

Настраиваем IPsec-туннель между офисами на оборудовании Mikrotik

 interface31.ru/tech_it/2022/01/nastraivaem-ipsec-tunnel-mezhdu-ofisami-na-oborudovanii-mikrotik.html

Записки IT специалиста

Технический блог специалистов ООО "Интерфейс"

- [Главная](#)
- Настраиваем IPsec-туннель между офисами на оборудовании Mikrotik

Задача объединения нескольких сетей в разных офисах одна из наиболее часто встречающихся у системных администраторов. Для ее решения могут использоваться различные виды VPN и туннельных соединений, выбор которых может зависеть от множества требований и условий. Одной из альтернатив туннелям и VPN может служить "чистое" IPsec-соединение, которое имеет как свои достоинства, так и недостатки. В данном материале мы рассмотрим реализацию подобного соединения между сетями офисов (site-to-site) с использованием оборудования Mikrotik.



Онлайн-курс по MikroTik

Научиться настраивать MikroTik с нуля или систематизировать уже имеющиеся знания можно на [углубленном курсе по администрированию MikroTik](#). Автор курса, сертифицированный тренер MikroTik Дмитрий Скоромнов, лично проверяет лабораторные работы и контролирует прогресс каждого своего студента. В три раза больше информации, чем в вендорской программе MTCNA, более 20 часов практики и доступ навсегда.

IPsec - набор протоколов для обеспечения защиты данных, передаваемых в сетях по протоколу IP. Основным преимуществом IPsec является высокий уровень безопасности, на сегодняшний день он является лучшим протоколом для защиты передаваемых данных. Также следует отметить высокий уровень производительности, при условии достаточного количества вычислительных ресурсов для работы с криптографией. Применительно к устройствам Mikrotik IPsec позволяет получить одни из самых высоких результатов, особенно на устройствах с аппаратной поддержкой шифрования.

Но есть и недостатки, они тоже достаточно существенны. IPsec сложен, как в настройке, так в понимании его работы, это требует от администратора более глубокого уровня знаний и может вызвать серьезные затруднения при отладке и диагностике неисправностей. Также IPsec не использует интерфейсы, а обрабатывает трафик на основании собственных политик, это также приводит к ряду затруднений, начиная от прохождения трафика через брандмауэр и

заканчивая невозможностью применения маршрутизации для таких соединений. Часть сетевых конфигураций легко реализуемых при помощи VPN и туннелей построить при помощи IPsec в принципе невозможно.

Далее мы рассмотрим объединение двух офисных сетей по представленной ниже схеме:



Где LAN 1 с диапазоном 192.168.111.0/24 и LAN 2 - 192.168.186.0/24 - это сети двух офисов, которые мы будем объединять, а 192.168.3.107 и 192.168.3.111 - выполняют роль внешних белых адресов в сети интернет. Наша задача обеспечить прозрачный доступ устройств одной сети в другую через защищенный канал связи.

Настройка IPsec соединения

Соединение IPsec имеет отличия как от предусматривающего клиент-серверную схему VPN, так и от stateless туннелей. В отличие от последних мы всегда можем проверить состояние соединения, но понятие клиента и сервера здесь отсутствует, в IPsec одно из устройств выступает в качестве **инициатора** (*initiator*), а второе в качестве **ответчика** (*responder*). Эти роли не являются жестко закрепленными и могут меняться между устройствами, хотя при необходимости мы можем закрепить за определенным устройством постоянную роль.

Например, это позволяет установить IPsec соединение, когда один из узлов не имеет выделенного IP-адреса, в этом случае ему следует настроить роль инициатора, а второму узлу роль ответчика. В нашем случае подразумевается наличие выделенных адресов с обеих сторон и каждое из устройств может выступать в любой роли.

