

MUM Russia

September 06–07, 2019

Moscow



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



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

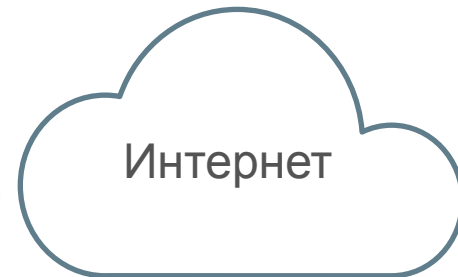


Мой телефон

Устройство сети для блондинок 👑💕



Magic



Устройство сети для продвинутых 🕶️



Мой компьютер



Мой роутер



Интернет



LAN



MikroTik
Router

WAN

WAN

WAN

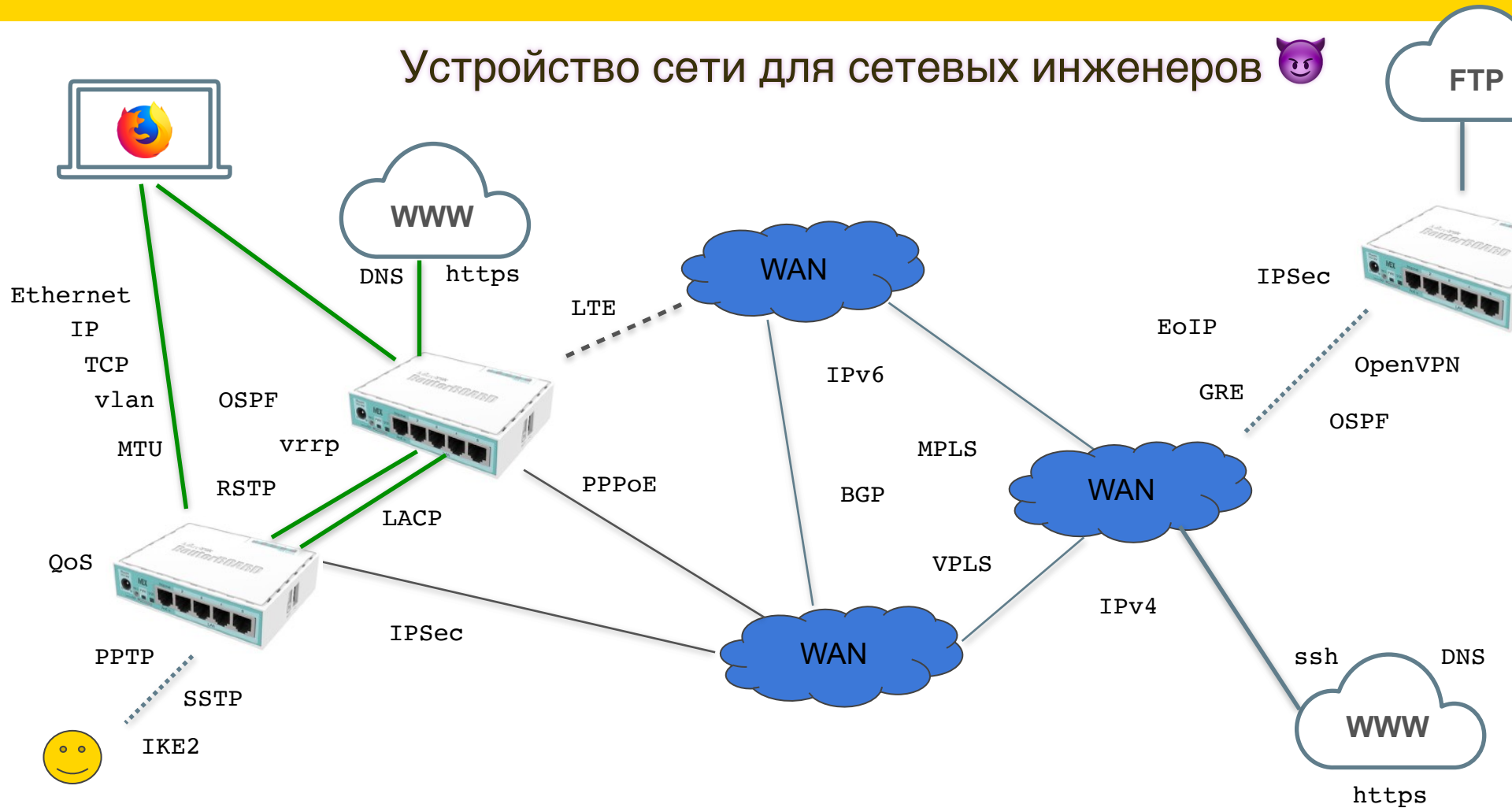
WAN

DNS
Apache
Wordpress

Устройство сети для админов



Устройство сети для сетевых инженеров



Устройство сети для кайт-серферов



IKEv2

IKEv2



 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%



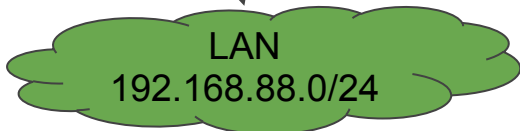




Мобильные абоненты VPN
10.0.88.0/24

IKEv2
VPN

NAT



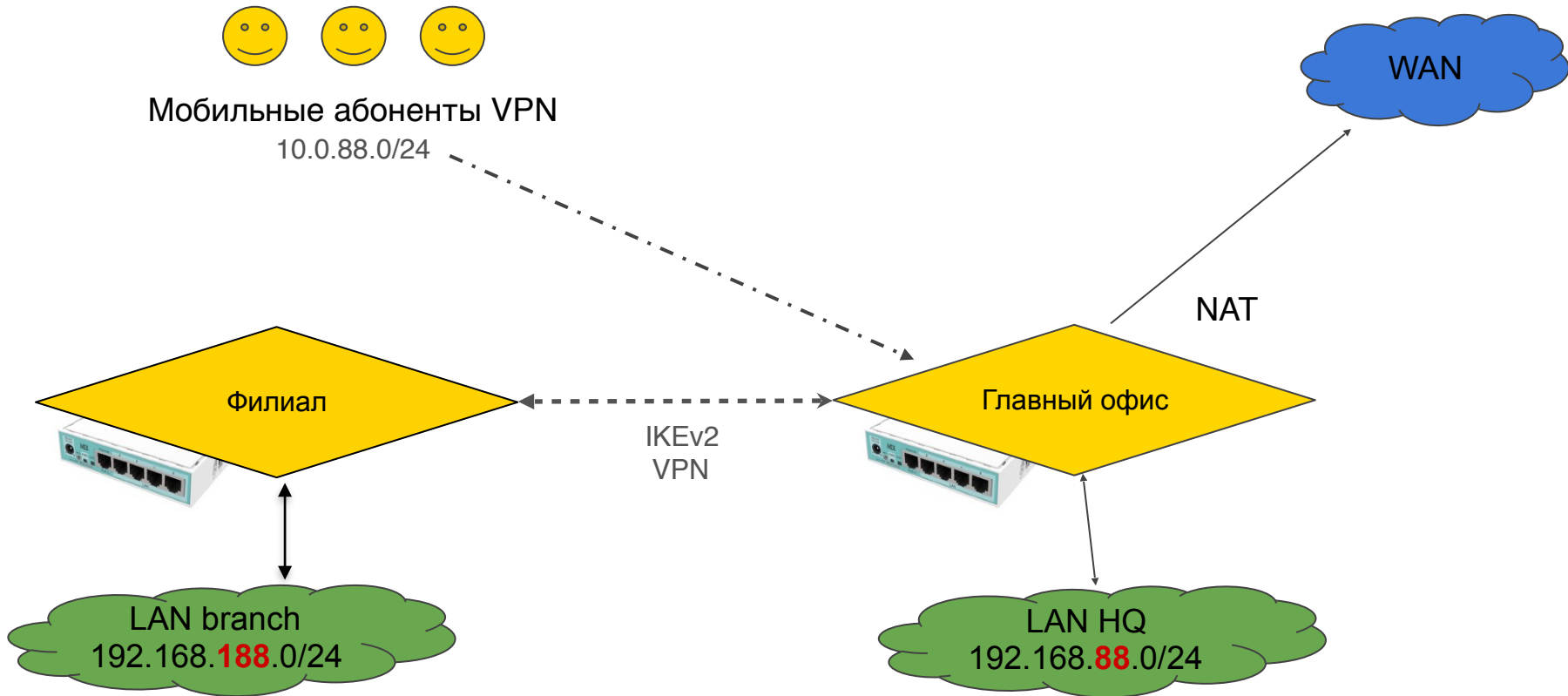
Сетевая диаграмма





Мобильные абоненты VPN

10.0.88.0/24



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



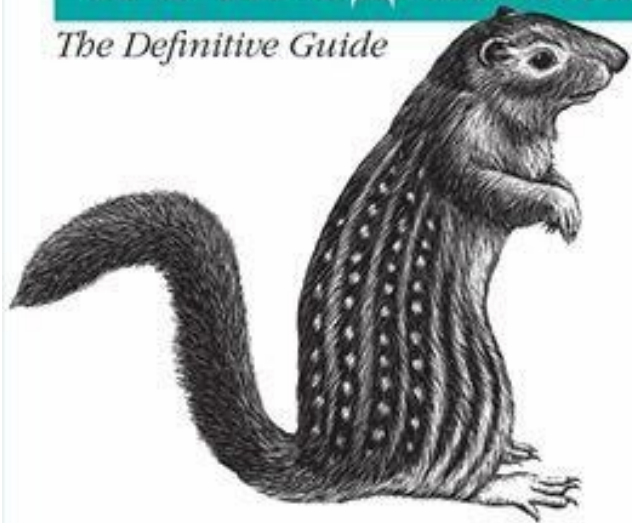
Подготовка к работе

1. Наличие знаний уровня МТСНА
(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

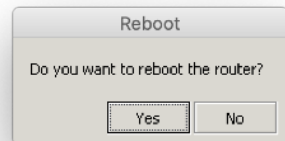
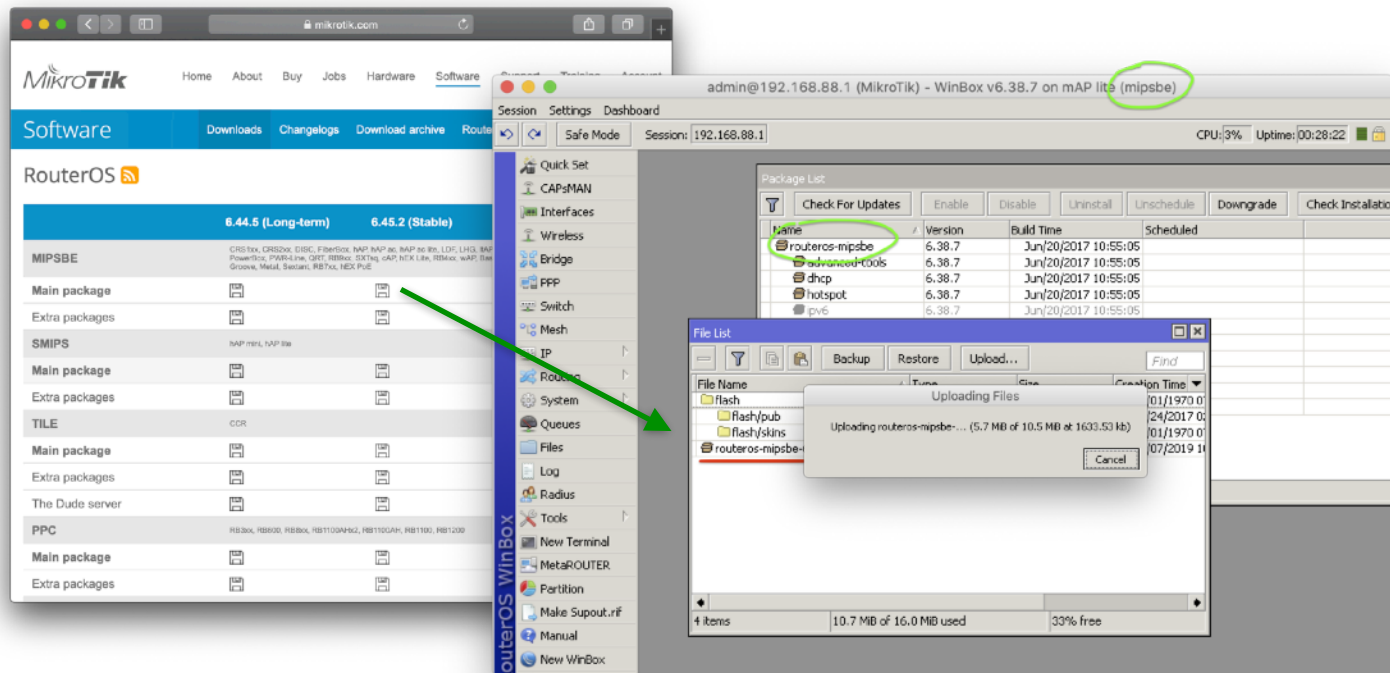


O'REILLY®

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



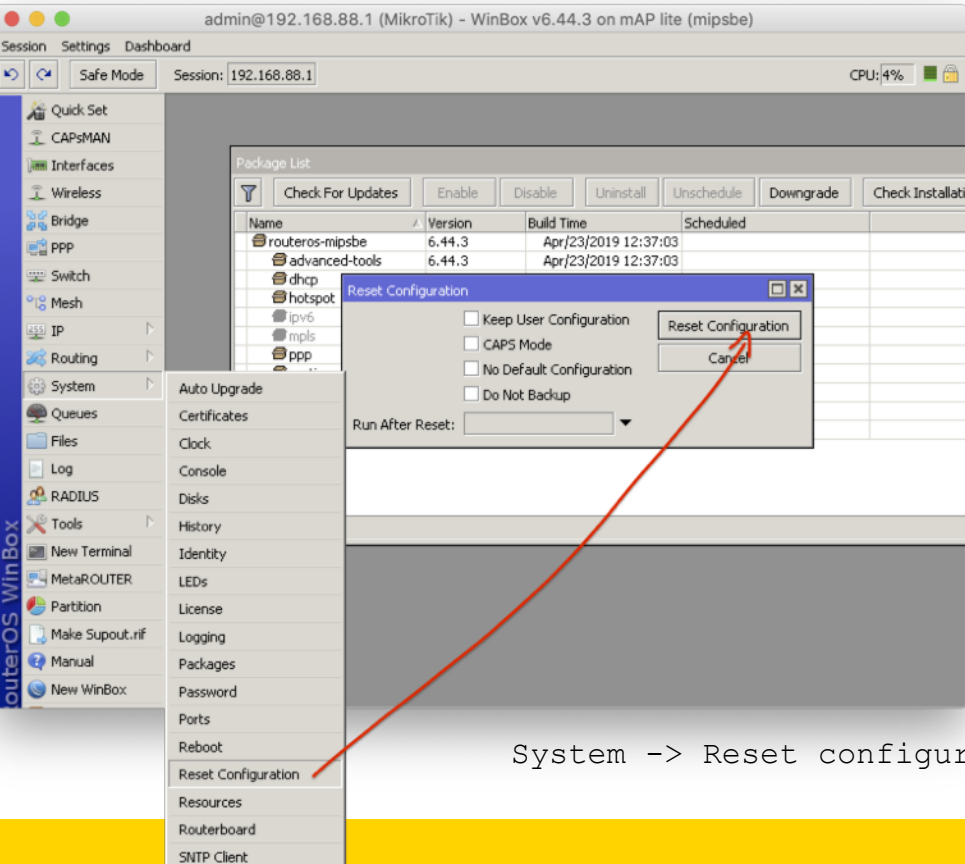
3. Перезагружаем

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

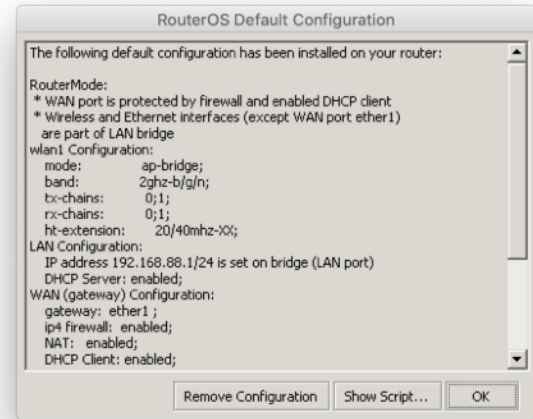
2. Заливаем пакет в корень файловой системы



Сбрасываем RouterBoard к заводской v6.45+ конфигурации



Сброс на заводской конфигурации 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

The screenshot shows the MikroTik WinBox interface. The main window displays the DHCP Client configuration for the 'ether1' interface, showing it is configured with IP address 123.45.67.8/24. An 'Address List' window is open, showing two entries: 123.45.67.8/24 on ether1 and 192.168.88.1/24 on bridge.

Interface	Use P...	Add D...	IP Address	Expires After	Status
;;; defconf					
ether1	yes	yes	123.45.67.8/24	00:09:33	bound

Address	Network	Interface
D 123.45.67.8/24	123.45.67.0	ether1
;;; defconf		
D 192.168.88.1/24	192.168.88.0	bridge

123.45.67.8 на WAN интерфейсе

Проверяем записи DNS:
Имя: **vpn.ike2.xyz**
Адрес: **123.45.67.8**

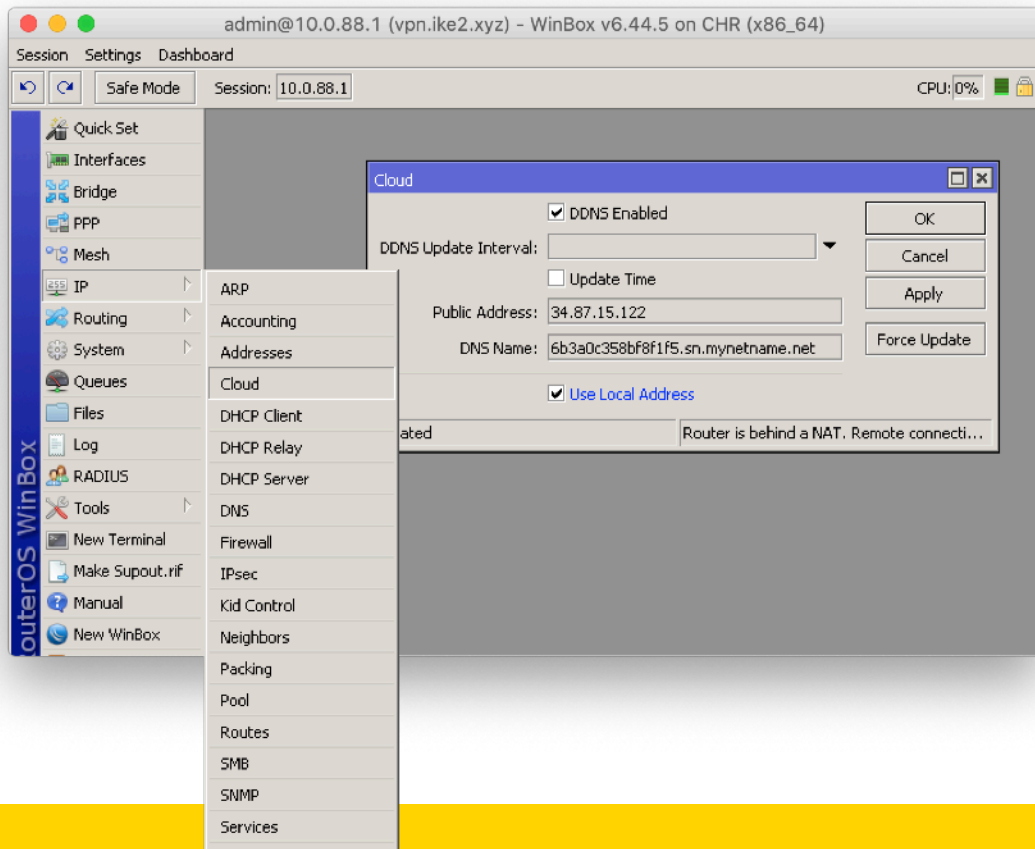
```
Last login: Tue May 7 11:04:11 on ttys001
→ ~ nslookup vpn.ike2.xyz
Server:         192.168.88.1
Address:        192.168.88.1#53

Non-authoritative answer:
Name:   vpn.ike2.xyz
Address: 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

admin@192.168.88.1 (MikroTik) - WinBox v6.45.2 on hAP lite (smips)

Session Settings Dashboard

Safe Mode Session: 192.168.88.1

- Quick Set
- CAPSMAN
- Interfaces
- Wireless
- Bridge
- PPP
- Switch
- Mesh
- IP
- Routing
- System
 - Auto Upgrade
 - Certificates
 - Clock
 - Console
 - History
 - Identity
 - LEDs
 - License
 - Logging
 - Packages
 - Password
 - Ports
 - Reboot
 - Reset Configuration
 - Resources
 - Routerboard
- Queues
- Dot1X
- Files
- Log
- RADIUS
- Tools
- New Terminal
- Make Supout.rif
- Manual
- New WinBox

Time Manual Time Zone

Time: 10:08:02

Date: Jan/01/1970

Time Zone Autodetect

Time Zone Name: Europe/Moscow

GMT Offset: +03:00

DST Active

OK

Cancel

Apply

System -> Clock

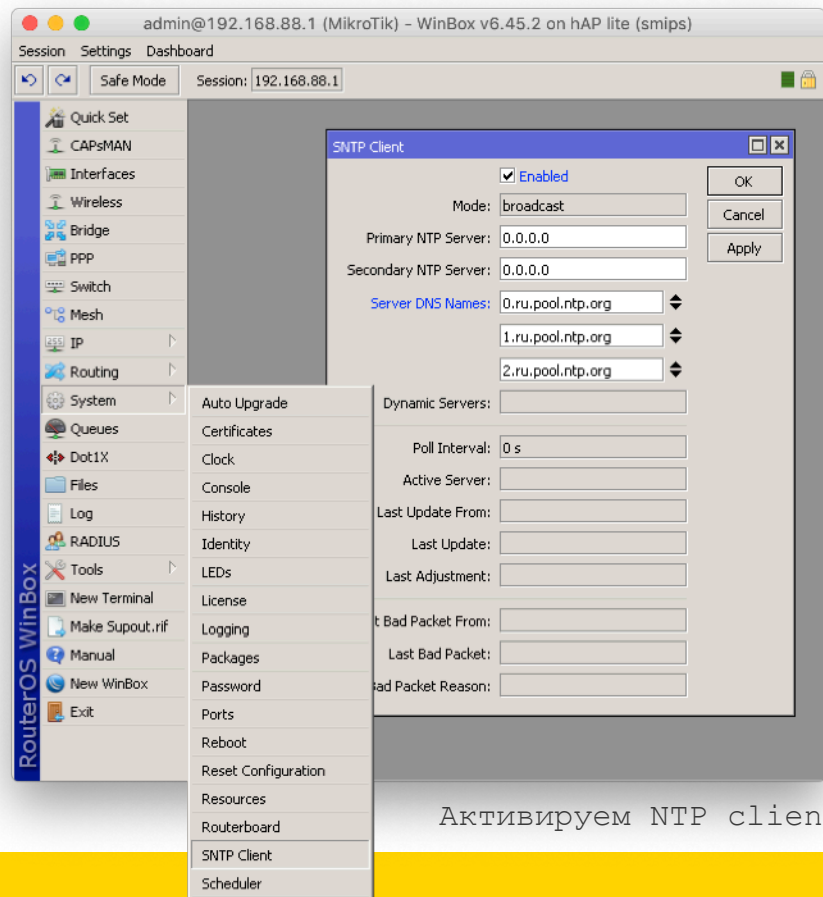
```
/system clock set time-zone-name=Europe/Moscow
```

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



Настройка автоматической синхронизации даты и времени

ЭТО ВАЖНО

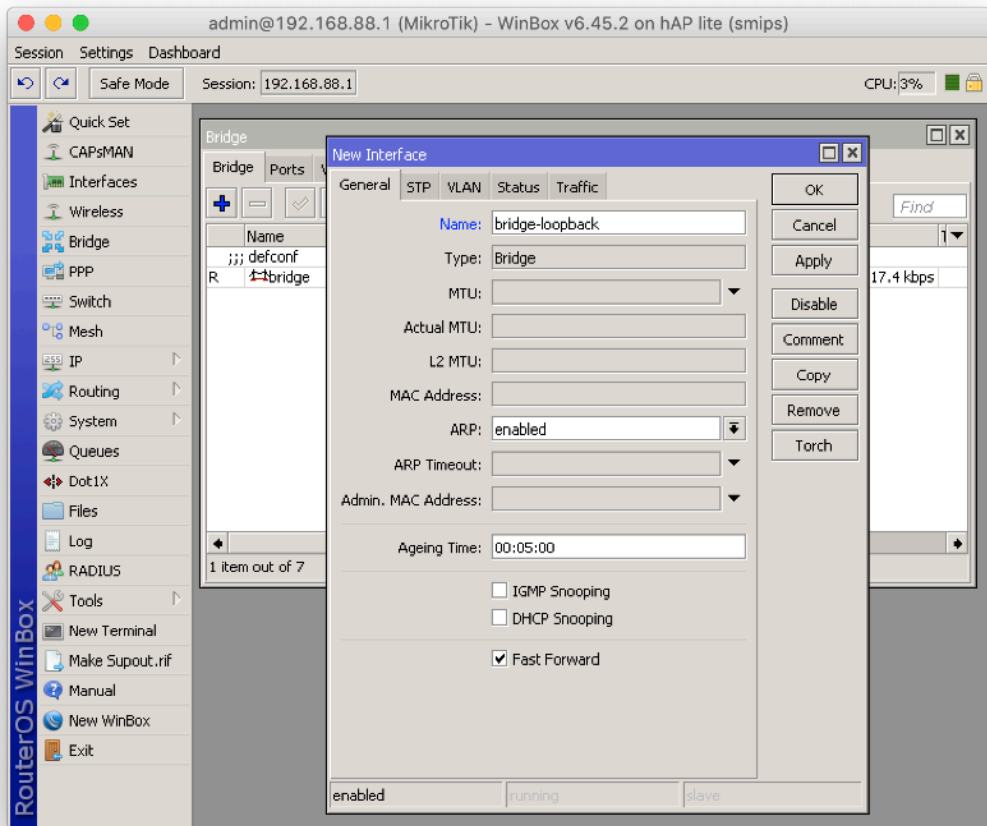


Активируем NTP client

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



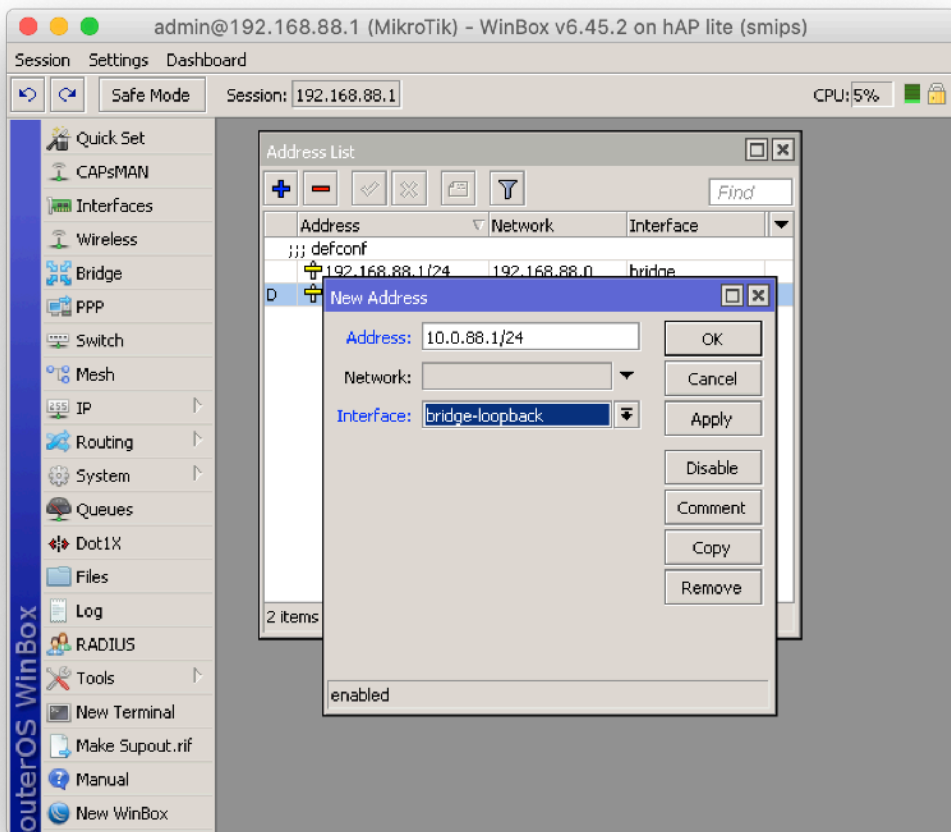
Добавляем новый loopback bridge



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

```
usage=pl tag6-loopback
```

Задаём IP адрес для loopback bridge

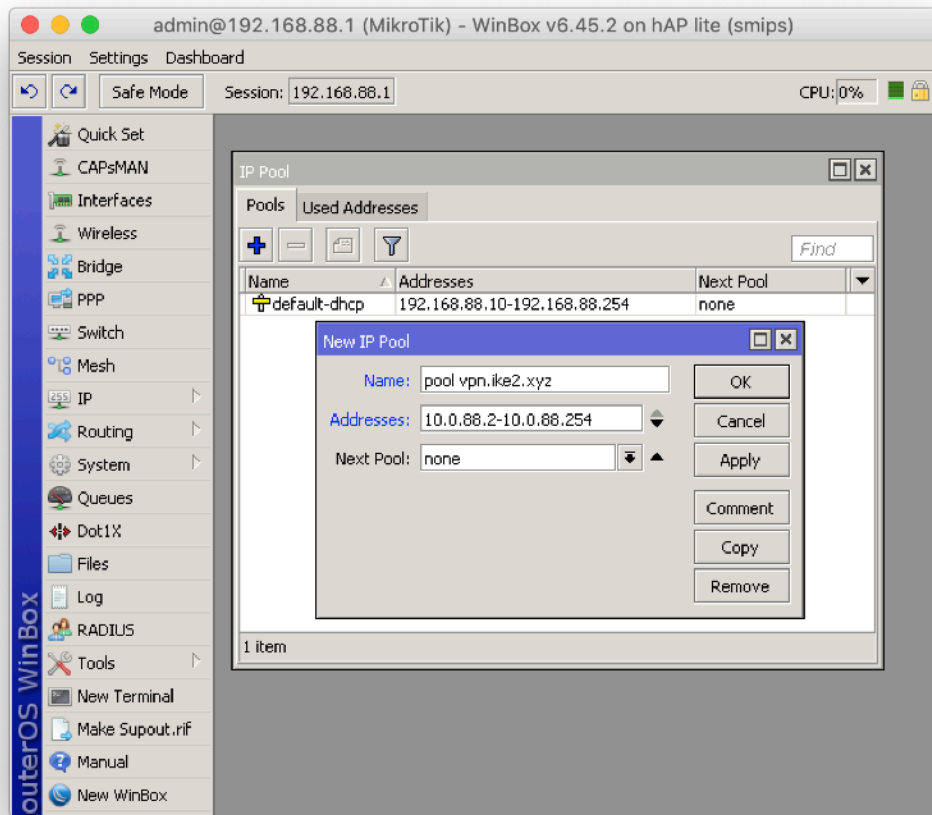


10.0.88.1

```
/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
```

```
192.168.88.10-192.168.88.254
```



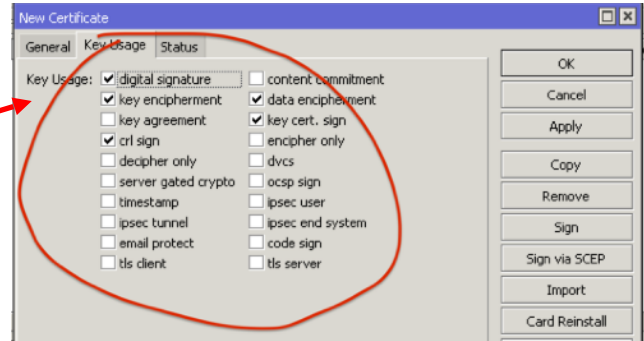
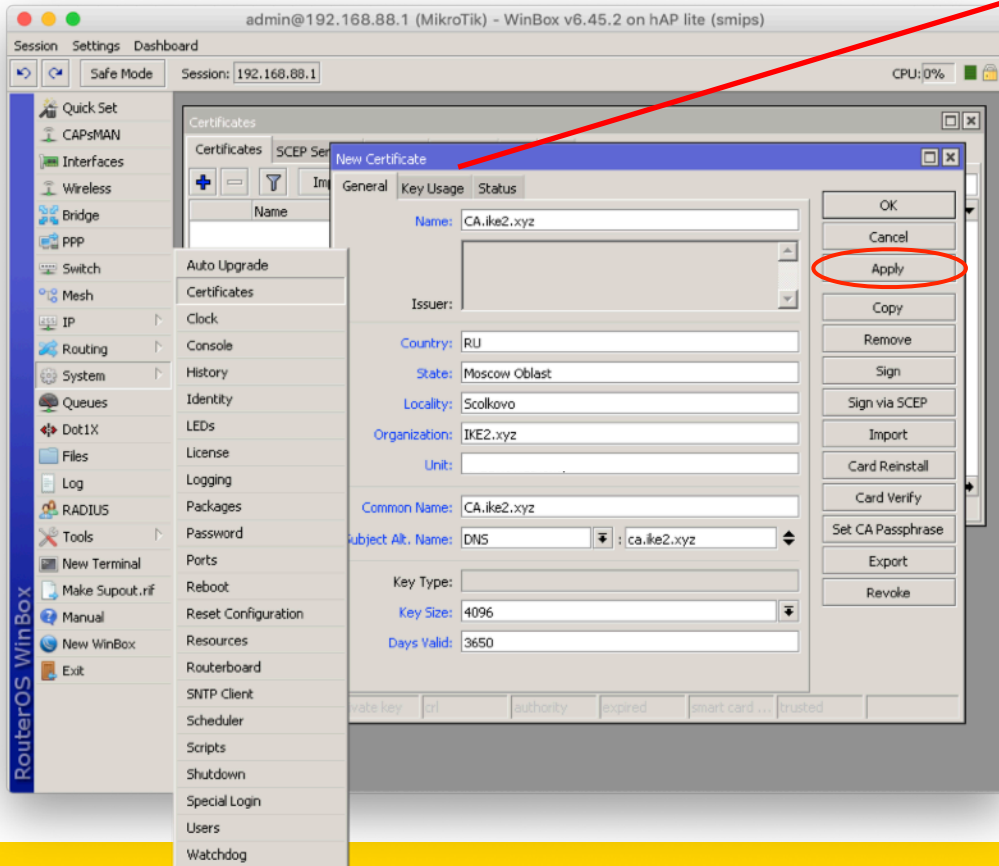
Генерируем правильные SSL сертификаты

План действий

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

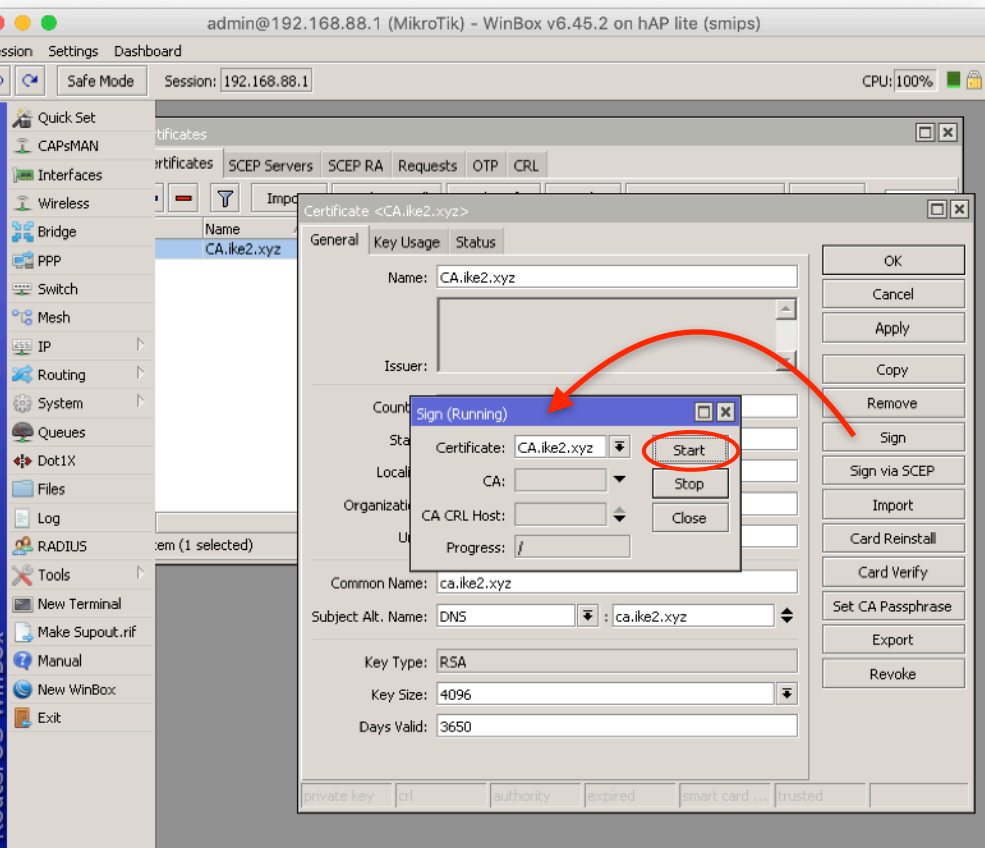


Генерируем главный CA SSL сертификат



```
/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
```

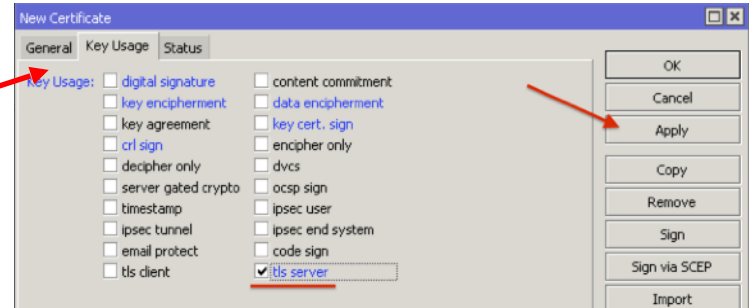
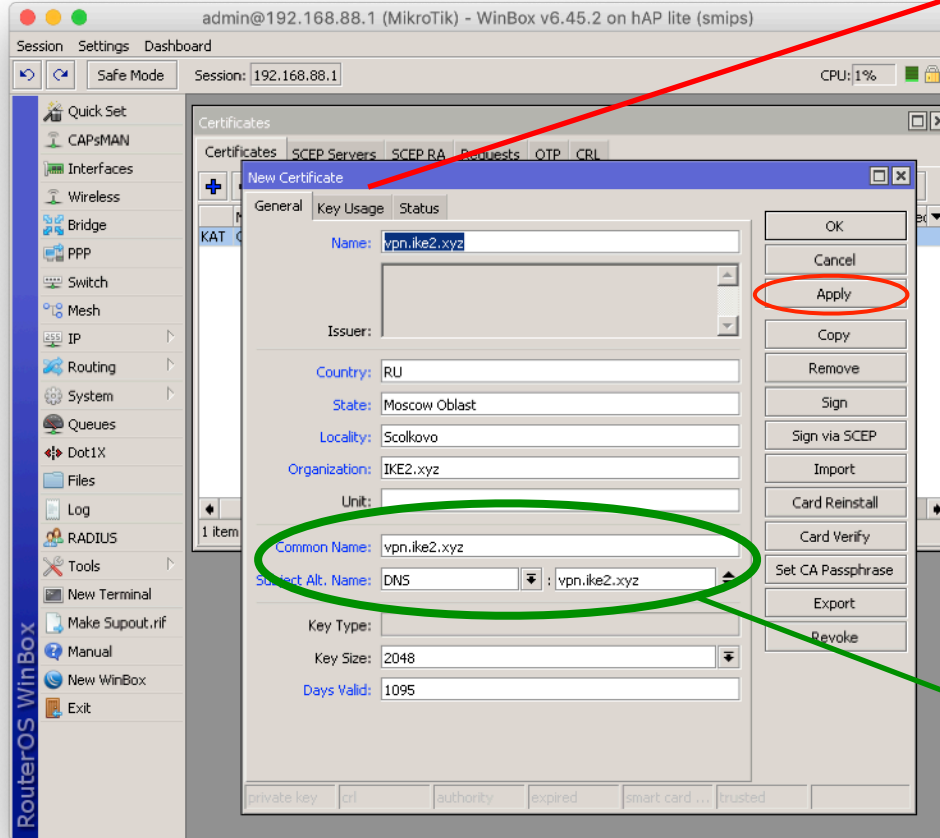
Само-подписываем новый CA SSL сертификат (*Certificate Authority*)



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

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

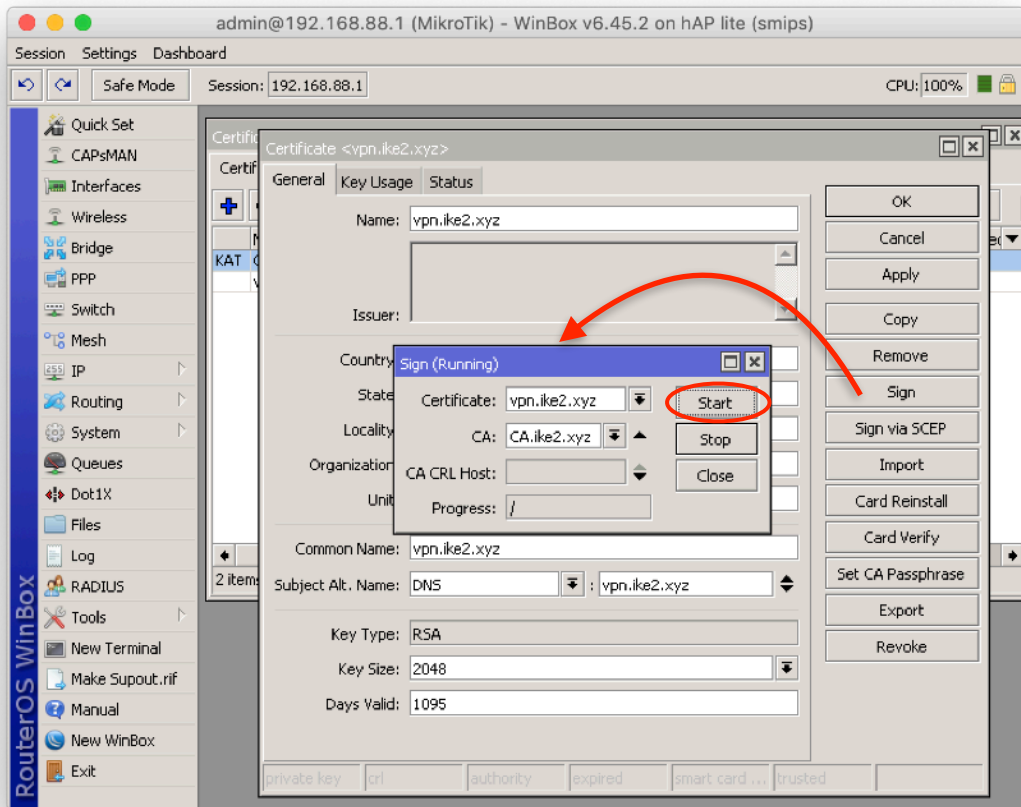
Генерируем серверный SSL сертификат



