MikroTik.Me

MikroTik.Me

- Васильев Кирилл
- Санкт-Петербург
- Курсы MikroTik
- Поддержка
- Разработка ПО
- Проекты

IPsec

Кто такой IPsec

- Расширяет маршрутизацию
- Позволяет защитить данные от модификации
- Позволяет шифровать данные

Кто такой IPsec

- **Расширяет маршрутизацию**
- Позволяет защитить данные от модификации
- Позволяет шифровать данные

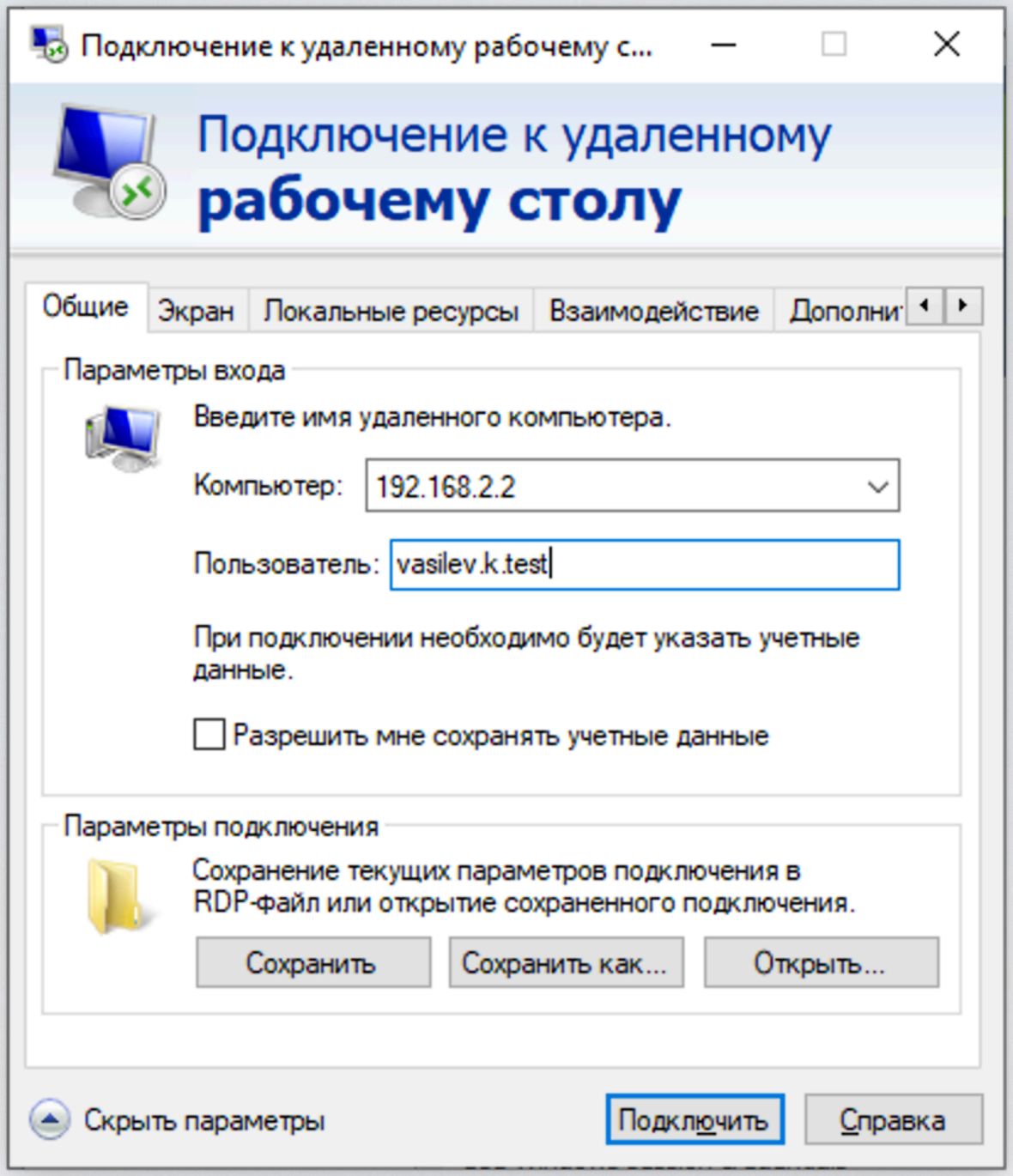
А нужен ли IPsec?

«Зачем, ведь и так большинство трафика шифруется на уровне приложения»

А нужен ли IPsec?

А нужен ли IPsec?

RDP

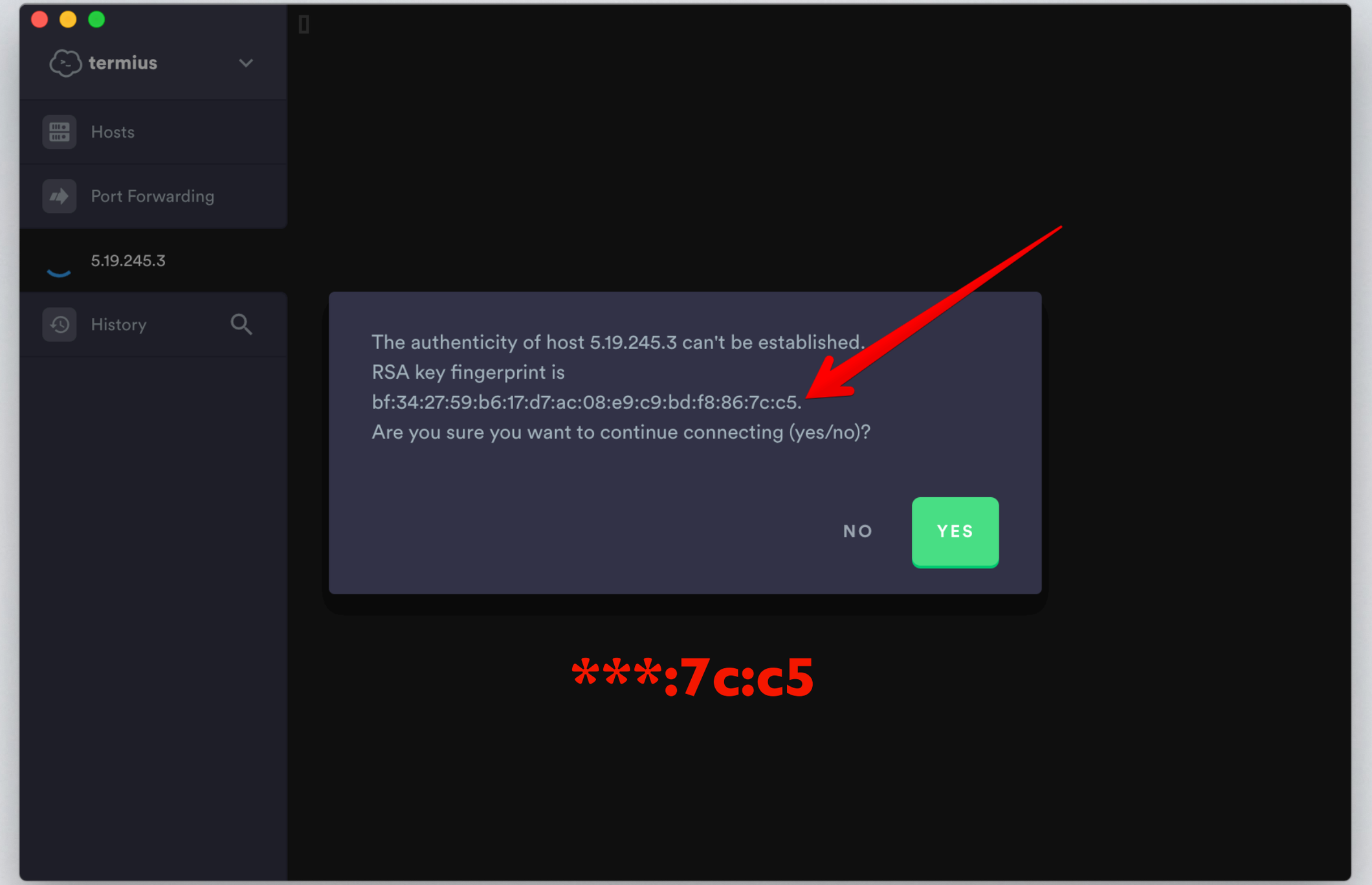


RDP

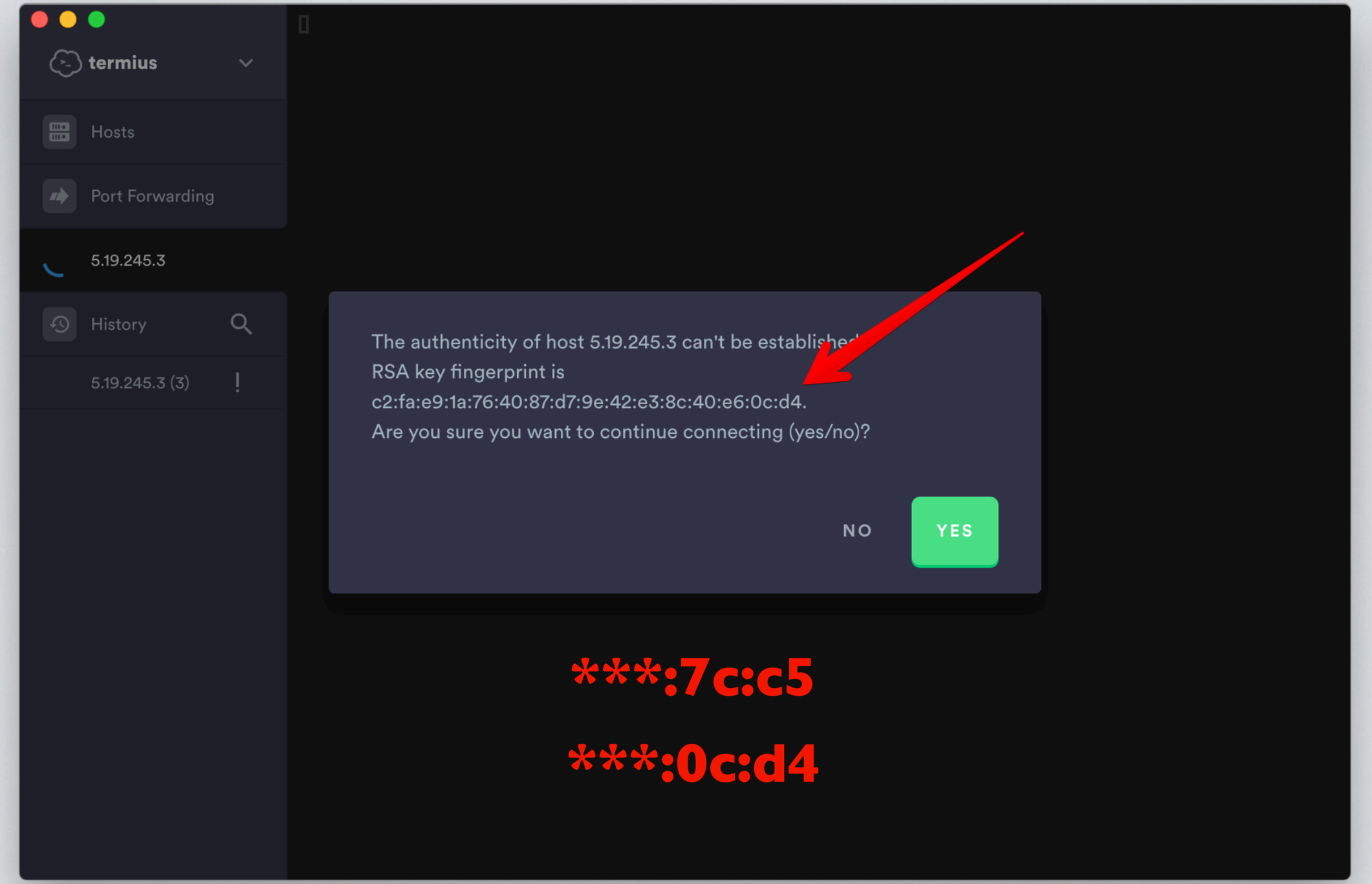
```
▶ Transmission Control Protocol, Src Port: 50770, Dst Port: 3389, Seq: 1, Ack: 1, Len: 47
▼ TPKT, Version: 3, Length: 47
    Version: 3
    Reserved: 0
    Length: 47
▼ ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
    Length: 42
    PDU Type: CR Connect Request (0x0e)
    Destination reference: 0x0000
    Source reference: 0x0000
    0000 .... = Class: 0
    .... ..0. = Extended formats: False
    .... ...0 = No explicit flow control: False
▼ Remote Desktop Protocol
    Routing Token/Cookie: Cookie: mstshash=vasilev.k
    Type: RDP Negotiation Request (0x01)
  ▼ Flags: 0x00
      .... ...0 = Restricted admin mode required: False
      .... 0... = Correlation info present: False
    Length: 8
  ▼ requestedProtocols: 0x0000000b, TLS security supported, CredSSP supported, Early User Authorization Result PDU supported
      .... .... .... .... .... .... .... ...1 = TLS security supported: True
      .... .... .... .... .... .... .... ..1. = CredSSP supported: True
      .... .... .... .... .... .... .... 1... = Early User Authorization Result PDU supported: True
```

