Wireless solutions
for M2M world

Защита локальной сети и сервисов средствами Firewall

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 подсистемы фильтрации сетевого трафика в решениях, построенных на базе роутеров iRZ. Данный документ не содержит всей информации по работе с роутером.

Версия документа		**Дата публикации**	
1.0		2013-04-30	
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 Port Forwarding;
  - **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. Обзор задач и функций сетевого экрана

2.1. Выполняемые задачи

Функционально, роутер с помощью сетевого экрана (firewall) решает следующие прикладные вопросы обслуживания сети в масштабе всего вычислительного комплекса:

- соблюдение заданных администратором сети политик разрешений и правил обработки трафика, следующего в обоих направлениях;
- зональное разделение адресного пространства локальной сети и ограничение его от адресного пространства сети оператора связи и/или сети Интернет.

Информация, представленная выше, является скорее обобщающей для процессов и событий, происходящих в сетевой подсистеме роутера. Ниже приведён более развёрнутый обзор задач и процессов, для выполнения которых подсистема обработки и фильтрации была встроена в роутер:

- **Защита/ограничение доступа к роутеру iRZ, локальной сети и её узлам:**
  - защита от несанкционированного доступа к:
    - службам управления роутером *(**HTTP/SSH/Telnet**);*
    - функциональным службам *(**COM-порт**, **GRE**,..);*
  - базовая защита от **сетевой атаки «на отказ»/DoS**
    Данная возможность достигается благодаря тому, что программное обеспечение роутера использует в своей основе ядро ОС Linux, позволяющее в ряде случаев установить некоторые ограничения по обработке сетевого трафика на уровне ядра.
    (за деталями по настройке данной функции требуется обратиться в отдел разработки компании «Радиофид», а так же к официальной документации ОС Linux, и в частности по параметрам ядра Linux)

- **Обеспечение возможности межсетевого взаимодействия:**
  - выполнение функции **Port Forwarding**;
  - в ряде случаев: переопределение маршрутов следования трафика;
  - **NAT**: Трансляция сетевых адресов/предоставление доступа в интернет участникам локальной сети, обслуживаемой роутером;
  - отбрасывание паразитного/избыточного трафика.

2.2. Режимы работы

Встроенный в роутер сетевой экран (firewall) предполагает три режима работы:

- **Выключен;**

  *(«**Disable firewall**» в выпадающем списке режимов на странице настроек)*

  Не применяется ни одно из правил, указанных в настройках сетевого экрана (firewall).

- **Запрещать по-умолчанию все соединения, кроме явно указанных в web-интерфейсе;**

  *(«**Allow specified, disable others**» в выпадающем списке режимов на странице настроек)*

  Будут запрещены все соединения, которые не разрешены явно с помощью установки соответствующих параметров на страницах web-интерфейса, отвечающих за настройку сетевого экрана (firewall) и доступа к службам удалённого управления.

- **Разрешать по-умолчанию все соединения, кроме явно указанных в web-интерфейсе;**

  *(«**Disable specified, allow others**» в выпадающем списке режимов на странице настроек)*

  Будут запрещены только те соединения, которые указаны на странице web-интерфейса, отвечающей за настройку сетевого экрана (firewall).

Сетевой экран (firewall), используемый в прошивке роутеров iRZ, представляет из себя урезанную версию программного пакета **iptables** и модуля ядра Linux – **netfilter**. Таким образом, критериями, на основе которых сетевым экраном (firewall) будет приниматься решение о дальнейшей судьбе пакета данных, являются правила. Web-интерфейс роутера позволяет задать до десяти одновременно активных правил. Параметры правил, на основе которых работает сетевой экран (firewall), описаны в разделе «Параметры правил сетевого экрана» этого документа.

В случае, когда количество необходимых к применению правил превышает 10 – можно воспользоваться средством расширения функционала роутеров iRZ – функциями сценариев Startup/IP-UP Script, позволяющих автоматически выполнять заданные команды и сценарии сразу после загрузки системы, или после установки Интернет-подключения соответственно.

Примечание: Если вы планируете использоваться сценарий Startup/IP-UP Script, настоятельно рекомендуем проверять синтаксис команды вызова **iptables**, чтобы избежать:

- потери доступа к устройству со стороны Интернет;
- потери доступа к устройству со стороны локальной сети;
- некорректного функционирования устройства в целом.