Настройку начнем с определения алгоритмов шифрования для каждой фазы соединения. Так как мы соединяем два собственных устройства, то можем не оглядываться на требования совместимости и настроить параметры шифрования на собственное усмотрение. Но без фанатизма, не забываем, что многие устройства Mikrotik достаточно слабые и не имеют аппаратной поддержки шифрования, а те, которые имеют, поддерживают различный набор протоколов.

Так популярный **RB750Gr3 (hEX)** поддерживает аппаратное ускорение только **SHA1/SHA256 - AES-CBC**, а более новый RB3011 уже поддерживает **SHA1/SHA256 - AES-CBC** и **SHA1/SHA256 - AES-CTR**. Желание использовать сильные шифры безусловно похвально, но оно не должно опережать возможности имеющегося оборудования.

Первая фаза - обмен ключами и взаимная идентификация устройств, за ее настройки отвечает раздел **IP - IPsec - Profiles**, перейдем в него и создадим новый профиль. Для него укажем: **Hash Algorithms - sha1**, **Encryption Algorithm - aes-256**, **DH Group - ecp384**. В поле **Name** укажем имя профиля, в нашем случае **ipsec-sts** (site-to-site).

The screenshot shows the 'IPsec Profile <ipsec-sts>' configuration window. The 'Name' field is set to 'ipsec-sts'. 'Hash Algorithms' is set to 'sha1' and 'PRF Algorithms' is set to 'auto'. Under 'Encryption Algorithm', 'aes-256' is selected. Under 'DH Group', 'ecp384' is selected. Other options like 'des', '3des', 'aes-128', 'aes-192', 'blowfish', 'camellia-128', 'camellia-192', 'camellia-256', 'modp768', 'modp1024', 'ec2n155', 'ec2n185', 'modp1536', 'modp2048', 'modp3072', 'modp4096', 'modp6144', 'modp8192', 'ecp256', and 'ecp521' are unselected. 'Proposal Check' is set to 'obey', 'Lifetime' is '1d 00:00:00', and 'Lifebytes' is empty. 'NAT Traversal' is checked. 'DPD Interval' is '120' and 'DPD Maximum Failures' is '5'. Buttons for 'OK', 'Cancel', 'Apply', 'Copy', and 'Remove' are on the right.

В терминале для выполнения этого же действия выполните:

```
/ip ipsec profile  
add dh-group=ecp384 enc-algorithm=aes-256 name=ipsec-sts
```

Это достаточно сильные настройки шифров, для устройств без аппаратного ускорения мы бы посоветовали ограничиться **aes-128** и **modp1024**, хотя никто не мешает протестировать желаемые варианты и остановиться на наиболее оптимальном.

Вторая фаза - установление защищённого соединения и передача данных, настройки шифров для нее задаются в **IP - IPsec - Proposal**, перейдем в данный раздел и создадим новое предложение. Укажем **Auth. Algorithms - sha1**, **Encr. Algorithms - aes-256-cbc**, **PFS Group - ecp384**.

IPsec Proposal <ipsec-sts>

Name: ipsec-sts

Auth. Algorithms: ☐ md5 ☒ sha1 ☐ null ☐ sha256 ☐ sha512

Encr. Algorithms: ☐ null ☐ des ☐ 3des ☐ aes-128 cbc ☐ aes-192 cbc ☒ aes-256 cbc ☐ blowfish ☐ twofish ☐ camellia-128 ☐ camellia-192 ☐ camellia-256 ☐ aes-128 ctr ☐ aes-192 ctr ☐ aes-256 ctr ☐ aes-128 gcm ☐ aes-192 gcm ☐ aes-256 gcm

