “ca.key”;
- “dh1024.pem”;
- “my-server.crt”;
- “my-server.key”.

Примечание: После того как все файлы созданы, следует выполнить их резервное копирование на другой физический носитель во избежание утери. В случае замены/обновления корневого сертификата на сервере также станет необходимым обновление корневого сертификата во всём парке роутеров.

2.1.3. Формирование файла конфигурации OpenVPN-сервера

Настройка OpenVPN-сервера происходит путём формирования конфигурационного текстового файла, состоящего из уникальных параметров/директив и выполненного в строгом соответствии с рекомендациями данного документа.

Примечание: При необходимости получить дополнительную информацию о других директивах конфигурации, а так же о других вариантах использования директив, описанных в данном документе, следует обратиться к официальному ресурсу разработчика программного пакета «OpenVPN Community Server» по адресу **http://openvpn.net/**

Файл конфигурации OpenVPN всегда можно отличить от других файлов по расширению **“.ovpn”** в конце имени файла. Ниже (см. листинг 1) приведён пример уже готового конфигурационного файла, а также описание наиболее важных параметров и пояснения их значений.

Листинг 1. Пример конфигурационного файла «server.ovpn»

```
dev tun
port 1194
proto tcp-server
mode server
server 10.1.0.0 255.255.255.0

client-config-dir ".\\ccd"
topology subnet

tls-server
ca ".\\..\\easy-rsa\\keys\\ca.crt"
cert ".\\..\\easy-rsa\\keys\\my-server.crt"
key ".\\..\\easy-rsa\\keys\\my-server.key"
dh ".\\..\\easy-rsa\\keys\\dh1024.pem"

client-cert-not-required
username-as-common-name
auth-user-pass-verify  ".\\..\\config\\ovpn-irz-auth.bat"  via-
env
script-security 3

keepalive 10 120
verb 2
```

Примечание: Для редактирования файлов рекомендуется использовать программу-редактор текстовых файлов Notepad++, свободно доступную для скачивания с сайта **http://notepad-plus-plus.org**

Таблица 1. Описание директив конфигурации сервера OpenVPN

Название	Значения	Описание
dev	tun tap	Определяет тип псевдо-устройства, используемого для связи сетевого пространства компьютера с виртуальным сетевым пространством сети OpenVPN. В большинстве ситуаций должен иметь значение **tun** – «туннель»
port	[1…65535]	Указывает порт, на котором будут приниматься подключения от клиентов OpenVPN. По умолчанию **1194**, не может быть больше **65535**
proto	tcp-server udp	Определяет протокол взаимодействия между клиентом и сервером, при неустойчивом канале связи рекомендуется использовать **tcp-server**. Значение **udp** может быть использовано, если и клиент и сервер имеют публичные («белые») IP-адреса, это повысит пропускную способность канала между сервером и клиентом
mode	server client	Определяет режим работы программы OpenVPN, в обсуждаемой конфигурации выбран сервер – **server**
server	10.1.0.0 255.255.255.0	Определяет виртуальное адресное пространство OpenVPN-сети, первая часть значения – IP-адрес сети (**10.1.0.0**), вторая – маска сети (**255.255.255.0**)
client-config-dir	".\\ccd"	Определяет путь к каталогу «CCD», содержащему конфигурационные файлы клиентов OpenVPN, рекомендуется использовать полные пути и кавычки *
topology	subnet	Определяет топологию связей между клиентами и сервером OpenVPN и правила распределения адресного пространства
tls-server	–	Определяет роль OpenVPN-сервера в процессе синхронизации TLS-протокола
dh	".\\dh1024.pem"	Определяет местоположение файла Diffie-Hellman
ca	".\\ca.crt "	Определяет местоположение файла корневого сертификата
cert	".\\my-server.crt "	Определяет местоположение файла сертификата сервера
key	".\\my-server.key "	Определяет местоположение файла ключа сервера
client-cert-not-required	–	Отключает принудительное требование предоставления клиентом сертификата в момент подключения
username-as-common-name	–	Определяет Common Name для клиента на основе имени учётной записи, представленном в момент аутентификации
auth-user-pass-verify	“.\\file.bat" via-env	Определяет команду/программу, выполняющую аутентификацию подключившегося клиента по собственной базе учетных записей
script-security	3	Определяет внутренние параметры безопасности процедруры взаимодействия с программой-аутентификатором
keepalive	10 120	Определяет интервал между проверками и предел, после которого туннель разрывается
verb	0 – 9	Определяет степень подробности log-файла журнала запуска
status	“.\\runtime-file.log”	Указывает путь для сохранения log-файла журнала

* при указании пути символ каталога должен быть обязательно экранирован таким же вторым символом: “ \\ ” во всех значениях параметров, указывающих путь к файлу или каталогу

2.1.4. Формирование набора файлов конфигурации клиентов

Настройку клиентских узлов следует начинать с их CCD-конфигураций.

CCD (**client configuration directory**) – специальная функция OpenVPN, призванная автоматизировать и упорядочить параметры всех клиентов OpenVPN-сети как на этапе пуско-наладки так и непосредственно в процессе функционирования сети. Параметр «**client-config-dir**» позволяет задействовать данную функцию и указать каталог, в котором будут храниться файлы настроек клиентов сети.

Основные правила создания CCD-файлов:

- имя файла должно в точности повторять имя Common Name клиента, к которому будет применяться конфигурация;
- имя файла не должно иметь расширения;
- пробелы, спецсимволы и непечатаемые символы недопустимы.

  пример правильного именования файла**: client_02**
  пример НЕправильного именования файла**: ~~client_02.txt~~**
- файл может содержать только следующие директивы:
  push / push-reset / iroute / ifconfig-push / config;
- два (и более) файла не могут содержать одинаковое значение параметра «**ifconfig-push**».

Пример клиенского CCD-файла приведён в листинге 2.

Листинг 2. Пример клиенсткого CCD-файла «client_02»

```
ifconfig-push 10.1.0.2 255.255.255.0
```

В данном файле использована директива **ifconfig-push,** указывающая серверу OpenVPN, что клиенту с именем Common Name **client_02** должен быть присвоен IP-адрес **10.1.0.2** с маской подсети **255.255.255.0**.

IP-адрес, присваиваемый клиенту должен находиться в адресном пространстве сети OpenVPN, которую обслуживает сервер. Диапазон сети указывается в конфигурационном файле сервера (см. табл. 1, директива **server**).

