Carbon Billing 5

Смотреть рекомендуется в максимально доступном разрешении. (~1080px) - откройте видео на полный экран, play, шестерёнка -> 1080hd.

Настройки сети следующие:

Хост система

гипервизор libvirt + kvm:

Имеются два bridge:

br0 - мост, через который виртуалки ходят в интернет.

br1 - мост без доступа в сеть, "псевдолокалка".

Carbon XGE Router 5

Имеет два интерфейса:

eth0 в br0, ip адрес - 10.90.140.70/16, он же - канал к вышестоящему провайдеру.

eth1 в br1, ip адрес - 192.168.70.1/24, он же - интерфейс для подключения абонентов.

Carbon Billing 5

eth0 в br0, ip адрес - 10.90.140.71/16, он же - локальный интерфейс биллинга, через него он общается и с Carbon XGE Router 5.

Пользователь

eth0 в br0, ip адрес только для подключения к нему по ssh - 10.70.140.222/16, без доступа в сеть.

eth1 в br1, ip адрес 192.168.70.3/24, шлюз - 192.168.70.1, то есть Carbon XGE Router 5.

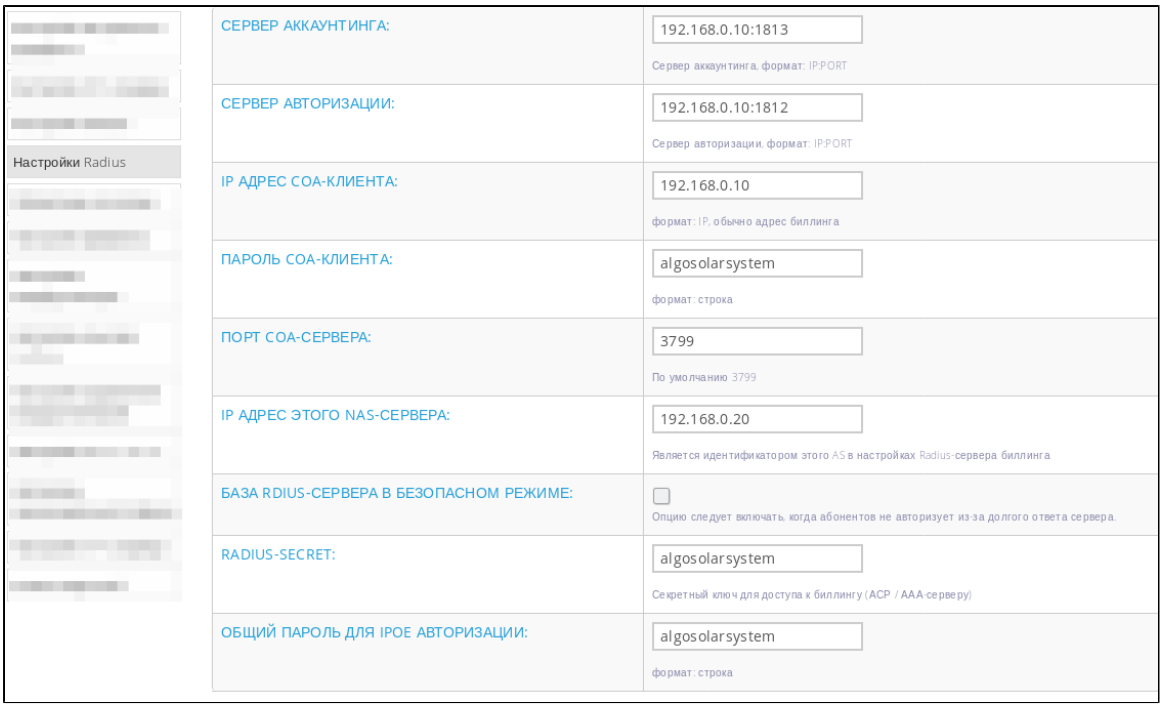
В качестве DNS - публичные DNS гугла (8.8.8.8 / 8.8.4.4).

