MikroTik

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, cmak, 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

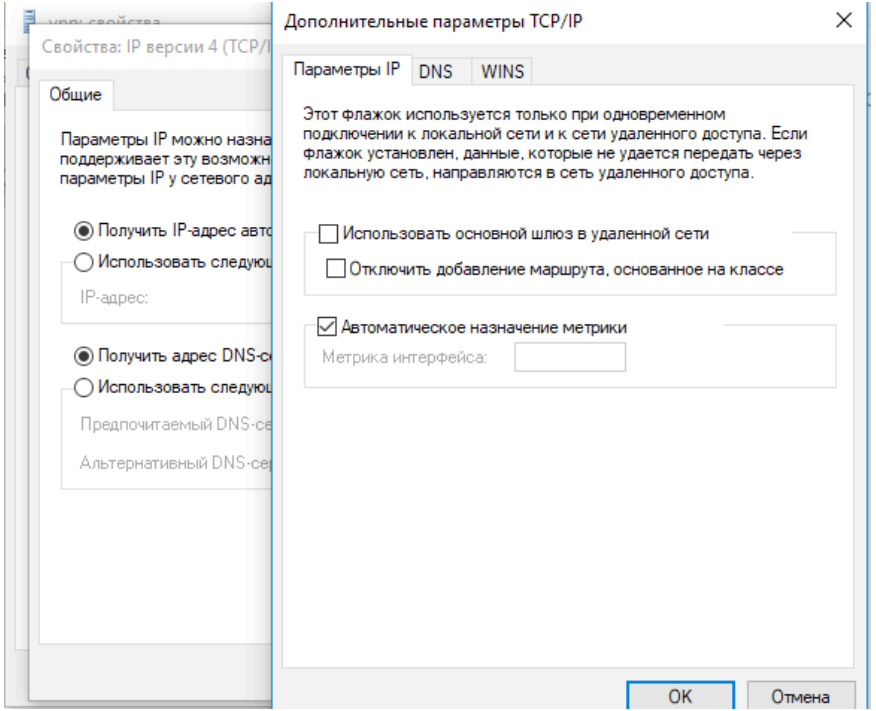
L2tp/PPTP/SSTP default gateway

Плюсы

- Легкая установка
- Полный контроль пользовательского трафика
- Мультиплатформенный

Минусы

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



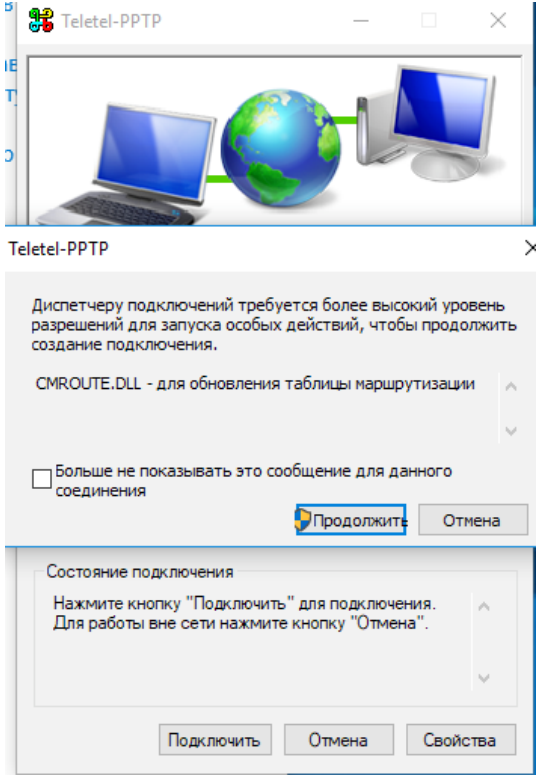
L2tp/PPTP/SSTP Cmak

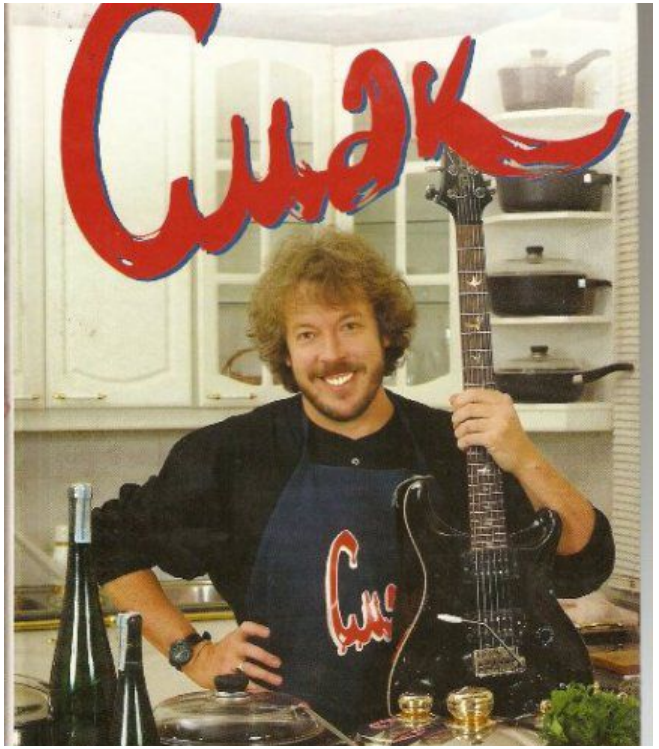
Плюсы

- легкая установка для пользователя

Минусы

- Требуются 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/Ovpn/IPseC классовая маршрутизация/VLSM

Плюсы

- Ничего прописывать не нужно на пользовательских OS
- 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

OpenVPN

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

IpSec split network

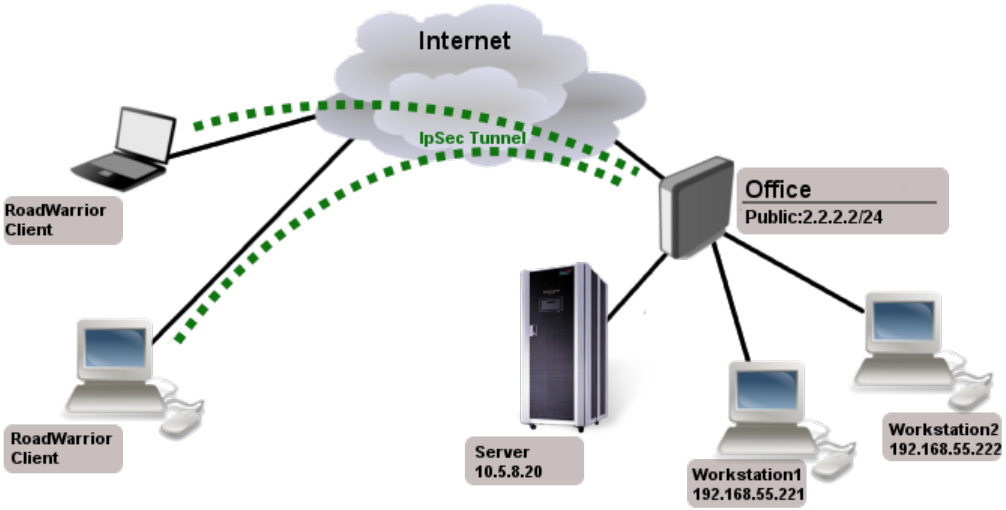
Плюсы

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

Минусы

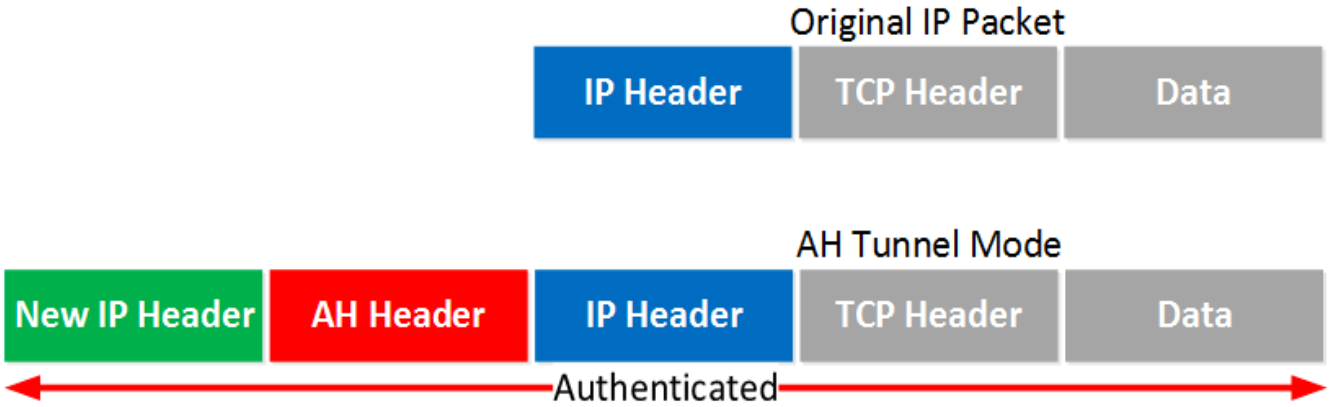
- Сложно настраивать
- Отсутствует интерфейс в routerOS
- Нет прямой связи с маршрутизацией
- Есть недоработки в пользовательских ОС

Схема подключения клиентов



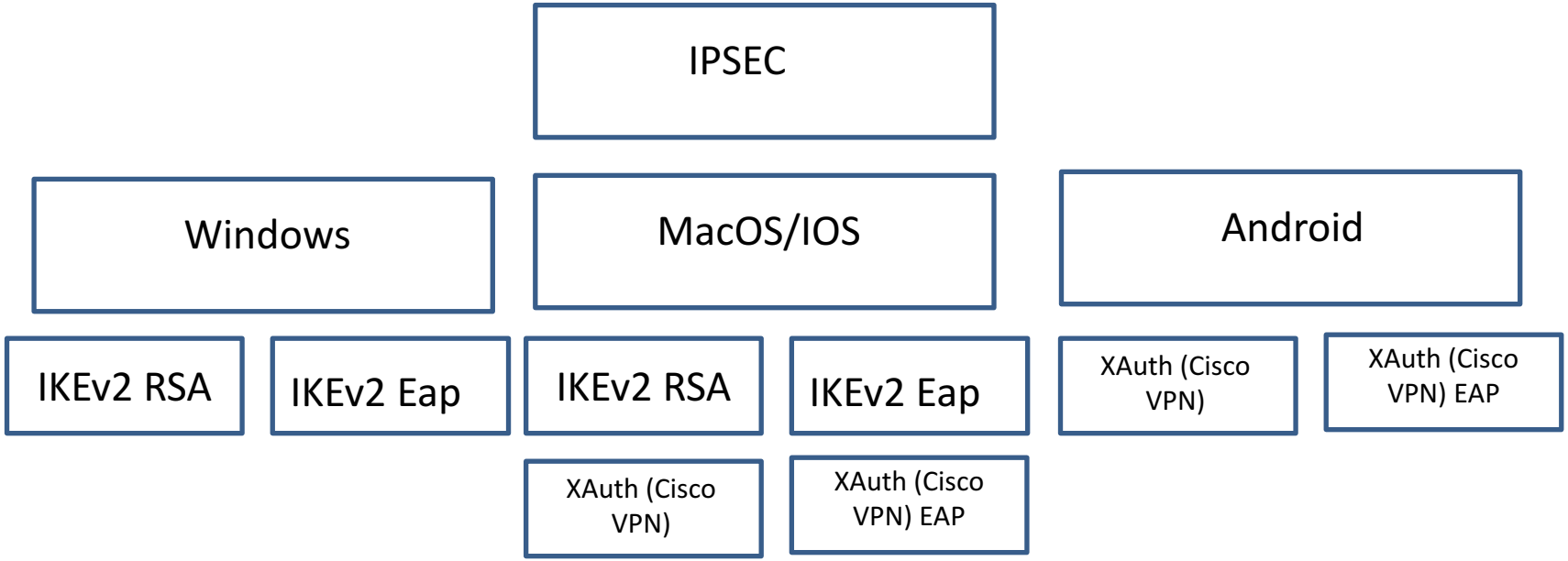
- Internet Protocol Security (IPsec) - это набор протоколов для защиты обмена пакетами через незащищенные сети IP / IPv6, такие как Интернет.
- Ipsec можно использовать как способ подключения клиентских устройств в сеть предприятия
- По сути это туннельный ipsec на пользователя
- Политики генерируются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