```
/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

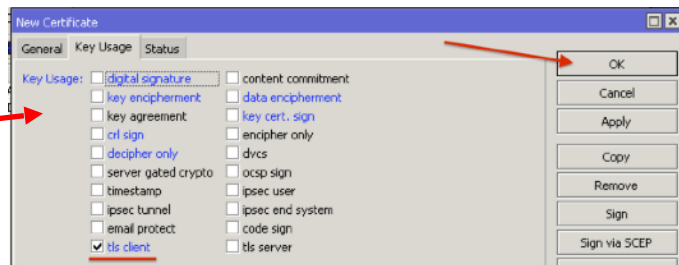
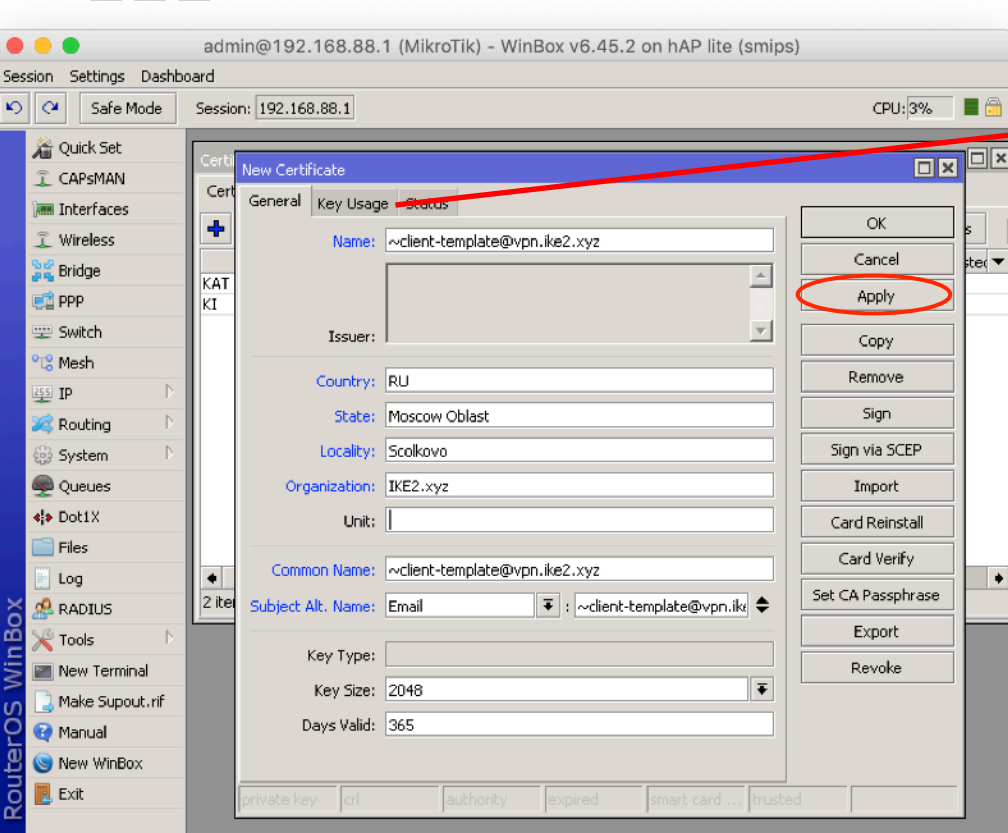


```
/certificate sign vpn.ike2.xyz
```

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

```
CA=CN=IK65.XYZ
```

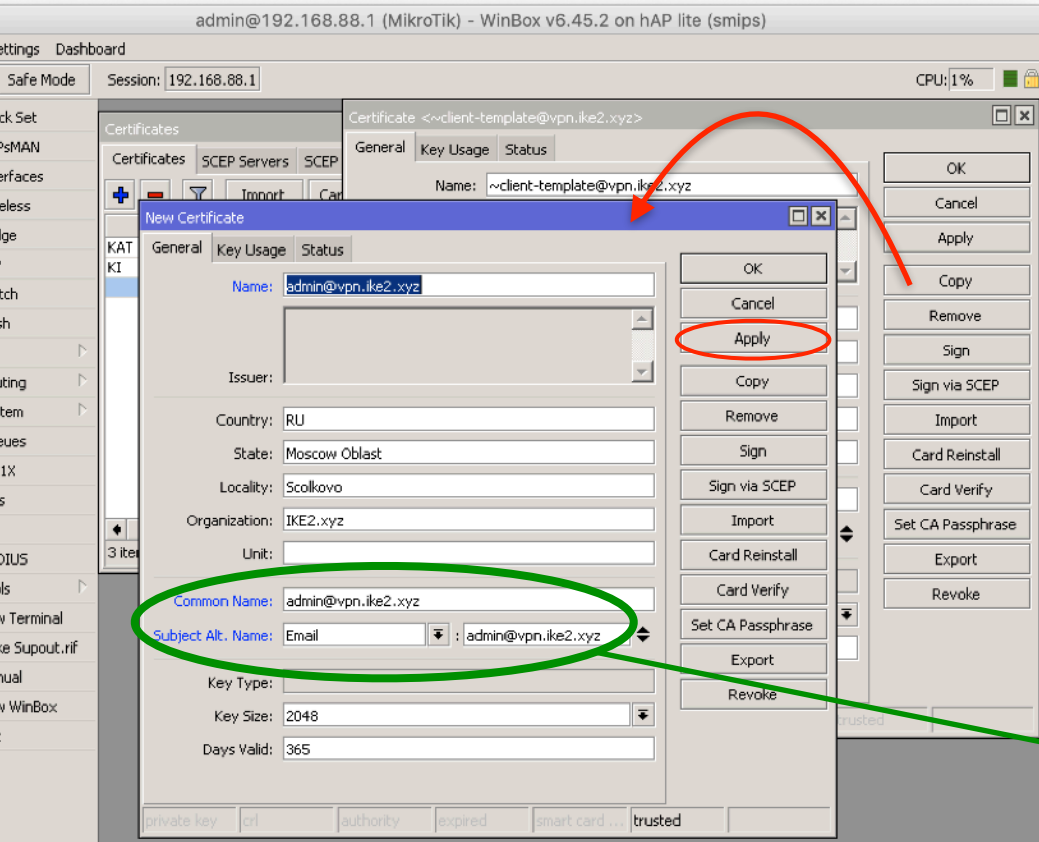
Создаем шаблон для тиражирования клиентских подписей



```
/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
```



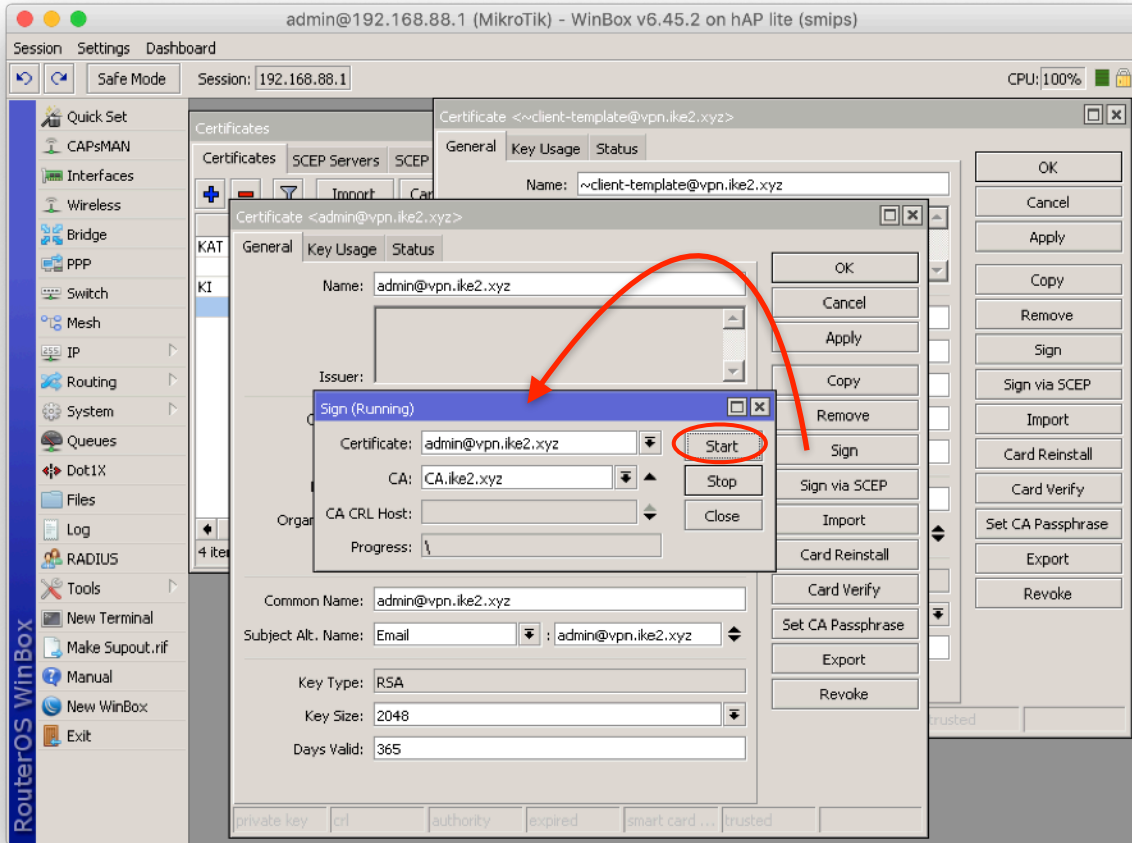
Создаем первую клиентскую подпись из заготовленного шаблона



```
/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

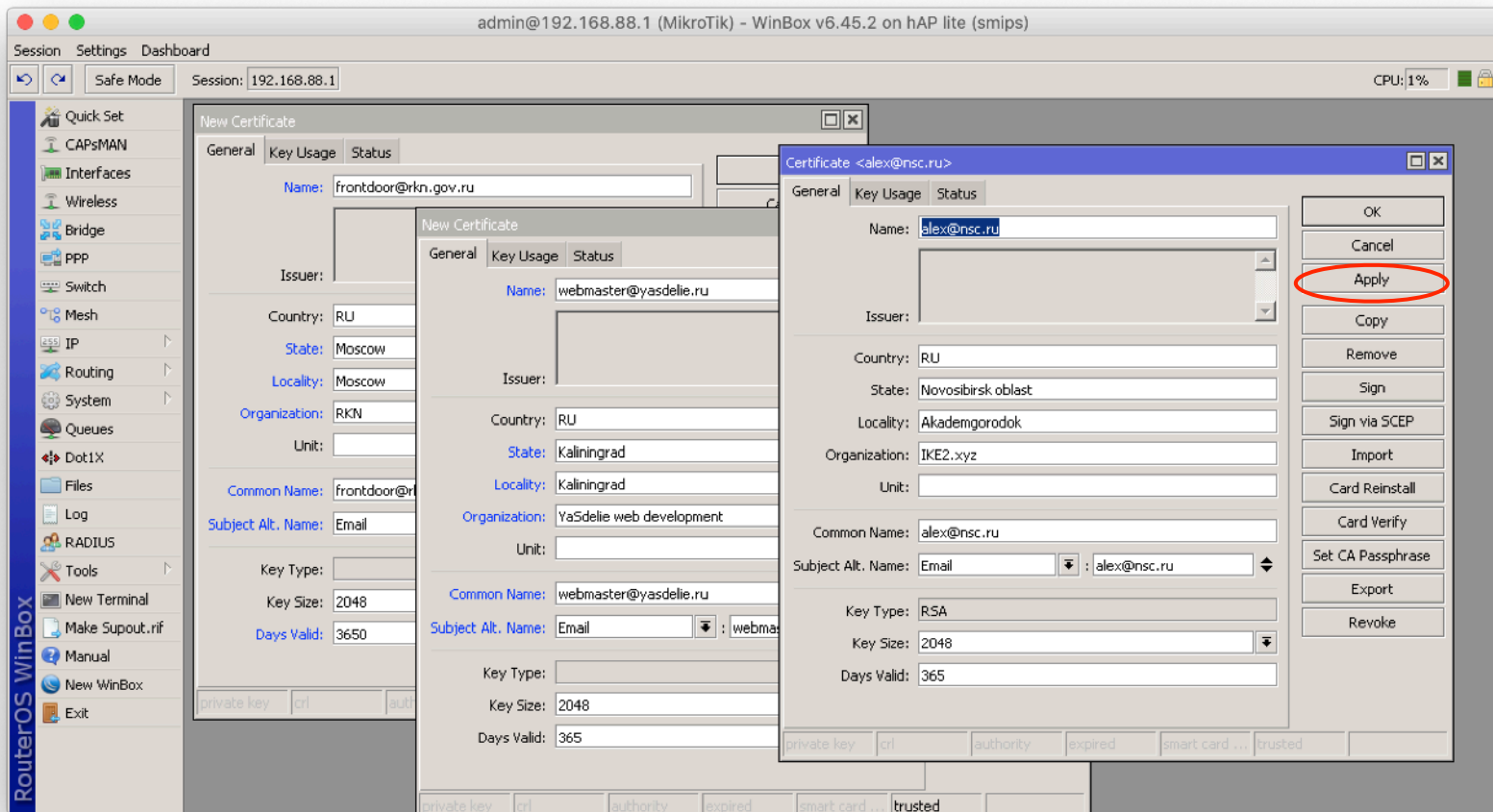


```
/certificate sign  
admin@vpn.ike2.xyz  
ca=CA.ike2.xyz
```

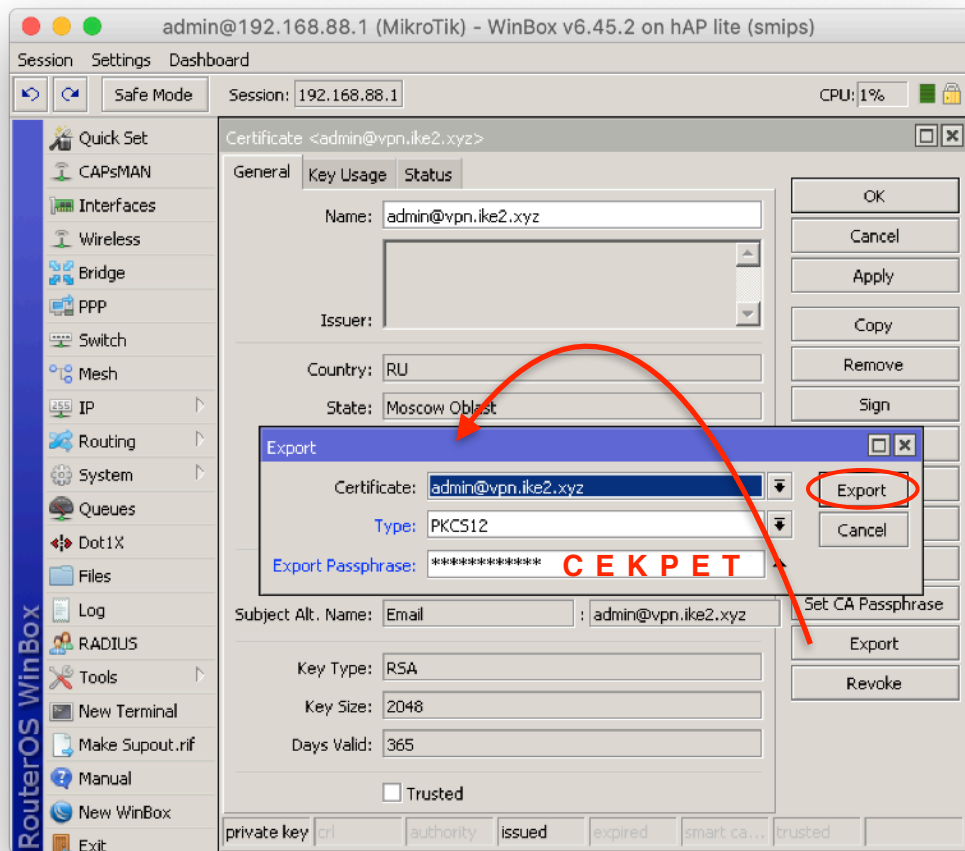
CG=Cv'IKG5'xλs



Создаем остальные клиентские подписи из шаблона (по аналогии)



Экспортируем клиентскую подпись + приватный ключ в файл .p12



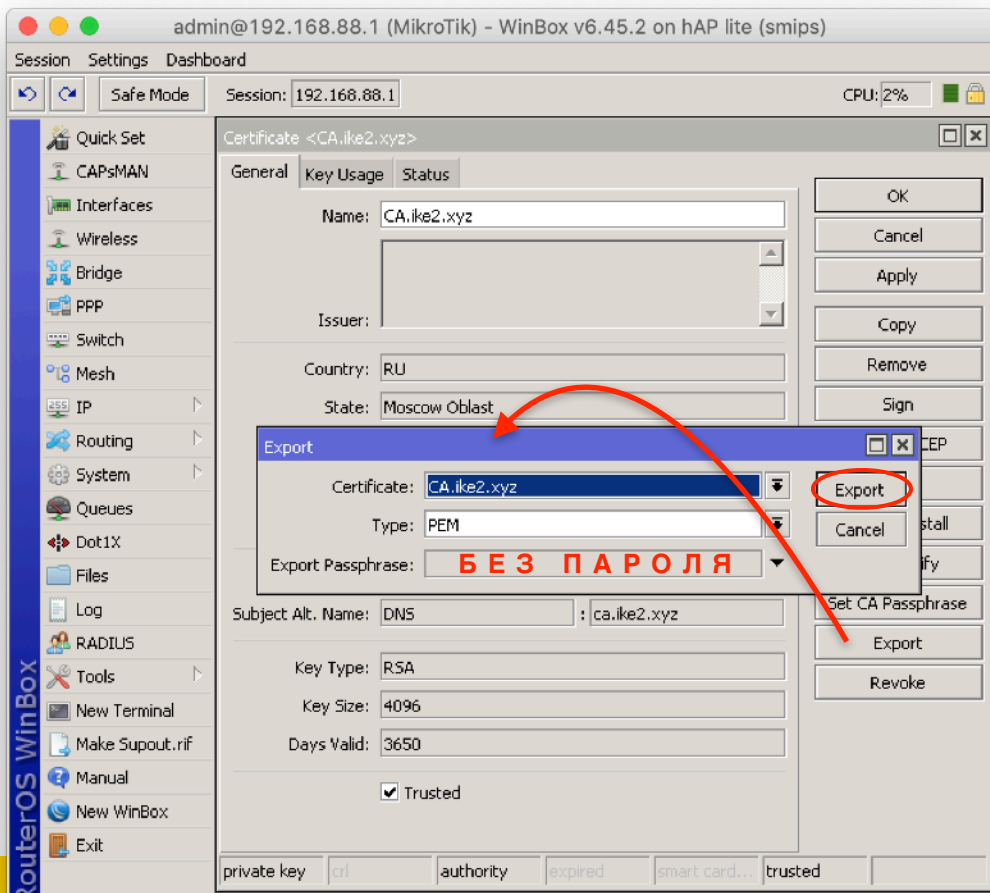
При экспорте **обязательно** указываем пароль.
Пустой пароль экспортирует **сертификат без ключа**.

Пароль храним в **секрете**.

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

```
export-certificate=keebtu26c1e6
```

Экспортируем сертификат авторитета CA в .crt файл



При экспорте **ни в коем случае** не указываем пароль. Экспорт **ключа CA** самопровозглашенного **авторитета УГРОЖАЕТ БЕЗОПАСНОСТИ ВСЕМ ЖИТЕЛЯМ БАНАНОВОЙ КОРПОРАЦИИ**

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


Скачиваем с роутера экспортированный CA сертификат + клиентские подписи

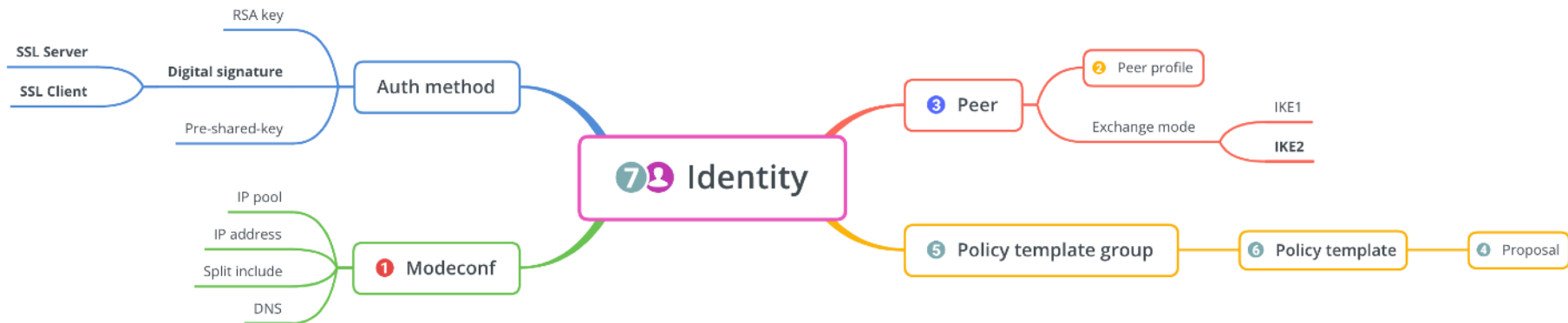
The screenshot shows the Mikrotik WinBox interface for a MikroTik router. The main window displays the 'Certificates' section, which includes a table of certificates and various management buttons. A 'File List' window is open over the certificates table, showing a list of files exported from the router. A red arrow points from the 'Files' menu in the left sidebar to the File List window.

Certificates Table:

Name	Issuer	Common Name	Subject Alt. Name	Key Size	Days Valid	Trusted
KAT CA.ike2.xyz		ca.ike2.xyz	DNS:ca.ike2.xyz	4096	3650	yes
KI admin@vpn.ike2.xyz		admin@vpn.i...	Email:admin@vpn.ike2.xyz	2048	365	no
KI alex@nsc.ru		alex@nsc.ru	Email:alex@nsc.ru	2048	365	no
KI frontdoor@rkn.gov.ru		frontdoor@r...	Email:frontdoor@rkn.gov.ru	2048	3650	no
KI office-spb@vpn.ike2.x...		office-spb@...	Email:office-spb@vpn.ike2.x...	2048	1825	no
KI vpn.ike2.xyz						
KI webmaster@yasdelie.r...						
KI ~client-template@vpn...						

File List Table:

File Name	Type	Size	Creation Time
cert_export_CA.ike2.xyz.crt	.crt file	2061 B	Aug/01/2019 10:17:14
cert_export_admin@vpn.ike2.xyz.p12	.p12 file	4494 B	Aug/01/2019 10:08:09
cert_export_alex@nsc.ru.p12	.p12 file	4456 B	Aug/01/2019 10:35:56
cert_export_frontdoor@rkn.gov.ru.p12	.p12 file	4490 B	Aug/01/2019 10:35:41
cert_export_office-spb@vpn.ike2.xyz.p12	.p12 file	4528 B	Aug/01/2019 10:35:22
cert_export_webmaster@yasdelie.ru.p12	.p12 file	4524 B	Aug/01/2019 10:36:14
skins	directory		Jan/01/1970 03:00:04



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;

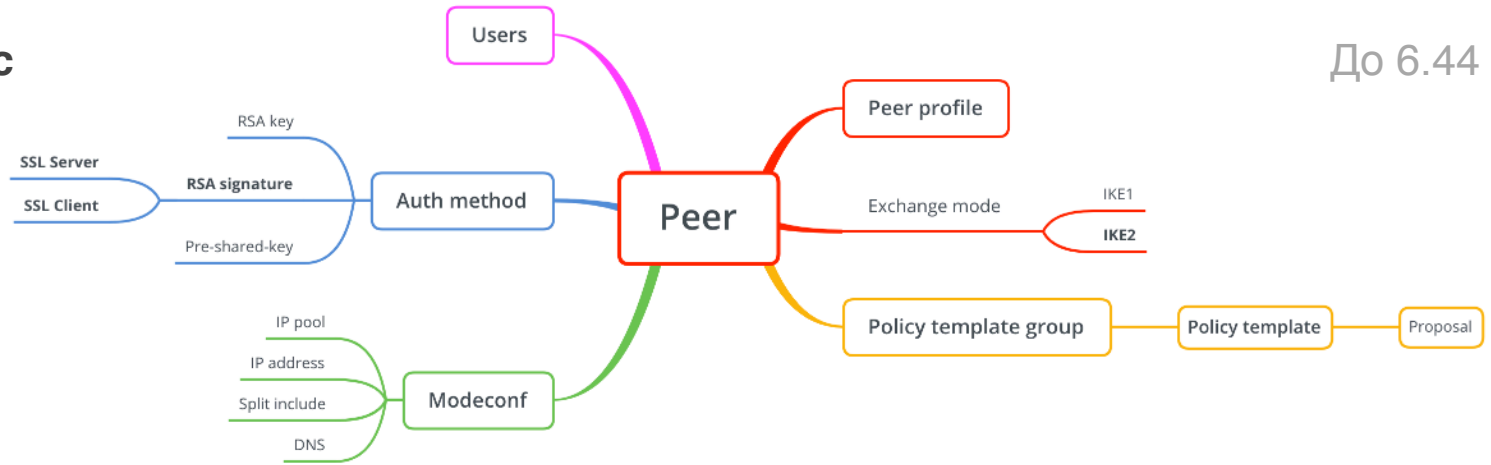
Ключевые изменения в RouterOS 6.44

- *) 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;

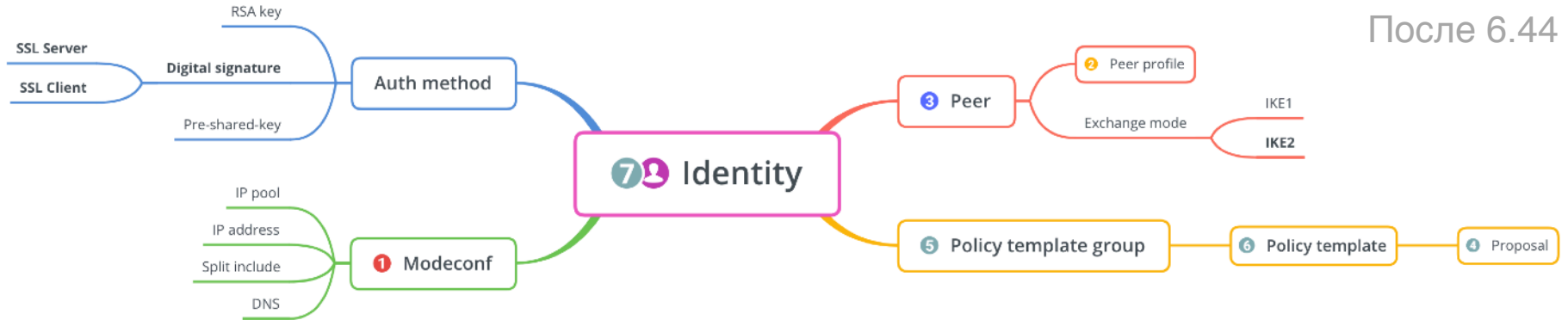


Структура IPSec

До 6.44



После 6.44



1. Настройка нового IPsec mode config

The screenshot shows the Mikrotik WinBox interface. The main window displays the IPsec configuration page with a table of existing configurations. A 'New IPsec Mode Config' dialog box is open, showing the following settings:

- Name: modeconf vpn.ike2.xyz
- Responder
- Address Pool: pool vpn.ike2.xyz
- Address: (empty)
- Address Prefix Length: 32
- Split Include: 0.0.0.0/0
- System DNS
- Static DNS: 10.0.88.1

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

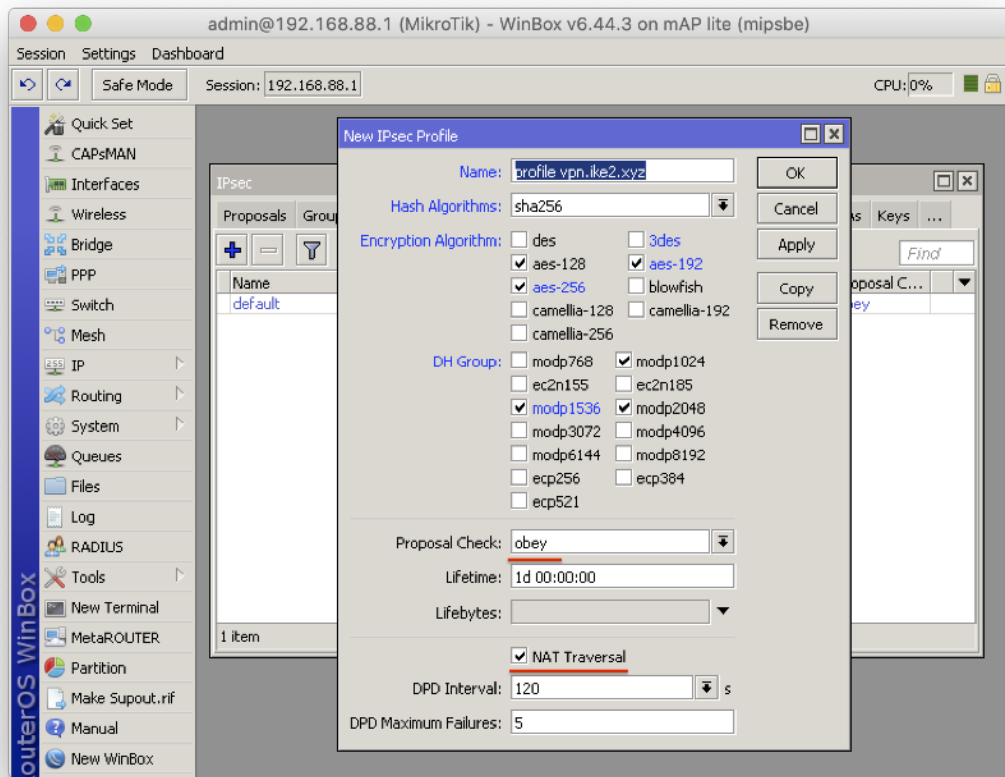
The screenshot shows the 'IPsec Mode Config <modeconf vpn.ike2.xyz>' dialog box with the following settings:

- Name: modeconf vpn.ike2.xyz
- Responder
- Address Pool: pool vpn.ike2.xyz
- Address: (empty)
- Address Prefix Length: 32
- Split Include: 192.168.88.0/24
- System DNS
- Static DNS: 10.0.88.1

```
/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
```

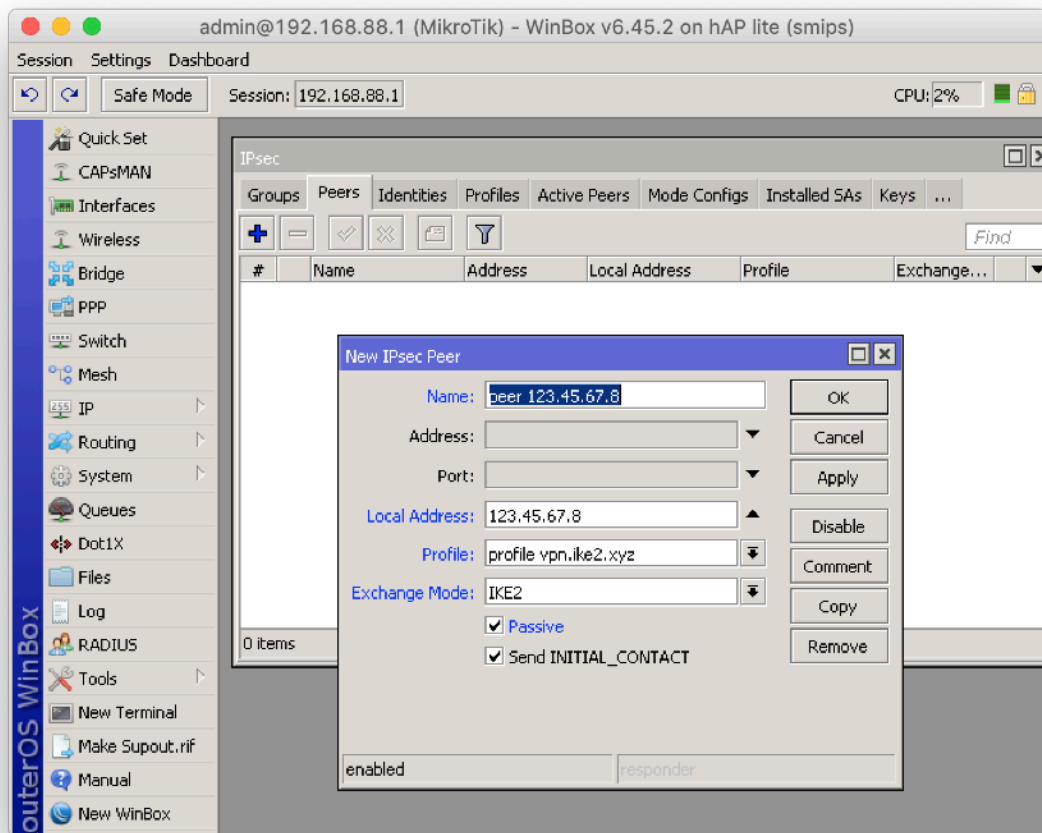


2. Настройка нового IPSec peer profile (фаза 1)



```
/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 реер на публичном IP адресе (режим IKE2)

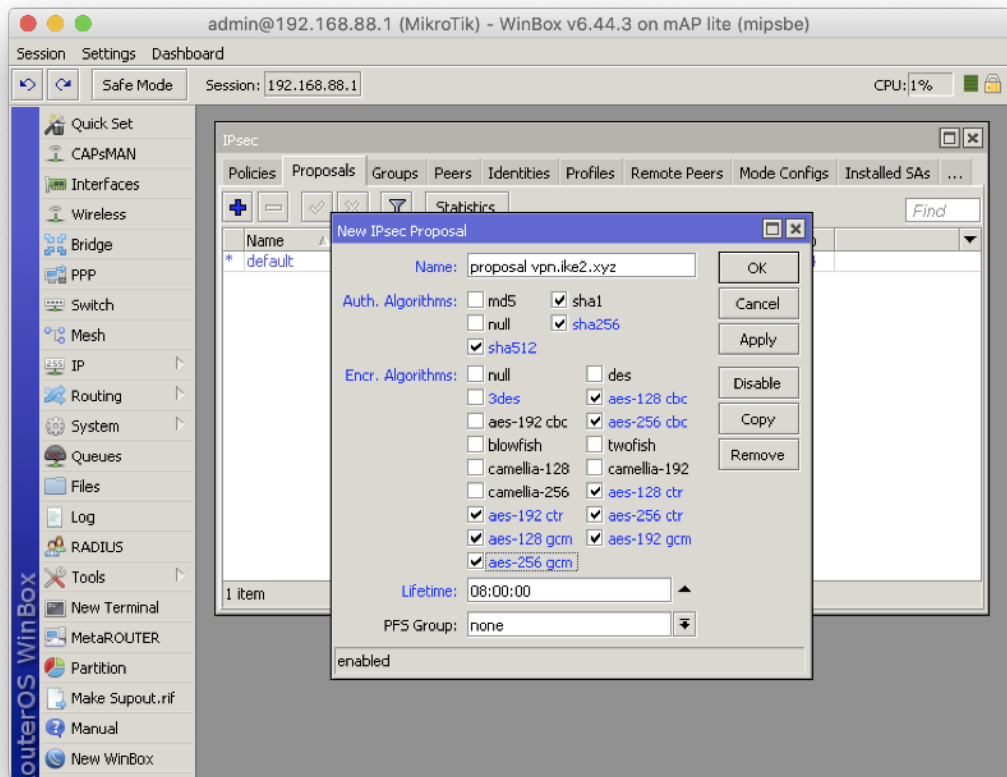


Принимаем клиентов со всех адресов 0.0.0.0/0

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"
```

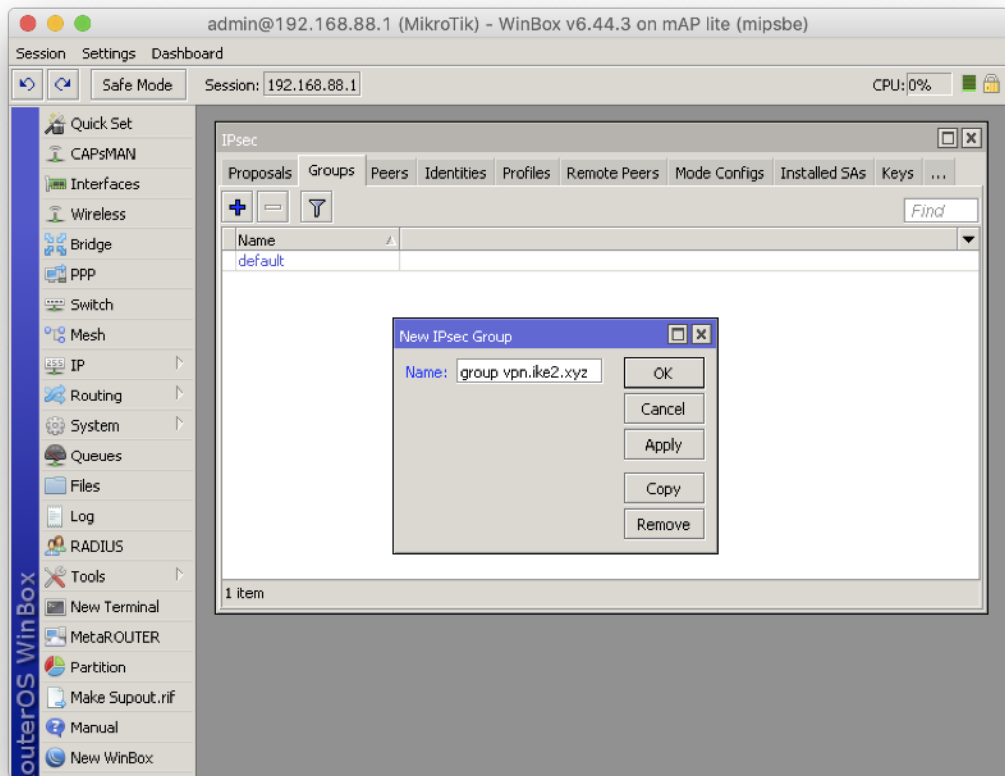

4. Настройка нового IPsec proposal (фаза 2)



```
/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

admin@192.168.88.1 (MikroTik) - WinBox v6.45.2 on hAP lite (smips)

Session Settings Dashboard

Safe Mode Session: 192.168.88.1 CPU: 2%

Quick Set CAPsMAN Interfaces Wireless Bridge PPP Switch Mesh IP Routing System Queues Dot1X Files Log RADIUS Tools New Terminal Make Supout.rif Manual New WinBox Exit

IPsec Policies Proposals Groups Peers Identities Profiles Active Peers Mode Configs ...

