Авторизация Internet IPoE

Предоставление некоммутируемых услуг Internet.

- Контроль доступа и нарезка трафика
  - FreeBSD
  - Linux
- Удалённый NAS
  - Проверка
- Включение активных пользователей
- Рестарт активных IPoE сессий
- Ротация логов сервиса IPN
- Утилиты
  - Online Snapshot

Контроль доступа и нарезка трафика

Активация сессий происходит одним из двух способов

1. Ручное включение через кабинет администратора
2. Автоматического включение активных абонентов

Сессии включаются только активным абонентам со статусом услуги "Активно". Чтобы поднять гостевые сессии абонентам со статусом услуги "Слишком маленькие депозит" нужно включить опцию **$conf{INTERNET_IPOE_NEGATIVE}**.
При поднятии негативной сессии срабатывает правило **$conf{INTERNET_IPOE_FILTER}** в него передается значение фильтра негативного депозита.

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 -p ${NAS_MNG_PORT} -o StrictHostKeyChecking=no -
i /usr/abills/Certs/id_rsa.${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 [ "${NAS_TYPE}" = "mikrotik" ]; then CMD="/usr/abills/libexec/linkupdown mikrotik down - %LOGIN %IP
NAS_HOST=${NAS_MNG_IP_PORT} NAS_MNG_USER=${NAS_MNG_USER}";
elif [ "${NAS_MNG_IP_PORT}" != "" ]; then CMD="/usr/bin/ssh -p ${NAS_MNG_PORT} -o StrictHostKeyChecking=no -
i /usr/abills/Certs/id_rsa.${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 командіпрописанной 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

abills_shaper_enable="YES"	Поднятие правил шейпера при перезапуске системы
abills_ipn_nas_id="Номер IPN наса"	Номер сервера доступа. Обязательный параметр
abills_ipn_if="интерфейс к которому подключаются пользователи"	Интерфейс к которому подключаются клиенты
abills_ipn_allow_ip="разрешённые ип адреса"	Разрешённые без авторизации IP адреса. Разделяются запятой
abills_nat="xx.xx.xx.xx:10.0.0.0/16:interface"	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(если нет, тогда нужно создать)

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

eth0,eth2	Интерфейс в локальную сеть, к которому подключены пользователи
eth1	Интерфейс наружу
192.168.0.1	Локальный IP сервера
192.168.0.0/255.255.255.0	Локальная сеть

или альтернативный скрипт

```
!/bin/sh

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


/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


/sbin/iptables -A FORWARD -j DROP
```

sudo

/etc/sudoers

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

Удалённый NAS

Управление удалённым сервером доступа.
Задача: открывать доступ пользователям на удалённом NAS.

При выполнении правил шейпера и фильтра в переменные среды передаются дополнительные параметры:

Параметр	Описание
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

Система автоматически определяет по переменной окрежения NAS_MNG_IP_PORT при старте сесии выполнять данную команду локально или на удалённом сервере.

На сервере биллинга.

1. Создать SSH ключ для выполнения команд на удалённом сервере. Установить право чтения ключа для пользователя под которым работает Веб сервер.

```
/usr/abills/misc/certs_create.sh ssh abills_admin
```

На удалённом сервере.

1. Создать пользователя abills_admin на удалённом сервере.
2. Скопировать созданный публичный ключ **abills/Certs/id_rsa.abills_admin.pub** в **/home/abills_admin/.ssh/authorized_keys** на удалённом сервере.
3. Сделать копию биллинга на удалённом сервере.
4. Создать правила для выполнения команд с правами суперпользователя на удалённом сервере.

/etc/sudoers (для FreeBSD - /usr/local/etc/sudoers)

```
#Allow ABillS shapper
abills_admin   ALL = NOPASSWD: /usr/abills/libexec/linkupdown
abills_admin   ALL = NOPASSWD: /sbin/ipfw
```

Проверка

На сервере биллинга

- активируете абонента (галочка IPN Activate). В тарифном плане абонента обязательно должны быть правила ограничения скорости

На сервере доступа

- Проверяем создались ли правила

```
ipfw table 10 list
```

При правильной настройке видите следующие правила

```
--- table(10), set(0) ---
192.168.11.11/32 432
```

если правила не создались проверяете лог вебсервера биллинга на наличие ошибок

/var/log/httpd/abills-error.log

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:

NAS_IDS=1;2	Идентификаторы серверов доступа. По умолчанию система переинициализирует пользователей на всех серверах доступа с типом 'ipcad'
TP_ID=3,6	Номера тарифных планов для активации. По умолчанию все
LOGIN=test, test3	Логины пользователей. По умолчанию все

GID=1	Группы пользователей
DEBUG=...	Дебаг режимы 1-4 Детализация процесса 5 - Отображать команды на выполнение 6 - Отображать команды но не выполнять

$conf{INTERNET_IPOE_NAS_TYPES}='nas_type1, nas_type2';	список типов серверов доступа которые будут работать как IPoE сервера с ручным включением

Рестарт активных IPoE сессий

Рестартовать 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
```

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

Ротация логов сервиса IPN

Ротация логов происходит каждый день, система пробует их оптимизировать под экономию места. Для этого происходит групирование статистики в несколько этапов

- Раз в день групируется по часам
- Раз в месяц групируется по дням и выносится в отдельный файл

Для сохранения более одного месяца несгрупированную статику используйте опцию **$conf{IPN_LOG_KEEP_PERIOD}=1;** В данной опции указывается количество месяцев без групировки статистики

Утилиты

Online Snapshot

Утилита для сохранения журнала Online и повторно активации сессий из сохраненного журнала

Сохранение журнала онлайн

```
/usr/abills/libexec/billd online_snapshot
```

Восстановление сессий их сохраненного журнала

```
/usr/abills/libexec/billd online_snapshot start
```