



Использование Ipsec IKEv2 для подключения клиентских ОС.

MUM Kaliningrad 2019
mikrotik-training.ru





ОБО МНЕ

- Козлов Роман Сергеевич
- Сертифицированный тренер по MikroTik
- Технический директор IntegaSky
- Провожу бесплатные обучающие вебинары по MikroTik
- Более 200 выполненных проектов MikroTik
- Проводим мини-тренинги – mikrotik.team
- Являюсь соведущим linkmeup_sysadmins



Канал на youtube

<https://goo.gl/DSL6VG>



Запись на вебинары

<http://mikrotik-training.ru/webinar/>



Канал в телеграм

<https://t.me/miktrain>



Содержание

- Как отправить маршруты пользователю
- Схема подключения клиентов
- Варианты подключения клиентов
- Настройки IPSEC xauth
- Настройки IPSEC Ikev2
- Настройки IPSEC Ikev2 eap



Как отправить маршруты пользователю

- **PPTP/L2TP/SSTP** – proxy-arp, default gateway, cmaк, static route, rip, классовая маршрутизация
- **OpenVPN** – push route/add route
- **IpSec** – split network

L2tp/PPTP/SSTP proxy arp

Плюсы

- Не нужны административные привилегии для запуска VPN на пользовательской рабочей станции
- Клиент сразу в сети компании
- Простота для начинающих администраторов

Минусы

- Только одна сеть для доступа
- Лишние манипуляции с arp

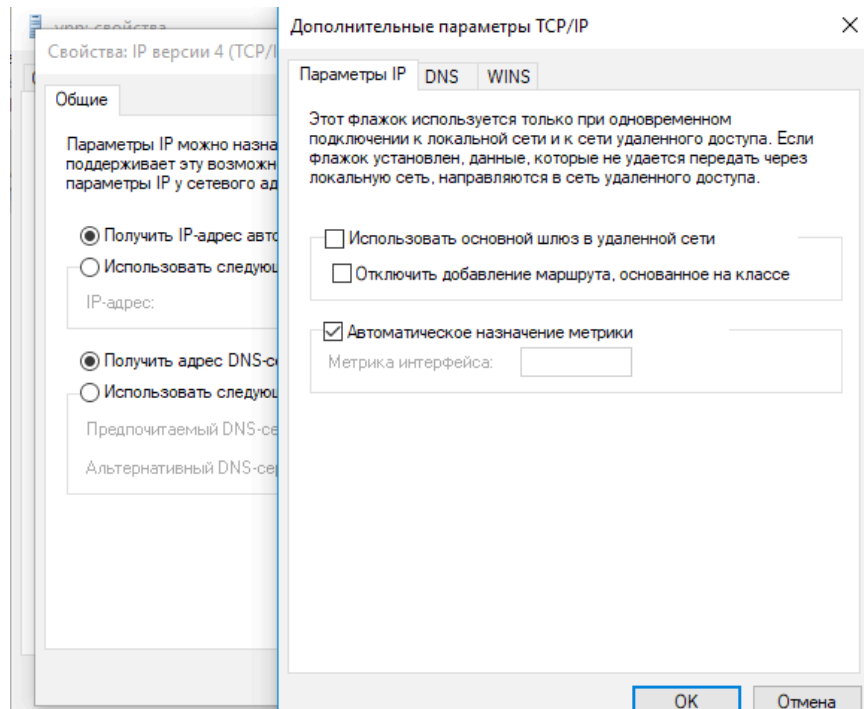
L2tp/PPTP/SSTP default gateway

Плюсы

- Легкая установка
- Полный контроль пользовательского трафика
- Мультиплатформенный

Минусы

- Двойное потребление трафика на VPN концентраторе
- Дополнительные задержки при работе с внешними каналами



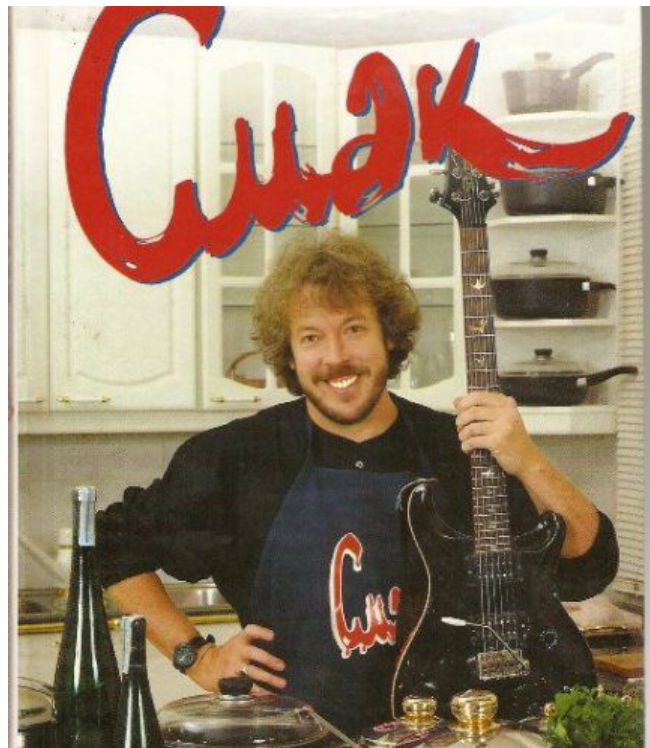
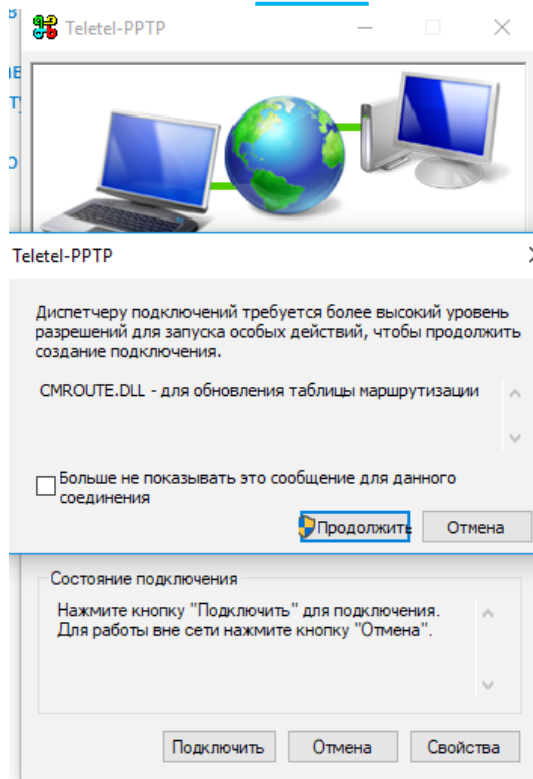
L2tp/PPTP/SSTP Cmak

Плюсы

- легкая установка для пользователя

Минусы

- Требуется административные привилегии на запуск с добавлением маршрутов или оператора настройки сети
- Нужен Windows server для сборки пакета cmak
- Не нравится вспоминать Макаревича
- В голове часто играет песня «Новый поворот»
- Не подходит для отличных от Windows OS



L2tp/PPTP/SSTP/OpenVPN/Ipsec static route

Плюсы

- Не нужны административные привилегии для запуска VPN на пользовательской рабочей станции, если изначально прописать постоянные маршруты
- Прозрачно для администратора – что прописал - то и работает
- Работает на различных операционных системах, кроме мобильных

Минусы

- На клиенте необходимо руками прописывать маршруты
- Если используете bat скрипты – их необходимо запускать из под администратора
- Иногда маршруты удаляются
- Не масштабируется
- Нет полноценной поддержки в мобильных операционных системах

L2tp/PPTP/SSTP rip

Плюсы

- Не нужны административные привилегии для запуска VPN на пользовательской рабочей станции
- Можно распространять большое количество маршрутов
- Изменение маршрутизации на VPN-клиентах на лету
- Можно фильтровать маршруты для конкретных клиентов

Минусы

- На клиенте необходимо установить роль слушатель RIP
- На VPN концентраторе так же требуется поднять rip
- Возможно на клиента отправить не нужные маршруты
- Не подходит для отличных от Windows OS
- Плохо пахнет



L2tp/PPTP/SSTP/OpenVPN/IPsec классовая маршрутизация/VLSM

Плюсы

- Ничего прописывать не нужно на пользовательских ОС
- Не требуются административные привилегии для запуска VPN

Минусы

- Требуется дополнительное планирование адресного пространства в организации
- Нет возможности прокинуть дополнительные маршруты
- Сложно работать с сетями 192.168.x.0/24
- Мобильные устройства под вопросом

Плюсы

- Мультиплатформенность
- Отличная проходимость
- Сильное шифрование
- Можно распространять в виде преднастроенного клиента или конфигурационных файлов

Минусы

- Запуск из под администратора
- Установка дополнительного ПО
- В mikrotik отсутствует PushRoutes
- В mikrotik отсутствует UDP
- В mikrotik работает на одном ядре