Ссылка: За разъяснениями деталей работы ПО **iptables**, а также уточнением синтаксиса команд управления таблицами правил рекомендуется обратиться к обучающему ресурсу Wikibooks – **http://ru.wikibooks.org/wiki/Iptables**

2.3. Принцип работы

Принцип работы сетевого экрана (firewall) можно рассмотреть на примере автомобильного КПП с большим количеством параллельных полос движения (TCP/UDP-портов). Для каждой из этих полос может быть определено правило, описывающее откуда машина (сетевой пакет с данными) должна следовать и куда, чтобы её пропустили. Количество правил сетевого экрана (firewall) ограничено только производительностью системы и объемом доступной энергонезависимой памяти на системном Flash-накопителе. На рис. 1 представлена импровизированная схема работы сетевого экрана (firewall) в процессе фильтрации пользовательского трафика.

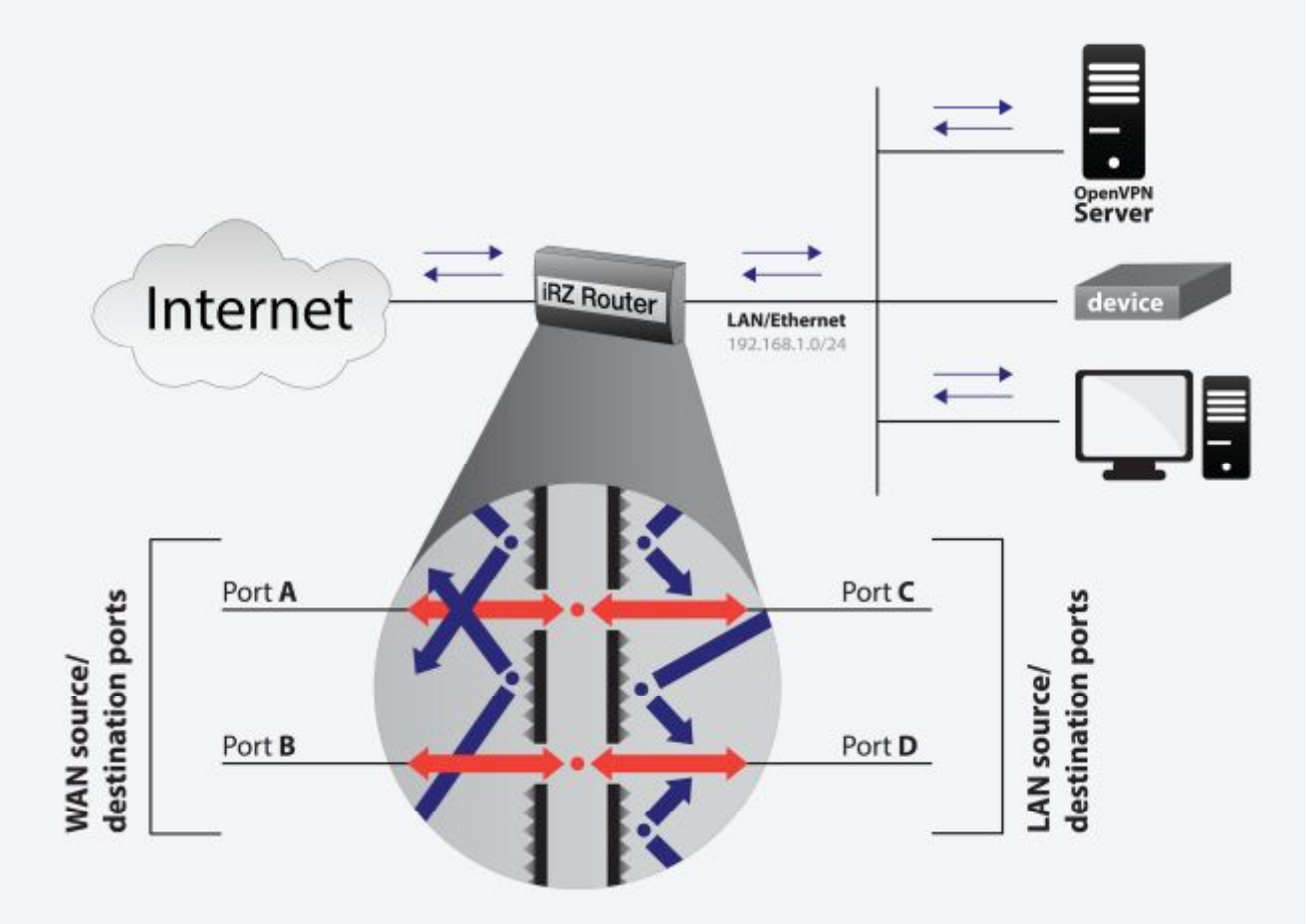

Рис. 1. Принцип работы сетевого экрана (firewall)

Ниже приведено описание параметров работы сетевого экрана (firewall) и их значений.