Ipsec tunnel mode

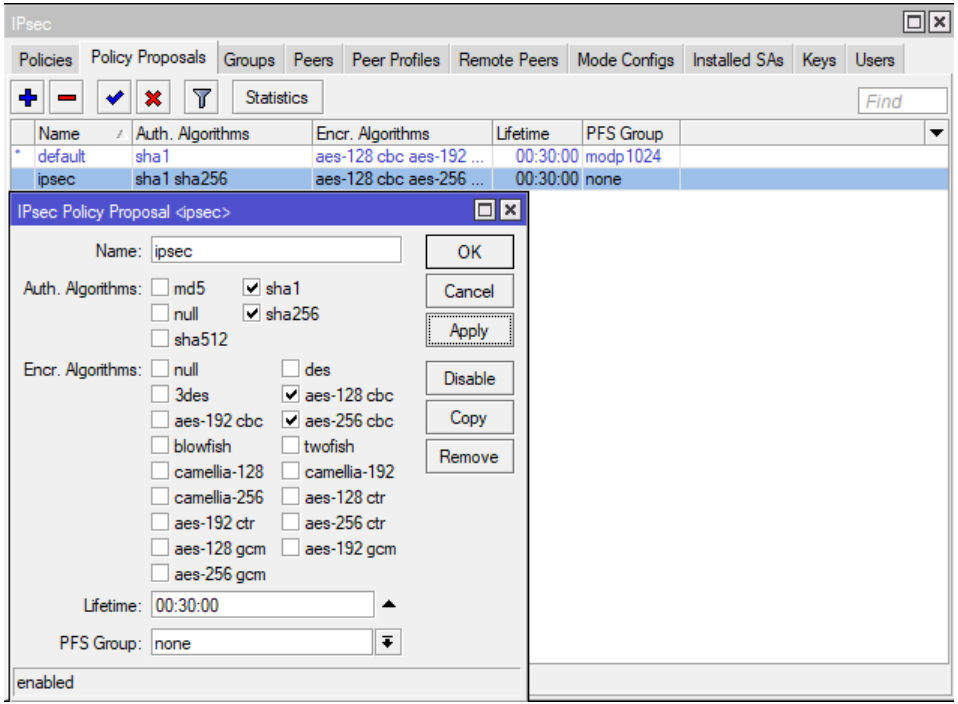


- Пакет который мы планируем передать попадает под условия ipsec policy и после этого происходит добавление нового IP заголовка.
- В этом режиме IPSEC выступает в режиме переносчика трафика.
- Не будут работать протоколы маршрутизации.
- Оригинальный заголовок IP теперь также зашифрован.

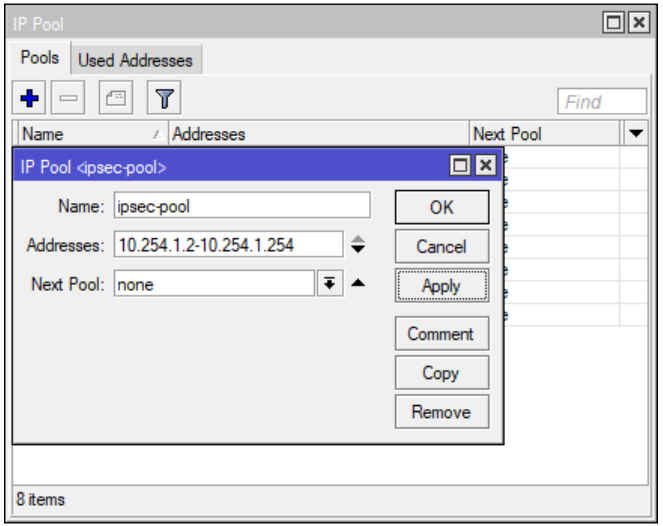
Варианты подключения ipsec для разных операционных систем



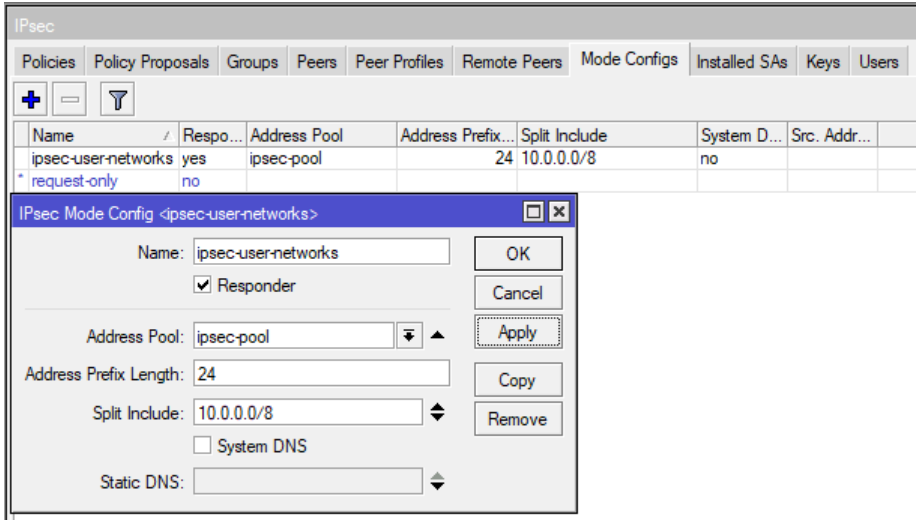
IPSec Policy Proposals (phase 1)



IP pool

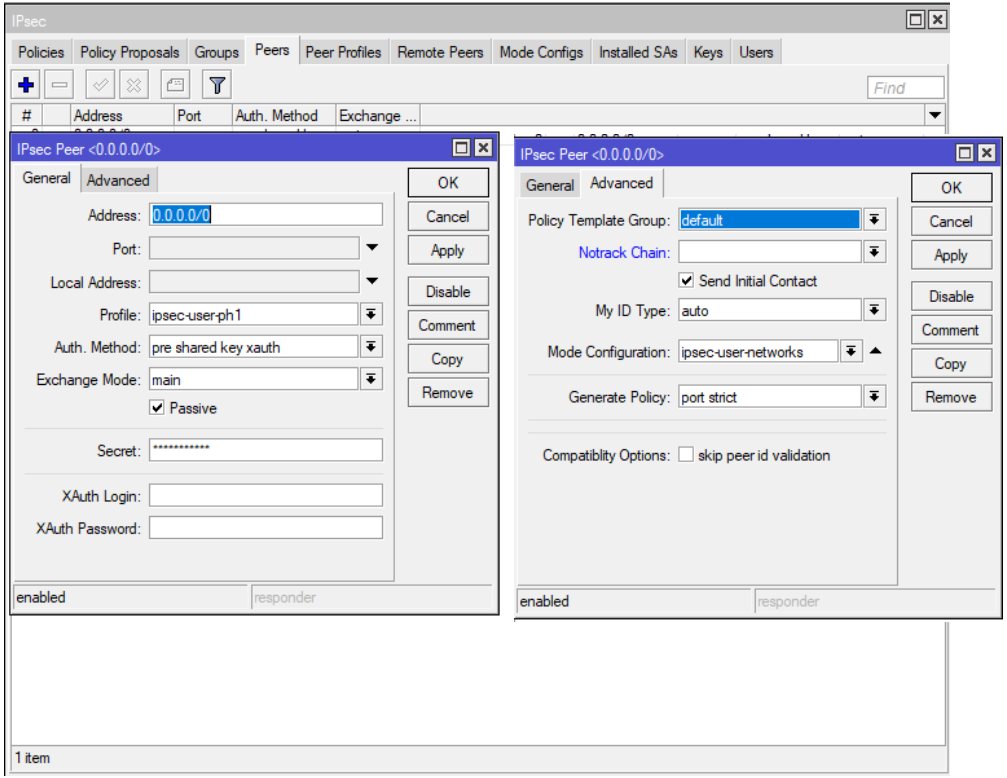

IP Pool
Pools
Used Addresses
Find
Name
Addresses
Next Pool
IP Pool <ipsec-pool>
Name: ipsec-pool
Addresses: 10.254.1.2-10.254.1.254
Next Pool: none
OK
Cancel
Apply
Comment
Copy
Remove
8 items

