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

MUM Russia

September 06–07, 2019

Moscow

MikroTik

Nikita Tarikin / nikita@tarikin.com

# 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

# Устройство сети для блондинок 👸💕


Мой телефон

Magic

Интернет

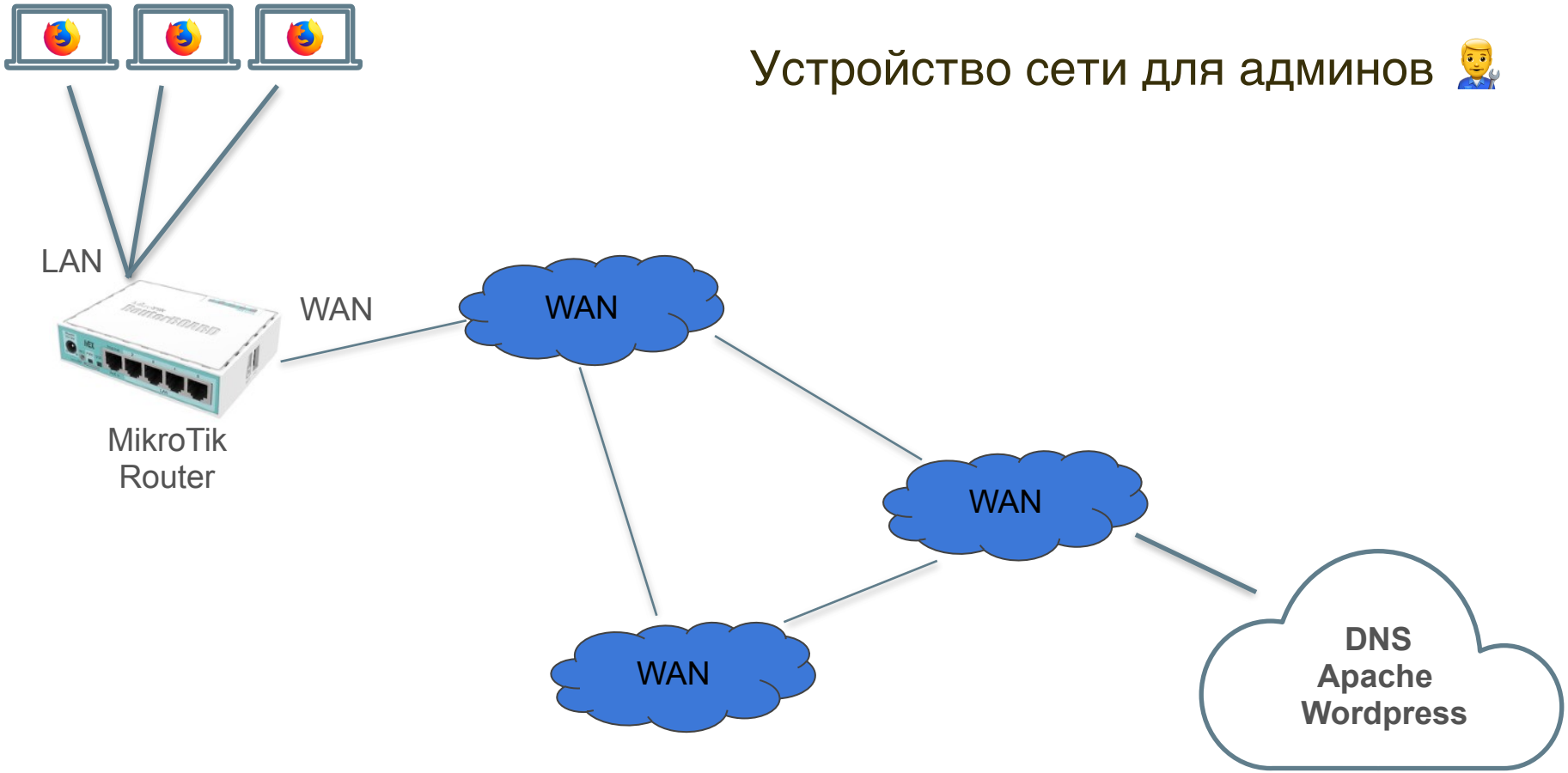
# Устройство сети для продвинутых 😎

Мой компьютер

Мой роутер

Инет

# Устройство сети для админов 👨‍🔧

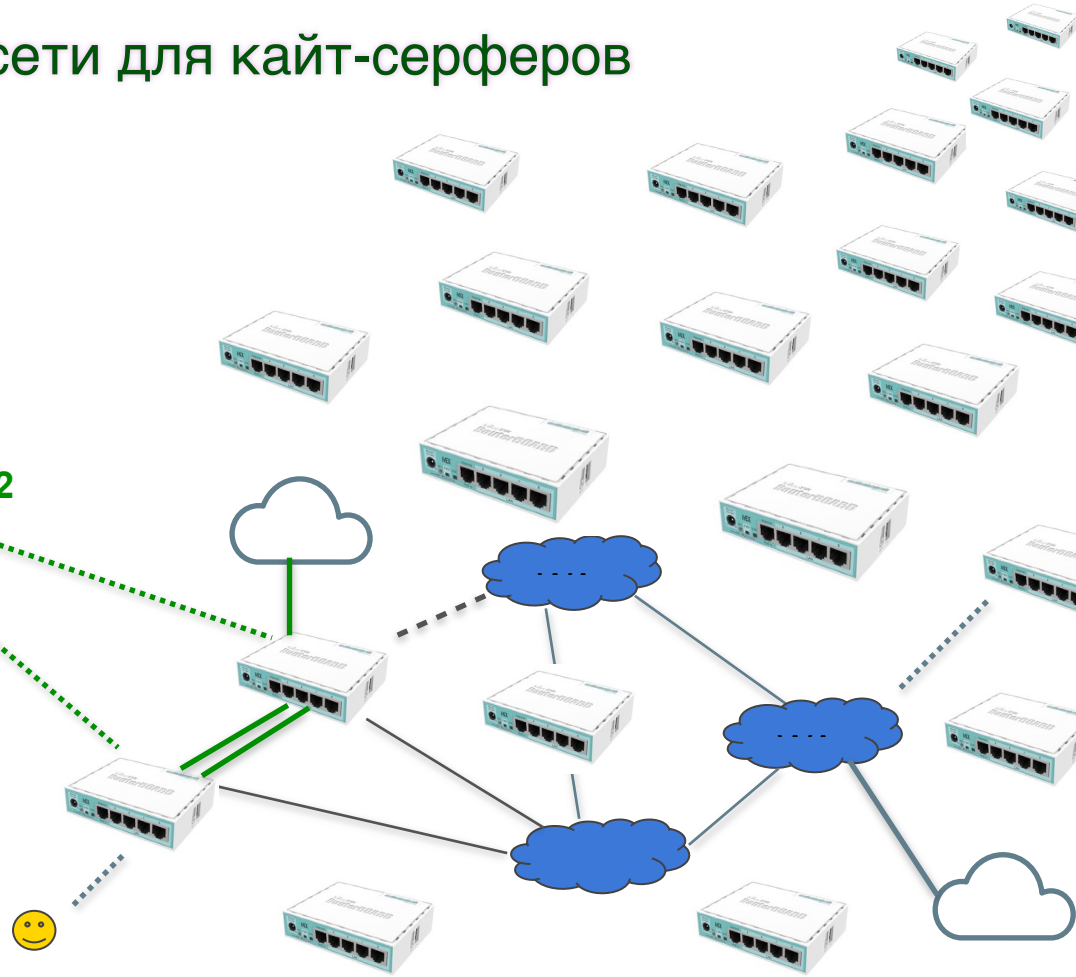


# Устройство сети для сетевых инженеров

# Устройство сети для кайт-серферов

IKEv2

IKEv2



t.me/tropicalengineer


BOARDSCHMIEDE
MikroTik
MALAYSIA

# Никита Тарикин

Сертифицированный
сетевой инженер
MikroTik PRO, Россия

MikroTik CERTIFIED

Nikita Tarikin / nikita@tarikin.com

# Никита Тарикин

Сертифицированный
сетевой инженер
MikroTik PRO, Россия

MTCNA 99%

MTCRE 95%

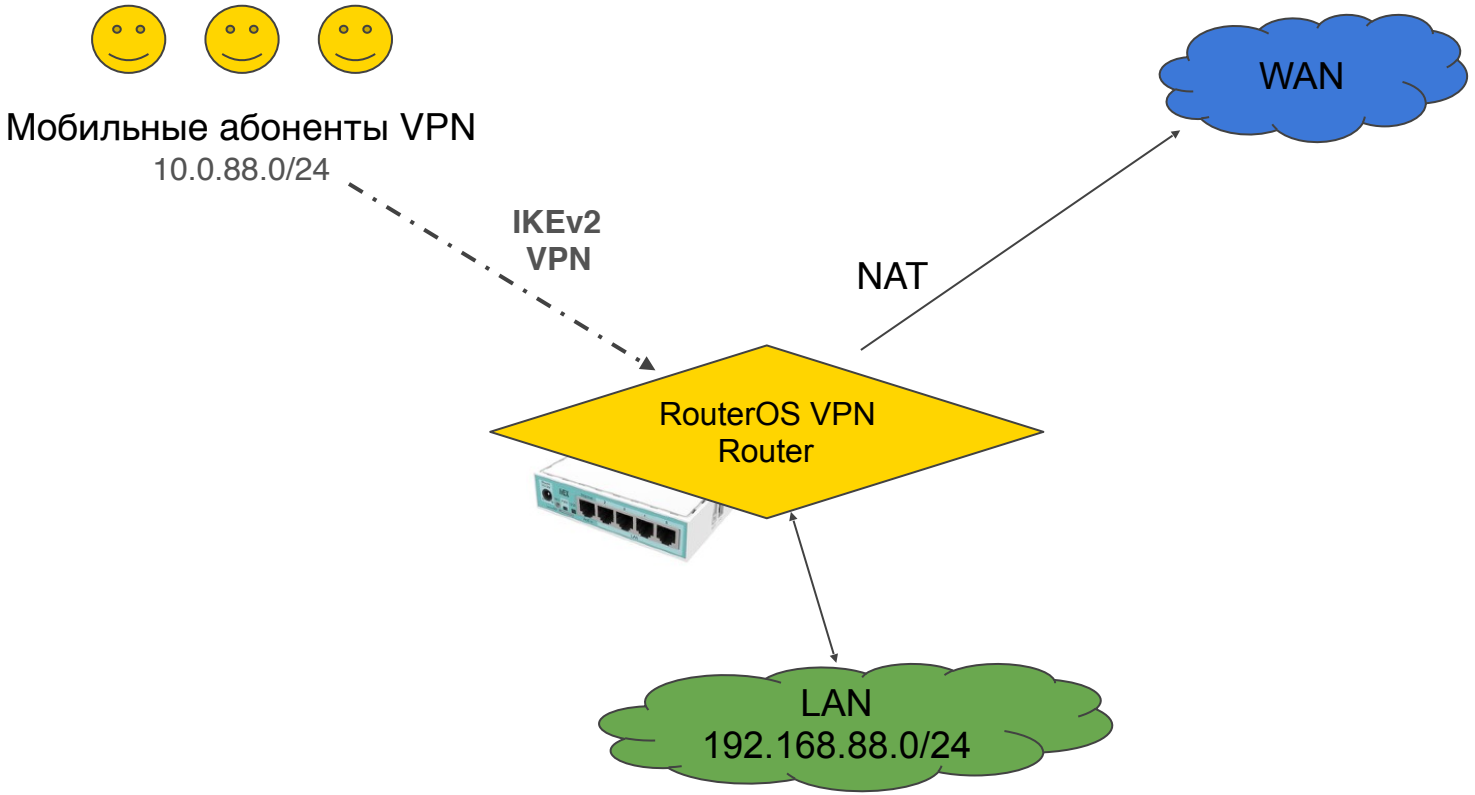
MTCTCE 96%

MTCWE 84%

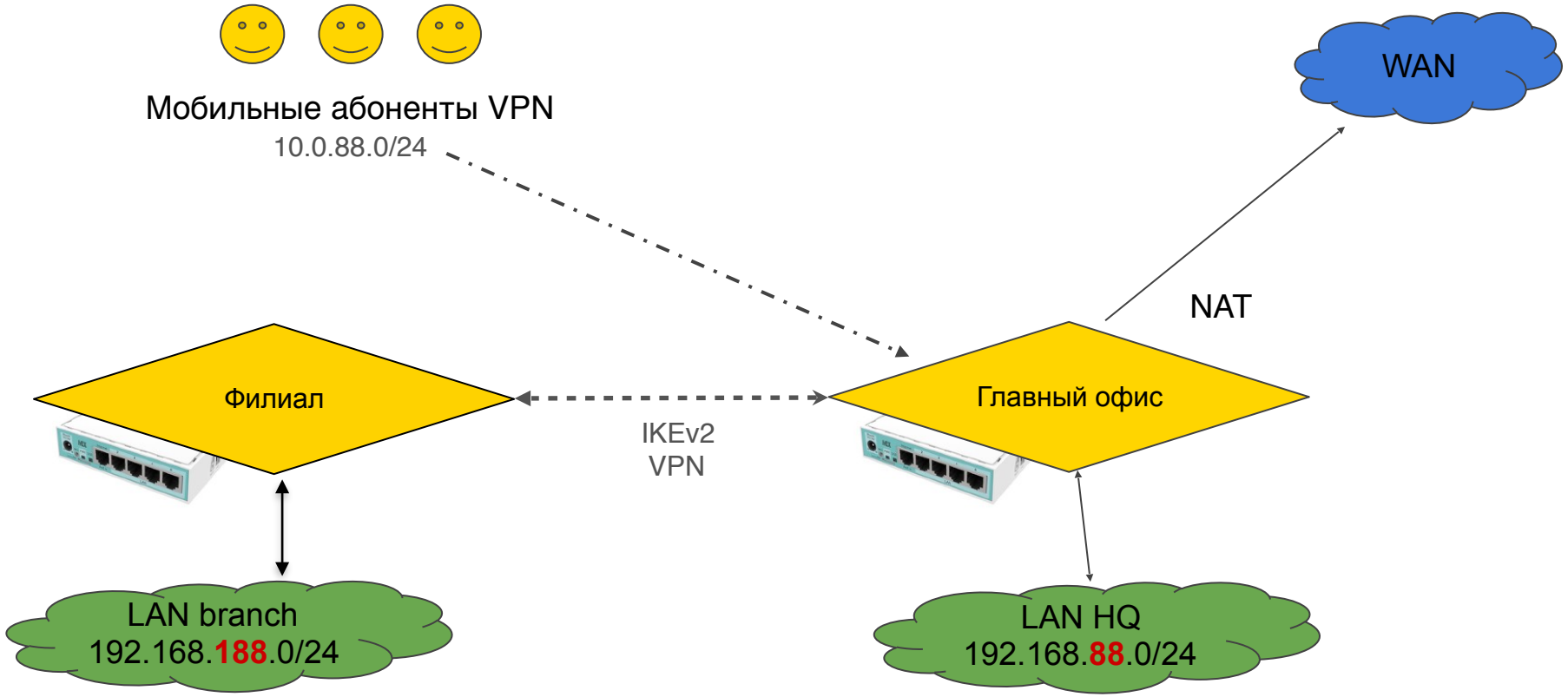
MTCUME 90%

MTCSE 94%


Как зарабатывать на технологиях MikroTik с видом на море?
Поиск клиентов
Рассказывать как зарабавать на MikroTik с видом на море
Выступать на конференциях MUM
Публиковать статьи и посты в соц сетях
Использовать хэш тэги
Предлагать новые фичи старым клиентам
Регулярно напоминать о себе вопросами о качестве работы настроенных систем
Ответственность
Не бухать
Не химичить в продакшне
Спать по ночам
Признавать и исправлять свои ошибки
Подключаться к инженерным системам с чистых компьютеров
Блокировать экран ноутбука
Скорость оказания услуг
Быть всегда на связи
Забыть про электронную почту
Отвечать быстро
Настроить VPN связь с инженерными системами клиента
Производительность
Строить быстрые каналы связи
Внимательно слушать претензии
Не экономить на оборудовании
Надежность
Дублировать критические участки
Иметь нажедного аватара на случай аварии
Мониторинг инфраструктуры с уведомлениями в Telegram
Автоматические резервные копии + контроль
Использовать long-term ветку в продакшне
Испытывать новые решения в лабораториях
Общение
Научиться улыбаться
Отчитываться на всех этапах
Разговаривать на понятном языке
Не задавать сложных вопросов
Стоимость
Предлагать бесплатный сыр новым клиентам
Избегать клиентов, которые ищут где подешевле
Не экономить на обучении
Безопасность
Многослойная защита периметра
Патчить уязвимости в день публикации
Шифровать весь инженерный трафик
Уникальные сложные пароли
Хранение ключей и паролей доступа в шифрованных контейнерах
Мониторинг новостей из мира инфобез




# Сетевая диаграмма




# Сетевая диаграмма

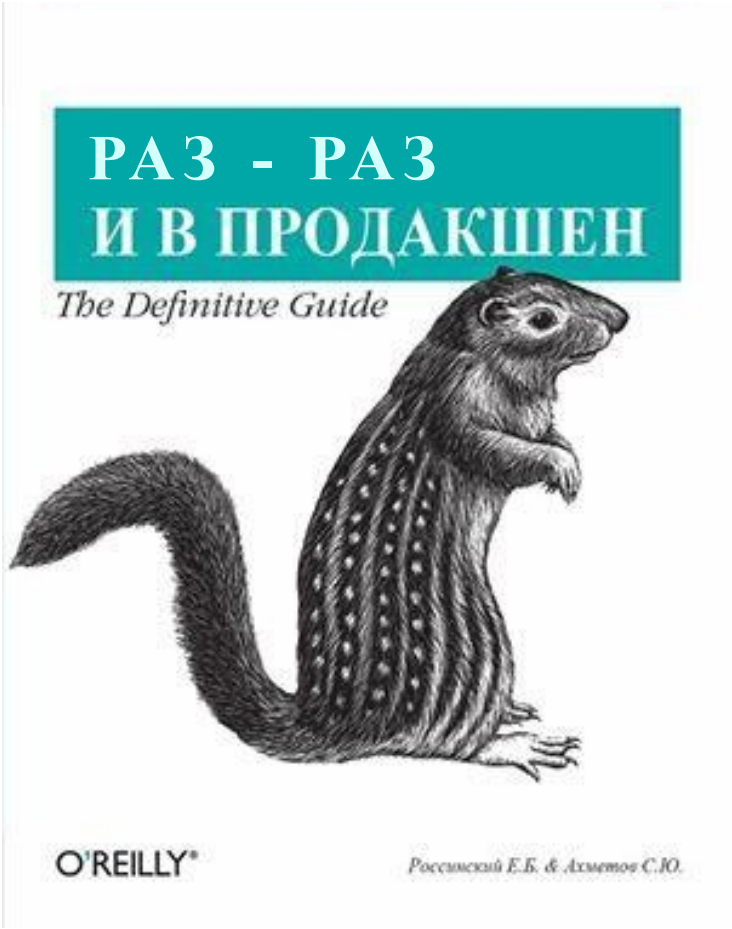
# Общий план презентации

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

Nikita Tarikin / nikita@tarikin.com

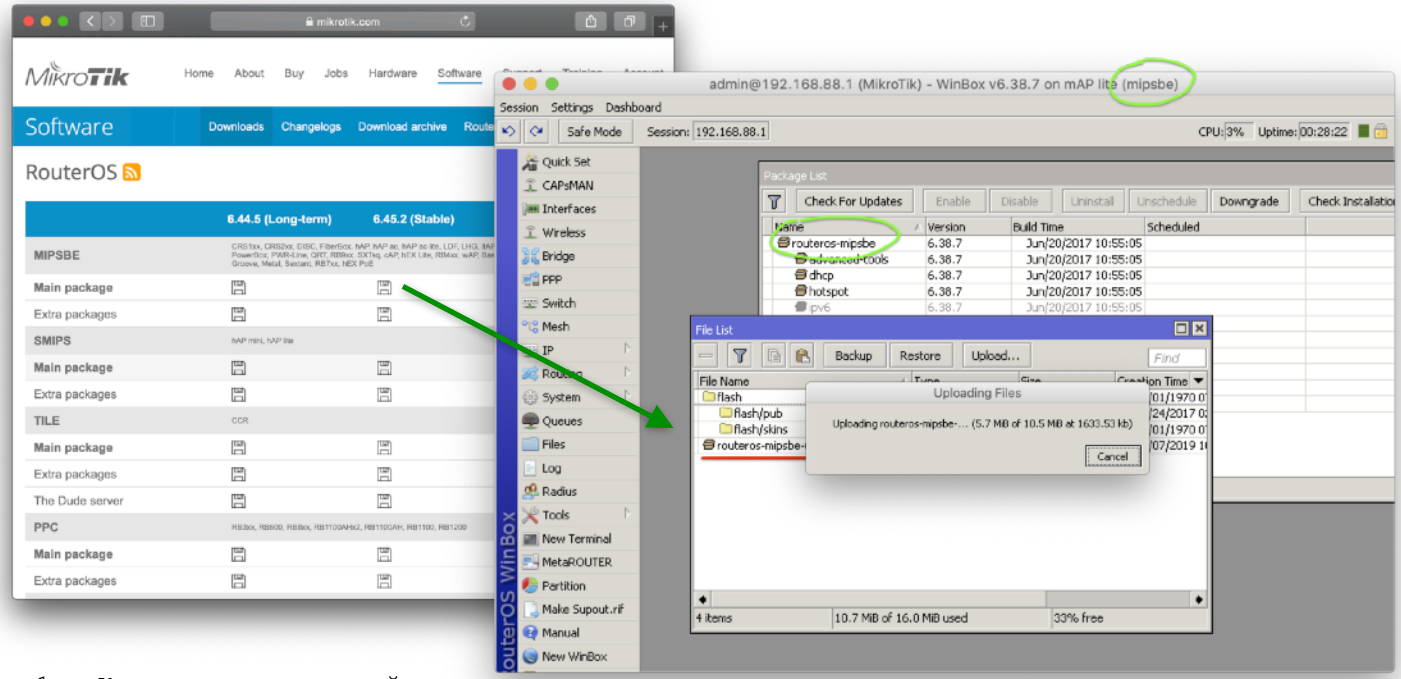
# Подготовка к работе

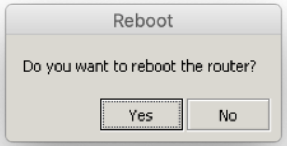
1. Наличие знаний уровня MTCNA (рекомендуется)
2. RouterOS 6.45 или новее
3. Все испытания строго **в лабораторных условиях** (настоятельно рекомендую)
4. Дефолт конфигурация 6.45+




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

# Обновляем RouterOS до версии 6.45 или новее



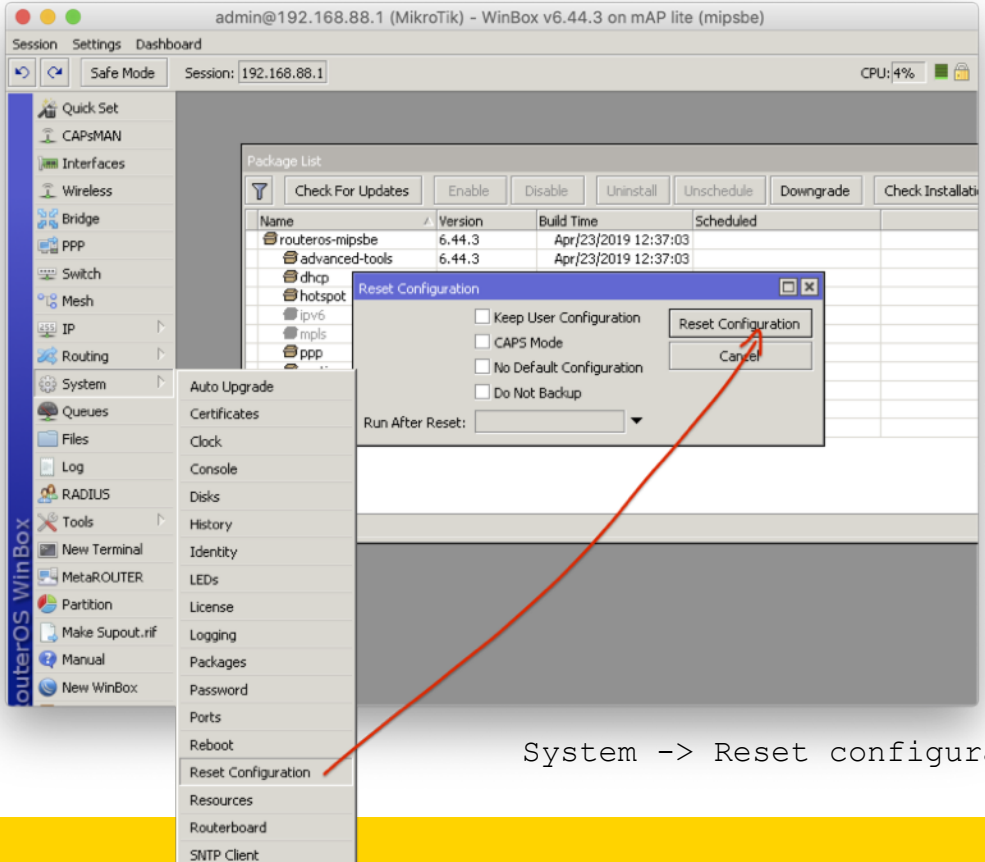




1. Качаем установочный пакет www.mikrotik.com/download

2. Заливаем пакет в корень файловой системы

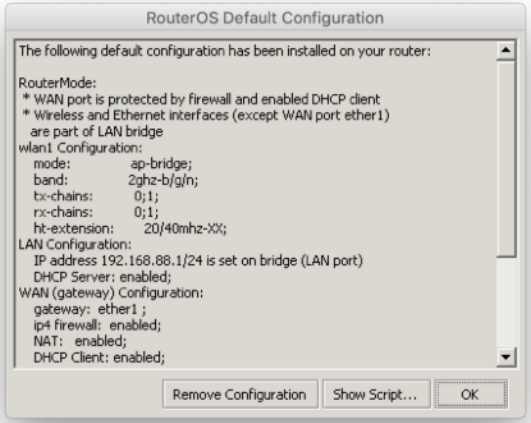
3. Перезагружаем

# Сбрасываем RouterBoard к заводской v6.45+ конфигурации




System -> Reset configuration

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

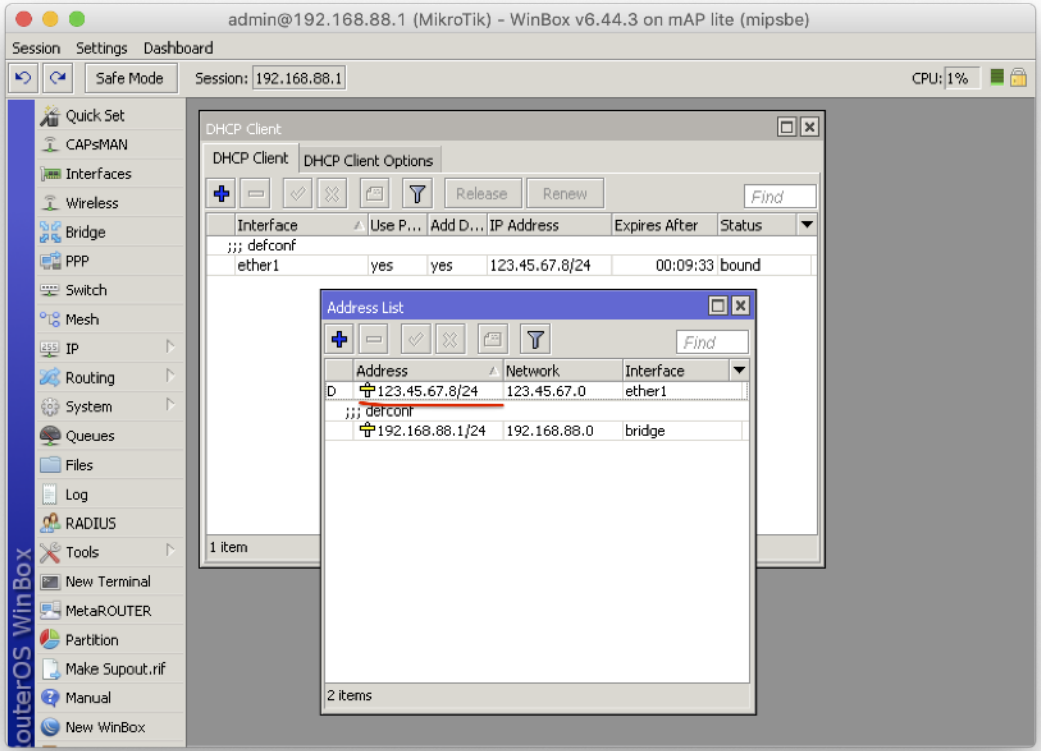


# Общие системные настройки

План действий:

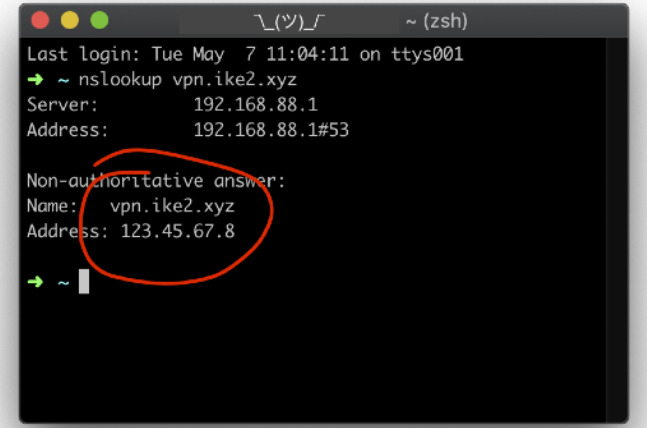
1. WAN IP/DNS адреса
2. Часовой пояс
3. Дата/время через NTP
4. Loopback bridge
5. IP pool

# Адреса WAN IP и DNS для IKE2 VPN сервера



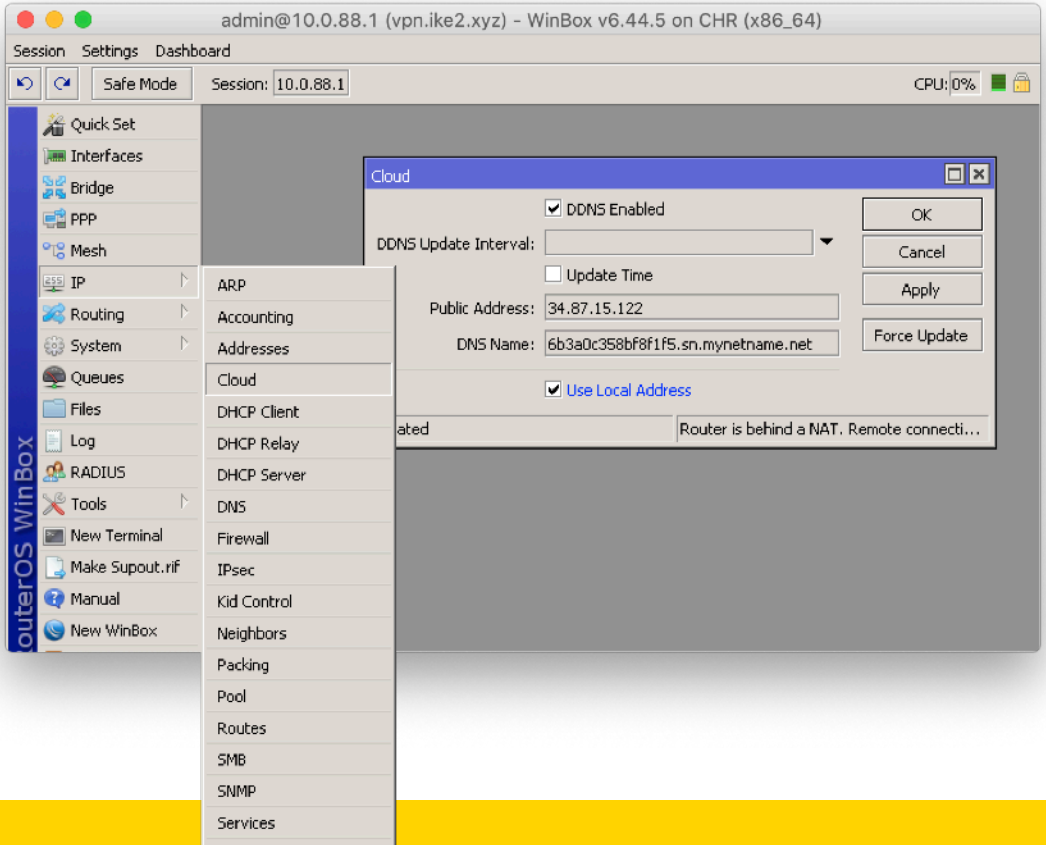

123.45.67.8 на WAN интерфейсе

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? 😎

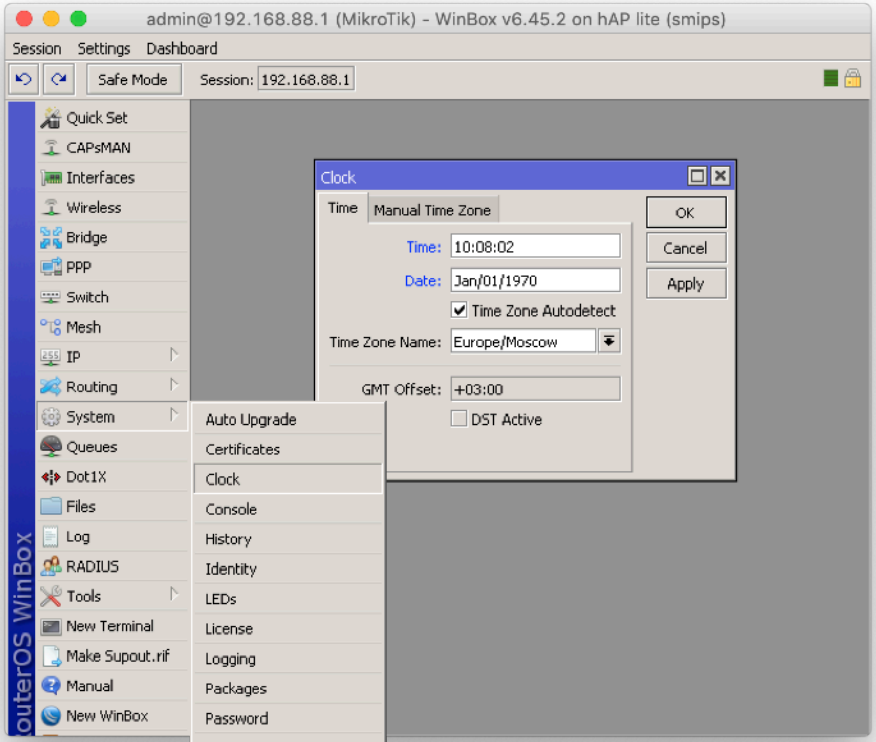



## IP -> Cloud

Проверяем записи DNS:
Имя: **blabla.sn.mynetname.net**
Адрес: **34.87.15.122**

# Настраиваем часовой пояс

ЭТО ВАЖНО

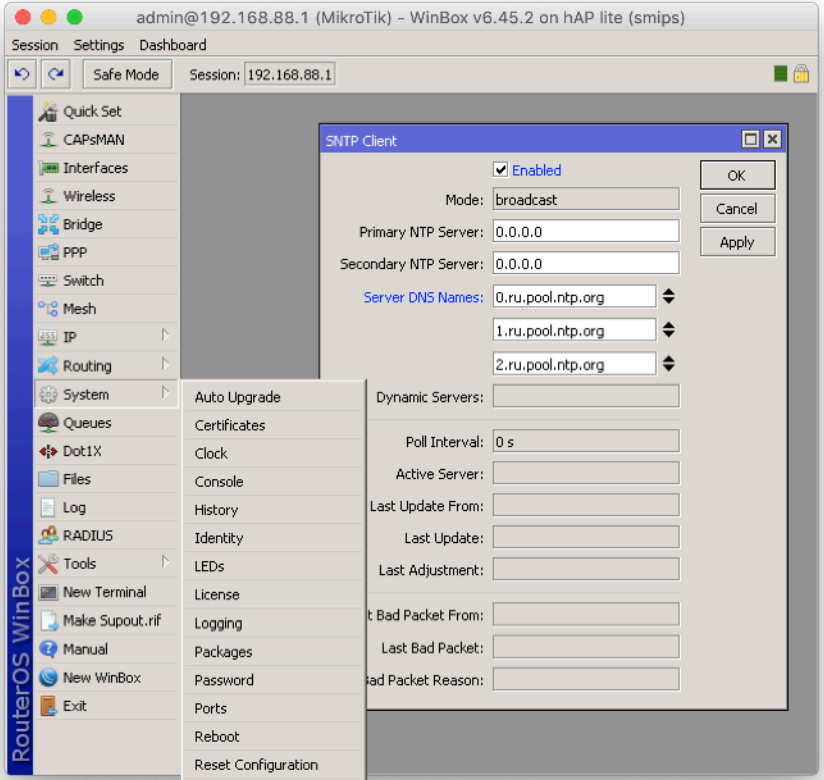



System -> Clock

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

# Настройка автоматической синхронизации даты и времени

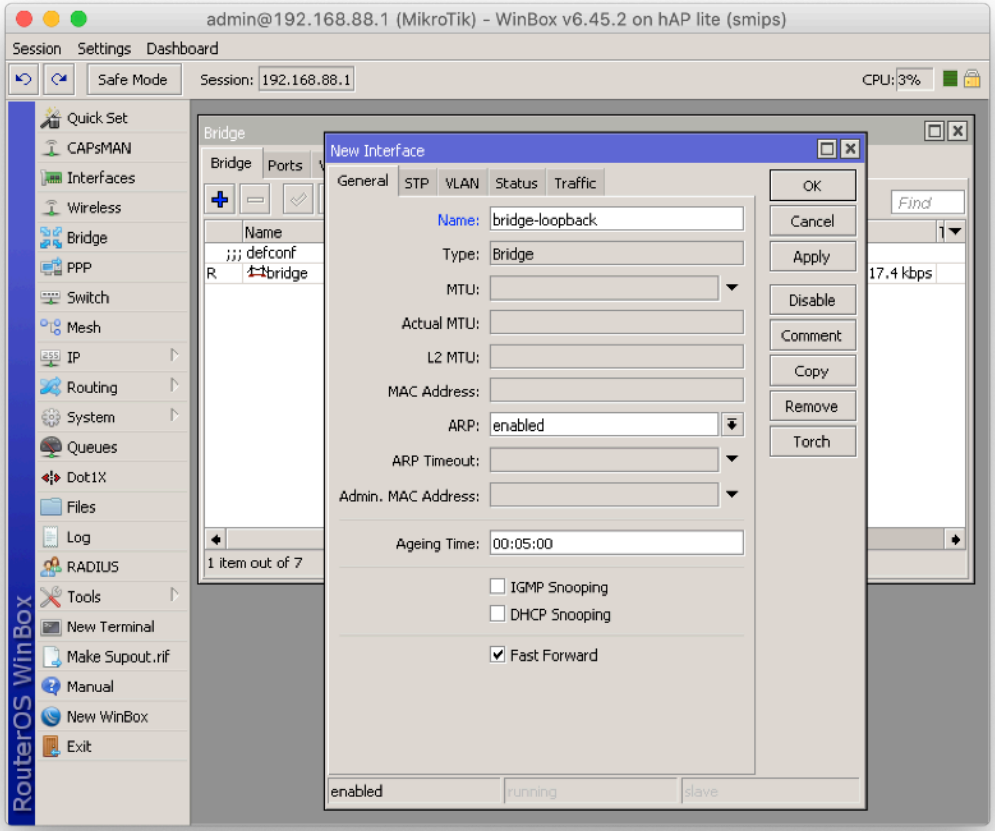
ЭТО ВАЖНО




Активируем NTP client

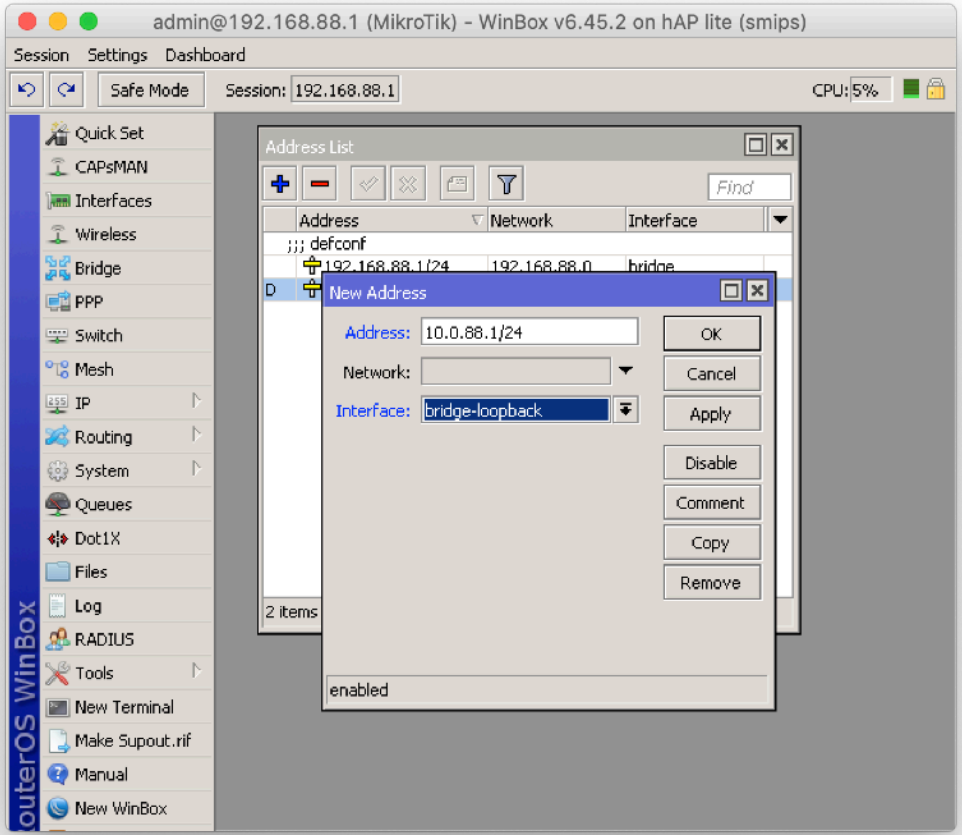
```
/system ntp client set enabled=yes
server-dns-names=0.ru.pool.ntp.org,
1.ru.pool.ntp.org,2.ru.pool.ntp.org
```

# Добавляем новый loopback bridge




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

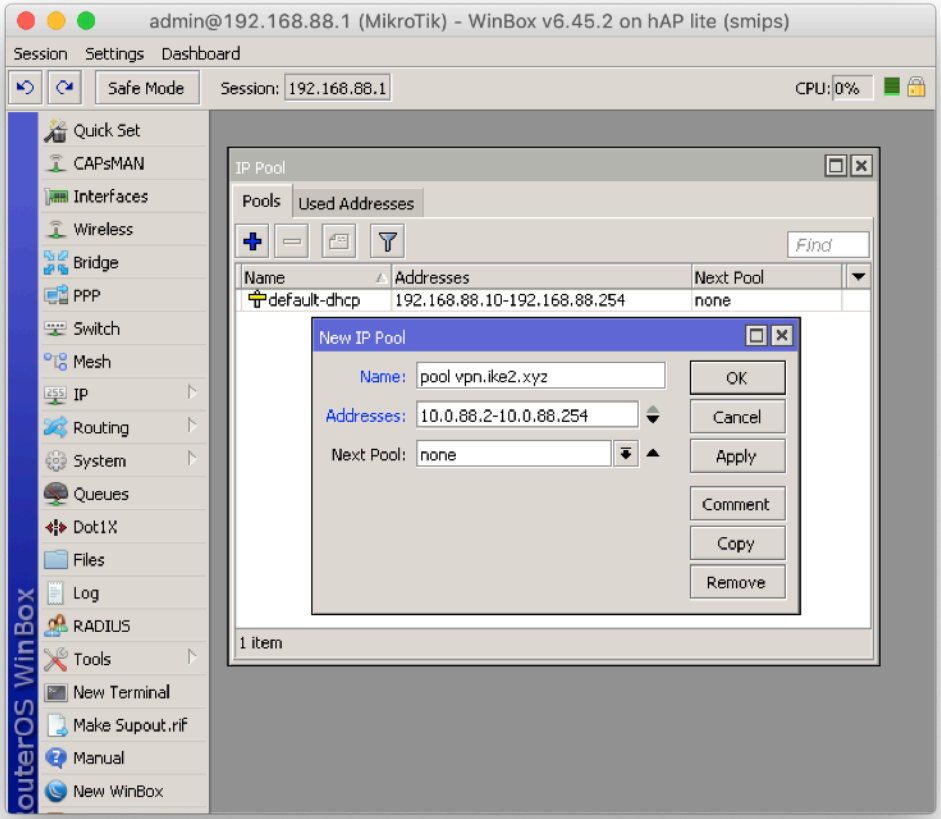
# Задаём IP адрес для loopback bridge




10.0.88.1

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

# 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
```

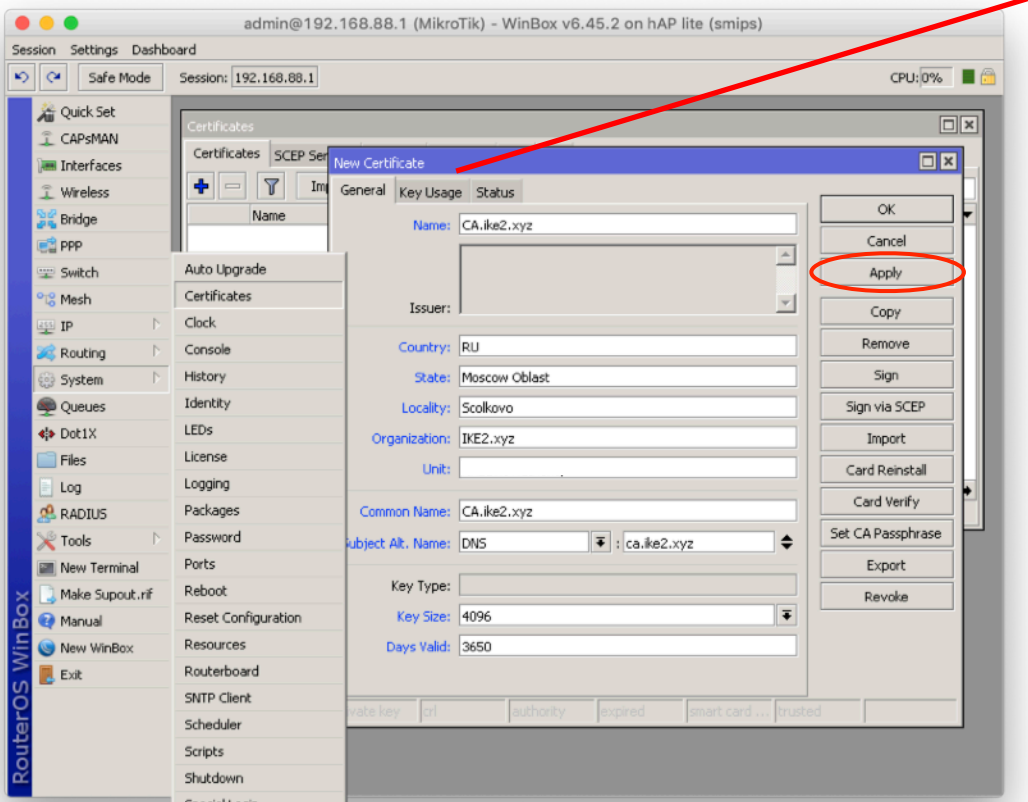
# Генерируем правильные SSL сертификаты

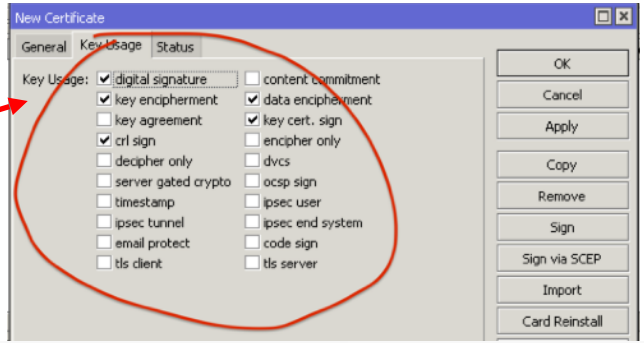
План действий

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

Nikita Tarikin / nikita@tarikin.com

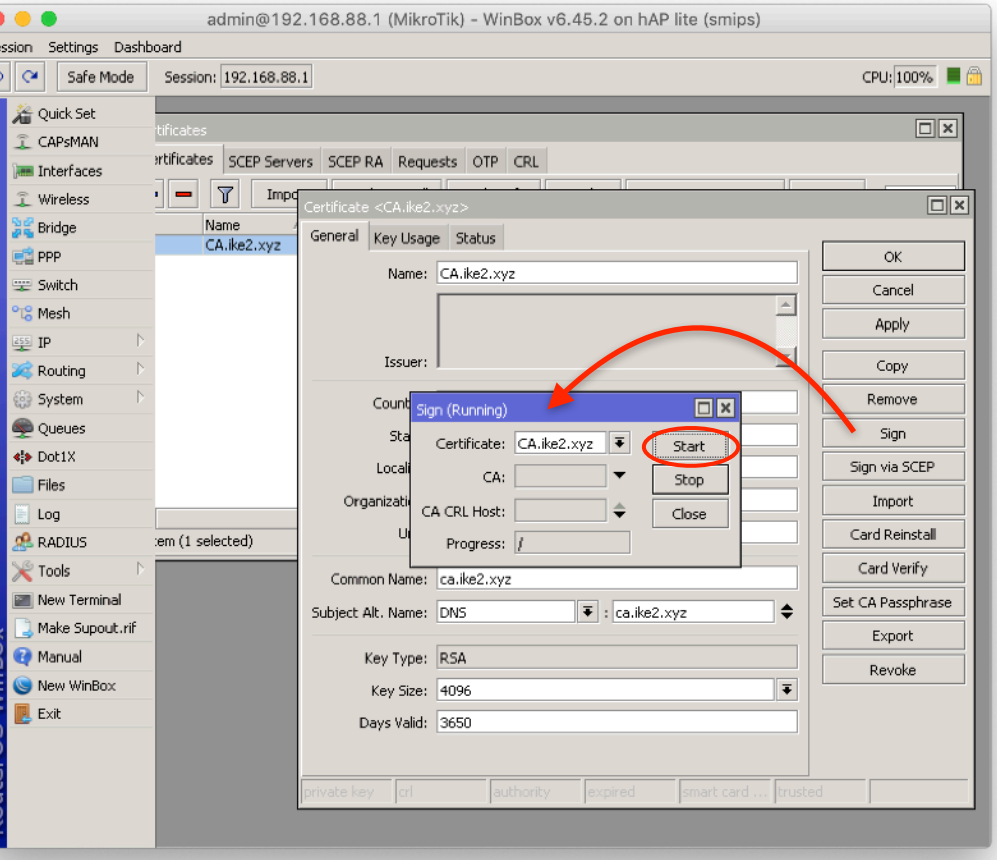
# Генерируем главный CA SSL сертификат




```
/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
```

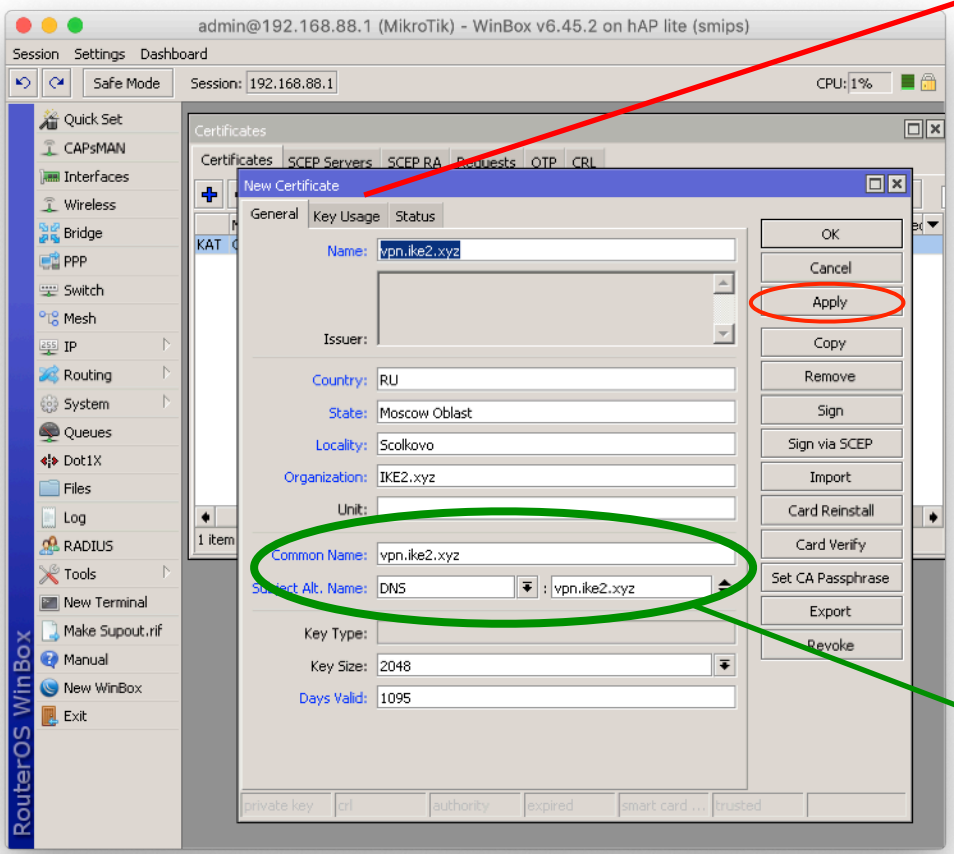
# Само-подписываем новый CA SSL сертификат *(Certificate Authority)*

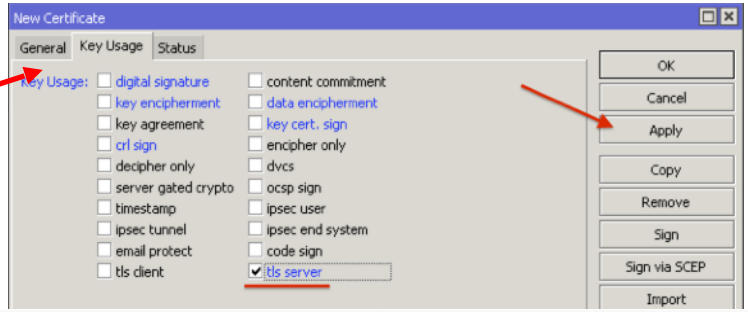