Первые 9 символов из MSTSC до 128 freeRDP

SSH



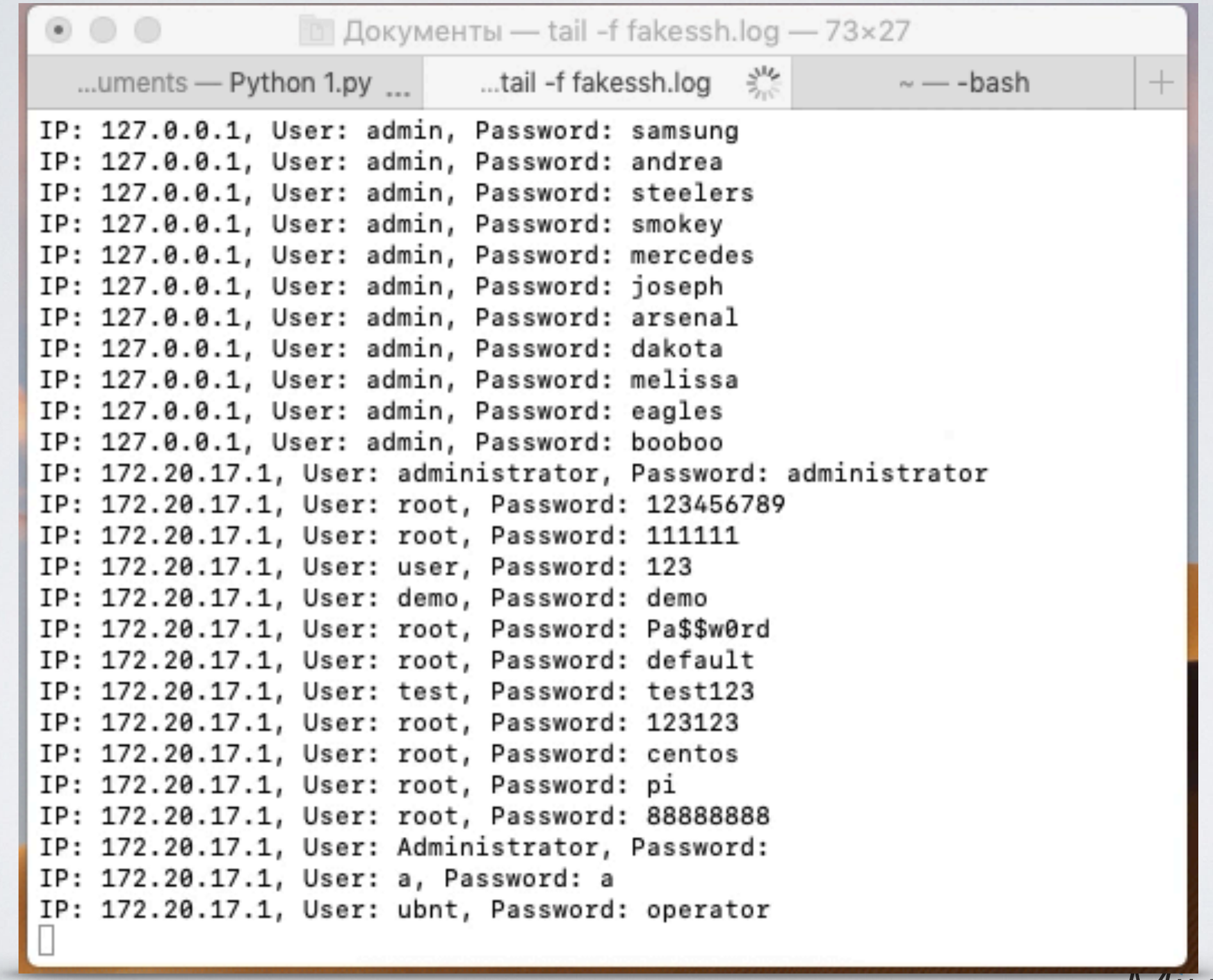
SSH



SSH

- Многие не понимают суть отпечатка ключа
- Гуглят как решить проблему, очисткой известных ключей (**rm ~/.ssh/known_hosts**)
- Некоторый софт пишет, о новом ключе, и даёт подключиться

Fake SSH сервер



Без дефолта

Без дефолта

Без дефолта

```
/ip route
add dst-address=1.1.1.0/24 gateway=3.3.3.1
```

```
/ip ipsec policy
add dst-address=192.168.0.0/24 src-address=192.168.3.0/24 \
tunnel=yes peer=R0
```

Без дефолта

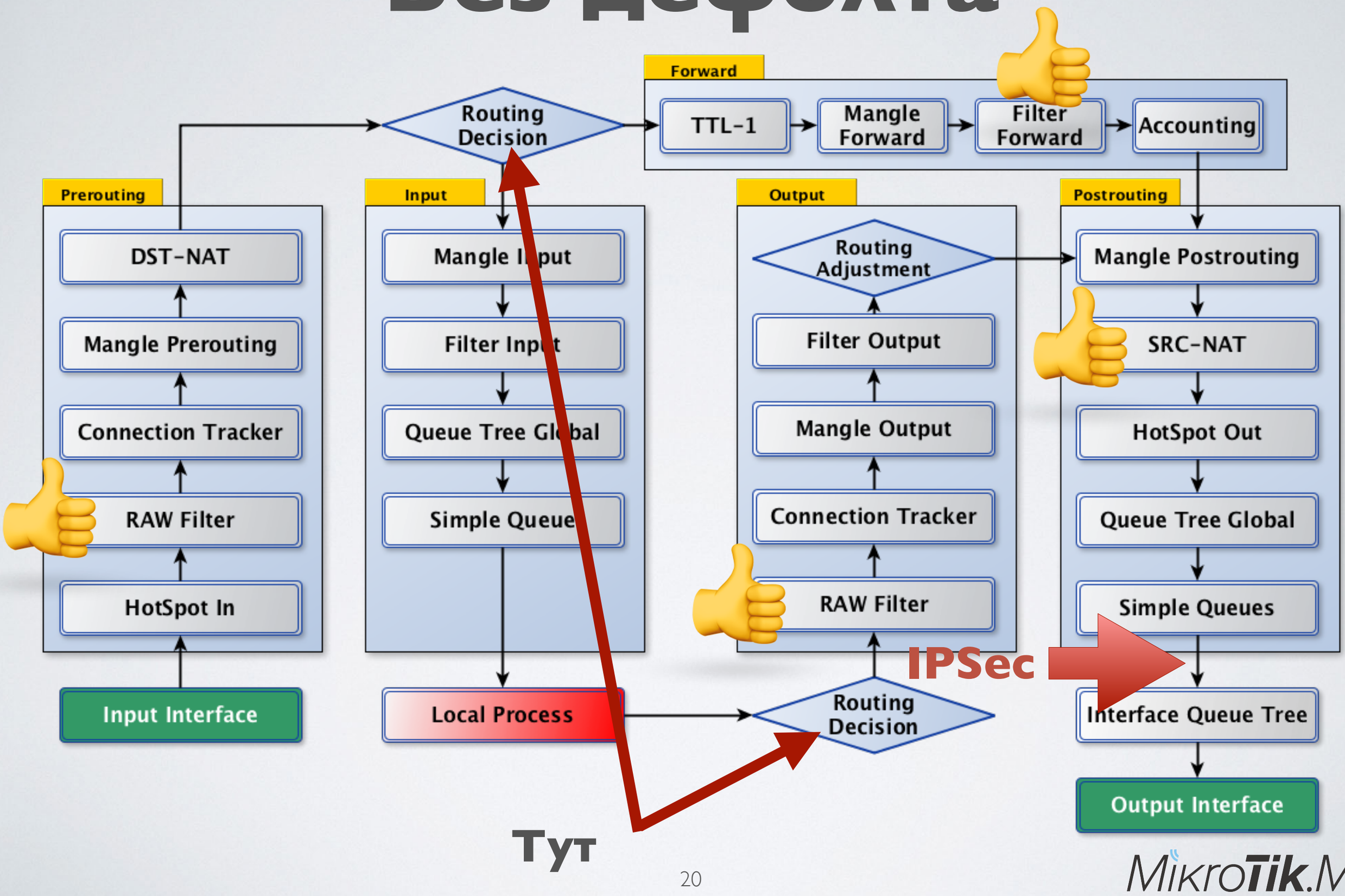
- R0 - настроен правильно
- R3 - настроен правильно
- На R3 фильтр пустой (разрешено всё)
- Проблемы с HAT-ом на R0 и R3 нет
- Вторая фаза согласованна и активна

Без дефолта

Не работает

почему?

Без дефолта



Без дефолта

Route List

Routes | Nexthops | Rules | VRF

Find | all

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
AS	1.1.1.0/24	3.3.3.1 reachable ether1	1		
DAC	3.3.3.0/30	ether1 reachable	0		3.3.3.2
DAC	192.168.3.0/24	Bridge-Local reachable	0		192.168.3.1