OpenVPN



IpSec split network

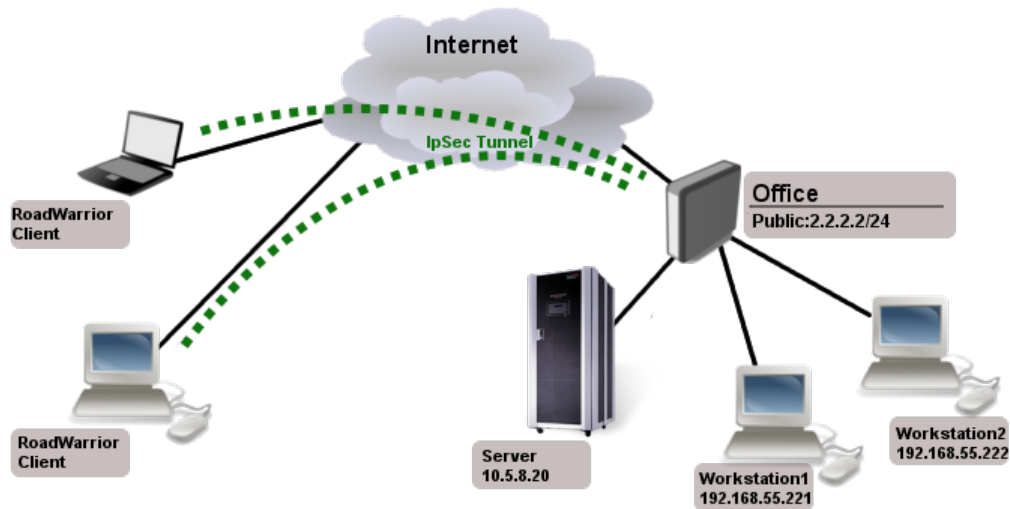
Плюсы

- Мультиплатформенность
- Не требуются административные привилегии на ОС
- Поддерживает аппаратное шифрование на RouterOS
- Быстрый

Минусы

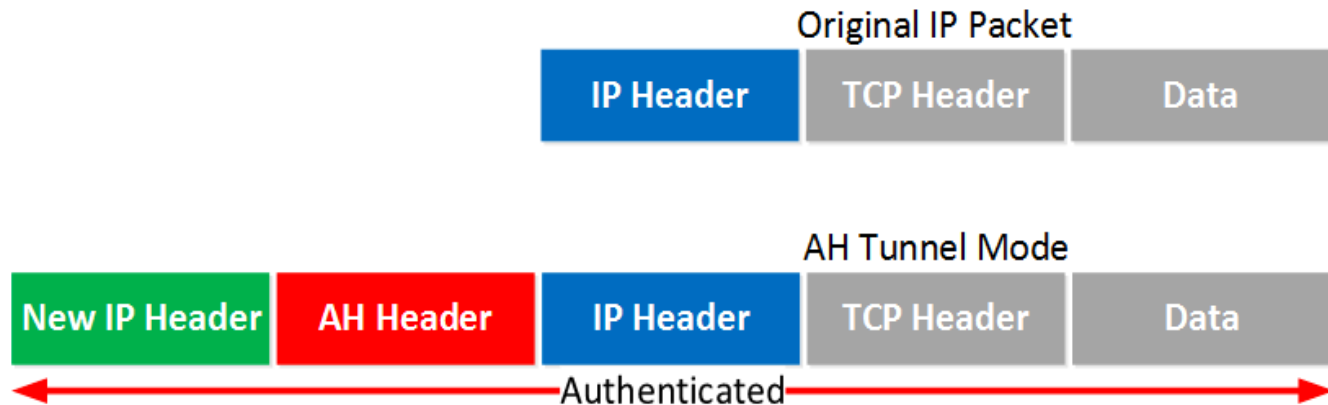
- Сложно настраивать
- Отсутствует интерфейс в routerOS
- Нет прямой связи с маршрутизацией
- Есть недоработки в пользовательских ОС

Схема подключения клиентов



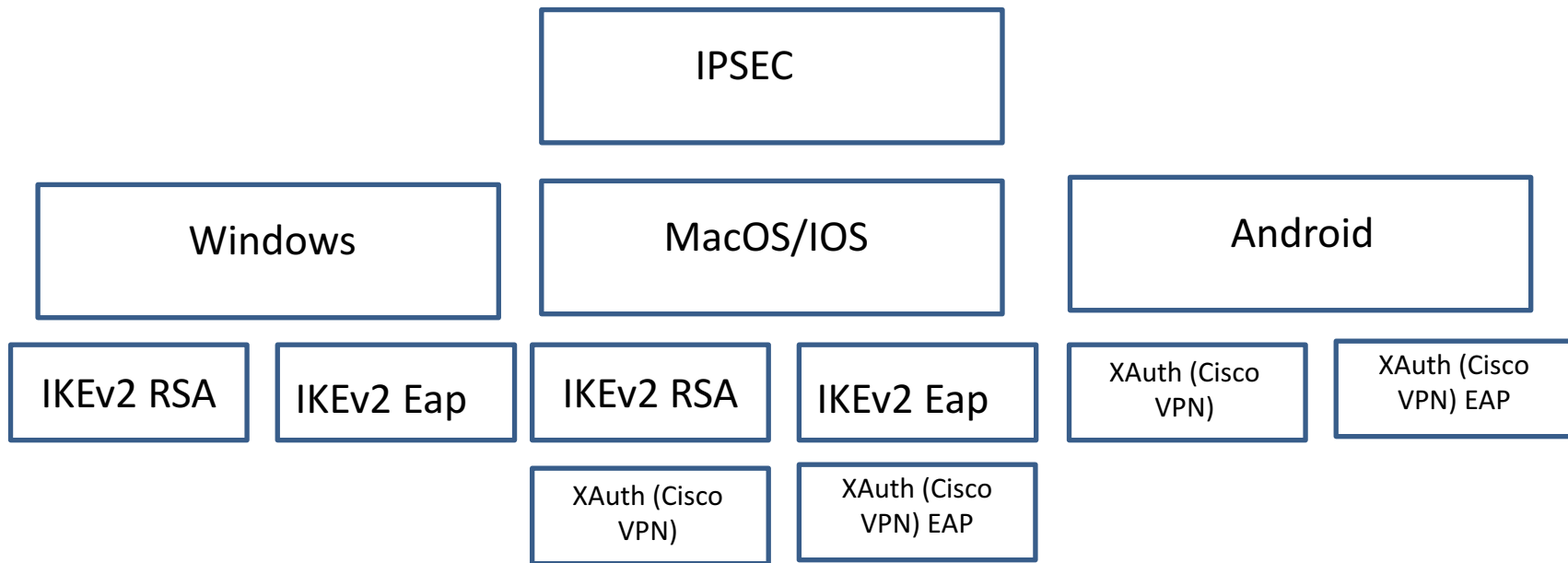
- Internet Protocol Security (IPsec) - это набор протоколов для защиты обмена пакетами через незащищенные сети IP / IPv6, такие как Интернет.
- Ipsec можно использовать как способ подключения клиентских устройств в сеть предприятия
- По сути это туннельный ipsec на пользователя
- Политики генерируются на основе Template

Ipsec tunnel mode

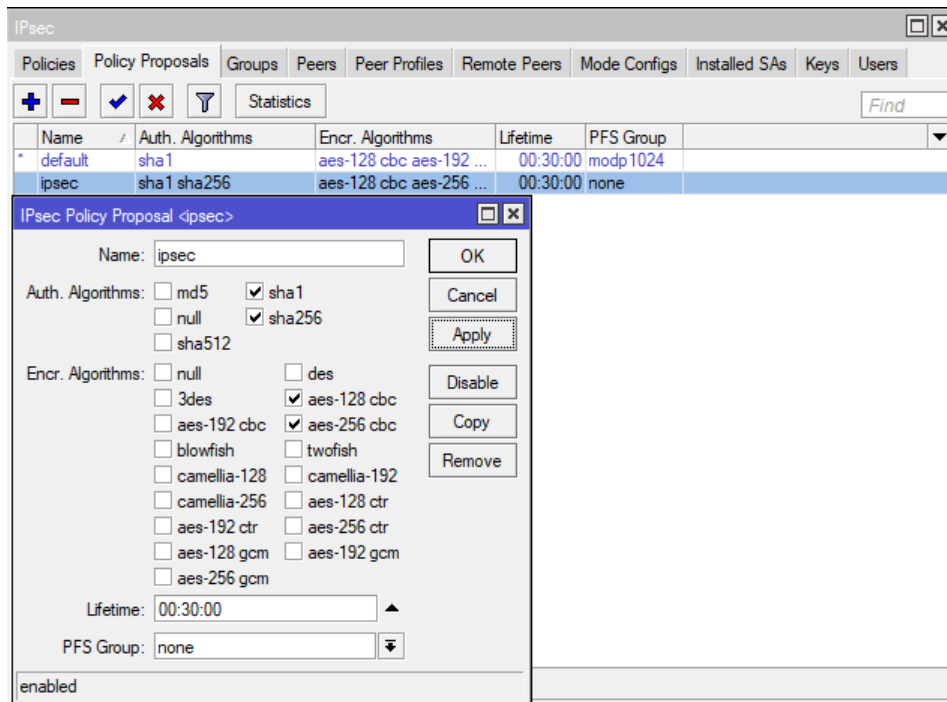


- Пакет который мы планируем передать попадает под условия ipsec policy и после этого происходит добавление нового IP заголовка.
- В этом режиме IPSEC выступает в режиме переносчика трафика.
- Не будут работать протоколы маршрутизации.
- Оригинальный заголовок IP теперь также зашифрован.