New IPsec Policy

General Action Status

Src. Address: 0.0.0.0/0

Src. Port: [Dropdown]

Dst. Address: 10.0.88.0/24

Dst. Port: [Dropdown]

Protocol: 255 (all)

Template

Group: group vpn.ike2.xyz

OK Cancel Apply Disable Comment Copy Remove

New IPsec Policy

General Action Status

Action: encrypt

IPsec Protocols: esp

Proposal: proposal vpn.ike2.xyz

OK Cancel Apply Disable Comment Copy Remove

enabled Template Active

```
/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

admin@192.168.88.1 (MikroTik) - WinBox v6.45.2 on hAP lite (smips)

Session: 192.168.88.1 CPU: 2%

IPsec Identity <peer 123.45.67.8>

Peer: peer 123.45.67.8

Auth. Method: digital signature

Certificate: vpn.ike2.xyz

Remote Certificate: frontdoor@r...

Policy Template Group: group vpn.ike...

Notrack Chain:

My ID Type: auto

Remote ID Type: user fqdn

Remote ID: frontdoor@r...

Match By: certificate

Mode Configuration: modeconf vpn...

Generate Policy: port strict

enabled

IPsec Identity <peer 123.45.67.8>

Peer: peer 123.45.67.8

Auth. Method: digital signature

Certificate: vpn.ike2.xyz

Remote Certificate: admin@vpn.ike2.xyz

Policy Template Group: group vpn.ike2.xyz

Notrack Chain:

My ID Type: auto

Remote ID Type: user fqdn

Remote ID: admin@vpn.ike2.xyz

Match By: certificate

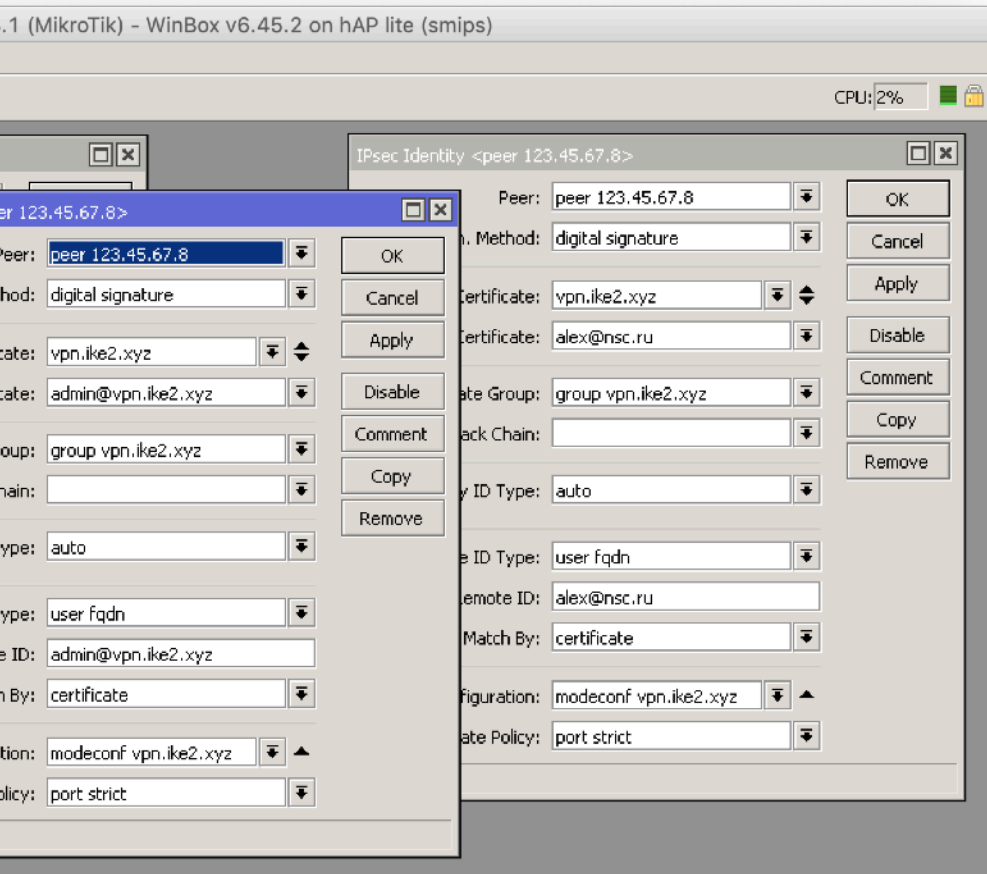
Mode Configuration: modeconf vpn.ike2.xyz

Generate Policy: port strict

enabled

```
/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

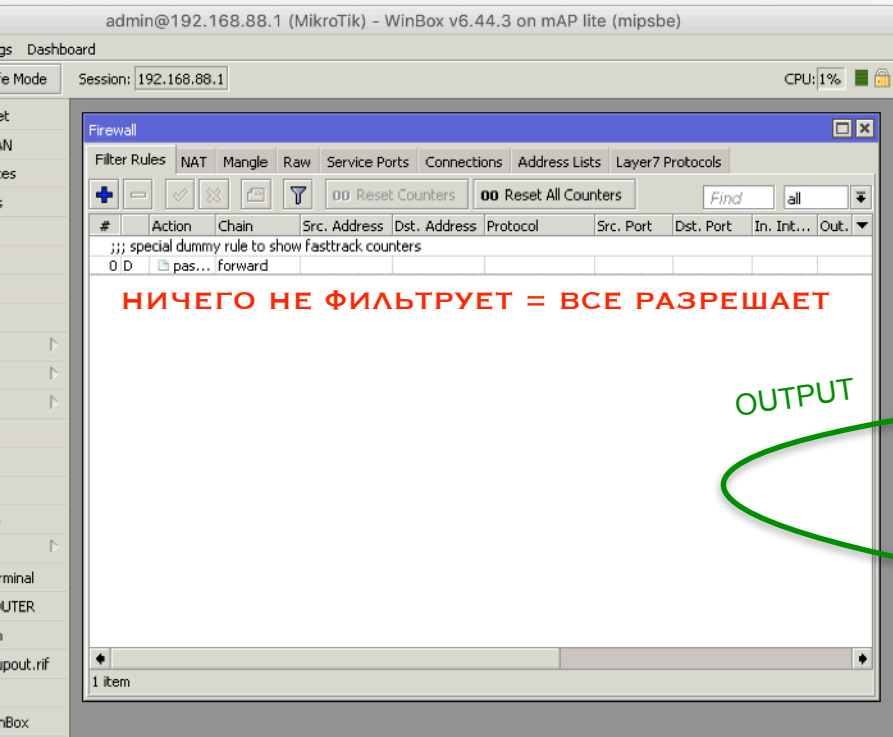
План действий

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

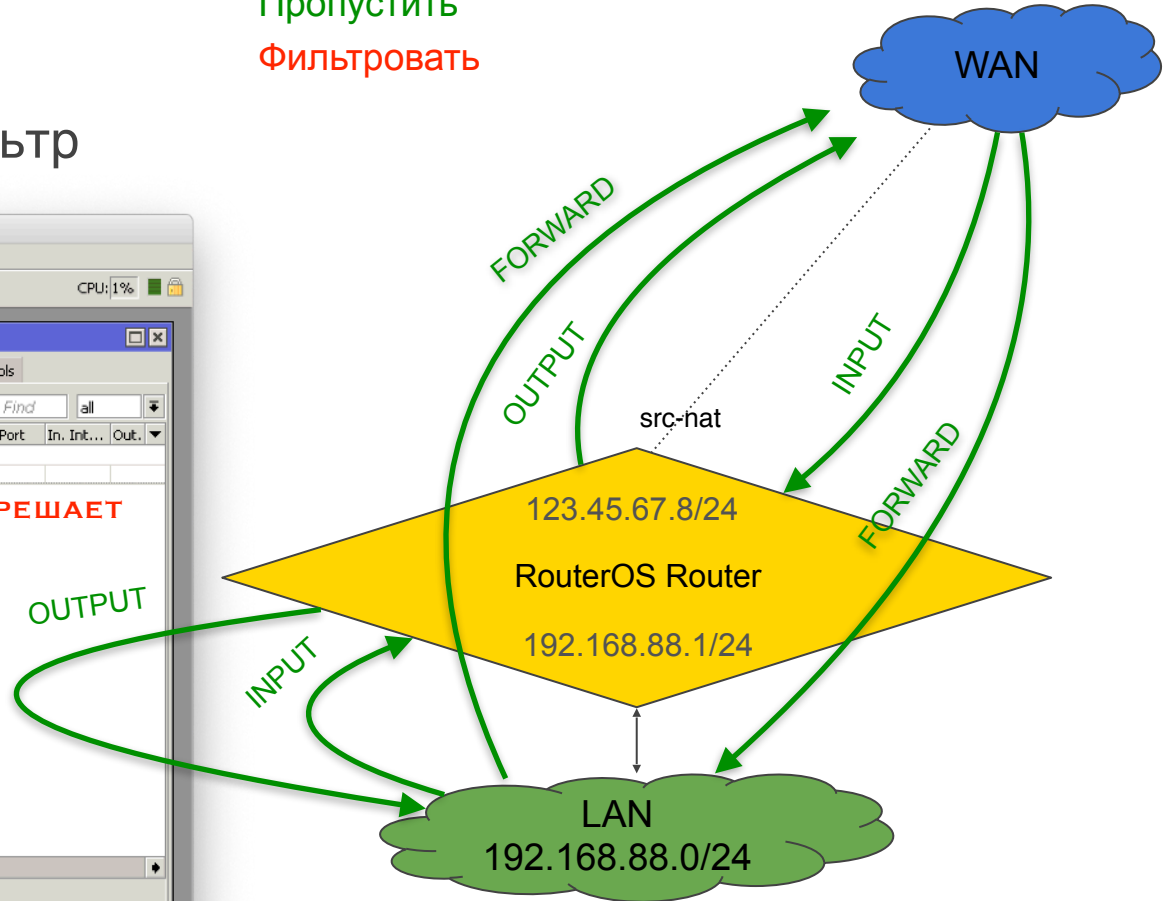


АХТУНГ

Пустой FIREWALL фильтр



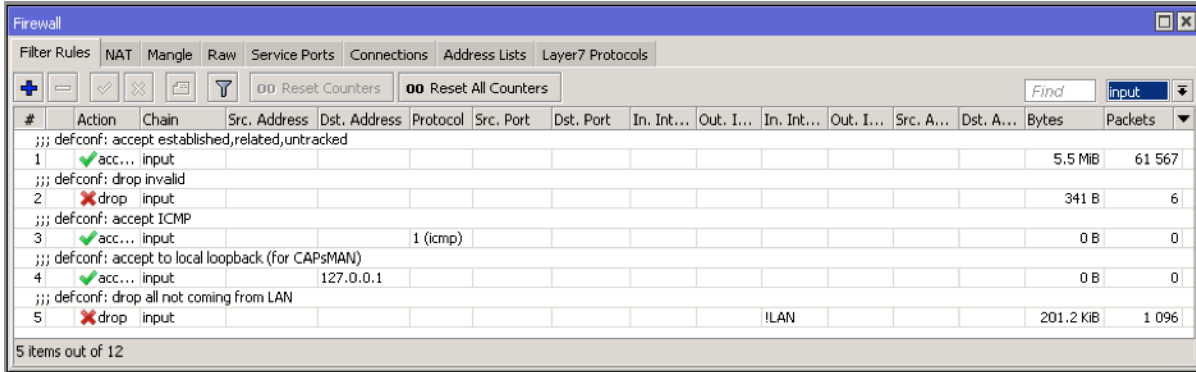
Пропустить
Фильтровать



Настройка Firewall

Краткий обзор стандартного фильтра (MTCNA)

Краткий обзор стандартного Firewall фильтра RouterOS 6.45



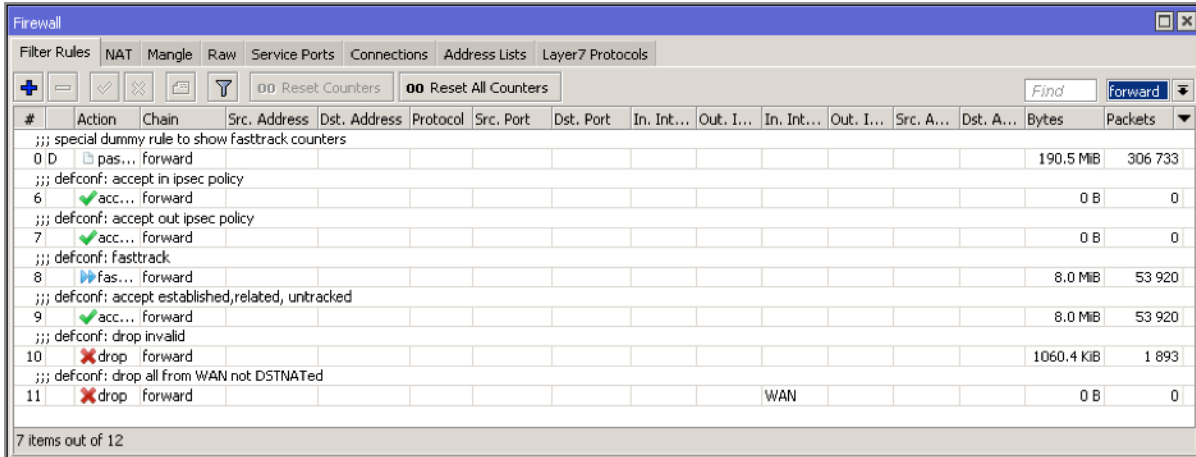
Firewall

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

Filter: Find

#	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	✓ acc...	input												5.5 MiB	61 567
;;; defconf: drop invalid															
2	✗ drop	input												341 B	6
;;; defconf: accept ICMP															
3	✓ acc...	input			1 (icmp)									0 B	0
;;; defconf: accept to local loopback (for CAPsMAN)															
4	✓ acc...	input	127.0.0.1											0 B	0
;;; defconf: drop all not coming from LAN															
5	✗ drop	input								!LAN				201.2 KiB	1 096

5 items out of 12



Firewall

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

Filter: Find

#	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
```

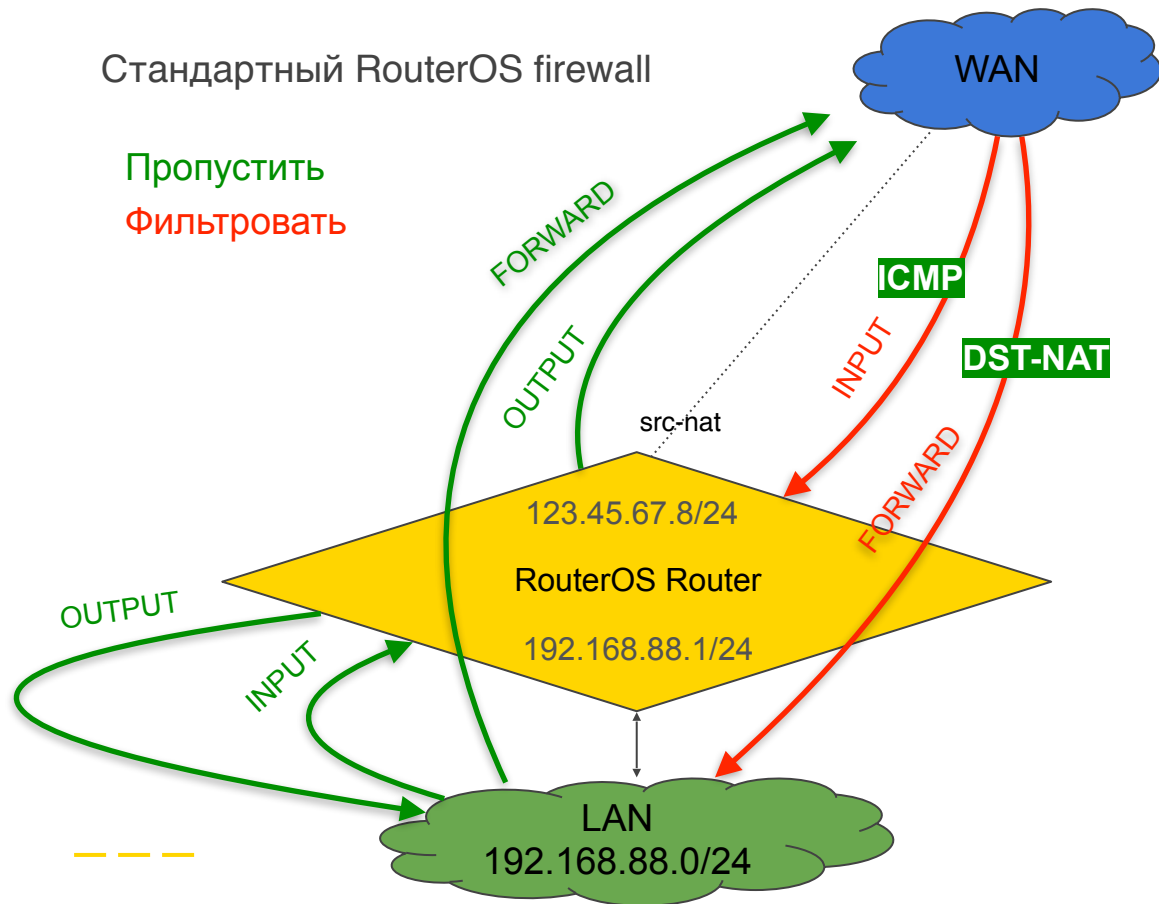
```
add action=drop chain=forward comment="defconf: drop invalid" connection-state=invalid
```

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



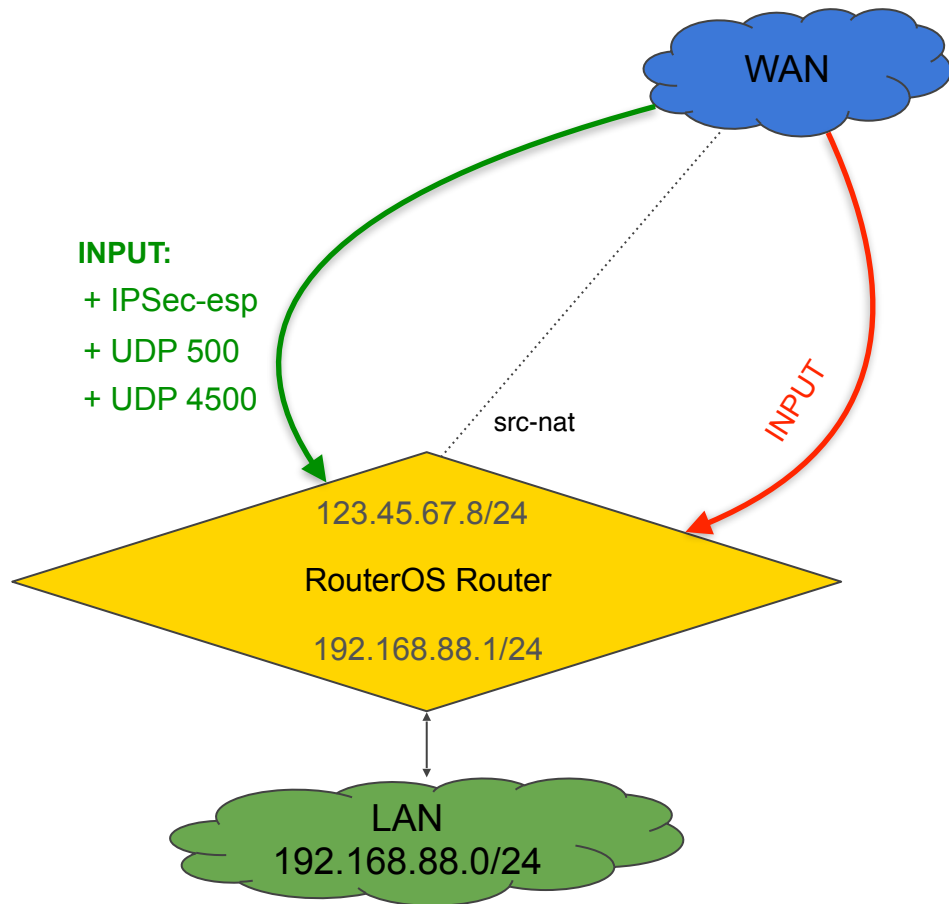
Настройка Firewall

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

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 Mar

#	Action	Chain
1	✓ acc...	input
2	✗ drop	input
3	✓ acc...	input
4	✗ drop	input

New Firewall Rule

General Advanced Extra Action Statistics

Chain: input

Src. Address:

Dst. Address: 123.45.67.8

Protocol: udp

Src. Port:

Dst. Port: 500,4500

Any. Port:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State:

Connection NAT State:

enabled

Comment for New Firewall Rule

Allow UDP 500,4500 IPSec for 123.45.67.8

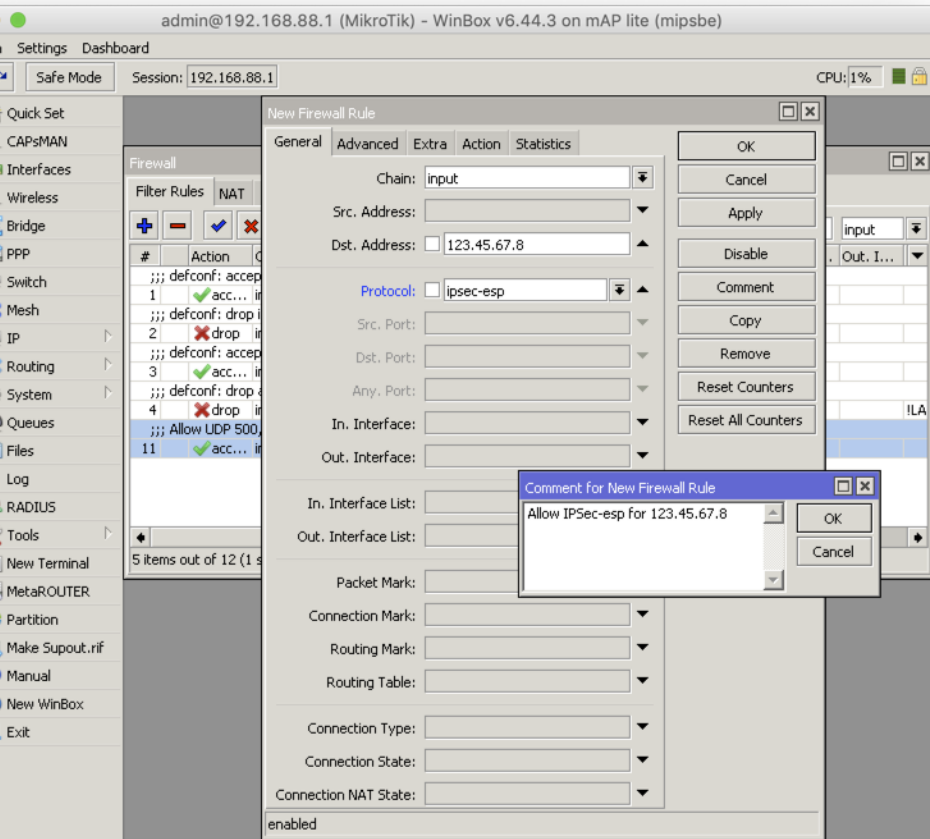
+ UDP 500
+ UDP 4500

```
/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"
```

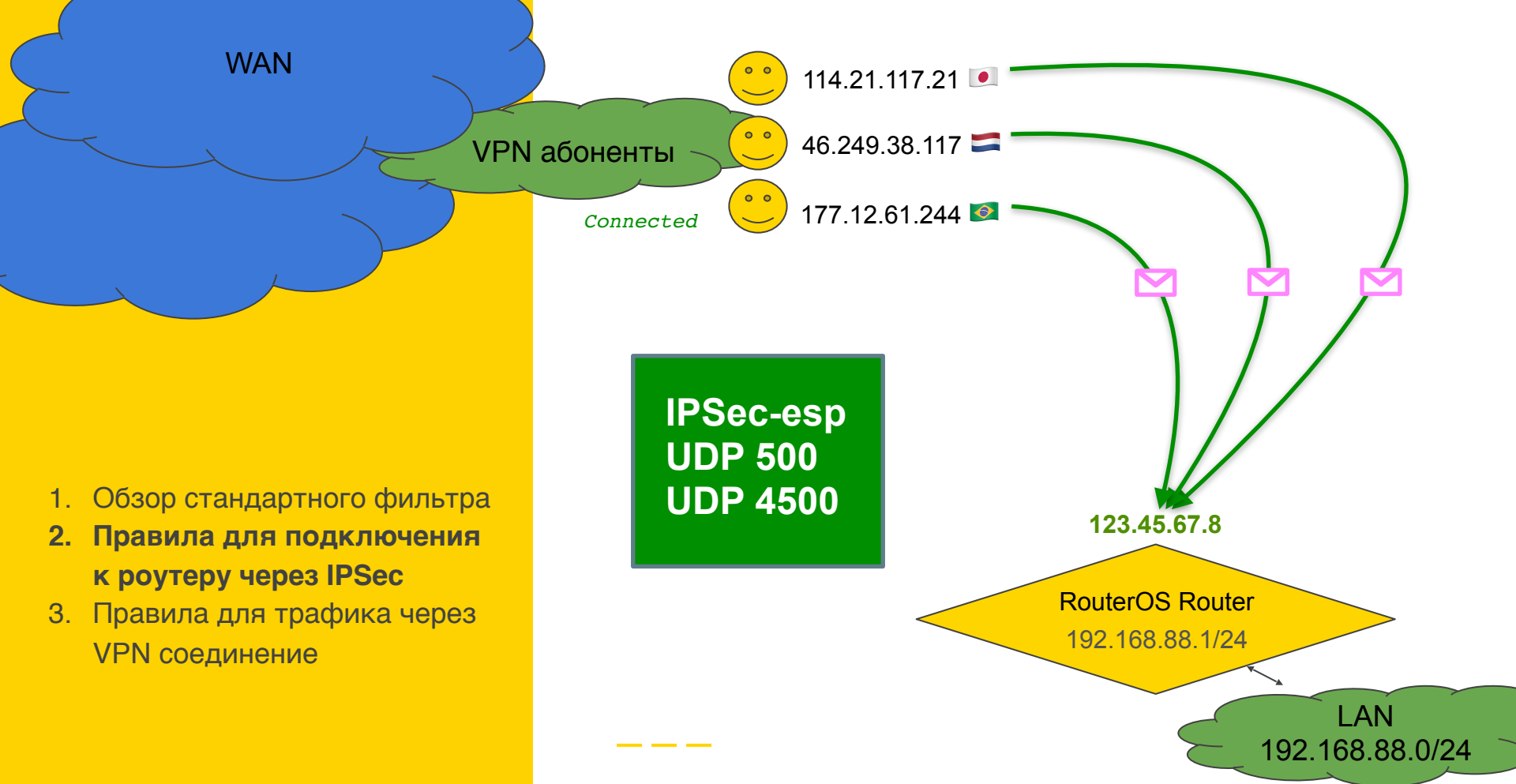
Порядок правил фильтра firewall для IPSec трафика (defconf)

INPUT chain

Поднимаем **accept** правила
ВШЕ **drop**

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Int...	Out. I...
1	accept	input							
2	drop	input							
3	accept	input			1 (icmp)				
4	drop	input							
11	accept	input	123.45.67.8	123.45.67.8	17 (udp)	500,4500			
12	accept	input	123.45.67.8	123.45.67.8	50 (ipsec-esp)				

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Int...	Out. I...
1	accept	input							
2	drop	input							
3	accept	input			1 (icmp)				
4	accept	input	123.45.67.8	123.45.67.8	17 (udp)	500,4500			
5	accept	input	123.45.67.8	123.45.67.8	50 (ipsec-esp)				
6	drop	input							

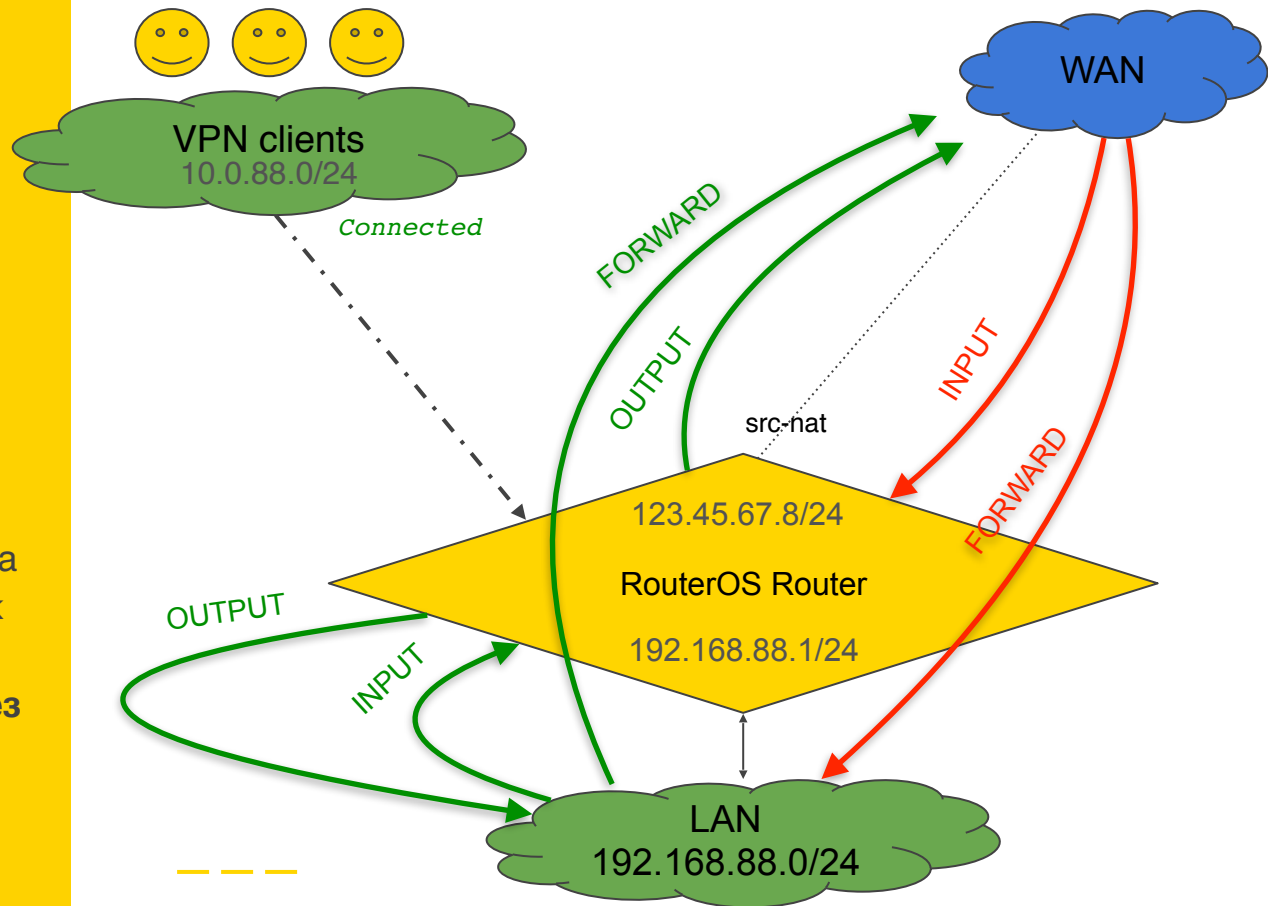


Настройка Firewall

Правила для трафика через VPN соединение

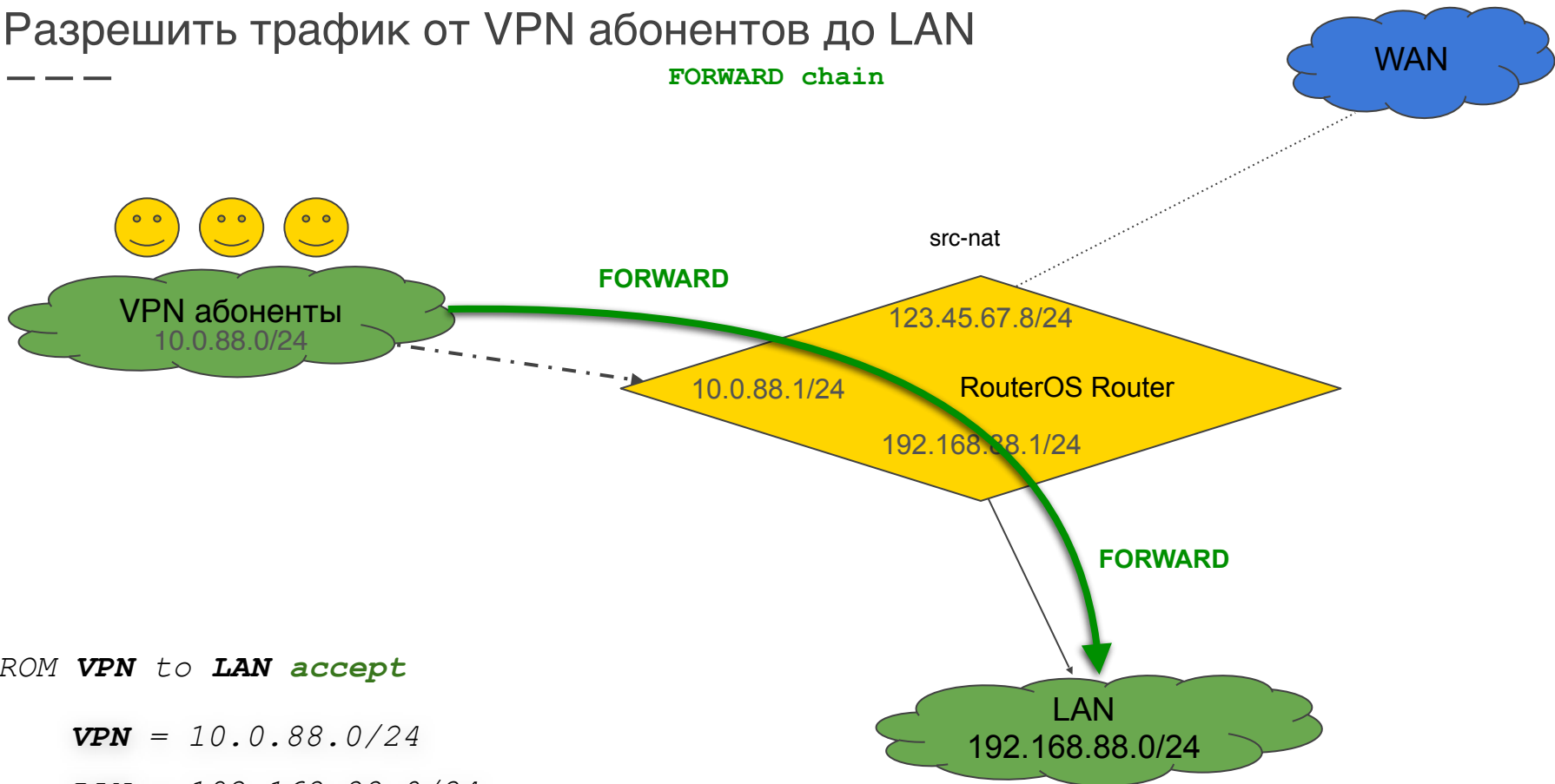
Настройка Firewall

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*

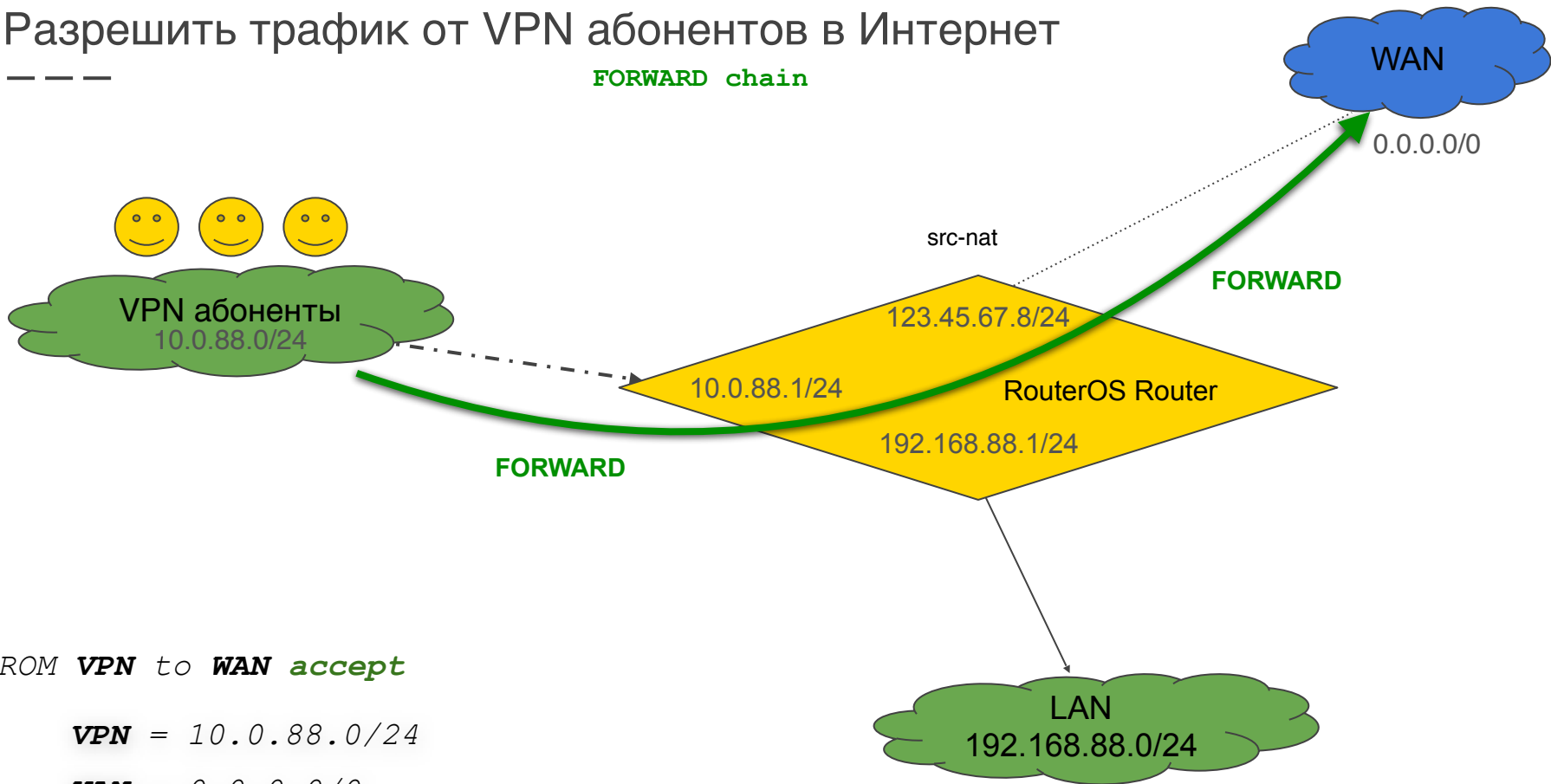
VPN = 10.0.88.0/24

LAN = 192.168.88.0/24



Разрешить трафик от VPN абонентов в Интернет

FORWARD chain



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

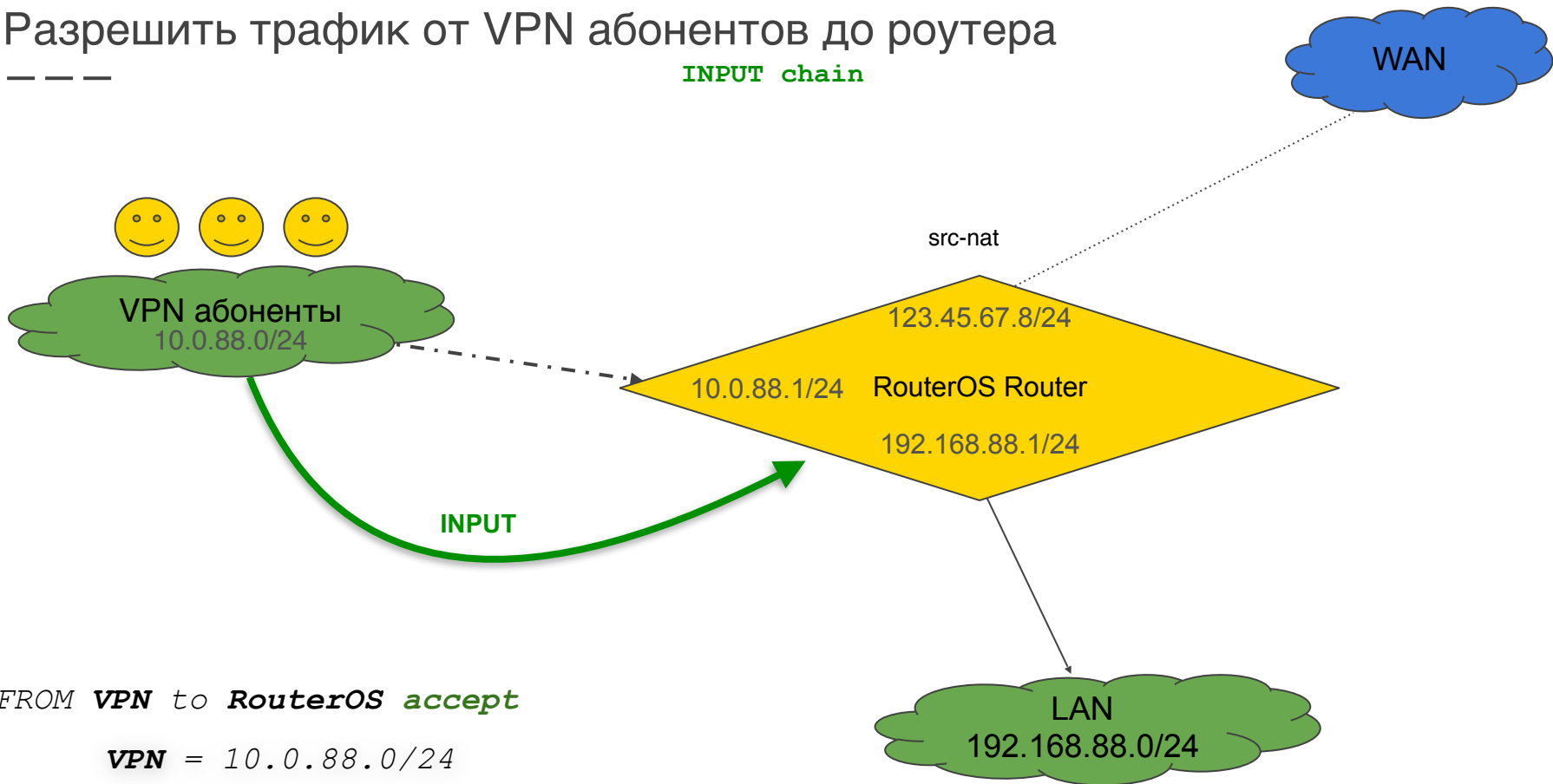
VPN = 10.0.88.0/24

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

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

Session: 192.168.88.1 CPU: 0%

New Firewall Rule

Chain: forward

Src. Address: 10.0.88.0/24

Dst. Address: 192.168.88.0/24

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

IPsec Policy: in : ipsec

Comment for New Firewall Rule

IKE2: Allow ALL forward traffic from 10.0.88.0/24 to LAN network

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

The screenshot shows the Mikrotik WinBox interface with the 'New Firewall Rule' dialog box open. The 'General' tab is selected, and the 'Chain' is set to 'forward'. The 'Src. Address' is '10.0.88.0/24' and the 'Dst. Address' is '0.0.0.0/0'. The 'Protocol' is set to 'ipsec'. The 'Action' is 'accept'. A comment dialog box is open, showing the text: 'IKE2: Allow ALL forward traffic from 10.0.88.0/24 to ANY network'. The 'Policy' is set to 'in' and 'ipsec'.

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

VPN = 10.0.88.0/24

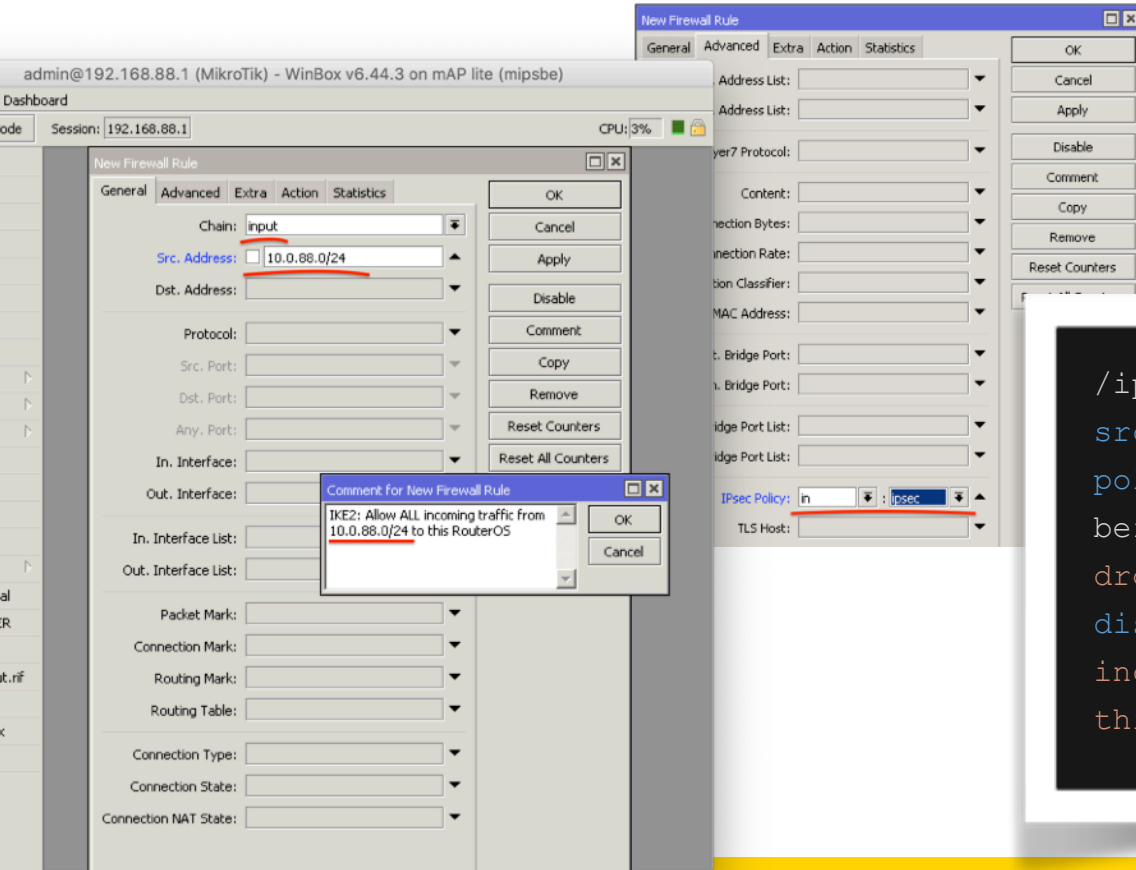
WAN = 0.0.0.0/0

