

MikroTik Training center

Network Academy

Chapter 5 UME

Chapter 6 SE

IPSec



MTCSE
MTCUME
MikroTik-Trainings.com
You become what you do

MikroTik Training center

Network Academy

Chapter 5 UME

Chapter 6 SE

IPSec



MTCSE
MTCUME
MikroTik-Trainings.com
You become what you do

IPSec

- Internet Protocol Security (IPsec) – набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP. Позволяет осуществлять подтверждение подлинности (аутентификацию), проверку целостности и/или шифрование IP-пакетов
- Первоначально разработанный для IPv6, позже был включен также в IPv4
- Так же обеспечивает шифрование IP protocol
- Можем использовать как в IPv4 так и IPv6
- IPSec - стандарт, но для него существуют RFC (Requests For Comments) RFC 4301, RFC 4302, RFC 4303, RFC 2408, RFC 5996, RFC 4835 and e.t.c



IPSec

Confidentiality
шифрует данные

Integrity (целостность)
Маршрутизаторы на каждом конце туннеля вычисляют контрольную сумму или хеш-значение данных

Authentication
ключи, подписи и сертификаты

IPsec Architecture



IPSec - Transport Mode

В транспортном режиме шифруются (или подписываются) только данные IP-пакета, исходный заголовок сохраняется.

- используется для установления соединения между хостами
- также используется между шлюзами для защиты туннелей, организованных каким-либо другим способом (L2TP, GRE, PIP, EoIP and etc)



IPsec single chain



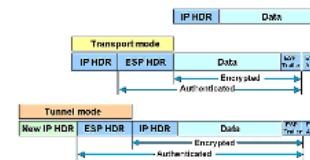
IPSec - Tunnel Mode

В туннельном режиме шифруется весь исходный IP-пакет: данные, заголовки, маршрутная информация, а затем он вставляется в поле данных нового пакета, то есть происходит инкапсуляция.

- используется для подключения удалённых компьютеров к виртуальной частной сети
- для организации безопасной передачи данных через открытые каналы связи (например, Интернет) между шлюзами для объединения разных частей виртуальной частной сети



IPSec Transporte and Tunnel mode



IPsec, протоколы

протоколы защиты передаваемых данных (AH, ESP)
протоколы обмена ключами (IKE/Internet Key Exchange)

Функции IKE:

- Устанавливает SA (Security Association, session IPsec)
- Определяет параметры безопасности
- Инициализирует ESP-порт 500 (UDP-500)
- Обмен ключами
- Путь передачи информации (IKE)
- Две режимы (адресный и анонимный режим)
- Три метода аутентификации (pre-shared, public key encryption, and public key signature)

Фазы IKE:

- Фаза 1
- Фаза 2

IKE Phase 1 и Phase 2

- IKE Phase 1**
- Establish secure channel (ISAKMP SA)
 - Using either main mode or aggressive mode
 - Authentication computer identity using certificates or pre-shared secret
 - Authentication method
 - DM group
 - Encryption algorithm
 - Integrity hash
 - Diffie-Hellman
 - NAT-T
 - DPD and lifetime function
- IKE Phase 2**
- Establish secure channel (IPsec SA)
 - Using either main mode or aggressive mode
 - Authentication computer identity using certificates or pre-shared secret
 - Authentication method
 - DM group
 - Encryption algorithm
 - Integrity hash
 - Diffie-Hellman
 - NAT-T
 - DPD and lifetime function

Инициализация IKE Phase 1 и Phase 2 осуществляется с помощью протокола ISAKMP. В фазе 1 устанавливается защищенный канал (ISAKMP SA) для обмена информацией о безопасности. В фазе 2 устанавливается защищенный канал (IPsec SA) для передачи данных.

SA (Security Association)

- "Ассоциация безопасности - это связь" - это термин IPsec для обозначения соединения.
- При настройке VPN, для каждого используемого протокола создается SA. Для ESP-порта 500 и для ESP-порта 4500.
- SA включает в себя, т.е. каждый SA - это совокупность параметров, а именно: алгоритмы шифрования и аутентификации.
- Каждый SA имеет свой уникальный номер, который используется для идентификации. SA идентифицируется по своему номеру и алгоритму шифрования.
- Каждый SA имеет свой уникальный номер, который используется для идентификации. SA идентифицируется по своему номеру и алгоритму шифрования.
- Каждый SA имеет свой уникальный номер, который используется для идентификации. SA идентифицируется по своему номеру и алгоритму шифрования.

Параметры SA, такие как алгоритмы шифрования и аутентификации, используются для защиты данных. SA идентифицируется по своему номеру и алгоритму шифрования.

IPSec

- Internet Protocol Security (IPsec) – набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP. Позволяет осуществлять подтверждение подлинности (аутентификацию), проверку целостности и/или шифрование IP-пакетов
- Первоначально разработанный для IPv6, позже был включен также в IPv4
- Так же обеспечивает шифрование IP protocol
- Можем использовать как в IPv4 так и IPv6
- IPSec - стандарт, но для него существуют RFC (Requests For Comments) RFC 4301, RFC 4302, RFC 4303, RFC 2408, RFC 5996, RFC 4835 and e.t.c

уровень OSI	Протокол реализации функции
Прикладной уровень	SSL, TLS
Транспортный уровень	SSL, TLS
Сетевой уровень	IPsec
Транспортный уровень	IPsec
Сетевой уровень	IPsec
Транспортный уровень	IPsec
Сетевой уровень	IPsec

IPsec: расположен на сетевом уровне, использует сетевой распределенный протокол этого уровня — IP. Это дает IPsec гибкость, которую можно использовать для защиты любых протоколов, работающих на TCP и UDP. Так же он прозрачен для безопасности приложений

Уровни OSI	Протокол защищённого канала
Прикладной уровень	S/MIME
Уровень представления	SSL, TLS
Сеансовый уровень	PPTP
Транспортный уровень	AH, ESP
Сетевой уровень	IPsec
Канальный уровень	PPP
Физический уровень	

IPsec : расположен на сетевом уровне, используя самый распространённый протокол этого уровня — IP. Что дает IPsec гибкость, может использоваться для защиты любых протоколов, базирующихся на TCP и UDP. Так же он прозрачен для большинства приложений

IPSec

Confidentiality

шифруя данные

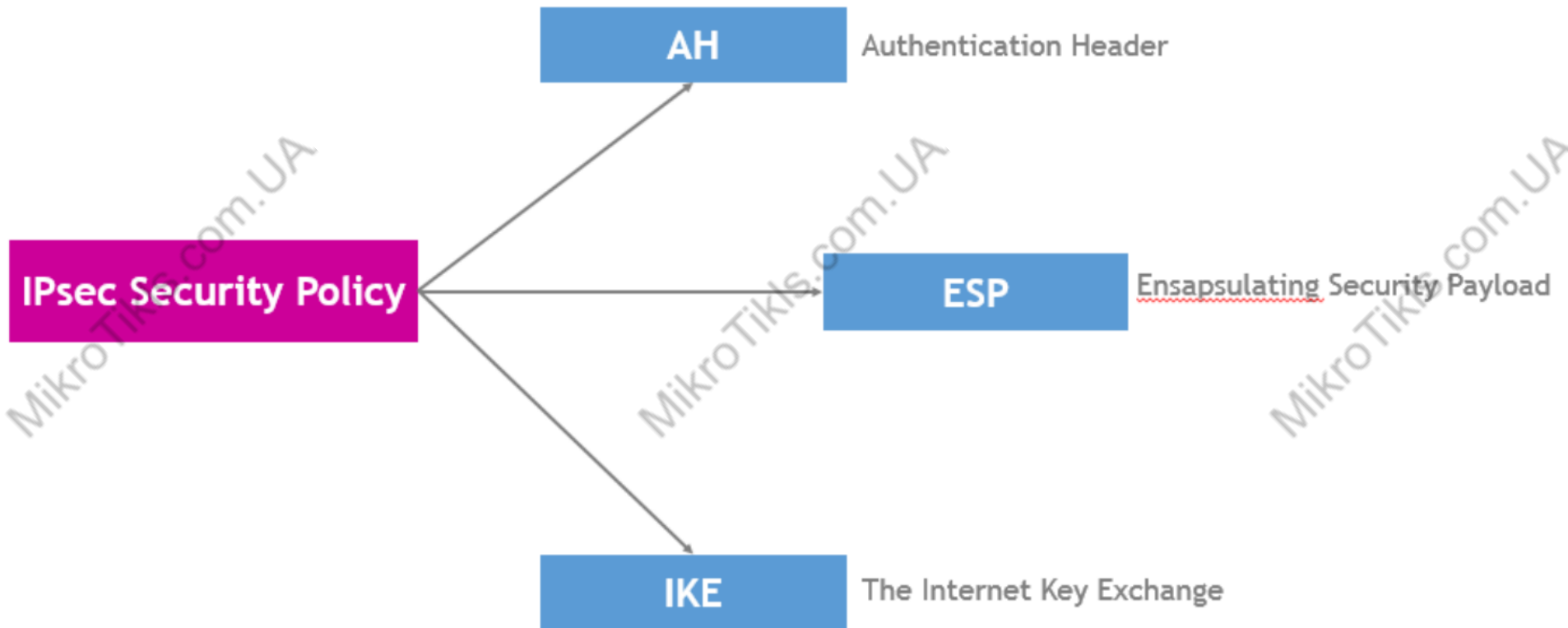
Integrity (целостность)

Маршрутизаторы на каждом конце туннеля
вычисляют контрольную сумму или
хеш-значение данных

Authentication

ключи, подписи и сертификаты

IPsec Architecture

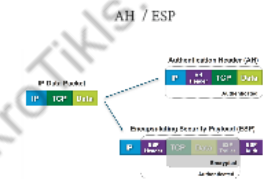


IPSec

AH, ESP - протоколы защиты передаваемых данных

Несколько подходов можно использовать для реализации IPsec:

- Обеспечения аутентификации отправителя, контроля целостности данных (**AH**)
- Протокол инкапсулирующей защиты содержимого (**ESP**) - шифрование данных



AH (Authentication Header)

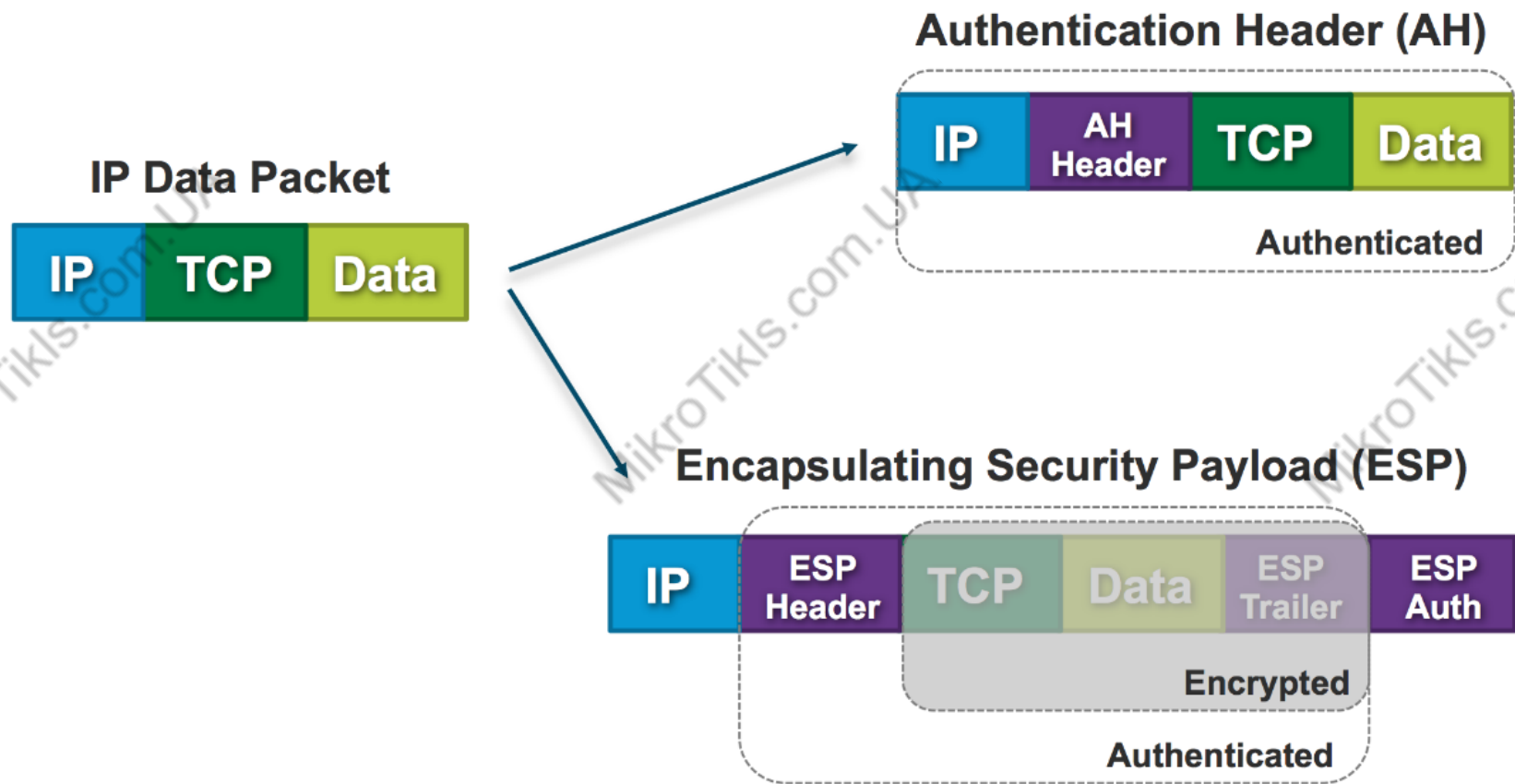
- AH (Authentication Header) - протокол заголовка аутентификации.
- Обеспечивает аутентификацию и целостность путем проверки того, что ни один бит в защищаемой части пакета не был изменен со времени отправки.
- AH разработывается только для обеспечения целостности. Он не гарантирует конфиденциальности путем шифрования содержимого пакета.
- Для AH номер ID - 51 (protocol 51).
- Описывается в RFC 4302.