3 items

Destination net unreachable

Нет маршрута для 192.168.0.0/24

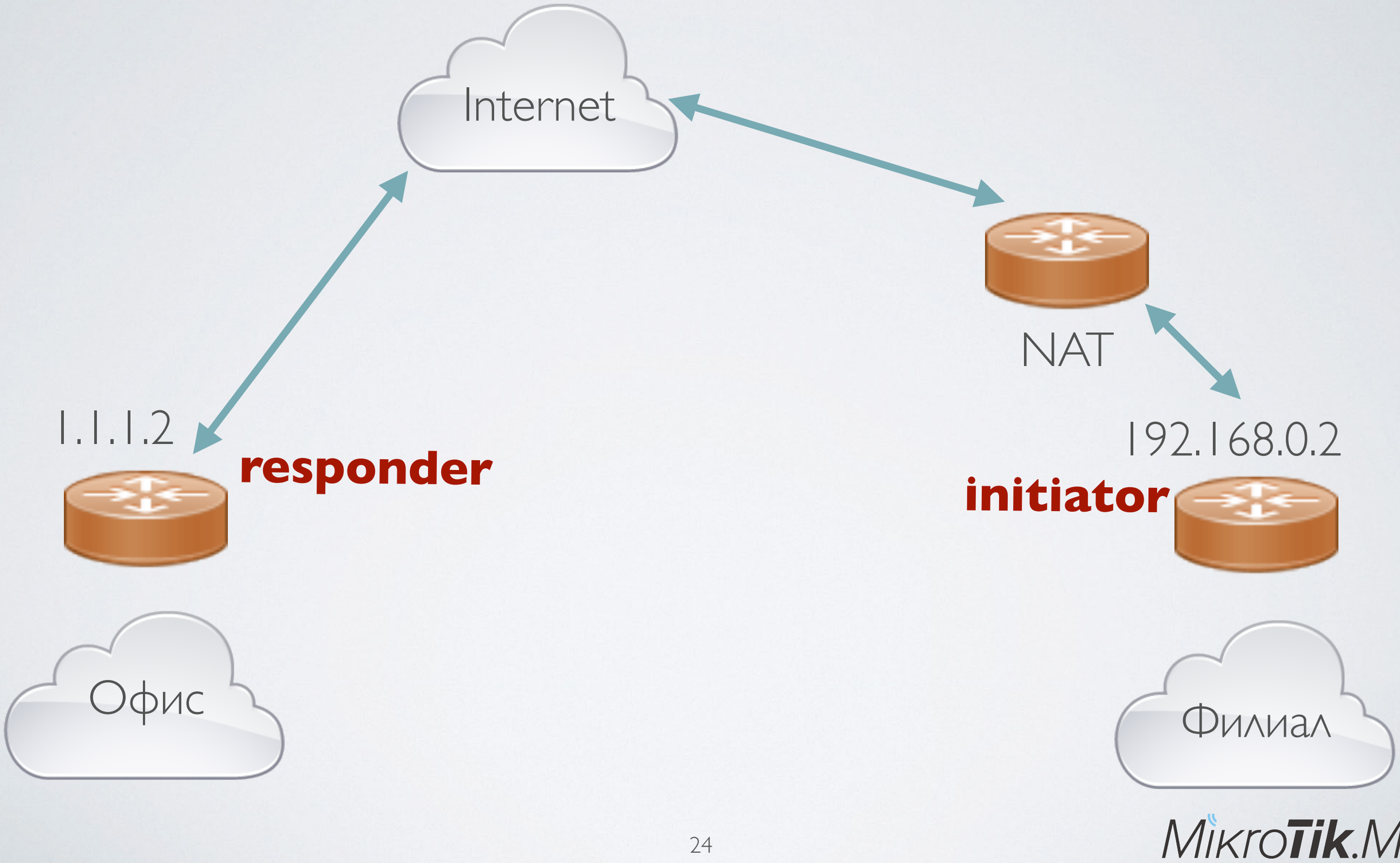
Без дефолта

Создайте маршрут через loopback

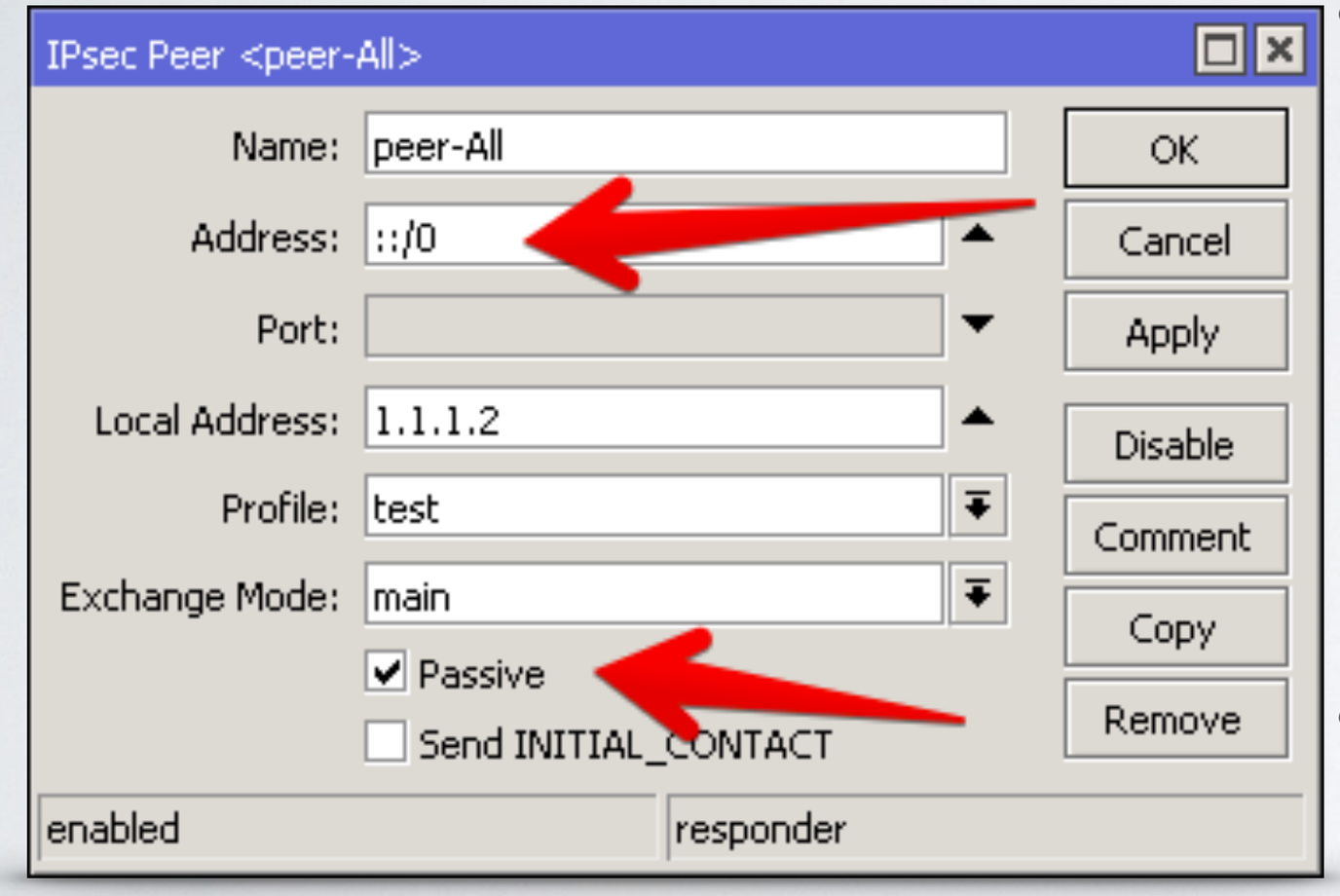
```
/interface bridge add name=Br-Lo

/ip route add dst-address=192.168.0.0/24 gateway=Br-Lo
```

NAT

Я слышал, что для работы IPSec нужны public IP с двух сторон.


Internet
NAT
1.1.1.2
responder
192.168.0.2
initiator
Офис
Филиал

За NAT - Peer



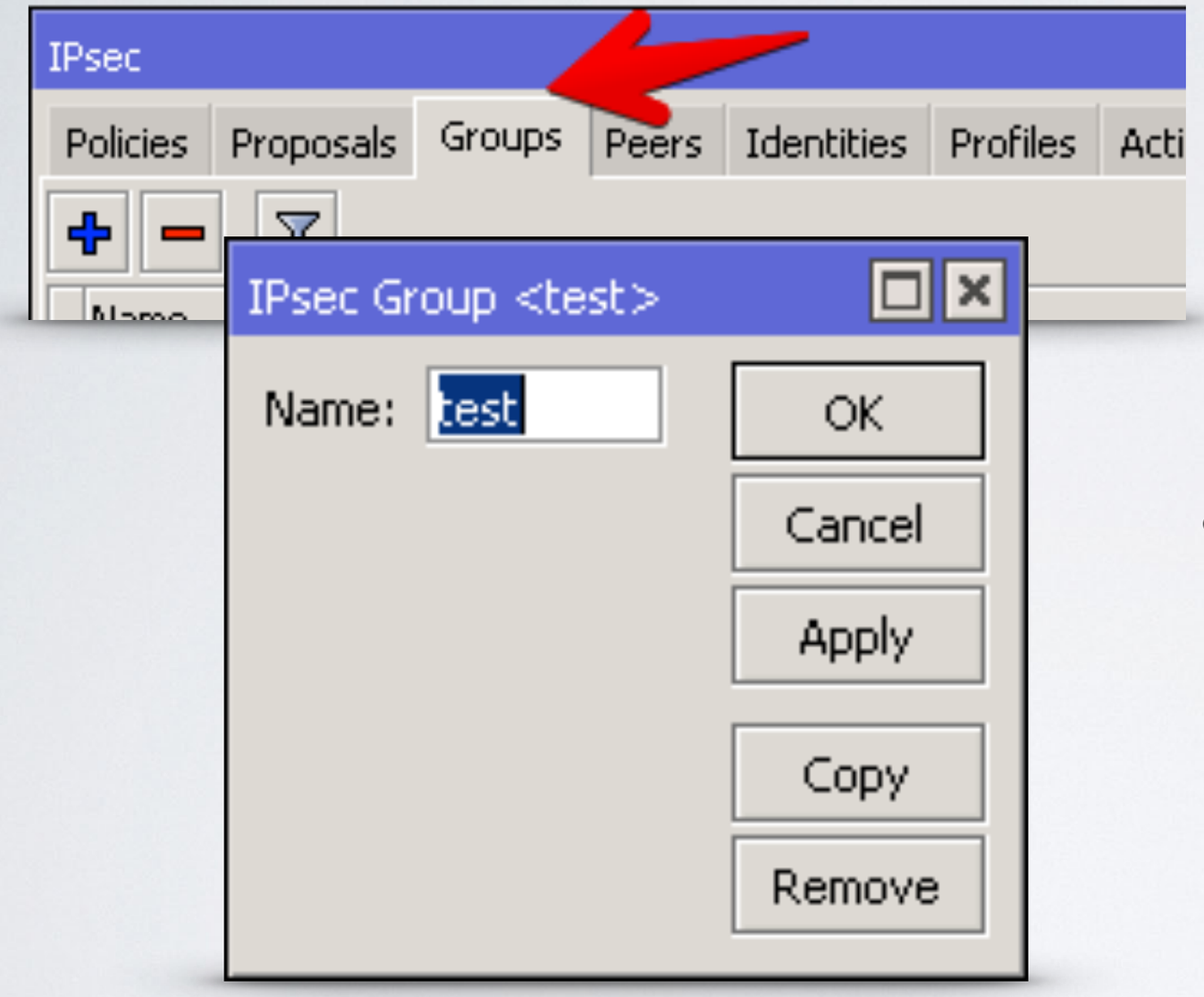
- Укажите префикс провайдера или все возможные адреса на «сервере»
- **Passive** - только отвечать на запросы