```
/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

00 Reset Counters 00 Reset All Counters 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...							
1	✓	defconf: accept in ipsec policy							
7	✓	acc...							
8	✓	defconf: accept out ipsec policy							
9	▶	defconf: fasttrack							
;;; defconf: accept established,related, untracked									
10	✓	acc...							
;;; defconf: drop invalid									
11	✗	drop							
;;; defconf: drop all from WAN not DSTNATED									
12	✗	drop							

7 items out of 13 (2 selected)

Per Connection Classifier: []

Src. MAC Address: []

Out. Br: []

Port List: []

Age Port List: []

IPsec Policy: in : ipsec

TLS Host: []

Priority: []

Packet Size: []

Reset Counters

Reset All Counters

Content: []

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: []

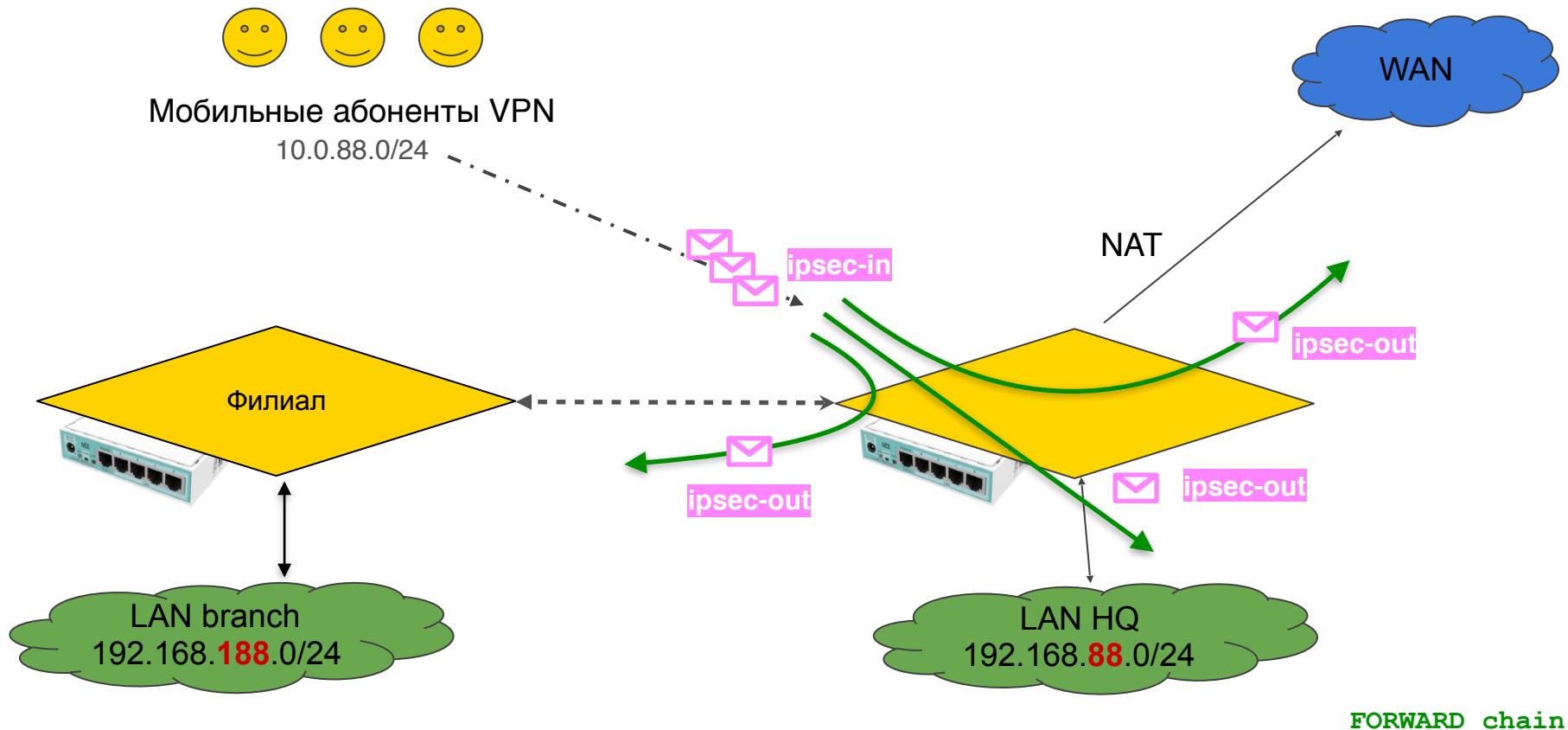
Comment

Copy

Remove

Reset Counters

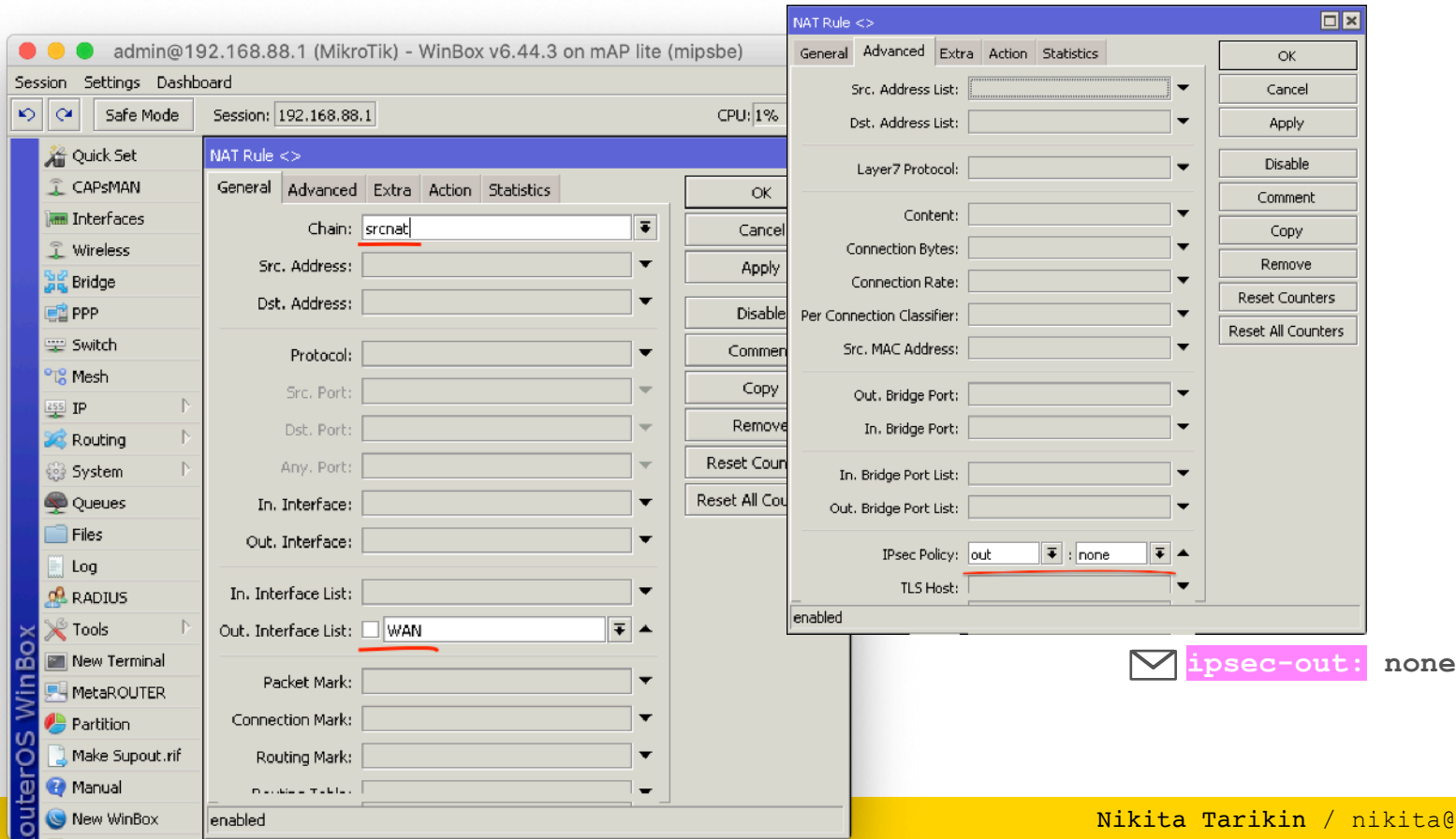
Reset All Counters



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

Настройка NAT

Обзор правила NAT стандартного Firewall (defconf)



The image displays the Mikrotik WinBox interface for configuring a NAT rule. The main window shows the 'General' tab of the 'NAT Rule <>' configuration. The 'Chain' is set to 'srcnat' and the 'Out. Interface List' includes 'WAN'. A smaller window in the foreground shows the 'IPsec Policy' dropdown menu, which is set to 'out' and 'none'. The 'IPsec Policy' dropdown is highlighted with a red underline and a red box around the text 'ipsec-out: none'.

routerOS WinBox

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%

Quick Set CAPsMAN Interfaces Wireless Bridge PPP Switch Mesh IP Routing System Queues Files Log RADIUS Tools New Terminal MetaROUTER Partition Make Supout.rif Manual New WinBox

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:

Enabled: 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

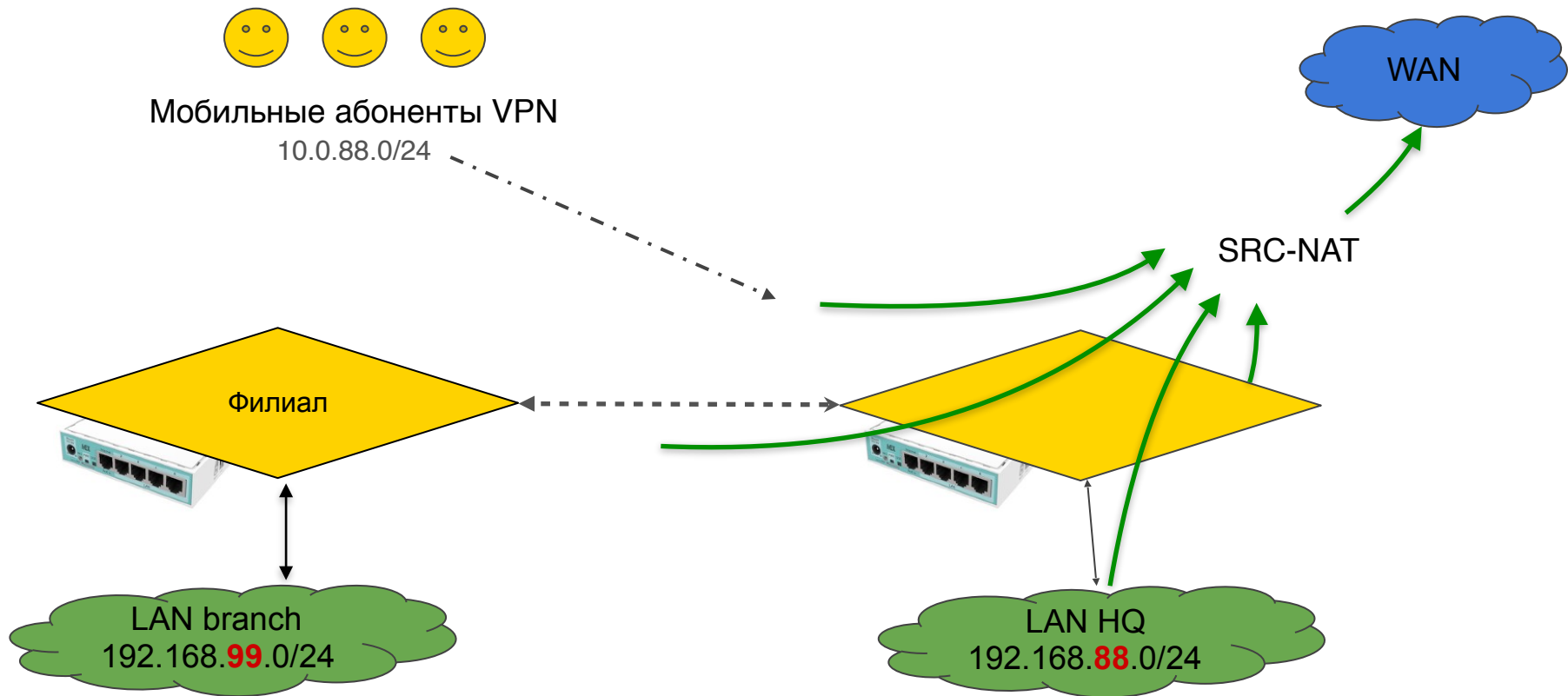
TLS Host:

enabled

OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters

ipsec-out: none

Nikita Tarikin / nikita@tarikin.com



Обзор правила NAT стандартного Firewall (defconf)

Маскарад VPN трафика

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

Session: 192.168.88.1 CPU: 2%

New NAT Rule

General | Advanced | Extra | Action | Statistics

Chain: srcnat

Src. Address: 10.0.88.0/24

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:

Routing Table:

Connection Type:

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, Reset All Counters

New NAT Rule

General | Advanced | Extra | Action | Statistics

Src. Address List:

Dst. Address List:

Layer7 Protocol:

Content:

Connection Bytes:

Connection Rate:

Connection Classifier:

Src. MAC Address:

Out. Bridge Port:

In. Bridge Port:

In. Bridge Port List:

Out. Bridge Port List:

Ipssec Policy: out : none

TLS Host:

Ingress Priority:

Priority:

DSCP (TOS):

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, Reset All Counters

New NAT Rule

General | Advanced | Extra | Action | Statistics

Action: masquerade

Log

Log Prefix:

To Ports:

```
/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)



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

Session: 192.168.88.1 CPU: 0%

Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
Routing
System
Queues
Files
Log
RADIUS
Tools
New Terminal
MetaROUTER
Partition
Make Supout.rif
Manual
New WinBox

New NAT Rule

General Advanced Extra Action Statistics

Chain: srcnat

Src. Address: 10.0.88.0/24

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface: ether1

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

Comment For New NAT Rule

SRC-NAT IKE2:10.0.88.0/24 --> ether1 traffic

OK
Cancel

New NAT Rule

General Advanced Extra Action Statistics

Action: src-nat

Log

Log Prefix:

To Addresses: 123.45.67.8

To Ports:

Reset Counters
Reset All Counters

```
/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"
```

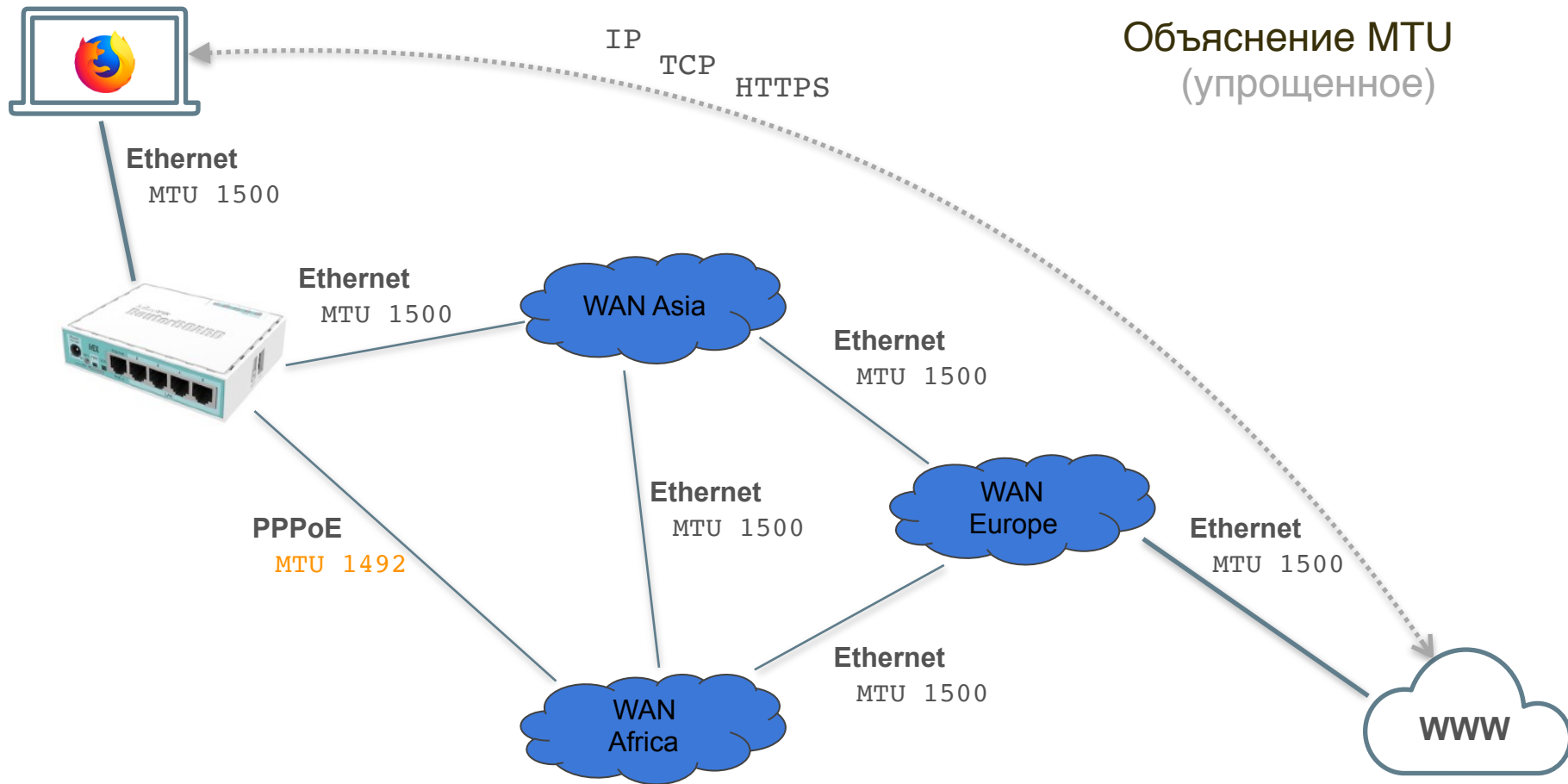


Настройка TCP MSS

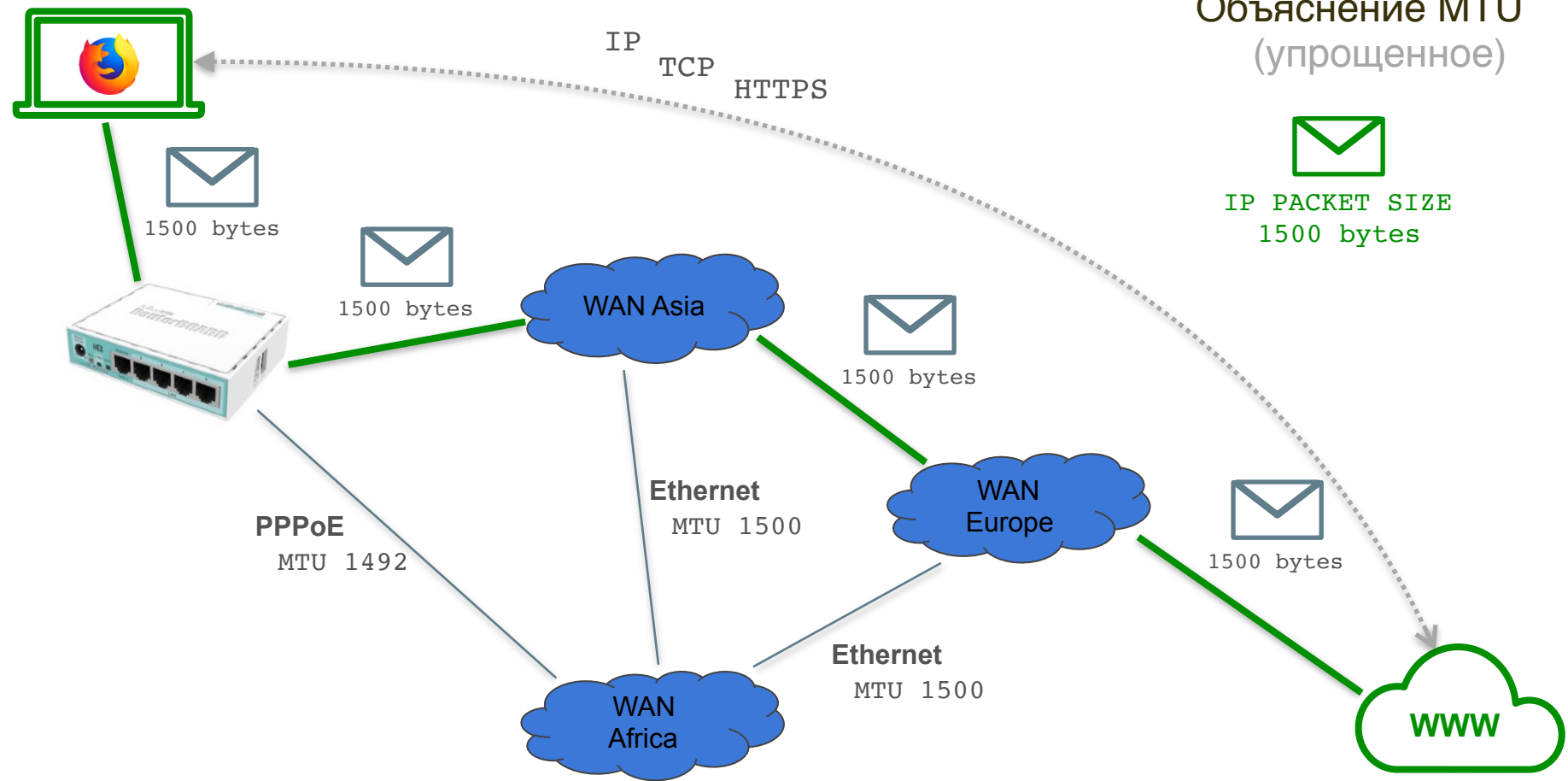
План действий

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

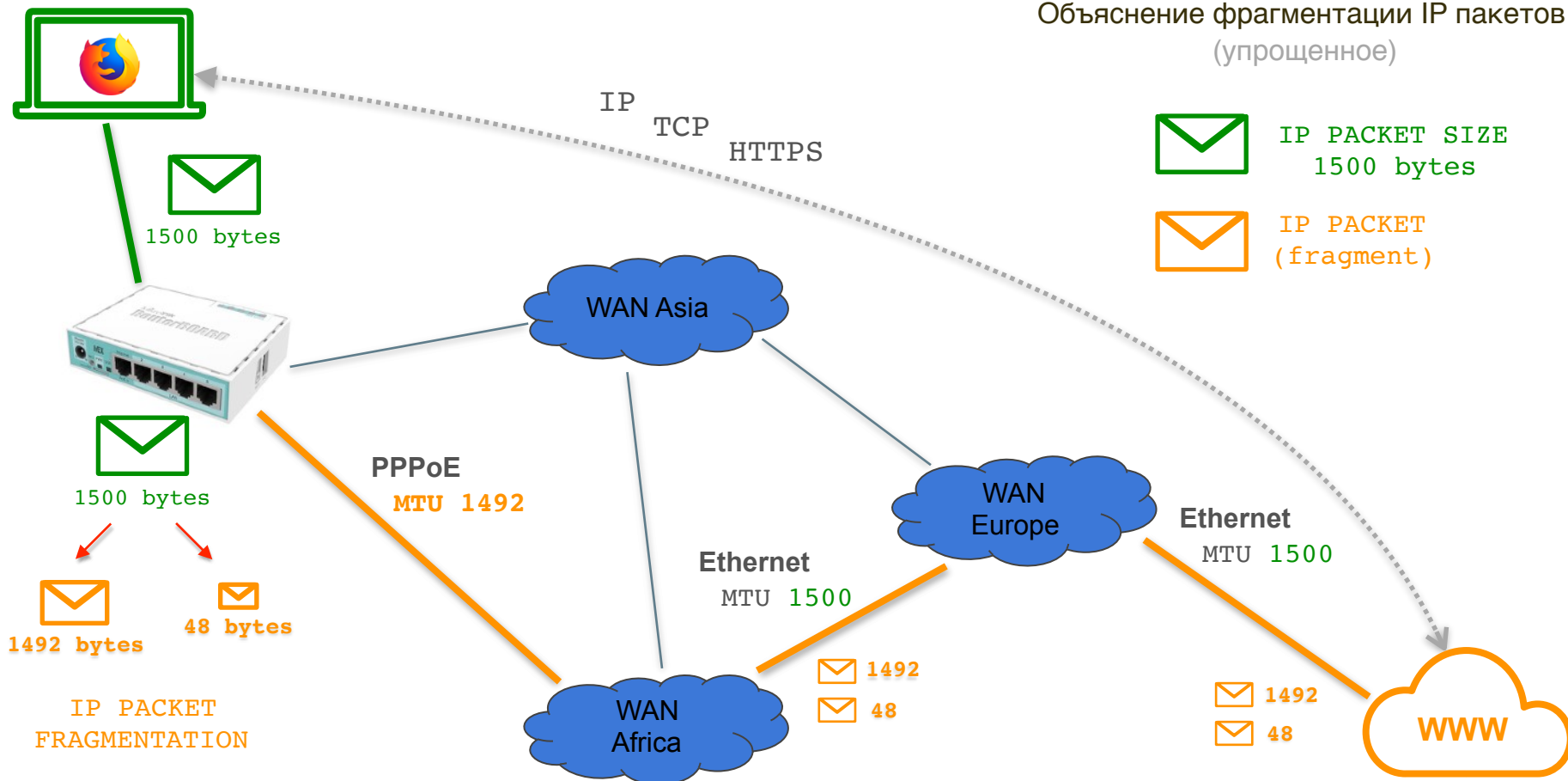




Объяснение MTU (упрощенное)



Объяснение фрагментации IP пакетов (упрощенное)



Несоответствие MTU → фрагментация IP пакетов



1500



Ethernet
MTU 1500



1500



PPPoE
MTU 1492



1492 bytes



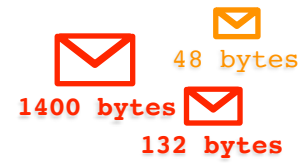
Ethernet
MTU 1500



48 bytes
1492 bytes



IPSec tunnel
MTU 1400

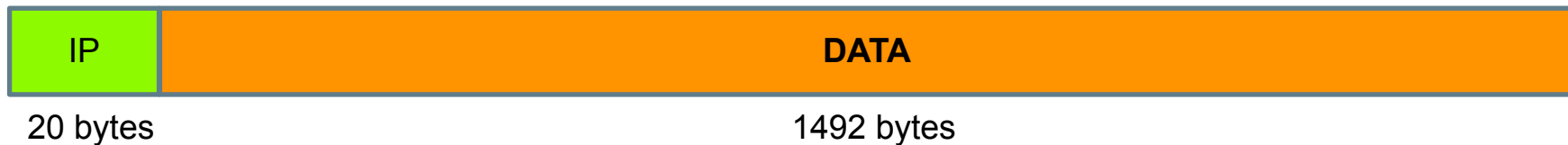


48 bytes
1400 bytes
132 bytes

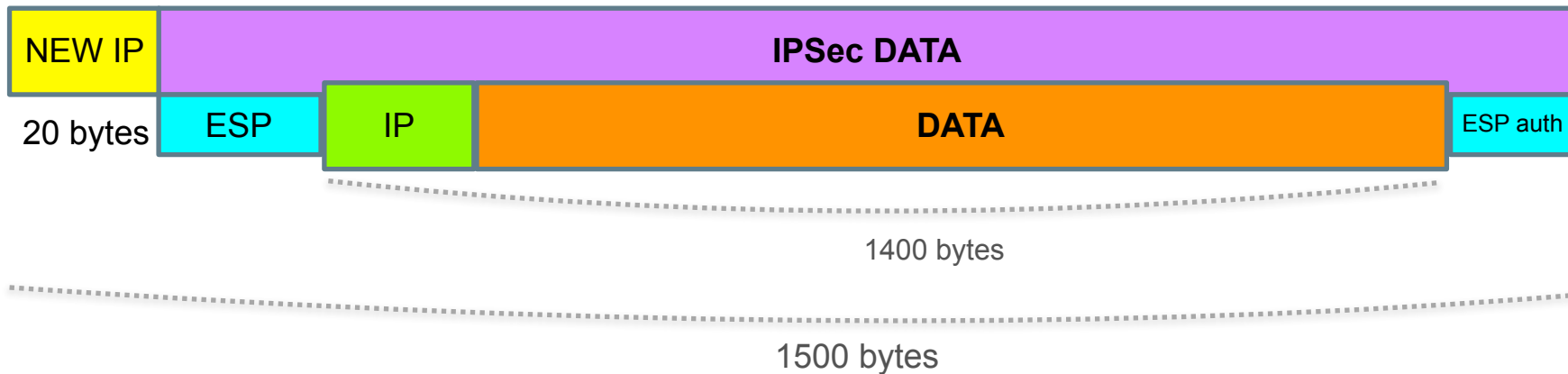


Объяснение IPSec MTU (упрощенное)

IP packet

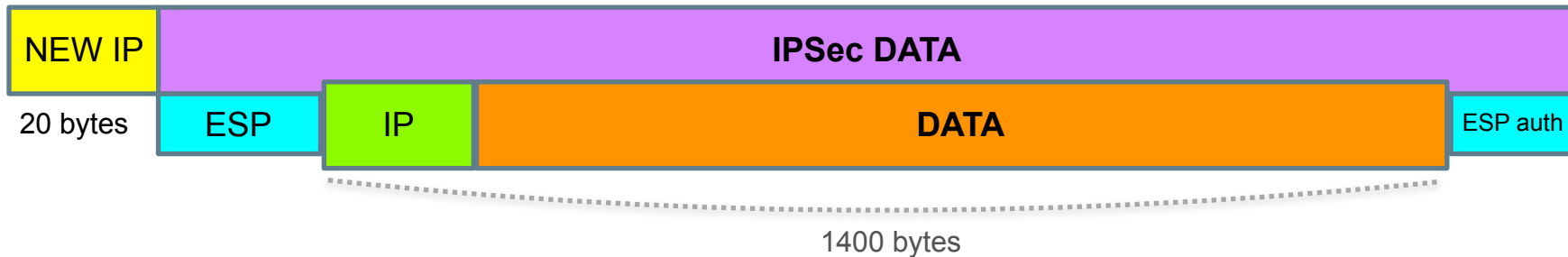


IPSec ESP packet (*tunnel mode*)

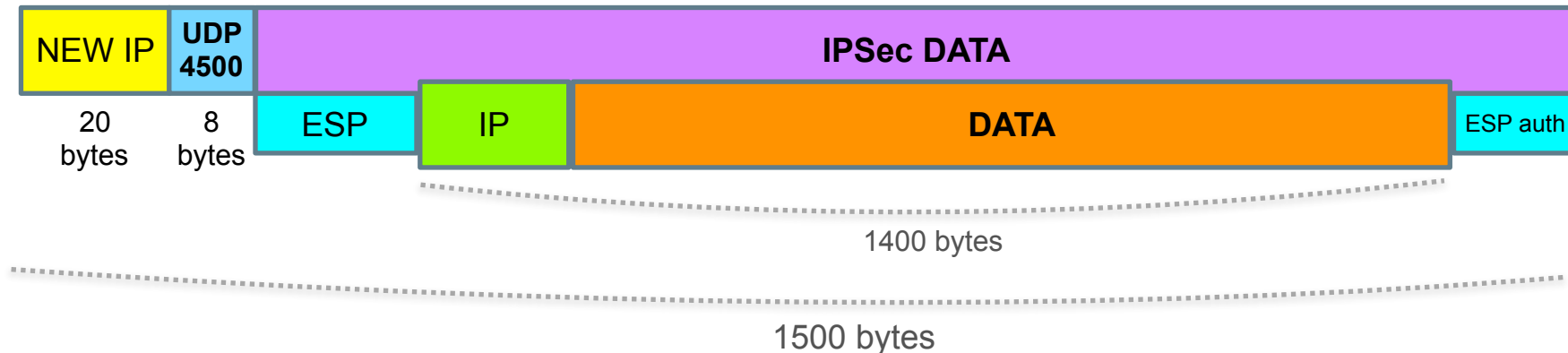


Объяснение IPSec MTU (упрощенное)

IPSec ESP packet (*tunnel mode*)

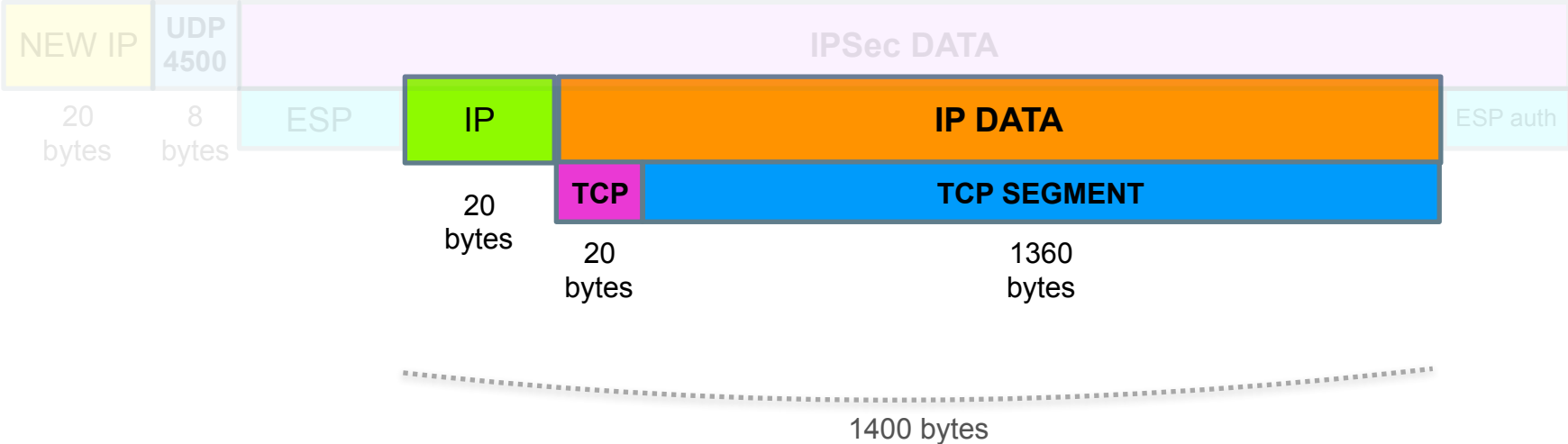


IPSec ESP packet with NAT-T (*tunnel mode*)



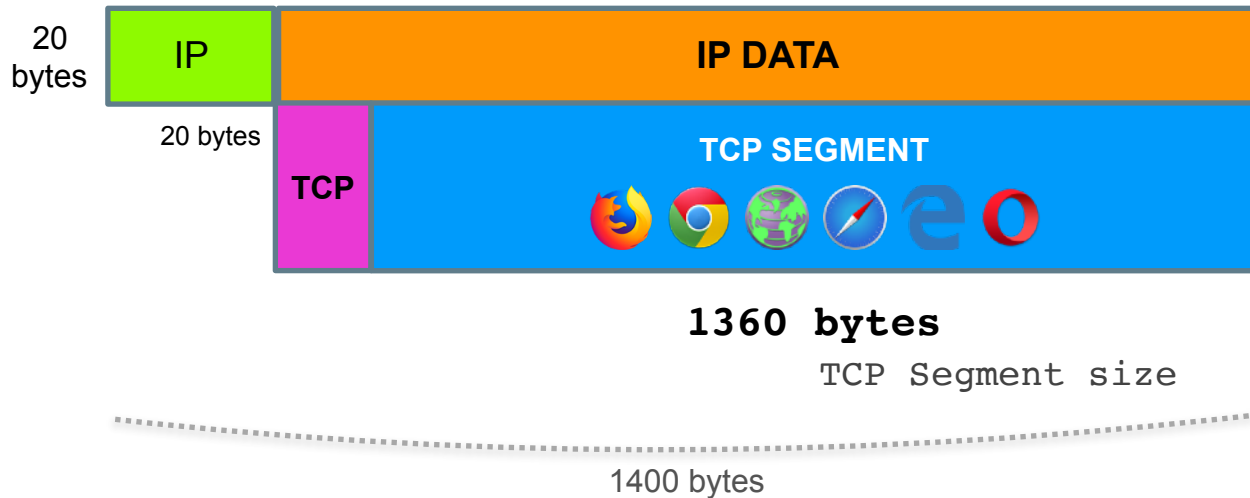
Объяснение IPSec MTU (упрощенное)

IPSec ESP packet with NAT-T (tunnel mode)

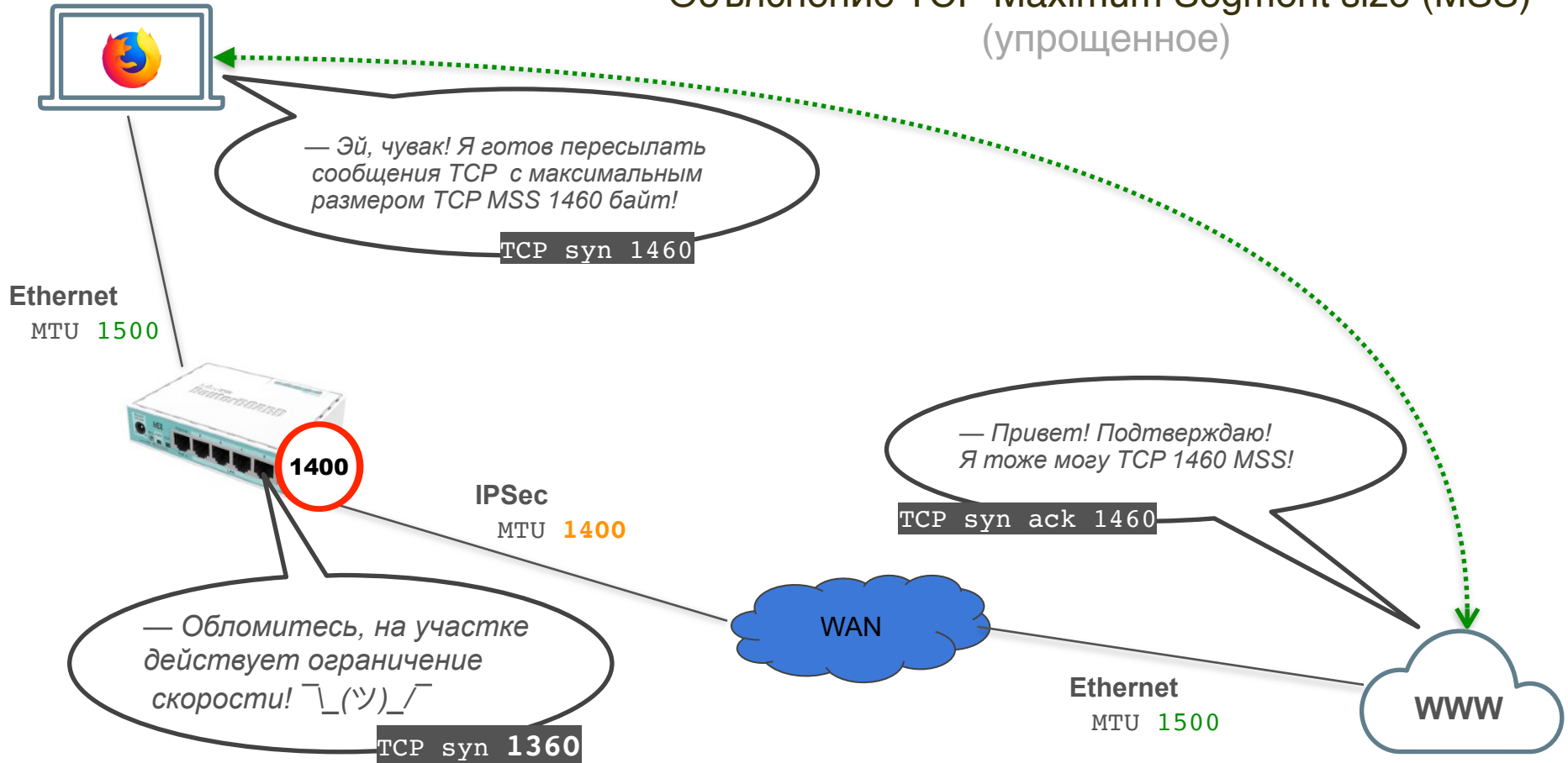


Объяснение IPSec MTU (упрощенное)

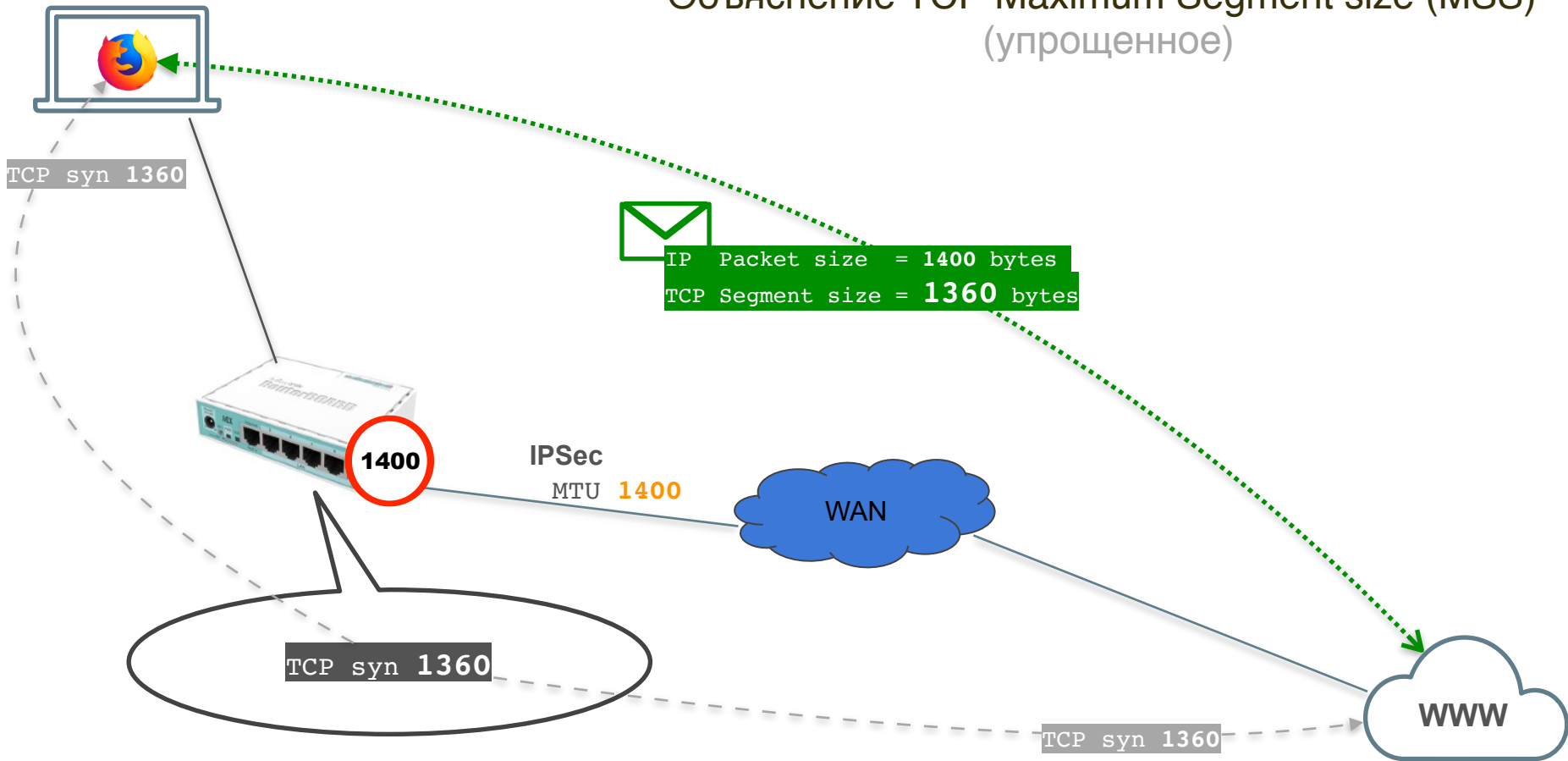
TCP Segment size = MTU - 40 bytes



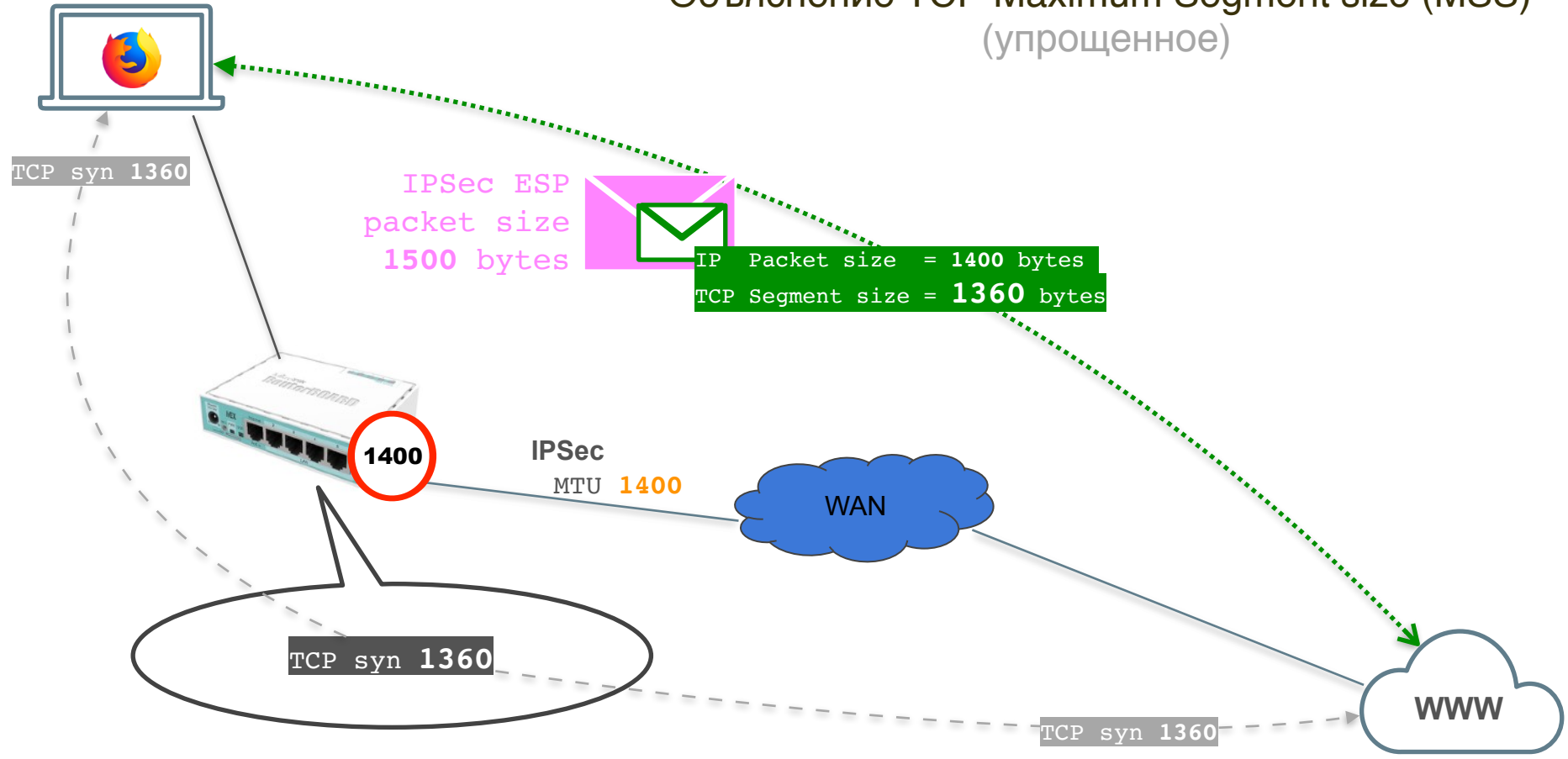
Объяснение TCP Maximum Segment size (MSS) (упрощенное)



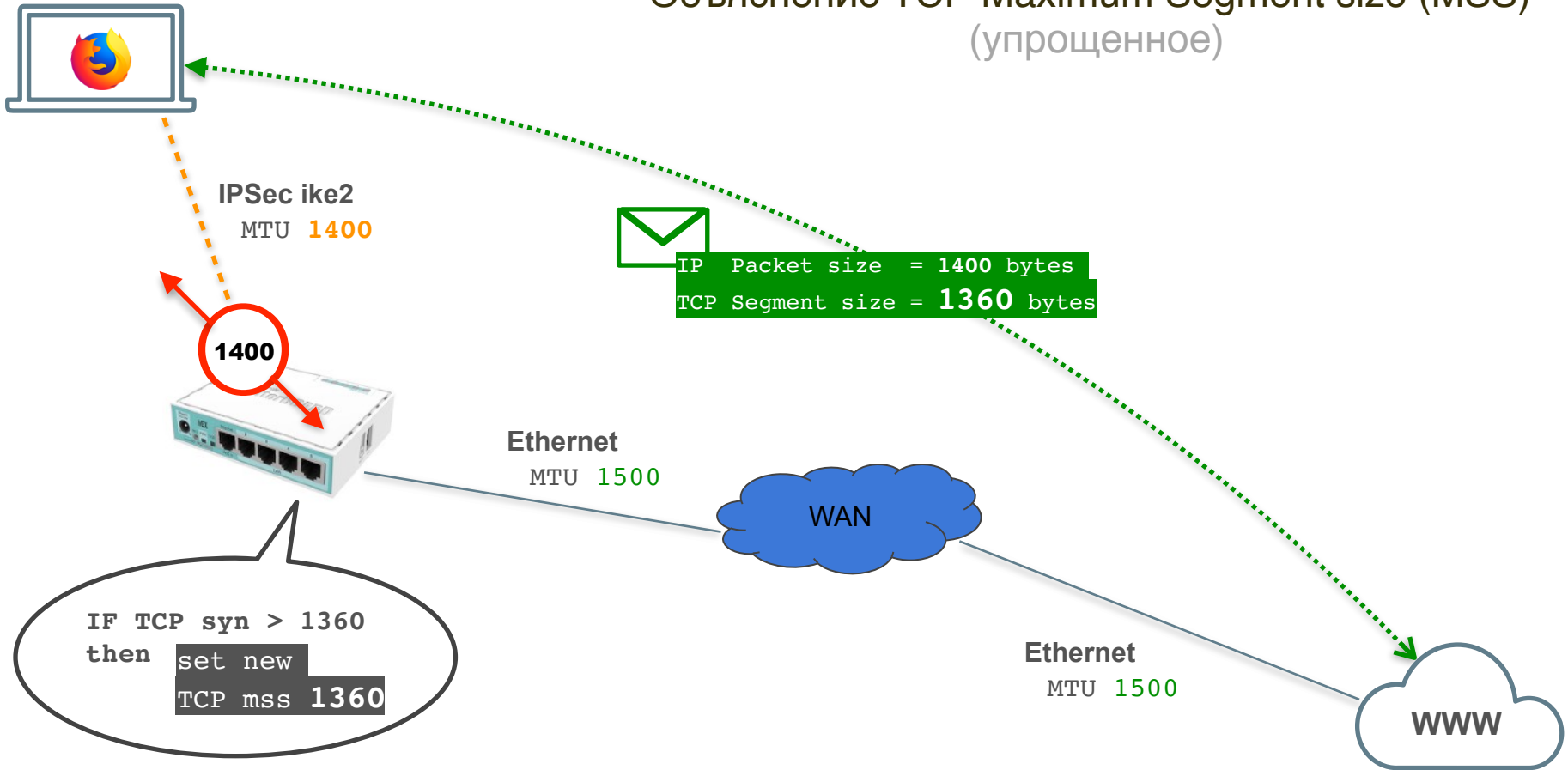
Объяснение TCP Maximum Segment size (MSS) (упрощенное)



Объяснение TCP Maximum Segment size (MSS) (упрощенное)



Объяснение TCP Maximum Segment size (MSS) (упрощенное)



Коррекция TCP MSS от IPsec IKE2 адресов

The image shows a sequence of three screenshots from Mikrotik WinBox v6.44.3 on mAP lite (mipsbe) illustrating the configuration of a Mangle rule to clamp TCP MSS for IKE2 traffic.

Left Screenshot: The 'New Mangle Rule' dialog box is open. The 'Chain' is set to 'forward', 'Src. Address' is '10.0.88.0/24', and 'Protocol' is 'tcp'. The 'Action' is set to '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 also open, containing the text: 'IKE2: Clamp TCP MSS from 10.0.88.0/24 to ANY'.

Middle Screenshot: The 'New Mangle Rule' dialog box is open. The 'Chain' is set to 'forward', 'Src. Address' is '10.0.88.0/24', and 'Protocol' is 'tcp'. The 'Action' is set to '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 also open, containing the text: 'IKE2: Clamp TCP MSS from 10.0.88.0/24 to ANY'.

Right Screenshot: The 'New Mangle Rule' dialog box is open. The 'Chain' is set to 'forward', 'Src. Address' is '10.0.88.0/24', and 'Protocol' is 'tcp'. The 'Action' is set to '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 also open, containing the text: '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 for configuring a New Mangle Rule. The rule is named "New Mangle Rule" and is configured with the following settings:

- Chain: forward
- Src. Address: (empty)
- Dst. Address: 10.0.88.0/24
- Protocol: 6 (tcp)
- Src. Port: (empty)
- Dst. Port: (empty)
- Any. Port: (empty)
- In. Interface: (empty)
- Out. Interface: (empty)
- In. Interface List: (empty)
- Out. Interface List: (empty)
- Packet Mark: (empty)
- Connection Mark: (empty)
- Routing Mark: (empty)
- Routing Table: (empty)
- Connection Type: (empty)
- Connection State: (empty)
- Connection NAT State: (empty)

The Action tab is selected, showing the action set to "change MSS". The "New TCP MSS" is set to 1360. The "Log" checkbox is unchecked, and "Passthrough" is checked. A comment box is open, containing the text: "IKE2: Clamp TCP MSS from ANY to 10.0.88.0/24".