ESP (Encapsulating Security Protocol)

- ESP (Encapsulating Security Protocol) - инкапсулирующий протокол безопасности, который обеспечивает и целостность и конфиденциальность.
- Для ESP номер ID - 50.
- Предоставляет то, что требуется для защиты конфиденциальности данных.
- ESP использует симметричный ключ шифрования.
- Описывается в RFC 4303.

ESP (packet data encryption) является наиболее широко используемым

AH / ESP



АН (Authentication Header)

- АН (Authentication Header) - протокол заголовка идентификации.
- Обеспечивает аутентификацию и целостность путём проверки того, что ни один бит в защищаемой части пакета не был изменён во время передачи
- АН разрабатывался только для обеспечения целостности. Он не гарантирует конфиденциальности путём шифрования содержимого пакета
- Для АН номер ID - 51 (protocol 51)
- Описывается в RFC 4302
- RouterOS поддерживает следующие алгоритмы аутентификации для АН:
 - SHA1
 - SHA2
 - MD5

ESP (Encapsulating Security Protocol)

- ESP (Encapsulating Security Protocol) - инкапсулирующий протокол безопасности, который обеспечивает и целостность и конфиденциальность.
- Для ESP имеет ID протокола равен 50
- Предоставляет все, что предлагает АН, плюс конфиденциальность данных
- Использует симметричный ключ шифрования
- Описывается в RFC 4303

RouterOS ESP поддерживает encryption and authentication:

Authentication:

- MD5
- **SHA1**
- **SHA2 (256-bit, 512-bit)**

Encryption:

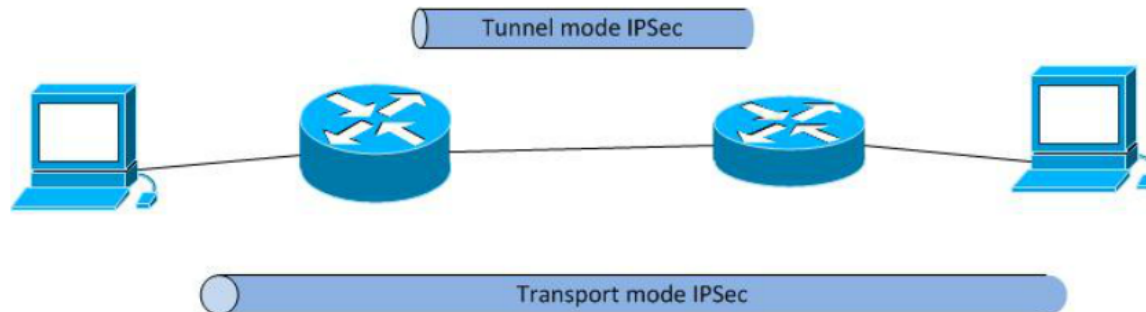
- AES - 128-bit, 192-bit and 256-bit key **AES-CBC**, AES-CTR and AES-GCM algorithms;
- Blowfish - added since v4.5
- Twofish - added since v4.5
- Camellia - 128-bit, 192-bit and 256-bit key Camellia encryption algorithm added since v4.5
- DES - 56-bit DES-CBC encryption algorithm;
- 3DES - 168-bit DES encryption algorithm;

Hardware: <https://wiki.mikrotik.com/wiki/Manual:IP/IPsec>

IPSec

Может быть настроен для работы в двух разных режимах

- Transport
- Tunnel

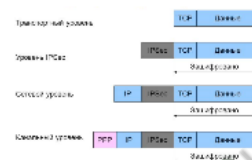


IPSec - Transport Mode

В транспортном режиме шифруются (или подписываются) только данные IP-пакета, исходный заголовок сохраняется.

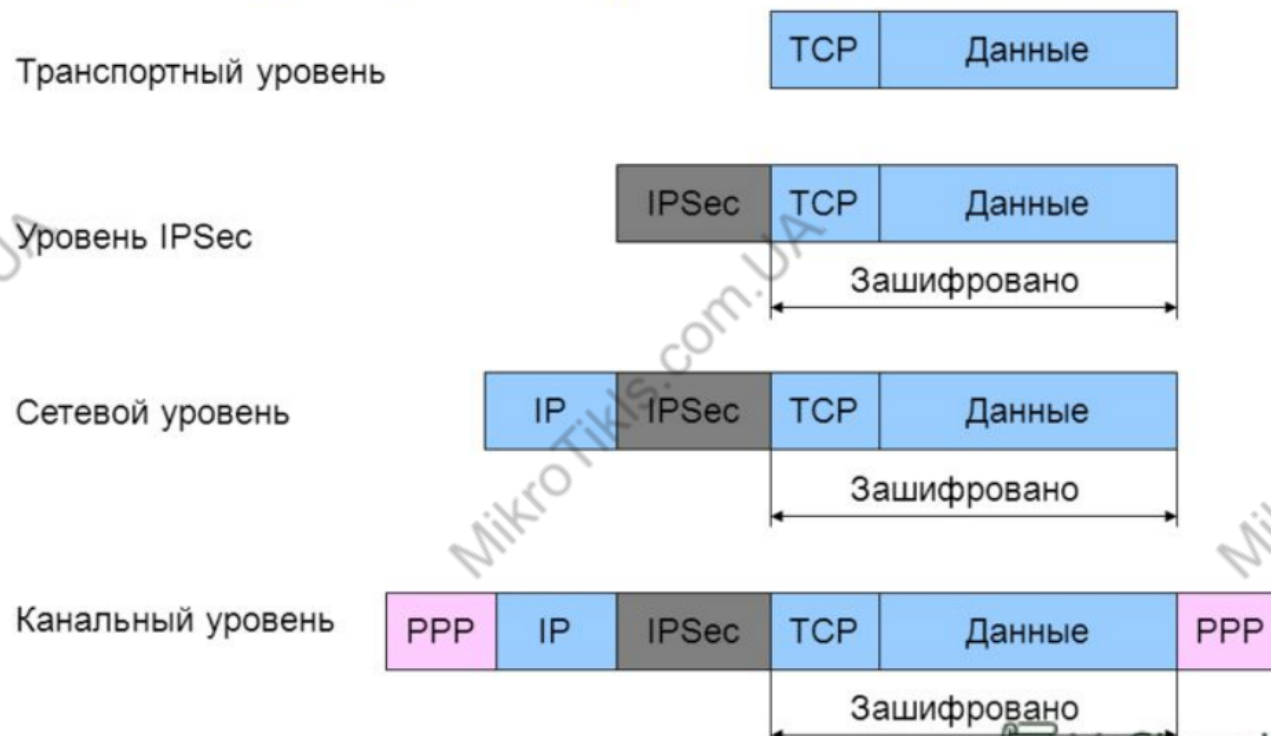
- используется для установления соединения между хостами
- также используется между шлюзами для защиты туннелей, организованных каким-нибудь другим способом (L2TP, GRE, IP/IP, EoIP and etc)

IPSec - Transport Mode



- используется исходный IP заголовок
- адреса конечных устройств остаются без изменений
- новый пакет не создается

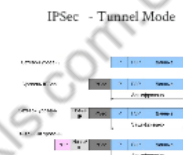
IPSec - Transport Mode



- используется исходный IP заголовок
- адреса конечных устройств остаются без изменения
- новый пакет не создается

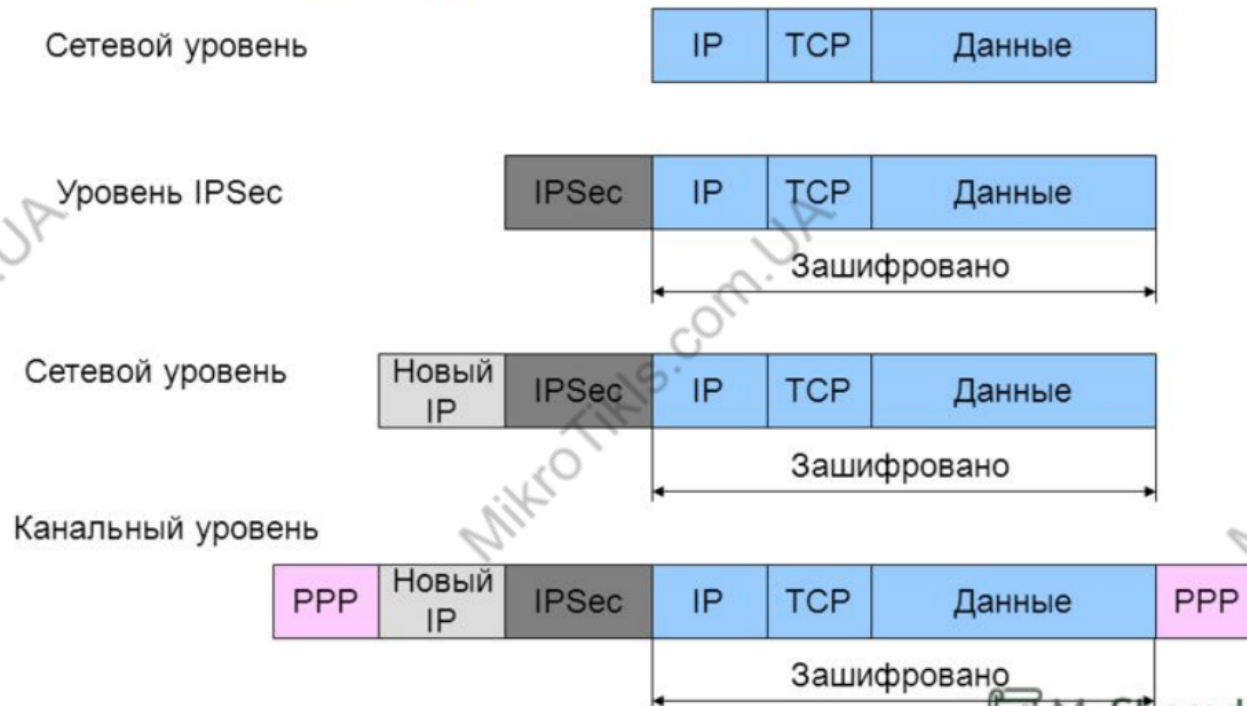
IPSec - Tunnel Mode

В туннельном режиме шифруется* весь исходный IP-пакет: данные, заголовок, маршрутная информация*, а затем он вставляется в поле данных нового пакета, то есть происходит инкапсуляция.