IPSec Mode Configs

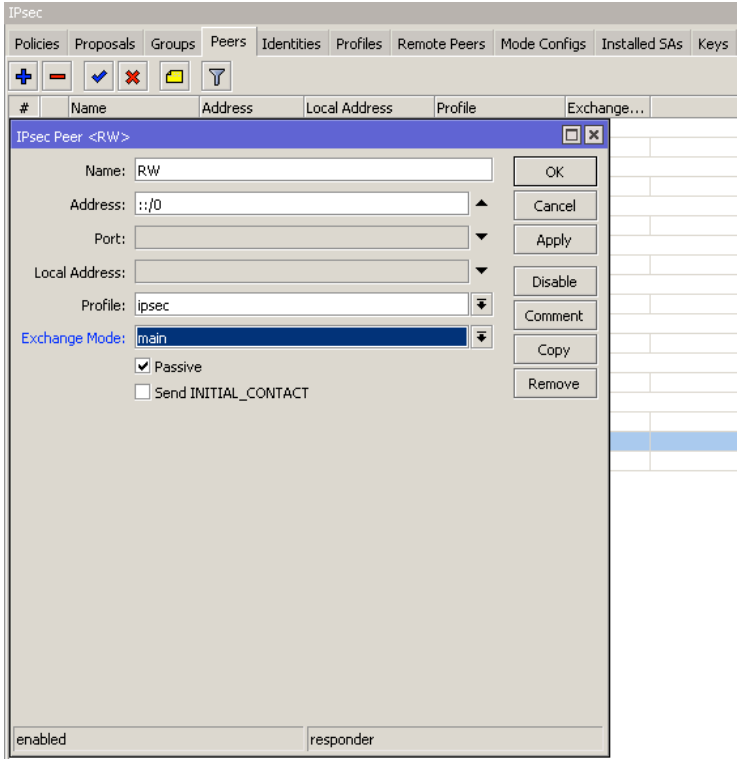


IPSec Peer

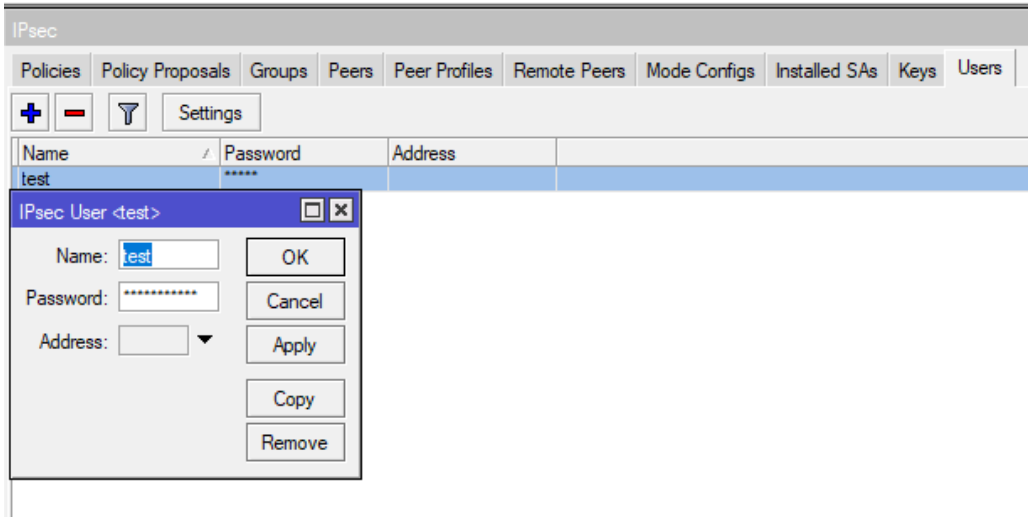
До 6.44

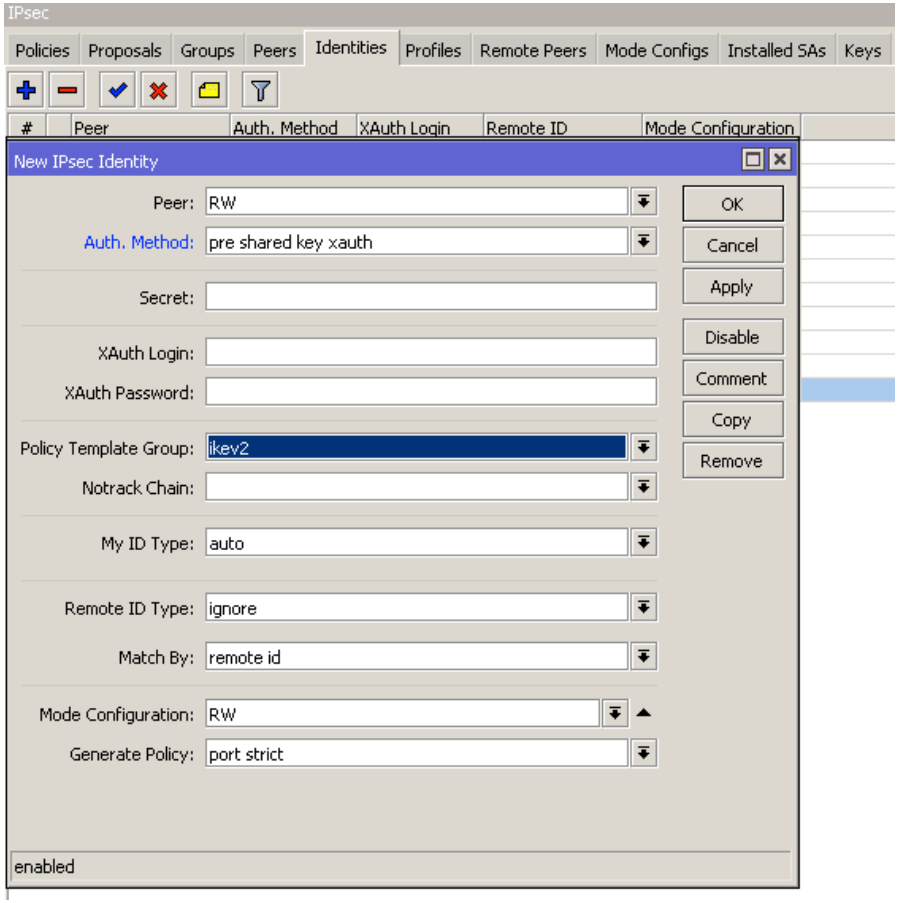


После 6.44



IPSec Users – до 6.44



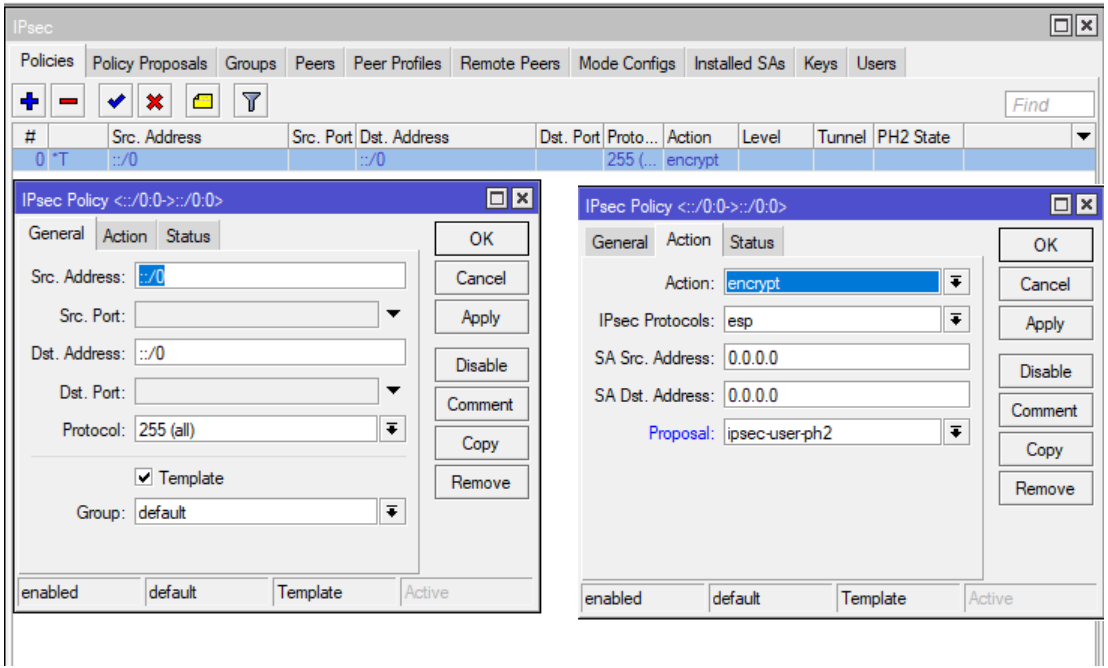


После 6.44

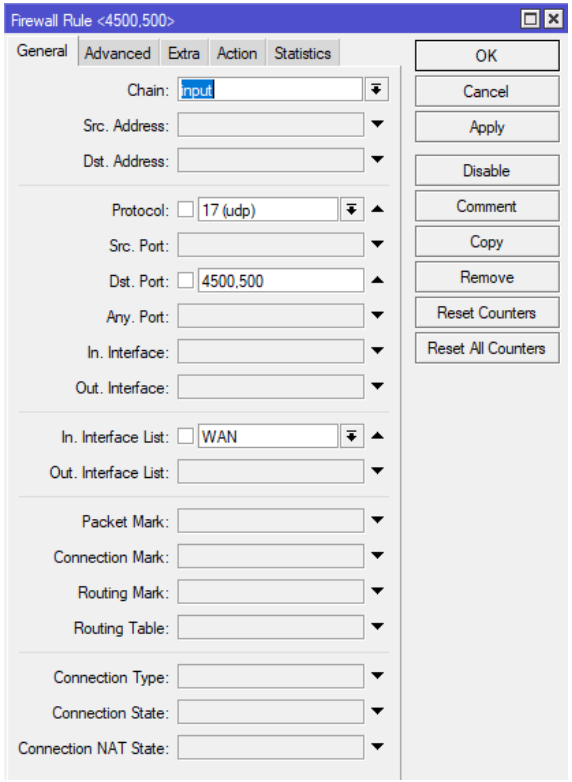
Режим авторизации pre shared key Xauth (Cisco VPN – в macOS/IOS)

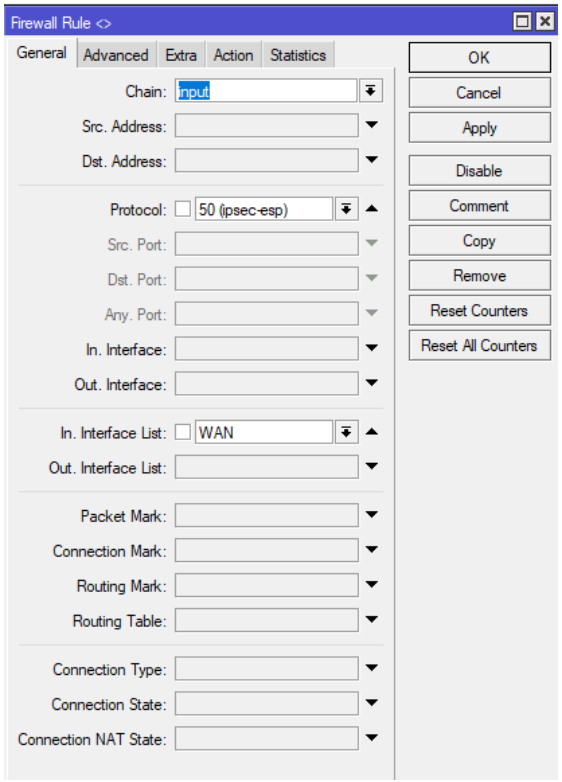
- С версии 6.44 настройка пользователей перенесена в раздел
- /ip ipsec identity
- Для preshared key xauth – необходим режим работы ipsec peers main

