Open VPN

Debian 9

Установка пакетов

```
apt-get install openvpn openvpn-auth-radius
```

Создание сертификата сервера, ключа и файлов шифрования

Создаём директорию под ключи:

```
mkdir /etc/openvpn/easy-rsa
```

В нее копируем утилиты и конфиги для работы с ключами:

```
cp -r /usr/share/easy-rsa/* /etc/openvpn/easy-rsa/
```

В файле **vars** настраиваем параметры ключа:

/etc/openvpn/easy-rsa/vars

```
export KEY_COUNTRY="UA"
export KEY_PROVINCE="Kievskaya"
export KEY_CITY="Kiev"
export KEY_ORG="Firma"
export KEY_EMAIL="me@domain.ua"
export KEY_OU="MyOrganizationalUnit"
```

Далее необходимо создать openssl.cnf

```
cd /etc/openvpn/easy-rsa/
cp openssl-1.0.0.cnf openssl.cnf
```

Инициируем переменные:

```
source ./vars
```

Генерируем ключи:

```
./build-ca
./build-key-server server
./build-key user
./build-dh
openvpn --genkey --secret keys/ta.key
```

Копируем серверные ключи в директорию /etc/openvpn:

```
cd keys
cp server.crt server.key ca.crt dh2048.pem ta.key /etc/openvpn/
```

Создаем недостающие папки:

```
mkdir /etc/openvpn/ccd
mkdir /var/log/openvpn
```

Конфигурация OpenVPN сервера

Создаем файл конфигурации OpenVPN сервера **server.conf**:

/etc/openvpn/server.conf

```
mode server
daemon vpn-server
port 1194
proto udp4
dev tun
ca /etc/openvpn/ca.crt
cert /etc/openvpn/server.crt
key /etc/openvpn/server.key
dh /etc/openvpn/dh2048.pem  #  dh1024.pem,
plugin /usr/lib/openvpn/radiusplugin.so /etc/openvpn/radius/radius.cnf
client-connect /etc/ppp/ip-up
script-security 3
client-disconnect /etc/ppp/ip-down
# ifconfig-pool-persist ipp.txt persist-key
tls-server
tls-auth /etc/openvpn/ta.key 0
cipher AES-256-CBC
server 192.168.50.0 255.255.255.0
push "redirect-gateway"
ifconfig-pool-persist ipp.txt
keepalive 10 120
#comp-lzo
user nobody
group nogroup
persist-key
persist-tun
status /var/log/openvpn/openvpn-status.log
log-append /var/log/openvpn/openvpn.log
verb 4
mute 20
client-to-client
client-config-dir /etc/openvpn/ccd
route 192.168.50.0 255.255.255.0
topology subnet
status-version 1
```

Создаем файл конфигурации RADIUS клиента:

/etc/openvpn/radius/radius.cnf

```
NAS-Identifier=OpenVPN

# The service type which is sent to the RADIUS server
Service-Type=5

# The framed protocol which is sent to the RADIUS server
Framed-Protocol=1

# The NAS port type which is sent to the RADIUS server
NAS-Port-Type=5

# The NAS IP address which is sent to the RADIUS server
NAS-IP-Address=127.0.0.1

# Path to the OpenVPN configfile. The plugin searches there for
# client-config-dir PATH   (searches for the path)
# status FILE                      (searches for the file, version must be 1)
# client-cert-not-required (if the option is used or not)
# username-as-common-name  (if the option is used or not)

# Path to our OpenVPN configuration file. Each OpenVPN configuration file needs its own radiusplugin
configuration file as well
OpenVPNConfig=/etc/openvpn/server.conf


# Support for topology option in OpenVPN 2.1
# If you don't specify anything, option "net30" (default in OpenVPN) is used.
# You can only use one of the options at the same time.
# If you use topology option "subnet", fill in the right netmask, e.g. from OpenVPN option "--server NETWORK
NETMASK"
subnet=255.255.255.0
# If you use topology option "p2p", fill in the right network, e.g. from OpenVPN option "--server NETWORK
NETMASK"
# p2p=10.8.0.1


# Allows the plugin to overwrite the client config in client config file directory,
# default is true
overwriteccfiles=true

# Allows the plugin to use auth control files if OpenVPN (>= 2.1 rc8) provides them.
# default is false
# useauthcontrolfile=false

# Only the accouting functionality is used, if no user name to forwarded to the plugin, the common name of
certificate is used
# as user name for radius accounting.
# default is false
# accountingonly=false


# If the accounting is non essential, nonfatalaccounting can be set to true.
# If set to true all errors during the accounting procedure are ignored, which can be
# - radius accounting can fail
# - FramedRouted (if configured) maybe not configured correctly
# - errors during vendor specific attributes script execution are ignored
# But if set to true the performance is increased because OpenVPN does not block during the accounting
procedure.
# default is false
nonfatalaccounting=false

# Path to a script for vendor specific attributes.
# Leave it out if you don't use an own script.
# vsascript=/root/workspace/radiusplugin_v2.0.5_beta/vsascript.pl
```

```
# Path to the pipe for communication with the vsascript.
# Leave it out if you don't use an own script.
# vsanamedpipe=/tmp/vsapipe

# A radius server definition, there could be more than one.
# The priority of the server depends on the order in this file. The first one has the highest priority.
server
{
        # The UDP port for radius accounting.
        acctport=1813
        # The UDP port for radius authentication.
        authport=1812
        # The name or ip address of the radius server.
        name=127.0.0.1
        # How many times should the plugin send the if there is no response?
        retry=1
        # How long should the plugin wait for a response?
        wait=1
        # The shared secret.
        sharedsecret=secretpass
}
```

Ограничение скорости клиентов

Скрипт, который выполняется при подключении клиента:

/etc/ppp/ip-up

```
#!/bin/sh

echo "pppd up $dev $username $ifconfig_pool_remote_ip LINUX_NEW_MODEL=1" >> /tmp/shaper
/usr/bin/sudo /usr/abills//libexec/linkupdown pppd up $dev $username $ifconfig_pool_remote_ip
LINUX_NEW_MODEL=1  >> /tmp/shaper

env >> /tmp/shaper
id >> /tmp/shaper
echo "--------------------" >> /tmp/shaper
```

Скрипт, который выполняется при отключении клиента:

/etc/ppp/ip-down

```
#!/bin/sh

echo "pppd down $dev $username $ifconfig_pool_remote_ip" >> /tmp/shaper
/usr/bin/sudo /usr/abills//libexec/linkupdown pppd down $dev $username $ifconfig_pool_remote_ip
LINUX_NEW_MODEL=1
echo "--------------------" >> /tmp/shaper
```

Добавить в **/etc/sudoers** следующие строки:

```
nobody   ALL = NOPASSWD: /usr/abills//libexec/linkupdown
nobody   ALL = NOPASSWD: /sbin/iptables
nobody   ALL = NOPASSWD: /sbin/tc
```

Добавляем сервер доступа в AbillS

Настройка>Сервер доступа>Сервер доступа

IP	IP Адрес сервера
Type	openvpn
Alive (sec.)	Время обновления статистики и подтверждения активности сессии. Рекомендуемое значение 120
Radius NAS-Identifier	используется только в случае нескольких радиус клиентов на одном IP
Пароль (PoD,RADIUS Secret,SNMP)	Параметр "sharedsecret" из файла /etc/openvpn/radius/radius.cnf