



МikroTik IKE2 VPN своими руками:
простая и понятная пошаговая
инструкция - by Nikita Tarikin
(MikroTik PRO, Russia)

MUM Russia

September 06–07, 2019

Moscow

MikroTik

Зачем IKEv2?

Сравнение клиент-серверных типов VPN (RouterOS)



	L2TP	L2TP/IPSEC + psk	OpenVPN	PPTP	SSTP	IPSec IKE2
Протокол	UDP	UDP over UDP/ESP	TCP	GRE	TCP	UDP, ESP
Скорость работы	Быстро	Средне	Медленно	Быстро	Медленно	Очень быстро
Скорость подключения	Средне	Медленно	Медленно	Средне	Средне	Очень быстро
Требуется мощный CPU	Нет	Да	Да	Нет	Да	Да
Балансируется между ядрами CPU	Да	Да	Нет	Да	Да	Да
Безопасность	Низкая	Высокая	Высокая	Низкая	Высокая	Очень высокая
Доставка маршрутов	Нет	Нет	Нет	Нет	Нет	Да
Работа через NAT	Да	Да	Да	Да	Да	Да
Наличие интерфейса	Да	Да	Да	Да	Да	Нет
Популярность	Высокая	Очень высокая	Высокая	Очень высокая	Низкая	Высокая

Зачем IKEv2?

1. Очень высокая скорость работы
2. **Мгновенное подключение**
3. Очень высокий уровень безопасности
4. Поддержка аппаратного шифрования
5. Поддерживается большинством современных операционных систем
6. Доставляет маршруты клиентам
7. Работает через NAT
8. **Адаптирован для хаотичных мобильных каналов связи**

— — —

Сетевая диаграмма

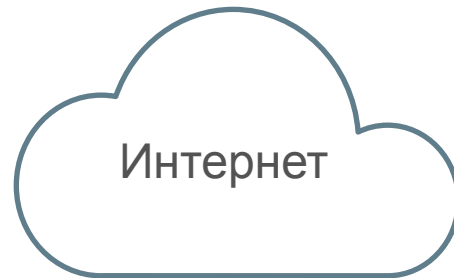


Мой телефон

Устройство сети для блондинок 👸💕



Magic



Устройство сети для продвинутых 😎



Мой компьютер



Мой роутер



Инет



LAN



MikroTik
Router

WAN

WAN

WAN

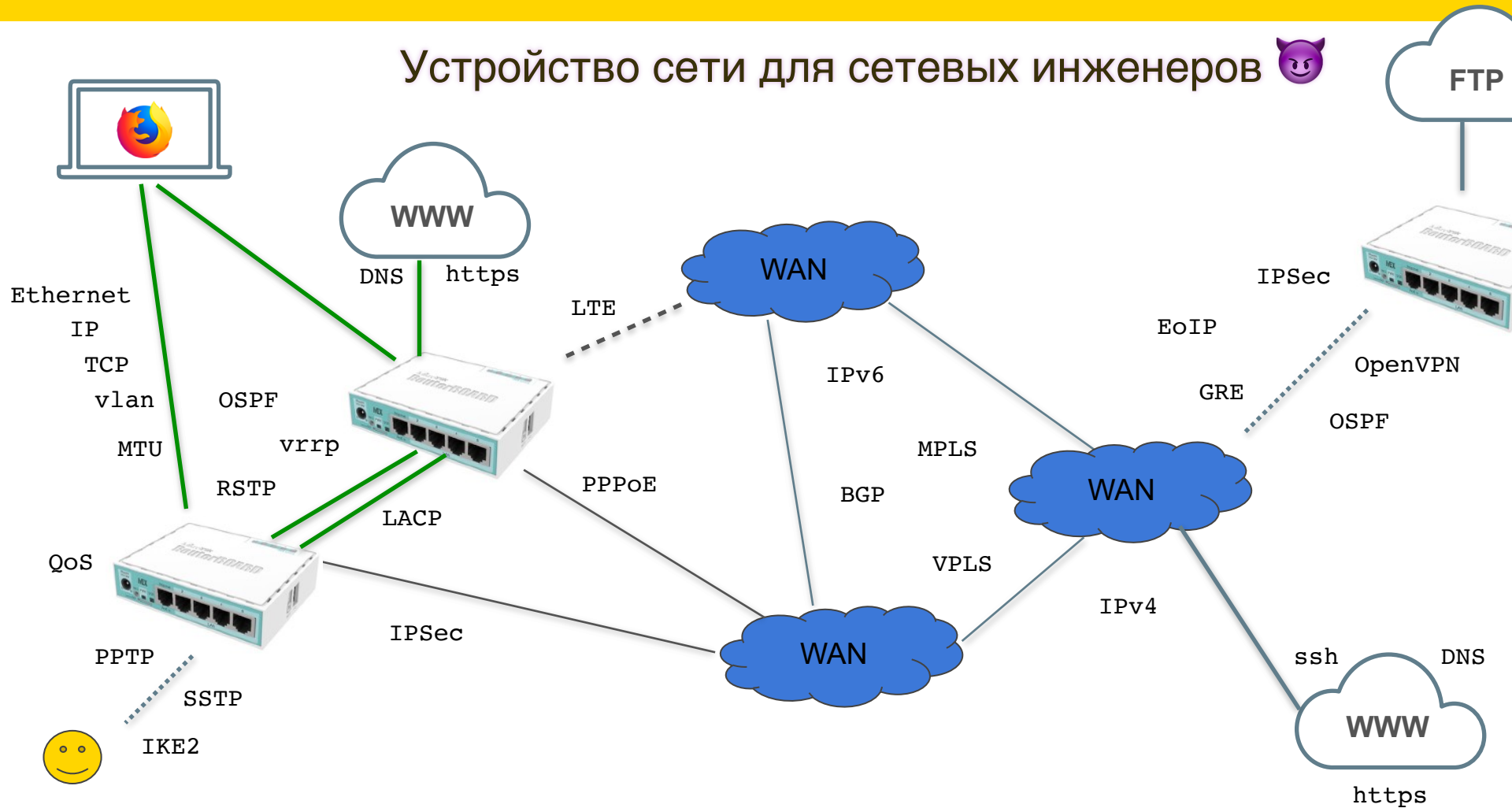
WAN

DNS
Apache
Wordpress

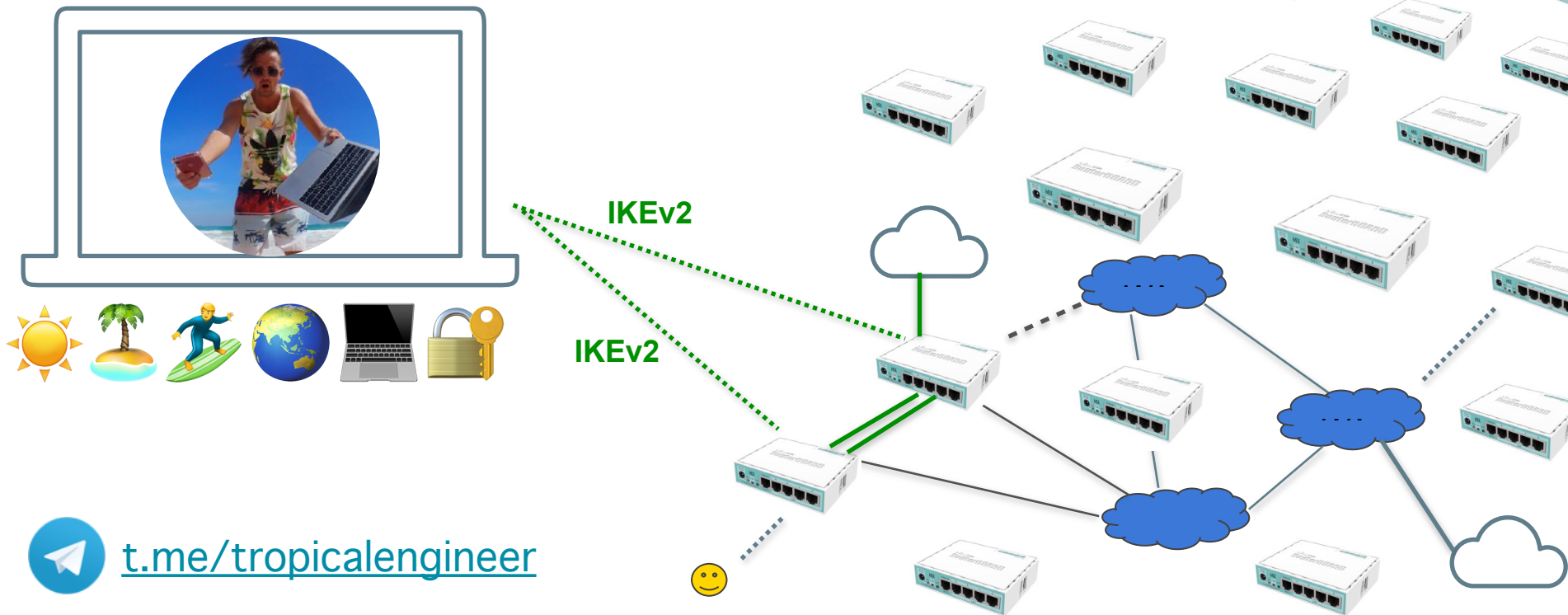
Устройство сети для админов



Устройство сети для сетевых инженеров 🐱



Устройство сети для кайт-серферов



t.me/tropicalengineer



Никита Тарикин

Сертифицированный
сетевой инженер
MikroTik PRO, Россия



MikroTik
C E R T I F I E D

Никита Тарикин

Сертифицированный
сетевой инженер
MikroTik PRO, Россия

MTCNA 99%

MTCRE 95%

MTCTSE 96%

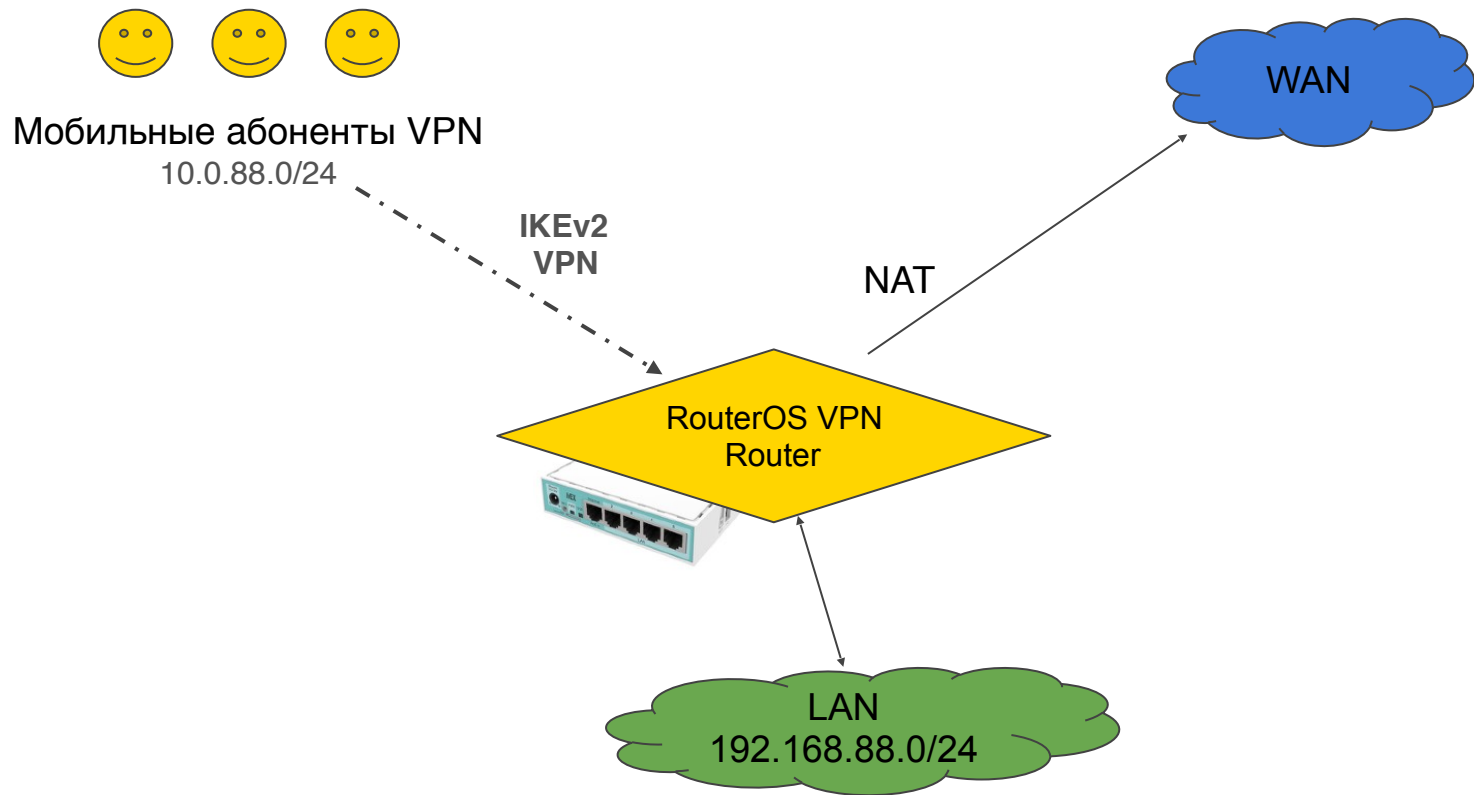
MTCWE 84%

MTCUME 90%

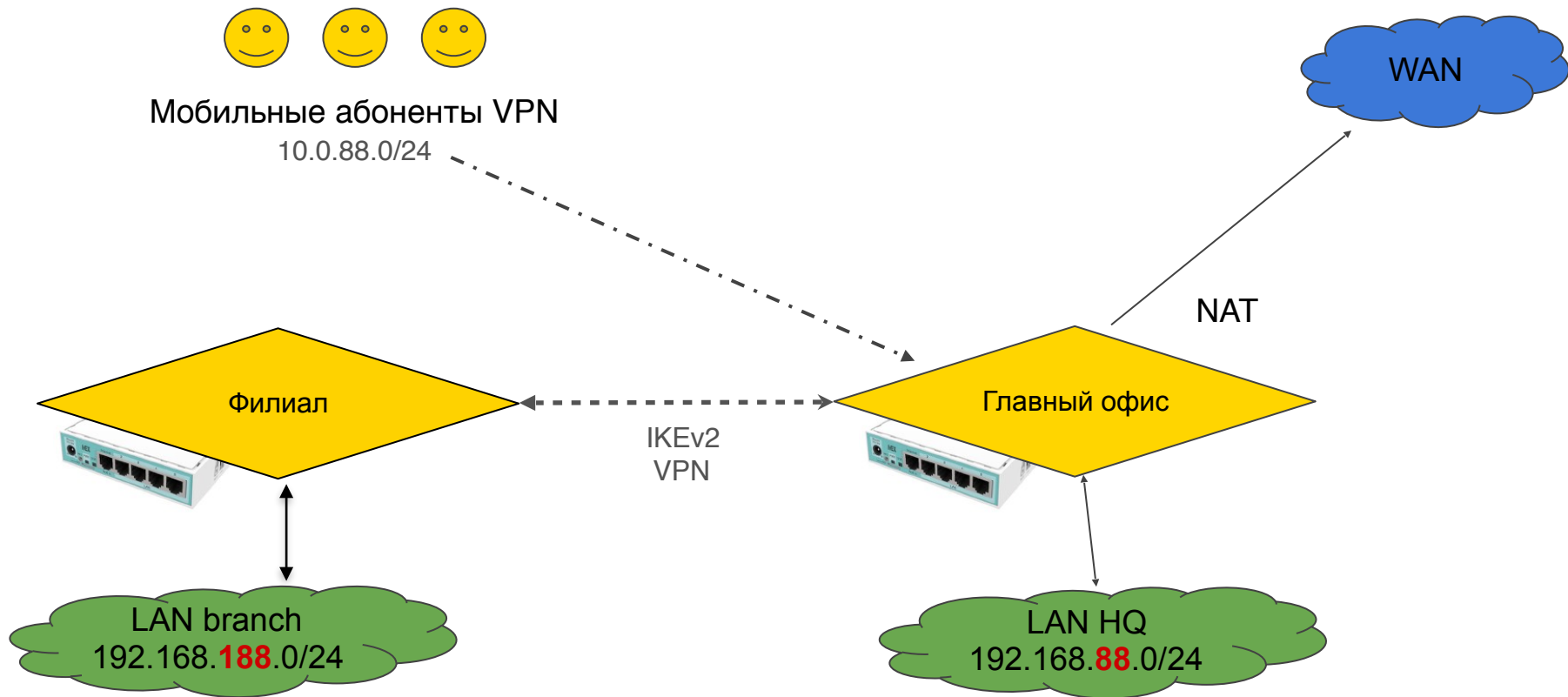
MTCSE 94%







Сетевая диаграмма



Сетевая диаграмма

Общий план презентации

1. Подготовка к работе
2. Настройка VPN сервера в главном офисе
3. Подключение Windows 10
4. Подключение MacOS, iOS, Android
5. Подключение филиала через роутер MikroTik
6. Конкурс



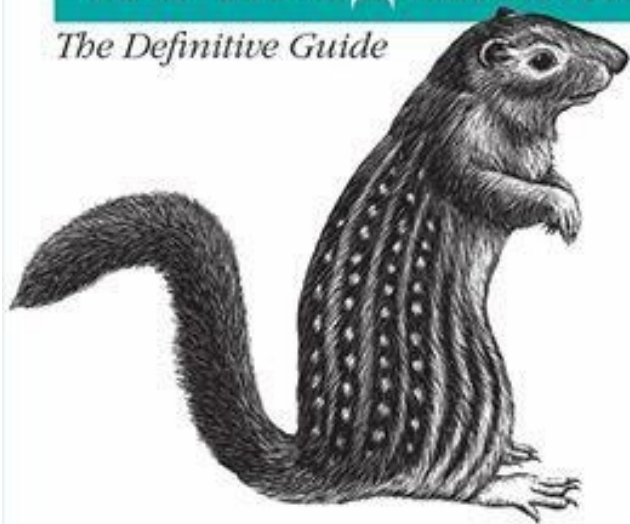
Подготовка к работе

1. Наличие знаний уровня MTCNA
(рекомендуется)
2. RouterOS 6.45 или новее
3. Все испытания строго **в лабораторных условиях** (настоятельно рекомендую)
4. Дефолт конфигурация 6.45+

— — —

РАЗ - РАЗ И В ПРОДАКШЕН

The Definitive Guide

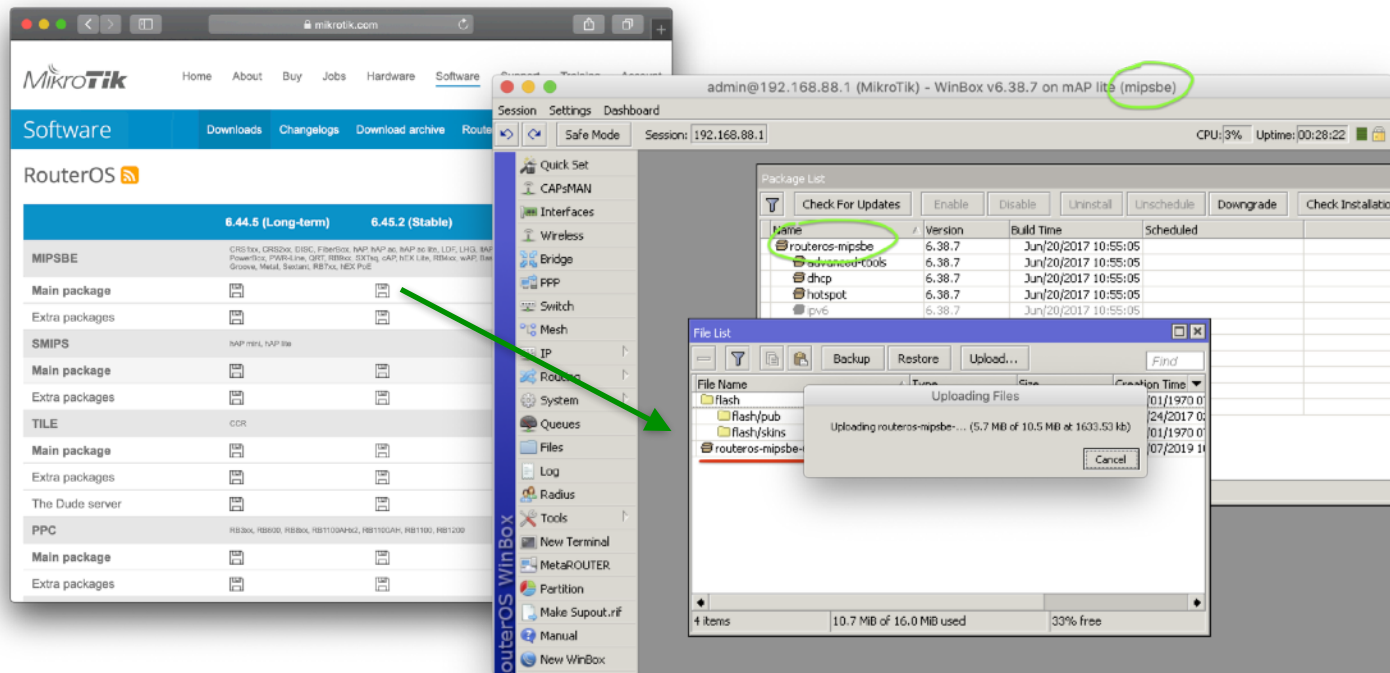


O'REILLY®

Россицкий Е.Б. & Ахметов С.Ю.

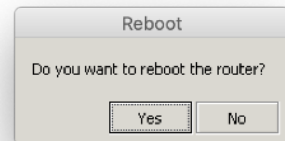
Пожалуйста!
Не применяйте методологию
раз-раз-продакшн на
исправно работающих
сетях!

Обновляем RouterOS до версии 6.45 или новее



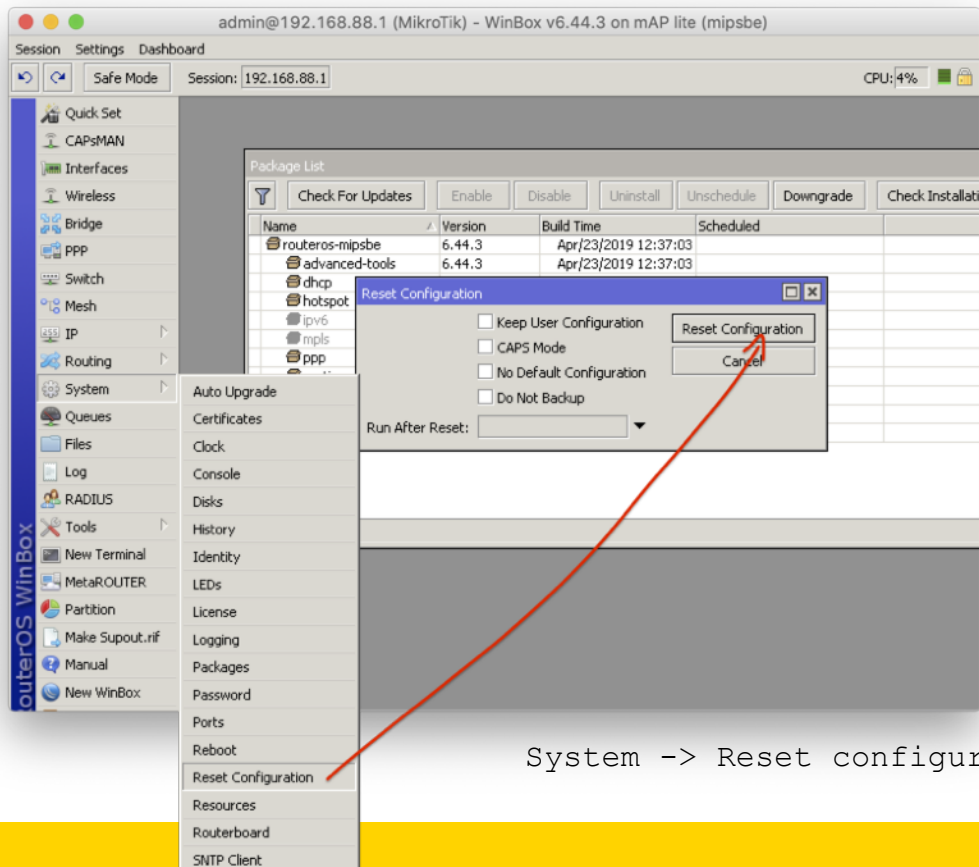
1. Качаем установочный пакет
www.mikrotik.com/download

2. Заливаем пакет в корень
файловой системы

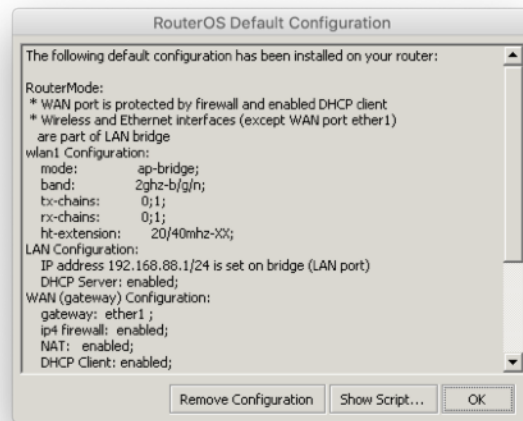


3. Перезагружаем

Сбрасываем RouterBoard к заводской v6.45+ конфигурации



Сброс на заводской конфиг
применит обновленные правила
файрволла, интерфейс листов,
улучшенные настройки
безопасности итп..



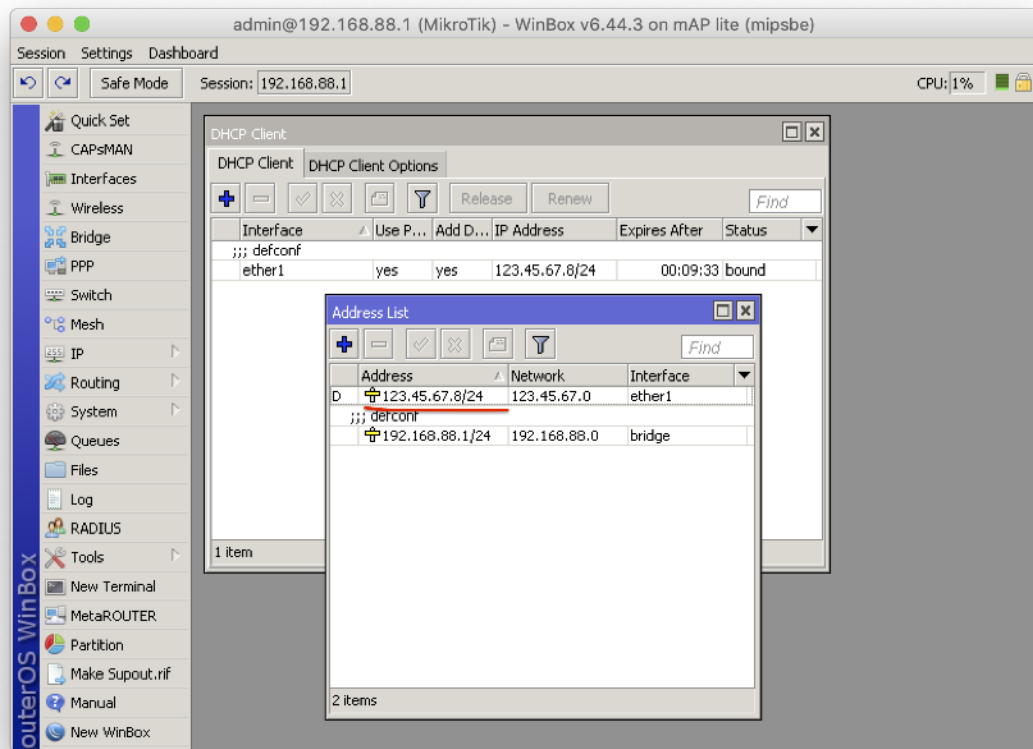
Общие системные настройки

План действий:

1. WAN IP/DNS адреса
2. Часовой пояс
3. Дата/время через NTP
4. Loopback bridge
5. IP pool

— — —

Адреса WAN IP и DNS для IKE2 VPN сервера

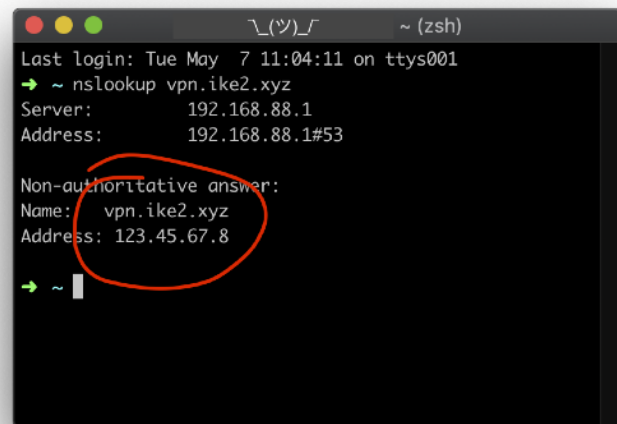


123.45.67.8 на WAN интерфейсе

Проверяем записи DNS:

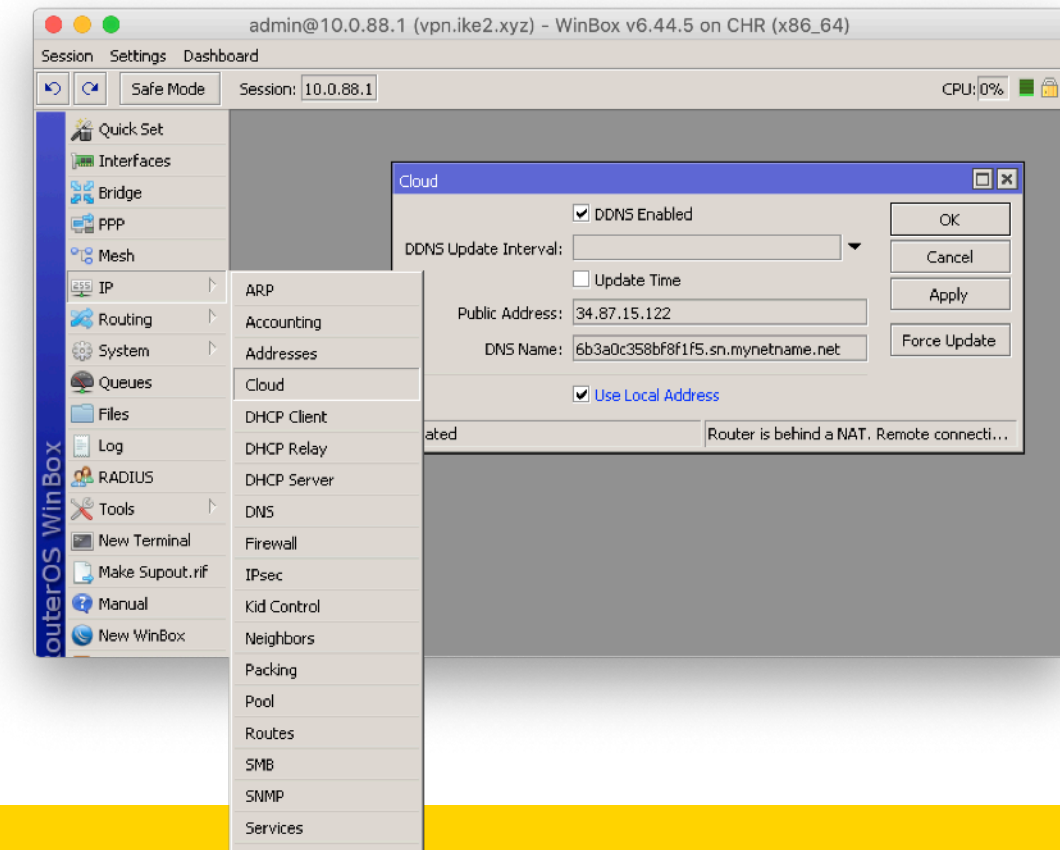
Имя: **vpn.ike2.xyz**

Адрес: **123.45.67.8**



* DNS записи настраиваются через панель управления **хостинг провайдера** или **регистратора доменного имени**

Нет денег на свой домен? 😎



IP -> Cloud

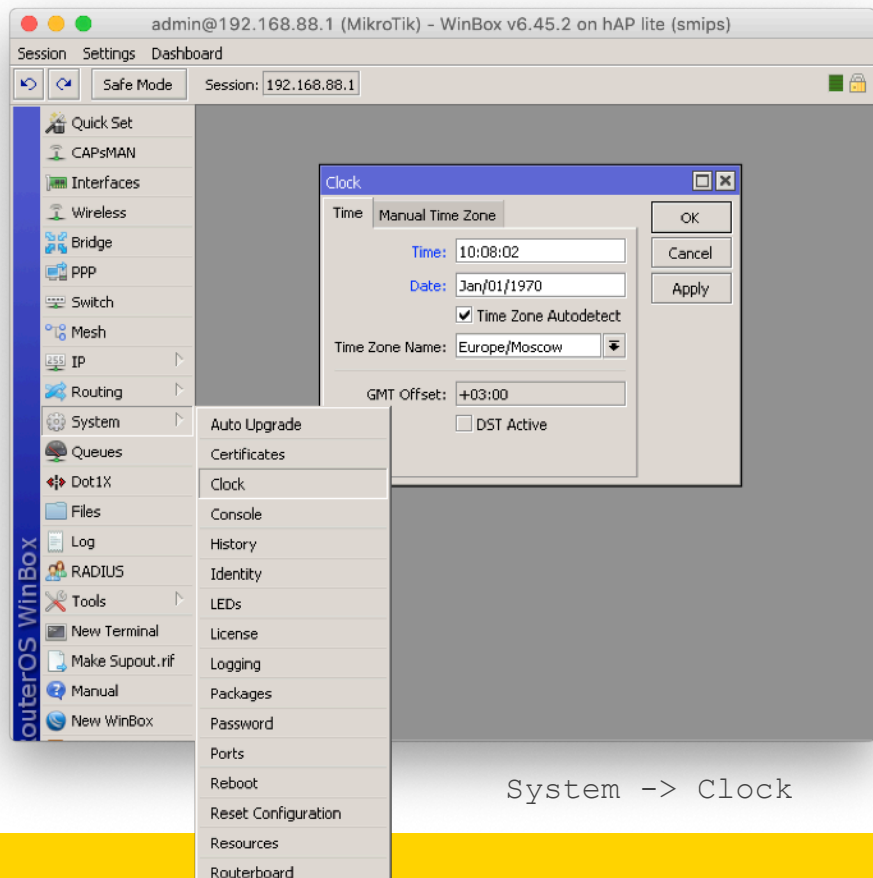
Проверяем записи DNS:

Имя: **blabla.sn.mynetname.net**

Адрес: **34.87.15.122**

Настраиваем часовой пояс

ЭТО ВАЖНО



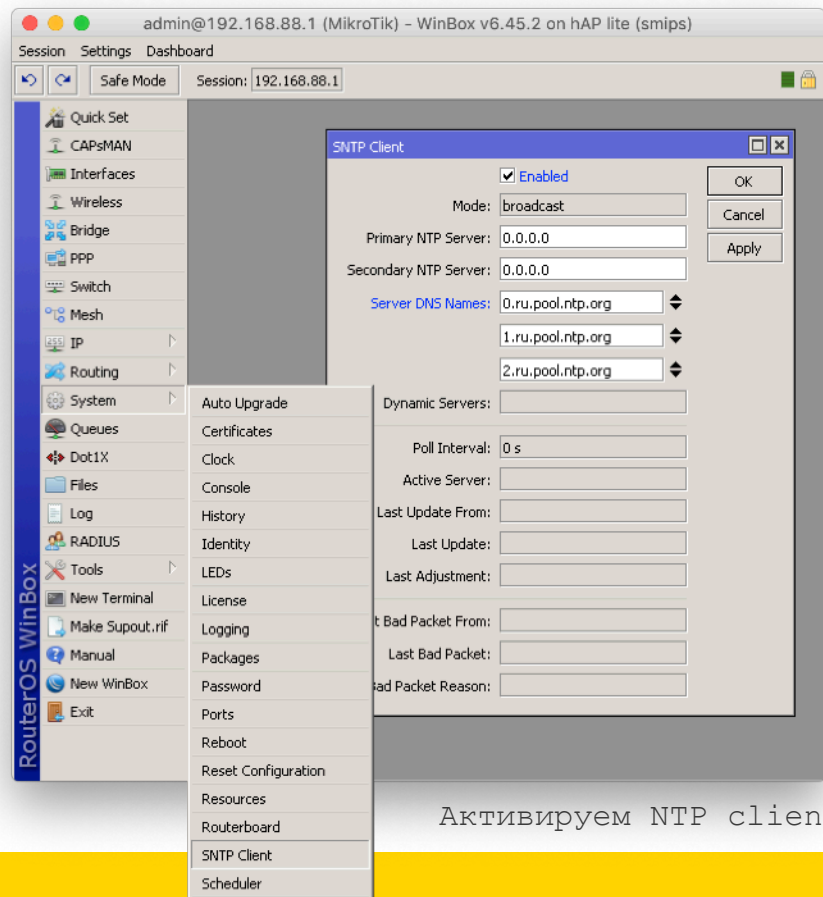
System -> Clock

```
/system clock set time-zone-  
name=Europe/Moscow
```

```
user@router:~$
```

Настройка автоматической синхронизации даты и времени

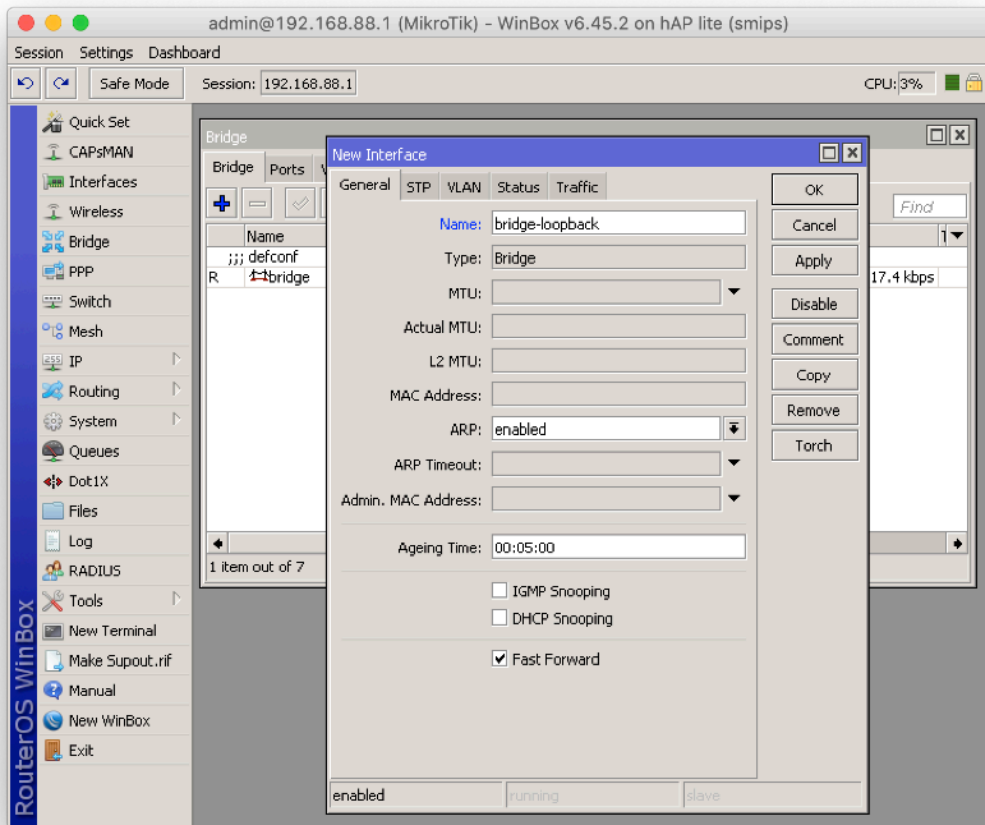
ЭТО ВАЖНО



Активируем NTP client

```
/system ntp client set enabled=yes  
server-dns-names=0.ru.pool.ntp.org,  
1.ru.pool.ntp.org,2.ru.pool.ntp.org
```

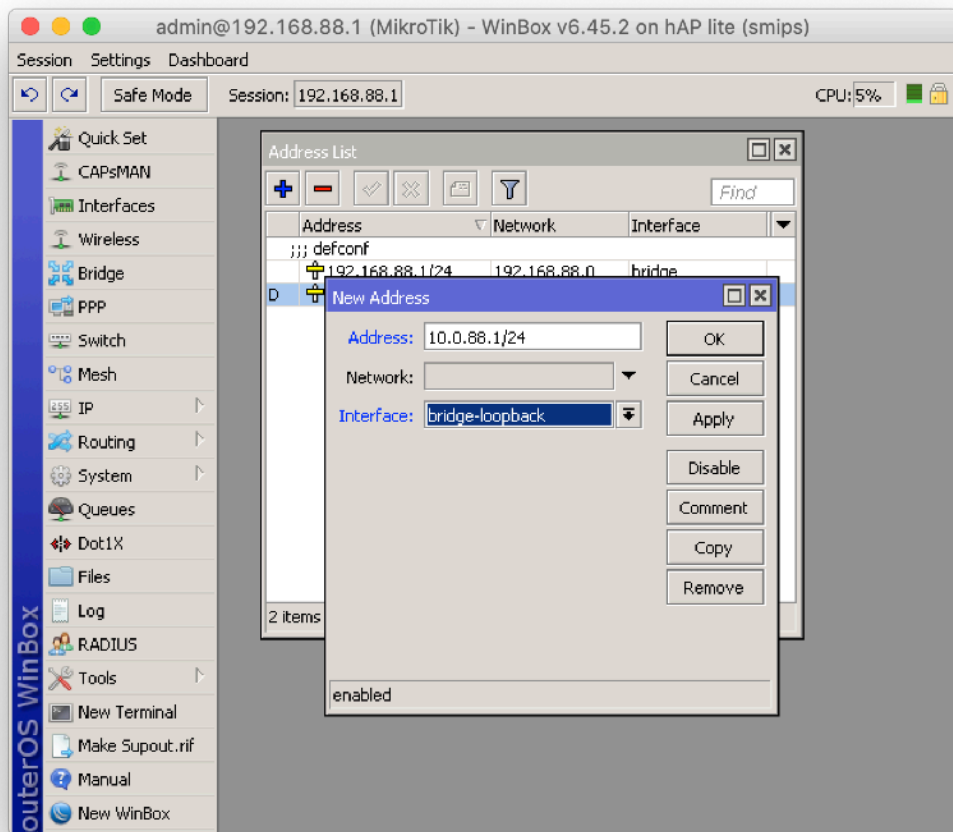
Добавляем новый loopback bridge



```
/interface bridge add  
name=bridge-loopback
```

```
usage=pl tag=loopback
```

Задаём IP адрес для loopback bridge

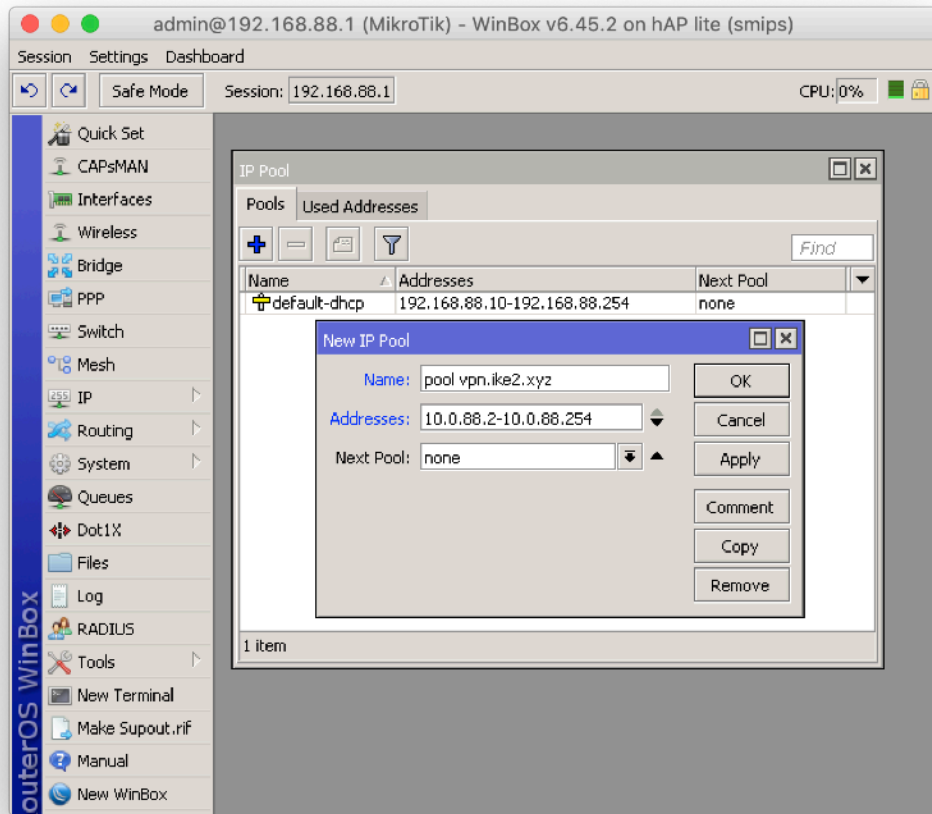


10.0.88.1

```
/ip address add  
address=10.0.88.1/24  
interface=bridge-loopback  
network=10.0.88.0
```

```
U6fMOLK=J0'0'88'0
```


Добавляем новый пул IP адресов для IKEv2 VPN клиентов



10.0.88.2-254

```
/ip pool add name="pool  
vpn.ike2.xyz"  
ranges=10.0.88.2-10.0.88.254
```

```
190d62=10*0*88*5-10*0*88*524
```

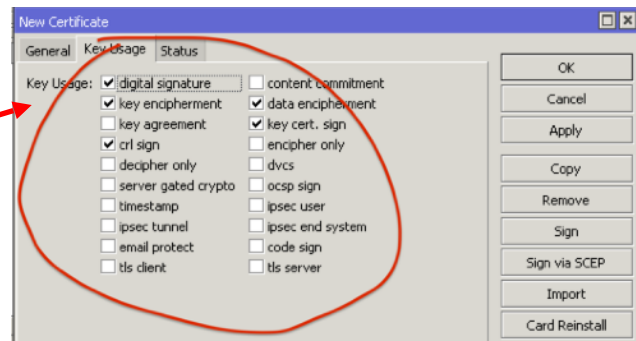
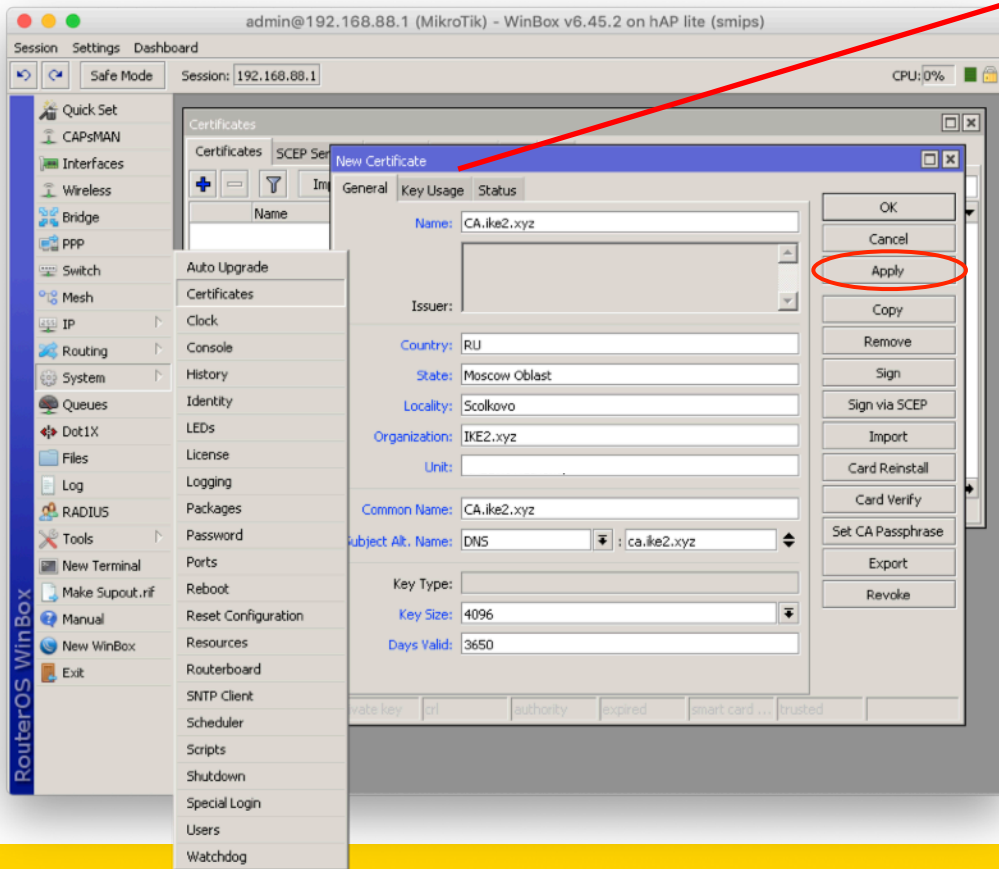
Генерируем правильные SSL сертификаты

План действий

1. Генерируем главный СА
2. Генерируем серверную пару
сертификат+ключ
3. Генерируем клиентские цифровые
подписи
4. Экспортируем клиентские подписи

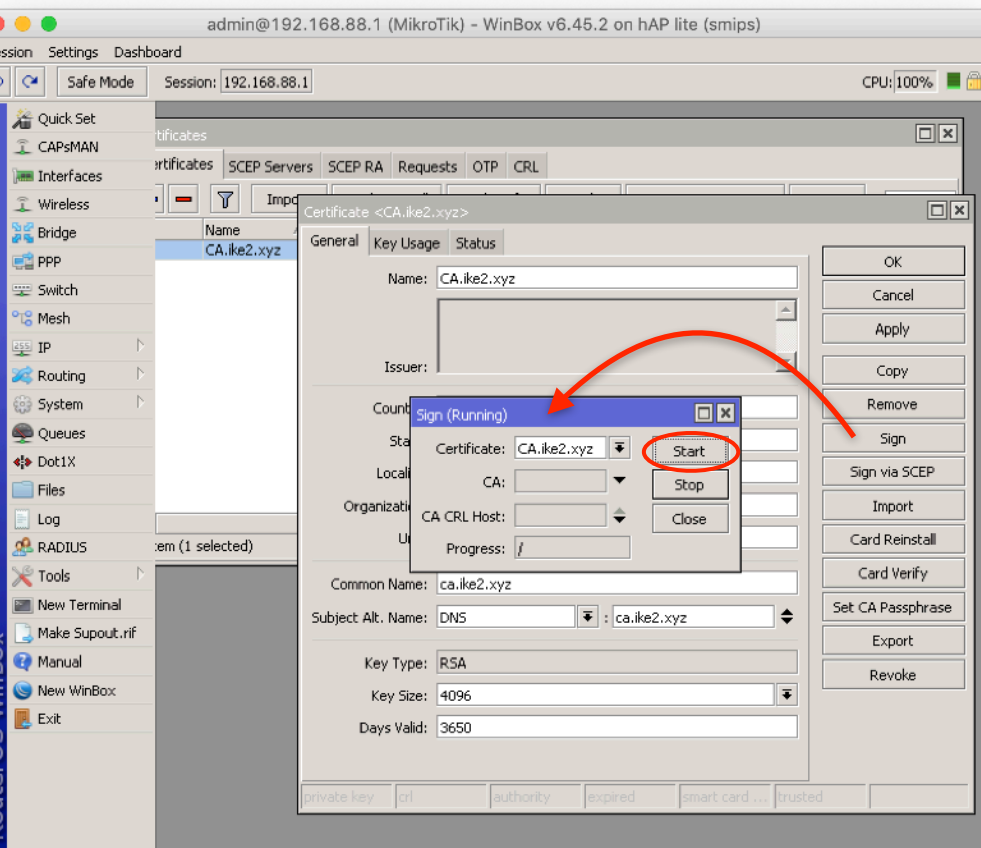
— — —

Генерируем главный CA SSL сертификат



```
/certificate add name=CA.ike2.xyz  
country=RU state="Moscow Oblast"  
locality=Scolkovo  
organization=IKE2.xyz common-  
name=ca.ike2.xyz subject-alt-  
name=DNS:ca.ike2.xyz key-size=4096  
days-valid=3650 trusted=yes key-  
usage=digital-signature,key-  
encipherment,data-encipherment,key-  
cert-sign,crl-sign
```