IPSec Policies

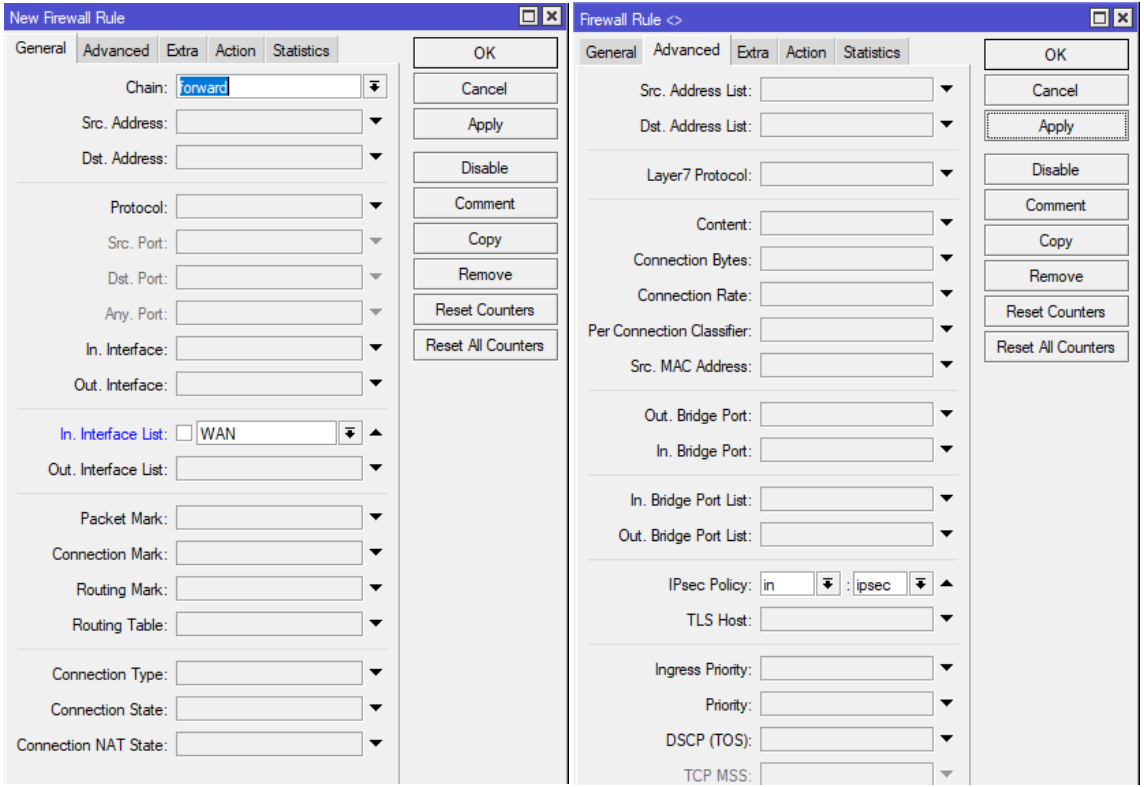


IP firewall filter

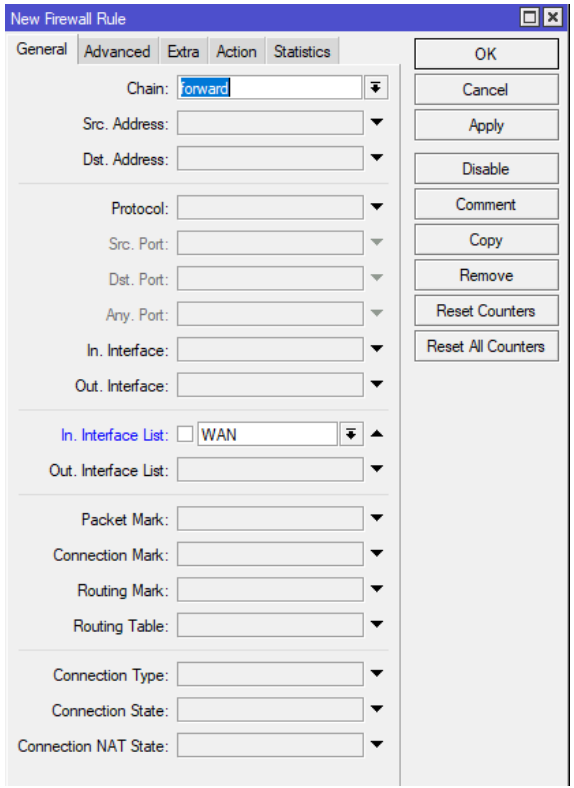


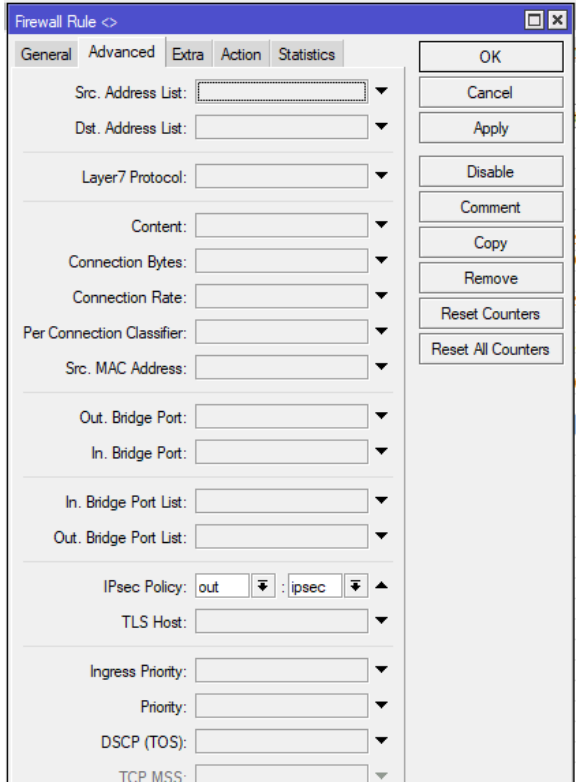


IP firewall filter

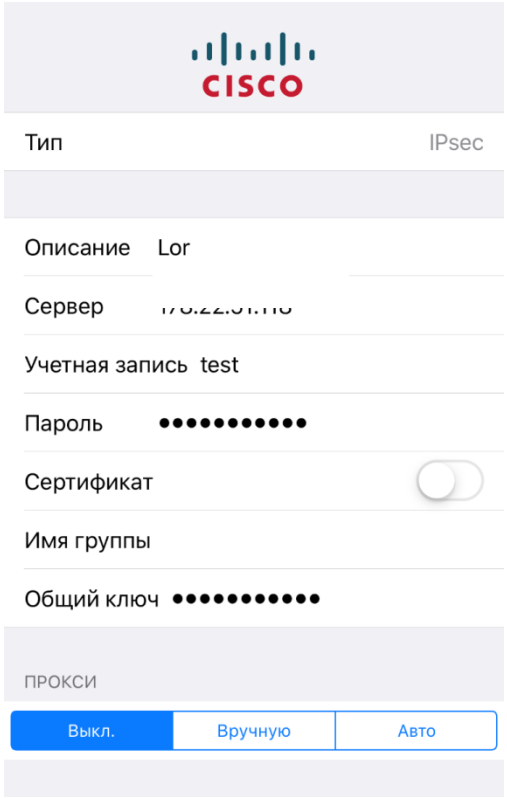


IP firewall filter





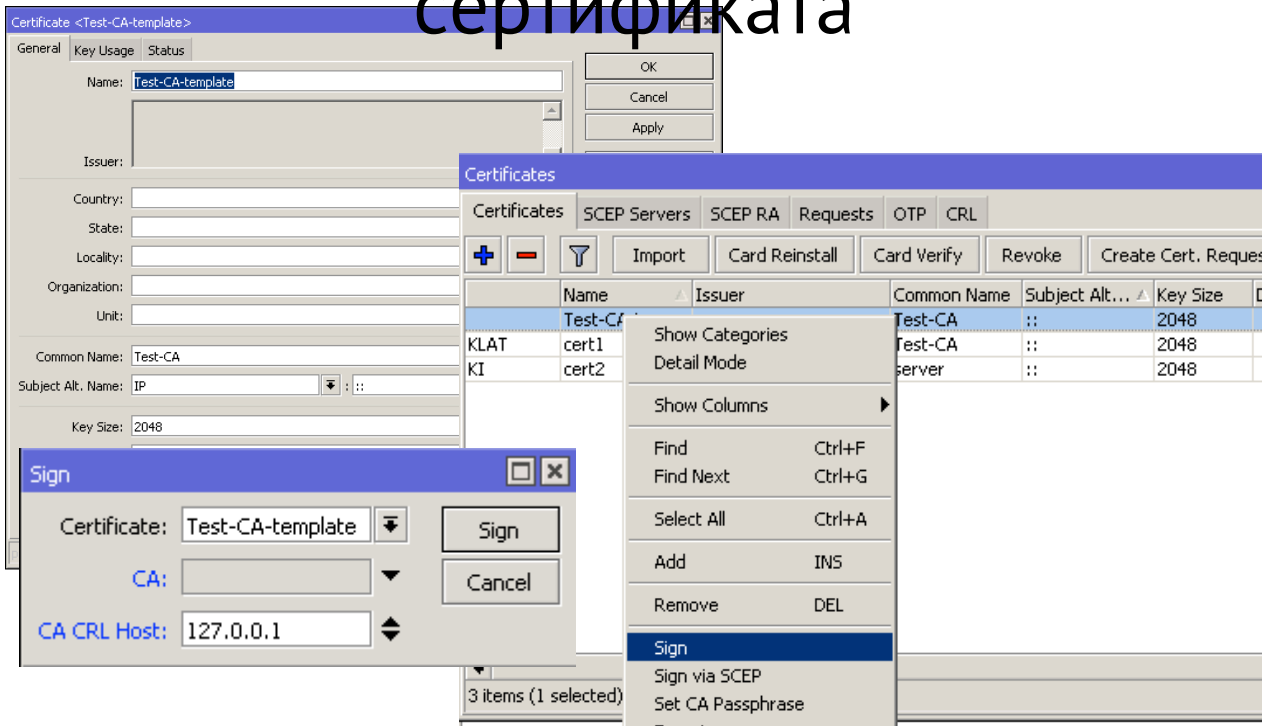
Настройка Ipsec X-auth на IOS



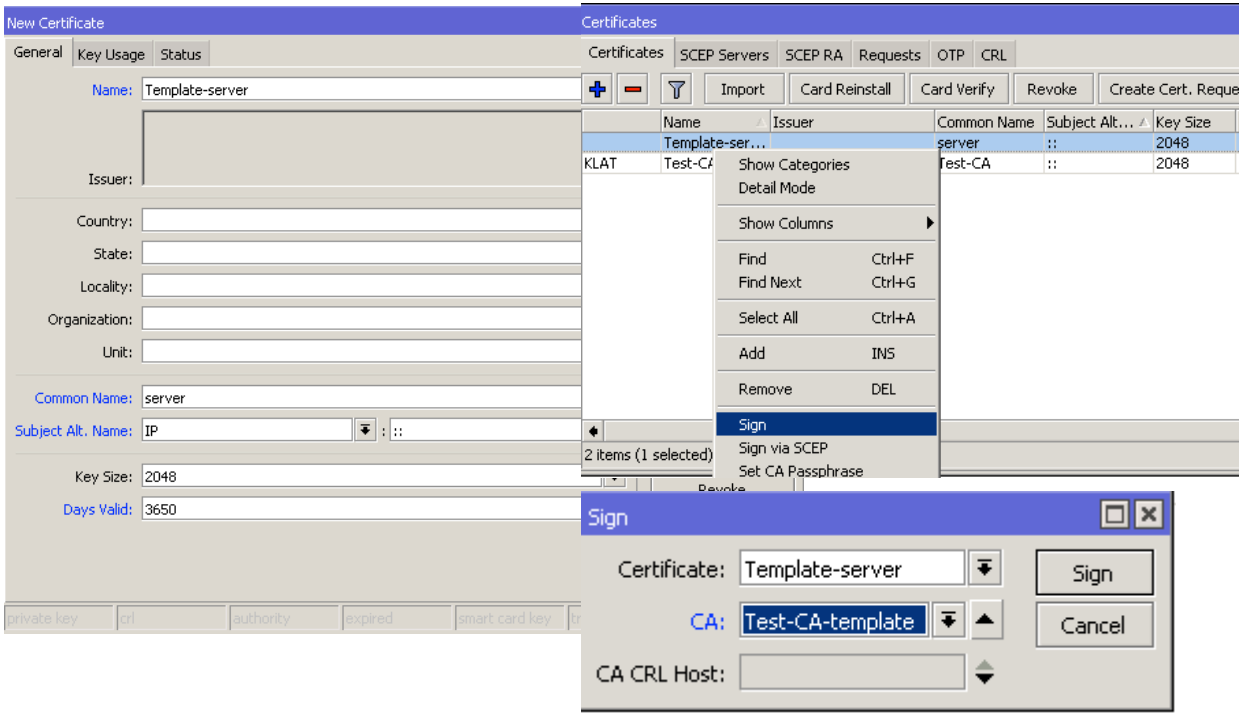
IKEv2 RFC7296

- 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 перегенерации 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

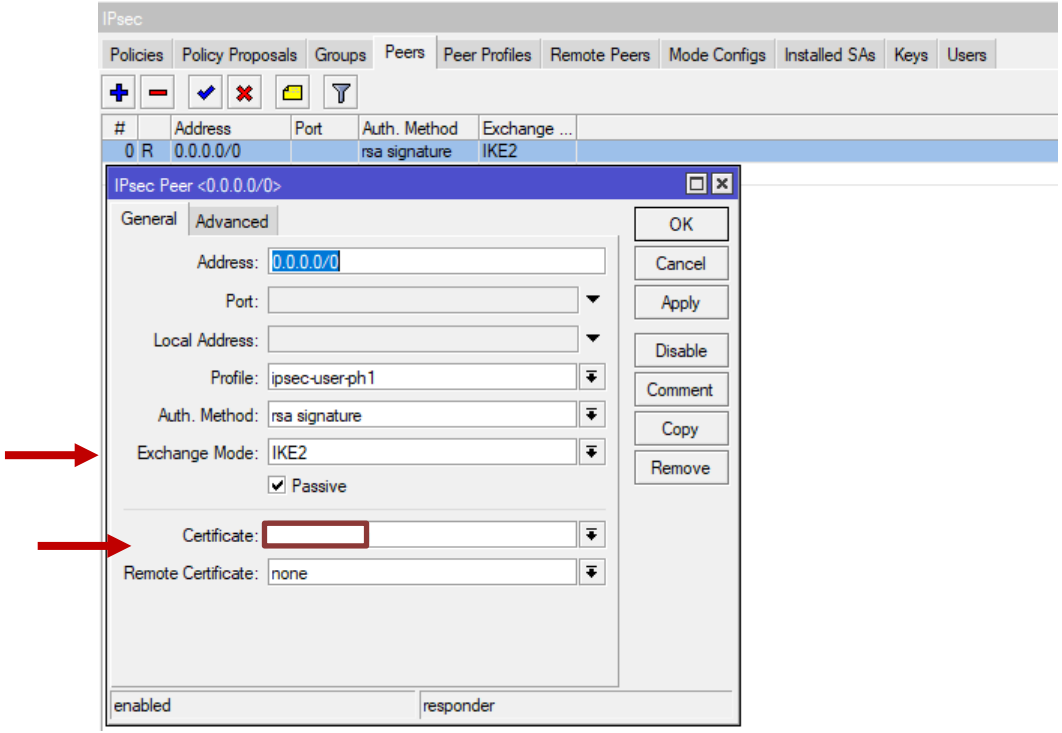


Common name – желательно dns имя сервера

