Настройка сервера доступа Juniper

- Версии прошивок
- Правка RADIUS словарей
- ABillS
- Гостевой профайл
- Настройка RADIUS
- Пример RADIUS запросов
- Автотестирование PPPoE
- Дополнительно

Версии прошивок

JUNOS 17.3R3-S3.3

JUNOS 18.4R3-S2

Лицензии

- S-MX80-SA-FP
- S-MX80-SSM-FP
- S-SA-16K

Правка RADIUS словарей

Freebsd путь **/usr/local/share/freeradius/**

В словарях нужно изменить атрибуты на следующие:

dictionary.erx

```
ATTRIBUTE     ERX-Dhcp-Options                    55      octets
```

dictionary.rfc4679

```
ATTRIBUTE     ADSL-Agent-Circuit-Id               1       octets
ATTRIBUTE     ADSL-Agent-Remote-Id                2       octets
```

ABillS

```
cp Mx802.pm /usr/abills/Abills/mysql
```

Файл настройки **config.pl**

Включение модуля авторизации. Данные параметры должны быть прописаны после секций %AUTH = (); %ACCT = ();

```
$AUTH{mx80} = 'Mx802';
$ACCT{mx80} = 'Mx802';
```

Параметры

$conf{MX80_IPOE_SWITCH_PORT}=1;	Авторизация по коммутатору и порту. Данные для авторизации берутся из IP (DHCP) сервиса
$conf{MX80_MAC_AUTH}=1;	Авторизация по MAC'у.

Настройка сервера доступа меню **Настройка>Сервер доступа**

IP:	IP адрес маршрутизатора
Название:	Название
Тип:	Указать тип: mx80
Alive	Время Alive пакетов для PPPoE и время DHCP lease для IPoE (рекомедуемое значение 600 и больше)

:Управление:

IP:PORT:	Адрес и порт для отправки RADIUS CoA команд. (По умолчанию 3799) xxx.xxx.xxx.xxx:3799
Пароль:	Пароль для отправки RADIUS и CoA пакетов

Дополнительные Радиус параметры для IPoE авторизации

```
Framed-Route=0.0.0.0 0.0.0.0 31.135.96.1,
MS-Primary-DNS-Server=10.0.0.1,
MS-Secondary-DNS-Server=8.8.8.8,
```

Гостевой профайл

Гостевой профайл разрешает перенаправлять не авторизированных пользователей на страничку уведомления о состоянии счёта и причине отказа авторизации

config.pl

$conf {MX80_GUEST_POOLS_PARAMS} ='POOL_ID:EXT_PARAMS';	Объявление гостевого пула адресов. Данный пул выдаётся не авторизированным абонентам которые не зарегистрированы в системе. **Параметры:** **POOL_ID** - Номер пула адресов в системе ABillS (заводится **Настройка>Сервер доступа>IP Pools**) **EXT_PARAMS** - Дополнительные радиус параметры для данного пула. Система предоставляет возможность заводить на каждый Vlan свой гостевой пул. Правила пулов разделяются точкой с запятой (;). Пример: $conf{MX80_GUEST_POOLS_PARAMS}='3:ERX-Primary-Dns = 192.168.1.1,Framed-IP-Netmask=255.255.224.0;';
$conf {MX80_DEFAULT_GUEST_PROFILE} ='NOAUTH';	Гостевой профайл по умолчанию. Если не указан явно будет использоваться NOAUTH
$conf{MX80_O82_EXPR}='Название опции:регулярное выражение: переменные;...';	Определение параметров опции 82
$conf{MX80_PROFILE_PREFIX}='svc';	Префикс профайла соединения по умолчанию 'svc'

$conf{MX80_PROFILES} ='WRONG_PASS:profile_wrong_pass;';	Определение разных профайлов для разных ошибок авторизации **Параметры:** **WRONG_PASS** - Неправильный правильный пароль для туннельных соединений (PPPoE) **NEG_DEPOSIT** - Отрицательный баланс на счету **AUTH_ERROR** - Другая ошибка авторизации **NOT_REGISTER** - Учётная запись с такими параметрами не зарегистрирована **NOT_ALLOW_SERVICE** - Использование услугу запрещено **DISABLE** - Пользователь отключен Пример $conf{MX80_PROFILES}='WRONG_PASS:profile_wrong_pass; NEG_DEPOSIT:profile_neg_deposit; AUTH_ERROR:profile_other_error; NOT_REGISTER:profile_not_register; NOT_ALLOW_SERVICE:profile_not_allow_service; DISABLE:profile_disable';
$conf{MX80_NAT_PROFILE}=1;	Включение NAT профайла (**svc-cgn-nat-pppoe** / **svc-cgn-nat-ipoe**) для серых адресов. система автоматически проверяет адрес и елси он попадает в приватные сети включает NAT Приватные сети: 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16 100.64.0.0/10

Пример config.pl Возможность использовать разные профайлы для разных ошибок подключения

```
#MX80-PPPoE
$conf{MX80_PROFILES}='
WRONG_PASS:svc-guest-pppoe(svc-filter-in-wrongpassword);
NEG_DEPOSIT:svc-guest-pppoe(svc-filter-in-nomoney);
AUTH_ERROR:svc-guest-pppoe(svc-filter-in-unknownerror);
USER_NOT_EXIST:svc-guest-pppoe(svc-filter-in-notregister);
NOT_ALLOW_SERVICE:svc-guest-pppoe(svc-filter-in-notallowservice);
DISABLE:svc-guest-pppoe(svc-filter-in-disable);
WRONG_PORT:svc-guest-pppoe(svc-filter-in-wrongport);
WRONG_CID:svc-guest-pppoe(svc-filter-in-wrongcid);
';
```