Примечание: Количество CCD-файлов ограничено адресным пространством OpenVPN-сети, т.е. максимальным количеством IP-адресов в диапазоне сети.

2.1.5. Формирование файла базы данных аутентификации

База аутентификации представляет из себя простой текстовый файл с расширением «**.db**», внутри которого располагаются имена пользователей и пароли учётных записей клиентов OpenVPN. Для создания файла базы данных достаточно воспользоваться простым текстовым редактором, к примеру «Notepad++». Пример файла базы данных приведён в листинге 3.

Листинг 3. Файл БД аутентификации клиентов OpenVPN-сети «ovpn-irz-users.db»

```
user2:passwd123
anonymous713:fee4513j1k32qeh
client_02:qwhjkjhf
user3:abdenfl
```

Правила формирования файла базы данных:

- пароль не может содержать пробелов, спецсимволов и непечатаемых символов;
- на каждой строке может быть размещена информация только об одном клиенте;
- напротив имени пользователя после знака двоеточия **неразрывно** следует пароль;
- файл базы данных должен всегда содержать в конце пустую строку.

Внимание! В случае не соблюдения правила «последней строки» учетная запись, чьё имя пользователя будет последним не будет иметь возможность предоставить клиенту доступа в OpenVPN-сеть!

Файл базы данных будет использован программой, имя которой передано в качестве параметра OpenVPN-серверу (таблица 1, директива **auth-user-pass-verify**).

Поскольку программный пакет OpenVPN не имеет встроенных средств работы с текстовыми базами данных, а также для обеспечения удобства и возможности без лишних временных затрат добавлять учётные записи, расширяя сеть OpenVPN, рекомендуется использовать программу-сценарий, предоставленную компаниям-заказчикам для свободного использования.

Данная программа выполняет промежуточную функцию в процессе получения клиентскими узлами доступа к виртуальной сети, управляемой данным сервером. Она производит аутентификацию узлов, подключившихся к OpenVPN-серверу и запрашивающих доступ к сети.

Текст программы приведён в листинге 4.

Листинг 4. Программа-сценарий авторизации клиентов OpenVPN «irz-auth-routine.bat»

```
@echo off
REM Preparing
set irz_usr=%username%
set irz_pw=%password%

REM Config section
set debug=0
set passwords_in_log=1
set auth_db=ovpn-irz-users.db

REM Main section
REM ---------------------------------------------
echo.
echo.
echo       iRZ Authentication routine
echo  ---------------------------------------------
echo.
if "%debug%"=="1" (
     echo  :::: system env stack ::::
     echo.
     set
     echo.
     echo  ::::::::::::::::::::::::::
     echo.
)
echo   [i] user [UID='%irz_usr%',IP=%untrusted_ip%] attempting to log in to
network..
if "%passwords_in_log%"=="1" echo   [^>] using password ['%irz_pw%']
echo   [*] checking users database [%auth_db%]..
"%systemroot%\system32\findstr.exe" /x /c:%irz_usr%:%irz_pw% "%cd%\%auth_db%"
>nul
if "%errorlevel%"=="0" goto :login
:fail
echo   [!] password failed, rejecting
set errorlevel=1
echo.
echo  ----------------------------------------
echo.
exit 1
:login
echo   [A] password succeed, access granted
echo  ----------------------------------------
echo.
echo.
```

Так же программу всегда можно получить на сайте компании **«Радиофид Системы»** (**www.radiofid.ru**).

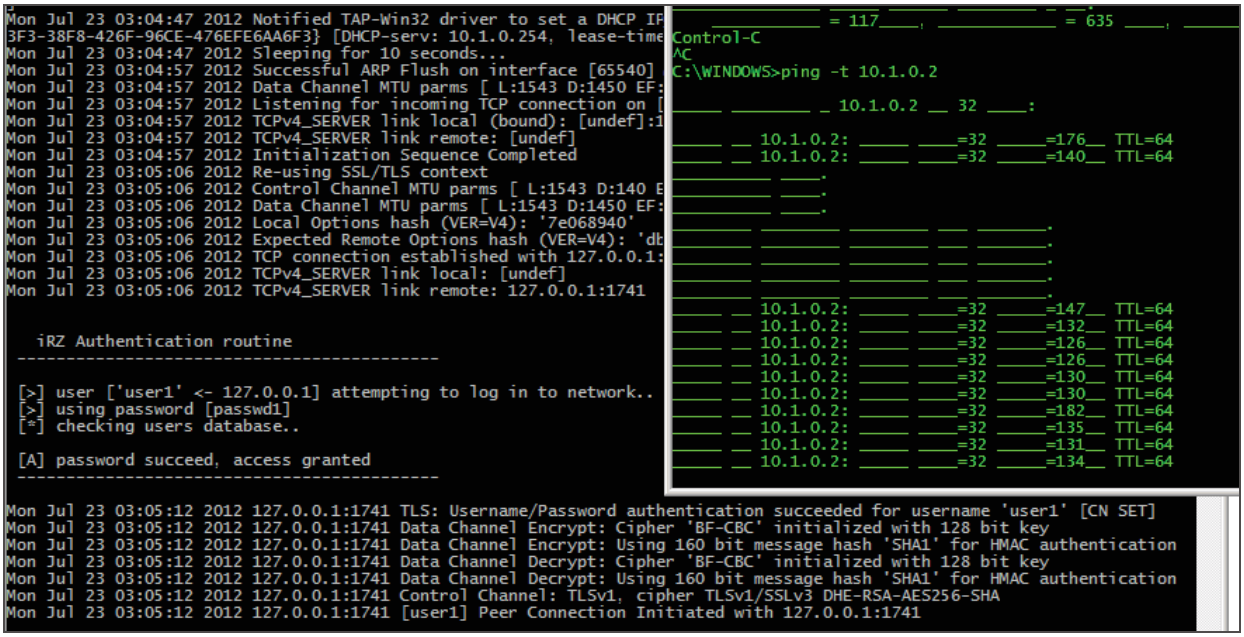

Рис. 2.2. Проверка имени пользователя и пароля клиента программой **iRZ Authentication routine**

2.1.6. Режимы конфигурации роутера

В роутерах существует возможность настроить работу OpenVPN двумя способами, краткое описание которых приведено ниже.