```
/certificate sign CA.ike2.xyz
```

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

# Генерируем серверный SSL сертификат

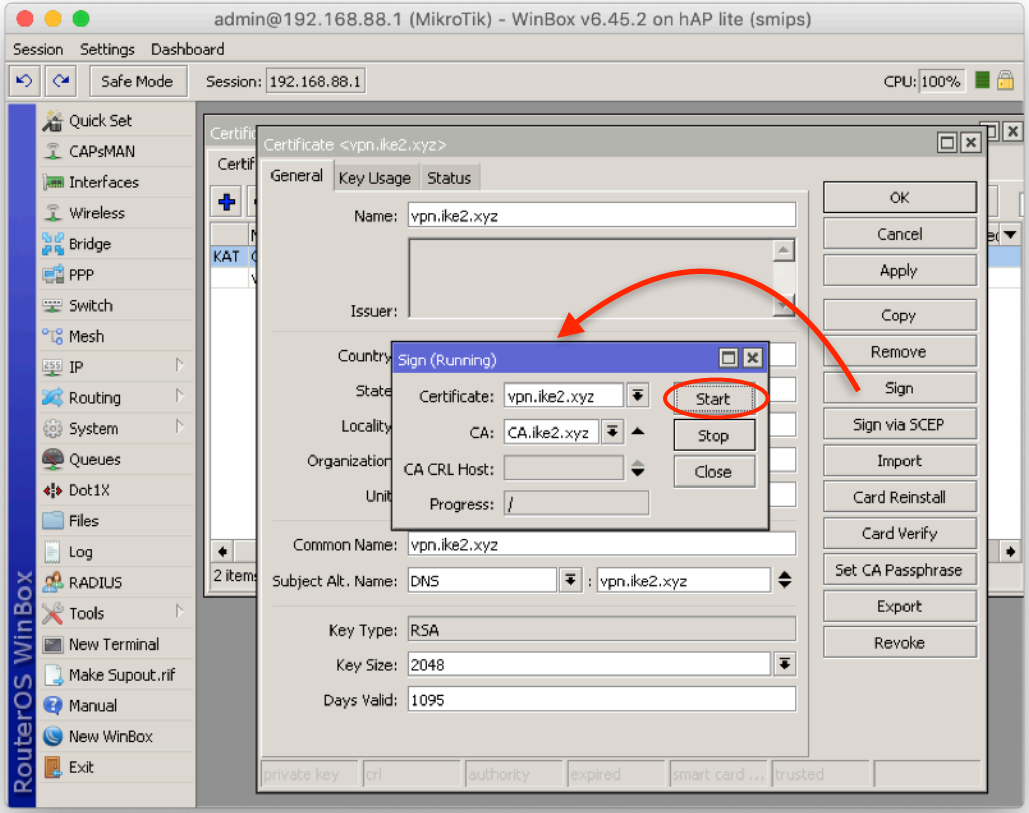



```
/certificate add name=vpn.ike2.xyz
country=RU state="Moscow Oblast"
locality=Scolkovo organization=IKE2.xyz
common-name=vpn.ike2.xyz subject-alt-
name=DNS:vpn.ike2.xyz key-size=2048
days-valid=1095 trusted=yes key-
usage=tls-server
```

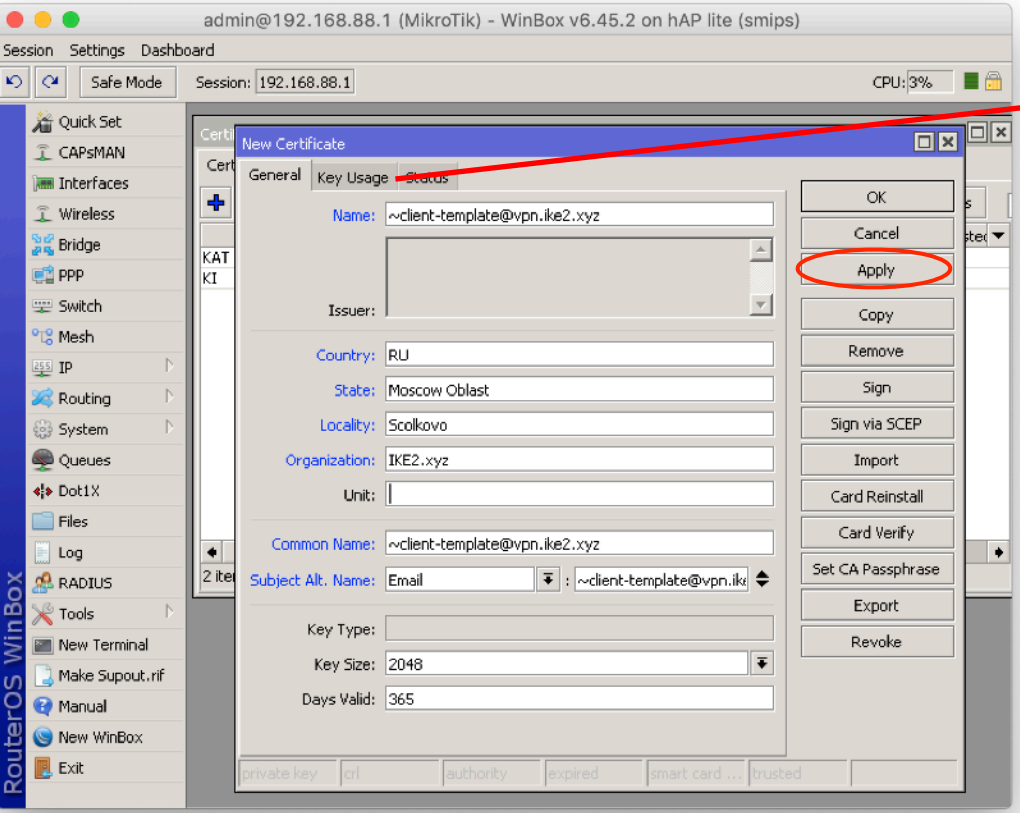
**vpn.ike2.xyz**

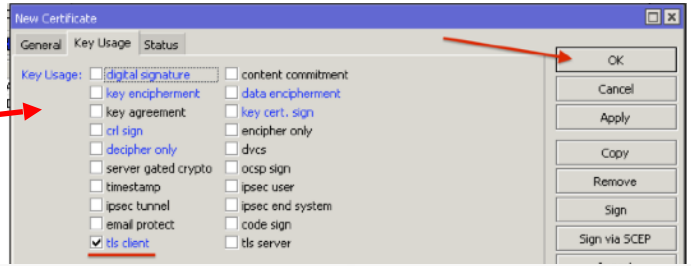
# Подписываем серверный сертификат у авторитета CA.ike2.xyz




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

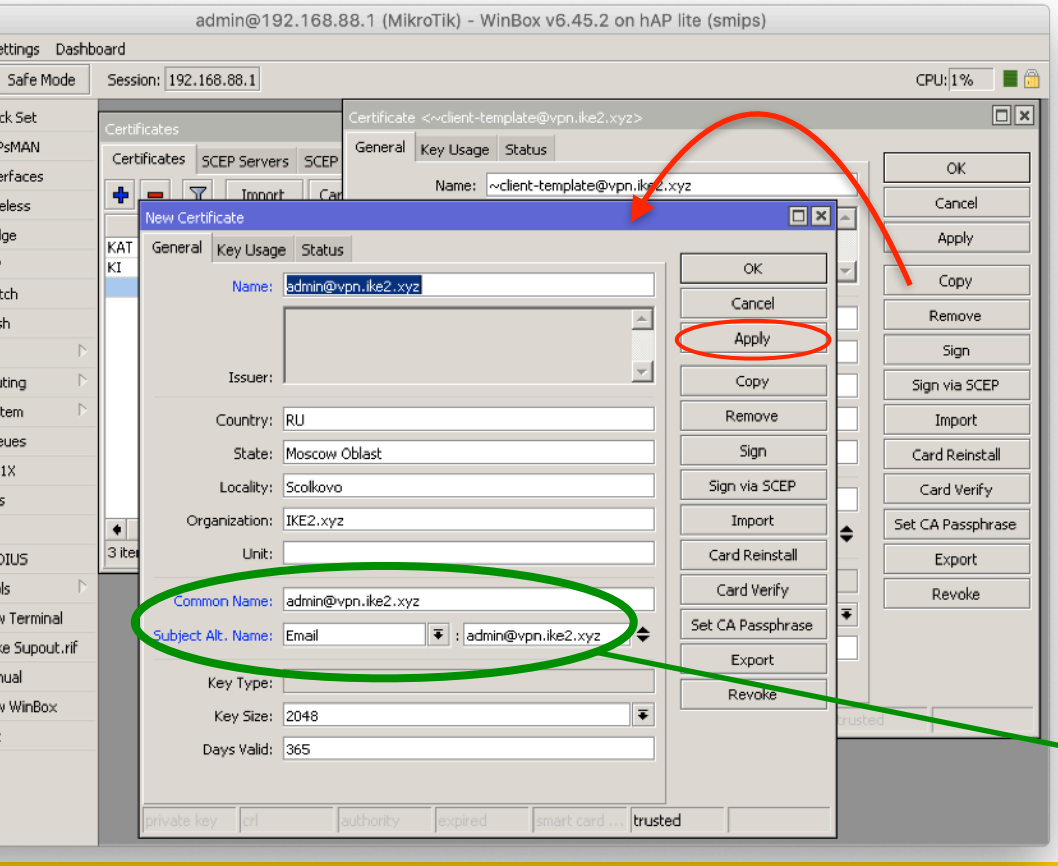
# Создаем шаблон для тиражирования клиентских подписей




```
/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
```

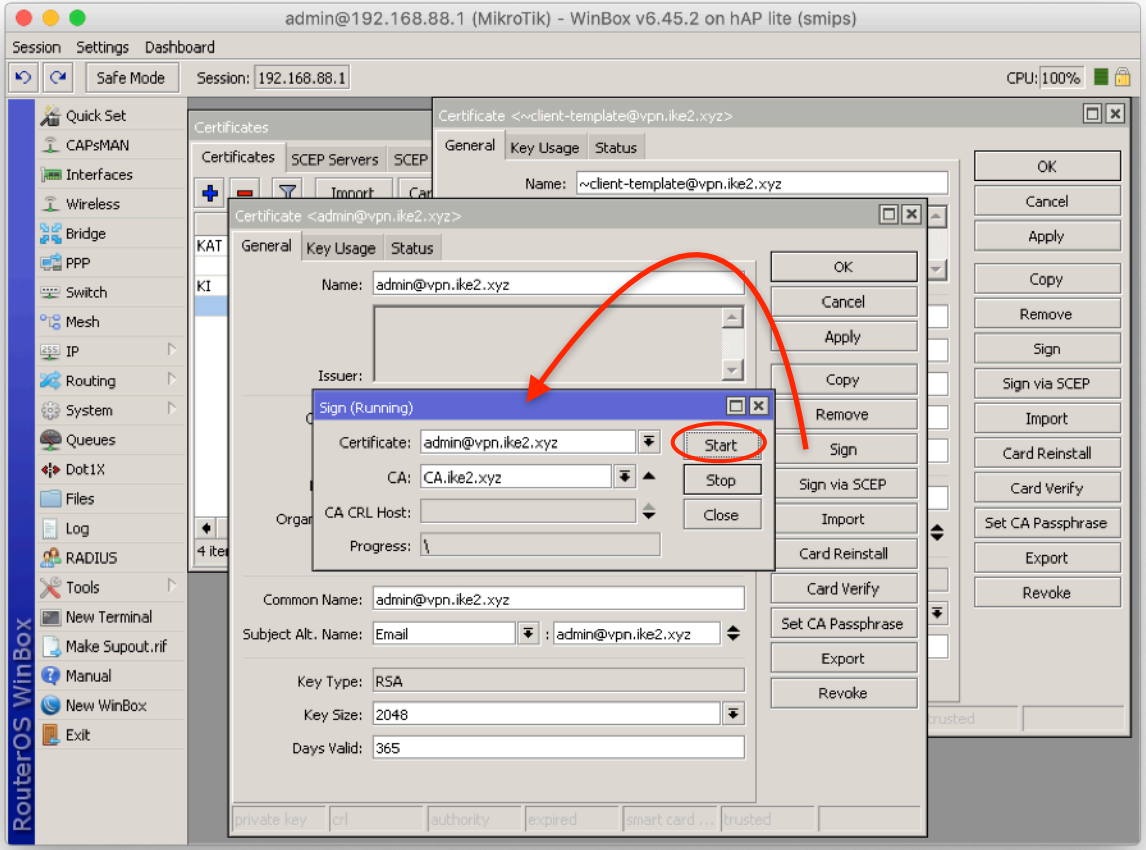
# Создаем первую клиентскую подпись из заготовленного шаблона




```
/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
```

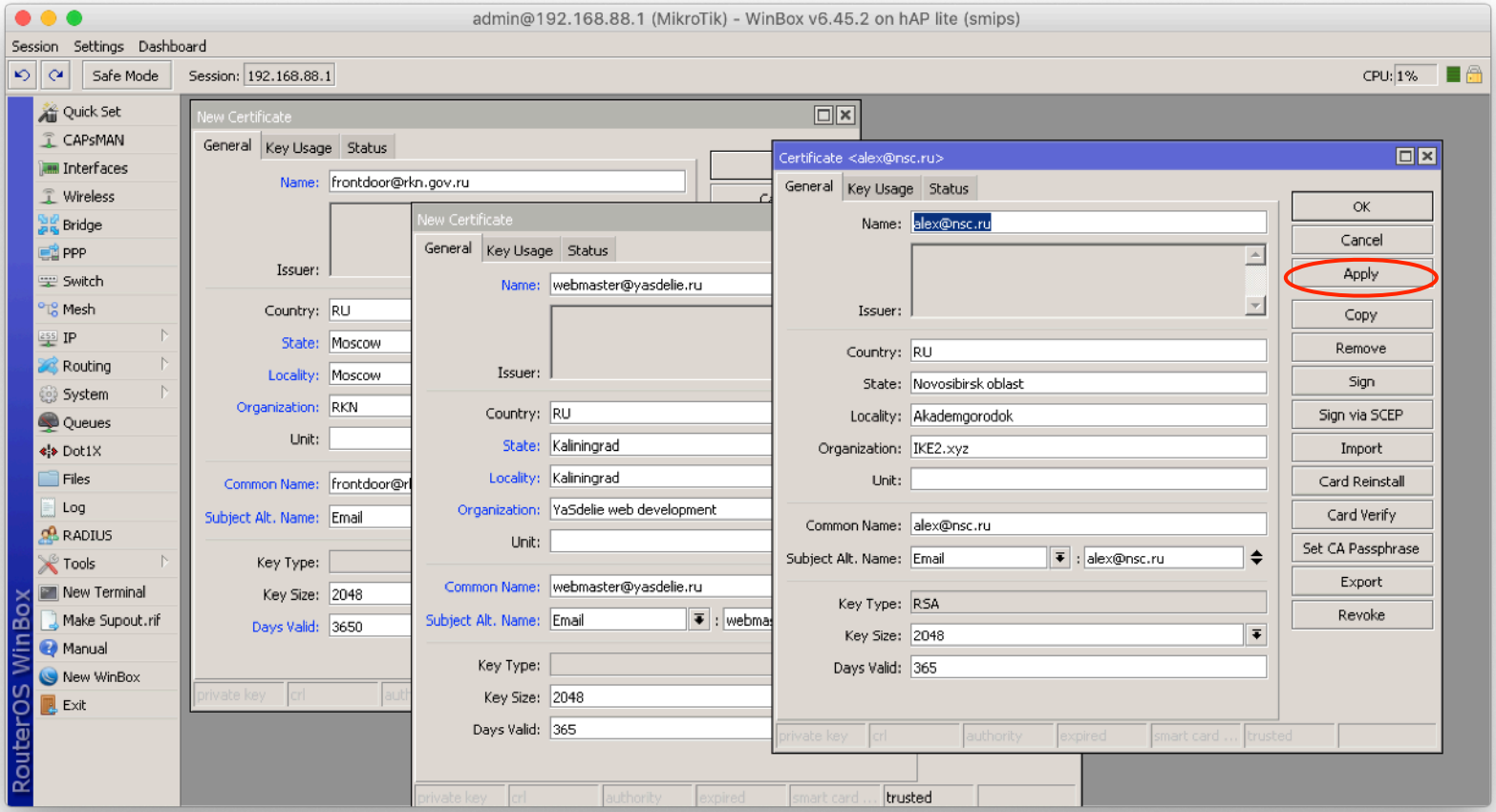
**admin@vpn.ike2.xyz**

# Подписываем клиентскую подпись у авторитета CA.ike2.xyz

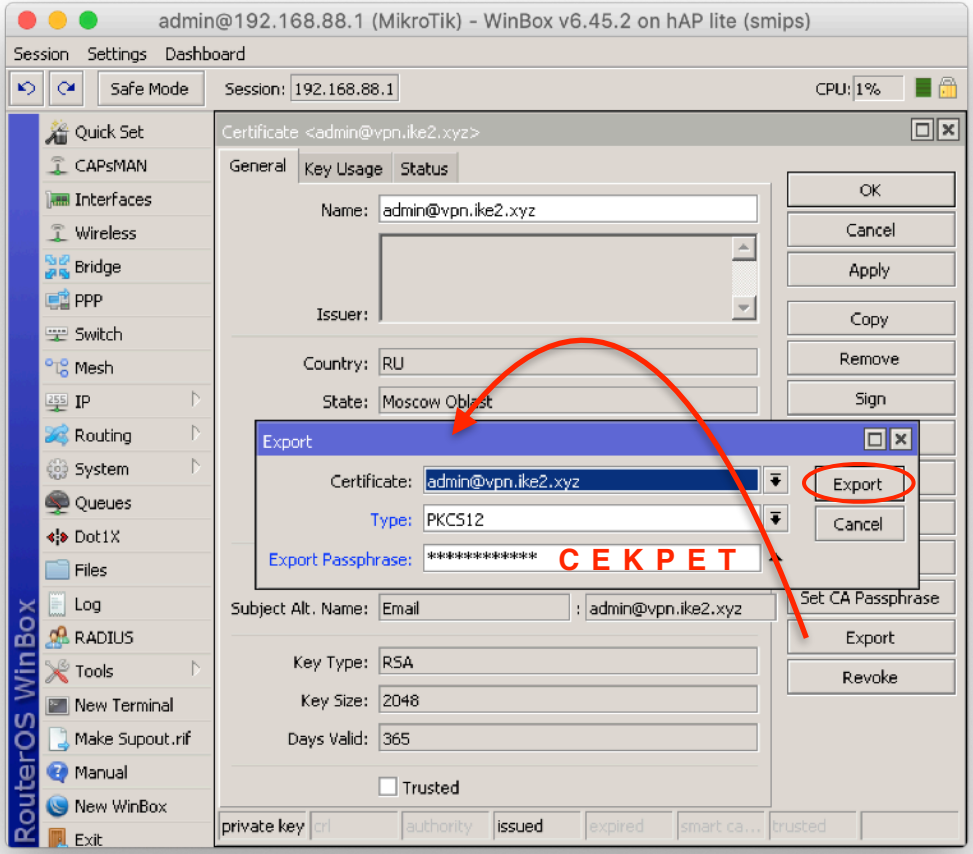



```
/certificate sign
admin@vpn.ike2.xyz
ca=CA.ike2.xyz
```

# Создаем остальные клиентские подписи из шаблона (по аналогии)



# Экспортируем клиентскую подпись + приватный ключ в файл .p12

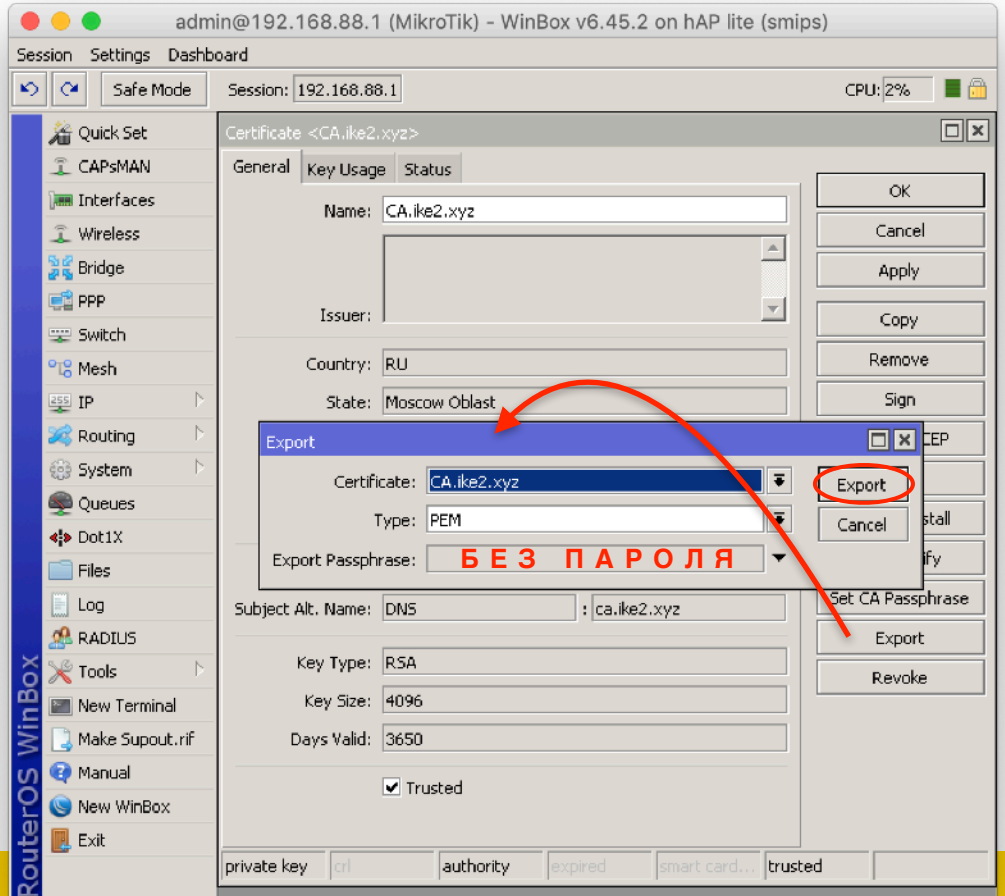



При экспорте **обязательно** указываем пароль.
Пустой пароль экспортирует **сертификат без ключа**.

Пароль храним в секрете.

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

# Экспортируем сертификат авторитета CA в .crt файл

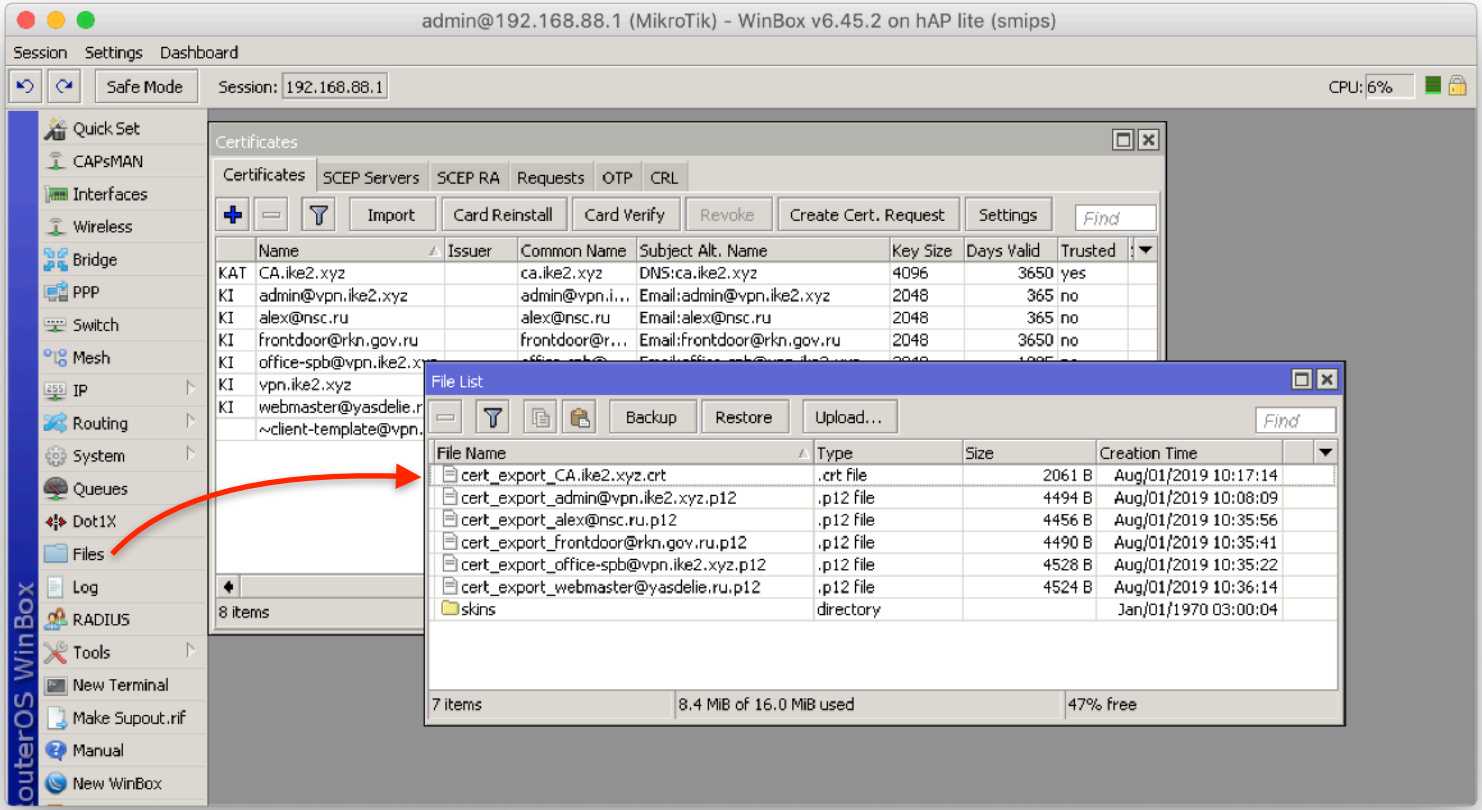


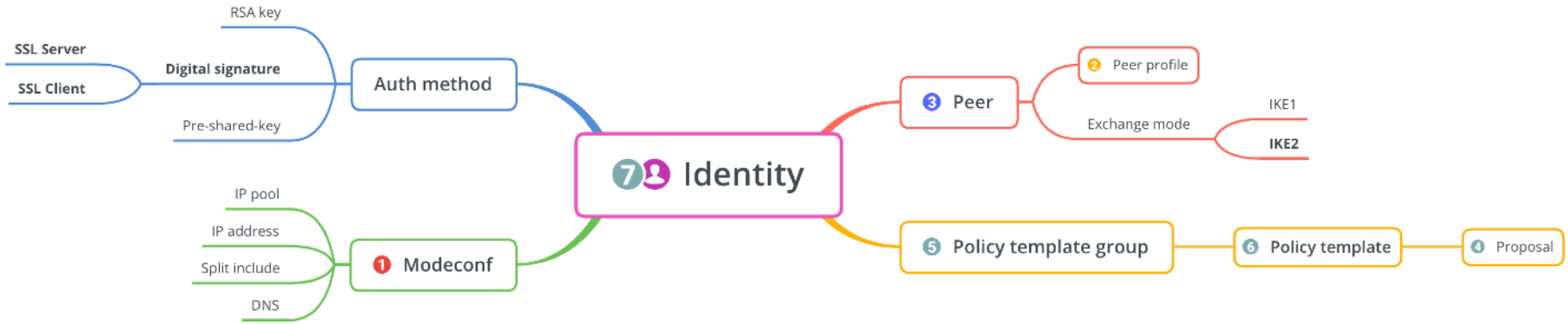

При экспорте **ни в коем случае** не указываем пароль.
Экспорт **ключа CA** само-провозглашенного **авторитета**

**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

Nikita Tarikin / nikita@tarikin.com

# 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;

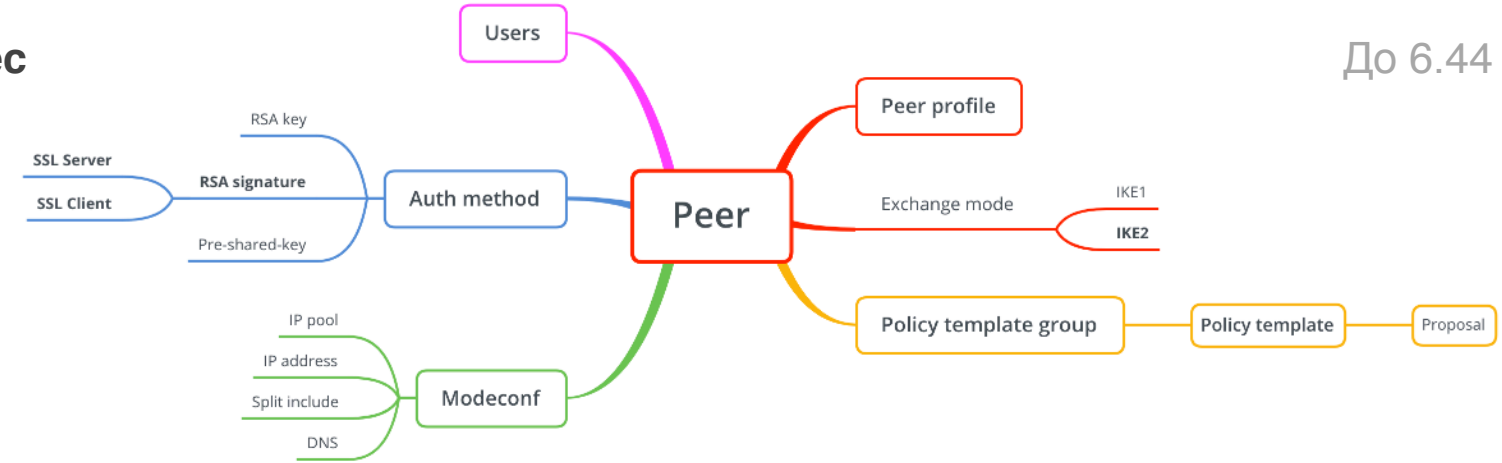
# Ключевые изменения в RouterOS 6.44

*) 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;

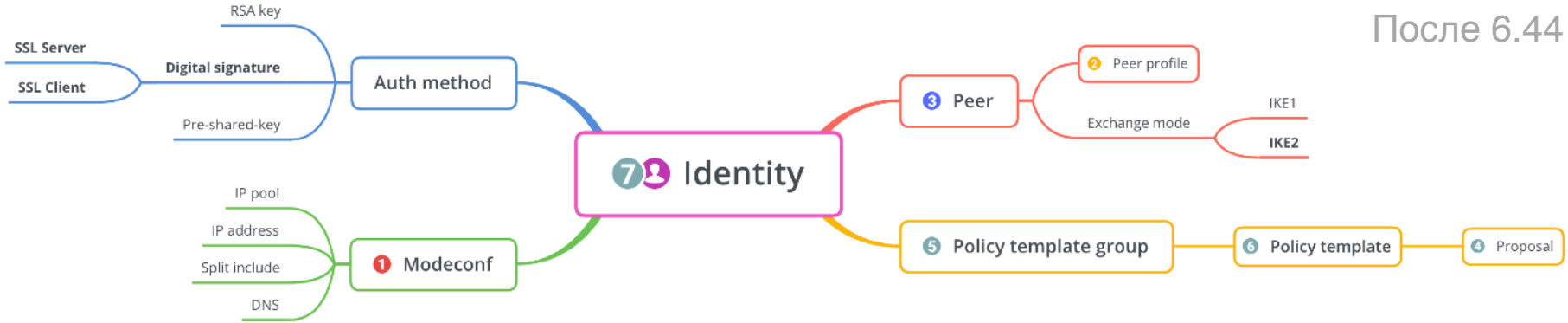
*) ike2 - added option to specify certificate chain;
*) ike2 - added peer identity validation for RSA auth (disabled after upgrade);
*) ike2 - allow to match responder peer by "my-id=fqdn" field;
*) ike2 - send split networks over DHCP (option 249) to Windows initiators if DHCP Inform is received;

# Структура IPSec

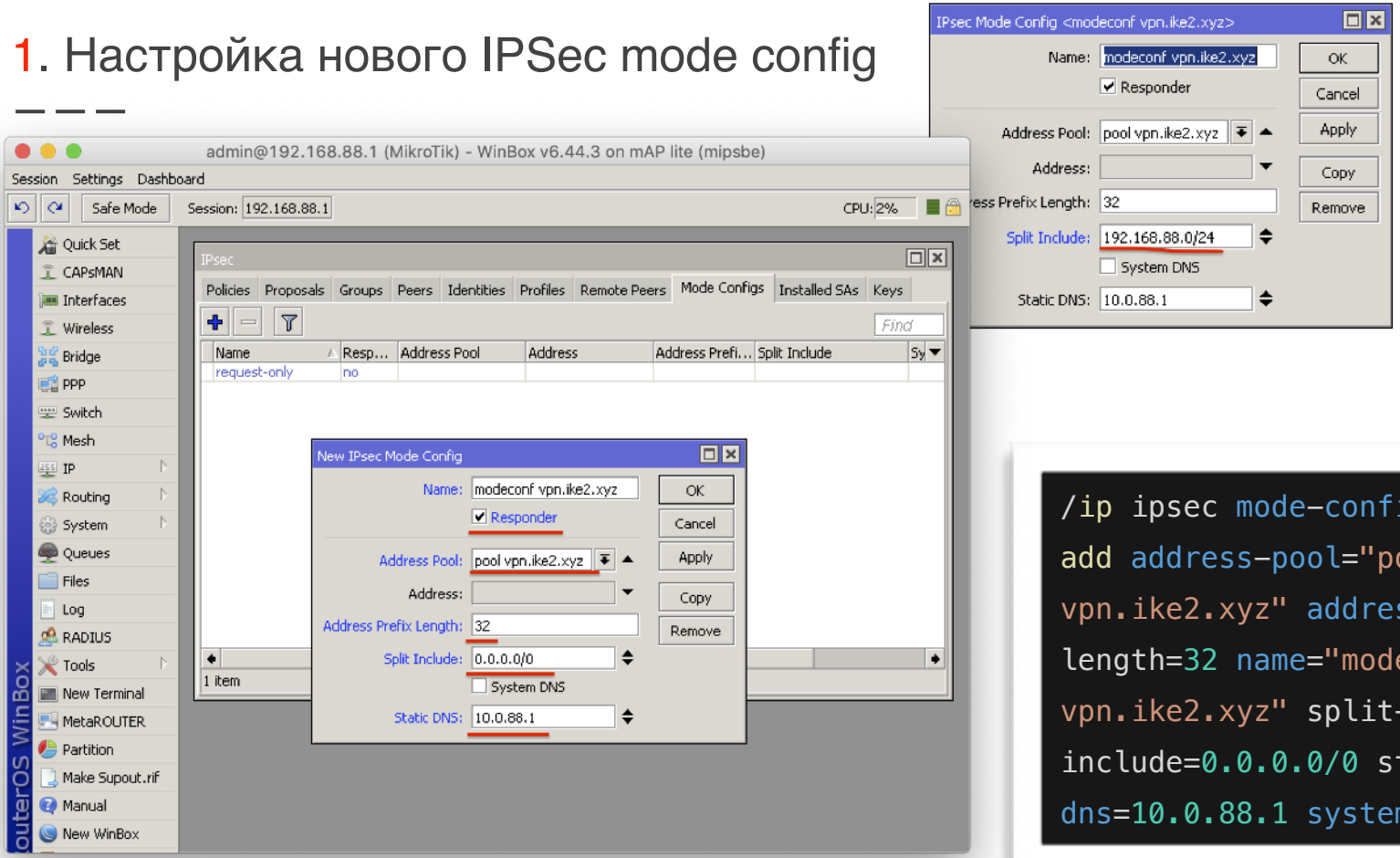
До 6.44




После 6.44

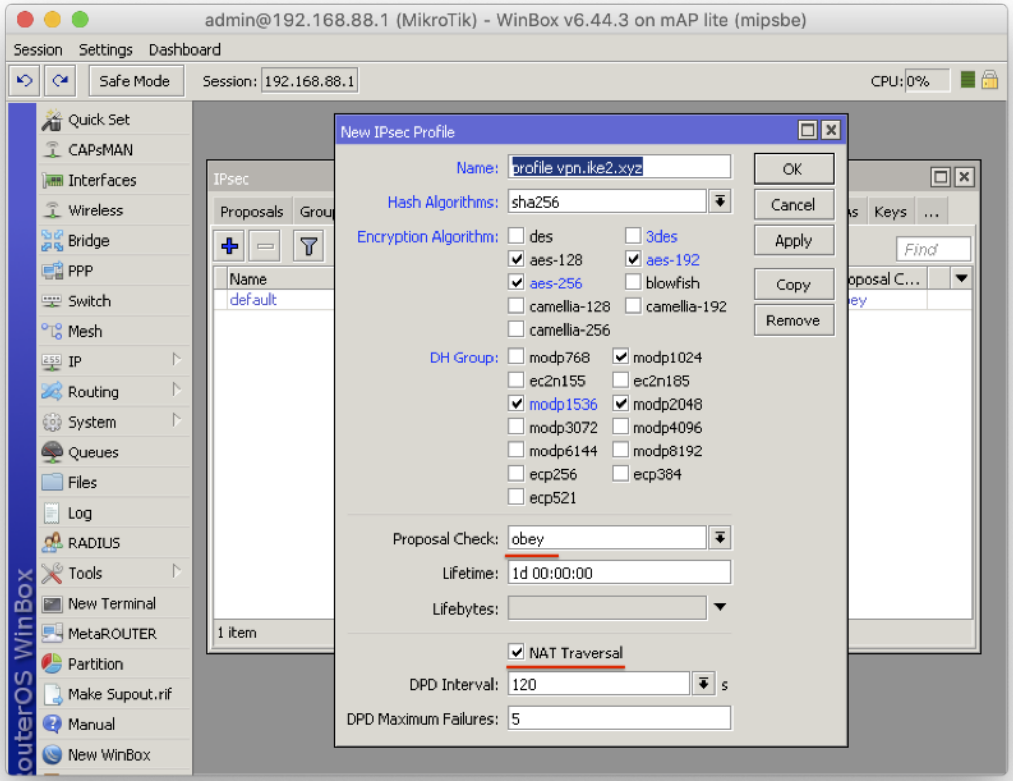


# 1. Настройка нового IPSec mode config



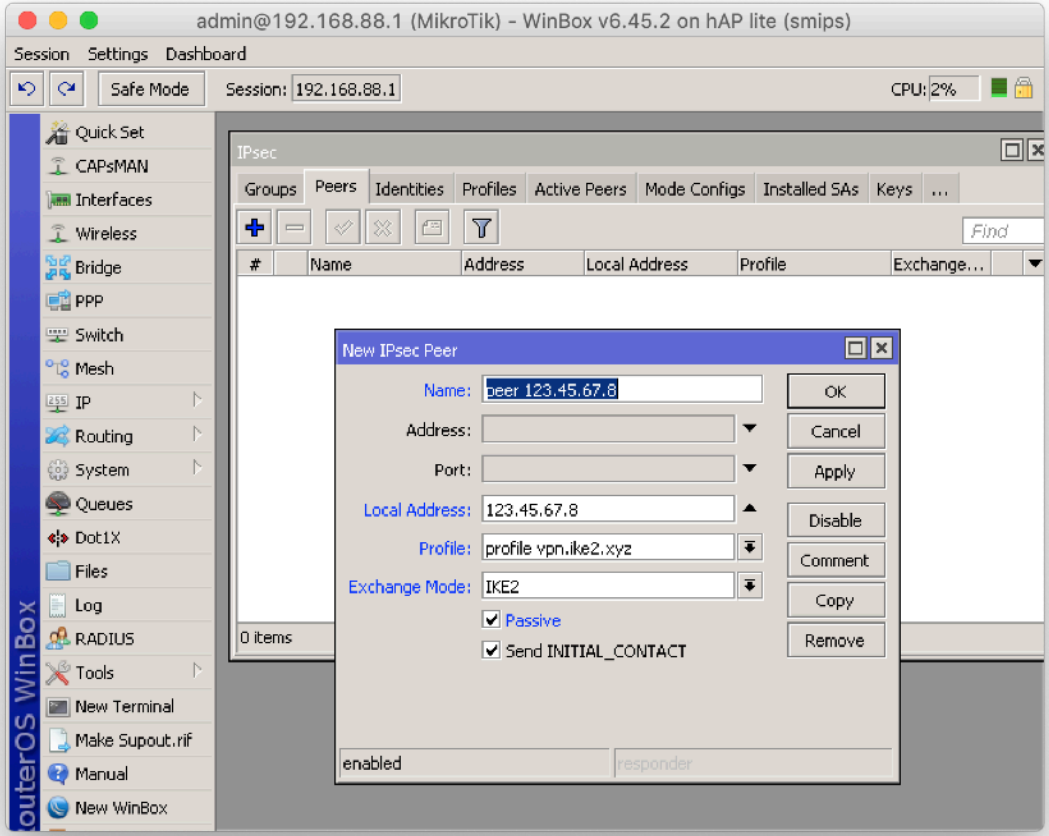

```
/ip ipsec mode-config
add address-pool="pool
vpn.ike2.xyz" address-prefix-
length=32 name="modeconf
vpn.ike2.xyz" split-
include=0.0.0.0/0 static-
dns=10.0.88.1 system-dns=no
```

# 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)

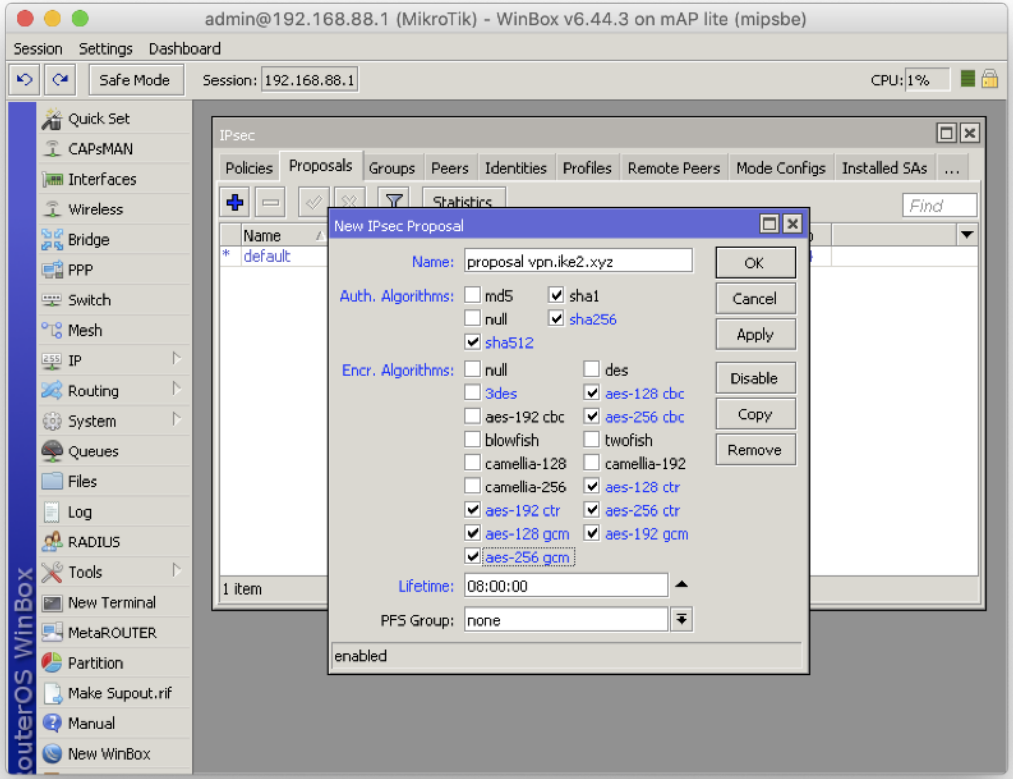



Принимаем клиентов со всех адресов **0.0.0.0/0**

Принимаем клиентов только на адрес **123.45.67.8**

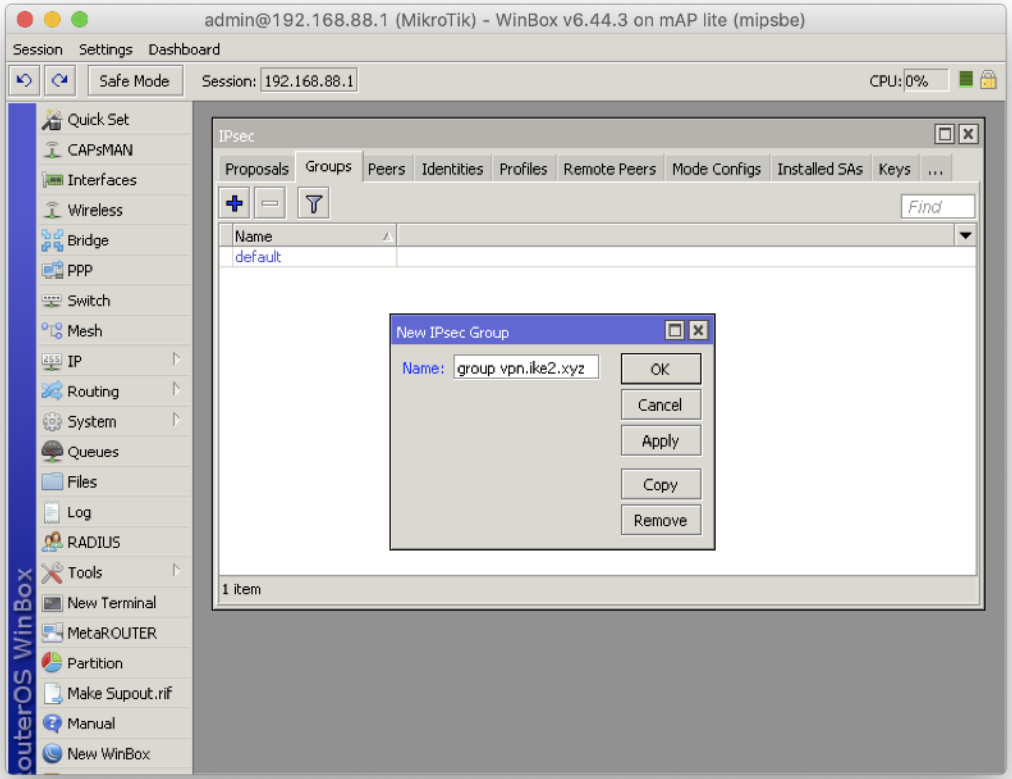
```
/ip ipsec peer add exchange-
mode=ike2 address=0.0.0.0/0
local-address=123.45.67.8
name="peer 123.45.67.8"
passive=yes send-initial-
contact=yes profile="profile
vpn.ike2.xyz"
```

# 4. Настройка нового IPSec proposal *(фаза 2)*



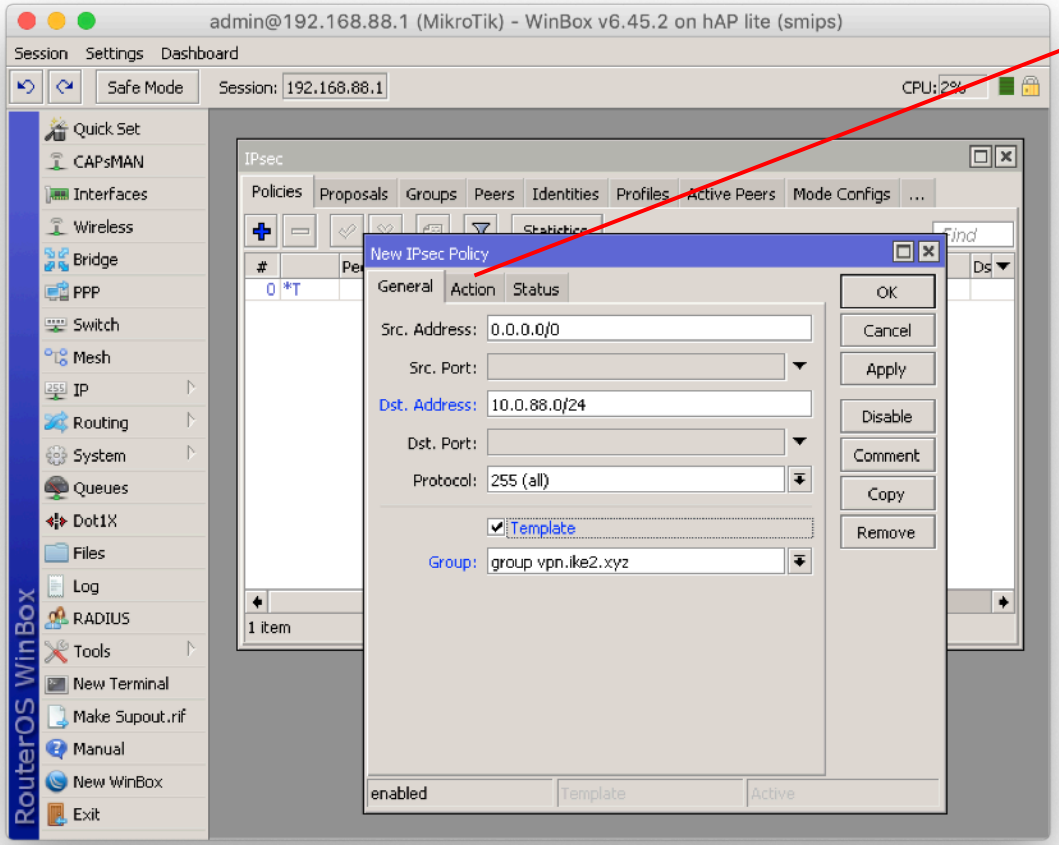

```
/ip ipsec proposal add auth-
algorithms=sha512,sha256,sha1
enc-algorithms=aes-256-
cbc,aes-256-ctr,aes-256-
gcm,aes-192-ctr,aes-192-
gcm,aes-128-cbc,aes-128-
ctr,aes-128-gcm lifetime=8h
name="proposal vpn.ike2.xyz"
pfs-group=none
```

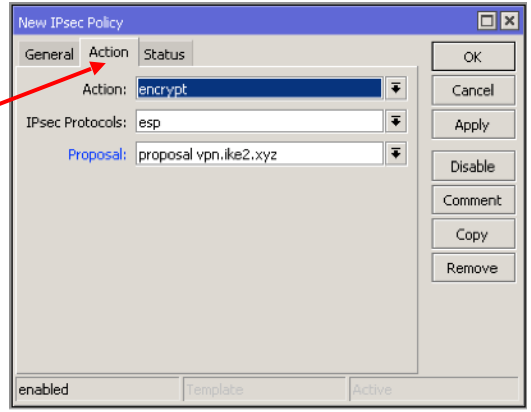
# 5. Добавление новой IPSec policy group




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

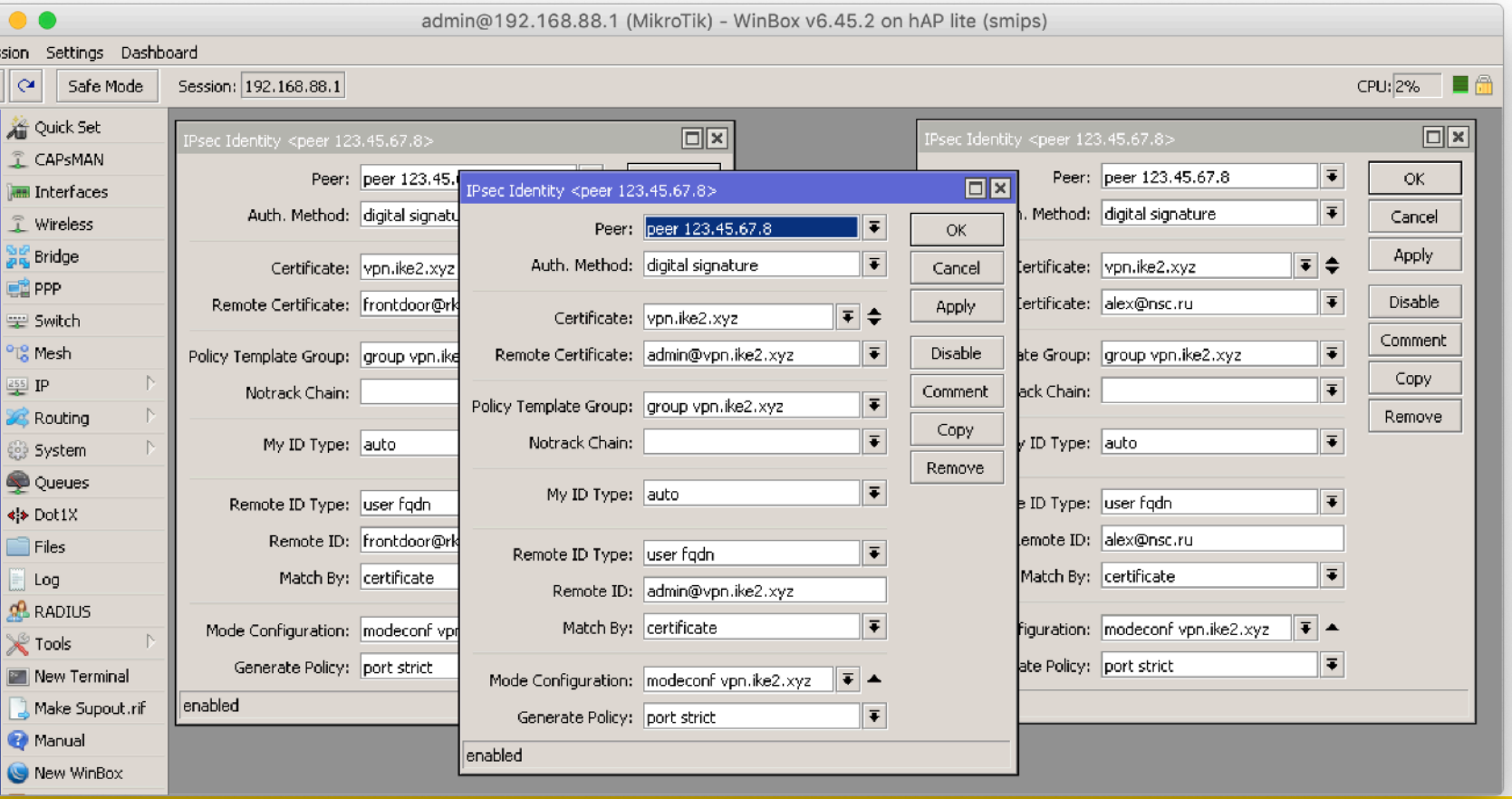
# 6. Настройка нового шаблона IPSec policy



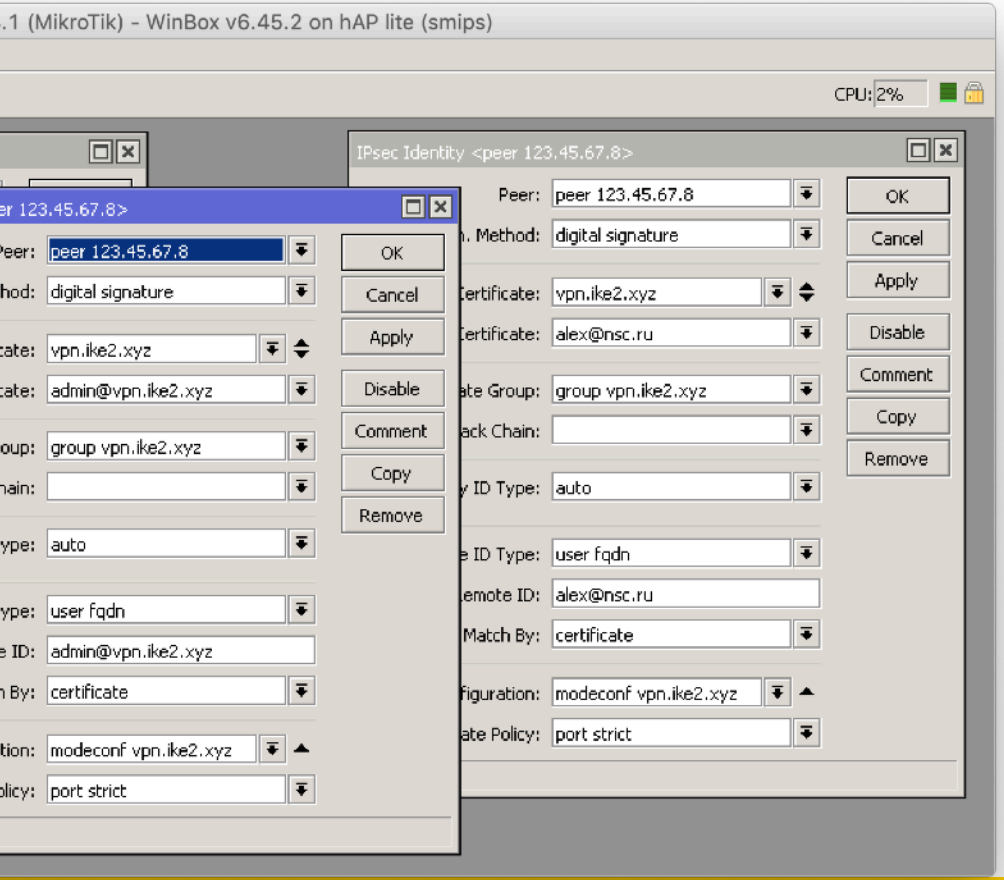