Lifetime: 00:30:00

PFS Group: ecp384

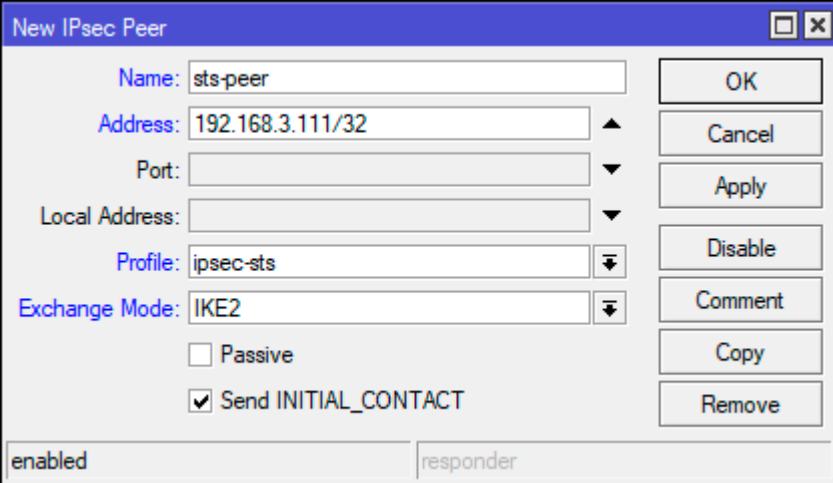
enabled

Это же действие в терминале:

```
/ip ipsec proposal  
add enc-algorithms=aes-256-cbc name=ipsec-sts pfs-group=ecp384
```

В данном примере мы использовали не самые сильные шифры, так режим шифрования **CBC** является наиболее слабым и при наличии аппаратной поддержки стоит использовать **CTR** или **GCM**. Но не забывайте о достаточной разумности, если нагрузка на устройство велика - понижайте уровень шифрования.

Теперь перейдем в **IP - IPsec - Peer** и создадим новое подключение. В поле **Address** указываем внешний адрес второго роутера, в **Profile** выбираем созданный нами на предыдущем этапе профиль, в нашем случае **ipsec-sts**, а в поле **Exchange Mode** указываем **IKE2**.



The 'New IPsec Peer' window shows the following configuration:

- Name: sts-peer
- Address: 192.168.3.111/32
- Port: (empty)
- Local Address: (empty)
- Profile: ipsec-sts
- Exchange Mode: IKE2
- ☐ Passive
- ☒ Send INITIAL_CONTACT

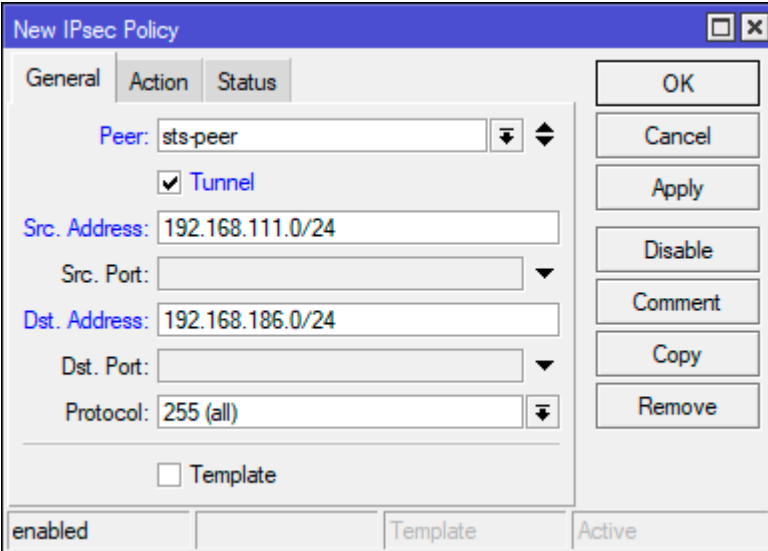
Buttons on the right: OK, Cancel, Apply, Disable, Comment, Copy, Remove.