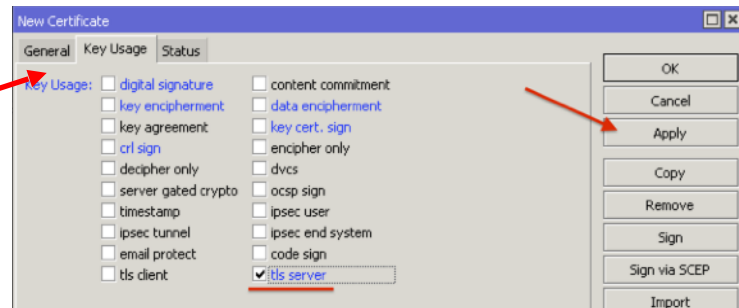
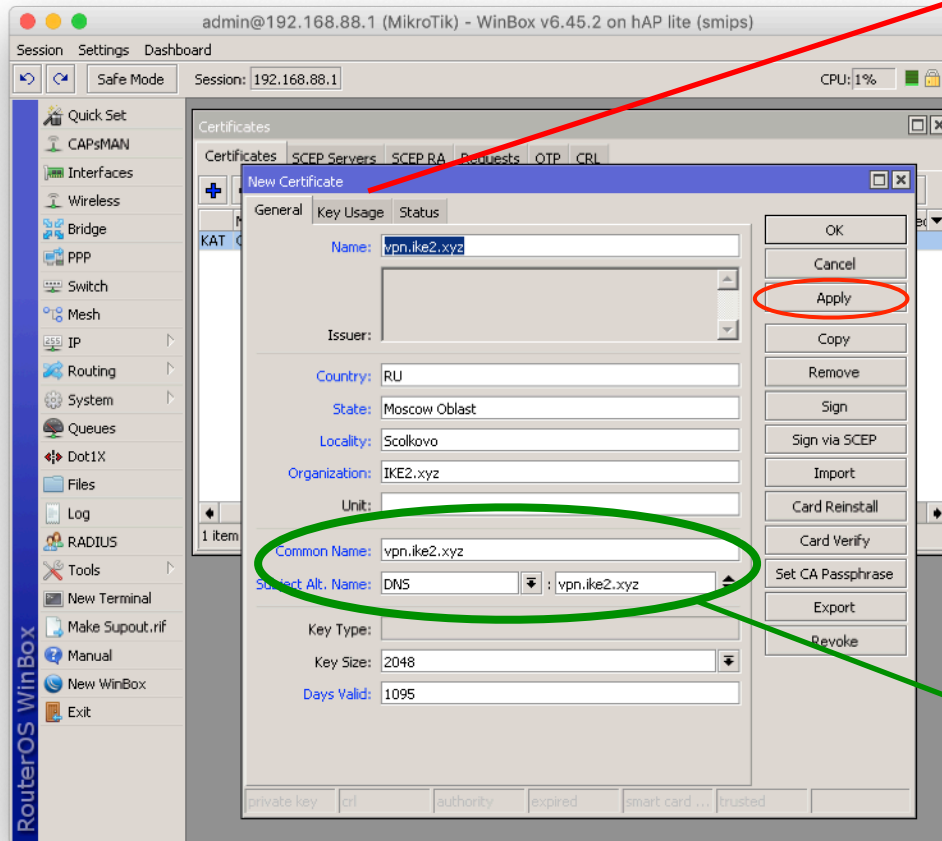
Само-подписываем новый CA SSL сертификат (*Certificate Authority*)



```
/certificate sign CA.ike2.xyz
```

**САМО-ПРОВОЗГЛАШЕНИЕ СЕБЯ
ГЛАВНЫМ АВТОРИТЕТОМ
В БАНАНОВОЙ КОРПОРАЦИИ**

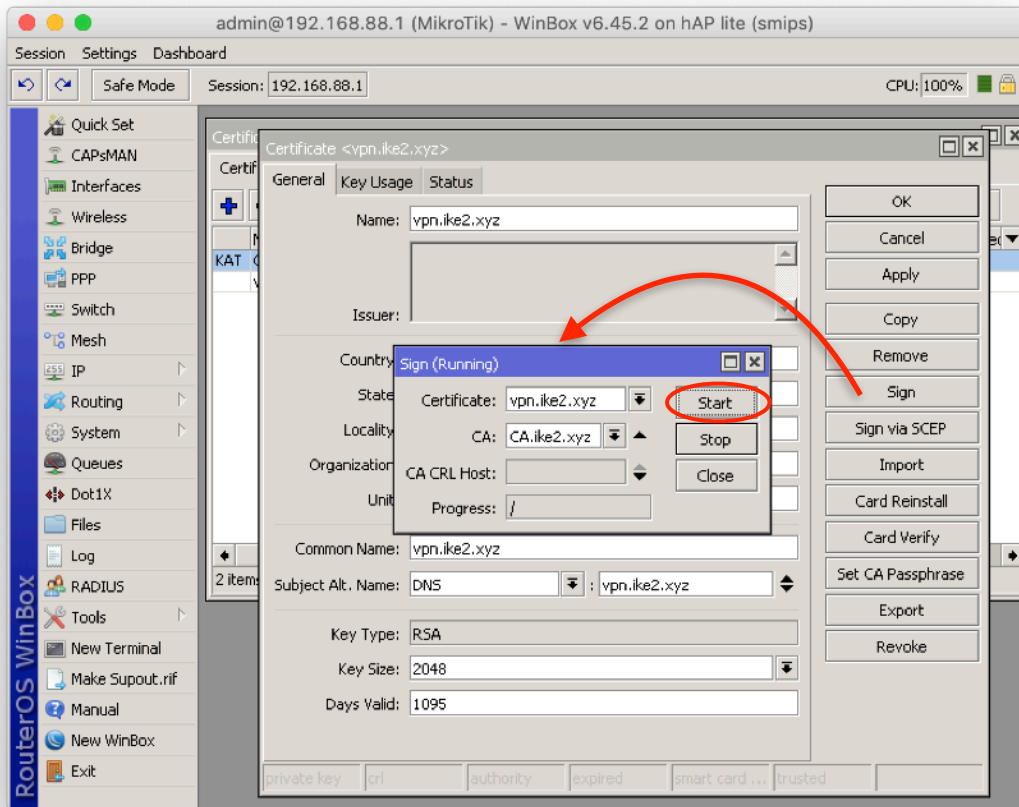
Генерируем серверный SSL сертификат



```
/certificate add name=vpn.ike2.xyz  
country=RU state="Moscow Oblast"  
locality=Scolkovo organization=IKE2.xyz  
common-name=vpn.ike2.xyz subject-alt-  
name=DNS:vpn.ike2.xyz key-size=2048  
days-valid=1095 trusted=yes key-  
usage=tls-server
```

vpn.ike2.xyz

Подписываем серверный сертификат у авторитета CA.ike2.xyz

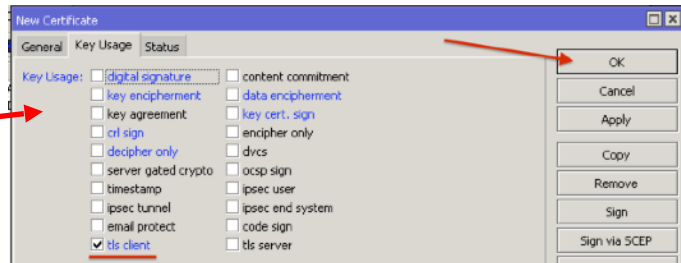
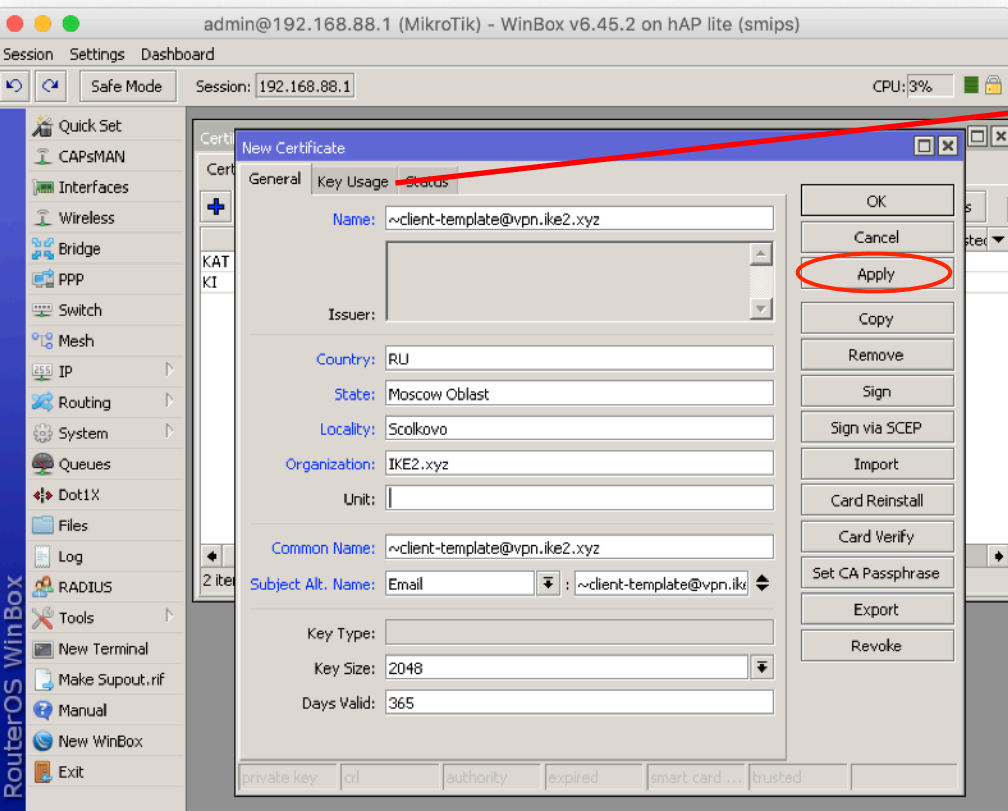


```
/certificate sign vpn.ike2.xyz
```

```
ca=CA.ike2.xyz
```

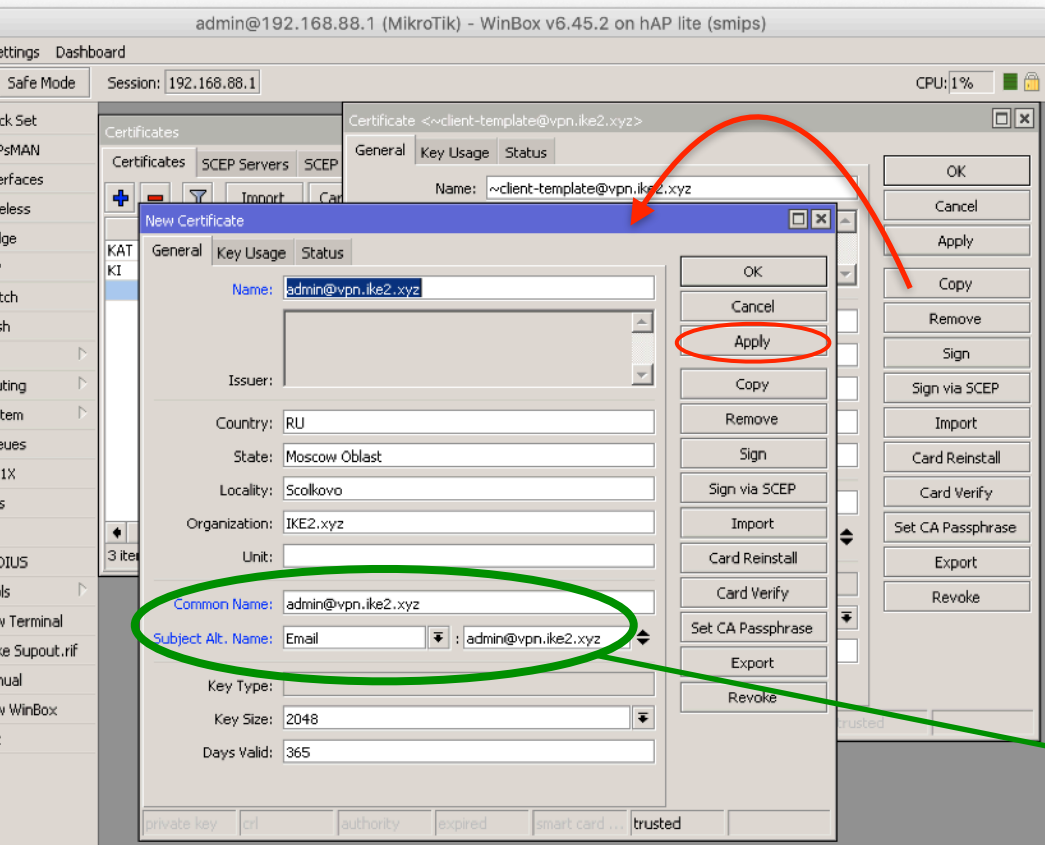
```
C9=CV*TK65*XΛ5
```

Создаем шаблон для тиражирования клиентских подписей



```
/certificate add name=~client-  
template@vpn.ike2.xyz country=RU  
state="Moscow Oblast"  
locality=Scolkovo  
organization=IKE2.xyz common-  
name=~client-template@vpn.ike2.xyz  
subject-alt-name=email:~client-  
template@vpn.ike2.xyz key-size=2048  
days-valid=365 trusted=yes key-  
usage=tls-client
```

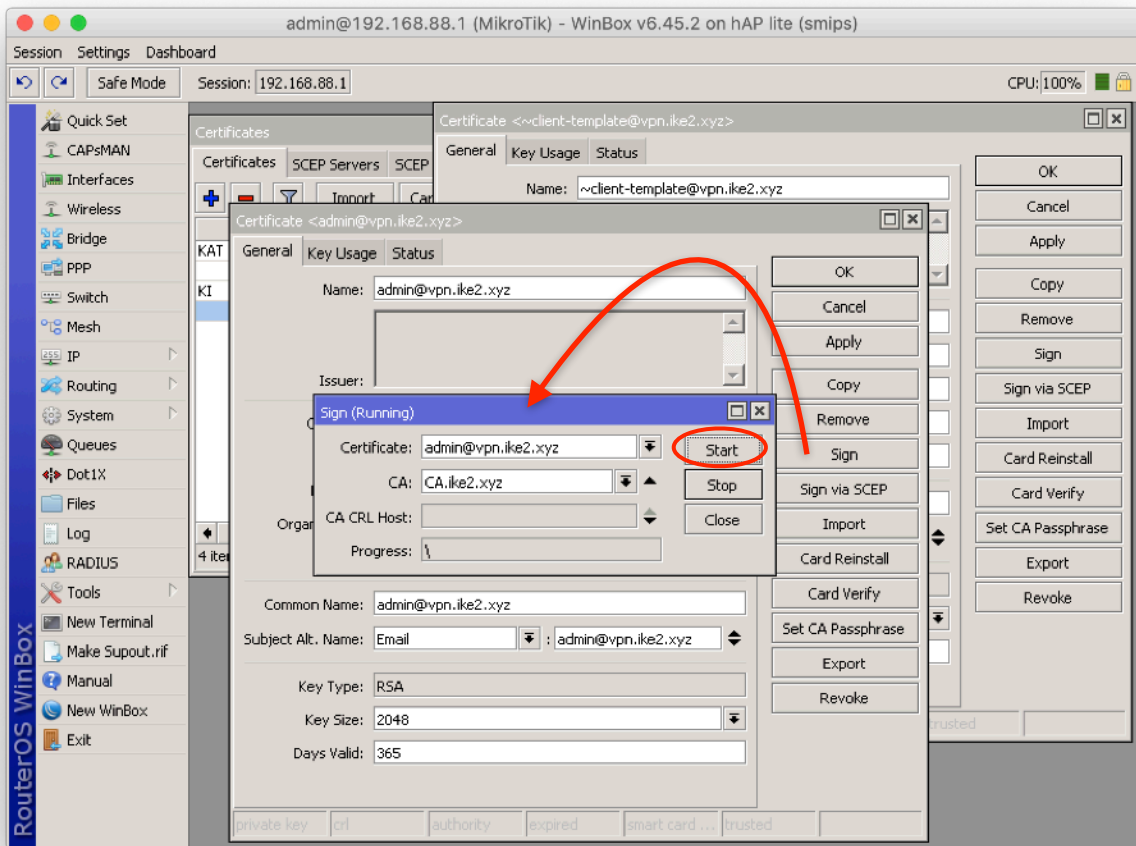
Создаем первую клиентскую подпись из заготовленного шаблона



```
/certificate add copy-from=~client-  
template@vpn.ike2.xyz  
name=admin@vpn.ike2.xyz common-  
name=admin@vpn.ike2.xyz subject-alt-  
name=email:admin@vpn.ike2.xyz
```

admin@vpn.ike2.xyz

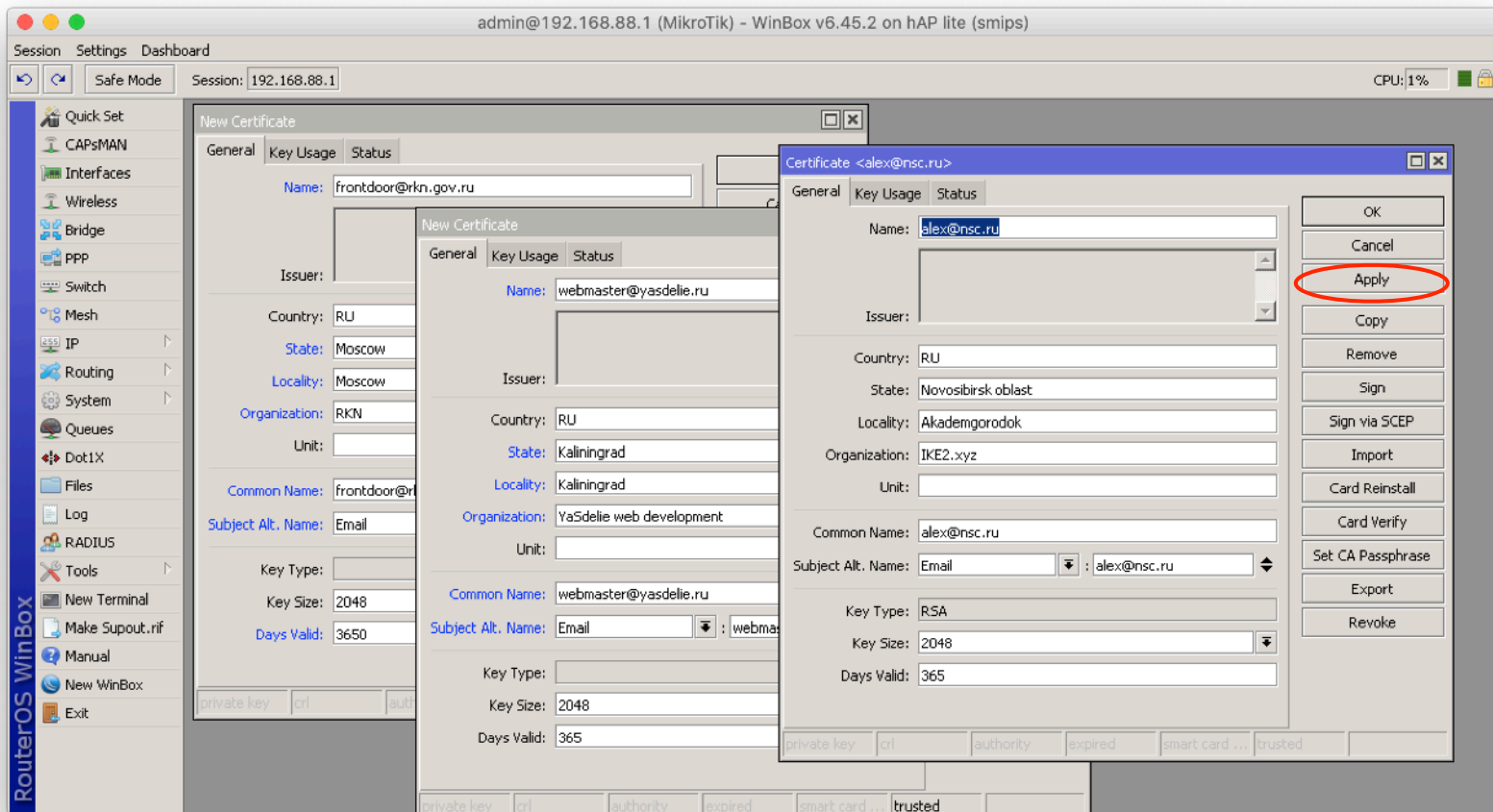
Подписываем клиентскую подпись у авторитета CA.ike2.xyz



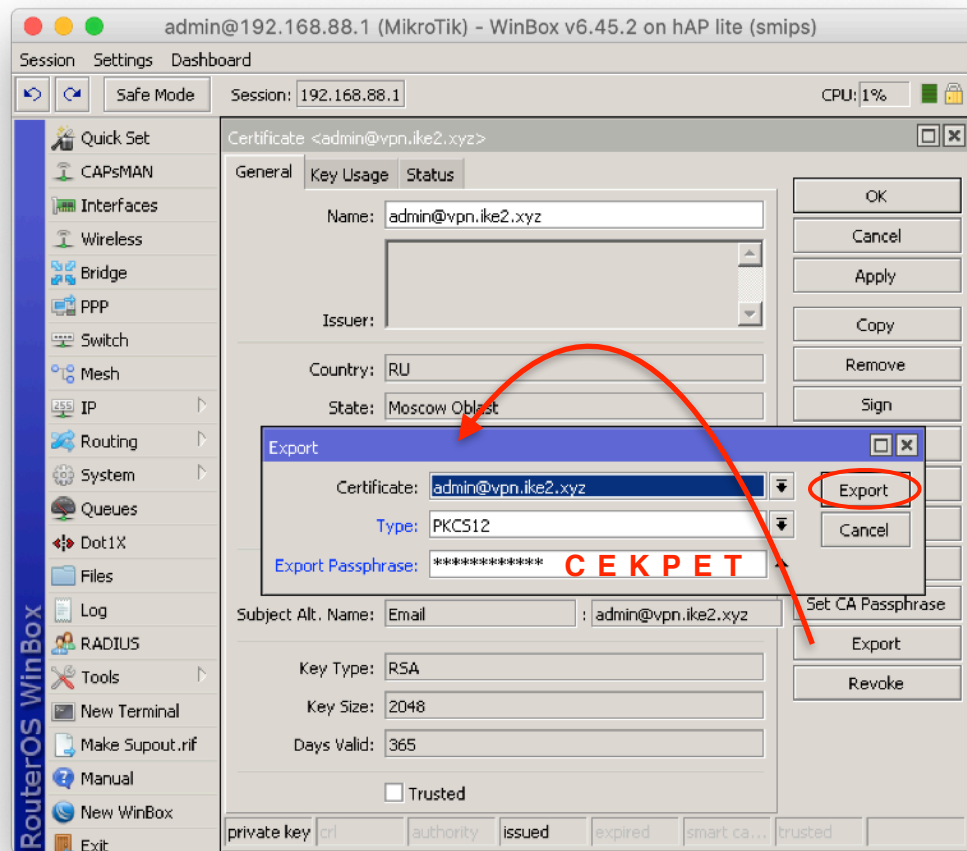
```
/certificate sign  
admin@vpn.ike2.xyz  
ca=CA.ike2.xyz
```

C9=Cv*IK65*xλs

Создаем остальные клиентские подписи из шаблона (по аналогии)



Экспортируем клиентскую подпись + приватный ключ в файл .p12

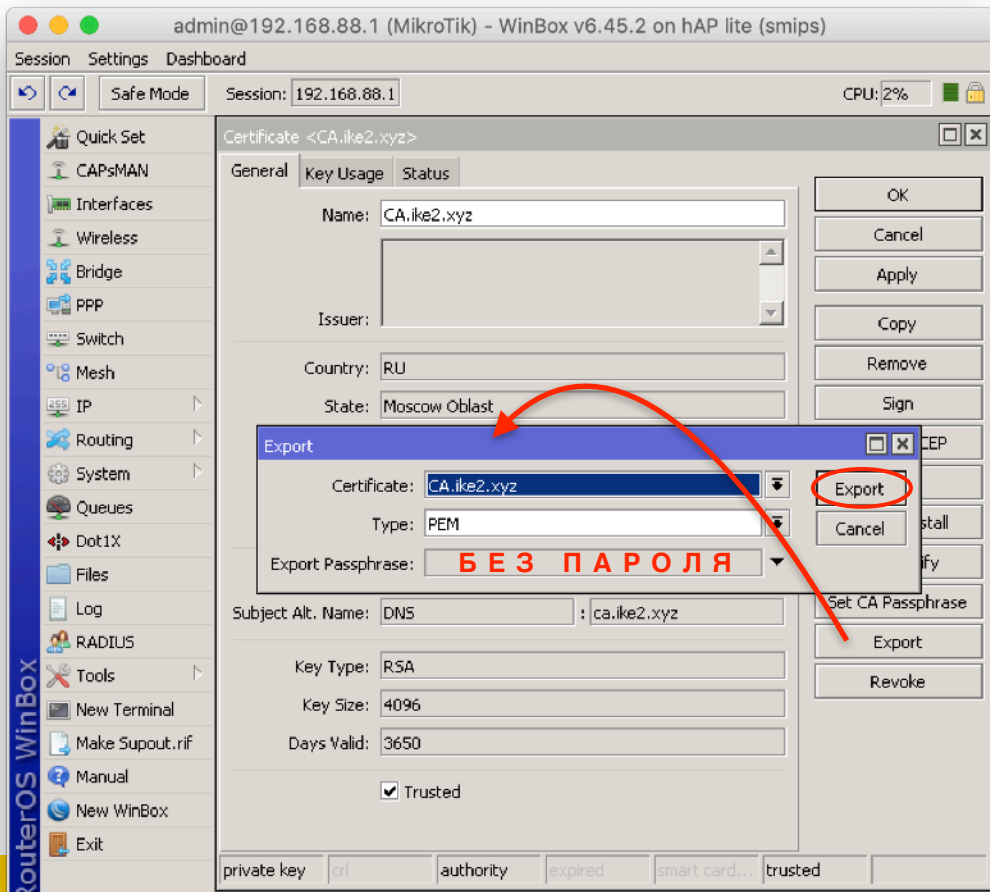


При экспорте **обязательно** указываем пароль.
Пустой пароль экспортирует сертификат без ключа.

Пароль храним в **секрете**.

```
/certificate export-certificate  
admin@vpn.ike2.xyz type=pkcs12  
export-passphrase=keepinsecret  
exboLf-b922bpl926=k66bTuz6C6f
```

Экспортируем сертификат авторитета CA в .crt файл



При экспорте **ни в коем случае** не указываем пароль.

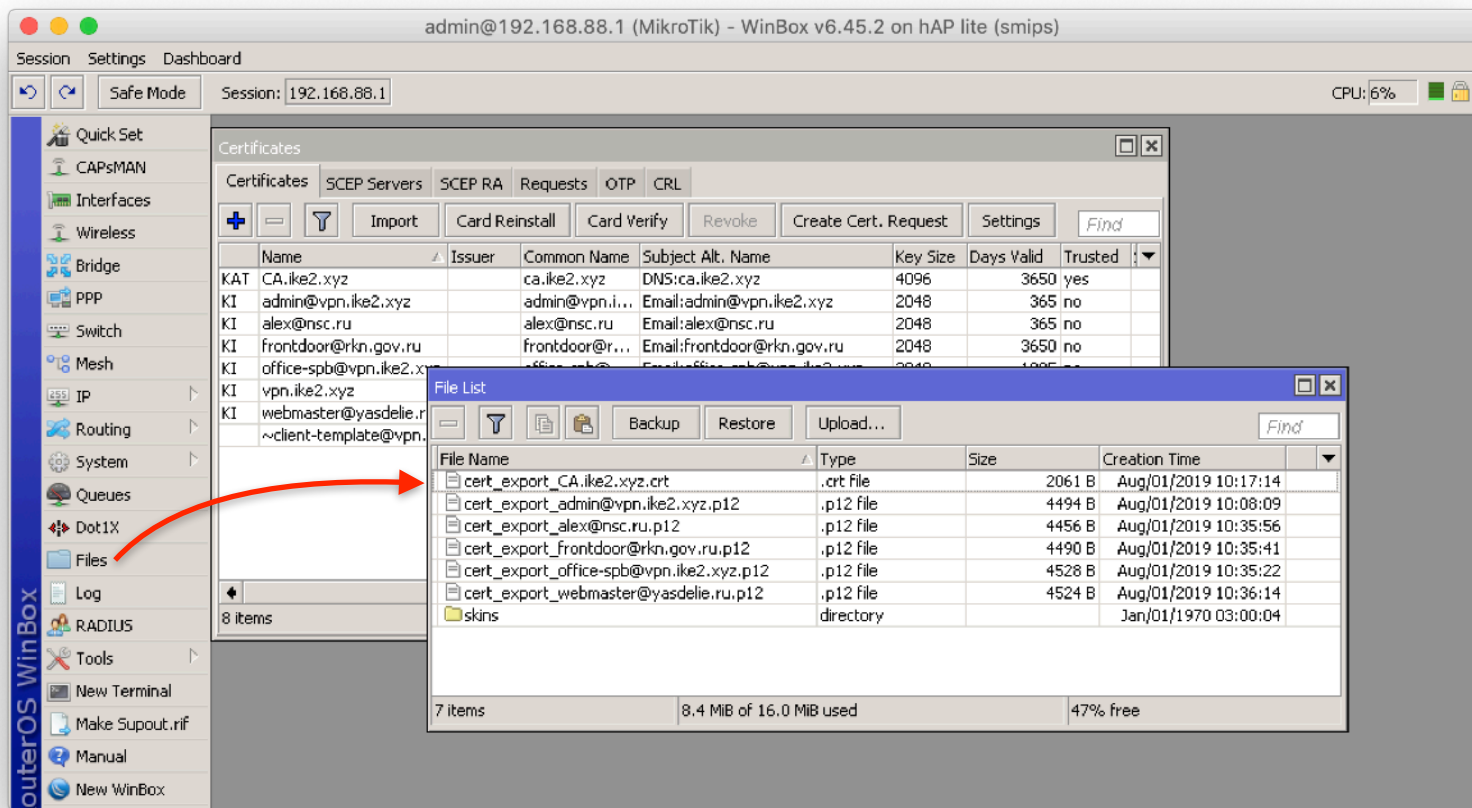
Экспорт **ключа СА** само-
провозглашенного **авторитета**

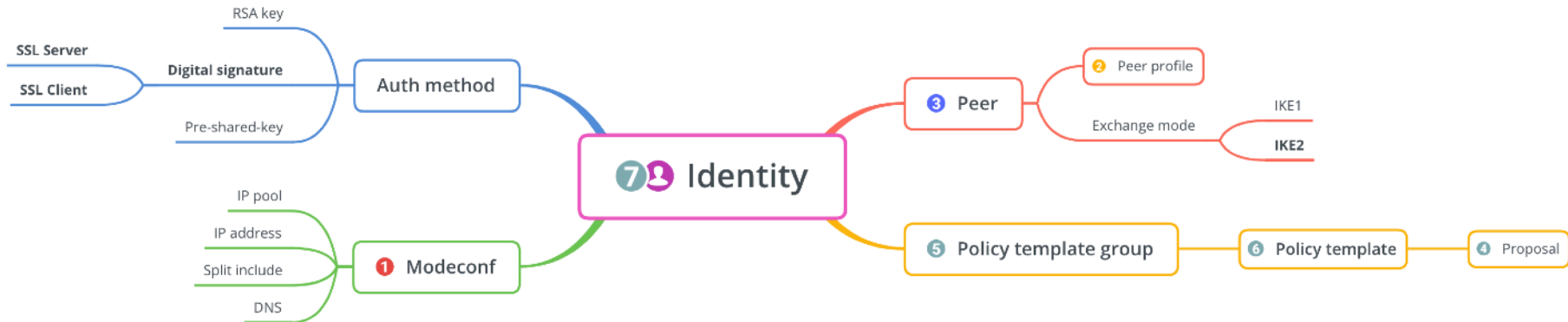
**УГРОЖАЕТ БЕЗОПАСНОСТИ
ВСЕМ ЖИТЕЛЯМ
БАНАНОВОЙ КОРПОРАЦИИ**

```
/certificate
```

```
export-certificate CA.ike2.xyz type=pem
```

Скачиваем с роутера экспортированный CA сертификат + клиентские подписи





Настройка IPSec

1. Настройка Mode Configs
2. Настройка Peer Profiles
3. Настройка Peers
4. Настройка Proposals
5. Настройка Policy Groups
6. Настройка Policy Template
7. Настройка Identities

What's new in 6.44

- *) ipsec - added account log message when user is successfully authenticated;
- *) ipsec - added basic pre-shared-key strength checks;
- *) ipsec - added new "remote-id" peer matcher;
- *) ipsec - allow to specify single address instead of IP pool under "mode-config";
- *) ipsec - fixed active connection killing when changing peer configuration;
- *) ipsec - fixed all policies not getting installed after startup (introduced in v6.43.8);
- *) ipsec - fixed stability issues after changing peer configuration (introduced in v6.43);
- *) ipsec - hide empty prefixes on "peer" menu;
- *) ipsec - improved invalid policy handling when a valid policy is uninstalled;
- *) ipsec - made dynamic "src-nat" rule more specific;
- *) ipsec - made peers autosort themselves based on reachability status;
- *) ipsec - moved "profile" menu outside "peer" menu;
- *) ipsec - properly detect AES-NI extension as hardware AEAD;
- *) ipsec - removed limitation that allowed only single "auth-method" with the same "exchange-mode" as responder;
- *) ipsec - require write policy for key generation;
- *) ike2 - added option to specify certificate chain;
- *) ike2 - added peer identity validation for RSA auth (disabled after upgrade);
- *) ike2 - allow to match responder peer by "my-id=fqdn" field;
- *) ike2 - fixed local address lookup when initiating new connection;
- *) ike2 - improved subsequent phase 2 initialization when no childs exist;
- *) ike2 - properly handle certificates with empty "Subject";
- *) ike2 - retry RSA signature validation with deduced digest from certificate;
- *) ike2 - send split networks over DHCP (option 249) to Windows initiators if DHCP Inform is received;
- *) ike2 - show weak pre-shared-key warning;

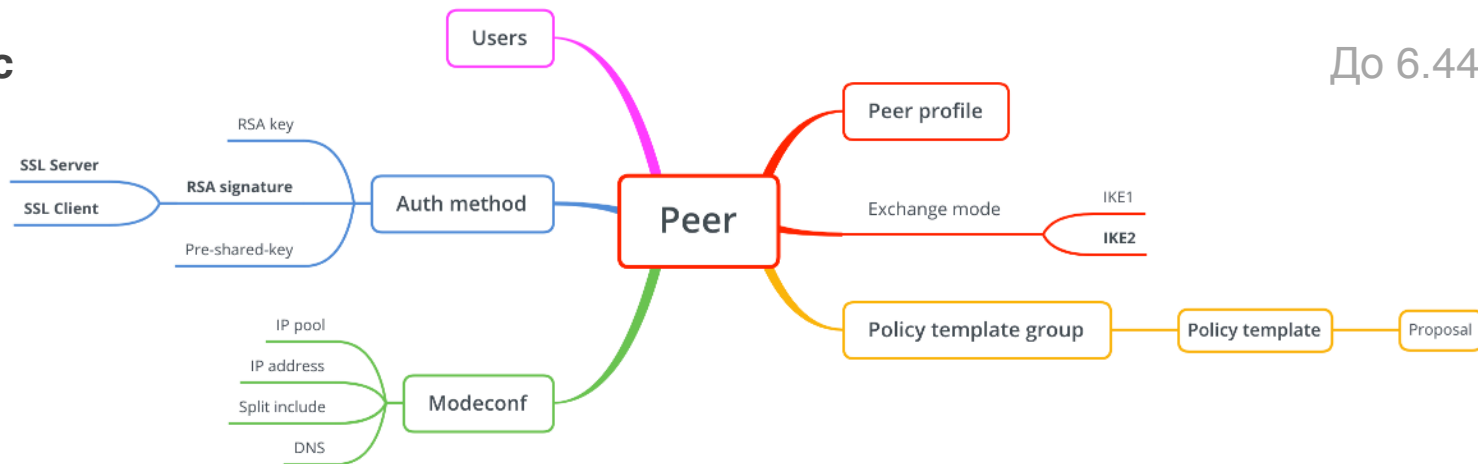
Ключевые изменения в RouterOS 6.44

- *) ipsec - added new "remote-id" peer matcher;
- *) ipsec - allow to specify single address instead of IP pool under "mode-config";
- *) ipsec - moved "profile" menu outside "peer" menu;
- *) ipsec - removed limitation that allowed only single "auth-method" with the same "exchange-mode" as responder;

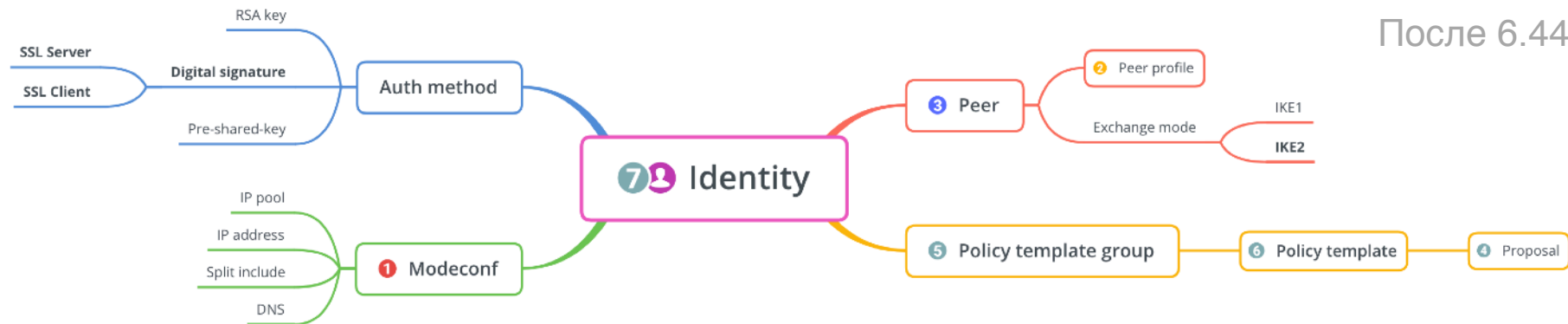
- *) ike2 - added option to specify certificate chain;
- *) ike2 - added peer identity validation for RSA auth (disabled after upgrade);
- *) ike2 - allow to match responder peer by "my-id=fqdn" field;
- *) ike2 - send split networks over DHCP (option 249) to Windows initiators if DHCP Inform is received;

Структура IPsec

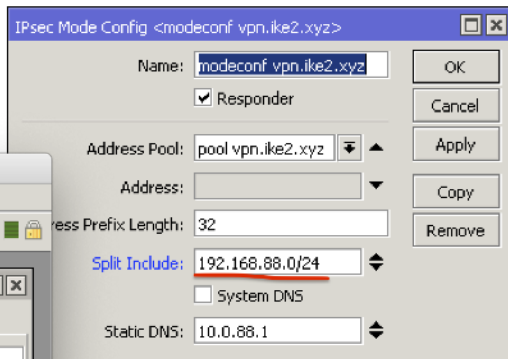
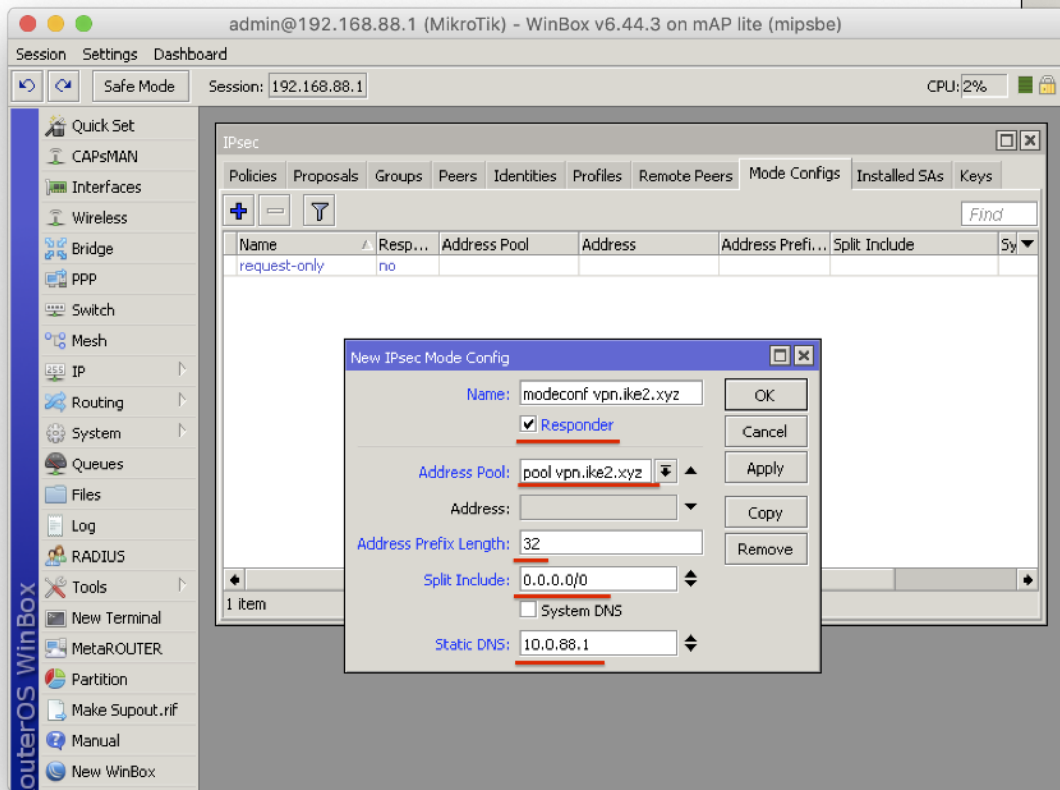
До 6.44



После 6.44

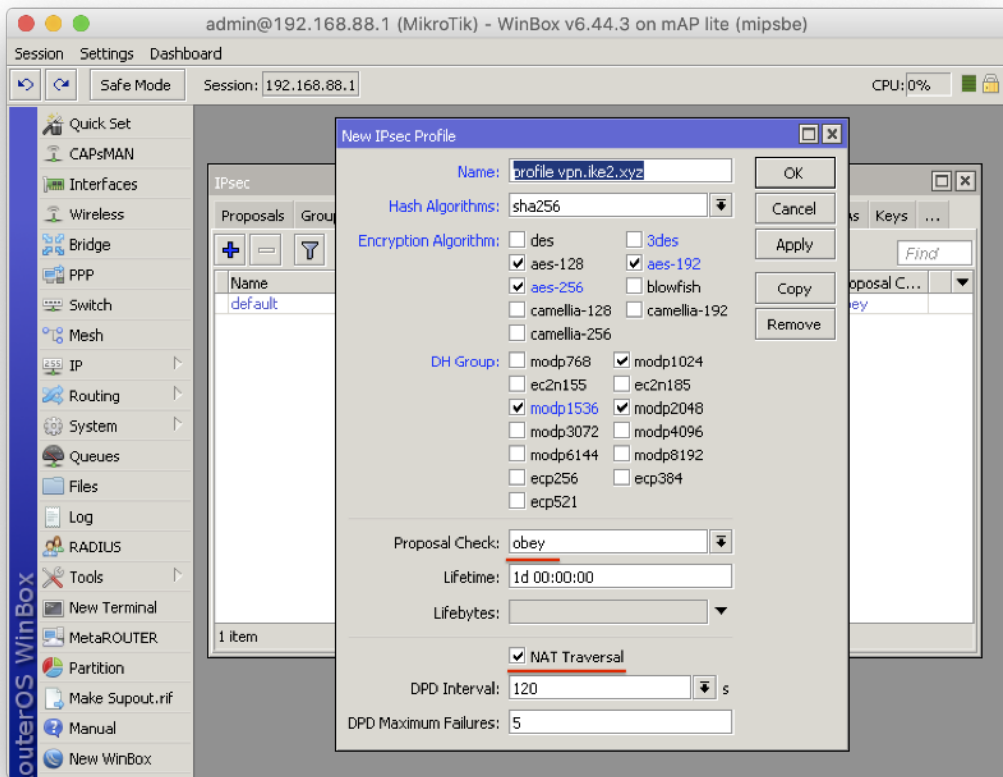


1. Настройка нового IPsec mode config



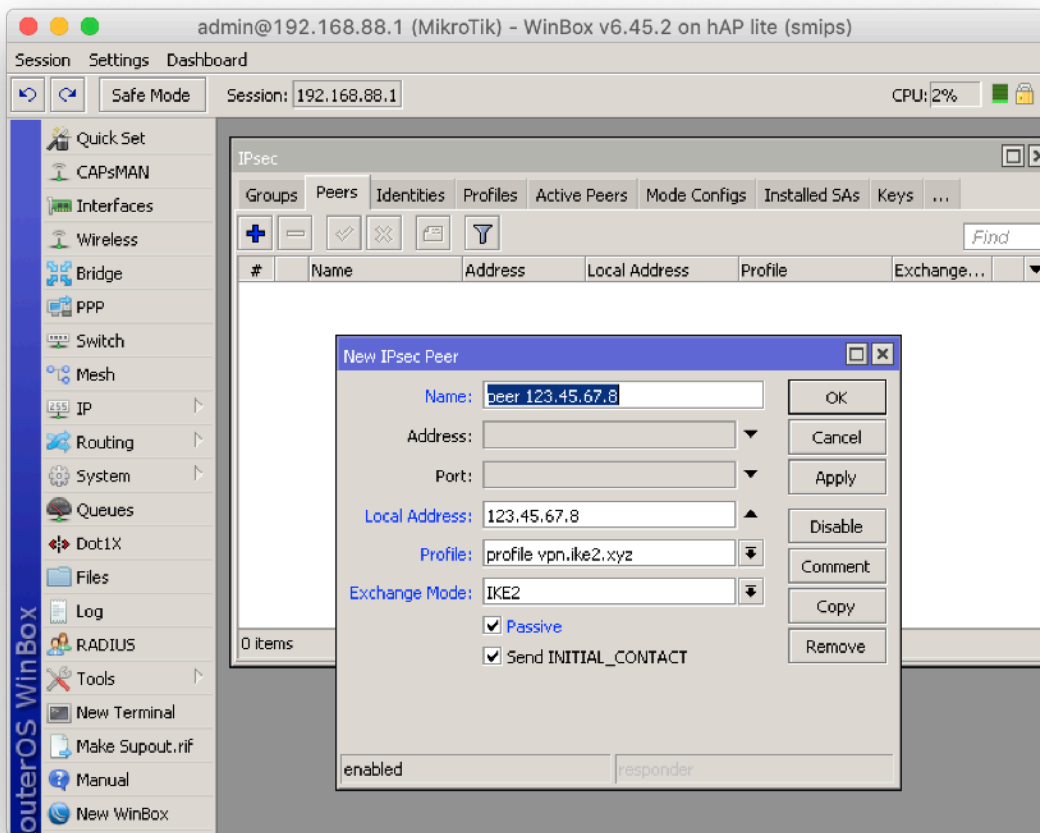
```
/ip ipsec mode-config
add address-pool="pool
vpn.ike2.xyz" address-prefix-
length=32 name="modeconf
vpn.ike2.xyz" split-
include=0.0.0.0/0 static-
dns=10.0.88.1 system-dns=no
```

2. Настройка нового IPSec peer profile (фаза 1)



```
/ip ipsec profile add dh-  
group=modp2048,modp1536,modp10  
24 enc-  
algorithm=aes-256,aes-192,aes-  
128 hash-algorithm=sha256  
name="profile.vpn.ike2.xyz"  
nat-traversal=yes proposal-  
check=obey
```

3. Создание нового IPsec peer на публичном IP адресе (режим IKE2)

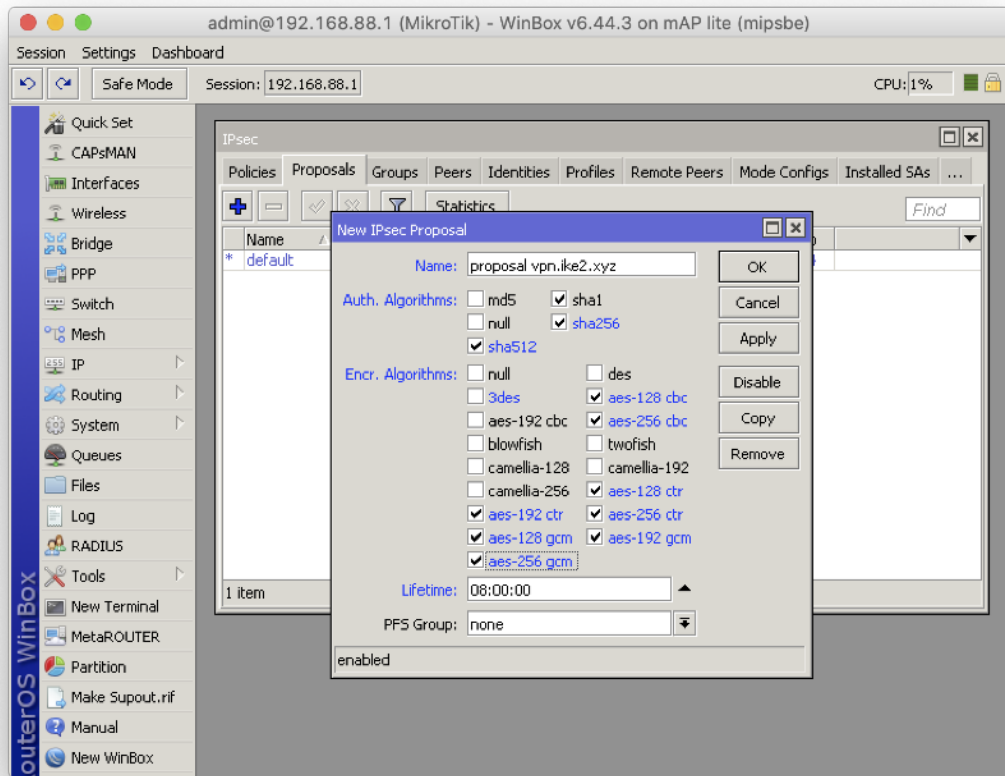


Принимаем клиентов со всех адресов **0.0.0.0/0**

Принимаем клиентов только на адрес **123.45.67.8**

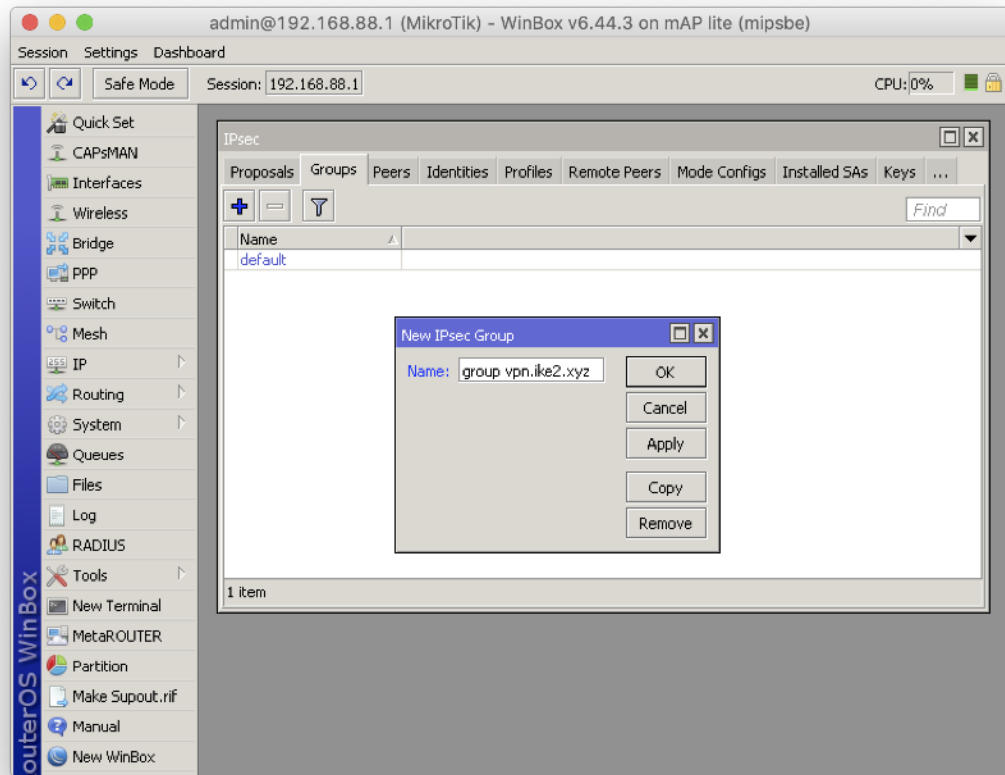
```
/ip ipsec peer add exchange-  
mode=ike2 address=0.0.0.0/0  
local-address=123.45.67.8  
name="peer 123.45.67.8"  
passive=yes send-initial-  
contact=yes profile="profile  
vpn.ike2.xyz"
```