- Настройка через web-интерфейс. Основное преимущество данного способа это возможность быстро и интуитивно определить поведение OpenVPN-клиента, встроенного в роутер, не вдаваясь в детали синтаксиса директив конфигурации OpenVPN, определение допустимых значений каждой из них и сократить время на формирование файла данных директив в целом.

- Настройка с помощью конфигурационного файла. Позволяет определить параметры работы OpenVPN, не отражённые элементами web-интерфейса, что существенно расширяет границы возможностей использования OpenVPN в специфической конфигурации, а также обеспечивает возможность создать более тонкие настройки политик работы с трафиком и определить правила обслуживания клиентских узлов и др.

Примечание: Возможно, на составление конфигурационного файла у неподготовленного пользователя может уйти *значительно* больше времени, чем на установку предусмотренных web-интерфейсом параметров, по этим причинам описание конфигурации OpenVPN на роутере в данном документе опущено.

Когда конфигурация уже подготовлена, и осталось только задать настройки через web-интерфейс, можно открыть в Интернет-браузере страницу настройки OpenVPN (Configuration → OpenVPN Tunnel) и включить его использование, поставив галочку напротив надписи «Create OpenVPN tunnel».

Для выбора режима конфигурации используйте параметр «Take settings from» на странице конфигурации OpenVPN.

2.1.7. Настройка роутера через web-интерфейс

Для применения конфигурации из web-интерфейса, для параметра «**Take settings from**» выберите значение «**Web Interface**».

Параметр Protocol

Для лучшего соответствия характеристикам сети рекомендуется начинать настройку с установки параметра «Protocol» в наиболее предпочтительное значение. Этот параметр определяет протокол, используемый для связи с сервером OpenVPN (TCP/UDP) и позволяет, в ряде случаев, повысить пропускную способность OpenVPN-сети. Если оператор сотовой связи предоставил роутеру публичный («белый») IP-адрес рекомендуется использовать протокол UDP, т.к. он не затрачивает дополнительно ресурсы системы и сети на проверку успешности доставки отправленной информации.

Допустимые значения параметра для данной конфигурации: **UDP, TCP-client**

Параметр Remote IP Address

Обязательный параметр. Определяет IP-адрес или доменное имя сервера OpenVPN. IP-адрес должен быть внешним и фиксированным. За редким исключением IP-адрес может принадлежать private-пространству IP-адресов, когда доподлинно известно, что сервер OpenVPN и роутер находятся в одной частной подсети, либо могут установить соединение между связанными частными подсетями без использования шлюзов глобальной сети.

Параметр Local Interface IP Address

IP-адрес локального виртуального интерфейса, может быть явно задан в случае использования схемы сети «звезда» (точка-многоточка), однако в данном примере будет описана опция **CCD** (**client-config-dir**) обеспечивающая автоматический контроль адресации клиентов OpenVPN-сети со стороны сервера.

Внимание! Если IP-адрес роутера указан в качестве виртуального интерфейса, опция CCD должна быть отключена во избежание аварийного завершения клиента OpenVPN на стороне роутера.

Параметр Authenticate Mode

Параметр определяет политики и уровни защиты доступа к OpenVPN-сети. В данной конфигурации предполагается использование авторизации клиентов сети базовыми средствами (с использованием имени пользователя и секретного пароля).

Допустимое значение параметра в данной конфигурации – **Client: username / password**

Внимание! При необходимости передачи конфиденциальной информации через развёртываемую OpenVPN-сеть не рекомендуется использовать такой способ аутентификации, как ненадёжный. Описание корректной конфигурации OpenVPN-сети, использующей в процессе аутентификации сертификаты и криптографические ключи, планируется к публикации в следующих версиях данного документа. Обновления можно получить на официальном **сайте компании «Радиофид Системы»** (**www.radiofid.ru**) и при обращении в тех. поддержку (см. раздел «Поддержка»).

Параметры Username и Password

Определяются при формировании базы данных аутентификации, см. п. 2.1.5.

2.2. Конфигурация «OpenVPN Server ← RXX. Точка - многоточка. Защищённая сертификатом»

Данная конфигурация позволяет организовать виртуальную защищённую частную OpenVPN-сеть между роутерами и операционным центром по принципу, представленному в конфигурации «**OpenVPN Server ← RXX. Точка-многоточка. Незащищённая**», однако с использованием клиентских сертификатов и криптографических ключей. Топология сети в данной конфигурации представлена на рис. 2.3.

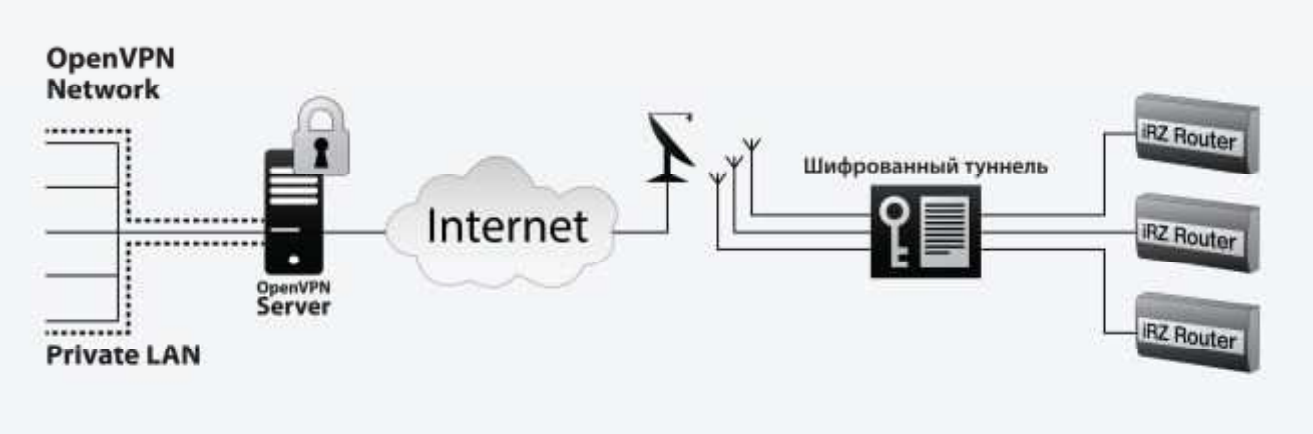

Рис. 2.3. Схема соединения «OpenVPN-сервер – роутеры iRZ (защищенная сертификатом)»

2.2.1. Подготовка к настройке

Процесс проектирования и развертывания OpenVPN-сети состоит из этапов, описанных в примере конфигурации «**OpenVPN Server ← RXX. Точка-многоточка. Незащищённая**», за исключением одного пункта, представленного ниже.

