Mikrotik: Настраиваем тоннель GRE между Mikrotik и Ubuntu

Почему именно GRE: легко, просто, удобно. А в сочетании с IPSEC довольно безопасно.

Исходные данные:

- XXX.XXX.XXX.XXX - белый IP Mikrotik
- YYY.YYY.YYY.YYY - белый IP сервера с Ubuntu
- 172.16.1.1 - внутренний адрес тоннеля на сервере с Ubuntu
- 172.16.1.2 - внутренний адрес тоннеля на Mikrotik

Настраиваем тоннель GRE

Настраиваем Mikrotik

Создаем новый тоннель: Interfaces → GRE Tunnel, заполняем настройки:

- Name: GRE1
- Local Address: XXX.XXX.XXX.XXX
- Remote Address: YYY.YYY.YYY.YYY
- DSCP: inherit
- Don't fragment: no
- Clamp TCP MSS: yes

Назначаем интерфейсу адрес:

IP → Addresses:

- Address: 172.16.1.2/24
- Interface: GRE1

Разрешаем ходить пакетам:

IP → Firewall → Filter Rules, добавляем новое правило:

- Chain: input

- Src Address: YYY.YYY.YYY.YYY
- Protocol: 47(gre)
- Action: accept

Настройки сервера с Ubuntu

В файле /etc/network/interfaces добавляем интерфейс tun1 в самый конец файла:

```
 iface tun1 inet static
    address 172.16.1.1
    netmask 255.255.255.0
    pre-up iptunnel add tun1 mode gre local YYY.YYY.YYY.YYY remote
XXX.XXX.XXX.XXX ttl 255
    up ifconfig tun1 multicast
    pointopoint 172.16.1.2
    post-down iptunnel del tun1
```

Даем команду на поднятие тоннеля:

```
sudo ifup tun1
```

Проверяем - тоннель должен подняться. Для проверки можно попинговать внутренние IP 172.16.1.1 и 172.16.1.2 соответственно.

Настройка IPSEC

В тоннеле GRE по умолчанию нет никакой шифрации, т.е. данные ходят в открытом виде и все можно прекрасно посмотреть любым сниффером (tcpdump, wireshark). Для обеспечения безопасности необходимо настроить IPSEC.

Исходные данные:

- Ключ шифрования: VerySecretChipherKey

IPSEC на Mikrotik

IP → IPsec → Proposals

Изменяем default:

- Auth Algorithms: sha256
- Encr Algorithms: aes-128 cbc, aes-192 cbc, aes-256 cbc
- Lifetime: 00:30:00
- PFS Group: modp1024

А в свойствах GRE-тоннеля настраиваем:

- IPsec Secret: VerySecretChipherKey

Настройки IPSEC на сервере с Ubuntu

Для Ubuntu и прочих линуксов есть несколько пакетов: racoon и несколько форков *swan (StrongSwan, LibreSwan, OpenSwan). Я остановился на StrongSwan - т.к. он мне больше понравился и в сети много готовых примеров.

Установка проста:

```
sudo apt install strongswan
```

Редактируем файл конфигурации /etc/ipsec.conf

```
# ipsec.conf - strongSwan IPsec configuration file

config setup
    charondebug="ike 2, knl 2, cfg 2, net 2, esp 2, dmn 2,  mgr 2"

conn %default
#    keyexchange=ikev2

conn mikrotik
    # Try connect on daemon start
    auto=start

    # Authentication by PSK (see ipsec.secret)
    authby=secret

    # Disable compression
    compress=no

    # Re-dial setings
    closeaction=clear
    dpddelay=30s
    dpdtimeout=150s
    dpdaction=restart

    # ESP Authentication settings (Phase 2)
    esp=aes128-sha256-modp1024,aes192-sha256-modp1024,aes256-sha256-modp1024

    # UDP redirects
    forceencaps=no

    # IKE Authentication and keyring settings (Phase 1)
    ike=aes128-sha256-modp1024,aes192-sha256-modp1024,aes256-sha256-modp1024
    ikelifetime=86400s
    keyingtries=%forever
    lifetime=1800s

    # Internet Key Exchange (IKE) version
    # Default: Charon - ikev2, Pluto: ikev1
```

```
    keyexchange=ikev1

    # connection type
    type=transport

    # Peers
    left=XXX.XXX.XXX.XXX
    right=YYY.YYY.YYY.YYY

    # Protocol type. May not work in numeric then need set 'gre'
    leftprotoport=47
    rightprotoport=47
```

Добавляем ключ шифрования в файл /etc/ipsec.secrets

```
YYY.YYY.YYY.YYY XXX.XXX.XXX.XXX : PSK VerySecretChipherKey
```

Перезапускаем IPSEC:

```
sudo ipsec restart
```

Проверяем /var/log/syslog на Ubuntu и командой

```
ipsec status
```

На Mikrotik смотрим Log и IP → IPsec → Peers

Настройка MTU

Если есть проблемы при работе с тоннелем - желательно уменьшить MTU до 1435 на обоих концах туннеля.

Mikrotik: Изменить в свойствах GRE-тоннеля MTU на 1435

Ubuntu: В файле /etc/network/interfaces добавить строку в настройку интерфейса tun1

```
mtu 1435
```

Настройка firewall

Так же может понадобиться настройка firewall на Микротике и Ubuntu, но тут уж сам настраивает под себя.

Чтобы с Микротика все благополучно проходило через тоннель необходимо сделать маскарадинг:

IP → Firewall → NAT со следующими настройками:

- Chain: srcnat

- Out Interface: GRE1
- Action: Accept

mikrotik, ubuntu, gre, tunnel