3. Описание параметров сетевого экрана

Сетевой экран (firewall) роутера работает в 3-х режимах: полностью отключен, запрещены или разрешены по умолчанию все соединения, кроме указанных в web-интерфейсе.

3.1. Параметры правил сетевого экрана

Рекомендация: Настоятельно рекомендуется выполнять установку параметров правил только после того, как сформирован первоначальный список правил в соответствии с выбранной политикой обработки трафика. Не рекомендуется настраивать сетевой экран (firewall) устройства без предварительных подготовительных мероприятий, особенно если оно подлежит к последующей установке на производственных, либо других критичных к сбоям объектах.

Параметр Type

Определяет тип адреса источника/получателя сетевых пакетов. Может иметь следующие значения:

- Любой узел (**«any address»**);
- Один IP-адрес (**«single address»**);
- IP-подсеть (**«subnet»**).

Параметр IP Address

Определяет IP-адрес сети, либо узла, который должен будет выступать в качестве источника или получателя сетевого пакета для успешного прохождения этого пакета через сетевой экран (firewall).

Параметр Net Mask

Определяет маску подсети, может быть задан только в случае, когда параметру **Type** присвоено значение **«subnet»**.

Параметр Protocol

Определяет протокол, который должен будет использоваться между узлами сетей, соединяемых роутером, для передачи данных. Для того, чтобы пользовательский трафик смог продолжить свой путь до пункта назначения, тип протокола, используемый для передачи данных должен совпадать с типом протокола, указанным в данном правиле.

Параметр Port

Номер TCP/UDP-порта отправителя, либо получателя данных.

ПРЕДУПРЕЖДЕНИЕ! Ввиду ограничений web-интерфейса для каждого из правил, применённых в таблице настроек сетевого экрана (firewall) создаётся два обратных правила, определяющих правила работы **iptables**: в одном из правил указаны IP-адрес и номер порта узла-источника; в другом же – IP-адрес и номер порта узла-получателя. Следует обратить внимание на то, что web-интерфейс не позволяет в рамках одного правила в качестве условий установить IP-адрес узла-отправителя и номер порта узла-получателя, равно как и IP-адрес узла-получателя и номер порта узла-отправителя.

Для выполнения условий в данной комбинации рекомендуется воспользоваться средствами командной строки (правило будет работать до перезагрузки устройства), либо средствами сценариев **Startup/IP-UP Script**

4. Возможные конфигурации

Данный раздел содержит три конфигурации, выступающие в качестве примеров, на основе которых технический персонал может сформировать для существующей сети конфигурацию, соблюдающую принятую в компании-заказчика политику защиты информации.

Прежде чем выполнять настройку сетевого экрана (firewall) необходимо определиться с тем, какие службы требуется защитить, какие TCP/UDP-порты используют данные службы и в каких адресных пространствах находятся узлы, доступ к службам которых необходимо запретить, либо разрешить.

Примечание: примеры конфигураций, представленные в данном документе могут быть применены в режиме сетевого экрана (firewall) «разрешить всё, что не указано в правилах»

4.1. Конфигурация «Запрет служебного трафика ICMP»

Данная конфигурация позволяет запретить служебный трафик, сигнализирующей о доступности узла для стороны, которая его генерирует. Как правило, ICMP протокол используется для проверки применённых правил маршрутизации в процессе построения сети заказчика, а так же для определения факта того, что тот или иной узел включён, либо работоспособен. Однако данный трафик рекомендован к запрещению, т.к. в случае, когда роутер будет отвечать на сообщения поступающие со стороны Интернет, это может стать поводом для возможного сканирования устройства на наличие уязвимых/открытых сетевых служб и последующих попыток проникновения в защищённую сеть заказчика. Ниже приведёны параметры, позволяющие запретить ICMP-трафик со стороны Интернет.