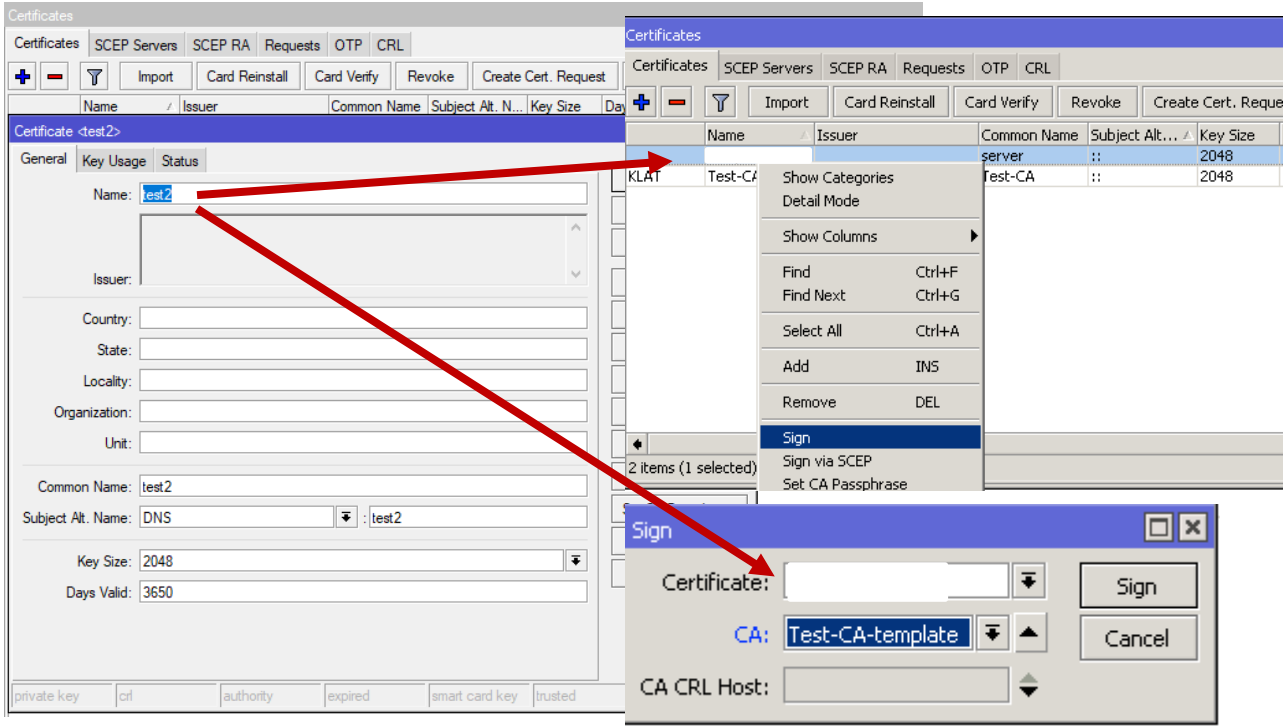
Sybject Alt. Name – dns имя сервера

Key usgate – tls server

IPSec IKEv2

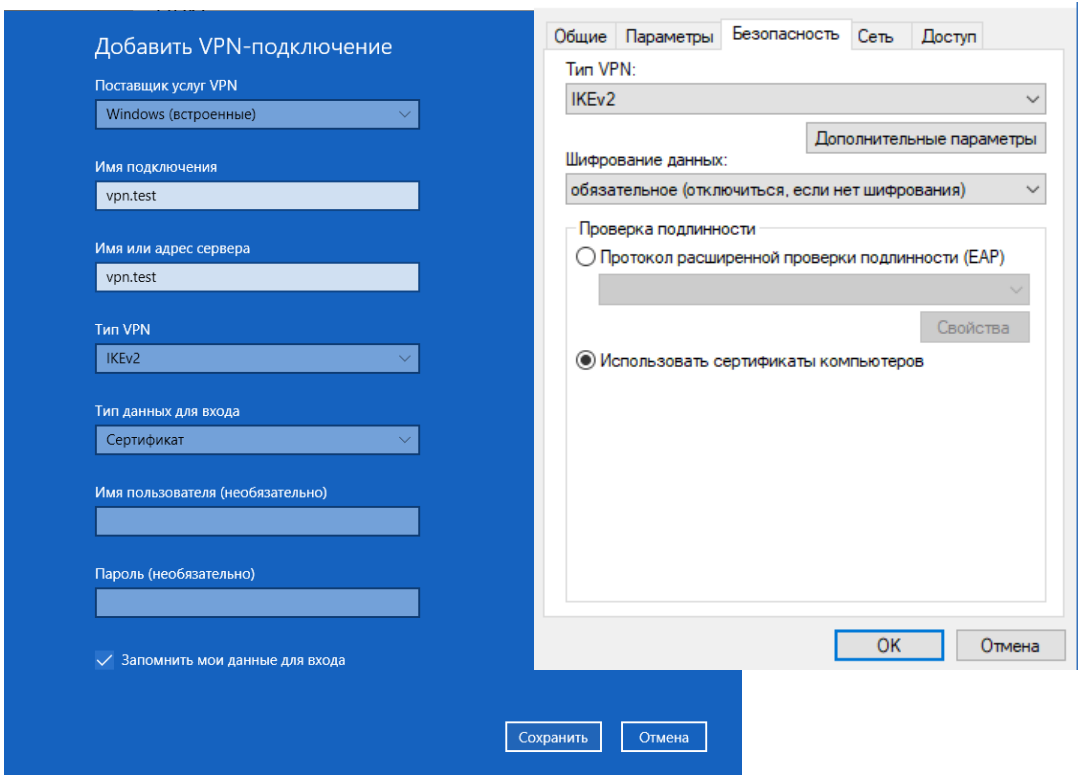

IPsec
Policies
Policy Proposals
Groups
Peers
Peer Profiles
Remote Peers
Mode Configs
Installed SAs
Keys
Users
Address Port Auth. Method Exchange ...
0 R 0.0.0.0/0 rsa signature IKE2
IPsec Peer <0.0.0.0/0>
General
Advanced
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Address: 0.0.0.0/0
Port:
Local Address:
Profile: ipsec-user-ph1
Auth. Method: rsa signature
Exchange Mode: IKE2
Passive
Certificate:
Remote Certificate: none
enabled
responder

