OpenVPN

Особая благодарность Ck-NoSFeRaTU

Установка

Пример настройки в среде FreeBSD.

1. Ставим openvpn из портов:

```
# cd /usr/ports/security/openvpn
# make clean install
```

2. Radiusplugin for OpenVPN
Забираем последнюю версию радиус-плагина для openvpn с cvs и собираем его(последний выложенный релиз на сайте глючит)

```
# cd /tmp
# cvs -z3 -d:pserver:anonymous@cvs.savannah.nongnu.org:/sources/radiusplugin co radiusplugin
# cd radiusplugin
# g++ -Wall -I/usr/local/include -L/usr/local/lib -shared -o radiusplugin.so \
AccountingProcess.cpp Exception.cpp PluginContext.cpp UserAuth.cpp AcctScheduler.cpp \
IpcSocket.cpp radiusplugin.cpp User.cpp AuthenticationProcess.cpp main.cpp UserAcct.cpp \
UserPlugin.cpp Config.cpp RadiusClass/RadiusAttribute.cpp RadiusClass/RadiusPacket.cpp \
RadiusClass/RadiusConfig.cpp RadiusClass/RadiusServer.cpp \
RadiusClass/RadiusVendorSpecificAttribute.cpp -lgcrypt -lgpg-error -lstdc++ -lm
```

3. Создаем папку с конфигами, копируем туда радиус-плагин, его конфиг

```
# mkdir /usr/local/etc/openvpn
# cp radiusplugin.so /usr/local/etc/openvpn/
# cp radiusplugin.cnf /usr/local/etc/openvpn/
```

Создаем сертификаты (Читаем команды для openssl тут)

4. Файл **/usr/local/etc/openvpn/server.conf**

```
dev tap8
port 1194
mode server
tls-server
server 10.1.100.0 255.255.255.0 10.1.100.1
management 127.0.0.1 7505
ca /usr/local/etc/openvpn/keys/server/ca.crt
cert /usr/local/etc/openvpn/keys/server/server.crt
key /usr/local/etc/openvpn/keys/server/server.key
dh /usr/local/etc/openvpn/keys/server/dh1024.pem
tls-auth /usr/local/etc/openvpn/keys/server/ta.key
keepalive 10 60
client-connect /usr/local/abills/libexec/openvpn-up
client-disconnect /usr/local/abills/libexec/openvpn-down
ifconfig-pool-persist /usr/local/etc/openvpn/keys/server/ip.txt 1300000
plugin /usr/local/etc/openvpn/radiusplugin.so /usr/local/etc/openvpn/radiusplugin.cnf
username-as-common-name
comp-lzo
push "redirect-gateway def1"
push "route 0.0.0.0 0.0.0.0"
push "dhcp-option DNS 10.1.100.1"
```

```
log-append /var/log/openvpn-server.log
```

5. Файл **/usr/local/etc/openvpn/radiusplugin.cnf**

```
NAS-Identifier=openvpn
Service-Type=2
Framed-Protocol=1
NAS-Port-Type=5
NAS-IP-Address=127.0.0.1
OpenVPNConfig=/usr/local/etc/openvpn/server.conf
#subnet=255.255.255.0
server
{
acctport=1813
authport=1812
name=127.0.0.1
retry=1
wait=1
sharedsecret=наш_секретный_пароль_от_радиуса
}
```

6. Файл **/usr/local/abills/libexec/openvpn-up**

```
#!/bin/bash

/usr/local/abills/libexec/linkupdown openvpn up $dev inet $ifconfig_local  $ifconfig_pool_remote_ip
$common_name >& /dev/null

**/usr/local/abills/libexec/openvpn-down**\\

#!/bin/bash

/usr/local/abills/libexec/linkupdown openvpn down $dev inet $ifconfig_local $ifconfig_pool_remote_ip
$common_name >& /dev/null
```

7. Заводим ещё один nas с NAS-Identifier=тому, что мы указывали в radiusplugin.cnf, тип Other nas server. В radius-параметры не забываем Acct-Interim-Interval=300.

8. /usr/local/sbin/openvpn –daemon –config /usr/local/etc/openvpn/server.conf

Теперь про клиентов (Мастдай):

9. Openvpn/config/example.ovpn

```
nobind
remote ип_нашего_сервера
port 1194
client
dev tap
proto udp
auth-user-pass authinfo
tls-auth ta.key
pull
tls-client
reneg-sec 1209600
ca tmp-ca.crt
cert client.crt
key client.key
comp-lzo
```

В Openvpn/config/authinfo две строчки:

логин
пароль

Примечания

Примечание по клиентскому openvpn:
С какой-то версии openvpn`а заблокирована возможность хранения в текстовом файле логина и пароля пользователя, я не хотел напрягать пользователей каждый раз вводить его вручную, поэтому собрал собственный инсталятор openvpn для клиентов. В него входят уже разблокированные бинарники openvpn, драйвера, openvpn-gui, набор нужных сертификатов и конфигов, а также форма, где просит указать логин и пароль, т.е. клиенту нужно только вписать свой логин/пароль прямо в формочку в инсталяторе, а остальное всё настроит он уже сам. Если кому нужно, то поделюсь скриптами для nsis`а.

Примечание по radiusplugin:
Обработку Framed-IP-Address завести не удалось. Автор пишет следующее:

- OpenBSD(BSD):

1. RADIUS attributes FramedIP and FramedRoutes mandatory
2. RADIUS attribute FramedIP is ignored

Надо бы связаться с автором и спросить будет ли чинить FramedIP в бсд или нет...

Поэтому пока как костыль, если нужно использование статики, юзаем ifconfig-pool-persist в конфиге openvpn, к примеру ifconfig-pool-persist /usr/local/etc/openvpn/keys/server/ip.txt 1300000.
И в этот ip.txt прописываем вручную/скриптами статические ипшники, в таком формате: логин,ип
логин2,ип2