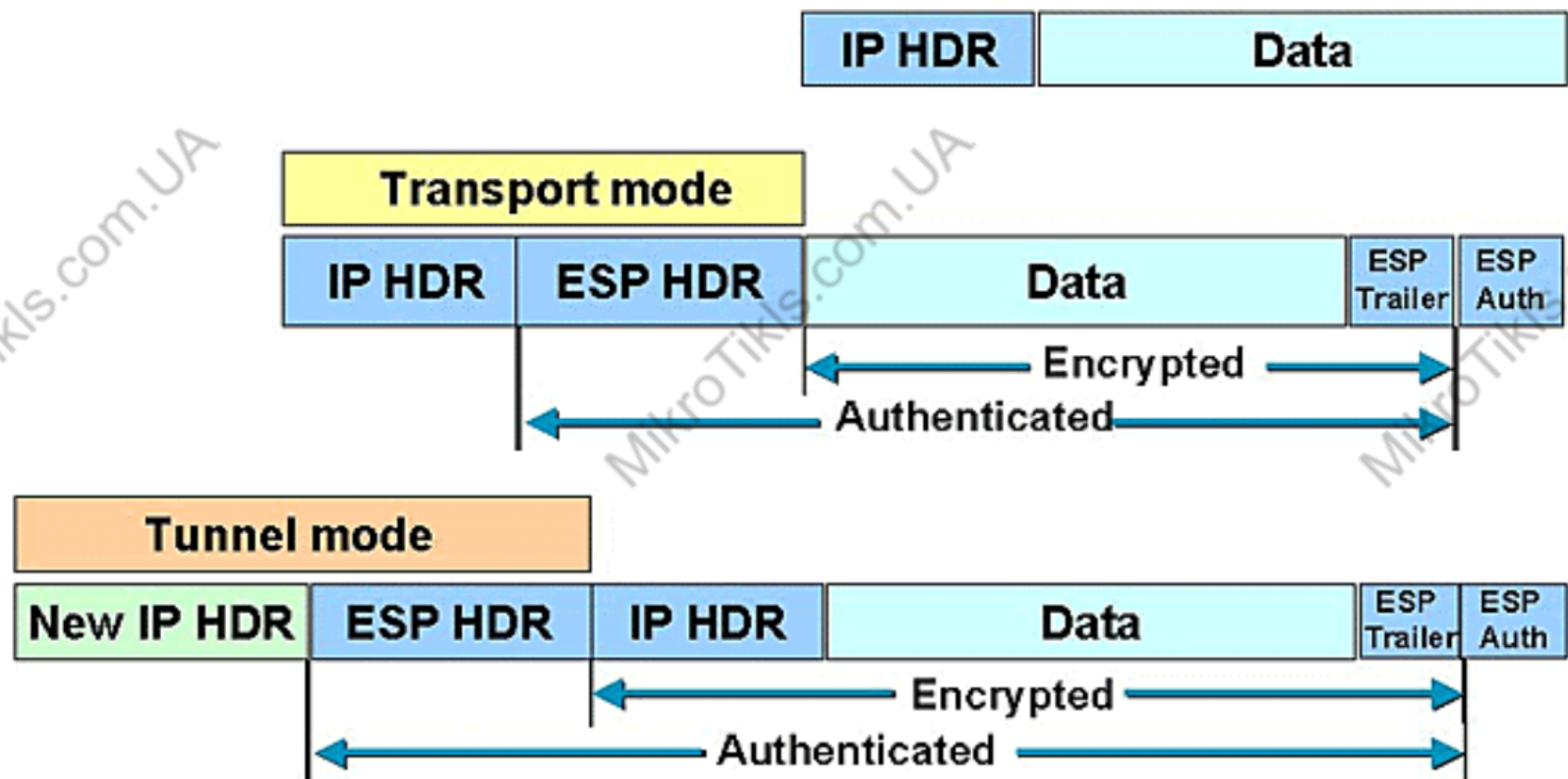


- используется для подключения удалённых компьютеров к виртуальной частной сети
- для организации безопасной передачи данных через открытые каналы связи (например, Интернет) между шлюзами для объединения разных частей виртуальной частной сети

IPSec - Tunnel Mode

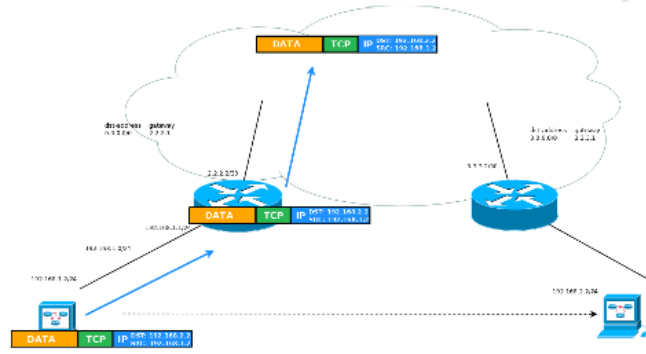


IPSec Transport and Tunnel mode



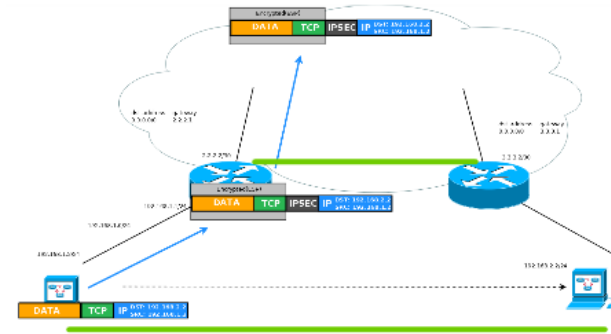
Routing without IPSec

if IPSec then Tunnel mode or Transport mode?



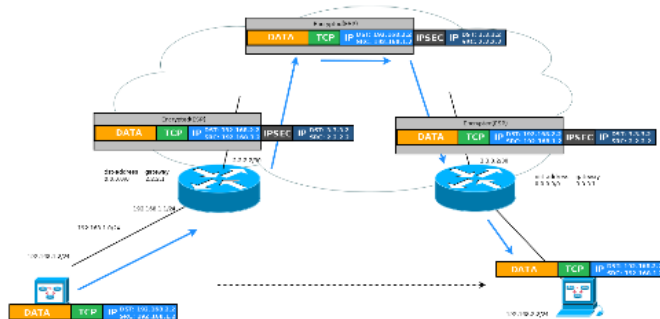
IPSec Transport mode - Wrong shema! (not right)

используется для установления соединения между хостами (или маршрутизаторами)



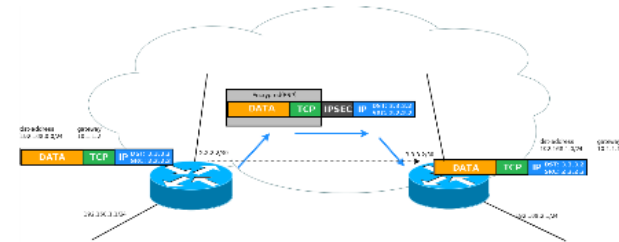
IPSec Tunnel mode

В туннельном режиме шифруется весь исходный IP-пакет, используется для подключения удалённых компьютеров к виртуальной частной сети



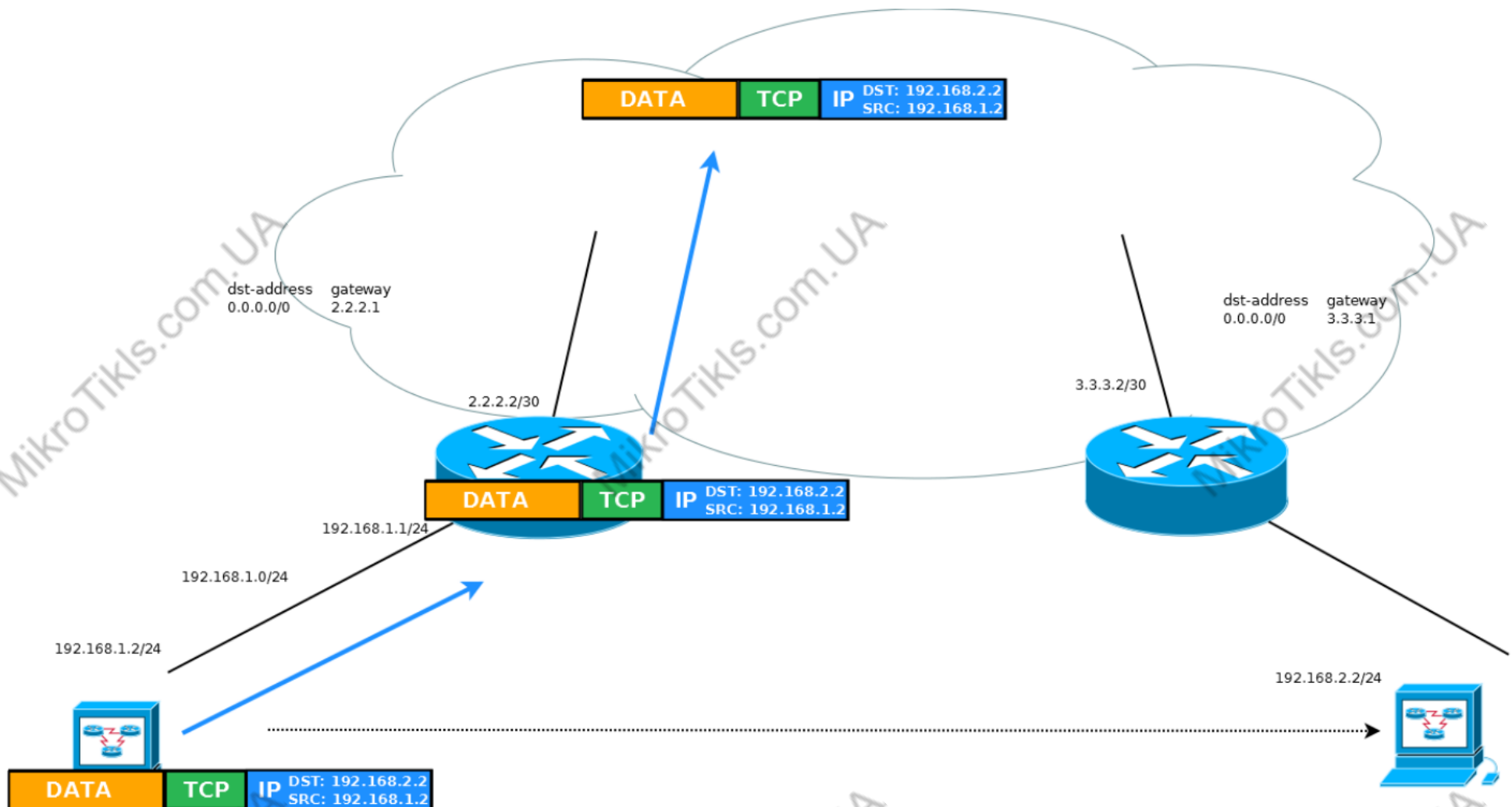
IPSec Transport mode

используется для установления соединения между хостами (или маршрутизаторами)



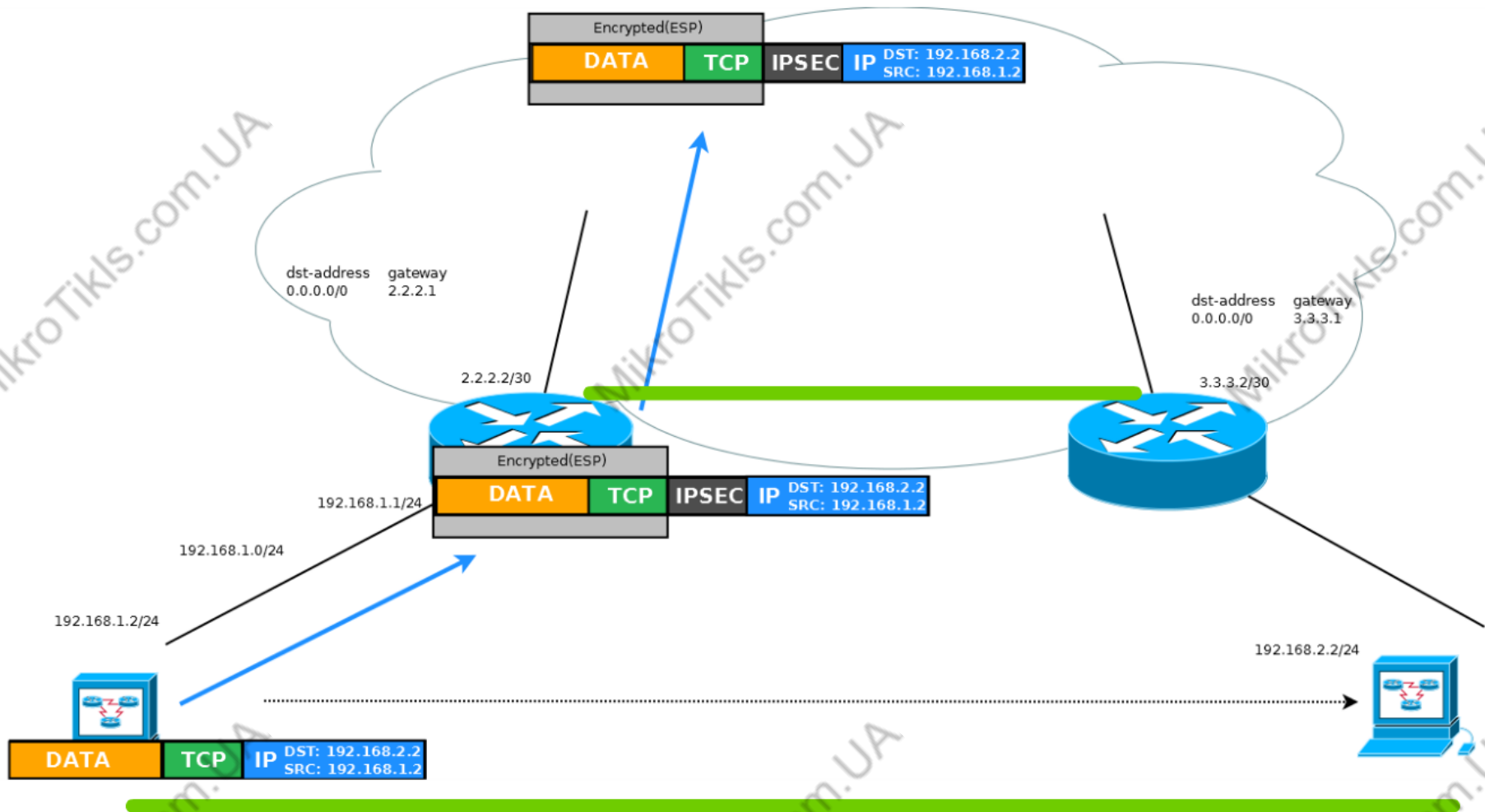
Routing without IPSec

if IPSec then Tunnel mode or Transport mode?