responder

MikroTik.Me

responder

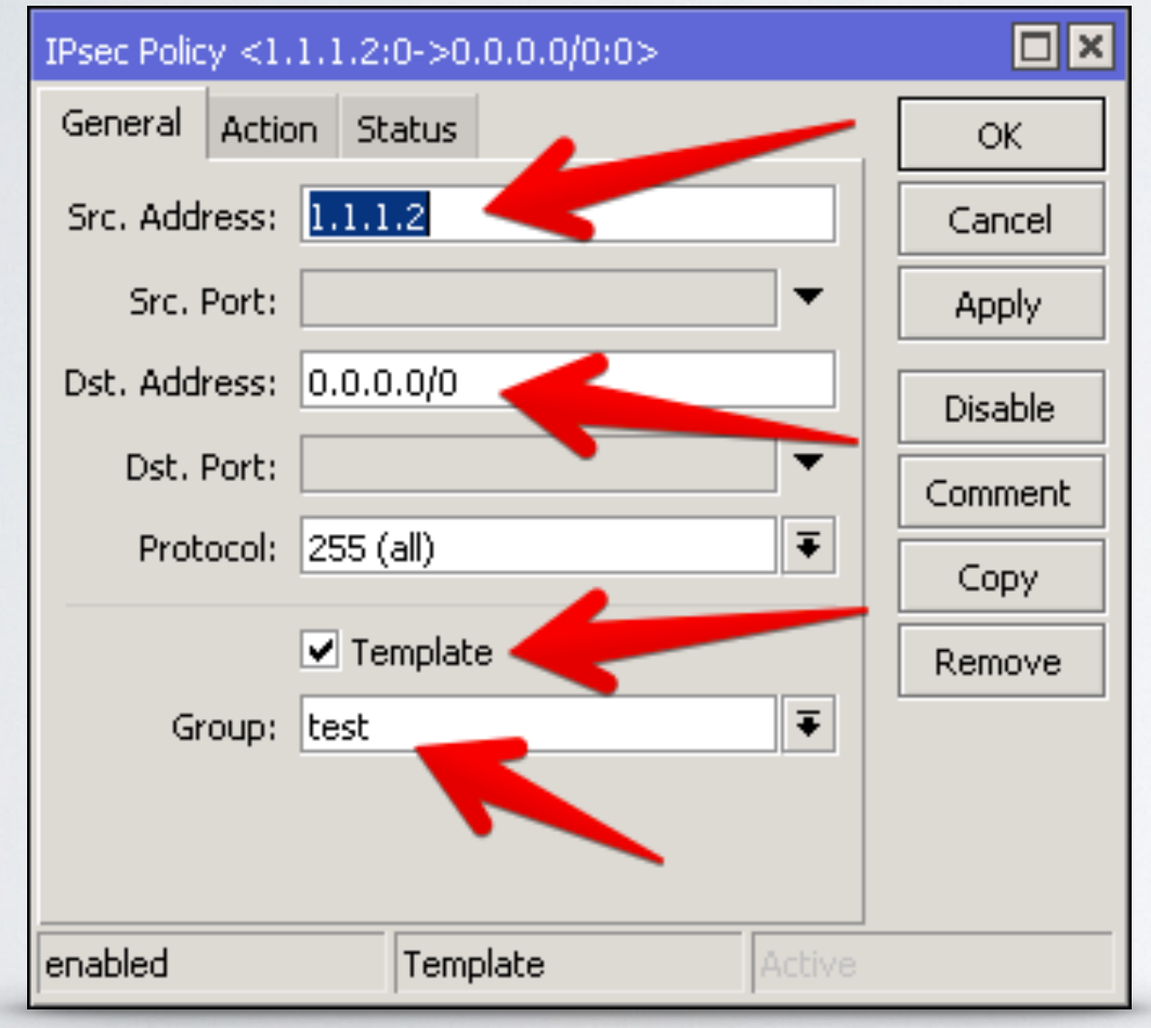
3a NAT - Group



- Создайте группу шаблонов

За NAT - Template

responder

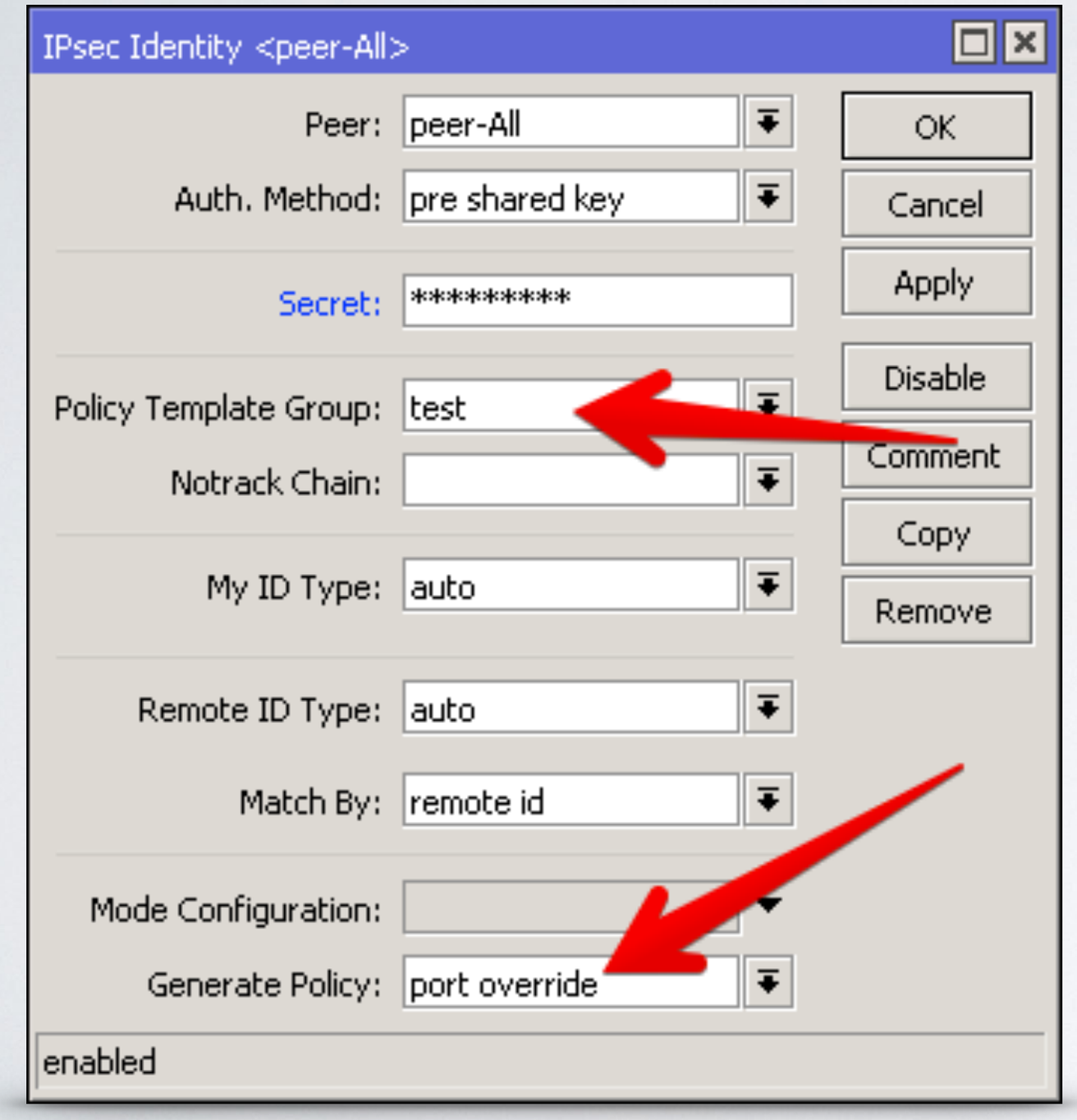


- Укажите public IP «Сервера»
- Укажите IP адреса за NAT-ом «клиентов», или оставьте все
- Назначьте группу шаблонов

MikroTik.Me

За NAT - Identity

responder

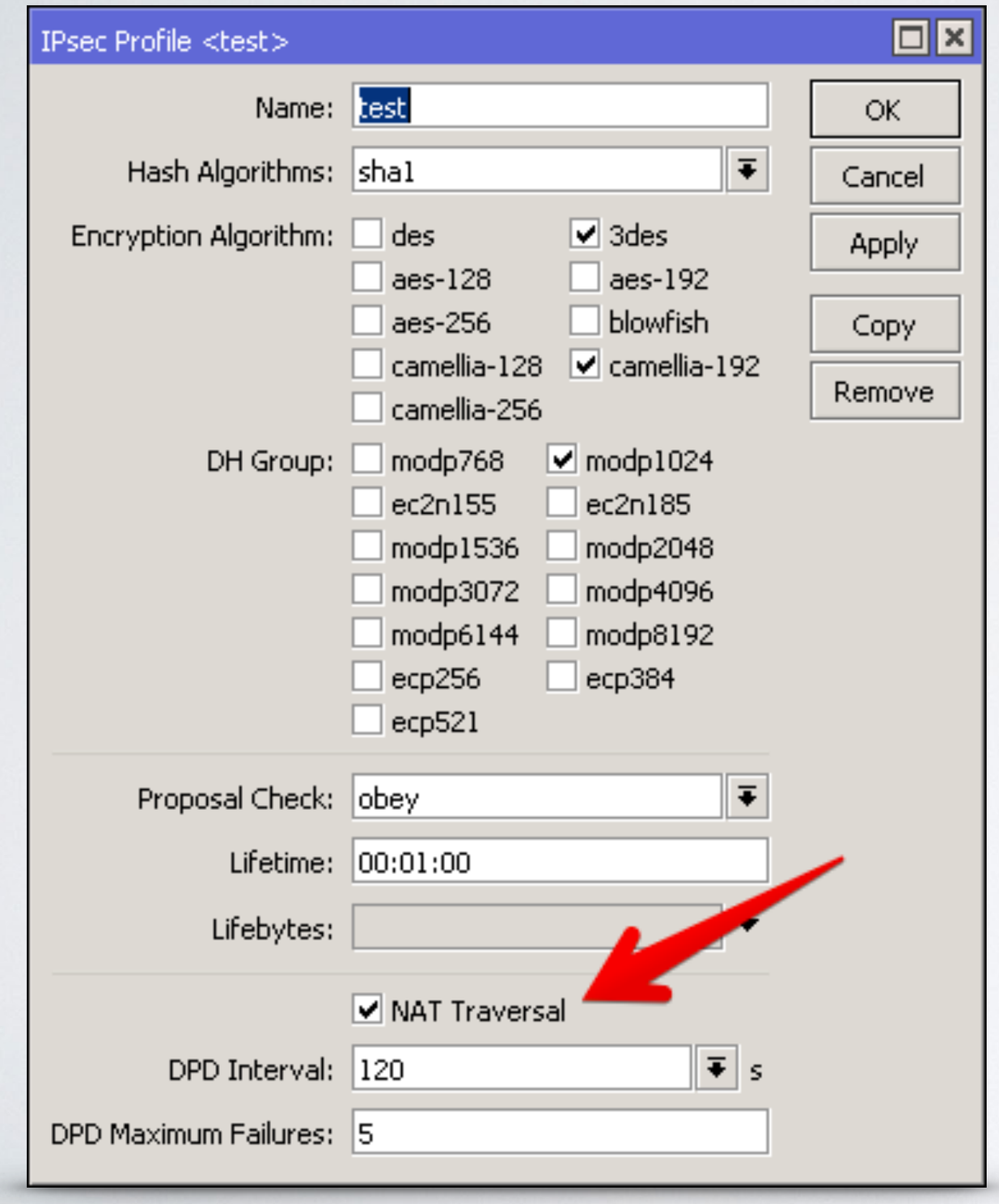


- Выберите какую группу будет использовать данный peer
- Как будут генерироваться policy из шаблона

MikroTik.Me

3a NAT - Profile

Initiator

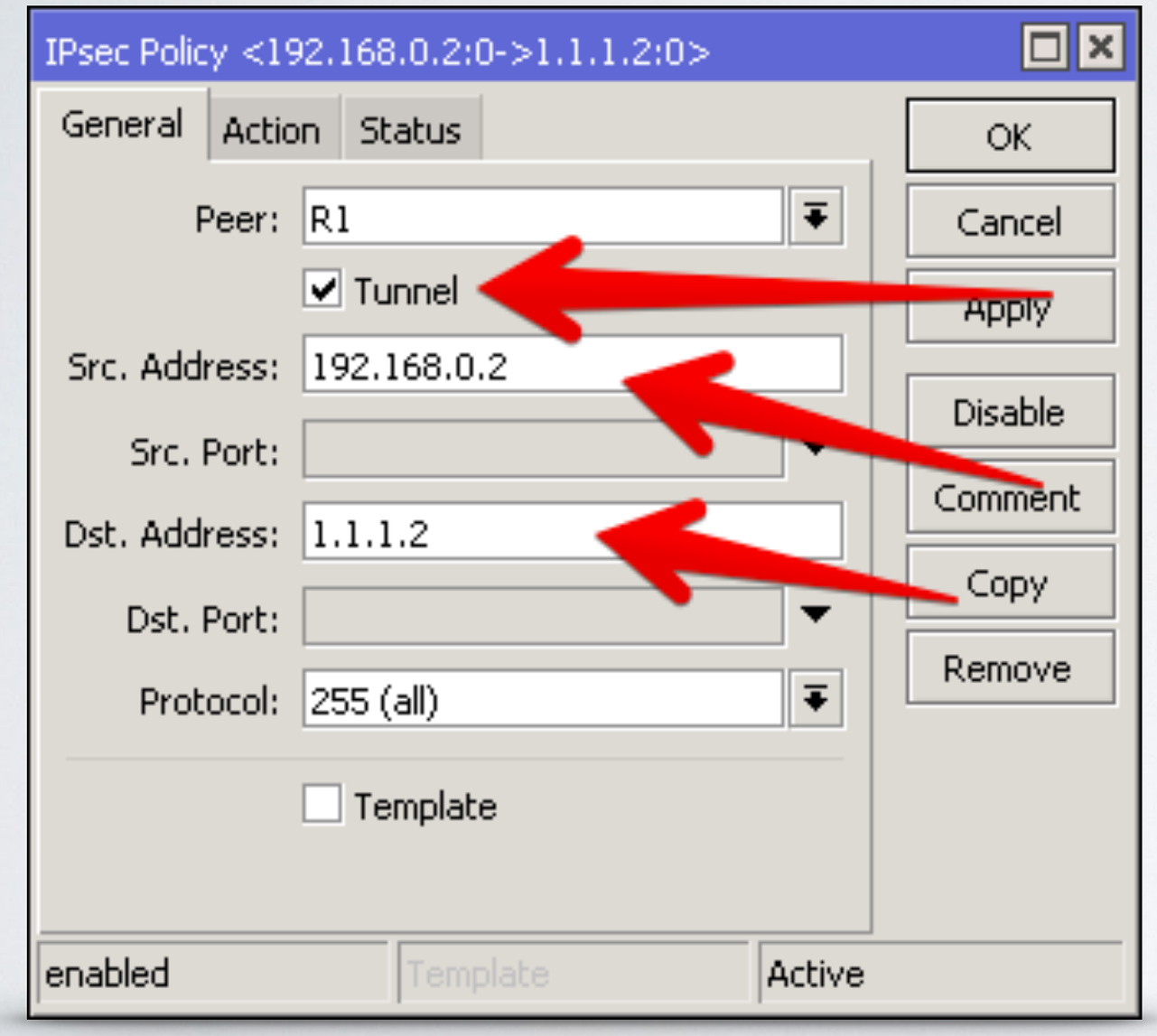


- Включите поддержку NAT-T на клиенте

MikroTik.Me

За NAT - Policy

Initiator



- Укажите ваш внутренний IP за HAT-ом
- Включите Tunnel режим

MikroTik.Me

3a NAT - Firewall

responder

/ip firewall filter

```
add chain=input in-interface-list=ISP ipsec-policy=in,ipsec

add chain=input in-interface-list=ISP protocol=udp dst-port=4500 \
comment="PH2 NAT-T"

add chain=input in-interface-list=ISP protocol=udp dst-port=500 \
comment="PH1"

add chain=forward in-interface-list=ISP ipsec-policy=in,ipsec
```