Bottom status: enabled responder

В терминале:

```
/ip ipsec peer
add address=192.168.3.111/32 exchange-mode=ike2 name=sts-peer profile=ipsec-sts
```

В целом того, что мы уже настроили достаточно для установления защищенного соединения, но IPsec не VPN и работает по-другому. Для того, чтобы трафик начал шифроваться он должен соответствовать одной из политик IPsec, поэтому перейдем в **IP - IPsec - Policies** и создадим новую политику. В поле Peer укажем созданное ранее соединение, ниже установим флаг **Tunnel** для работы соединения в туннельном режиме, в поле **Src. Address** укажем диапазон собственной сети - **192.168.111.0/24**, а в поле **Dst. Address** - диапазон удаленной сети - **192.168.186.0/24**.



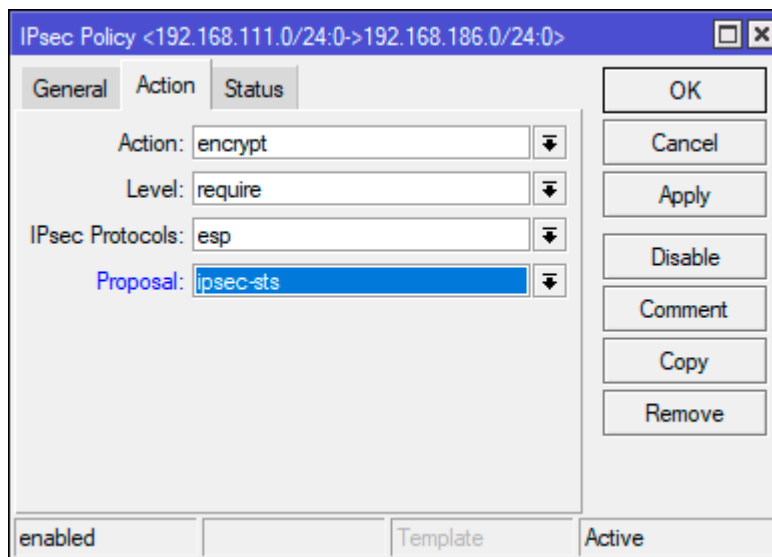
The 'New IPsec Policy' window shows the following configuration:

- Peer: sts-peer
- ☒ Tunnel
- Src. Address: 192.168.111.0/24
- Src. Port: (empty)
- Dst. Address: 192.168.186.0/24
- Dst. Port: (empty)
- Protocol: 255 (all)
- ☐ Template

Buttons on the right: OK, Cancel, Apply, Disable, Comment, Copy, Remove.

Bottom status: enabled Template Active

Затем на закладке **Action** установите **Proposal - ipsec-sts**, предложение которое мы создали ранее.



Для терминала используйте следующие команды:

```
/ip ipsec policy  
add dst-address=192.168.186.0/24 peer=sts-peer proposal=ipsec-sts src-  
address=192.168.111.0/24 tunnel=yes
```

Ну и осталось совсем немного - научить узлы идентифицировать друг друга, так как оба роутера контролируются администратором и настроены принимать подключения только от другого узла, то мы будем использовать аутентификацию по предварительному ключу. Перейдем в IP - IPsec - Identities и создадим новую настройку идентификации. Здесь нам нужно заполнить поля: **Peer** - указываем созданное нами соединение, в нашем случае **ipsec-sts**, **Auth. Method - pre shared key**, **Secret** - предварительный ключ. В качестве предварительного ключа рекомендуется использовать строку с использованием цифр, букв в разных регистрах и специальных символов, сформированных в случайном порядке и с длиной не менее 16-32 символов. Не следует использовать в качестве ключа словарные слова и фразы. Предупреждения внизу окна можно проигнорировать.

