

shaper_start.sh

Программа shaper_start.sh для инициализации шейпера и управления фаерволом для OS FreeBSD.

Установка

```
cp /usr/abills/misc/freebsd/shaper_start.sh /usr/local/etc/rc.d/
```

Аргументы программы

start [test]	Включить шейпер
stop [test]	Отключить шейпер
test	Включить шейпер на 10 минут. Сделано с целью тестирования и предотвращения блокировки сервера

Список rc.conf параметров для шейпера

abills_shaper_enable="YES"	Включить шейпер. При включении шейпера удаляются все текущие настройки фаервола и устанавливаются только те, которые прописаны для shaper_start.sh. Если нужно добавить дополнительные параметры их стоит внести в файл /etc/fw.conf
abills_shaper_if="em0"	Интерфейс шейпера (по умолчанию ng*)
abills_nas_id=""	
abills_ip_sessions=""	Лимитирование количества IP сесий для клиента
abills_nat="EXTERNAL_IP: INTERNAL_IPS, INTERNAL_IPS2:NAT_IF"	Включение NAT EXTERNAL_IP - IP адрес интерфейса смотрящего в интернет. Если параметр не указан система автоматически выбирает первый адрес с интерфейса маршрутизации по умолчанию INTERNAL_IPS - пул адресов, которым разрешён доступ в интернет INTERNAL_IPS2 - второй пул, адресов которым разрешён доступ в интернет NAT_IF - имя интерфейса смотрящего в интернет. Если параметр не указан система автоматически определяет интерфейс маршрутизации по умолчанию. Можно указать несколько правил для трансляции во внешний адрес через точку с запятой ;
abills_dhcp_shaper=""	Включить IPoE шейпер. Только если у Вас установлен модуль FreeRADIUS DHCP
abills_neg_deposit=""	Включение перенаправления на портал при израсходованном депозите
abills_portal_ip="me"	IP адрес портала. По умолчанию me
abills_mikrotik_shaper=""	Поднятие правил шейпера на Mikrotik серверах доступа, аргумент номера серверов доступа
abills_ipn_nas_id="1;5;6"	Номер IPN сервера доступа
abills_ipn_if=""	Интерфейс для IPN шейпера
abills_ipn_allow_ip=""	Список адресов, разрешенных без авторизации
abills_squid_redirect="YES"	Включение перенаправления на прокси сервер всего трафика в 40-й таблице (ipfw table 40 list) Для работы с перенаправления пользователей IP в 40-й таблицу: настройка squid версии 2.6 и выше: squid.conf http_port 192.168.0.1:3128 transparent

Шейпер ng_car

При использовании шейпера ng_car в **abills/libexec/config.pl** добавьте \$conf{ng_car}=1;

Шейпер DUMMYNET

При использовании шейпера DUMMYNET в [abills/libexec/config.pl](#) ничего добавлять не надо.

Дополнительные параметры

2 внешних канала

```
GW2_IF_IP="192.168.0.2"      # IP
GW2_IP="192.168.0.1"        # IP
GW2_REDIRECT_IPS="10.0.0.0/24" #
```

Внесение дополнительных правил в фаервол

Для внесения дополнительных правил в фаервол нужно занести их в файл **/etc/fw.conf** и прописать в **/etc/rc.conf**. Дополнительные правила берутся исключительно с файла **/etc/fw.conf**

```
firewall_type="/etc/fw.conf"
```

Правила вносятся в таком формате

```
add 10 allow ip from any to 10.0.0.1 via em0
add 12 allow ip from 10.0.0.1 to any via em0
```

Правила в файле /etc/fw.conf не должны дублировать номера уже существующих правил

NAT

для работы NAT необходимо скомпилировать ядро системы ([Сборка ядра FreeBSD](#)) с опцией

```
options      IPFIREWALL_NAT
```

Таблицы NAT

33	Таблица с исходящими IP адреса
34	Таблица с внутренними IP адреса

Активация нетблок

Номера правил

115	Перенаправление на страницу предупреждения
116	Блокировка ресурса

Таблицы

13	Адреса для блокировки
----	-----------------------

Временный доступ для пополнения

/etc/rc.conf

```
abills_paysys_tmp_access="YES"
```

Правило

120	Открытие временного доступа для пополнения счета
121	Открытие временного доступа для пополнения счета

Таблицы

16	Адреса клиентов с временным доступом. Аргумент передается как UID
----	--

```
${IPFW} add 120 allow all from "table(16)" to any via ${IF}  
${IPFW} add 121 allow all from any to "table(16)" via ${IF}
```

Дополнительно

[FreeBSD Dummynet/table шейпер](#)