Настройка IPFW + NAT в FreeBSD 14

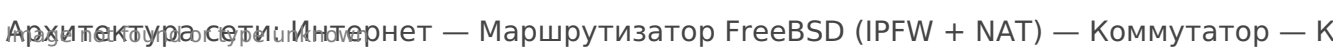
Сервер FreeBSD будет выступать в качестве маршрутизатор (роутера) локальной сети, для этого будет использоватся Firewall IPFW и модуль маршрутизации NAT. Необходимо настроить раздачу интернета во внутреннею сеть и открыть порты сервисов которые работают на сервере. Одна сетевая карта сервера смотрит в интернет, вторая в локальную сеть. На сервера FreeBSD работает веб-сервер.

Оглавление статьи:

1. Архитектура маршрутизатора сети

Настроить можно как угодно и что угодно. Архитектура, которая используется в примере идентична по возможностям для большинства домашних роутеров.

Сервер FreeBSD имеет два сетевых интерфейса. К одной сетевой карте подключен кабель интернет провайдера с внешним IP адресом, к другой подключен кабель до коммутатора внутренний сети. Компьютеры внутренней сеть должно иметь доступ в интернет.



На сервере работает веб-сервер и другие сервисы, для это необходимо открыть порты доступа. Также надо настроить возможность проброса портов с внешнего IP адреса на компьютеры локальной сети, для торрент-клиентов, сетевых игр и так далее...

2. Включение IPFW + NAT

Открываем файл **/etc/rc.conf**

```
nano /etc/rc.conf
```

Добавляем строки

```
gateway_enable="YES" # Использовать сервер FreeBSD в качестве шлюза
firewall_enable="YES" # Включить IPFW
firewall_nat_enable="YES" # Включить NAT
firewall_script="/etc/ipfw.rules" # Файл с правилами IPFW + NAT
```

Добавляем строку если необходимо логировать какие-то правила. Запись событий будет происходить в файл **/var/log/security** журнала безопасности.

```
firewall_logging="YES"
```

В результате фрагмент файла **rc.conf** с параметрами сетевых карт и включённым маршрутизатором должен выглядеть следующим образом

Открыт файл /etc/rc.conf редактором nano в FreeBSD. Настроены параметры сетевых кар

Дополнительно можно добавить загрузку модулей ядра IPFW + NAT непосредственно в момент загрузки системы.

Открываем файл **/boot/loader.conf**

```
nano /boot/loader.conf
```

Добавляем строки

```
ipfw_load="YES"
ipfw_nat_load="YES"
libalias_load="YES"
```

При загрузке FreeBSD сразу будут загружатся: **ipfw** – модуля ядра IPFW, **ipfw_nat** – модуль базовых функций NAT, **libalias** – модуль полных функций NAT.

По умолчанию в IPFW весь трафик запрещен, поэтому при его запуске или после перезагрузки, без настройки файла правил, будет невозможно подключится через SSH.

Настраиваем файл правил IPFW до его запуска или временно изменяем поведение IPFW на “разрешить все по умолчанию”.

Для этого в файл **/boot/loader.conf** добавляем строку

```
net.inet.ip.fw.default_to_accept="1"
```

Теперь по умолчанию последнее правило IPFW будет разрешать любой трафик на всех сетевых картах. После завершения настройки рекомендую убрать добавленную строку.

IPFW + NAT может быть включен непосредственно в ядре FreeBSD. Для этого включаем в ядро необходимые модули

```
options IPFIREWALL # Включить IPFW
options IPFIREWALL_VERBOSE # Включить возможность логирования трафика
options IPFIREWALL_VERBOSE_LIMIT=5 # Количество одинаковых пакетов в одну запись лога
#options IPFIREWALL_DEFAULT_TO_ACCEPT # По умолчанию пропускать все, за исключением запрещенного правилами
options IPFIREWALL_NAT # Включить базовые возможности NAT
options LIBALIAS # Включить полные возможности NAT
#options IPFIREWALL_NAT64 # Включить поддержку NAT64
#options IPFIREWALL_NPTV6 # Включить поддержку IPv6 NPT
#options IPFIREWALL_PMOD # Поддержку модулей модификации протоколов
#options IPDIVERT # Включить NAT через natd(8)
```

Читать как собрать ядро FreeBSD: Конфигурация и сборка ядра FreeBSD 14

3. Синтаксис правил IPFW + NAT

Правила IPFW имеют примерно следующий синтаксис:

```
add <номер правила> [allow/deny] [ip/tcp/udp/...] from [any/me/<IP-адрес>] <порт> to [any/me/<IP-адрес>] <порт> {Опции}
```

Работу правила лучше объяснить на примере, например открываем 80 порт для веб-сервера

```
add 00400 allow tcp from any to me 80 in via em0 setup keep-state
```

Добавляется правило с номером 00400 (необязательный параметр) которое разрешает TCP пакеты с любого IP адреса до IP адреса сервера с **80** портом входящие через сетевую карту **em0** и устанавливаются опции **setup** и **keep-state**. Опция **setup** сопоставляет TCP-пакеты, у которых установлен бит SYN, но отсутствует бит ACK, **keep-state** создает динамическое правило двунаправленного трафика.