Конфигурация, описанная в данном разделе не предусматривает процесса формирования базы данных аутентификации клиентских узлов, однако для обеспечения защиты передаваемых данных, а так же контроля уникальности создаваемых клиентскими роутерами подключений, данные операции замещаются процессом генерирования клиентских сертификатов и криптографических ключей.

Кроме того, в процессе настройки клиентских роутеров через web-интерфейс должны быть задействованы другие параметры (описанные в главе «Формирование файла конфигурации OpenVPN-сервера») туннеля, создаваемого службой OpenVPN. Описание процесса настройки роутера через web-интерфейс в соответствии с данной конфигурацией представлено после описания процесса генерирования клиентских сертификатов и ключей и настройки OpenVPN-сервера.

Описание процесса проектирования развёртываемой сети, а также настройки интернет-подключения на роутерах выходит за рамки данного документа. Для получения рекомендаций по проектированию следует обратиться к документу «**Руководство по развёртыванию решений на базе роутера iRZ**». Описание настройки Интернет-подключения на роутерах представлено в документе «**Руководство по эксплуатации роутеров iRZ**» (см. разд. «Интернет соединение по GSM-каналу»).

В последующих разделах представлен процесс настройки OpenVPN-сервера. К настройке OpenVPN-сервера следует приступать, когда комплект подготовительной информации уже сформирован техническим персоналом компании-заказчика.

2.2.2. Генерирование сертификатов и ключей клиентов OpenVPN

После установки программного пакета OpenVPN необходимо создать файлы корневого и серверных сертификатов, а так же ключ сервера. Данный процесс описан в разделе «Генерация сертификатов и ключей сервера OpenVPN» данного документа.

ВНИМАНИЕ! Процесс генерирования клиентских сертификатов и ключей не может и не должен предшествовать процессу генерирования серверных файлов. Это недопустимо, т.к. файлы реквизитов клиентов OpenVPN могут быть созданы только на основе корневого закрытого ключа сервера OpenVPN!

Набор файлов, необходимых для успешного прохождения процедуры аутентификации клиента при подключении к сети OpenVPN, включает в себя:

- корневой сертификат – должен использоваться на всех узлах сети компании (файл **“ca.crt”**) *(должен уже быть создан в процессе генерирования ключей и сертификатов сервера);*
- сертификат клиента OpenVPN-сети (файл “**client.crt**”);
- криптографический ключ клиента (файл **“client.key”**).

Для создания файлов клиентов необходимо выполнить следующие действия:

1. Открыть командную строку ОС Windows;
   («Пуск» → «Выполнить» → ввести «cmd» → [Enter])
2. Перейти в каталог OpenVPN с набором утилит “EasyRSA”;
   (команда «cd /d “%programfiles%\OpenVPN\easy-rsa”», [Enter])
3. Ввести команду «vars», [Enter]
4. Запустить генерацию клиентского ключа и сертификата вводом команды «build-key ИМЯ_КЛИЕНТА», [Enter]
   (нажимать [Enter], до появления запроса Common Name)
5. Ввести значение Common Name, нажать [Enter]
   (должно соответствовать общему правилу именования клиентских узлов, например: “client_01”)
6. Убедиться в наличии созданных файлов сертификата (“client_N.crt” и “client_N.key”) и ключа клиента в каталоге.
   (требуется только один раз, при условии точного повторения всей процедуры в дальнейшем)

При необходимости повторить.

После выполнения указанных действий в каталоге **“[диск]:\Program Files\OpenVPN\easy-rsa”** должны появится следующие файлы:

- client_01.crt
- client_01.key
- client_02.crt
- client_02.key
- …
- client_N.crt
- client_N.key

Рекомендация: После того, как все файлы созданы, следует выполнить их резервное копирование на другой физический носитель во избежание утери. В случае замены/обновления корневого сертификата на сервере необходимо генерирование и обновление корневого сертификата, а также сертификатов и ключей сервера OpenVPN и клиентов во всём парке роутеров.

2.2.3. Формирование файла конфигурации OpenVPN-сервера

Детальное описание процесса формирования файла конфигурации сервера OpenVPN представлено в разделе «**Формирование файла конфигурации OpenVPN-сервера**».

В данной конфигурации следующие параметры (а так же их значения) должны быть исключены из файла конфигурации сервера OpenVPN:

- Параметр **client-cert-not-required**
- Параметр **username-as-common-name**
- Параметр **auth-user-pass-verify**
- Параметр **script-security**

Примечание: При необходимости получить дополнительную информацию о других директивах конфигурации, а также о других вариантах использования директив, описанных в данном документе следует обратиться к официальному ресурсу разработчика программного пакета «OpenVPN Community Server» по адресу **http://openvpn.net**/

Файл конфигурации OpenVPN всегда можно отличить от других файлов по расширению **.ovpn** в конце имени файла. Ниже (см. листинг 5) приведён пример уже готового конфигурационного файла, а также описание наиболее важных параметров и пояснения их значений.

Листинг 5. Пример конфигурационного файла «server.ovpn»

```
dev tun
port 1194
proto tcp-server
mode server
server 10.1.0.0 255.255.255.0

client-config-dir ".\\config\\ccd"
topology subnet

tls-server
ca ".\\..\\easy-rsa\\keys\\ca.crt"
cert ".\\..\\easy-rsa\\keys\\my-server.crt"
key ".\\..\\easy-rsa\\keys\\my-server.key"
dh ".\\..\\easy-rsa\\keys\\dh1024.pem"

comp-lzo yes

keepalive 10 120
verb 2

log ".\\..\\log\\OpenVPN-connections.log"
```

Примечание: Для редактирования файлов рекомендуется использовать программу-редактор текстовых файлов Notepad++, свободно доступную для скачивания с сайта **http://notepad-plus-plus.org**

Параметр comp-lzo [no/yes/adaptive]

Определяет необходимость использования встроенного механизма сжатия пользовательского трафика при его передаче между конечными точками OpenVPN-туннеля.