За NAT - Итог

IPsec

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

Statistics | Find

#		Peer	Src. Ad...	Dst. Address	Action	IPsec Protocols	PH2 C...	PH2 State	SA Src. Address	SA Dst. Address
0	*T		::/0	::/0	encrypt	esp			0.0.0.0	0.0.0.0
1	T		1.1.1.2	0.0.0.0/0	encrypt	esp			0.0.0.0	0.0.0.0
2	DA	peer-All	1.1.1.2	192.168.0.2	encrypt	esp	1	established	1.1.1.2	2.2.2.2
3	DA	peer-All	1.1.1.2	192.168.0.1	encrypt	esp	1	established	1.1.1.2	2.2.2.2

4 items

IPsec

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

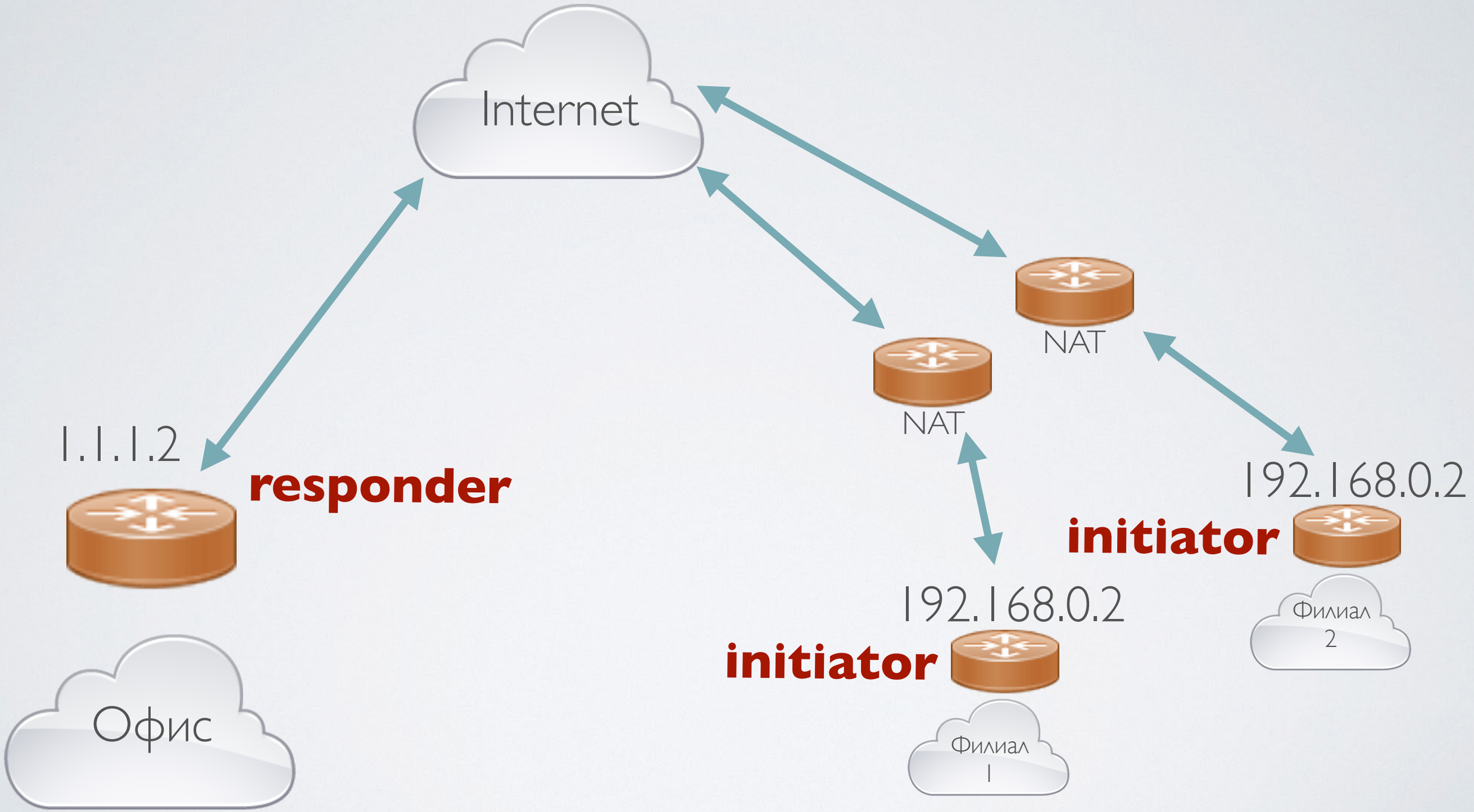
Flush | Find

	SPI	Src. Address	Dst. Address	Auth. Algorithm	Encr. Algorithm	Encr...	Current ...
E	7480b01	1.1.1.2	2.2.2.2	sha1	aes cbc	256	17880
E	8aec62e	1.1.1.2	2.2.2.2	sha1	aes cbc	256	4450
E	3f95244	2.2.2.2	1.1.1.2	sha1	aes cbc	256	17320
E	7a92ace	2.2.2.2	1.1.1.2	sha1	aes cbc	256	4450

4 items

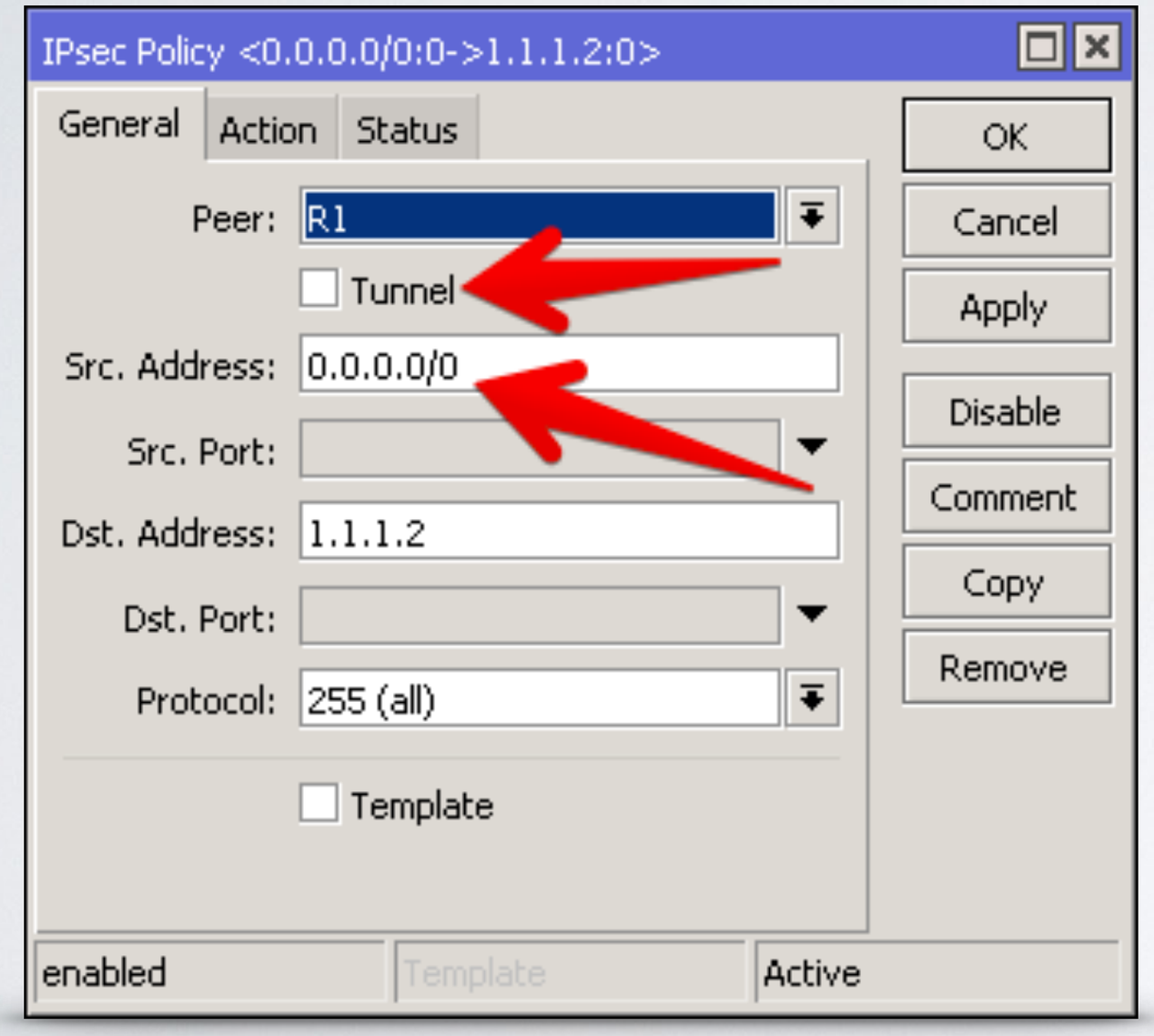
NAT

Два устройства за NAT-ом с одинаковым Внутренним IP


Internet
1.1.1.2
responder
Офис
NAT
NAT
192.168.0.2
initiator
Филиал 1
192.168.0.2
initiator
Филиал 2