Таблица 1. Настройки конфигурации «Запрет доступа к сервису из Интернет»

Название параметра	Значение в данной конфигурации	Описание
Type	**Single address**	Тип правила – единственный IP-адрес
IP Address	**192.168.1.1**	IP-адрес роутера, на котором запущена служба
Net Mask	**[значение отсутств.]**	
Protocol	**ICMP**	Тип порта
Port	**[значение отсутств.]**	№ TCP-порта OpenVPN

4.2. Конфигурация «Запрет доступа к удаленным службам»

Данная конфигурация призвана запретить со стороны локальной сети доступ к одной или нескольким удаленным службам. Далее приведены настройки сетевого экрана (firewall), запрещающие доступ к web-страницам и службе ICQ.

Предупреждение:

В случае, если требуется запретить доступ со стороны локальной сети к службе, находящейся не на роутере, а на одном из узлов локальной сети не рекомендуется использовать сетевой экран (firewall) роутера, а установить ПО, выполняющее роль сетевого фильтра на самом узле, доступ к которому требуется запретить, т.к. топология сети может позволить обойти правила маршрутизатора, использующегося по-умолчанию и получить несанкционированный доступ к службе.

Кроме того доступ к службе, узел которой находится в локальной сети можно запретить только средствами командной строки роутера. Web-интерфейс предусматривает возможность запрета трафика только со стороны Интернет в локальную сеть и в обратном направлении.

Примечание: для множественного запрета доступа к нескольким службам одновременно необходимо настроить несколько правил, подобных приведённому в данном примере. Одно правило может содержать описание поведения только для одного узла

Таблица 2. Настройки конфигурации «Запрет доступа к сервису из локальной сети»

Название параметра	Значение в данной конфигурации	Описание
Правило №1		
Type	**Any address**	Тип правила – любой конечный адрес
IP Address	**[значение отсутств.]**	-
Net Mask	**[значение отсутств.]**	-
Protocol	**TCP**	Тип порта
Port	**80**	№ TCP-порта web-служб серверов Интернет
Правило №2		
Type	**Any address**	Тип правила – любой конечный адрес
IP Address	**[значение отсутств.]**	-
Net Mask	**[значение отсутств.]**	-
Protocol	**TCP**	Тип порта
Port	**5190**	№ TCP-порта службы ICQ

4.3. Конфигурация «Запрет доступа к локальным службам»

Данная конфигурация позволяет запретить доступ к службе со стороны Интернет. В этом примере будет запрещён доступ к службе OpenVPN. Эта конфигурация может быть использована в случае, когда техническое решение подразумевает использование OpenVPN-туннеля, но сервер OpenVPN находится в локальной сети компании заказчика. Если механизм аутентификации упрощён и подразумевает использование имени пользователя и пароля, то рекомендуется запретить доступ к OpenVPN со стороны Интернет во избежание перебора пароля и вероятного получения несанкционированного доступа к защищаемой сети.

Таблица 3. Настройки конфигурации «Запрет доступа к сервису из Интернет»

Название параметра	Значение в данной конфигурации	Описание
Type	**Single address**	Тип правила – единственный IP-адрес
IP Address	**192.168.1.1**	IP-адрес роутера, на котором запущена служба
Net Mask	**-**	-
Protocol	**TCP**	Тип порта
Port	**1194**	№ TCP-порта OpenVPN

4.4. Конфигурация «Запрет доступа к определенному узлу локальной сети»

Данная конфигурация подразумевает запрет любого вида трафика по направлению к указанному узлу. Полный запрет означает невозможность получения доступа ни к службам узла, ни определению его состояния с помощью ICMP-запросов. Данный пример может быть полезен в случае, когда используется топология сети, подразумевающая зону DMZ, в которой находится более одного узла, и доступ к этим узлам должен быть ограничен.

Таблица 4. Настройки конфигурации «Запрет доступа к узлу локальной сети»

Название параметра	Значение в данной конфигурации	Описание
Type	**Any address**	Тип правила – единственный IP-адрес
IP Address	**[значение отсутств.]**	IP-адрес узла, трафик от которого будет блокирован
Net Mask	**[значение отсутств.]**	Тип порта
Protocol	**All**	IP-адрес узла, на котором запущена служба
Port	**[значение отсутств.]**	№ TCP/UDP-порта

5. 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.