IPSec IKEv2 создание сертификата клиента

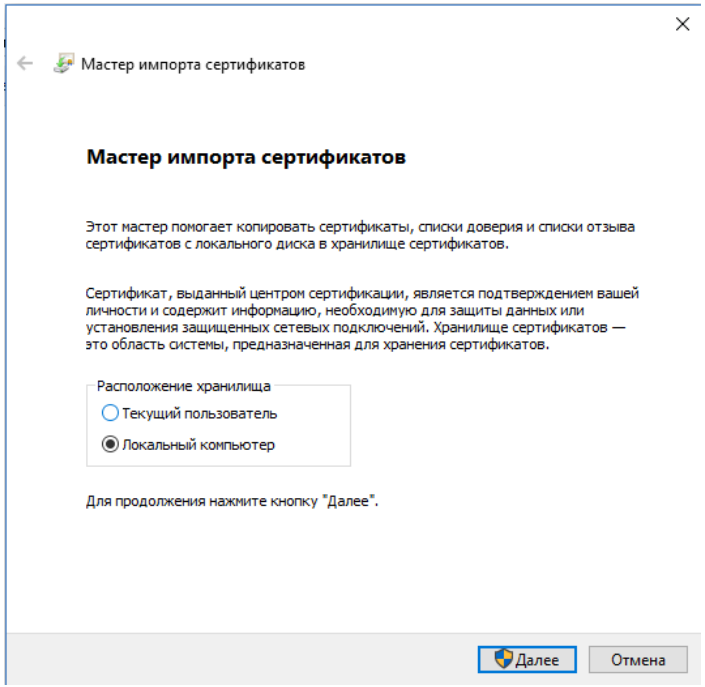


Key Usgate – tls user

IPSec IKEv2 настройка на Windwos



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

BAT 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
- Отключиченное расширенную проверку сертификатов, добавьте параметр типа DWORD под именем "DisableIKENameEkuCheck" в следующий путь реестра VPN-клиента.
- reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters" /v DisableIKENameEkuCheck /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
[redacted]	[redacted]	On-link	10.253.2.10	281
[redacted]	[redacted]	10.211.55.1	10.211.55.3	26
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
169.254.255.255	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