За NAT - Peer

Initiator



- Отключите Tunnel режим
- Не указывайте явно адрес источника

За NAT - Итог

IPsec

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

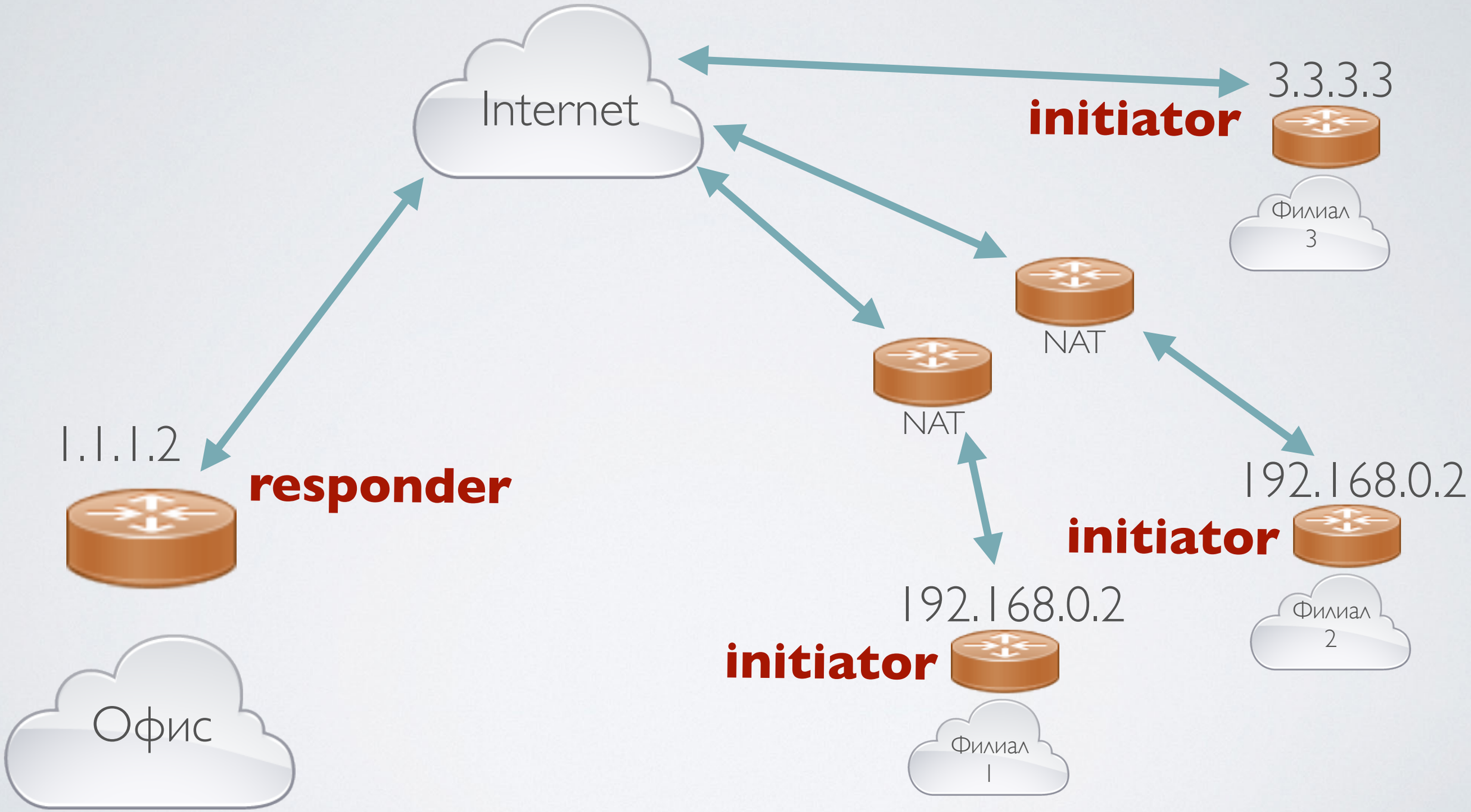
Statistics | Find

#		Peer	Src. Ad...	Dst. Address	Action	IPsec Protocols	PH2 C...	PH2 State	SA Src. Address	SA Dst. Address
0	*T		::/0	::/0	encrypt	esp			0.0.0.0	0.0.0.0
1	T		1.1.1.2	0.0.0.0/0	encrypt	esp			0.0.0.0	0.0.0.0
2	DA	peer-All	1.1.1.2	2.2.2.2	encrypt	esp	1	established	1.1.1.2	2.2.2.2

3 items

Только транспортный режим

Мне нужен интерфейс для маршрутизации и прочего


Internet
3.3.3.3
initiator
Филиал
3
NAT
NAT
1.1.1.2
responder
192.168.0.2
initiator
192.168.0.2
initiator
Филиал
2
Филиал
1
Офис

Подготовка

- Каждому филиалу присвойте порядковый номер
  - 1,2,3,4…
- Выберите префикс, который не используется в вашей сети и количество IP адресов достаточно для всех филиалов
  - 172.31.255.0/24 - 256шт.

Подготовка

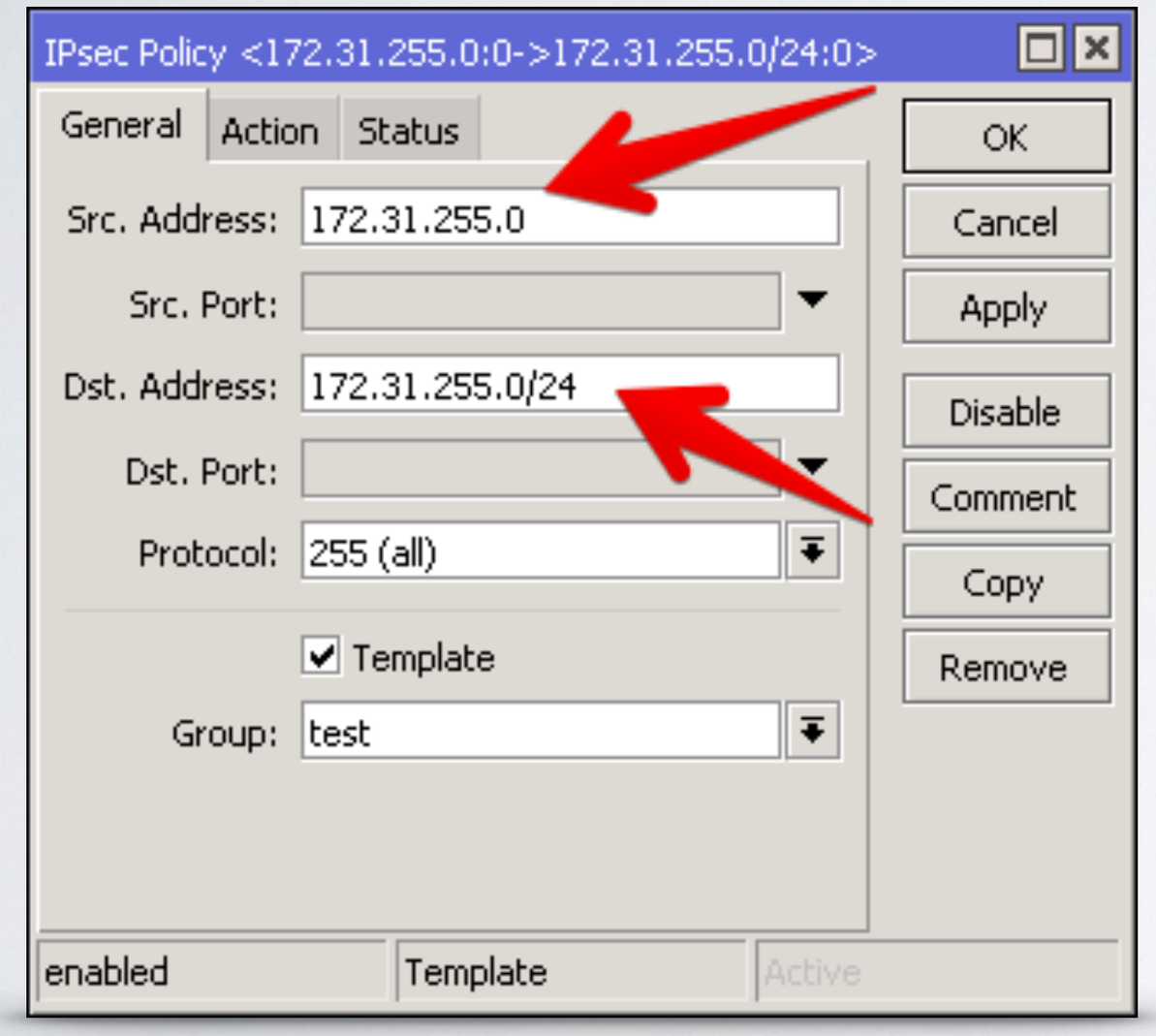
- Создайте на каждом маршрутизаторе Loopback интерфейс

```
/interface bridge add name=Br-Lo
```

- Назначьте на Loopback адрес из выбранного ранее префикса **/32**

```
/ip address add address=172.31.255.0/32 interface=Br-Lo
```

За NAT - Template

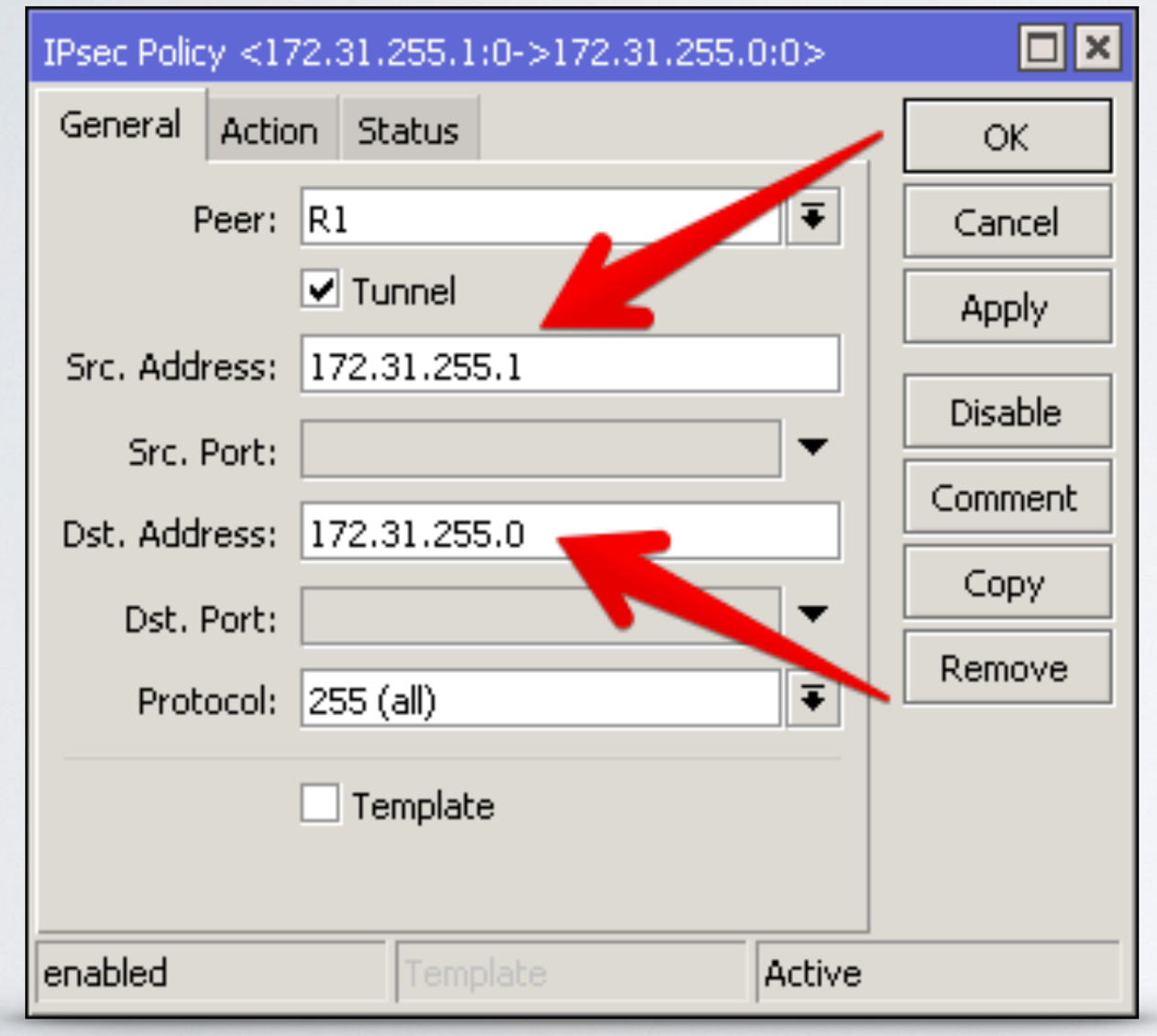


- Укажите адрес loopback «сервера»
- Укажите **префикс** для loopback адресов
- Назначьте группу шаблонов

MikroTik.Me

За NAT - Policy

Initiator



- Укажите ваш адрес loopback
- Укажите адрес loopback «сервера»

MikroTik.Me

За NAT - Итог

responder

IPsec

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

Statistics | Find

#		Peer	Src. Address	Dst. Address	Action	IPsec Protocols	PH2 C...	PH2 State	SA Src. Address	SA Dst. Address
0	*T		::/0	::/0	encrypt	esp			0.0.0.0	0.0.0.0
1	T		172.31.255.0	172.31.255.0/24	encrypt	esp				
2	DA	peer-All	172.31.255.0	172.31.255.1	encrypt	esp	1	established	1.1.1.2	2.2.2.2
3	DA	peer-All	172.31.255.0	172.31.255.2	encrypt	esp	1	established	1.1.1.2	2.2.2.2
4	DA	peer-All	172.31.255.0	172.31.255.3	encrypt	esp	1	established	1.1.1.2	3.3.3.2

5 items

3a NAT - Interfaces

responder

Interface List

Interface | Interface List | Ethernet | EoIP Tunnel | IP Tunnel | GRE Tunnel | VLAN | VRRP | Bonding | LTE

	Name	Type	Actual ...	L2 MTU	Tx
R	gre-1	GRE Tunnel	1398	65535	0
R	gre-2	GRE Tunnel	1398	65535	0
R	gre-3	GRE Tunnel	1414	65535	0

Neighbor List

Discovery Settings | Find

				Platform
gre-1		00:00:00:00:00:00	NAT-1	MikroTik
gre-2		00:00:00:00:00:00	NAT-2	MikroTik
gre-3		00:00:00:00:00:00	R3	MikroTik

3 items

3 items out of 7 (1 selected)

Interface <gre-1>

General | Status | Traffic

OK | Cancel | Apply | Disable | Comment | Copy | Remove | Torch

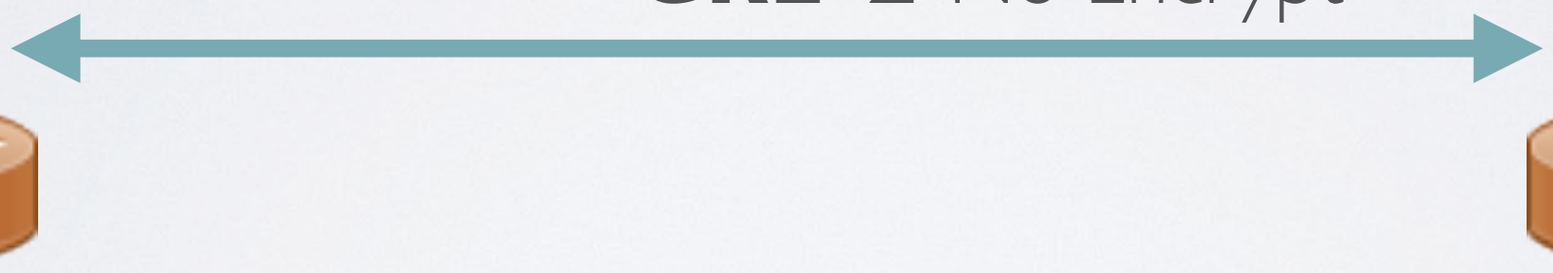
Name: gre-1
Type: GRE Tunnel
MTU:
Actual MTU: 1398
L2 MTU: 65535
Local Address: 172.31.255.0
Remote Address: 172.31.255.1
IPsec Secret:
Keepalive: 00:00:10 , 10
DSCP: inherit
Dont Fragment: no
Clamp TCP MSS

MikroTik.Me

У меня много «слабых» железок.

