Wireless solutions
for M2M world

Защита передаваемых данных средствами IPSec для роутеров iRZ

RUH, RUH2, RUH2b, RUH3, RCA

Содержание

Таблицы

Рисунки

1. Введение

1.1. Описание документа

Данный документ является частью пакета инструкций по применению роутера iRZ и содержит примеры корректной конфигурации сетевой службы IPSec в решениях, построенных на базе роутеров iRZ. Данный документ **не содержит** всей информации по работе с роутером.

Версия документа		**Дата публикации**	
1.01		2013-08-12	
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 GRE-туннелей;
  - Отказоустойчивость 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. Так же, не следует ограничиваться синтетическими тестами, а максимально реалистично воспроизвести условия, в которых будет эксплуатироваться оборудование.

2. Примеры конфигурации службы IPSec

В данном разделе приведены примеры конфигураций службы IPSec, детально описывающие её функциональные возможности, а также такие особенности технологии как: используемые методы авторизации, алгоритмы шифрования пользовательских данных, поддерживаемые схемы соединения объединяемых узлов и сетей, минимизация объёма передаваемых данных при простое. Для наглядности в некоторых примерах в качестве оконечного оборудования одной из сторон в схеме подключения был использован роутер **Cisco** класса SMB/SOHO серии **c800**.

Примечание: Описание некоторых процессов подготовки к развертыванию конфигурации (например - *настройка Интернет-подключения на роутере*) уже представлено в других документах пакета документации и выходит за рамки данного документа. Данное описание не включает материалы примеров конфигураций. Для получения рекомендаций по настройке Интернет-соединения на роутере обратитесь к документу «**Руководство по эксплуатации роутеров iRZ**» (см. разд. «Интернет соединение по GSM-каналу»

Примечание: На данный момент роутеры iRZ официально поддерживают только туннельный режим IPSec. В роутерах функцию службы IPSec выполняет открытый программный пакет **ipsec-tools**. В случае необходимости настройки транспортного режима работы IPSec это можно сделать вручную, сформировав соответствующие файлы конфигурации данного программного пакета.

Заказчик может обратиться в службу технической поддержки или к менеджеру по продажам компании «Радиофид Системы» и сделать запрос отдельной версии прошивки, включающей в себя уникальную конфигурацию службы IPSec.

2.1. Организация адресного пространства объединяемых подсетей

Прежде чем приступать к настройке службы IPSec необходимо переопределить адреса IP-сетей, которые будут объединяться роутерами средствами службы IPSec. Адресное пространство локальных интерфейсов роутеров не может быть идентичным в виду ограничений существующей реализации IPSec. Настроить эти IP-адреса в роутерах iRZ можно, обратившись к странице **Configuration → LAN** web-интерфейса роутера iRZ. Далее, к каждому примеру конфигурации службы IPSec будут приложены настройки интерфейсов, подключённых к обслуживаемым роутерами подсетям.

Примечание: Для получения информации о способе настройки IP-адреса локальной подсети (подсетей) на роутере Cisco требуется обратиться к разделу «Configuring a LAN with DHCP and VLANs» официальной документации на сайте Cisco.

2.2. Профили службы IPSec

Конфигурирование параметров службы IPSec выполняется на странице **Configuration → IPSec**. Для настройки доступно до 5 одновременно активных профилей.

Страница «**IPSEC Tunnel Configuration**» позволяет выполнять быстрое включение и отключение профилей через параметр **Create**, избавляя пользователя от необходимости открывать страницу полной конфигурации каждого профиля, тем самым сокращая общее время настройки службы.

Значения параметра **Create**: **yes** – указанный профиль будет активен после нажатия кнопки «**Apply**» и после каждой загрузки роутера, **no** – не активен ни при каких обстоятельствах.

Получить доступ ко всем параметрам профиля IPSec можно нажав на ссылку «**[Edit]**» напротив редактируемого профиля.

Групповое сохранение и применение новых настроек выполняется нажатием на кнопку «**Apply**».

2.3. Конфигурация

«RXX: fixed static IP-address ←→ RXX: fixed static IP-address»

Данная конфигурация позволяет решить одновременно несколько задач:

- прозрачное объединение подсетей филиалов, разнесённых территориально;
- защита информации, передаваемой между объединяемыми подсетями;
- исключение избыточного служебного трафика проверки соединения.

Для реализации данной конфигурации в обоих роутерах должны быть использованы SIM-карты с внешними фиксированными IP-адресами, либо внутренними фиксированными IP-адресами (в рамках виртуальной частной сети с выделенным APN, предоставляемой оператором связи).

Ниже приведена схема соединения узлов (рис. 2.1) с описанием процесса применения данной конфигурации на роутере.

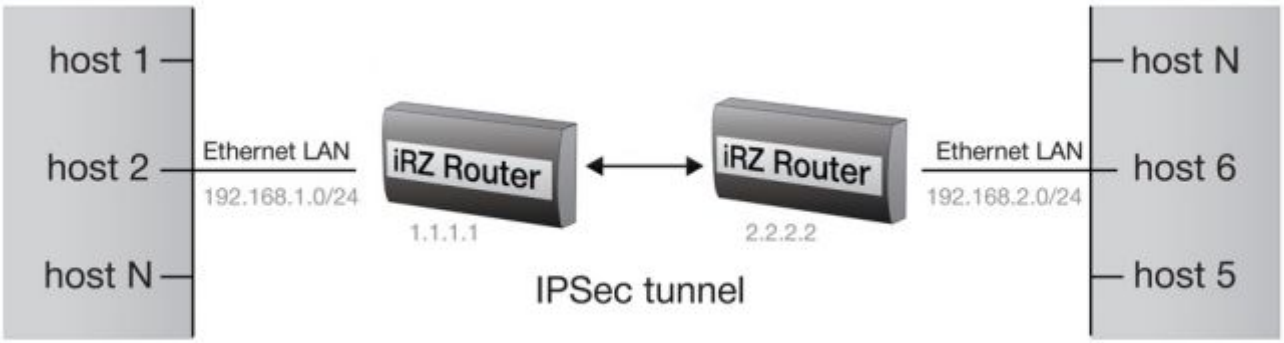

Рис. 2.1. Схема соединения узлов «роутер – роутер» со статическими IP-адресами

2.3.1. Подготовка к настройке

Процесс подготовки и развертывания данной конфигурации состоит из следующих этапов:

- настройка параметров локальных интерфейсов роутеров;
- настройка и проверка Интернет-подключения на обоих роутерах;
- проверка доступности роутеров:
  - проверка доступности роутеров по их внешнему фиксированному IP-адресу;
  - проверка прямой доступности между роутерами через Интернет;
- настройка IPSec-туннеля на роутере №1;
- настройка IPSec-туннеля на роутере №2;
- нагрузочная проверка возможности создания двунаправленного зашифрованного соединения.