```
/ip ipsec policy add template=yes
dst-address=10.0.88.0/24
protocol=all src-address=0.0.0.0/0
group="group vpn.ike2.xyz"
proposal="proposal vpn.ike2.xyz"
ipsec-protocols=esp action=encrypt
```

# 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

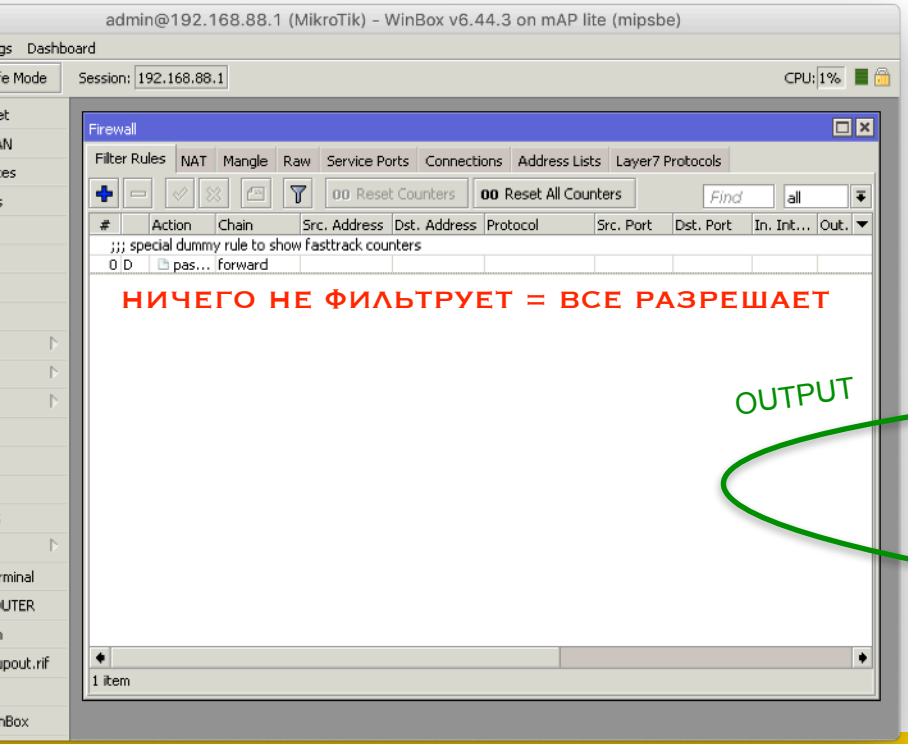
Nikita Tarikin / nikita@tarikin.com

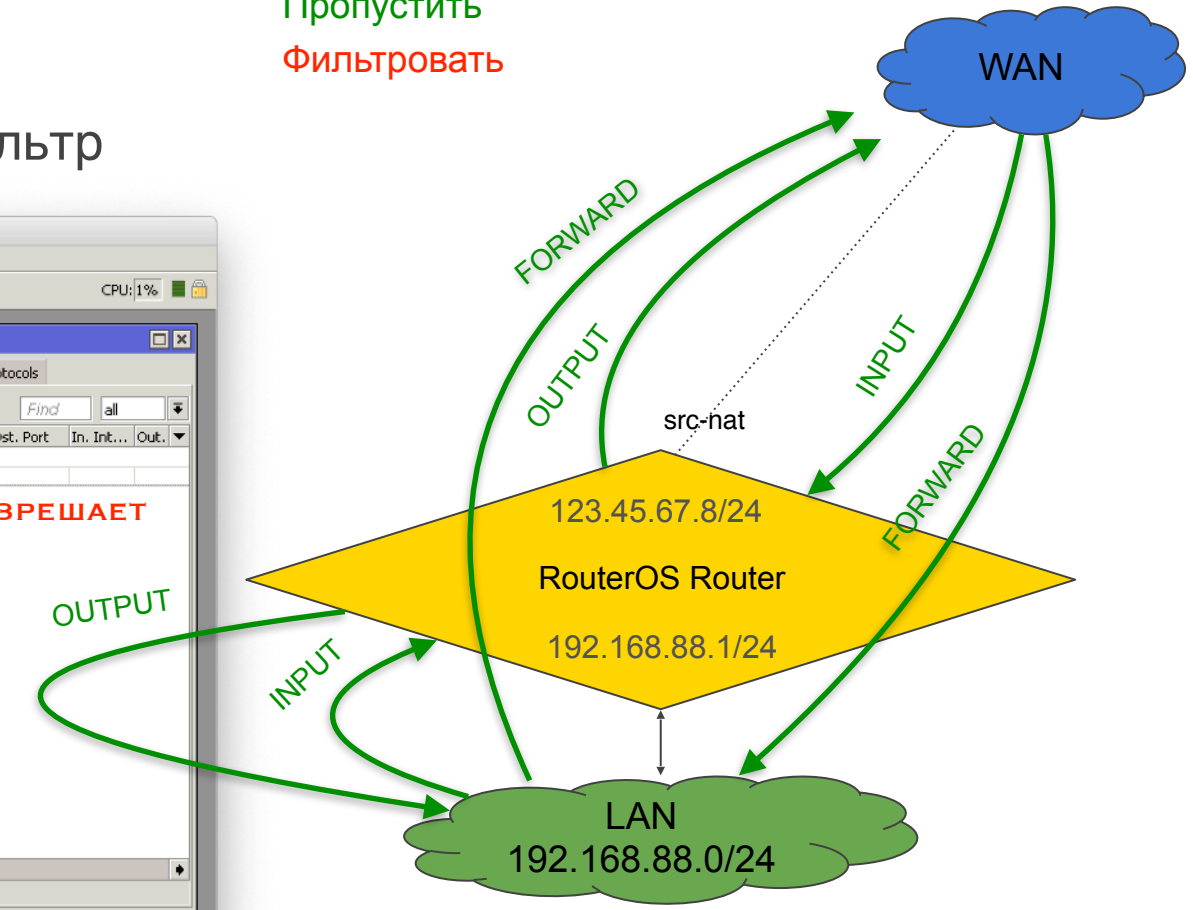
АХТУНГ

# Пустой FIREWALL фильтр

Пропустить

Фильтровать



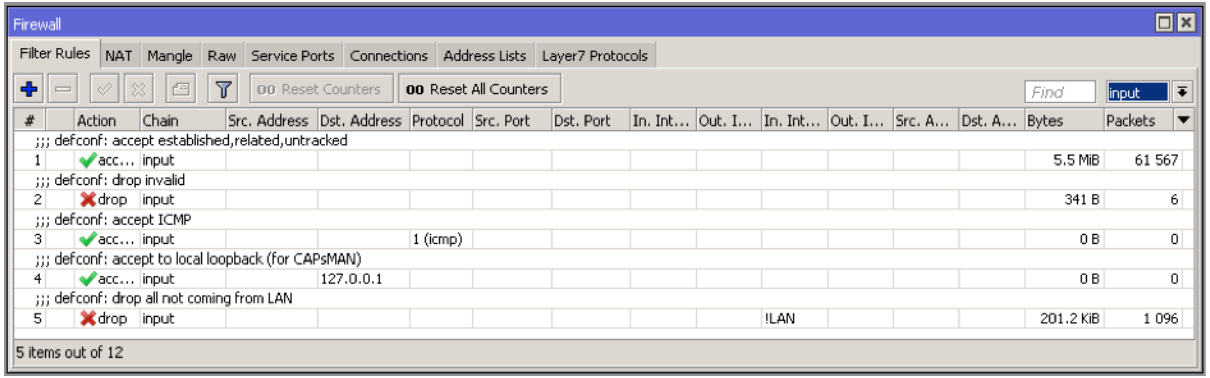



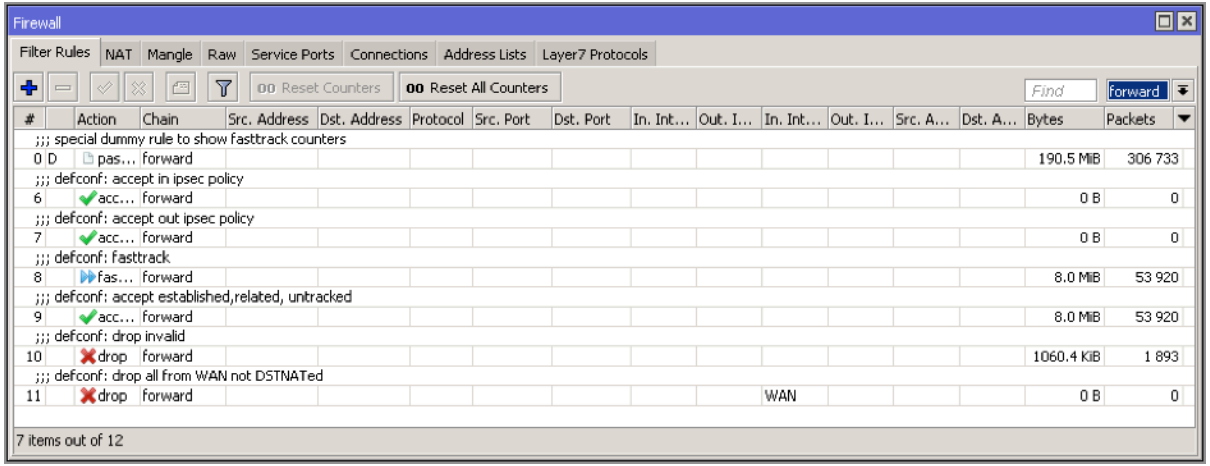
# Настройка Firewall

## Краткий обзор стандартного фильтра (MTCNA)

**Nikita Tarikin** / nikita@tarikin.com

# Краткий обзор стандартного Firewall фильтра RouterOS 6.45



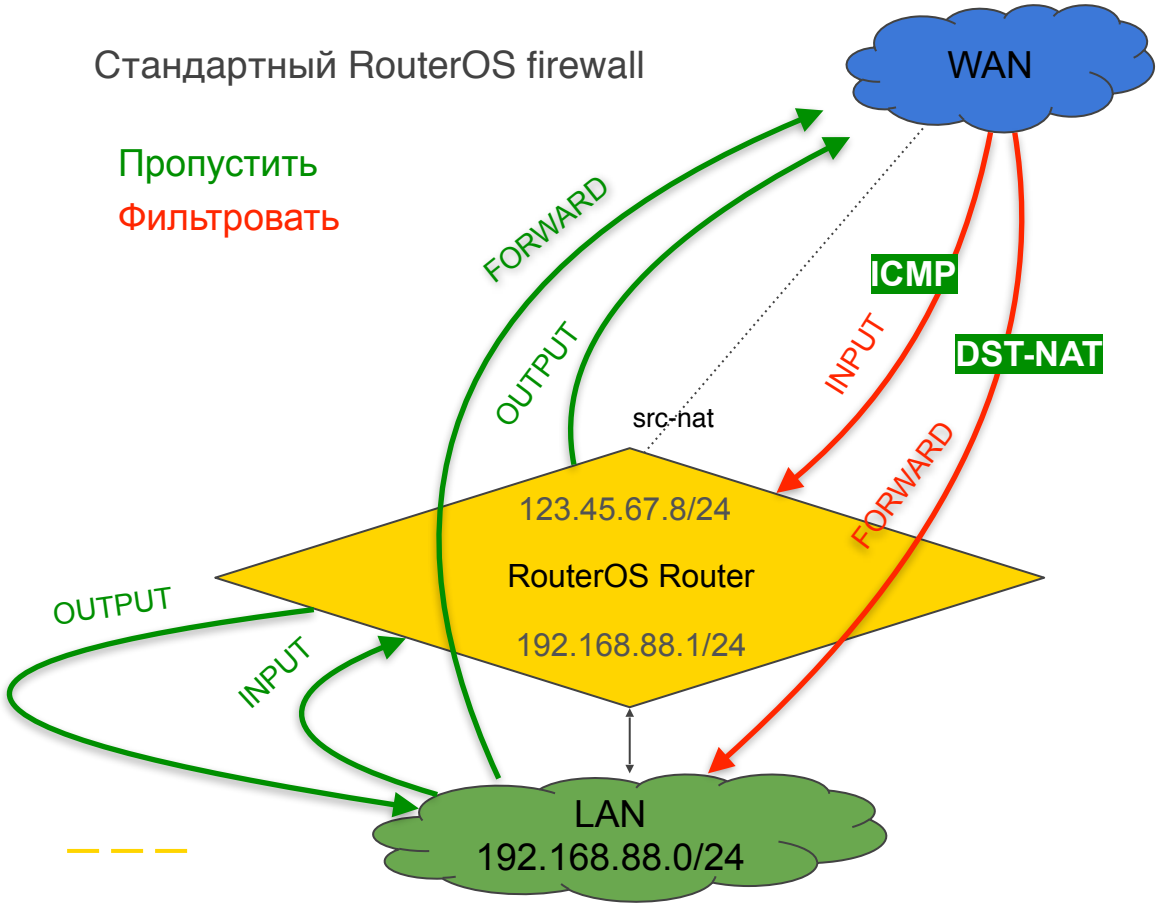



```
#Input Chain Rules
/ip firewall filter
add action=accept chain=input comment="defconf: accept established,related,untracked" connection-
state=established,related,untracked
add action=drop chain=input comment="defconf: drop invalid" connection-state=invalid
add action=accept chain=input comment="defconf: 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

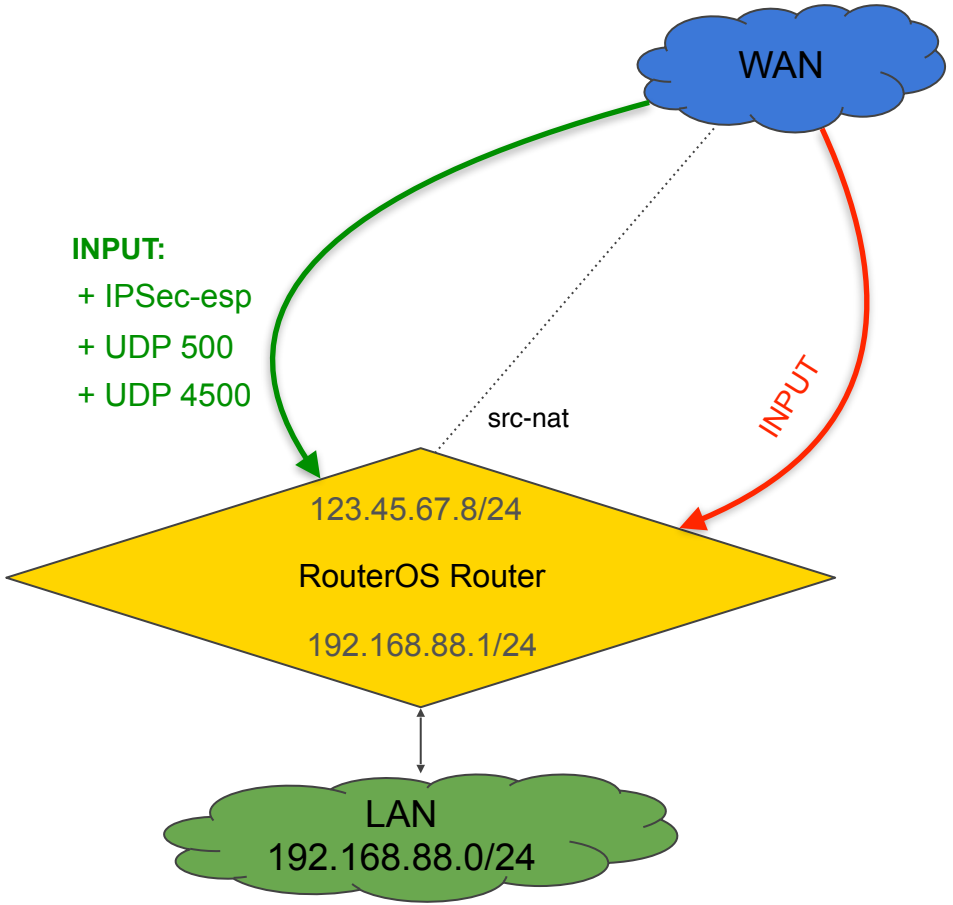
1. **Обзор стандартного фильтра**
2. Правила для подключения к роутеру через IPSec
3. Правила для трафика через VPN соединение




Nikita Tarikin / nikita@tarikin.com

# Настройка Firewall

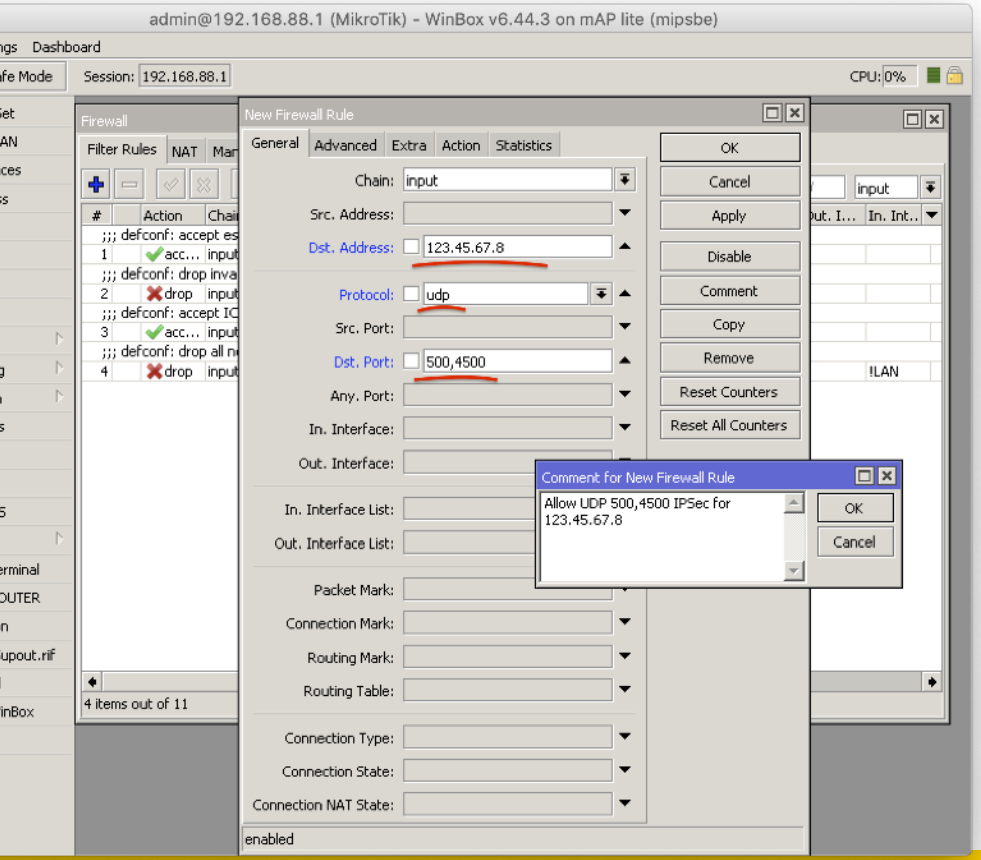
1. Обзор стандартного фильтра
2. **Правила для подключения к роутеру через IPSec**
3. Правила для трафика через VPN соединение




Nikita Tarikin / nikita@tarikin.com

# Правила фильтра firewall для IPSec трафика (defconf)

**INPUT chain**

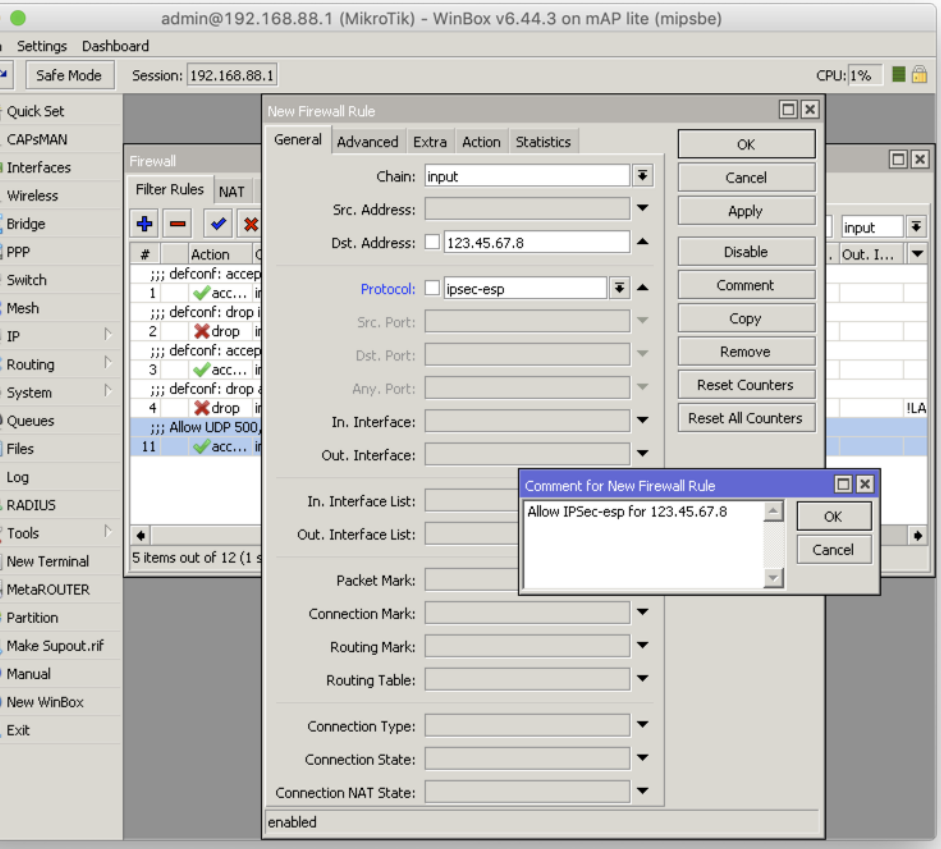



**+ UDP 500**
**+ UDP 4500**

```
/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**



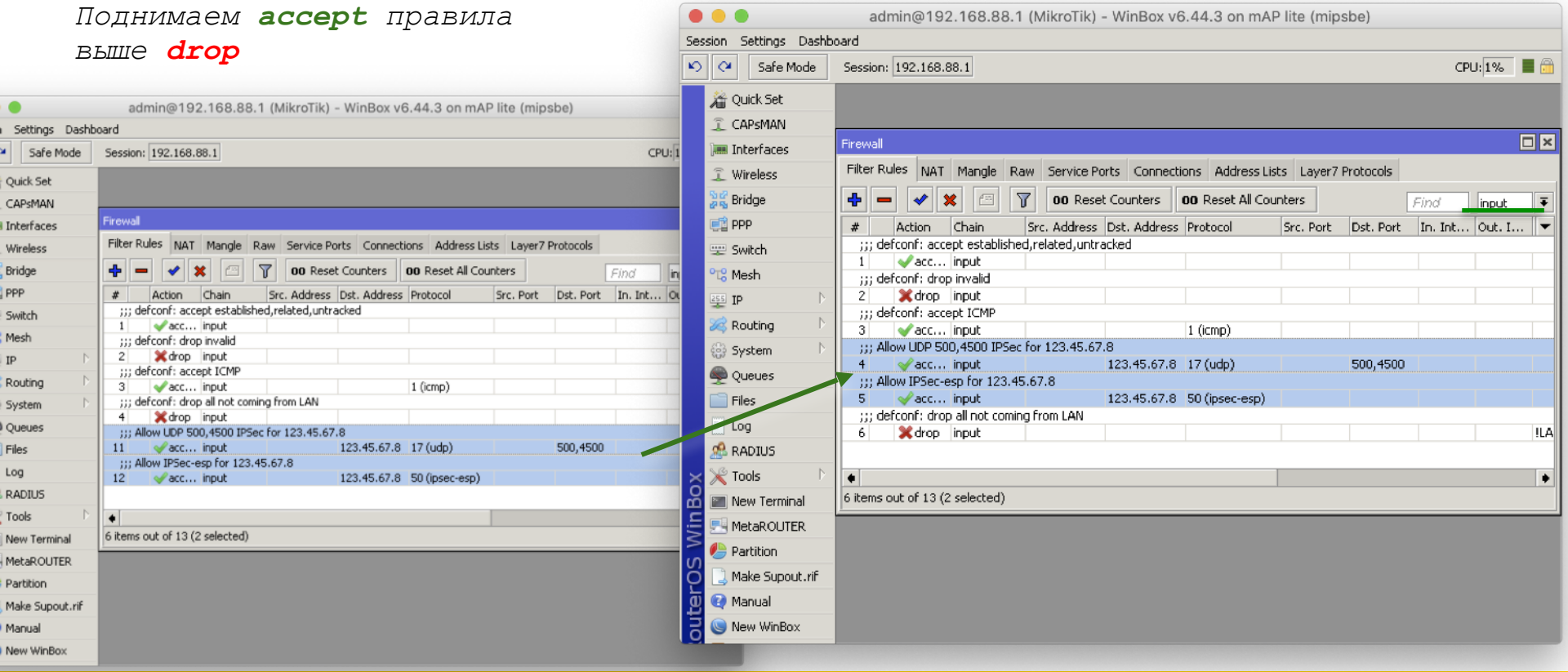

**+ IPSec-esp** (protocol 50)

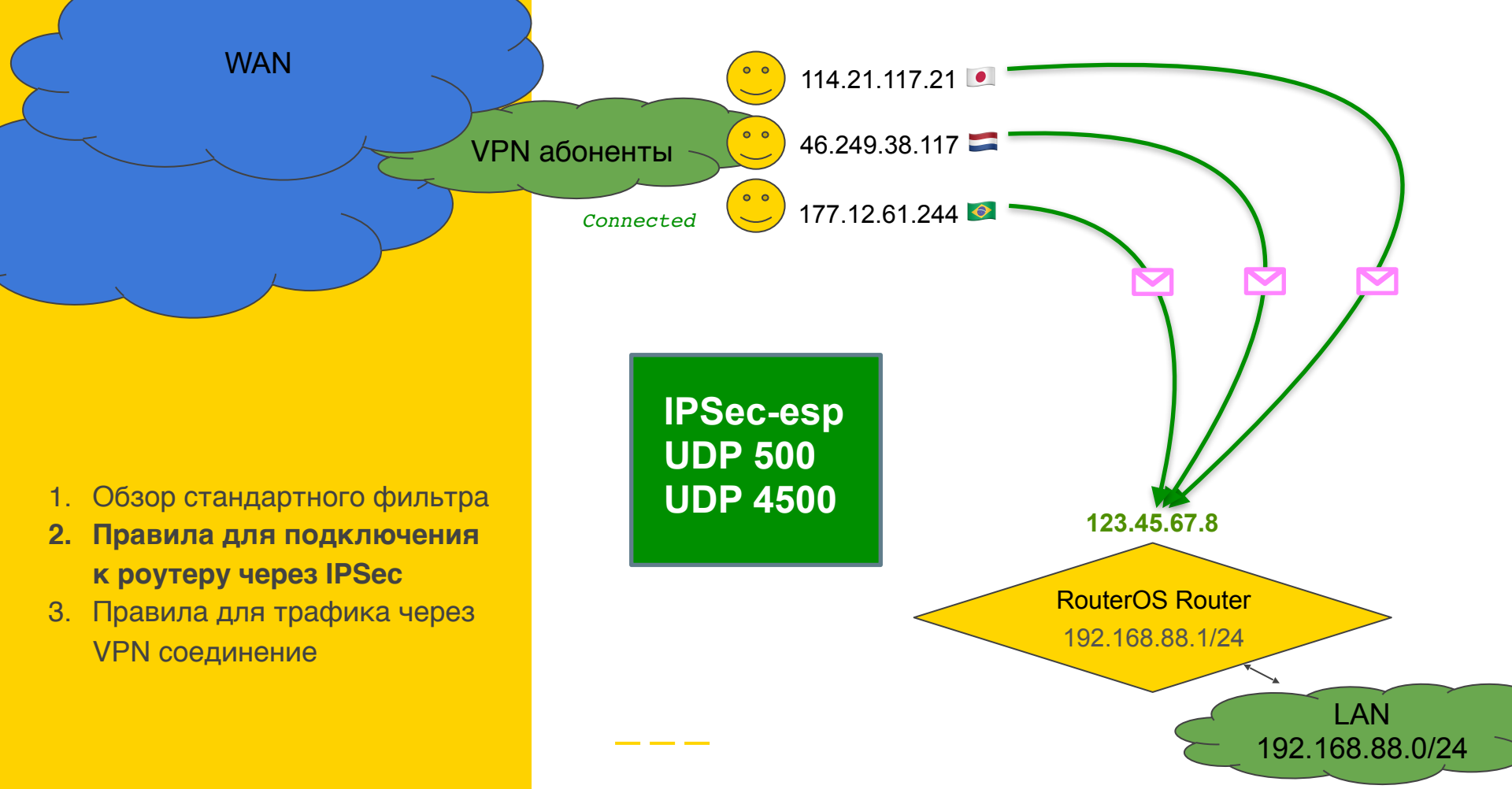
```
/ip firewall filter add place-
before=[ find where
comment~"defconf: drop all not
coming from LAN" ] protocol=ipsec-
esp dst-address=123.45.67.8
action=accept  chain=input
comment="Allow IPSec-esp for
123.45.67.8"
```

# Порядок правил фильтра firewall для IPSec трафика (defconf)

**INPUT chain**

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






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

Nikita Tarikin / nikita@tarikin.com

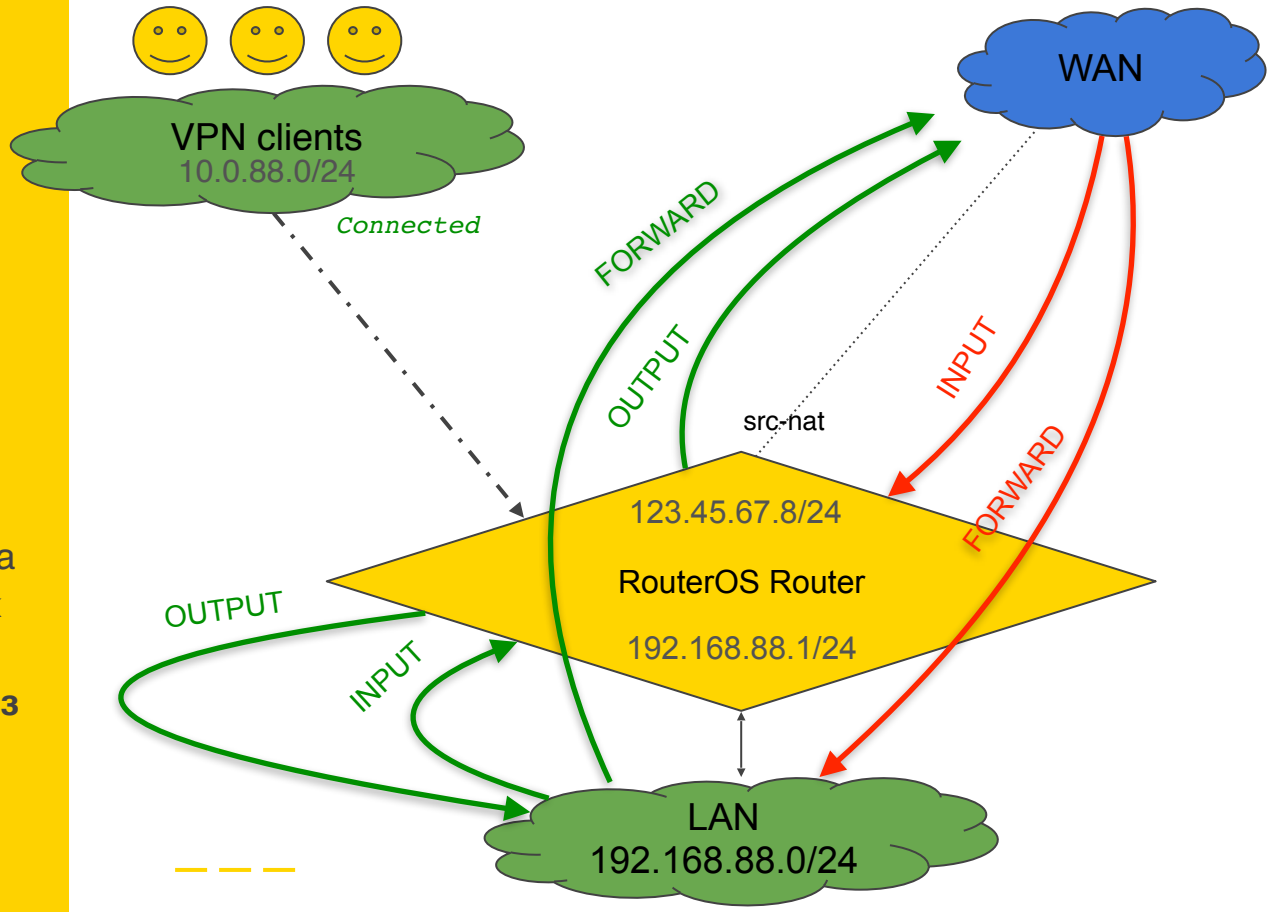
# Настройка Firewall

## Правила для трафика через VPN соединение

**Nikita Tarikin** / nikita@tarikin.com

# Настройка Firewall

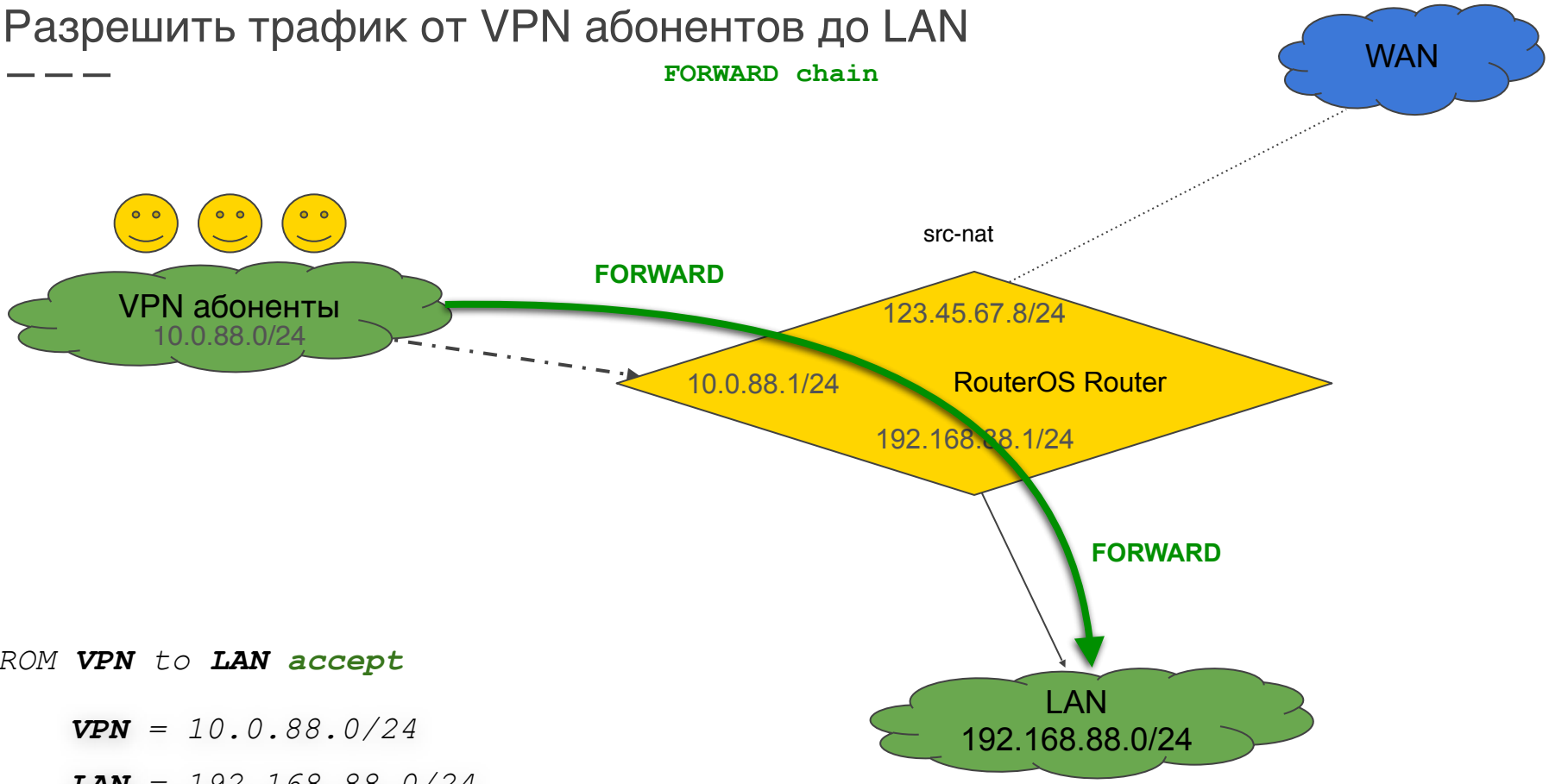
1. Обзор стандартного фильтра
2. Правила для подключения к роутеру через IPSec
3. **Правила для трафика через VPN соединение**




Nikita Tarikin / nikita@tarikin.com

# Разрешить трафик от VPN абонентов до LAN

**FORWARD chain**



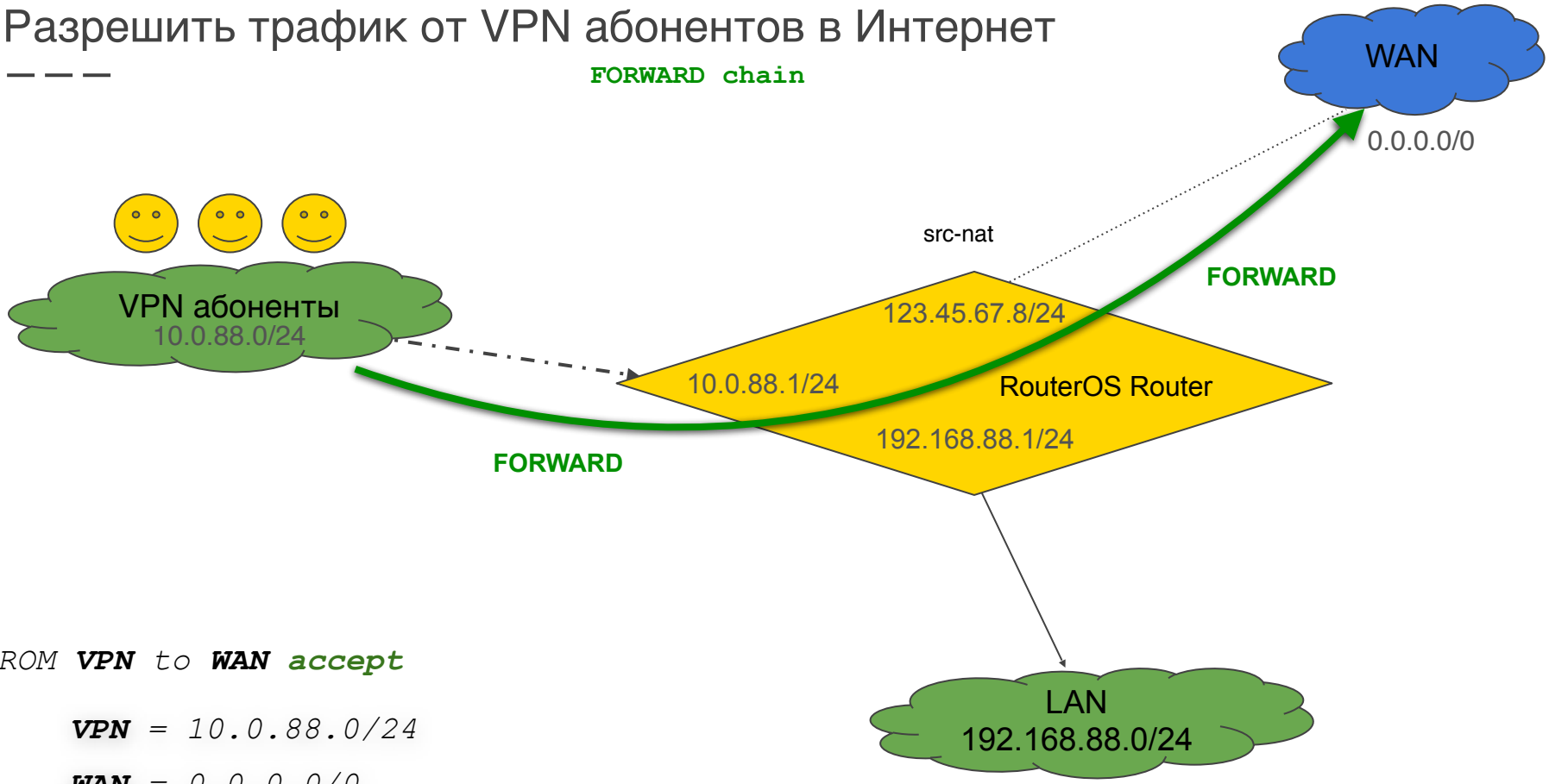

*FROM **VPN** to **LAN** accept*

***VPN** = 10.0.88.0/24*

***LAN** = 192.168.88.0/24*

# Разрешить трафик от VPN абонентов в Интернет

**FORWARD chain**



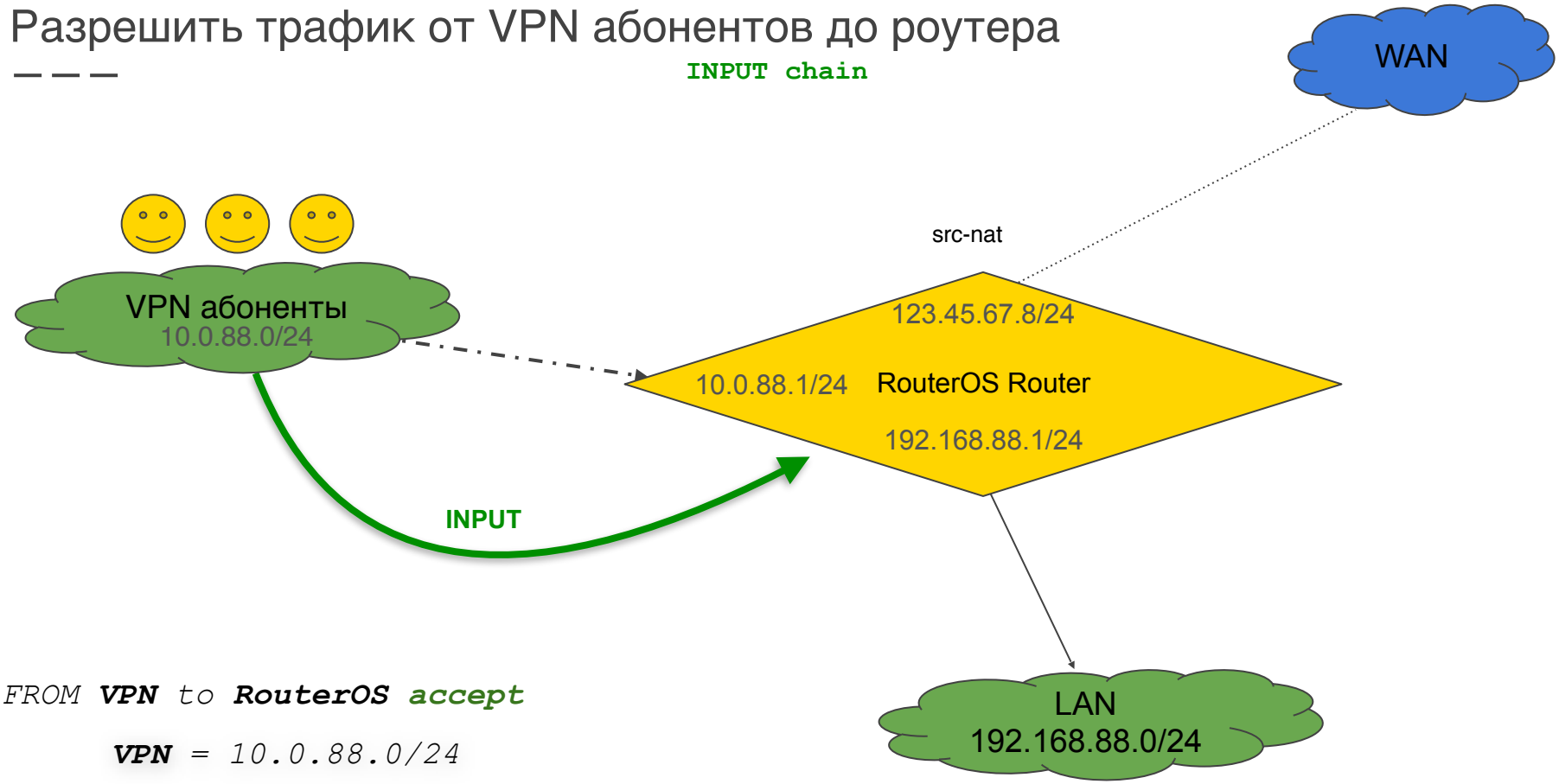

*FROM **VPN** to **WAN** accept*

***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*

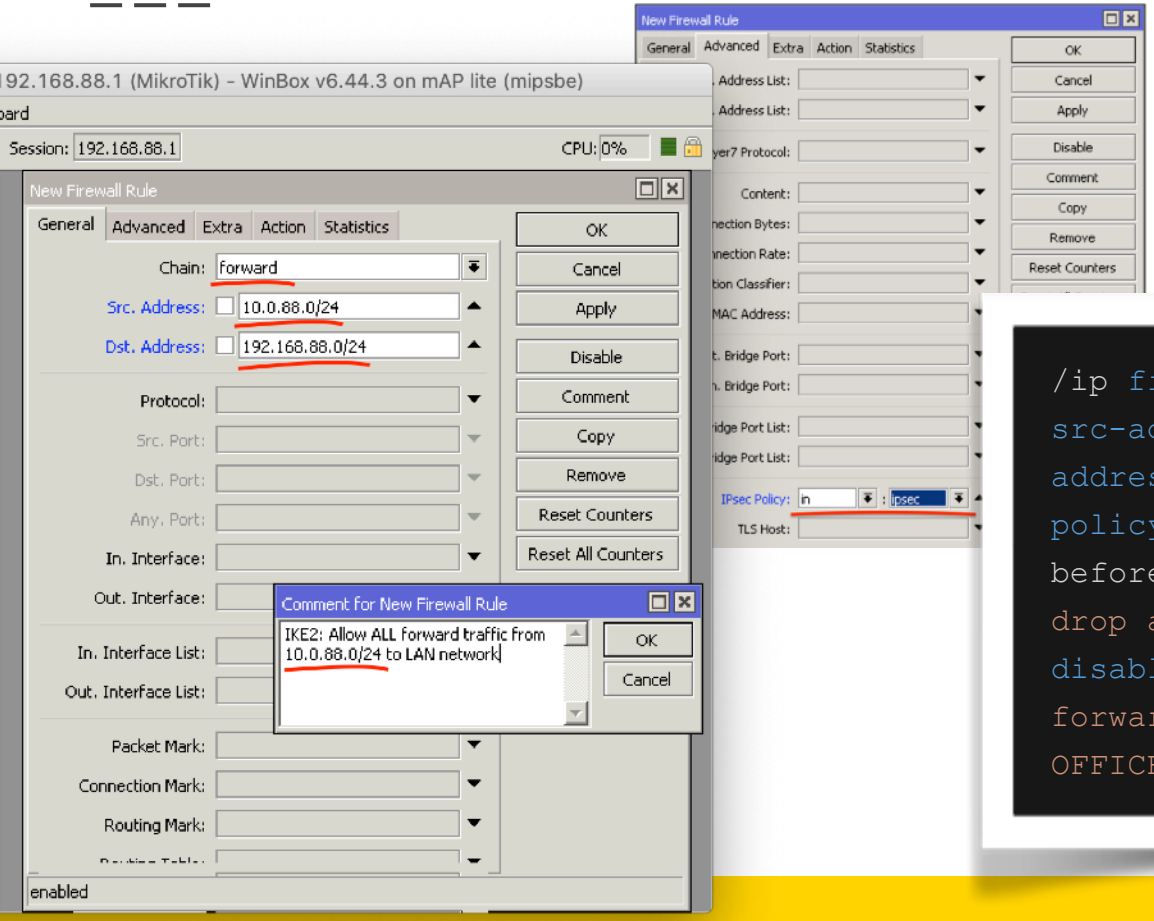
# Правила от VPN абонентов до LAN сети

**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"
```

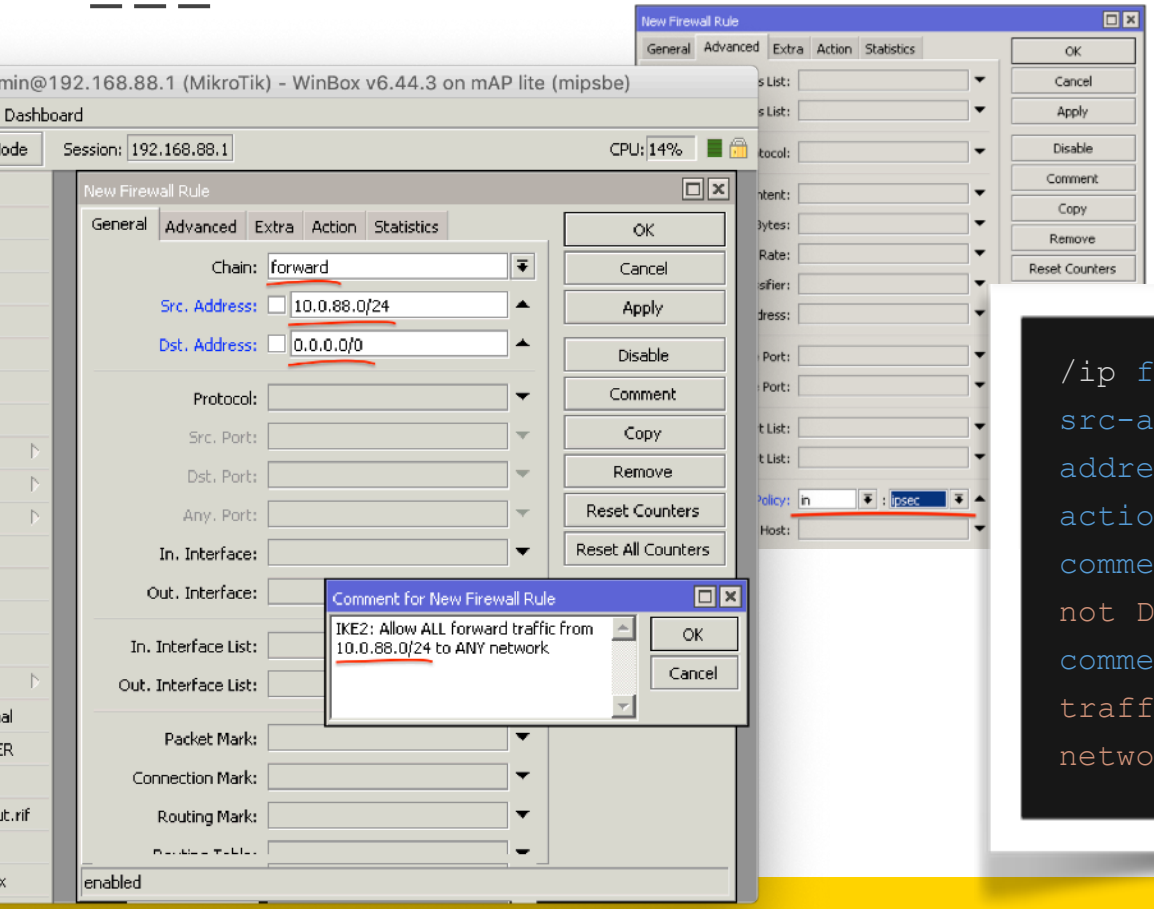
# Правила от VPN абонентов до WAN

**FORWARD chain**

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

***VPN** = 10.0.88.0/24*

***WAN** = 0.0.0.0/0*



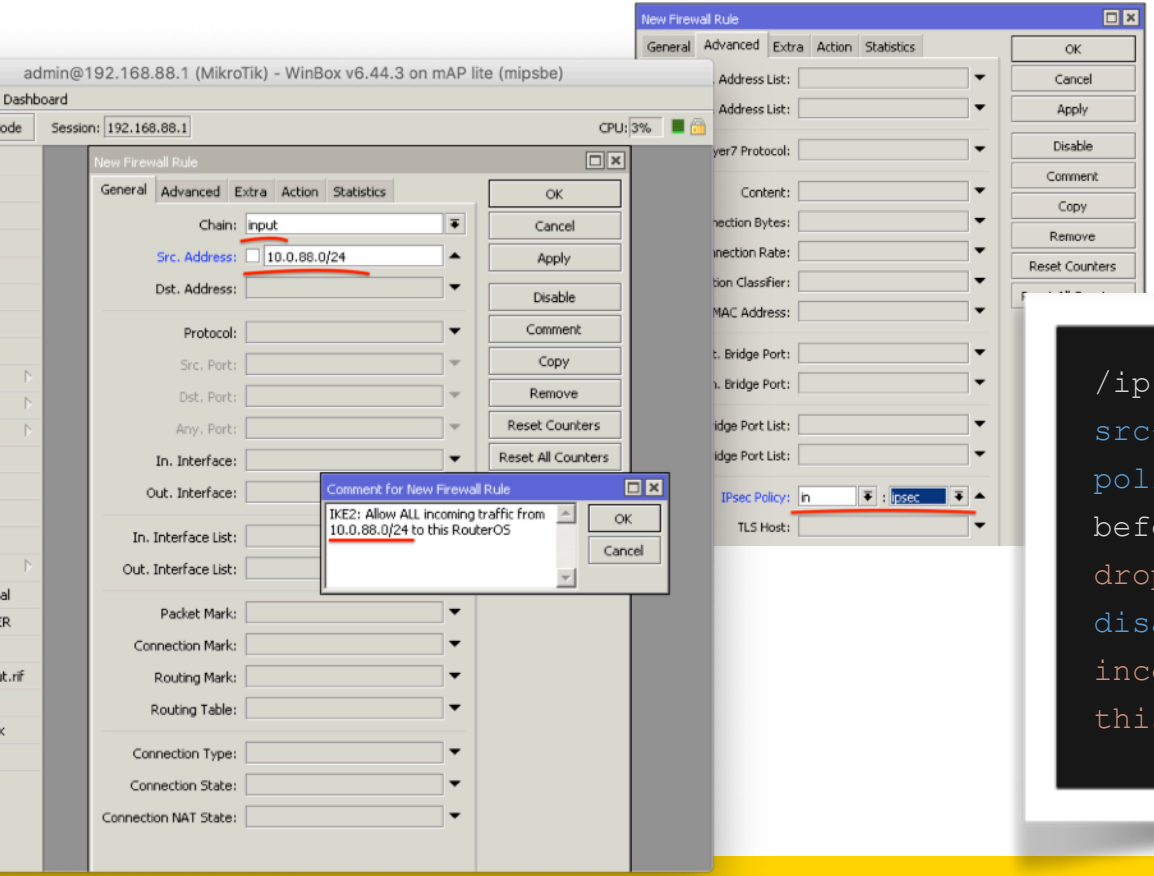

```
/ip firewall filter add chain=forward
src-address=10.0.88.0/24 dst-
address=0.0.0.0/0 ipsec-policy=in,ipsec
action=accept place-before=[ find where
comment~"defconf:  drop all from WAN
not DSTNATed" ] disabled=no
comment="IKE2: Allow ALL forward
traffic from 10.0.88.0/24 to ANY
network"
```