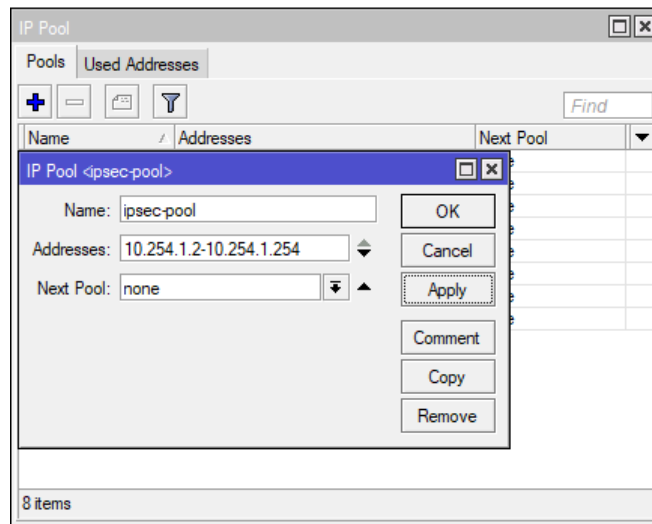
Варианты подключения ipsec для разных операционных систем



IPSec Policy Proposals (phase 1)



IP pool



IPSec Mode Configs

IPsec

Policies Policy Proposals Groups Peers Peer Profiles Remote Peers Mode Configs Installed SAs Keys Users

+ - Y

Name	Respo...	Address Pool	Address Prefix...	Split Include	System D...	Src. Addr...
ipsec-user-networks	yes	ipsec-pool	24	10.0.0.0/8	no	
* request-only	no					

IPsec Mode Config <ipsec-user-networks>

Name: ipsec-user-networks OK

☒ Responder Cancel

Address Pool: ipsec-pool Apply

Address Prefix Length: 24 Copy

Split Include: 10.0.0.0/8 Remove

☐ System DNS

Static DNS:

IPSec Peer

До 6.44

После 6.44

IPsec Peer <0.0.0.0/0>

General Advanced

Address: 0.0.0.0/0

Port:

Local Address:

Profile: ipsec-user-ph1

Auth. Method: pre shared key xauth

Exchange Mode: main

☒ Passive

Secret:

XAuth Login:

XAuth Password:

OK Cancel Apply Disable Comment Copy Remove

enabled responder

1 item

IPsec Peer <RW>

General Advanced

Name: RW

Address: ::/0

Port:

Local Address:

Profile: ipsec

Exchange Mode: main

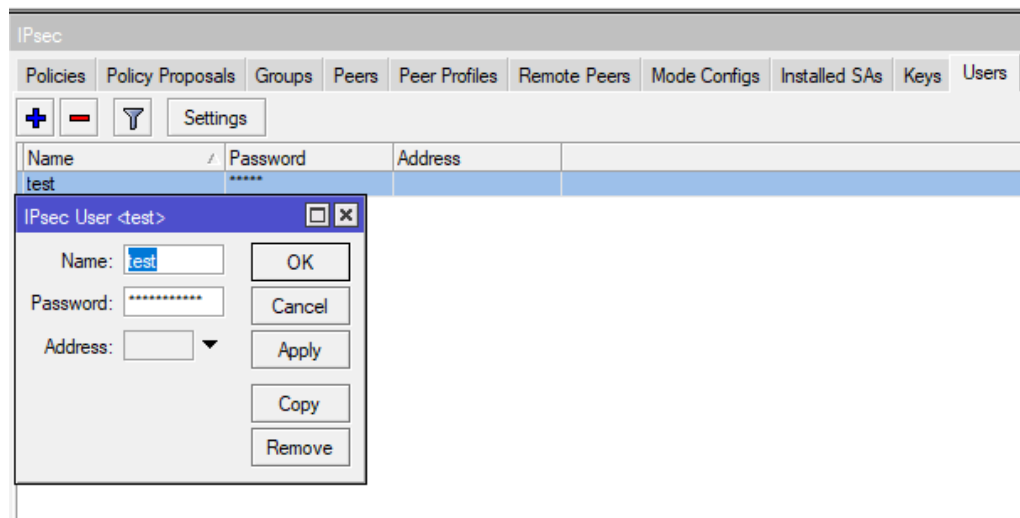
☒ Passive

☐ Send INITIAL_CONTACT

OK Cancel Apply Disable Comment Copy Remove

enabled responder

IPSec Users – до 6.44



IPsec

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

+ - ✓ ✗ 📁 🔍

#	Peer	Auth. Method	XAuth Login	Remote ID	Mode Configuration
New IPsec Identity					

Peer: RW

Auth. Method: pre shared key xauth

Secret:

XAuth Login:

XAuth Password:

Policy Template Group: ikev2

Notrack Chain:

My ID Type: auto

Remote ID Type: ignore

Match By: remote id

Mode Configuration: RW

Generate Policy: port strict

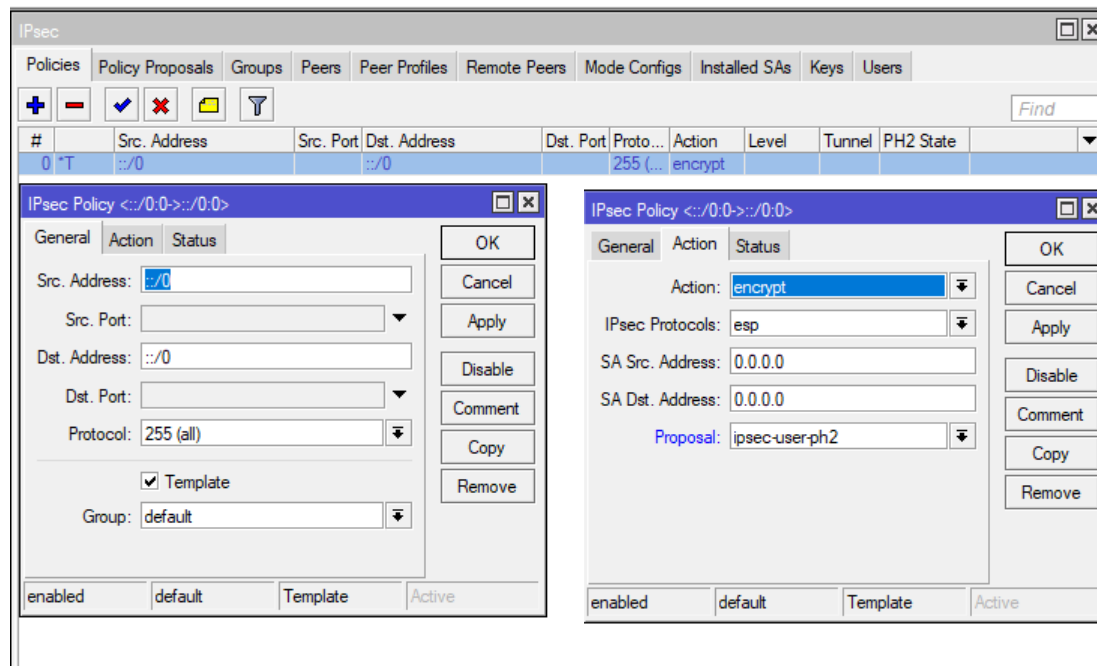
enabled

После 6.44

Режим авторизации pre shared key Xauth (Cisco VPN – в macOS/IOS)

- С версии 6.44 настройка пользователей перенесена в раздел
- `/ip ipsec identity`
- Для preshared key xauth – необходим режим работы ipsec peers main

IPSec Policies



IP firewall filter

Firewall Rule <4500,500>

General

Advanced

Extra

Action

Statistics

Chain:

Src. Address:

Dst. Address:

Protocol: ☐ 17 (udp)

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface:

In. Interface List: ☐ WAN

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State:

Connection NAT State:

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

Firewall Rule <>

General

Advanced

Extra

Action

Statistics

Chain:

Src. Address:

Dst. Address:

Protocol: ☐ 50 (ipsec-esp)

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface:

In. Interface List: ☐ WAN

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State:

Connection NAT State:

OK

Cancel

Apply

Disable

Comment

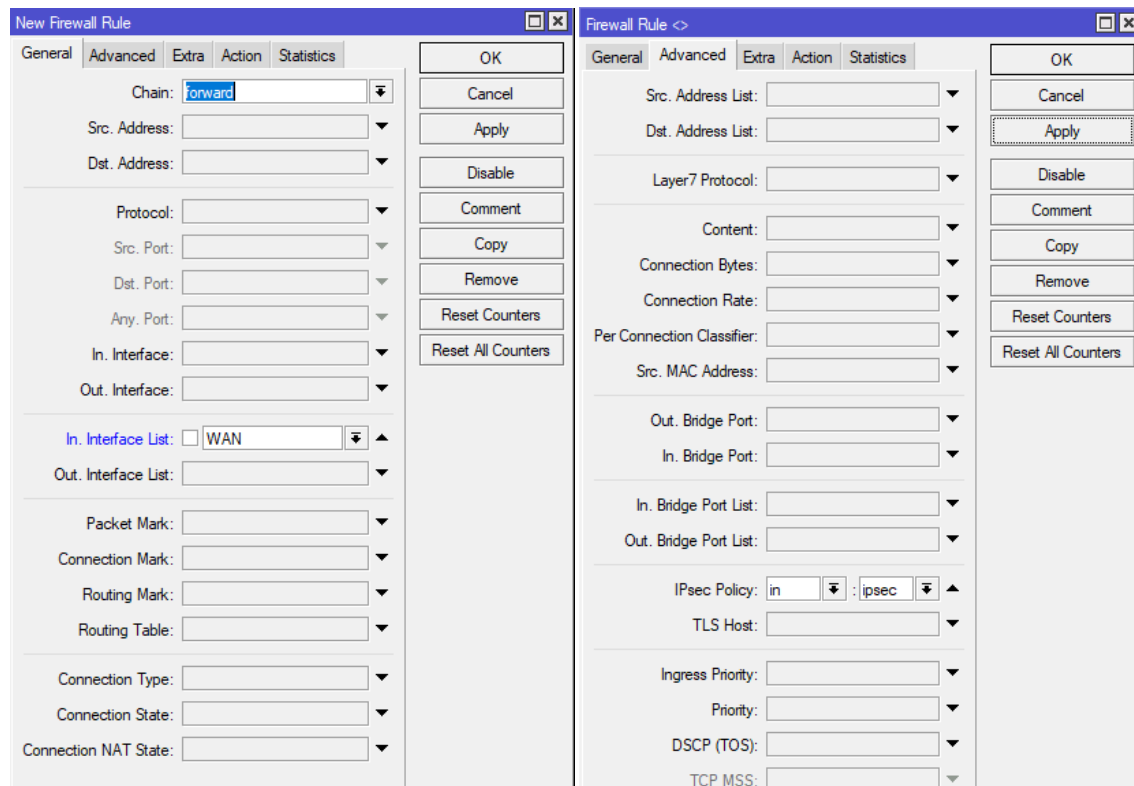
Copy

Remove

Reset Counters

Reset All Counters

IP firewall filter



The image displays two side-by-side screenshots of the Mikrotik WinBox interface, showing the configuration of a new IP firewall rule.

Left Window: New Firewall Rule

- General Tab:**
 - Chain: **forward**
 - Src. Address: [Empty]
 - Dst. Address: [Empty]
 - Protocol: [Empty]
 - Src. Port: [Empty]
 - Dst. Port: [Empty]
 - Any. Port: [Empty]
 - In. Interface: [Empty]
 - Out. Interface: [Empty]
 - In. Interface List: ☐ **WAN**
 - 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]
- Action Tab:**
 - OK
 - Cancel
 - Apply
 - Disable
 - Comment
 - Copy
 - Remove
 - Reset Counters
 - Reset All Counters

Right Window: Firewall Rule

- General Tab:**
 - Src. Address List: [Empty]
 - Dst. Address List: [Empty]
 - Layer7 Protocol: [Empty]
 - Content: [Empty]
 - Connection Bytes: [Empty]
 - Connection Rate: [Empty]
 - Per Connection Classifier: [Empty]
 - Src. MAC Address: [Empty]
 - Out. Bridge Port: [Empty]
 - In. Bridge Port: [Empty]
 - In. Bridge Port List: [Empty]
 - Out. Bridge Port List: [Empty]
 - IPsec Policy: **in** : **ipsec**
 - TLS Host: [Empty]
 - Ingress Priority: [Empty]
 - Priority: [Empty]
 - DSCP (TOS): [Empty]
 - TCP MSS: [Empty]
- Action Tab:**
 - OK
 - Cancel
 - Apply
 - Disable
 - Comment
 - Copy
 - Remove
 - Reset Counters
 - Reset All Counters

IP firewall filter

New Firewall Rule

General Advanced Extra Action Statistics

Chain: **forward**

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface:

In. Interface List: ☐ WAN

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State:

Connection NAT State:

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

Firewall 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** : **ipsec**

TLS Host:

Ingress Priority:

Priority:

DSCP (TOS):

TCP MSS:

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

Настройка Ipsec X-auth на IOS



Тип

IPsec

Описание

Lor

Сервер

178.22.31.110

Учетная запись

test

Пароль

●●●●●●●●

Сертификат

☐

Имя группы

Общий ключ

●●●●●●●●

ПРОКСИ

Выкл.

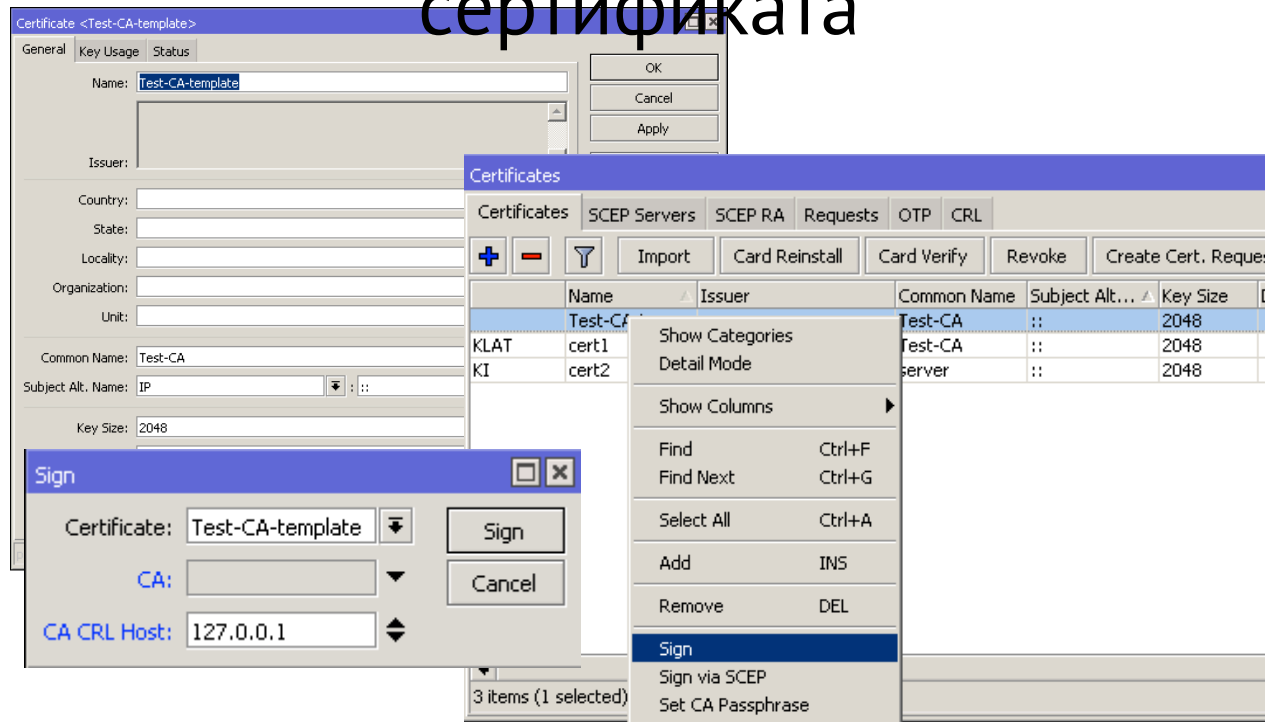
Вручную

Авто

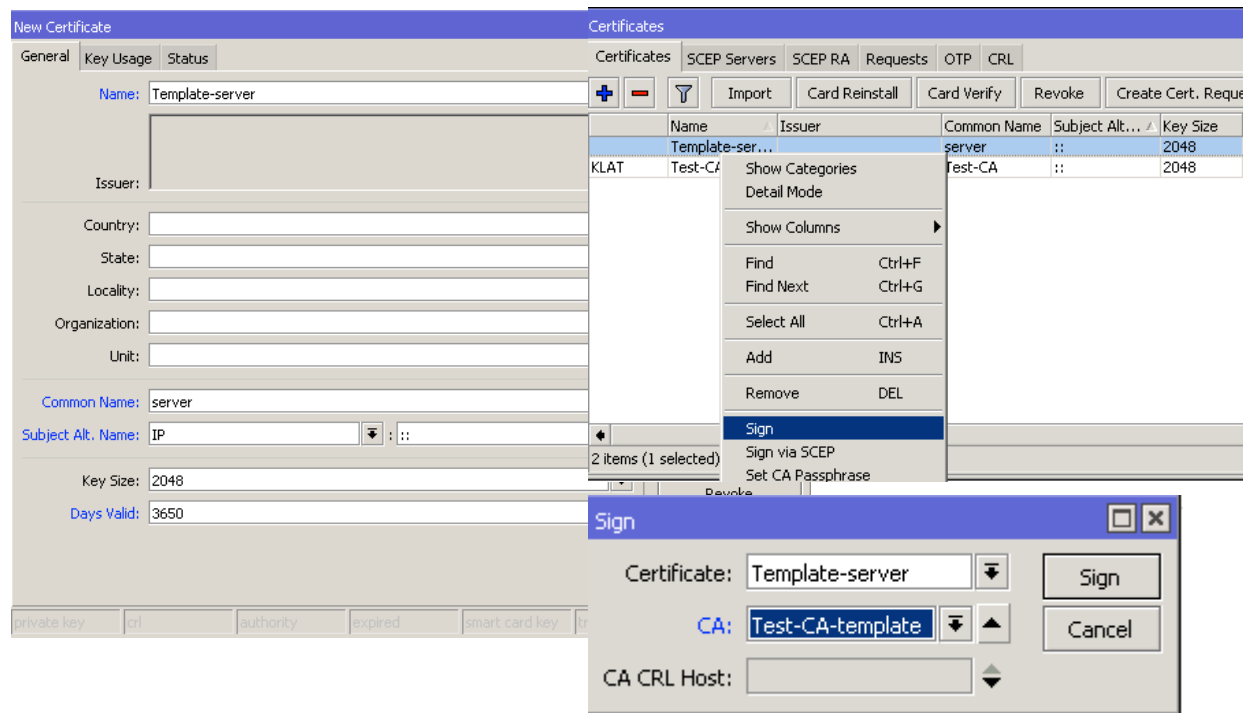
IKEv2 RFC7296

- Режимы обмена IKEv1 устарели – используется упрощенный обмен, всего 4 сообщения
- RFC4555, IKEv2 Mobility and Multihoming Protocol (MOBIKE) - механизм обновления IP-адреса у клиента без полной регенерации SA
- PSK и RSA-Sig аутентификация Асимметричная аутентификация
- Lifetime не нужны
- NAT-T: Поддерживается по умолчанию
- RFC3706 DPD: Поддерживается по умолчанию - Dead Peer Detection (более быстрое обнаружение мертвых клиентов)
- RoadWarrior: поддерживается EAP и config payload(CP)
- Сопротивление DOS улучшено
- Для режима RSA-signature требуются сертификаты
- Встроенная поддержка в Windows*
- Встроенная поддержка в IOS**