Для настройки Интернет-подключения, следует обратиться к документу «**Руководство по эксплуатации роутеров iRZ**» (см. разд. «Интернет соединение по 3G/GSM-каналу»).

2.3.2. Настройка параметров локальных интерфейсов роутеров

В данном разделе в таблице 2.1 описаны параметры локальных Ethernet-интерфейсов настраиваемых роутеров.

Таблица 2.1. Настройки локальных роутеров с интерфейсом Ethernet

Название роутера	Название	Значение параметра	Описание параметра
(раздел Primary IP Address страницы Configuration → LAN) web-интерфейса роутеров			
роутер №1	IP Address	192.168.1.1	IP-адрес локального интерфейса
	Subnet Mask	255.255.255.0	Маска обслуживаемой подсети
роутер №2	IP Address	192.168.2.1	IP-адрес локального интерфейса
	Subnet Mask	255.255.255.0	Маска обслуживаемой подсети

2.3.3. Проверка доступности роутеров

Прежде чем переходить непосредственно к настройке службы IPSec на роутерах, необходимо убедиться в их доступности из сети Интернет, а также по отношению друг к другу. Это требуется для сокращения времени устранения проблем при создании IPSec-соединения на ранней стадии развертывания решения.

2.3.4. Проверка доступности роутеров по их внешнему фиксированному IP-адресу

После того, как на роутере настроено Интернет-подключение, требуется выполнить проверку доступности устройства из сети Интернет. Дело в том, что в случае неверной настройки параметров подключения, роутер может успешно выходить в сеть Интернет, однако устройство при этом может оказаться недоступным.

Предупреждение: Выполнять проверку доступности устройства при помощи программы **ping** не рекомендуется, т.к. полученные в ответ ICMP-пакеты не будут свидетельствовать о том, что они были отправлены именно настраиваемым роутером, а не неизвестным устройством, обладающим проверяемым IP-адресом (это возможно в случае некорректной конфигурации Интернет-подключения на роутере iRZ).

Для проверки доступности обоих настраиваемых роутеров требуется выполнить следующие действия:

- Включить на каждом роутере любую из служб удалённого доступа (в случае, если роутер производства iRZ - можно обратиться к разделу «Настройка удалённого доступа» документа **«Описание средств управления роутером iRZ»**);
- Открыть Интернет-браузер, либо командую консоль;
- Осуществить попытку получения доступа к устройствам через сеть Интернет.

Рекомендация: Если при включении удаленного доступа реквизиты (имя пользователя и пароль) не были изменены, рекомендуется убедиться, что проверяемый IP-адрес принадлежит именно настраиваемому роутеру. Проверьте уникальную информацию – строку **UNIT NAME** или настройки локальной сети и сетевых служб.

2.3.5. Проверка прямой доступности между роутерами через Интернет

После проверки доступности роутеров по их фиксированному IP-адресу следует убедиться в доступности роутеров в отношении друг для друга. Проверку необходимо выполнить в обоих направлениях.

Предупреждение: Для Северо-Западного региона России характерна невозможность установления связи между роутерами, когда на обоих устройствах используются SIM-карты одного и того же оператора сотовой связи – «Мегафон» или «МТС» (независимо от используемого тарифа и подключённых услуг, в т.ч. «Фиксированный IP-адрес» у «Мегафон», или «Реальный IP» у «МТС»). Поэтому перед заключением договора на предоставление телематических услуг с оператором, рекомендуется провести ряд тестов на возможность осуществления связи между устройствами, использующими SIM-карты данного оператора.
Данное ограничение недействительно для случаев использования выделенного APN.

Для проверки доступности роутера №2 со стороны роутера №1 выполните следующие действия:

1. Включите роутер №2 и подключите его к компьютеру;
   (с помощью «crossover»-патчкорда)
2. Откройте интернет-браузер;
   (любой современный браузер: «Internet Explorer», «Firefox», «Opera», «Chrome» и пр.)
3. Введите в адресную строку локальный IP-адрес роутера №2;
   (В данной конфигурации: **192.168.2.1**)
4. Откройте страницу статуса Интернет-соединения;
   (Status and log → Internet)
5. После подключения роутера №2 к Интернет, запишите его внешний IP-адрес;
6. Отключите роутер №2 от компьютера;
   (сохранив коммутацию с сетью питания и GSM/3G-антенной)
7. Подключите к компьютеру роутер №1;
   (с помощью «crossover»-патчкорда)
8. На компьютере, вернитесь к окну интернет-браузера;
9. Введите в адресную строку локальный IP-адрес роутера №1;
   (В данной конфигурации: **192.168.1.1**)
10. Откройте страницу проверки соединения «Ping Test»;
    (Administration → Ping Test)
11. Напротив надписи «Ping Address/URL» введите внешний IP-адрес роутера №2;
    (В данной конфигурации: **2.2.2.2**)
12. Нажмите [*Enter*];
13. Подождите некоторое время до загрузки страницы.

Сообщение страницы должно содержать информацию, подобную приведённой в листинге 1:

Листинг 1

```
PING 2.2.2.2 (2.2.2.2): 56 data bytes
64 bytes from 2.2.2.2: seq=0 ttl=64 time=4.822 ms
64 bytes from 2.2.2.2: seq=1 ttl=64 time=1.098 ms
64 bytes from 2.2.2.2: seq=2 ttl=64 time=0.976 ms
```

2.3.6. Настройка IPSec-туннеля на роутере №1

В этом разделе описаны параметры службы IPSec, настраиваемые в данной конфигурации, и их значения.