4. Настройка нового IPsec proposal (фаза 2)



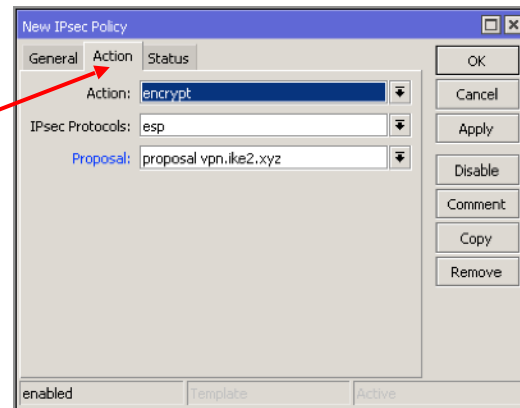
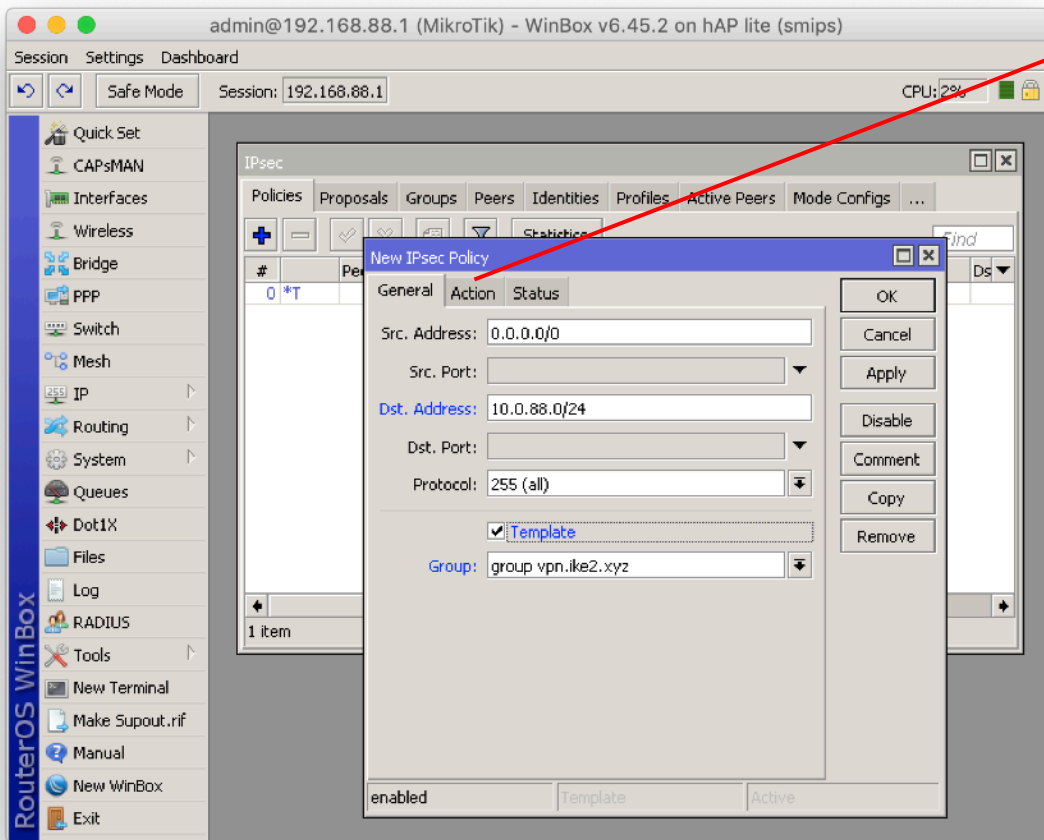
```
/ip ipsec proposal add auth-  
algorithms=sha512,sha256,sha1  
enc-algorithms=aes-256-  
cbc,aes-256-ctr,aes-256-  
gcm,aes-192-ctr,aes-192-  
gcm,aes-128-cbc,aes-128-  
ctr,aes-128-gcm lifetime=8h  
name="proposal vpn.ike2.xyz"  
pfs-group=none
```

5. Добавление новой IPSec policy group



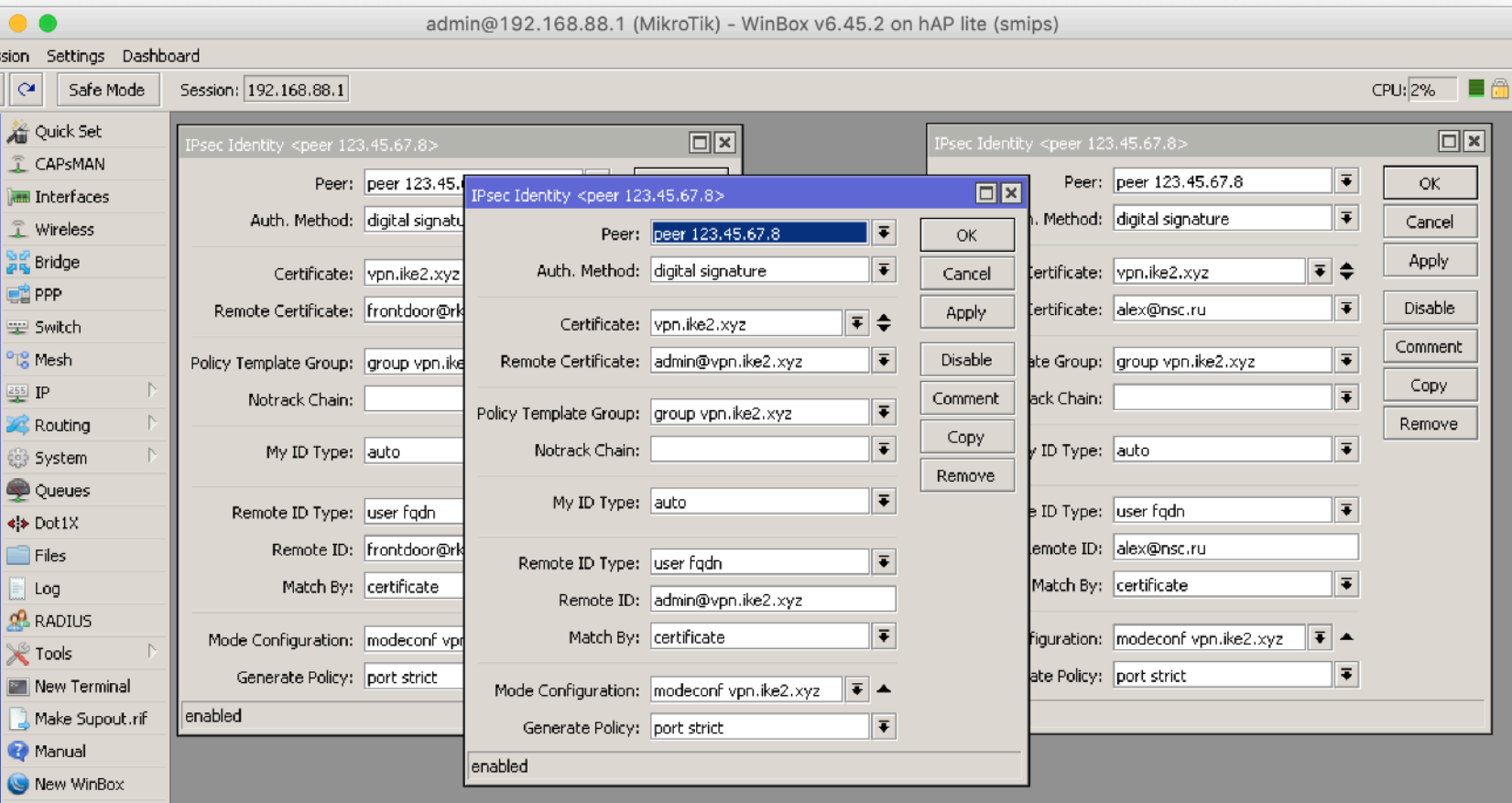
```
/ip ipsec policy group  
add name="group vpn.ike2.xyz"
```

6. Настройка нового шаблона IPsec policy



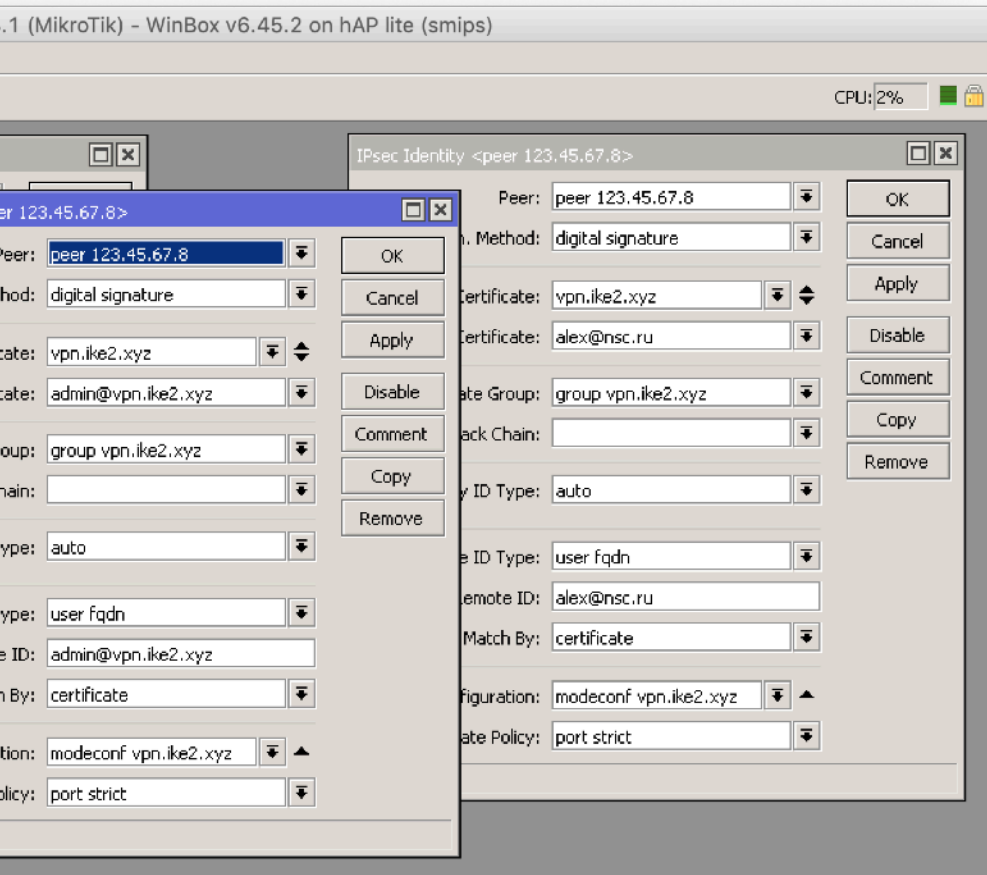
```
/ip ipsec policy add template=yes  
dst-address=10.0.88.0/24  
protocol=all src-address=0.0.0.0/0  
group="group vpn.ike2.xyz"  
proposal="proposal vpn.ike2.xyz"  
ipsec-protocols=esp action=encrypt
```

7. Внимательно создаем IPsec identities для каждого клиента



```
/ip ipsec identity add auth-method=digital-  
signature certificate=vpn.ike2.xyz remote-  
certificate=admin@vpn.ike2.xyz generate-
```


Внимательно создаем IPsec identities для каждого клиента



```
/ip ipsec identity add auth-method=digital-  
signature certificate=vpn.ike2.xyz remote-  
certificate=admin@vpn.ike2.xyz generate-  
policy=port-strict match-by=certificate mode-  
config="modeconf vpn.ike2.xyz" peer="peer  
123.45.67.8" policy-template-group="group  
vpn.ike2.xyz" remote-id=user-  
fqdn:admin@vpn.ike2.xyz
```

```
/ip ipsec identity add auth-method=digital-  
signature certificate=vpn.ike2.xyz remote-  
certificate=alex@nsc.ru generate-policy=port-strict  
match-by=certificate mode-config="modeconf  
vpn.ike2.xyz" peer="peer 123.45.67.8" policy-  
template-group="group vpn.ike2.xyz" remote-id=user-  
fqdn:alex@nsc.ru
```

Настройка Firewall

План действий

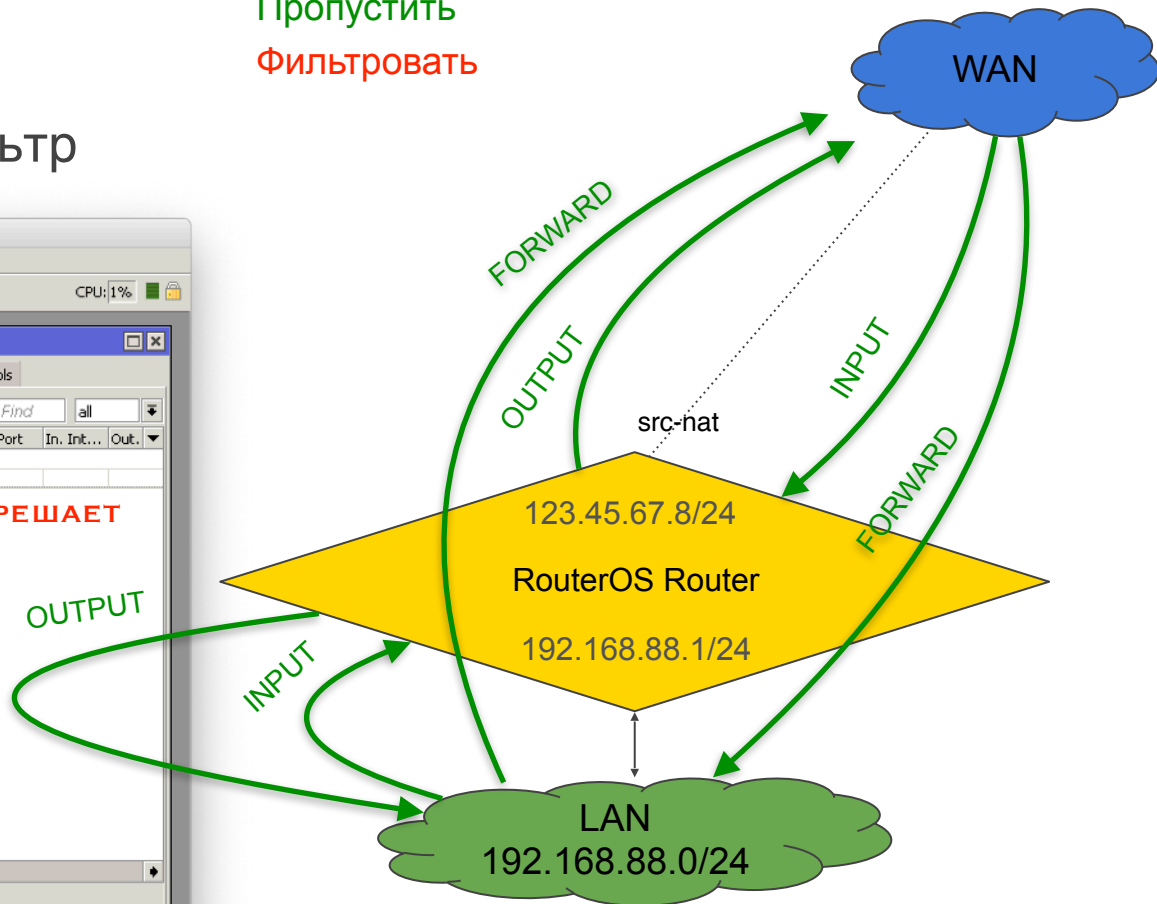
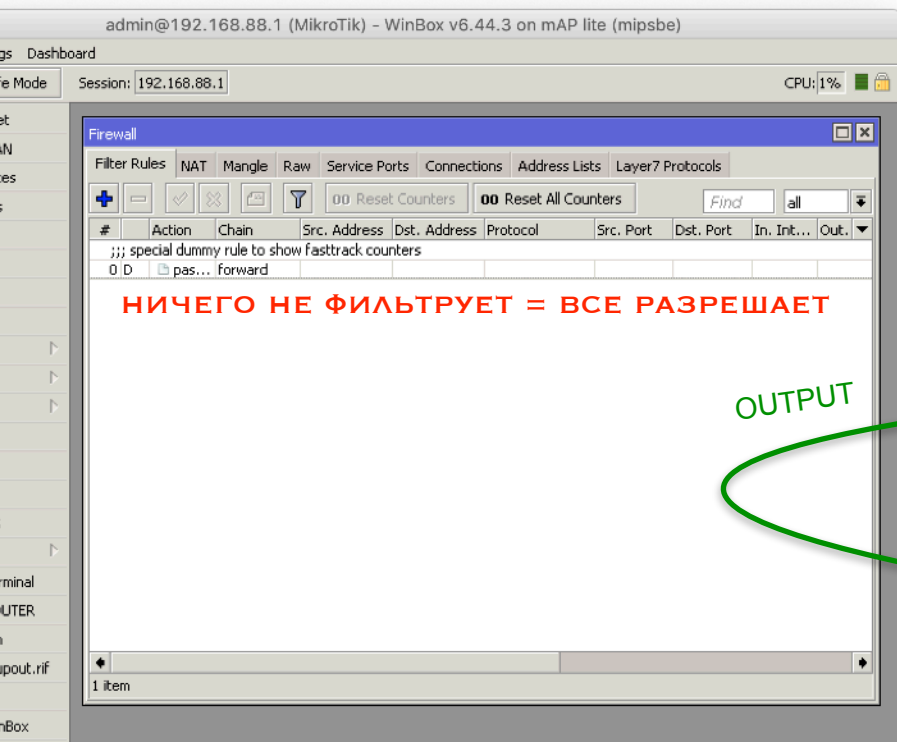
1. Краткий обзор стандартного Firewall
2. Правила для подключения к роутеру через IPSec
3. Правила для трафика через VPN соединение



АХТУНГ

Пропустить
Фильтровать

Пустой FIREWALL фильтр



Настройка Firewall

Краткий обзор стандартного фильтра (MTCNA)

Краткий обзор стандартного Firewall фильтра RouterOS 6.45

Firewall

Filter Rules

NAT

Mangle

Raw

Service Ports

Connections

Address Lists

Layer7 Protocols

00 Reset Counters

00 Reset All Counters

Find

input

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Int...	Out. I...	In. Int...	Out. I...	Src. A...	Dst. A...	Bytes	Packets
;;; defconf: accept established,related,untracked															
1	<div>✓</div> acc...	input												5.5 MiB	61 567
;;; defconf: drop invalid															
2	<div>✗</div> drop	input												341 B	6
;;; defconf: accept ICMP															
3	<div>✓</div> acc...	input			1 (icmp)									0 B	0
;;; defconf: accept to local loopback (for CAPsMAN)															
4	<div>✓</div> acc...	input		127.0.0.1										0 B	0
;;; defconf: drop all not coming from LAN															
5	<div>✗</div> drop	input								lLAN				201.2 KiB	1 096

5 items out of 12

Firewall															
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols															
<div><div><div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div><div><div>00 Reset Counters</div><div>00 Reset All Counters</div></div><div><div>Find</div><div>forward</div></div></div></div>															
#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Int...	Out. I...	In. Int...	Out. I...	Src. A...	Dst. A...	Bytes	Packets
;;; special dummy rule to show fasttrack counters															
0	D	pas...	forward											190.5 MIB	306 733
;;; defconf: accept in ipsec policy															
6	✓	acc...	forward											0 B	0
;;; defconf: accept out ipsec policy															
7	✓	acc...	forward											0 B	0
;;; defconf: fasttrack															
8	▶	fas...	forward											8.0 MIB	53 920
;;; defconf: accept established,related, untracked															
9	✓	acc...	forward											8.0 MIB	53 920
;;; defconf: drop invalid															
10	✗	drop	forward											1060.4 KIB	1 893
;;; defconf: drop all from WAN not DSTNATed															
11	✗	drop	forward							WAN				0 B	0
7 items out of 12															

#Input Chain Rules

```
/ip firewall filter
```

```
add action=accept chain=input comment="defconf: accept established,related,untracked" connection-  
state=established,related,untracked
```

```
add action=drop chain=input comment="defconf: drop invalid" connection-state=invalid
```

```
add action=accept chain=input comment="defconf: accept ICMP" protocol=icmp
```

```
add action=accept chain=input comment="defconf: accept to local loopback (for CAPsMAN)" dst-address=127.0.0.1
```

```
add action=drop chain=input comment="defconf: drop all not coming from LAN" in-interface-list=!LAN
```

#Forward Chain Rules

```
/ip firewall filter
```

```
add action=accept chain=forward comment="defconf: accept in ipsec policy" ipsec-policy=in,ipsec
```

```
add action=accept chain=forward comment="defconf: accept out ipsec policy" ipsec-policy=out,ipsec
```

```
add action=fasttrack-connection chain=forward comment="defconf: fasttrack" connection-state=established,related
```

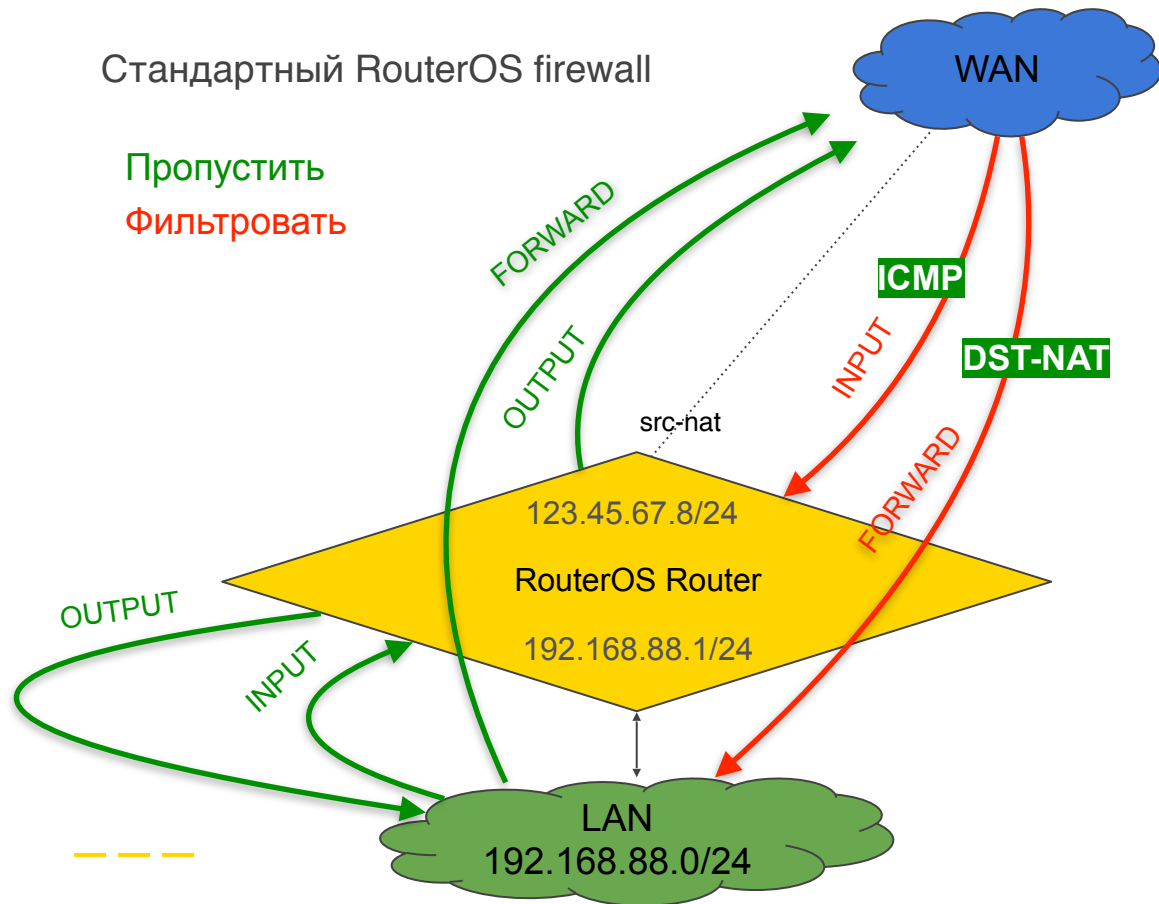
```
add action=accept chain=forward comment="defconf: accept established,related, untracked" connection-  
state=established,related,untracked
```

```
add action=drop chain=forward comment="defconf: drop invalid" connection-state=invalid
```

```
add action=drop chain=forward comment="defconf: drop all from WAN not DSTNATed" connection-nat-state=!dstnat  
connection-state=new in-interface-list=WAN
```

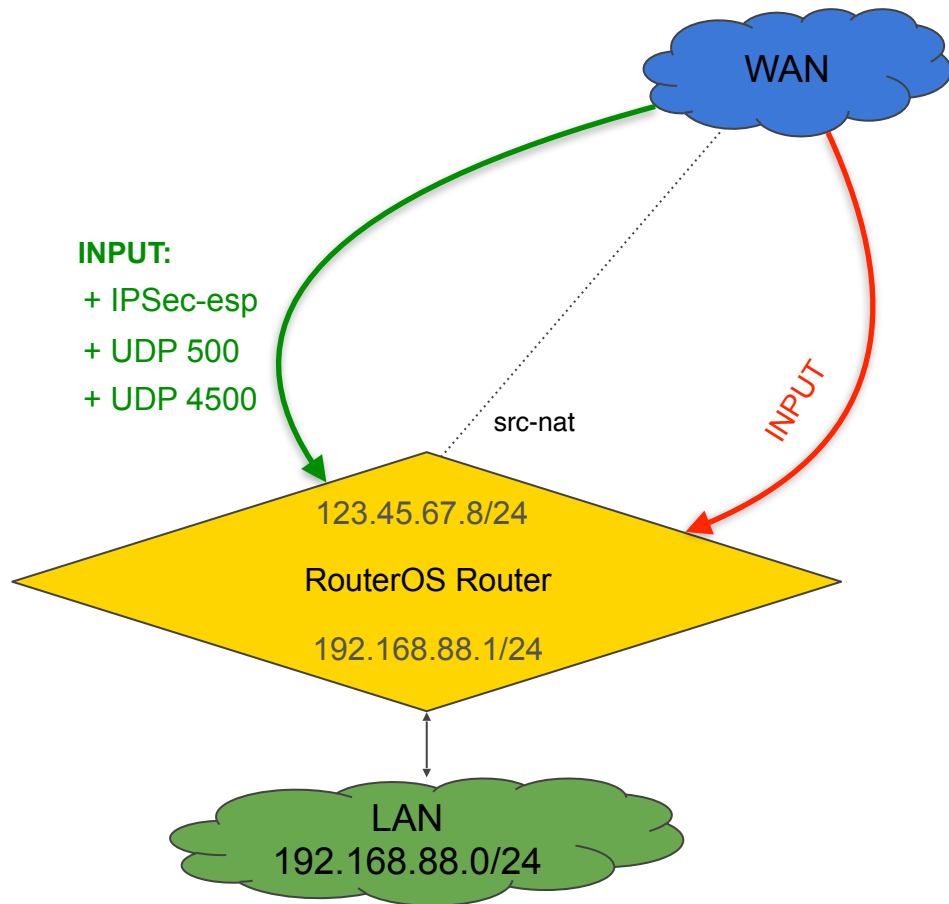
Настройка Firewall

1. Обзор стандартного фильтра
2. Правила для подключения к роутеру через IPSec
3. Правила для трафика через VPN соединение



Настройка Firewall

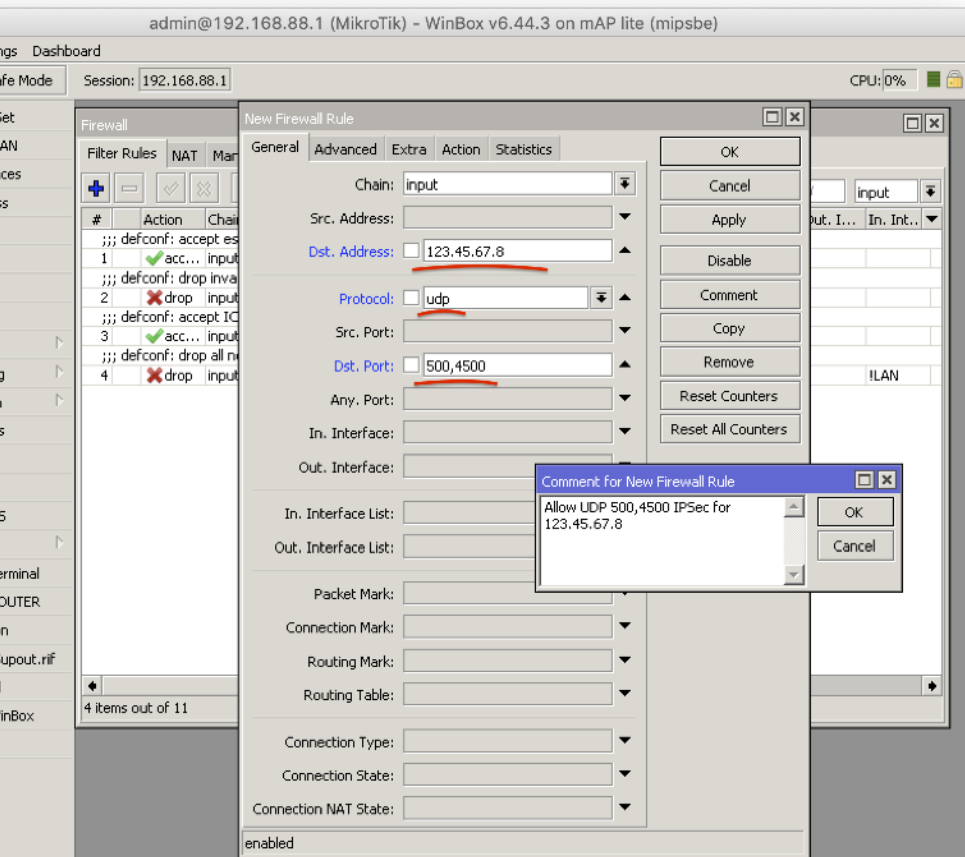
1. Обзор стандартного фильтра
2. **Правила для подключения к роутеру через IPSec**
3. Правила для трафика через VPN соединение



Правила фильтра firewall для IPSec трафика (defconf)

INPUT chain

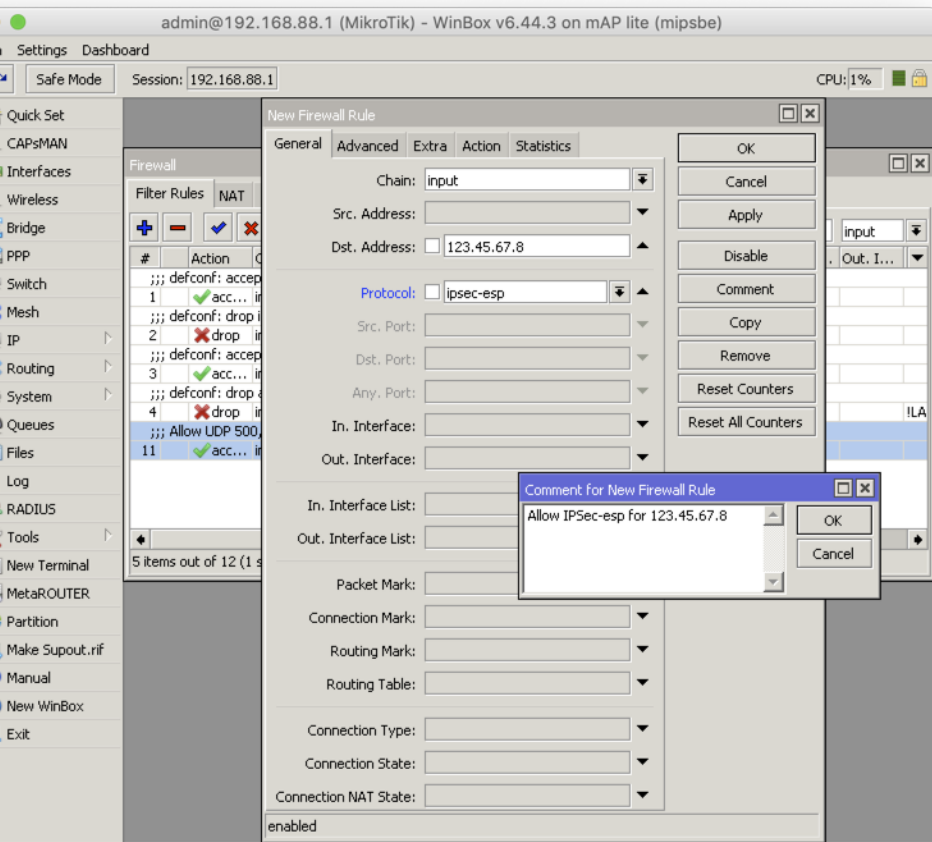
+ UDP 500
+ UDP 4500



```
/ip firewall filter add place-  
before=[ find where  
comment~"defconf: drop all not  
coming from LAN" ] protocol=udp dst-  
port=500,4500 dst-  
address=123.45.67.8 action=accept  
chain=input comment="Allow UDP  
500,4500 IPSec for 123.45.67.8"
```

Правила фильтра firewall для IPSec трафика (defconf)

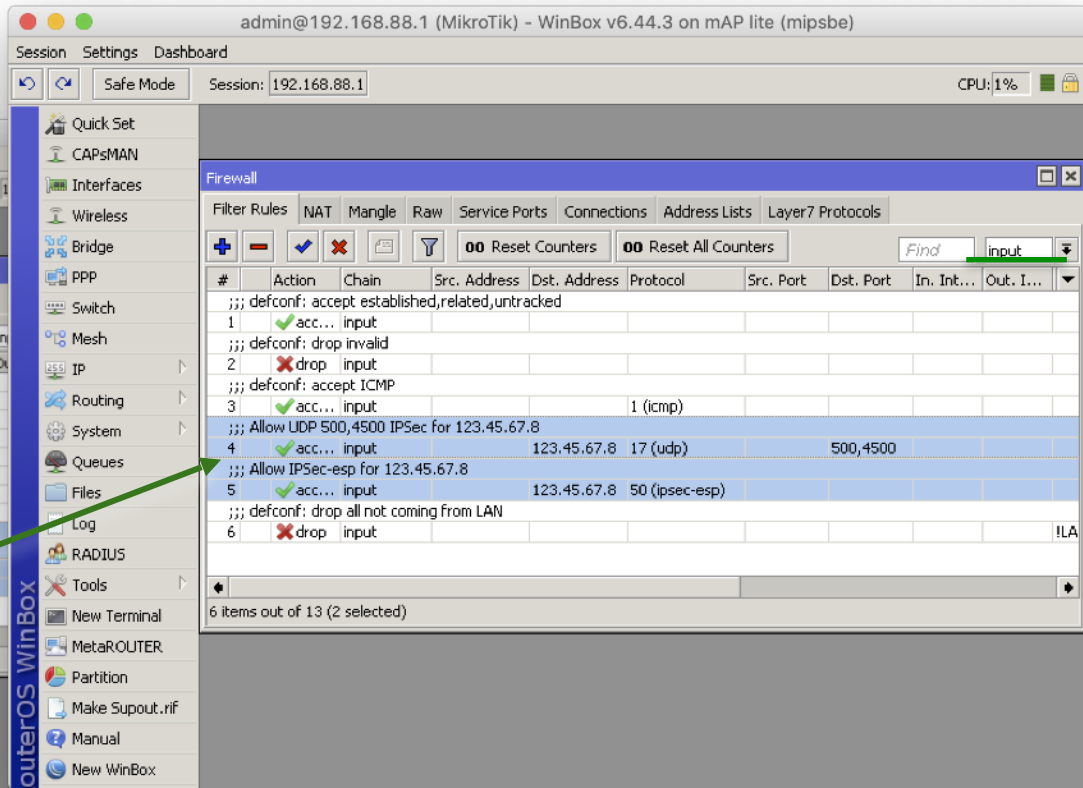
INPUT chain



+ IPSec-esp (protocol 50)

```
/ip firewall filter add place-  
before=[ find where  
comment~"defconf: drop all not  
coming from LAN" ] protocol=ipsec-  
esp dst-address=123.45.67.8  
action=accept chain=input  
comment="Allow IPSec-esp for  
123.45.67.8"
```

Поднимаем **accept** правила
выше **drop**



WAN

VPN абоненты

Connected



114.21.117.21 🇯🇵



46.249.38.117 🇭🇺



177.12.61.244 🇧🇷

IPSec-esp
UDP 500
UDP 4500

123.45.67.8

RouterOS Router
192.168.88.1/24

LAN
192.168.88.0/24

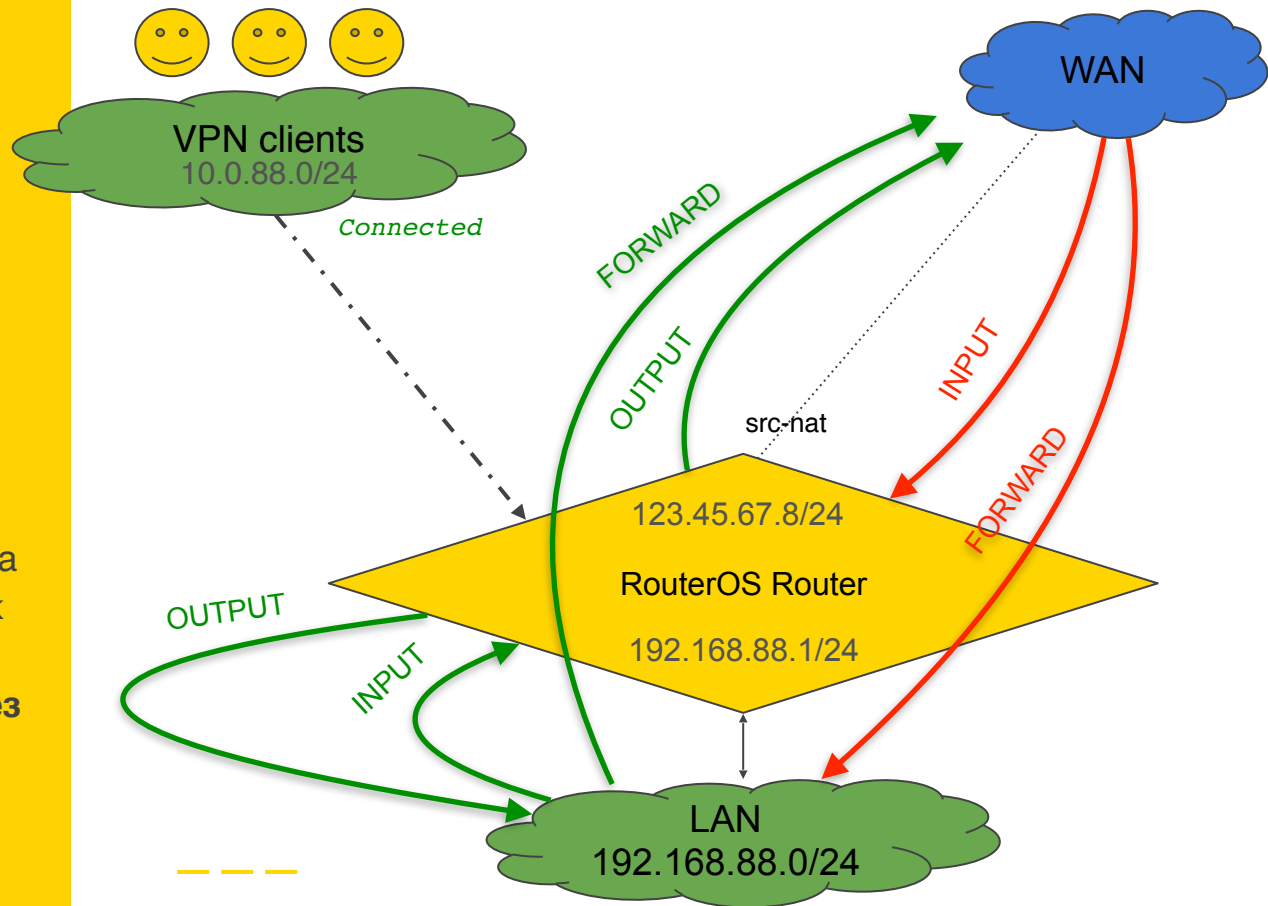
1. Обзор стандартного фильтра
2. **Правила для подключения к роутеру через IPSec**
3. Правила для трафика через VPN соединение

Настройка Firewall

Правила для трафика через VPN соединение

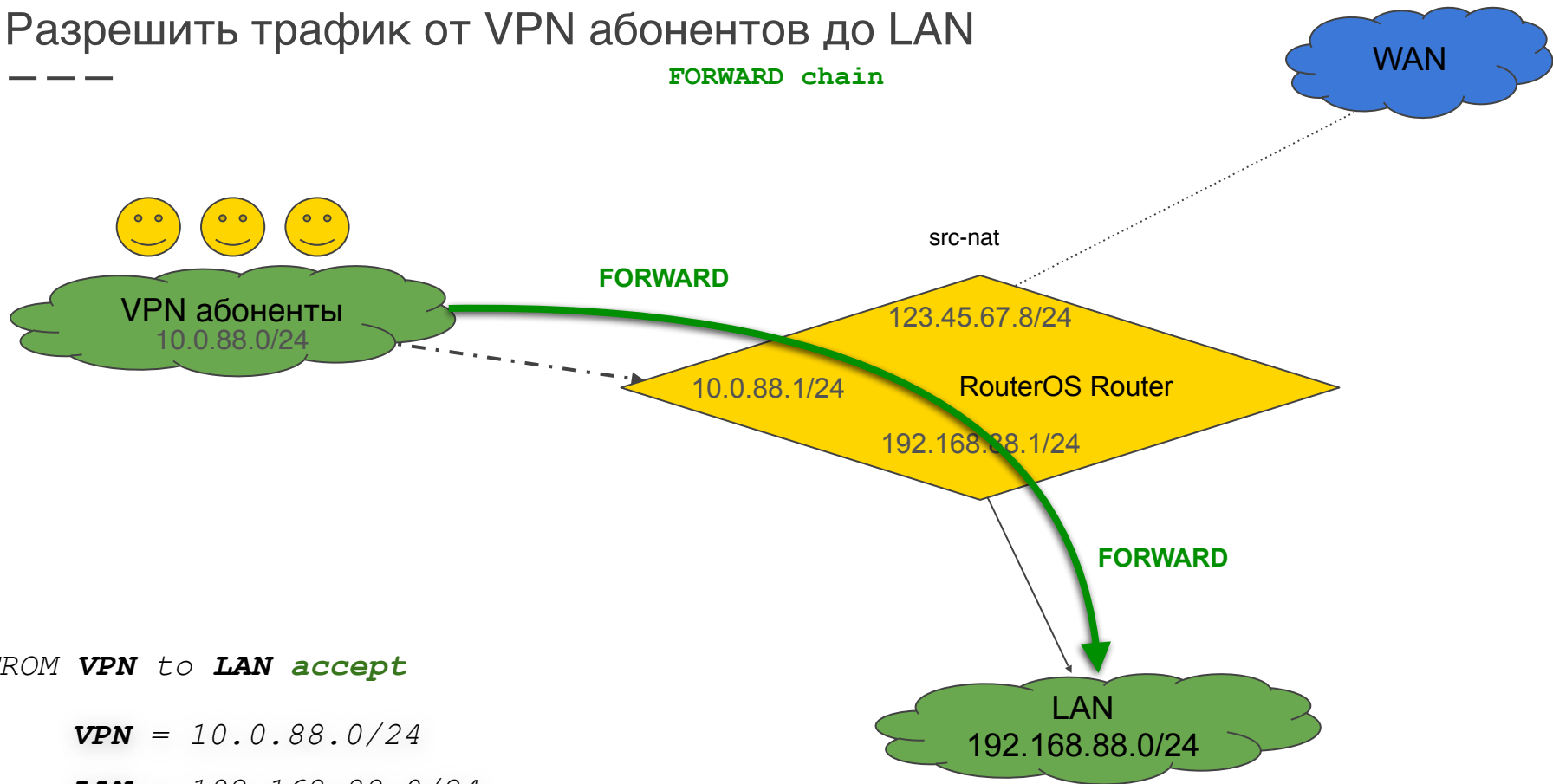
Настройка Firewall

1. Обзор стандартного фильтра
2. Правила для подключения к роутеру через IPSec
3. **Правила для трафика через VPN соединение**



Разрешить трафик от VPN абонентов до LAN

FORWARD chain



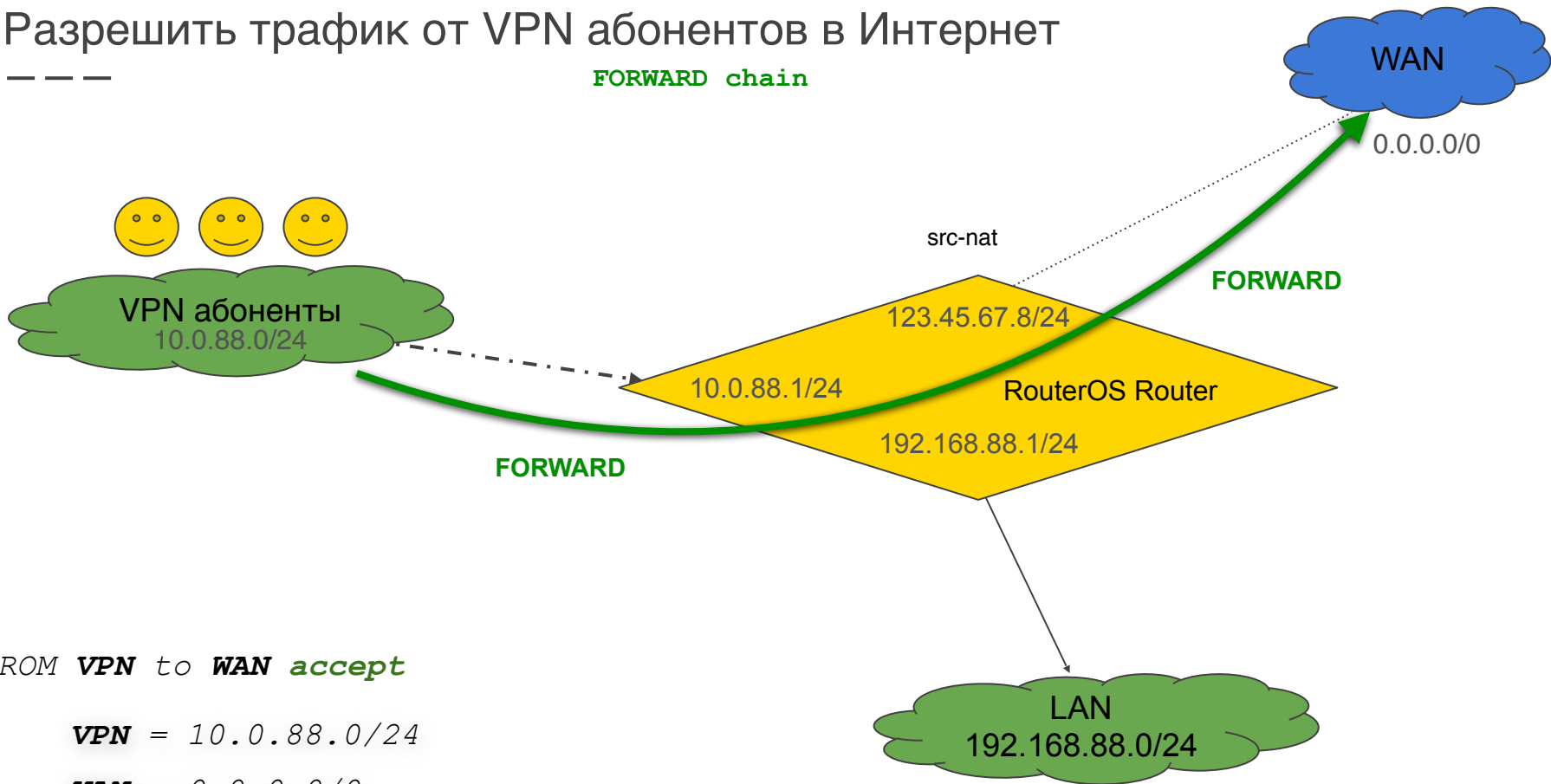
FROM **VPN** to **LAN** *accept*

VPN = 10.0.88.0/24

LAN = 192.168.88.0/24

Разрешить трафик от VPN абонентов в Интернет

FORWARD chain



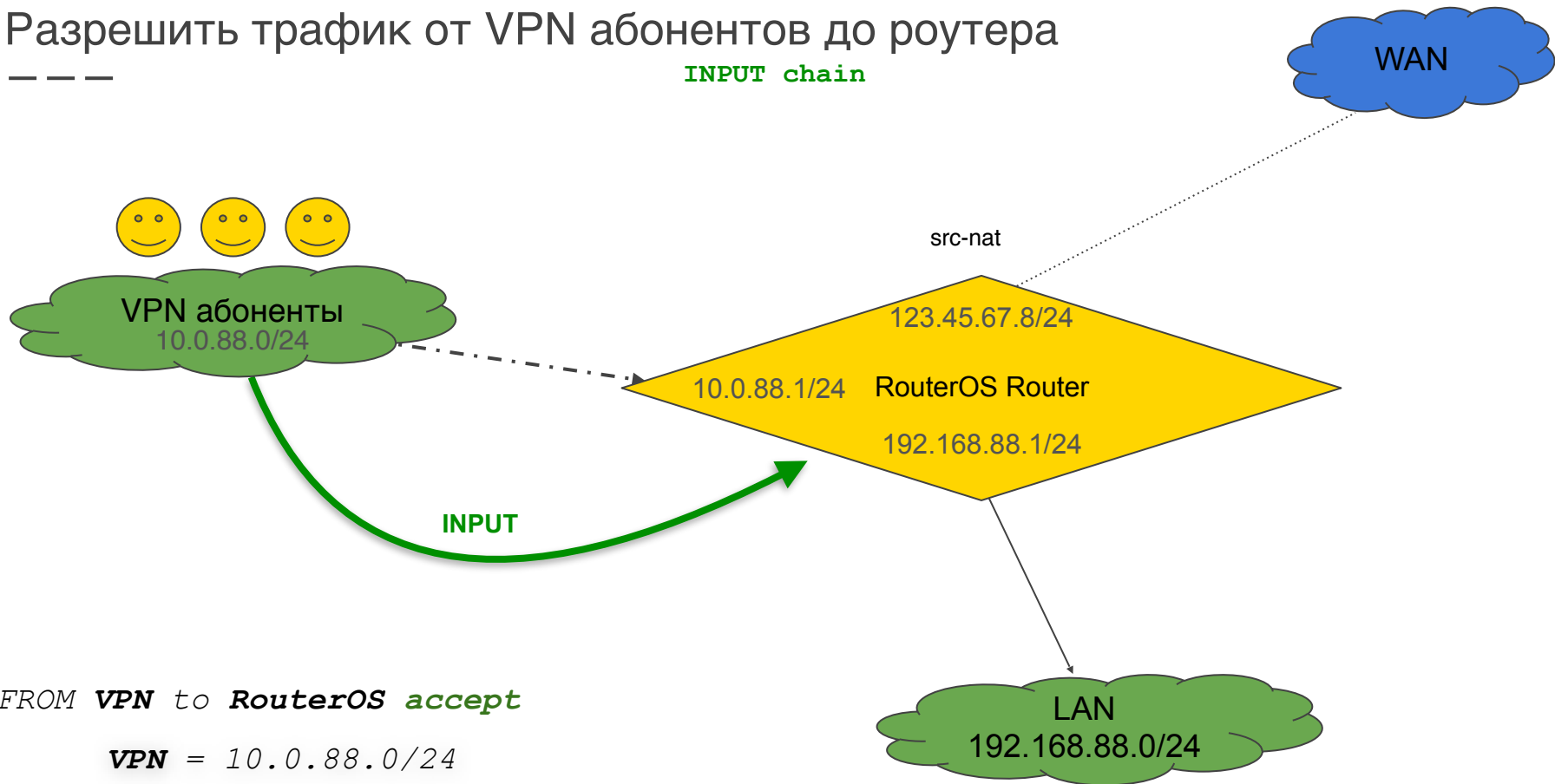
FROM **VPN** to **WAN** *accept*

VPN = 10.0.88.0/24

WAN = 0.0.0.0/0

Разрешить трафик от VPN абонентов до роутера

INPUT chain

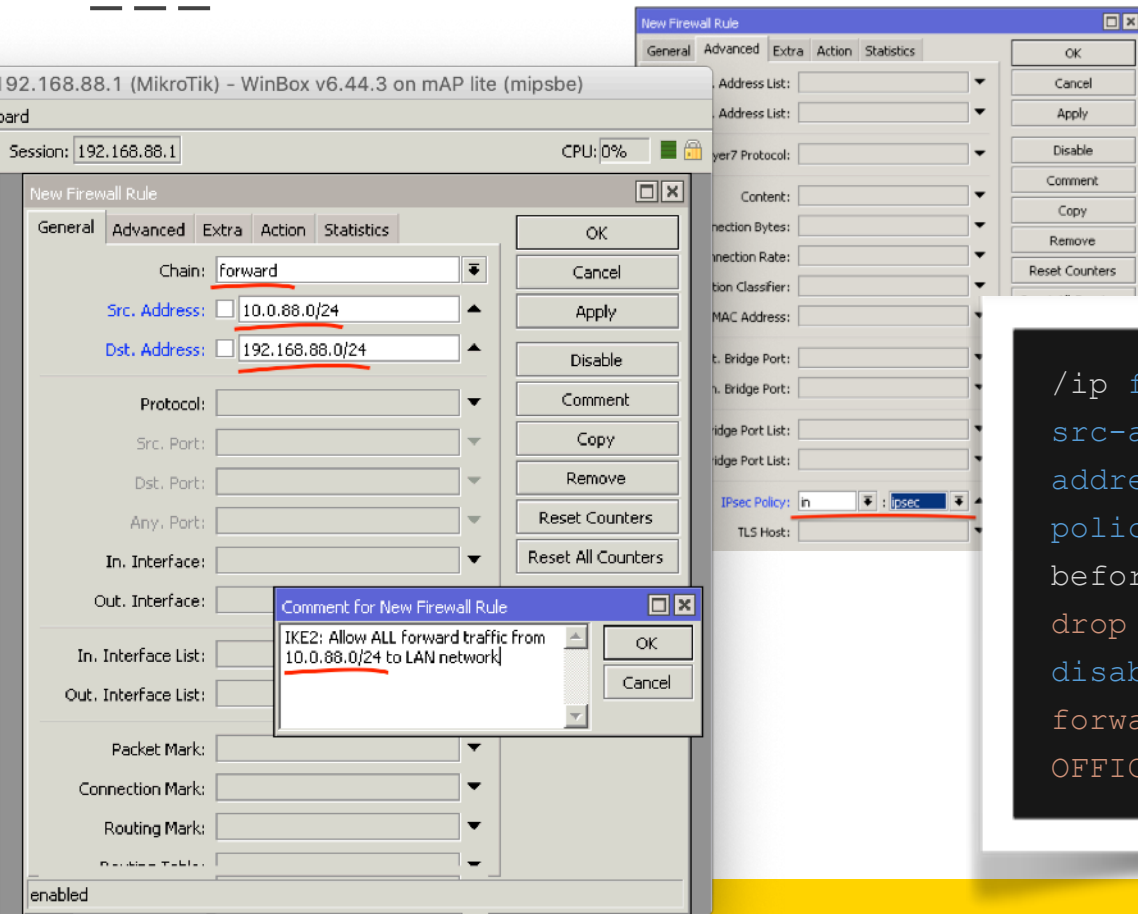


FROM **VPN** to **RouterOS** **accept**

VPN = 10.0.88.0/24

Правила от VPN абонентов до LAN сети

FORWARD chain



FROM VPN to LAN accept

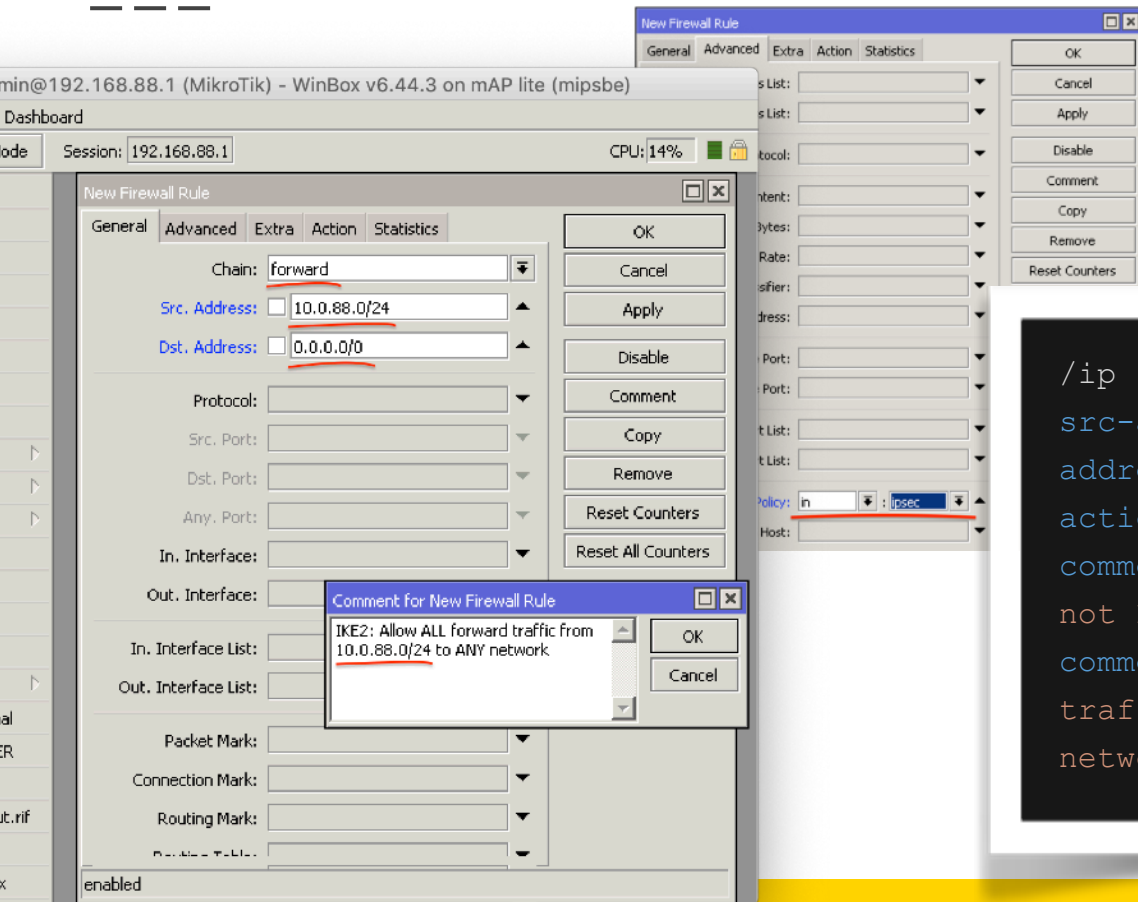
VPN = 10.0.88.0/24

LAN = 192.168.88.0/24

```
/ip firewall filter add chain=forward  
src-address=10.0.88.0/24 dst-  
address=192.168.88.0/24 ipsec-  
policy=in,ipsec action=accept place-  
before=[ find where comment~"defconf:  
drop all from WAN not DSTNATED" ]  
disabled=no comment="IKE2: Allow ALL  
forward traffic from 10.0.88.0/24 to  
OFFICE network"
```