# Правила от VPN абонентов до RouterOS

**INPUT chain**

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

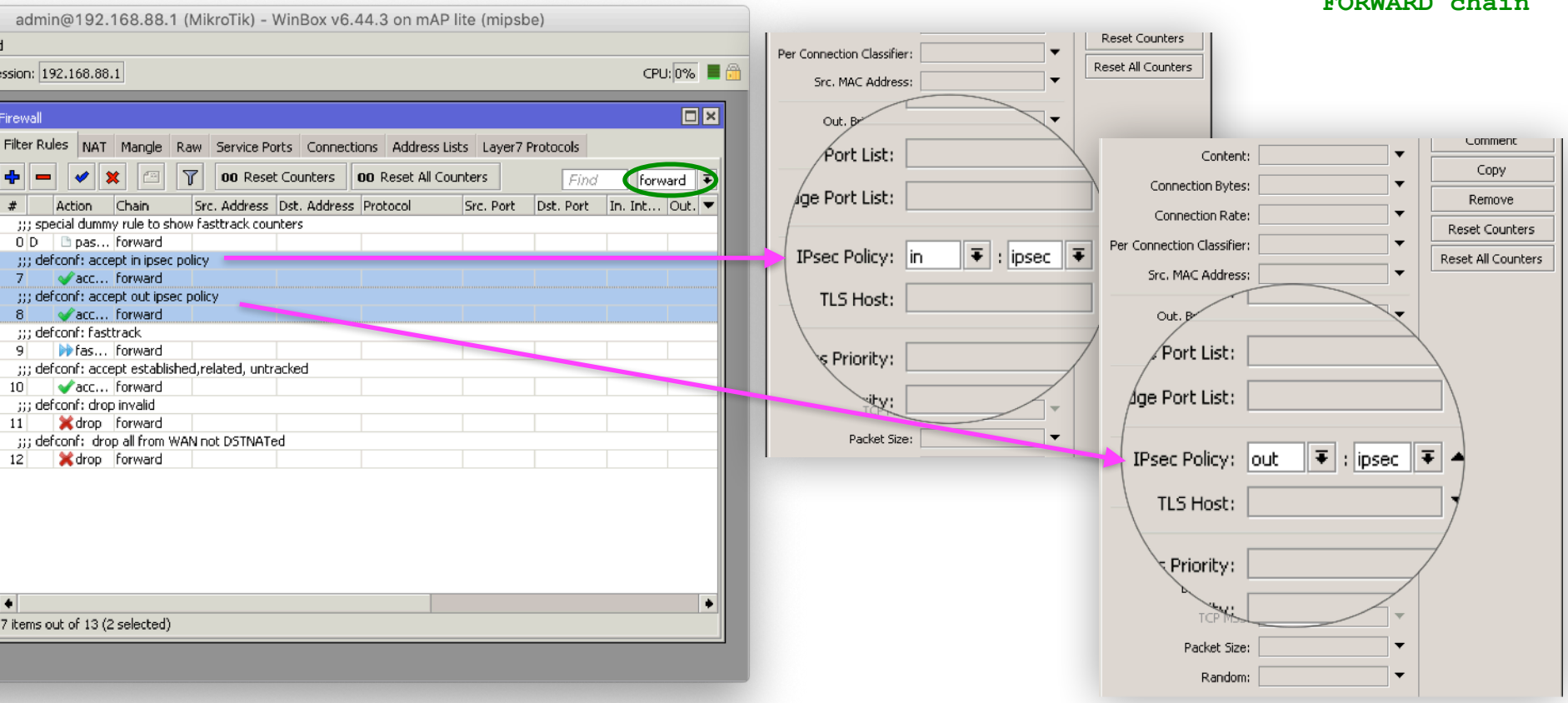
***VPN*** *= 10.0.88.0/24*

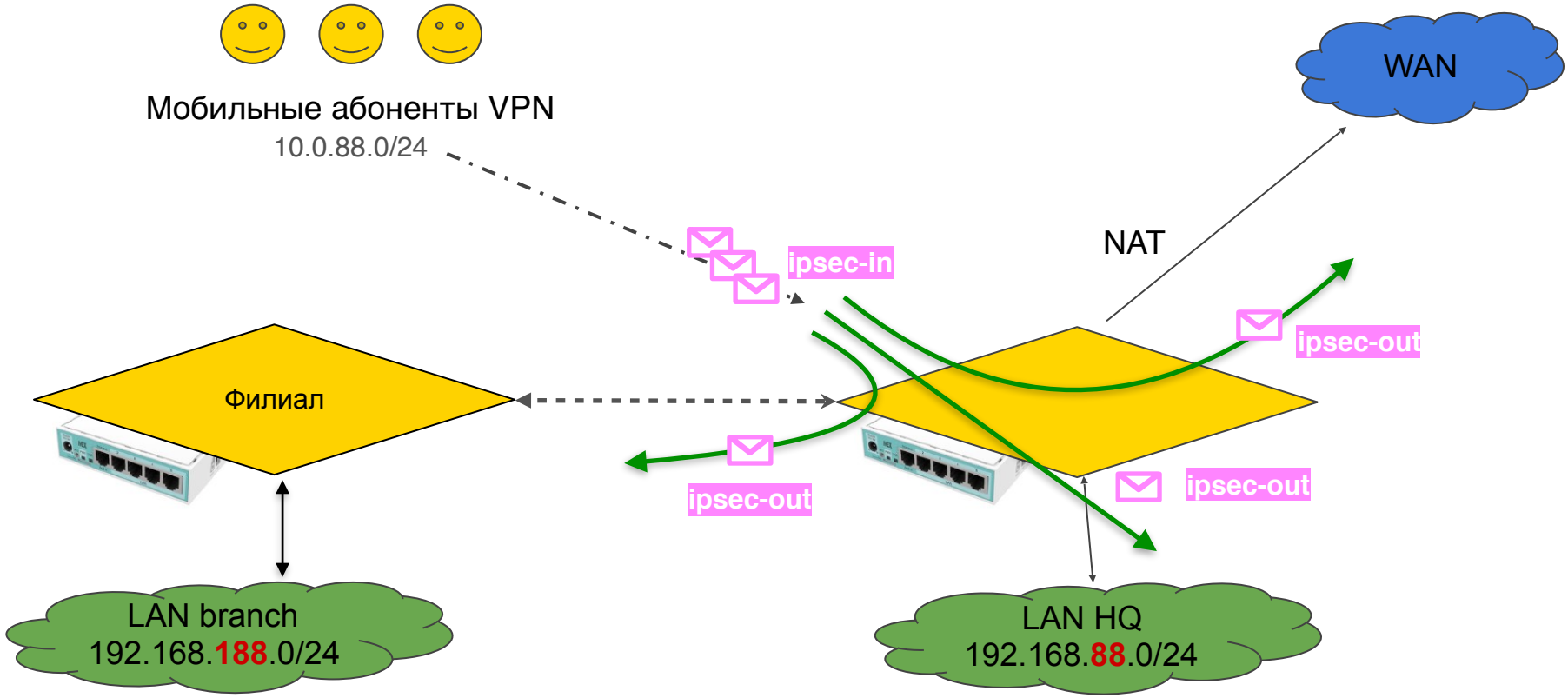



```
/ip firewall filter add chain=input
src-address=10.0.88.0/24 ipsec-
policy=in,ipsec action=accept place-
before=[ find where comment~"defconf:
drop all not coming from LAN" ]
disabled=no comment="IKE2: Allow ALL
incoming traffic from 10.0.88.0/24 to
this RouterOS"
```

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

**FORWARD chain**



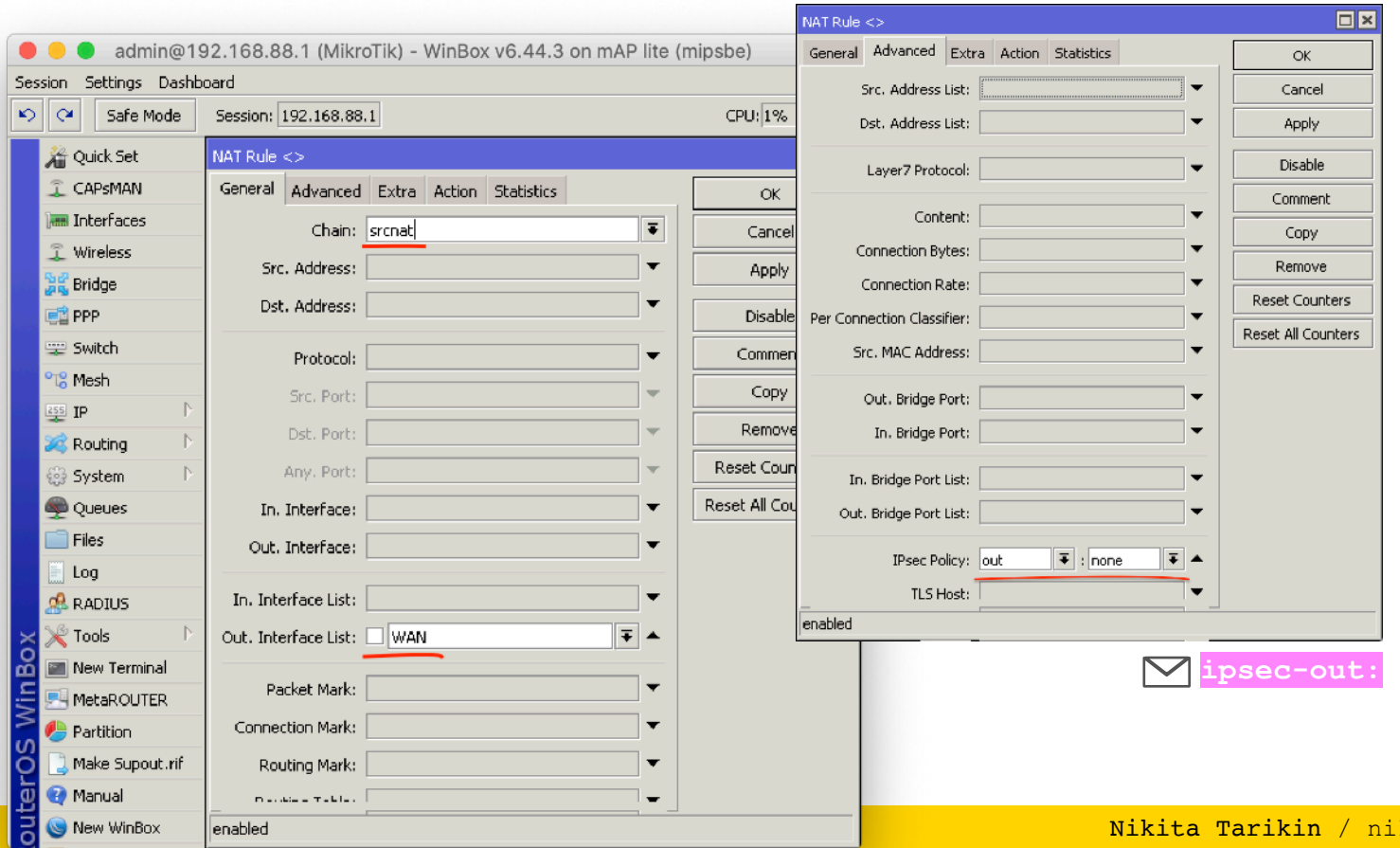



FORWARD chain

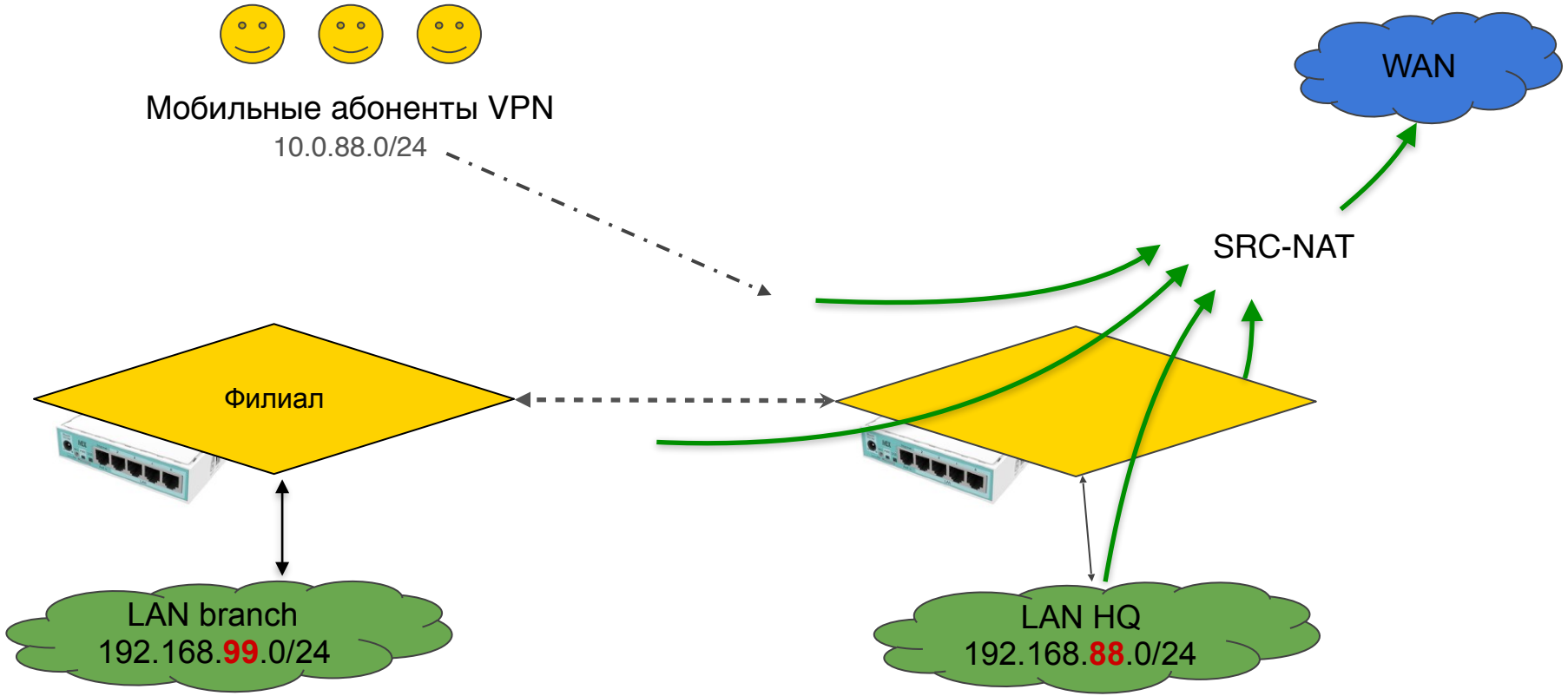
Стандартные правила Firewall для любого трафика в ipsec упаковке (defconf)

# Настройка NAT

# Обзор правила NAT стандартного Firewall (defconf)

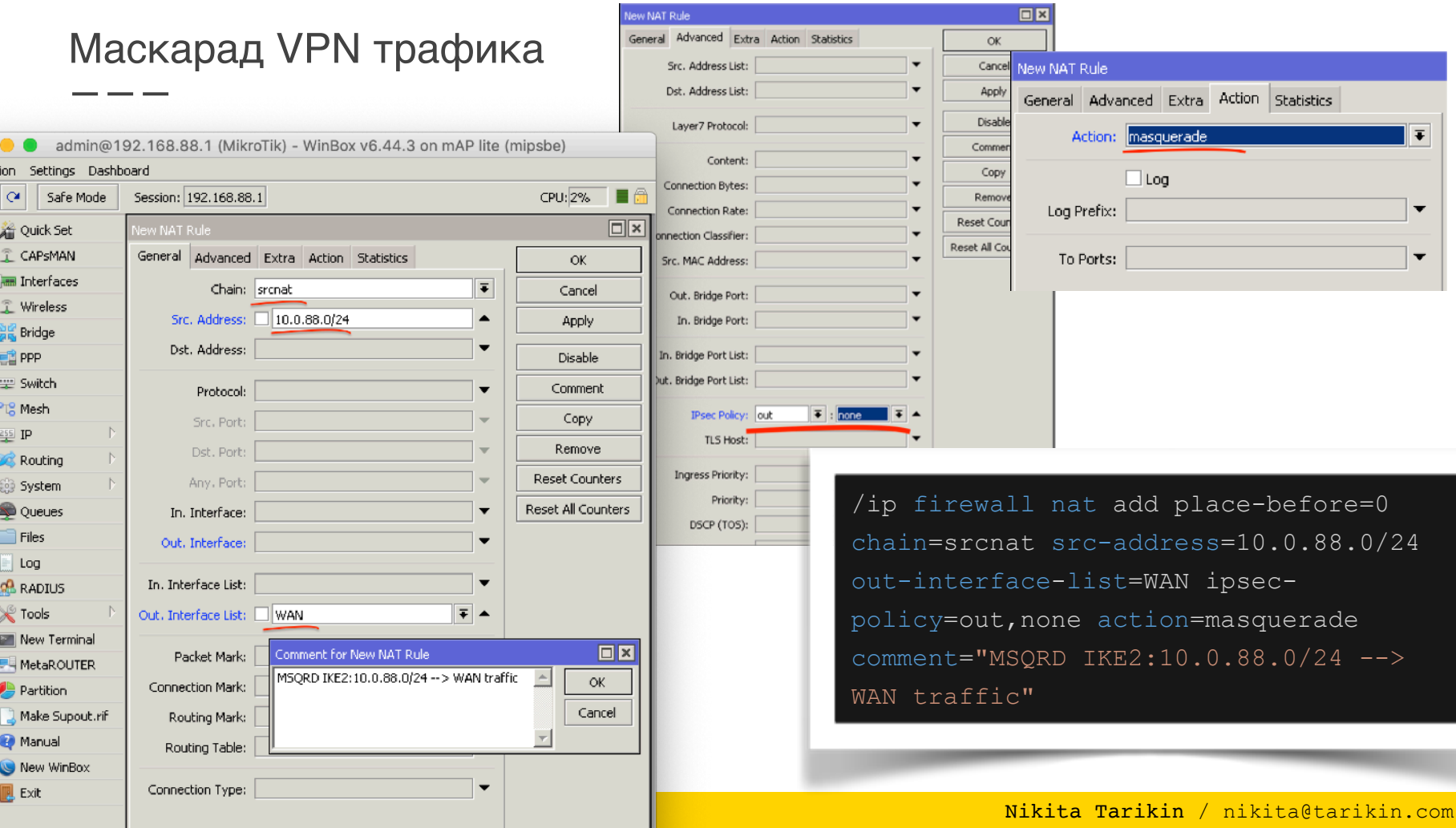



ipsec-out: none



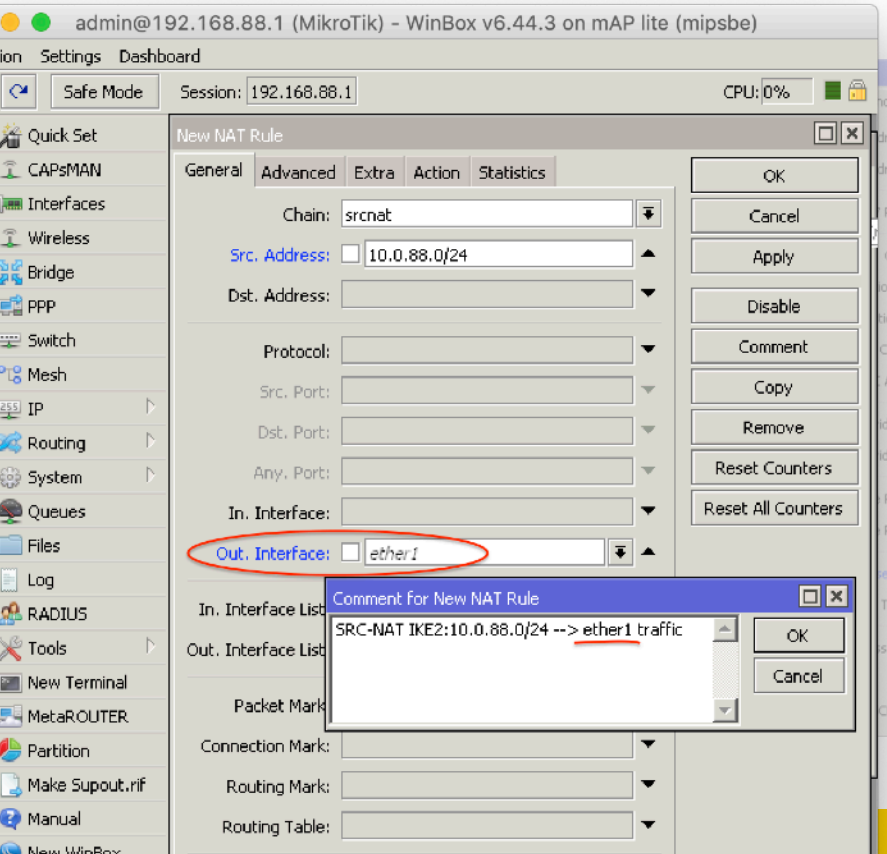

# Обзор правила NAT стандартного Firewall (defconf)

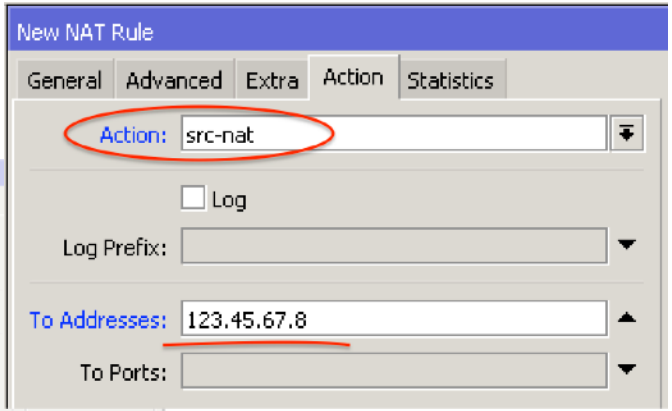
# Маскарад VPN трафика




```
/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"
```

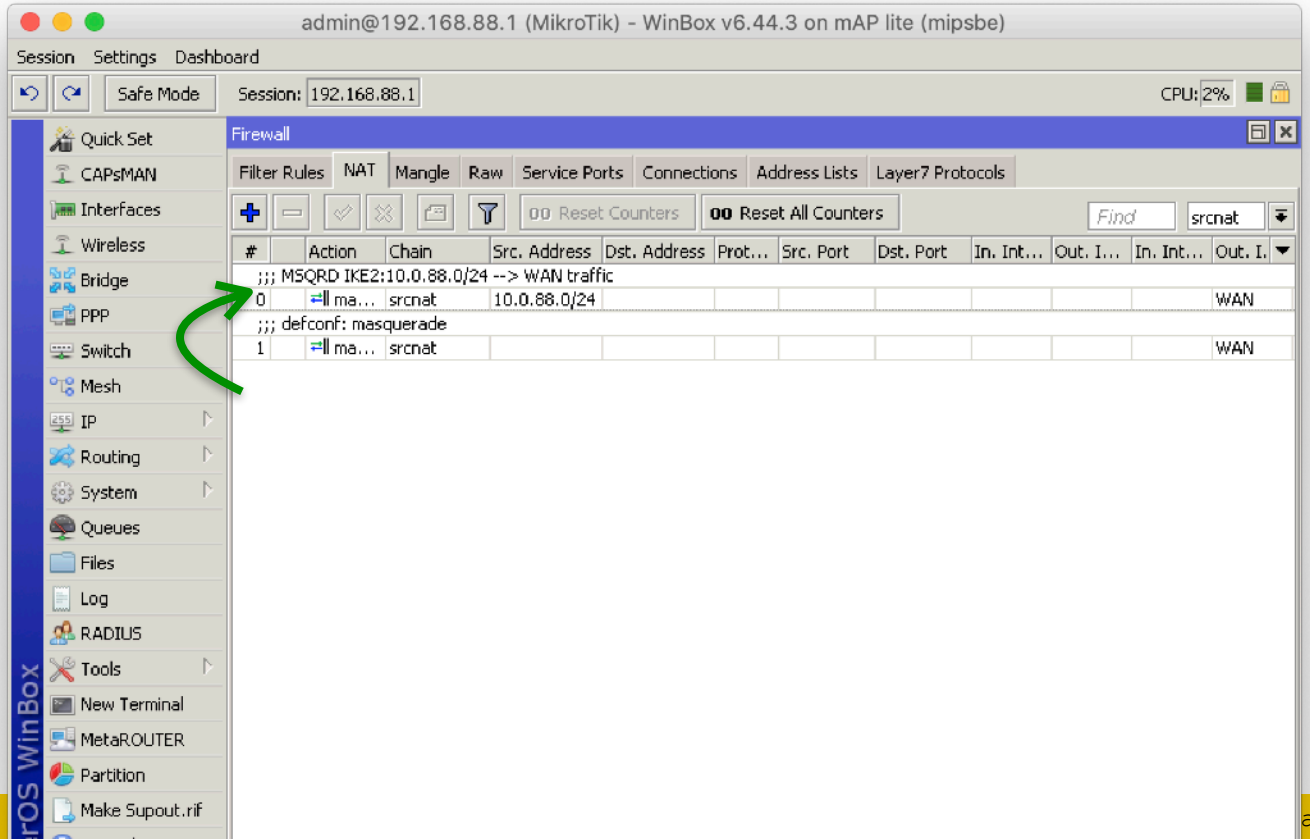
# SRC-NAT VPN трафика (рекомендуется)




```
/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



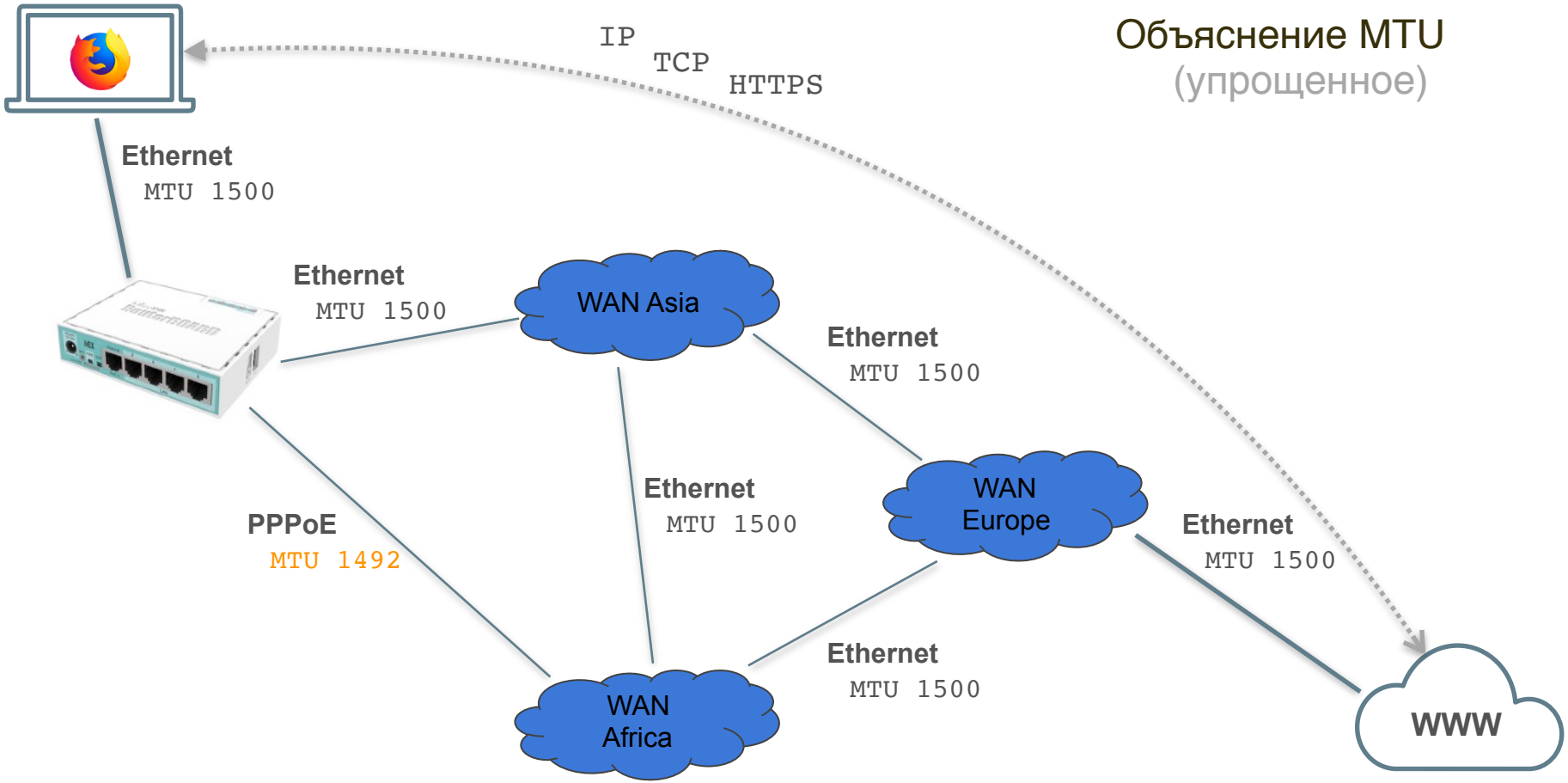
# Настройка TCP MSS

План действий

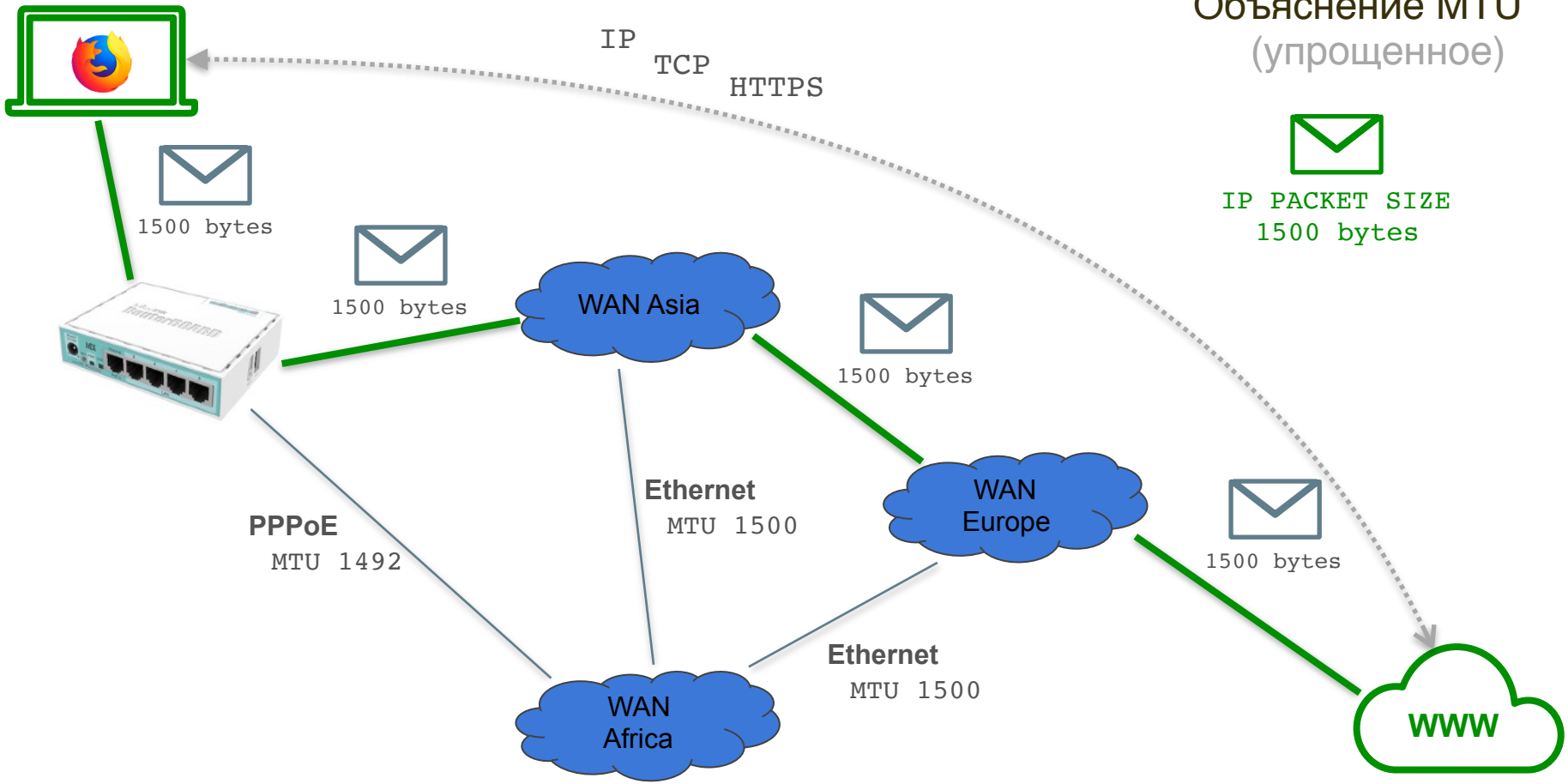
1. Объяснение MTU и фрагментации IP пакетов
2. Объяснение IPSec MTU
3. Объяснение TCP MSS
4. Настройка TCP MSS через IKE2

Nikita Tarikin / nikita@tarikin.com

# Объяснение MTU
(упрощенное)

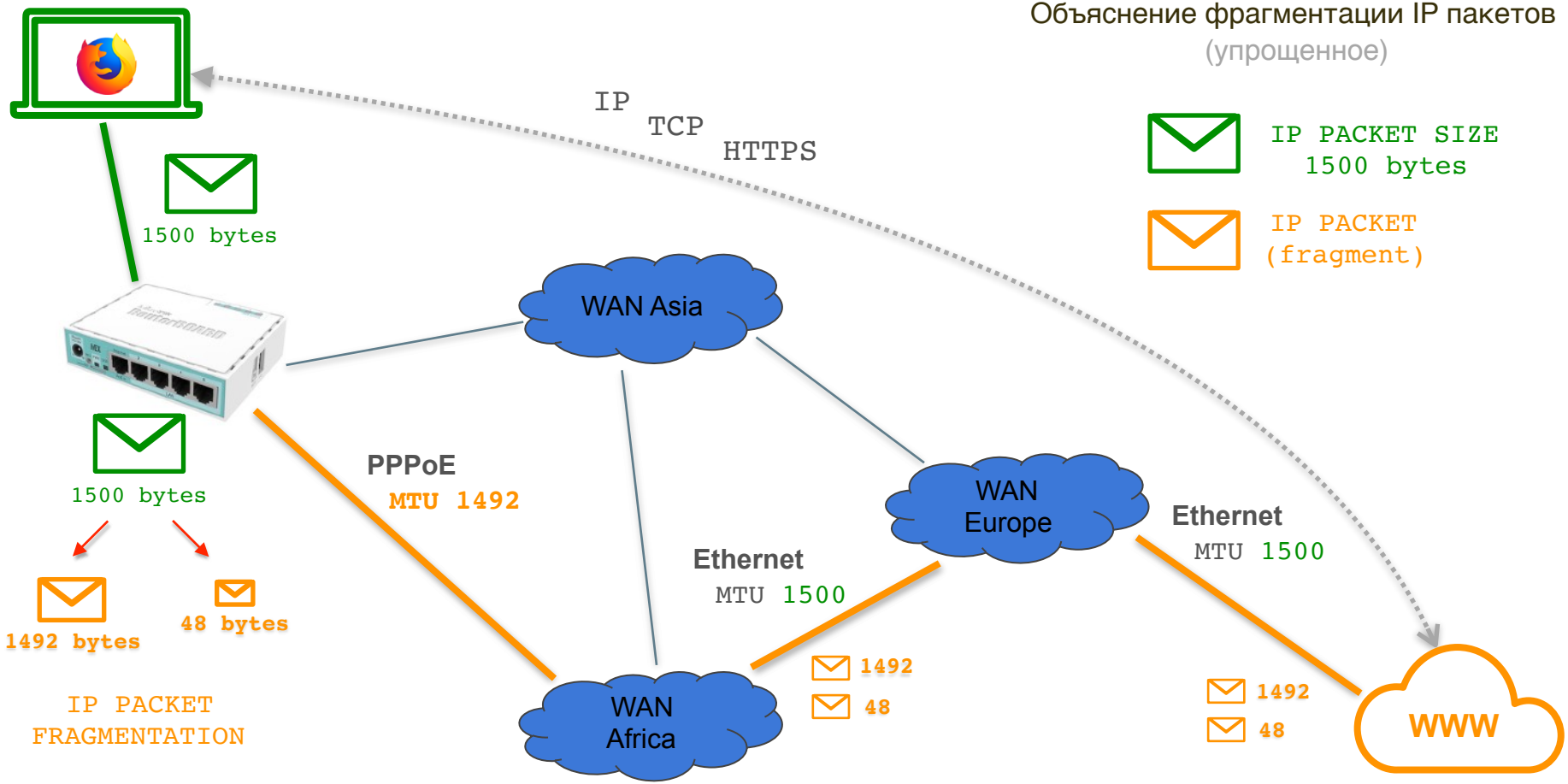


# Объяснение MTU
(упрощенное)

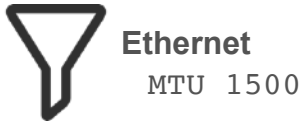


# Объяснение фрагментации IP пакетов

(упрощенное)



# Несоответствие MTU —> фрагментация IP пакетов



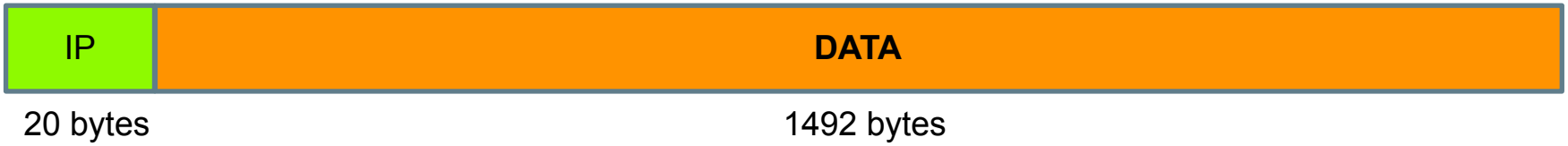




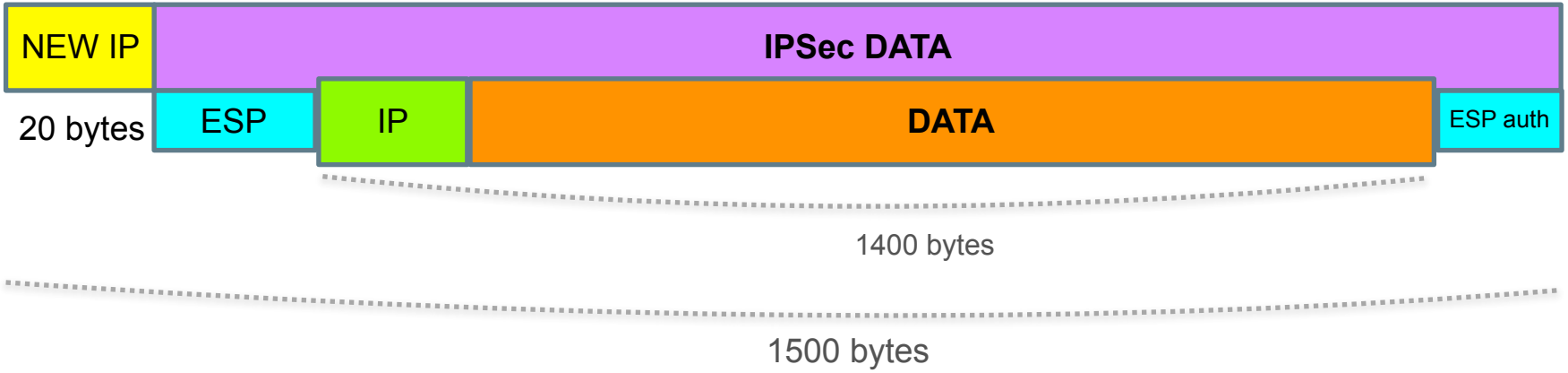


# Объяснение IPSec MTU (упрощенное)

**IP packet**

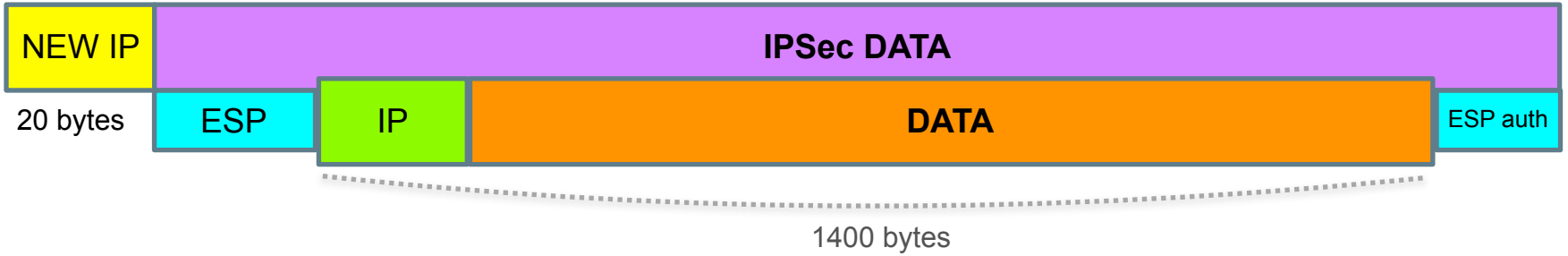



**IPSec ESP packet** *(tunnel mode)*

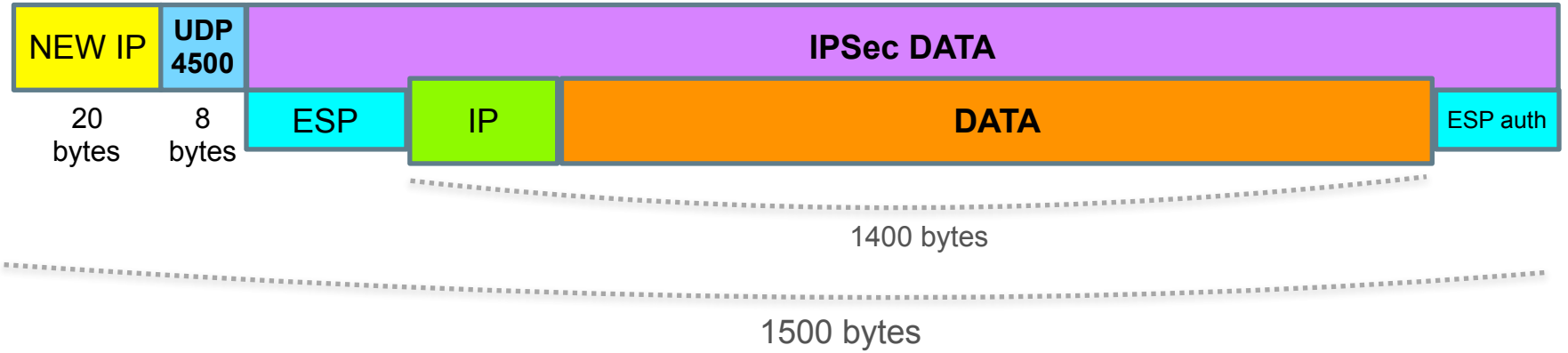


# Объяснение IPSec MTU (упрощенное)

**IPSec ESP packet** *(tunnel mode)*

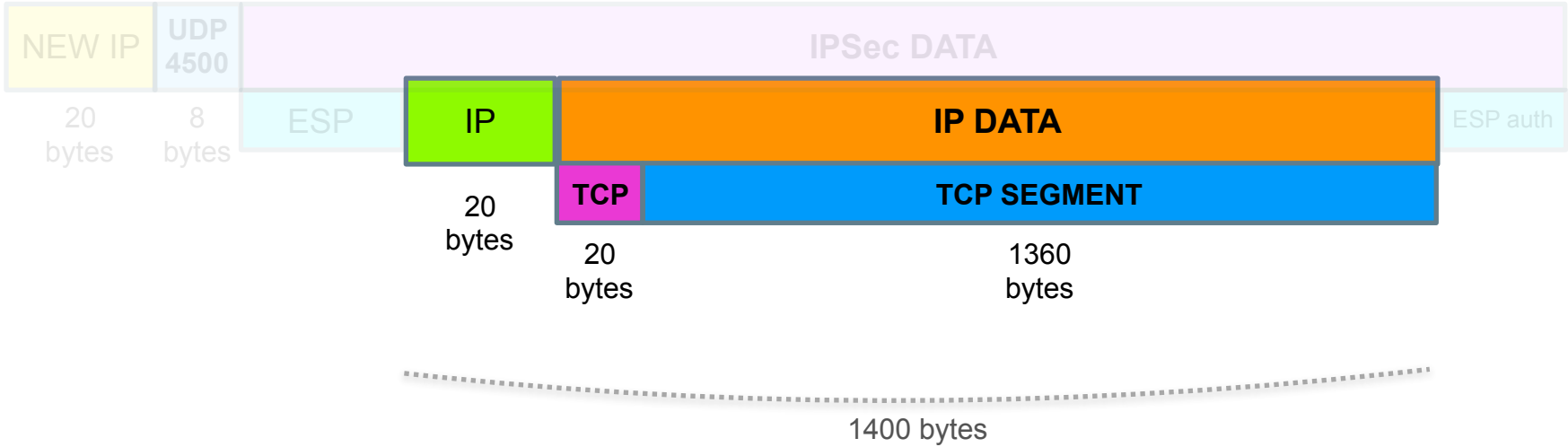



**IPSec ESP packet with NAT-T** *(tunnel mode)*



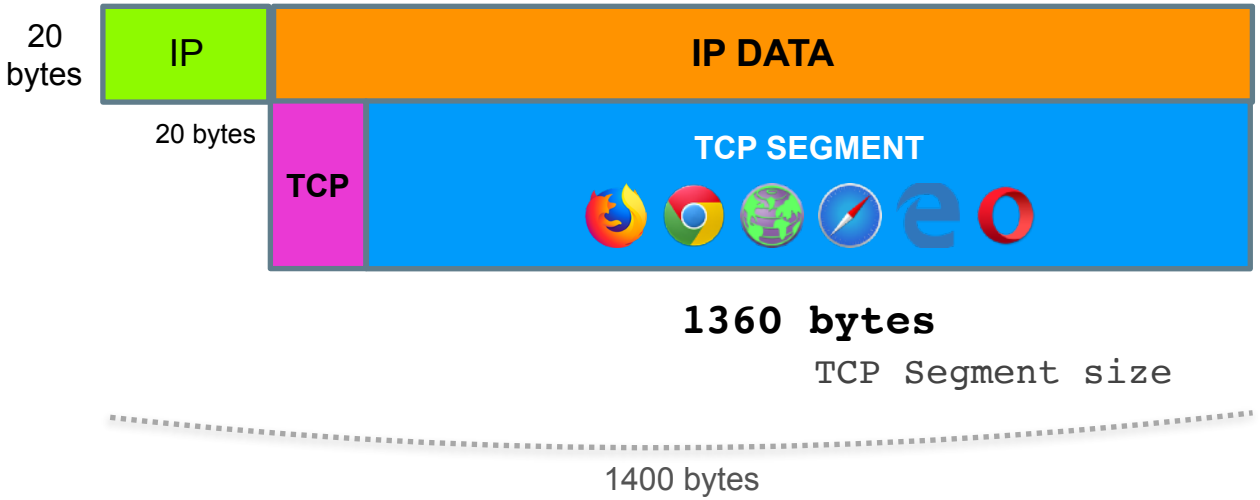
# Объяснение IPSec MTU (упрощенное)

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

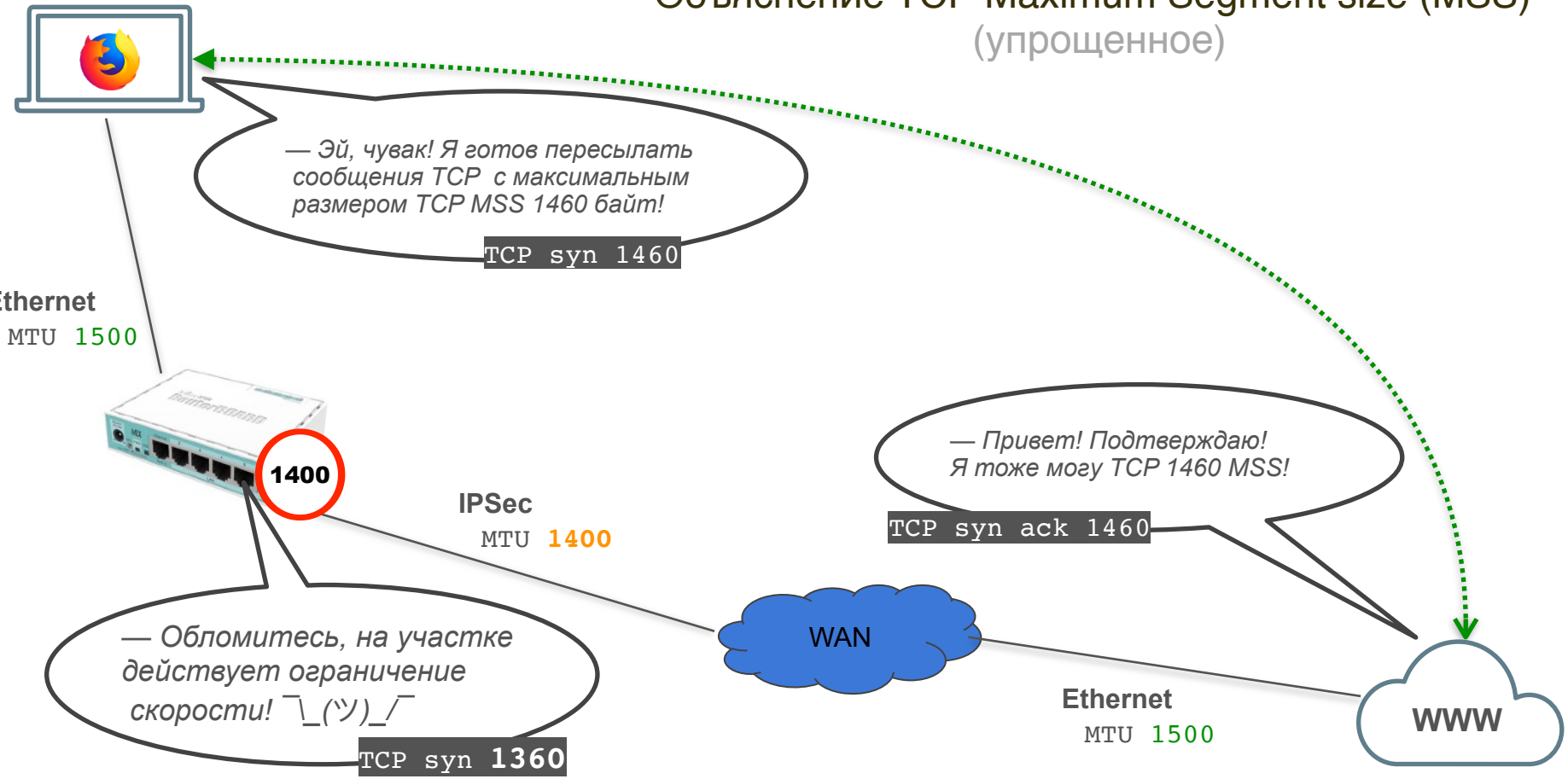


# Объяснение IPSec MTU (упрощенное)

TCP Segment size = MTU - 40 bytes

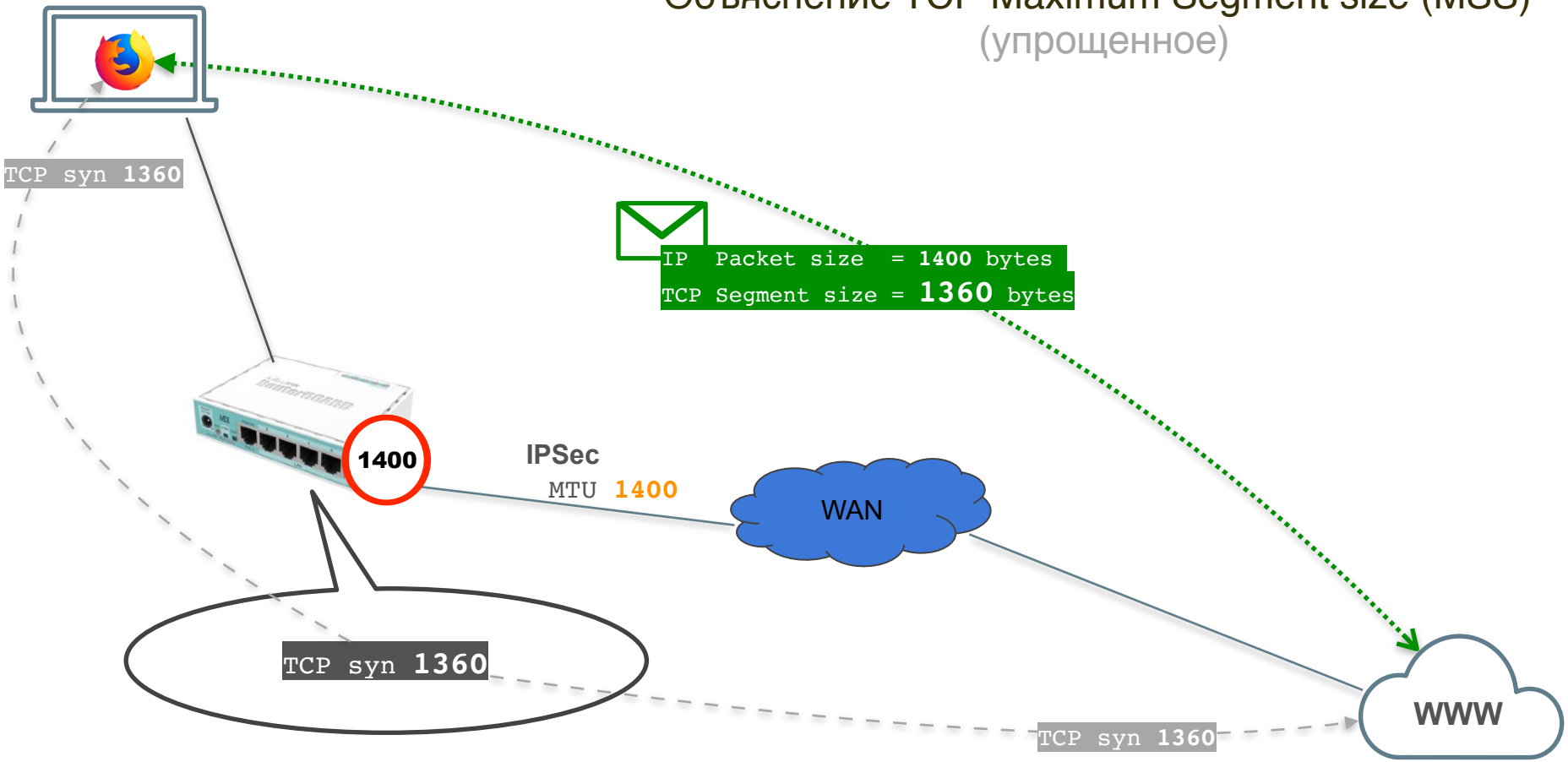


# Объяснение TCP Maximum Segment size (MSS)
(упрощенное)



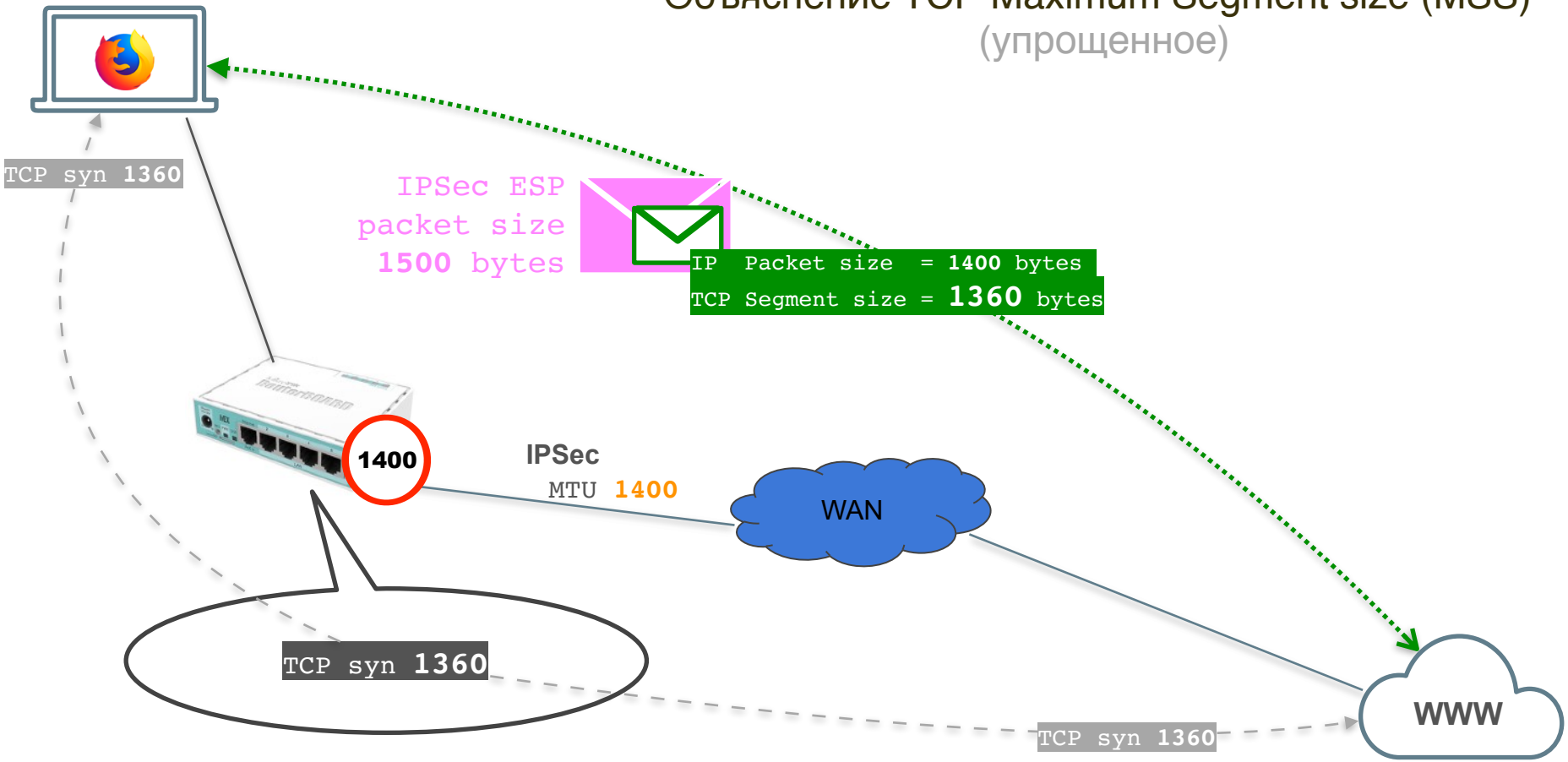
# Объяснение TCP Maximum Segment size (MSS)

(упрощенное)

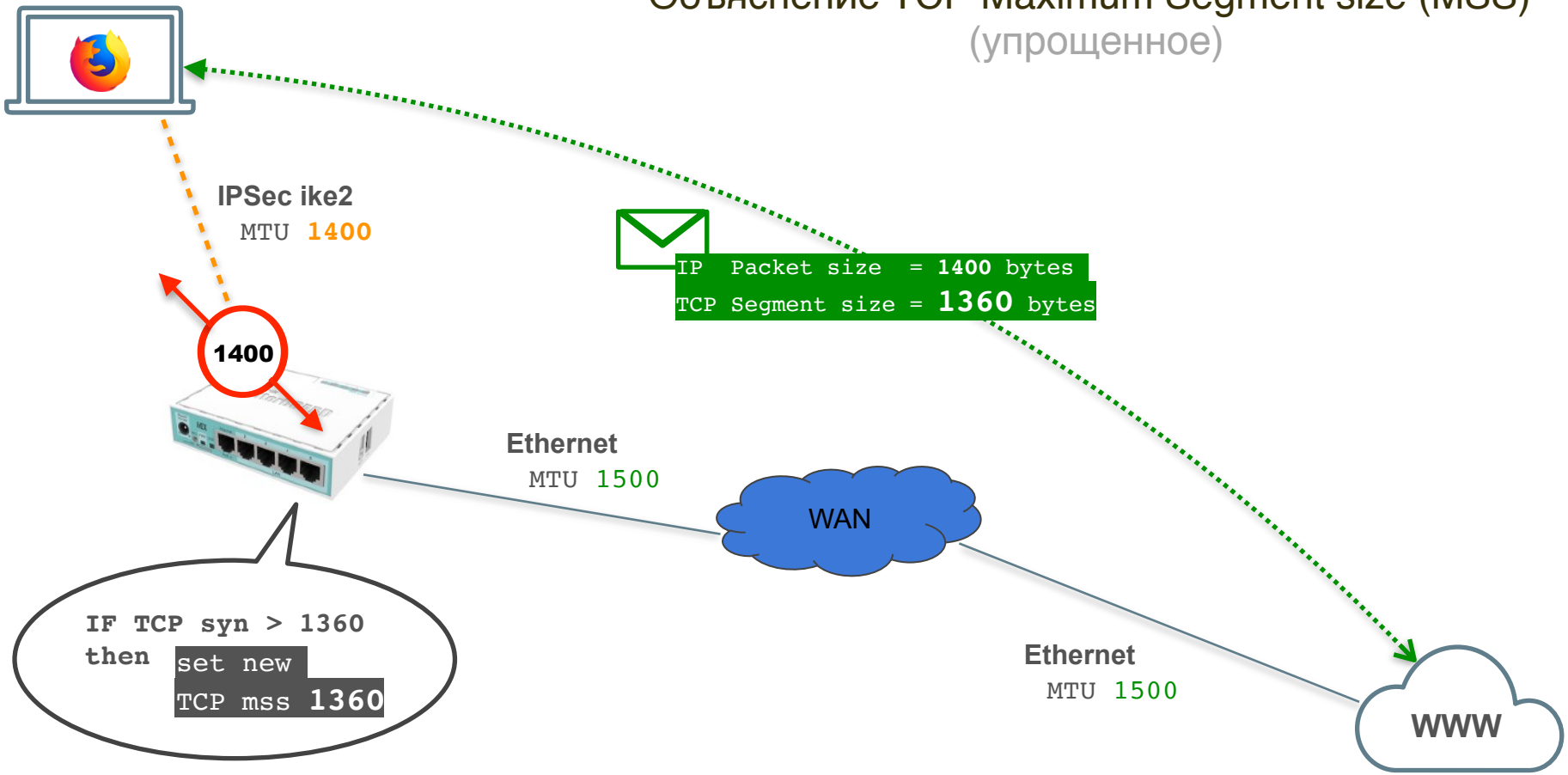


# Объяснение TCP Maximum Segment size (MSS)

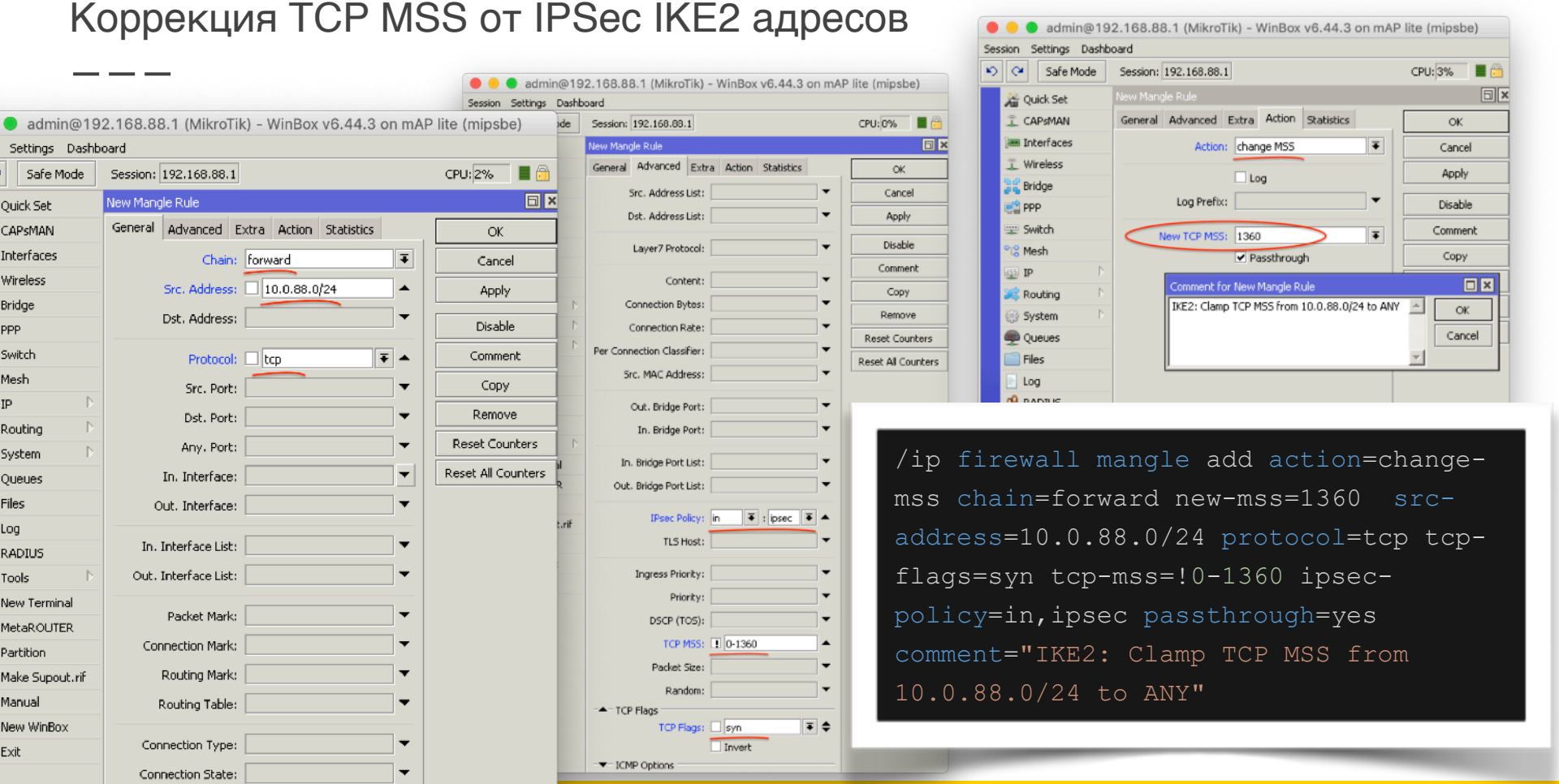
(упрощенное)



# Объяснение TCP Maximum Segment size (MSS)
(упрощенное)



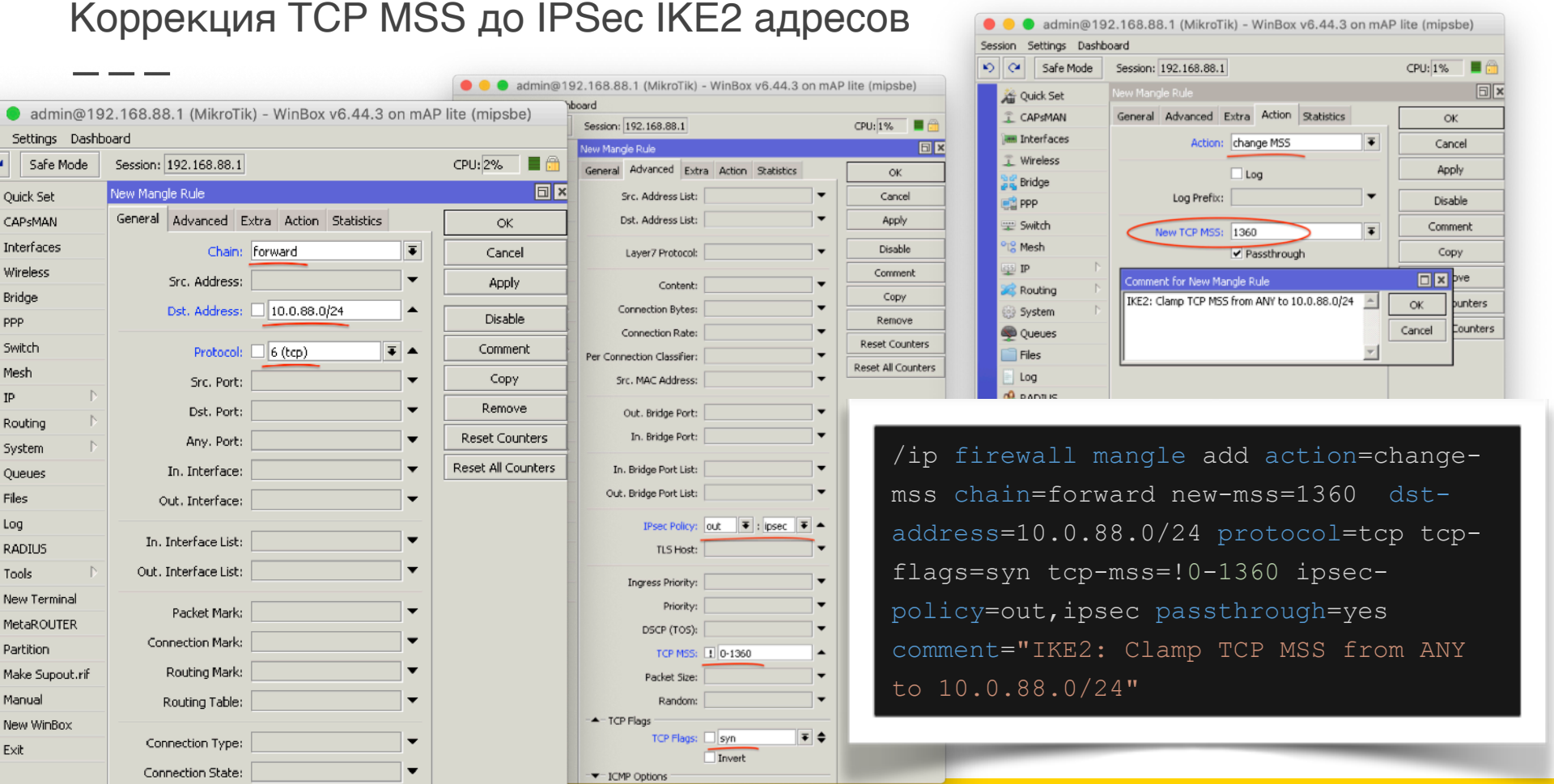
# Коррекция TCP MSS от IPSec IKE2 адресов