Примечание: Перед настройкой службы IPSec необходимо убедиться в отсутствии запрещающих правил сетевого экрана роутера; в заводских настройках роутера служба сетевого экрана выключена.

Таблица 2.2. Настройки службы IPSec для роутера №1

Название параметра	Значение в данной конфигурации	Описание
Create IPSec tunnel #[N]	[включено]	Определяет будет ли использован данный профиль после каждой загрузки устройства
Description	[fixed-ip-to-fixed-ip]	Краткое описание/название профиля (допустимо использование только латинских символов)
Remote IP Address	2.2.2.2	Внешний фиксированный IP-адрес роутера №2
Remote Subnet	192.168.2.0	IP-адрес подсети, обслуживаемой удалённым роутером №2. С данной подсетью будет обеспечена возможность обмениваться данными из локальной подсети настраиваемого роутера №1
Remote Subnet Mask	255.255.255.0	Маска подсети, обслуживаемой удалённым роутером №2
Local Subnet	192.168.1.0	IP-адрес подсети, обслуживаемой настраиваемым роутером №1
Local Subnet Mask	255.255.255.0	Маска подсети, обслуживаемой настраиваемым роутером №1
NAT Traversal	disabled	Определяет необходимость использования дополнительных параметров согласования соединения, в случае, если роутер находится за NAT. В данной конфигурации – **disabled**
Aggressive Mode	disabled	Определяет режим согласования параметров обмена ключами первой фазы. Рекомендуемое значение в данной конфигурации – **disabled** *Значение параметра должно быть идентичным значению данного параметра профиля роутера №2*
Authenticate Mode	pre-shared key	Способ аутентификации узлов. Значение **pre-shared key** обеспечивает аутентификацию по секретной ключевой фразе (паролю). Значение **X.509 Certificate** определяет требование выполнять аутентификацию на основе криптографических сертификатов Значение в данной конфигурации – **произвольное** *Значение параметра должно быть идентичным значению данного параметра профиля роутера №2*
Pre-shared Key	[qwerty]	Ключевая фраза для двунаправленной аутентификации обоих узлов. Допустимое значение - **любая комбинация печатаемых латинских символов кроме пробела**. Диапазон используемых символов: **a-z, A-Z, 0-9, спецсимволы**. *Значение параметра должно быть идентичным значению данного параметра профиля роутера №2*

Таблица 2.3. Параметры методов шифрования службы IPSec для обоих устройств

Название параметра	Значение в данной конфигурации	Описание
Раздел **Phase 1**		
Encryption Algorythm	3DES	Определяет алгоритм шифрования, используемый при проверке подлинности Значение в данной конфигурации – **произвольное** *Значение параметра должно быть идентичным значению данного параметра профиля роутера №2*
Hash Algorythm	SHA1	Определяет алгоритм расчёта хэша в фазе IKE (первой фазе). Значение в данной конфигурации – **произвольное** *Значение параметра должно быть идентичным значению данного параметра профиля роутера №2*
DH Group	DH Group 2 (1024 bits)	Определяет группу Diffie-Hellman, задающую уровень энтропии для проверки подлинности. Значение в данной конфигурации – **произвольное** *Значение параметра должно быть идентичным значению данного параметра профиля роутера №2*
Раздел **Phase 2**		
Encryption Algorythm	3DES	Определяет алгоритм шифрования, используемый при проверке подлинности Значение в данной конфигурации – **произвольное** *Значение параметра должно быть идентичным значению данного параметра профиля роутера №2*
Authentication Algorythm	HMAC-SHA1	Определяет метод проверки подлинности, используемый при согласовании узлов Значение в данной конфигурации – **произвольное** *Значение параметра должно быть идентичным значению данного параметра профиля роутера №2*
PFS Group	None	Определяет протокол обмена ключами Diffie-Hellman, задающий алгоритм, по которому роутеры устанавливают общий временный ключ сеанса для второй фазы Значение в данной конфигурации – **произвольное** *Значение параметра должно быть идентичным значению данного параметра профиля роутера №2*

Внимание! При определении значений параметров, определяющих методы шифрования, приведённых в таблице 2.2 и 2.3 следует исходить из требований к уровню защищенности передаваемой информации.

Внимание! Значение **pre-shared key** для параметра **Authenticate Mode** не рекомендовано к применению в сфере финансовых операций и платёжных транзакций, а так же в решениях с повышенными требованиями к уровню защиты передаваемой информации.

2.3.7. Настройка IPSec-туннеля на роутере №2

Настройка роутера №2 выполняется способом, аналогичным процессу настройки роутера №1.

Перечень параметров профиля роутера №2, значения которых должны быть идентичны значениям этих же параметров в профиле роутера №1:

- *Aggressive Mode;*
- *Authenticate Mode;*
- *Pre-shared Key;*
- блок Phase 1: *Encryption Algorythm;*
- блок Phase 1: *Hash Algorythm;*
- блок Phase 1: *DH Group;*
- блок Phase 2: *Encryption Algorythm;*
- блок Phase 2: *Authentication Algorythm;*
- блок Phase 2: *PFS Group.*

Предупреждение: Если значения параметров **Encryption Algorythm**, **Hash Algorythm** и **DH Group** в блоке **Phase 1**, а также значения параметров **Encryption Algorythm**, **Authentication Algorythm** и **PFS Group** в блоке **Phase 2** роутера №1 не соответствуют значениям этих же параметров роутера №2, то служба IPSec не сможет обеспечить передачу пользовательских данных.
Для исключения временных затрат на поиск и устранение неисправности рекомендуется проверить соответствие значений описанных параметров на обоих устройствах

Далее приведены параметры профиля IPSec роутера №2 и описание их значений. На эти параметры не распространяется «правило идентичности».