Правила от VPN абонентов до WAN

FORWARD chain



FROM **VPN** to **WAN** *accept*

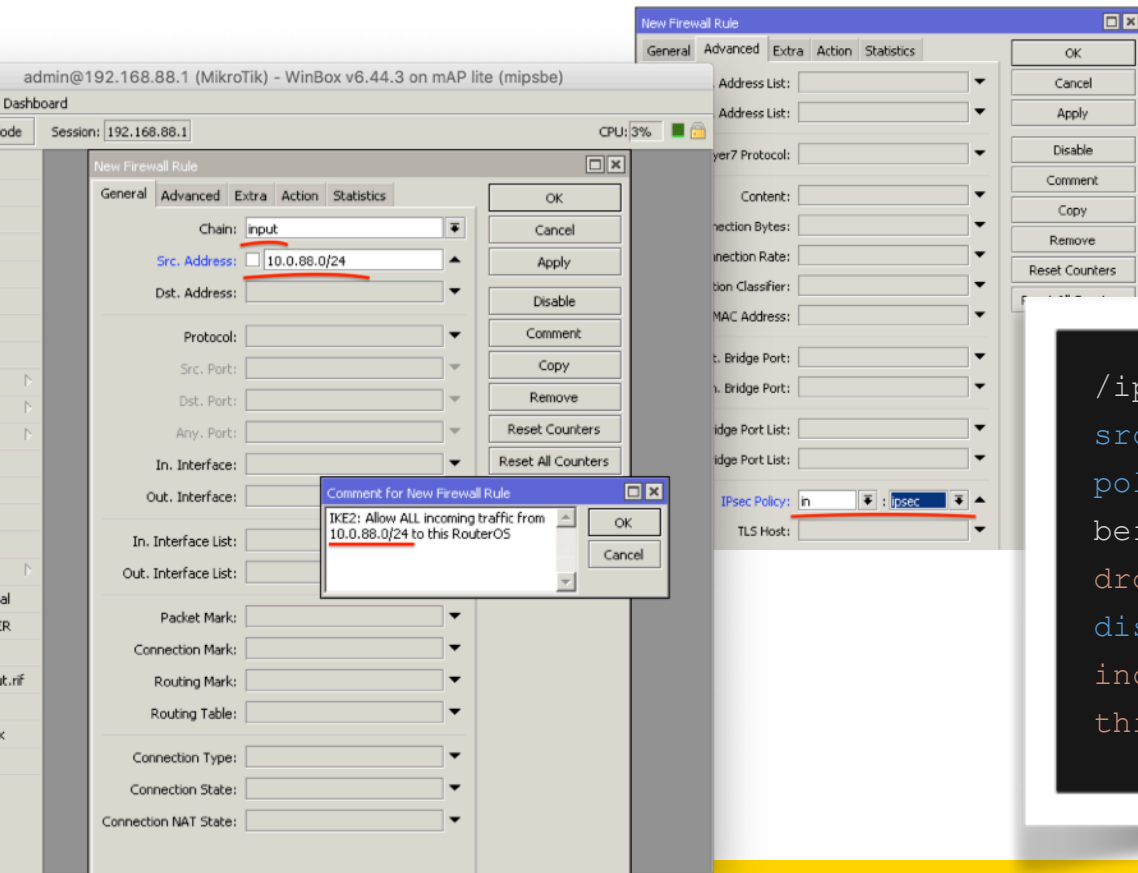
VPN = 10.0.88.0/24

WAN = 0.0.0.0/0

```
/ip firewall filter add chain=forward  
src-address=10.0.88.0/24 dst-  
address=0.0.0.0/0 ipsec-policy=in,ipsec  
action=accept place-before=[ find where  
comment~"defconf: drop all from WAN  
not DSTNATED" ] disabled=no  
comment="IKE2: Allow ALL forward  
traffic from 10.0.88.0/24 to ANY  
network"
```

Правила от VPN абонентов до RouterOS

INPUT chain



FROM VPN to RouterOS accept

VPN = 10.0.88.0/24

```
/ip firewall filter add chain=input  
src-address=10.0.88.0/24 ipsec-  
policy=in,ipsec action=accept place-  
before=[ find where comment~"defconf:  
drop all not coming from LAN" ]  
disabled=no comment="IKE2: Allow ALL  
incoming traffic from 10.0.88.0/24 to  
this RouterOS"
```

Стандартные правила Firewall для любого FORWARD трафика в **ipsec** упаковке (defconf)



FORWARD chain

admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)

Session: 192.168.88.1 CPU: 0%

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

Find forward

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Int...	Out...
;;; special dummy rule to show fasttrack counters									
0	D	pas...	forward						
7	✓ acc...	forward							
8	✓ acc...	forward							
;;; defconf: fasttrack									
9	fas...	forward							
;;; defconf: accept established, related, untracked									
10	✓ acc...	forward							
;;; defconf: drop invalid									
11	✗ drop	forward							
;;; defconf: drop all from WAN not DSTNATED									
12	✗ drop	forward							

7 items out of 13 (2 selected)

Per Connection Classifier: Reset Counters
Src. MAC Address: Reset All Counters

Out. Br:

Port List:

Age Port List:

IPsec Policy: in : ipsec

TLS Host:

Priority:

Packet Size:

Content: Comment
Copy
Remove
Reset Counters
Reset All Counters

Connection Bytes:
Connection Rate:

Per Connection Classifier:
Src. MAC Address:

Out. Br:

Port List:

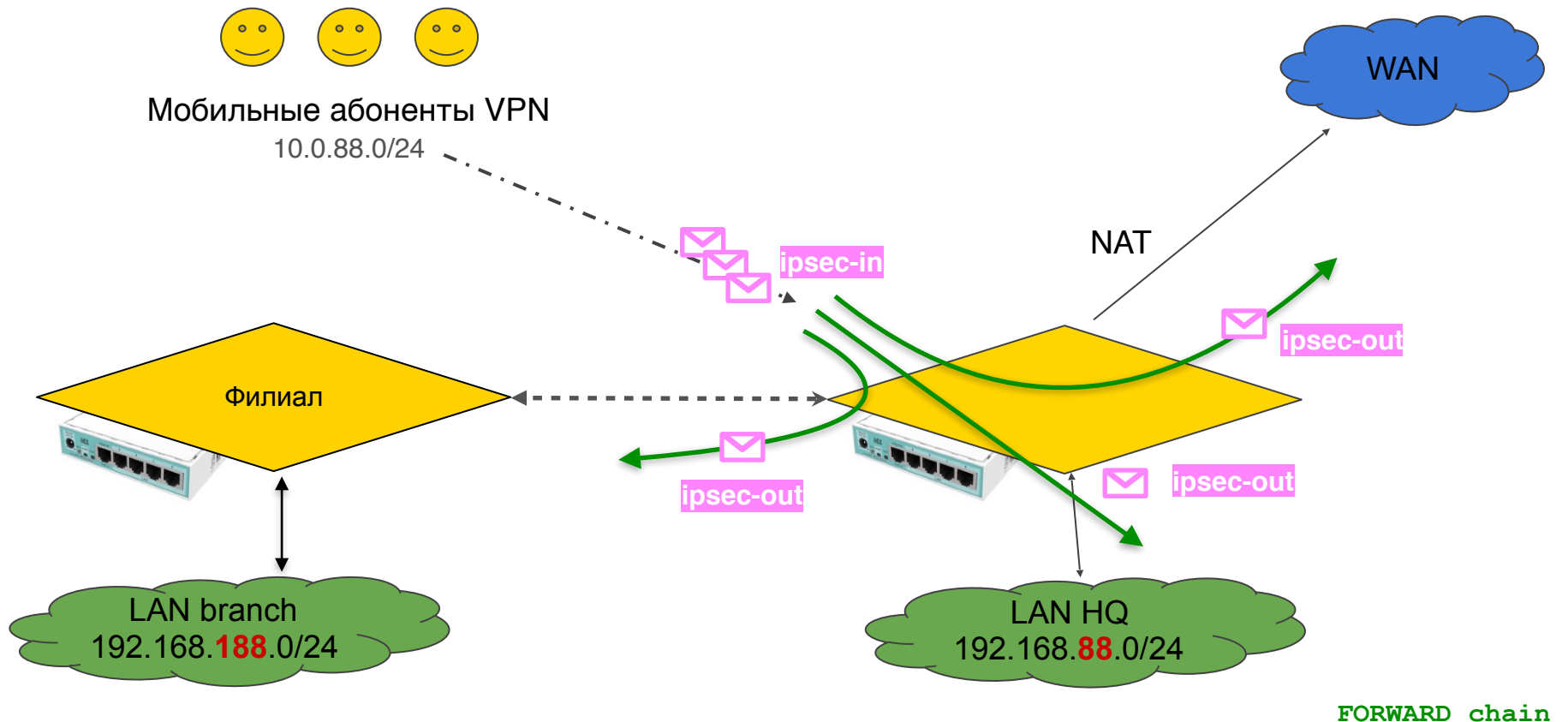
Age Port List:

IPsec Policy: out : ipsec

TLS Host:

Priority:

Packet Size:
Random:



Стандартные правила Firewall для любого трафика в **ipsec** упаковке (defconf)

Настройка NAT

Обзор правила NAT стандартного Firewall (defconf)

admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)

Session Settings Dashboard

Safe Mode

Session: 192.168.88.1

CPU: 1%

NAT Rule <>

General Advanced Extra Action Statistics

Chain: srcnat

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List: WAN

Packet Mark:

Connection Mark:

Routing Mark:

Dynamic Table:

enabled

NAT Rule <>

General Advanced Extra Action Statistics

Src. Address List:

Dst. Address List:

Layer7 Protocol:

Content:

Connection Bytes:

Connection Rate:

Per Connection Classifier:

Src. MAC Address:

Out. Bridge Port:

In. Bridge Port:

In. Bridge Port List:

Out. Bridge Port List:

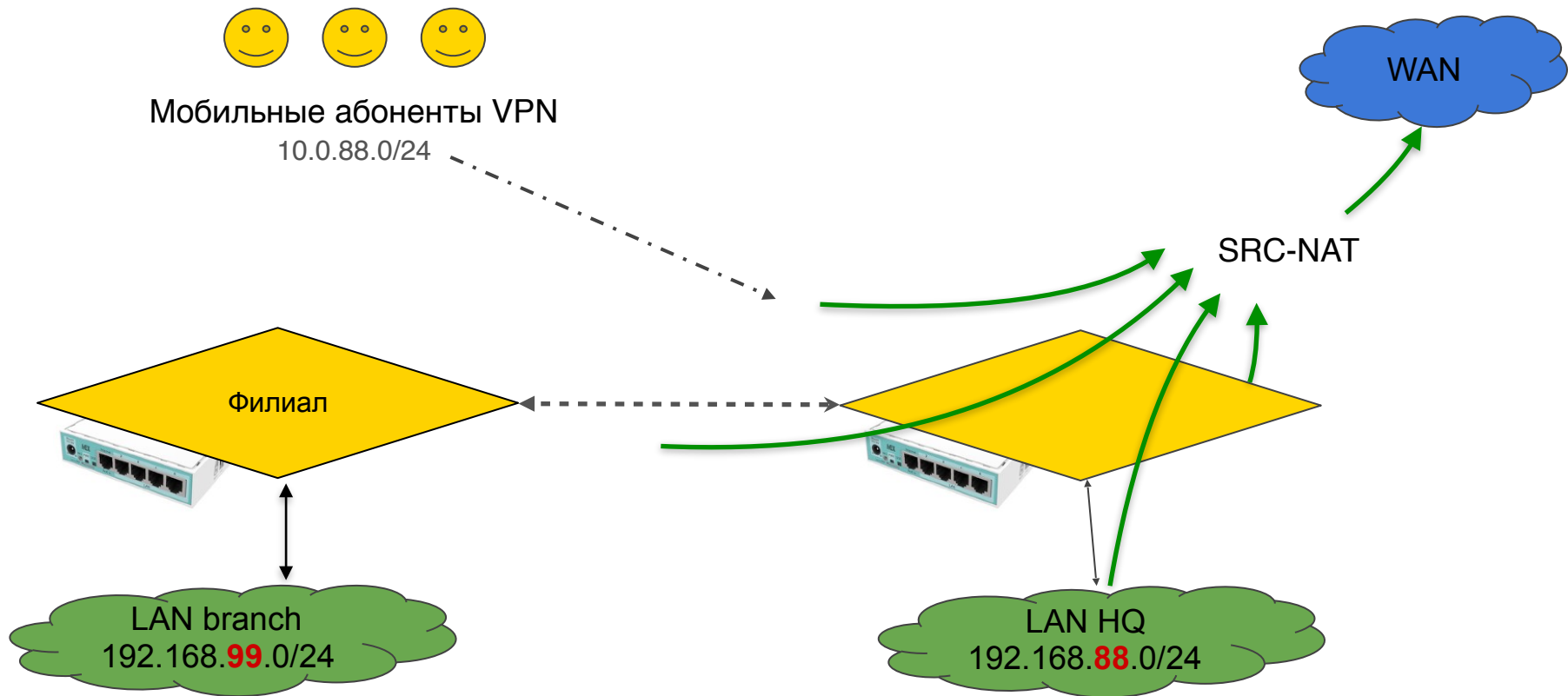
IPsec Policy: out : none

TLS Host:

enabled

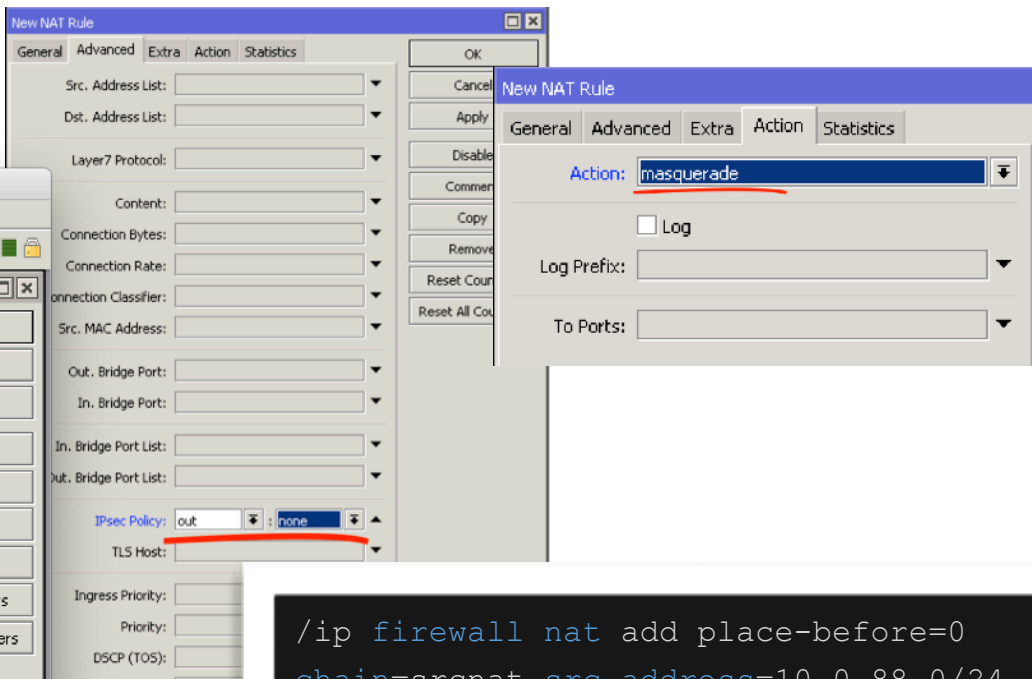
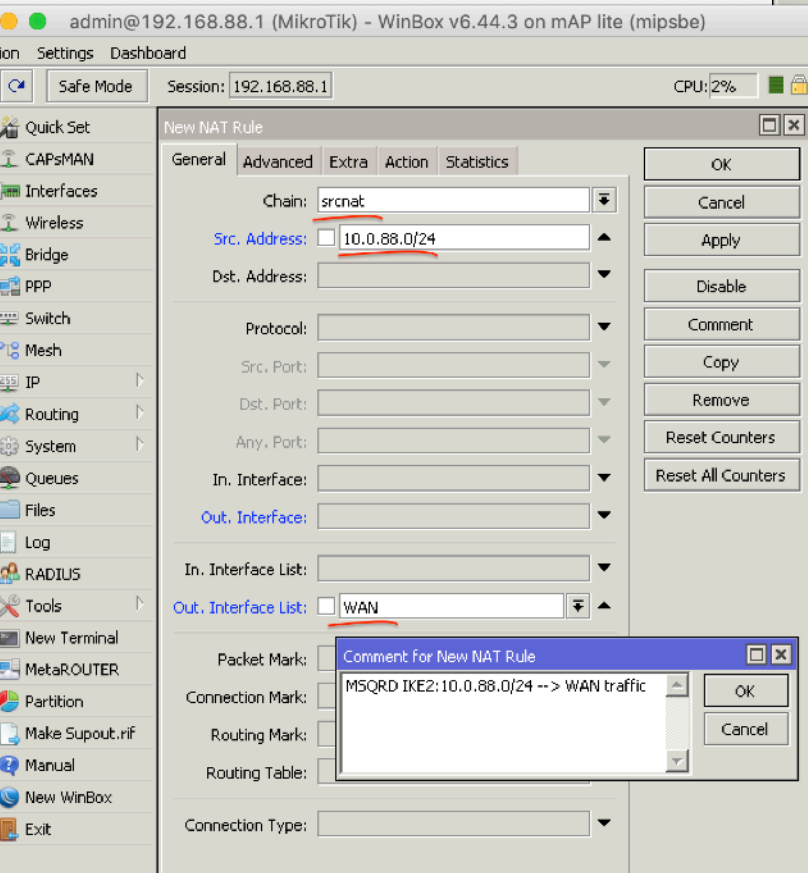


ipsec-out: none



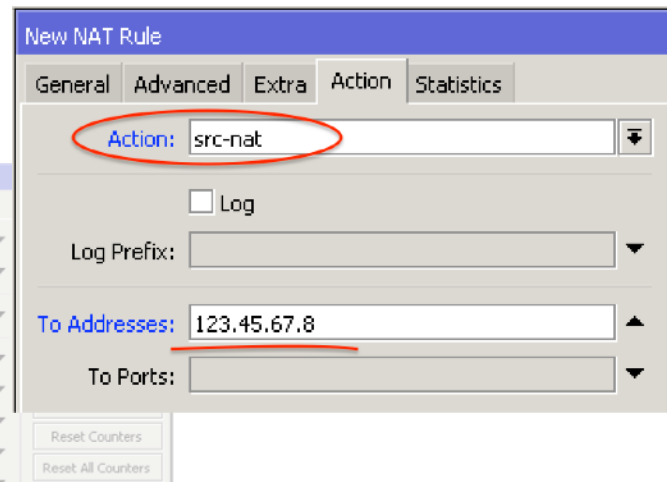
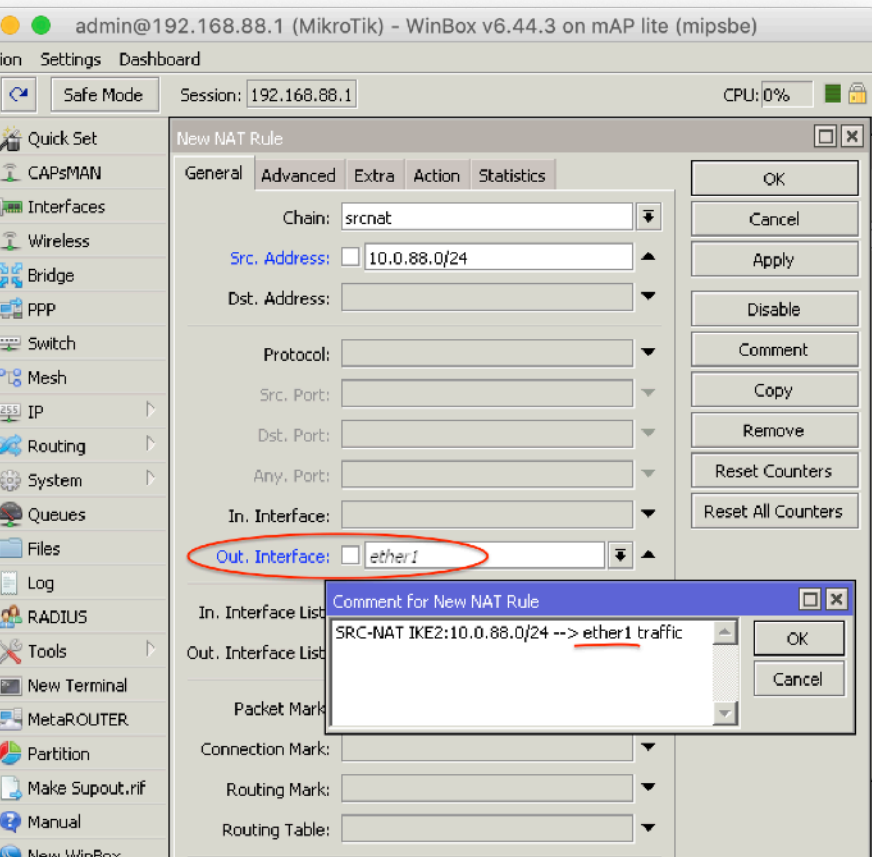
Обзор правила NAT стандартного Firewall (defconf)

Маскарад VPN трафика



```
/ip firewall nat add place-before=0
chain=srcnat src-address=10.0.88.0/24
out-interface-list=WAN ipsec-
policy=out,none action=masquerade
comment="MSQRD IKE2:10.0.88.0/24 -->
WAN traffic"
```

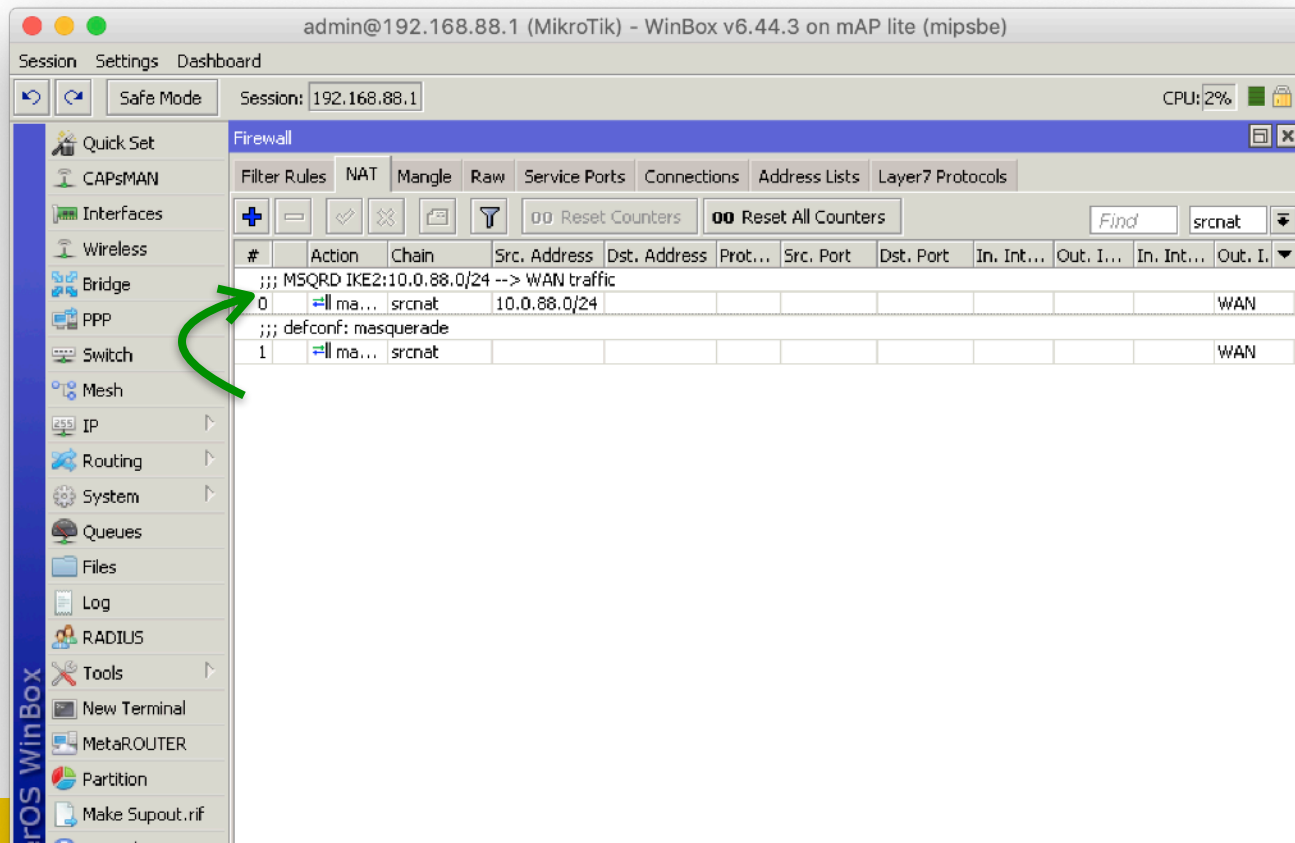
SRC-NAT VPN трафика (рекомендуется) 👍



```
/ip firewall nat add place-before=0
chain=srcnat src-address=10.0.88.0/24
out-interface=ether1 ipsec-
policy=out,none action=src-nat to-
addresses=123.45.67.8 comment="SRC-NAT
IKE2:10.0.88.0/24 --> ether1 traffic"
```

Поднимаем SRC-NAT или MSQRD NAT правило выше стандартного

— — —

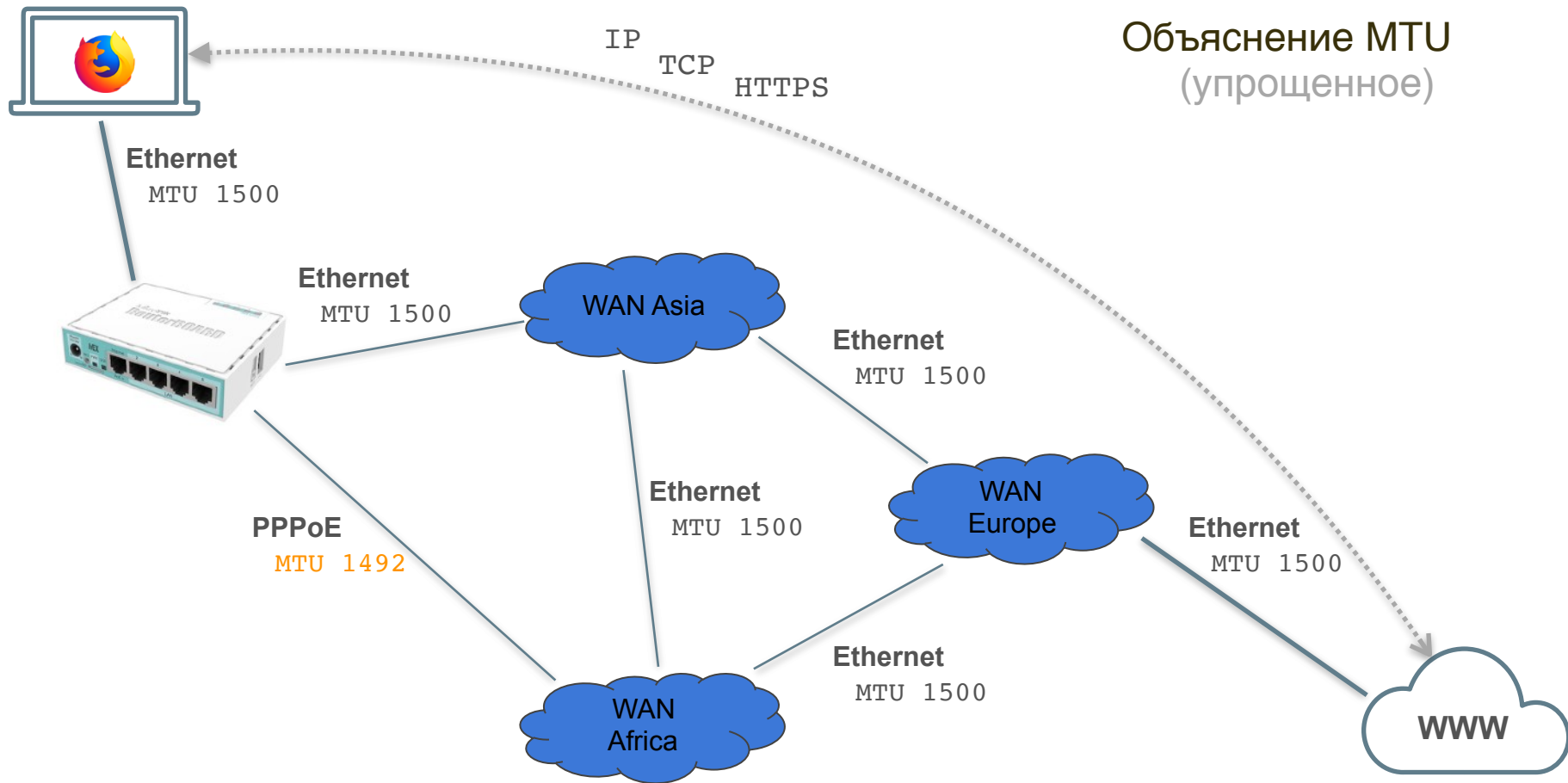


Настройка TCP MSS

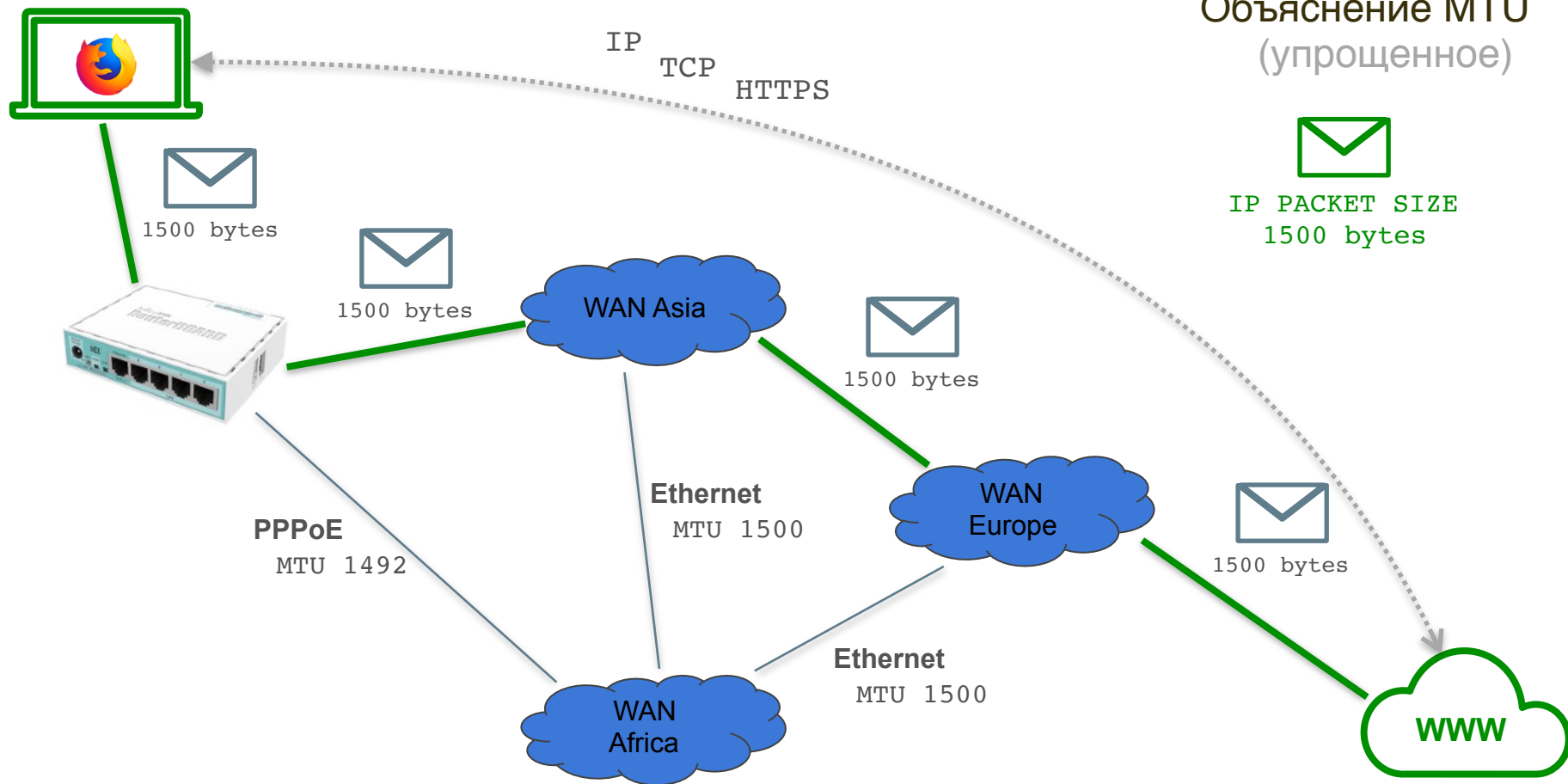
План действий

1. Объяснение MTU и фрагментации IP пакетов
2. Объяснение IPSec MTU
3. Объяснение TCP MSS
4. Настройка TCP MSS через IKE2

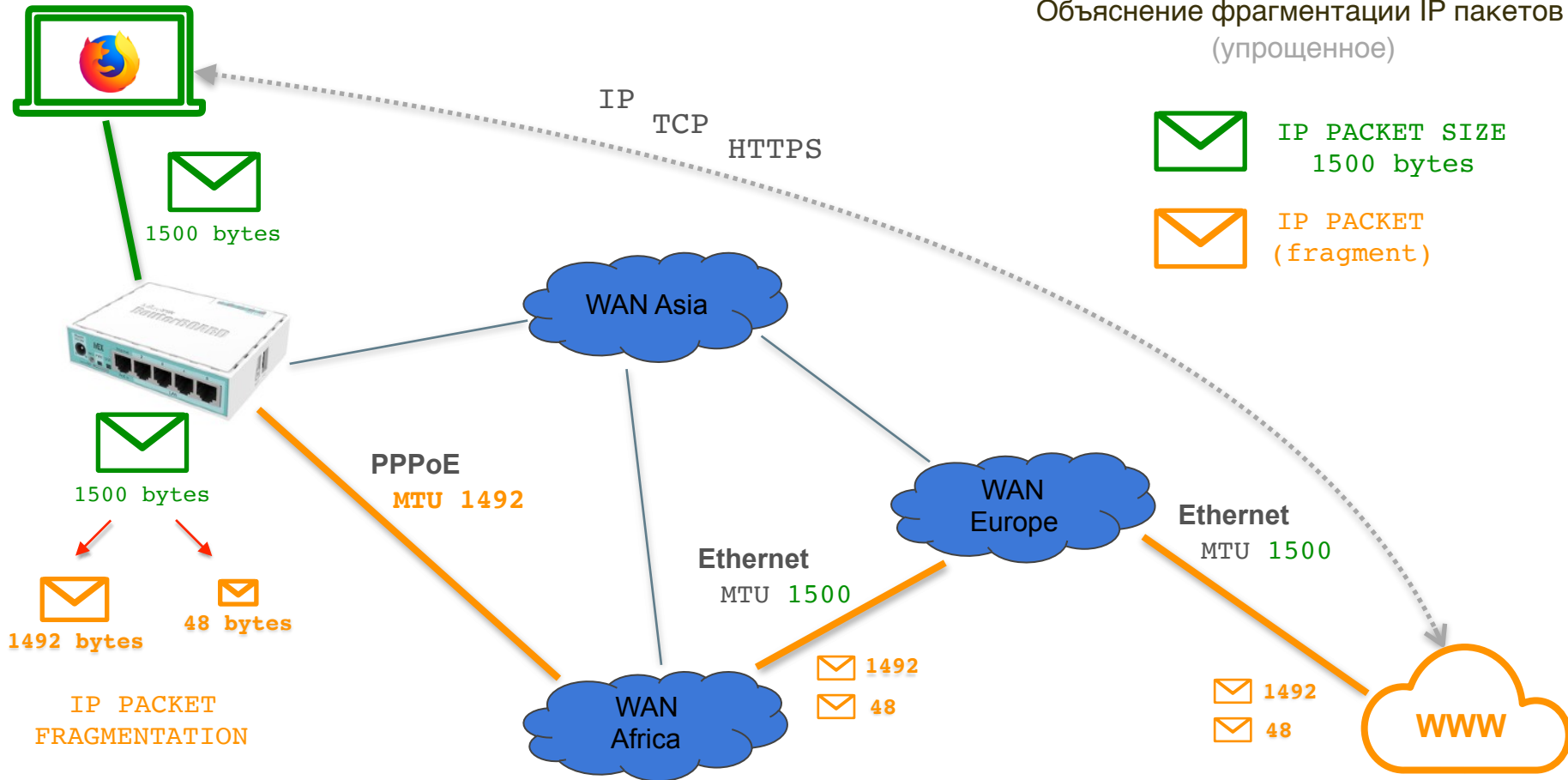
— — —



Объяснение MTU (упрощенное)



Объяснение фрагментации IP пакетов (упрощенное)





Несоответствие MTU —> фрагментация IP пакетов



1500



Ethernet

MTU 1500



1500



PPPoE

MTU 1492



1492 bytes

48 bytes



Ethernet

MTU 1500



1492 bytes



48 bytes



IPSec tunnel

MTU 1400



1400 bytes



48 bytes

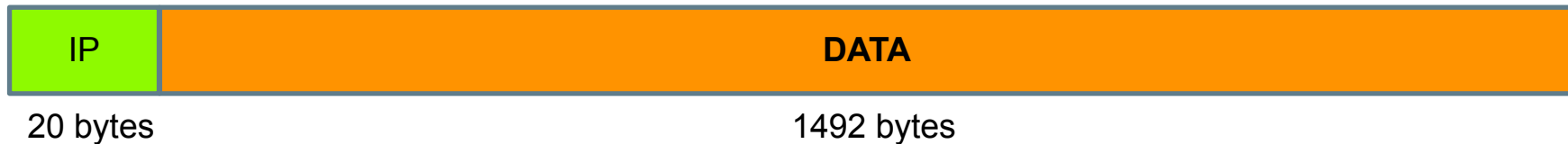


132 bytes

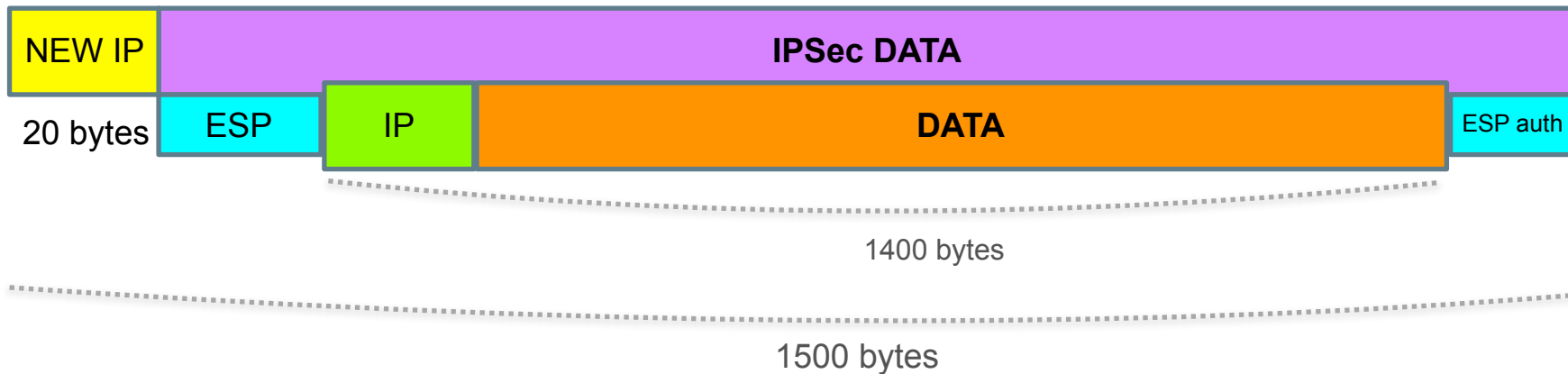


Объяснение IPSec MTU (упрощенное)

IP packet

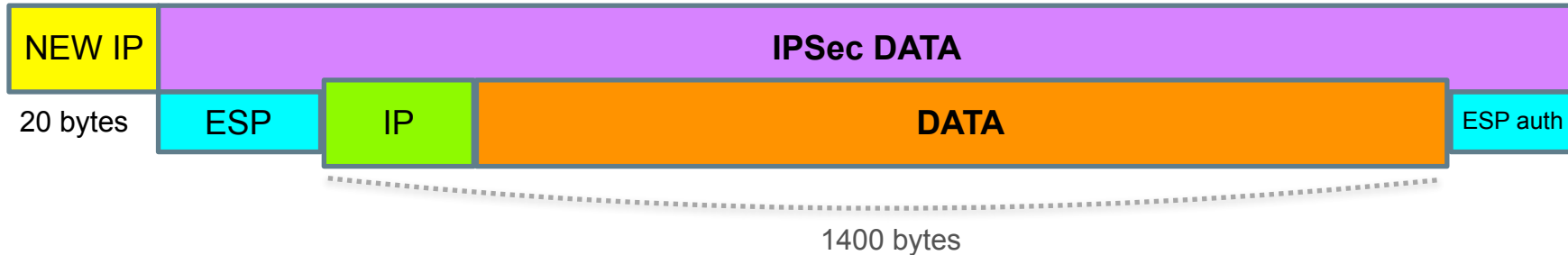


IPSec ESP packet (*tunnel mode*)

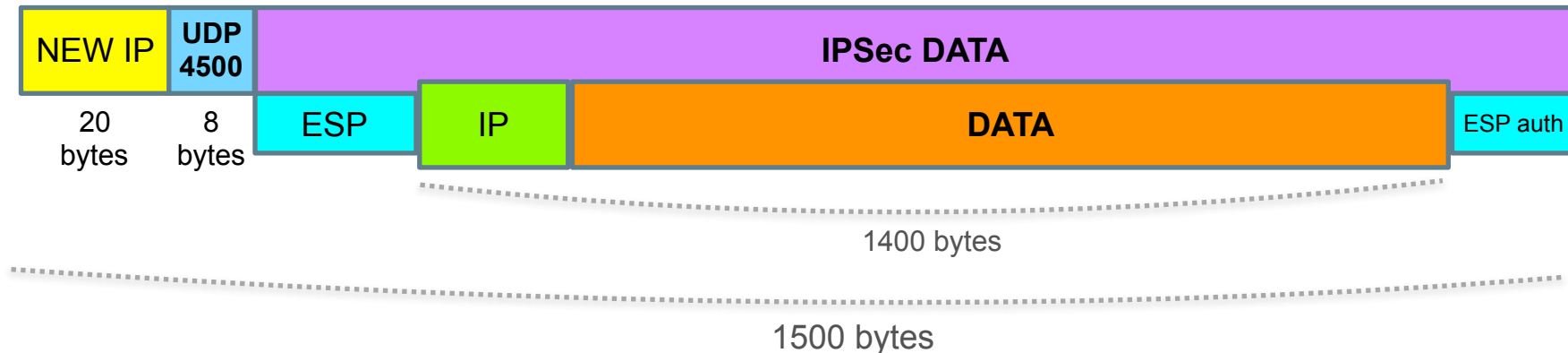


Объяснение IPSec MTU (упрощенное)

IPSec ESP packet (*tunnel mode*)

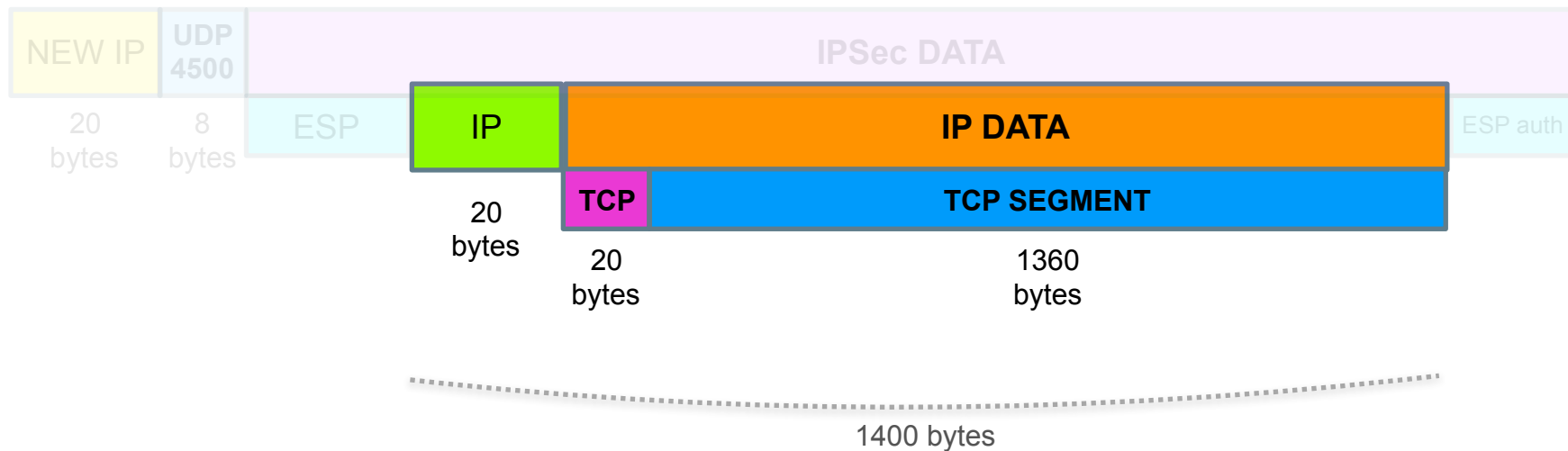


IPSec ESP packet with NAT-T (*tunnel mode*)