Значение данного параметра должно совпадать с его значением на стороне клиентского роутера. Для обеспечения требуемого соответствия, в случае, если на стороне клиентов OpenVPN значение неизвестно либо различается, рекомендуется использовать встроенную в OpenVPN возможность отправки управляющей директивы. Для этого необходимо добавить к существующей рабочей конфигурации сервера OpenVPN строку «**push "comp-lzo adaptive"**».

Значение в данной конфигурации: **yes**

Параметр verb [N]

Определяет необходимость фиксирования событий сетевой службы OpenVPN в системном журнале. Диапазон возможных значений – от «0» до «9».

Примечание: При определении значения параметра verb следует пользоваться следующим правилом:
0 – минимальный вывод информации, регистрируются только критичные события;
1-4 – стандартный рекомендуемый режим вывода информации, сообщения предыдущих режимов так же выводятся;
5 – отображение символов «R» и «W» верхнего регистра для сигнализации о TCP/UDP/ICMP-трафике, нижнего регистра – для сигнализации о TUN/TAP-трафике, а также сообщений предыдущих режимов;
6-9 – уровень отладки, включает в себя сообщения предыдущих режимов.

Параметр log / log-append ["DISK:\\FILEPATH\\"]

Определяет путь к файлу журнала службы OpenVPN. Данный параметр имеет две разновидности. В случае указания директивы **log** служба OpenVPN будет создавать заново журнал своей работы при каждом запуске, тем самым уничтожая уже имеющуюся в файле информацию о предыдущих запусках службы и ходе её работы. В режиме **log-append** новые записи добавляются в конце журнала.

Примечание: Для обеспечения гарантированного сохранения информации об истории предыдущих подключений необходимо использовать директиву **log-append**.

Единственное возможное значение для обеих директив – полный путь к файлу журнала, ***сформированный с соблюдением правил экранирования косой черты (в Windows) и использования кавычек при наличии пробелов в строке пути***.

Рекомендация: Для сокращения времени определения причин неисправности вычислительного комплекса, включающего в себя ПО OpenVPN, рекомендуется использовать директиву **log-append**. Это обеспечит фиксирование всех событий в работе службы.

Во избежание потери места на хранящем файл журнала накопителе рекомендуется использовать механизм «ротации» лог-файлов, предусматривающий регулярное перемещение текущего файла журнала в архив.

Параметр status ["DISK:\\FILEPATH\\"]

Сообщает службе OpenVPN о необходимости создания файла статуса подключившихся узлов. Может быть полезен при организации мониторинга клиентов OpenVPN-сети в режиме реального времени.

В качестве второго аргумента может быть задан интервал обновления в секундах (установка аргумента интервала обновления не обязательна).

Примечание: Период обновления файла мониторинга клиентов, по умолчанию – 1 секунда.

Параметр status-version [N]

Определяет формат создаваемого службой OpenVPN файла мониторинга, а именно – один из вариантов представления информации о подключившихся узлах.

Примечание: Формат, наиболее подходящий для «ручного» анализа, соответствует значению «1» данного параметра.

В случае автоматизированной обработки предпочтительнее использовать значение «2».

Если же требуется использовать и ручную, и автоматизированную обработку файла мониторинга, выберите значение «3» для этого параметра.

2.2.4. Настройка роутера через web-интерфейс

Существует два способа настройки OpenVPN-клиента роутера. Они определяются режимами его конфигурации, описанными в разделе «Режимы конфигурации роутера» данного документа.

Здесь будет описан режим настройки через web-интерфейс. Работа OpenVPN-клиента в данной конфигурации предполагает установку следующих параметров:

- Protocol;
- Remote IP Address;
- Local Interface IP Address.

Описание перечисленных в списке параметров и их значения приведены в разделе «Настройка роутера через web-интерфейс».

Параметр Authenticate Mode

Параметр определяет политики и уровни защиты доступа к OpenVPN-сети. В данной конфигурации предполагается авторизация клиентов сети с использованием клиентского сертификата и криптографического ключа.

Значение параметра в данной конфигурации – **Client: X.509 Certificate**

Установка параметров, описанных ниже, предполагает получение их значений из файлов клиентских сертификатов и ключей, процесс генерации которых описан в разделе «Генерирование сертификатов и ключей клиентов OpenVPN».

Рекомендация: В ходе заполнения текстовых полей для описанных далее параметров следует проявить особое внимание при копировании содержимого файлов сертификатов и ключей, и полностью повторять блок текста, находящийся между строками вида «**----- BEGIN *** -----**» и «**----- END *** -----**», включая эти строки.

Параметр CA Certificate

Определяет содержание корневого сертификата для данного подключения. Может содержать только криптографический текстовый блок, сгенерированный программой OpenVPN на стороне сервера.

Значением данного параметра будет содержимое файла корневого сертификата **ca.crt**.

Значение должно начинается со строки «**-----BEGIN CERTIFICATE-----**»

Параметр Local Certificate

Определяет содержание сертификата клиентского узла для данного подключения. Может содержать только криптографический текстовый блок, сгенерированный программой OpenVPN на стороне сервера.

Значением данного параметра будет содержимое файла клиентского сертификата **client_N.crt**.

Значение должно начинаться со строки «**-----BEGIN CERTIFICATE-----**»

Параметр Local Private Key

Определяет закрытый ключ клиентского узла для данного подключения. Может содержать только криптографический текстовый блок, сгенерированный программой OpenVPN на стороне сервера.

Значением данного параметра будет содержимое файла клиентского закрытого ключа **client_N.key**.

Значение должно начинаться со строки «**-----BEGIN RSA PRIVATE KEY-----**»

2.3. Конфигурация «RXX ← RXX. Точка - точка. Незащищённая»

Данная конфигурация позволяет организовать виртуальный защищённый OpenVPN-туннель между двумя роутерами по принципу «точка-точка» без использования средств защиты передаваемой информации. Связь между узлами может быть установлена через интернет-соединение, либо с использованием выделенного канала, предоставленного оператором сотовой связи. Схема соединения узлов приведена далее на рис. 2.4.

