

Настройка MikroTik, IPsec-туннеля, проблема работы RDP и прочих сервисов

И так - суть проблемы:

1. Два маршрутизатора Микротик, между ними поднят туннель IPsec

Маршрутизатор R1:

```
/ip ipsec proposal
add enc-algorithms=des name=proposal1 pfs-group=modp768
/ip ipsec peer
add address=1.1.1.1/32 comment=router2_net dh-group=modp768 enc-
algorithm=des secret=1234567890
/ip ipsec policy
add dst-address=192.168.2.0/24 level=unique proposal=proposal1 sa-dst-
address=1.1.1.1 sa-src-address=2.2.2.2 src-address=192.168.1.0/24 tunnel=yes
```

```
/ip firewall nat
add action=accept chain=srcnat dst-address=192.168.2.0/24 src-
address=192.168.1.0/24
```

Маршрутизатор R2:

```
/ip ipsec proposal
add enc-algorithms=des name=proposal1 pfs-group=modp768
/ip ipsec peer
add address=2.2.2.2/32 comment=router1_net dh-group=modp768 enc-
algorithm=des secret=1234567890
/ip ipsec policy
add dst-address=192.168.1.0/24 level=unique proposal=proposal1 sa-dst-
address=2.2.2.2 sa-src-address=1.1.1.1 src-address=192.168.2.0/24 tunnel=yes
```

```
/ip firewall nat
add action=accept chain=srcnat dst-address=192.168.1.0/24 src-
address=192.168.2.0/24
```

2. Ping до ресурсов из одной сети в другую проходит, но не работают (или очень долго открываются) сервисы типа RDP, SMB и т.п.

В этом случае нам мешает механизм fasttrack - исключим ipsec из fasttrack:

3. Помечаем ipsec на обоих маршрутизаторах:

```
/ip firewall mangle
add action=mark-connection chain=forward comment="IPsec_mark" ipsec-
policy=out,ipsec new-connection-mark=ipsec_mark passthrough=yes
add action=mark-connection chain=forward comment="IPsec_mark" ipsec-
```

```
policy=in,ipsec new-connection-mark=ipsec_mark passthrough=yes
```

4. Искключаем помеченный трафик IPsec из fasttrack:

```
/ip firewall filter  
add action=fasttrack-connection chain=forward comment="fasttrack"  
connection-mark=!ipsec connection-  
state=established,related
```

После вышеуказанных действий - всё начинает прекрасно работать.

From:

<http://wiki.netair.by/> - **NetAir Wiki**

Permanent link:

http://wiki.netair.by/wiki/article/ipsec_rdp

Last update: **2017/11/22 22:57**