Таблица 2.4. Настройка службы IPSec для роутера №2

Название параметра	Значение в данной конфигурации	Описание
Create IPSec tunnel #[N]	[включено]	Определяет будет ли использован данный профиль после каждой загрузки устройства
Description	[fixed-ip-to-fixed-ip]	Краткое описание/название профиля (допустимо использование только латинских символов)
Remote IP Address	1.1.1.1	Внешний фиксированный IP-адрес роутера №1
Remote Subnet	192.168.1.0	IP-адрес подсети, обслуживаемой удалённым роутером №1. С данной подсетью будет обеспечена возможность обмениваться данными из локальной подсети настраиваемого роутера №2
Remote Subnet Mask	255.255.255.0	Маска подсети, обслуживаемой удалённым роутером №1
Local Subnet	192.168.2.0	IP-адрес подсети, обслуживаемой настраиваемым роутером №2
Local Subnet Mask	255.255.255.0	Маска подсети, обслуживаемой настраиваемым роутером №2

2.3.8. Нагрузочная проверка возможности создания двунаправленного зашифрованного соединения

Для подтверждения работоспособности данной конфигурации необходимо осуществить передачу полезной информации между подсетями в обоих направлениях. Для проверки доступности подсети, обслуживаемой роутером №2, из подсети, обслуживаемой роутером №1, выполните следующие действия:

1. Включите роутер №1 и подключить его к компьютеру;
2. Откройте Интернет-браузер;
   (любой современный браузер: «Internet Explorer», «Firefox», «Opera», «Chrome» и пр.)
3. Введите в адресную строку локальный IP-адрес роутера №1;
   (В данной конфигурации: **192.168.1.1**)
4. Дождитесь установления Интернет-соединения;
5. Откройте страницу журнала событий службы IPSec;
   (Status an log → IPSec)
6. Дождитесь появления в журнале сообщения;
   (смотрите **листинг 2**)
7. Откройте страницу проверки соединения «Ping Test»;
   (Administration → Ping Test)
8. Напротив надписи «Ping Address/URL» введите локальный IP-адрес для роутера №2;
   (В данной конфигурации: **192.168.2.1**)
9. Нажмите [*Enter*];
10. Подождите некоторое время до загрузки страницы.

Сообщение страницы должно содержать информацию, подобную приведённой в **листинге 3**.

Листинг 2

```
2012-10-04 06:47:06: INFO: IPsec-SA established: ESP/Tunnel 1.1.1.1[500]-
>2.2.2.2[500] spi=219072948(0xd0ec9b4)
2012-10-04 06:47:06: INFO: IPsec-SA established: ESP/Tunnel 1.1.1.1[500]-
>2.2.2.2[500] spi=4083749915(0xf369141b)
...
```

Листинг 3

```
PING 192.168.2.1 (192.168.2.1): 56 data bytes
64 bytes from 192.168.2.1: seq=0 ttl=64 time=4.822 ms
64 bytes from 192.168.2.1: seq=1 ttl=64 time=1.098 ms
64 bytes from 192.168.2.1: seq=2 ttl=64 time=0.976 ms
...
```

Для выполнения проверки связи с роутером №1 со стороны роутера №2 следует выполнить действия, аналогичные процессу, описанному выше:

1. Включите роутер №2 и подключите его к компьютеру;
2. Откройте Интернет-браузер;
   (любой современный браузер: «Internet Explorer», «Firefox», «Opera», «Chrome» и пр.)
3. Введите в адресную строку локальный IP-адрес роутера №2;
   (В данной конфигурации: **192.168.2.1**)
4. Откройте страницу проверки соединения «Ping Test»;
   (Administration → Ping Test)
5. Напротив надписи «Ping Address/URL» введите локальный IP-адрес для роутера №1;
   (В данной конфигурации: **192.168.1.1**)
6. Нажмите [*Enter*];
7. Подождите некоторое время до загрузки страницы.

Сообщение страницы должно содержать информацию, подобную приведённой в листинге 4:

Листинг 4

```
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: seq=0 ttl=64 time=4.822 ms
64 bytes from 192.168.1.1: seq=1 ttl=64 time=1.098 ms
64 bytes from 192.168.1.1: seq=2 ttl=64 time=0.976 ms
...
```

Если сообщения на странице «Ping test» после нажатия кнопки «Ping» не появились, необходимо провести ряд проверок в следующем порядке:

- локальный IP-адрес каждого роутера находится в пределах адресного пространства обслуживаемой данным роутером локальной сети;
- отсутствуют запрещающие правила сетевого экрана роутера, блокирующие работу служб IPSec;
- качество GSM/3G-сигнала соответствует приемлемому уровню по классификации таблицы «Градации уровня сигнала» документа «**Руководство по эксплуатации роутеров iRZ**»;
- гарантированная пропускная способность канала оператора связи – более 64 кбит/с;
- оператор связи не блокирует работу протоколов службы IPSec: ISAKMP, OAKLEY, и пр.

После выполнения всех проверок можно приступать непосредственно к построению решения на базе службы IPSec.

Рекомендация: Если одна или несколько проверок не увенчались успехом, а также если возникли проблемы в ходе эксплуатации развернутой конфигурации рекомендуется обратиться к документу «**Диагностика и методы устранения неисправностей роутеров iRZ**» за рекомендациями по разрешению возникшей проблемы.

2.4. Конфигурация

«Cisco: static fixed IP-address ←→ RXX: static fixed IP-address»

Данная конфигурация позволяет решить одновременно несколько задач:

- прозрачное объединение подсетей филиалов, разнесённых территориально;
- защита информации, передаваемой между объединяемыми подсетями;
- исключение избыточного служебного трафика проверки соединения.

Для реализации данной конфигурации на роутере iRZ должна быть использована SIM-карта с внешним фиксированным IP-адресом.

Ниже приведена схема соединения узлов (рис. 2.2) с описанием процесса применения данной конфигурации на роутере.