```
/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"
```

Nikita Tarikin / nikita@tarikin.com

# Коррекция TCP MSS до IPSec IKE2 адресов




```
/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"
```

Nikita Tarikin / nikita@tarikin.com

# Настройка клиентов

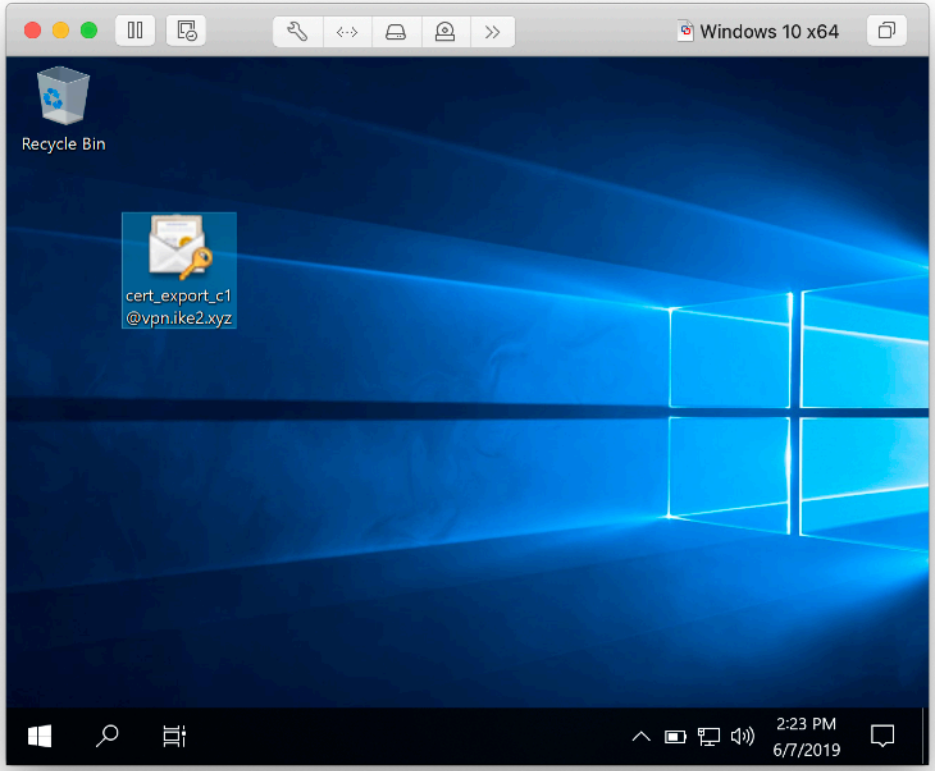
# Windows 8 / 8.1 / 10

План действий

1. Импорт SSL сертифкатов
2. Настройка IKEv2 соеденения
3. Проверка маршрутов IKEv2

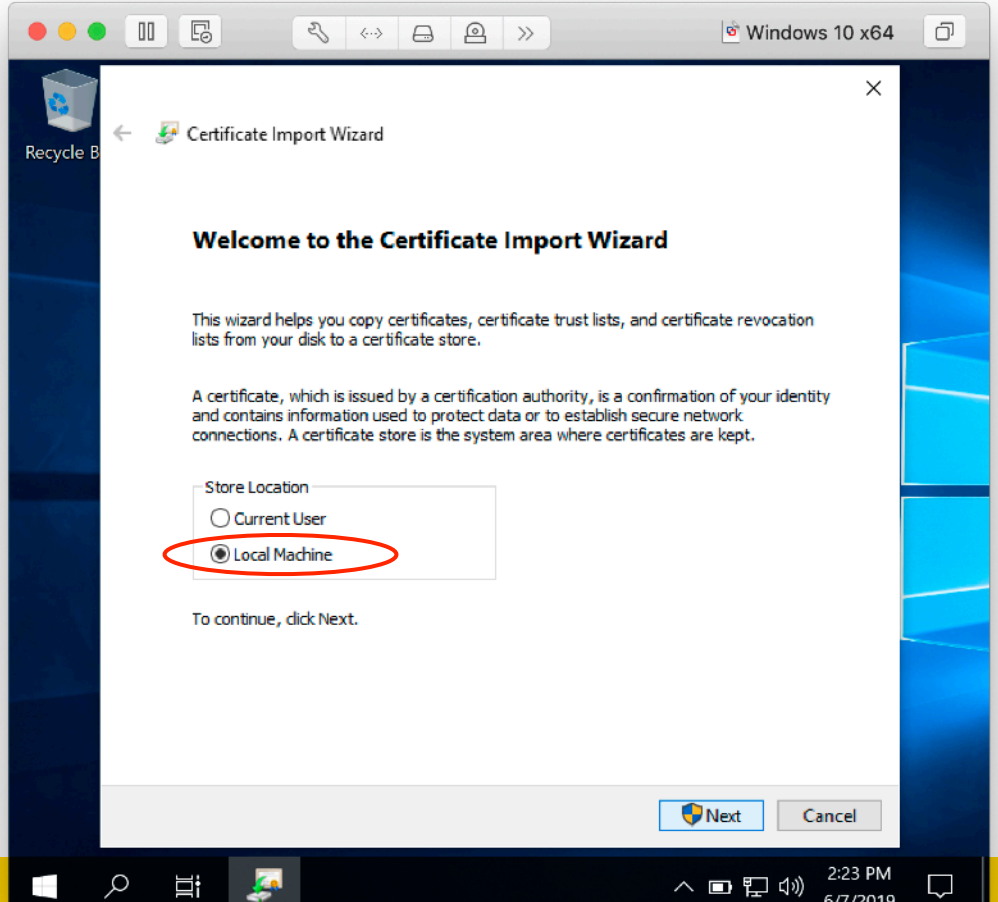
Nikita Tarikin / nikita@tarikin.com

# Windows 10: Импорт SSL сертификатов




Скачать .p12 сертификат

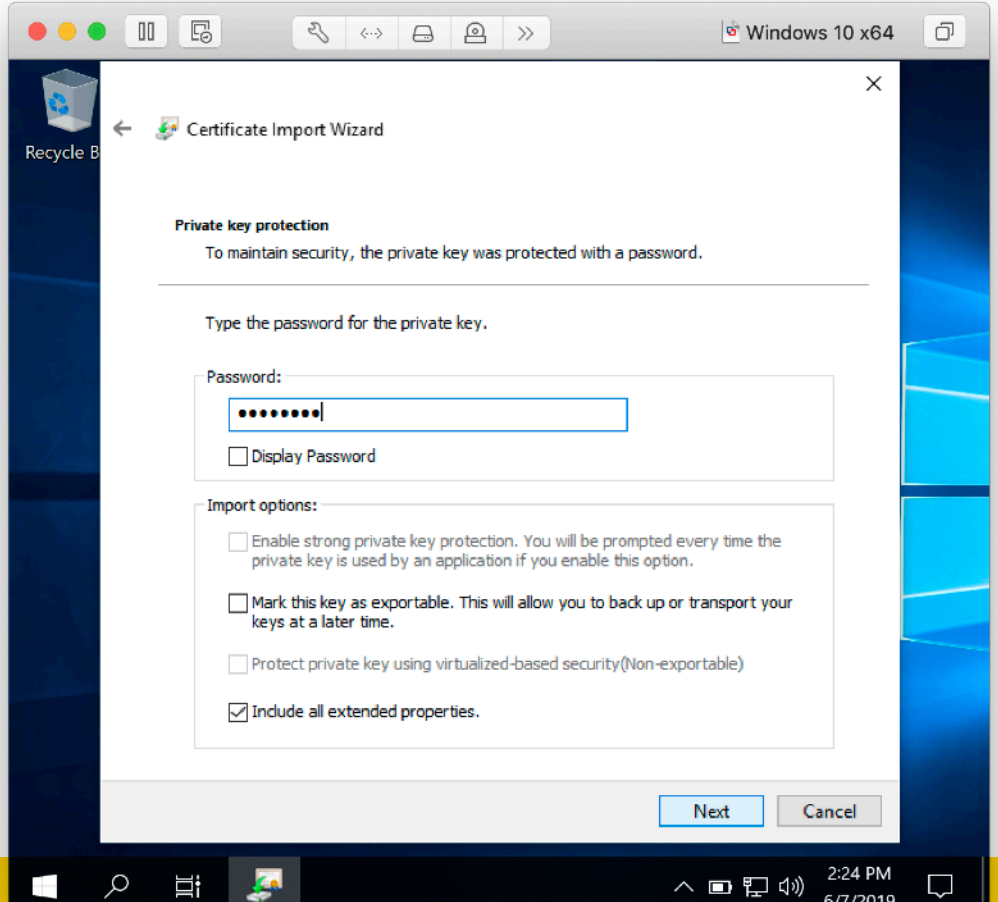
# Windows 10: Импорт SSL сертификатов

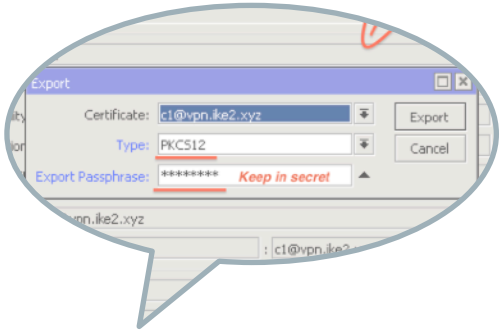



Выбрать **Local Machine** хранилище

—> **Далее**

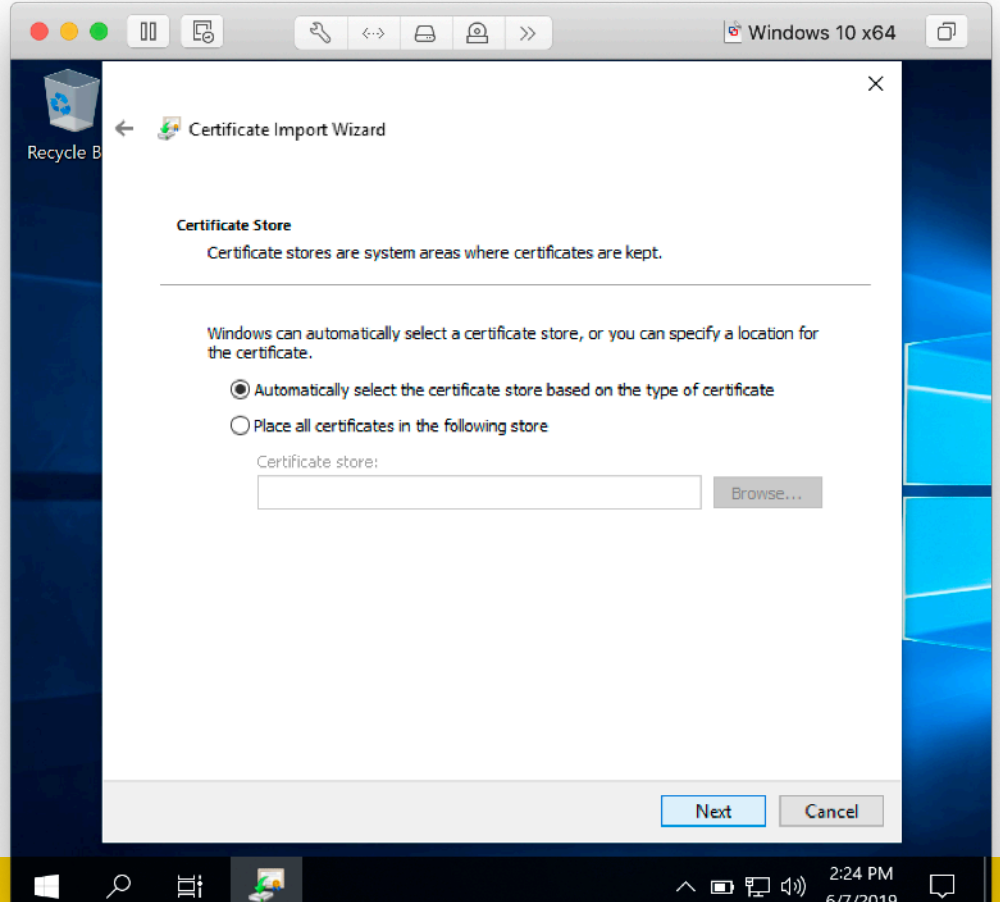
# Windows 10: Импорт SSL сертификатов



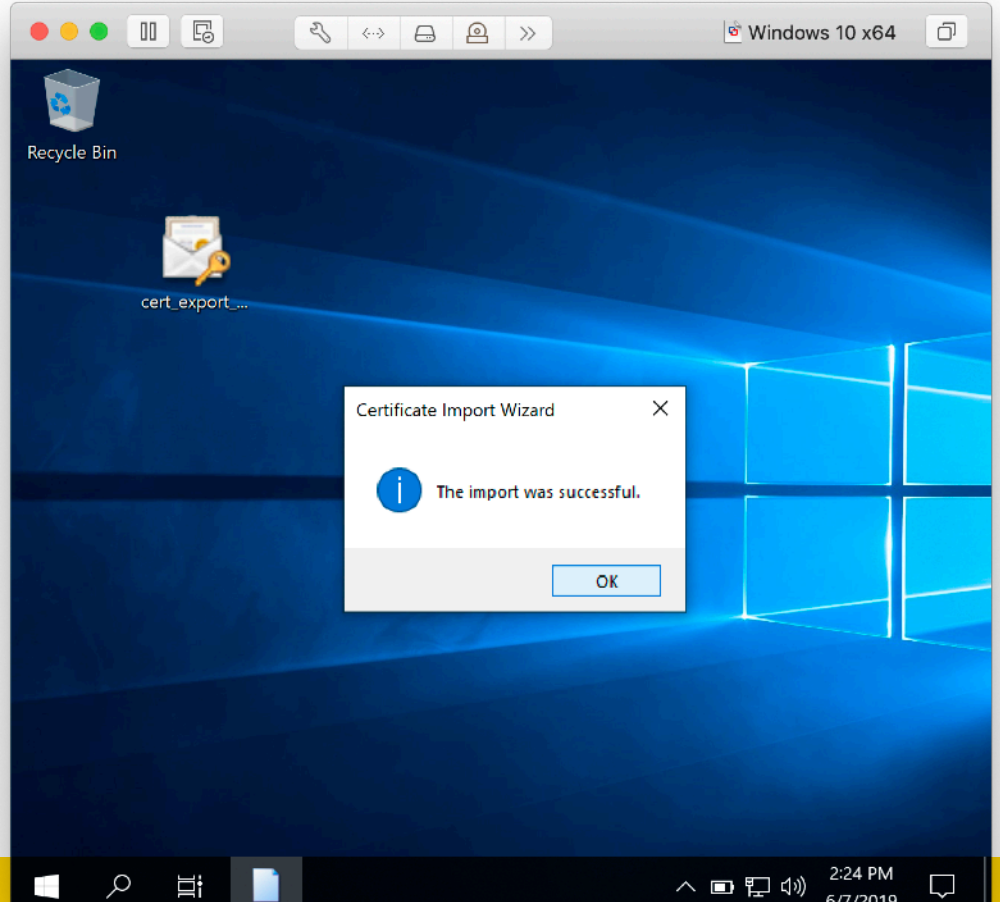

Ввести пароль
SSL сертификата клиента
—> **Далее**

# Windows 10: Импорт SSL сертификатов



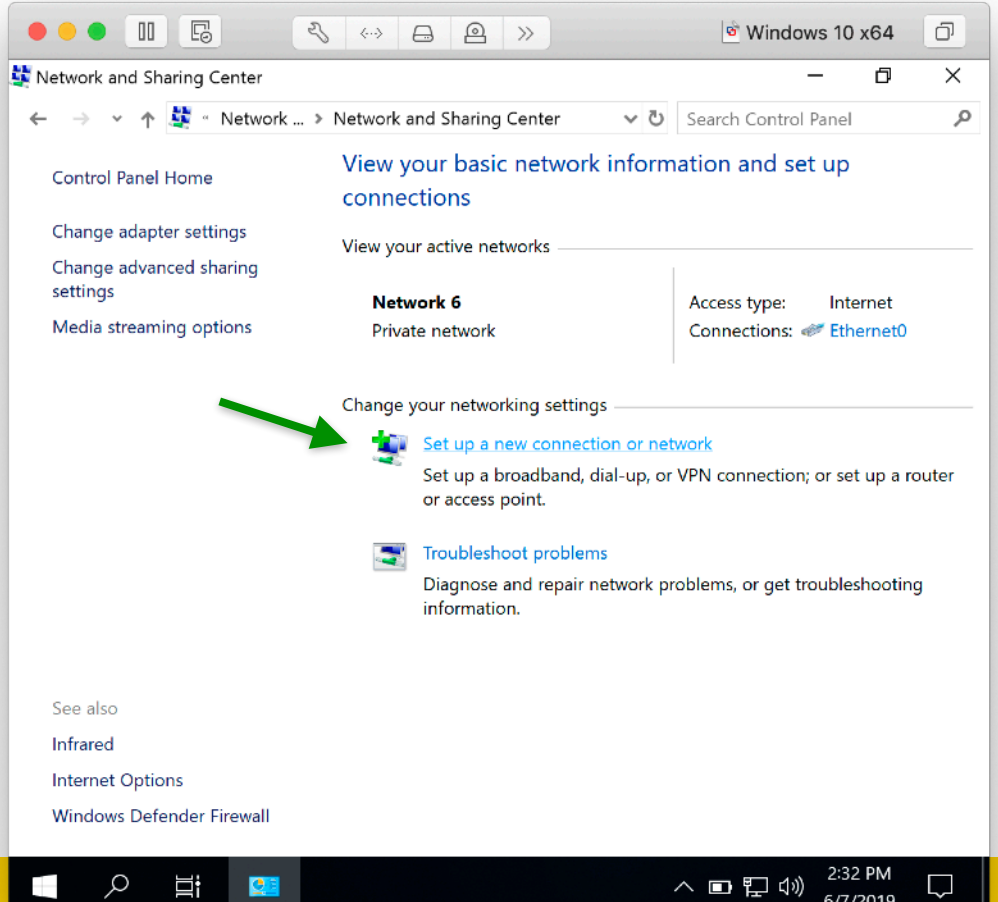

Автоматический выбор
—> **Далее**

# Windows 10: Импорт SSL сертификатов




SSL сертификат
успешно импортирован
—> **OK**

# Windows 10: Настройка IKEv2 VPN соединения



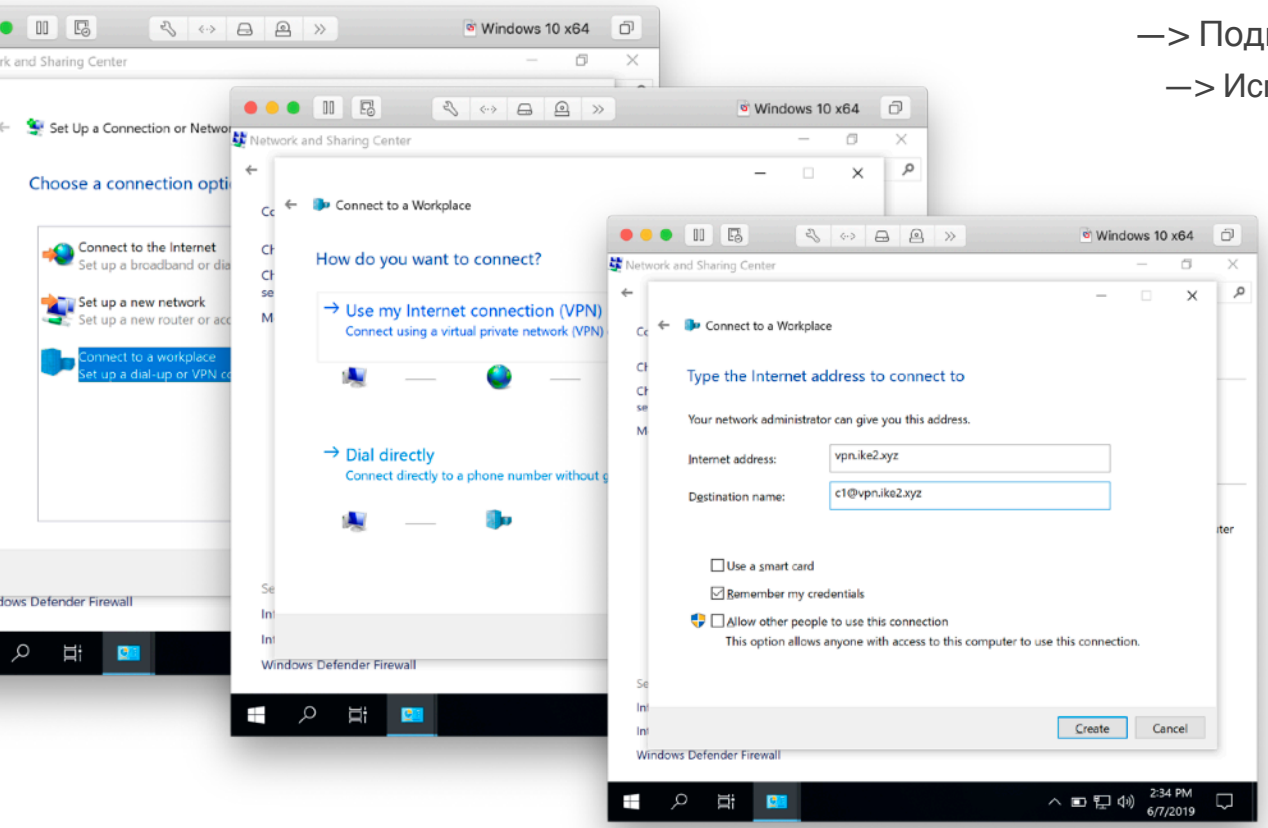

—> Панель управления

—> 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:

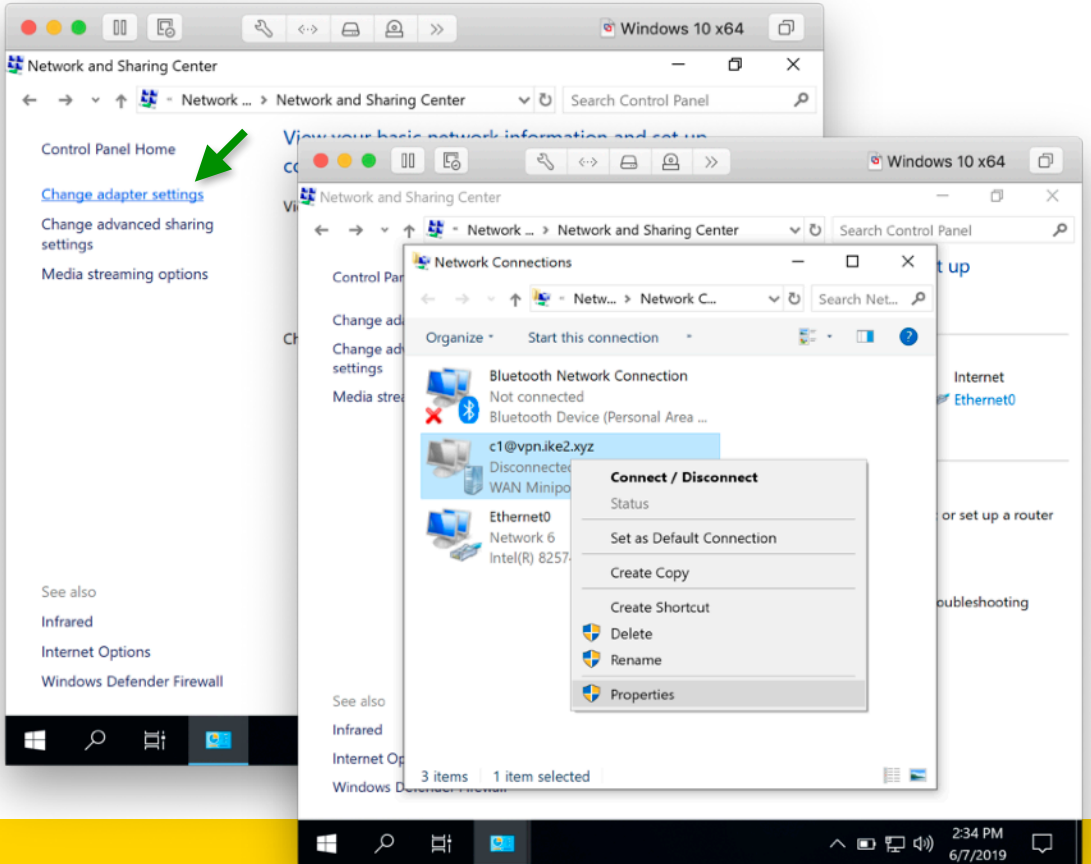
**`vpn.ike2.xyz`**

Имя назначения:

**`c1@vpn.ike2.xyz`**

—> **Создать**

# Windows 10: Настройка IKEv2 VPN соединения

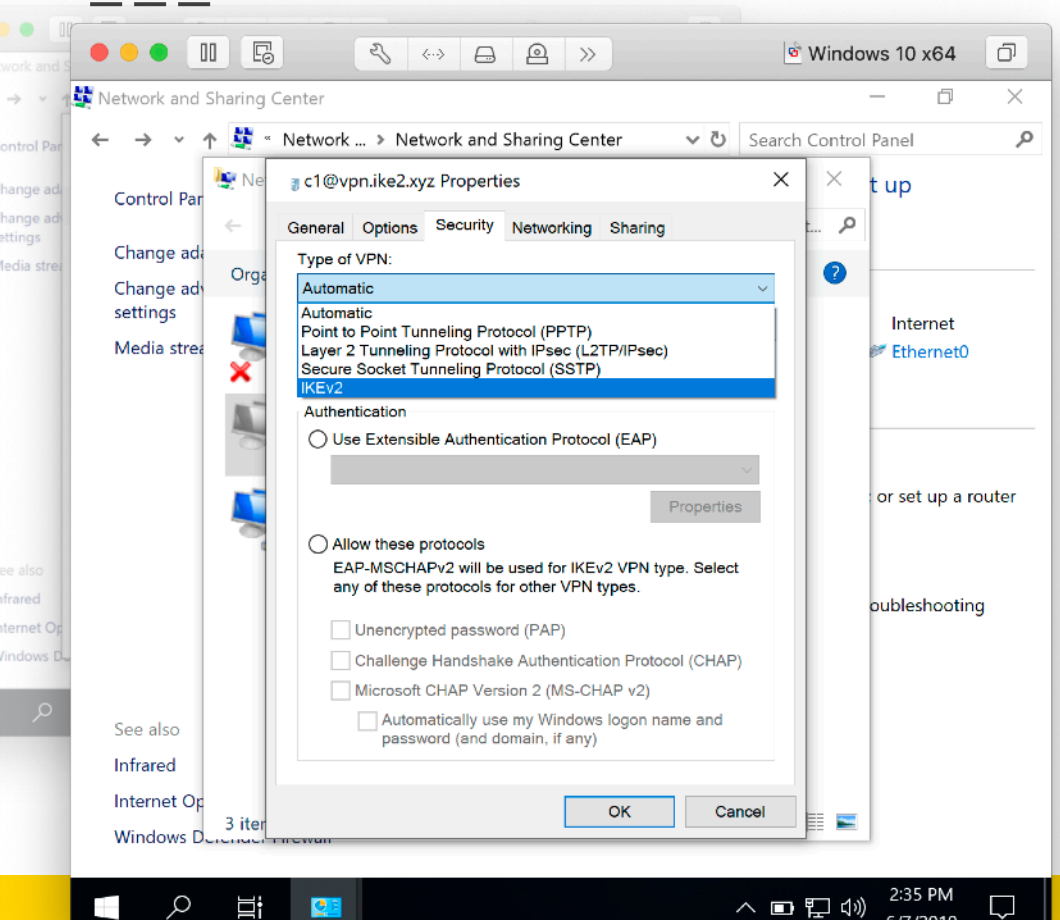



—> Изменение параметров адаптера

`c1@vpn.ike2.xyz`

—> **Свойства**

# Windows 10: Настройка IKEv2 VPN соединения

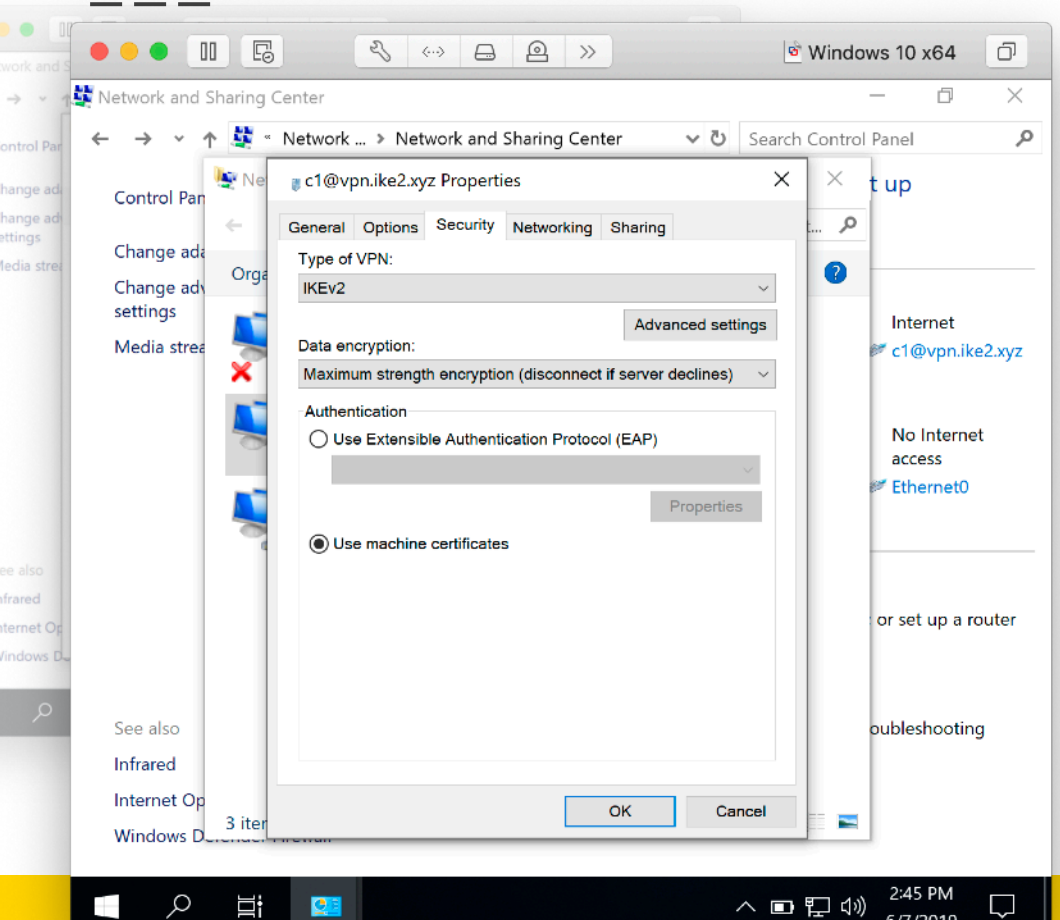



Свойства -> Безопасность

Тип VPN:

**IKEv2**

# Windows 10: Настройка IKEv2 VPN соединения




Свойства -> Безопасность

Шифрование данных:

Самое стойкое

Проверка подлинности:

Использовать сертификаты компьютеров

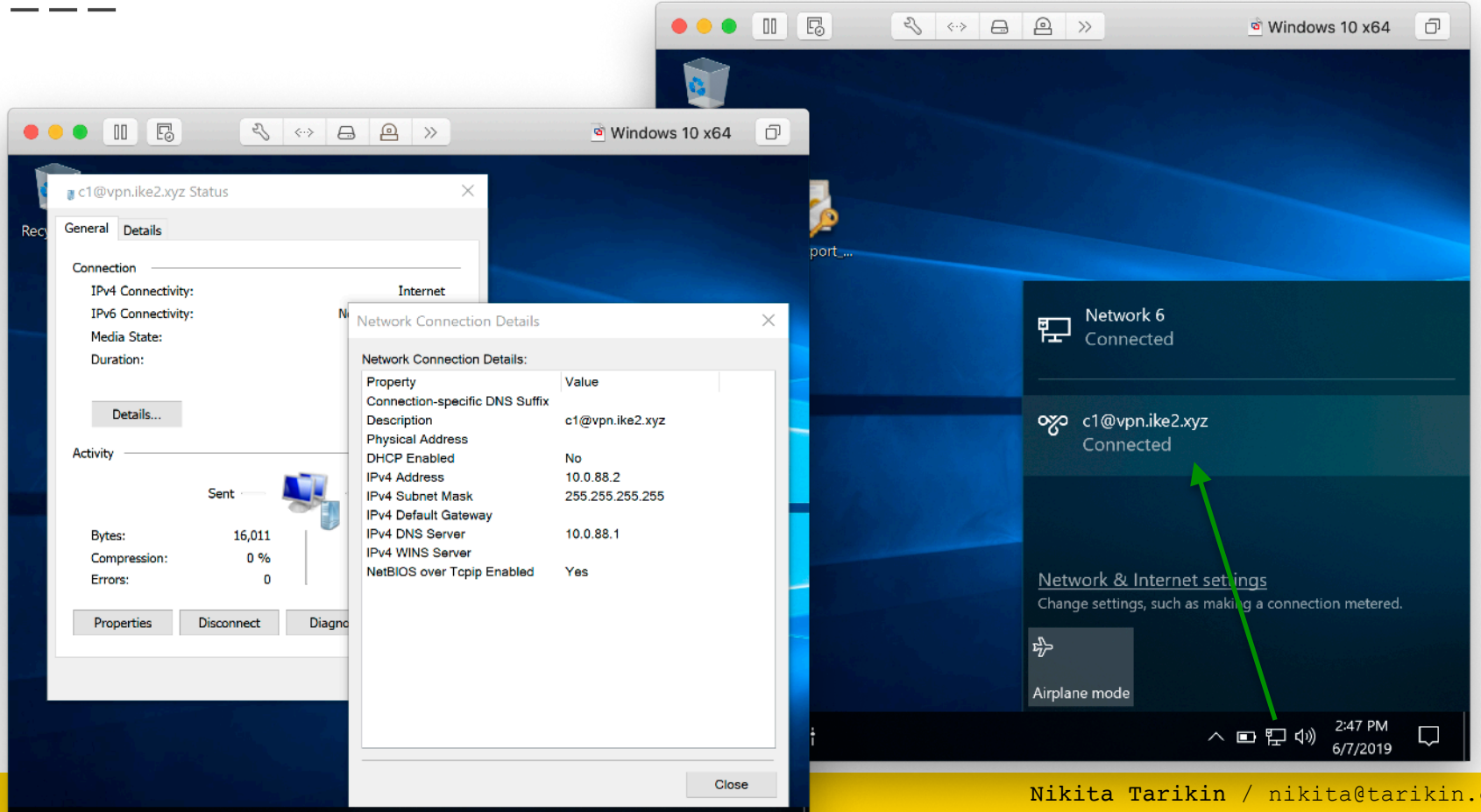
—> **OK**

# Явный выбор сертификата для IKEv2 соединения

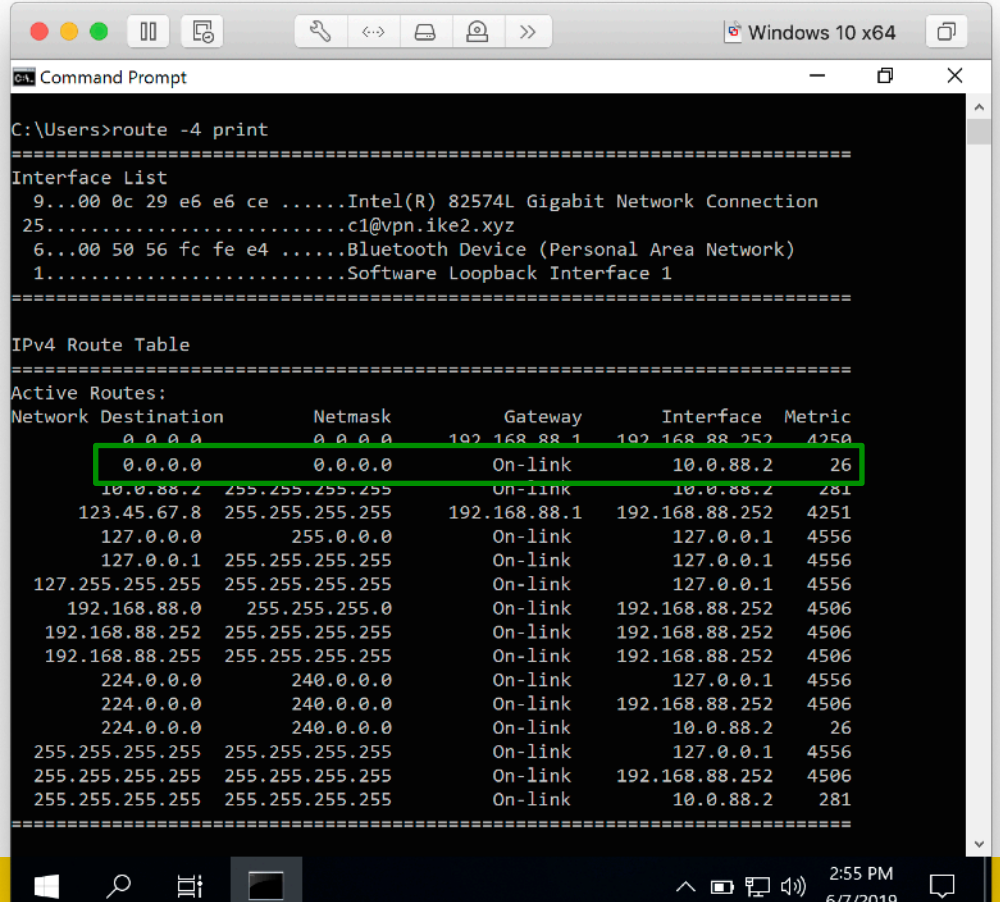
```
Set-VpnConnection -Name
"c1@vpn.ike2.xyz" -
MachineCertificateIssuerFilter
'C:\mycerts\CA.crt'
```

Через уточнение издателя авторитета CA

# Windows 10: проверка IKEv2 VPN соединения



# Windows 10: проверка IKEv2 VPN маршрутов




`route -4 print`

Destination

`0.0.0.0/0` (default)

Gateway:

`On-link`

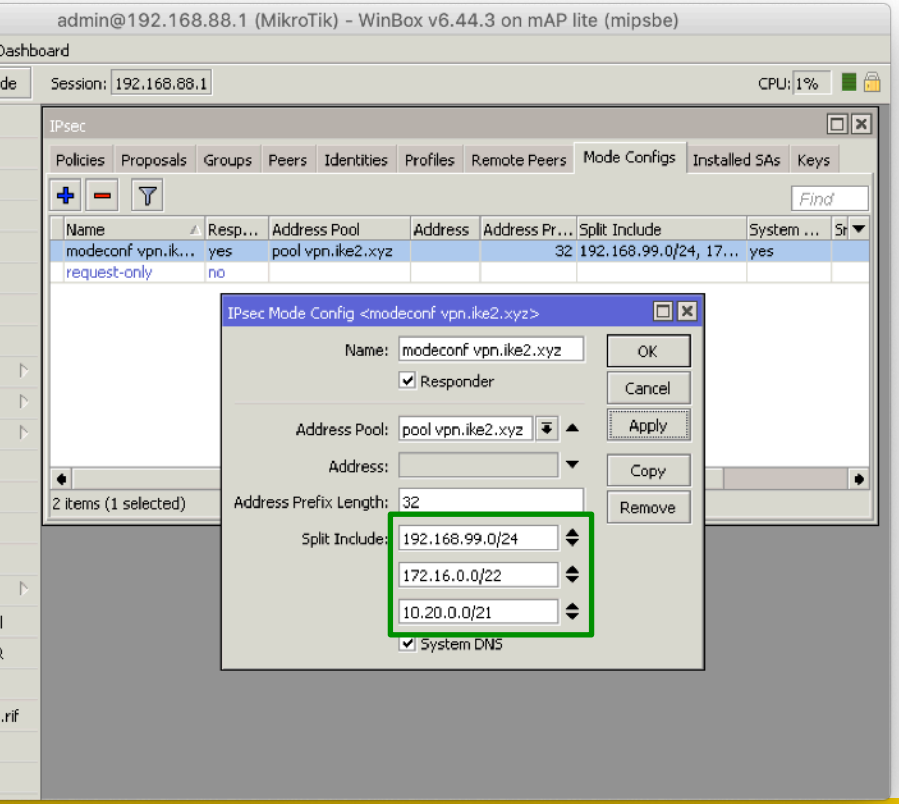
Interface:

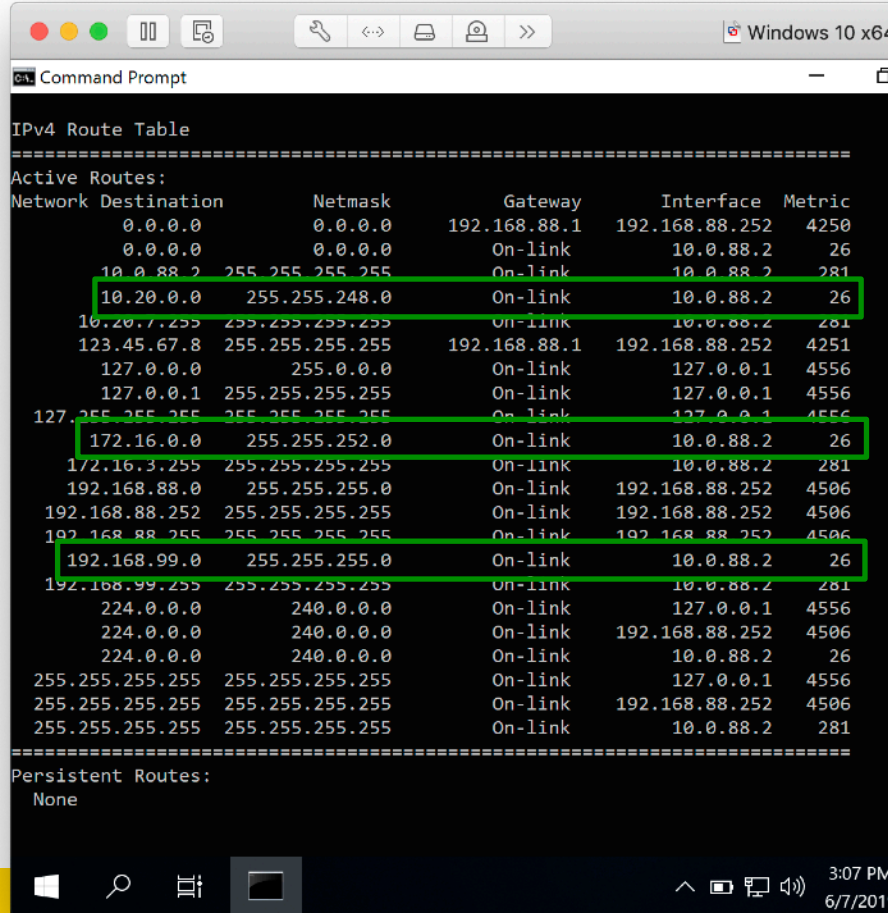
`10.0.88.2`

Metric (distance):

`26`

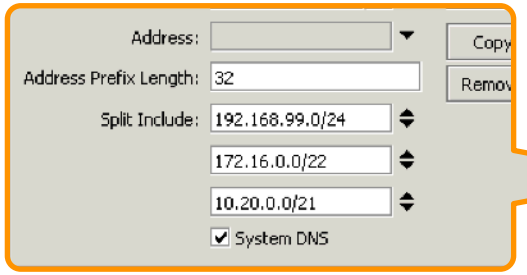
# Windows 10: проверка IKEv2 VPN маршрутов

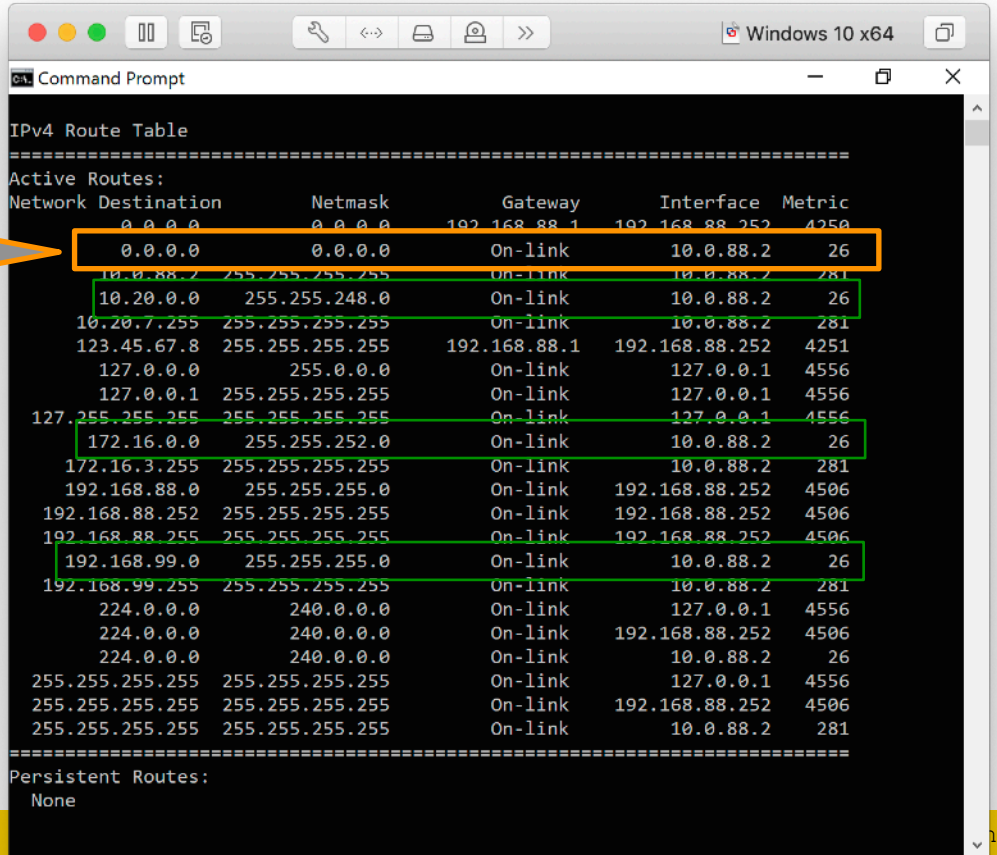


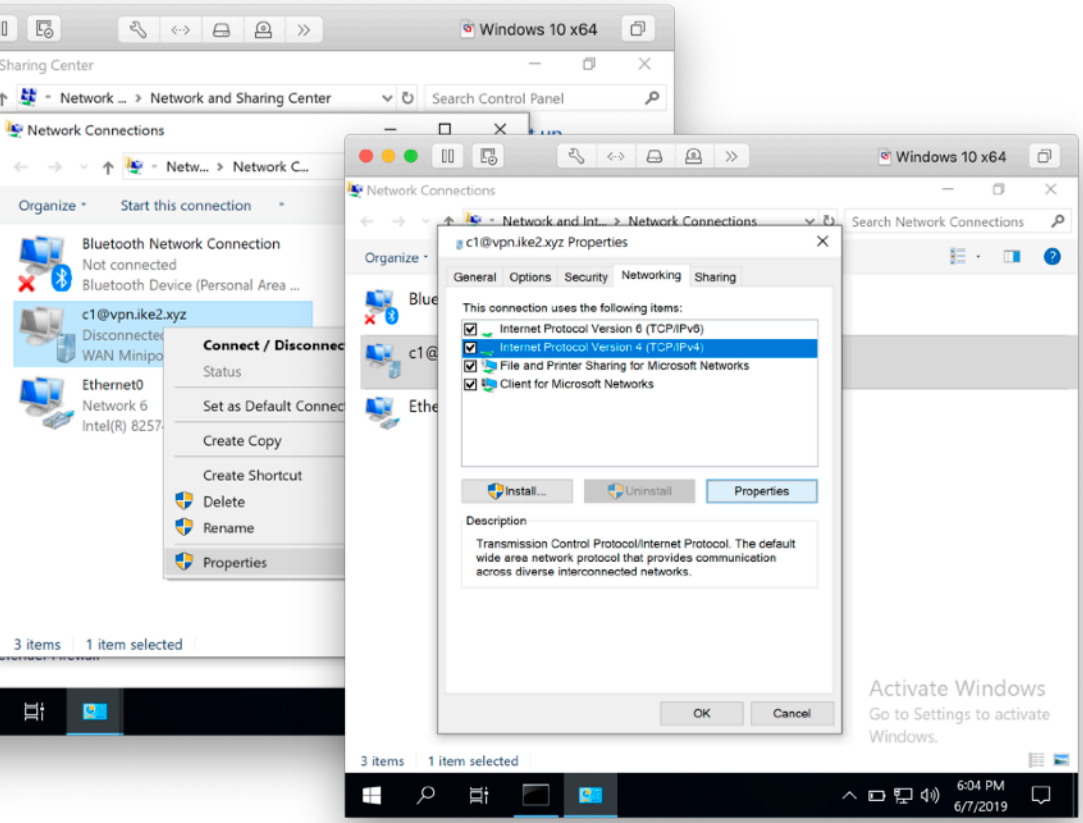
# Windows 10: проверка IKEv2 VPN маршрутов

— 0.0.0.0/0 ???



# Windows 10: отключаем пересылку всего трафика через IKEv2 VPN

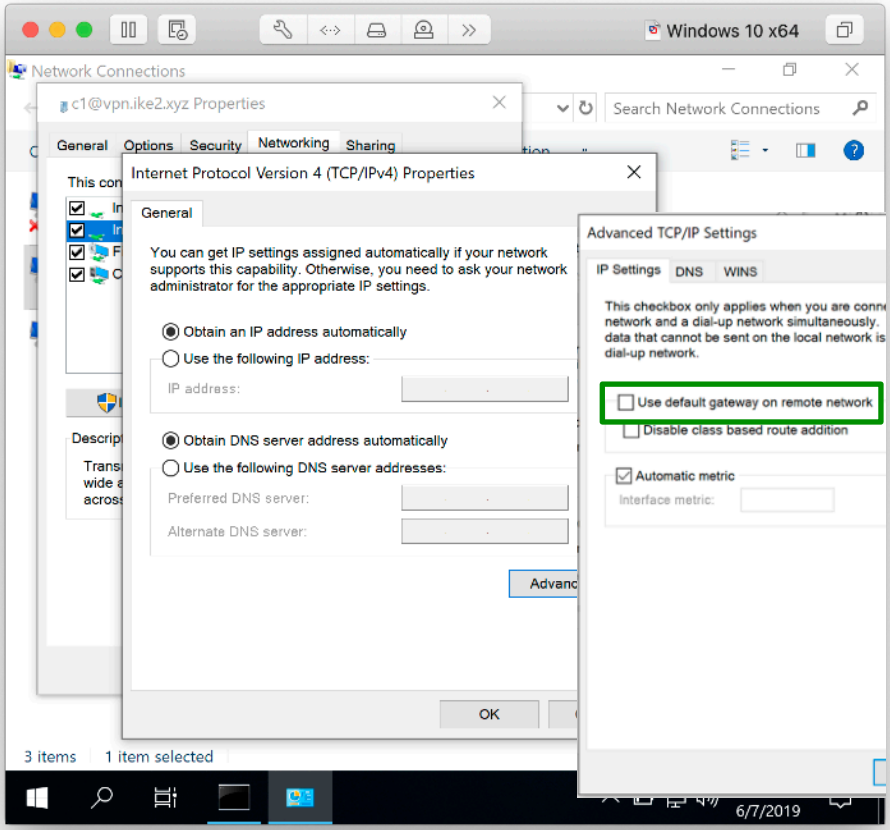



Свойства -> Сеть

✓ 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

—>

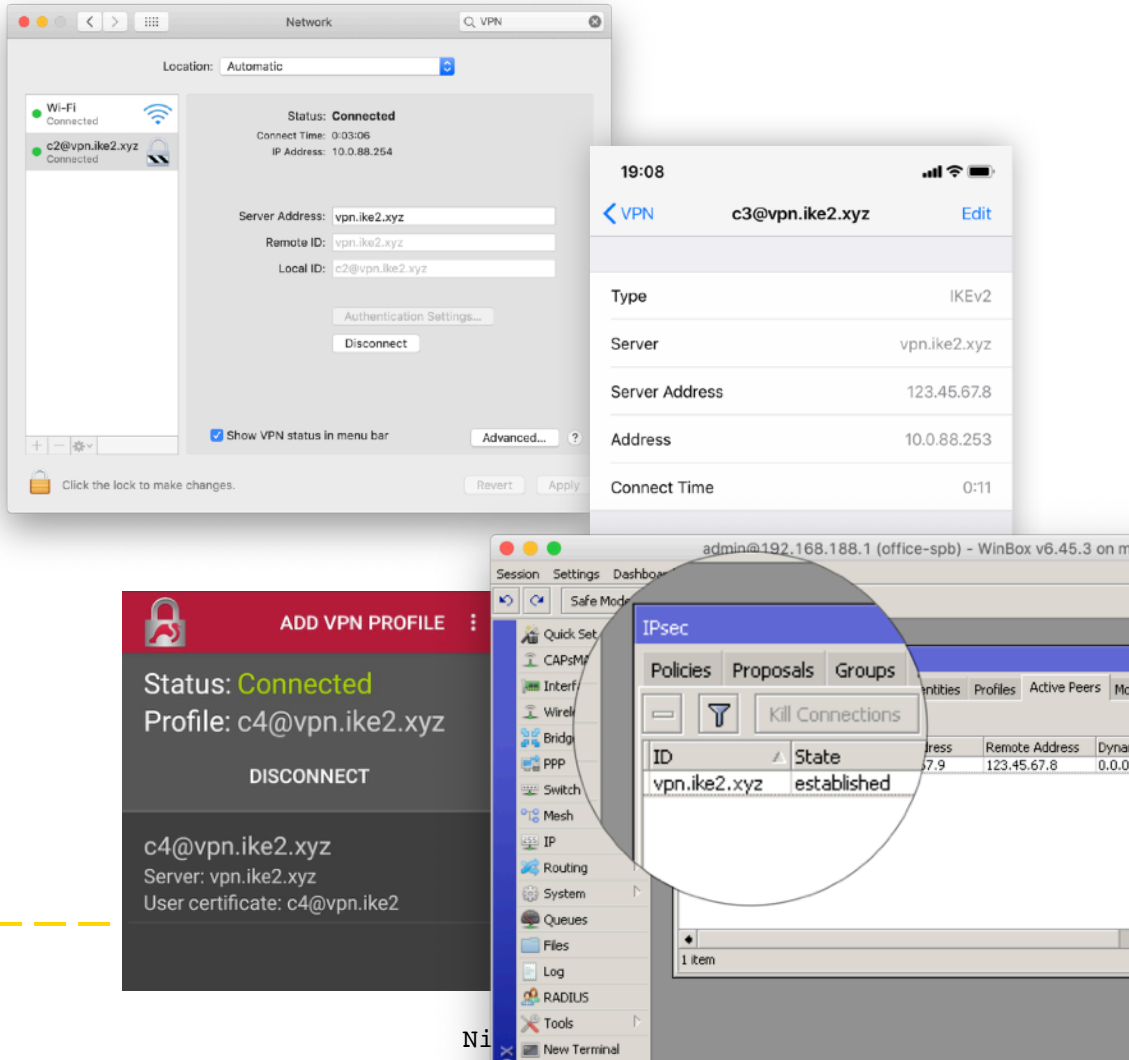
**Дополнительно**

Дополнительные параметры TCP/IP

