

## Internet IPoE

Предоставление некоммутируемых услуг Internet

### Контроль доступа и нарезка трафика

При включении сессии выполняется правило указанное в конфигурационном файле (config.pl) **\$conf{INTERNET\_IPOE\_START}** при завершении **\$conf{INTERNET\_IPOE\_STOP}**. Система данным командам передаёт следующие атрибуты

%IP	IP адрес клиента
%MASK	битная маска (32,24)
%NUM	номер правила (\$conf{INTERNET_IPOE_FIRST_RULE} + (PORT или последняя цифра IP адреса) )
%LOGIN	Логин
%SPEED_IN	входящая скорость
%SPEED_OUT	исходящая скорость

а также переменные окружения

NAS_IP_ADDRESS	IP адрес сервера доступа
NAS_MNG_USER	Пользователь для управления сервером доступа
NAS_MNG_IP_PORT	IP:PORT управления сервером доступа
NAS_MNG_IP	NAS IP управления
NAS_MNG_PORT	порт управления сервером доступа
NAS_ID	Номер сервера доступа
NAS_TYPE	Тип сервера доступа

В качестве шейпера удобно использовать **/usr/abills/libexec/linkupdown**.

#### 1. Пример правила открытия доступа

##### abills/libexec/config.pl

```

$conf{INTERNET_IPOE_START}='SUDO=/usr/local/bin/sudo;
CMD="${SUDO} /usr/abills/libexec/linkupdown ipn up getif %LOGIN %IP %DEBUG > /dev/null 2>&1";
if [ "${NAS_TYPE}" = "mikrotik" ]; then CMD="/usr/abills/libexec/linkupdown mikrotik up - %LOGIN %IP
NAS_HOST=${NAS_MNG_IP_PORT} NAS_MNG_USER=${NAS_MNG_USER}";
elif [ "${NAS_MNG_IP_PORT}" != "" ]; then CMD="/usr/bin/ssh -o StrictHostKeyChecking=no -i
/usr/abills/Certs/id_rsa.${NAS_MNG_USER} ${NAS_MNG_USER}@${NAS_MNG_IP_PORT} \"${CMD}\""; fi;
eval "${CMD}";

$conf{INTERNET_IPOE_STOP}='SUDO=/usr/local/bin/sudo;
CMD="${SUDO} /usr/abills/libexec/linkupdown ipn down getif %LOGIN %IP %DEBUG > /dev/null 2>&1";
if [ "${NAS_TYPE}" = "mikrotik" ]; then CMD="/usr/abills/libexec/linkupdown mikrotik down - %LOGIN %IP
NAS_HOST=${NAS_MNG_IP_PORT} NAS_MNG_USER=${NAS_MNG_USER}";
elif [ "${NAS_MNG_IP_PORT}" != "" ]; then CMD="/usr/bin/ssh -o StrictHostKeyChecking=no -i
/usr/abills/Certs/id_rsa.${NAS_MNG_USER} ${NAS_MNG_USER}@${NAS_MNG_IP} \"${CMD}\""; fi;
eval "${CMD}";

```

Для типа сервера - mikrotik-dhcp:

```

$conf{INTERNET_IPOE_START}='SUDO=/usr/local/bin/sudo;
CMD="${SUDO} /usr/abills/libexec/linkupdown ipn up getif %LOGIN %IP %DEBUG > /dev/null 2>&1";
if [ "${NAS_TYPE}" = "mikrotik_dhcp" ]; then CMD="/usr/abills/libexec/linkupdown mikrotik up - %LOGIN
%IP NAS_HOST=${NAS_MNG_IP_PORT}

```

```
| NAS_MNG_USER=${NAS_MNG_USER}";  
| elif [ "${NAS_MNG_IP_PORT}" != "" ]; then CMD="/usr/bin/ssh -o StrictHostKeyChecking=no -i  
| /usr/abills/Certs/id_rsa.${NAS_MNG_USER}  
| ${NAS_MNG_USER}@${NAS_MNG_IP} \"${CMD}\""; fi;  
| eval "${CMD}";  
|  
| $conf{INTERNET_IPOE_STOP}='SUDO=/usr/local/bin/sudo;  
| CMD="${SUDO} /usr/abills/libexec/linkupdown ipn down getif %LOGIN %IP %DEBUG > /dev/null 2>&1";  
| if [ "${NAS_TYPE}" = "mikrotik_dhcp" ]; then CMD="/usr/abills/libexec/linkupdown mikrotik down - %LOGIN  
| %IP NAS_HOST=${NAS_MNG_IP_PORT}  
| NAS_MNG_USER=${NAS_MNG_USER}";  
| elif [ "${NAS_MNG_IP_PORT}" != "" ]; then CMD="/usr/bin/ssh -o StrictHostKeyChecking=no -i  
| /usr/abills/Certs/id_rsa.${NAS_MNG_USER}  
| ${NAS_MNG_USER}@${NAS_MNG_IP} \"${CMD}\""; fi;  
| eval "${CMD}";
```

И дополнительная команда фильтров

### **\$conf{INTERNET\_IPOE\_FILTER}**

Полный путь к программе, которая запустится, если у клиента заполнено поле Filter ID. Данная программа запускается после команд прописанной в \$conf{IPN\_FW\_START\_RULE} и \$conf{IPN\_FW\_STOP\_RULE}. Программе передаются следующие аргументы %STATUS (ONLINE\_ENABLE, ONLINE\_DISABLE, HANGUP)

```
%LOGIN  
%IP  
%FILTER_ID  
%PORT  
%UID
```

в виде аргументов.