GRE-1 Encrypt

GRE-2 No Encrypt



Подготовка

responder

- Создайте на каждом маршрутизаторе Loopback интерфейс

```
/interface bridge add name=Br-Lo
```

- Назначьте на Loopback адреса из выбранного ранее префикса **/32**

```
/ip address add address=172.31.255.0/32 interface=Br-Lo

/ip address add address=172.31.255.254/32 interface=Br-Lo
```

Подготовка

172.31.255.0 - для шифрования

172.31.255.254 - без шифрования

Proposal

Responder и initiator

/ip ipsec proposal

add enc-algorithms=null name=pr-null

add enc-algorithms=aes-256-cbc name=pr-encrypt

Template

responder

```
/ip ipsec policy

add dst-address=172.31.255.0/24 \
src-address=172.31.255.0/32 proposal=pr-encrypt \
template=yes

add dst-address=172.31.255.0/24 \
src-address=172.31.255.254/32 proposal=pr-null template=yes
```

Policy

Initiator

/ip ipsec policy

```
add dst-address=172.31.255.0 src-address=172.31.255.3 \
proposal=pr-encrypt tunnel=yes peer=R0 level=unique

add dst-address=172.31.255.254 src-address=172.31.255.3 \
proposal=pr-null tunnel=yes peer=R0 level=unique
```

Tunnels

Создайте туннели между loopback адресами

Трафик от 254 адреса без шифрования

Трафик от 0 адреса с шифрованием

```
[admin@R3] /interface gre> pr
Flags: X - disabled, R - running
 0  R name="gre3-encrypt" mtu=auto actual-mtu=1422 local-address=172.31.255.3
      remote-address=172.31.255.0 keepalive=10s,10 dscp=inherit clamp-tcp-mss=yes dont-fragment=no
      allow-fast-path=no

 1  R name="gre3-null" mtu=auto actual-mtu=1434 local-address=172.31.255.3
      remote-address=172.31.255.254 keepalive=10s,10 dscp=inherit clamp-tcp-mss=yes
      dont-fragment=no allow-fast-path=no
```

Tunnels

Создайте туннели между loopback адресами

Трафик от 254 адреса без шифрования

Трафик от адреса с шифрованием

```
[admin@R3] /interface gre> print
Flags: X - disabled, R - running
 0  R name="gre3-encrypt" mtu=auto actual-mtu=1422 local-address=172.31.255.3
      remote-address=172.31.255.0 keepalive=10s,10 dscp=inherit clamp-tcp-mss=yes dont-fragment=no
      allow-fast-path=no

 1  R name="gre3-null" mtu=auto actual-mtu=1434 local-address=172.31.255.3
      remote-address=172.31.255.254 keepalive=10s,10 dscp=inherit clamp-tcp-mss=yes
      dont-fragment=no allow-fast-path=no
```

Tunnels

```
[admin@R3] /ip ipsec installed-sa> pr
Flags: H - hw-a...  A - AH, E - ESP
 0  E spi=0x6955... src-address=1.1.1.2 dst-address=3.3.3.2 state=mature auth-algorithm=sha1
      enc-algorithm=des enc-key-size=64 auth-key="df6e609e661fc9eef1d14f54d911b1dd8c267f2f"
      enc-key="2854a03a4c835ab7" addtime=sep/02/2019 18:42:20 expires-in=25m44s
      add-lifetime=24m/30m current-bytes=3732 current-packets=67 replay=128

 1  E spi=0xF...94B08 src-address=3.3.3.2 dst-address=1.1.1.2 state=mature auth-algorithm=sha1
      enc-alg...thm=des enc-key-size=64 auth-key="0fc488c007a39d3a8b662f112b8d2e1eda1a9d44"
      enc-key="...67a4ed103486e1" addtime=sep/02/2019 18:42:20 expires-in=25m44s
      add-lifeti...24m/30m current-bytes=3732 current-packets=67 replay=128

 2  E spi=0x3C74D9A...c-address=1.1.1.2 dst-address=3.3.3.2 state=mature auth-algorithm=sha1
      enc-algorithm=null auth-key="53be1a14dde89b00897f5ab6f0076527bad75e5c" enc-key=""
      addtime=sep/02/2019 18:42:24 expires-in=25m48s add-lifetime=24m/30m current-bytes=3324
      current-packets=64 replay=128

 3  E spi=0x525B70B src-address=3.3.3.2 dst-address=1.1.1.2 state=mature auth-algorithm=sha1
      enc-algorithm=null auth-key="36a05994cd75723a30394118349d7e77a6be3a45" enc-key=""
      addtime=sep/02/2019 18:42:24 expires-in=25m48s add-lifetime=24m/30m current-bytes=3324
      current-packets=64 replay=128
```

По две ассоциации

Tunnels

Neighbor List

Discovery Settings

Find

Interface	IP Address	MAC Address	Identity	Platform	Version	Board Na...	IPv6	Age (s)	Uptime
gre3-encrypt		00:00:00:00:00:00	R0	MikroTik	6.45.5 (stable)	CHR	no	12	02:47:35
gre3-null		00:00:00:00:00:00	R0	MikroTik	6.45.5 (stable)	CHR	no	12	02:47:35

RB751 Null

~60Mbps

Не работает

Не работает IPsec, что мне делать?

Обновлял и делал downgrade.

Нечего не помогает.

NAT

Пакет выходя с маршрутизатора попадает под src-nat

```
/ip firewall nat
add action=masquerade chain=srcnat \
ipsec-policy=out,none out-interface-list=ISP
```

```
/ip firewall nat
add action=accept chain=srcnat ipsec-policy=out,ipsec
```

```
/ip firewall raw
add action=notrack chain=prerouting \
dst-address=172.31.255.0/24 src-address=172.31.255.0/24
add action=notrack chain=output \
dst-address=172.31.255.0/24 src-address=172.31.255.0/24
```

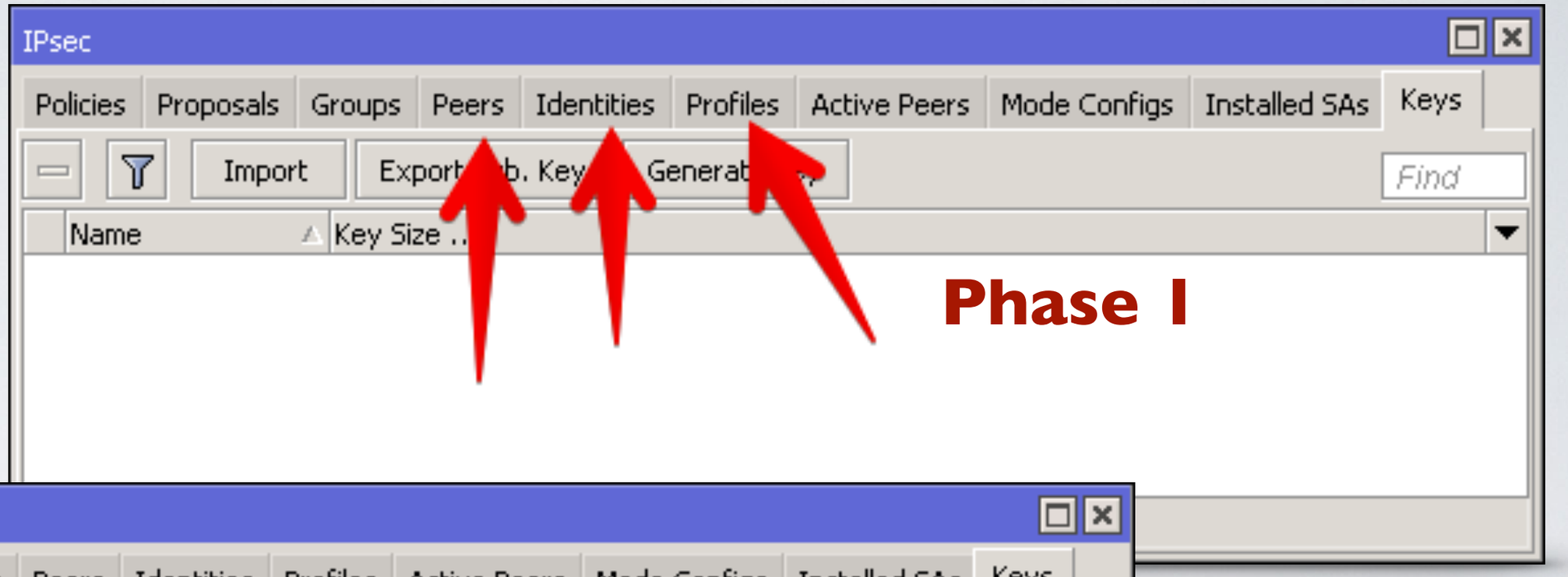
Логи

- ipsec,error no suitable proposal found.
- ipsec,error 3.3.3.2 failed to get valid proposal.
- ipsec,error 3.3.3.2 failed to pre-process ph1 packet (side: 1, status 1).
- ipsec,error 3.3.3.2 phase1 negotiation failed.

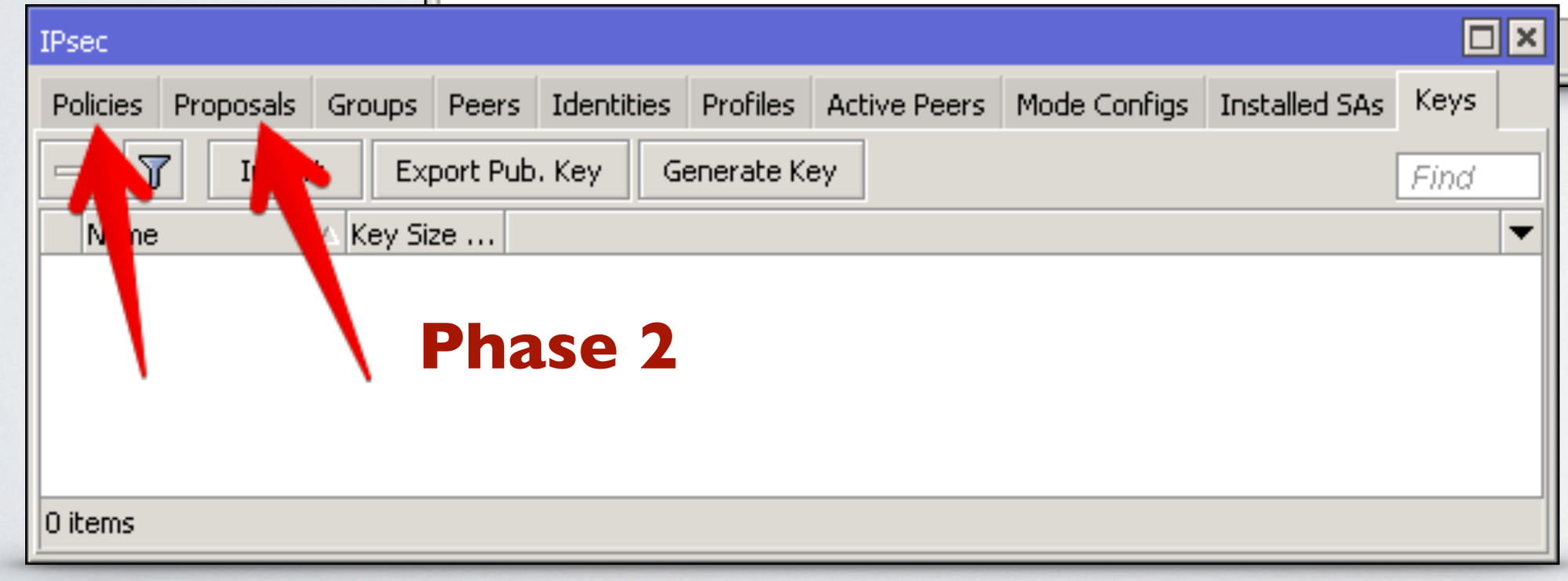
Логи

- ipsec,error no suitable proposal found.
- ipsec,error 3.3.3.2 failed to get valid proposal.
- ipsec,error 3.3.3.2 failed to pre-process ph1 packet (side: 1, status 1).
- ipsec,error 3.3.3.2 phase1 negotiation failed.