IpSec IKEv2 создание CA сертификата



IPSec IKEv2 создание сертификата сервера

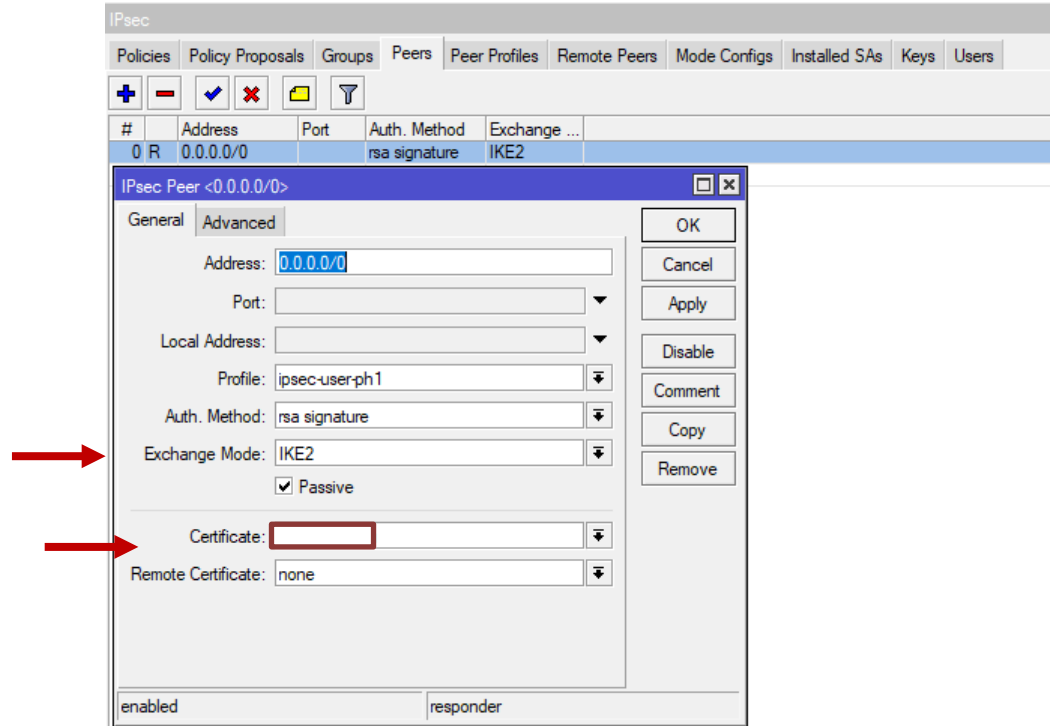


Common name – желательно
dns имя сервера

Subject Alt. Name – dns имя
сервера

Key usgate – tls server

IPSec IKEv2



IPsec

Polices Policy Proposals Groups Peers Peer Profiles Remote Peers Mode Configs Installed SAs Keys Users

#	Address	Port	Auth. Method	Exchange ...
0 R	0.0.0.0/0		rsa signature	IKE2

IPsec Peer <0.0.0.0/0>

General Advanced

Address: 0.0.0.0/0

Port:

Local Address:

Profile: ipsec-user-ph1

Auth. Method: rsa signature

Exchange Mode: IKE2

☒ Passive

Certificate:

Remote Certificate: none

OK Cancel Apply Disable Comment Copy Remove

enabled responder

IPSec IKEv2 создание сертификата клиента

The screenshot shows the MikroTik WinBox interface for managing certificates. The 'Certificates' window is open, and the 'Certificate <test2>' form is visible. The 'Name' field is set to 'test2'. A red arrow points from the 'Name' field to the 'Sign' button in the context menu. Another red arrow points from the 'Sign' button to the 'Sign' dialog box. The 'Sign' dialog box shows 'Certificate:' and 'CA: Test-CA-template'.

Key Usage – tls user

IPSec IKEv2 настройка на Windwos

The image shows two overlapping Windows configuration windows for setting up a VPN connection.

Left Window: "Добавить VPN-подключение" (Add VPN connection)

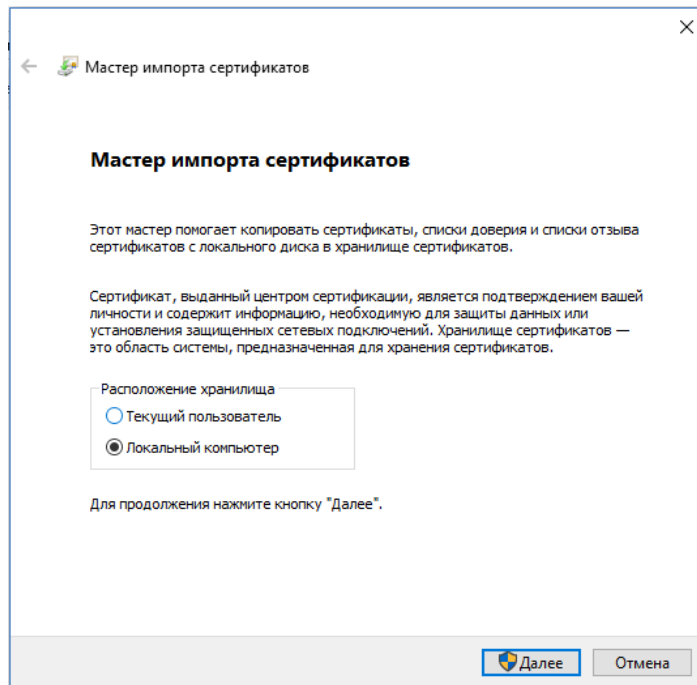
- Поставщик услуг VPN: Windows (встроенные)
- Имя подключения: vpn.test
- Имя или адрес сервера: vpn.test
- Тип VPN: IKEv2
- Тип данных для входа: Сертификат
- Имя пользователя (необязательно):
- Пароль (необязательно):
- ☒ Запомнить мои данные для входа

Right Window: "Общие" (General) tab

- Тип VPN: IKEv2
- Дополнительные параметры
- Шифрование данных: обязательное (отключиться, если нет шифрования)
- Проверка подлинности:
 - ☐ Протокол расширенной проверки подлинности (EAP)
 - ☒ Использовать сертификаты компьютеров

Buttons: OK, Отмена

IPSec IKEv2



- Требуется импортировать сертификаты пользователя в формате p12 в контейнер компьютера – при выгрузке из mikrotik указать пароль
- /certificate
- export-certificate ca
- export-certificate rw-client1
export-passphrase=1234567890
- Также требуется загрузить публичный ключ CA в контейнер компьютера

ВАТ для настройки в Windows

- @setlocal enableextensions
- @cd /d "%~dp0"
- certutil -addstore -f "ROOT" CA.crt
- certutil -p PassWord123 -importpfx cert.p12
- powershell Add-VpnConnection -Name "vpn" -ServerAddress "vpn1.integrasky.ru" - TunnelType ikev2 -EncryptionLevel Required -AuthenticationMethod MachineCertificate - SplitTunneling -PassThru
- Отключившее расширение проверку сертификатов, добавьте параметр типа DWORD под именем "DisableIKENNameEkuCheck" в следующий путь реестра VPN-клиента.
- reg add
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters" /v
DisableIKENNameEkuCheck /t REG_DWORD /d 1
- copy vpn.lnk "C:\Users\Default\Desktop\"

DHCP INFORM запрос от клиента

prerouting: in:ether1, proto UDP, 10.253.2.10:68->255.255.255.255:67, len 328

output: out:ether1, proto UDP, 1.1.1.1:67->10.253.2.10:68, len 328

```
Transaction ID: 0x4618eae4
▶ Seconds elapsed: 6
▶ Bootp flags: 0x0000 (Unicast)
  Client IP address: 10.253.2.10
  Your (client) IP address: 0.0.0.0
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
▶ Client address not given
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
▶ Option: (53) DHCP Message Type (Inform)
▶ Option: (61) Client identifier
▶ Option: (12) Host Name
▶ Option: (60) Vendor class identifier
▼ Option: (55) Parameter Request List
  Length: 6
  Parameter Request List Item: (6) Domain Name Server
  Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
  Parameter Request List Item: (43) Vendor-Specific Information
  Parameter Request List Item: (1) Subnet Mask
  Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
  Parameter Request List Item: (15) Domain Name
▶ Option: (255) End
Padding: 0000
```