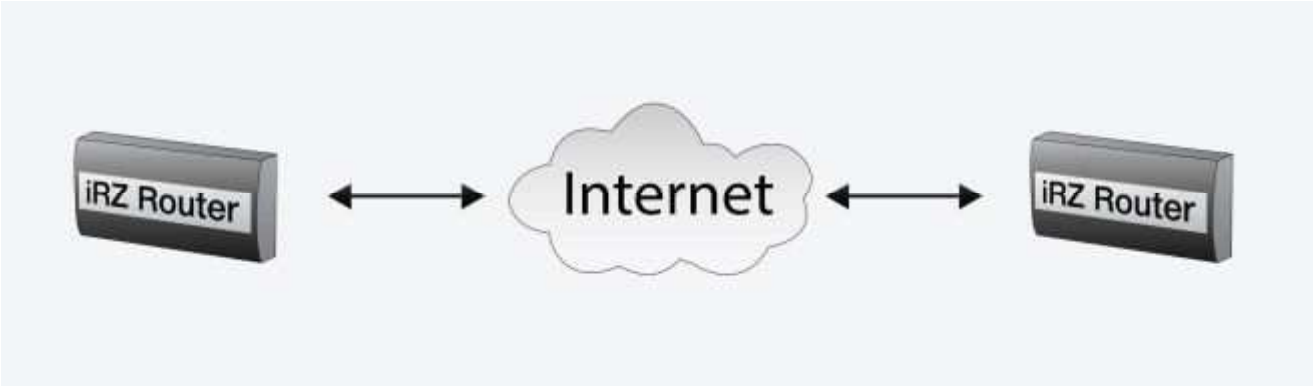

Рис. 2.4. Схема соединения «роутер iRZ – роутер iRZ (незащищенная)»

2.3.1. Подготовка к настройке

Процесс развертывания OpenVPN-туннеля значительно проще и не требует подготовительных мероприятий. Единственным требованием к данной конфигурации является наличие SIM-карты с фиксированным внешним («белым») IP-адресом. Данная конфигурация подразумевает определение ролей «клиента» и «сервера» между роутерами. «Сервером» будет роутер, использующий SIM-карту, предоставляющую внешний фиксированный IP-адрес роутеру в сети Интернет, а «клиентом» роутер, использующий SIM-карту с обычным GPRS/EDGE/3G-подключением.

Развертывание OpenVPN-туннеля состоит из следующих этапов:

- Создание ключа «pre-shared secret»
- Настройка OpenVPN-клиента на роутере № 1 (сервер)
- Проверка доступности роутера № 1 из сети Интернет по IP-адресу
- Настройка OpenVPN-клиента на роутере № 2 (клиент)
- Проверка виртуального туннеля между роутерами

2.3.2. Создание ключа “pre-shared secret”

Ключ «pre-shared secret» используется в процедуре аутентификации узла, подключающегося к программе OpenVPN, независимо от того, в каком режиме она запущена (сервер сети, либо туннеля).

Для генерации ключа «pre-shared secret» рекомендуется использовать «родной» программный пакет OpenVPN. Получить его можно на официальном ресурсе в Интернет – **http://openvpn.net**, либо на **сайте компании «Радиофид Системы»** (**www.radiofid.ru**).

Для генерации общего ключа туннеля выполните следующие действия:

1. Откройте командную строку ОС Windows;
   («Пуск» → «Выполнить» → ввести «cmd» → [Enter])
2. Перейдите в каталог исполняемых файлов OpenVPN;
   (команда «cd /d “%programfiles%\OpenVPN\bin”», [Enter])
3. Введите команду «openvpn --genkey --secret static.key», [Enter]

2.3.3. Настройка роутера № 1 (сервер)

Параметр Take settings from

Определяет режим настройки OpenVPN-соединения

> **Напоминание:** Режимы настройки OpenVPN описаны в разд. «**Режимы конфигурации роутера**».

Параметр Protocol

Значение параметра в данной конфигурации идентично описанному в разд. **«Настройка роутера через web-интерфейс»**.

Параметр Remote IP Address

Не задается для роутера №1, так как он находится в режиме сервера и принимает подключения от других узлов.

Параметр Authenticate Mode

Используется для определения метода аутентификации входящего соединения. В данной конфигурации доступны следующие методы аутентификации:

- **Tunnel: none**

  Аутентификация отсутствует.
- **Tunnel: pre-shared secret**

  Аутентификация проходит по общему ключу.
- **Tunnel: X.509 certificate (client)**

  Аутентификация проходит с передачей реквизитов клиентского узла, защищённых цифровой подписью, которая обеспечивает их подлинность. Этот вариант выбирается на «клиентском» роутере.
- **Tunnel: X.509 certificate (server)**

  Аналогичный предыдущему метод, дополненный необходимостью вводить параметры Diffie-Hellman. Этот вариант выбирается на «серверном» роутере.

Данный документ не содержит описания настройки аутентификации OpenVPN с использованием сертификатов и ключей.

Рекомендуемое значение параметра **Authenticate Mode** для решений в области телемеханики и телеметрии – **Tunnel: pre-shared secret**

Используйте для роутера SIM-карту, к которой привязан фиксированный внешний IP-адрес. Только использование фиксированного внешнего IP-адреса обеспечит возможность подключения к роутеру №1 второго роутера.

Напоминание: Если IP-адрес роутера является локальным (частным), либо является внешним, но динамическим (не постоянным) – связать роутеры не получится.

Параметр Local Interface IP Address

Определяет IP-адрес для локального виртуального интерфейса OpenVPN-туннеля. Обычно используется диапазон подсети класса A **10.0.0.0/8**, например – **10.1.0.1**

Параметр Pre-shared Secret

Значением параметра должен выступать статический «pre-shared secret» ключ, сгенерированный по инструкции в разд. «**Создание ключа "pre-shared secret"**». Для того чтобы поместить созданный ключ в настройки роутера необходимо выполнить следующие действия:

1. Открыть в текстовом редакторе (например Notepad++) файл «static.key»;
   (полный путь к файлу static.key: "%programfiles%\OpenVPN\bin\static.key",
   его можно ввести непосредственно в строку диалога открытия файла)
2. В редакторе выделить текст ключа;
   (фрагмент текста, начинающийся с фразы «-----BEGIN OpenVPN Static key V1-----»
   и заканчивающийся фразой «-----END OpenVPN Static key V1-----» включительно
3. Нажать комбинацию клавиш [CTRL+C], либо вызвать меню окна «Правка» → «Копировать»;
4. Перейти в окно Интернет-браузера;
   (страница роутера настройки OpenVPN-туннеля должна быть уже открыта)
5. Если все предыдущие параметры уже установлены как описано выше, поместить курсор в текстовое поле напротив надписи «Pre-shared secret»;
6. Нажать комбинацию клавиш [CTRL+V], либо вызывать контекстное меню браузера правой кнопкой мыши, затем выбрать «Вставить».