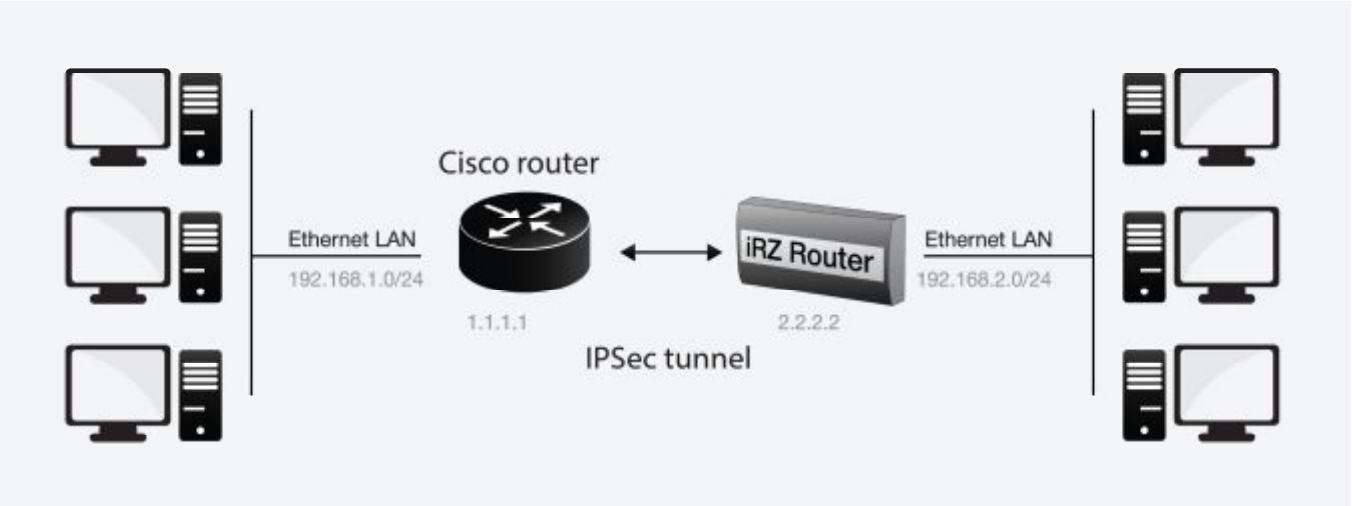

Рис. 2.2. Схема соединения узлов «Cisco – роутер»

2.4.1. Подготовка к настройке

Процесс подготовки и развертывания данной конфигурации состоит из следующих этапов:

- настройка параметров локальных интерфейсов роутеров;
- настройка и проверка Интернет-подключения на роутере iRZ;
- проверка доступности роутеров:
  - проверка роутеров по их внешнему фиксированному IP-адресу;
  - проверка доступности роутера Cisco со стороны роутера iRZ;
  - проверка доступности роутера iRZ со стороны роутера Cisco;
- настройка IPSec-туннеля на роутере Cisco;
- настройка IPSec-туннеля на роутере iRZ.
- нагрузочная проверка возможности создания двунаправленного зашифрованного соединения.

Для настройки Интернет-подключения роутера iRZ следует обратиться к документу «**Руководство по эксплуатации роутеров iRZ**» (см. разд. «Интернет соединение по GSM-каналу»).

Для настройки Интернет-подключения на роутере Cisco следует обратиться к официальному Интернет-ресурсу компании-производителя – http://www.cisco.com/cisco/web/RU/support/index.html

2.4.2. Настройка параметров локальных интерфейсов роутеров

В данном разделе в таблице 2.5 описаны параметры локальных Ethernet-интерфейсов настраиваемых роутеров.

Таблица 2.5. Настройки локальных интерфейсов роутеров

Название роутера	Название	Значение параметра
роутер Cisco	*Настройки параметров локального интерфейса **роутера Cisco** должны быть сформированы на основе справочных материалов, представленных на официальном сайте Cisco. В данной конфигурации IP-адрес локального интерфейса Cisco имеет значение: **192.168.1.1**, маска подсети – **255.255.255.0***	
роутер iRZ	*(раздел Primary IP Address страницы Configuration → LAN) **роутера iRZ***	
	IP Address	192.168.2.1
	Subnet Mask	255.255.255.0

2.4.3. Проверка доступности роутеров

Проверка доступности роутеров по их внешнему фиксированному IP-адресу должна быть выполнена по методу, описанному в разделе «**Проверка доступности роутеров по их внешнему фиксированному IP-адресу**». Проверка доступности роутера Cisco со стороны роутера iRZ RXX должна быть выполнена по методу, описанному в разделе «**Проверка прямой доступности между роутерами через Интернет**».

2.4.4. Проверка доступности роутера iRZ со стороны роутера Cisco

Для выполнения проверки доступности роутера iRZ со стороны роутера Cisco необходимо выполнить следующие действия:

Примечание: На момент данной проверки Интернет-подключение на роутере Cisco должно быть настроено и проверено.

1. Включите роутер iRZ и подключите его к компьютеру;
   (с помощью «crossover»-патчкорда)
2. Откройте Интернет-браузер;
   (любой современный браузер: «Internet Explorer», «Firefox», «Opera», «Chrome» и пр.)
3. Введите в адресную строку локальный IP-адрес роутера iRZ;
   (В данной конфигурации: **192.168.2.1**)
4. Откройте страницу статуса Интернет-соединения;
   (Status and log → Internet)
5. После подключения роутера iRZ к Интернету, запишите его внешний IP-адрес;
6. Отключите роутер iRZ от компьютера;
   (сохранив коммутацию с сетью питания и GSM/3G-антенной)
7. Включите роутер Cisco и подключите его к компьютеру;
   (с помощью «crossover»-патчкорда, либо кабеля Cisco «COM» → «AUX»)
8. Подключитесь к роутеру Cisco удалённо через Telnet, либо через COM-порт;
   (с помощью программы «PuTTY», либо «HyperTerminal»)
9. Дождитесь приглашения консоли управления Cisco;
   (как правило, приглашение содержит строку: « [имя_роутера]>_ »)
10. Введите команду: «ping [*внешний фиксированный IP-адрес роутера iRZ*]»;
    (В данной конфигурации: «**ping 2.2.2.2**»)
11. Нажмите [*Enter*];
12. Подождите некоторое время до конца выполнения команды PING.