Для работы маршрутизации и проброса портов, необходимо создавать экземпляр NAT, он имеет следующий синтаксис:

```
nat <номер> config [ip <IP-адрес> / if <сетевая карта>] {Опции}
```

Например, создаем экземпляр NAT с номером 1, через сетевой интерфейс em0 осуществляется выход в интернет, пробрасываем TCP порт 5530 с внешнего IP на компьютер внутренний сети с адресом 192.168.0.5 на том же порту

```
nat 1 config if em0 same_ports unreg_only deny_in reset redirect_port tcp 192.168.0.5:5530 5530
```

Доступные опции для **nat**:

- **same_ports** – следит за тем, чтобы псевдонимы портов и локальные номера портов были сопоставлены одинаково;
- **unreg_only** – обрабатывать только частный адресные пространства (192.168.0.0, 10.0.0.0, ...);
- **deny_in** – запретить любое входящие соединение из внешнего мира;
- **reset** – сбрасывать и обновлять таблицу маршрутизации, если изменится внешний IP;
- **redirect_port** – перенаправление порта;
- **redirect_addr** – перенаправление IP-адреса.

4. Конфигурация IPFW + NAT

Создаем файл конфигурации **/etc/ipfw.rules**

```
nano /etc/ipfw.rules
```

Чем меньше правил, тем выше производительность IPFW. Объединяй по возможности несколько правил в одно.

Файл конфигурации IPFW + NAT будет выглядеть примерно так:

```
#!/bin/sh
# Очищаем список правил IPFW
ipfw -q -f flush
# Команда добавления правила, -q — режим без вывода сообщений
cmd="ipfw -q add"
# Сетевые карты заносим в переменные
net="em0" # сетевая карта интернета
lan="em1" # сетевая карта локальной сети

# Разрешить любой трафик внутри loopback интерфейса
$cmd 00010 allow all from any to any via lo0
# Запретить любой трафик извне до локальных адресов
$cmd 00011 deny ip from any to 127.0.0.0/8
$cmd 00012 deny ip from 127.0.0.0/8 to any

# Разрешить любые пакеты внутри локальной сети
$cmd 00050 allow ip from any to any via $lan

# Разрешить доступ к SSH серверу по 22 порту
$cmd 00510 allow tcp from any to me 22 in via $net
# Разрешить доступ к веб-серверу по 80 и 443 портам (HTTP/HTTPS)
$cmd 00520 allow tcp from any to me 80,443 in via $net

# Настройка маршрутизации IPFW + NAT
# Создаем экземпляр NAT с номером 1 и перенаправляем TCP 5530 порт на компьютер локальной сети с адресом 192.168.0.5
ipfw -q nat 1 config if $net same_ports unreg_only deny_in reset redirect_port tcp 192.168.0.5:5530 5530
# Разрешить проходить TCP и UDP пакетам, ping через NAT на сетевую карту интернета
$cmd nat 1 tcp from any to any via ${net}
$cmd nat 1 udp from any to any via ${net}
$cmd nat 1 icmp from any to any via ${net}
```

В таком варианте все исходящие пакеты с сервера и локальный сети проходят через NAT и создается двунаправленное правило для входящих пакетов. Входящие пакеты из интернета запрещены параметром **deny_in** в экземпляре NAT. Для открытия порта веб-серверу и SSH созданы правила, которые разрешают только входящие пакеты, а для исходящих пакетов будет использоватся правило NAT. В такой конфигурации firewall работает без динамических правил создаваемых опцией keep-state.

Вносим изменения и сохраняем файл с правила IPFW + NAT и можно приступать к запуску IPFW.

5. Запуск и перезапуск IPFW + NAT

Будь внимателен. Если есть ошибка или неточность в правилах, можно потерять доступ по SSH.

Запускаем службу IPFW

```
service ipfw start
```

Когда будут внесены какие-то изменения в файл с правилами межсетевого экрана и маршрутизации, необходимо перезапустить IPFW.

Перезапускаем службу IPFW

```
service ipfw restart
```

6. Команды IPFW + NAT

Вывести статистику по работе правил IPFW

```
ipfw -a -d -t list
```

- **-a** — количество совпавших пакетов и переданных байт;
- **-d** — вывести динамические правила;
- **-t** — время когда сработало правило последний раз;
- **-e** — динамические правила с истекшим сроком действия.

Удалить правило с указанным номером, например 00500

```
ipfw delete 00500
```

Вывести список экземпляром NAT и их параметры

```
ipfw nat show config
```

Revision #1
Created 4 July 2025 10:48:32 by buzz
Updated 4 July 2025 10:49:35 by buzz