```
/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

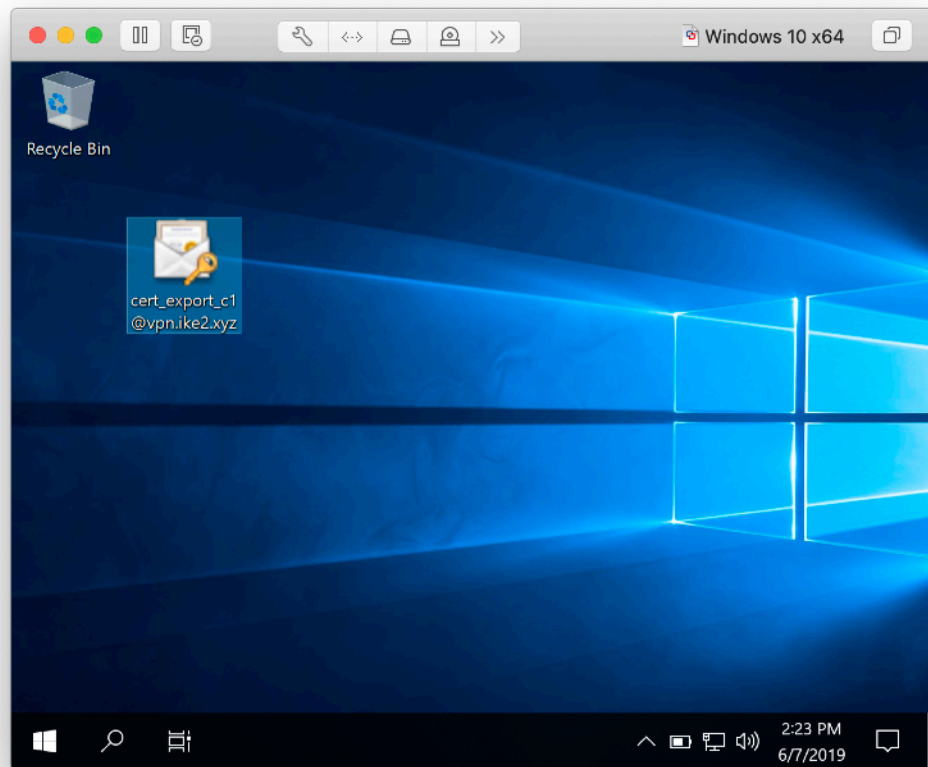
План действий

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



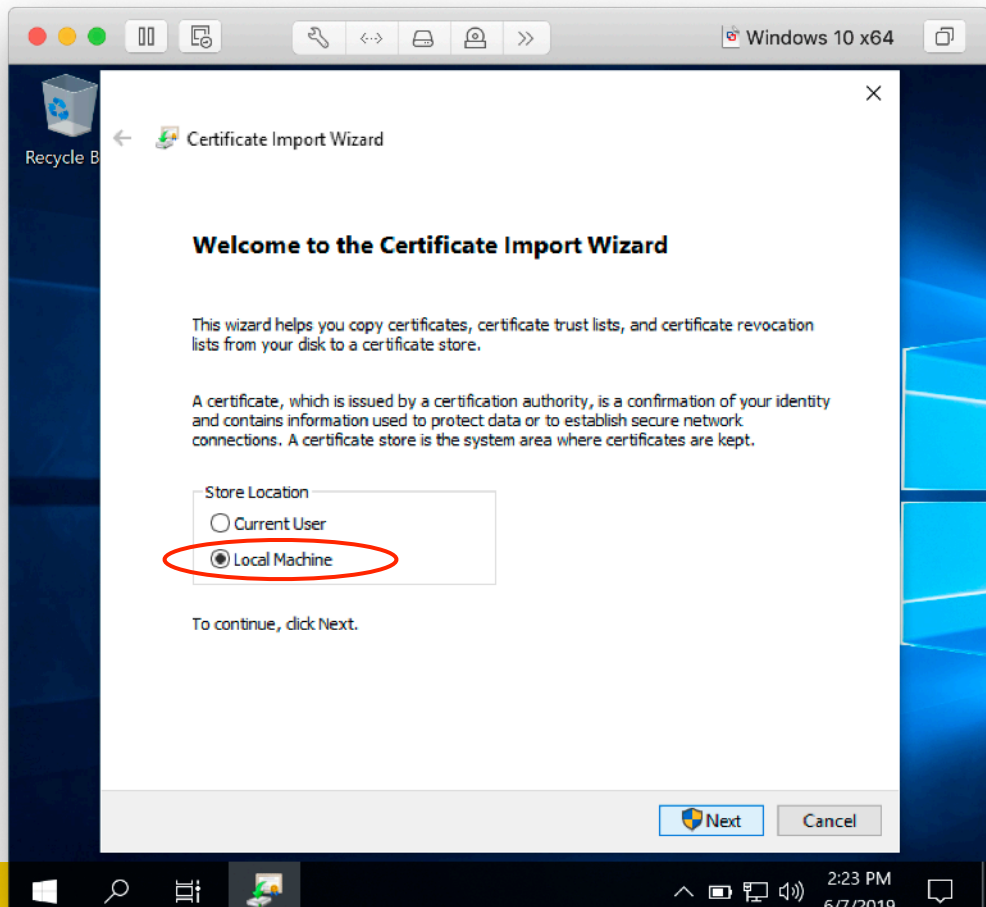
Windows 10: Импорт SSL сертификатов

— — —



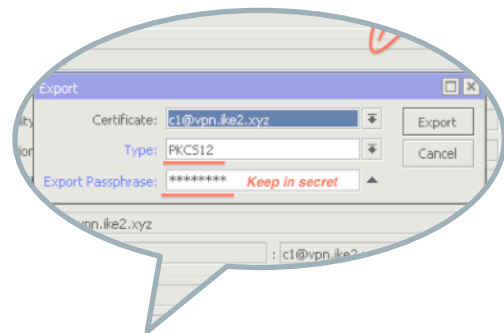
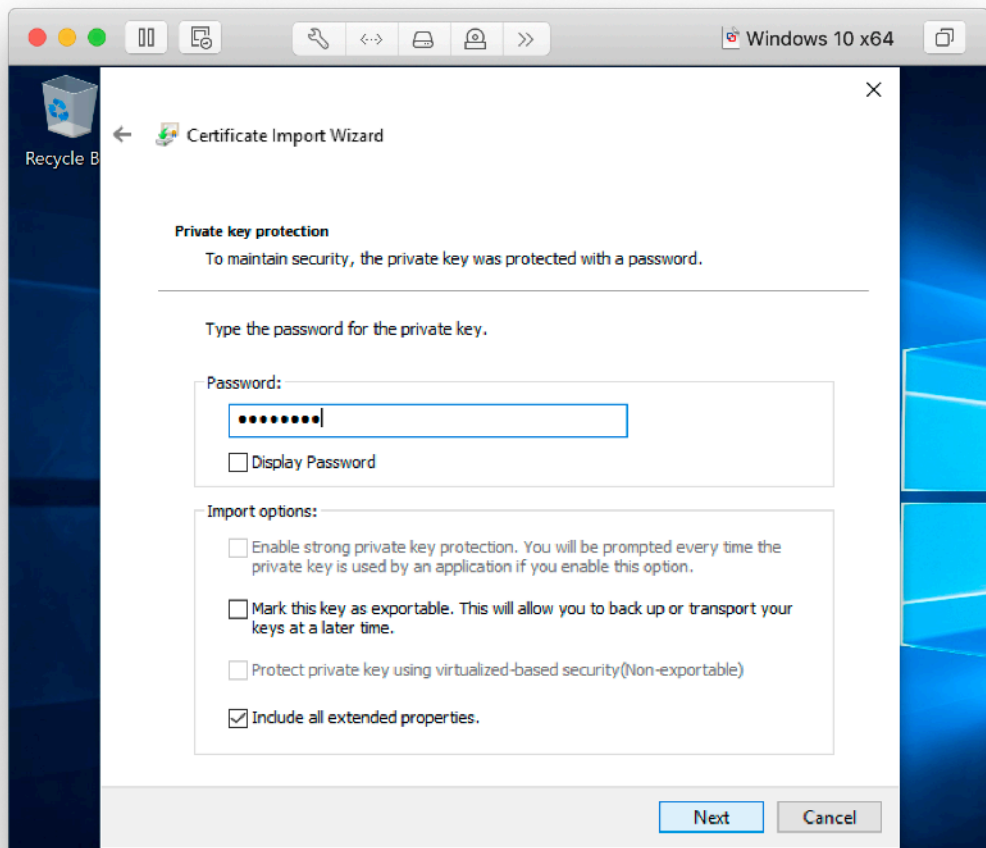
Скачать .p12 сертификат

Windows 10: Импорт SSL сертификатов



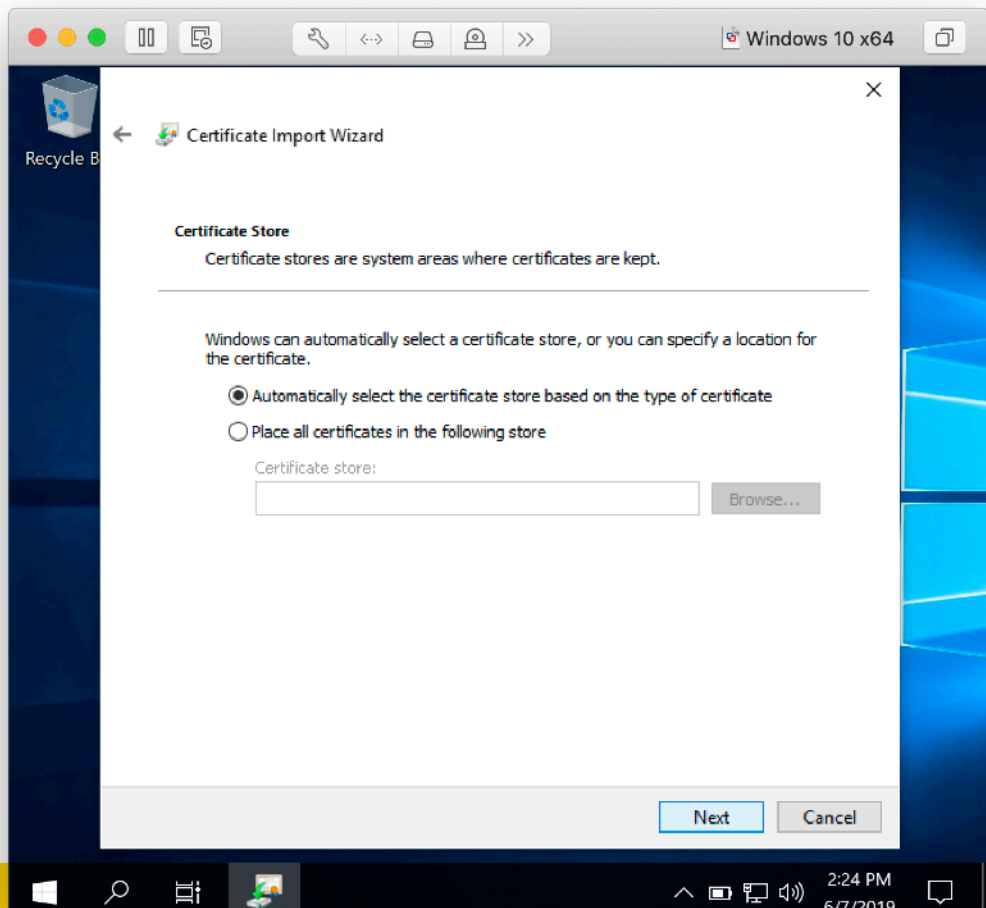
Выбрать **Local Machine** хранилище
—> **Далее**

Windows 10: Импорт SSL сертификатов



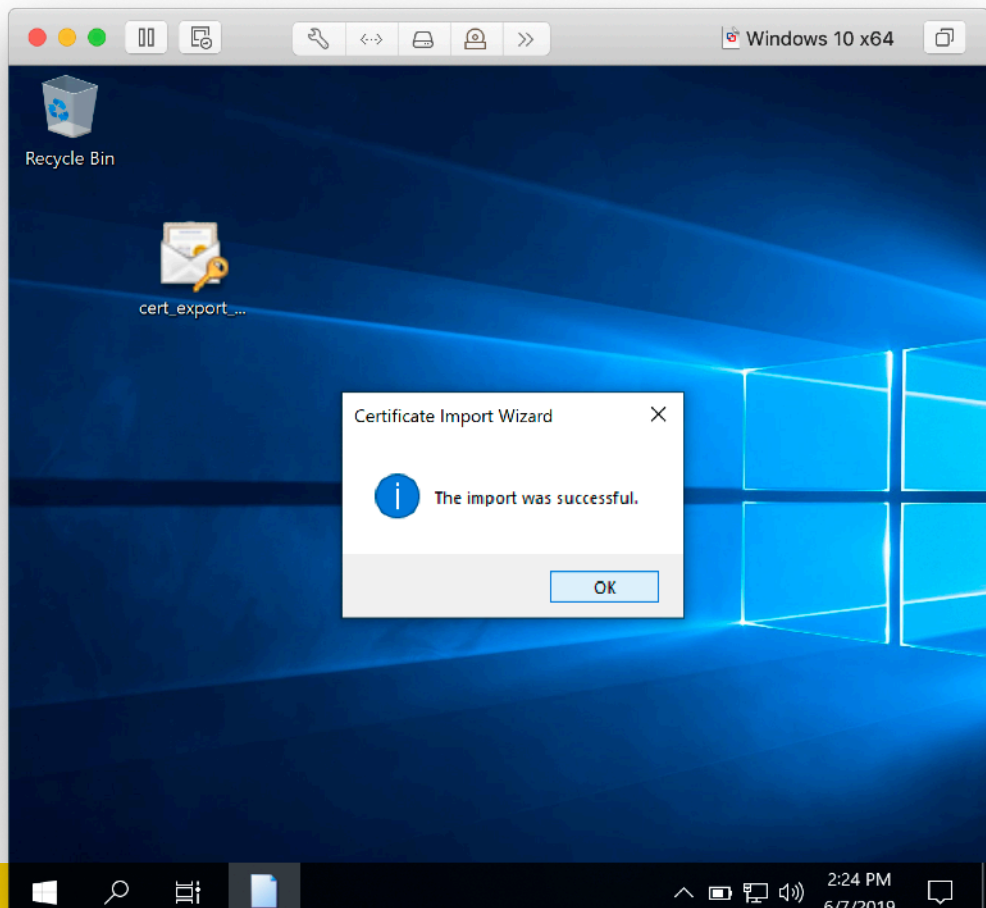
Ввести пароль
SSL сертификата клиента
—> **Далее**

Windows 10: Импорт SSL сертификатов



Автоматический выбор
—> **Далее**

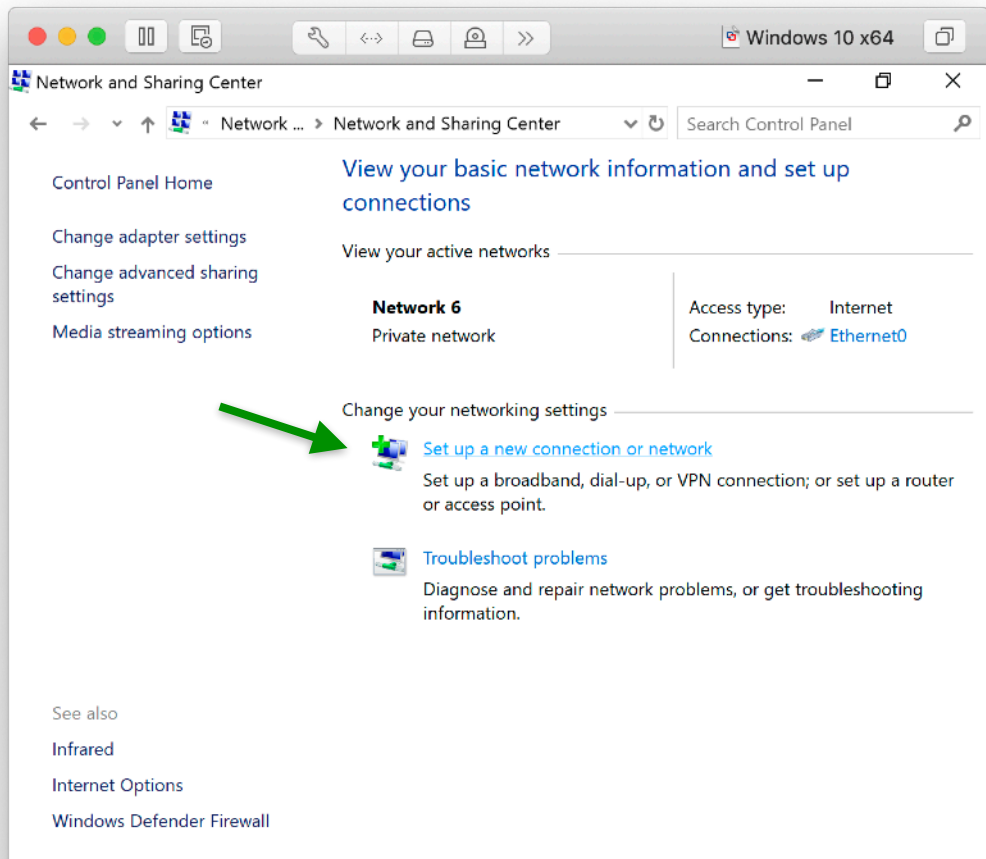
Windows 10: Импорт SSL сертификатов



SSL сертификат
успешно импортирован

—> **OK**

Windows 10: Настройка IKEv2 VPN соединения

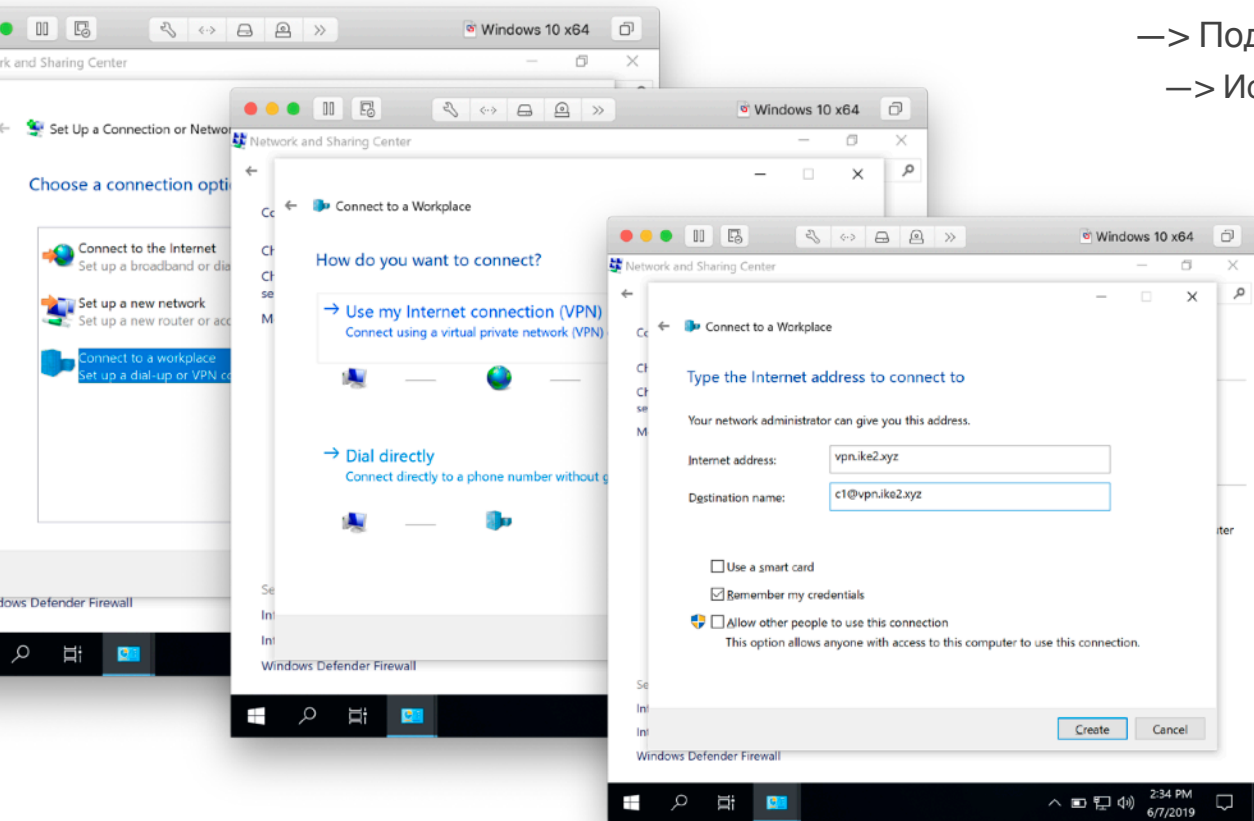


- > Панель управления
- > Сеть и интернет
- > Центр управления сетями

Создание нового подключения



Windows 10: Настройка IKEv2 VPN соединения



- > Подключение к рабоче у месту
- > Использовать мое подключение (VPN)
- > **Далее**

Адрес:

vpn.ike2.xyz

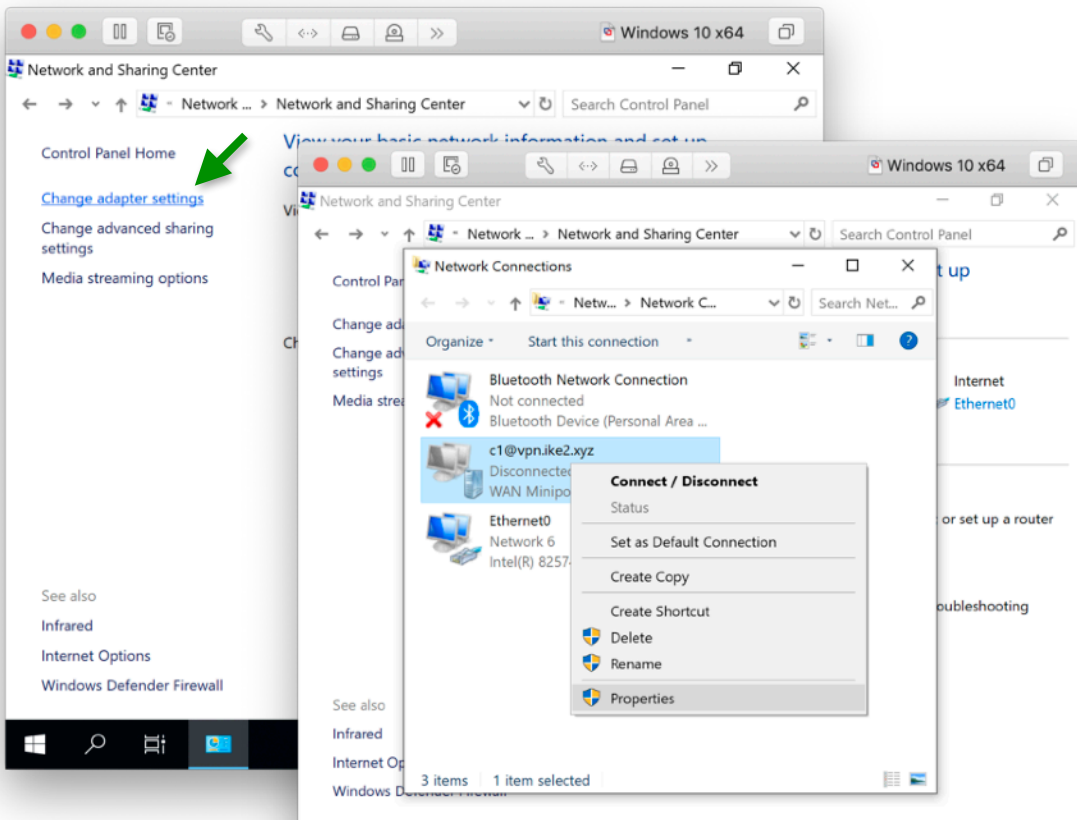
Имя назначения:

c1@vpn.ike2.xyz

—> **Создать**

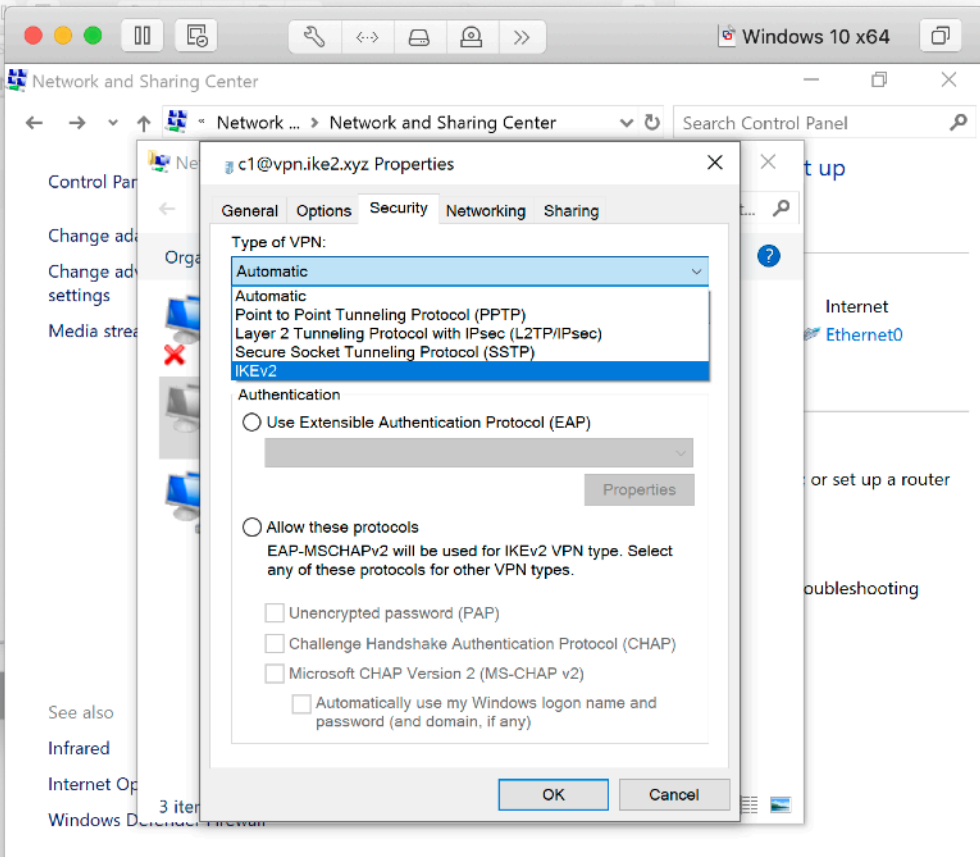


Windows 10: Настройка IKEv2 VPN соединения



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

Windows 10: Настройка IKEv2 VPN соединения



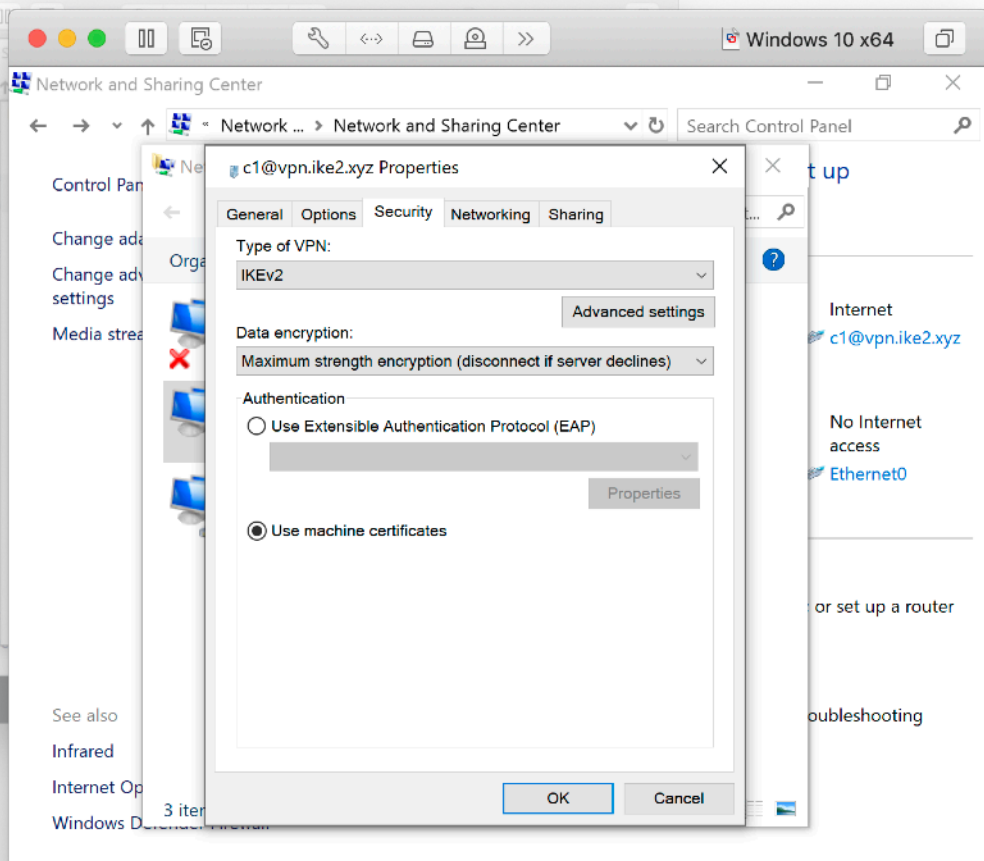
Свойства -> Безопасность

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

The screenshot displays a Windows 10 desktop with several windows open to verify an IKEv2 VPN connection. The background shows the Windows 10 desktop environment with the taskbar at the bottom displaying the time as 2:47 PM on 6/7/2019.