Сообщение страницы должно содержать информацию, подобную приведённой в листинге 5:

Листинг 5

```
User Access Verification

Password:
Router>ping 2.2.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 120/124/140 ms
Router>
```

Показателем проверки в данном случае будет наличие и количество символов «!» (восклицательного знака) после ввода команды «**ping**».

Полное, либо частичное отсутствие (менее 5) этих знаков говорит о том, что проверка завершилась неудачей. В данной ситуации для разрешения проблемы рекомендуется обратиться к документу «**Диагностика и методы устранения неисправностей роутера iRZ**», раздел «Служба IPSec».

2.4.5. Настройка IPSec-туннеля на роутере Cisco

Далее приведён сценарий автоматической настройки (листинг 6), реализующий конфигурацию роутера Cisco в полуавтоматическом режиме (отсутствует необходимость ручного ввода каждой команды, сценарий применяется копированием его текста в консоль управления Cisco).

Внимание! Данный пример может быть непосредственно применён только на моделях серии **c800**. Для применения данного сценария на других моделях Cisco рекомендуется ознакомиться с возможными изменениями в синтаксисе интерфейса управления роутерами других серий.

Внимание! Применение данного сценария может повлечь за собой **порчу**, **модификацию**, либо необратимую потерю критичной конфигурационной информации роутера заказчика. Перед применением данного сценария на рабочем роутере Cisco настоятельно рекомендуется ознакомление с его конфигурационными директивами и замена значений параметров из данного примера на актуальные для развёртываемой конфигурации.

Перед применением сценария на роутере Cisco необходимо войти в режим администрирования устройством. Для этого требуется ввести команду «**enable**», затем нажать [Enter] и ввести пароль доступа к уровню администрирования устройством. Далее можно вставить текст сценария конфигурации в окно консоли управления.

Примечание: В программе «PuTTY» вставка текста из буфера осуществляется нажатием правой кнопки мыши. В консольной программе «telnet» вставка осуществляется нажатием правой кнопки мыши и выбором пункта меню «Вставить» в контекстном меню.

Листинг 6

```
conf t
! -----ISAKMP-----
crypto isakmp enable
crypto isakmp key 0 qwerty address 2.2.2.2
crypto isakmp aggressive-mode disable
crypto isakmp policy 1
encryption 3des
hash sha
authentication pre-share
group 2
lifetime 3600
exi
!
! -----IPSEC-----
ip access-list extended CRYPTO-ACL
10 perm ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
exi
crypto ipsec trans CRYPTO-SET esp-3des esp-sha-hmac
exi
crypto map CRYPTO-MAP 1 ipsec-isakmp
set peer 2.2.2.2
set transform-set CRYPTO-SET
match address CRYPTO-ACL
exi
! ----- applying IPSec usage -----
int fa4
crypto map CRYPTO-MAP
exi
exi
wr
!
```

ISAKMP

включение ISAKMP
ключевая фраза доступа
режим aggressive

алгоритм шифрования
тип хэша
режим аутентификации
группа Diffie-Hellman
время жизни ключа

IPSEC

объединяемые подсети

набор криптозащиты

IP-адрес роутера iRZ

внешний (WAN) интерфейс
применение IPSec

Далее приведена таблица 2.6 с описанием использованных директив конфигурации Cisco в сценарии, представленном в листинге 6.

Таблица 2.6. Настройка службы IPSec для роутера Cisco

Название параметра	Значение в данной конфигурации	Описание
Параметры ISAKMP / IKE		
включение ISAKMP	`enable`	Определяет – будет ли использован для обмена ключами протокол IKE ISAKMP. Значение в данной конфигурации – **enable**
ключевая фраза доступа	`qwerty`	Ключевая фраза для двунаправленной аутентификации обоих узлов. Допустимое значение - **любая комбинация печатаемых латинских символов кроме пробела**. Диапазон используемых символов: **a-z, A-Z, 0-9, спецсимволы**. *Значение параметра должно быть идентичным значению данного параметра профиля роутера iRZ*
режим aggressive	`disabled`	Определяет использование режима **aggressive**. Значение в данной конфигурации – **произвольное** *Значение параметра должно соответствовать значению данного параметра профиля роутера iRZ*
алгоритм шифрования	`3des`	Определяет алгоритм шифрования, используемый при проверке подлинности Значение в данной конфигурации – **произвольное** *Значение параметра должно соответствовать значению данного параметра профиля роутера iRZ*
тип хэша	`sha`	Определяет алгоритм расчёта хэша в фазе IKE (первой фазе). Значение в данной конфигурации – **произвольное** *Значение параметра должно соответствовать значению данного параметра профиля роутера iRZ*
режим аутентификации	`pre-share`	Способ аутентификации узлов. Значение **pre-shared key** обеспечивает аутентификацию по секретной ключевой фразе (паролю). Значение в данной конфигурации – **произвольное** *Значение параметра должно соответствовать значению данного параметра профиля роутера iRZ*
группа Diffie-Hellman	2	Определяет группу Diffie-Hellman, задающую уровень энтропии для проверки подлинности. Значение в данной конфигурации – **произвольное** *Значение параметра должно быть идентичным значению данного параметра профиля роутера iRZ*
время жизни ключа	`3600`	Срок жизни ассоциации безопасности (SA), в секундах

(продолжение на след. странице)

Таблица 2.6. Настройка службы IPSec для роутера Cisco (продолжение)