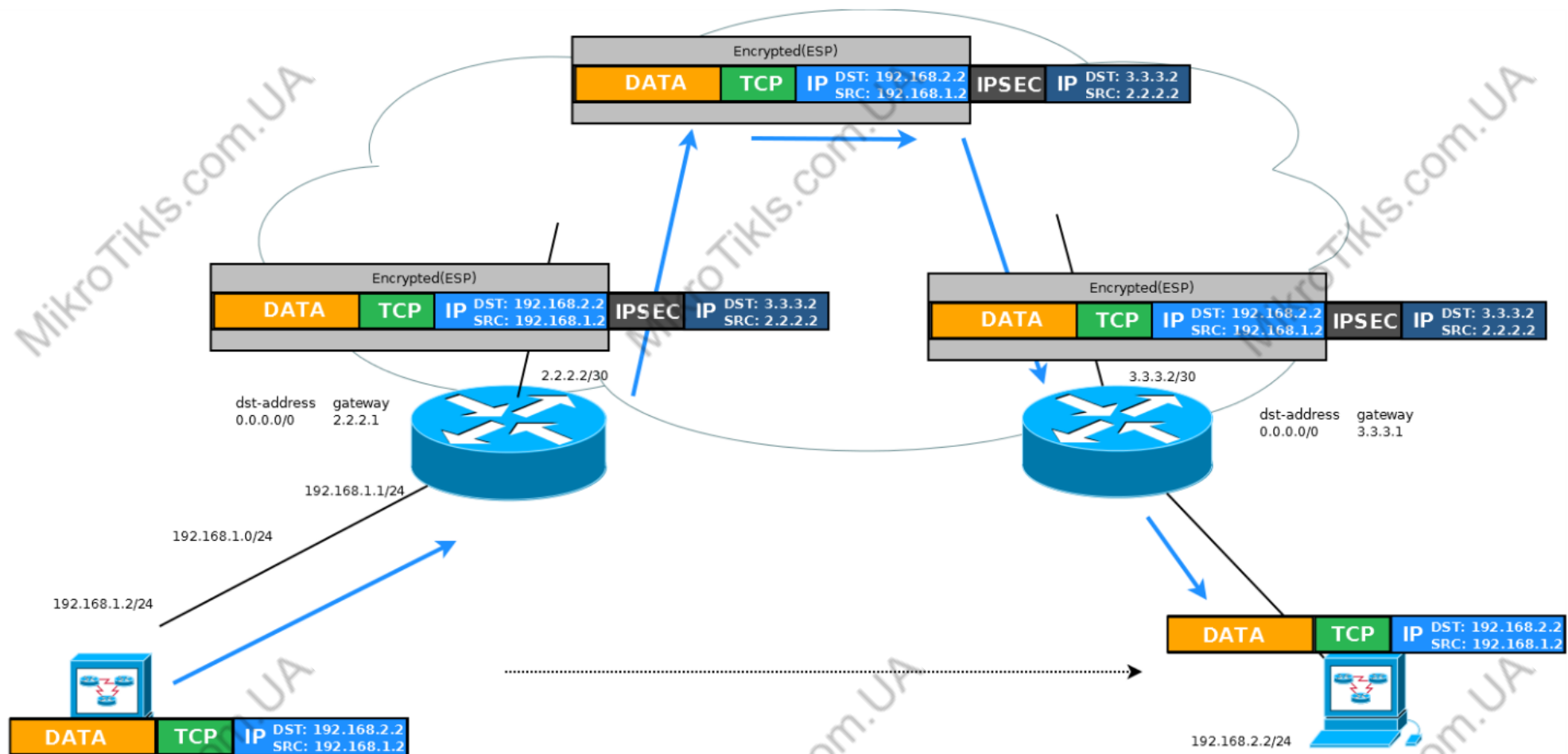
IPSec Transport mode - Wrong shema! (not right)

используется для установления соединения между
хостами (или маршрутизаторами)



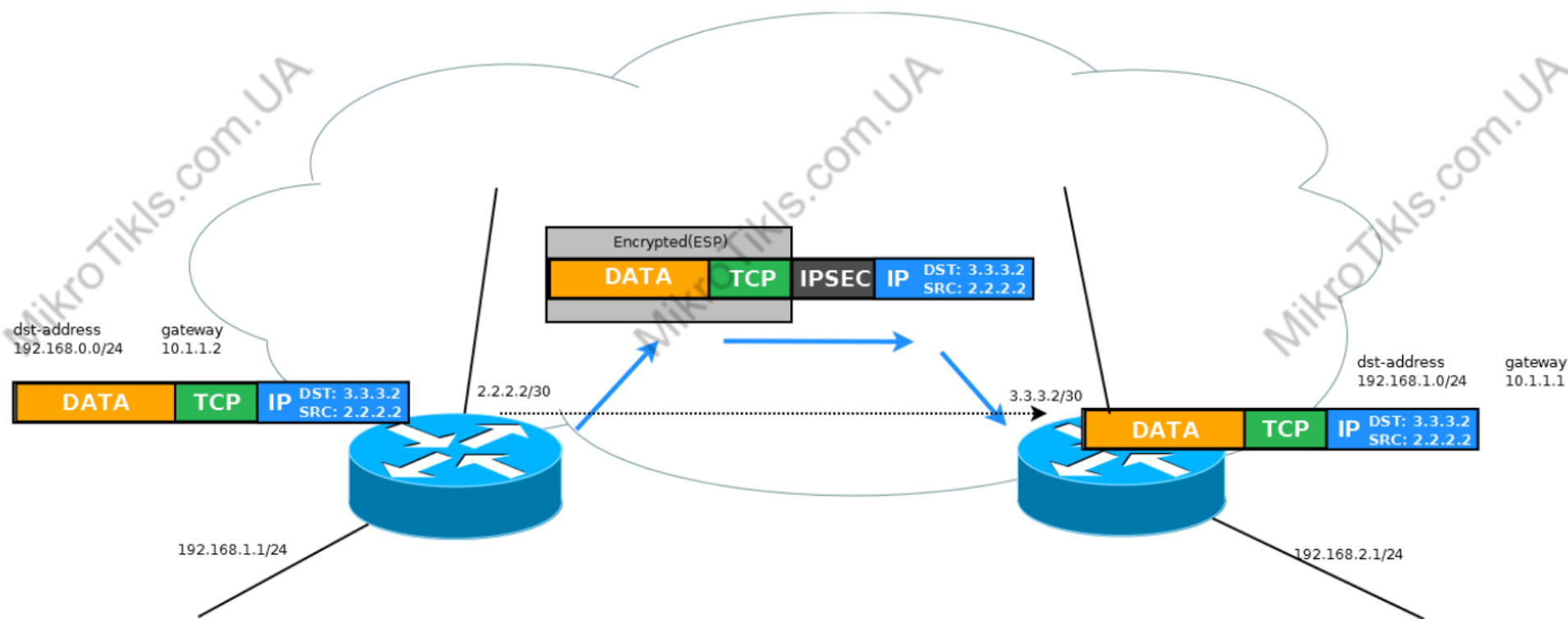
IPSec Tunnel mode

В туннельном режиме шифруется весь исходный IP-пакет, используется для подключения удалённых компьютеров к виртуальной частной сети



IPSec Transport mode

используется для установления соединения между
хостами (или маршрутизаторами)



IPSec, протоколы

протоколы защиты передаваемых данных (**AH, ESP**)

протоколы обмена ключами (**IKE**) Internet Key Exchanger

Функции IKE:

- Установление SA (Security Association, сеансов IPsec)
- Определение параметров безопасности
- Использует UDP-порт 500 (UDP-4500*)
- Обмен ключам
- Пять вариантов переговоров IKE:
 - - Два режима (агрессивный и основной режим)
 - - Три метода аутентификации (pre-shared, public key encryption, and public key signature)

аутентифицировать друг друга, сгенерировать и обменяться общими ключами (через не публичную сеть), установить какой трафик шифровать (от какого отправителя и к какому получателю), договориться с помощью каких протоколов шифровать, а с помощью каких — аутентифицировать

Работа IKE:

- Фаза 1
- Фаза 2

SA (Security Association)

- "ассоциация безопасности - или связь" - это термин IPSec для обозначения соединения.
- При настроенном VPN, для каждого используемого протокола создаётся одна SA пара (т.е. одна пара для АН и одна для ESP).
- SA создаются парами, т.к. каждая SA - это однонаправленное соединение, а данные необходимо передавать в двух направлениях.
- Полученные SA пары хранятся на каждом узле. Если ваш узел имеет SA, значит VPN туннель был установлен успешно.
- Каждый SA имеет уникальный номер, позволяющий определить к какому узлу он относится - SPI (Security Parameter Index) или индекс параметра безопасности.
- Для автоматического установления SA используется IKE

Параметры SA: индекс параметра безопасности SPI, адрес приемника, идентификатор протокола безопасности (АН или ESP), алгоритм безопасности, методы аутентификации, обмена ключами, шифрования, режим протокола (транспортный или туннельный), таймеры и т.д.

IKE фаза 1 и фаза 2

IKE Фаза 1

- Establish a secure channel (ISAKMP SA)
- Using either main mode or aggressive mode
- Authenticate computer identity using certificates or pre-shared secret

Main Mode (6 сообщений),
Aggressive Mode (3 сообщения)

- authentication method
- DH group
- encryption algorithm
- exchange mode
- hash algorithm
- NAT-T
- DPD and lifetime (optional)

создается SA первой Фазы - Phase 1 SA
(также называемый IKE SA)

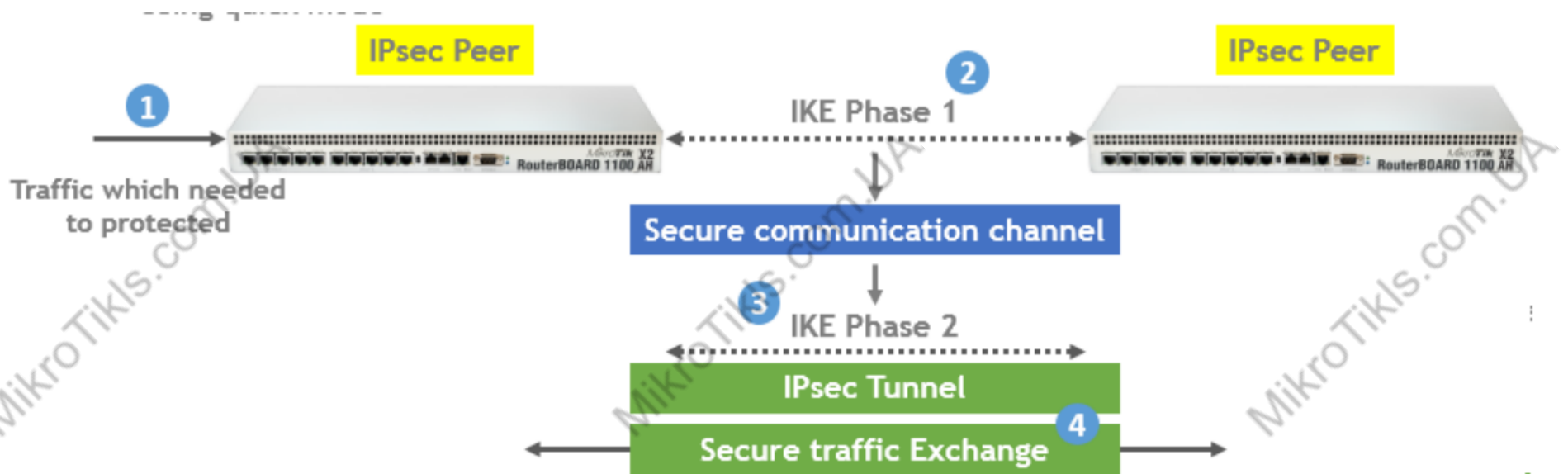
IKE Фаза 2

На этом этапе ISAKMP ответственен за обмен сессионными ключами и согласование политик безопасности (SA) для обеспечения конфиденциальности и целостности пользовательского трафика (Establishes a secure channel between computers intended for the transmission of data (IPsec SA))

- Ipsec protocol
- mode (tunnel or transport)
- authentication method
- PFS (DH) group
- lifetime