Также передаются переменные окружения:

```
NAS_IP_ADDRESS  
NAS_MNG_USER  
NAS_MNG_IP_PORT  
NAS_MNG_IP  
NAS_MNG_PORT
```

Не забывайте, что при ручной активации пользователя программа может выполняться с правами веб-сервера, поэтому лучше её запускать через sudo. Пример: abills/misc/ipn\_filter.sh

Также внизу указано настройка дополнительных параметров для разных операционных систем и удалённых серверов доступа

## FreeBSD

Управление доступом, шейпером и переинициализация сессий при перезагрузке сервера осуществляется программой **/usr/local/etc/rc.d/shaper\_start.sh**

параметры /etc/rc.conf

<b>abills_shaper_enable=«YES»</b>	Поднятие правил шейпера при перезапуске системы
<b>abills_ipn_nas_id=«Номер IPN наса»</b>	Номер сервера доступа. Обязательный параметр
<b>abills_ipn_if=«интерфейс к которому подключаются пользователи»</b>	Интерфейс к которому подключаются клиенты
<b>abills_ipn_allow_ip=«разрешённые ип адреса»</b>	Разрешённые без авторизации IP адреса. Разделяются запятой

<code>abills_nat=«xx.xx.xx.xx:10.0.0.0/16:interface»</code>	Если нужно использовать NAT
---	-----------------------------

При использовании шейпера ipfw система по умолчанию использует правила с номера 20000 по 40000. Для изменения номера начального правила можно воспользоваться опцией \$conf{IPN\_FW\_FIRST\_RULE}.

sudo

Установка sudo, для запуска правил фаервола от имени пользователя, под которым работает WEB сервер. freebsd:

```
# cd /usr/ports/security/sudo
# make
# make install
```

**/usr/local/etc/sudoers**

```
#Allow ABills shapper
www ALL = NOPASSWD: /usr/abills/libexec/linkupdown
www ALL = NOPASSWD: /sbin/ipfw
```

**Linux**

Скрипт которые подготавливает интерфейс для использования шейпера и устанавливает контроль доступа .

**/etc/rc.d/init.d/shaper\_start.sh**

**/etc/rc.conf**

```
abills_shaper_enable="YES"
abills_ipn_if="eth0,eth2"
abills_nat_enable=":192.168.0.0/24:eth1"
```

<b>eth0,eth2</b>	интерфейс в локальную сеть к которому подключены пользователи
<b>eth1</b>	интерфейс наружу
<b>192.168.0.1</b>	локальный IP сервера
<b>192.168.0.0/255.255.255.0</b>	локальная сеть

или альтернативный скрипт

```
#!/bin/sh
# При использовании нескольких интерфейсов указываем их через пробел
INTERFACES='eth0 eth2';
TC="/sbin/tc"

for INTERFACE in ${INTERFACES}; do
  TCQA="${TC} qdisc add dev ${INTERFACE}"
  TCQD="${TC} qdisc del dev ${INTERFACE}"

  $TCQD root &>/dev/null
  $TCQD ingress &>/dev/null

  $TCQA root handle 1: htb
  $TCQA handle ffff: ingress

  echo "Shaper UP ${INTERFACE}"
done
```

```
# Доступ к странице авторизации
/sbin/iptables -t nat -A PREROUTING -s 192.168.0.0/24 -p tcp --dport 80 -j REDIRECT --to-ports 80
/sbin/iptables -t nat -A PREROUTING -s 192.168.0.0/24 -p tcp --dport 443 -j REDIRECT --to-ports 80

# Закрыть доступ неактивизированным хостам
/sbin/iptables -A FORWARD -j DROP
```

sudo

### /etc/sudoers

```
#Allow ABills shapper
apache ALL = NOPASSWD: /usr/abills/libexec/linkupdown
apache ALL = NOPASSWD: /sbin/iptables
```

## Включение активных пользователей

Данная команда автоматически включает всех пользователей с положительным депозитом и правами получать сервис (статус услуги активно). Активируются только те пользователи у которых прописан IP адрес сервиса Internet. Также обязательно на IPN серверах доступа прописать пулы адресов для таких пользователей чтобы система знала на каких серверах доступа активировать абонентов. Данную команду стоит запускать через crontab с промежутком раз в 5 минут.

```
# /usr/abills/libexec/periodic monthly MODULES=Internet LOGON_ACTIVE_USERS
```

Параметры:

<b>NAS_IDS=1;2</b>	Идентификаторы серверов доступа. По умолчанию система переинициализирует пользователей на всех серверах доступа с типом 'ircad'
<b>TP_ID=3,6</b>	Номера тарифных планов для активации. По умолчанию все
<b>LOGIN=test,test3</b>	Логины пользователей. По умолчанию все
<b>GID=1</b>	Группы пользователей
<b>DEBUG=...</b>	Дебаг режимы 1-4 Детализация процесса 5 - Отображать команды на выполнение 6 - Отображать команды но не выполнять

## Рестарт активных IPoE сессий

### Растартовать только сессии которые поднимаются в ручном режиме

```
/usr/abills/libexec/periodic monthly MODULES=Internet SRESTART=1 NO_ADM_REPORT=1 NAS_IDS=1 LOCAL_NAS=1 FN=ipoe_periodic_session_restart
```

<b>NAS_IDS=1</b>	Список серверов доступа для рестарта
<b>LOCAL_NAS=1</b>	работать как с локальным сервером доступа. Указывается номер NAS. Опция NAS_IDS игнорируется
<b>FN=ipoe_periodic_session_restart</b>	Функция рестарта

## УТИЛИТЫ

- [Online snapshot](#)

From:  
<http://abills.asmodeus.com.ua/wiki/> - **Advanced Billing Solution**

Permanent link:  
**<http://abills.asmodeus.com.ua/wiki/doku.php/abills:docs:modules:internet:ipoe:ru>**

Last update: **2018/04/06 10:39**