☐ Использовать основной шлюз

# Подключение non-Windows

MacOS
iOS
Android
RouterOS



# Apple MacOS

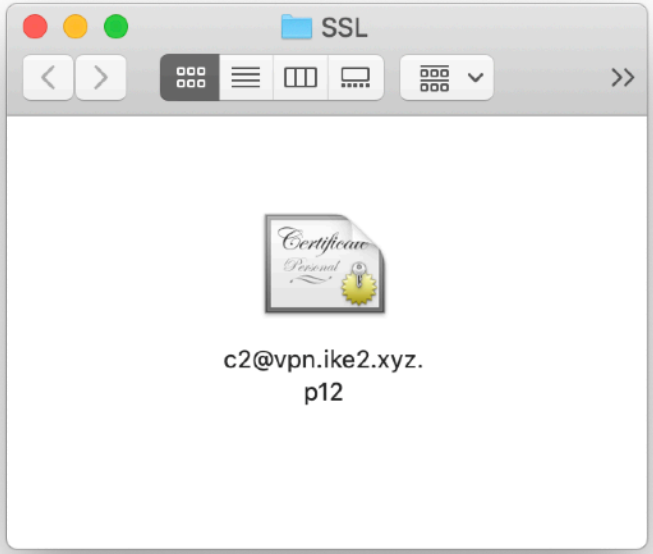
≥ 10.11 El Capitan

## План действий

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

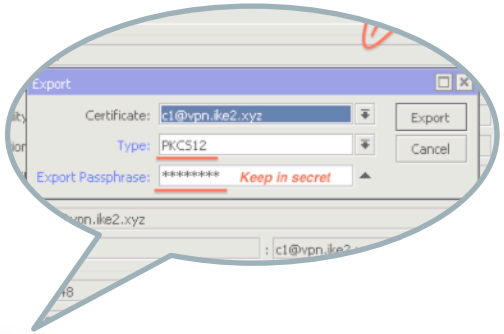
**Nikita Tarikin** / nikita@tarikin.com

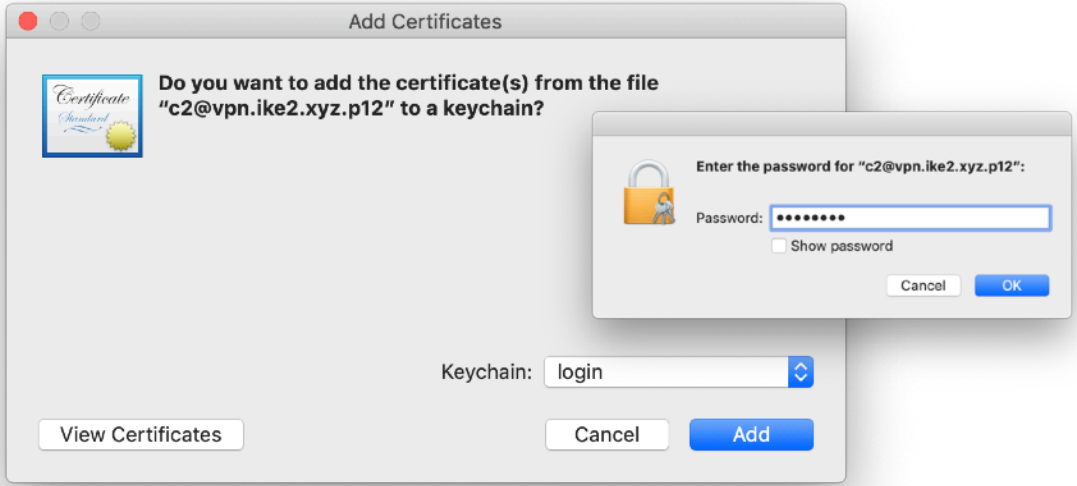
# MacOS: Импорт SSL сертификатов




Скачать .p12 сертификат

# MacOS: Импорт SSL сертификатов



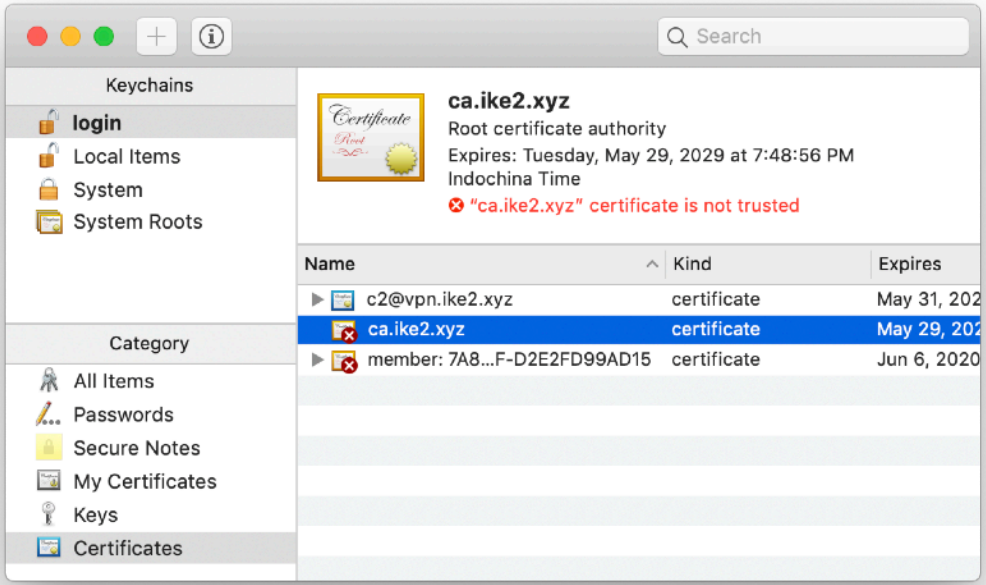

Keychain:
login (default)

—> **Add**

Type your
SSL certificate password

—> **OK**

# MacOS: Управление импортированными SSL сертификатами

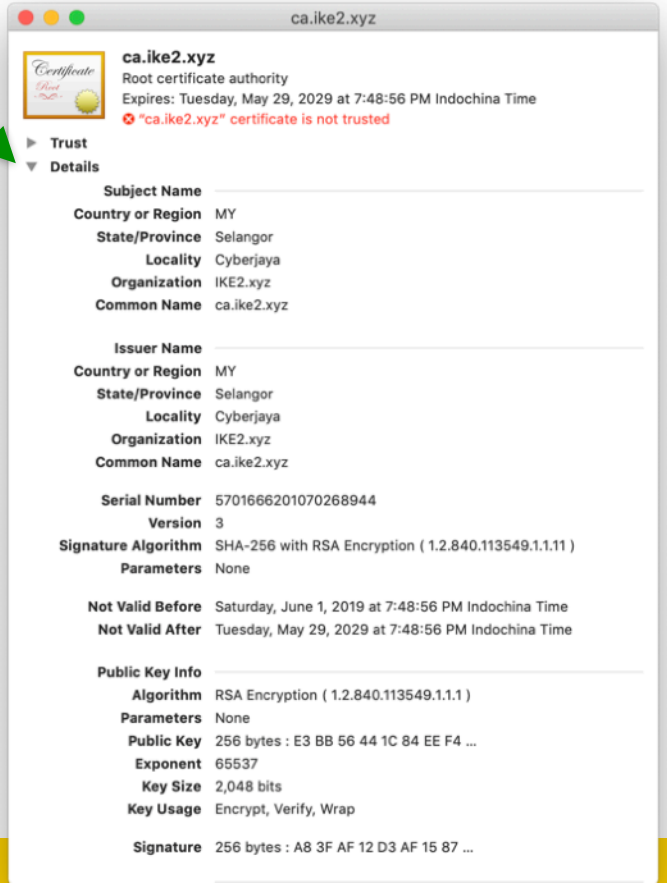



Keychain access

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

# MacOS: Управление импортированными SSL сертификатами

Important



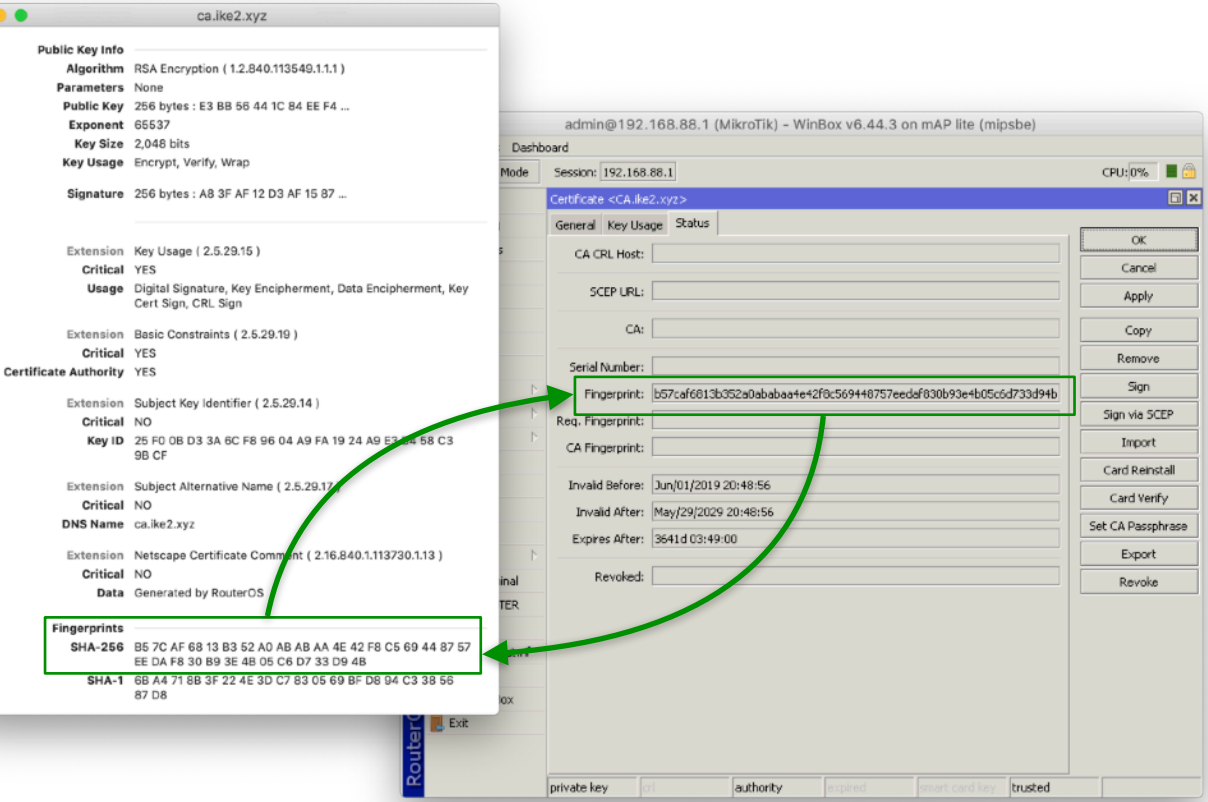

Keychain access

Verify CA certificate details

# MacOS: Управление импортированными SSL сертификатами

Important

Keychain access

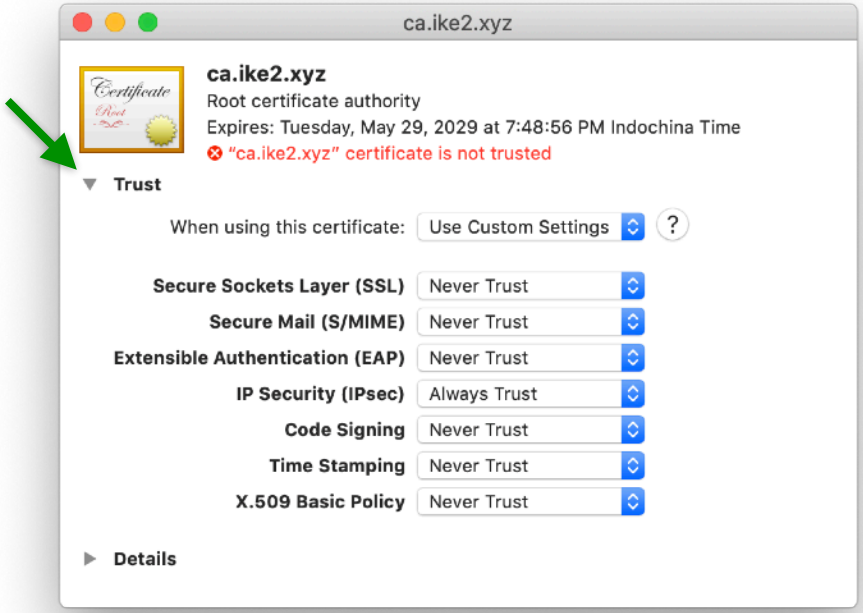



Сверяем **отпечатки** CA сертификата

# MacOS: Управление импортированными SSL сертификатами

Important

Keychain access

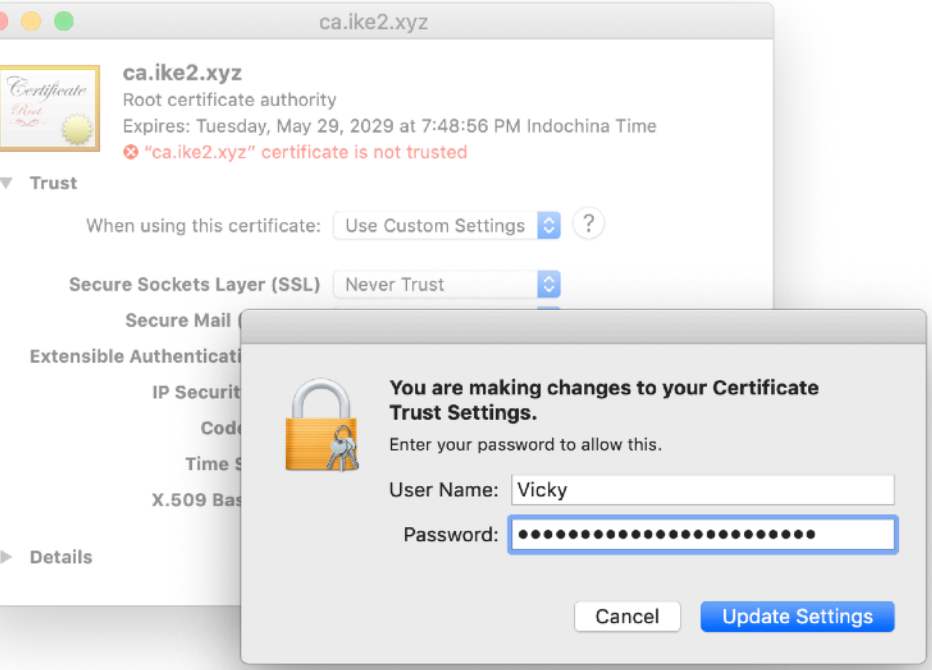



✅ IP Security (IPSec)

❌ Everything else

# MacOS: Управление импортированными SSL сертификатами

Important

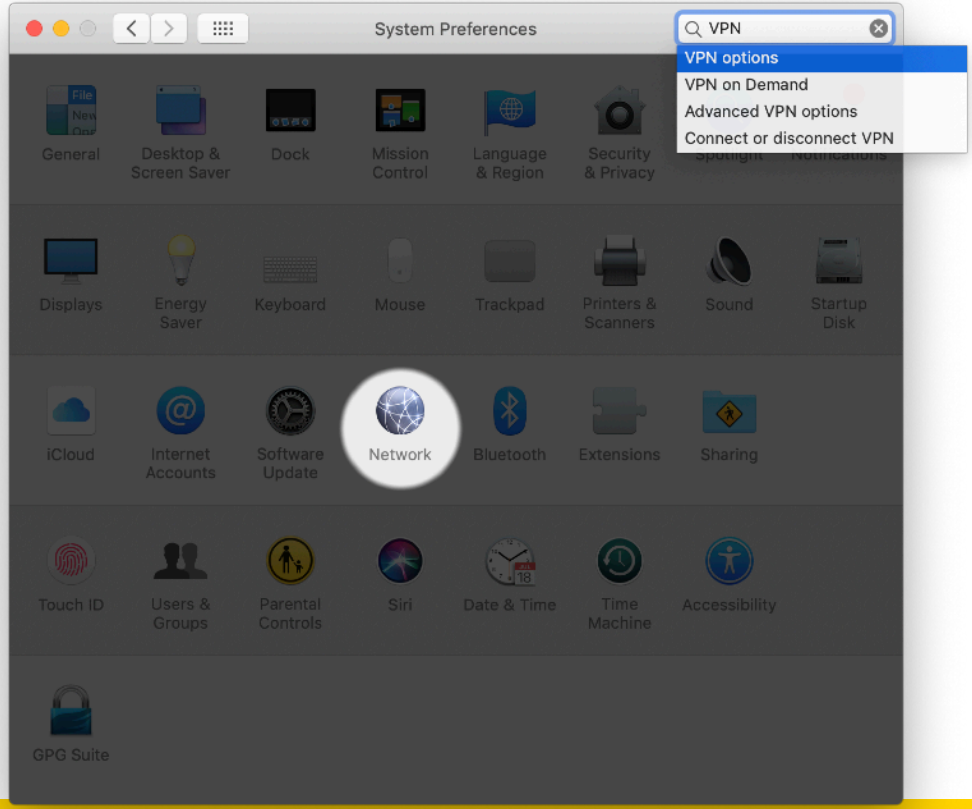



Keychain access

Type your
MacOS password

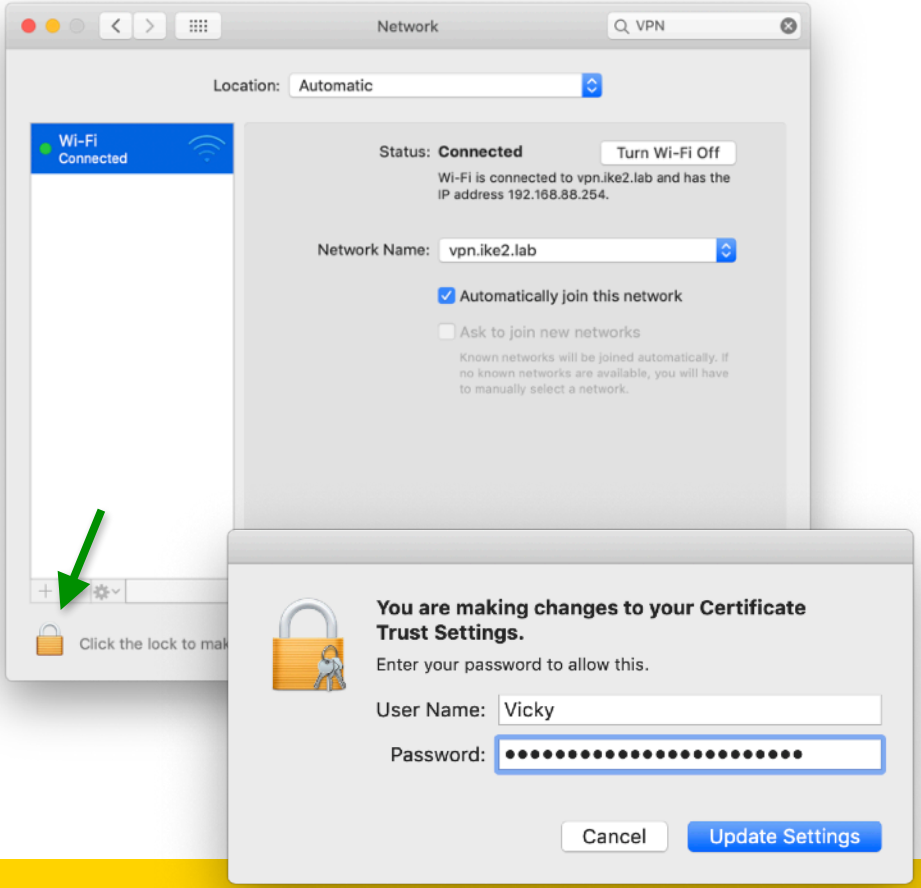
—> **Update settings**

# MacOS: Настройка IKEv2 VPN соединения



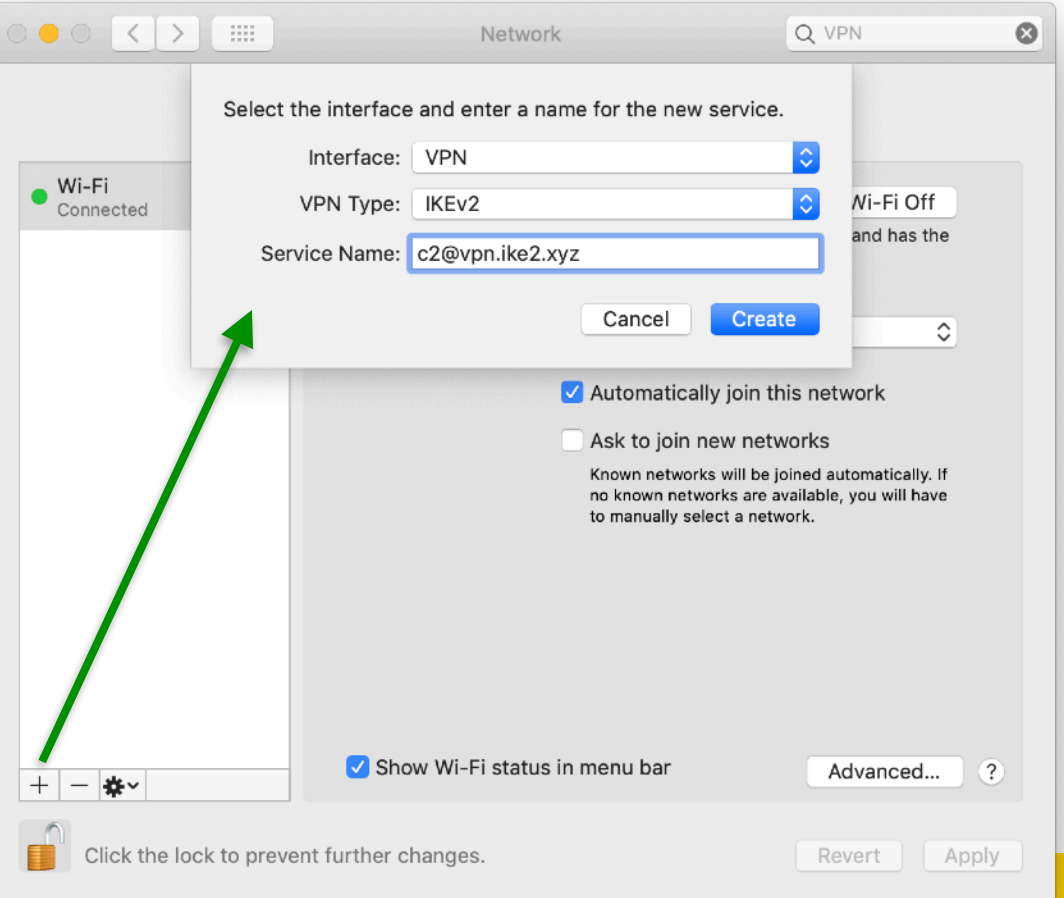

System preferences ->
Network

# MacOS: Настройка IKEv2 VPN соединения




Unlock to make changes

# MacOS: Настройка IKEv2 VPN соединения




## Create new connection

Interface:

**VPN**

VPN Type:

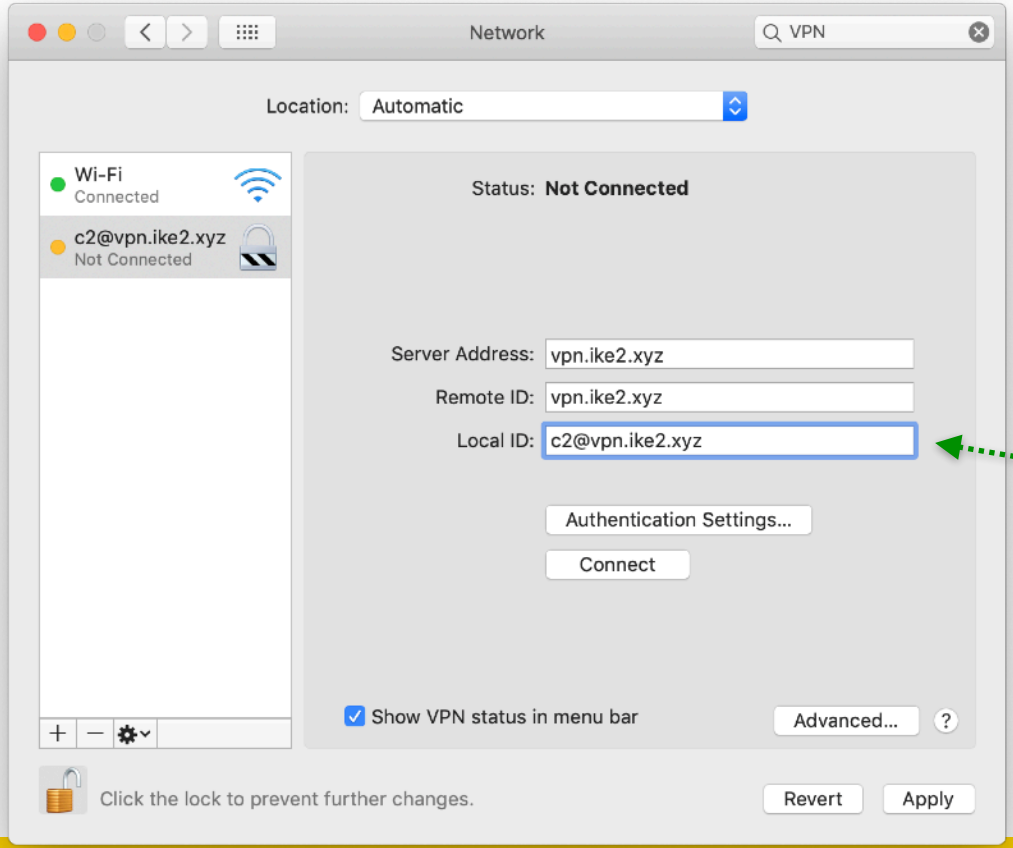
**IKEv2**

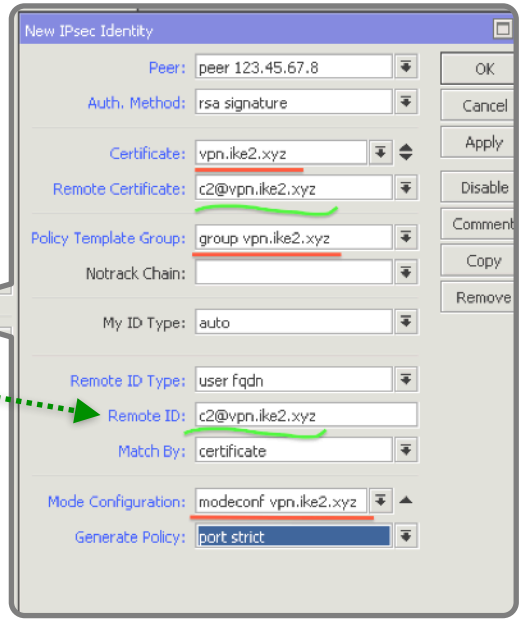
Service name:

**c2@vpn.ike2.xyz**

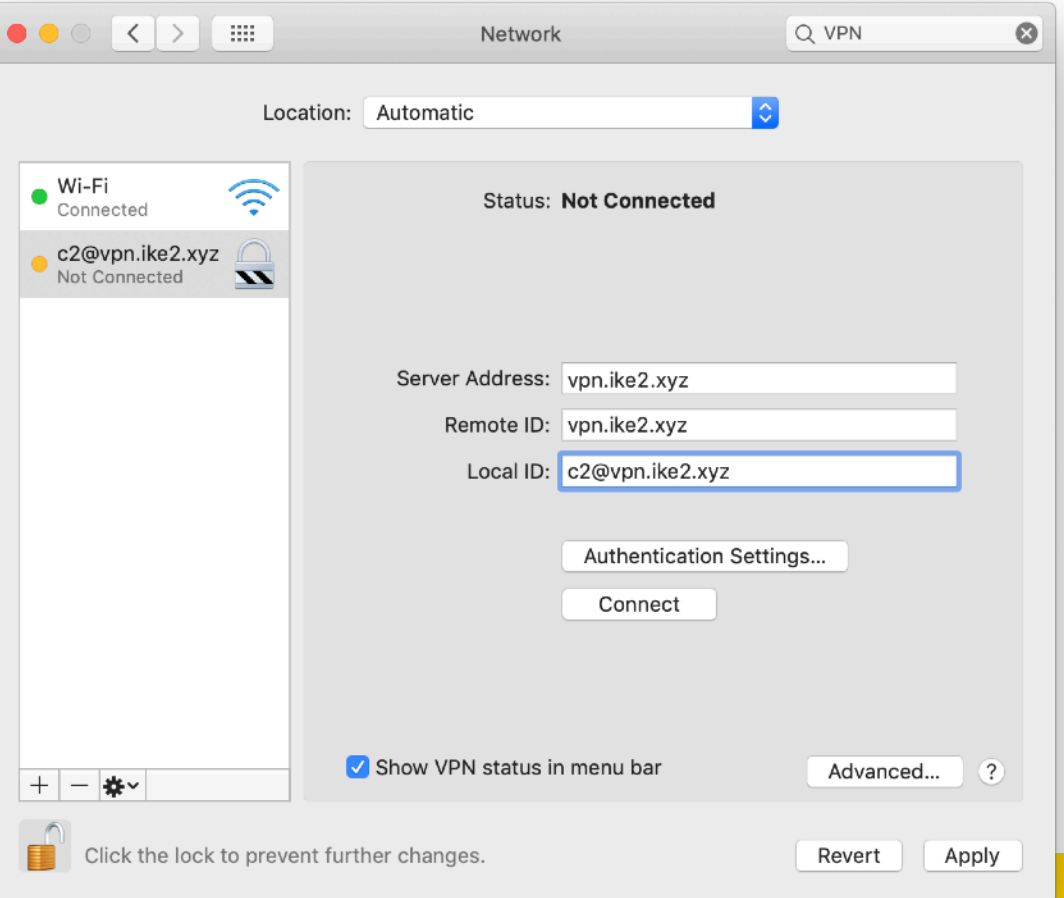
**–> Create**

# MacOS: Настройка IKEv2 VPN соединения



# MacOS: Настройка IKEv2 VPN соединения




## Create new connection

Server Address:

**`vpn.ike2.xyz`**

Remote ID:

**`vpn.ike2.xyz`**

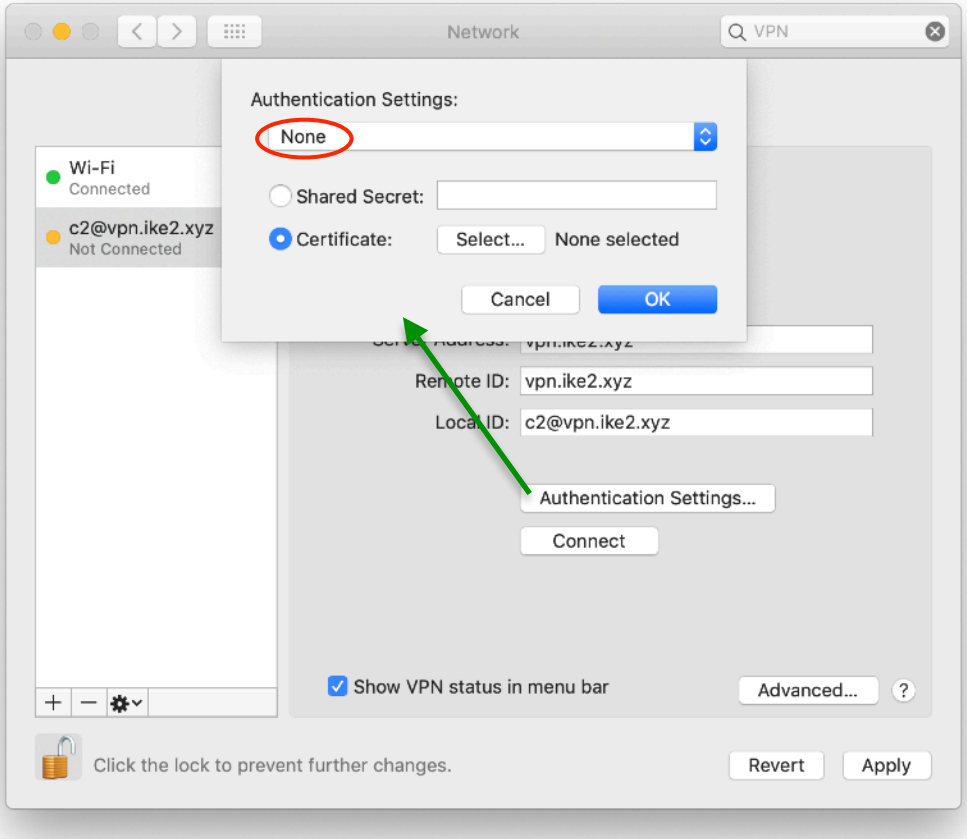
Local ID:

**`c2@vpn.ike2.xyz`**

✓ Show VPN status in menu bar

**`–> Apply`**

# MacOS: Настройка IKEv2 VPN соединения




## Authentication Settings

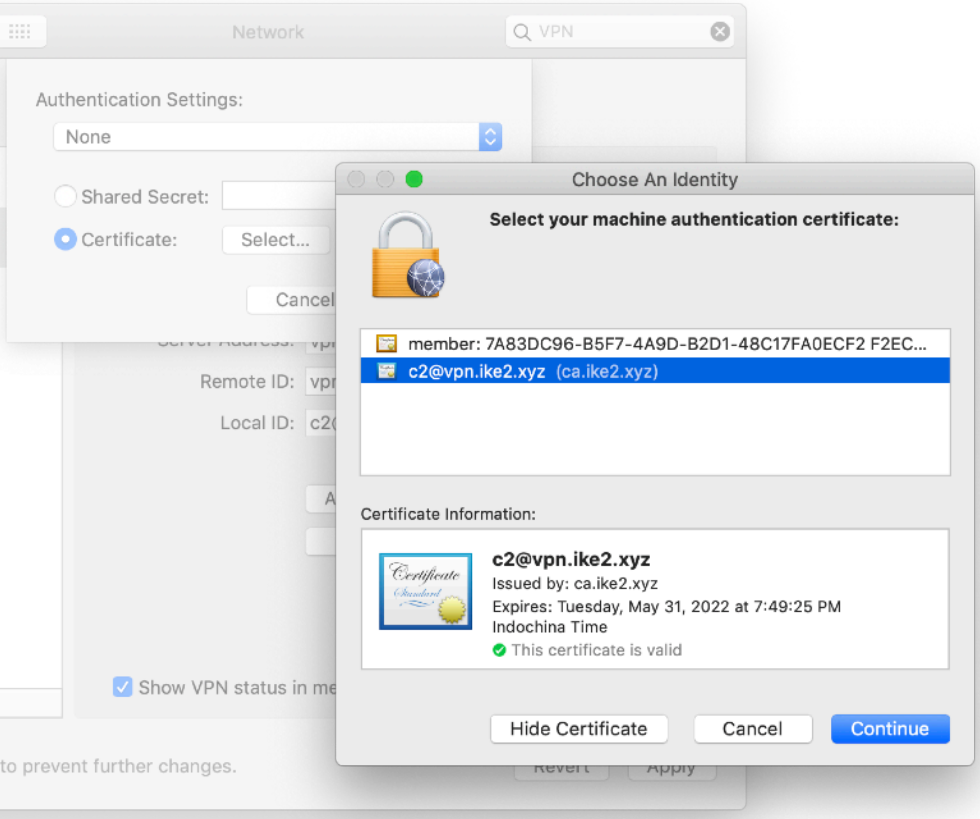
Authentication Settings:

**None**

Certificate:

**–> Select**

# MacOS: Настройка IKEv2 VPN соединения



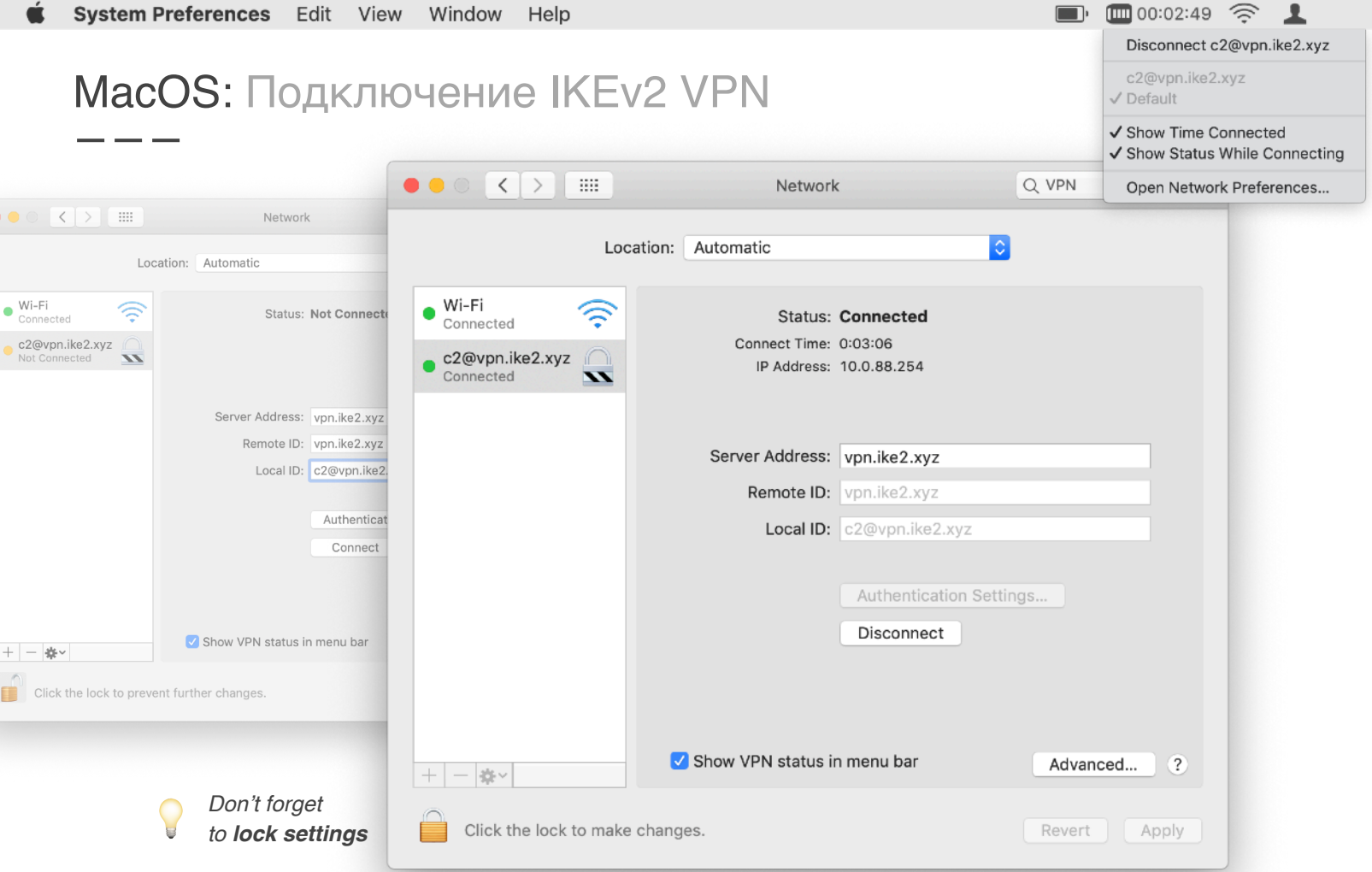

## Authentication Settings

Select machine auth certificate:

**`c2@vpn.ike2.xyz`**

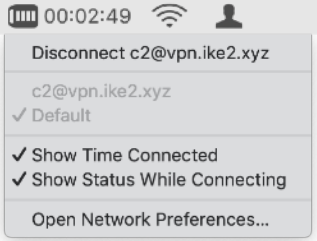
**`–> Continue`**

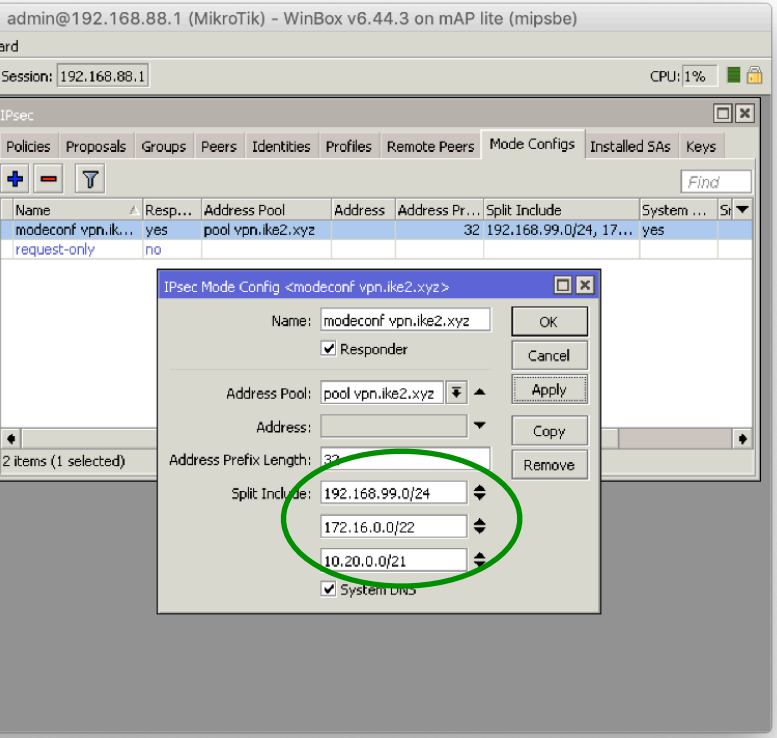
# MacOS: Подключение IKEv2 VPN

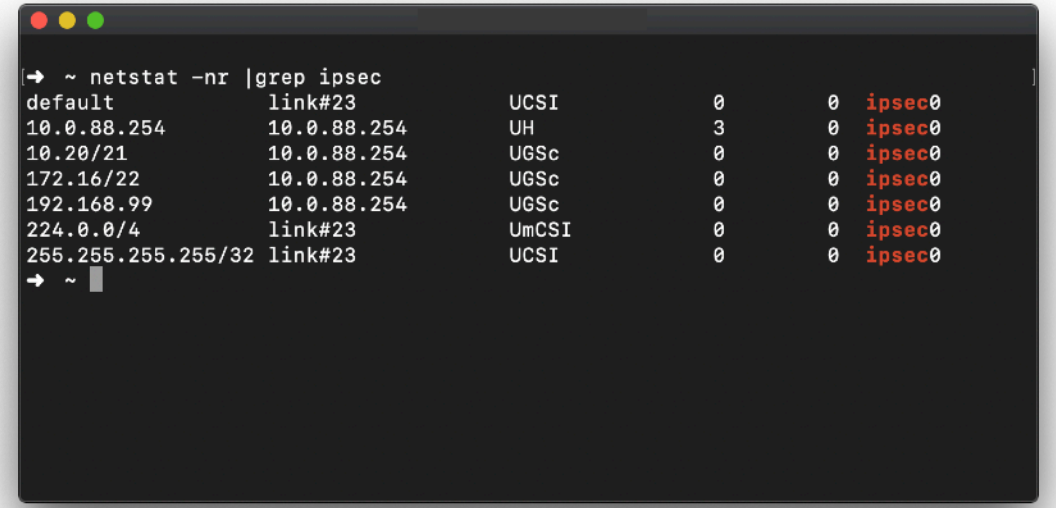



*Don't forget to **lock settings***

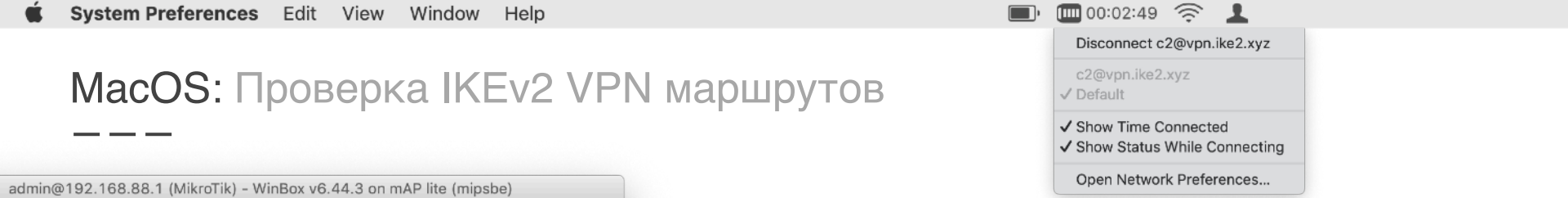
# MacOS: Проверка IKEv2 VPN маршрутов

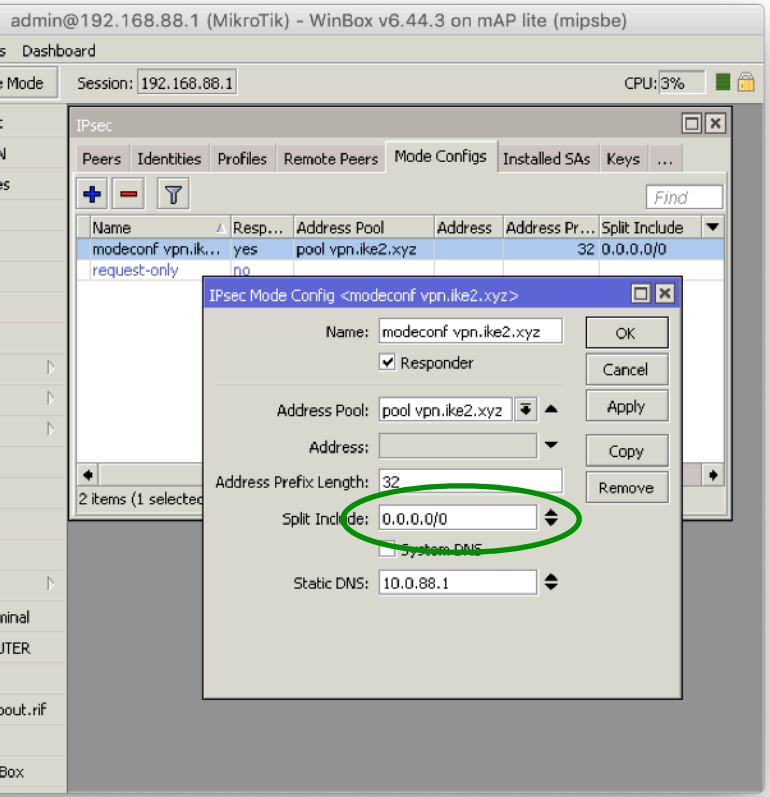


# MacOS: Проверка IKEv2 VPN маршрутов