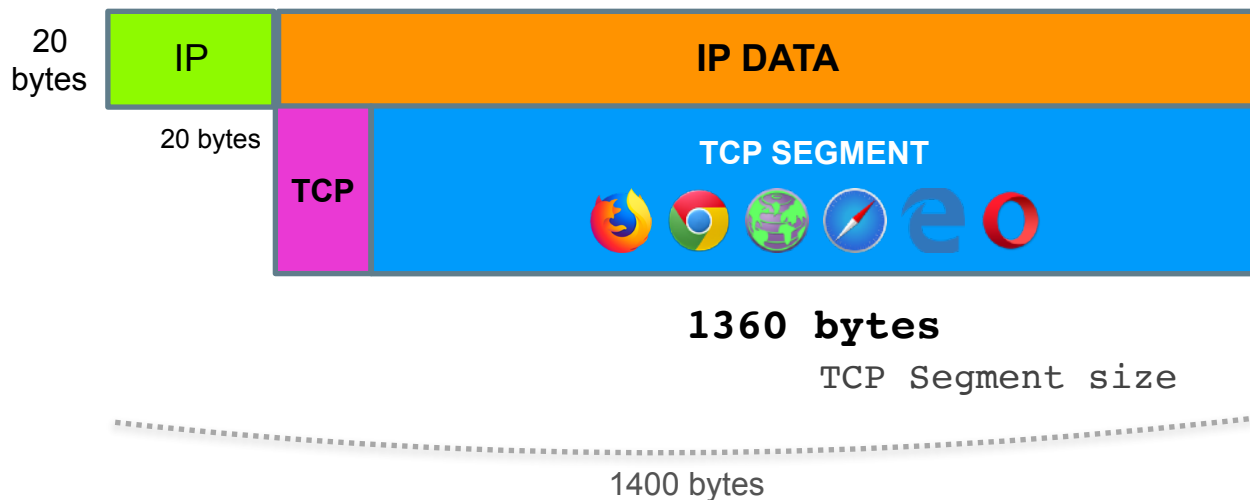
Объяснение IPSec MTU (упрощенное)

IPSec ESP packet with NAT-T (*tunnel mode*)

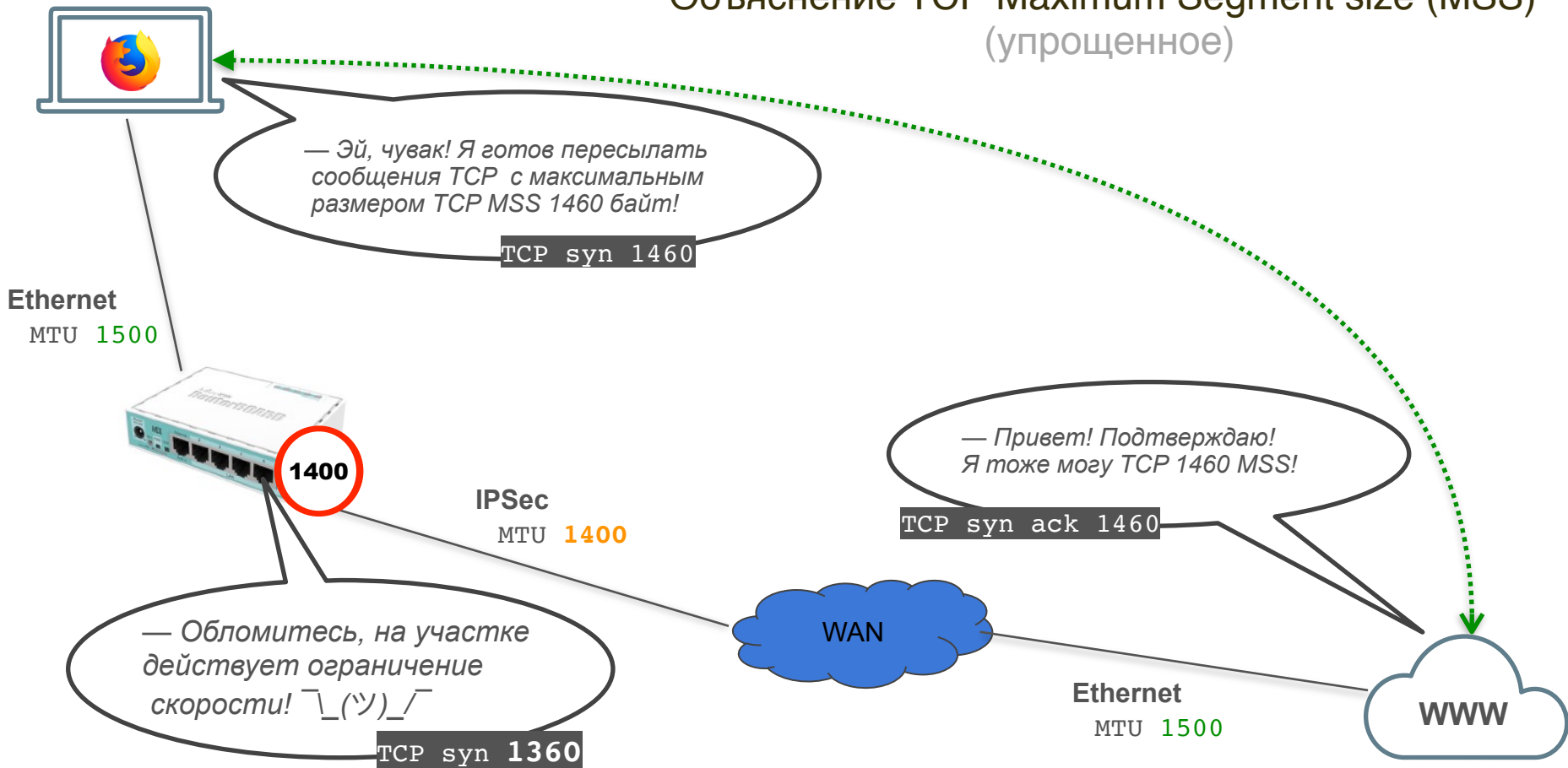


Объяснение IPSec MTU (упрощенное)

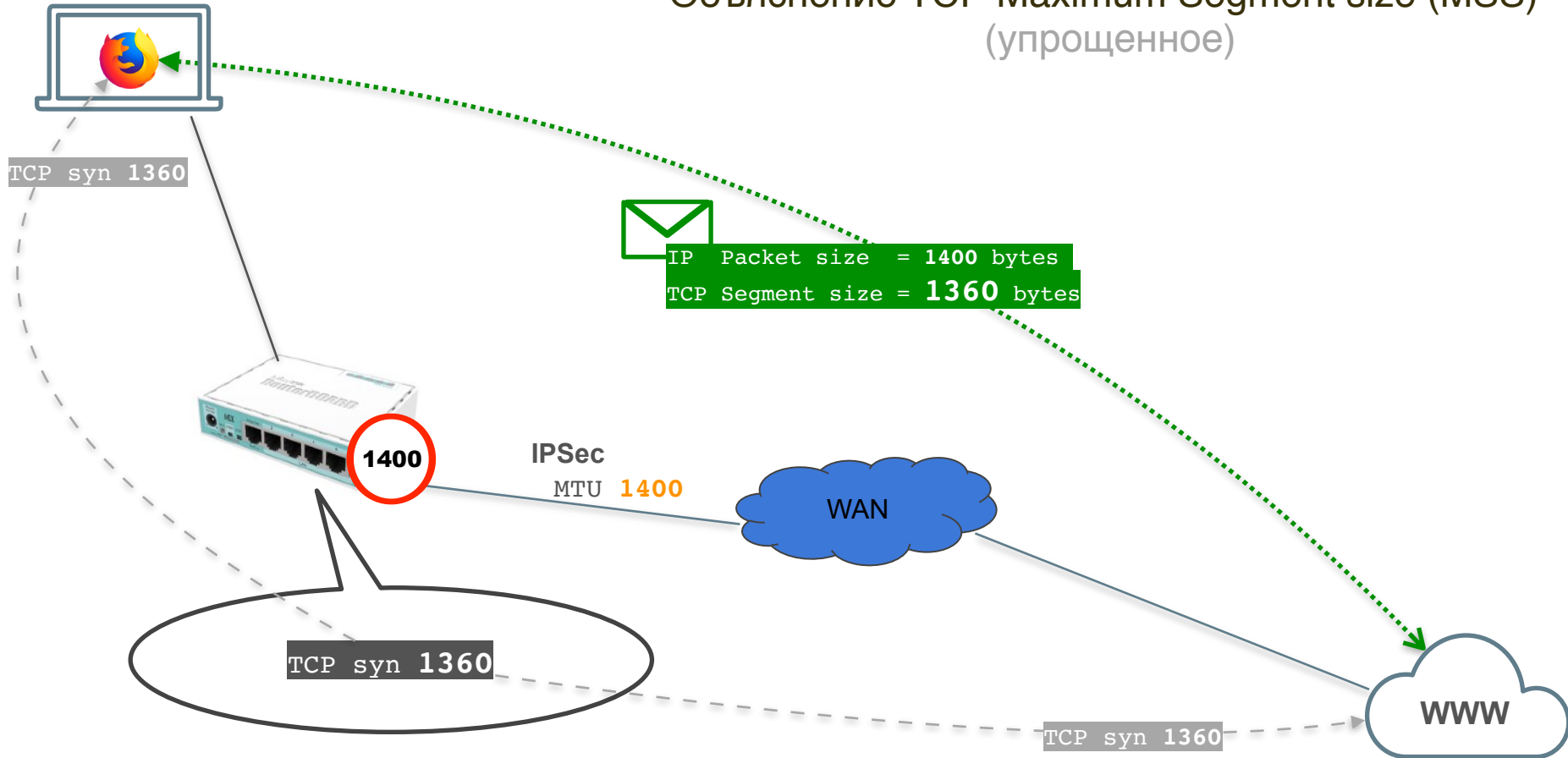
TCP Segment size = MTU - 40 bytes



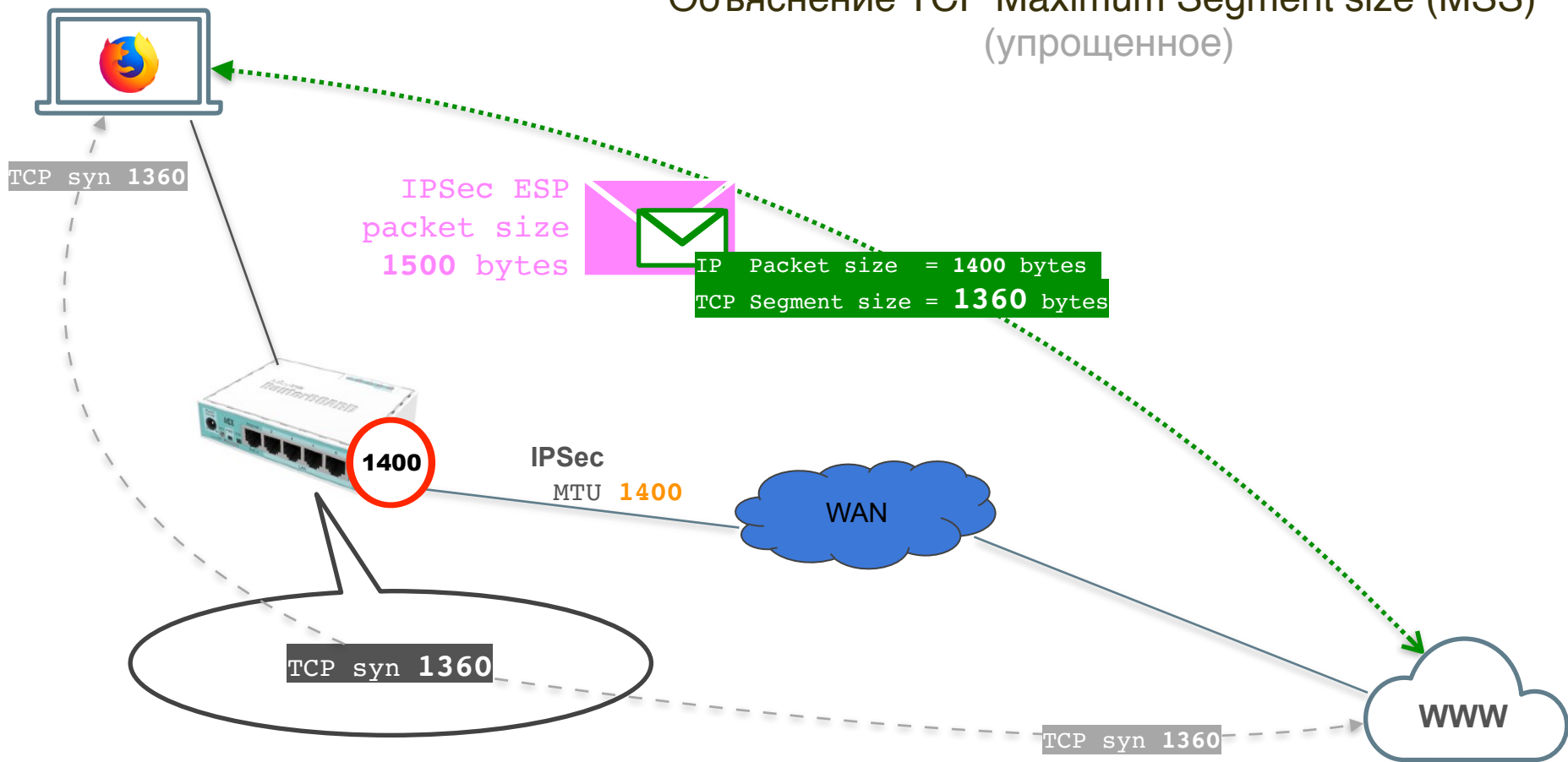
Объяснение TCP Maximum Segment size (MSS) (упрощенное)



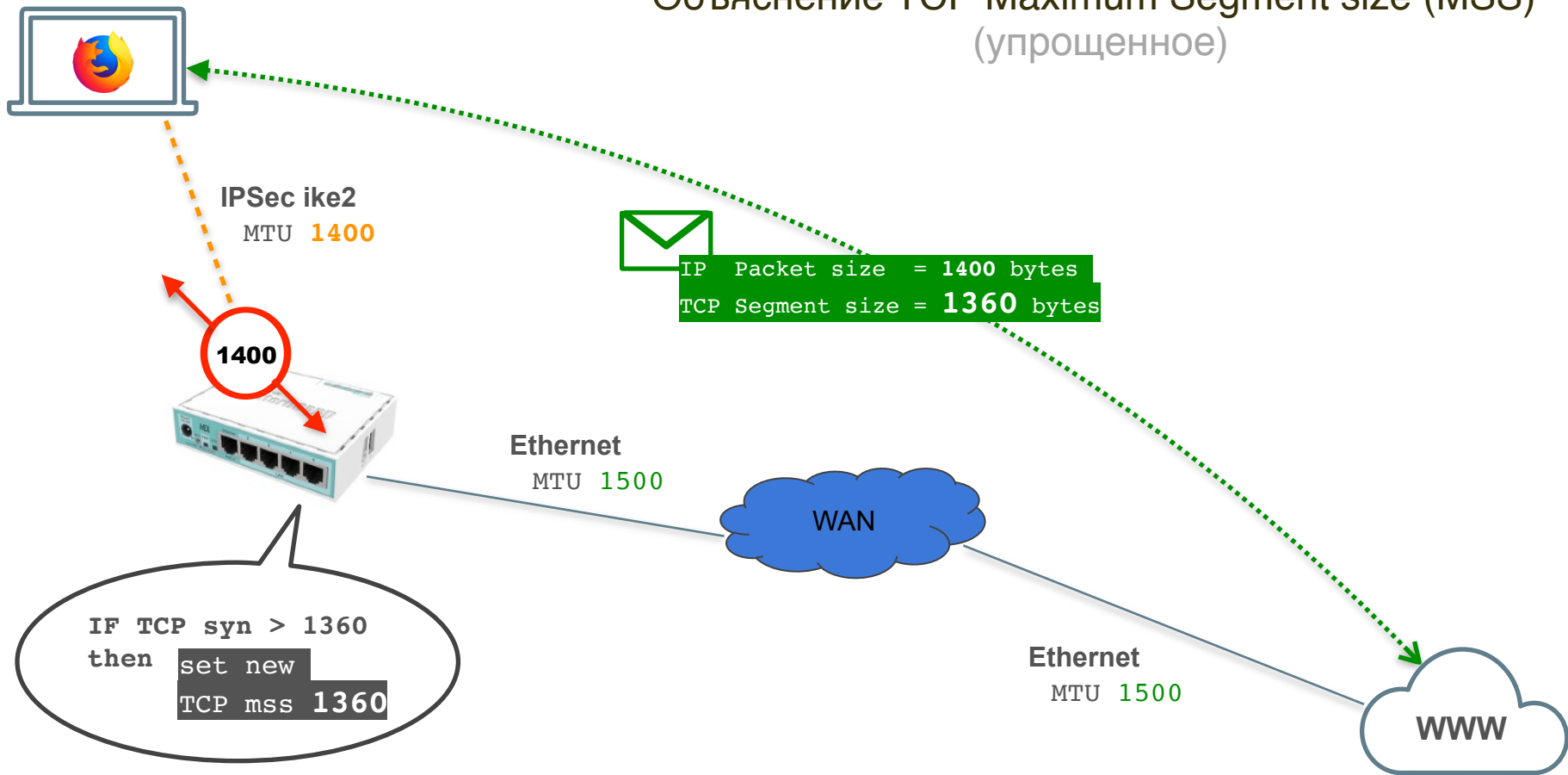
Объяснение TCP Maximum Segment size (MSS) (упрощенное)



Объяснение TCP Maximum Segment size (MSS) (упрощенное)



Объяснение TCP Maximum Segment size (MSS) (упрощенное)



Коррекция TCP MSS от IPsec IKE2 адресов

The image displays three sequential screenshots from the MikroTik WinBox v6.44.3 interface, illustrating the configuration of a new mangle rule to adjust the TCP Maximum Segment Size (MSS) for IKE2 traffic originating from the 10.0.88.0/24 network.

Screenshot 1 (Left): The 'New Mangle Rule' dialog box is shown in the 'General' tab. The 'Chain' is set to 'forward', 'Src. Address' is '10.0.88.0/24', and 'Protocol' is 'tcp'. The 'Action' tab is selected, showing 'Action: change MSS'. The 'Log' checkbox is unchecked, and 'Log Prefix' is empty. The 'New TCP MSS' is set to '1360'. The 'Passthrough' checkbox is checked. A 'Comment for New Mangle Rule' dialog box is open, showing the comment: 'IKE2: Clamp TCP MSS from 10.0.88.0/24 to ANY'.

Screenshot 2 (Middle): The 'New Mangle Rule' dialog box is shown in the 'Advanced' tab. The 'IPsec Policy' is set to 'in', and the 'TLS Host' is empty. The 'TCP MSS' is set to '10-1360'. The 'TCP Flags' are set to 'syn'.

Screenshot 3 (Right): The 'New Mangle Rule' dialog box is shown in the 'Statistics' tab. The 'Action' is 'change MSS', 'Log' is unchecked, 'Log Prefix' is empty, 'New TCP MSS' is '1360', and 'Passthrough' is checked. The 'Comment for New Mangle Rule' dialog box is open, showing the comment: 'IKE2: Clamp TCP MSS from 10.0.88.0/24 to ANY'.

```
/ip firewall mangle add action=change-mss chain=forward new-mss=1360 src-address=10.0.88.0/24 protocol=tcp tcp-flags=syn tcp-mss=!0-1360 ipsec-policy=in,ipsec passthrough=yes comment="IKE2: Clamp TCP MSS from 10.0.88.0/24 to ANY"
```

Коррекция TCP MSS до IPsec IKE2 адресов

The screenshot displays the Mikrotik WinBox interface with three overlapping windows for configuring a new mangle rule:

- New Mangle Rule (General tab):** Chain is set to forward, Dst. Address is 10.0.88.0/24, and Protocol is 6 (tcp).
- New Mangle Rule (Extra tab):** Action is set to change MSS, Log Prefix is empty, and New TCP MSS is set to 1360. The Passthrough checkbox is checked.
- Comment for New Mangle Rule:** The comment is "IKE2: Clamp TCP MSS from ANY to 10.0.88.0/24".

In the background, another window shows the IPsec Policy configuration with the policy set to out and ipsec.

```
/ip firewall mangle add action=change-mss chain=forward new-mss=1360 dst-address=10.0.88.0/24 protocol=tcp tcp-flags=syn tcp-mss=!0-1360 ipsec-policy=out,ipsec passthrough=yes comment="IKE2: Clamp TCP MSS from ANY to 10.0.88.0/24"
```

Настройка КЛИЕНТОВ

Windows

8 / 8.1 / 10

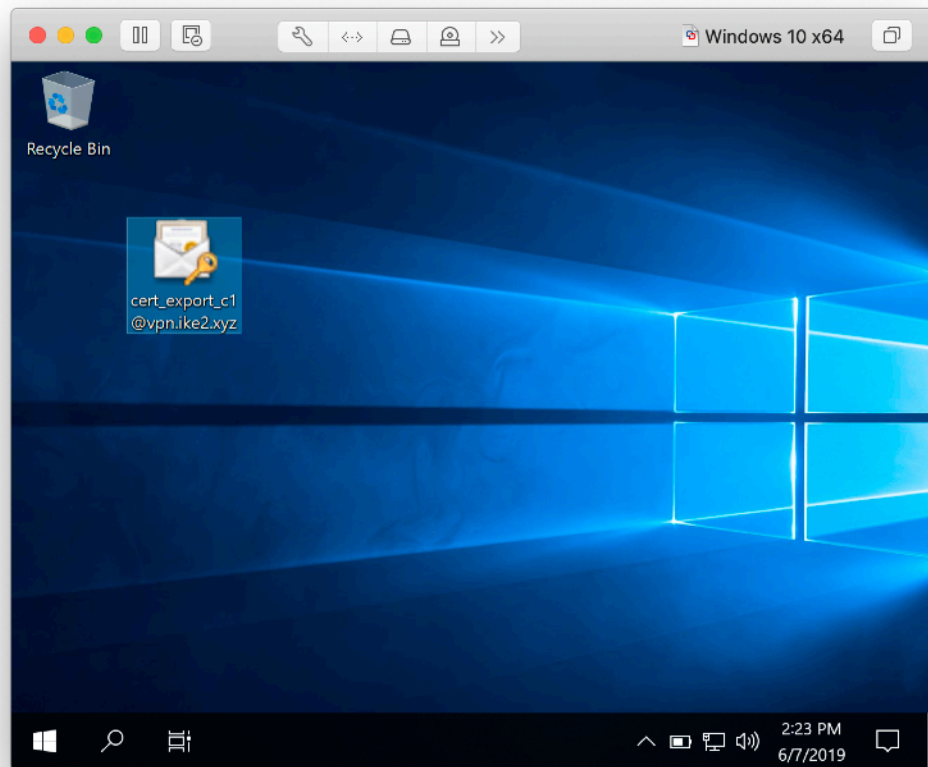
План действий

1. Импорт SSL сертификатов
2. Настройка IKEv2 соединения
3. Проверка маршрутов IKEv2

— — —

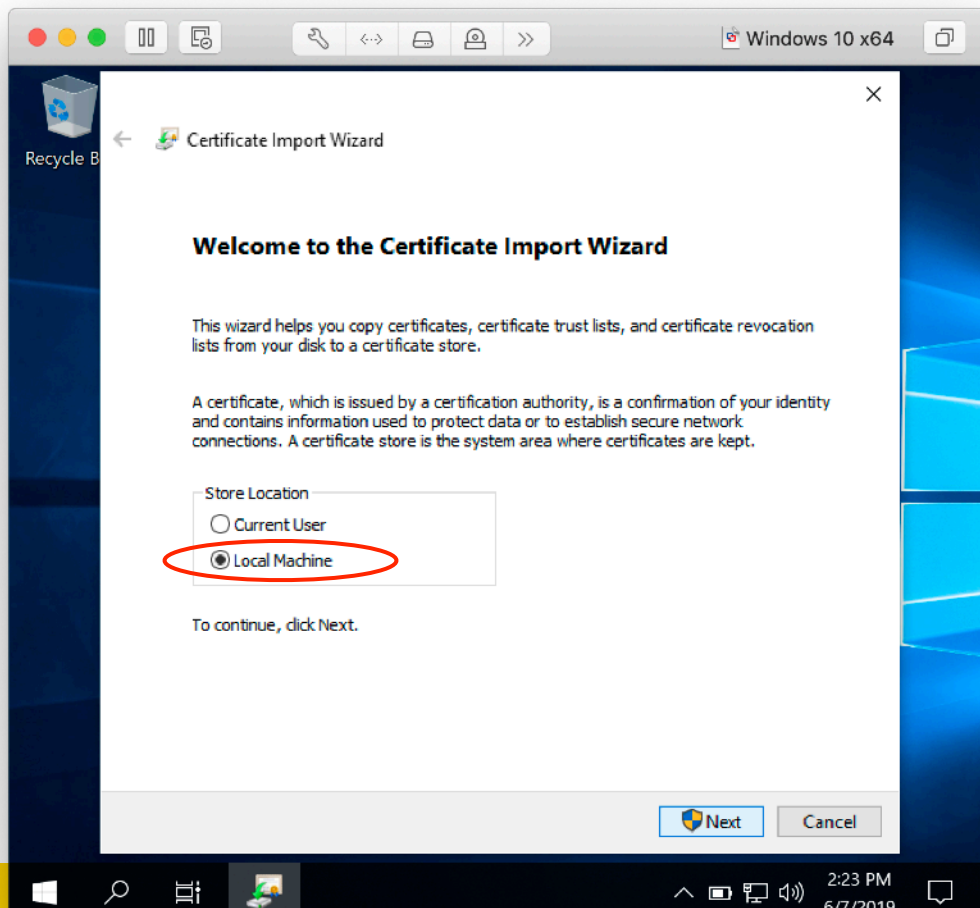
Windows 10: Импорт SSL сертификатов

— — —



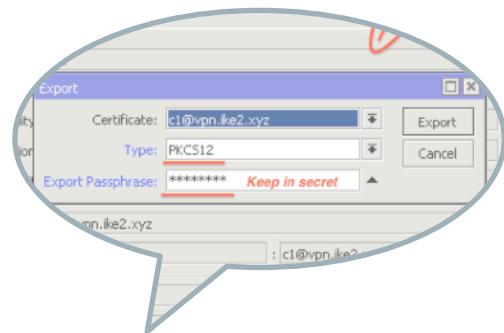
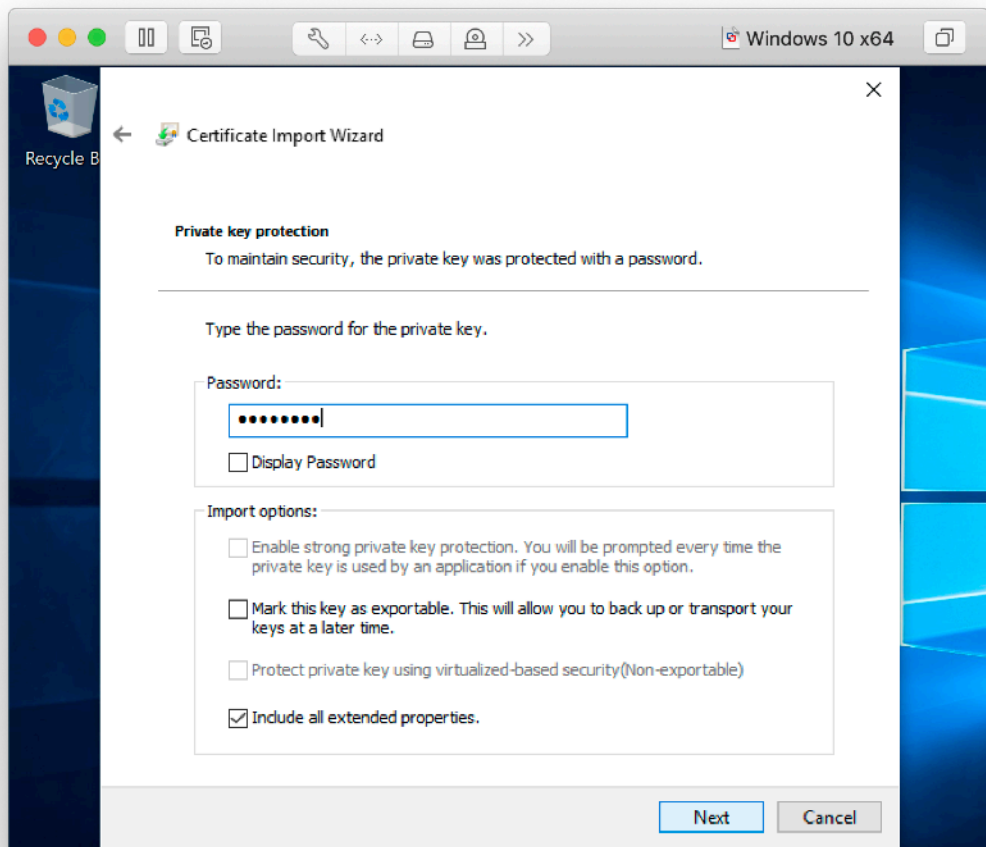
Скачать .p12 сертификат

Windows 10: Импорт SSL сертификатов



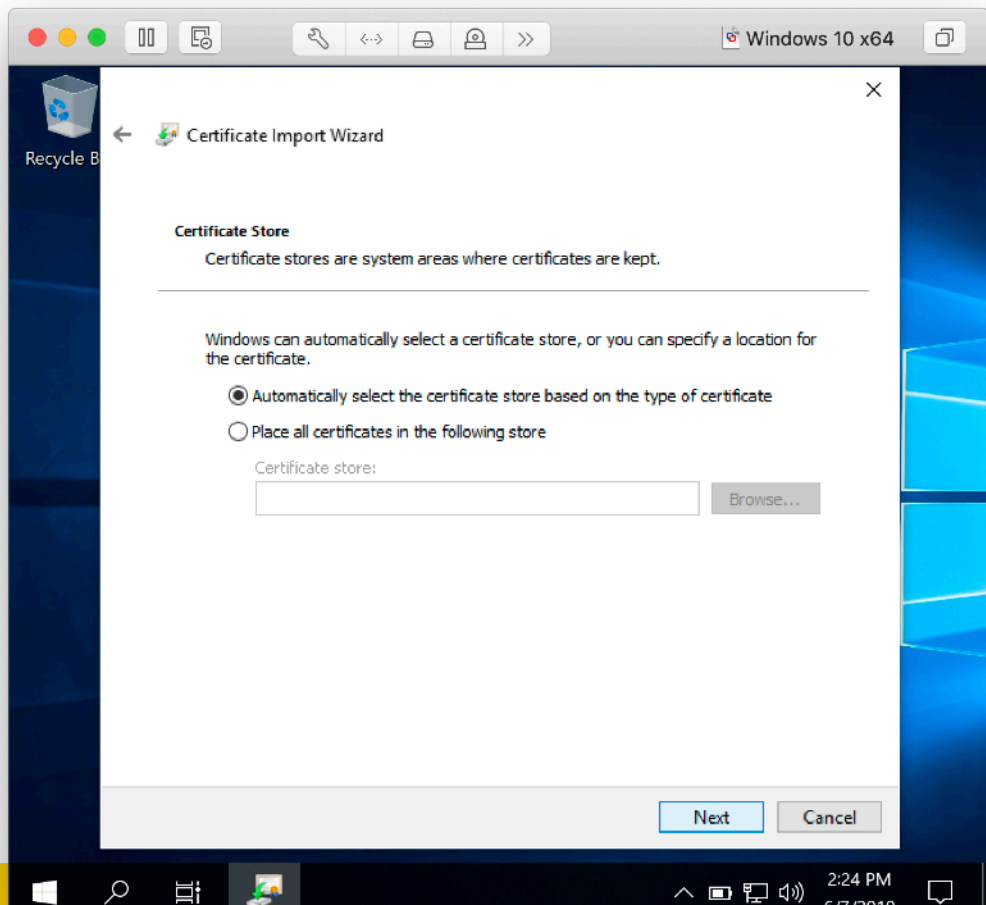
Выбрать **Local Machine** хранилище
—> **Далее**

Windows 10: Импорт SSL сертификатов



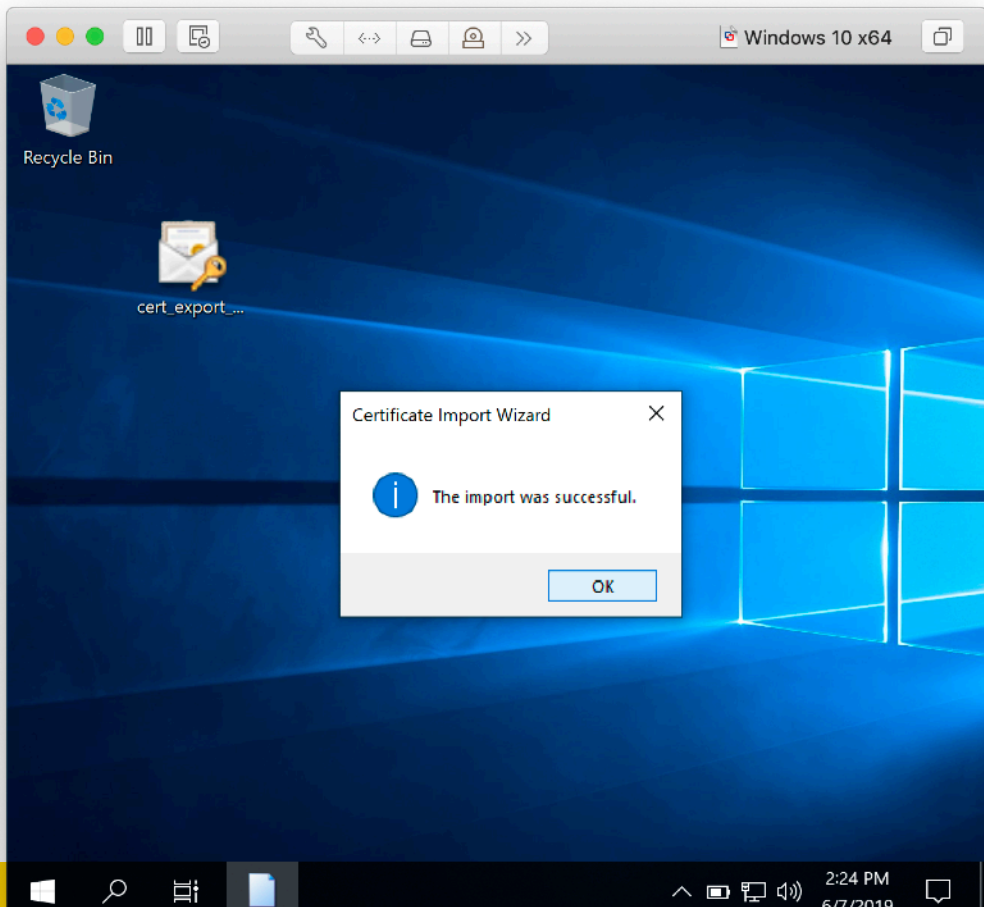
Ввести пароль
SSL сертификата клиента
—> **Далее**

Windows 10: Импорт SSL сертификатов



Автоматический выбор
—> **Далее**

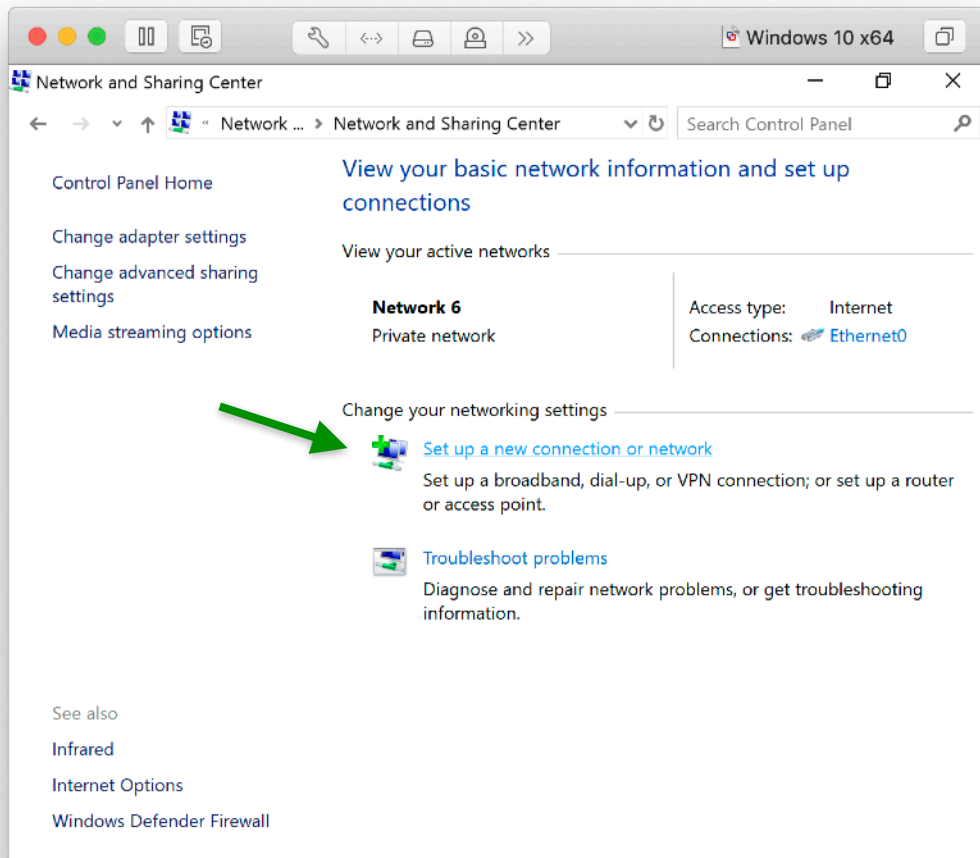
Windows 10: Импорт SSL сертификатов



SSL сертификат
успешно импортирован

—> OK

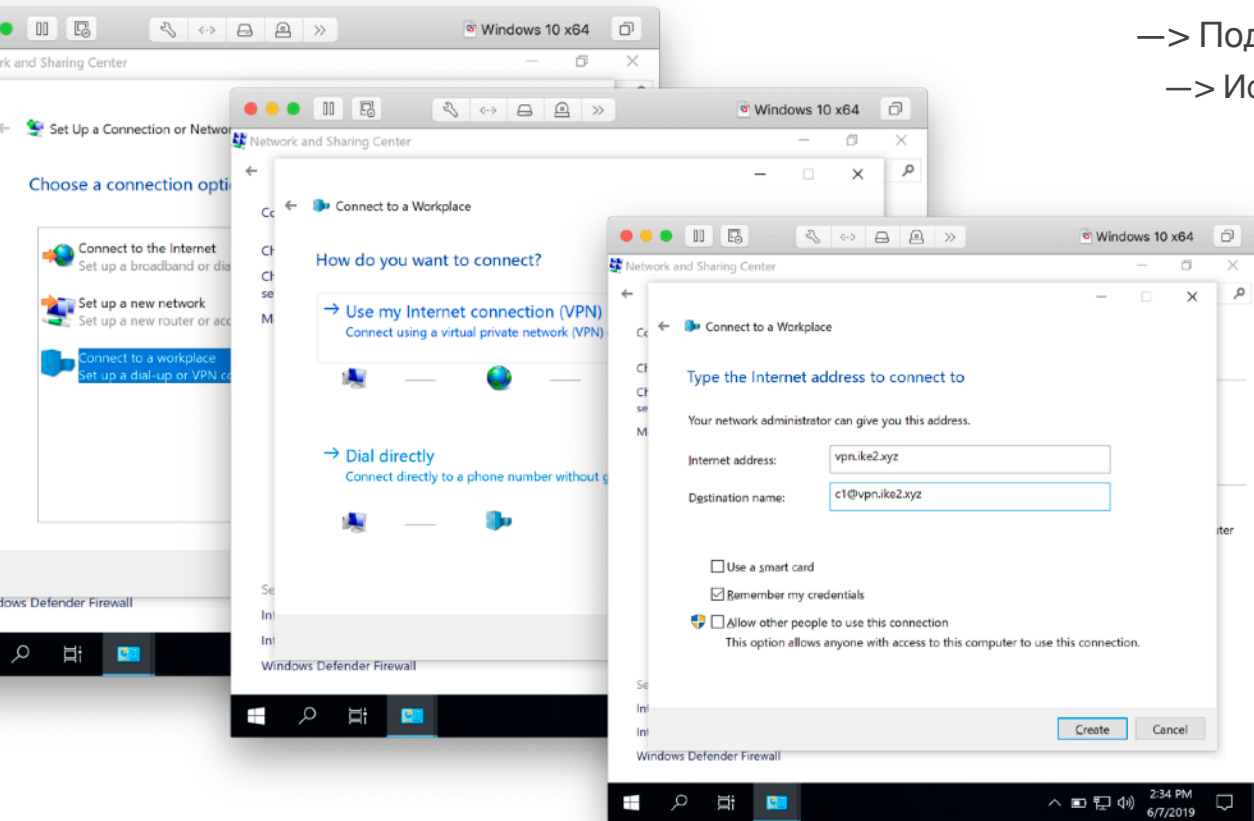
Windows 10: Настройка IKEv2 VPN соединения



- > Панель управления
- > Сеть и интернет
- > Центр управления сетями

Создание нового подключения

Windows 10: Настройка IKEv2 VPN соединения



—> Подключение к рабоче у месту

—> Использовать мое подключение (VPN)

—> **Далее**

Адрес:

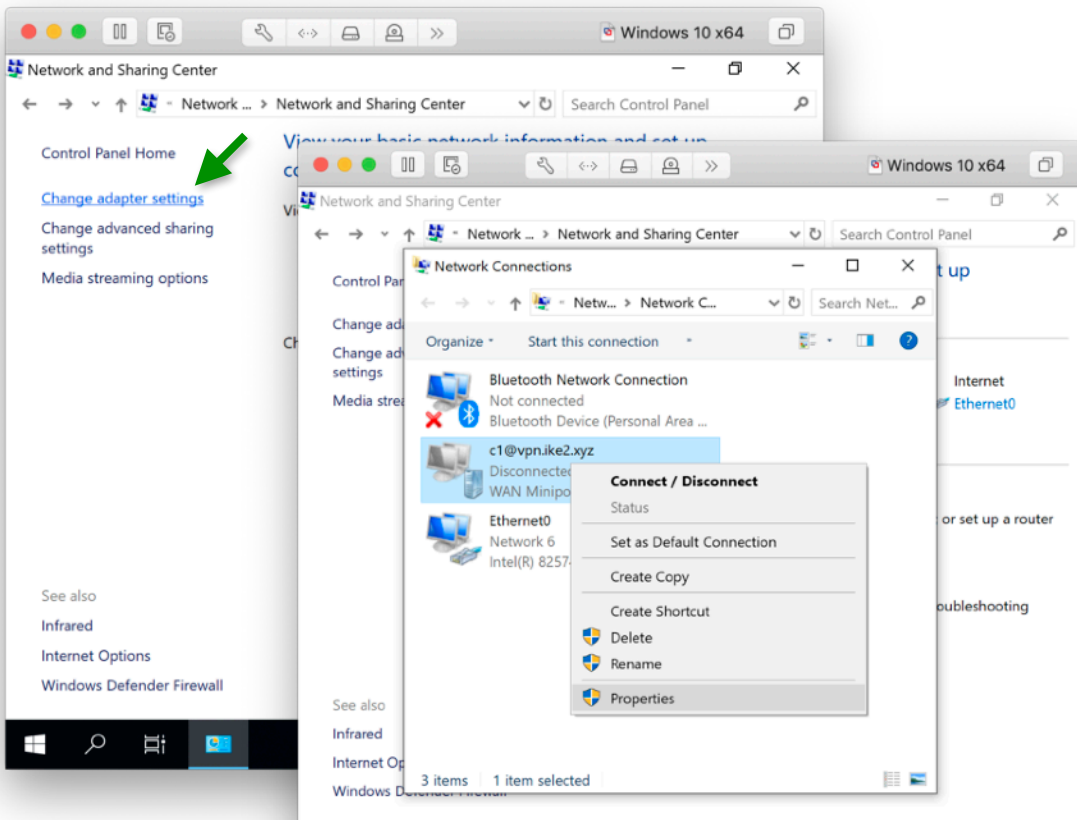
vpn.ike2.xyz

Имя назначения:

c1@vpn.ike2.xyz

—> **Создать**

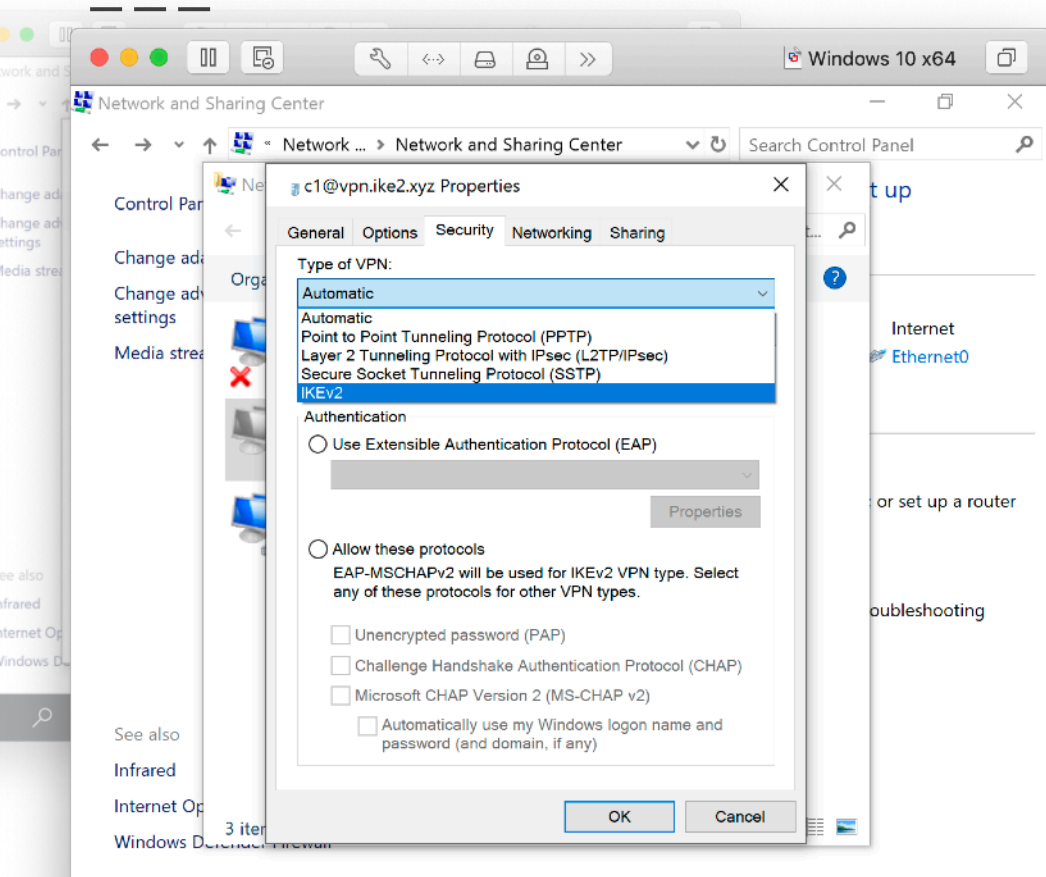
Windows 10: Настройка IKEv2 VPN соединения



—> Изменение параметров адаптера
c1@vpn.ike2.xyz

—> **Свойства**

Windows 10: Настройка IKEv2 VPN соединения

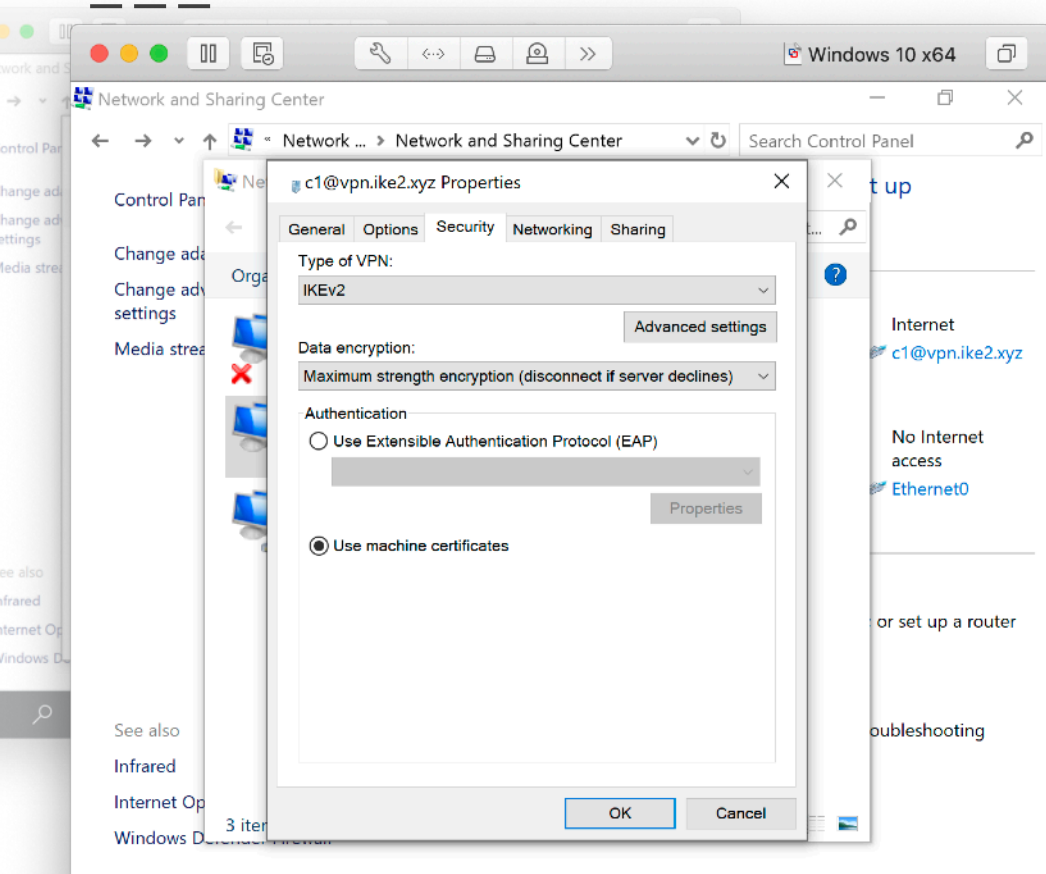


Свойства -> Безопасность

Тип VPN:

IKEv2

Windows 10: Настройка IKEv2 VPN соединения



Свойства -> Безопасность

Шифрование данных:
Самое стойкое

Проверка подлинности:
Использовать
сертификаты
компьютеров

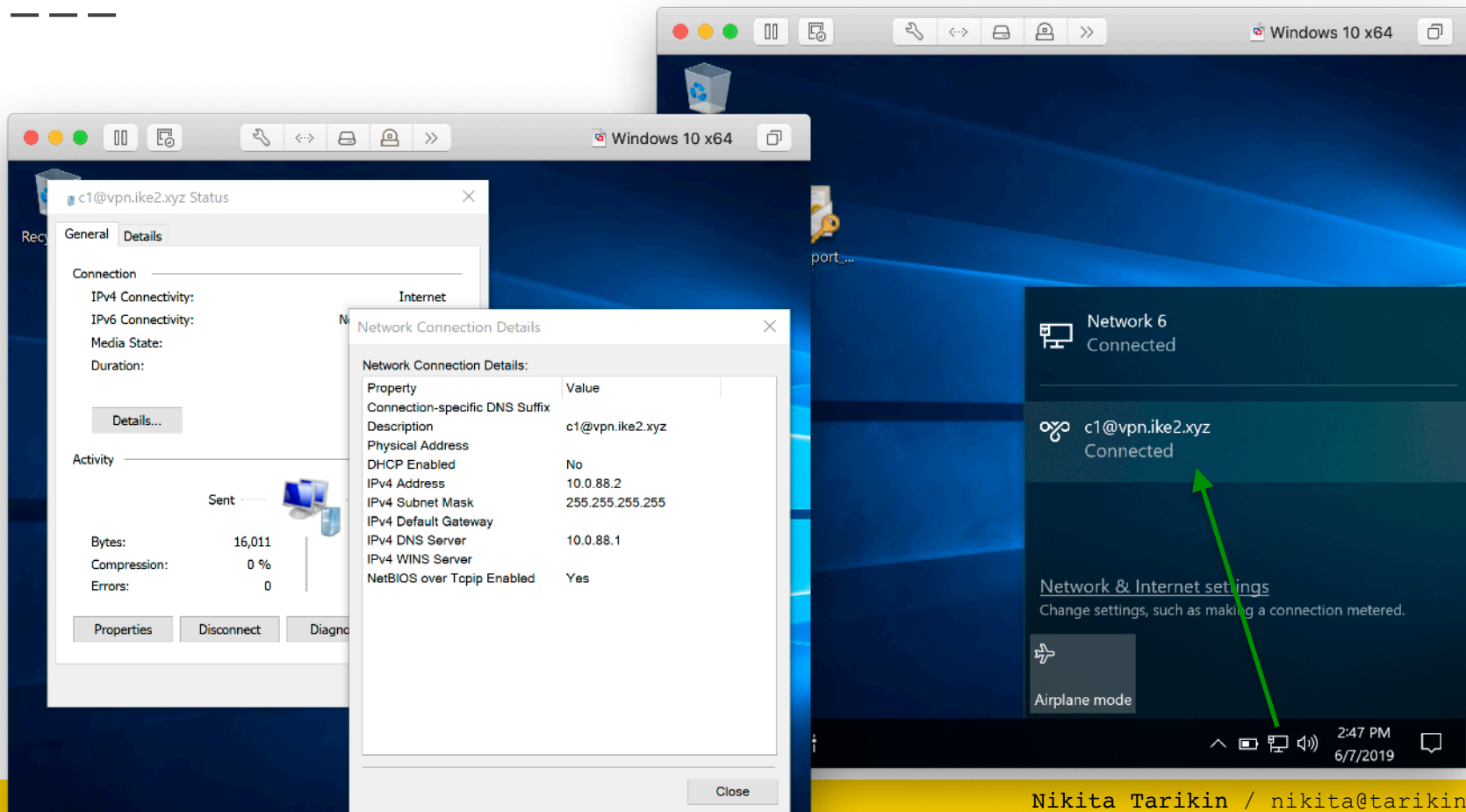
—> OK

Явный выбор сертификата для IKEv2 соединения

```
Set-VpnConnection -Name  
"c1@vpn.ike2.xyz" -  
MachineCertificateIssuerFilter  
'C:\mycerts\CA.crt'
```

Через уточнение издателя авторитета CA

Windows 10: проверка IKEv2 VPN соединения



Windows 10: проверка IKEv2 VPN маршрутов

```
Command Prompt

C:\Users>route -4 print

=====
Interface List
 9...00 0c 29 e6 e6 ce .....Intel(R) 82574L Gigabit Network Connection
25.....c1@vpn.ike2.xyz
 6...00 50 56 fc fe e4 .....Bluetooth Device (Personal Area Network)
 1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          192.168.88.1     192.168.88.252   4250
0.0.0.0                    0.0.0.0          On-link          10.0.88.2        26
10.0.88.2                  255.255.255.255  On-link          10.0.88.2        281
123.45.67.8                255.255.255.255  192.168.88.1     192.168.88.252   4251
127.0.0.0                  255.0.0.0        On-link          127.0.0.1        4556
127.0.0.1                  255.255.255.255  On-link          127.0.0.1        4556
127.255.255.255            255.255.255.255  On-link          127.0.0.1        4556
192.168.88.0                255.255.255.0    On-link          192.168.88.252   4506
192.168.88.252              255.255.255.255  On-link          192.168.88.252   4506
192.168.88.255              255.255.255.255  On-link          192.168.88.252   4506
224.0.0.0                  240.0.0.0        On-link          127.0.0.1        4556
224.0.0.0                  240.0.0.0        On-link          192.168.88.252   4506
224.0.0.0                  240.0.0.0        On-link          10.0.88.2         26
255.255.255.255            255.255.255.255  On-link          127.0.0.1        4556
255.255.255.255            255.255.255.255  On-link          192.168.88.252   4506
255.255.255.255            255.255.255.255  On-link          10.0.88.2        281
=====
```

route -4 print

Destination

0.0.0.0/0 (default)

Gateway:

On-link

Interface:

10.0.88.2

Metric (distance):

26

Windows 10: проверка IKEv2 VPN маршрутов

admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)

Dashboard

Session: 192.168.88.1 CPU: 1%

IPsec

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

Find

Name	Resp...	Address Pool	Address	Address Pr...	Split Include	System ...	Sr
modeconf vpn.ike2...	yes	pool vpn.ike2.xyz		32	192.168.99.0/24, 17...	yes	
request-only	no						

IPsec Mode Config <modeconf vpn.ike2.xyz>

Name: modeconf vpn.ike2.xyz

☒ Responder

Address Pool: pool vpn.ike2.xyz

Address:

Address Prefix Length: 32

Split Include:

- 192.168.99.0/24
- 172.16.0.0/22
- 10.20.0.0/21

☒ System DNS

Windows 10 x64

Command Prompt

IPv4 Route Table

Active Routes:

Network	Destination	Netmask	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	192.168.88.1	192.168.88.252	4250
	0.0.0.0	0.0.0.0	On-link	10.0.88.2	26
	10.0.88.2	255.255.255.255	On-link	10.0.88.2	281
	10.20.0.0	255.255.248.0	On-link	10.0.88.2	26
	10.20.7.255	255.255.255.255	On-link	10.0.88.2	281
	123.45.67.8	255.255.255.255	192.168.88.1	192.168.88.252	4251
	127.0.0.0	255.0.0.0	On-link	127.0.0.1	4556
	127.0.0.1	255.255.255.255	On-link	127.0.0.1	4556
	127.255.255.255	255.255.255.255	On-link	127.0.0.1	4556
	172.16.0.0	255.255.252.0	On-link	10.0.88.2	26
	172.16.3.255	255.255.255.255	On-link	10.0.88.2	281
	192.168.88.0	255.255.255.0	On-link	192.168.88.252	4506
	192.168.88.252	255.255.255.255	On-link	192.168.88.252	4506
	192.168.88.255	255.255.255.255	On-link	192.168.88.252	4506
	192.168.99.0	255.255.255.0	On-link	10.0.88.2	26
	192.168.99.255	255.255.255.255	On-link	10.0.88.2	281
	224.0.0.0	240.0.0.0	On-link	127.0.0.1	4556
	224.0.0.0	240.0.0.0	On-link	192.168.88.252	4506
	224.0.0.0	240.0.0.0	On-link	10.0.88.2	26
	255.255.255.255	255.255.255.255	On-link	127.0.0.1	4556
	255.255.255.255	255.255.255.255	On-link	192.168.88.252	4506
	255.255.255.255	255.255.255.255	On-link	10.0.88.2	281

Persistent Routes:

None

Windows 10: проверка IKEv2 VPN маршрутов

— 0.0.0.0/0 ???