Название параметра	Значение в данной конфигурации	Описание
Параметры IPSEC		
объединяемые подсети	**192.168.2.0** 0.0.0.255 **192.168.1.0** 0.0.0.255	Определяет IP-адреса и маски объединяемых подсетей, где: 1-й адрес → удалённая подсеть; 2-й адрес → подсеть, обслуживаемая роутером Cisco
набор криптозащиты	esp-3des esp-sha-hmac	Определяет набор параметров для обработки трафика: 1-й параметр → алгоритмы, используемые для защиты пользовательских данных (шифрование трафика) 2-й параметр → функции, используемые для проверки подлинности (аутентификация трафика) *Значение обоих параметров должно соответствовать аналогичным значениям этих же параметров профиля роутера iRZ*
IP-адрес роутера iRZ	[2.2.2.2]	Определяет внешний фиксированный IP-адрес удалённого узла IPSec
внешний (WAN) интерфейс	fa4	Имя внешнего (WAN) интерфейса в системе Cisco iOS
применение IPSec	crypto map CRYPTO-MAP	Определяет необходимость применения операций и правил обработки пользовательского трафика службой IPSec для интерфейса, указанного в параметре "внешний (WAN) интерфейс", описанным выше

Примечание: На роутерах Cisco не требуется задавать явные разрешающие правила для обеспечения прохождения ISAKMP- и IPSec-трафика до их внутренней криптоподсистемы. Данные правила могут потребоваться только в случае использования в вычислительном комплексе заказчика вышестоящего сетевого экрана.

2.4.6. Настройка IPSec на роутере iRZ

Настройка службы IPSec на роутере должна быть выполнена по методу, описанному в разделе «**Настройка IPSec-туннеля на роутере №1**», за исключением параметров **Local Subnet** и **Remote Subnet** службы IPSec и параметров локального интерфейса. Значения этих параметров в данной конфигурации для роутера iRZ изменены на следующие:

- **Remote Subnet → 192.168.1.0**
- **Local Subnet → 192.168.2.0**
- Параметры обслуживаемой подсети:
  - IP-адрес локального интерфейса → **192.168.2.1**
  - IP-адрес обслуживаемой роутером iRZ подсети → **192.168.2.0 255.255.255.0**

2.4.7. Нагрузочная проверка возможности создания двунаправленного зашифрованного соединения

Для подтверждения работоспособности данной конфигурации необходимо передать полезную информацию между подсетями в обоих направлениях.

Для проверки доступности подсети, обслуживаемой роутером Cisco, из подсети, обслуживаемой роутером iRZ, выполните следующие действия:

1. Включите роутер iRZ и подключите его к компьютеру;
2. Откройте командную строку Windows;
3. Введите команду: «telnet 192.168.2.1»;
4. Введите имя пользователя и пароль доступа к роутеру iRZ;
5. Дождитесь появления строки приглашения консоли: «# _»;
6. Введите команду: «ping 192.168.1.1 –I 192.168.2.1 –c 4»;
   ("I" - прописная "i", от слова Interface)
7. Нажмите [*Enter*];
8. Дождитесь выполнения команды.

Вывод команды должен содержать информацию, подобную приведённой в листинге 7:

Листинг 7

```
PING 192.168.1.1 (192.168.2.1): 56 data bytes
64 bytes from 192.168.2.1: seq=0 ttl=64 time=4.822 ms
64 bytes from 192.168.2.1: seq=1 ttl=64 time=1.098 ms
64 bytes from 192.168.2.1: seq=2 ttl=64 time=0.976 ms
...
```

Для проверки доступности подсети, обслуживаемой роутером iRZ, из подсети, обслуживаемой роутером Cisco, выполните следующие действия:

1. Подключитесь к роутеру Cisco удалённо через Telnet, либо через COM-порт;
   (с помощью программы «PuTTY», либо «HyperTerminal»)
2. Дождитесь приглашения консоли управления Cisco;
   (как правило, приглашение содержит строку: « [имя_роутера]>_ »)
3. Введите команду: «ping [IP внутреннего интерфейса iRZ] source [IP внутреннего интерфейса Cisco]»;
   (В данной конфигурации: «ping 192.168.1.1 source 192.168.2.1»)
4. Нажмите [*Enter*];
5. Подождите некоторое время до окончания выполнения команды.

Сообщение страницы должно содержать информацию, подобную приведённой в листинге 8:

Листинг 8

```
Router>ping 192.168.1.1 source 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 120/124/140 ms
Router>
```

Показателем проверки в данном случае будет наличие и количество символов «!» (восклицательного знака) после ввода команды «**ping**».

Полное либо частичное отсутствие (менее 5) этих знаков говорит о том, что проверка завершилась неудачей, в данной ситуации для разрешения проблемы рекомендуется обратиться к документу «**Диагностика и методы устранения неисправностей роутера iRZ**», раздел «Служба IPSec».

2.5. Конфигурация

«RXX: static fixed IP-address ← RXX: private IP-address + NAT-T»

Предупреждение: Данная конфигурация не может быть использована в качестве примера, если в развертываемом решении предполагается использование выделенного APN.

Предупреждение: Данная конфигурация может быть использована только в случае, когда IP-адрес устройства NAT (NAPT) известен и гарантированно не изменится со временем, независимо ни от каких факторов.

Данная конфигурация позволяет решить одновременно несколько задач:

- прозрачное объединение подсетей филиалов, разнесённых территориально;
- защита информации, передаваемой между объединяемыми подсетями;
- исключение дополнительных затрат на внешний фиксированный IP-адрес.

Для реализации данной конфигурации на одном из роутеров должна быть использована SIM-карта с внешним фиксированным IP-адресом.

Ниже приведена схема соединения узлов (рис. 2.3) с описанием процесса применения данной конфигурации на роутере.