```
➜  ~ netstat -nr |grep ipsec
default            link#23            UCS          1614        0  ipsec0
1.         9       link#23            UHW3I           0        1  ipsec0      !
1.       159       link#23            UHW3I           0        1  ipsec0      !
1.      .112       link#23            UHW3I           0        1  ipsec0      !
1.      .222       link#23            UHW3I           0        1  ipsec0      !
1.      .131       link#23            UHW3I           0        1  ipsec0      !
1.       .22       link#23            UHW3I           0        1  ipsec0      !
1.        31       link#23            UHW3I           0        1  ipsec0      !
1.       143       link#23            UHW3I           0        1  ipsec0      !
2.       156       link#23            UHW3I           0        1  ipsec0      2
2.        64       link#23            UHW3I           0        1  ipsec0      !
2.        27       link#23            UHW3I           0        1  ipsec0      !
2.        01       link#23            UHW3I           0        1  ipsec0      !
2.       204       link#23            UHW3I           0        1  ipsec0      !
2.        23       link#23            UHW3I           0        1  ipsec0      1
2.         5       link#23            UHW3I           0        1  ipsec0      !
2.        53       link#23            UHW3I           0        1  ipsec0      !
2.        21       link#23            UHW3I           0        1  ipsec0      !
2.        33       link#23            UHW3I           0        1  ipsec0      !
2.      .111       link#23            UHW3I           0        5  ipsec0      1
2.       .62       link#23            UHW3I           0        1  ipsec0      !
2.       100       link#23            UHW3I           0        1  ipsec0      2
2.        95       link#23            UHW3I           0        1  ipsec0      !
```

# Apple iOS

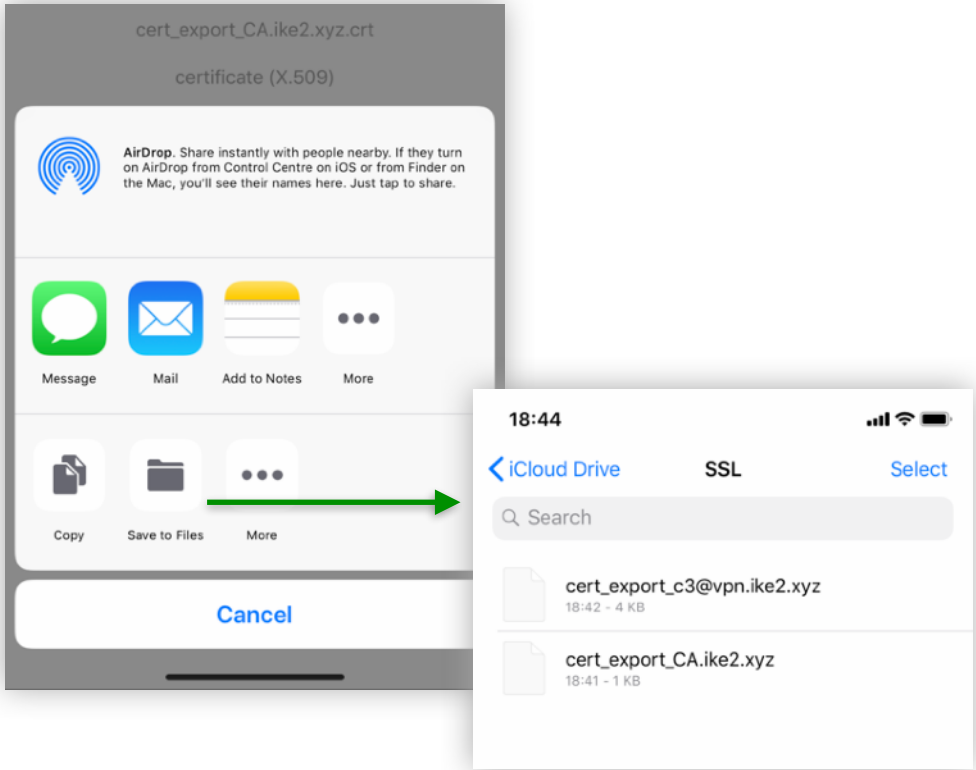
≥ версия 9

План действий

1. Импорт SSL сертификатов
2. Настройка IKEv2 VPN соединения

Nikita Tarikin / nikita@tarikin.com

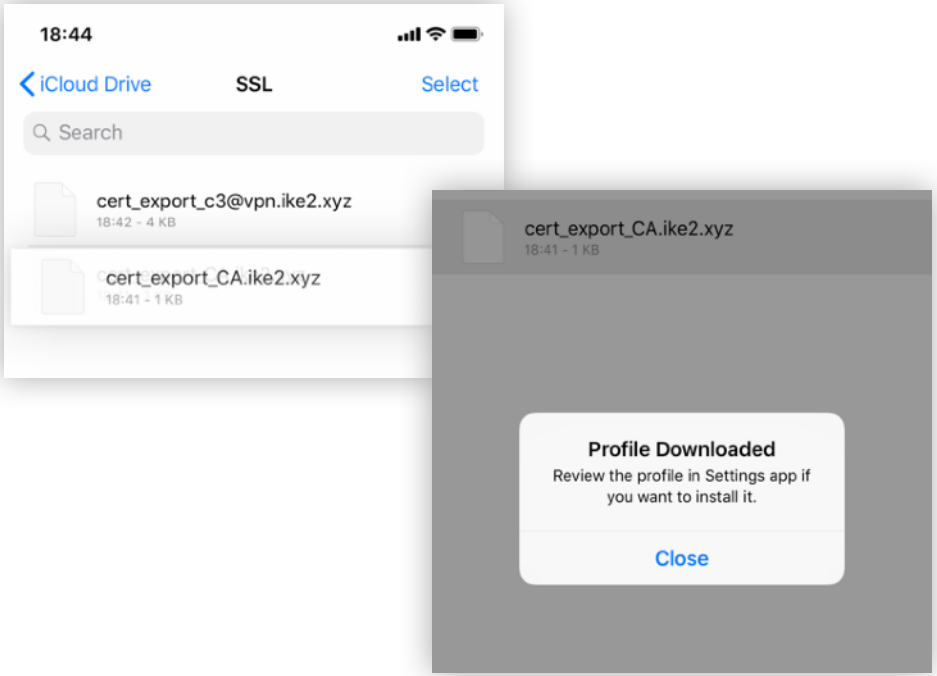
# iOS: Загрузка SSL сертификатов



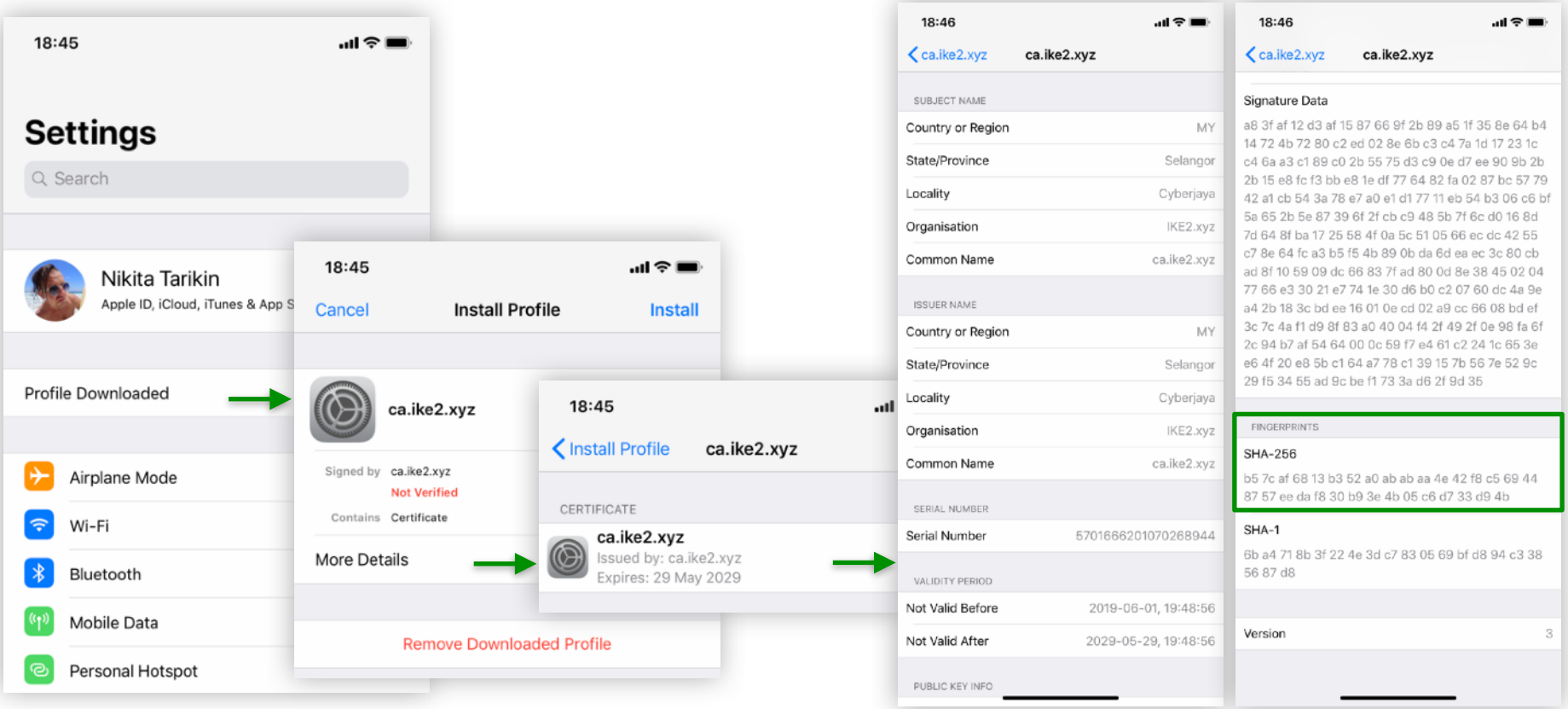

Download **CA** certificate .crt

Download **client** certificate .p12

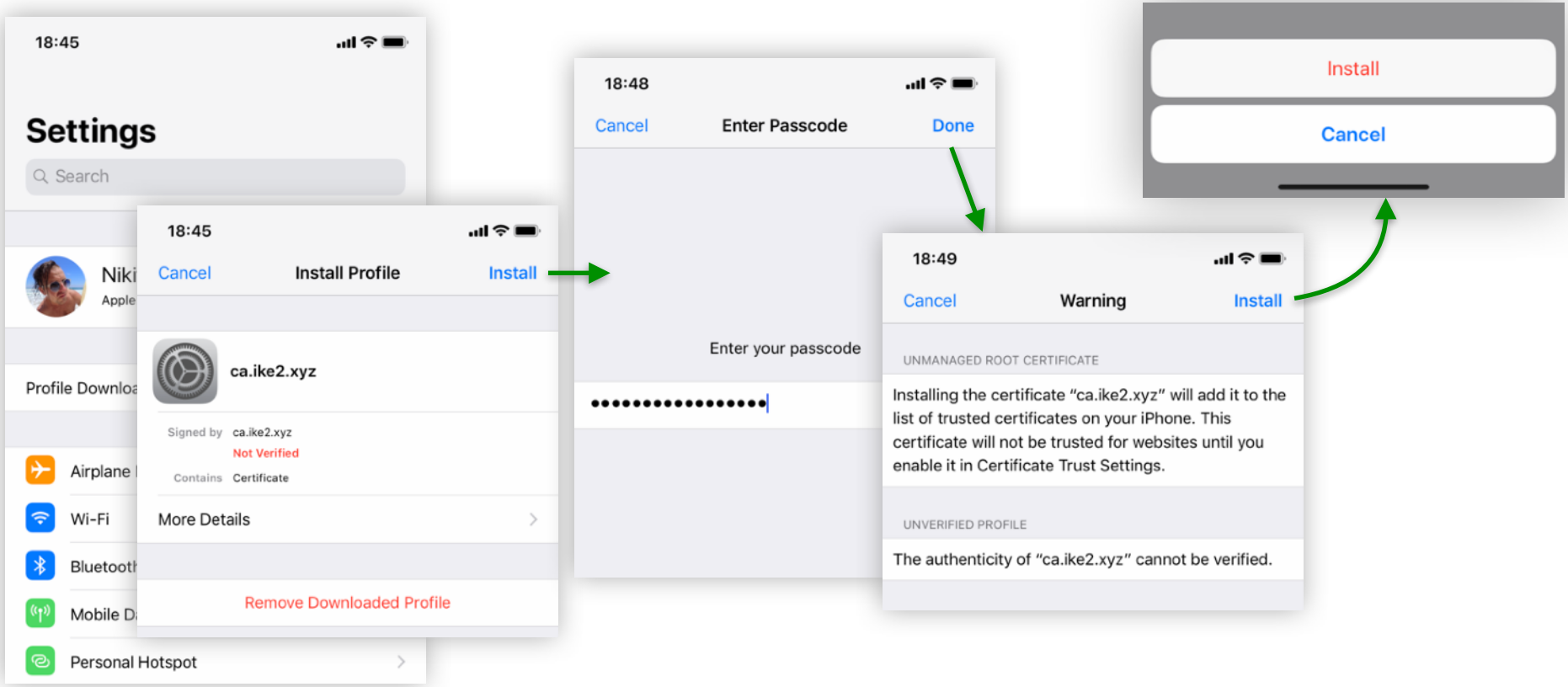
# iOS: Импорт SSL сертификата авторитета CA



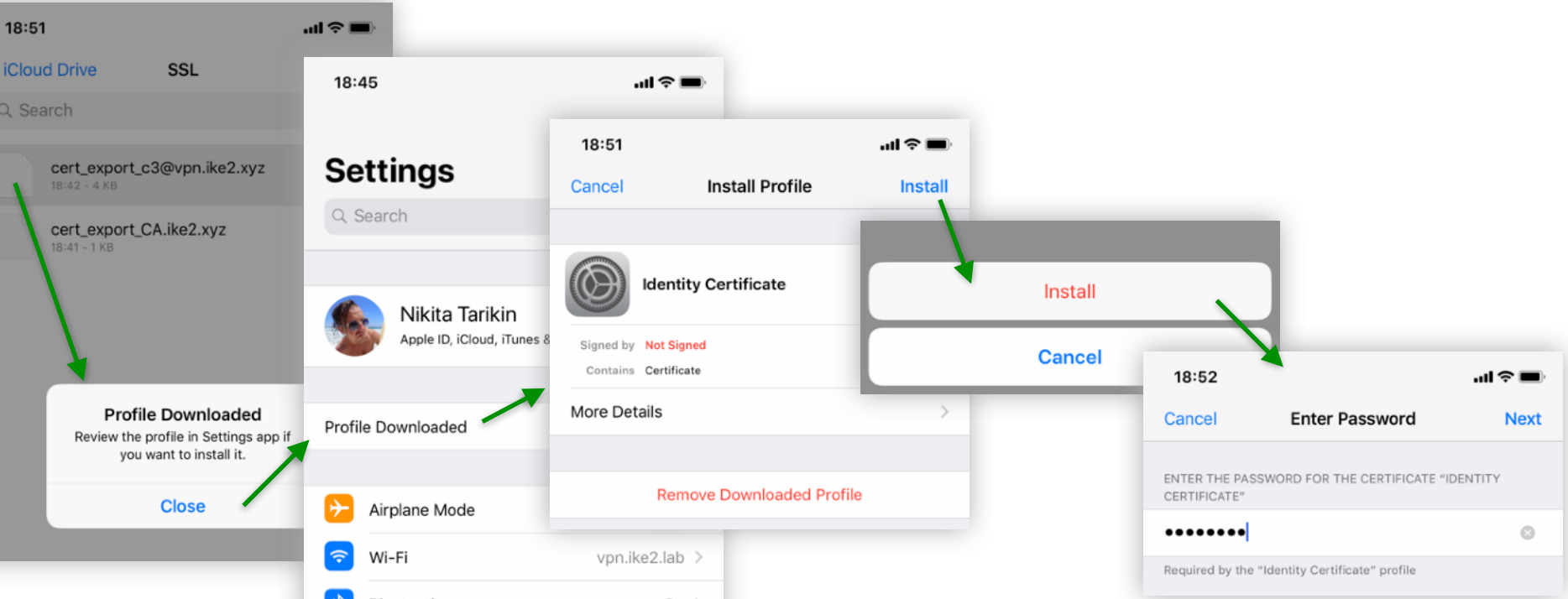
# iOS: Импорт SSL сертификата авторитета CA



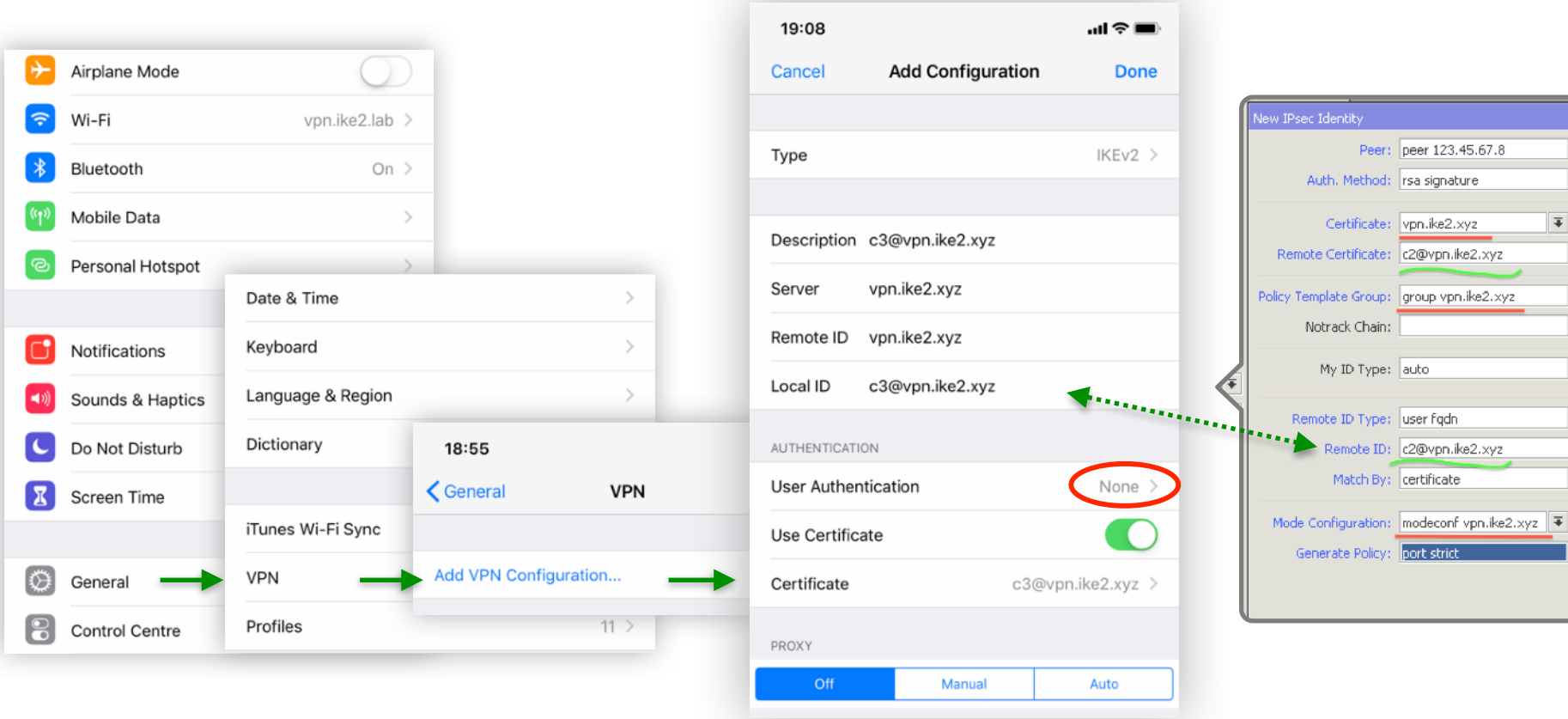
# iOS: Импорт SSL сертификата авторитета CA



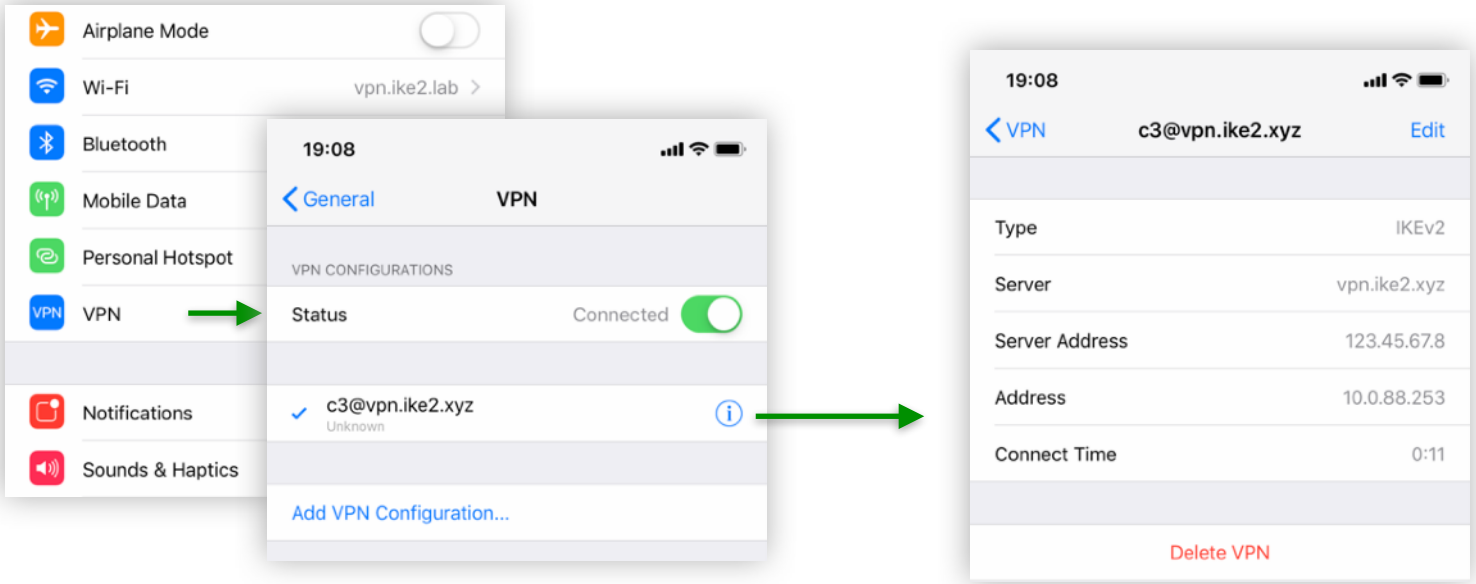
# iOS: Импорт SSL сертификата клиента



# iOS: Настройка IKEv2 VPN соединения



# iOS: Подключение IKEv2 VPN



# Android

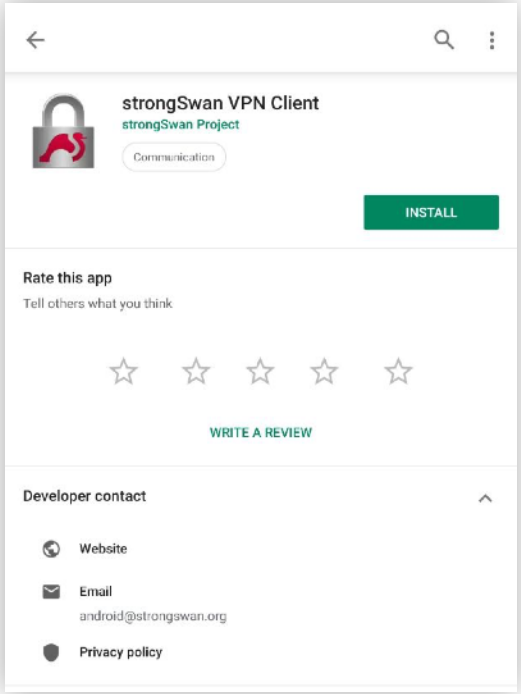
версия 9 <

План действий

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

Nikita Tarikin / nikita@tarikin.com

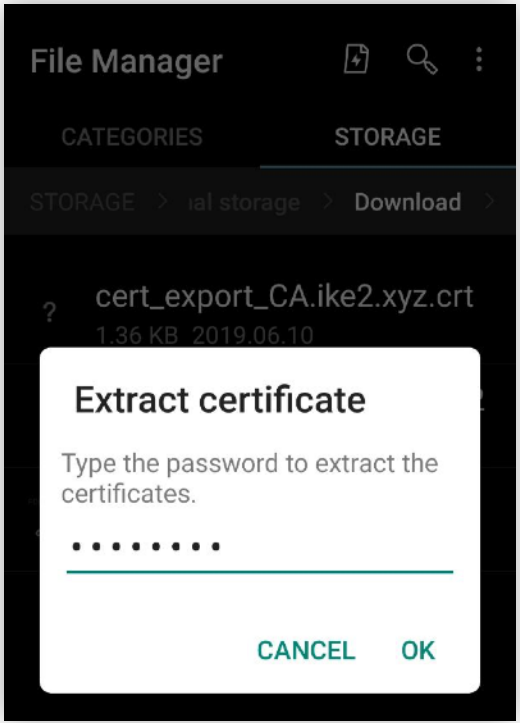
# Android: Установка StrongSwan

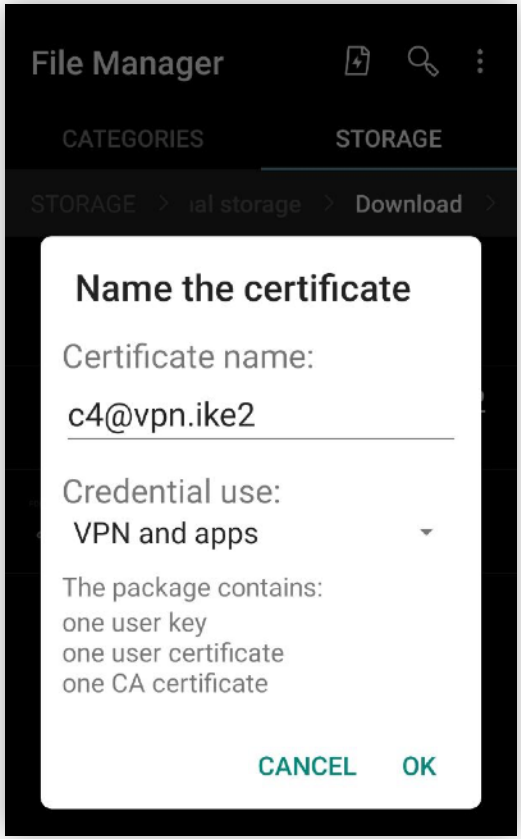



Найти и установить **StrongSwan**

через Google Play

# Android: Импорт SSL сертифкатов

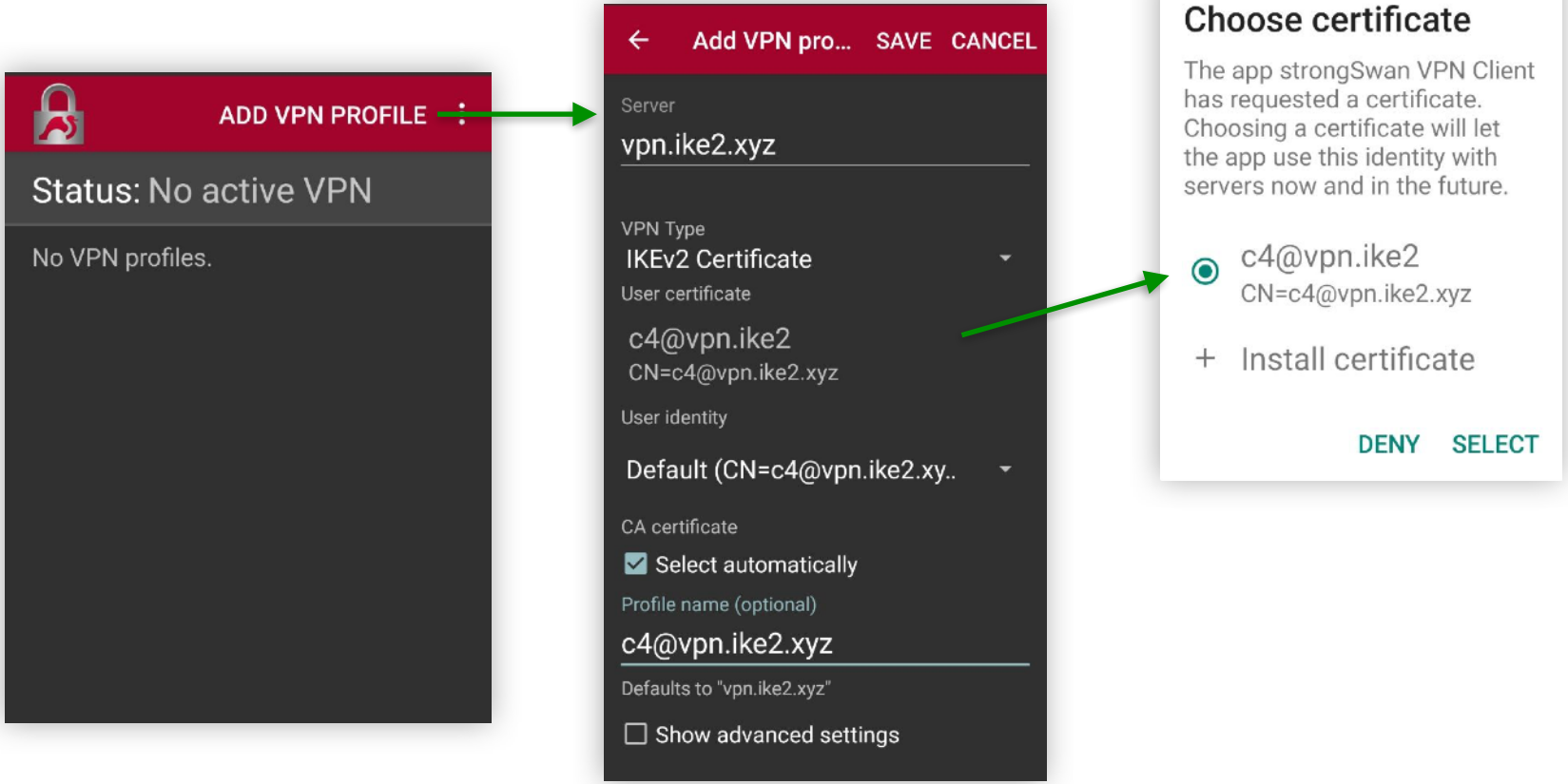


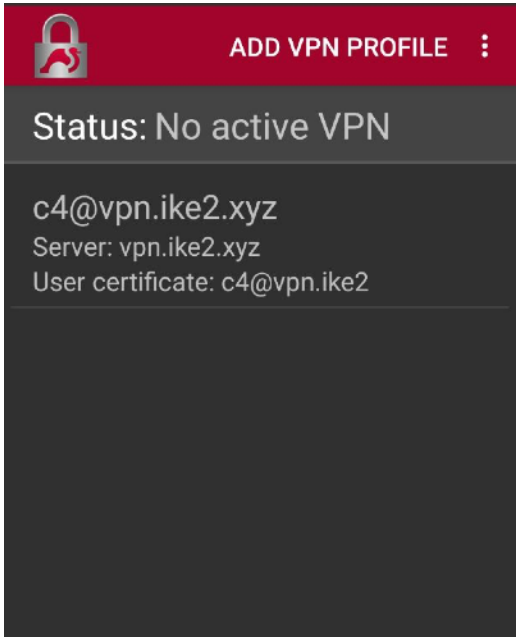

Download and install

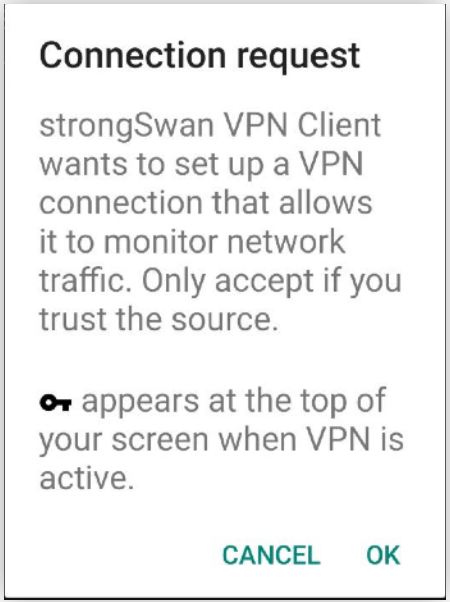
**user** certificate .p12

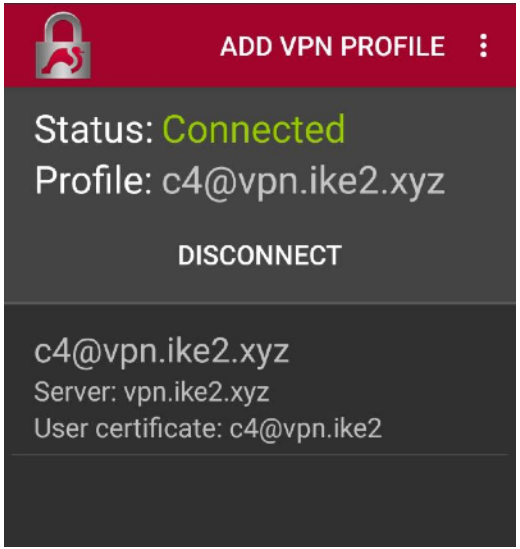
# Android: Настройка IKEv2 VPN соединения



# Android: Подключение IKEv2 VPN

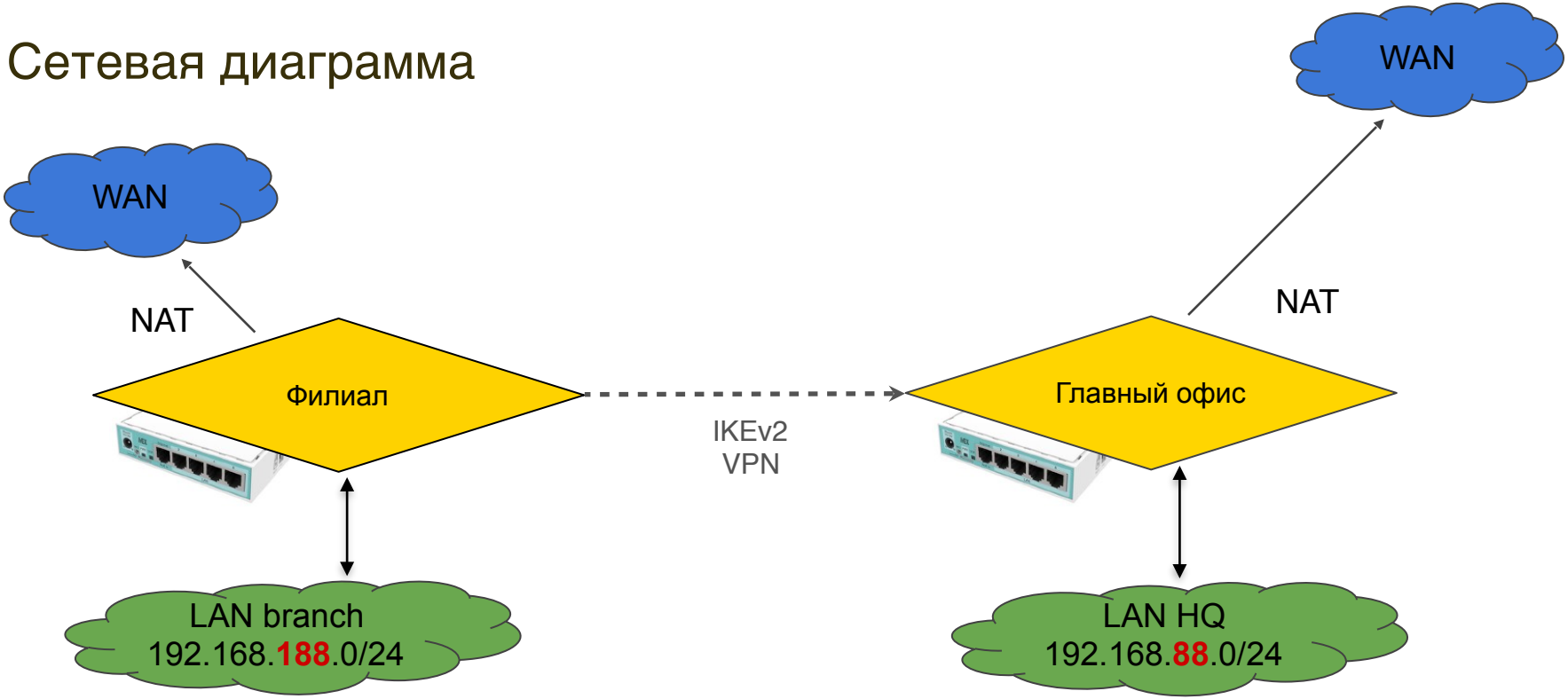


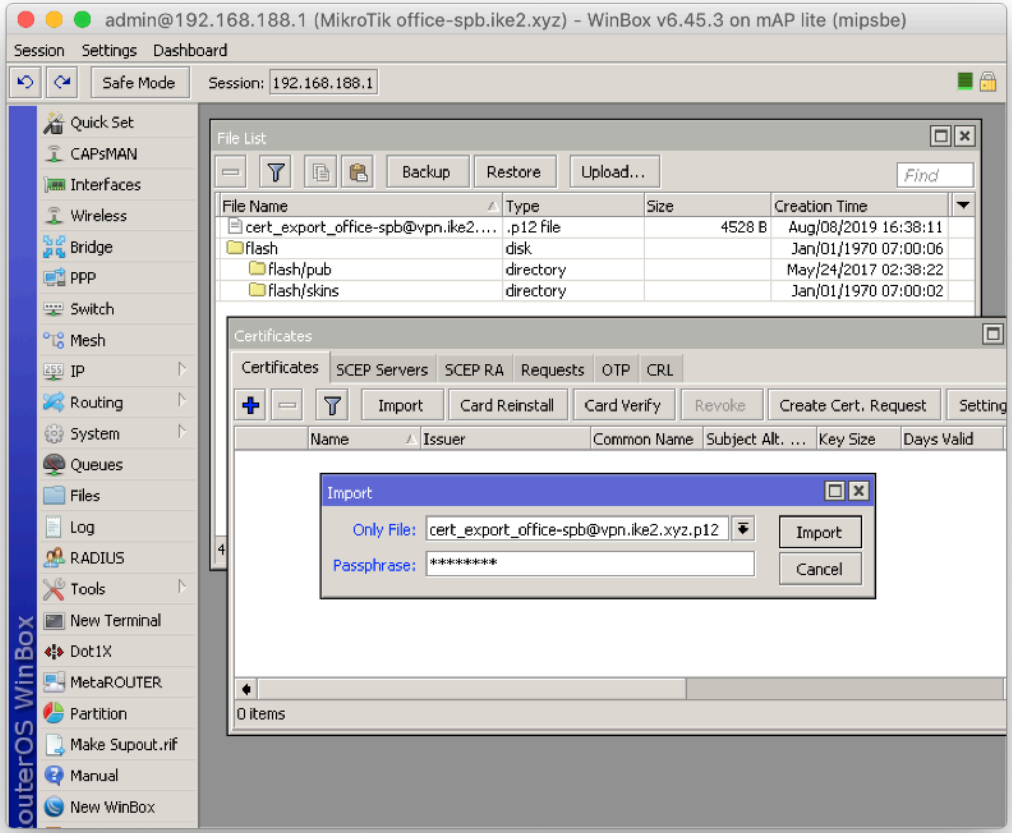



# Подключение RouterOS

# Сетевая диаграмма

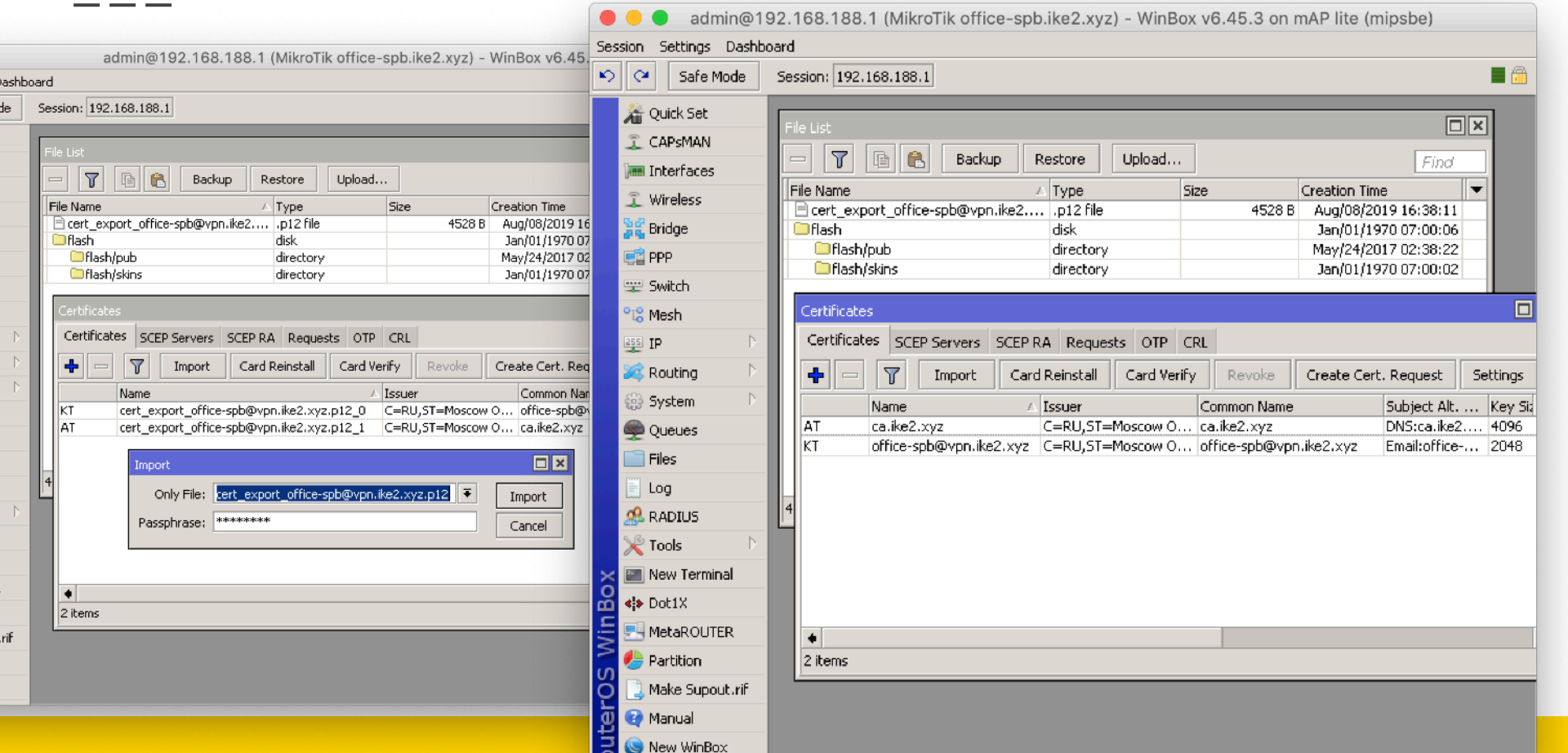


# Загрузка и установка клиентского SSL сертификата

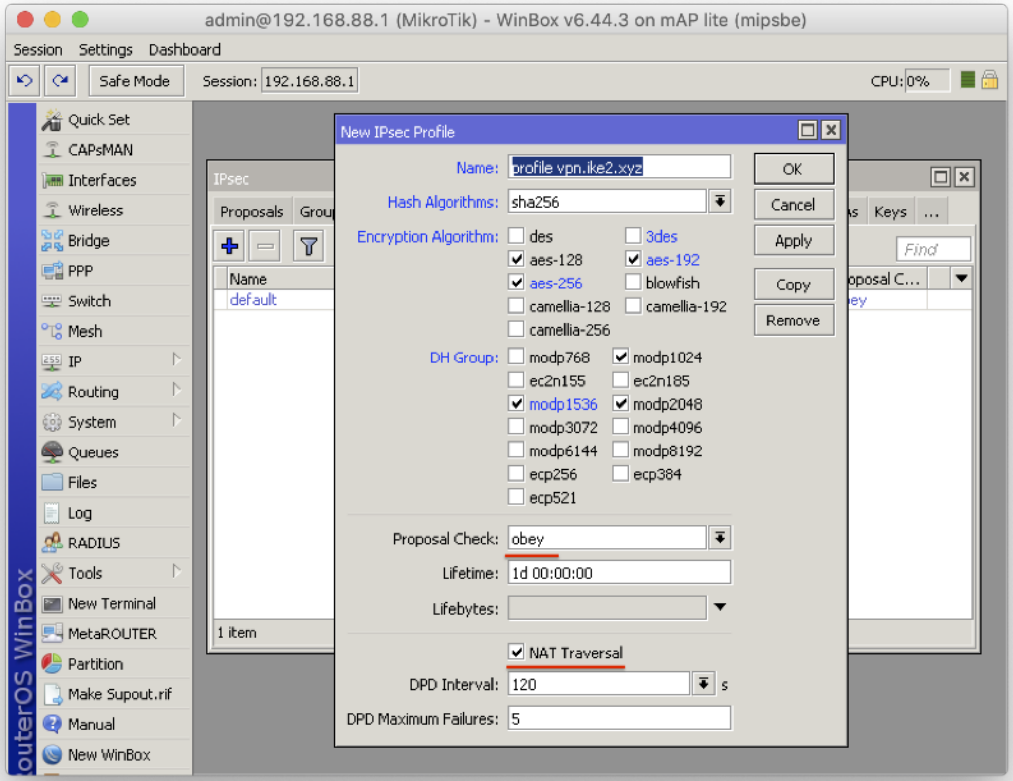