Three windows are visible:

- c1@vpn.ike2.xyz Status**: Shows connection details for the VPN. The 'General' tab is active, displaying:
 - Connection: Internet
 - IPv4 Connectivity: (checked)
 - IPv6 Connectivity: (checked)
 - Media State: (checked)
 - Duration: (empty)The 'Activity' section shows a graph with 'Sent' data: Bytes: 16,011, Compression: 0 %, Errors: 0. Buttons for 'Properties', 'Disconnect', and 'Diagnose' are visible at the bottom.
- Network Connection Details**: A table showing network configuration for the 'Internet' connection:

Property	Value
Connection-specific DNS Suffix	
Description	c1@vpn.ike2.xyz
Physical Address	
DHCP Enabled	No
IPv4 Address	10.0.88.2
IPv4 Subnet Mask	255.255.255.255
IPv4 Default Gateway	
IPv4 DNS Server	10.0.88.1
IPv4 WINS Server	
NetBIOS over Tcpip Enabled	Yes
- Network & Internet settings**: Shows the VPN connection 'c1@vpn.ike2.xyz' as 'Connected'. A green arrow points to this status. Below it, the text 'Network & Internet settings' and 'Change settings, such as making a connection metered.' is visible. The 'Airplane mode' toggle is also present.



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

Mode Configs

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

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
10.20.0.0/22              255.255.255.255 On-link          10.0.88.2        281
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
172.16.0.0/22             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: 32

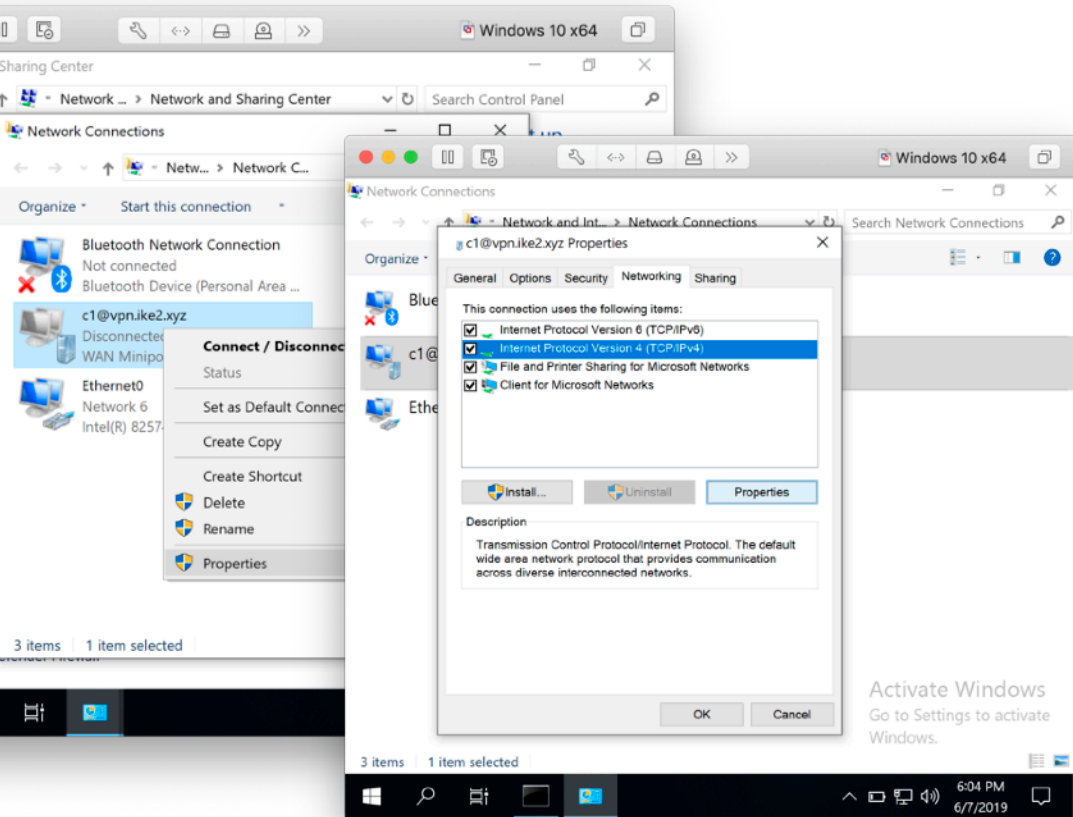
Split Include: 192.168.99.0/24
172.16.0.0/22
10.20.0.0/21

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: отключаем пересылку всего трафика через IKEv2 VPN

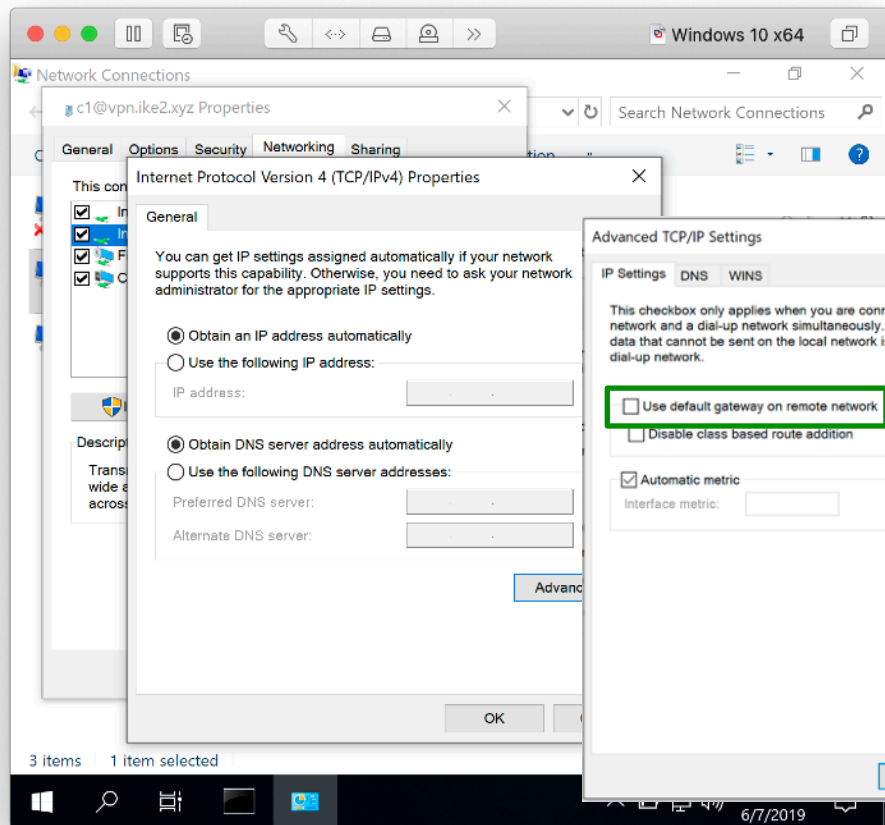


Свойства -> Сеть

✓ 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

—>

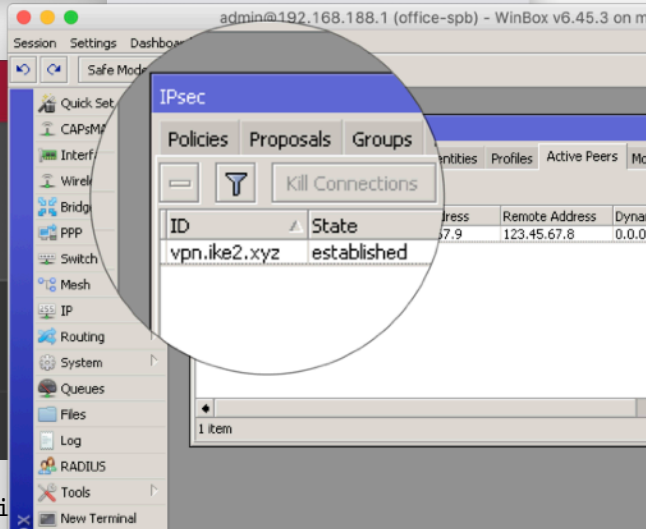
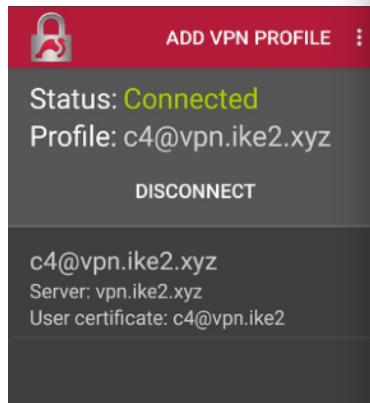
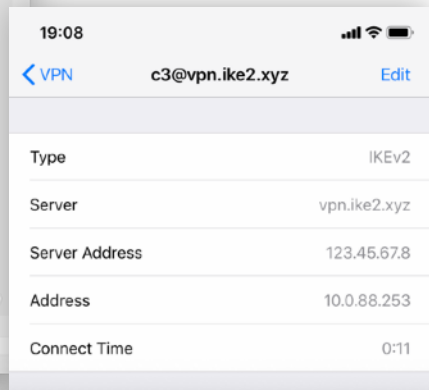
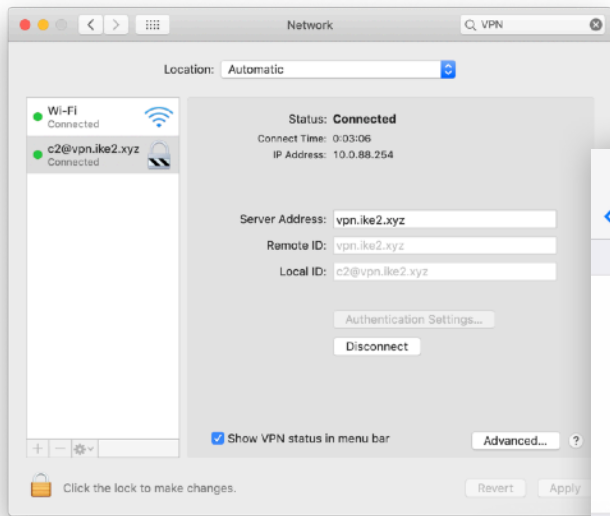
Дополнительно

Дополнительные параметры TCP/IP

- Использовать основной шлюз

Подключение non-Windows

MacOS
iOS
Android
RouterOS



Apple MacOS

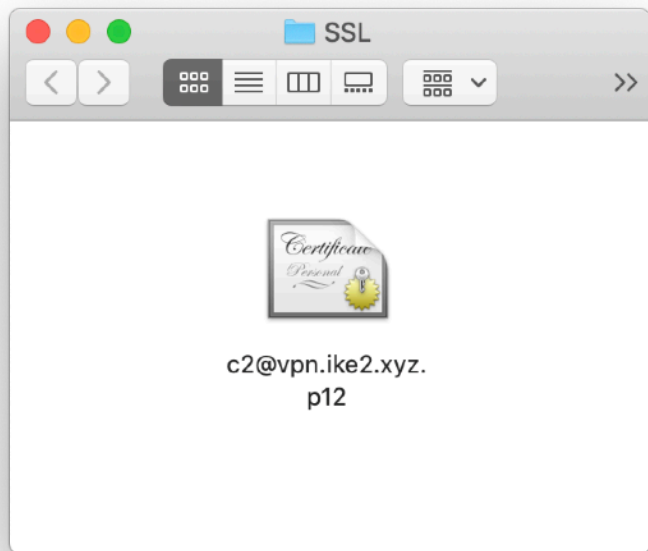
≥ 10.11 El Capitan

План действий

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

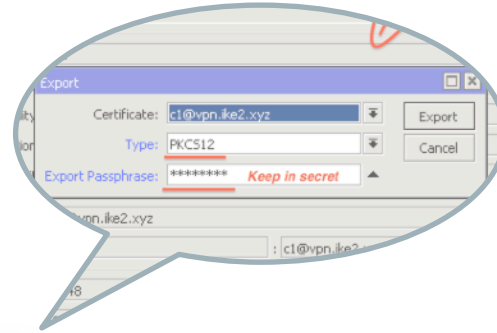
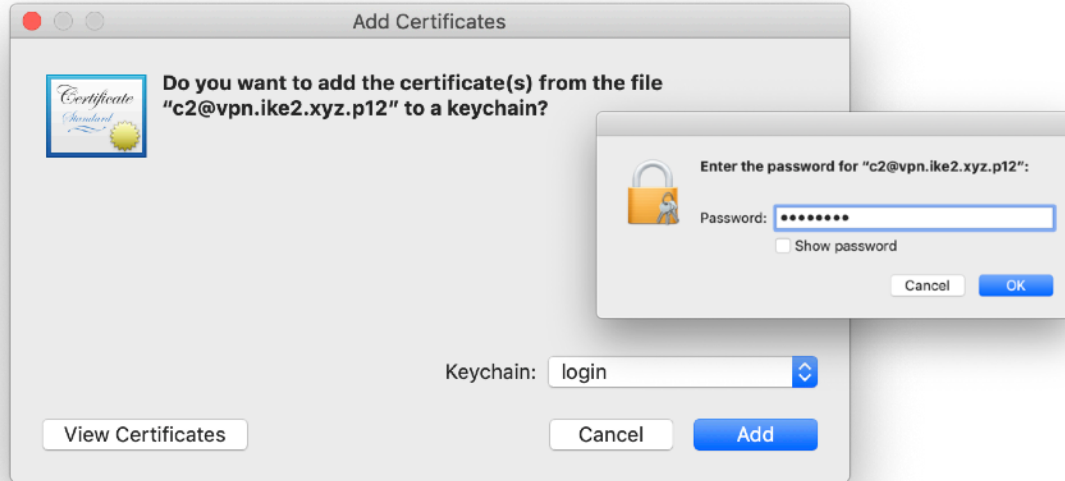


MacOS: Импорт SSL сертификатов



Скачать .p12 сертификат

MacOS: Импорт SSL сертификатов



Keychain:
login (default)

→ Add

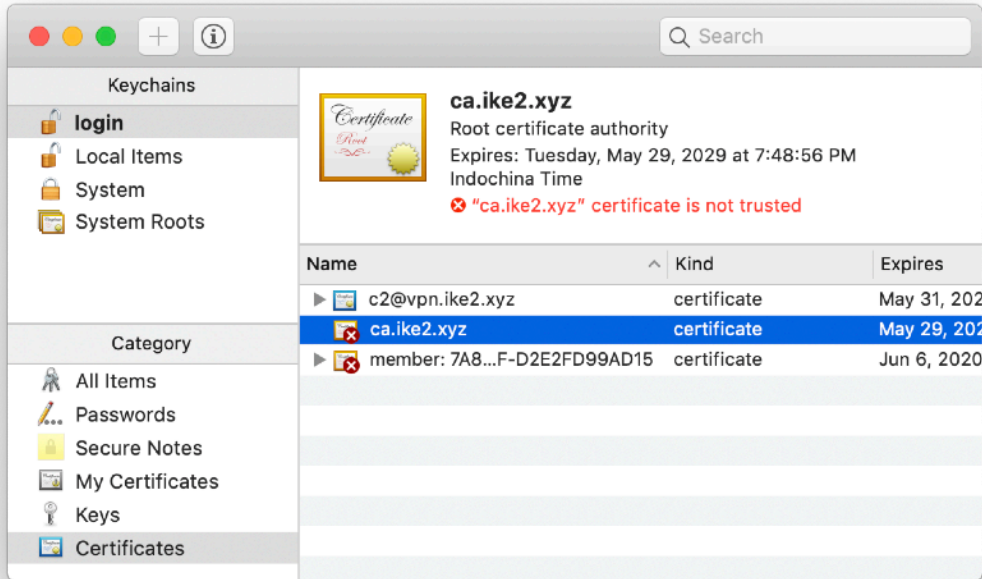
Type your
SSL certificate password

→ OK

MacOS: Управление импортированными SSL сертификатами



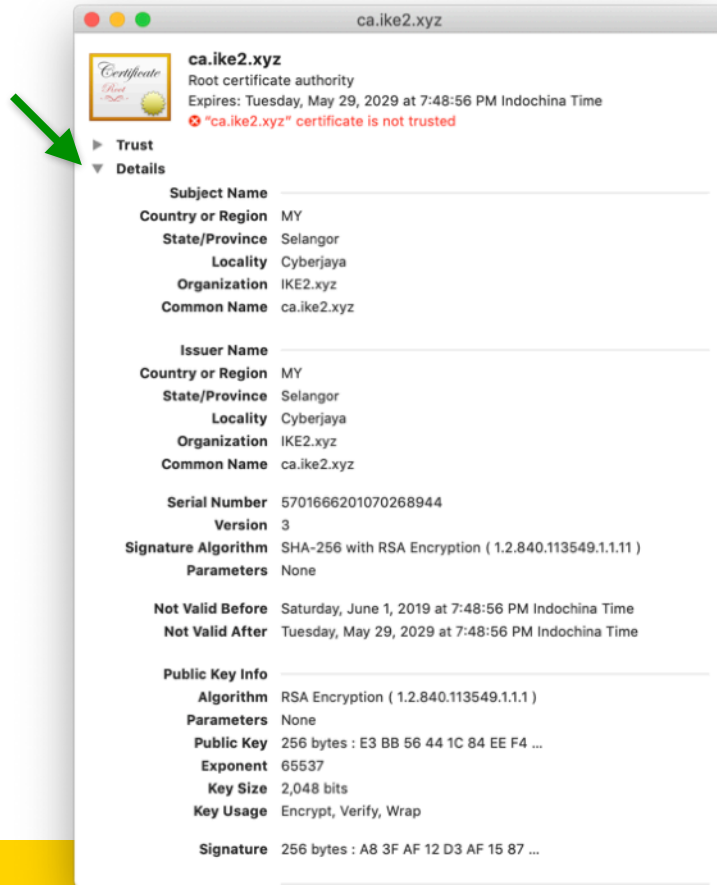
Keychain access



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

The image shows two overlapping windows. On the left is the MacOS Keychain Access window for a certificate from 'ca.ike2.xyz'. On the right is the Mikrotik WinBox interface showing the configuration for the same certificate. Green boxes and arrows highlight the fingerprint fields in both windows to show they match.

MacOS Keychain Access - Public Key Info

- Algorithm: RSA Encryption (1.2.840.113549.1.1.1)
- 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 ...

MacOS Keychain Access - Certificate Authority

- 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: Digital Signature, Key Encipherment, Data Encipherment, Key Cert Sign, CRL Sign
- Extension: Subject Key Identifier (2.5.29.14)
Critical: NO
Key ID: 25 FD 0B D3 3A 6C F8 96 04 A9 FA 19 24 A9 E3 05 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

MacOS Keychain Access - 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 B9 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

WinBox Certificate Configuration

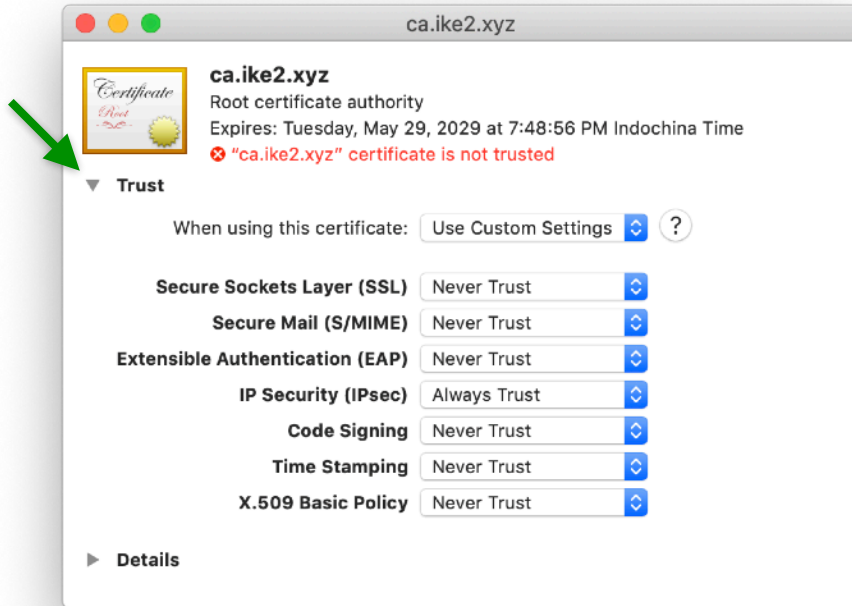
- Serial Number: [Fingerprint: b57c af68 13b3 52a0 ababa a4e4 2f8c 5694 4875 eedf 630b 93e4 b05c 6d73 3d94 b]
- Req. Fingerprint: [SHA-256: B5 7C AF 68 13 B3 52 A0 AB AB AA 4E 42 F8 C5 69 44 87 57 EE DA F8 30 B9 3E 4B 05 C6 D7 33 D9 4B]

MacOS: Управление импортированными SSL сертификатами

Important



Keychain access

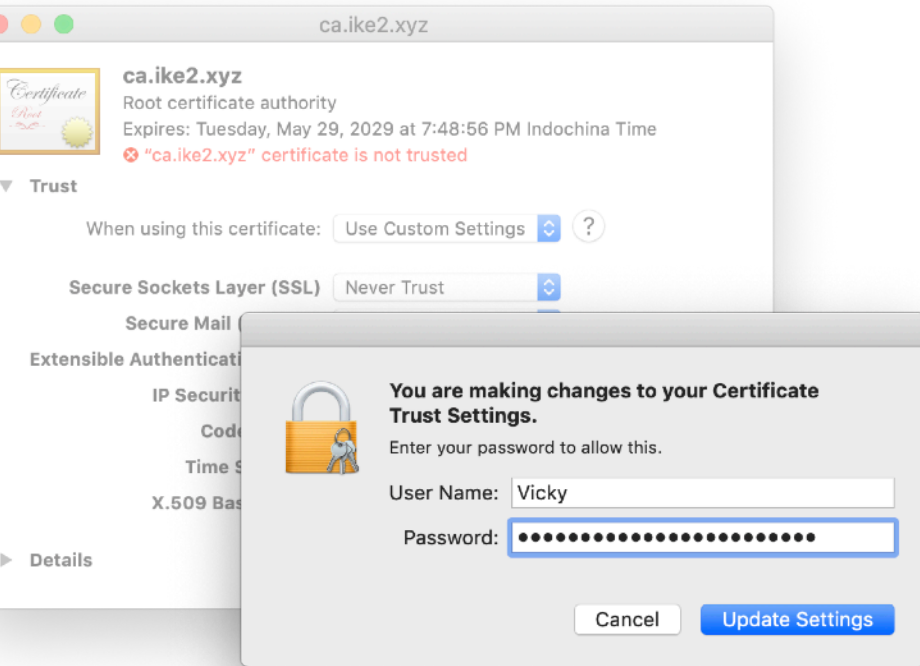


IP Security (IPSec)

Everything else

MacOS: Управление импортированными SSL сертификатами

Important



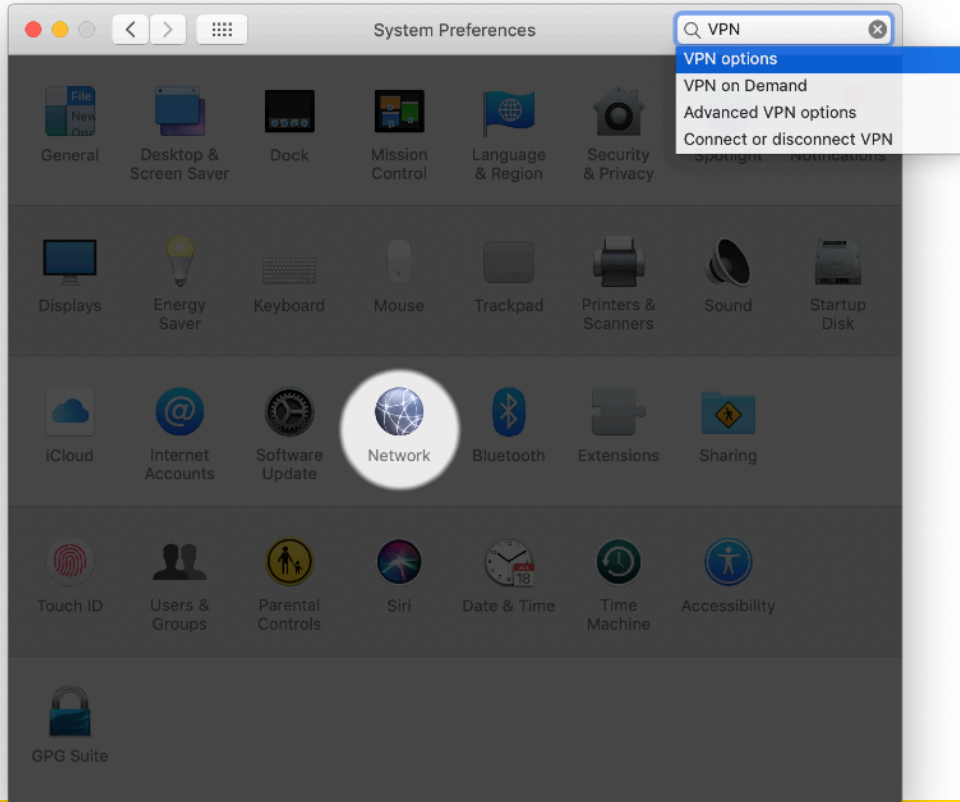
Keychain access

Type your
MacOS password

—> Update settings

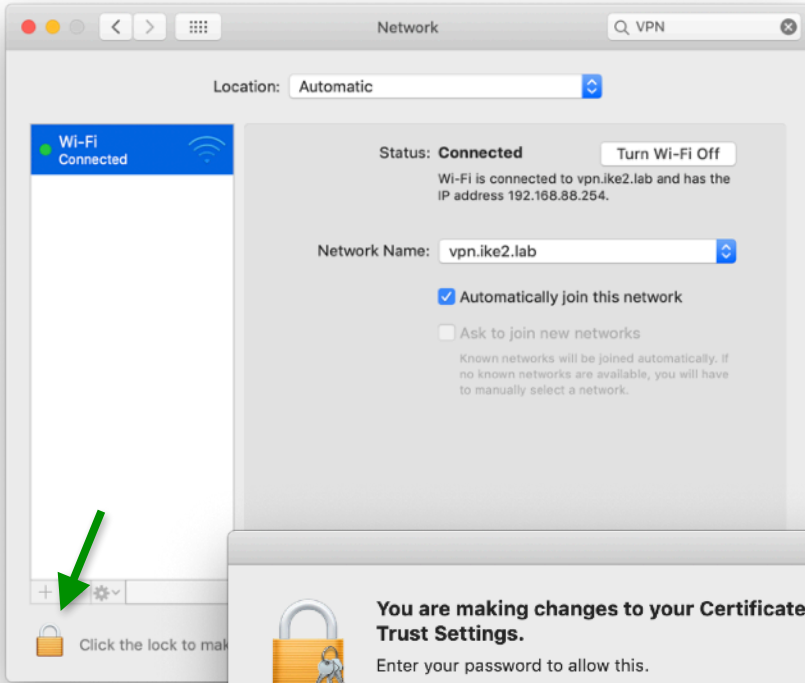
MacOS: Настройка IKEv2 VPN соединения

— — —

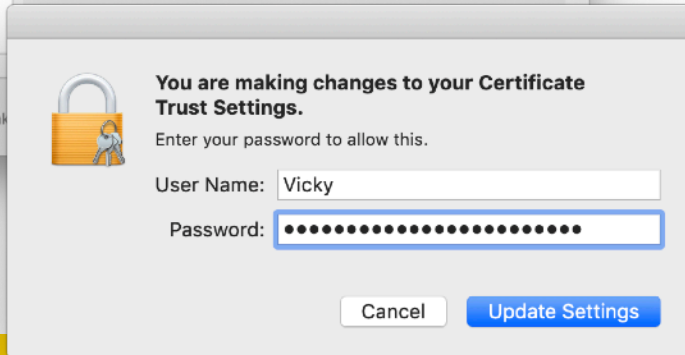


System preferences ->
Network

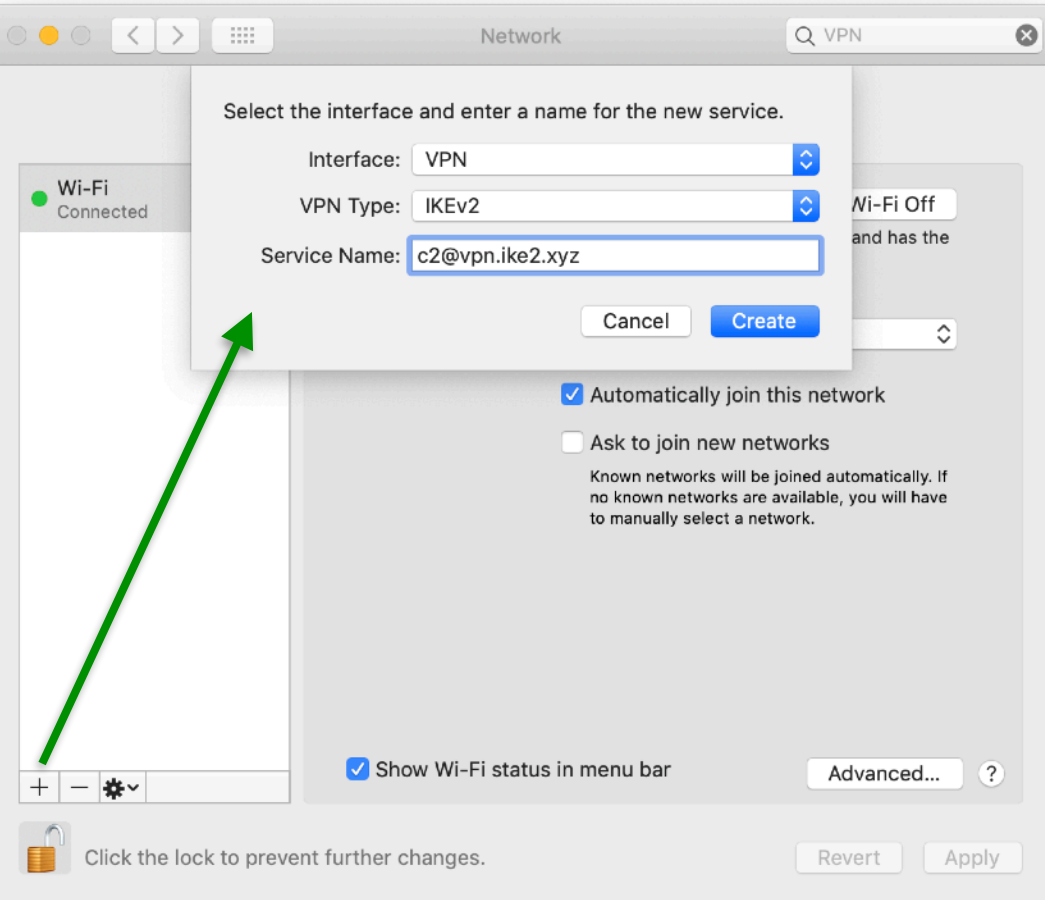
MacOS: Настройка IKEv2 VPN соединения



Unlock to make changes



MacOS: Настройка IKEv2 VPN соединения



Create new connection

Interface:

VPN

VPN Type:

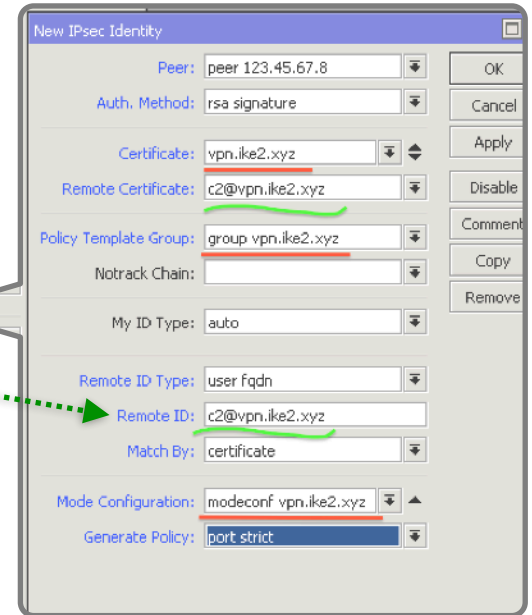
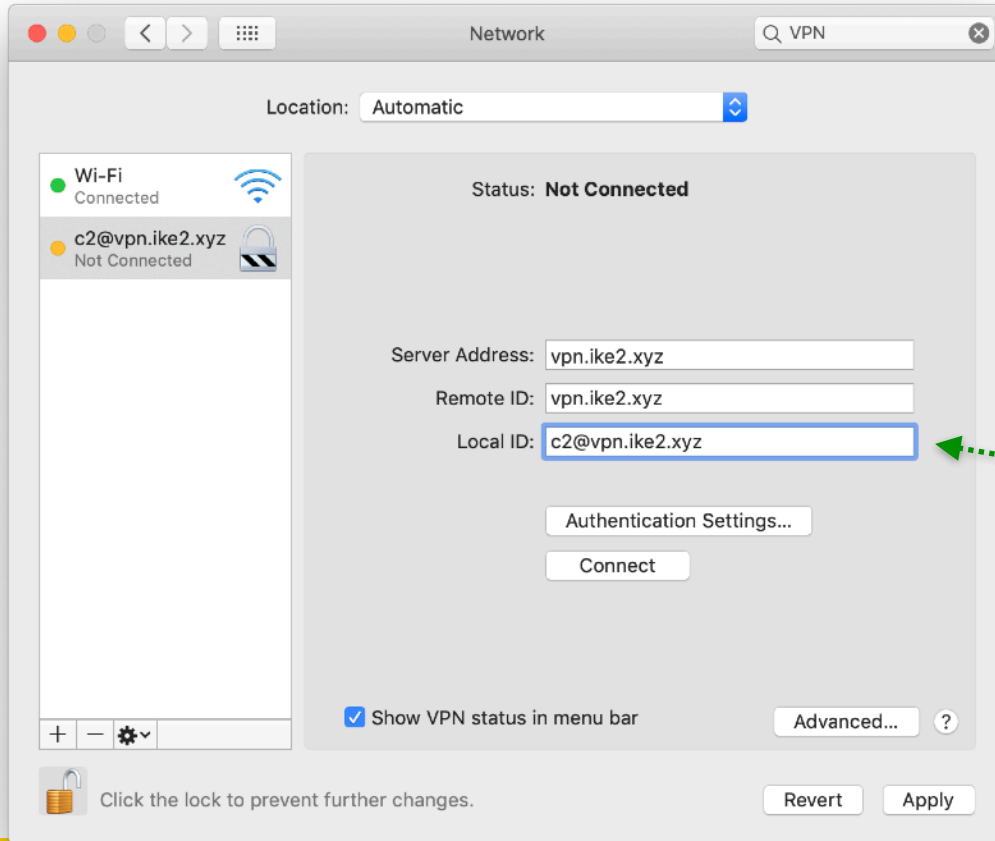
IKEv2

Service name:

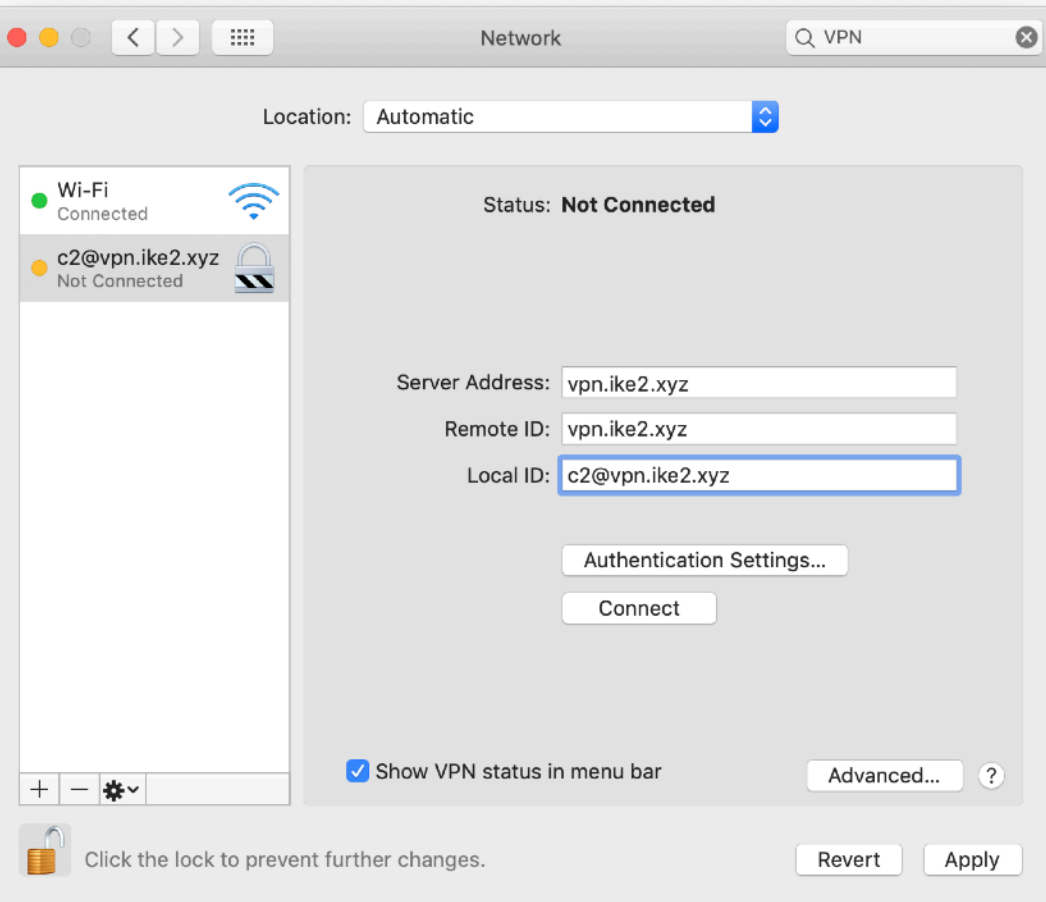
c2@vpn.ike2.xyz

→ **Create**

MacOS: Настройка IKEv2 VPN соединения



MacOS: Настройка IKEv2 VPN соединения



Create new connection

Server Address:

vpn.ike2.xyz

Remote ID:

vpn.ike2.xyz

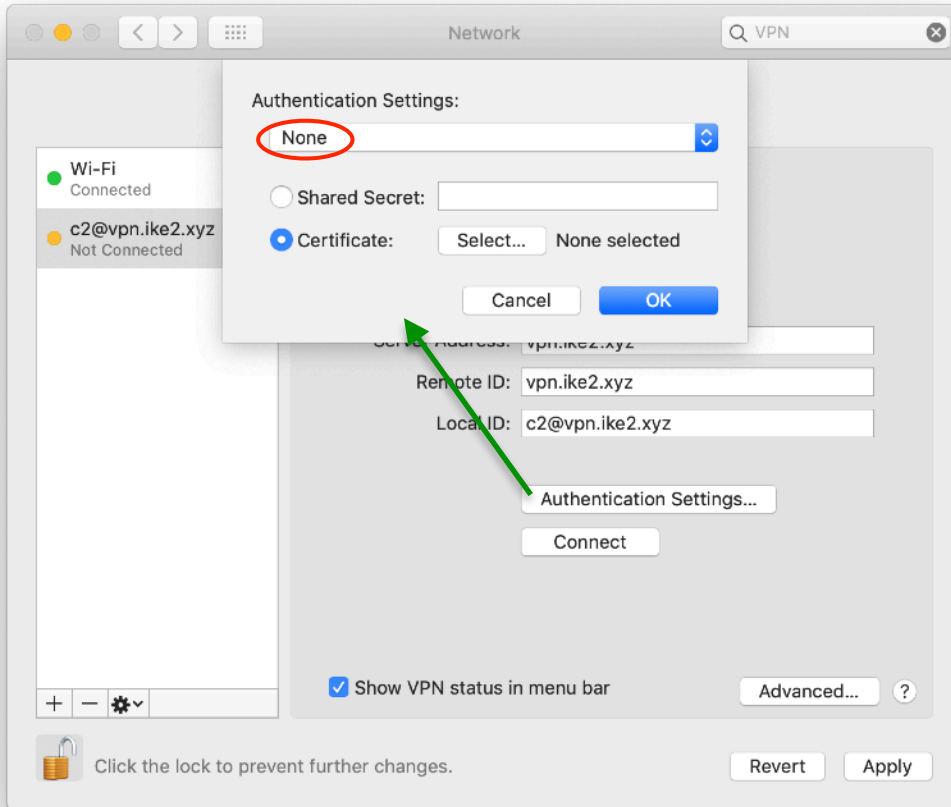
Local ID:

c2@vpn.ike2.xyz

✓ Show VPN status in menu bar

→ **Apply**

MacOS: Настройка IKEv2 VPN соединения



Authentication Settings

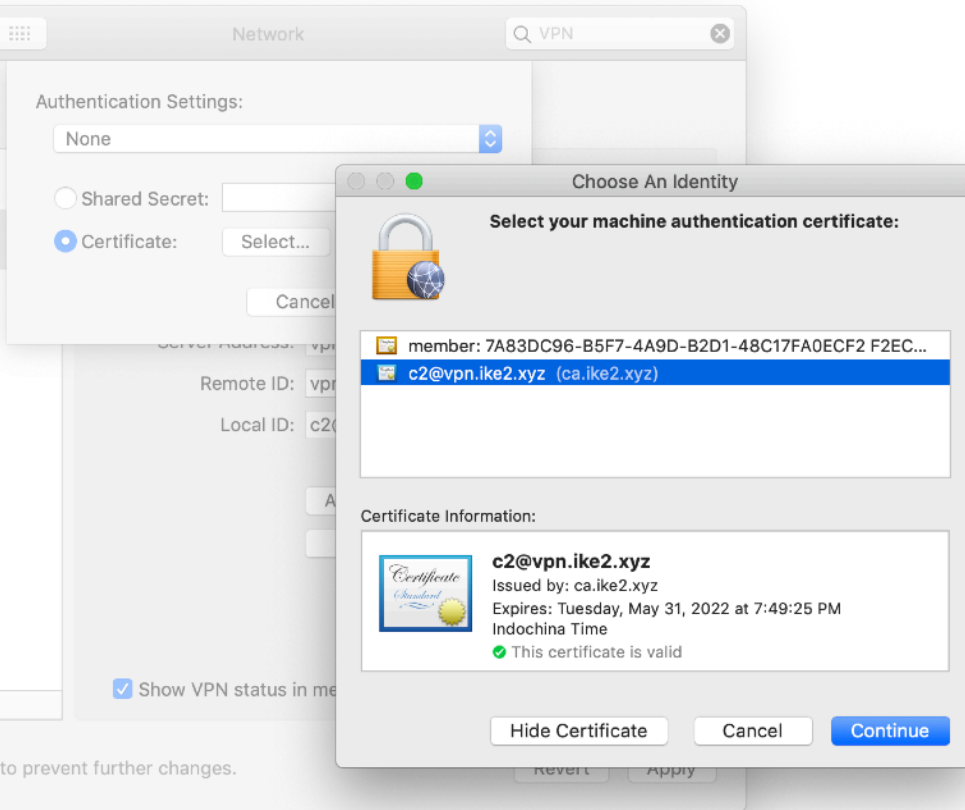
Authentication Settings:

None

Certificate:

→ **Select**

MacOS: Настройка IKEv2 VPN соединения

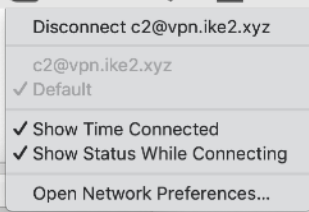
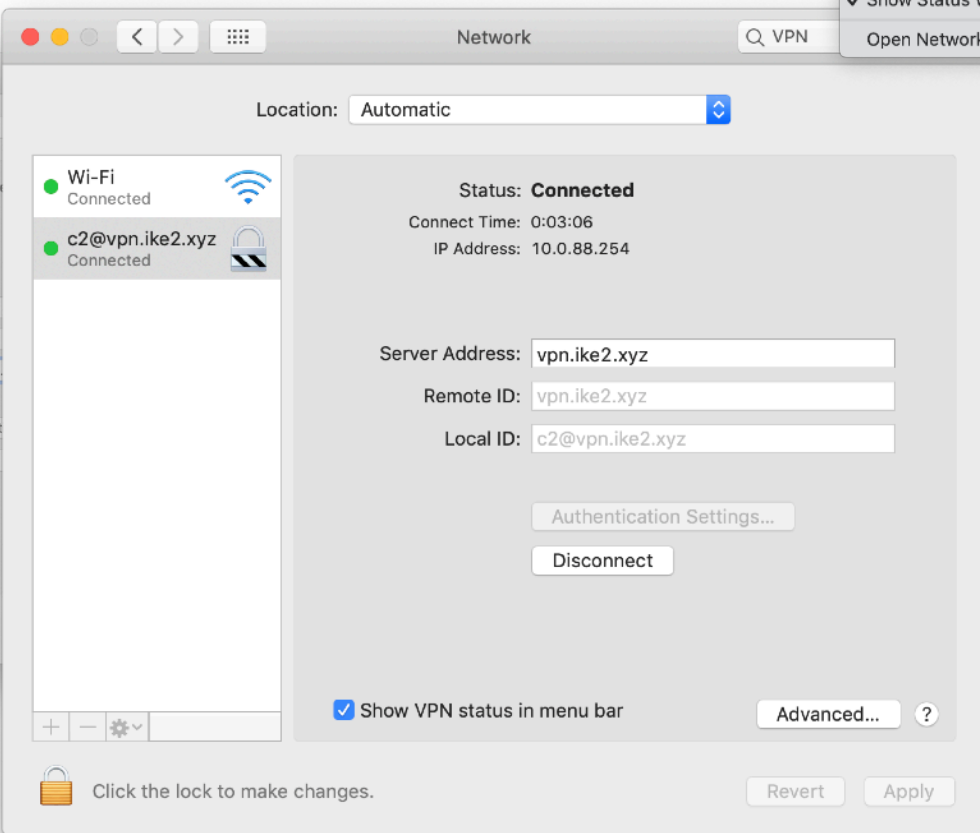
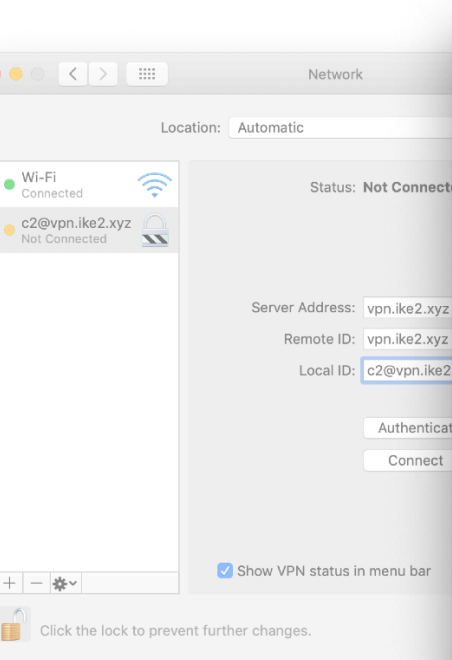



Authentication Settings


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

→ **Continue**

MacOS: Подключение IKEv2 VPN



 *Don't forget to lock settings*

 Click the lock to make changes.

MacOS: Проверка IKEv2 VPN маршрутов

Disconnect c2@vpn.ike2.xyz

c2@vpn.ike2.xyz

- ✓ Default
- ✓ Show Time Connected
- ✓ Show Status While Connecting

Open Network Preferences...

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

Session: 192.168.88.1 CPU: 1%

IPsec

Name	Resp...	Address Pool	Address	Address Pr...	Split Include	System ...
modeconf vpn.ike...	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

```

➔ ~ 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

Disconnect c2@vpn.ike2.xyz

c2@vpn.ike2.xyz
 Default

Show Time Connected
 Show Status While Connecting

Open Network Preferences...

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

Dashboard

Mode Session: 192.168.88.1 CPU: 3%

IPsec

Peers Identities Profiles Remote Peers Mode Configs Installed SAs Keys ...

Name	Resp...	Address Pool	Address	Address Pr...	Split Include
modeconf vpn.ike...	yes	pool vpn.ike2.xyz		32	0.0.0.0/0
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: 0.0.0.0/0

Static DNS: 10.0.88.1

```

~ 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.          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
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
2.          .62         link#23      UHW3I       0           1 ipsec0
2.          100        link#23      UHW3I       0           1 ipsec0
2.          95          link#23      UHW3I       0           1 ipsec0
    
```

Apple iOS

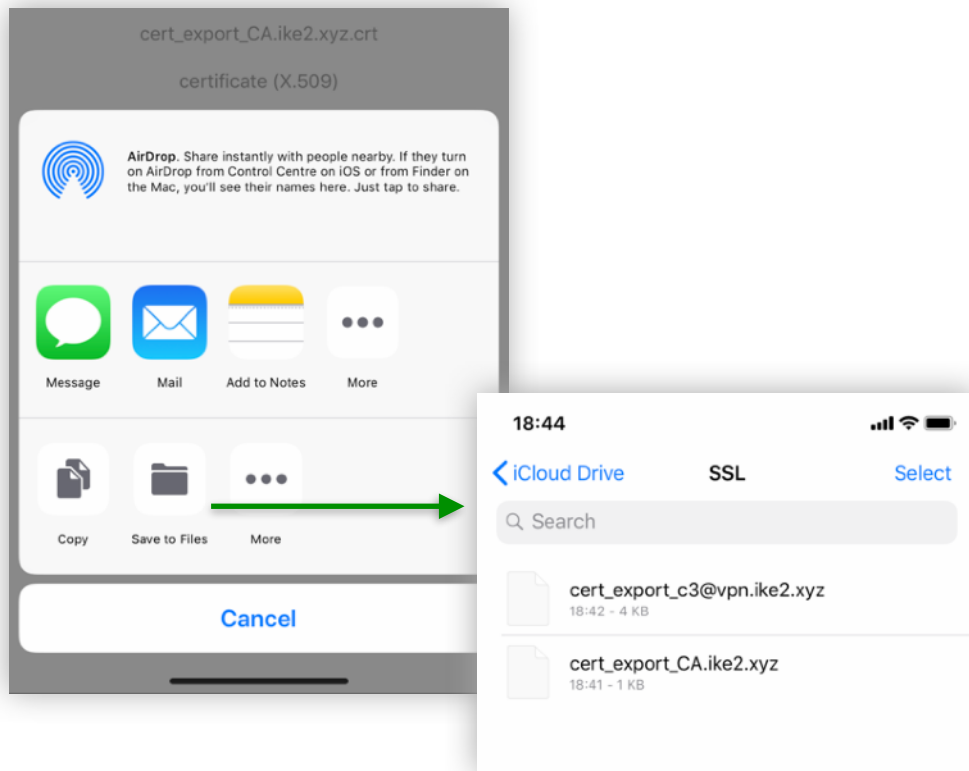
≥ версия 9

План действий

1. Импорт SSL сертификатов
2. Настройка IKEv2 VPN соединения



iOS: Загрузка SSL сертификатов

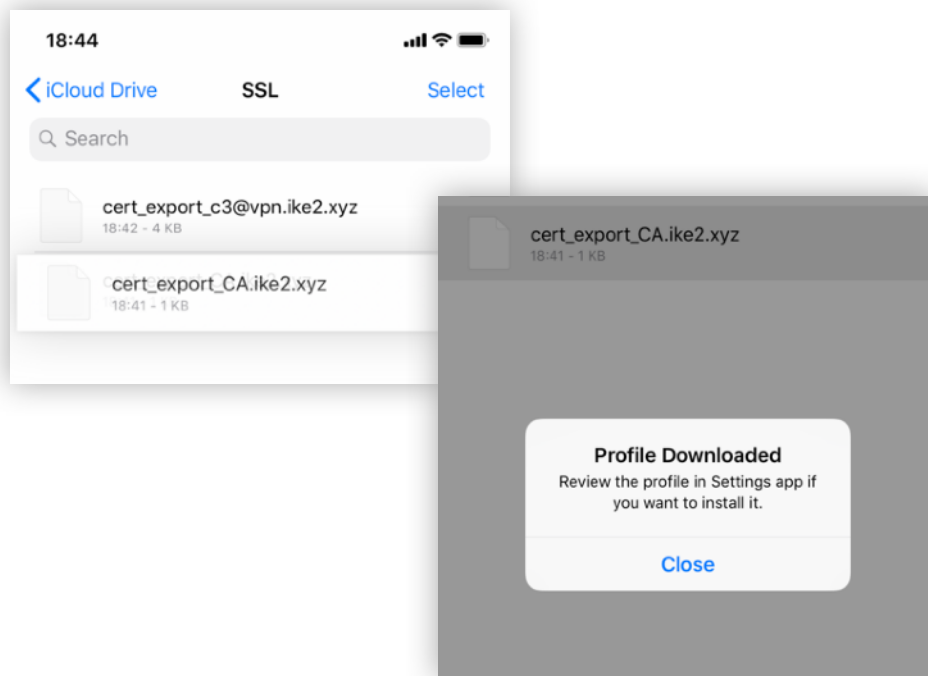


Download **CA** certificate .crt

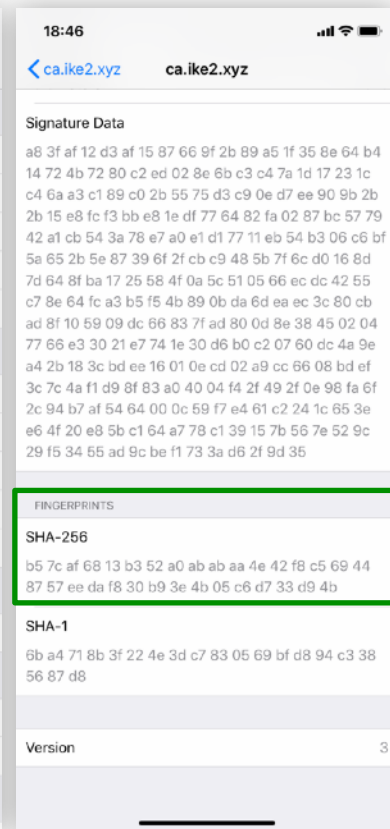
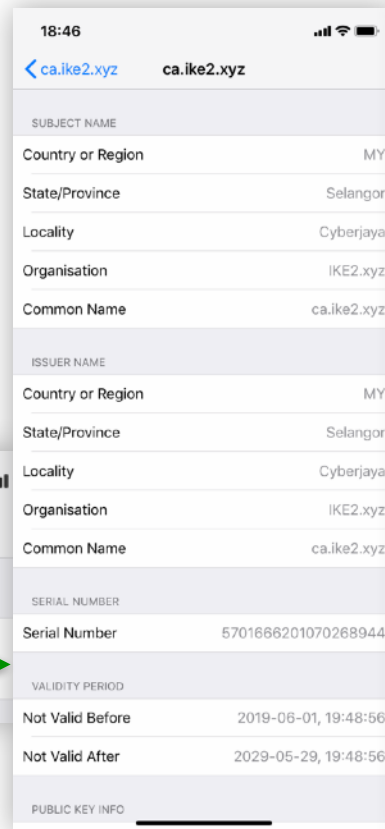
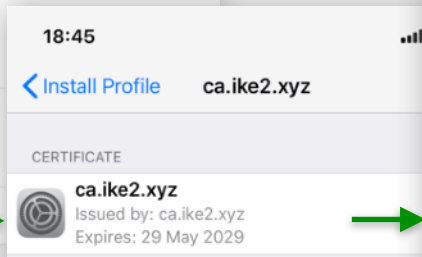
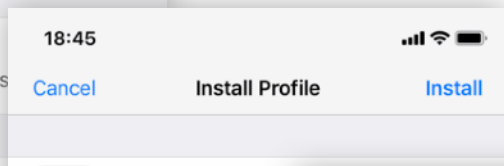
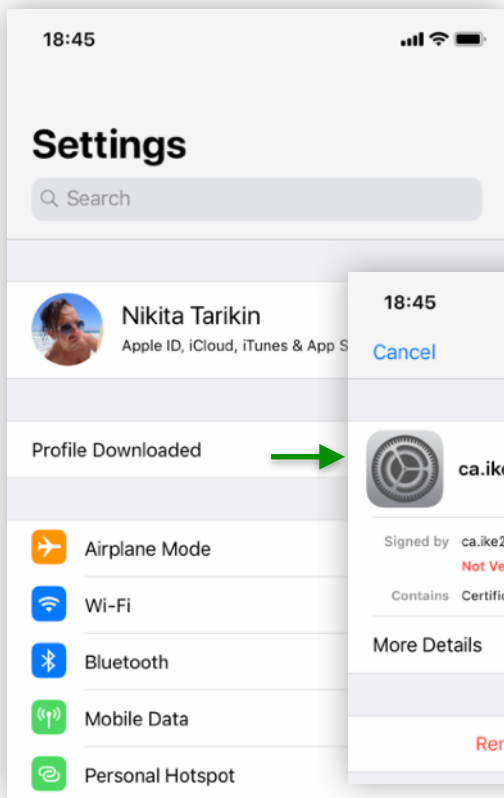
Download **client** certificate .p12

iOS: Импорт SSL сертификата авторитета CA

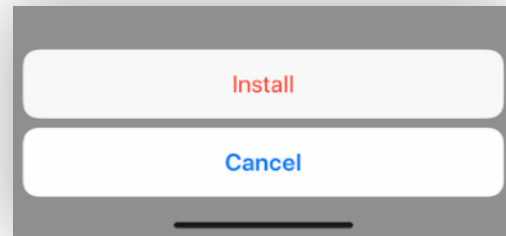
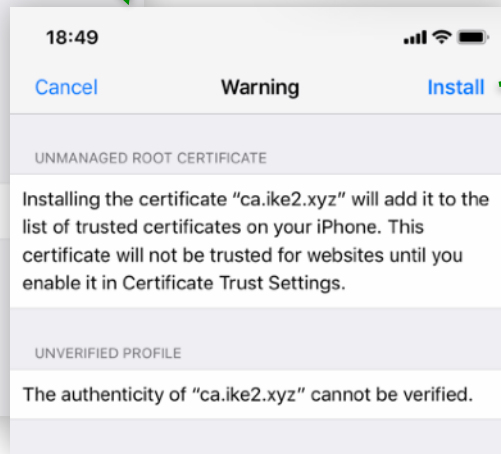
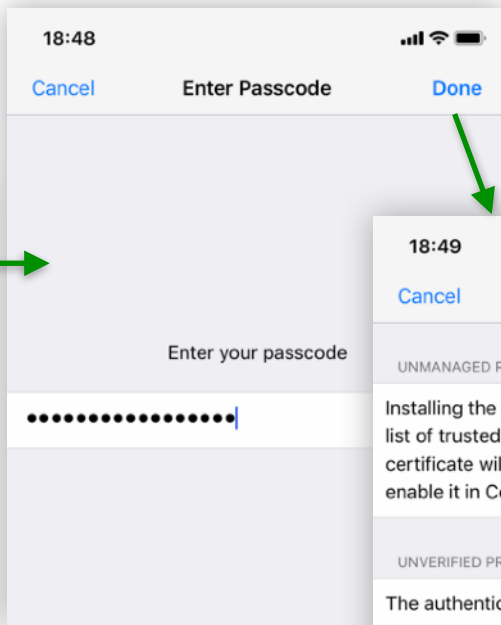
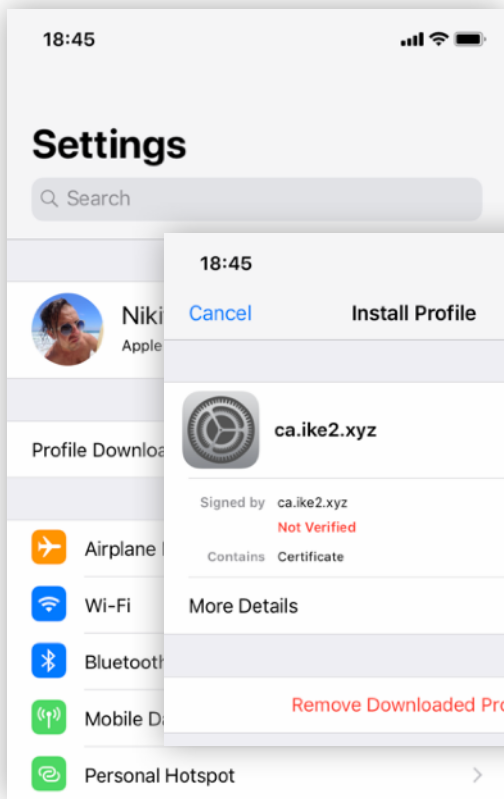
— — —



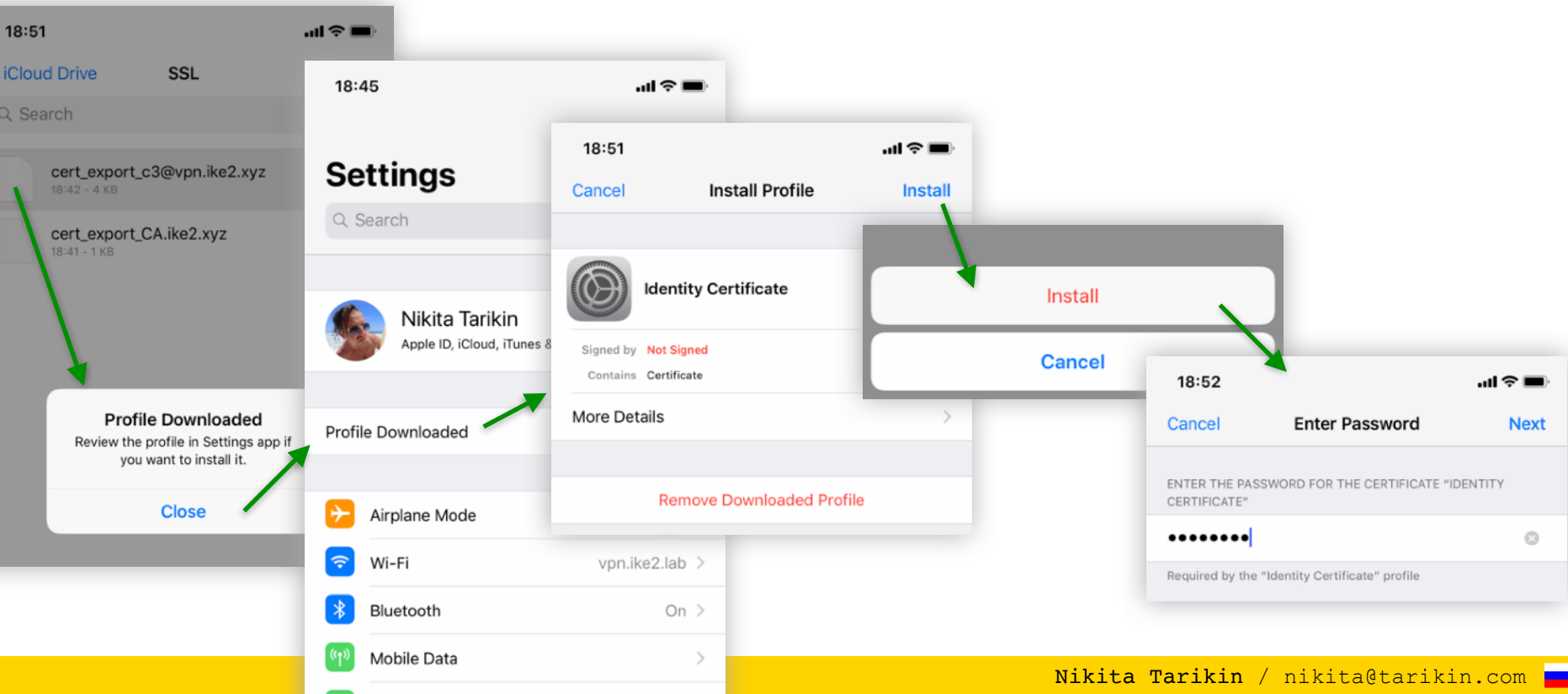
iOS: Импорт SSL сертификата авторитета CA



iOS: Импорт SSL сертификата авторитета CA



iOS: Импорт SSL сертификата клиента

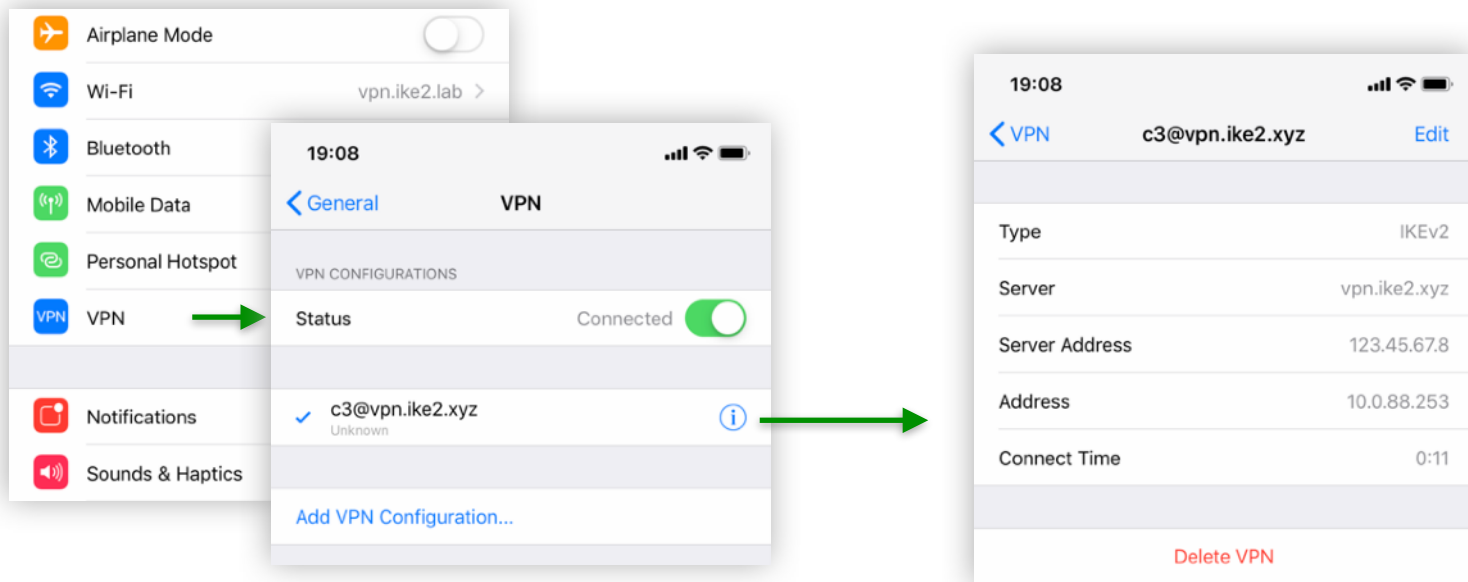


iOS: Настройка IKEv2 VPN соединения

The image illustrates the process of configuring an IKEv2 VPN on an iPhone. It is divided into three main sections:

- Settings App:** Shows the path from the main Settings menu to the VPN section. Green arrows indicate the navigation from 'Settings' to 'VPN' and then to 'Add VPN Configuration...'. The time shown is 18:55.
- Add Configuration Screen:** Shows the 'Add Configuration' screen with the time 19:08. The configuration type is 'IKEv2'. The 'Local ID' is set to 'c3@vpn.ike2.xyz'. The 'User Authentication' is set to 'None', which is circled in red. The 'Use Certificate' toggle is turned on. The 'Certificate' is set to 'c3@vpn.ike2.xyz'. At the bottom, there are 'Off', 'Manual', and 'Auto' options.
- New IPsec Identity Screen:** A detailed view of the IPsec identity configuration. The 'Peer' is 'peer 123.45.67.8'. The 'Auth. Method' is 'rsa signature'. The 'Certificate' is 'vpn.ike2.xyz'. The 'Remote Certificate' is 'c2@vpn.ike2.xyz'. The 'Policy Template Group' is 'group vpn.ike2.xyz'. The 'Remote ID Type' is 'user fqdn'. The 'Remote ID' is 'c2@vpn.ike2.xyz'. The 'Match By' is 'certificate'. The 'Mode Configuration' is 'modeconf vpn.ike2.xyz'. The 'Generate Policy' is 'port strict'. A green dashed arrow points from the 'Remote ID' field in this screen to the 'Local ID' field in the 'Add Configuration' screen.

iOS: Подключение IKEv2 VPN



Android

версия 9 <

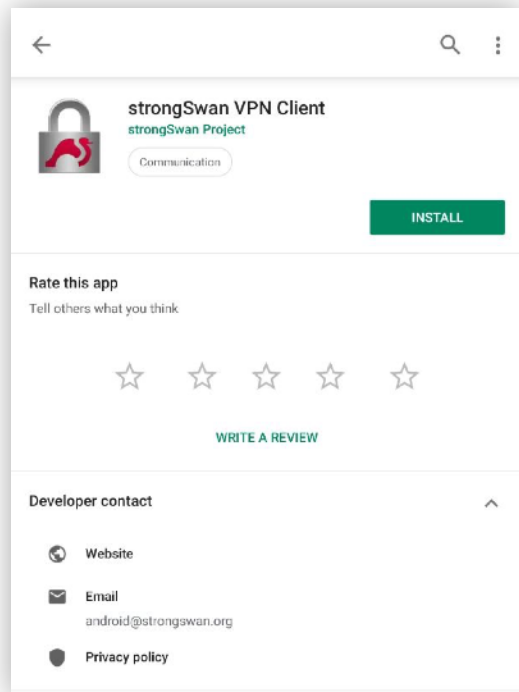
План действий

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



Android: Установка StrongSwan

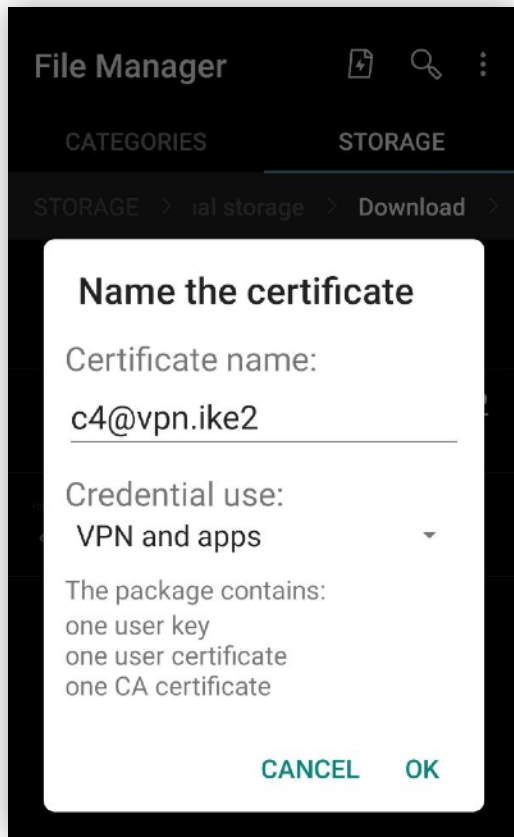
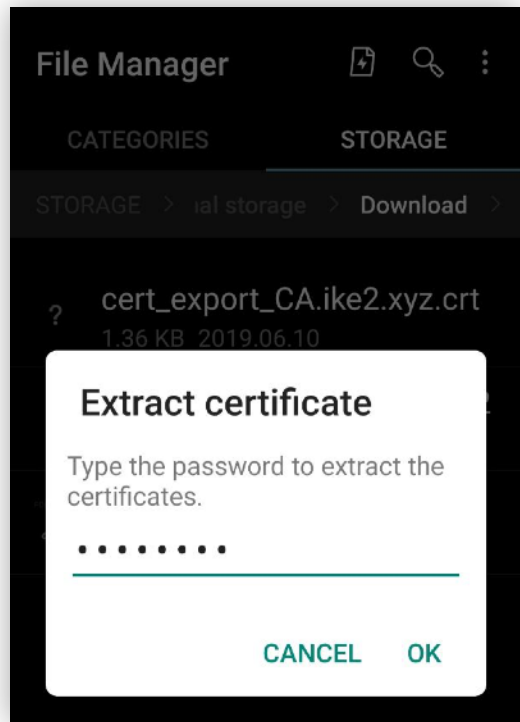
— — —



Найти и установить **StrongSwan**

через Google Play

Android: Импорт SSL сертификатов



Download and install

user certificate .p12

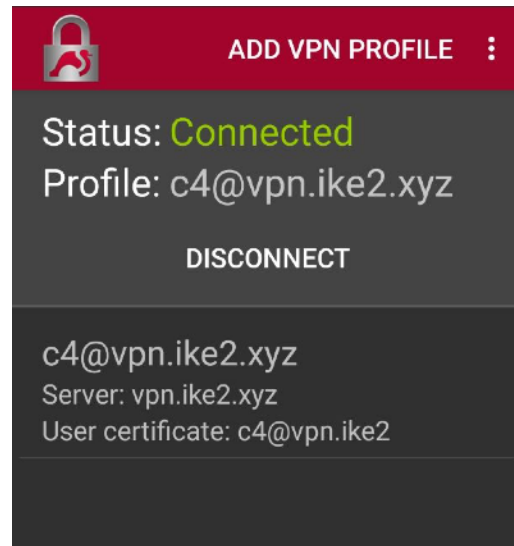
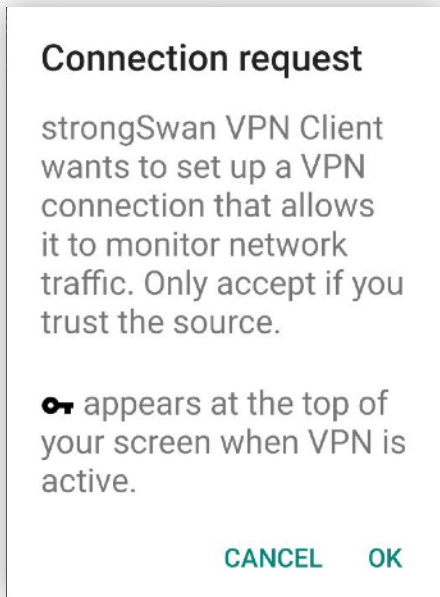
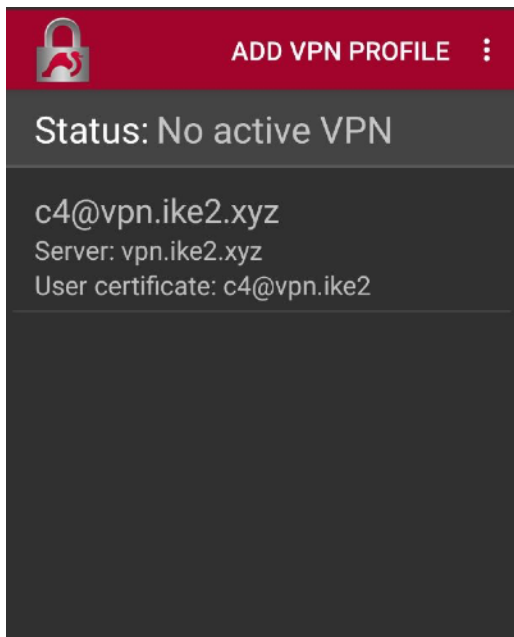
Android: Настройка IKEv2 VPN соединения

ADD VPN PROFILE :
Status: No active VPN
No VPN profiles.

Add VPN pro... SAVE CANCEL
Server
vpn.ike2.xyz
VPN Type
IKEv2 Certificate
User certificate
c4@vpn.ike2
CN=c4@vpn.ike2.xyz
User identity
Default (CN=c4@vpn.ike2.xy..
CA certificate
 Select automatically
Profile name (optional)
c4@vpn.ike2.xyz
Defaults to "vpn.ike2.xyz"
 Show advanced settings

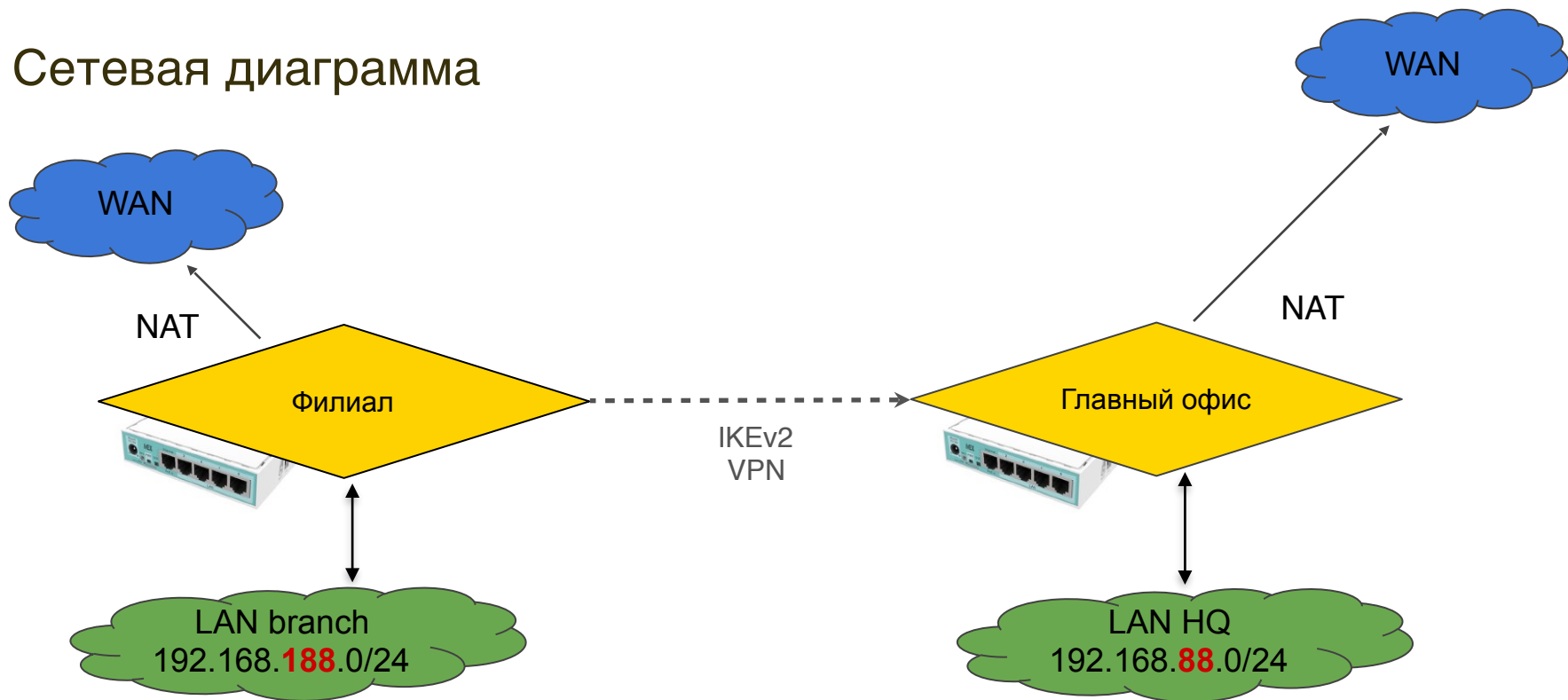
Choose certificate
The app strongSwan VPN Client has requested a certificate. Choosing a certificate will let the app use this identity with servers now and in the future.
 c4@vpn.ike2
CN=c4@vpn.ike2.xyz
+ Install certificate
DENY SELECT

Android: Подключение IKEv2 VPN

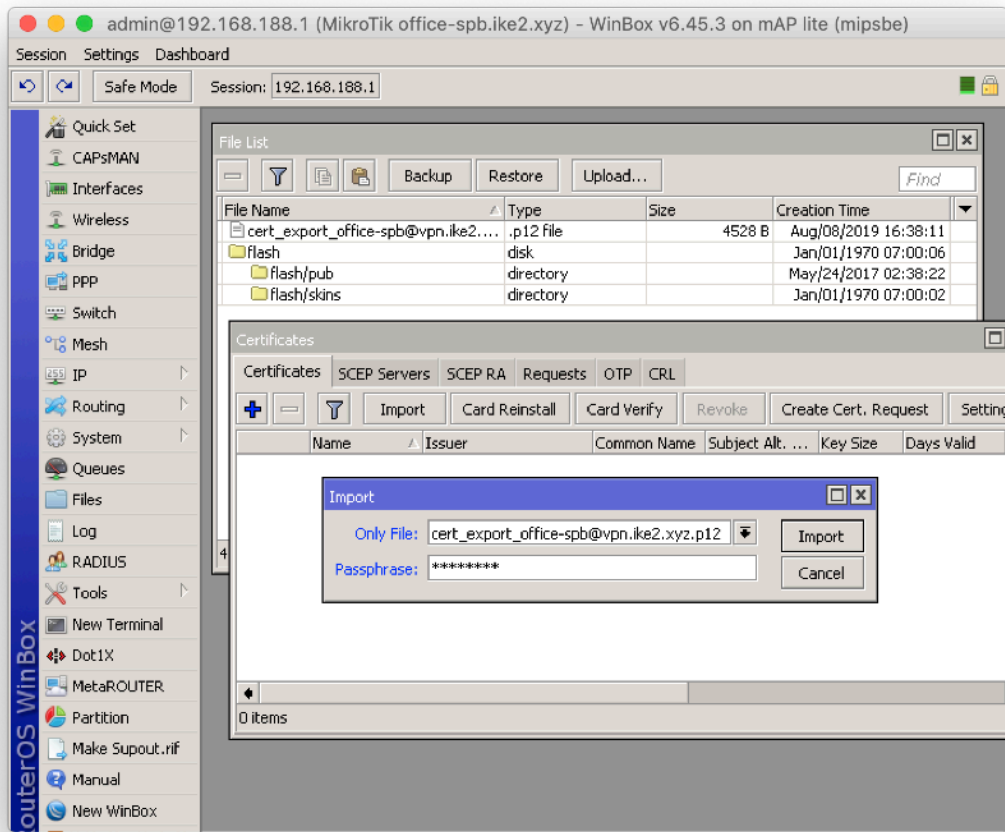


Подключение RouterOS

Сетевая диаграмма



Загрузка и установка клиентского SSL сертификата



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



Переименовываем установленные SSL сертификаты

admin@192.168.188.1 (MikroTik office-spb.ike2.xyz) - WinBox v6.45.3

File List

File Name	Type	Size	Creation Time
cert_export_office-spb@vpn.ike2....	.p12 file	4528 B	Aug/08/2019 16:38:11
flash	disk		Jan/01/1970 07:00:06
flash/pub	directory		May/24/2017 02:38:22
flash/skins	directory		Jan/01/1970 07:00:02

Certificates

Name	Issuer	Common Name
KT	C=RU,ST=Moscow O...	office-spb@...
AT	C=RU,ST=Moscow O...	ca.ike2.xyz

Import

Only File: cert_export_office-spb@vpn.ike2.xyz.p12

Passphrase: *****

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

Session Settings Dashboard

Safe Mode Session: 192.168.188.1

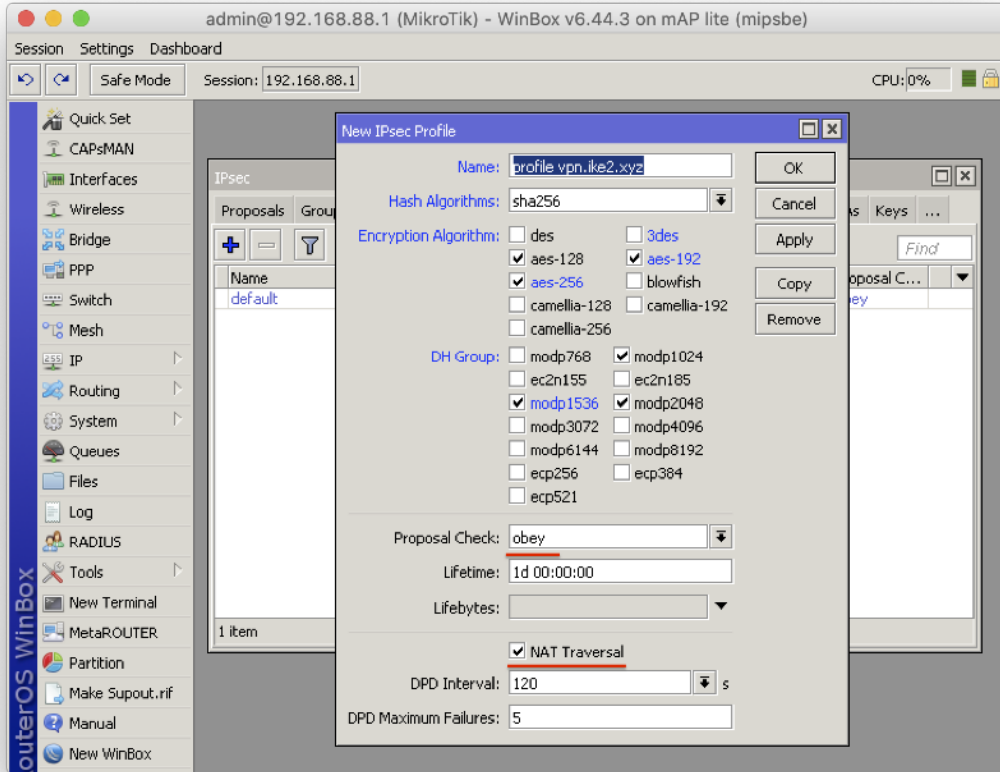
File List

File Name	Type	Size	Creation Time
cert_export_office-spb@vpn.ike2....	.p12 file	4528 B	Aug/08/2019 16:38:11
flash	disk		Jan/01/1970 07:00:06
flash/pub	directory		May/24/2017 02:38:22
flash/skins	directory		Jan/01/1970 07:00:02

Certificates

Name	Issuer	Common Name	Subject Alt. ...	Key Si...
AT	ca.ike2.xyz	C=RU,ST=Moscow O...	DNS:ca.ike2...	4096
KT	office-spb@vpn.ike2.xyz	C=RU,ST=Moscow O...	Email:office-...	2048

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)

The screenshot shows the Mikrotik WinBox interface. The main window is titled "admin@192.168.188.1 (MikroTik office-spb.ike2.xyz) - WinBox v6.45.3 on mAP lite (mipsbe)". The "IPsec" tab is active, and the "Peers" sub-tab is selected. A "New IPsec Peer" dialog box is open, showing the following configuration:

- Name: peer vpn.ike2.xyz
- Address: vpn.ike2.xyz
- Port: (empty)
- Local Address: (empty)
- Profile: profile vpn.ike2.xyz
- Exchange Mode: IKE2
- Passive
- Send INITIAL_CONTACT

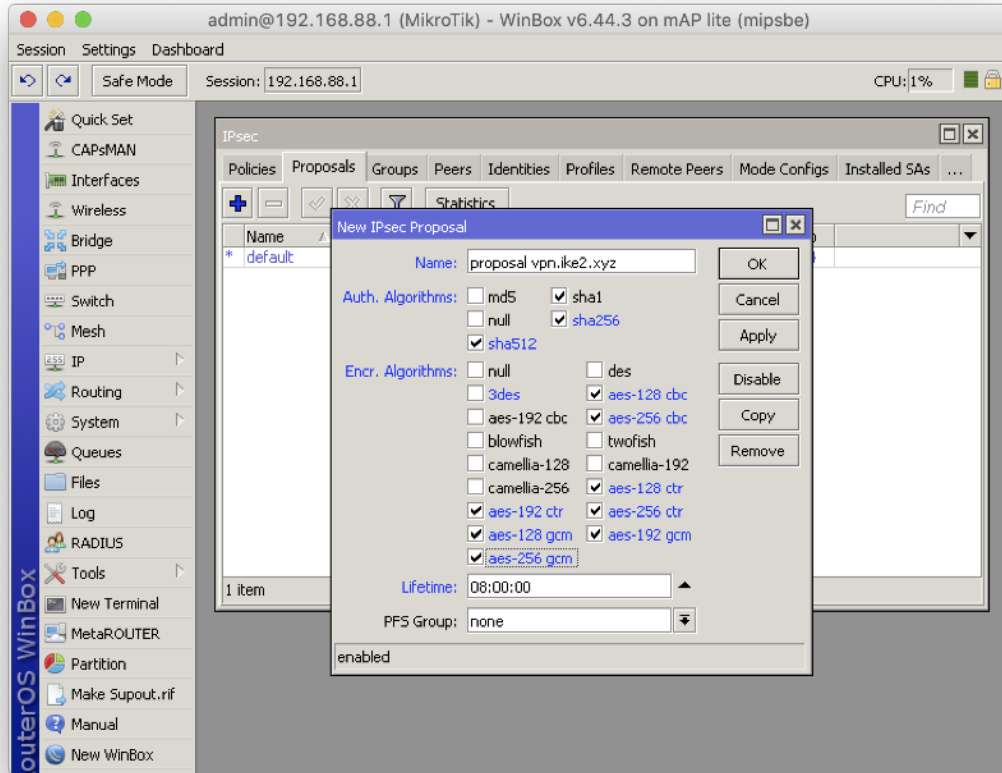
The dialog box has buttons for OK, Cancel, Apply, Disable, Comment, Copy, and Remove. The main window shows a table with columns: #, Name, Address, Local Address, Profile, Exchange... The table is currently empty.

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

блoтrгe=„блoтrгe λбу'ткeς'xλς,,



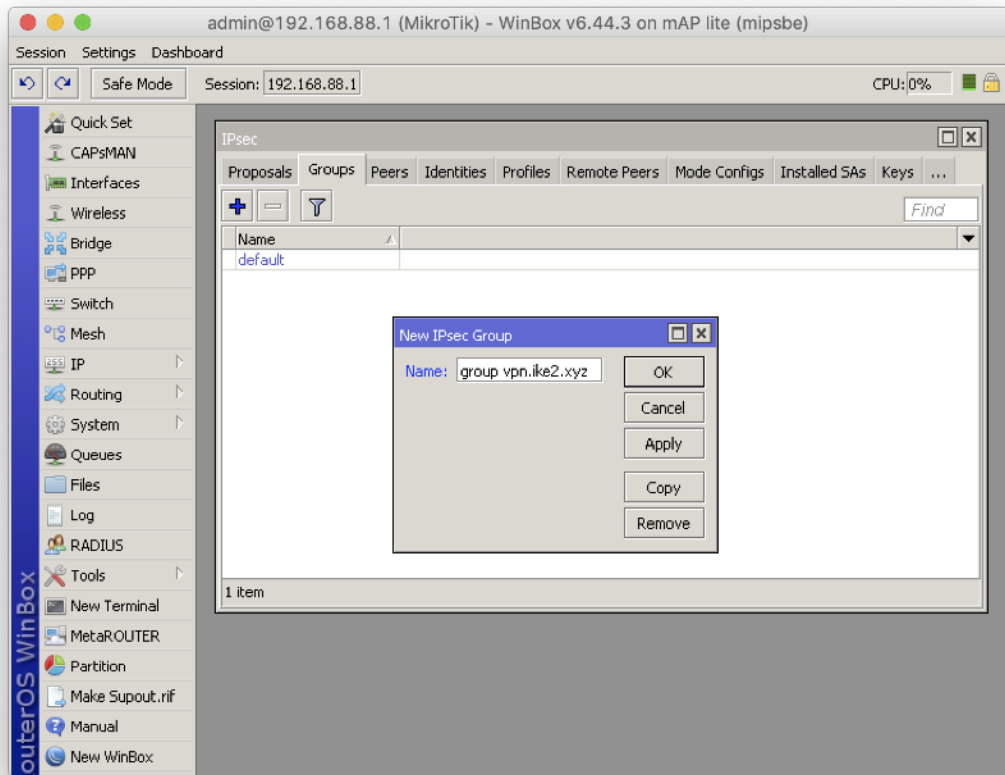
Настройка нового IPsec proposal (фаза 2)