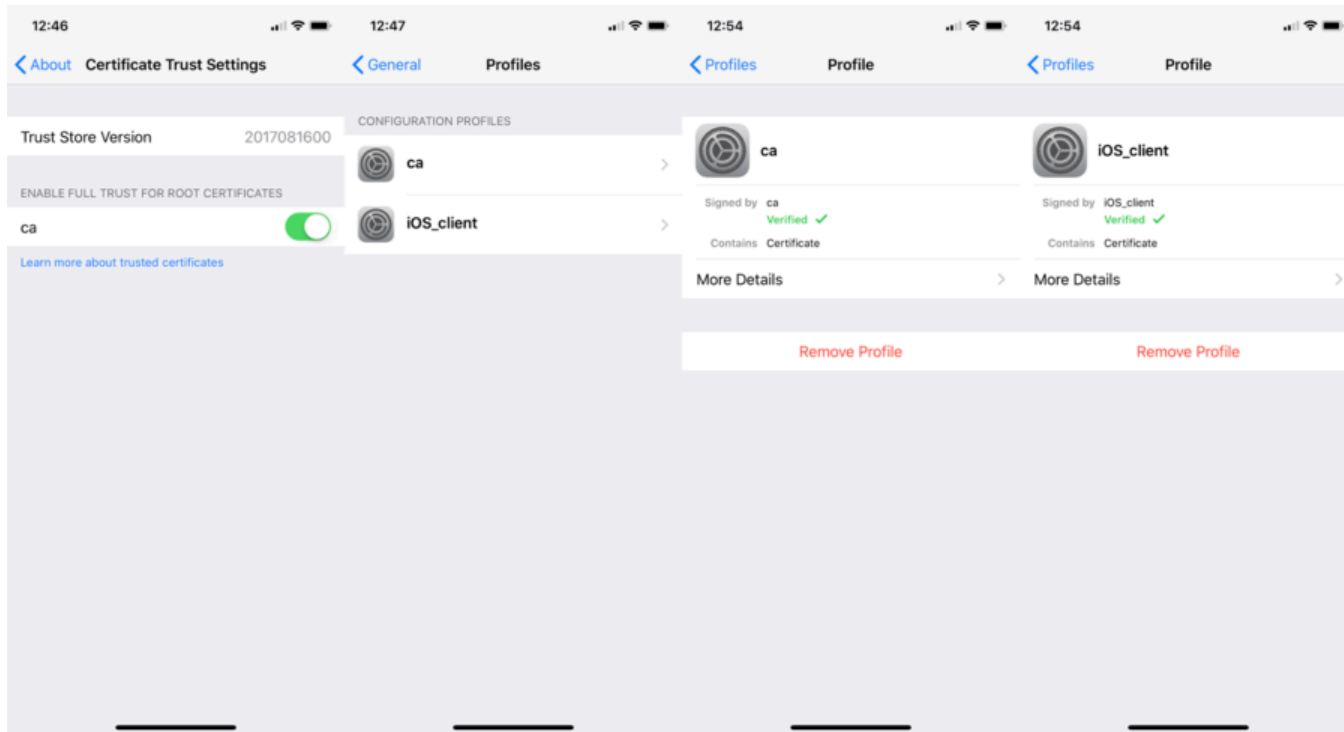
Маршруты у клиента

```
IPv4 таблица маршрута
=====
Активные маршруты:
Сетевой адрес      Маска сети      Адрес шлюза      Интерфейс      Метрика
0.0.0.0            0.0.0.0         10.211.55.1      10.211.55.3    25
10.0.0.0           255.0.0.0       On-link          10.253.2.10    26
10.211.55.0        255.255.255.0   On-link          10.211.55.3    281
10.211.55.3        255.255.255.255 On-link          10.211.55.3    281
10.211.55.255      255.255.255.255 On-link          10.211.55.3    281
10.253.2.10        255.255.255.255 On-link          10.253.2.10    281
10.255.255.255     255.255.255.255 On-link          10.253.2.10    281
10.255.255.255     255.255.255.255 On-link          10.253.2.10    281
10.255.255.255     255.255.255.255 On-link          10.253.2.10    281
127.0.0.0          255.0.0.0       On-link          127.0.0.1      331
127.0.0.1          255.255.255.255 On-link          127.0.0.1      331
127.255.255.255    255.255.255.255 On-link          127.0.0.1      331
169.254.0.0        255.255.0.0     On-link          169.254.228.220 281
169.254.228.220    255.255.255.255 On-link          169.254.228.220 281
169.254.228.220    255.255.255.255 On-link          169.254.228.220 281
192.168.0.0        255.255.0.0     On-link          10.253.2.10    26
192.168.255.255    255.255.255.255 On-link          10.253.2.10    281
224.0.0.0          240.0.0.0       On-link          127.0.0.1      331
224.0.0.0          240.0.0.0       On-link          10.211.55.3    281
224.0.0.0          240.0.0.0       On-link          169.254.228.220 281
224.0.0.0          240.0.0.0       On-link          10.253.2.10    281
255.255.255.255    255.255.255.255 On-link          127.0.0.1      331
255.255.255.255    255.255.255.255 On-link          10.211.55.3    281
255.255.255.255    255.255.255.255 On-link          169.254.228.220 281
255.255.255.255    255.255.255.255 On-link          10.253.2.10    281
=====
Постоянные маршруты:
Отсутствует
```

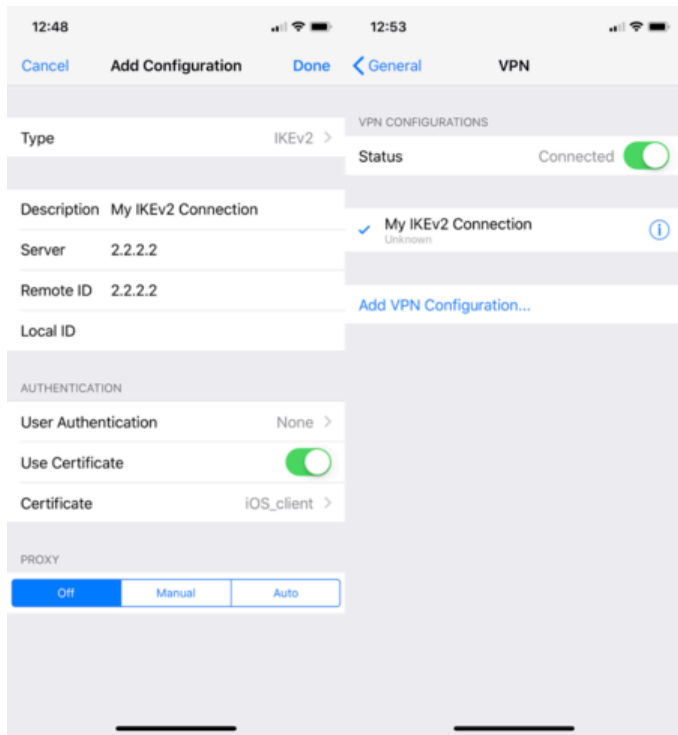
Маршруты у клиента macOS

Internet:						
Destination	Gateway	Flags	Refs	Use	Netif	Expire
default	192.168.191.1	UGSc	100	0	en0	
default	192.168.191.1	UGScI	1	0	en5	
default	link#17	UCSI	2	0	ipsec0	
10	10.253.2.11	UGSc	0	0	ipsec0	
10.37.129/24	link#16	UC	1	0	vnici1	!
10.211.55/24	link#15	UC	1	0	vnici0	!
10.253.2.11	10.253.2.11	UGSc	0	0	ipsec0	
127	127.0.0.1	UCS	0	7	lo0	
127.0.0.1	127.0.0.1	UH	31	803810	lo0	
169.254	link#5	UCS	0	0	en0	!
169.254	link#12	UCSI	0	0	en5	!
172.16/12	10.253.2.11	UGSc	0	0	ipsec0	
192.168.0/16	10.253.2.11	UGSc	3	0	ipsec0	
192.168.191	link#5	UCS	0	0	en0	!
192.168.191	link#12	UCSI	2	0	en5	!
192.168.191.1/32	link#5	UCS	1	0	en0	!
192.168.191.1	6c:3b:6b:5:70:ef	UHLWIir	57	6429	en0	1199
192.168.191.1	6c:3b:6b:5:70:ef	UHLWIir	1	1	en5	1199
192.168.191.1/32	link#12	UCSI	1	0	en5	!
192.168.191.10/32	link#5	UCS	1	0	en0	!
192.168.191.10	b8:e8:56:33:16:c6	UHLWI	0	26789	lo0	
192.168.191.30/32	link#12	UCS	0	0	en5	!
192.168.191.30	ac:87:a3:0:f0:43	UHLWI	0	12	lo0	
224.0.0/4	link#5	UmCS	2	0	en0	!
224.0.0/4	link#12	UmCSI	2	0	en5	!
224.0.0/4	link#17	UmCSI	0	0	ipsec0	
224.0.0.251	1:0:5e:0:0:fb	UHmLWI	0	20	en0	
224.0.0.251	1:0:5e:0:0:fb	UHmLWI	0	2484	en5	
239.255.255.250	1:0:5e:7f:ff:fa	UHmLWI	0	9	en0	
239.255.255.250	1:0:5e:7f:ff:fa	UHmLWI	0	665	en5	
255.255.255.255/32	link#5	UCS	0	0	en0	!
255.255.255.255/32	link#12	UCSI	0	0	en5	!
255.255.255.255/32	link#17	UCSI	0	0	ipsec0	