Фазы



Phase 1



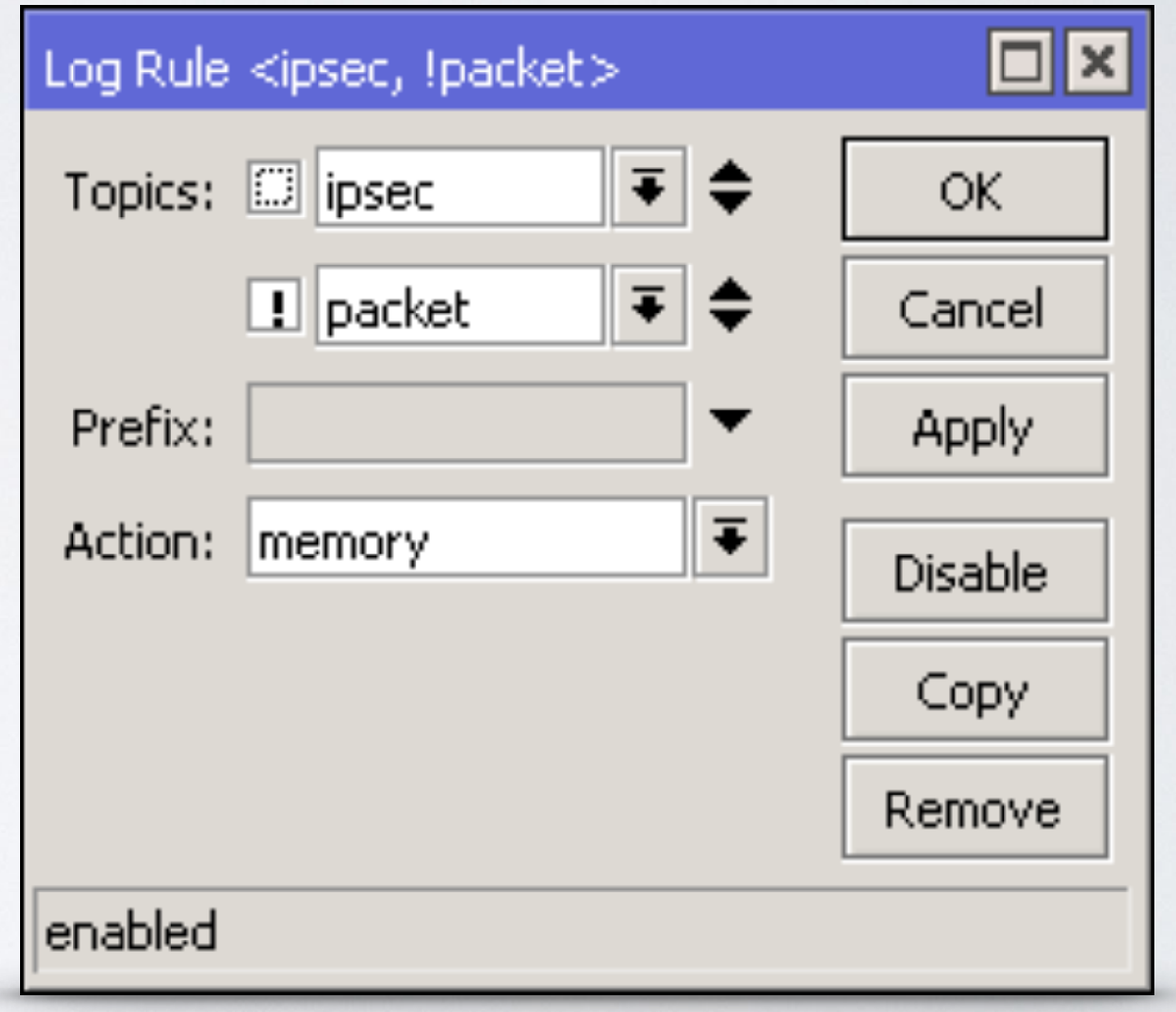
Phase 2

Debug

Имеет смысл только на responder

/system logging

add topics=ipsec,!packet



Debug

/log print where topics~"ipsec"

- ipsec rejected enctype:
  DB(prop#1:trns#1):Peer(prop#1:trns#1) = AES-CBC:Camellia-CBC

- ipsec rejected enctype:
  DB(prop#1:trns#2):Peer(prop#1:trns#1) = 3DES-CBC:Camellia-CBC

- ipsec,error no suitable proposal found.

Debug

/log print where topics~"ipsec"

- ipsec rejected enctype: DB(prop#1:trns#1):Peer(prop#1:trns#1) = AES-CBC:Camellia-CBC
- ipsec rejected enctype: DB(prop#1:trns#2):Peer(prop#1:trns#1) = 3DES-CBC:Camellia-CBC
- ipsec,error no suitable proposal found.

Debug

/log print where topics~"ipsec"

- ipsec **rejected** enct[illegible]:
  DB(prop#1:trns#1):Peer(prop#1:trns#1) = AES-CBC:Camellia-CBC

- ipsec **rejected** enct[illegible]:
  DB(prop#1:trns#2):Peer(prop#1:trns#1) = 3DES-CBC:Camellia-CBC

- ipsec,error no suitable proposal found.

Debug

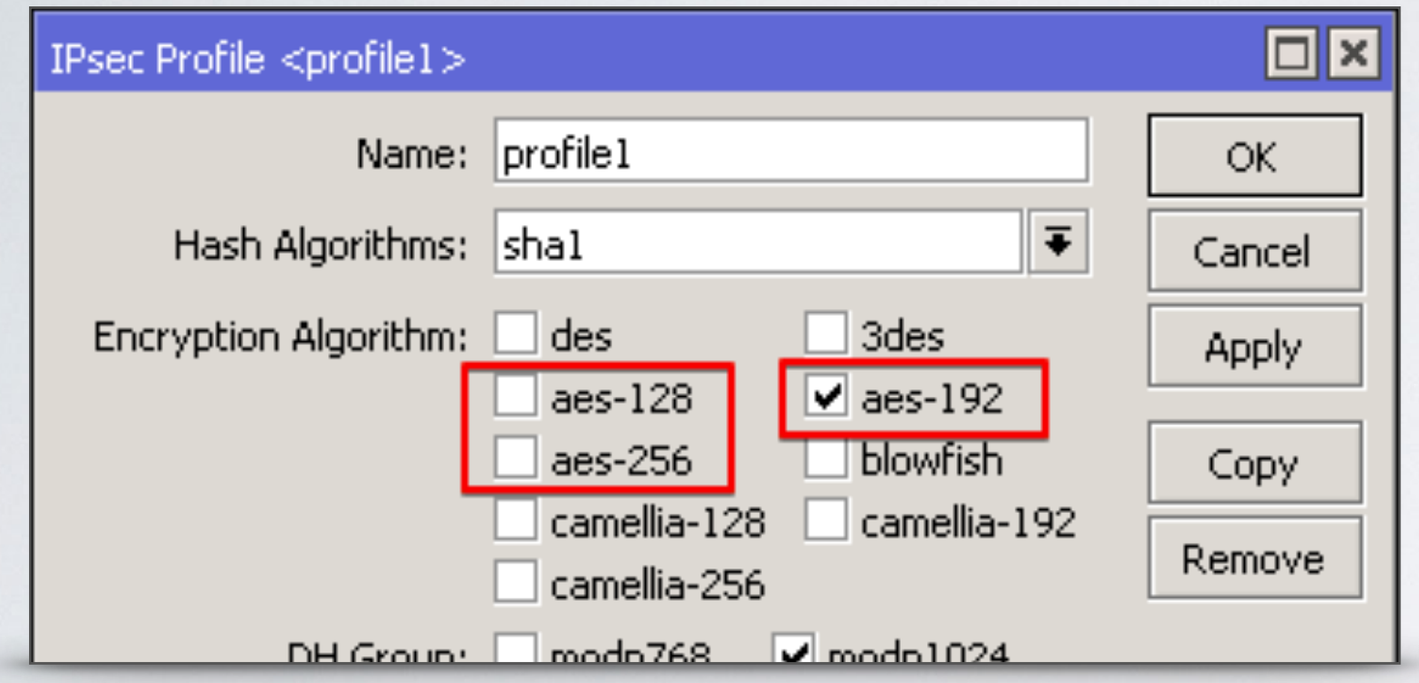
/log print where topics~"ipsec"

- Ipsec **rejected** enctype:
  DB(prop#1:trns#1):Peer(prop#1:trns#1) = AES-CBC:Camellia-CBC

- ipsec **rejected** enctype:
  DB(prop#1:trns#1):Peer(prop#1:trns#1) = 3DES-CBC:Camellia-CBC

- ipsec,error no suitable proposal found.

Debug



- Изменить первую фазу
  - Либо на **responder** добавить camellia
  - Либо на **initiator** добавить aes-cbc или 3des

Debug

```
-compare proposal #1: Local:Peer
(lifetime = 86400:86400)
(lifebyte = 0:0)
enctype = AES-CBC:AES-CBC
(encklen = 128:192)
hashtype = SHA:SHA
authmethod = pre-shared key:pre-shared key
dh_group = 1024-bit MODP group:1024-bit MODP group
-compare proposal #2: Local:Peer
(lifetime = 86400:86400)
(lifebyte = 0:0)
enctype = 3DES-CBC:AES-CBC
(encklen = 0:192)
hashtype = SHA:SHA
authmethod = pre-shared key:pre-shared key
dh_group = 1024-bit MODP group:1024-bit MODP group
```

128:192

3DES:192

Выбор RouterBoard

Мы купили 3011 но он не «качает»

Выбор RouterBoard

wiki.mikrotik.com/wiki/Manual:IP/IPsec#Hardware_acceleration

Выбор RouterBoard

Hardware acceleration allows to do faster encryption process by using built-in encryption engine inside CPU.

RouterBoard	DES and 3DES				AES-CBC			
	MD5	SHA1	SHA256	SHA512	MD5	SHA1	SHA256	SHA512
RB3011UiAS-RM *	no	yes	yes	no	no	yes	yes	no
RB4011iGS+RM and RB4011iGS+5HacQ2HnD-IN	yes	yes	yes	yes	yes	yes	yes	yes
Cloud Core Router series	yes	yes	yes	no	yes	yes	yes	no
x86 (AES-NI) ***	no	no	no	no	yes	yes	yes	yes

* supported only 128 bit and 256 bit key sizes

** c manufactured since 2016, serial numbers that begin with number 5 and 7

*** AES-C C and AES-CTR only encryption is accelerated, hashing done in software

**** DES is no upported, only 3DES and AES-CBC

Наш Выбор

- **RB750gr3 - клиент**
- **RB450Gx4 - клиент**
- **RB1100AHx4 - сервер**

Жить спокойно можно

- Не используйте дефолтный proposal
- Не используйте дефолтный profile
- Не используйте дефолтный template
- Не используйте дефолтную группу шаблонов
- Настраивайте всё «руками»

IPSex

IPSec

Вопросы?

- MikroTik.Me
- Vasilevkirill.com
- https://t.me/mikrotikme
- https://vk.com/mikrotikrus

MikroTik.Me