Настройка связки

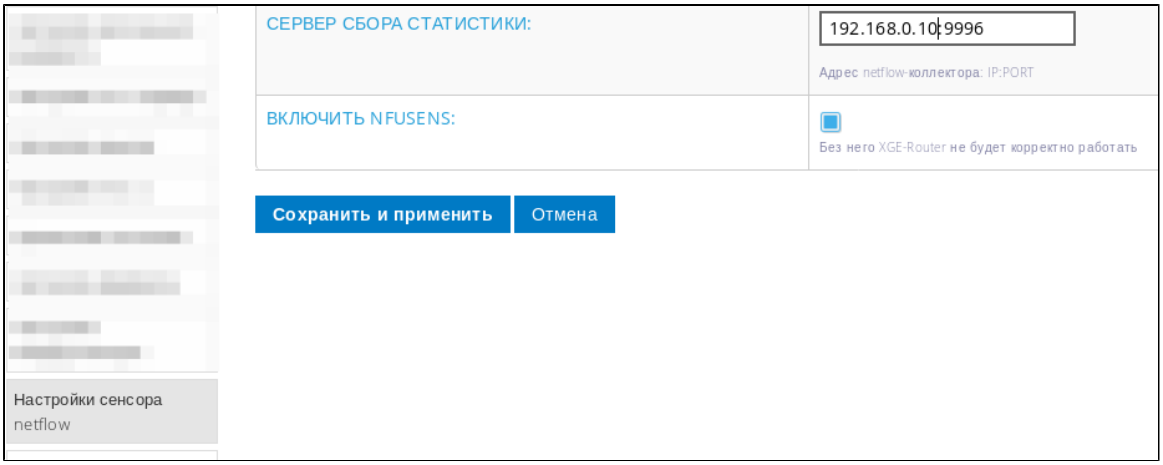
XGE

В XGE Router нужно указать IP адрес биллинга в качестве:

- Radius сервера авторизации.
- Radius сервера аккаунтинга.
- CoA клиента.



- Коллектора для нетфлоу статистики.



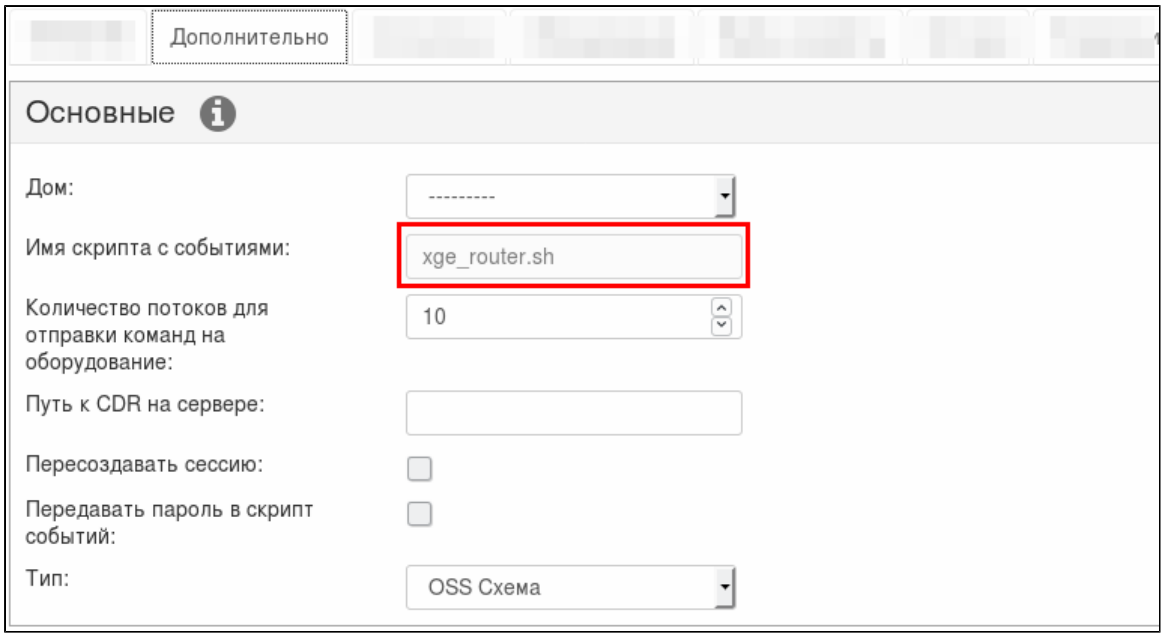
После чего применить и сохранить изменения.

Биллинг

В веб-интерфейсе биллинга

Добавляем XGE Router во вкладке оборудование > маршрутизаторы.

1. создаём маршрутизатор, называем как-нибудь (не переусердствуйте со спецсимволами)
2. прописываем его IP
3. выбираем тип Carbon XGE Router 5.
4. указываем скрипта для отправки команд xge_router.sh (в следующих версиях будет автоматически прописываться при выборе нужного типа).

