IPFW NAT

Начнем

```
uname -a
FreeBSD roller.amo.ka 10.3-STABLE FreeBSD 10.3-STABLE #0: Thu
Nov 9 22:33:21
EET 2017 svm@roller.amo.ka:/usr/obj/usr/src/sys/ROLLER i386
```

Собираем ядро с такими опциями:

```
IPFW NAT ########################
options IPFIREWALL
options IPFIREWALL_DEFAULT_TO_ACCEPT
options IPFIREWALL_VERBOSE
options IPFIREWALL_VERBOSE_LIMIT=50
options IPFIREWALL_NAT
options LIBALIAS
options ROUTETABLES=2
options DUMMYNET
####################################
```

и добавляем в sysctl и делаем sysctl restart

```
net.inet.ip.fw.one_pass=1
```

или просто даем команду

```
sysctl net.inet.ip.fw.one_pass=1
```

net.inet.ip.fw.one_pass: 1 Когда установлено, пакет, выходящий из потока *dummynet*, не проходит через брандмауэр повторно, в противном случае, после обработки канала пакет повторно вводится в брандмауэр по следующему правилу.

Синтаксис написания правил ядерного IPFW NAT следующий:

```
ipfw [-q] nat number config config-options
```

Если явно не указать номер правила nat, система присваивает правилу номер 123.

В /etc/rc.conf добавляем

```
gateway_enable=«YES»

firewall_enable="YES"
firewall_nat_enable="YES"
firewall_script="/etc/firewall.script"
firewall_logging="YES"
dummynet_enable="YES"
```

Делаем простейший файервол

```
ee /firewall.script

#!/bin/sh

# Задаём строку для обращения к ipfw.
ipfw="/sbin/ipfw -q"

# Сетевая карта в которую вставлен провод от провайдера.
LanOut="em0"
IpOut="192.168.1.134"

# Сетевая карта "смотрящая" во внутреннюю сеть.
LanIn="em2"
IpIn="10.0.0.1"

# DMZ
LanDmz="em1"
IpDmz="192.168.2.162"
NetDmz="192.168.2.0"
MaskDmz="28"

# Внутренняя подсеть.
NetIn="10.0.0.0"

# Сетевая маска внутренней подсети.
NetMask="24"

# Если до выполнения этого сценария в фаерволе
# были какие-то правила - сбрасываем их.
${ipfw} -f flush

# Создаём таблицу с пользователями, которым разрешен доступ в
```

```
Интернет.
# Если в таблице 0 были какие-то значения - сбрасываем их.
${ipfw} -f table 0 flush
${ipfw} table 0 add 10.0.0.0/24

# Сбрасываем все ограничители.
${ipfw} -f pipe flush

# Сбрасываем все очереди.
${ipfw} -f queue flush

# Таблица DMZ
${ipfw} table 10 add 192.168.2.161
${ipfw} table 10 add 192.168.2.163
${ipfw} table 10 add 192.168.2.164

${ipfw} add deny ip from any to any not verrevpath in

# MAIL
${ipfw} add allow tcp from any to 192.168.2.163 25, 587
${ipfw} add allow tcp from 192.168.2.163 to any 25, 587

# NAT
${ipfw} add nat 1 config log if em0 reset same_ports
${ipfw} add nat 1 ip from table\(0\) to not table\(10\) via
em0
#${ipfw} add nat 1 ip from 10.0.0.0/24 to not table\(10\) via
em0
${ipfw} add nat 1 ip from any to 192.168.1.134 via em0
```

Где *table 10* – не идет через *NAT*

Статистику можно посмотреть так:

```
ipfw nat 1 show
```

Пример: нужно сделать проброс портов для RDP сервера во внутренней сети с IP 10.0.0.20. Тогда правило HATa примет вид

```
${ipfw} add nat 1 config log if em0 reset same_ports \
       redirect_port tcp 10.0.0.20:3389 3389
```

Перезагружаем IPFW и смотрим

```
ipfw nat 1 show config
```

http://www.lissyara.su/articles/freebsd/tuning/ipfw_nat/
http://ipfw.ism.kiev.ua/ipfw.html
https://mdex-nn.ru/page/probros-portov-v-jadernom-ipfw-nat.html