Mikrotik: настраиваем IPSEC тоннель

Основной материал для прочтения: http://wiki.mikrotik.com/wiki/Manual:IP/IPsec

Начальные условия

Требуется поднять IPSEC-тоннель между двумя Mikrotik

Mikrotik1:

- Внешний IP: X.X.X.X
- Внутренная подсеть: 192.168.10.0/24

Mikrotik2:

- Внешний IP: Y.Y.Y.Y
- Внутренняя подсеть: 192.168.20.0/24

Этапы настройки:

- Настроить firewall для прохождения пакетов
- Настроить шифрование (Proposal) в IPSEC
- Настроить политику (Policies) в ipsec
- Настроить пир (Peer) в ipsec

Настройка Mikrotik1

Настройка Firewall

Разрешаем пакеты от Mikrotik2

IP → Firewall → Filter rules

```
> /ip firewall filter
```

```
> add chain=input action=accept protocol=udp dst-port=500 src-
address=Y.Y.Y.Y
> add chain=input action=accept protocol=ipsec-esp src-address=Y.Y.Y.Y
> add chain=input action=accept protocol=ipsec-ah src-address=Y.Y.Y.Y
```

Разрешаем пакеты для внутренних сетей

Данное правило необходимо поставить первым, чтобы трафик не уходил куда попало!

IP → Firewall → NAT

```
> /ip firewall nat
> add chain=srcnat action=accept src-address=192.168.10.0/23 dst-
address=192.168.20.0/24
```

Настройка IPSEC

Настройка шифрования

IP → IPsec → Proposals

```
> /ip ipsec proposals
> add name="Secure" auth-algorithms=sha1 enc-algorithms=aes-128-cbc
lifetime=30m pfs-group=modp1024
```

Настройка Policy

Не стоит оставлять поля «Src. Address» и «Dst. Address» со значениями по умолчанию (0.0.0.0/0) - в этом случае вы получите радостно моргающий лампочками кирпич и понадобится делать сброс настроек Mikrotik!

IP → IPsec → Policy

```
> /ip ipsec policy
> add src-address=192.168.10.0/24 src-port=any dst-address=192.168.20.0/24
dst-port=any
     protocol=all action=encrypt level=require ipsec-protocols=ah-esp
tunnel=yes
     sa-src-address=X.X.X.X sa-dst-address=Y.Y.Y.Y proposal=Secure
priority=0
```

Настройка Peer

IP → IPsec → Peers

```
> /ip ipsec peers
> add address=Y.Y.Y.Y local-address=:: passive=no port=500 auth-method=pre-
shared-key
     secret="Pa$$word" generate-policy=no policy-template-group=default
exchange-mode=main
     send-initial-contact=yes nat-traversal=no hash-algorithm=sha1 enc-
algorithm=aes-128
     dh-group=modp1024 lifetime=1d dpd-interval=2m dpd-maximum-failures=5
```

Настройка Mikrotik2

Настройка Firewall

Разрешаем пакеты от Mikrotik1

IP → Firewall → Filter rules

```
> /ip firewall filter
> add chain=input action=accept protocol=udp dst-port=500 src-
address=X.X.X.X
> add chain=input action=accept protocol=ipsec-esp src-address=X.X.X.X
> add chain=input action=accept protocol=ipsec-ah src-address=X.X.X.X
> add chain=input action=accept protocol=udp src-address=X.X.X.X
```

Разрешаем пакеты для внутренних сетей

Данное правило необходимо поставить первым, чтобы трафик не уходил куда попало!

IP → Firewall → NAT

```
> /ip firewall nat
> add chain=srcnat action=accept src-address=192.168.20.0/23 dst-
address=192.168.10.0/24
```

Настройка IPSEC

Настройка шифрования

IP → IPsec → Proposals

```
> /ip ipsec proposals
> add name="Secure" auth-algorithms=sha1 enc-algorithms=aes-128-cbc
lifetime=30m pfs-group=modp1024
```

Настройка Policy

Не стоит оставлять поля «Src. Address» и «Dst. Address» со значениями по умолчанию (0.0.0.0/0) - в этом случае вы получите радостно моргающий лампочками кирпич и понадобится делать сброс настроек Mikrotik!

IP → IPsec → Policy

```
> /ip ipsec policy
> add src-address=192.168.20.0/24 src-port=any dst-address=192.168.10.0/24
dst-port=any
     protocol=all action=encrypt level=require ipsec-protocols=ah-esp
tunnel=yes
     sa-src-address=Y.Y.Y.Y sa-dst-address=X.X.X.X proposal=Secure
priority=0
```

Настройка Peer

IP → IPsec → Peers

```
> /ip ipsec peers
> add address=X.X.X.X local-address=:: passive=no port=500 auth-method=pre-
shared-key
     secret="Pa$$word" generate-policy=no policy-template-group=default
exchange-mode=main
     send-initial-contact=yes nat-traversal=no hash-algorithm=sha1 enc-
algorithm=aes-128
     dh-group=modp1024 lifetime=1d dpd-interval=2m dpd-maximum-failures=5
```

Балансировка каналов и IPSEC

Mikrotik: балансировка двух WAN используя PCC

При эксплуатации IPSEC и балансировке каналов выяснился интересный факт: при установке IPSEC не получается обменяться всеми ключами. IPSEC вроде бы как и поднимается, но работать не работает. Если посмотреть IP → IPsec → Installed SAs - можно увидеть что счетчик

«Current Bytes» для одного из ключей равен 0, т.е. обмен ключами все-таки не прошел. Для правильной работы необходимо добавить еще два правила:

```
> /ip firewall mangle
> add chain=output action=mark-connection new-connection-mark=ISP1_conn
passthrough=no out-interface=WAN1
> add chain=output action=mark-connection new-connection-mark=ISP2_conn
passthrough=no out-interface=WAN2
```

mikrotik, ipsec, vpn