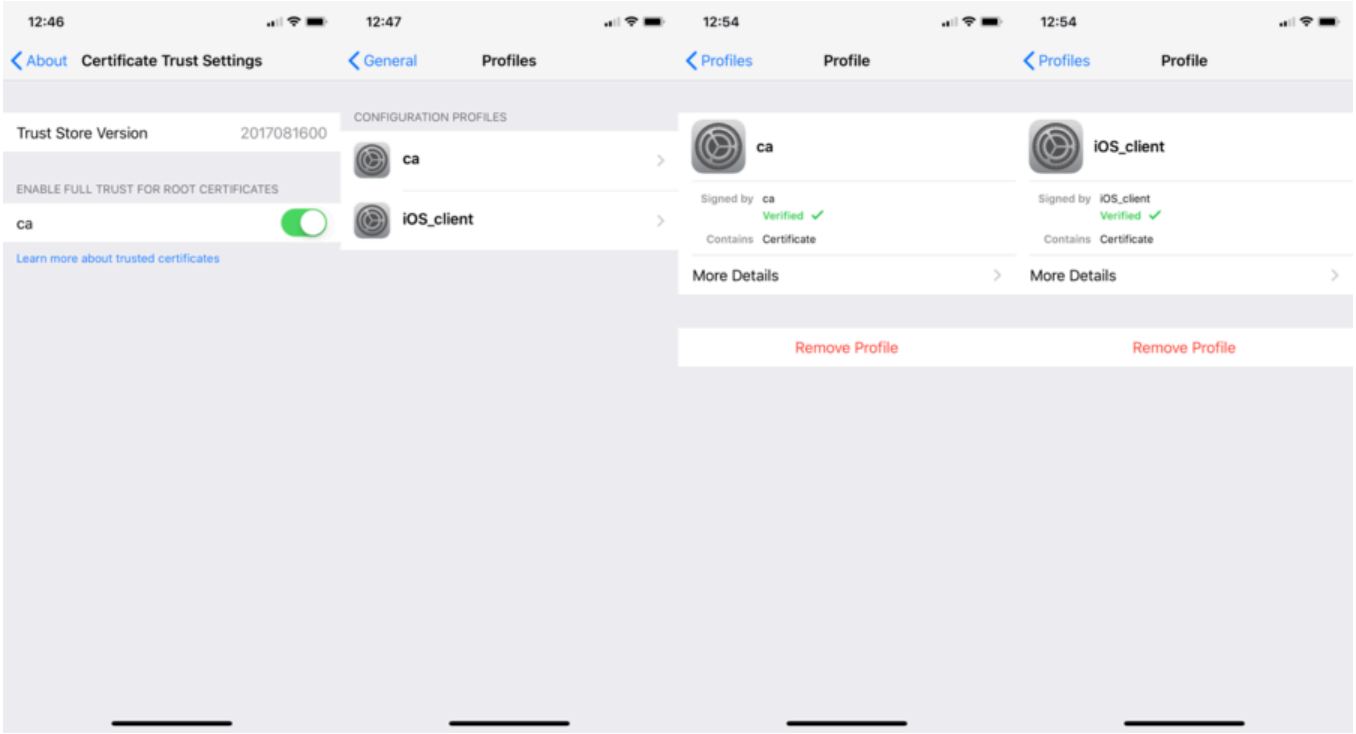
Постоянные маршруты:
Отсутствует

Маршруты у клиента macOS

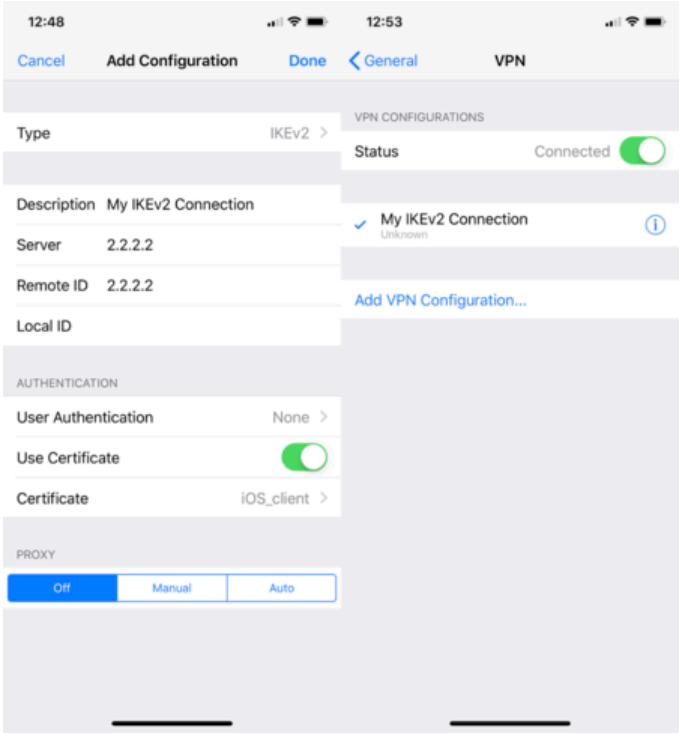
```
Internet:
Destination        Gateway            Flags        Refs      Use   Netif Expire
default            192.168.191.1      UGSc          100        0     en0
default            192.168.191.1      UGScI           1        0     en5
default            link#17            UCSI            2        0 ipsec0
10                 10.253.2.11        UGSc            0        0 ipsec0
10.37.129/24       link#16            UC              1        0   vnic1      !
10.211.55/24       link#15            UC              1        0   vnic0      !
10.253.2.11        10.253.2.11        UH              6        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      !
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

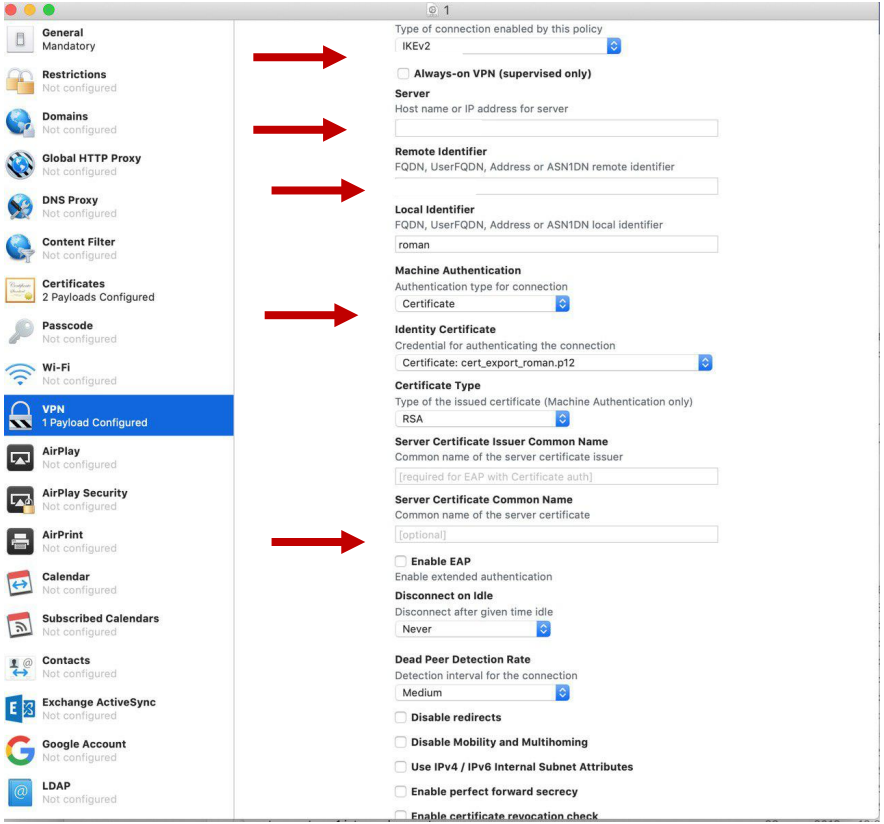

12:46
About
Certificate Trust Settings
Trust Store Version
2017081600
ENABLE FULL TRUST FOR ROOT CERTIFICATES
ca
Learn more about trusted certificates
12:47
General
Profiles
CONFIGURATION PROFILES
ca