После установки всех необходимых параметров требуется включить создание OpenVPN-туннеля. Для этого вверху страницы, перед надписью «**Create OpenVPN tunnel**» установите «галочку» и нажмите кнопку «**Apply**».

Напоминание: Прежде чем приступать к настройке второго роутера необходимо убедиться, что IP-адрес, привязанный к SIM-карте, известен. Если оператор сотовой связи не сообщил IP-адрес, требуется сначала настроить интернет-подключение на роутере №1 и зафиксировать полученный роутером IP-адрес. Информация о подключении доступна на главной странице статуса интернет-соединения (Status and log → Internet, поле «IP Address»).

Напоминание: Необходимо убедиться, что выданный оператором IP-адрес является внешним («белым»/«публичным»). На странице статуса соединения, напротив поля «IP Address» после IP-адреса должна присутствовать надпись "**(public)**", а при переподключении IP-адрес должен остаться прежним.

2.3.4. Проверка доступности роутера № 1 из сети Интернет по IP-адресу

Для проверки связи между узлами рекомендуется использовать программу PING. Для проверки доступности роутера извне выполните следующие действия:

1. Открыть командную строку ОС Windows;
   («Пуск» → «Выполнить» → ввести «cmd» → [Enter])
2. В окне командной строки ввести команду вида:
   «ping [IP-АДРЕС РОУТЕРА]» (например: ping 8.8.8.8);
   При выполнении команды должны появляться строки, подобные представленным в листинге 3 (см. ниже)
3. Если такие строки присутствуют, значит роутер доступен для подключения и настройка может быть продолжена;
4. Если ответ от роутера получить невозможно, необходимо тщательно проверить настройки интернет-соединения.

Листинг 6

```
Обмен пакетами с 8.8.8.8 с 32 байтами данных:
Ответ от 8.8.8.8: число байт=32 время=103мс TTL=56
Ответ от 8.8.8.8: число байт=32 время=324мс TTL=56
Ответ от 8.8.8.8: число байт=32 время=643мс TTL=56
...
```

Примечание: Если после запуска программы PING в окне появились сообщения «Превышен интервал ожидания для запроса», либо если значение параметра «время» в сообщениях листинга 3 превышает «1000 мс» необходимо обратиться к документу «Диагностика и устранение неисправностей» для разрешения проблем с Интернет-подключением роутера.

2.3.5. Настройка роутера №2 (клиент)

Настройки для второго роутера идентичны настройкам первого, за исключением параметров **Remote IP Address** и **Local Interface IP Address**.

Параметр Remote IP Address

Указывает на внешний фиксированный IP-адрес первого роутера, к которому будет осуществляться подключение при создании туннеля.

Параметр Local Interface IP Address

Определяет IP-адрес для локального виртуального интерфейса OpenVPN-туннеля. IP-адрес виртуального интерфейса второго роутера должен находиться в диапазоне подсети IP-адреса виртуального интерфейса первого роутера.

Например, если на роутере №1 параметр **Local Interface IP Address** имеет значение **10.1.0.1**, то на роутере №2 этот параметр может иметь значения в диапазоне **10.1.0.2 – 10.254.254.254**.

2.3.6. Проверка виртуального туннеля между роутерами

Для проверки OpenVPN-туннеля так же рекомендуется использовать программу PING. Методика действий идентична принципу проверки доступности роутера № 1, однако проверку необходимо проводить используя web-интерфейс роутера. Для этого необходимо выполнить следующие действия:

1. Включить питание роутера;
2. Подключить роутер к компьютеру, используя Ethernet-кабель;
3. Открыть Интернет-браузер;
   («Рабочий стол» → «Opera», либо «Internet Explorer», «Firefox», «Chrome»)
4. Открыть web-интерфейс роутера;
5. Открыть страницу проверки соединения «Ping Test»;
   (Administration → Ping Test)
6. Ввести IP-адрес виртуального интерфейса другого роутера;
   (10.1.0.1, либо 10.1.0.2)
7. Подождать некоторое время до загрузки страницы;
8. Сообщение страницы должно содержать информацию, подобную приведённой в листинге 4.

Листинг 7

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
64 bytes from 10.1.0.2: seq=0 ttl=64 time=4.822 ms
64 bytes from 10.1.0.2: seq=1 ttl=64 time=1.098 ms
64 bytes from 10.1.0.2: seq=2 ttl=64 time=0.976 ms
...
```

Примечание: Если после загрузки страница содержит сообщение, приведённое в листинге 5, либо если значение параметра «**ttl**» в сообщениях листинга 3 превышает «**1000 ms**», необходимо обратиться к документу «Диагностика и устранение неисправностей» для разрешения проблем с Интернет-подключением роутера.

Листинг 8