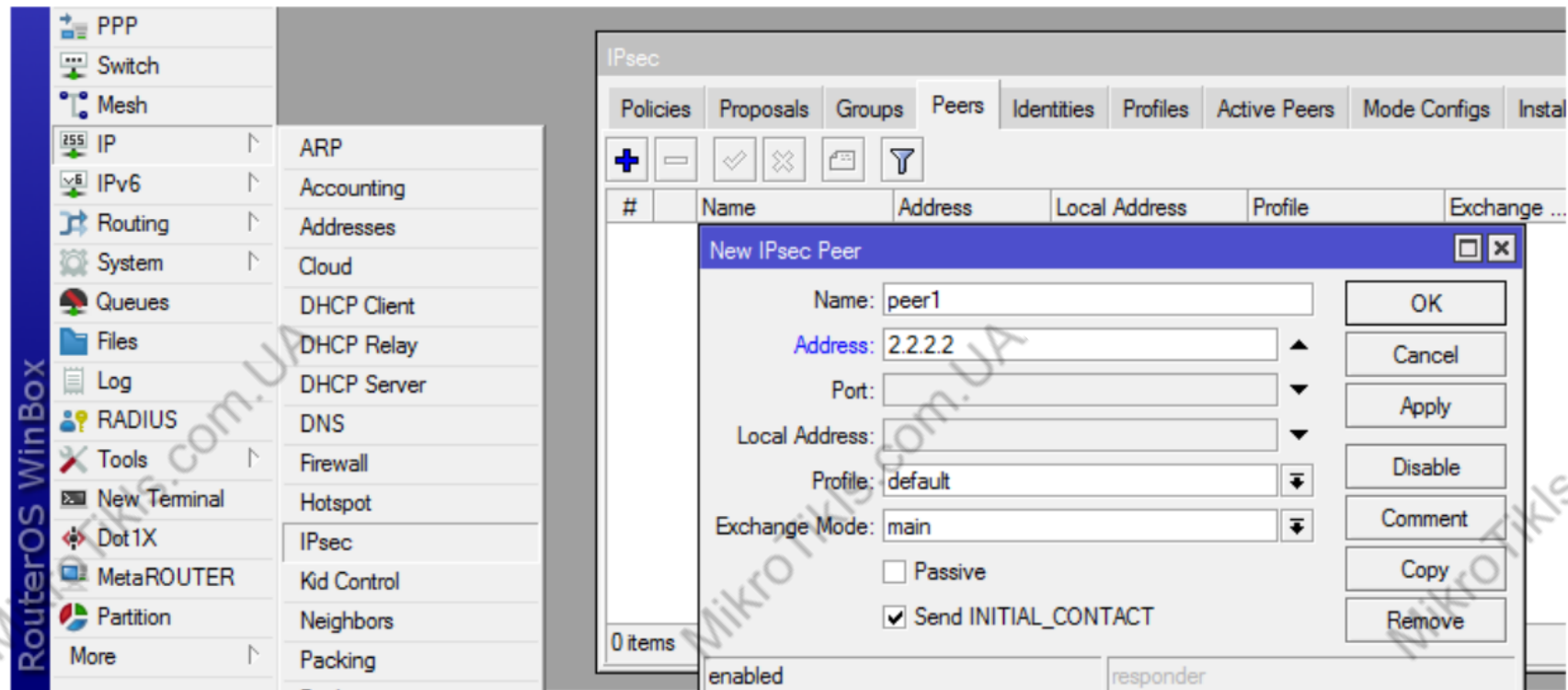
Правильное завершение второй фазы приводит к появлению Phase 2 SA или IPsec SA, и на этом установка туннеля считается завершённой

IPSec simple shema



IPsec Peers

/ip ipsec peer



- Настройки конфигурации Peers используются для установления соединений между демонами IKE.
- Затем это соединение будет использоваться для согласования ключей и алгоритмов для SA.
- С одним пиром может быть несколько SA

IPsec Peers and Identities

/ip ipsec peer

/ip ipsec identity

IPsec

Policies Proposals Groups Peers Identities Profiles Active Peers Mode Configs Insta

+ - ✓ ✗ [icon] [icon]

#	Name	Address	Local Address	Profile	Exchange ..
New IPsec Peer					
Name: peer1					
Address: 2.2.2.2					
Port:					
Local Address:					
Profile: default					
Exchange Mode: main					
<input type="checkbox"/> Passive					
<input checked="" type="checkbox"/> Send INITIAL_CONTACT					
OK					
Cancel					

0 items

enabled responder

IPsec

Policies Proposals Groups Peers Identities Profiles Active Peers Mode Configs Installed SAs Keys

+ - ✓ ✗ [icon] [icon] Settings

#	Peer	Auth. Method	Username	Remote ID	Mode Configuration
0	peer1	pre shared key			

1 item (1 selected)

IPsec Identity <peer1>

Peer: peer1

Auth. Method: pre shared key

Secret: 123123123

Policy Template Group: default

Notrack Chain:

My ID Type: auto

Remote ID Type: auto

Match By: remote id

OK

Cancel

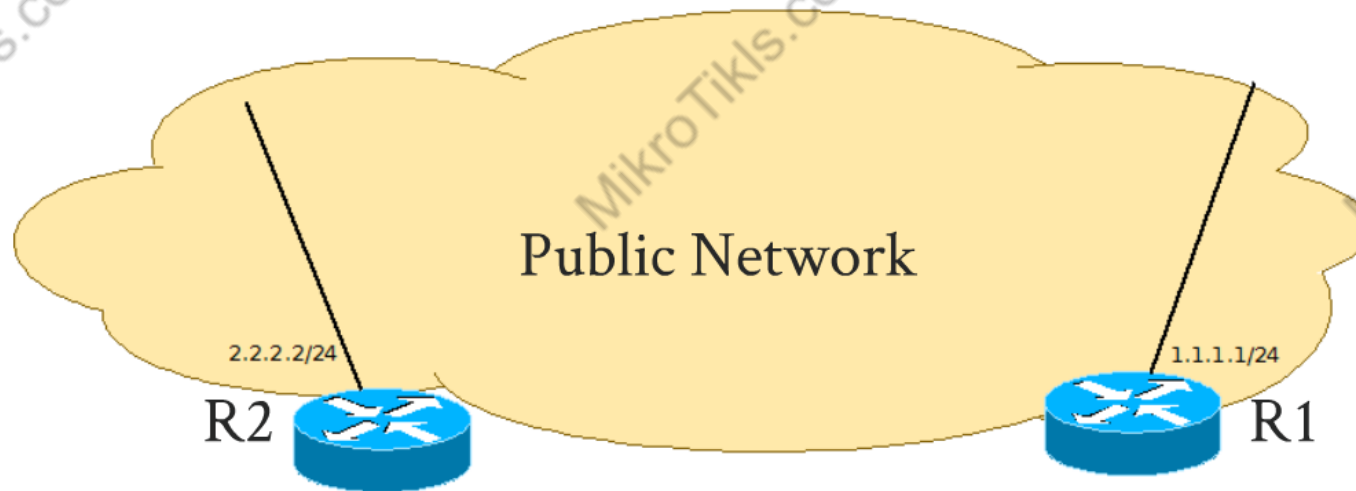
Apply

Disable

Comment

Copy

Remove



```
/ip ipsec peer
add address=1.1.1.1/32 name=peerR1
```

```
/ip ipsec identity
add peer=peerR1 secret=123123123
```

```
/ip ipsec peer
add address=2.2.2.2/32 name=peerR2
```

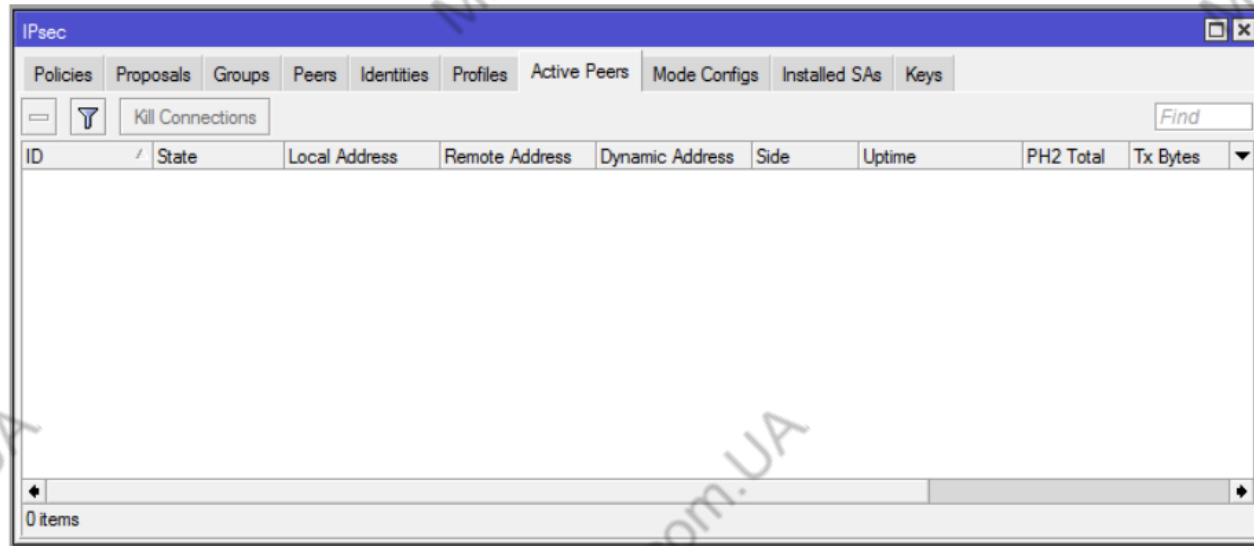
```
/ip ipsec identity
add peer=peerR2 secret=123123123
```

peer - most specific (largest netmask)

IPsec				
Policies Proposals Groups Peers Identities Profiles Active Peers				
<div> <div>+</div> <div>-</div> <div>✓</div> <div>✗</div> <div>📄</div> <div>🔍</div> </div>				
#	Name	Address	Local Address	Profile
0 R	peer4	2.2.2.0/27		default
1 R	peer3	2.2.2.0/26		default
2 R	peer2	2.2.2.0/25		default
3 R	peer1	2.2.2.0/24		default

IPsec Peers - status

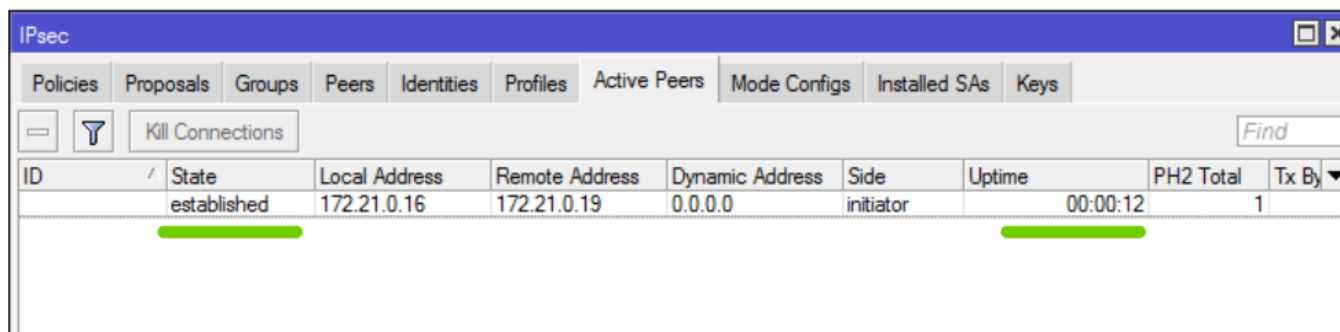
/ip ipsec active-peers



The screenshot shows the Mikrotik WinBox interface for the IPsec configuration. The 'Active Peers' tab is selected. The table below the tabs is empty, indicating no active peers are currently connected. The status bar at the bottom of the table area shows '0 items'.

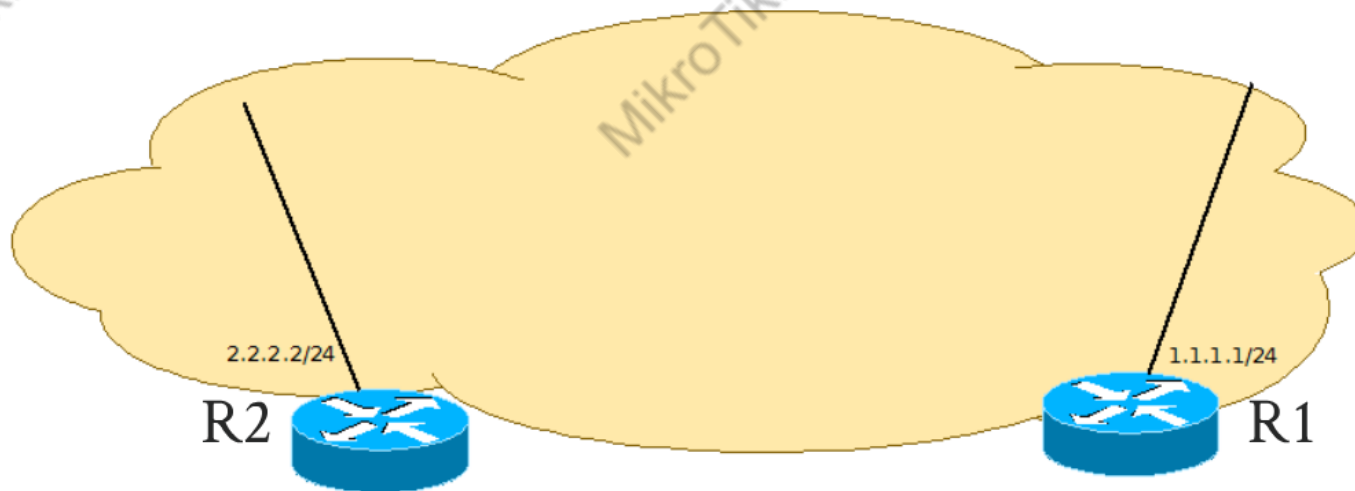
ID	State	Local Address	Remote Address	Dynamic Address	Side	Uptime	PH2 Total	Tx Bytes
----	-------	---------------	----------------	-----------------	------	--------	-----------	----------

результат 1 фазы - активный Peer, если нет - то проверяем - настройки peer, настройки идентификации, profiles - алгоритмы и т.д. Настройки Firewall filter



The screenshot shows the Mikrotik WinBox interface for the IPsec configuration. The 'Active Peers' tab is selected. The table below the tabs shows one active peer in the 'established' state. The 'State' and 'Uptime' columns are highlighted with green bars.