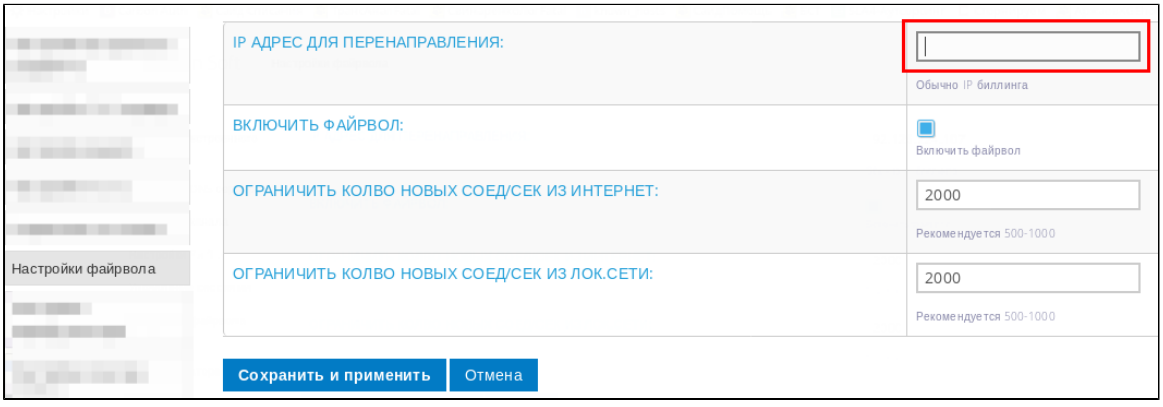


5. включаем radius auth проверку для VPN по login, для ip+web дополнительно ставим ip.
6. указываем пароли radius secret / user_psw / coa_pass аналогичные указанным в настройках XGE Router (смс настройки radius), я использовал пароль по умолчанию, в идеале стоит сменить.
7. сохраняем.

Для того, чтобы на xge работала штатная синхронизация с биллингом, на биллинге необходимо добавить следующие правила (в примере 192.168.20.1 - адрес XGE, адрес 169.254.30.50 менять не нужно):

```
iptables -t nat -A asr_billing_prerouting -p tcp -s 192.168.20.1/32 --dport 3050 -j DNAT
--to-destination 169.254.30.50:3050
iptables -A nas_clients -s 192.168.20.1/32 -p tcp -m tcp --dport 3050 -j ACCEPT
```

Так же эти правила необходимо добавить в hooks
Помимо этого необходимо на XGE в web интерфейсе - Настройки файрвола" и в пункте "IP адрес для перенаправления" указать ip адрес биллинга, который доступен с xge.



Теперь абонент:

1. Создаём абонента,
2. указываем ему какой-нибудь IP (в принципе можно было создать пул для динамической выдачи IP адреса).
3. включаем галочку "разрешить переподключение".
4. я на всякий случай поменял ему логин и пароль с автоматически сгенерированных на username/username.
5. закидываем ему немного денег.
6. ставим авторизацию по radius.
7. пробуем подключиться.

Пользователь

На Linux я воспользовался следующей командой:

```
sudo pppd nobsdcomp nodeflate defaultroute nomppe pty 'pptp 192.168.70.1 --nolaunchpppd' user
username password username
```

через пару секунд смотрим вывод ip addr и ip route.

```
[root@centosuser ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 52:54:00:7f:0b:31 brd ff:ff:ff:ff:ff:ff
    inet 10.70.140.222/16 brd 10.70.255.255 scope global eth0
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 52:54:00:13:0d:fa brd ff:ff:ff:ff:ff:ff
    inet 192.168.70.3/16 brd 192.168.255.255 scope global eth1
18: ppp0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1400 qdisc pfifo_fast state UNKNOWN qlen 3
    link/ppp
    inet 10.128.0.5 peer 10.128.0.1/32 scope global ppp0
[root@centosuser ~]# ip r
192.168.70.1 dev eth1  scope link  src 192.168.70.3
10.128.0.1 dev ppp0  proto kernel  scope link  src 10.128.0.5
10.70.0.0/16 dev eth0  proto kernel  scope link  src 10.70.140.222
169.254.0.0/16 dev eth0  scope link  metric 1002
169.254.0.0/16 dev eth1  scope link  metric 1003
192.168.0.0/16 dev eth1  proto kernel  scope link  src 192.168.70.3
default dev ppp0  scope link
```

вуаля, авторизация прошла успешно.

на всякий случай проверяем:

доступ в сеть:

```
[root@centosuser ~]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=48 time=51.8 ms
```

работающий dns

```
[root@centosuser ~]# ping ya.ru
PING ya.ru (93.158.134.3) 56(84) bytes of data.
64 bytes from www.yandex.ru (93.158.134.3): icmp_seq=1 ttl=55 time=27.8 ms
^C
--- ya.ru ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 365ms
rtt min/avg/max/mdev = 27.886/27.886/27.886/0.000 ms
```

что разрешён не только icmp:

```
wget ya.ru
```

радуемся что всё замечательнейшим образом работает!

Примечания

Q: Почему не надо настраивать radius атрибуты?

A: Потому что и Carbon Billing 5 и Carbon XGE Router 5 - наши продукты, делать с ними в целях удобства мы можем что угодно (хо-хо), поэтому Radius атрибуты зашиты в тип маршрутизатора Carbon XGE Router.
По умолчанию отправляются команды:

```
ip forward_allow add Framed-IP-Address
ip snat add Framed-IP-Address $snat_ip
ip redirect $overlimit Framed-IP-Address
policy set Framed-IP-Address in $rate_in $ceil_in out $rate_out $ceil_out
```