New IPsec Identity

Peer: sts-peer

Auth. Method: pre shared key

Secret:

Policy Template Group: default

Notrack Chain:

My ID Type: auto

Remote ID Type: auto

Match By: remote id

Mode Configuration:

Generate Policy: no

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove

Status: enabled

Error: Peer does not exist

Suggestion: Suggestion to use stronger pre-shared key or different authentication method

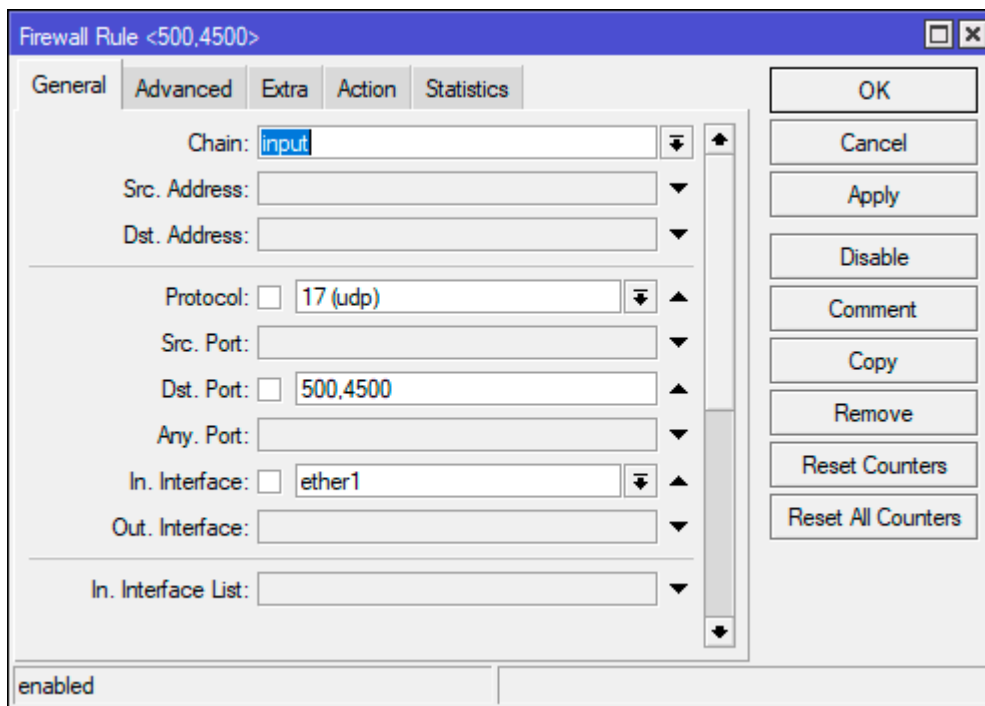
В терминале:

```
/ip ipsec identity
add peer=sts-peer secret="2KuSY2%QKt\$\$gs8V9nrERD@V8zAuh\$3S"
```

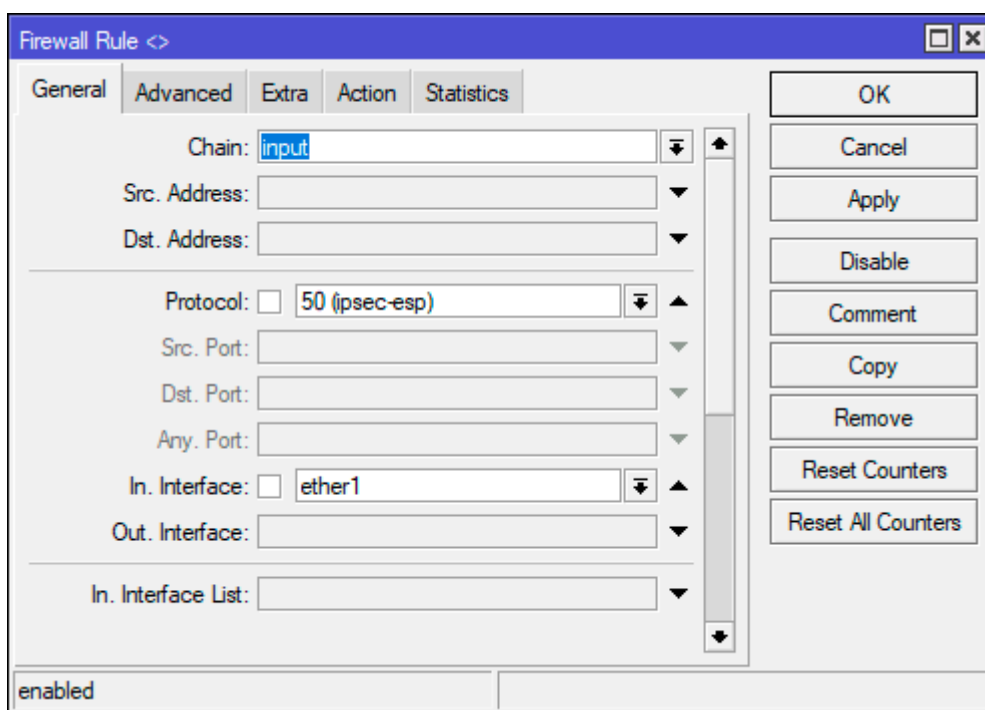
На втором узле следует выполнить аналогичные настройки, только в качестве адреса в **Peer** указав внешний адрес первого роутера, а в **Policy** поменяв местами сеть источника и сеть назначения.