Address:
Address Prefix Length:
Split Include:

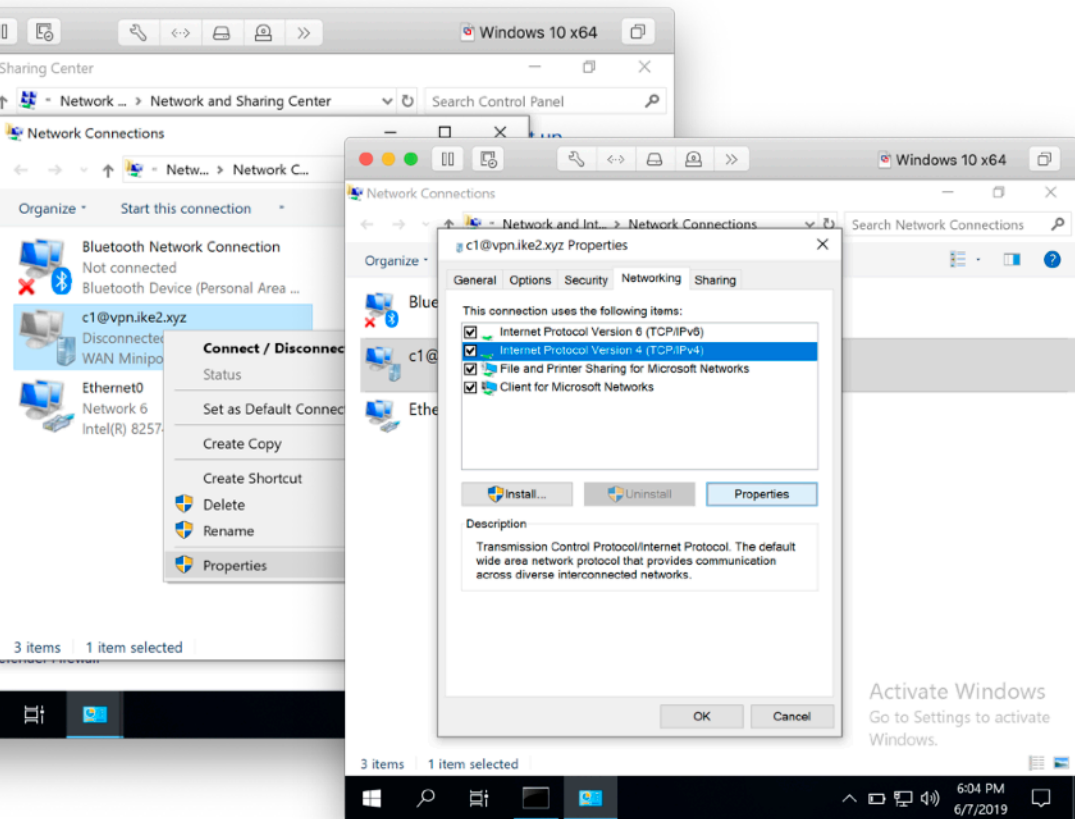
☒ System DNS

```
Windows 10 x64
Command Prompt

IPv4 Route Table
=====
Active Routes:
Network Destination    Netmask          Gateway          Interface        Metric
0.0.0.0                0.0.0.0          192.168.88.1     192.168.88.252    4250
0.0.0.0                0.0.0.0          On-link          10.0.88.2         26
10.0.88.2              255.255.255.255  On-link          10.0.88.2         281
10.20.0.0              255.255.248.0    On-link          10.0.88.2         26
10.20.7.255           255.255.255.255  On-link          10.0.88.2         281
123.45.67.8           255.255.255.255  192.168.88.1     192.168.88.252    4251
127.0.0.0              255.0.0.0        On-link          127.0.0.1         4556
127.0.0.1              255.255.255.255  On-link          127.0.0.1         4556
127.255.255.255        255.255.255.255  On-link          127.0.0.1         4556
172.16.0.0             255.255.252.0    On-link          10.0.88.2         26
172.16.3.255           255.255.255.255  On-link          10.0.88.2         281
192.168.88.0           255.255.255.0    On-link          192.168.88.252    4506
192.168.88.252         255.255.255.255  On-link          192.168.88.252    4506
192.168.88.255         255.255.255.255  On-link          192.168.88.252    4506
192.168.99.0           255.255.255.0    On-link          10.0.88.2         26
192.168.99.255         255.255.255.255  On-link          10.0.88.2         281
224.0.0.0              240.0.0.0        On-link          127.0.0.1         4556
224.0.0.0              240.0.0.0        On-link          192.168.88.252    4506
224.0.0.0              240.0.0.0        On-link          10.0.88.2         26
255.255.255.255        255.255.255.255  On-link          127.0.0.1         4556
255.255.255.255        255.255.255.255  On-link          192.168.88.252    4506
255.255.255.255        255.255.255.255  On-link          10.0.88.2         281
=====
Persistent Routes:
None
```

Windows 10: отключаем пересылку всего трафика через IKEv2 VPN

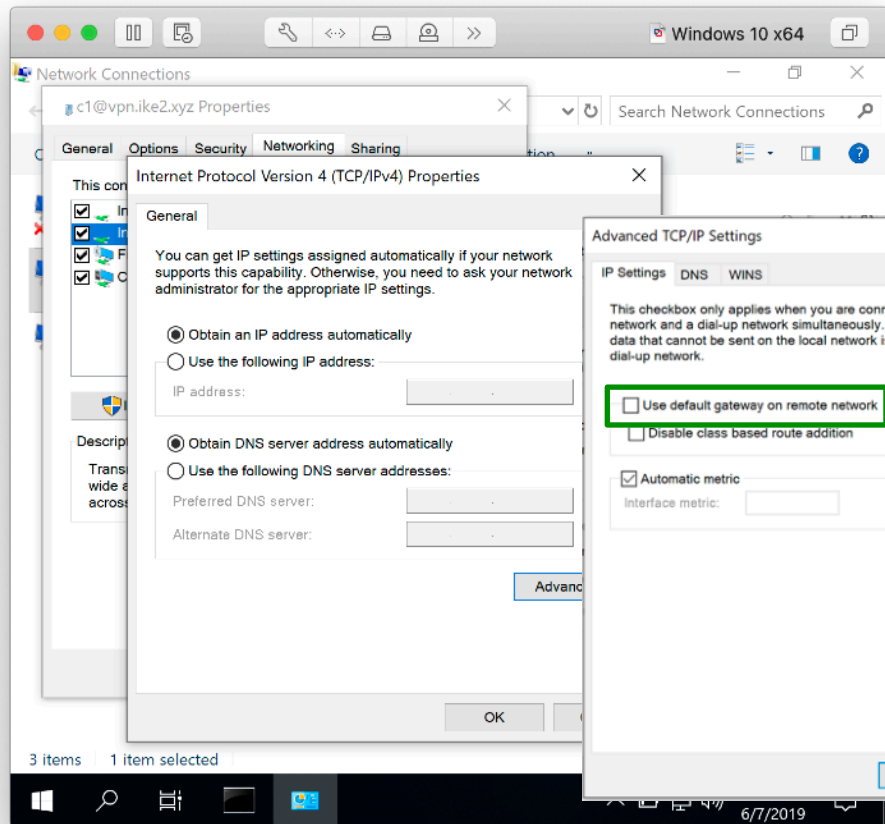
Свойства -> Сеть



✓ TCP/IPv4

—> Свойства

Windows 10: отключаем пересылку всего трафика через IKEv2 VPN



Свойства -> Сеть

Свойства TCP/IPv4

- ✓ Получить IP адрес автоматически
- ✓ Получить адрес DNS автоматически

—>

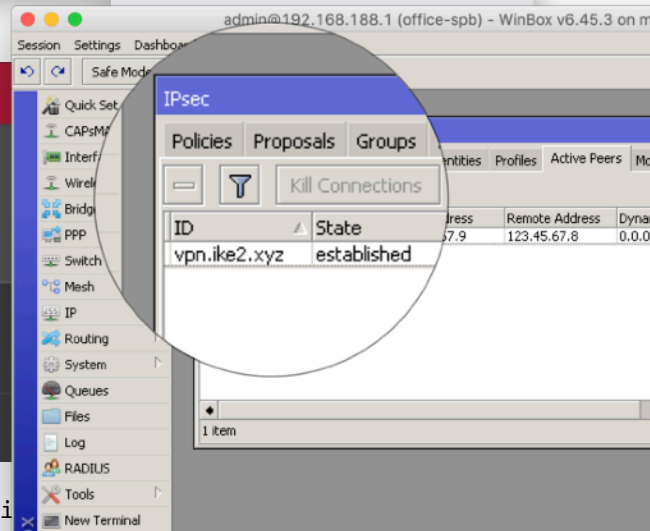
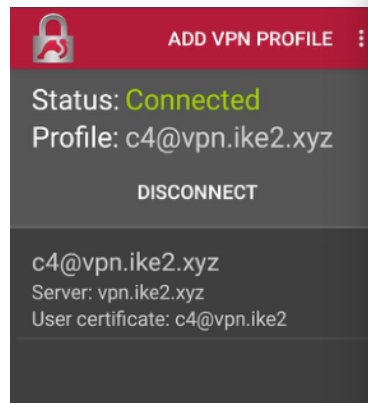
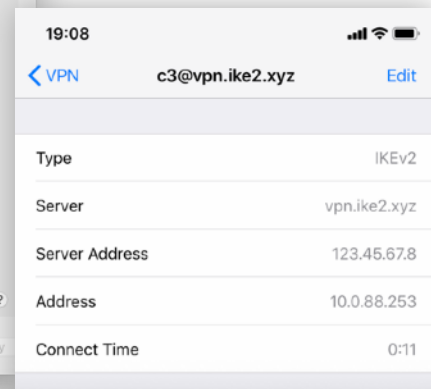
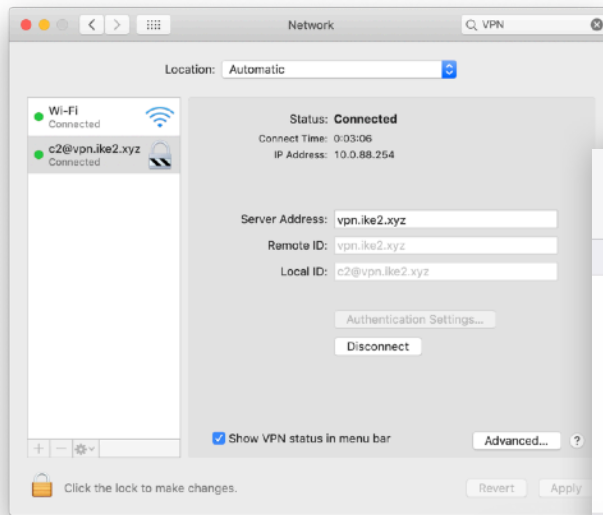
Дополнительно

Дополнительные параметры TCP/IP

☐ Использовать основной шлюз

Подключение non-Windows

MacOS
iOS
Android
RouterOS



Apple MacOS

≥ 10.11 El Capitan

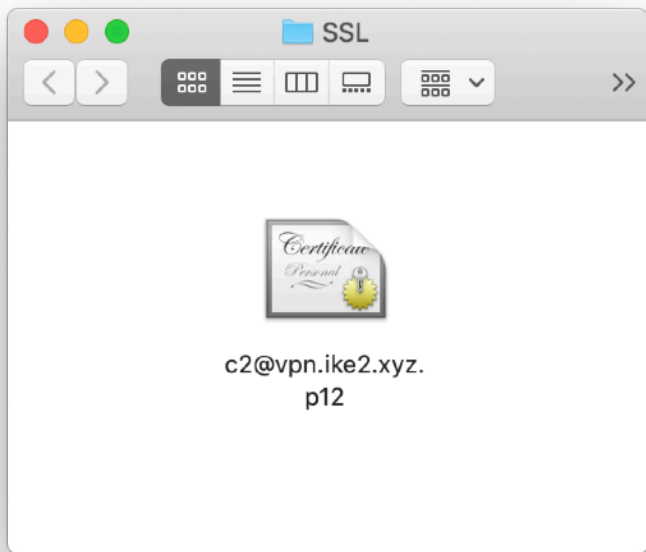
План действий

1. Импорт SSL сертификатов
2. Настройка IKEv2 VPN соединения
3. Проверка IKEv2 VPN маршрутов

— — —

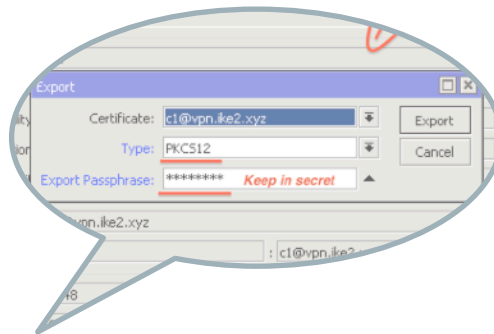
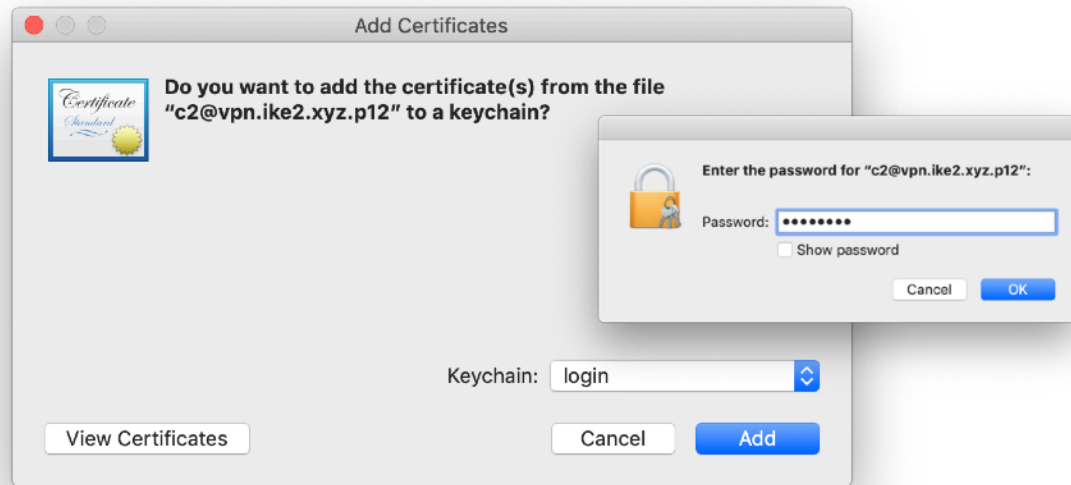
MacOS: Импорт SSL сертификатов

— — —



Скачать .p12 сертификат

MacOS: Импорт SSL сертификатов



Keychain:
login (default)

—> **Add**

Type your
SSL certificate password

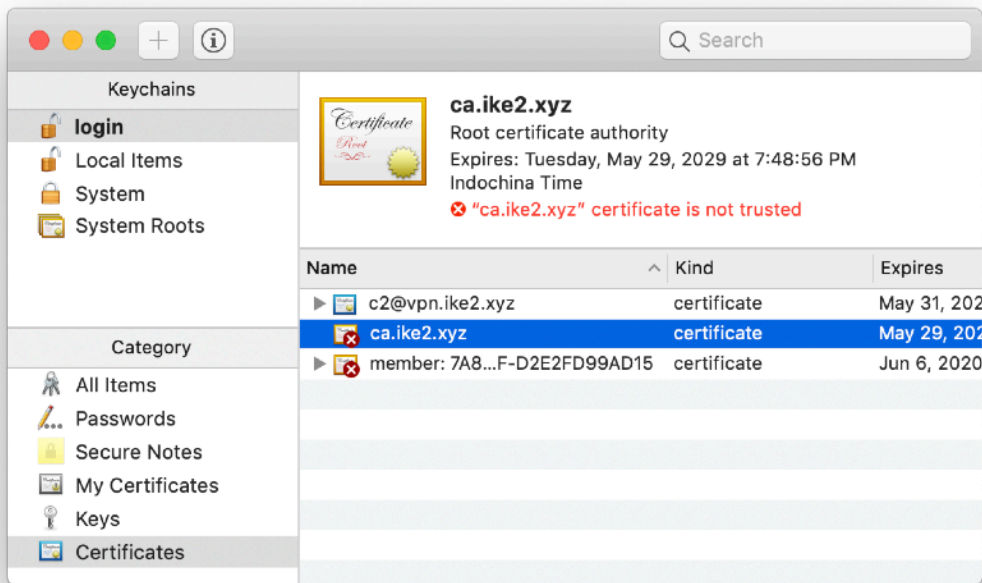
—> **OK**

MacOS: Управление импортированными SSL сертификатами

— — —



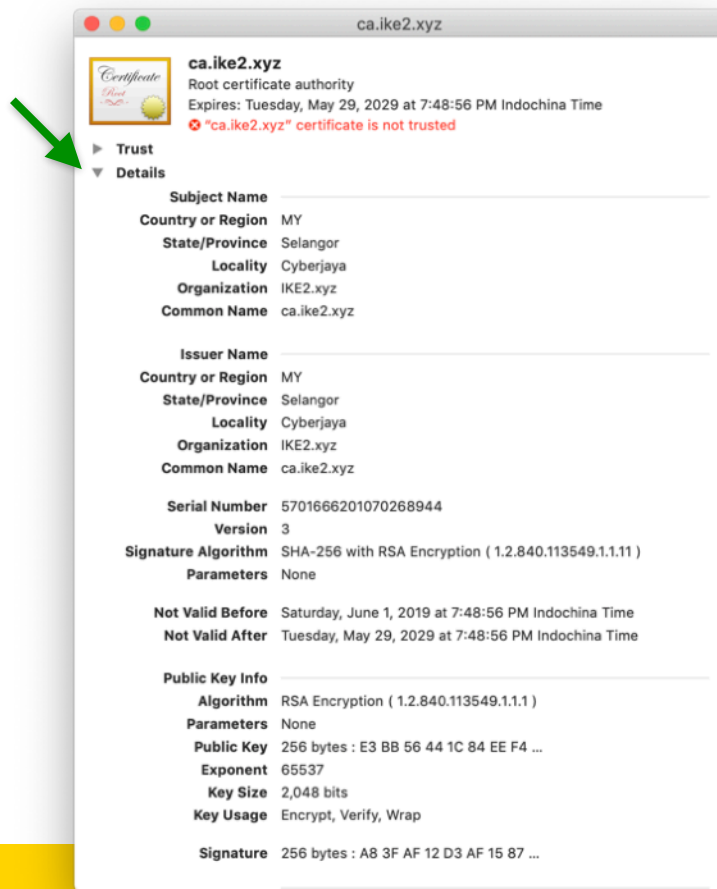
Keychain access



1. Launch keychain access
2. Find **ca.ike2.xyz** root certificate authority

MacOS: Управление импортированными SSL сертификатами

Important



Keychain access

Verify CA certificate details

MacOS: Управление импортированными SSL сертификатами

Important



Keychain access

Сверяем **отпечатки** CA сертификата

Public Key Info

Algorithm RSA Encryption (1.2.840.113549.1.1)

Parameters None

Public Key 256 bytes : E3 BB 56 44 1C 84 EE F4 ...

Exponent 65537

Key Size 2,048 bits

Key Usage Encrypt, Verify, Wrap

Signature 256 bytes : A8 3F AF 12 D3 AF 15 87 ...

Extension Key Usage (2.5.29.15)

Critical YES

Usage Digital Signature, Key Encipherment, Data Encipherment, Key Cert Sign, CRL Sign

Extension Basic Constraints (2.5.29.19)

Critical YES

Usage

Extension Subject Key Identifier (2.5.29.14)

Critical NO

Key ID 25 F0 0B D3 3A 6C F8 96 04 A9 FA 19 24 A9 E3 56 58 C3 9B CF

Extension Subject Alternative Name (2.5.29.17)

Critical NO

DNS Name ca.ike2.xyz

Extension Netscape Certificate Comment (2.16.840.1.113730.1.13)

Critical NO

Data Generated by RouterOS

Fingerprints

SHA-256 B5 7C AF 68 13 B3 52 A0 AB AB AA 4E 42 F8 C5 69 44 87 57 EE DA F8 30 89 3E 4B 05 C6 D7 33 D9 4B

SHA-1 6B A4 71 8B 3F 22 4E 3D C7 83 05 69 BF D8 94 C3 38 56 87 D8

admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)

Dashboard

Mode Session: 192.168.88.1 CPU:0%

Certificate <ca.ike2.xyz>

General Key Usage Status

CA CRL Host:

SCEP URL:

CA:

Serial Number:

Fingerprint: b57caf6813b352a0ababaa4e42f8c569440757eedaf830b93e4b05c6d733d94b

Req. Fingerprint:

CA Fingerprint:

Invalid Before: Jun/01/2019 20:48:56

Invalid After: May/29/2029 20:48:56

Expires After: 3641d 03:49:00

Revoked:

OK Cancel Apply Copy Remove Sign Sign via SCEP Import Card Reinstall Card Verify Set CA Passphrase Export Revoke

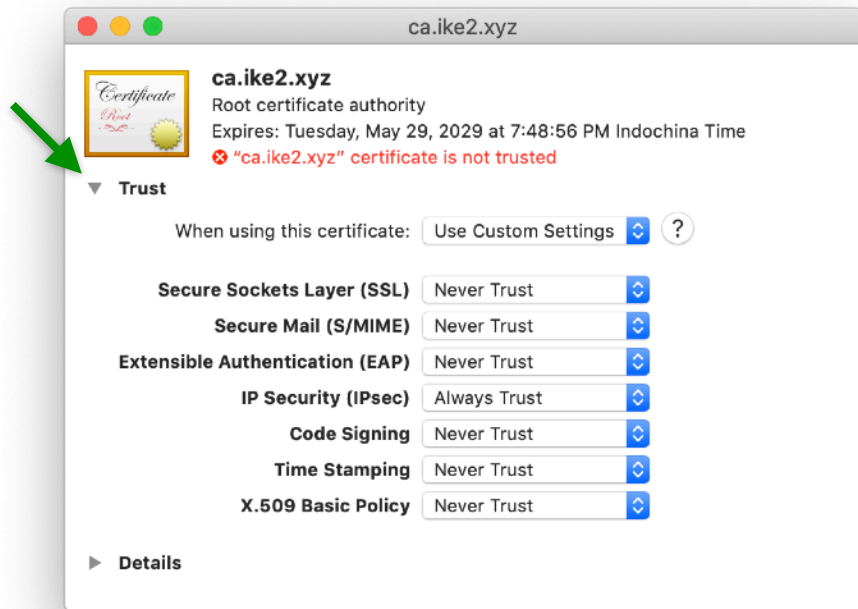
private key authority expired smart card key trusted

MacOS: Управление импортированными SSL сертификатами

Important



Keychain access



✓ IP Security (IPSec)

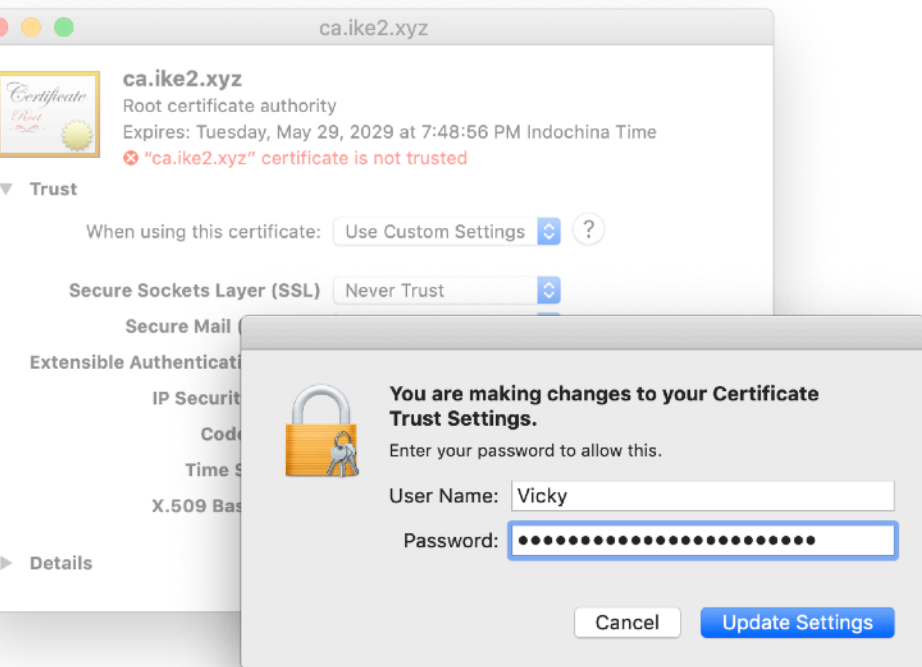
✗ Everything else

MacOS: Управление импортированными SSL сертификатами

Important



Keychain access

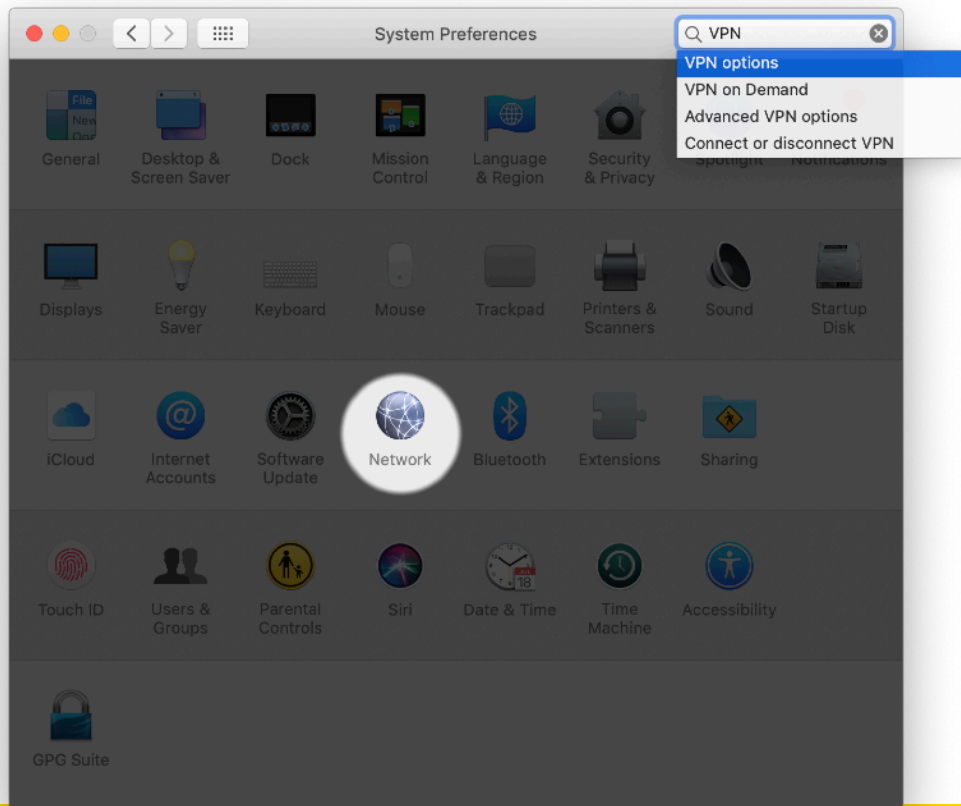


Type your
MacOS password

—> Update settings

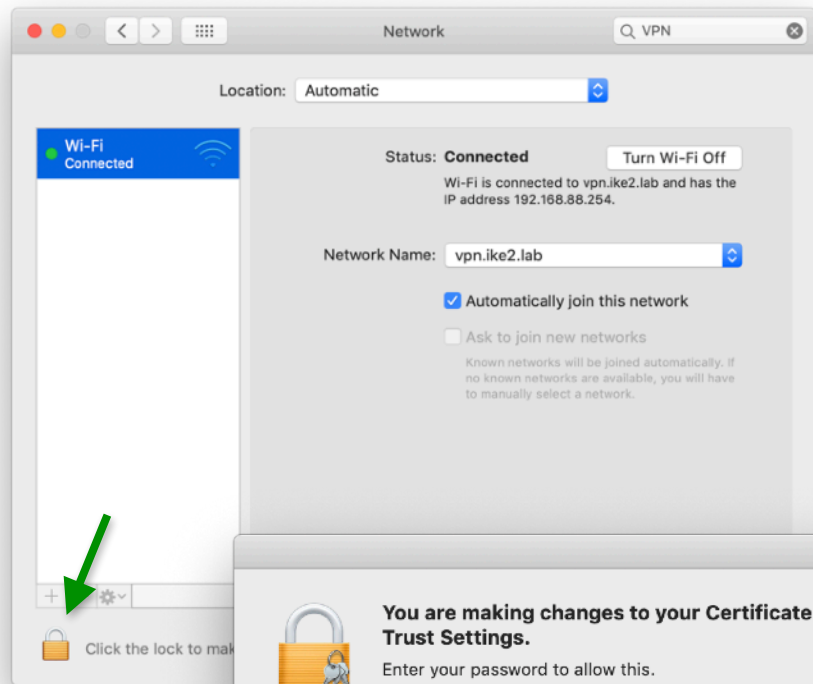
MacOS: Настройка IKEv2 VPN соединения

— — —

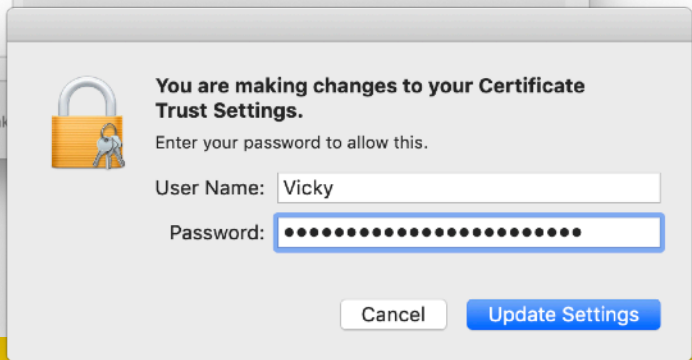


System preferences ->
Network

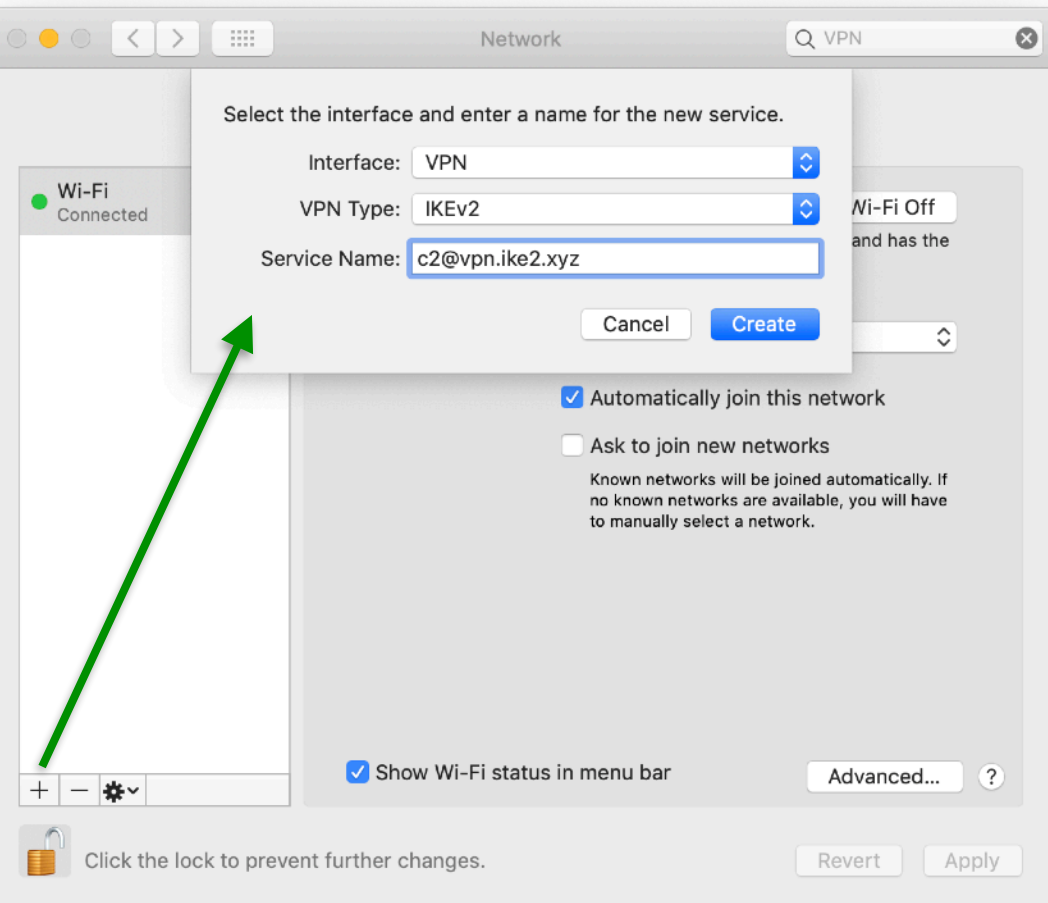
MacOS: Настройка IKEv2 VPN соединения



Unlock to make changes



MacOS: Настройка IKEv2 VPN соединения



Create new connection

Interface:

VPN

VPN Type:

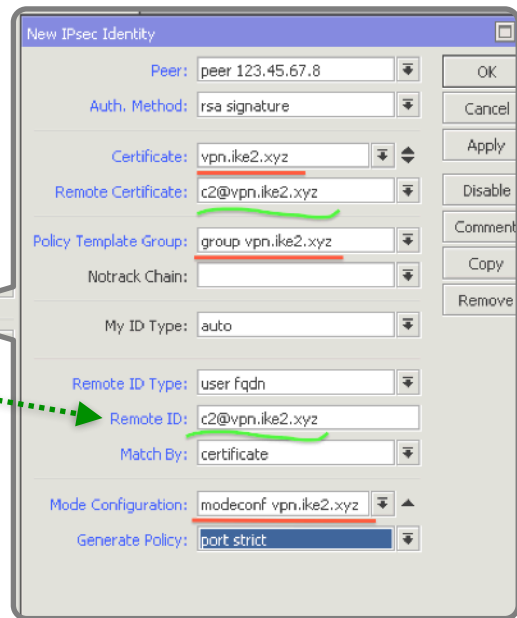
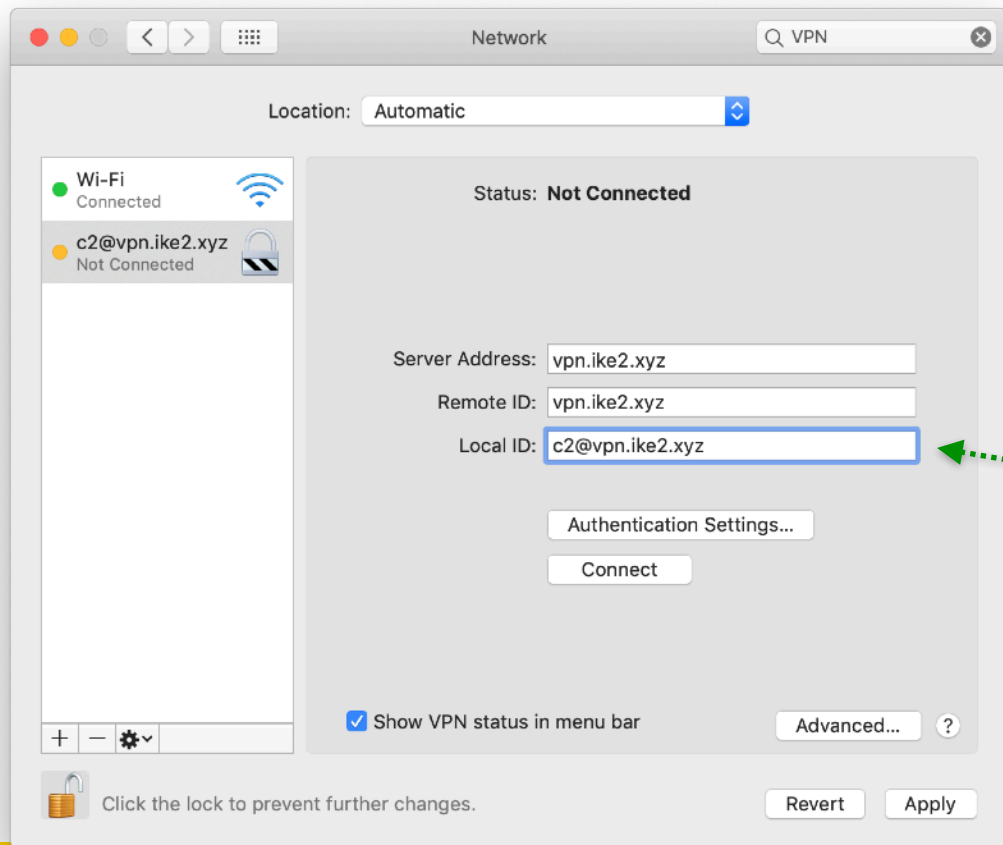
IKEv2

Service name:

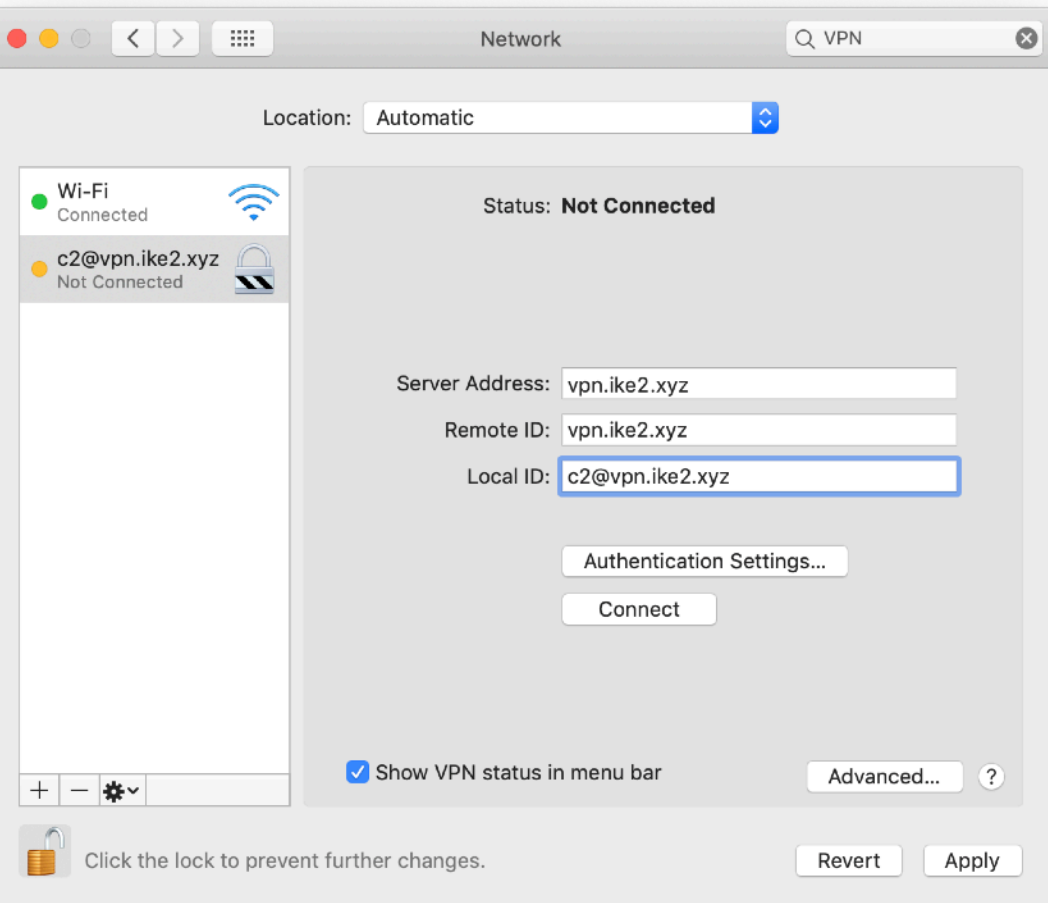
c2@vpn.ike2.xyz

→ **Create**

MacOS: Настройка IKEv2 VPN соединения



MacOS: Настройка IKEv2 VPN соединения



Create new connection

Server Address:

vpn.ike2.xyz

Remote ID:

vpn.ike2.xyz

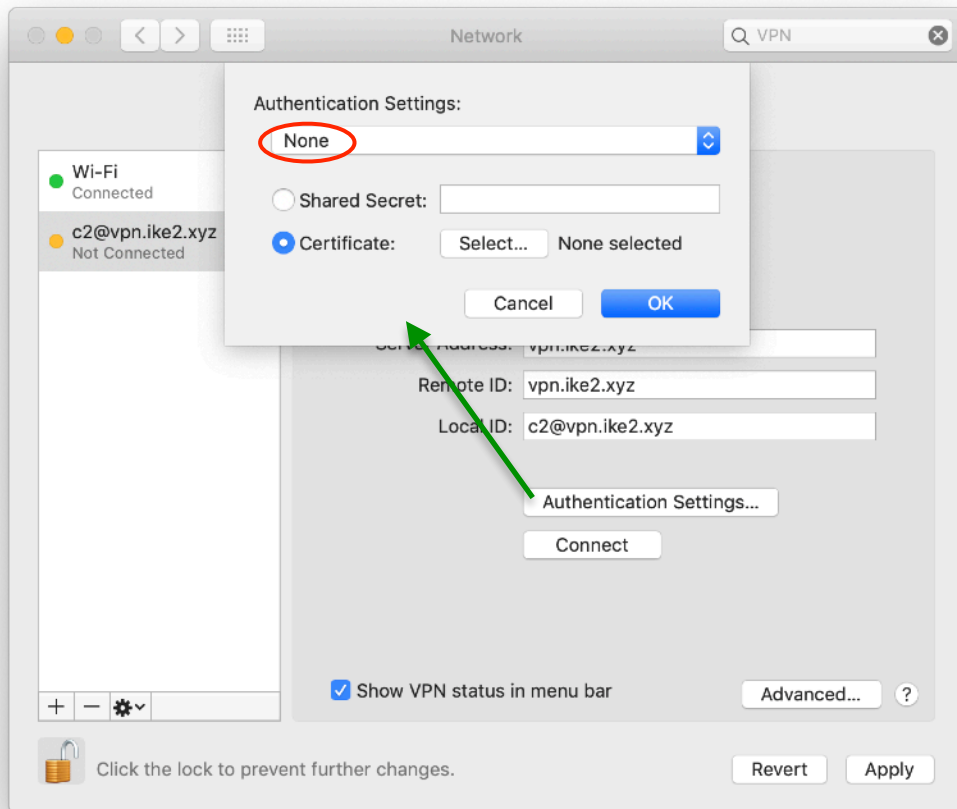
Local ID:

c2@vpn.ike2.xyz

✓ Show VPN status in menu bar

→ **Apply**

MacOS: Настройка IKEv2 VPN соединения



Authentication Settings

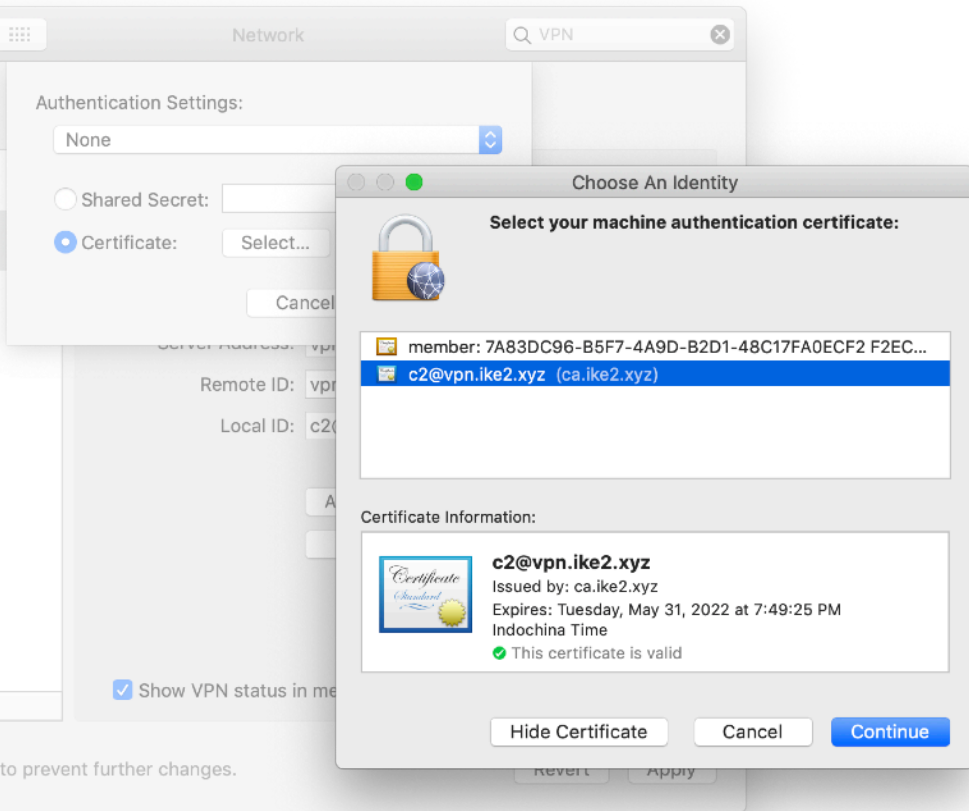
Authentication Settings:

None

Certificate:

→ **Select**

MacOS: Настройка IKEv2 VPN соединения



Authentication Settings

Select machine auth certificate:
c2@vpn.ike2.xyz

→ **Continue**

MacOS: Подключение IKEv2 VPN

The screenshot displays the macOS System Preferences window, specifically the Network section. The 'VPN' tab is selected, showing a list of network services on the left. The 'c2@vpn.ike2.xyz' service is highlighted, and its configuration window is open. The configuration window shows the 'Location' set to 'Automatic' and the 'Status' as 'Connected'. The 'Connect Time' is 0:03:06 and the 'IP Address' is 10.0.88.254. The 'Server Address' is 'vpn.ike2.xyz', the 'Remote ID' is 'vpn.ike2.xyz', and the 'Local ID' is 'c2@vpn.ike2.xyz'. The 'Authentication Settings...' button is visible. The 'Show VPN status in menu bar' checkbox is checked. The 'Disconnect' button is also present. The 'Advanced...' button is visible at the bottom right of the configuration window. The 'Revert' and 'Apply' buttons are at the bottom of the configuration window.