ID	State	Local Address	Remote Address	Dynamic Address	Side	Uptime	PH2 Total	Tx Bytes
	established	172.21.0.16	172.21.0.19	0.0.0.0	initiator	00:00:12	1	



```
/ip ipsec peer  
add address=1.1.1.1/32 name=peerR1
```

```
/ip ipsec identity  
add peer=peerR1 secret=123123123
```

```
/ip ipsec peer  
add address=2.2.2.2/32 name=peerR2
```

```
/ip ipsec identity  
add peer=peerR2 secret=123123123
```

Кто к кому соединяется? (как это регулировать?)

Какой порт(ы) открыть в Firewall?

IPSec Peers

/ip ipsec peer

New IPsec Peer

Name: peer1

Address: 5.5.5.5

Port:

Local Address:

Profile: default

Exchange Mode: main

☐ Passive

☒ Send INITIAL_CONTACT

OK

Cancel

Apply

Disable

Comment

Copy

Remove

enabled responder

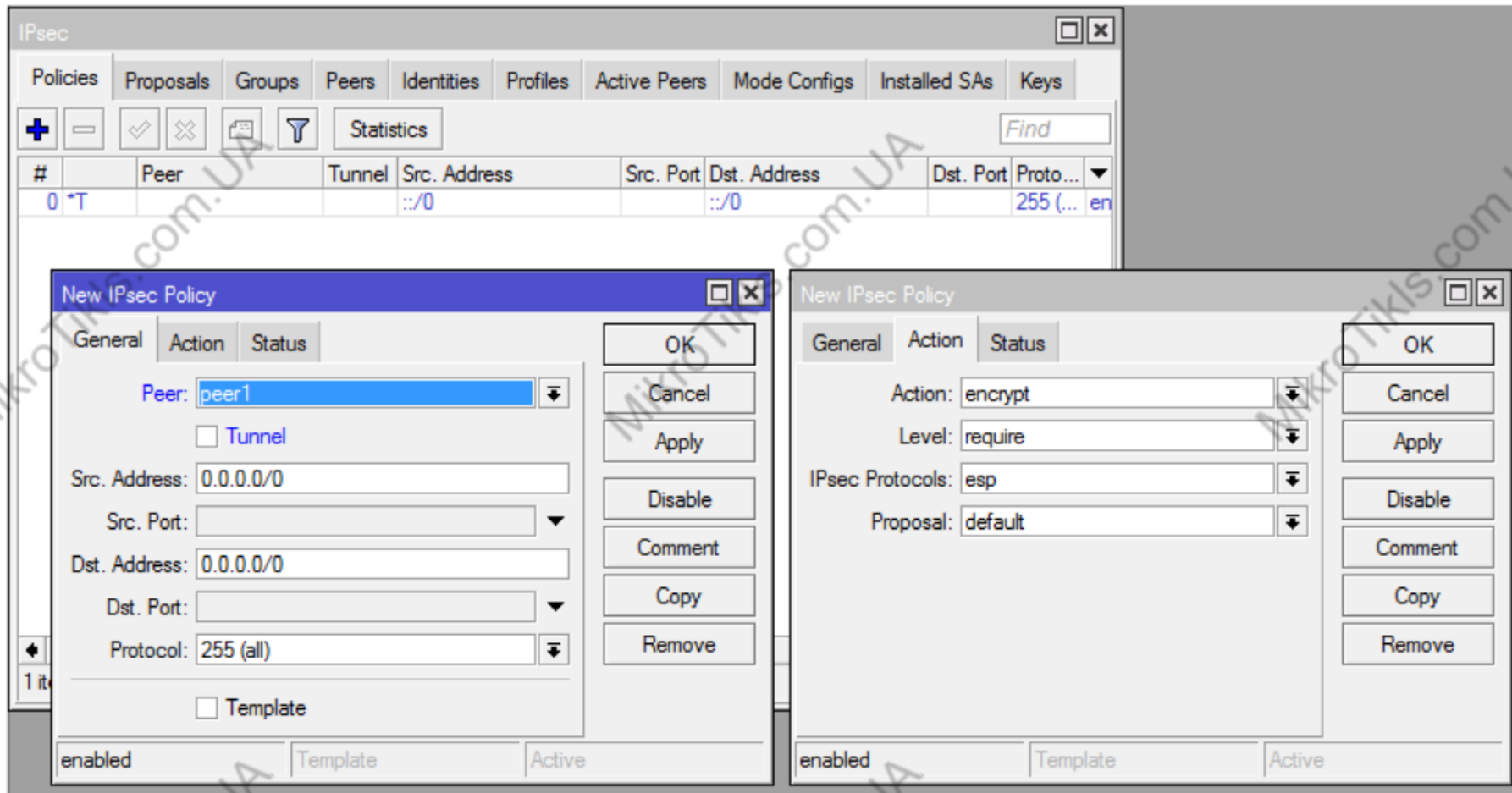
Passive - когда пассивный режим включен, то с этим пиром будет ждать, пока он иницирует соединение IKE (мы не будем с ним иницировать соединение)

Local Address - с какого src адреса необходимо взаимодействовать с данным пиром.

IPsec Policies

/ip ipsec policy

Таблица политик использующаяся для определения того, следует ли применять параметры безопасности к пакету.

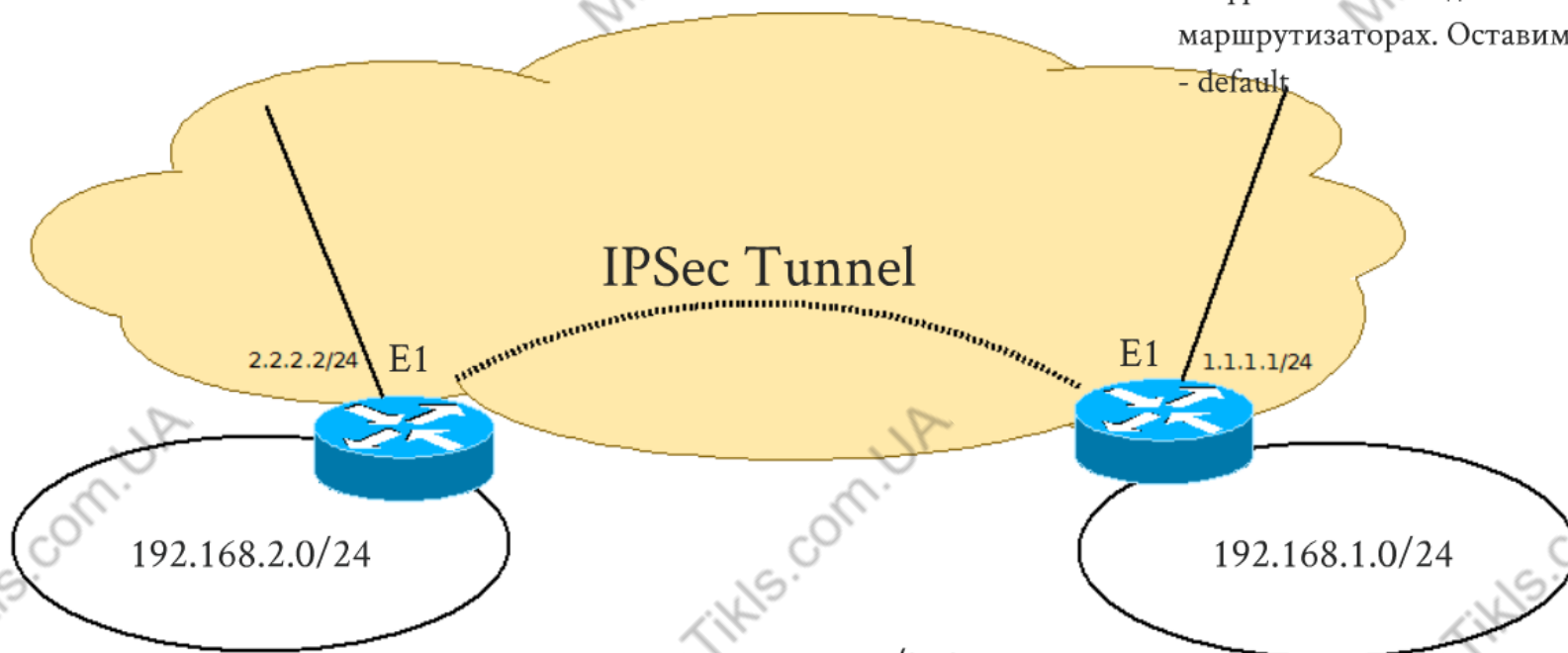


принцип - IF (General) - To(Action)

IPSec Tunnel Mode

Policy - Сценарий 1

/ip ipsec proposal - Для следующих шагов важно, чтобы предлагаемые алгоритмы аутентификации и шифрования совпадали на обоих маршрутизаторах. Оставим дефолтные - default



```
/ip ipsec peer  
add address=1.1.1.1 name=peer16  
/ip ipsec identity  
add peer=peer16 secret=1234567890
```

```
/ip ipsec policy  
add peer=peer16 src-address=192.168.2.0/24 dst-  
address=192.168.1.0/24 tunnel=yes
```

```
/ip ipsec peer  
add address=2.2.2.2 name=peer19  
/ip ipsec identity  
add peer=peer19 secret=1234567890
```

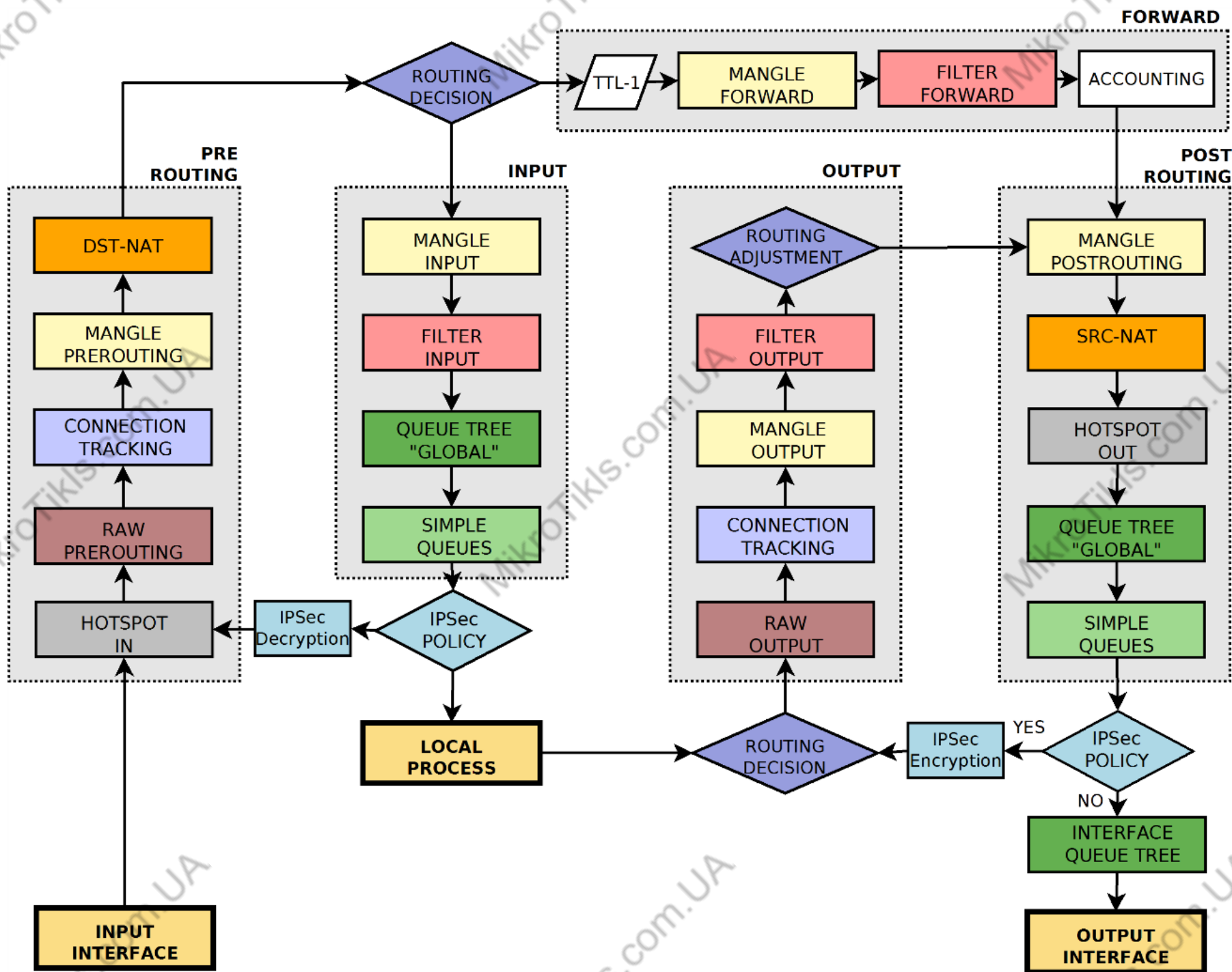
```
/ip ipsec policy  
add peer=peer16 src-address=192.168.1.0/24 dst-  
address=192.168.2.0/24 tunnel=yes
```

сколько SA? на каждом маршрутизаторе: /ip ipsec installed-sa print
работает? SRC-NAT?