Настройка брандмауэра

Будем считать, что вы используете нормально закрытый брандмауэр настроенный в соответствии с нашими рекомендациями. Для того, чтобы разрешить входящее IPsec-соединение перейдем в **IP - Firewall - Filter Rules** и добавим следующие правила. Первое из них разрешает работу протокола обмена ключами IKE: **Chain - input, Protocol - udp, Dst. Port - 500,4500, In. Interface -** внешний интерфейс, в нашем случае **ether1**.



Второе правило разрешает протокол шифрования полезной нагрузки Encapsulating Security Payload (ESP): **Chain - input, Protocol - 50 (ipsec-esp), In. Interface -** внешний интерфейс - **ether1**.

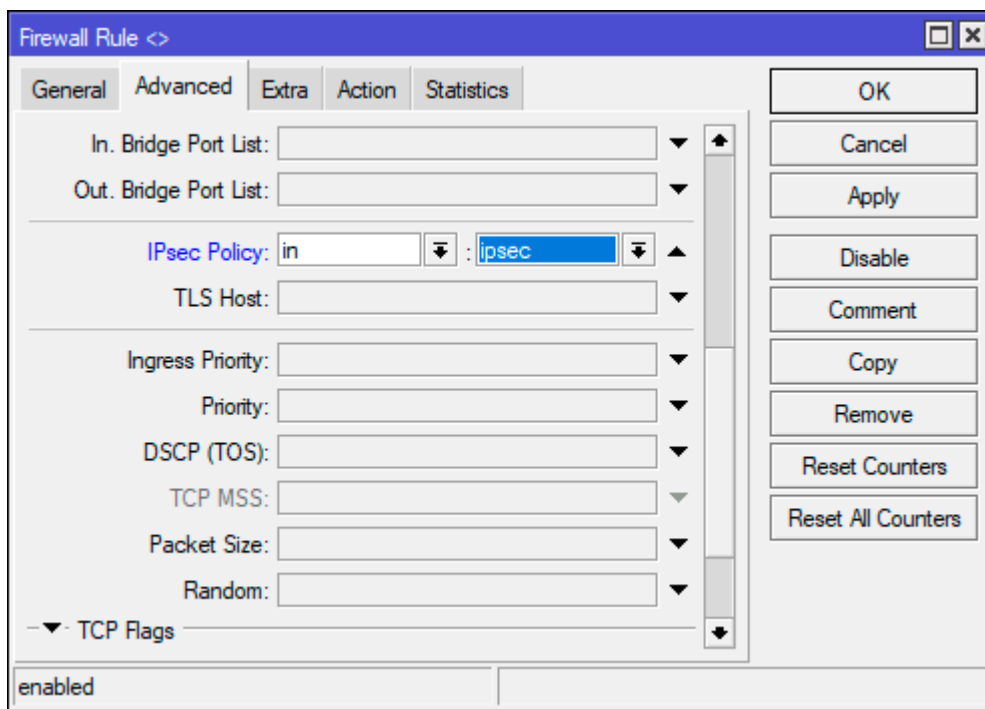


Обратите внимание, что мы нигде не указываем действие, потому что по умолчанию все правила имеют в качестве действия **accept** - разрешить.

