ИНСТРУКЦИЯ ПО НАСТРОЙКЕ ПОДКЛЮЧЕНИЯ К VPN-ШЛЮЗУ TELPHIN
С ИСПОЛЬЗОВАНИЕМ LINUX REDHAT-СОВМЕСТИМЫХ ДИСТРИБУТИВОВ

Подключение с использованием Linux-сервера предназначено:

- для защищенного соединения с Telphin программной телефонной станции Asterisk, установленной на сервере с ОС Linux RedHat/CentOS
- для использования Linux-сервера в качестве VPN-маршрутизатора и выполнения защищенных звонков с SIP-телефонов/SIP-шлюзов

Внимание! Для подключения со стороны клиента потребуется статический внешний IP-адрес.
Получите от Telphin настройки вашего подключения – внутренняя подсеть и ключ шифрования.

1. ***Отредактируйте файл /etc/sysctl.conf***

```
# Controls IP packet forwarding
net.ipv4.ip_forward = 1
```

2. ***Назначьте локальному сетевому интерфейсу адрес из полученной подсети***

```
# system-config-network
Edit Devices
ethX
Use DHCP = [ ]      Static IP = 10.128.X.1    Netmask = 255.255.255.0        Default gateway IP = <пусто>
# reboot
```

3. ***Создайте файл /etc/sysconfig/network-scripts/ifcfg-ipsec0, где X – полученный номер подсети***

```
TYPE=IPSEC
ONBOOT=yes
IKE_METHOD=PSK
SRCGW=10.128.X.1
DSTGW=10.128.0.1
SRCNET=10.128.X.0/24
DSTNET=10.128.0.0/24
DST=213.170.81.142
AH_PROTO=none
```

4. ***Создайте файл /etc/sysconfig/network-scripts/keys-ipsec0, где clientkey – полученный ключ шифрования***

```
IKE_PSK=clientkey
```

5. ***Отредактируйте файл /etc/racoon/racoon.conf, где X – полученный номер подсети, Y.Y.Y.Y – ваш внешний IP-адрес***

```
# Racoon IKE daemon configuration file.
# See 'man racoon.conf' for a description of the format and entries.

path include "/etc/racoon";
path pre_shared_key "/etc/racoon/psk.txt";
path certificate "/etc/racoon/certs";
listen
{
        isakmp Y.Y.Y.Y [500];
        isakmp_natt Y.Y.Y.Y [4500];
}
sainfo address 10.128.X.0/24 any address 10.128.0.0/24 any
{
        pfs_group 2;
        lifetime time 28800 sec;
        encryption_algorithm 3des ;
        authentication_algorithm hmac_sha1 ;
        compression_algorithm deflate ;
```

}

Выполните в консоли
chmod 600 /etc/sysconfig/network-scripts/keys-ipsec0
ifup ipsec0
ifdown ipsec0

6. ***Файл /etc/racoon/213.170.81.142.conf должен создаться автоматически, добавьте в него строки***

```
remote 213.170.81.142
{
    nat_traversal force;
    lifetime time 86400 sec;
    exchange_mode aggressive, main;
    my_identifier address;
    proposal {
        encryption_algorithm 3des;
        hash_algorithm sha1;
        authentication_method pre_shared_key;
        dh_group 2;
    }
}
```

7. ***Выполните в консоли***

```
# ifup ipsec0
# ping 10.128.0.1
PING 10.128.0.1 (10.128.0.1) 56(84) bytes of data.
64 bytes from 10.128.0.1: icmp_seq=1 ttl=255 time=1.21 ms
64 bytes from 10.128.0.1: icmp_seq=2 ttl=255 time=1.08 ms
<если ping есть - значит VPN-подключение установлено>
# reboot
<проверка автозапуска VPN при перезагрузке сервера>
# ping 10.128.0.1
PING 10.128.0.1 (10.128.0.1) 56(84) bytes of data.
64 bytes from 10.128.0.1: icmp_seq=1 ttl=255 time=1.21 ms
64 bytes from 10.128.0.1: icmp_seq=2 ttl=255 time=1.08 ms
```

8. ***Измените настройки SIP вашего устройства телефонии:***

SIP-сервер = 10.128.0.2 Порт = 5060
Outbound proxy-сервер = 10.128.0.2 Порт = 5060

9. ***Выполните телефонный звонок***

Дополнительно:

1. При загрузке системы происходит автозапуск демона racoon.

2. Туннель и VPN-сессия устанавливается автоматически при сетевой активности на подсеть 10.128.0.0/24.

3. Трафик VPN передается по портам 500/udp и 4500/udp – должен быть разрешен в межсетевом экране.

4. Режим VPN – туннельный, PSK, шифрование 3DES, хеширование SHA1, инкапсуляция UDP

5. Подробную информацию по установленному VPN-подключению вы можете увидеть, выполнив команды:

```
# racoonctl show-sa isakmp
# racoonctl show-sa esp
# tail –n 50 /var/log/messages | grep racoon
```