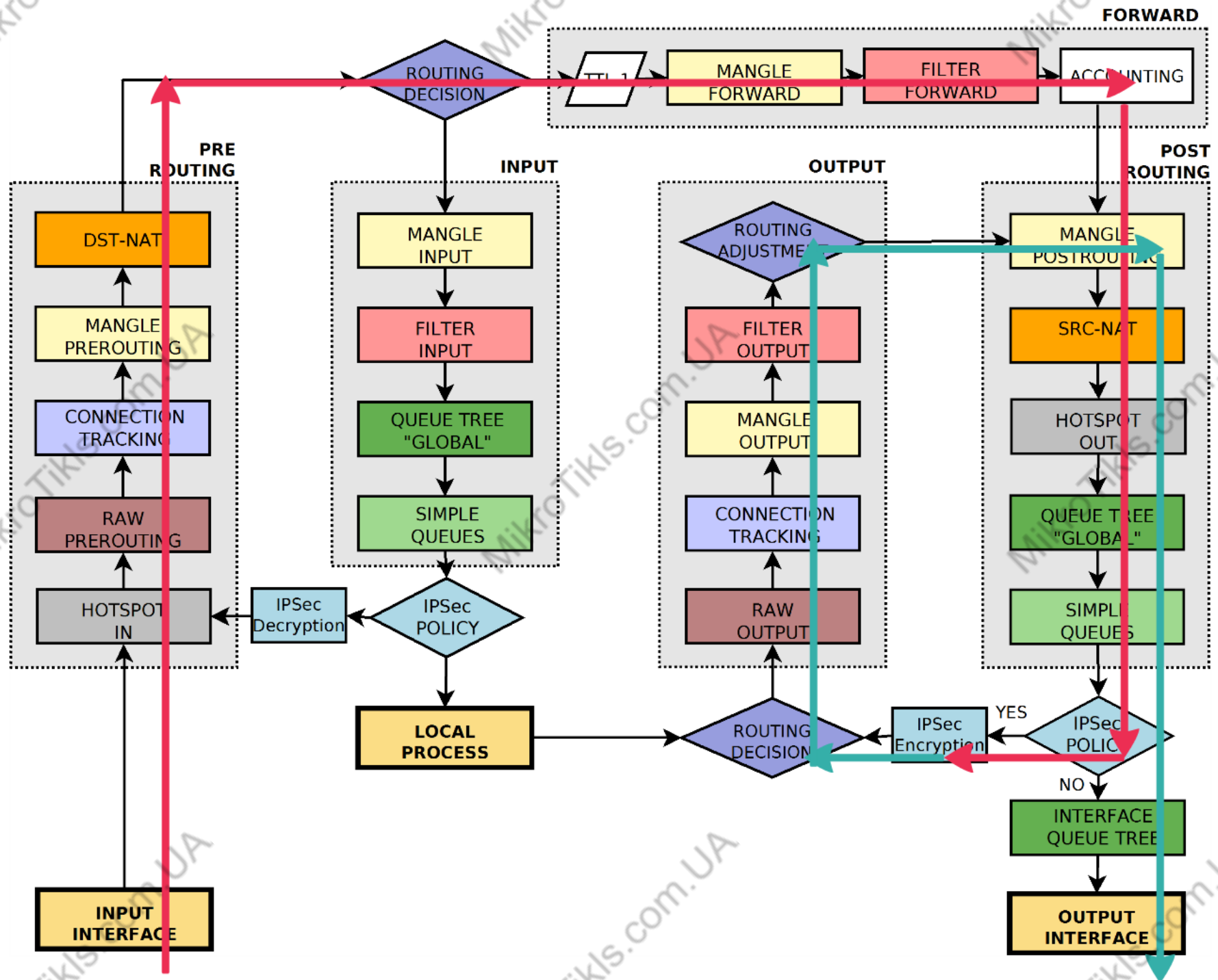
IPsec											
Policies Proposals Groups Peers Identities Profiles Active Peers Mode Configs Installed SAs Keys											
<div> </div> <div>Statistics</div> <div>Find</div>											
#	Peer	Tunnel	Src. Address	Src. Port	Dst. Address	Dst. Port	Proto...	Action	Level	PH2 State	
0	T		::/0		::/0		255 (...)	encrypt			
1	A peer19	yes	192.168.1.0/24		192.168.2.0/24		255 (...)	encrypt	require	established	

IPsec							
Policies Proposals Groups Peers Identities Profiles Active Peers Mode Configs Installed SAs Keys							
<div> </div> <div>Flush</div>							
	SPI	Src. Address	Dst. Address	Auth....	Encr....	Encr....	Current B...
E	46755c7	172.21.0.19	172.21.0.16	sha1	aes c...	256	0
E	74dd5a5	172.21.0.16	172.21.0.19	sha1	aes c...	256	0

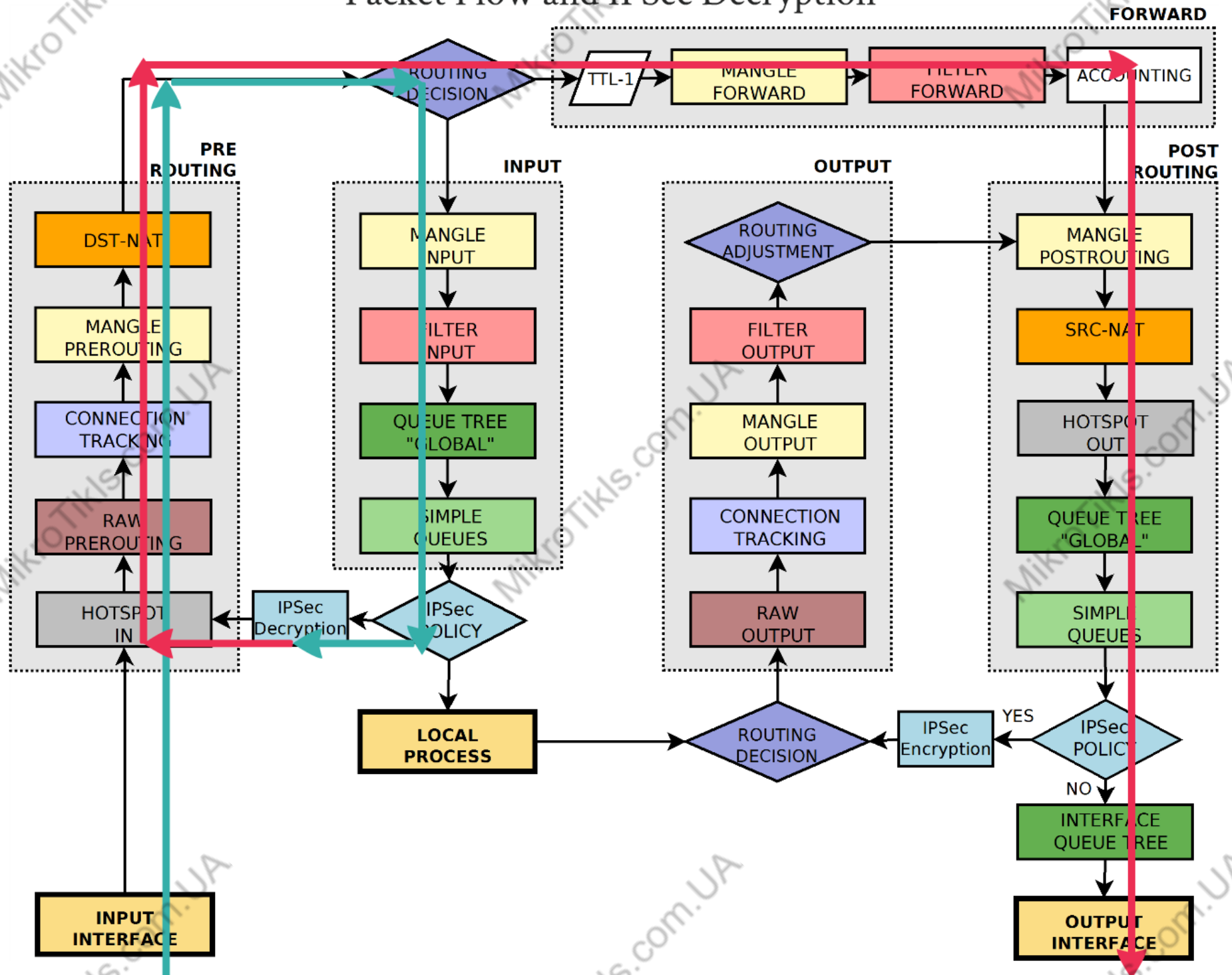
Packet Flow and IPsec



Packet Flow and IPsec Encryption



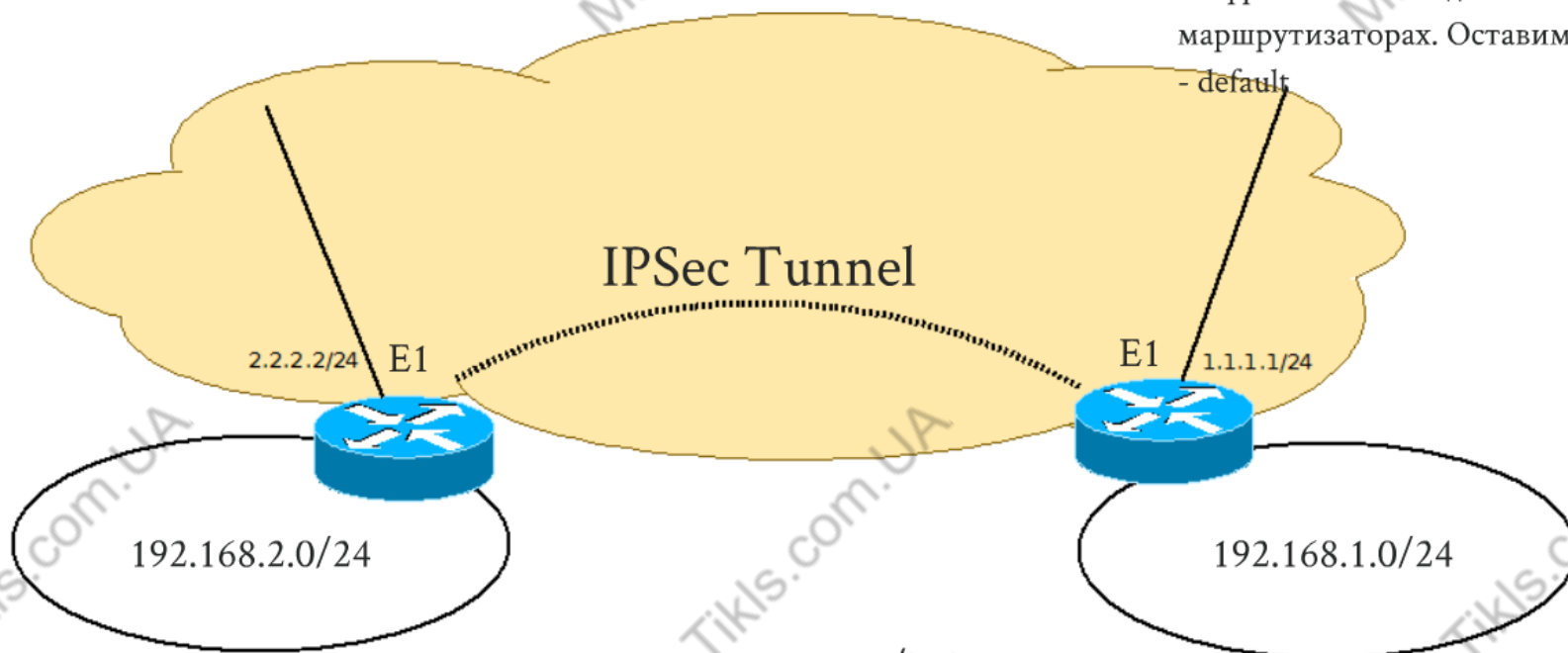
Packet Flow and IPSec Decryption



IPSec Tunnel Mode

Policy - Сценарий 1

/ip ipsec proposal - Для следующих шагов важно, чтобы предлагаемые алгоритмы аутентификации и шифрования совпадали на обоих маршрутизаторах. Оставим дефолтные - default



```
/ip ipsec peer  
add address=1.1.1.1 name=peer16  
/ip ipsec identity  
add peer=peer16 secret=1234567890
```