IPSec IKEv2

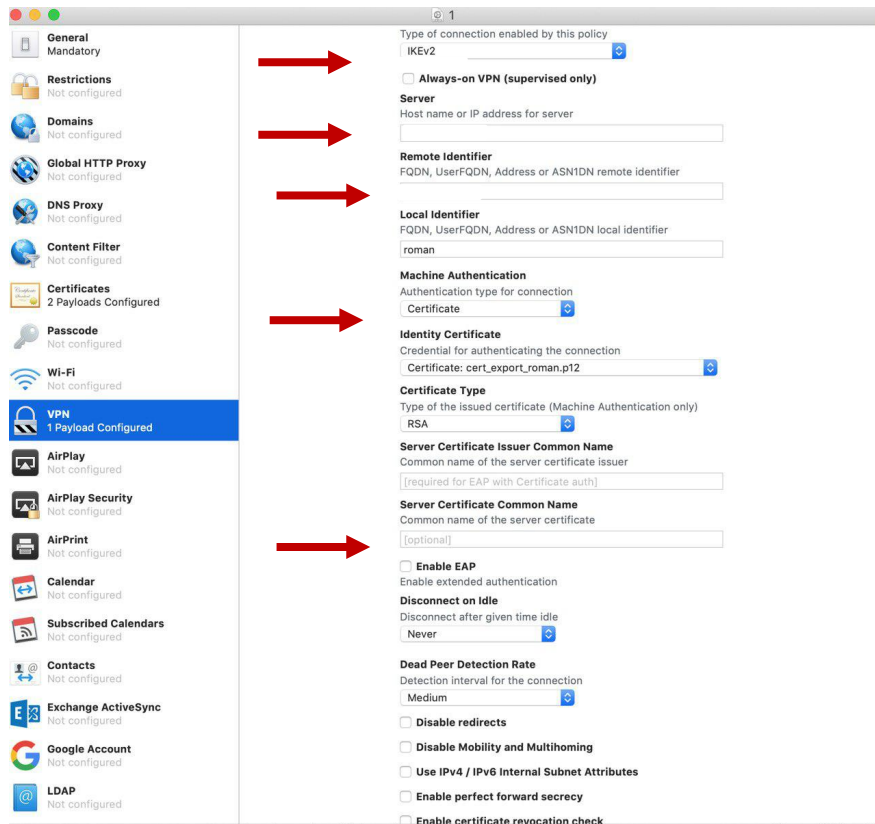


IPSec IKEv2



- Но это не работает
- В логах ipsec вы увидите
 - No eap configured
- Сейчас по умолчанию устройства от Apple требуют EAP авторизацию(RADIUS)
- Вариант обхода – apple configurator 2 – работает только на MacOS
- Или ручное создание .mobileconfig

IPSec IKEv2



- Указываем identity сервера(FQDN) и клиента(common name)
- Добавляем сертификаты в конфигурацию
- Указываем в настройках сертификаты клиента
- Так же заполняем поля Server certificate Common name – имя сертификата сервера

IPSec IKEv2 + EAP

- Mikrotik User-Manager не поддерживает EAP method
- Используем Windows Server NPS
- FreeRadius

New RADIUS Server

General Status

Service: ☐ ppp ☐ login
☐ hotspot ☐ wireless
☐ dhcp ☒ ipsec

Called ID:

Domain:

Address: 10.1.1.1

Protocol: udp

Secret: 123

Authentication Port: 1812

Accounting Port: 1813

Timeout: 300 ms

☐ Accounting Backup

Realm:

Certificate: none

Src. Address:

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Status

enabled

IPSec IKEv2 + EAP

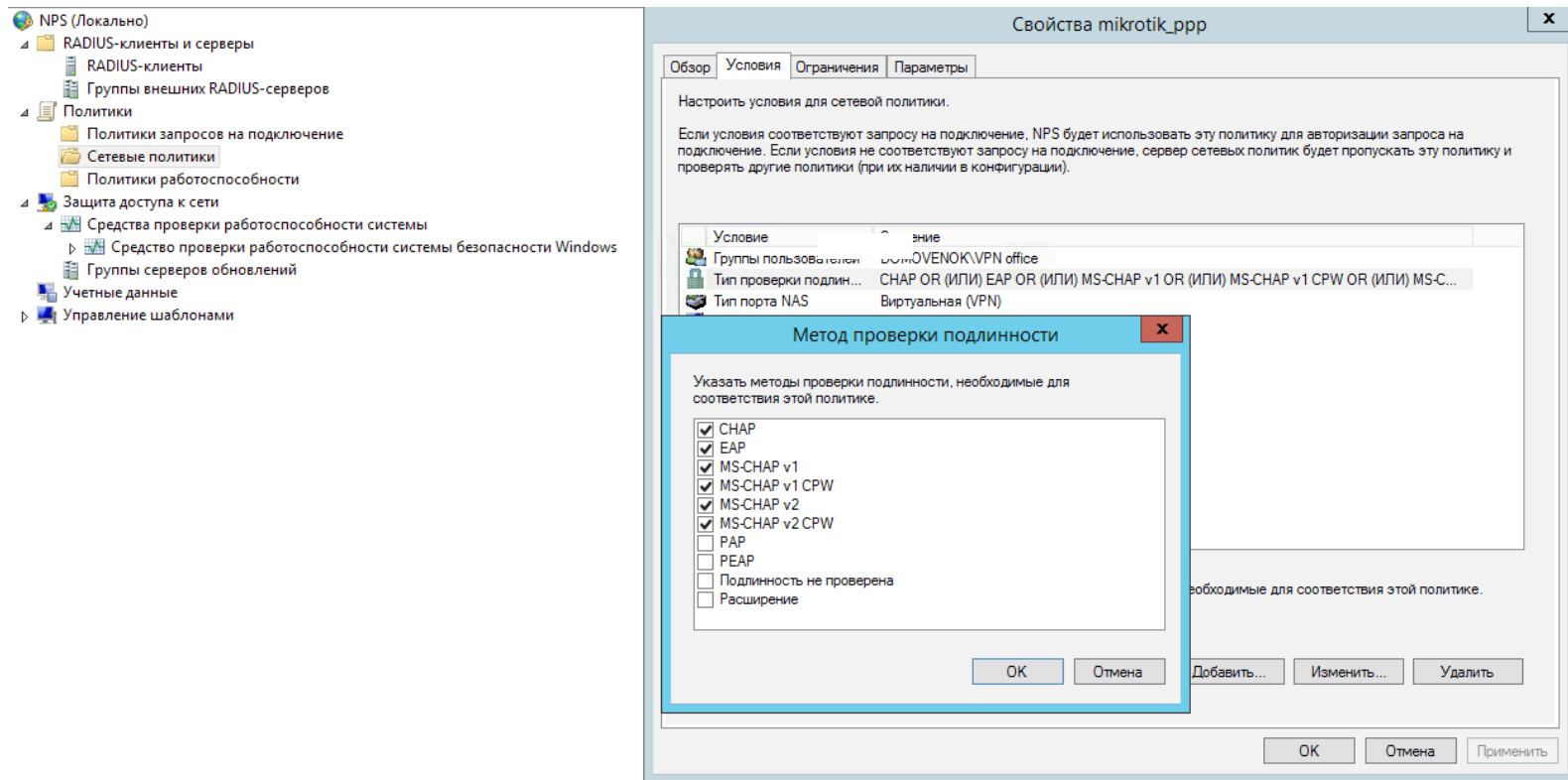
Метод - eap radius

Указываем сертификат сервера

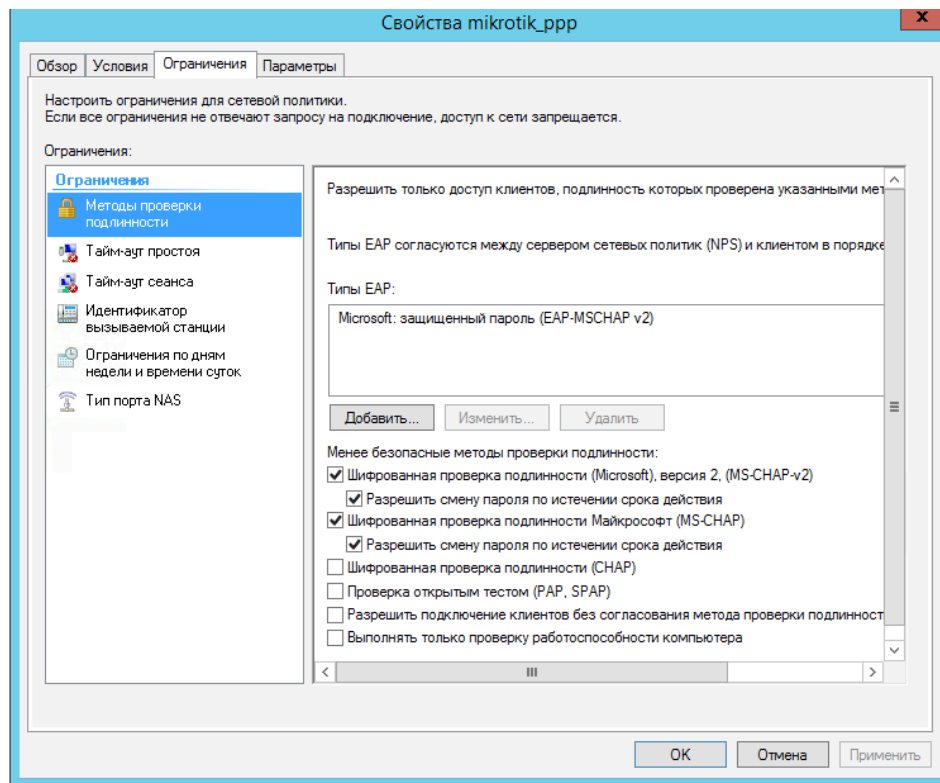
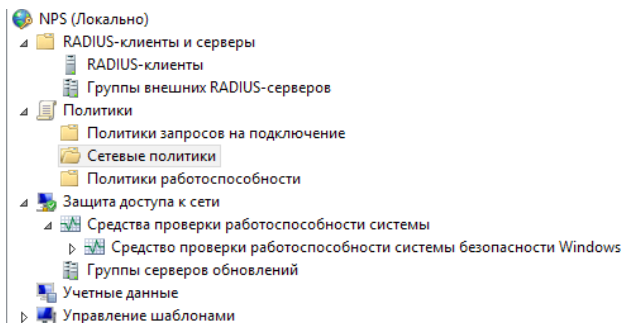
The screenshot shows the 'IPsec Identity <RW>' configuration window in WinBox. The 'Auth. Method' is set to 'eap radius' and the 'Certificate' field is highlighted with a blue selection bar. Red arrows from the text on the left point to these two fields. Other settings include 'Peer: RW', 'Policy Template Group: ikev2', 'My ID Type: auto', 'Remote ID Type: auto', 'Match By: remote id', 'Mode Configuration: RW', and 'Generate Policy: port strict'. The window has tabs for Policies, Proposals, Groups, Peers, Identities, Profiles, Remote Peers, Mode Configs, Installed SAs, and Keys. At the bottom, the status 'enabled' is shown.