```
/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

admin@192.168.188.1 (MikroTik office-spb.ike2.xyz) - WinBox v6.45.3 on MAP li...

Session Settings Dashboard

Safe Mode Session: 192.168.188.1

Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
Routing
System
Queues
Files
Log
RADIUS
Tools
New Terminal
Dot1X
MetaROUTER
Partition
Make Supout.rif
Manual
New WinBox

IPsec

Policies Proposals Groups Peers Identities Profiles Active Peers ...

#	Peer	Tunnel	Src. Address	Src. P...	Dst. Addr
0	*T		::/0		::/0

New IPsec Policy

General Action Status

Src. Address: 10.0.88.0/24

Src. Port:

Dst. Address: 0.0.0.0/0

Dst. Port:

Protocol: 255 (all)

Template

Group: group vpn.ike2.xyz

enabled Template Active

New IPsec Policy

General Action Status

Action: encrypt

IPsec Protocols: esp

Proposal: proposal vpn.ike2.xyz

enabled Template Active

```
/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

The screenshot shows the WinBox interface for configuring Firewall Address Lists. The main window is titled "Firewall" and has tabs for "Mangle", "Raw", "Service Ports", "Connections", "Address Lists", and "Layer7 Protocols". The "Address Lists" tab is active, showing a table with columns "Name", "Address", "Timeout", and "Creation Time". The table is currently empty, displaying "0 items". A "New Firewall Address List" dialog box is open in the foreground, with the following fields:

- Name: LAN-address-list
- Address: 192.168.188.0/24
- Timeout: (empty)
- Creation Time: (empty)

The dialog box has buttons for "OK", "Cancel", "Apply", "Disable", "Comment", "Copy", and "Remove". The status bar at the bottom of the dialog shows "enabled".

```
/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

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

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

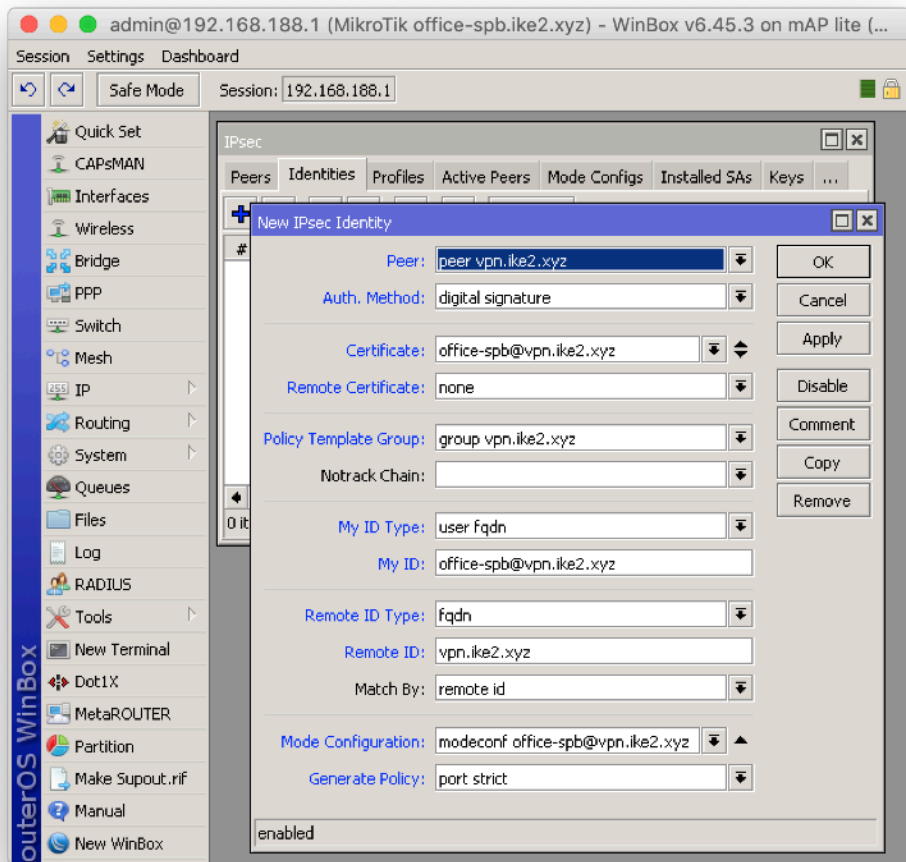
1 item

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

900LG22-(T2)-(GM)-900LG22-(T2)-(GM)



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
```

Ἰq=ἰdqu:λbu·τκς·χλς

ἰlonb=, ἰlonb 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

Active peers
state: **established**

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**

#	Peer	Tunnel	Src. Address	Src. P...	Dst. Address	Dst. P...	Protocol	Action	Level	PH2 State
0	*T		::/0		::/0		255 (all)	encrypt		
1	T		10.0.88.0/24		0.0.0.0/0		255 (all)	encrypt		
2	DA	peer vpn.ike2.xyz	yes	10.0.88.254	0.0.0.0/0		255 (all)	encrypt	unique	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

Генерировано
динамическое
src-nat правило

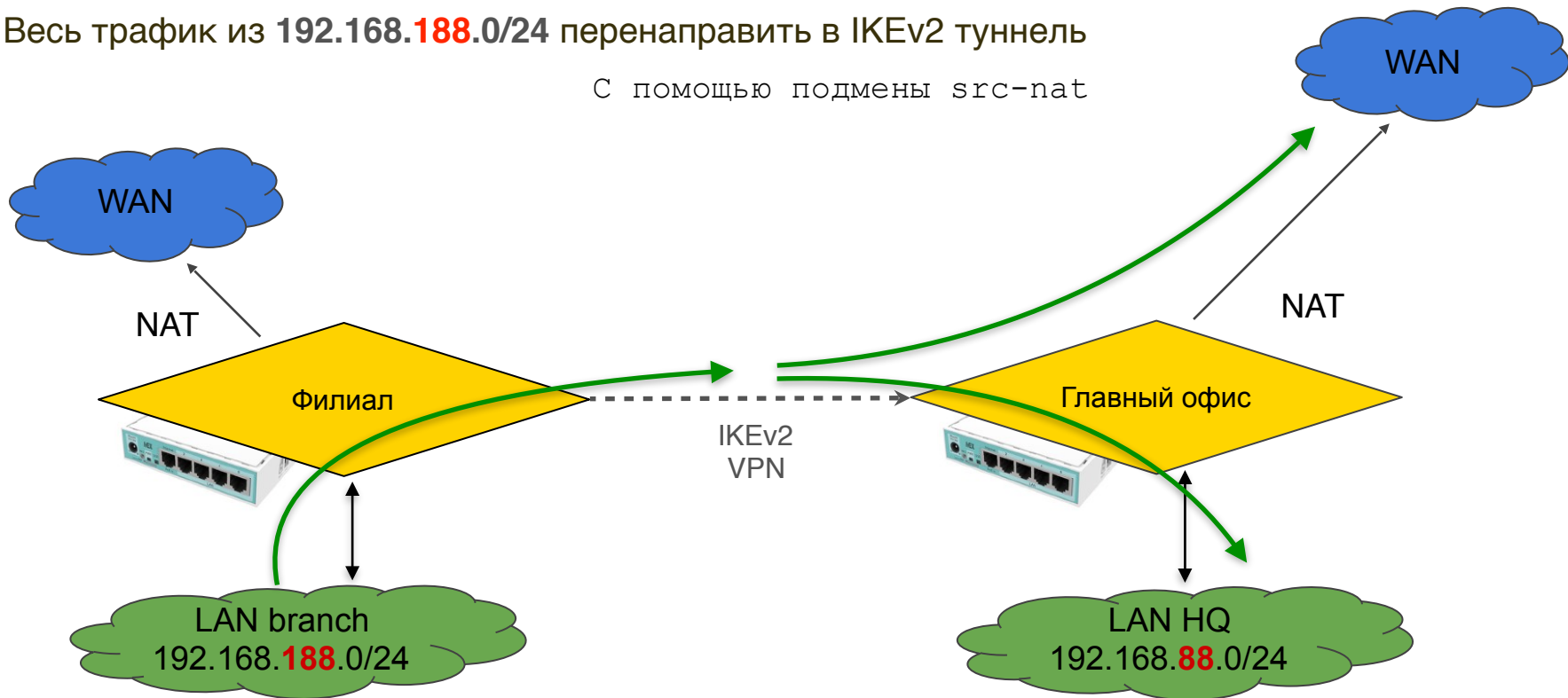
#	Chain	Action	Log	Bytes	Packets	Rate
0	D	ipsec mode-config	no	168 B	4	0 bps
1	D	defconf: masquerade	no	0 B	0	0 bps

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

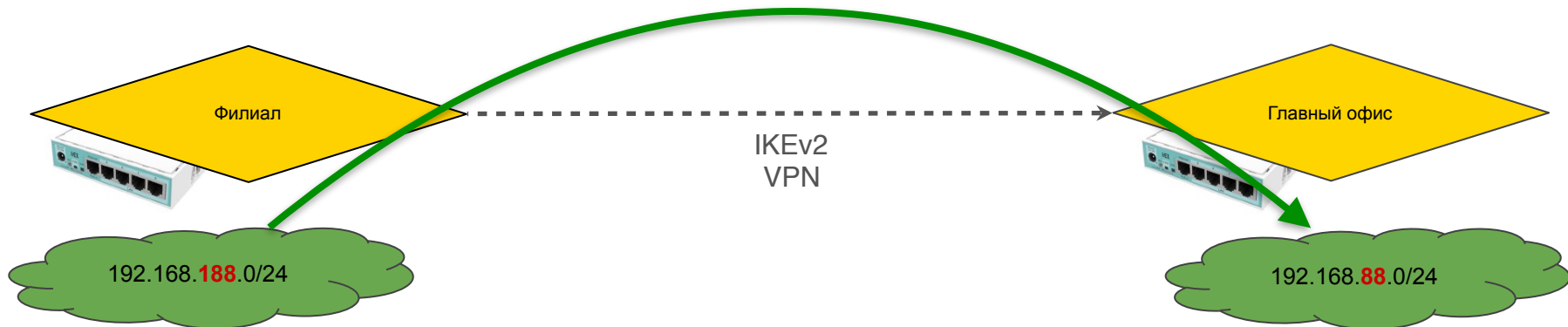
FROM: 192.168.188.0/24

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 lms
 1 192.168.88.1                          56 64 lms
 2 192.168.88.1                          56 64 lms
 3 192.168.88.1                          56 64 lms
 4 192.168.88.1                          56 64 lms
 5 192.168.88.1                          56 64 lms
 6 192.168.88.1                          56 64 lms
 7 192.168.88.1                          56 64 lms
 8 192.168.88.1                          56 64 lms
 9 192.168.88.1                          56 64 lms
10 192.168.88.1                          56 64 lms
11 192.168.88.1                          56 64 lms
12 192.168.88.1                          56 64 lms
13 192.168.88.1                          56 64 lms
  sent=14 received=14 packet-loss=0% min-rtt=lms avg-rtt=lms max-rtt=lms

[admin@office-spb] >
```

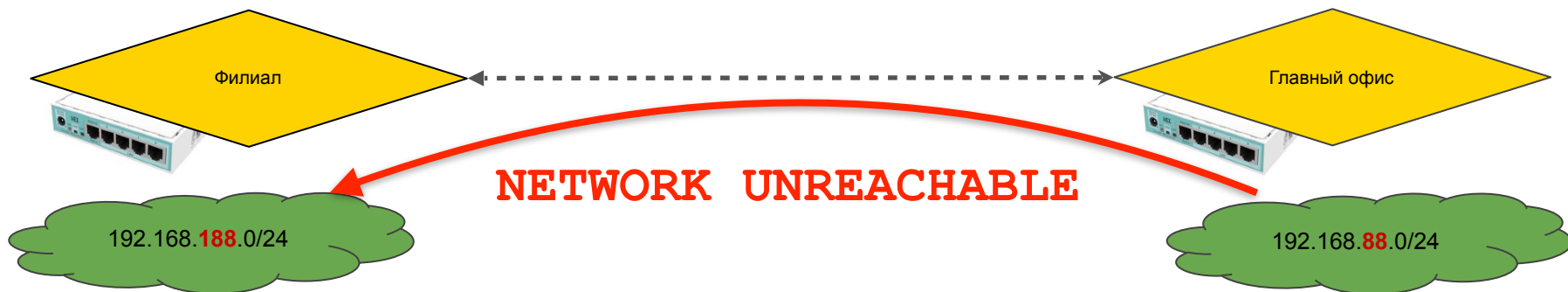


Проверка связи IKEv2: из главного офиса в филиалы

```
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
```



192.168.88.0/24



RouterOS IKEv2 site-to-site

Двусторонняя связь между офисами

192.168.188.0/24





MUM Indonesia

October 24–25, 2019

KUTA, BALI, Indonesia



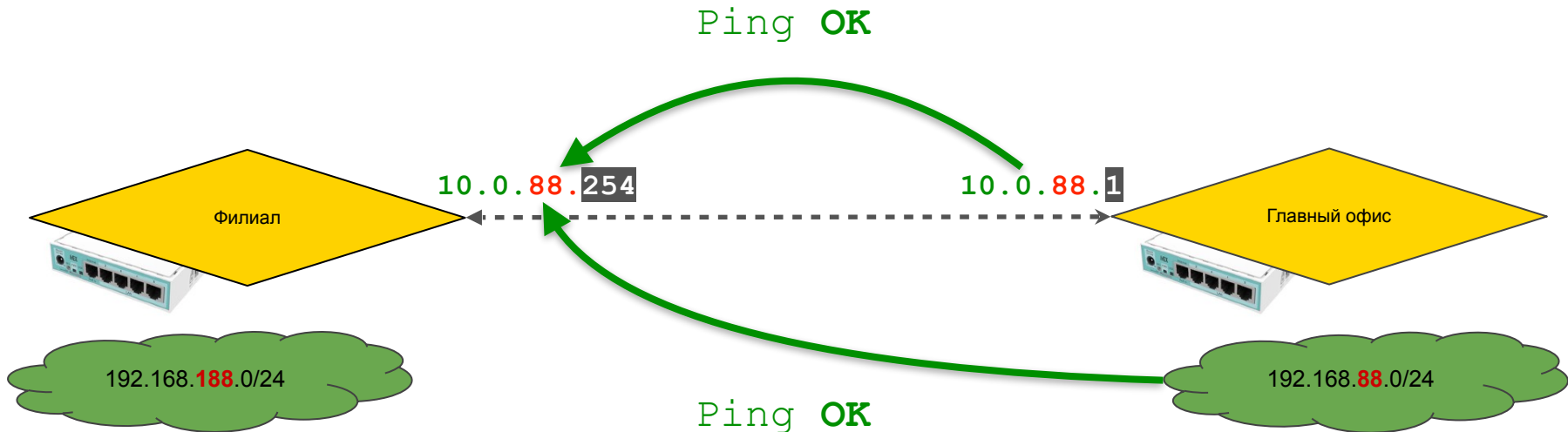
MikroTik IPSec IKEv2 VPN site-to-site:
easy step-by-step guide by Nikita Tarikin
(MikroTik PRO, Russia)

Проверка связи IKEv2: site-to-site

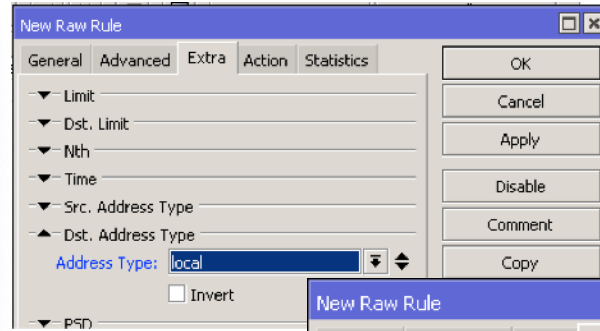
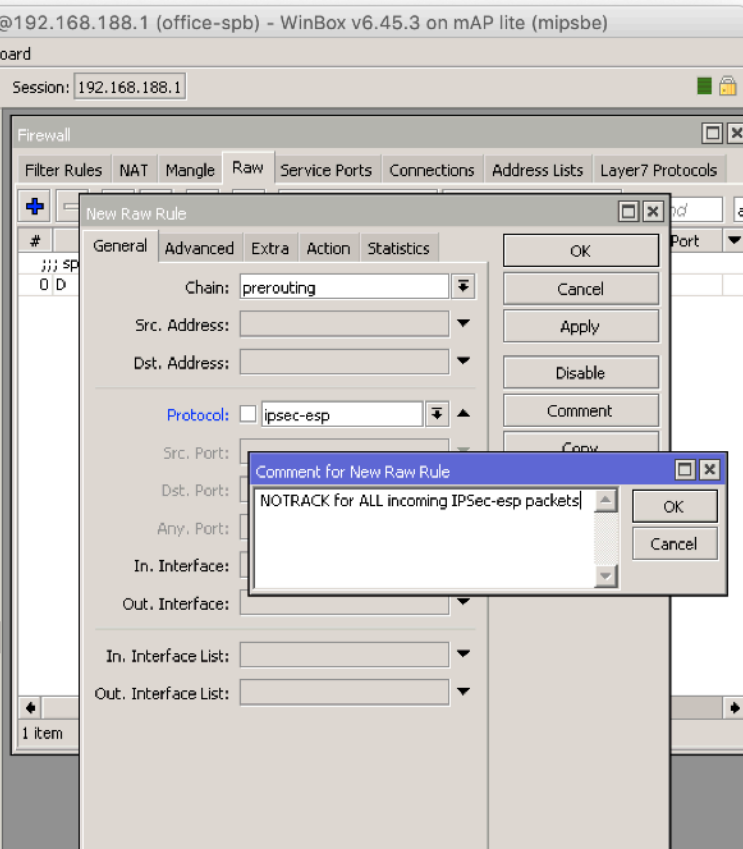
TO: 10.0.88.254

FROM: 192.168.88.0/24

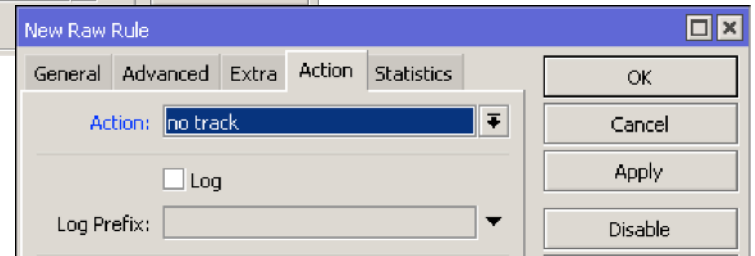
FROM: 10.0.88.1



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



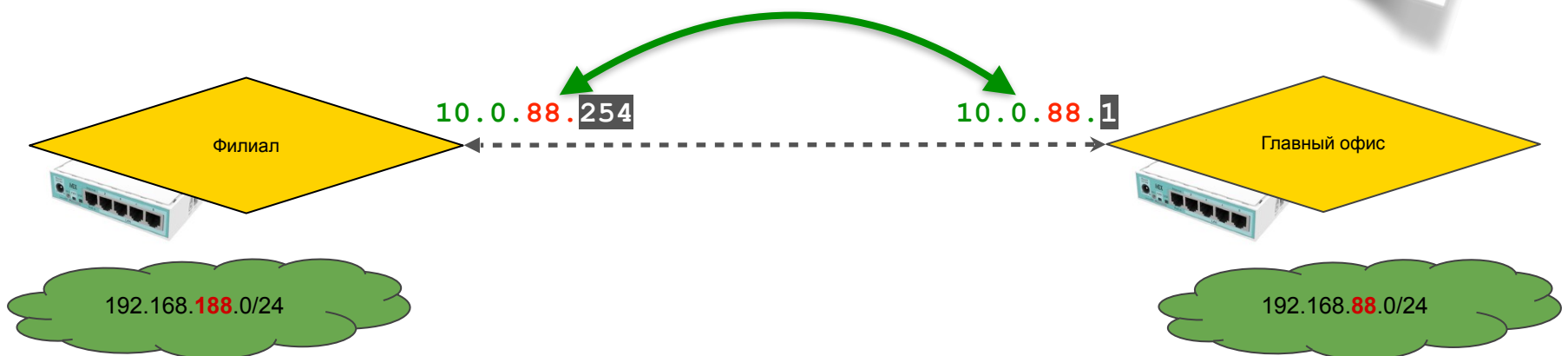
RAW
prerouting chain



```
/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

EoIP
IPsec
GRE



Корректируем клиентский IPsec modeconf

The screenshot shows the Mikrotik WinBox interface. The main window is titled "admin@192.168.188.1 (MikroTik office-spb.ike2.xyz) - WinBox v6.45.3 on mAP lite (mipsbe)". The "IPsec" tab is active, showing the "Mode Configs" sub-tab. A "New IPsec Mode Config" dialog box is open, with the following fields:

- Name: modeconf office-spb@vpn.ike2.xyz
- Responder:
- Connection Mark: (empty)
- Src. Address List: LAN-address-list

The "Src. Address List" field is crossed out with a red X. The background shows the "Firewall" tab with a table of rules:

#	Action	Chain	Log
0	;;: ipsec mode-config		
	Action: src-nat	Chain:	
	Dst. Address List: !LAN-address-list	Log:	
	Bytes: 168 B	Packets:	
	Packet Rate: 0		
1	;;: defconf: masquerade		
	Action: masquerade	Chain:	
	IPsec Policy: out:none	Log:	
	Packets: 1 033	Rate:	

The screenshot shows the Mikrotik WinBox Firewall tab. The "Filter Rules" sub-tab is active. A table of rules is displayed:

#	Action	Chain	Log
0	;;: ipsec mode-config		
	Action: src-nat	Chain:	
	Dst. Address List: !LAN-address-list	Log:	
	Bytes: 168 B	Packets:	
	Packet Rate: 0		
1	;;: defconf: masquerade		
	Action: masquerade	Chain:	
	IPsec Policy: out:none	Log:	
	Packets: 1 033	Rate:	

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

Демо лаба.

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



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



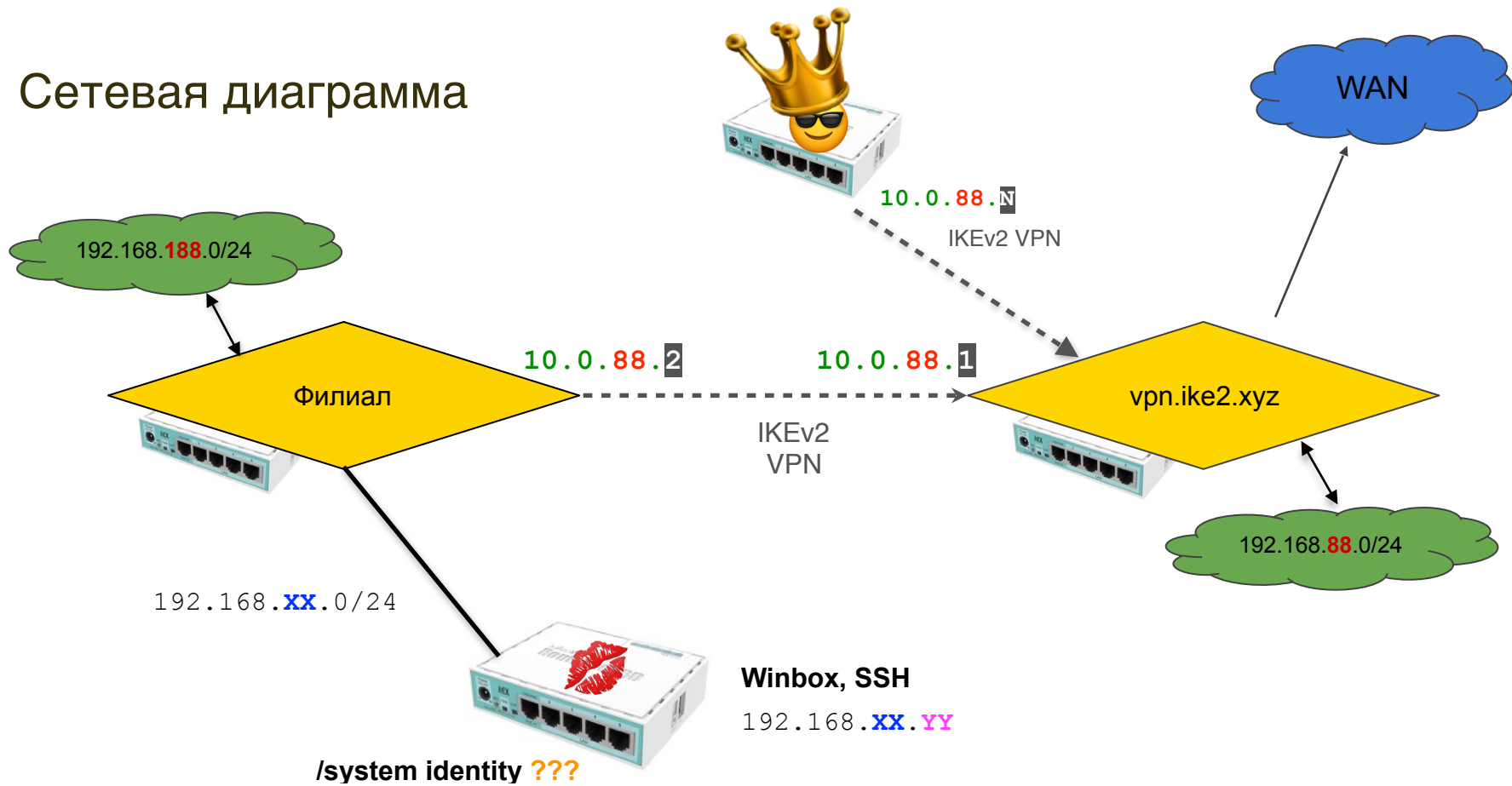
Внимание, конкурс!

“ Hack the princess ”



Открыта до 31 декабря 2019

Сетевая диаграмма

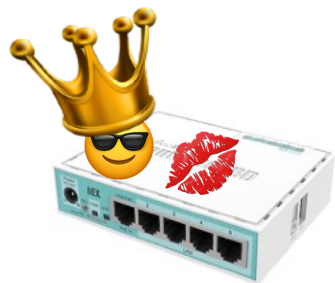




Чтобы пройти этот квест нужно:

- 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

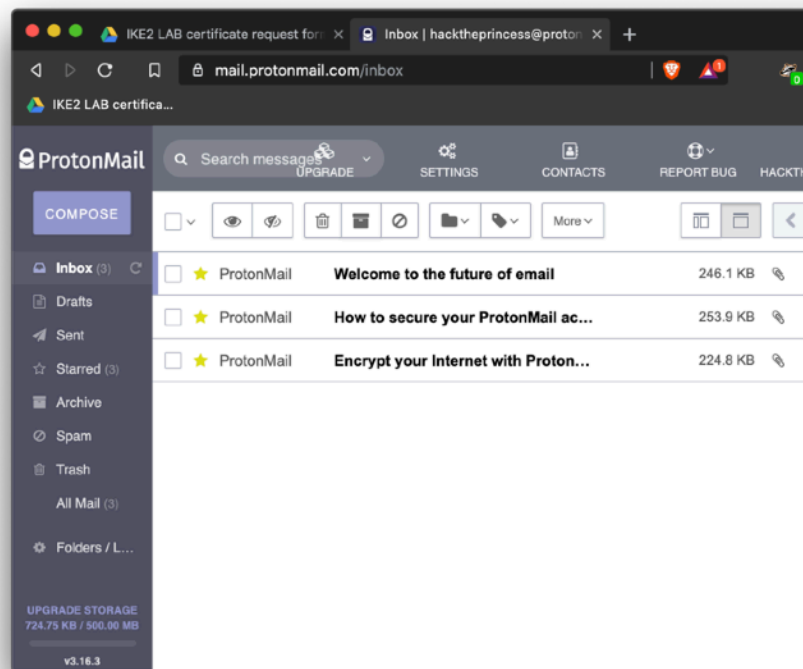


192.168.**XX**.0/24

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`