Эти же действия можно быстро выполнить в терминале:

```
/ip firewall filter
add action=accept chain=input dst-port=500,4500 in-interface=ether1 protocol=udp
add action=accept chain=input in-interface=ether1 protocol=ipsec-esp
```


Для того, чтобы пакеты из одной сети могли попасть в другую, следует разрешить их транзит. Создадим еще одно правило: **Chain - forward, In. Interface - ether1**, затем на закладке **Advanced** укажем **IPsec Policy - in:ipsec**. Это разрешит транзит любых входящих пакетов, которые попадают под любую установленную политику IPsec.



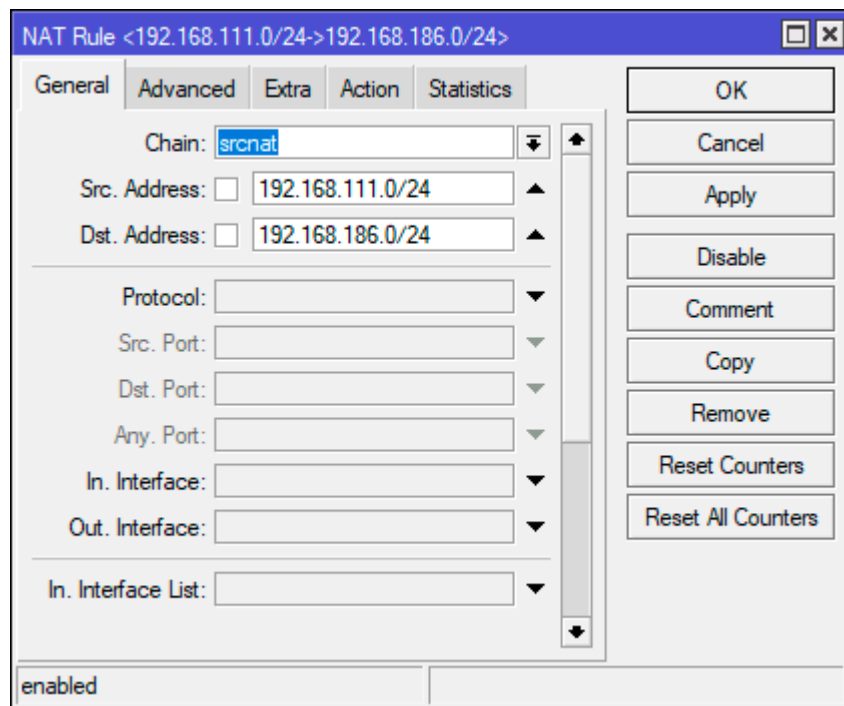
В терминале:

```
/ip firewall filter
add action=accept chain=forward in-interface=ether1 ipsec-policy=in,ipsec
```

Аналогичные настройки следует выполнить на втором узле.

Обход NAT и Fasttrack

Как мы уже говорили, IPsec не использует интерфейсы, а следовательно, обрабатываемый им трафик, хоть и уходит в защищенный туннель, но продолжает использовать в качестве исходящего внешний интерфейс, что может привести к ряду коллизий. Прежде всего нужно исключить обработку такого трафика правилами **snat** или **masquerade**. Для этого перейдем в **IP - Firewall - NAT** и создадим новое правило: **Chain - srcnat, Src. Address - 192.168.111.0/24** - диапазон локальной сети, **Dst. Address - 192.168.186.0/24** - диапазон удаленной сети, так как действие по умолчанию ассерт, то явно его не указываем. Данное правило поднимаем в самый верх, одно должно быть первым в цепочке **srcnat**.