#	Peer	Auth. Method	XAuth Login	Remote ID	Mode Configuration
1	RW	eap radius			RW

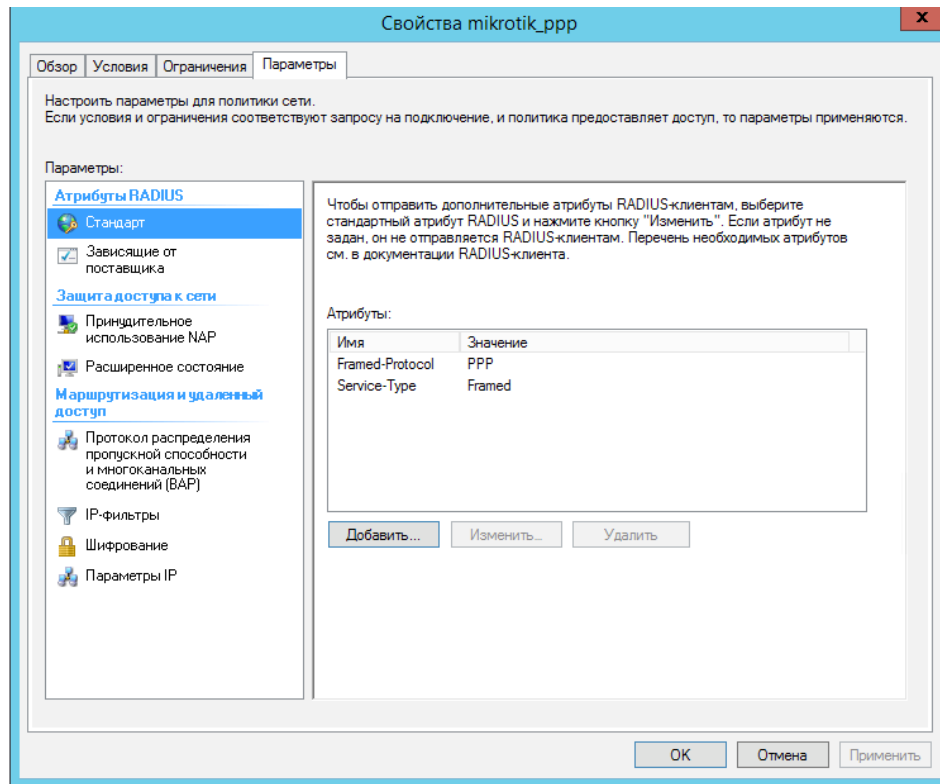
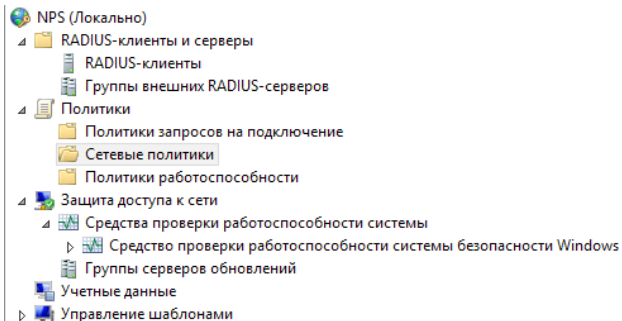
Windows Server NPS



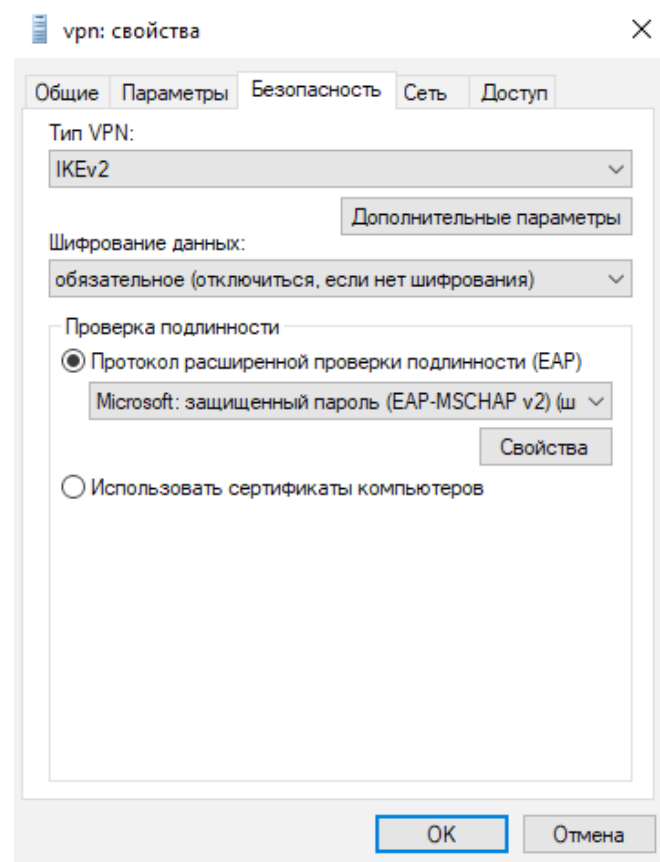
Windows Server NPS



Windows Server NPS



Windows Client



IPSec IKEv2 IOS/MacOS

17:50 100% LTE

Отменить Ikev2 Eap Готово

Тип IKEv2

Описание Ikev2 Eap

Сервер 1.1.1.1

Удаленный ID 1.1.1.1

Локальный ID name

АУТЕНТИФИКАЦИЯ

Аутент. польз. Имя пользователя >

Имя пользователя name

Пароль ••••

ПРОКСИ

Выкл. Вручную Авто

- Но это не работает
- Вариант обхода – apple configurator 2 – работает только на MacOS
- Или ручное создание .mobileconfig

MacOS/iOS

General
Mandatory

Restrictions
Not configured

Domains
Not configured

Global HTTP Proxy
Not configured

DNS Proxy
Not configured

Content Filter
Not configured

Certificates
1 Payload Configured

Passcode
Not configured

Wi-Fi
Not configured

VPN
1 Payload Configured

AirPlay
Not configured

AirPlay Security
Not configured

AirPrint
Not configured

Calendar
Not configured

Subscribed Calendars
Not configured

Contacts
Not configured

Exchange ActiveSync
Not configured

Google Account
Not configured

LDAP
Not configured

VPN

Connection Name
Display name of the connection (displayed on the device)
name-connect

Connection Type
Type of connection enabled by this policy
IKEv2

☐ Always-on VPN (supervised only)

Server
Host name or IP address for server
1.1.1.1

Remote Identifier
FQDN, UserFQDN, Address or ASN1DN remote identifier
1.1.1.1

Local Identifier
FQDN, UserFQDN, Address or ASN1DN local identifier
name

Machine Authentication
Authentication type for connection
None

Certificate Type
Type of the issued certificate (Machine Authentication only)
RSA

Server Certificate Issuer Common Name
Common name of the server certificate issuer
common.name.server

Server Certificate Common Name
Common name of the server certificate
common.name.server

☒ **Enable EAP**
Enable extended authentication

Disconnect on Idle
Disconnect after given time idle
Never

EAP Authentication
Authentication type for connection
Certificate

Identity Certificate
Credential for authenticating the connection
Add certificates in the Certificates payload

- Добавляем сертификат в конфигурацию
- Указываем identity сервера(FQDN) и клиента(common name)
- Так же заполняем поля **Server certificate Common name** – имя сертификата сервера

БЕСПЛАТНЫЙ ВЕБИНАР

IPSec

Презентация
<http://bit.ly/2HTuXn9>

<http://mikrotik-training.ru/webinar/>





linkmeup

УЧАСТВИЕ В ПОДКАСТЕ

LINKMEUP SYSADMINS



СПАСИБО ЗА ВНИМАНИЕ

<http://bit.ly/2HTuXn9>

Приходите на наши курсы по
Mikrotik и Asterisk

*Mikro***Tik**