Network

Location: Automatic

Wi-Fi
Connected

c2@vpn.ike2.xyz
Not Connected

Status: Not Connected

Server Address: vpn.ike2.xyz

Remote ID: vpn.ike2.xyz

Local ID: c2@vpn.ike2.xyz

Authentication Settings...

Disconnect

✓ Show VPN status in menu bar

Click the lock to prevent further changes.

Don't forget
to **lock settings**

Click the lock to make changes.

Disconnect c2@vpn.ike2.xyz

c2@vpn.ike2.xyz

✓ Default

✓ Show Time Connected

✓ Show Status While Connecting

Open Network Preferences...

Network

VPN

Location: Automatic

Status: **Connected**

Connect Time: 0:03:06

IP Address: 10.0.88.254

Server Address: vpn.ike2.xyz

Remote ID: vpn.ike2.xyz

Local ID: c2@vpn.ike2.xyz

Authentication Settings...

Disconnect

✓ Show VPN status in menu bar

Advanced... ?

Revert Apply

MacOS: Проверка IKEv2 VPN маршрутов

admin@192.168.88.1 (MikroTik) - WinBox v6.44.3 on mAP lite (mipsbe)

ard

Session: 192.168.88.1

CPU: 1%

IPsec

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

Name	Resp...	Address Pool	Address	Address Pr...	Split Include	System ...
modeconf vpn.ike2...	yes	pool vpn.ike2.xyz		32	192.168.99.0/24, 17...	yes
request-only	no					

IPsec Mode Config <modeconf vpn.ike2.xyz>

Name: modeconf vpn.ike2.xyz

☒ Responder

Address Pool: pool vpn.ike2.xyz

Address:

Address Prefix Length: 32

Split Include: 192.168.99.0/24, 172.16.0.0/22, 10.20.0.0/21

☒ System DNS

Disconnect c2@vpn.ike2.xyz

c2@vpn.ike2.xyz

✓ Default

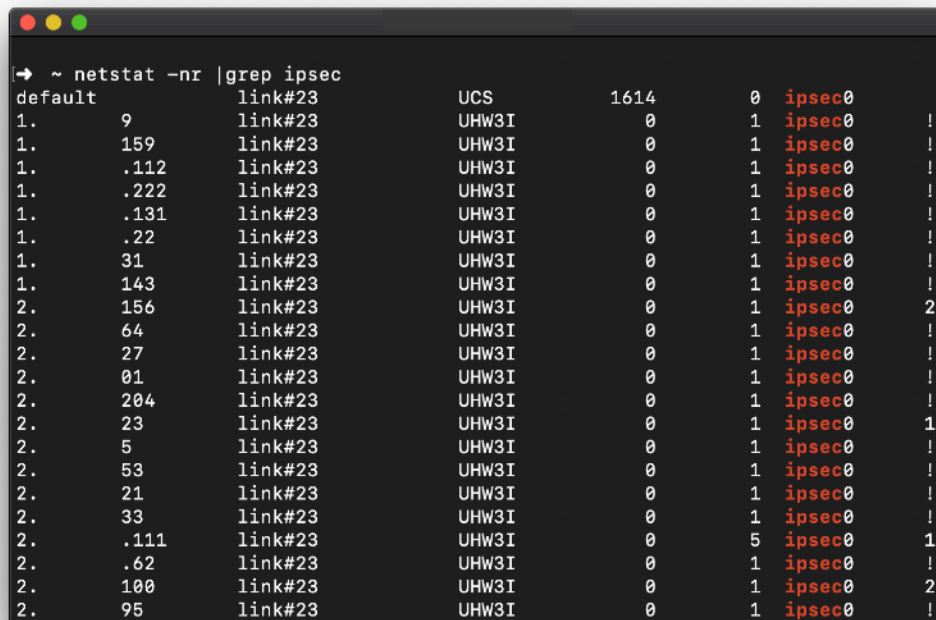
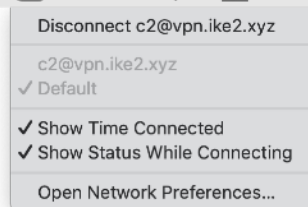
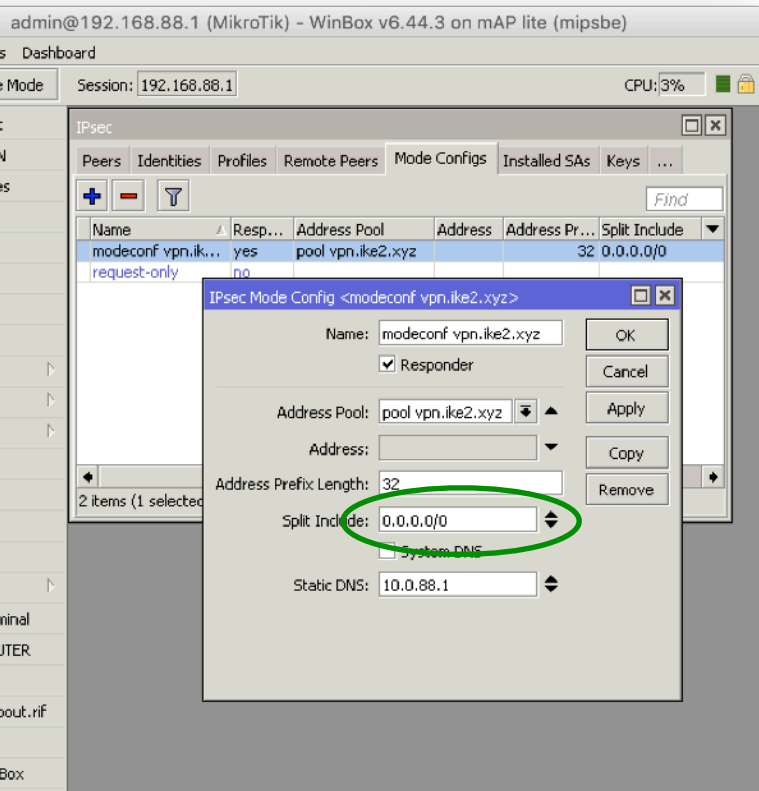
✓ Show Time Connected

✓ Show Status While Connecting

Open Network Preferences...

```
➔ ~ netstat -nr |grep ipsec
default          link#23          UCSI             0             0 ipsec0
10.0.88.254      10.0.88.254      UH               3             0 ipsec0
10.20/21         10.0.88.254      UGSc            0             0 ipsec0
172.16/22        10.0.88.254      UGSc            0             0 ipsec0
192.168.99       10.0.88.254      UGSc            0             0 ipsec0
224.0.0/4        link#23          UmCSI           0             0 ipsec0
255.255.255.255/32 link#23          UCSI             0             0 ipsec0
➔ ~
```


MacOS: Проверка IKEv2 VPN маршрутов



Apple iOS

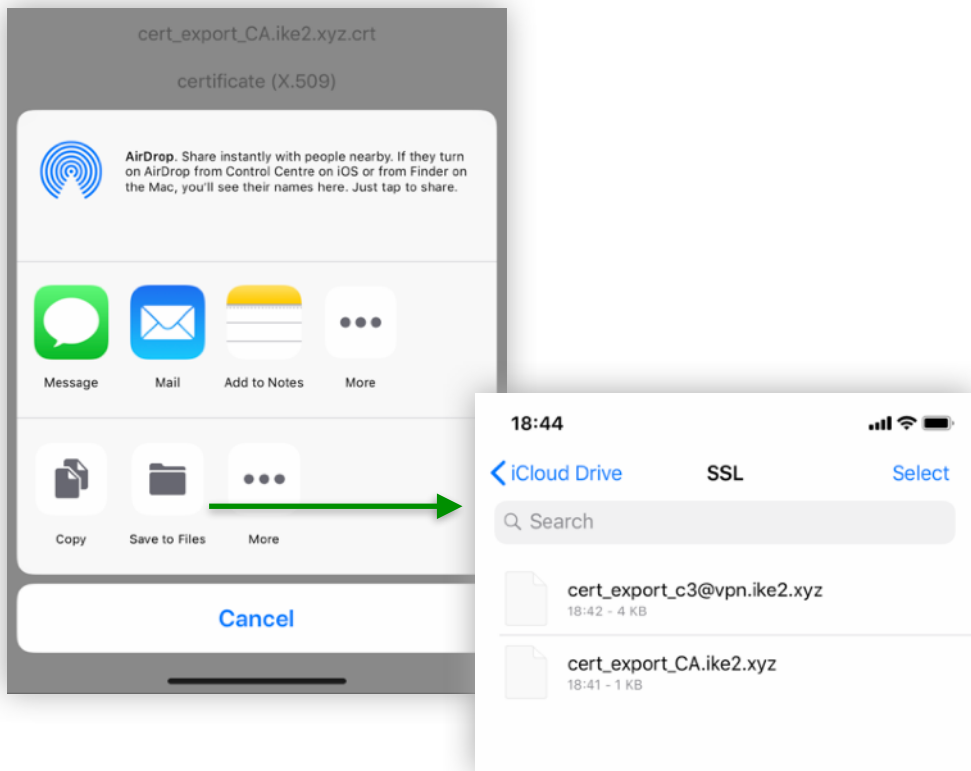
≥ версия 9

План действий

1. Импорт SSL сертификатов
2. Настройка IKEv2 VPN соединения

— — —

iOS: Загрузка SSL сертификатов

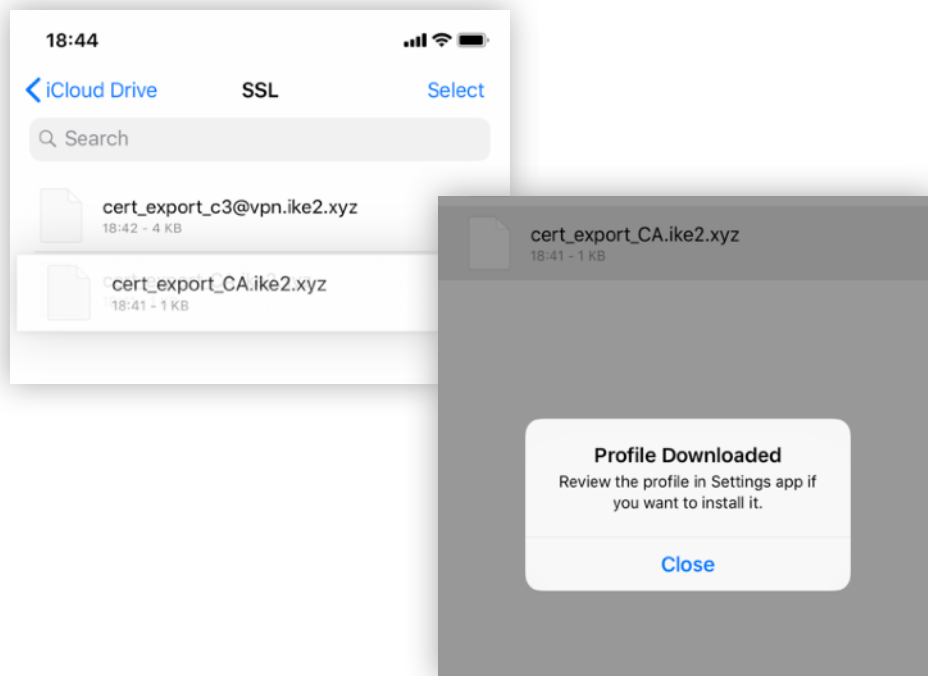


Download **CA** certificate .crt

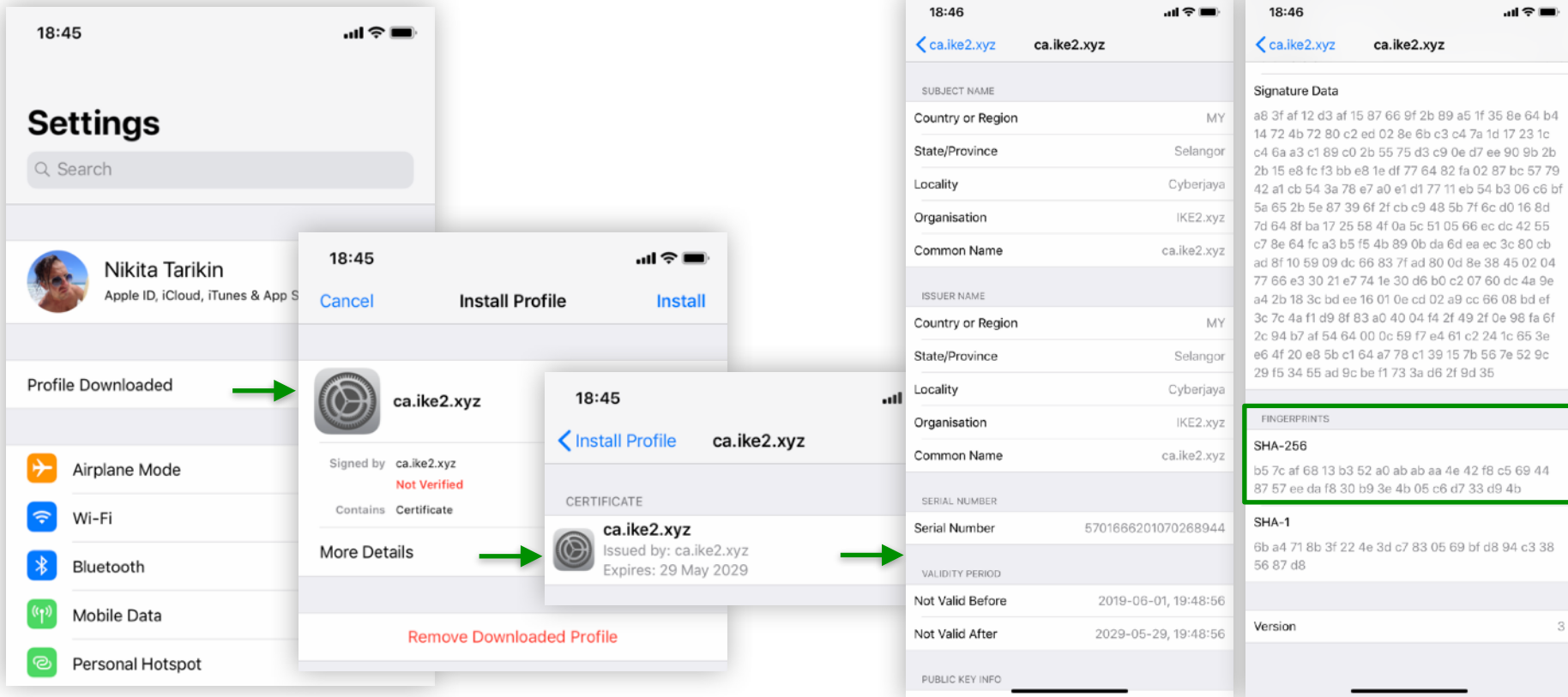
Download **client** certificate .p12

iOS: Импорт SSL сертификата авторитета CA

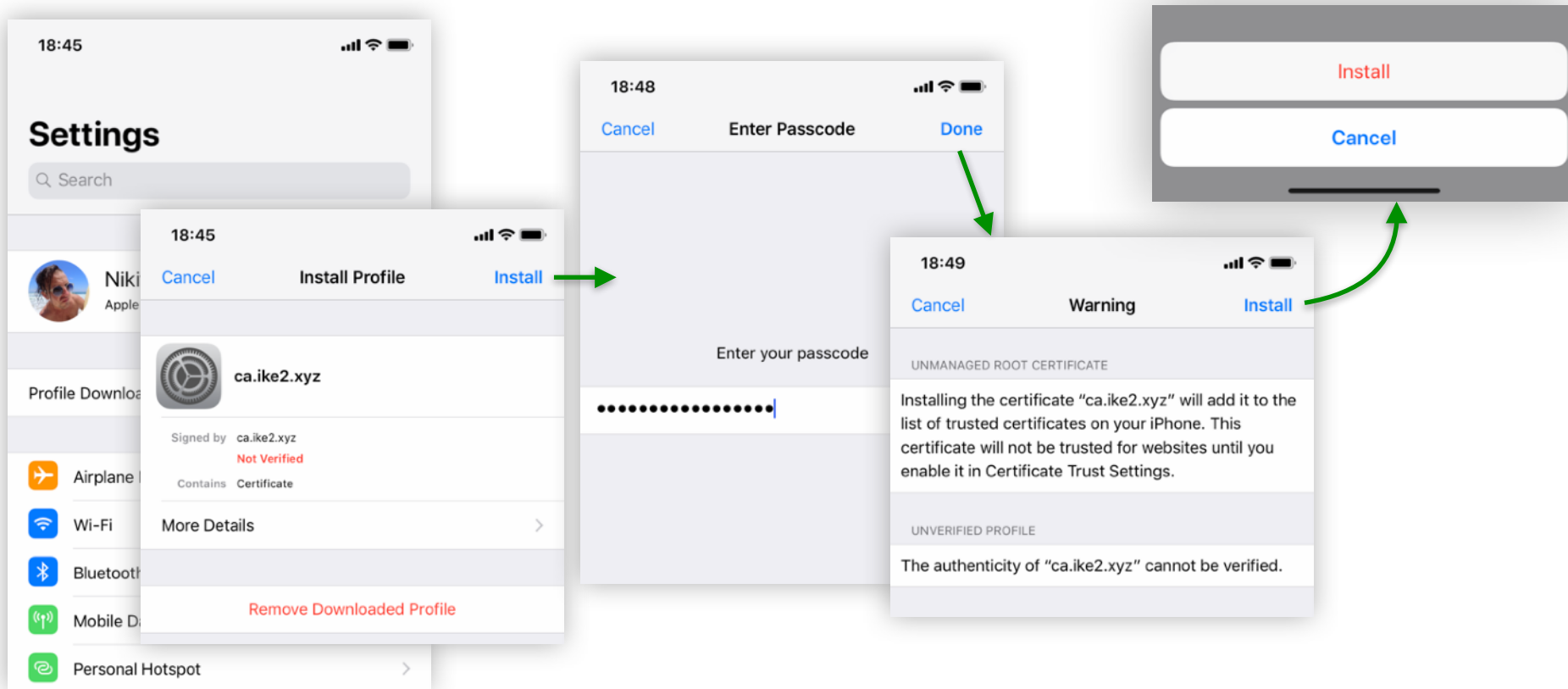
— — —



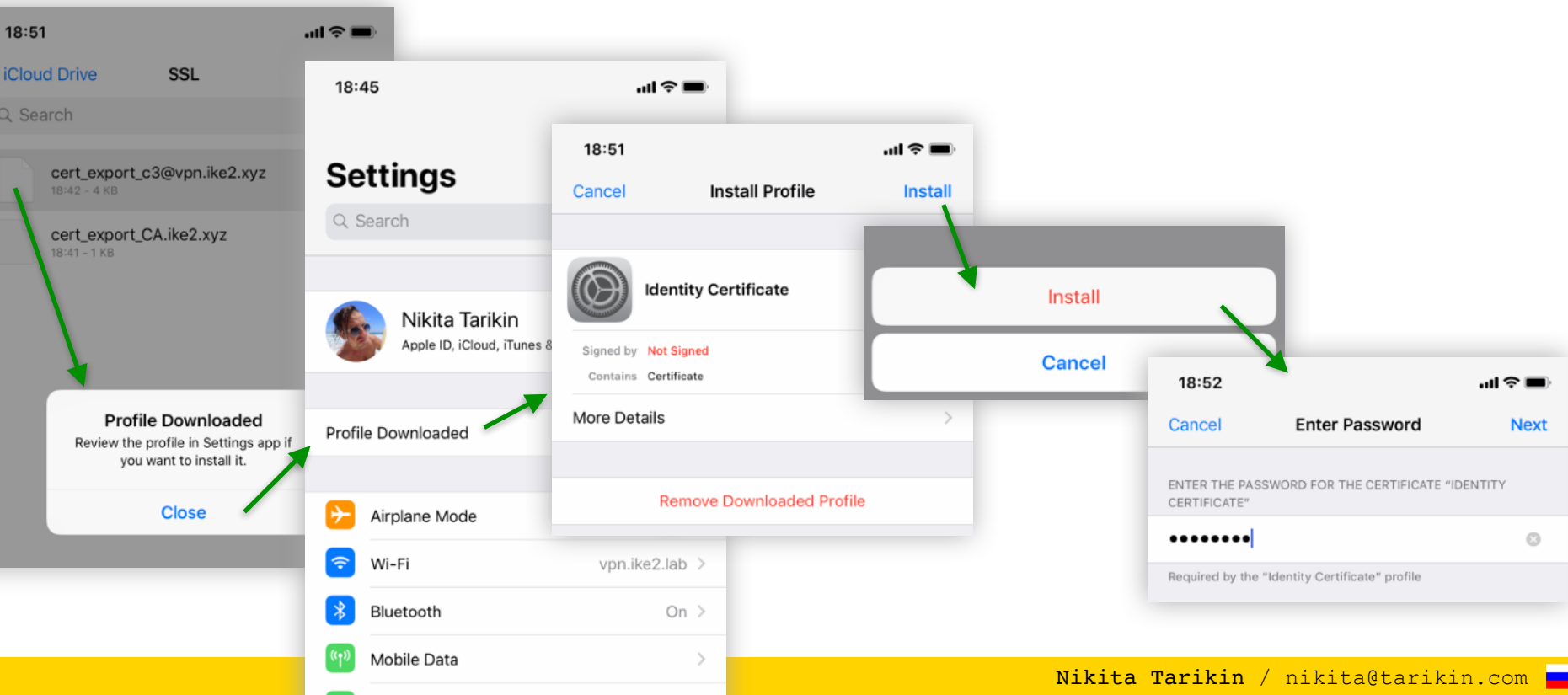
iOS: Импорт SSL сертификата авторитета CA



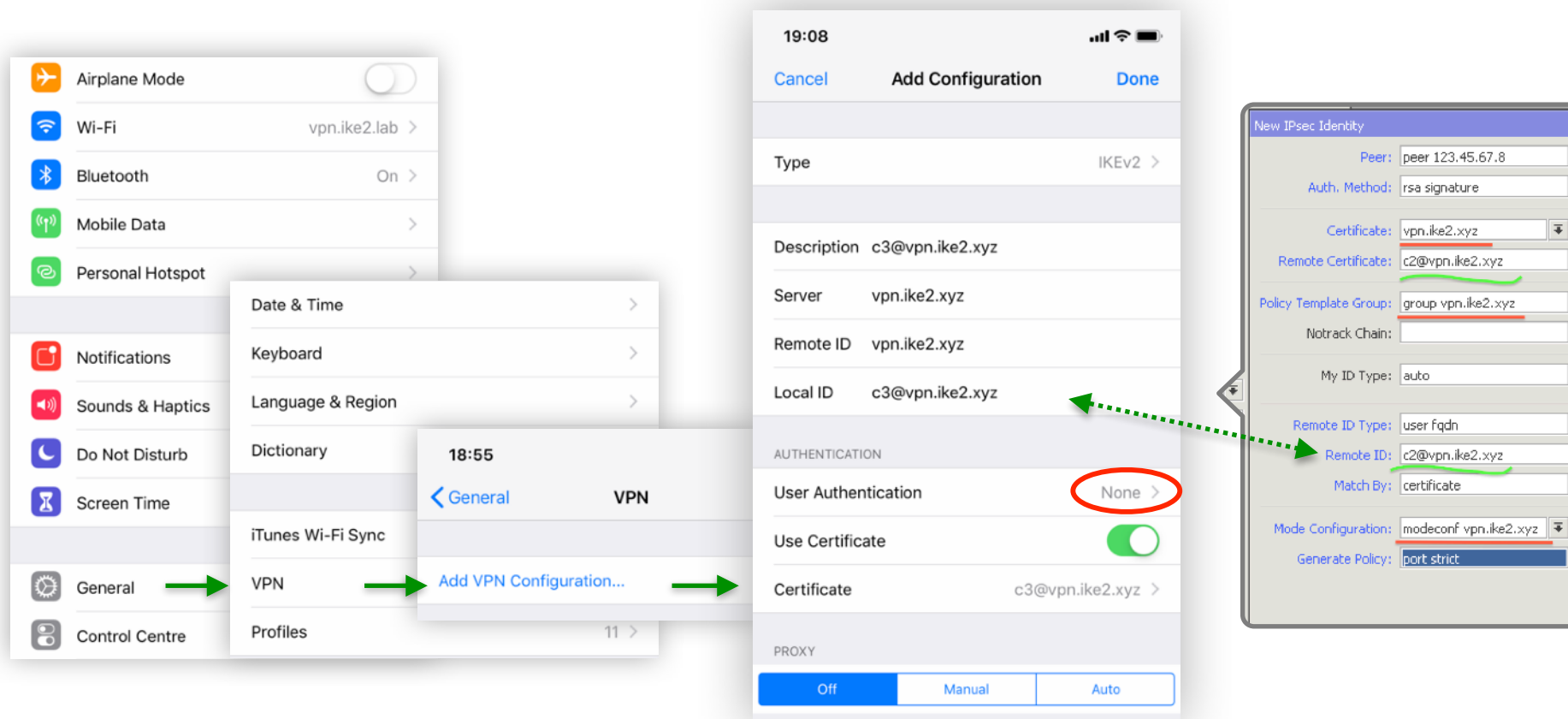
iOS: Импорт SSL сертификата авторитета CA



iOS: Импорт SSL сертификата клиента

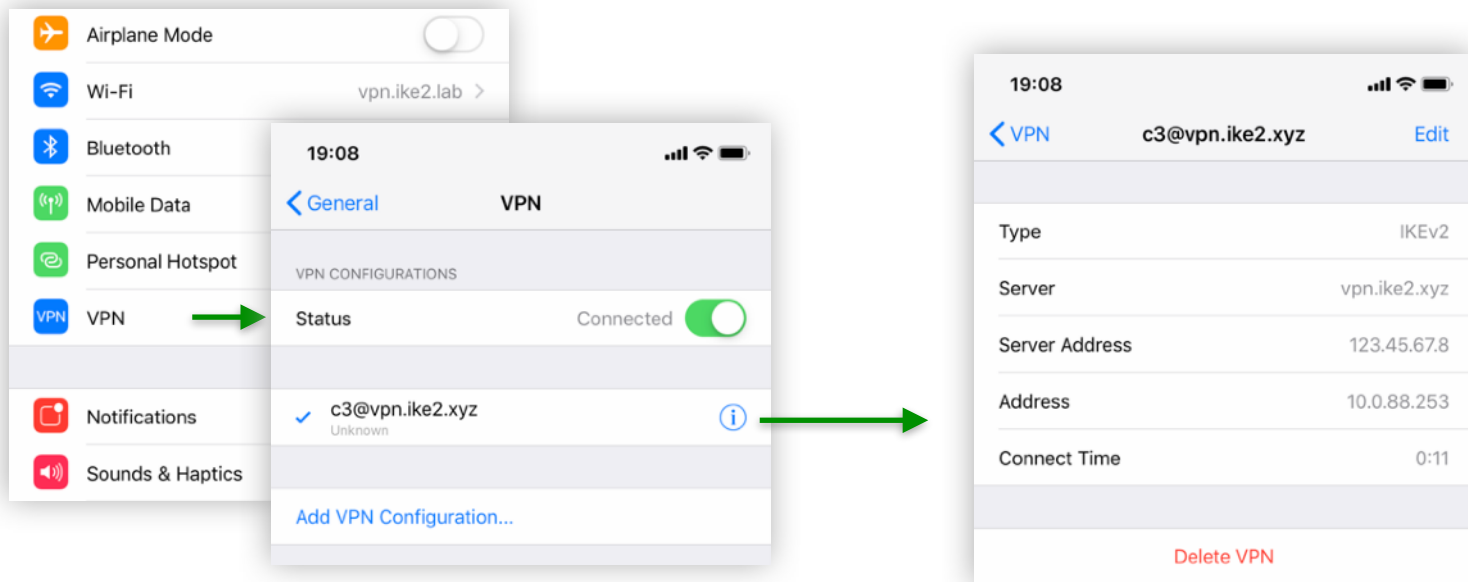


iOS: Настройка IKEv2 VPN соединения



iOS: Подключение IKEv2 VPN

— — —



Android

версия 9 <

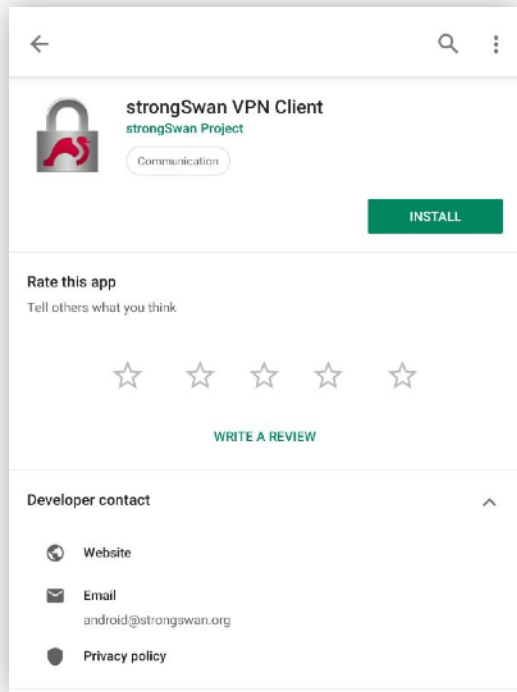
План действий

1. Установка приложения StrongSwan
2. Импорт SSL сертификатов
3. Настройка IKEv2 VPN подключения

— — —

Android: Установка StrongSwan

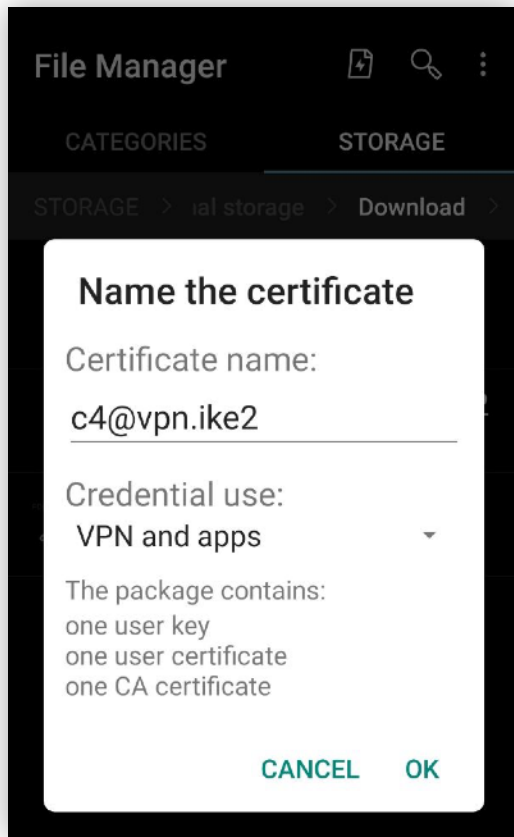
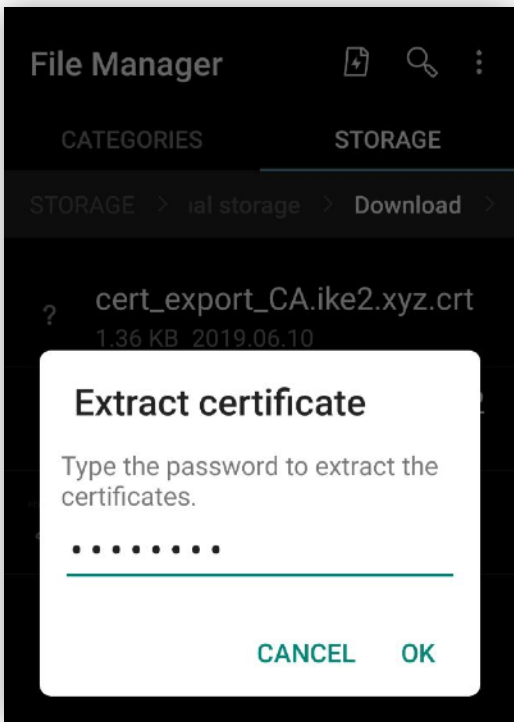
— — —



Найти и установить **StrongSwan**

через Google Play

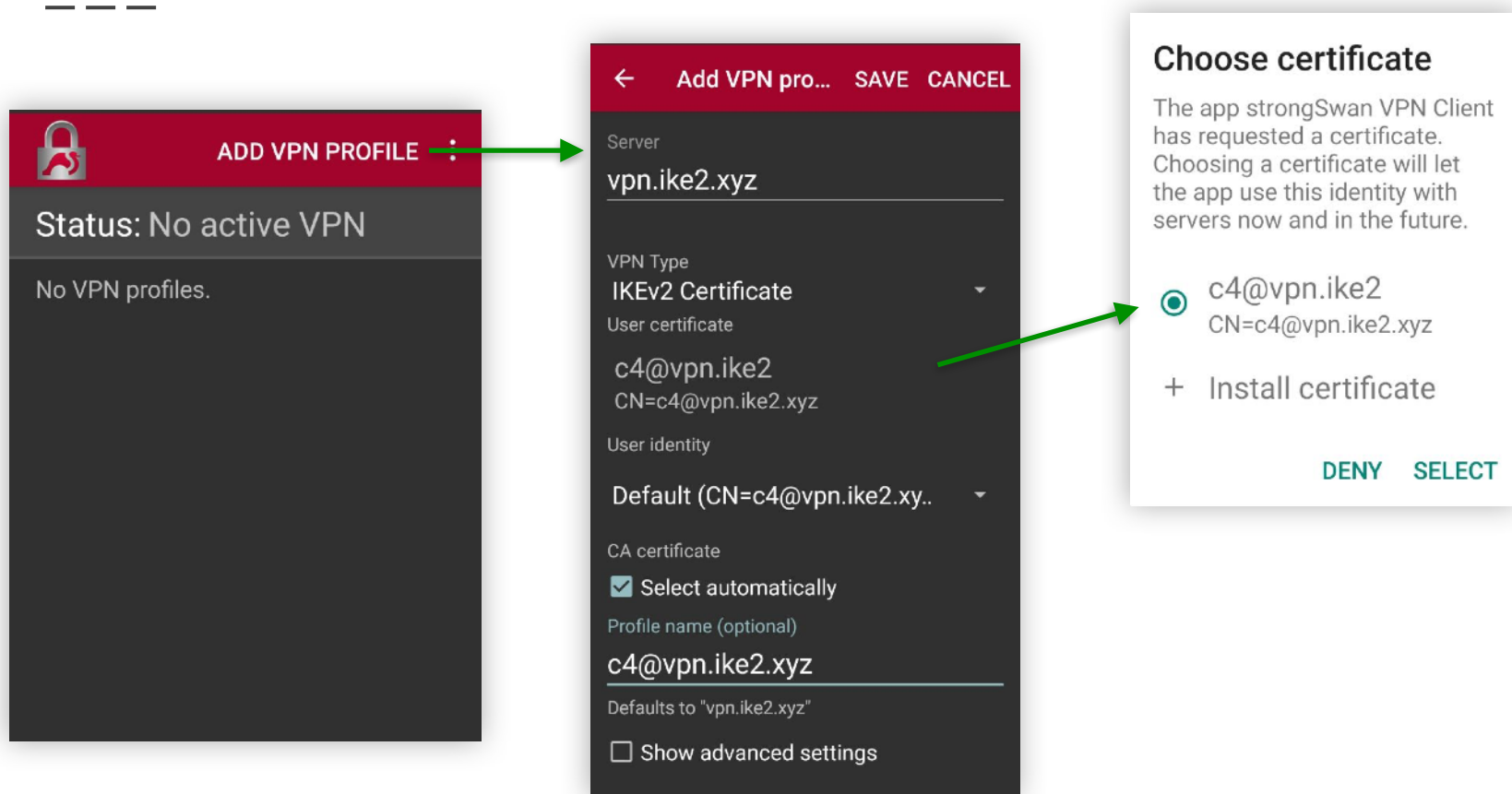
Android: Импорт SSL сертификатов



Download and install

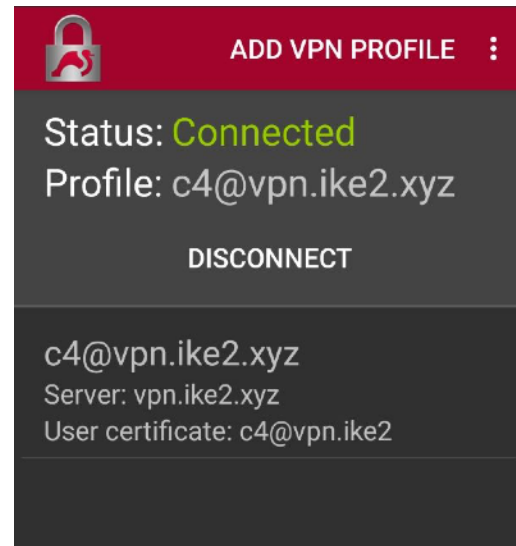
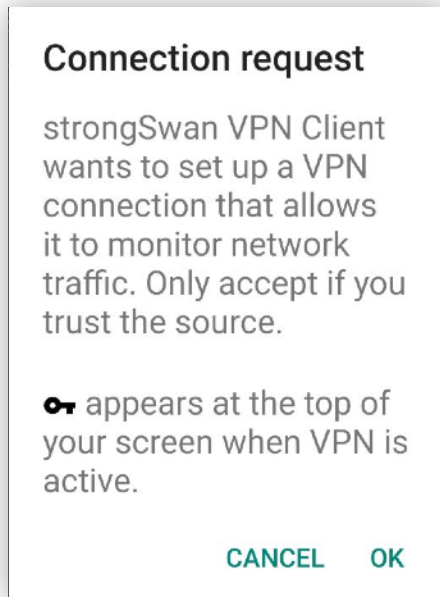
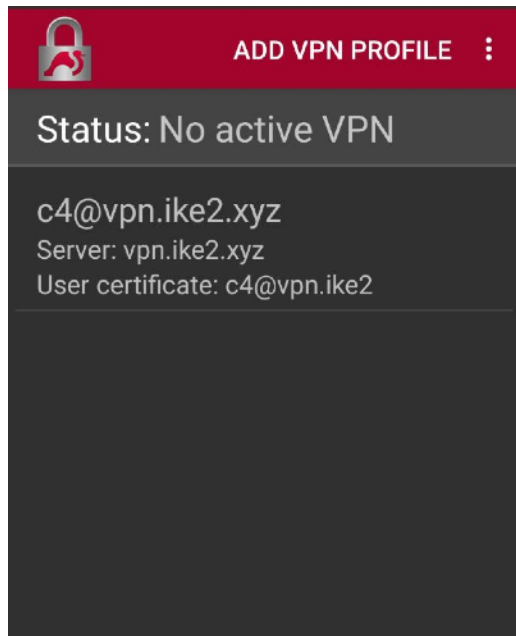
user certificate .p12

Android: Настройка IKEv2 VPN соединения



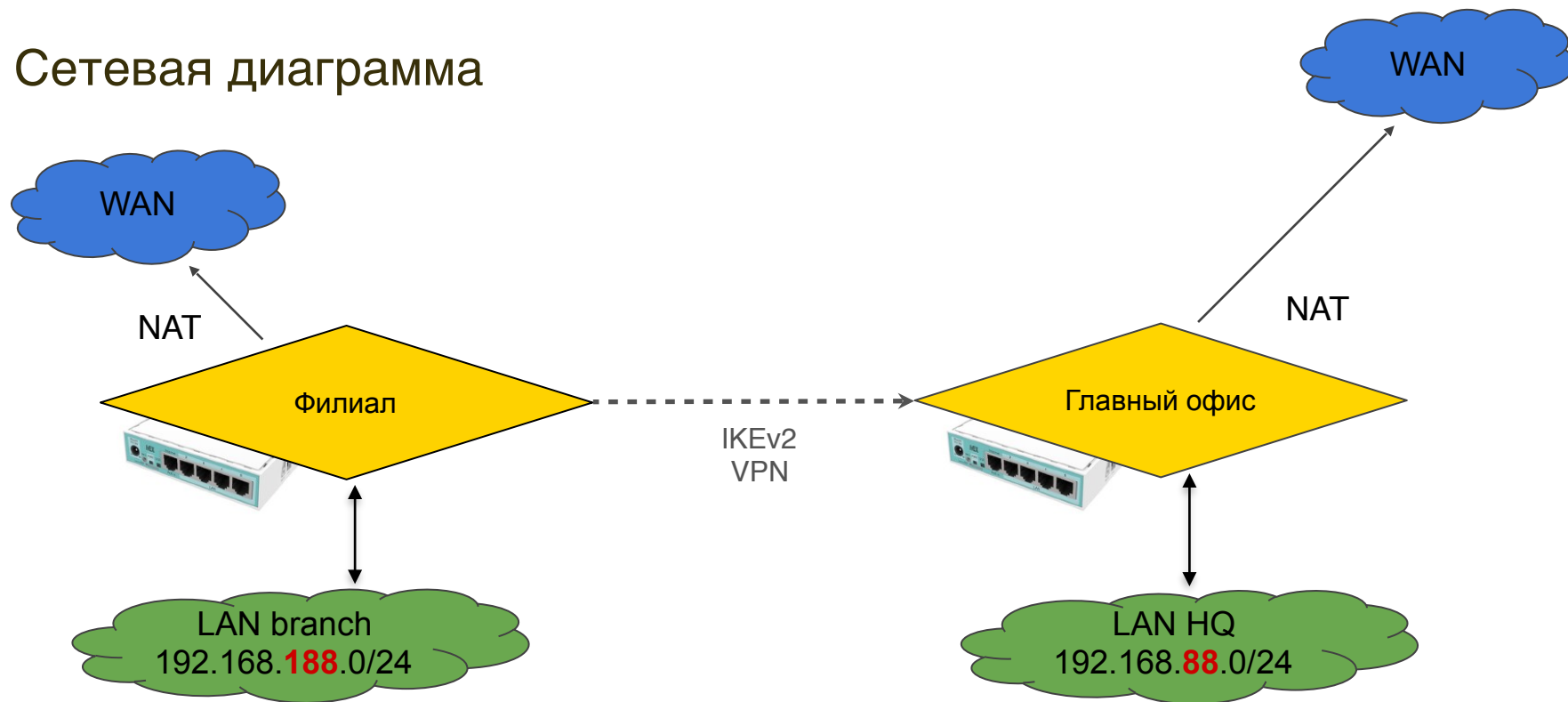
Android: Подключение IKEv2 VPN

— — —

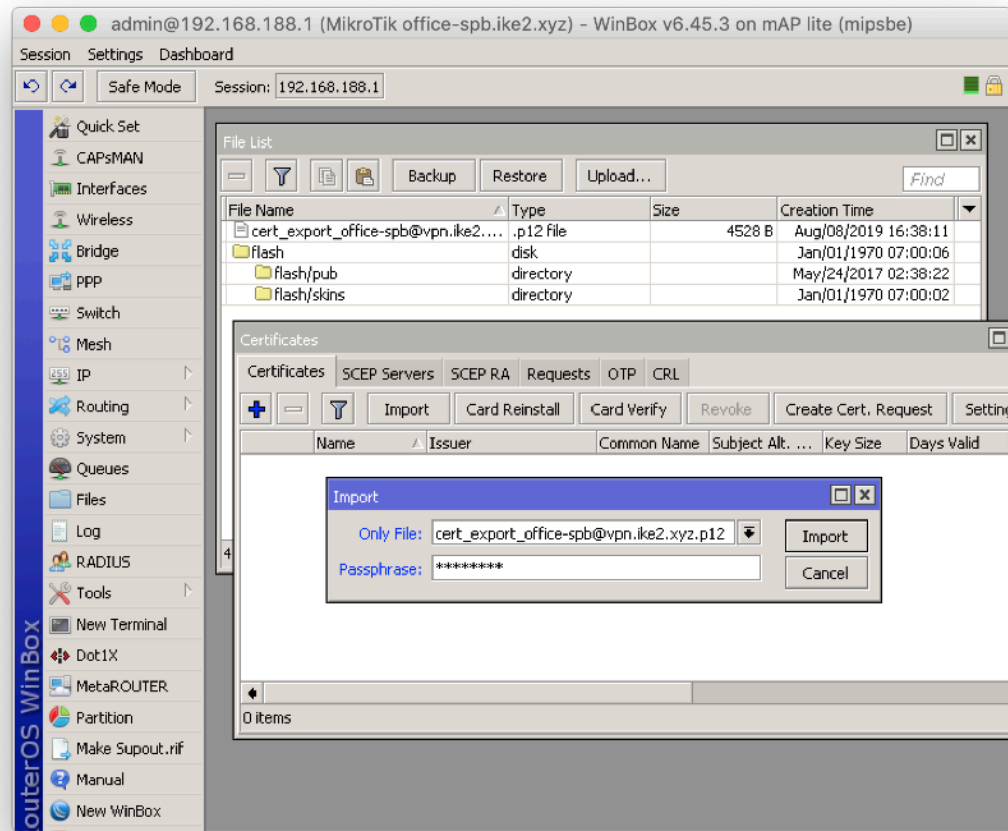


Подключение RouterOS

Сетевая диаграмма

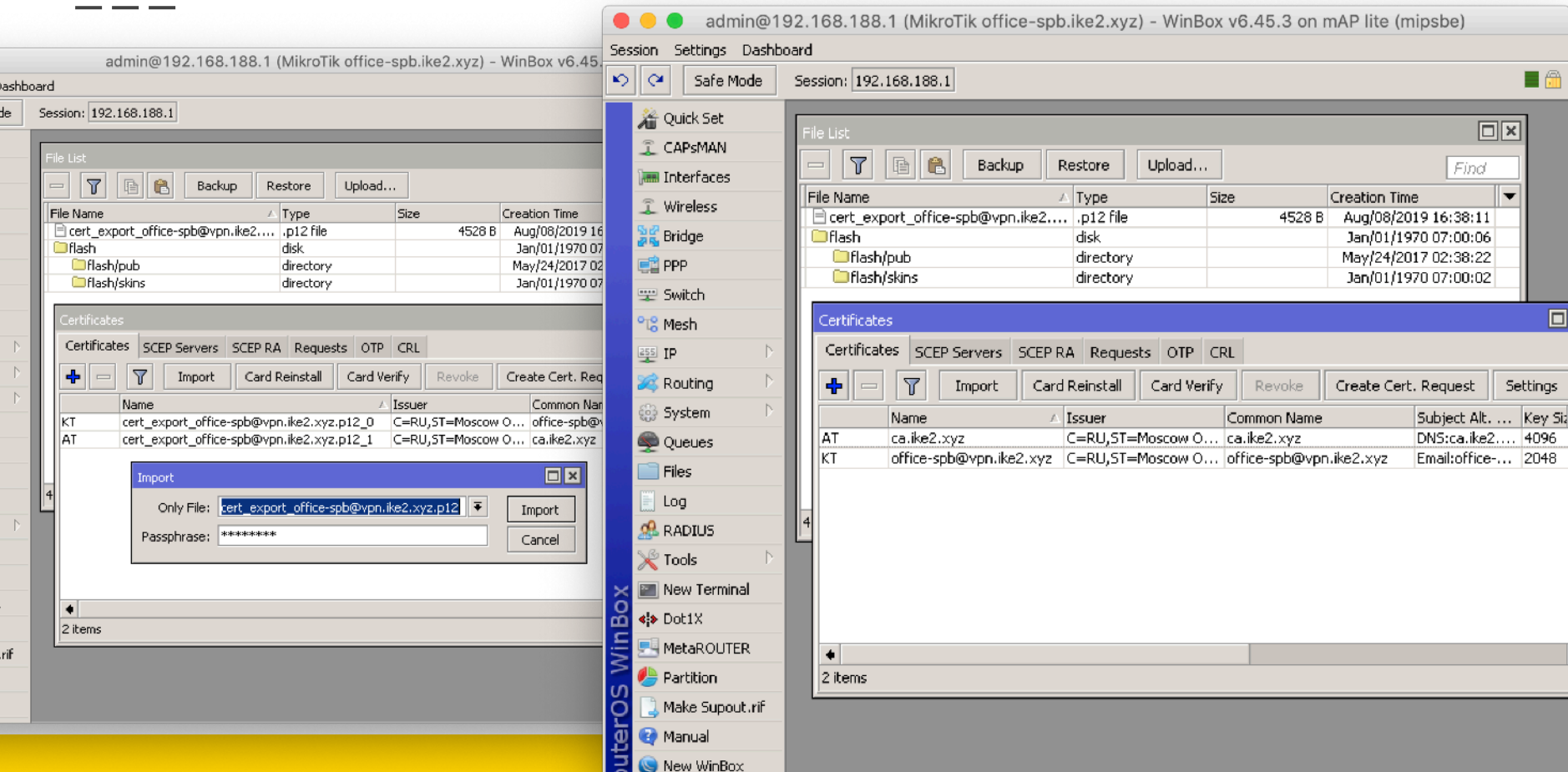


Загрузка и установка клиентского SSL сертификата

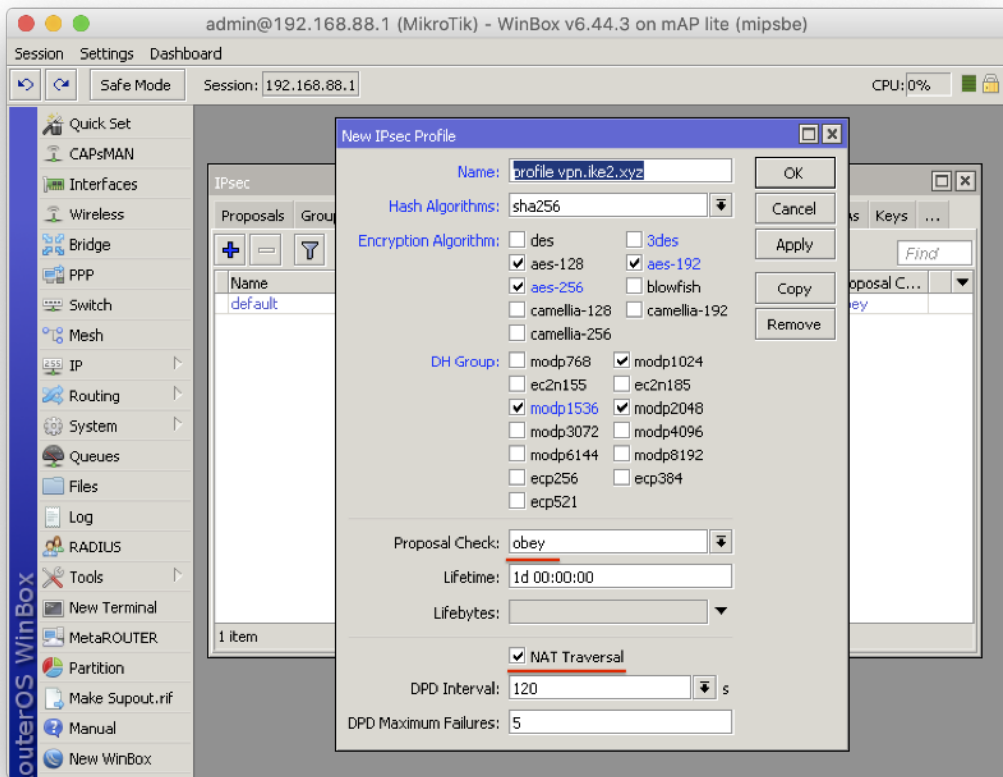


```
/certificate import file-  
name=cert_export_office-  
spb@vpn.ike2.xyz.p12
```

Переименовываем установленные SSL сертификаты



Настройка нового IPsec peer profile (фаза 1)

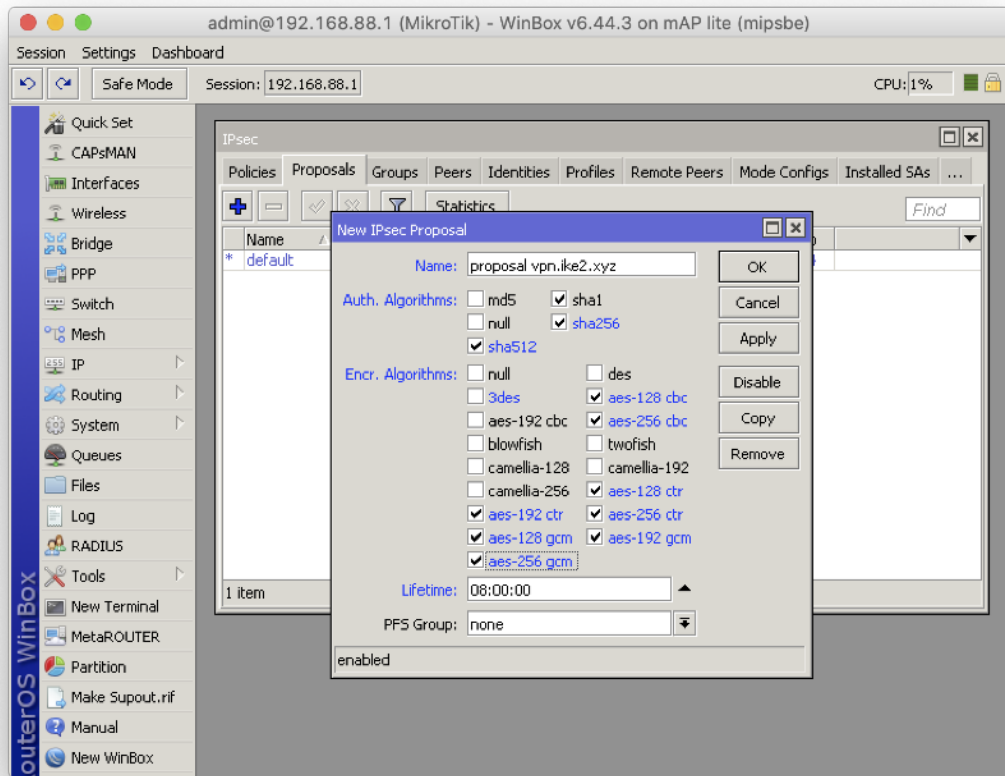


```
/ip ipsec profile add dh-  
group=modp2048,modp1536,modp10  
24 enc-  
algorithm=aes-256,aes-192,aes-  
128 hash-algorithm=sha256  
name="profile.vpn.ike2.xyz"  
nat-traversal=yes proposal-  
check=obey
```