Пример настройки MX80

```
dynamic-profiles svc-guest-pppoe
interfaces {
    pp0 {
        unit "$junos-interface-unit" {
            family inet {
                filter {
                    input guest-filter-in;
                }
            }
        }
    }
}
```

Выражения для определения параметров Option 82

$conf{MX80_O82_EXPR}='Название опции:регулярное выражение:переменные;…';

Пример:
для коммутаторов Foxgate

```
Agent-Remote-Id = 0x70726f626e696b2e6c6f63616c
ADSL-Agent-Circuit-Id = "Vlan202+Ethernet1/5"
```

config.pl

```
$conf{MX80_O82_EXPR}='ADSL-Agent-Circuit-Id:Vlan(\d+)\+Ethernet\d\/(\d+):VLAN,PORT;ADSL-Agent-Remote-Id:0x
([a-f0-9]{12}):MAC';
```

Пример:
Edge-core ES-3528(M)
Edge-core ES-3510M

```
$conf{MX80_O82_EXPR}='ADSL-Agent-Circuit-Id:[a-f0-9]{10}([a-f0-9]{2}):PORT;ADSL-Agent-Remote-Id:0x0006([a-f0-
9]{12}):MAC';
```

Alcatel LS6224
EdgeCore 3528M

```
$conf{MX80_O82_EXPR}='ADSL-Agent-Circuit-Id:\d{4}(\d{4})\d{2}(\d{2}):VLAN,PORT;ADSL-Agent-Remote-Id:0x0006
([a-f0-9]{12}):MAC';
```

Выражения

Настройка RADIUS

Работа паралельно 2 радиусов

```
radius-server {
192.168.1.1 {
secret "$9$Nl-YoasdarevL"; ## SECRET-DATA
timeout 6;
retry 3;
max-outstanding-requests 200;
source-address 192.168.1.61;
}
192.168.6.1 {
secret "$9$Aessdst1heK8x-wO1asdasmfTz6"; ## SECRET-DATA
timeout 6;
retry 3;
max-outstanding-requests 200;
source-address 192.168.6.4;
}
```

Пример RADIUS запросов

Пример авторизации IPoE с использование Option 82

```
  User-Name = "000e.0cc1.6c8a"
  User-Password = "sub321"
  Service-Type = Framed-User
  Chargeable-User-Identity = ""
  Acct-Session-Id = "129"
  ERX-Dhcp-Options = 0x3501013d0701000e0cc16c8a0c0563616374693707011c02030f0
60c52120106000400150105020800067072cf36b340
  ERX-Dhcp-Mac-Addr = "000e.0cc1.6c8a"
  NAS-Identifier = "gw-subsriber"
  NAS-Port = 4190229
  NAS-Port-Id = "ae0.1073741824:21"
  NAS-Port-Type = Ethernet
  ADSL-Agent-Circuit-Id = 0x000400150105
  ADSL-Agent-Remote-Id = 0x00067072cf36b340
```

Ответ авторизации для рабочих сессий

```
  Acct-Interim-Interval = 90
  NAS-Identifier = "gw-subsriber"
  ERX-Dhcp-Options = "0x0304c0a80001"
  ERX-Service-Activate:2 = "svc-local_1-ipoe(3072000,2048000)"
  Service-Type = Framed-User
  Framed-IP-Address = 192.168.47.232
  Framed-IP-Netmask = 255.255.0.0
  ERX-Service-Activate:3 = "svc-global-ipoe(524288,1048576)"
```

Пример ответа авторизации при гостевой сессии

```
 Reply-Message = "NEG_DEPOSIT '-5'"
 Session-Timeout = 90
 Service-Type = Framed-User
 ERX-Service-Activate:1 = "svc-guest-ipoe(svc-filter-in-nomoney)"
 ERX-Dhcp-Options = "0x03041f876001"
 ERX-Primary-Dns = 10.10.0.1
 Framed-IP-Address = 192.168.11.236
 Framed-IP-Netmask = 255.255.0.0
```

Название профайла

```
ERX-Service-Activate:[3-{traffic_class_id}] = svc-{traffic_class_name}-{profile_sufix}
```

{traffic_class_id}	Номер класса трафика 3 - Глобальный 2 - Локальный 3 - Внутренний Для гостевых сервисов используется номер 1
{traffic_class_name}	Название класса трафика
{profile_sufix}	**pppoe** **ipoe** Если присутствует RADIUS пара Framed-Protocol система подставляет **pppoe** в противном случае **ipoe**

Автотестирование PPPoE

Juniper PPPoE auto test

```
user> test aaa ppp user test password 123456
    Authentication Grant
    ************User Attributes***********
             User Name -                          test
             Virtual Router Name (LS:RI) -        default:default
             Service Type -                       Framed
             Agent Remote Id -                    <not set>
             Client IP Address -                  10.20.0.2
             Client IP Netmask -                  255.255.255.255
```

Дополнительно

Описание кодов завершения сессий Juniper