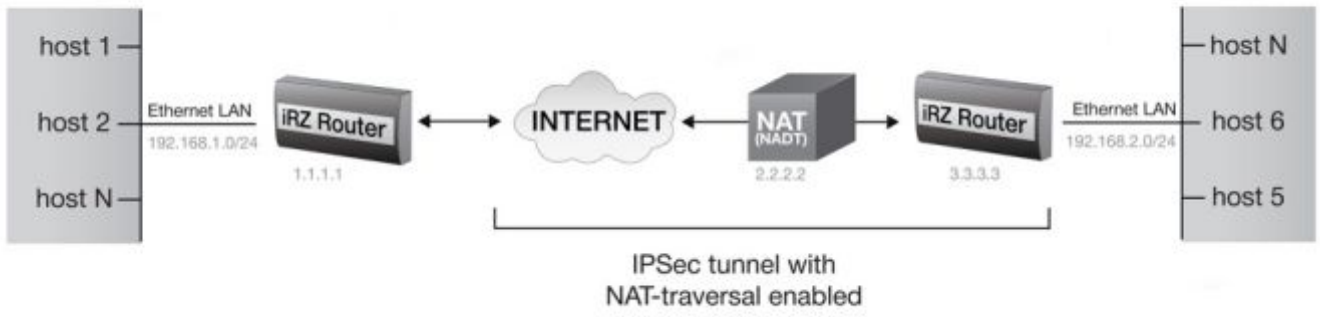

Рис. 2.3. Схема соединения узлов «роутер – роутер + NAT» (со статичным и приватным IP-адресом)

2.5.1. Подготовка к настройке

Процесс подготовки и развертывания данной конфигурации состоит из следующих этапов:

- настройка параметров локальных интерфейсов роутеров;
- настройка и проверка Интернет-подключения на обоих роутерах;
- проверка доступности роутеров:
  - проверка доступности роутера №1 по его внешнему фиксированному IP-адресу;
  - проверка доступности роутера №1 со стороны роутера №2 через Интернет;
- определение IP-адреса NAT-устройства;
- настройка IPSec-туннеля на обоих роутерах;
- нагрузочная проверка возможности создания двунаправленного зашифрованного соединения.

Для настройки Интернет-подключения следует обратиться к документу «**Руководство по эксплуатации роутеров iRZ**» (см. разд. «Интернет соединение по GSM-каналу»).

2.5.2. Настройка параметров локальных интерфейсов роутеров

В данном разделе в таблице 2.7 описаны параметры локальных Ethernet-интерфейсов настраиваемых роутеров.

Таблица 2.7. Настройки локальных роутеров с интерфейсом Ethernet

Роутер	Параметр	Значение параметра	Описание параметра
раздел Primary IP Address страницы Configuration → LAN) web-интерфейса роутеров			
роутер №1	IP Address	192.168.1.1	IP-адрес локального интерфейса
	Subnet Mask	255.255.255.0	Маска обслуживаемой подсети
роутер №2	IP Address	192.168.2.1	IP-адрес локального интерфейса
	Subnet Mask	255.255.255.0	Маска обслуживаемой подсети

2.5.3. Определение IP-адреса NAT-устройства

Для определения IP-адреса устройства NAT, к которому, в данной конфигурации подключён роутер №2, требуется выполнить следующие действия:

1. Включите роутер №2 и подключите его к компьютеру;
   (с помощью «crossover»-патчкорда)
2. Откройте Интернет-браузер;
   (любой современный браузер: «Internet Explorer», «Firefox», «Opera», «Chrome» и пр.)
3. Введите IP-адрес роутера в адресную строку браузера;
   (В данной конфигурации: **192.168.2.1**)
4. Убедитесь, что роутер установил Интернет-подключение;
   (состояние подключения отслеживается на странице Status an log → Internet,
   с помощью команды ping)
5. Введите в адресную строку адрес одного из сайтов: «myip.ru», «ip.xss.ru», или «2ip.ru»;
6. Нажмите [*Enter*];
7. Дождитесь загрузки страницы;
8. Запишите IP-адрес, который, как правило, указан явно на первой странице сайта.
   (данный IP-адрес является IP-адресом NAT-устройства)

2.5.4. Проверка доступности роутеров

Прежде чем переходить непосредственно к настройке службы IPSec на роутерах необходимо убедиться в их доступности из сети Интернет, а так же по отношению друг к другу. Это требуется для сокращения времени устранения проблем при создании IPSec-соединения на ранней стадии развертывания решения.

Проверка доступности роутера №1 по его внешнему фиксированному IP-адресу должна быть выполнена по методу, описанному в разделе «**Проверка доступности роутеров по их внешнему фиксированному IP-адресу**».

Проверка доступности роутера №1 со стороны роутера №2 через Интернет должна быть выполнена по методу, описанному в разделе «**Проверка прямой доступности между роутерами через Интернет**».

Проверка доступности роутера №2 со стороны роутера №1 через Интернет должна так же быть выполнена по методу, описанному в разделе «**Проверка прямой доступности между роутерами через Интернет**», однако вместо IP-адреса роутера №2 необходимо выполнять подстановку IP-адреса NAT-устройства.

2.5.5. Настройка IPSec-туннеля на обоих роутерах

Для выполнения условий конфигурации на роутере №1 будет использована SIM-карта с внешним фиксированным IP-адресом.

Настройка IPSec-туннеля на роутерах должна быть выполнена по методу, описанному в разделе «**Настройка IPSec-туннеля на роутере №1**», с одним отличием: параметр **NAT Traversal** настраиваемого профиля должен иметь значение **enabled**.

Примечание: Значение **enabled** параметра **NAT Traversal** должно быть установлено в профиле каждого роутера. В случае несоблюдения этого требования служба IPSec не будет функционировать корректно.

Предупреждение: Если устройство, выполняющее роль NAT, является подведомственным узлом заказчика и выполняет роль сетевого экрана с политикой, запрещающей по умолчанию любые соединения, то для работы службы IPSec в данной конфигурации необходимо явно задать два разрешающих правила. Они должны позволять трафику с портом назначения UDP 4500 следовать в обоих направлениях.

Для наглядности, в листинге 9 приведено схематичное представление необходимых правил.

Пренебрежение данной рекомендацией приведёт к невозможности работы службы IPSec.

Листинг 9

```
source.ip=iRZ-RXX-IP, source.port.udp=4500 permit TO destination.ip=ANY,
 destination.port.udp=ANY
source.ip=ANY, source.port.udp=4500 permit TO destination.ip=iRZ-RXX-IP,
 destination.port.udp=ANY
```

3. 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
Москва	
сайт компании в Интернете:	www.digitalangel.ru
тел. в Москве:	+7 (495) 974 74 22
e-mail:	info@digitalangel.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.