— 200 —



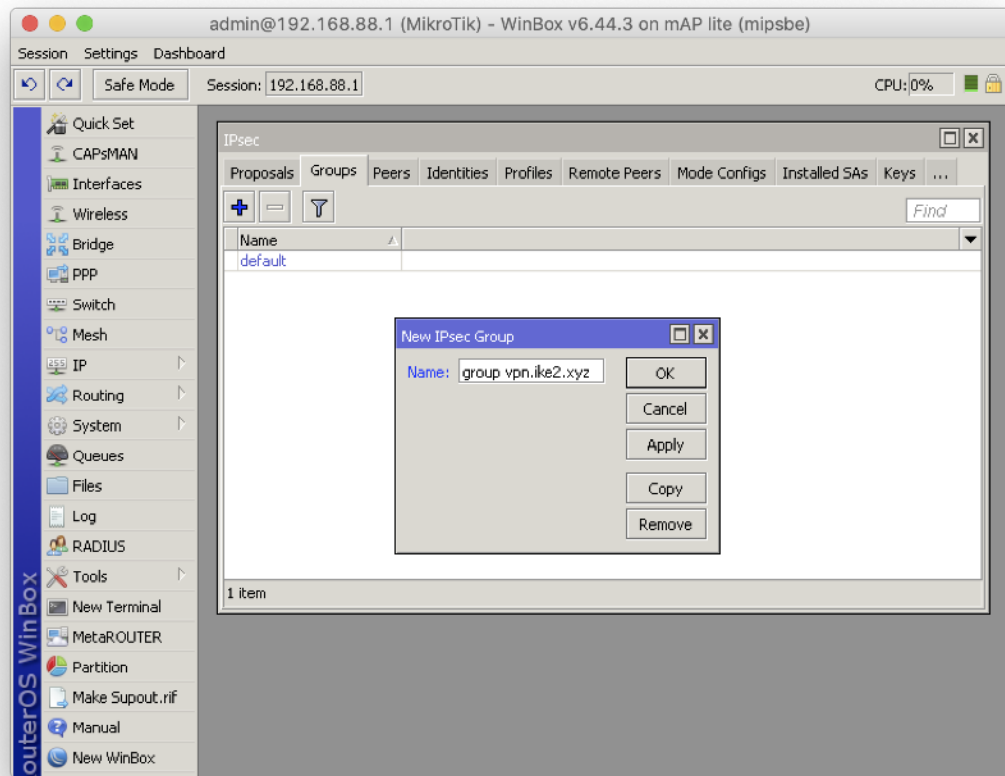
Настройка нового IPsec proposal (фаза 2)



```
/ip ipsec proposal add auth-  
algorithms=sha512,sha256,sha1  
enc-algorithms=aes-256-  
cbc,aes-256-ctr,aes-256-  
gcm,aes-192-ctr,aes-192-  
gcm,aes-128-cbc,aes-128-  
ctr,aes-128-gcm lifetime=8h  
name="proposal vpn.ike2.xyz"  
pfs-group=none
```

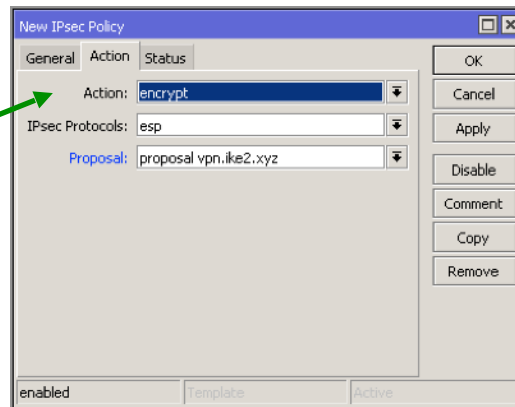
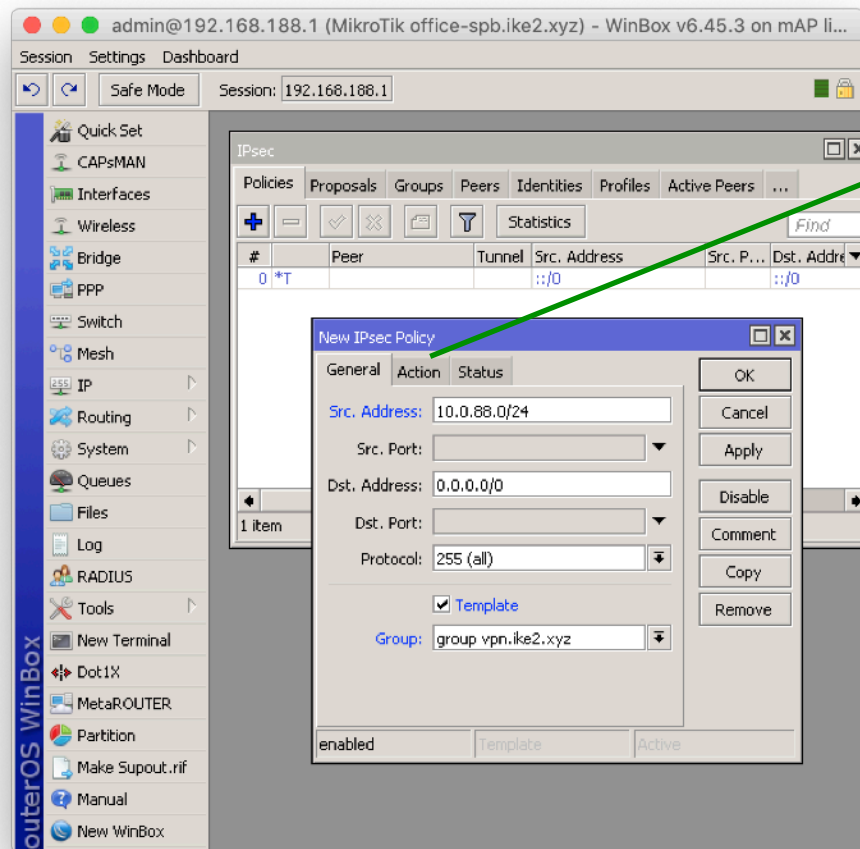
Добавление новой IPSec policy group

— — —



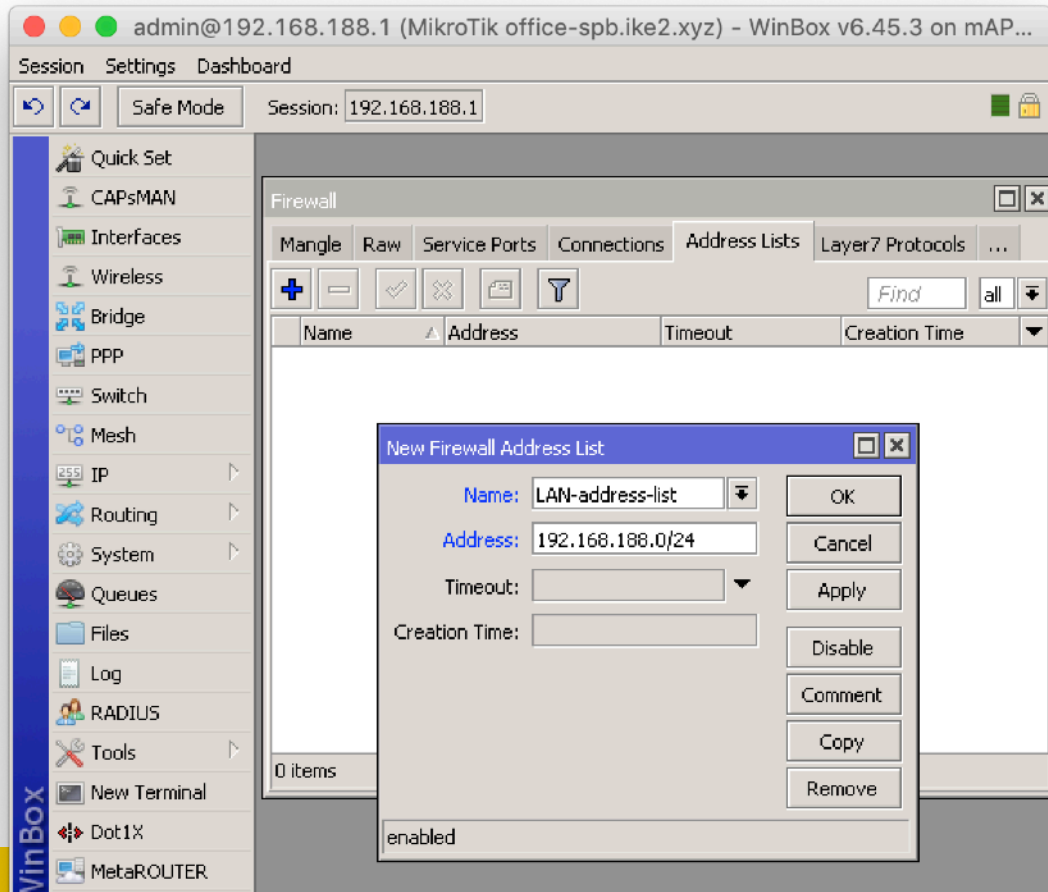
```
/ip ipsec policy group  
add name="group vpn.ike2.xyz"
```

Добавление нового шаблона IPsec policy



```
/ip ipsec policy
add comment="policy template vpn.ike2.xyz"
dst-address=0.0.0.0/0 group="group
vpn.ike2.xyz" proposal="proposal vpn.ike2.xyz"
src-address=10.0.88.0/24 template=yes
```

Добавление нового списка LAN сетей в firewall address list



```
/ip firewall address-list  
add address=192.168.188.0/24  
list=LAN-address-list
```


Добавление нового клиента IPsec modeconf (инициатор)

admin@192.168.188.1 (MikroTik office-spb.ike2.xyz) - WinBox v6.45.3 on mAP lite (mipsbe)

Settings Dashboard

Safe Mode Session: 192.168.188.1

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

Find all

Name	Address	Timeout	Creation Time
LAN-addr...	192.168.188.0/24		Aug/08/2019 17:...

IPsec

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

Find

Name	Resp...	Address Pool	Address	Address Prefi...	Split Include
request-only	no				

New IPsec Mode Config

Name: modeconf office-spb@vpn.ike2.xyz

☐ Responder

Connection Mark:

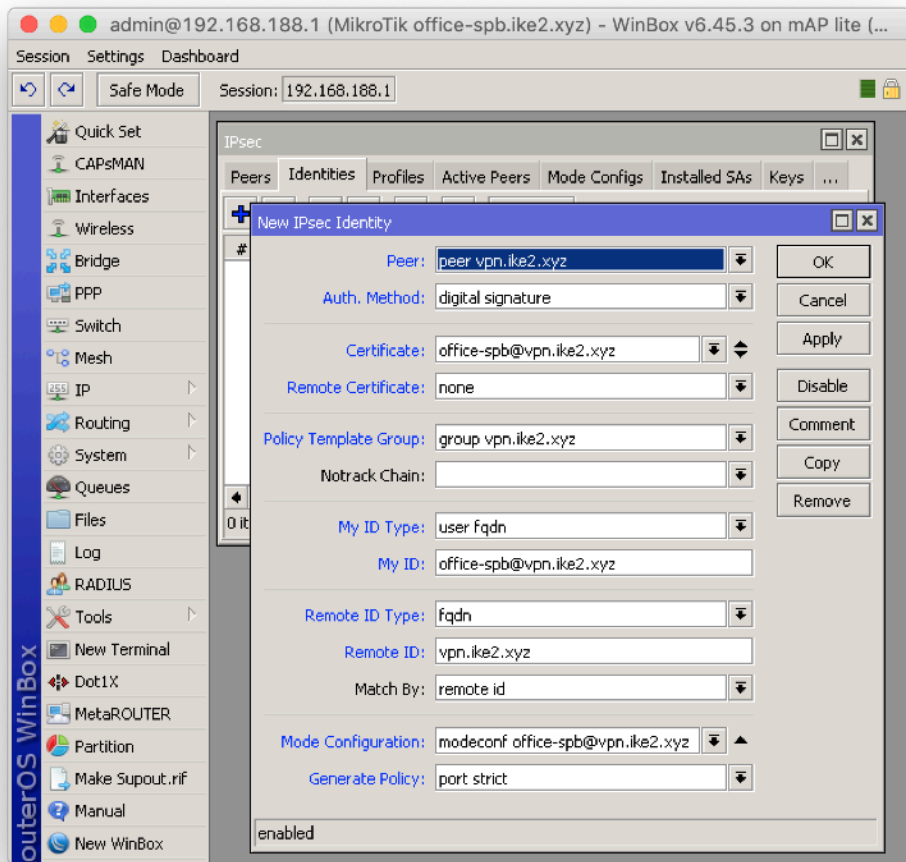
Src. Address List: LAN-address-list

OK Cancel Apply Copy Remove

```
/ip ipsec mode-config  
add name="modeconf office-  
spb@vpn.ike2.xyz" responder=no src-  
address-list=LAN-address-list
```

900LG22-(T2)-(YM-900LG22-(T2)

Добавление нового удостоверения IPsec identity



```
/ip ipsec identity
add auth-method=digital-signature
certificate=office-spb@vpn.ike2.xyz
generate-policy=port-strict mode-
config="modeconf office-spb@vpn.ike2.xyz"
my-id=user-fqdn:office-spb@vpn.ike2.xyz
peer="peer vpn.ike2.xyz" policy-template-
group="group vpn.ike2.xyz" remote-
id=fqdn:vpn.ike2.xyz
```

Имя пользователя: office-spb@vpn.ike2.xyz

Имя хоста: vpn.ike2.xyz

Nikita Tarikin / nikita@tarikin.com

Сверка удостоверений IPsec identity

Сервер

Клиент

IPsec Identity <peer 123.45.67.8>

Peer: peer 123.45.67.8

Auth. Method: digital signature

Certificate: vpn.ike2.xyz

Remote Certificate: office-spb@vpn.ike2.xyz

Policy Template Group: group vpn.ike2.xyz

Notrack Chain:

My ID Type: fqdn

My ID: vpn.ike2.xyz

Remote ID Type: user fqdn

Remote ID: office-spb@vpn.ike2.xyz

Match By: certificate

Mode Configuration: modeconf vpn.ike2.xyz

Generate Policy: port strict

enabled

IPsec Identity <peer vpn.ike2.xyz>

Peer: peer vpn.ike2.xyz

Auth. Method: digital signature

Certificate: office-spb@vpn.ike2.xyz

Remote Certificate: none

Policy Template Group: group vpn.ike2.xyz

Notrack Chain:

My ID Type: user fqdn

My ID: office-spb@vpn.ike2.xyz

Remote ID Type: fqdn

Remote ID: vpn.ike2.xyz

Match By: remote id

Mode Configuration: modeconf office-spb@vpn.ike2.xyz

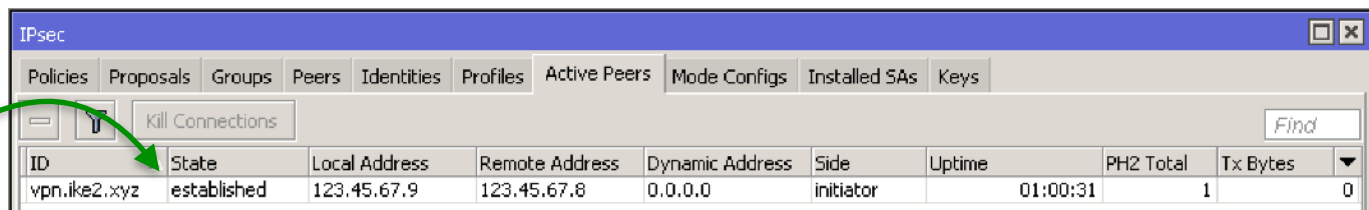
Generate Policy: port strict

enabled

Проверка связи IKEv2

Клиент

Active peers
state: **established**



IPsec									
Policies Proposals Groups Peers Identities Profiles Active Peers Mode Configs Installed SAs Keys									
Kill Connections Find									
ID	State	Local Address	Remote Address	Dynamic Address	Side	Uptime	PH2 Total	Tx Bytes	
vpn.ike2.xyz	established	123.45.67.9	123.45.67.8	0.0.0.0	initiator	01:00:31	1	0	

Генерирована
динамическая policy
PH state: **established**

IPsec

Policies

Proposals

Groups

Peers

Identities

Profiles

Active Peers

Mode Configs

Installed SAs

Keys

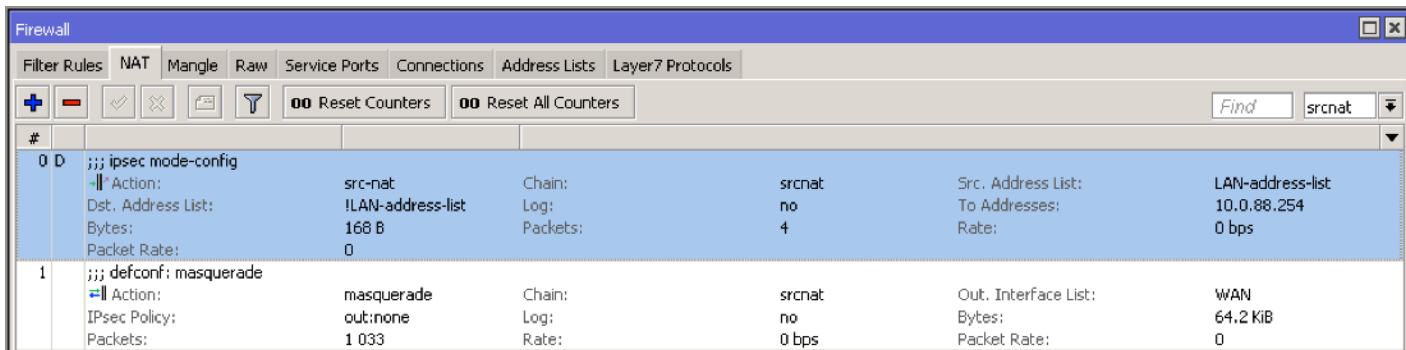
Peer: **authorized**
Address: **acquired**

Aug/08/2019 15:51:58	memory	ipsec, info	new ike2 SA (R): 123.45.67.8[4500]-123.45.67.9[4500] spi:39d4a4bf6c5f4e2b:099b4c2c836ffe5d
Aug/08/2019 15:51:58	memory	ipsec, info, account	peer authorized: 123.45.67.8[4500]-123.45.67.9[4500] spi:39d4a4bf6c5f4e2b:099b4c2c836ffe5d
Aug/08/2019 15:51:58	memory	ipsec, info	acquired 10.0.88.254 address for 123.45.67.9, office-spb@vpn.ike2.xyz

Проверка связи IKEv2

Клиент

Генерировано
динамическое
src-nat правило



The screenshot shows the Mikrotik WinBox Firewall Filter Rules configuration window. The 'Filter Rules' tab is active. Two rules are listed:

#	Chain	Outgoing	Filter Rule Name	Action	Chain	Log	Bytes	Packets	Rate
0	D	;;;	ipsec mode-config	src-nat	srcnat	no	168 B	4	0 bps
1		;;;	defconf: masquerade	masquerade	srcnat	no	1 033	0 bps	0

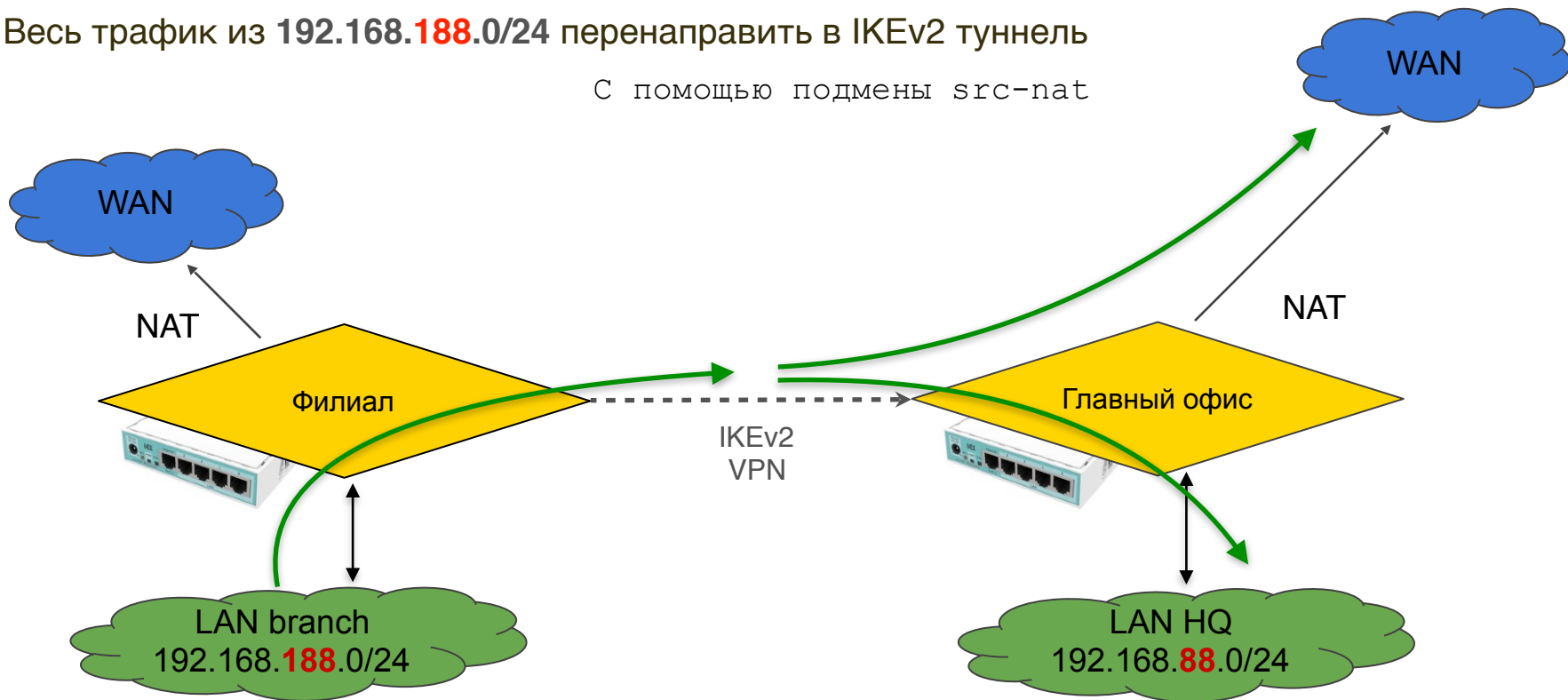
Rule 0 details: Action: src-nat, Dst. Address List: !LAN-address-list, Chain: srcnat, Log: no, Bytes: 168 B, Packets: 4, Rate: 0 bps. Rule 1 details: Action: masquerade, IPsec Policy: out:none, Chain: srcnat, Log: no, Bytes: 1 033, Packets: 0 bps, Rate: 0.

FROM: LAN-address-list 192.168.188.0/24
TO: NOT-LAN-address-list NOT-192.168.188.0/24

Action: SRC-NAT
TO-address: 10.0.88.254

Весь трафик из 192.168.188.0/24 перенаправить в IKEv2 туннель

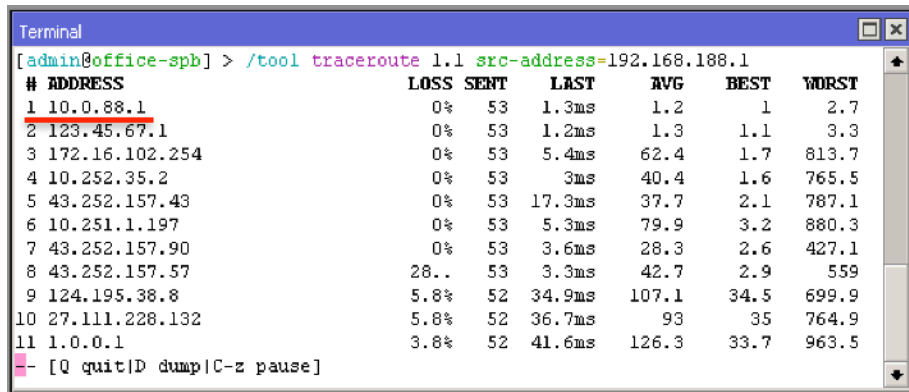
С помощью подмены src-nat



Проверка связи IKEv2: В Интернет

FROM: LAN-address-list

```
/tool traceroute 1.1 src-address=192.168.188.1
```



Terminal

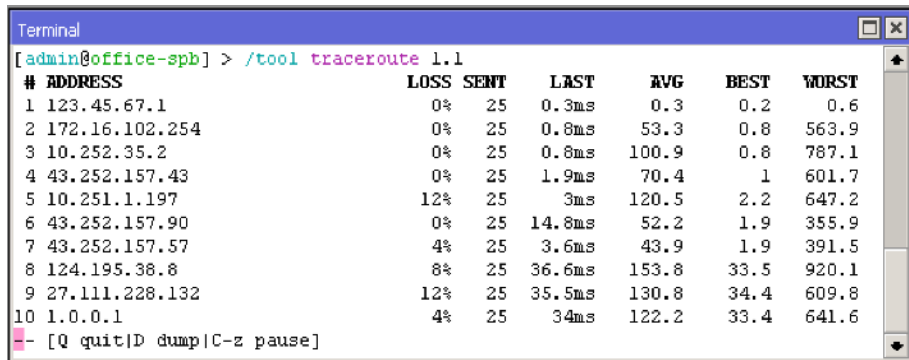
```
[admin@office-spb] > /tool traceroute 1.1 src-address=192.168.188.1
```

#	ADDRESS	LOSS	SENT	LAST	AVG	BEST	WORST
1	10.0.88.1	0%	53	1.3ms	1.2	1	2.7
2	123.45.67.1	0%	53	1.2ms	1.3	1.1	3.3
3	172.16.102.254	0%	53	5.4ms	62.4	1.7	813.7
4	10.252.35.2	0%	53	3ms	40.4	1.6	765.5
5	43.252.157.43	0%	53	17.3ms	37.7	2.1	787.1
6	10.251.1.197	0%	53	5.3ms	79.9	3.2	880.3
7	43.252.157.90	0%	53	3.6ms	28.3	2.6	427.1
8	43.252.157.57	28..	53	3.3ms	42.7	2.9	559
9	124.195.38.8	5.8%	52	34.9ms	107.1	34.5	699.9
10	27.111.228.132	5.8%	52	36.7ms	93	35	764.9
11	1.0.0.1	3.8%	52	41.6ms	126.3	33.7	963.5

[Q quit|D dump|C-z pause]

FROM: NOT-LAN-address-list

```
/tool traceroute 1.1
```



Terminal

```
[admin@office-spb] > /tool traceroute 1.1
```

#	ADDRESS	LOSS	SENT	LAST	AVG	BEST	WORST
1	123.45.67.1	0%	25	0.3ms	0.3	0.2	0.6
2	172.16.102.254	0%	25	0.8ms	53.3	0.8	563.9
3	10.252.35.2	0%	25	0.8ms	100.9	0.8	787.1
4	43.252.157.43	0%	25	1.9ms	70.4	1	601.7
5	10.251.1.197	12%	25	3ms	120.5	2.2	647.2
6	43.252.157.90	0%	25	14.8ms	52.2	1.9	355.9
7	43.252.157.57	4%	25	3.6ms	43.9	1.9	391.5
8	124.195.38.8	8%	25	36.6ms	153.8	33.5	920.1
9	27.111.228.132	12%	25	35.5ms	130.8	34.4	609.8
10	1.0.0.1	4%	25	34ms	122.2	33.4	641.6

[Q quit|D dump|C-z pause]

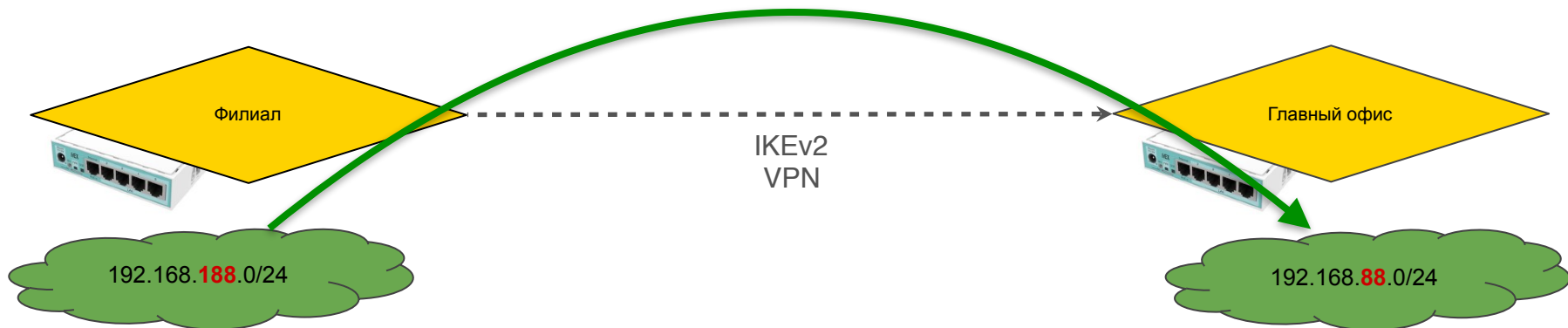
Проверка связи IKEv2: в главный офис

FROM: 192.168.188.0/24

TO: 192.168.88.0/24

```
ping 192.168.88.1 src-  
address=192.168.188.1
```

```
Terminal  
[admin@office-spb] > ping 192.168.88.1 src-address=192.168.188.1  
SEQ HOST                                SIZE TTL TIME STATUS  
0 192.168.88.1                          56 64 1ms  
1 192.168.88.1                          56 64 1ms  
2 192.168.88.1                          56 64 1ms  
3 192.168.88.1                          56 64 1ms  
4 192.168.88.1                          56 64 1ms  
5 192.168.88.1                          56 64 1ms  
6 192.168.88.1                          56 64 1ms  
7 192.168.88.1                          56 64 1ms  
8 192.168.88.1                          56 64 1ms  
9 192.168.88.1                          56 64 1ms  
10 192.168.88.1                         56 64 1ms  
11 192.168.88.1                         56 64 1ms  
12 192.168.88.1                         56 64 1ms  
13 192.168.88.1                         56 64 1ms  
sent=14 received=14 packet-loss=0% min-rtt=1ms avg-rtt=1ms max-rtt=1ms  
[admin@office-spb] >
```



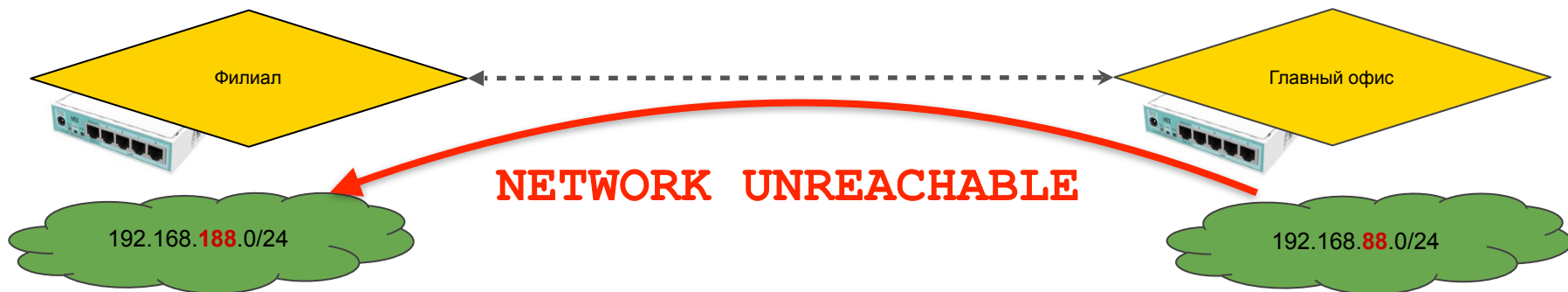
Проверка связи IKEv2: из главного офиса в филиалы

```
Terminal
[admin@MikroTik] > ping 192.168.188.1 src-address=192.168.88.1
SEQ HOST                SIZE TTL TIME  STATUS
0 123.45.67.1           84  64 0ms   net unreachable
1 123.45.67.1           84  64 0ms   net unreachable
2 123.45.67.1           84  64 0ms   net unreachable
3 123.45.67.1           84  64 0ms   net unreachable
4 123.45.67.1           84  64 0ms   net unreachable
5 123.45.67.1           84  64 0ms   net unreachable
6 123.45.67.1           84  64 0ms   net unreachable
7 123.45.67.1           84  64 0ms   net unreachable
```

FROM: 192.168.88.0/24

TO: 192.168.188.0/24

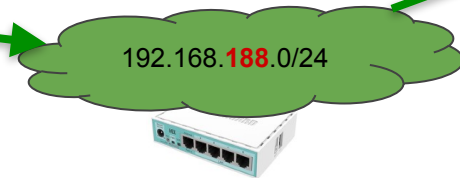
```
ping 192.168.188.1 src-
address=192.168.88.1
```

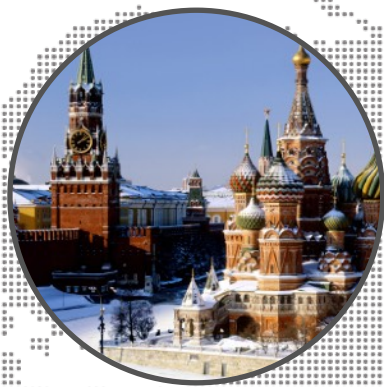




RouterOS IKEv2 site-to-site

Двусторонняя связь между офисами





MUM Indonesia

October 24–25, 2019

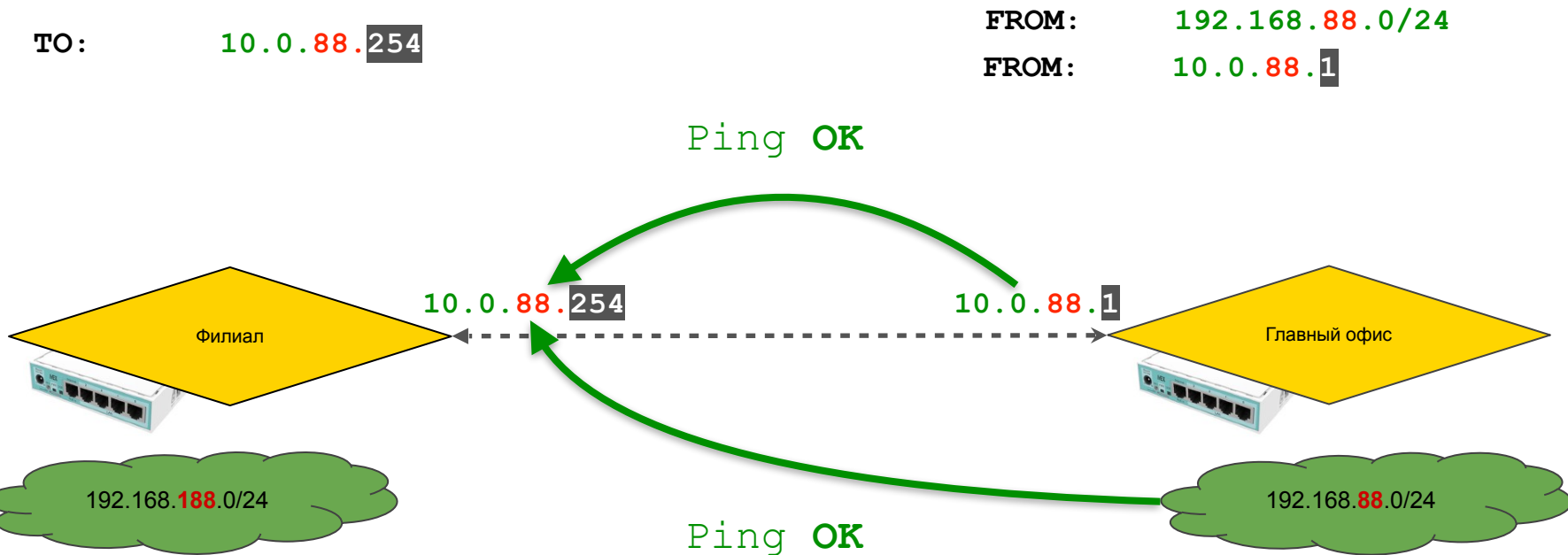
KUTA, BALI, Indonesia



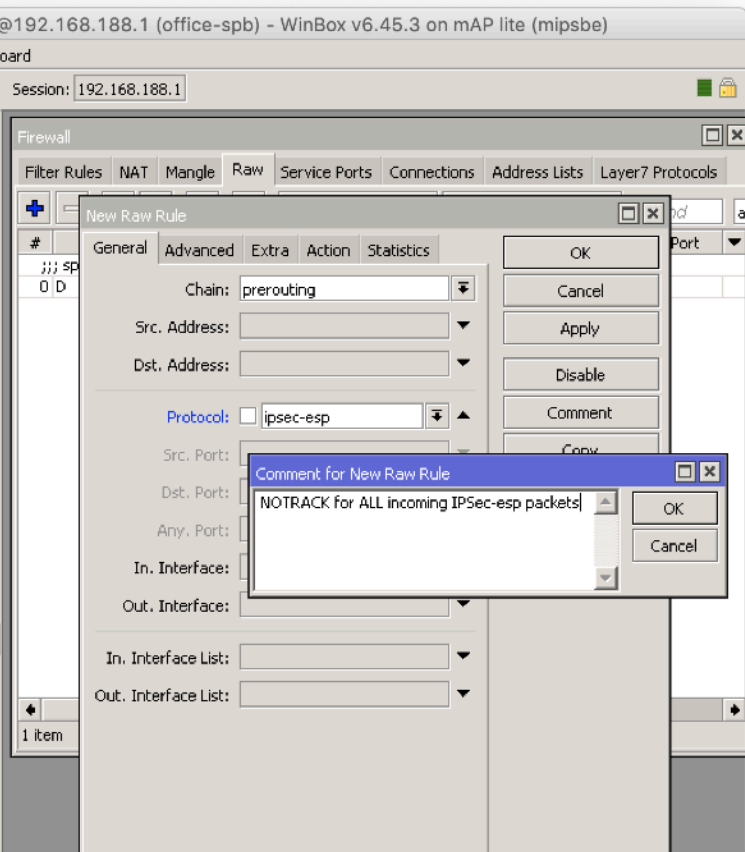
MikroTik IPSec IKEv2 VPN site-to-site:
easy step-by-step guide by Nikita Tarikin
(MikroTik PRO, Russia)



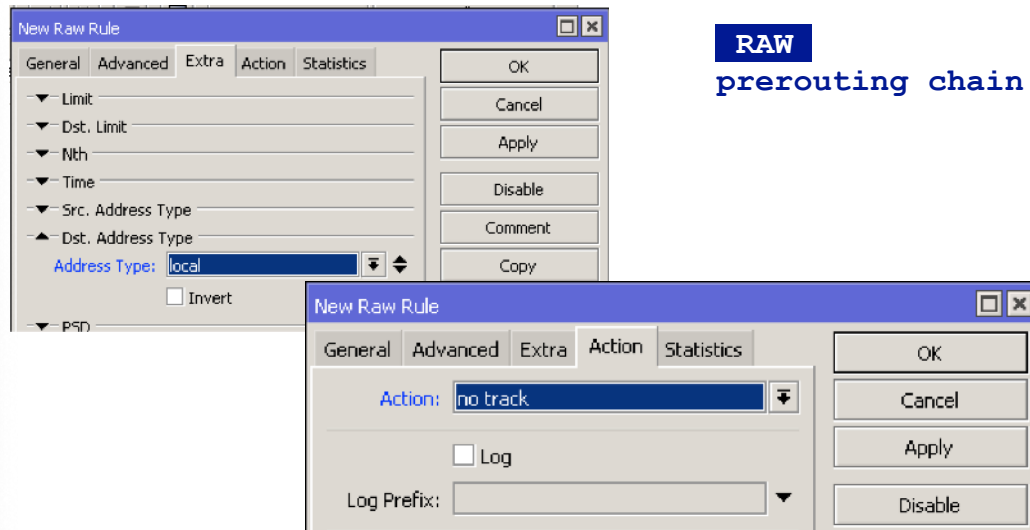
Проверка связи IKEv2: site-to-site



Пропускаем входящие IPSec-esp пакеты на клиенте *(на всякий случай)*



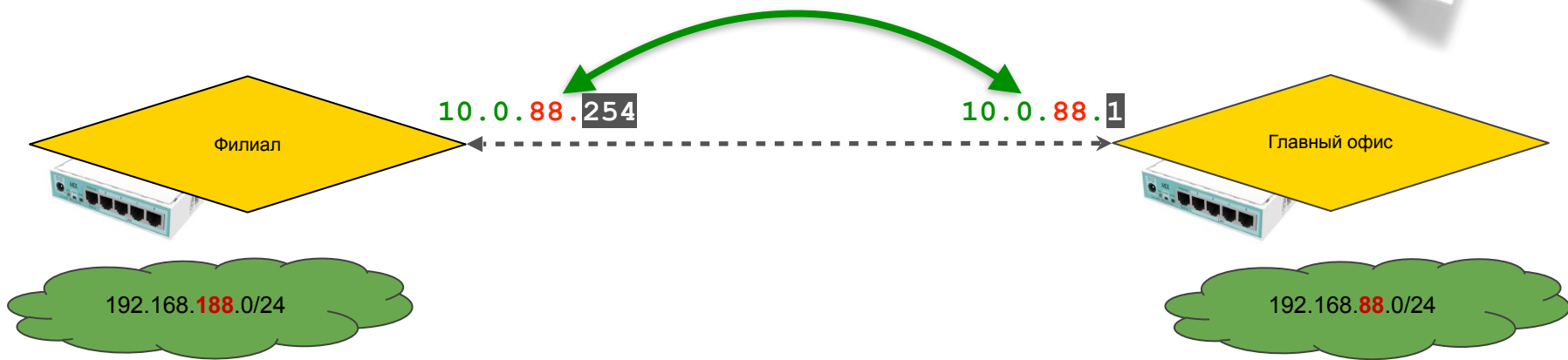
RAW
prerouting chain



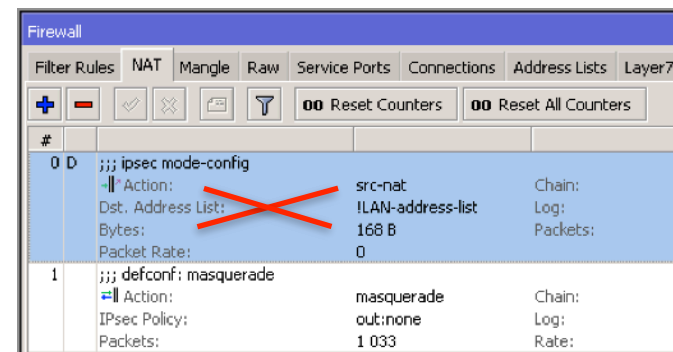
```
/ip firewall raw
add action=notrack chain=prerouting protocol=ipsec-esp
comment="NOTRACK for ALL incoming IPSec-esp packets"
dst-address-type=local
```

Маршрутизируемый трафик через IKEv2: добавление интерфейса

EoIP
IPsec
GRE



RouterOS WinBox



```
/ip ipsec mode-config
add name="modeconf office-
spb@vpn.ike2.xyz" responder=no
```

Демо лаба.

Демо лаба

Доступна по подписке
бесплатная демо
лаборатория в облаке

1. Заполнить гугло-форму
2. Получить по почте **индивидуальный сертификат**
3. Подключиться к VPN серверу
4. Подключиться к лабе через Winbox или SSH

— — —

Демо лаба

1. Заполнить форму
2. Получить сертификат
3. Подключить VPN
4. Войти через Winbox

Заполнить эту гугло-форму

<https://forms.gle/NxYVAcpgaQfvCSXc6>



Демо лаба

1. Заполнить форму
2. **Получить
сертификат**
3. Подключить VPN
4. Войти через Winbox

Дождаться своего сертификата

Дед Мороз рассылает сертификаты вручную, сорян :)

— — —

Демо лаба

1. Заполнить форму
2. Получить сертификат
3. **Подключить VPN**
4. Войти через Winbox

Подключиться к IKE2 VPN серверу

Адрес сервера: `vpn.ike2.xyz`

< полученный сертификат вместо логинов и паролей >

— — —

Демо лаба

1. Заполнить форму
2. Получить сертификат
3. Подключить VPN
4. **Войти через Winbox**

Войти на лабораторный роутер
через Winbox

Address

10.0.88.1

Login lab

Password lab

— — —

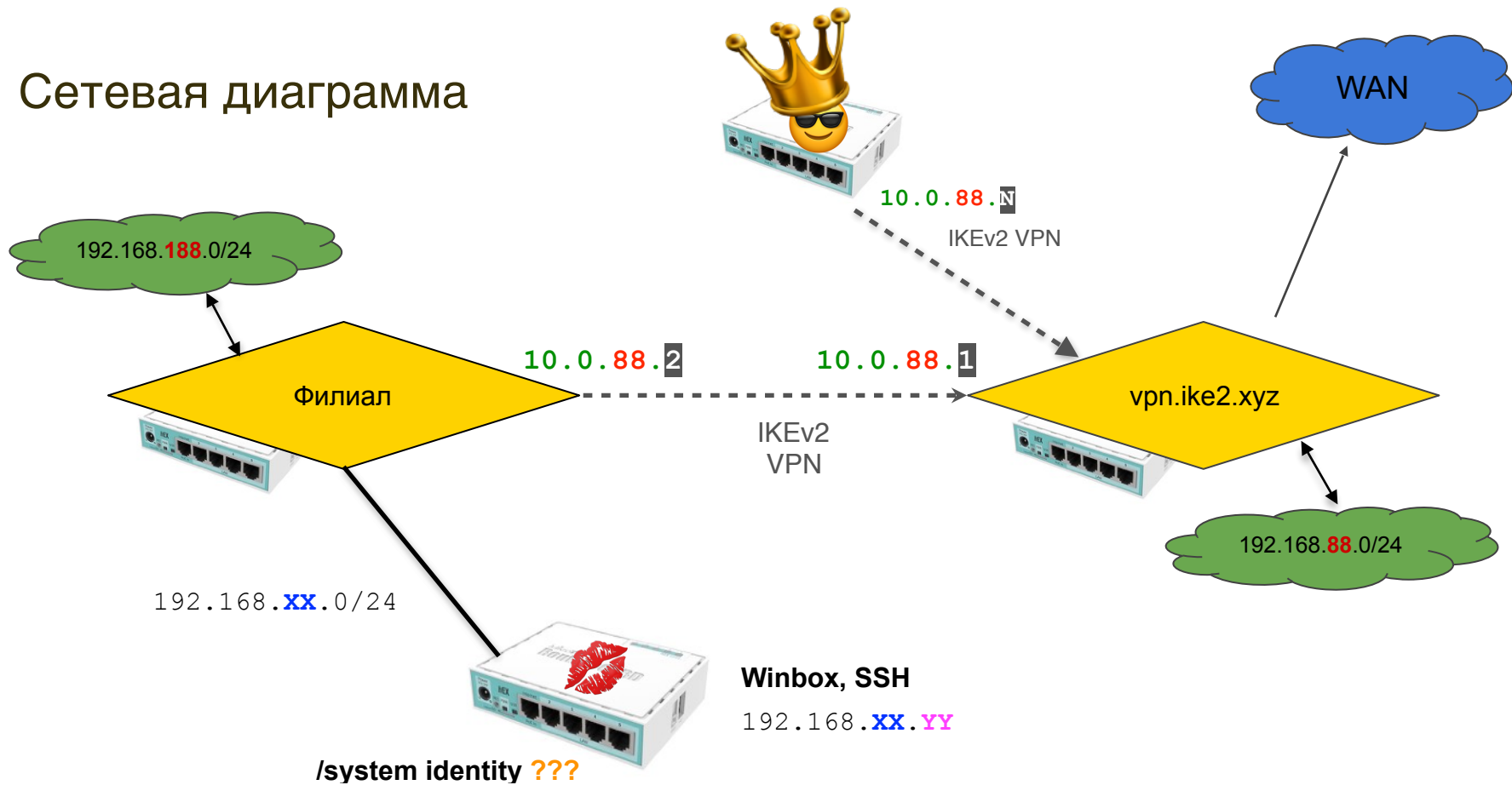
Внимание, конкурс!

“ Hack the princess ”



Открыта до 31 декабря 2019

Сетевая диаграмма

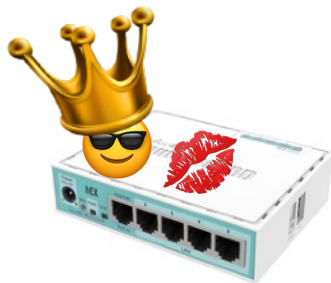




Чтобы пройти этот квест нужно:

- 1) подключиться к главному офису и найти проход на филиал
- 2) подключиться к филиалу и разобраться каким образом организована связь между зелеными сетями
- 3) обратить **особое внимание** на шаблоны политик + каким образом формируются динамические политики на клиенте и на сервере
- 4) построить новую политику между своим роутером и целевой сетью **по аналогии с политикой между зелеными сетями**
- 5) зайти на целевой роутер и вытащить system identity

hacktheprincess@protonmail.com

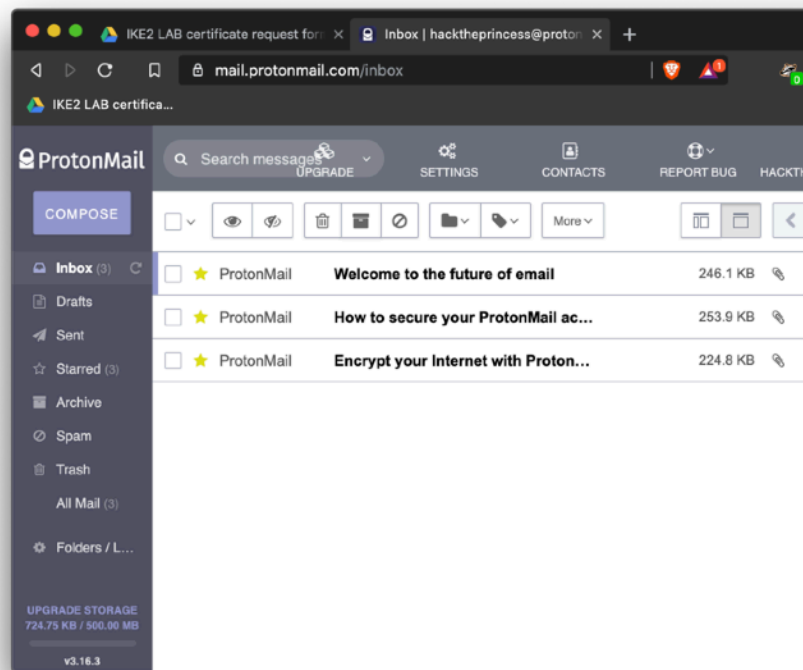


192.168.**XX**.0/24

192.168.**XX**.**YY**

/system identity ???

Результаты на почту



Демо лаба

1. Заполнить форму
2. Получить сертификат
3. Подключить VPN
4. Войти через Winbox

Заполнить эту гугло-форму

<https://forms.gle/NxYVAcpgaQfvCSXc6>



Давайте дружить

Пишите на почту:

nikita@tarikin.com

Найти меня в Facebook:



Nikita Tarikin

Подписаться:



@tarikin



@tropicalengineer

А лучше сразу сюда:



Telegram t.me/tarikin



Messenger Nikita Tarikin

— — —

Nikita Tarikin

`nikita@tarikin.com`

