

## Редирект порта с гейта на внутреннюю машину (natd)

Автор: Administrator

07.01.2010 22:18 - Обновлено 28.05.2010 13:18

---

### Редирект порта с гейта на внутреннюю машину (natd)

Автор: lissyara.

Оригинал: [http://www.lissyara.su/articles/freebsd/trivia/natd\\_redirect\\_port/](http://www.lissyara.su/articles/freebsd/trivia/natd_redirect_port/)

Понадобилось выпустить локальную машину по одному из портов в инет (www сервер, но, ввиду занятости 80 порта, снаружи он будет на 81-м. А вообще народ это юзает для всяких edonkey и прочего хламу). Гейт на FreeBSD6.0 - на нём уже стоял natd - народу из локалки надо же лазить в инет. Почитавши man natd, конкретно, раздел про redirect\_port, стало ясно - сложностей особых нету. Для начала, для собственного удобства, решил переделать запуск natd - у меня он стартовал из /etc/rc.conf с указанием в виде флагов всех ключей запуска. Неудобно - а если завтра понадобится ещё на 5-ти машинах подобное мутить? Там строка запуска в километр будет. Итак. Приводим /etc/rc.conf к такому состоянию (показан кусок касающийся тока natd):# NATD  
natd\_enable="YES"  
natd\_flags="-f /etc/natd.conf"

ну и создаём указанный файл, такого содержания:# Интерфейс на котором работает natd (внешний)

```
interface rl0
# Пробовать оставить тот же самый порт у исходящих пакетов.
# При таком флаге лучше работают протоколы типа RPC. Если это
# невозможно то порт будет изменён.
same_ports
# nat`ить только частные сети (у вас же внутри частная сеть?)
unregistered_only
# самое интересное - то, ради чего все и затевалось.
# Редиректим пакеты по протоколу tcp, приходящие на внешний порт
# 81 на машину с адресом 192.168.20.251 и на 80-й порт.
redirect_port tcp 192.168.20.251:80 81
```

Заметьте в файле используется не краткая а полная форма записи ключей. Потом перезапускаем машину (или убиваем natd и запускаем с командной строки с нужными ключами-файлами), интернет должен работать как и работал, а вот при попытке зайти на 81 порт - скорей всего будет облом. Файрволл. Я убил минут 30 пока понял почему оно работаете так и только так:\${FwCMD} add allow tcp from any to 192.168.20.251 80 via \${LanOut}

Видать, пакеты в nat попадают ещё до файрволла, потому и приходится изгаляться с разрешением внутреннего адреса на внешнем интерфейсе (Вообще, если вдаваться в подробности - то пакеты через файр проходят неоднократно, и на каком из заходов

## Редирект порта с гейта на внутреннюю машину (natd)

Автор: Administrator

07.01.2010 22:18 - Обновлено 28.05.2010 13:18

---

действует это правило - я не знаю :()

Вот тока после этого и заработало.