```
PING 7.0.0.1 (7.0.0.1): 56 data bytes

--- 7.0.0.1 ping statistics ---
10 packets transmitted, 0 packets received, 100% packet
loss
```

2.4. Конфигурация

«RXX ← RXX. Точка - точка. Защищённая сертификатом»

Данная конфигурация позволяет организовать шифрованный OpenVPN-туннель между двумя роутерами по принципу «точка-точка». Связь между узлами может быть установлена через интернет-соединение с использованием выделенного канала, предоставленного оператором сотовой связи, либо по проводному соединению. Схема соединения узлов приведена далее на рис. 2.5.

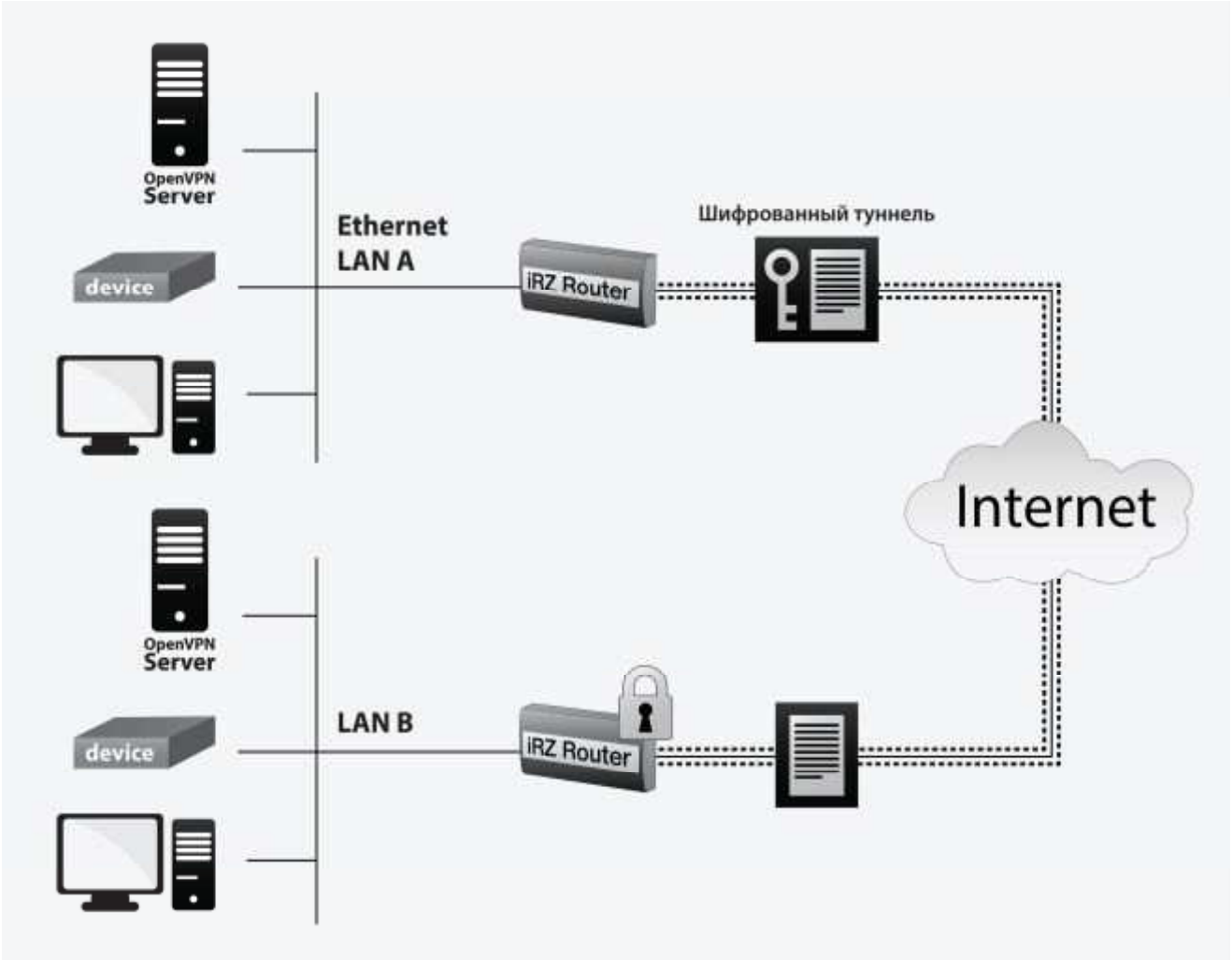

Рис. 2.5. Схема соединения «роутер iRZ – роутер iRZ (защищенная сертификатом)»

2.4.1. Подготовка к настройке

Для развертывания защищенного OpenVPN-туннеля необходимо создать ключи и сертификаты. Процесс создания сертификатов и ключей уже описан в разделах «Генерирование сертификатов и ключей сервера OpenVPN» и «Генерирование сертификатов и ключей клиентов OpenVPN» данного документа.

Кроме того, требованием к данной конфигурации является наличие SIM-карты с фиксированным внешним («белым») IP-адресом. Данная конфигурация подразумевает распределение ролей «клиента» и «сервера» между роутерами. «Серверным» будет роутер, использующий SIM-карту с внешним фиксированным IP-адресом, а «клиентским» – роутер использующий SIM-карту с обычным GPRS/EDGE/3G-подключением.

Развертывание OpenVPN-туннеля состоит из следующих этапов:

- генерирование ключей и сертификатов для обоих роутеров;
- настройка OpenVPN-клиента на роутере № 1 (сервер);
- проверка доступности роутера № 1 из сети Интернет по IP-адресу;
- настройка OpenVPN-клиента на роутере № 2 (клиент);
- проверка виртуального туннеля между роутерами.

Процедура настройки OpenVPN-соединения на роутере описана в данном документе в разделе «Настройка роутера через web-интерфейс».

3. Термины и сокращения

Пуско-наладка

Вычислительный комплекс – совокупность технических (программных и/или аппаратных) средств, выполняющих по заданному принципу общую задачу, сформулированную конкретным техническим решением;

Техническое решение – идея, либо документ, описывающие набор технических мер и/или мероприятий, направленных на реализацию конкретной задачи, для воплощения которой используются функциональные возможности используемых в данном решении компонентов, связанных между собой и взаимодействующих друг с другом определённым образом;

Пуско-наладка – мероприятие, задачей которого является развертывание (сборка, установка, настройка и подключение) вычислительного комплекса, выполненного в соответствии с заданным техническим решением, проверка и оценка работоспособности данного комплекса, а так же меры, направленные на обеспечение его стабильной работы;

Объект – географическая точка, в которой будет производиться эксплуатация вычислительного комплекса (либо его части), включающего в себя роутер iRZ;

USECASE-схема – сценарий развития событий (нормальных и ошибочных) в процессе работы/функционирования конкретного программного продукта или вычислительного комплекса, является частью технического решения;

Доступ к устройству (физический, удалённый) – получение непосредственной возможности влиять на работу устройства, изменять его настройки, режим и логику работы через команды управления (удалённый доступ), либо воздействуя на устройство физически: отключение питания, подключение кабеля компьютерной сети, подключение к управляемому устройству через COM-порт и т.п. (физический доступ);

Нагрузочная проверка – мероприятие, позволяющее в реальных условиях выявить и оценить недостатки существующего программного/аппаратного средства, вычислительного комплекса или технического решения в целом, с помощью преднамеренного создания ожидаемой в условиях реальной работы нагрузки, а так же нагрузки, превышающей ожидаемую (для выявления максимальных значений, при которых система сохраняет работоспособность);

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).

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.