Через терминал добавить его можно следующей командой:

```
/ip firewall nat
add action=accept chain=srcnat dst-address=192.168.186.0/24 src-
address=192.168.111.0/24 place-before=0
```

Опция **place-before=0** позволяет поставить правило в самое начало цепочки.

Если вы используете Fasttrack, то также следует исключить обработку проходящего через IPsec трафика этим механизмом, для этого следует добавить два правила.

Первое для трафика из локальной сети в удаленную: **Chain - forward, Src. Address - 192.168.111.0/24** - диапазон локальной сети, **Dst. Address - 192.168.186.0/24** - диапазон удаленной сети, **Connection State - established, related**.

Второе правило для трафика из удаленной сети в локальную, оно полностью повторяет первое, только меняем местами сеть источника (Src. Address) и сеть назначения (Dst. Address).

В терминале:

```
/ip firewall filter
add chain=forward action=accept place-before=0 src-address=192.168.111.0/24 dst-address=192.168.186.0/24 connection-state=established,related
add chain=forward action=accept place-before=0 src-address=192.168.186.0/24 dst-address=192.168.111.0/24 connection-state=established,related
```

Аналогичные настройки, с учетом адресов, следует выполнить и на втором узле.

Заключение

После того, как мы завершили процесс настройки перейдем в **IP - IPsec - Active Peers** и убедимся, что соединение между двумя узлами установлено. Если это не так - еще раз проверяем все настройки и изучаем файл лога, скорее всего у вас не совпадают параметры шифрования или идентификации.

The screenshot shows the 'Active Peers' tab in the IPsec configuration utility. A table lists the active peers with the following data:

ID	State	Local Address	Remote Address	Dynamic Address	Side	Uptime	PH2 Total	Tx Bytes	Rx Bytes	Tx Packets	Rx Packets
192.168.3.111	established	192.168.3.107	192.168.3.111	0.0.0.0	responder	07:53:33	1	3 273 626	1 575 877	22 813	22 697

At the bottom of the window, it indicates '1 item'.

Теперь откроем **IP - IPsec - Installed SAs**. В терминах IPsec - **SA (Security Association)** - ассоциация безопасности, обозначает установленное защищенное соединение. Для каждого соединения создается отдельная пара SA, так как каждая SA - это однонаправленное соединение, а данные нужно передавать по двум направлениям. Если запустить обмен данными между сетями, скажем пропинговать с узла одной сети узел другой сети, то мы увидим, что данные счетчика **Current Bytes** начинают меняться, а следовательно, шифрование работает и данные передаются внутри защищенного соединения.

The screenshot shows the 'Installed SAs' tab in the IPsec configuration utility. A table lists the installed security associations with the following data:

SPI	Src. Address	Dst. Address	Auth. Algorithm	Encr. Algorithm	Encr....	Current Bytes
4eb22fb	192.168.3.107	192.168.3.111	sha1	aes cbc	256	4951
c2d5ec4	192.168.3.111	192.168.3.107	sha1	aes cbc	256	2507

At the bottom of the window, it indicates '2 items'.

Как видим, если хотя бы на базовом уровне понимать принципы действия IPsec, то настроить туннель между двумя сетями относительно несложно. Надеемся, что данный материал будет вам полезен.

Онлайн-курс по MikroTik

Научиться настраивать MikroTik с нуля или систематизировать уже имеющиеся знания можно на [углубленном курсе по администрированию MikroTik](#). Автор курса, сертифицированный тренер MikroTik Дмитрий Скоромнов, лично проверяет лабораторные работы и контролирует прогресс каждого своего студента. В три раза больше информации, чем в вендорской программе MTCNA, более 20 часов практики и доступ навсегда.
