Настройка L2TP-IPsec подключения на роутере Крокс

Общее

Настройка будет состоять из двух частей:

1. Установка и настройка Strongswan. Это пакет, в котором работают протоколы, отвечающие за обмен ключами, аутентификацию и шифрование.
2. Создание и настройка интерфейса L2TP, устанавливающего соединение и управляющего сессией.

Основной момент - плохая совместимость с балансировщиком трафика mwan3, а также системой резервирования канала по совместительству. Поэтому, если вы его не используете или он вам не нужен, то этот вариант настройки вам подойдет.

Также необходимо использовать прошивку KROKS на основе 19.07.3 и выше. Прошивки от начала 2021 года и выше имеют версию 19.07.4 и старше.

В инструкции присутствуют следующие обозначения, которые необходимо заменить на свои значения:

- VPN SERVER - IP адрес L2TP/IPSEC сервера
- USER - имя пользователя для подключения
- PASS - пароль пользователя для подключения
- IPSEC KEY - общий ключ IPSEC для подключения
- GATEWAY IP - IP адрес L2TP/IPSEC сервера во внутренней сети

Подключение к устройству

Для того, чтобы выполнить настройку - нужно подключиться к устройству по ssh. Для Linux/MacOS есть встроенный клиент, а для Windows рекомендуем использовать PUTTY.

Для установки пакетов и дальнейшей настройки необходимо, чтобы роутер имел активное подключение и выход в интернет.

Удаляем mwan3

```
opkg remove mwan3 --force-removal-of-dependent-packages
sed -i '/metric/d' /etc/config/network
```

Устанавливаем IPSEC клиент strongswan

```
opkg update && opkg install strongswan-isakmp
```

Создаем файлы для strongswan

Конфигурационный файл

```
cat > /etc/ipsec.conf <<EOF
conn ipsec
    auto=start
    dpdaction=restart
    closeaction=restart
    type=transport
    authby=secret
    left=%defaultroute
    leftprotoport=udp/l2tp
    rightprotoport=udp/l2tp
    right=<VPN SERVER>
    rightid=%any
    keyingtries=%forever
    ike=aes128-sha1-modp1024
    esp=aes128-sha1
    forceencaps=yes
    keyexchange=ikev1
EOF
```

Файл с общим ключом IPSEC

```
cat > /etc/ipsec.secrets <<EOF
# /etc/ipsec.secrets - strongSwan IPsec secrets file
: PSK "<IPSEC KEY>"
EOF
```

Настройка L2TP подключения

Это можно сделать как с помощью команд (как в примере ниже), так и с помощью средств веб-интерфейса.

```
uci -q batch <<-EOF
set network.office="interface"
set network.office.proto="l2tp"
set network.office.ipv6="0"
```

```
set network.office.defaultroute="0"
set network.office.delegate="0"
set network.office.force_link="1"
set network.office.mtu="1400"
set network.office.checkup_interval="10"
set network.office.keepalive="20 5"
set network.office.server="<VPN SERVER>"
set network.office.username="<USER>"
set network.office.password="<PASS>"
EOF
uci commit network
```

Добавляем новое подключение в зону WAN firewall’a

```
uci set firewall.@zone[1].network="$(uci get firewall.@zone[1].network) office"
uci commit firewall
```

Настраиваем маршруты для доступа к внутренней сети (при необходимости)

```
uci -q batch <<-EOF
add network route
set network.@route[-1].target='10.0.0.0'
set network.@route[-1].gateway='<GATEWAY IP>'
set network.@route[-1].netmask='255.255.255.0'
set network.@route[-1].interface='office'
EOF
uci commit network
```

Перезагружаем устройство через веб-интерфейс или с помощью команды

```
sync && reboot
```

Дополнительно стоит отметить, что возможно вам придется указать алгоритмы шифрования для фаз подключения IPSEC в описании конфигурационного файла strongswan. Править необходимо следующие значения:

```
ike=aes128-sha1-modp1024
esp=aes128-sha1
```