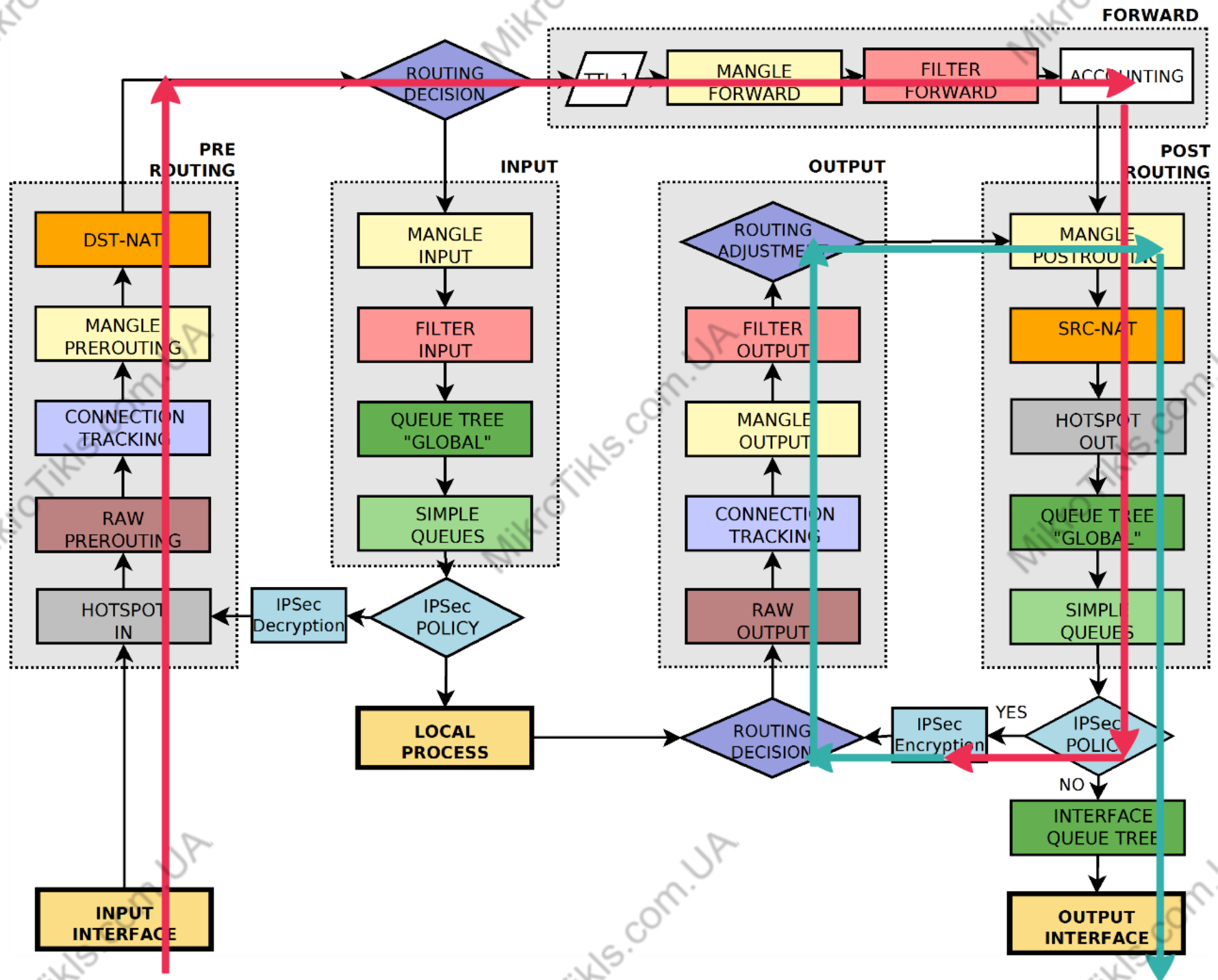
```
/ip ipsec policy  
add peer=peer16 src-address=192.168.2.0/24 dst-  
address=192.168.1.0/24 tunnel=yes
```

```
/ip ipsec peer  
add address=2.2.2.2 name=peer19  
/ip ipsec identity  
add peer=peer19 secret=1234567890
```

```
/ip ipsec policy  
add peer=peer16 src-address=192.168.1.0/24 dst-  
address=192.168.2.0/24 tunnel=yes
```

сколько SA? на каждом маршрутизаторе: /ip ipsec installed-sa print
работает? SRC-NAT?

Packet Flow and IPsec Encryption



IPSec and NAT

- На этом этапе, если вы попытаетесь отправить трафик через туннель IPSec, он не будет работать, пакеты будут потеряны.
- Это связано с тем, что если оба маршрутизатора имеют правила NAT (маскарад) (src-nat out-interface=ether1 action=masquerade, которые меняют адрес источника до того, как пакет используется политики шифрования (цепочка src-nat срабатывает раньше чем происходит ipsec-encryption).
- Маршрутизатор не может зашифровать пакет, поскольку адрес источника не соответствует адресу, указанному в конфигурации политики.
- Чтобы исправить это, нам нужно настроить правило обхода SNAT (или..).

R2 /ip firewall nat

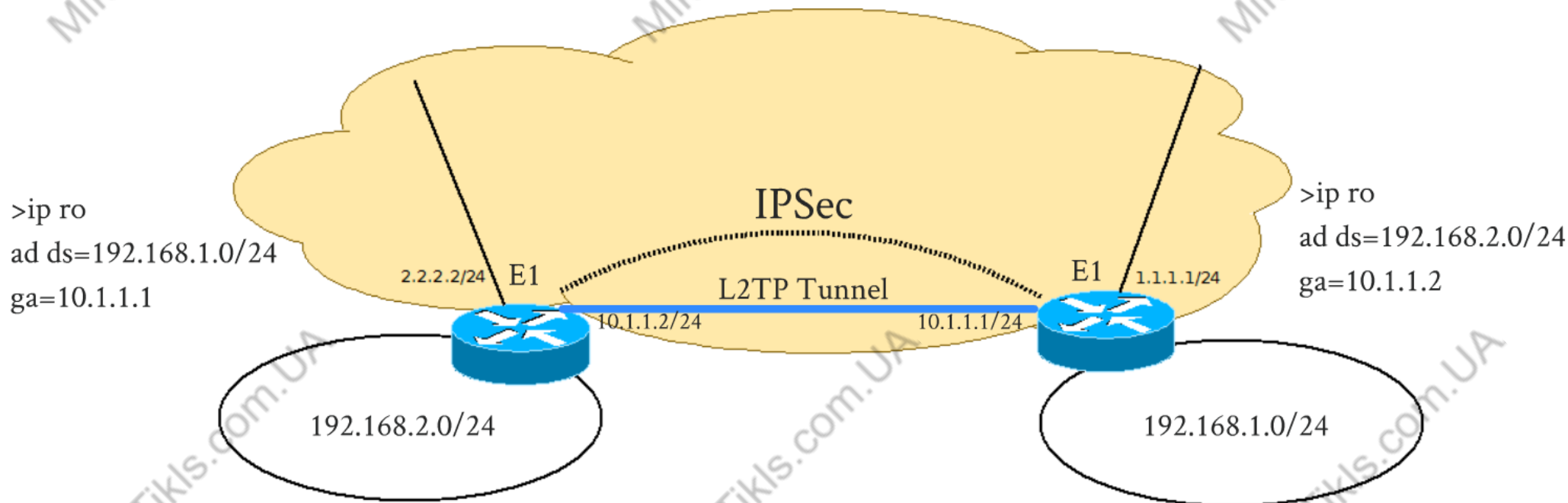
```
add chain=srcnat action=accept place-before=0 \  
src-address=192.168.2.0/24 dst-address=192.168.1.0/24
```

R1: /ip firewall nat

```
add chain=srcnat action=accept place-before=0 \  
src-address=192.168.1.0/24 dst-address=192.168.2.0/24
```

для гибкости используйте поля IPsec Policy в
Firewall filter, nat, mangle, raw

The screenshot shows a configuration window for a Firewall rule. The 'Out. Bridge Port List' field is at the top. Below it, the 'IPsec Policy' field is set to 'in' with a dropdown arrow. To its right, a colon is followed by a field set to 'ipsec' with a dropdown arrow and an up arrow icon. Below these fields is the 'TLS Host' field with a dropdown arrow.



```
>ip ro
ad ds=192.168.1.0/24
ga=10.1.1.1
```

```
>ip ro
ad ds=192.168.2.0/24
ga=10.1.1.2
```

```
/ip ipsec peer
add address=1.1.1.1 name=peer16
/ip ipsec identity
add peer=peer16 secret=1234567890
```

```
/ip ipsec peer
add address=2.2.2.2 name=peer19
/ip ipsec identity
add peer=peer19 secret=1234567890
```

```
/ip ipsec policy
add peer=peer16 dst-address=1.1.1.1 tunnel=no
```

```
/ip ipsec policy
add peer=peer19 dst-address=2.2.2.2 tunnel=no
```

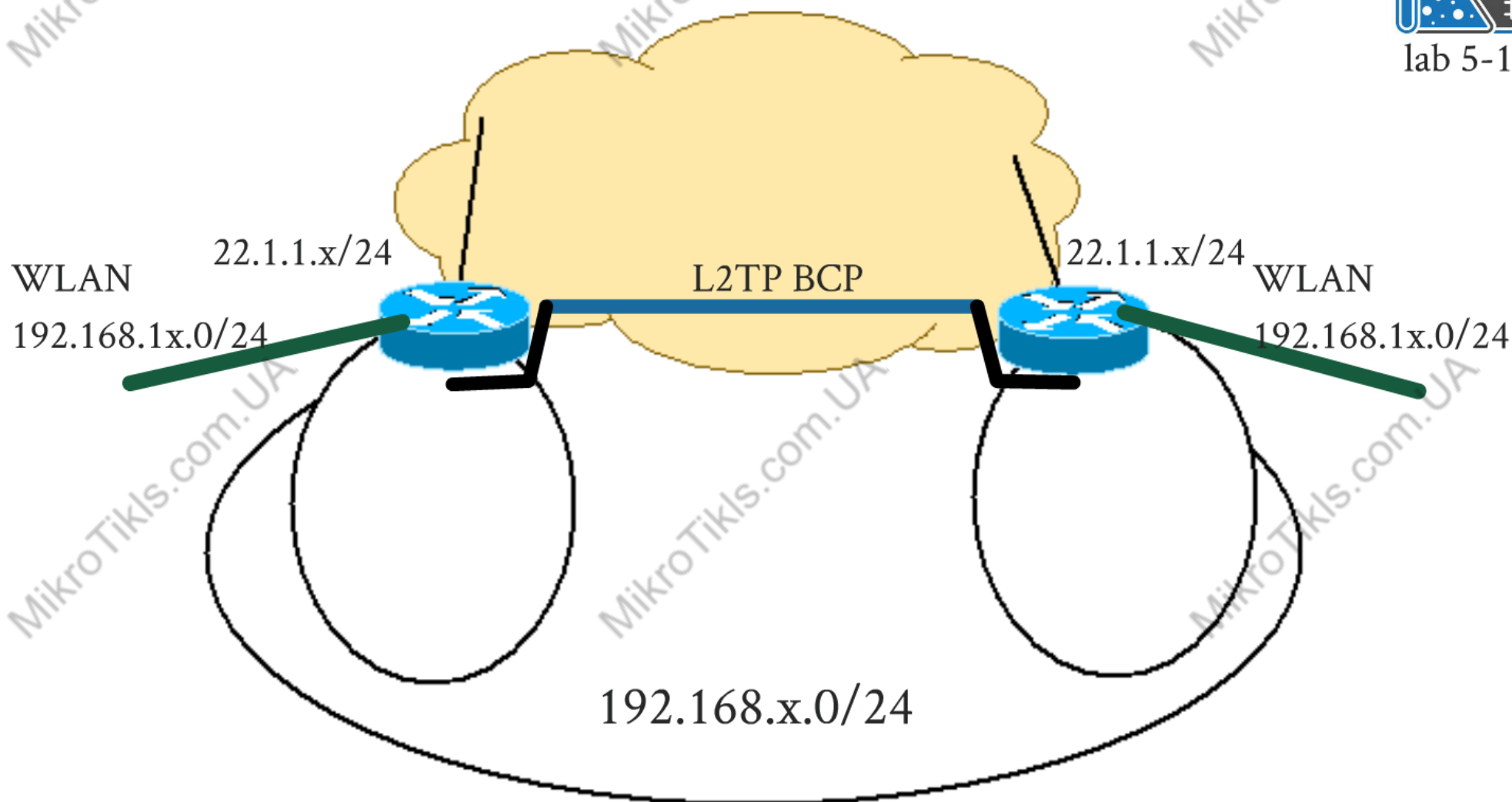
сколько SA? на каждом маршрутизаторе: /ip ipsec installed-sa print

работает? SRC-NAT?

PPP BCP and MLPPP



lab 5-1



- обеспечьте безопасность вашей распределенной broadcast сети используя IPSec
- между локальными сетями LAN2 - поднимите IPSec Tunnel