```
/certificate import file-
name=cert_export_office-
spb@vpn.ike2.xyz.p12
```

# Переименовываем установленные SSL сертификаты

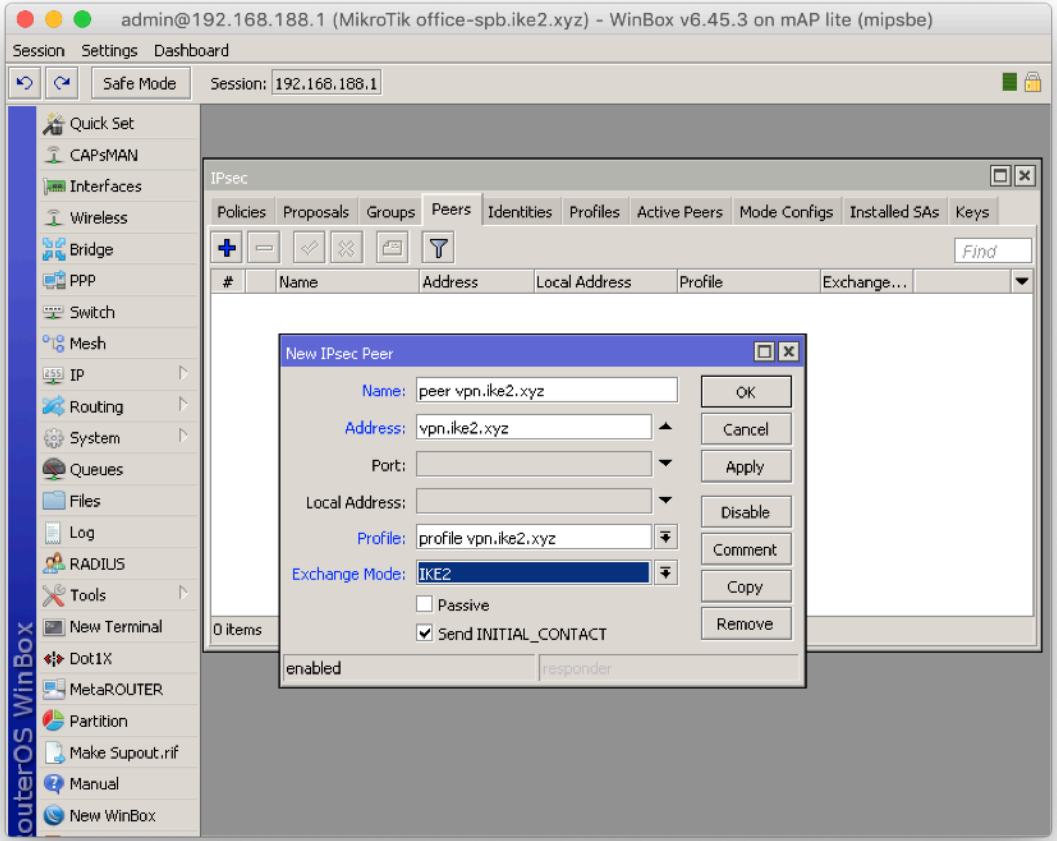


# Настройка нового IPSec peer profile *(фаза 1)*



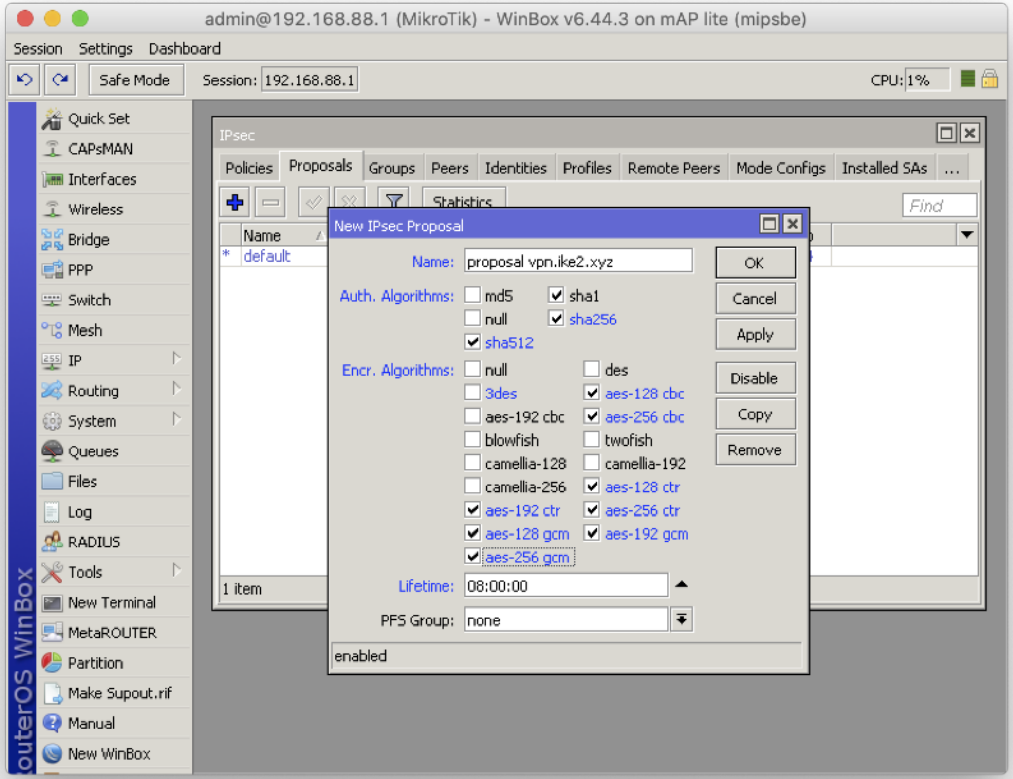

```
/ip ipsec profile add dh-
group=modp2048,modp1536,modp10
24 enc-
algorithm=aes-256,aes-192,aes-
128 hash-algorithm=sha256
name="profile vpn.ike2.xyz"
nat-traversal=yes proposal-
check=obey
```

# Добавление нового клиентского IPSec peer (инициатор)



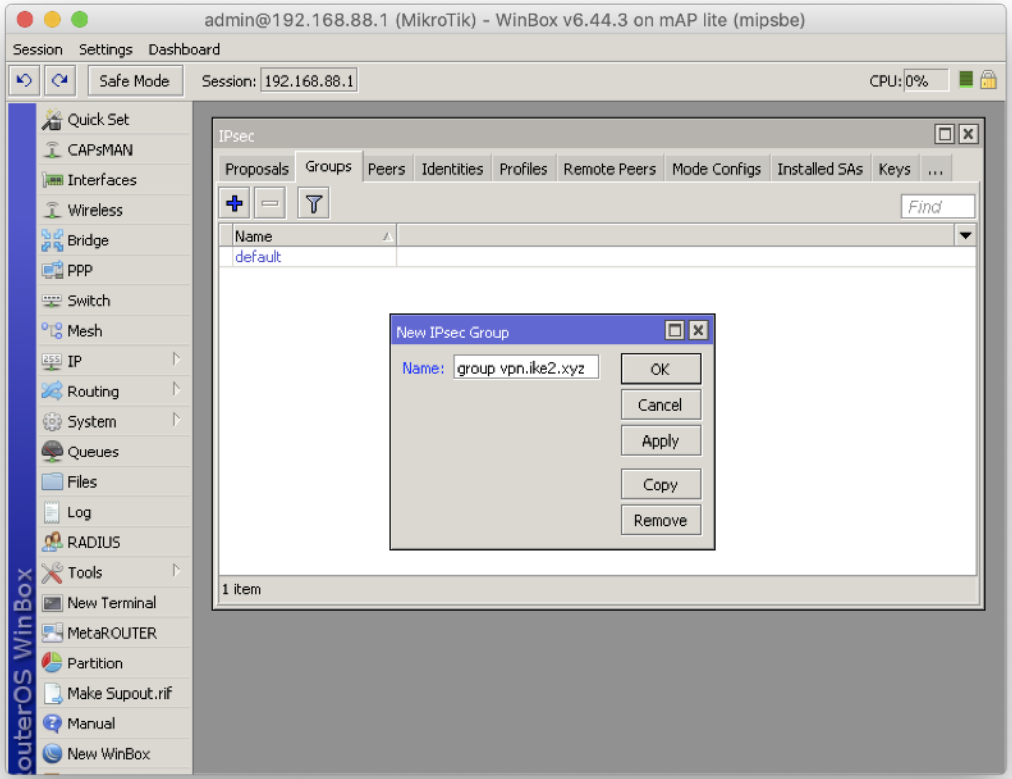

```
/ip ipsec peer
add address=vpn.ike2.xyz exchange-
mode=ike2 name="peer vpn.ike2.xyz"
profile="profile vpn.ike2.xyz"
```

# Настройка нового IPSec proposal *(фаза 2)*



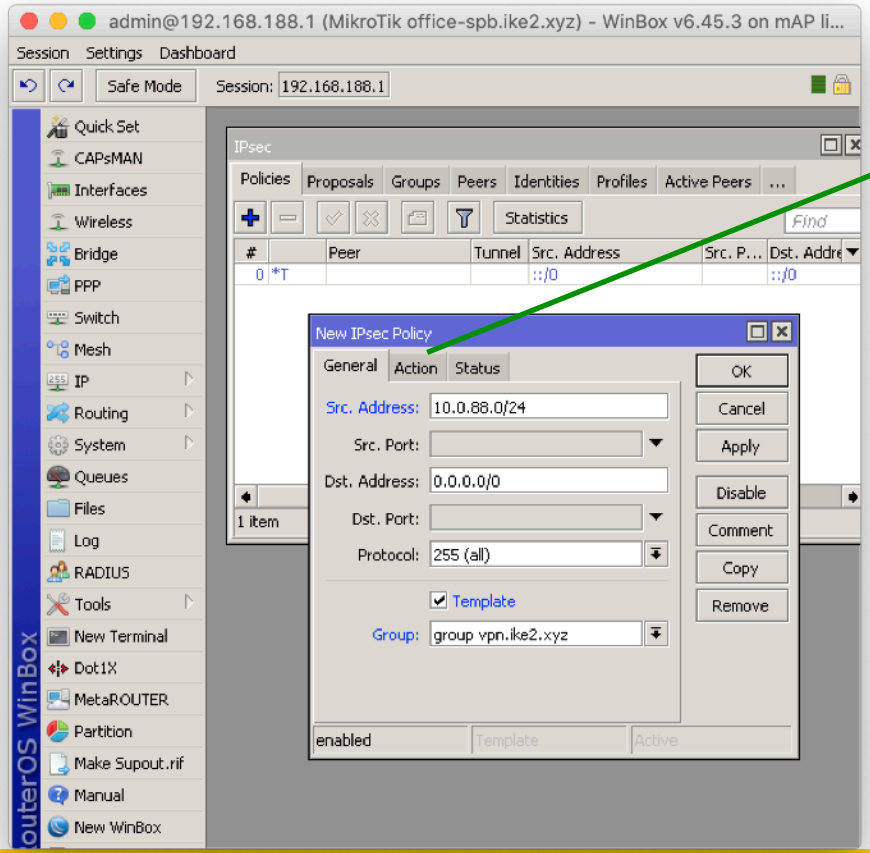

```
/ip ipsec proposal add auth-
algorithms=sha512,sha256,sha1
enc-algorithms=aes-256-
cbc,aes-256-ctr,aes-256-
gcm,aes-192-ctr,aes-192-
gcm,aes-128-cbc,aes-128-
ctr,aes-128-gcm lifetime=8h
name="proposal vpn.ike2.xyz"
pfs-group=none
```

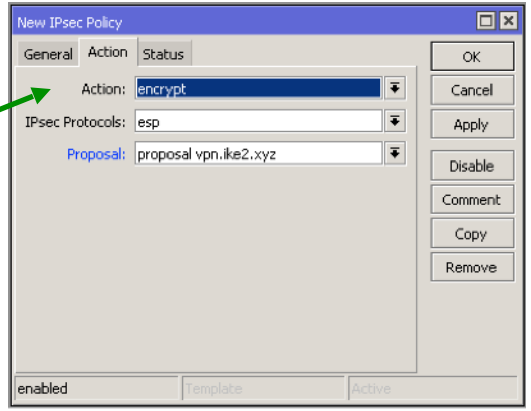
# Добавление новой IPSec policy group




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

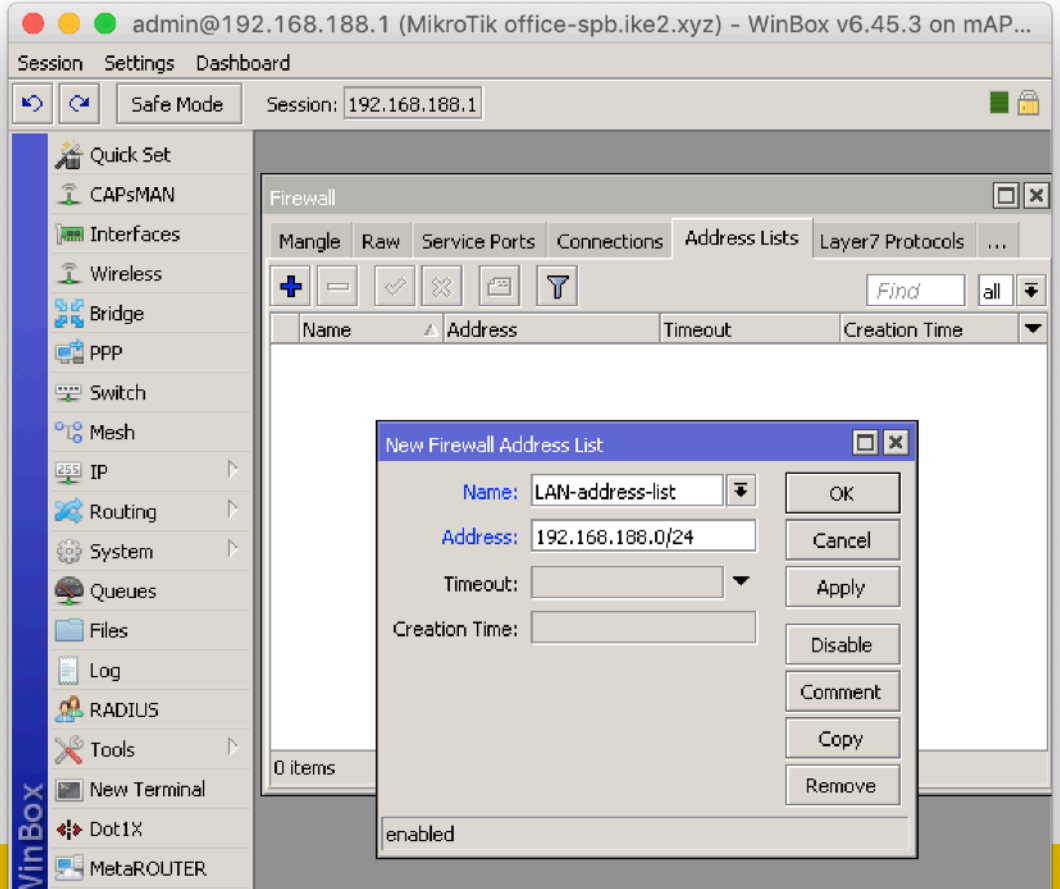
# Добавление нового шаблона IPSec policy



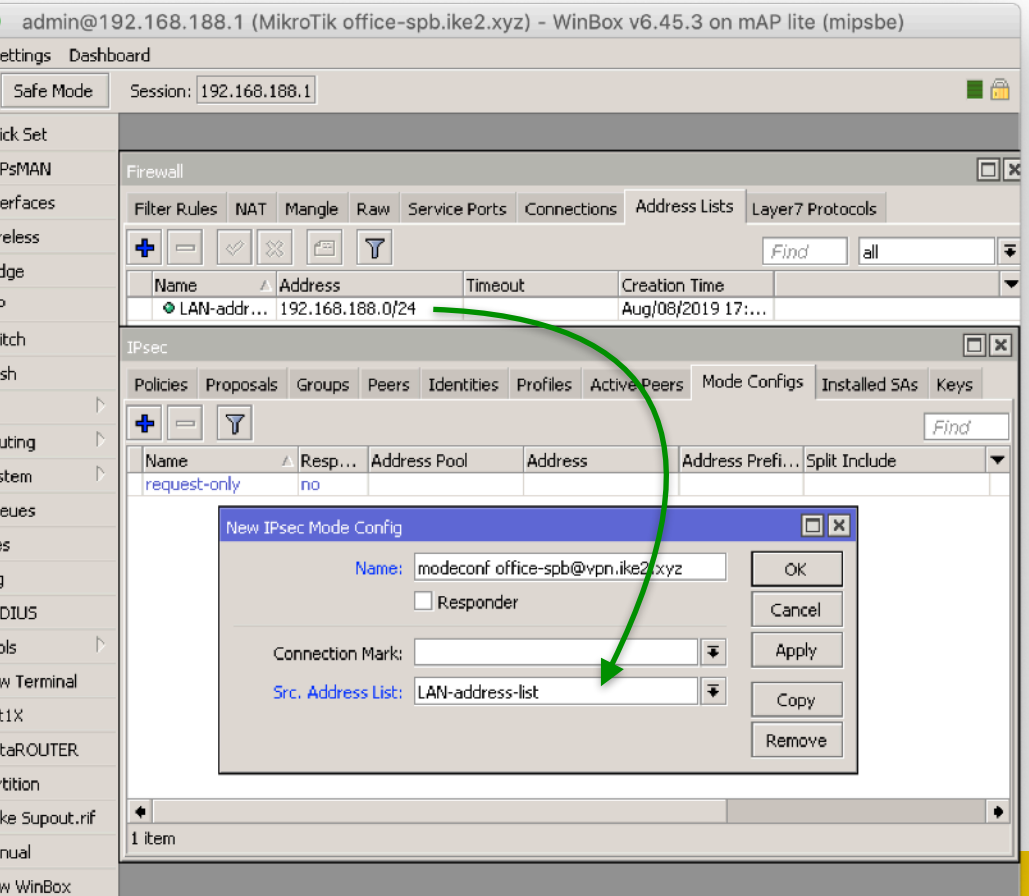

```
/ip ipsec policy
add comment="policy template vpn.ike2.xyz"
dst-address=0.0.0.0/0 group="group
vpn.ike2.xyz" proposal="proposal vpn.ike2.xyz"
src-address=10.0.88.0/24 template=yes
```

# Добавление нового списка LAN сетей в firewall address list



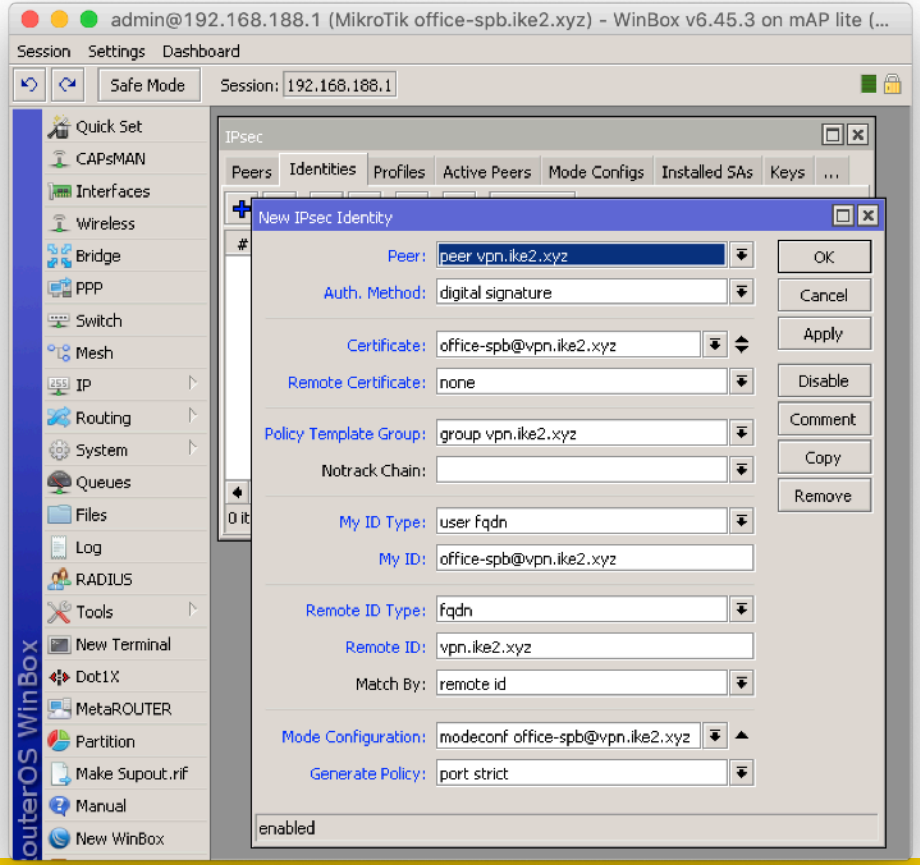

```
/ip firewall address-list
add address=192.168.188.0/24
list=LAN-address-list
```

# Добавление нового клиента IPSec modeconf (инициатор)




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

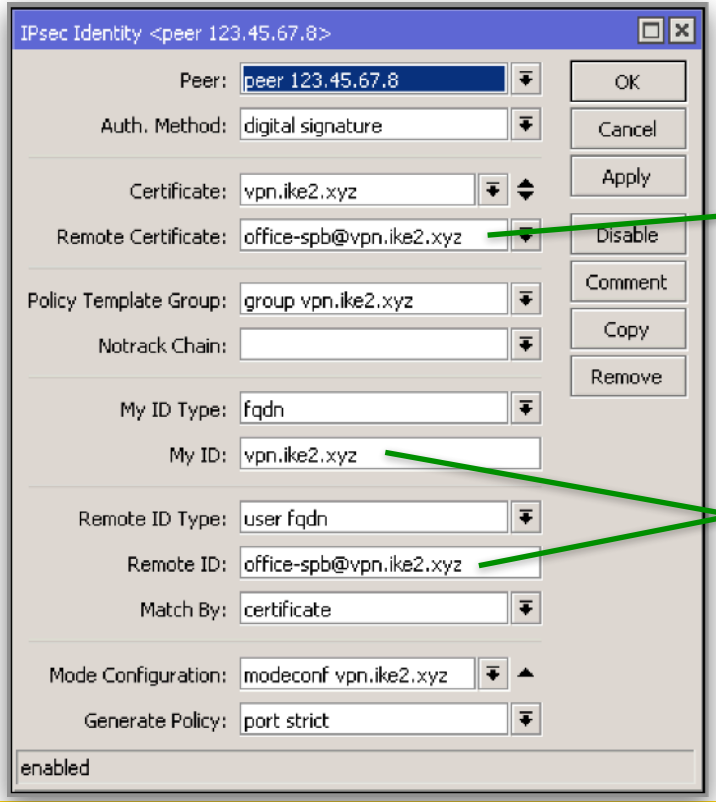
# Добавление нового удостоверения IPSec identity



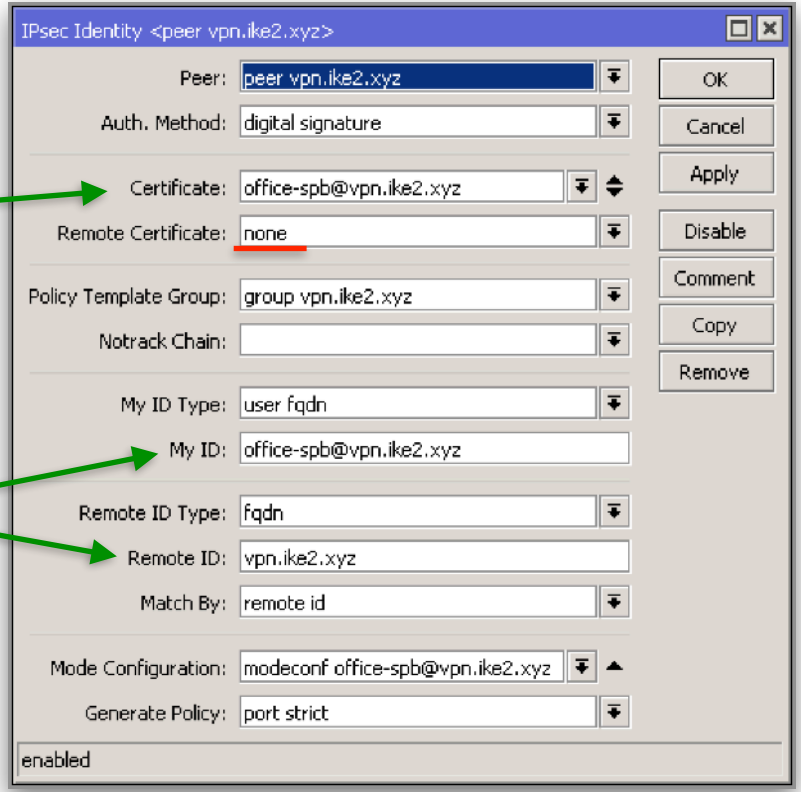

```
/ip ipsec identity
add auth-method=digital-signature
certificate=office-spb@vpn.ike2.xyz
generate-policy=port-strict mode-
config="modeconf office-spb@vpn.ike2.xyz"
my-id=user-fqdn:office-spb@vpn.ike2.xyz
peer="peer vpn.ike2.xyz" policy-template-
group="group vpn.ike2.xyz" remote-
id=fqdn:vpn.ike2.xyz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

# Сверка удостоверений IPSec identity

Сервер

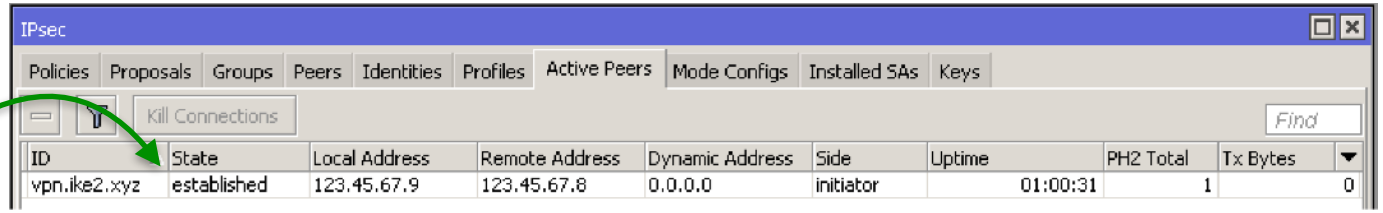



Клиент

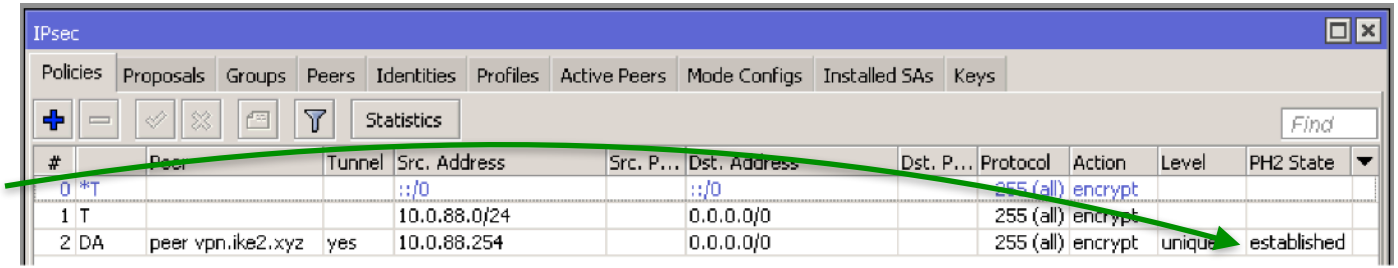


# Проверка связи IKEv2

Active peers
**state: established**




Генерирована
динамическая policy
**PH state: established**



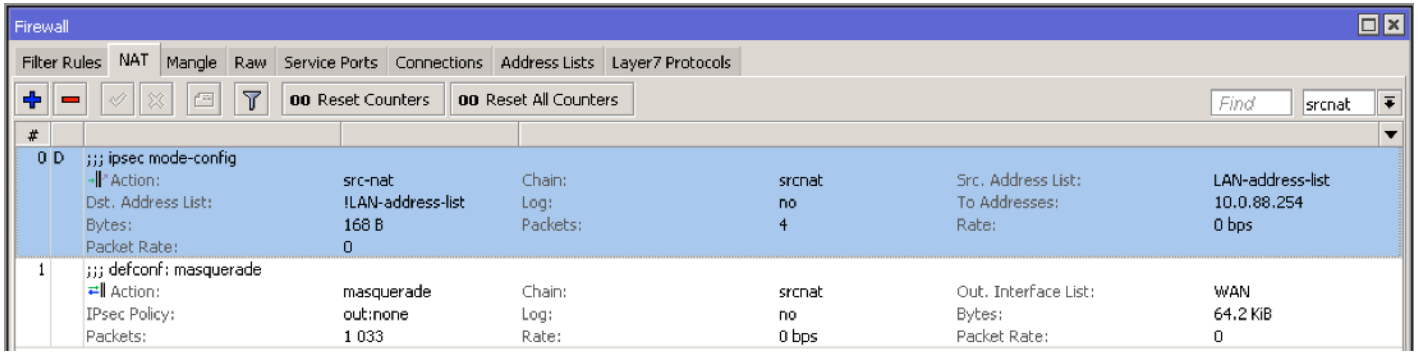

**Peer: authorized**
**Address: acquired**

| | | | |
|---|---|---|---|
| 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




**FROM:** LAN-address-list 192.168.188.0/24

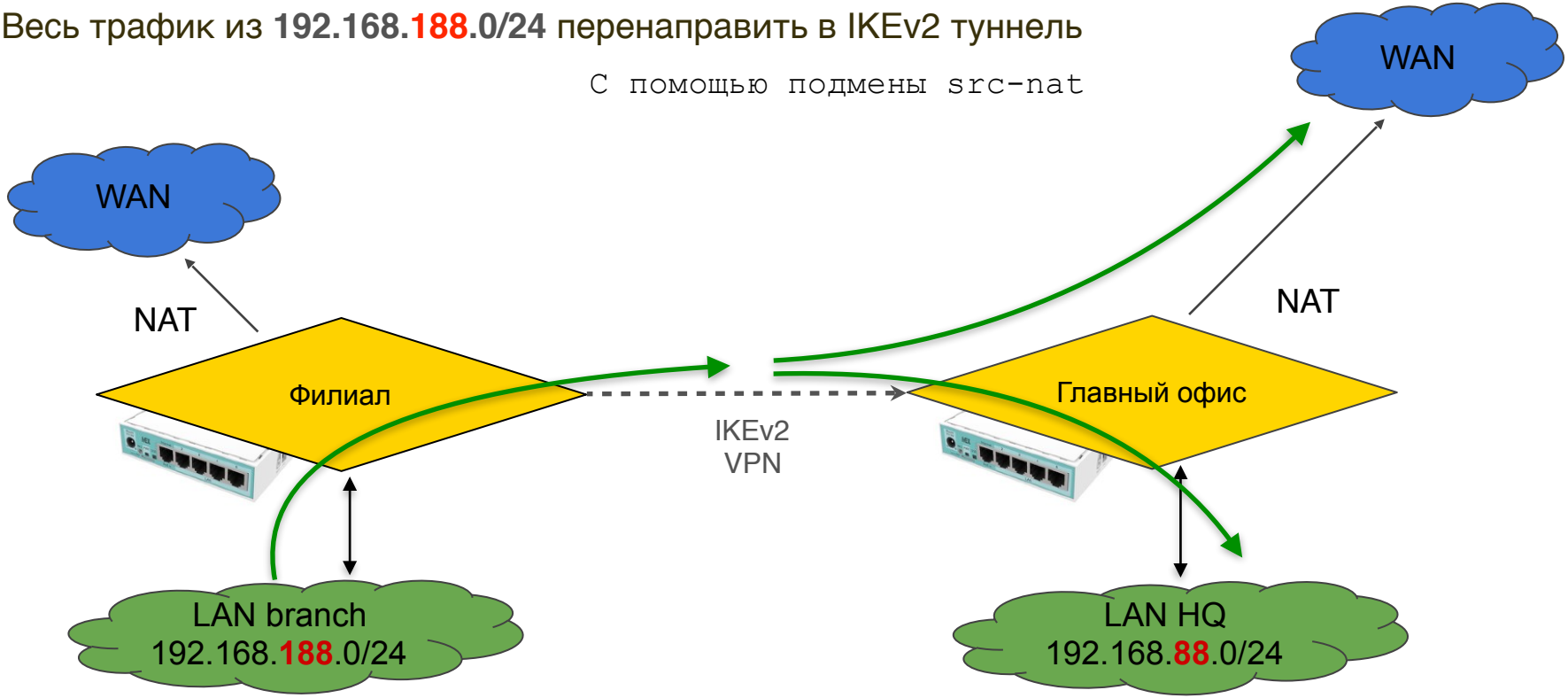
**TO:** NOT-LAN-address-list NOT-192.168.188.0/24

**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

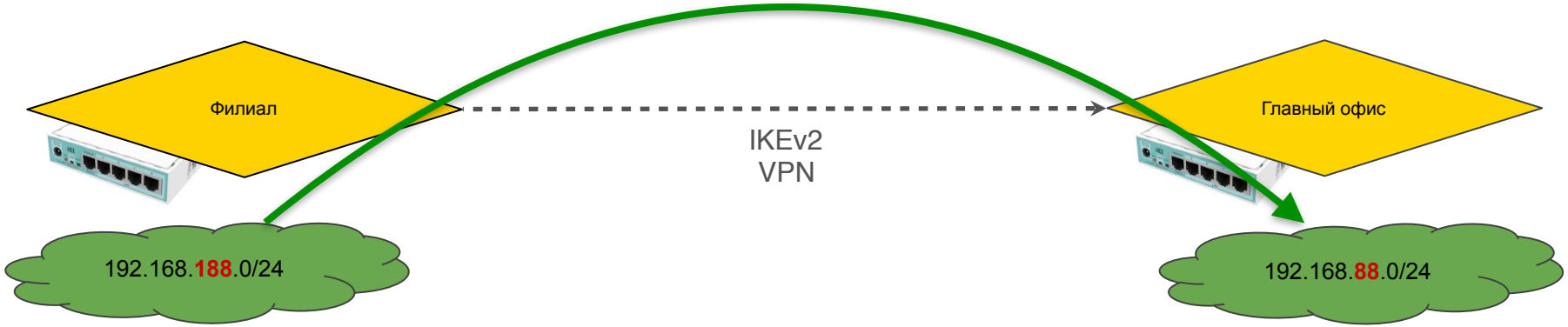
**FROM:** 192.168.188.0/24

**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

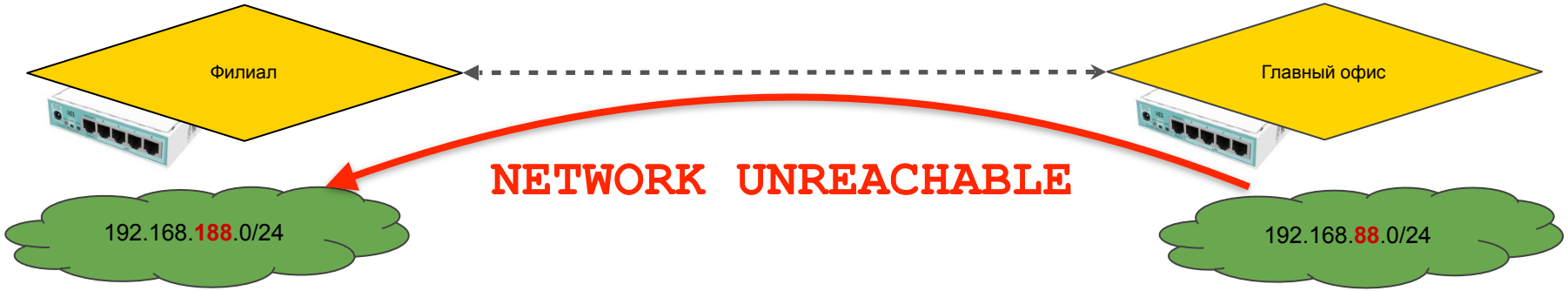
Terminal

```
[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

Nikita Tarikin / nikita@tarikin.com

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)

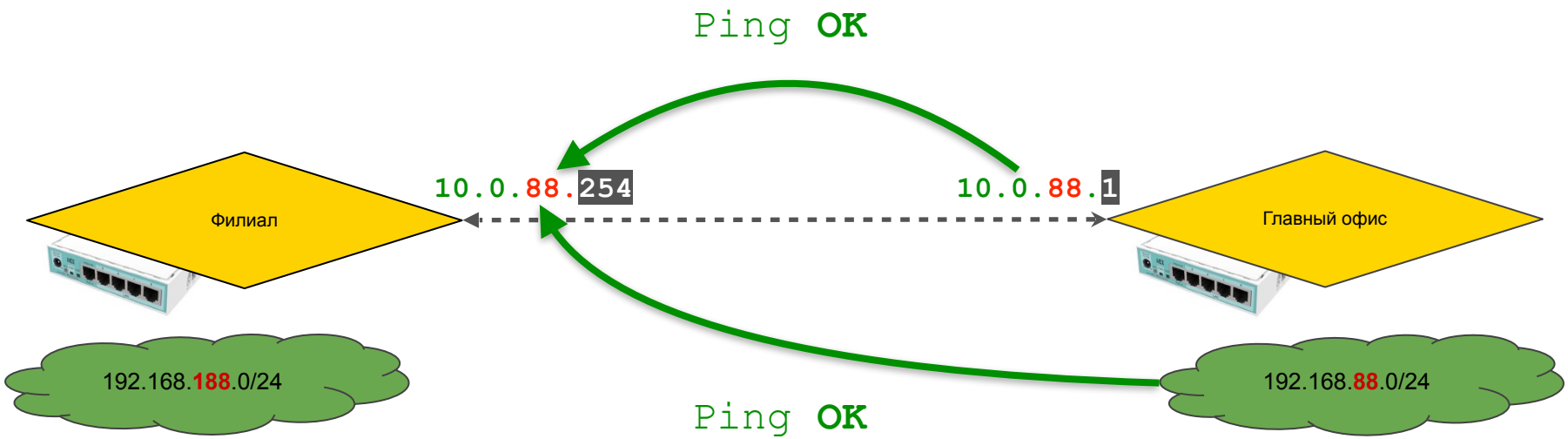
Nikita Tarikin / nikita@tarikin.com

# Проверка связи IKEv2: site-to-site

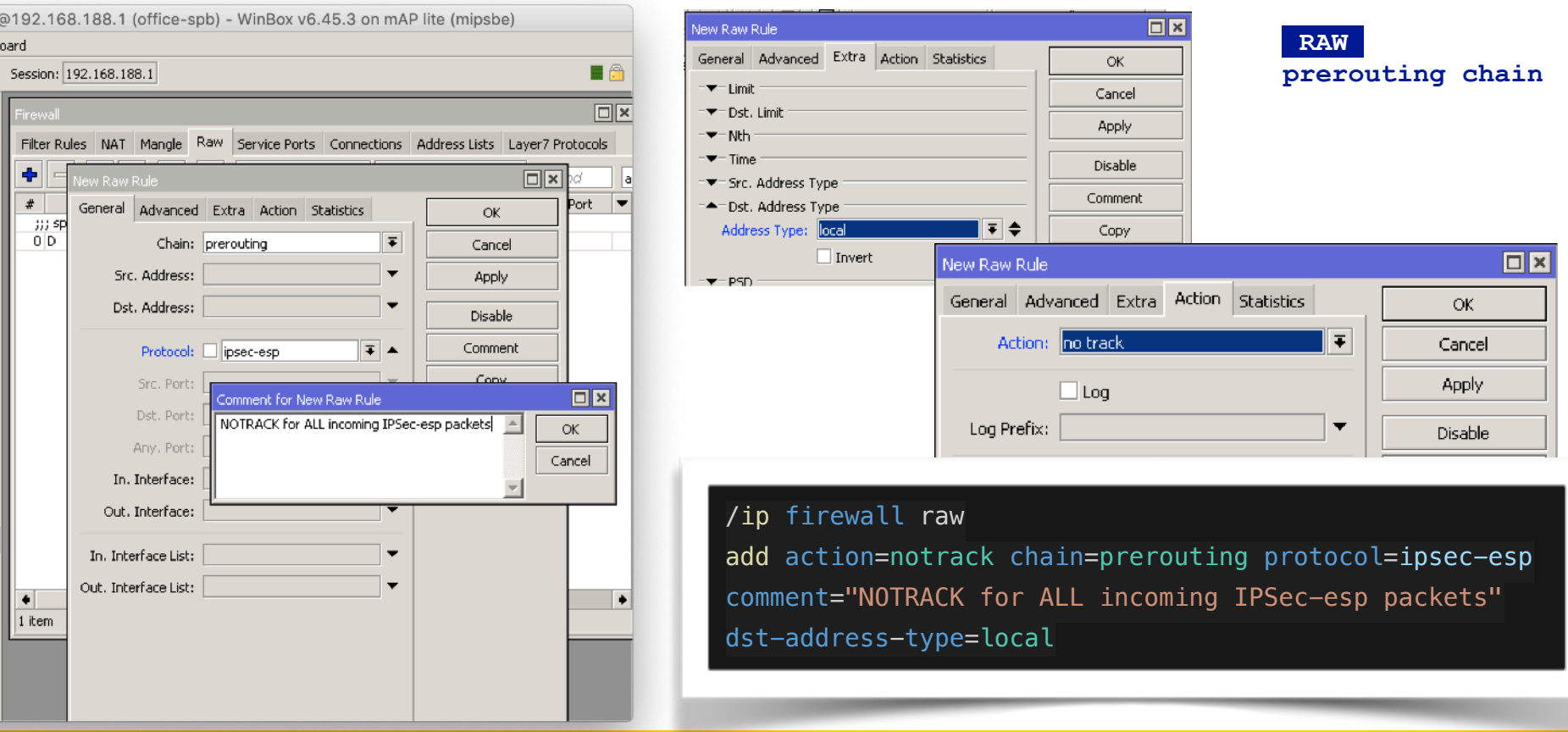
**TO:** 10.0.88.254

**FROM:** 192.168.88.0/24

**FROM:** 10.0.88.1



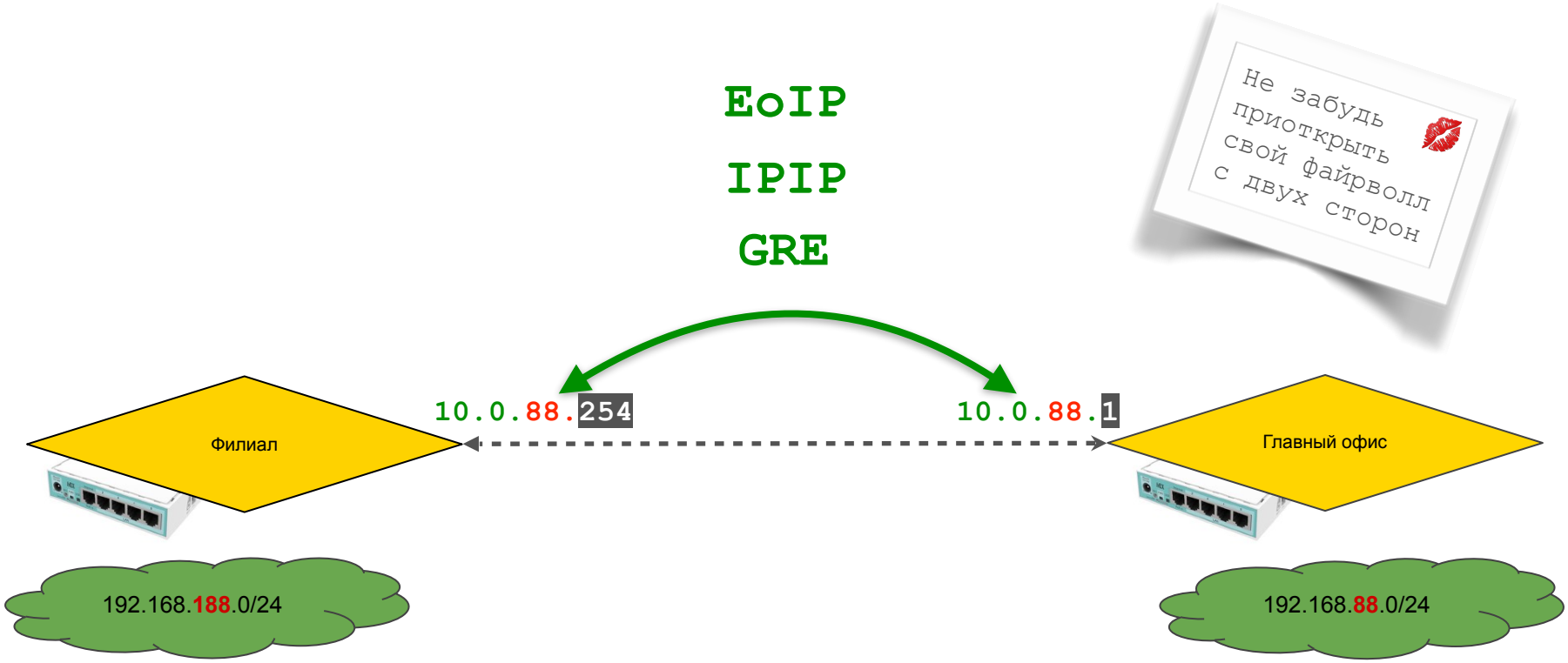
# Пропускаем входящие IPSec-esp пакеты на клиенте *(на всякий случай)*



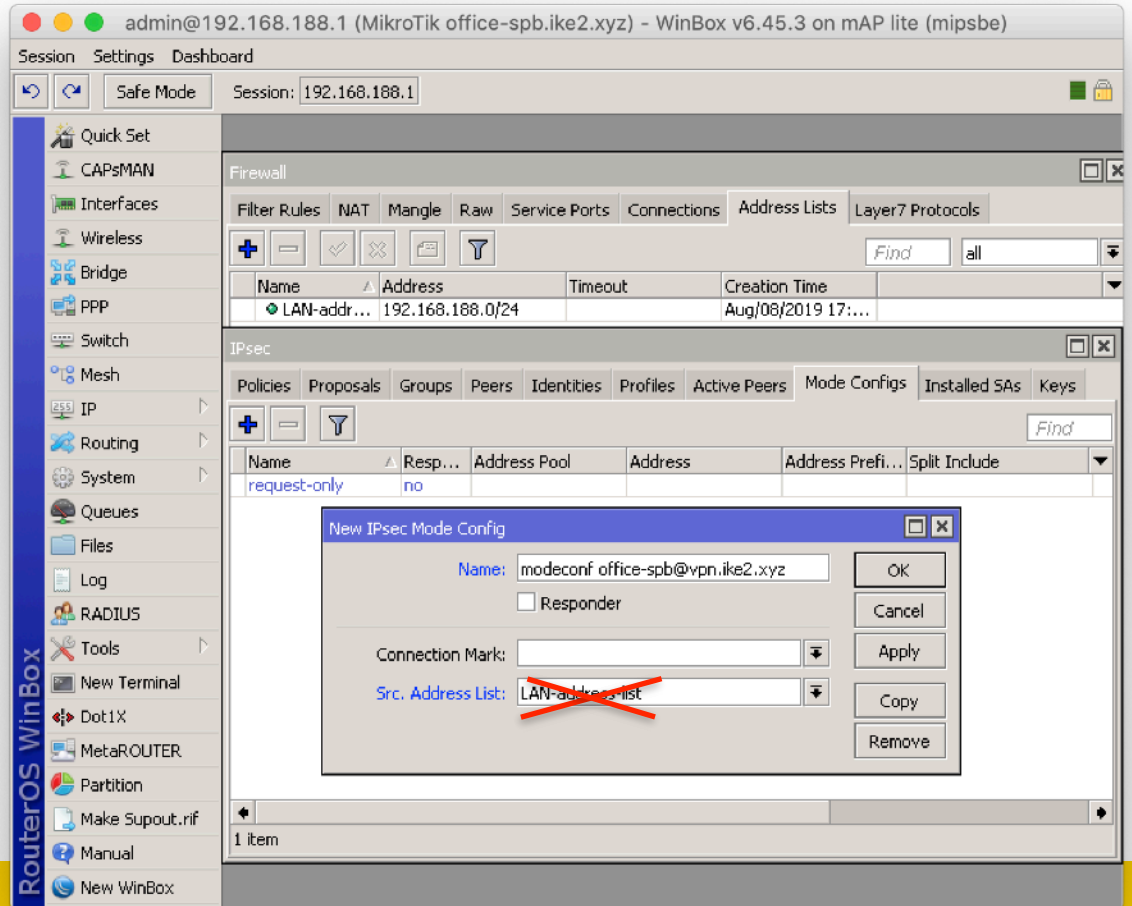

**RAW**
**prerouting chain**

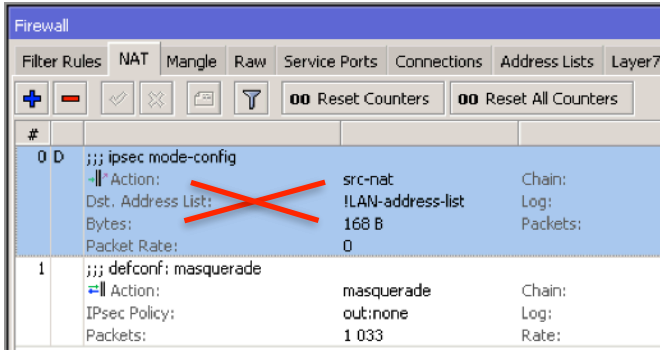
```
/ip firewall raw
add action=notrack chain=prerouting protocol=ipsec-esp
comment="NOTRACK for ALL incoming IPSec-esp packets"
dst-address-type=local
```

# Маршрутизируемый трафик через IKEv2: добавление интерфейса



# Корректируем клиентский IPSec modeconf




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

# Демо лаба.

Открыта до 31 декабря 2019

# Демо лаба

Доступна ~~по подписке~~
халявная 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

**Nikita Tarikin** / nikita@tarikin.com

# Демо лаба

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

## Заполнить эту гугло-форму

https://forms.gle/NxYVAcpgaQfvCSXc6

Nikita Tarikin / nikita@tarikin.com

# Демо лаба

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

## Дождаться своего сертификата

Дед Мороз рассылает сертификаты вручную, сорян :)

**Nikita Tarikin** / nikita@tarikin.com

# 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 >`

**Nikita Tarikin** / nikita@tarikin.com

# 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

**Nikita Tarikin** / nikita@tarikin.com

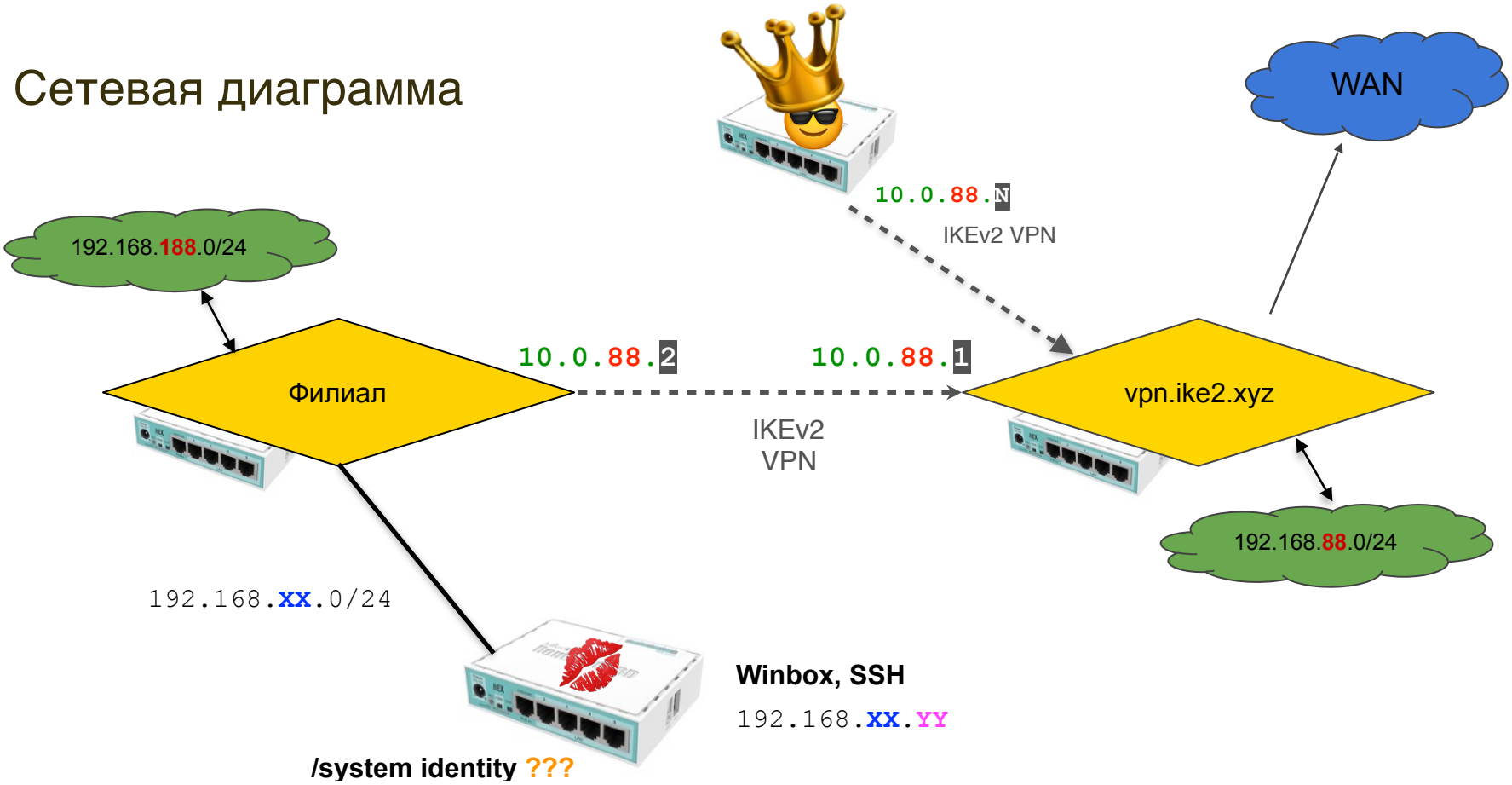
# Внимание, конкурс!


“ Hack the princess ”

Открыта до 31 декабря 2019

**Nikita Tarikin** / nikita@tarikin.com

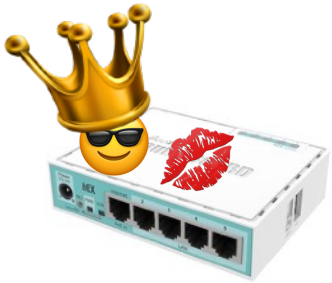
# Сетевая диаграмма



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

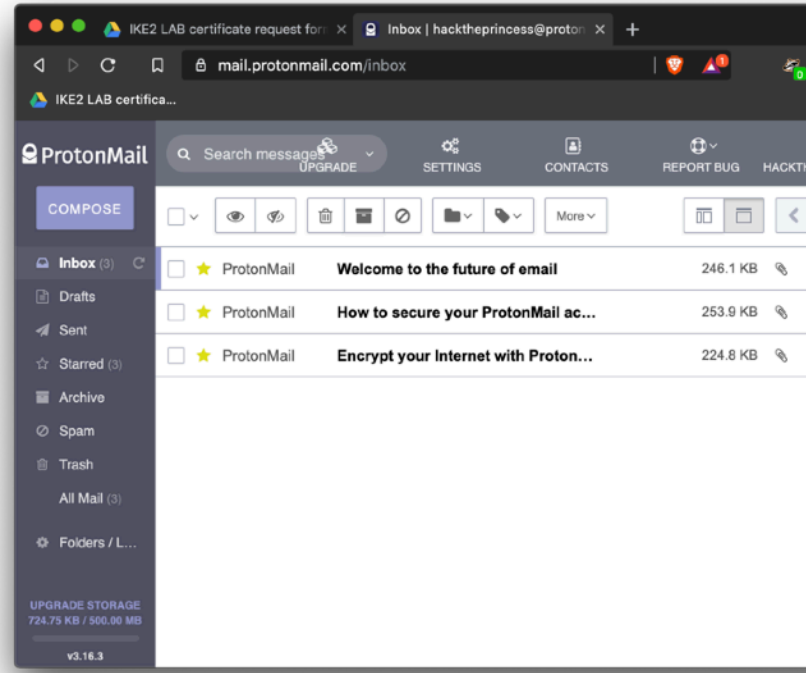
# hacktheprincess@protonmail.com



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

Nikita Tarikin / nikita@tarikin.com

# 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