iOS_client
12:54
Profiles
Profile
ca
Signed by ca
Verified
Contains Certificate
More Details
Remove Profile
12:54
Profiles
Profile
iOS_client
Signed by iOS_client
Verified
Contains Certificate
More Details
Remove Profile

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

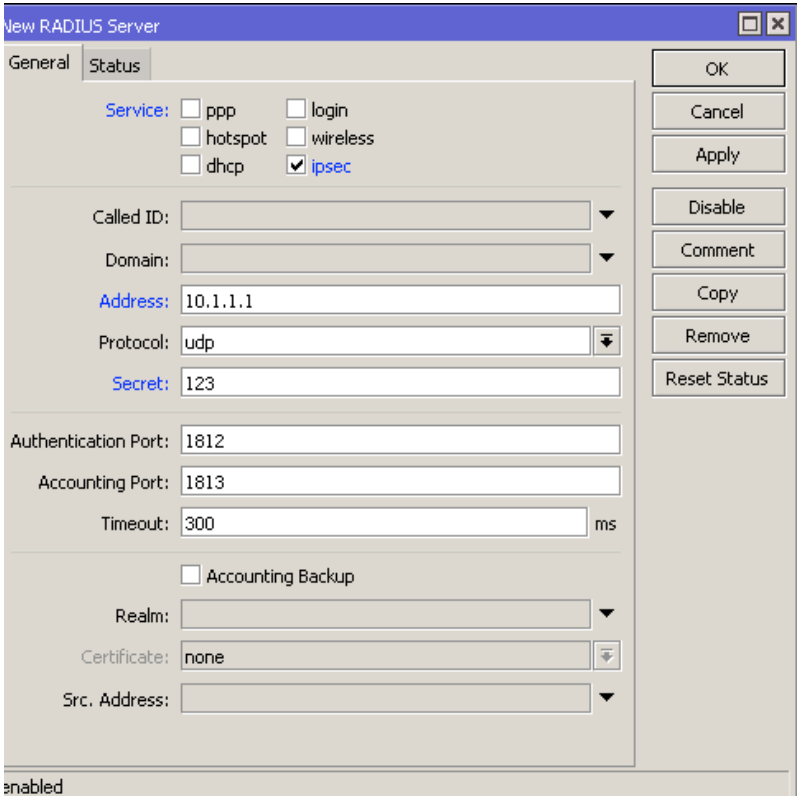
IPSec IKEv2



- 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

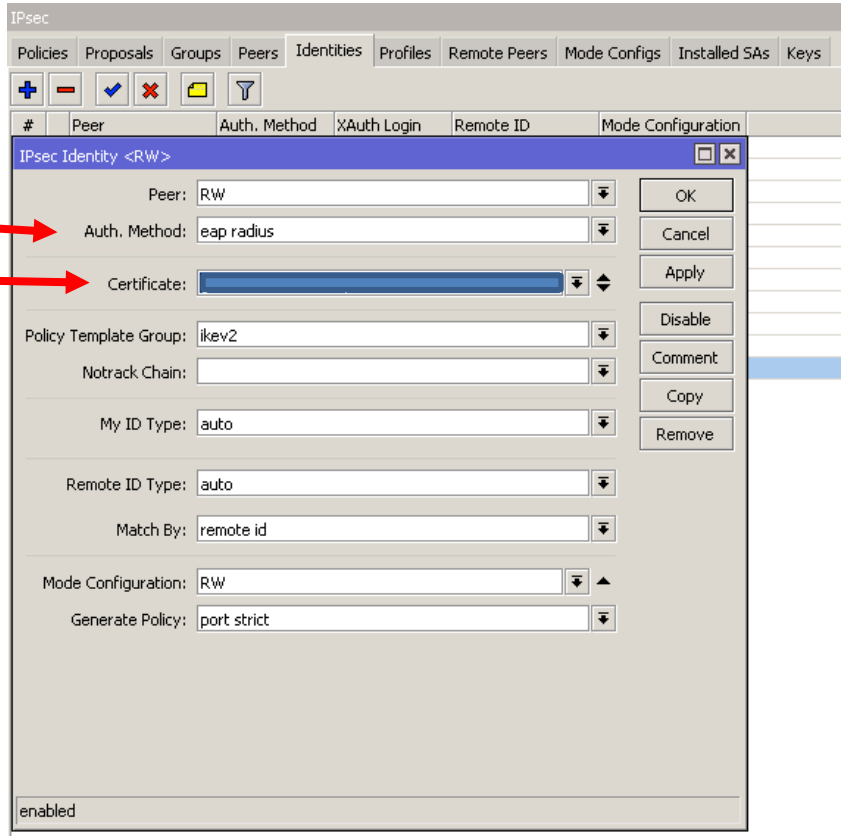
- Mikrotik User-Manager не поддерживает EAP method
- Используем Windows Server NPS
- FreeRadius



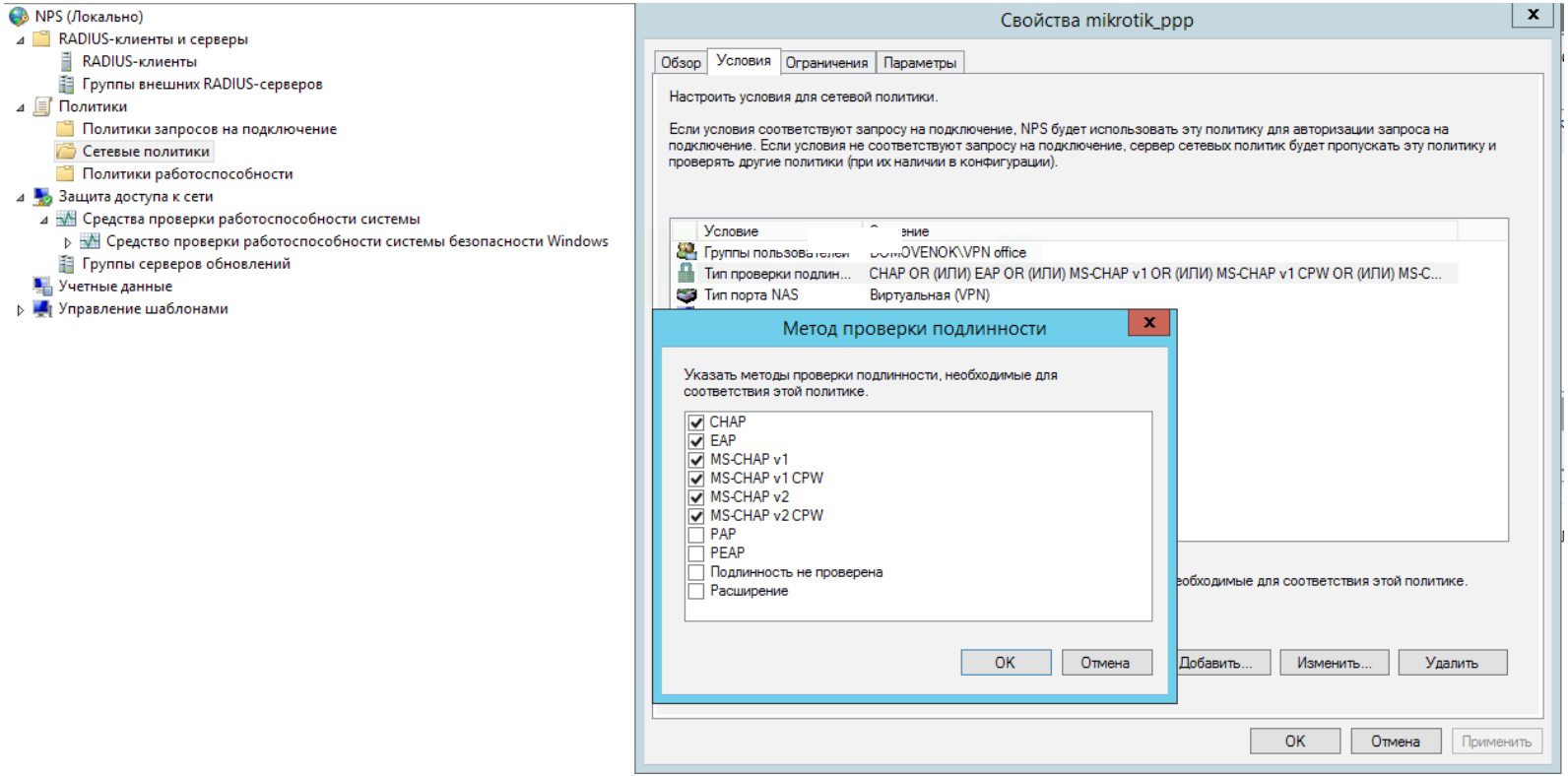
IPSec IKEv2 + EAP

Метод - eap radius

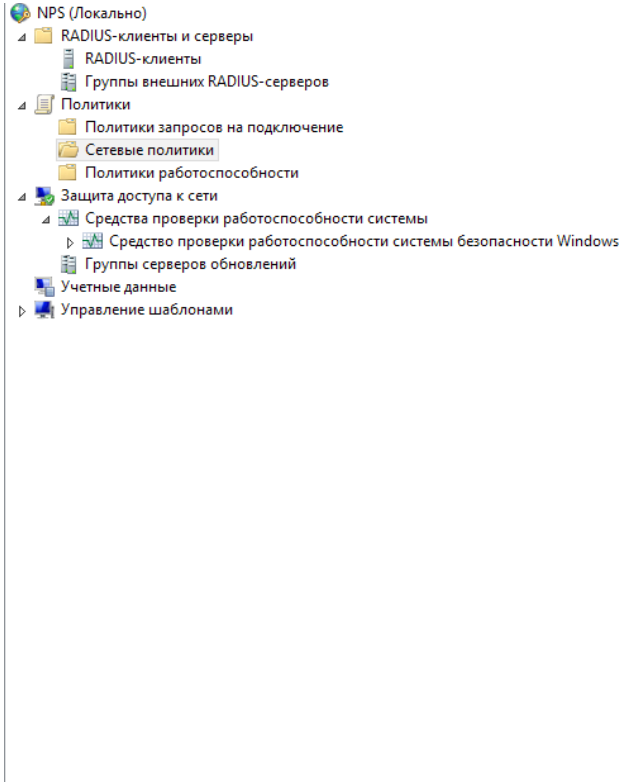
Указываем сертификат сервера

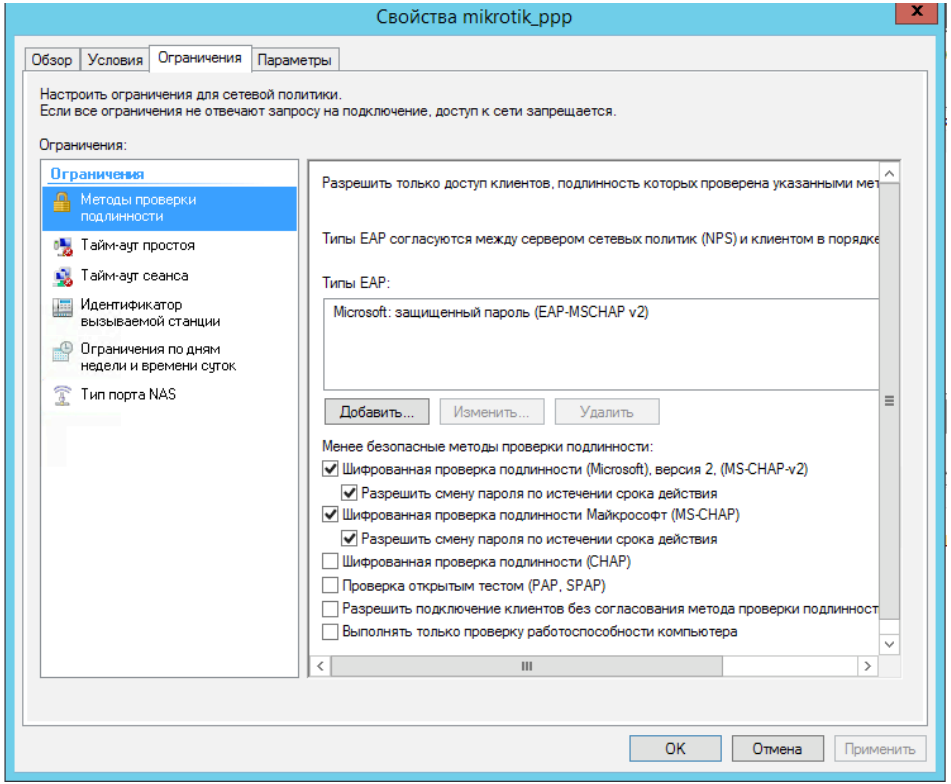


Windows Server NPS

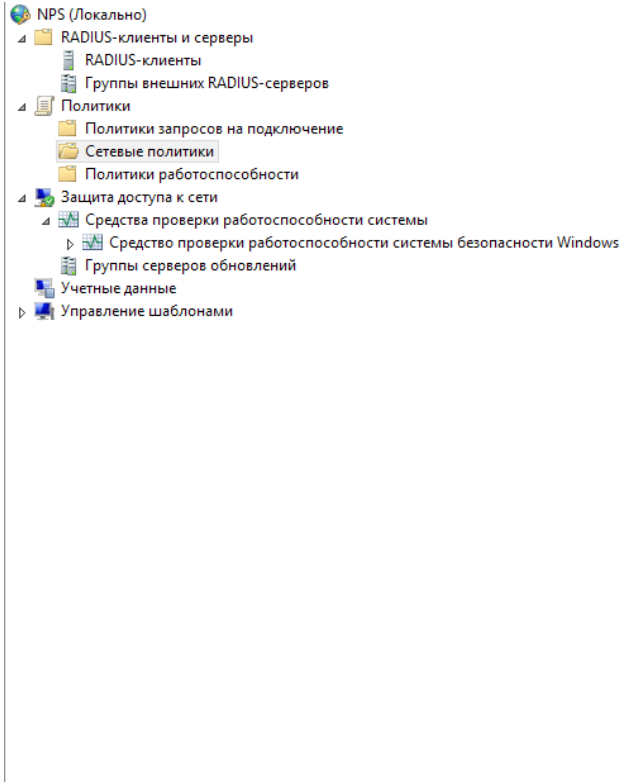


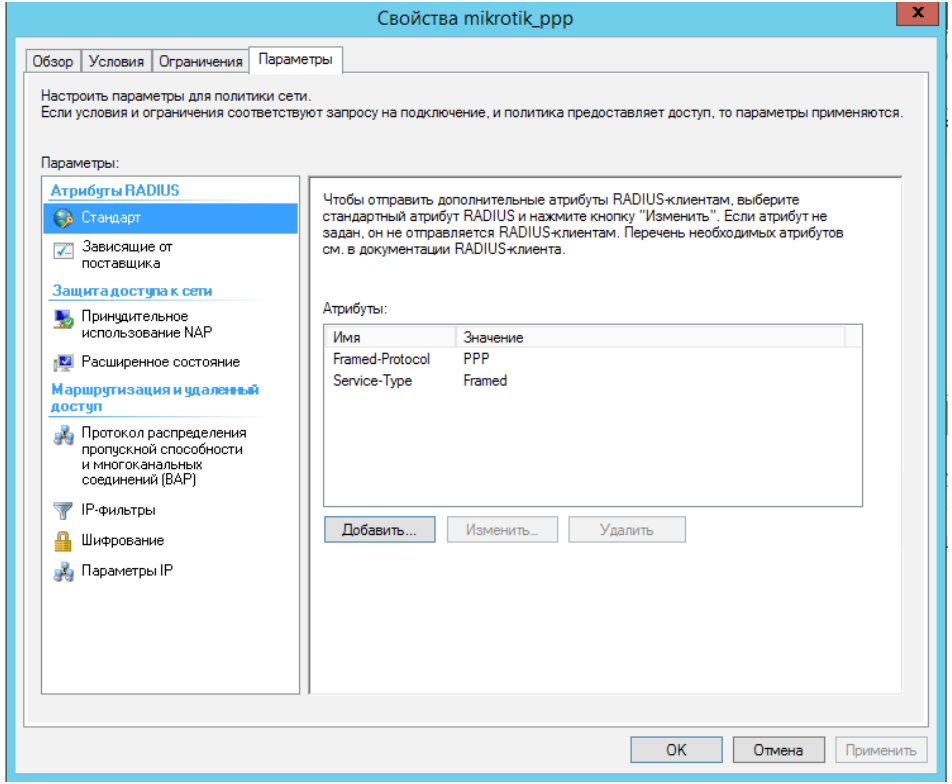
Windows Server NPS



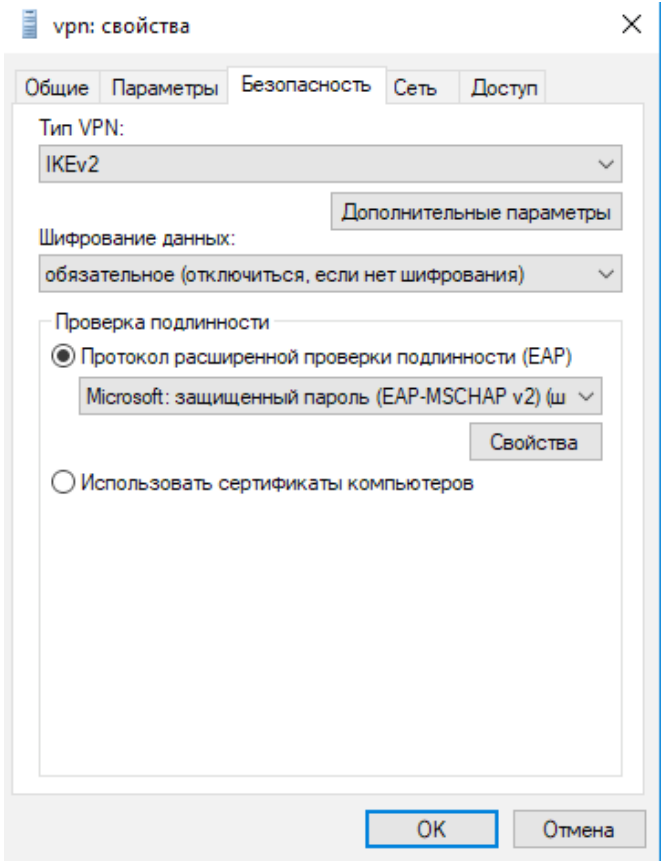


Windows Server NPS

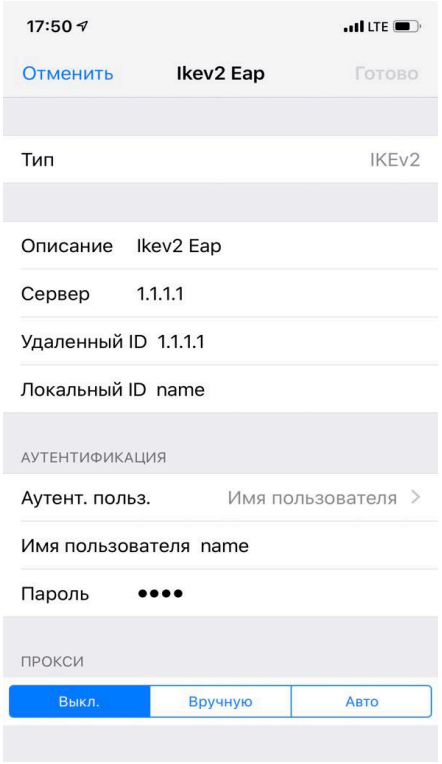




Windows Client

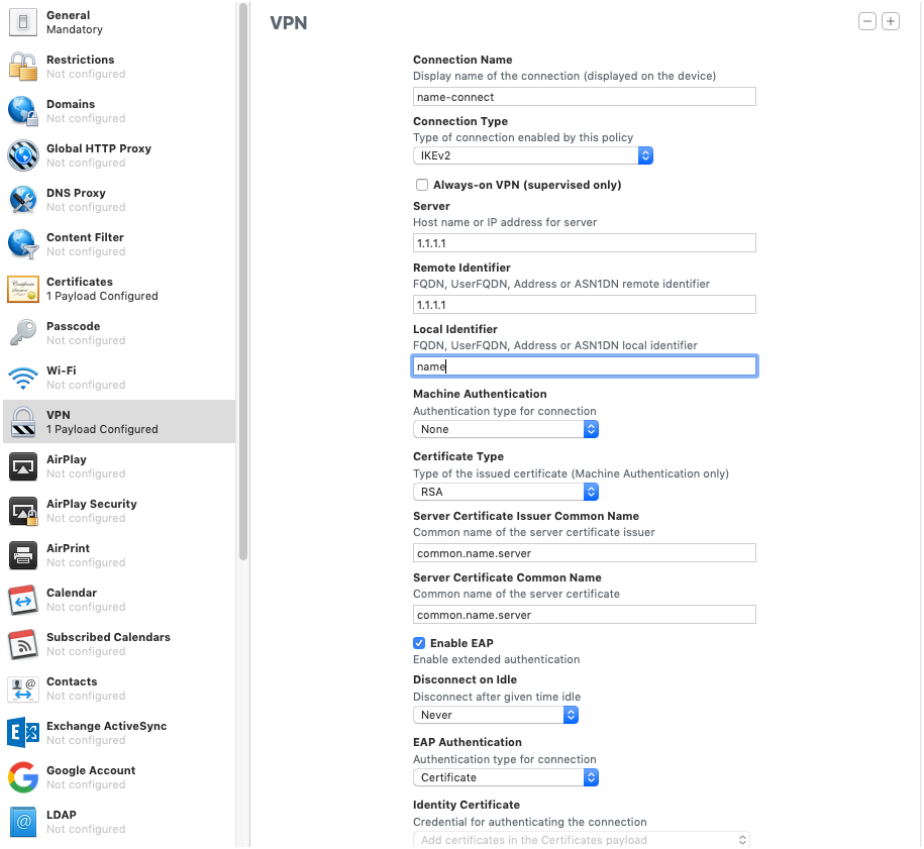


IPSec IKEv2 IOS/MacOS



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

MacOS/IOS

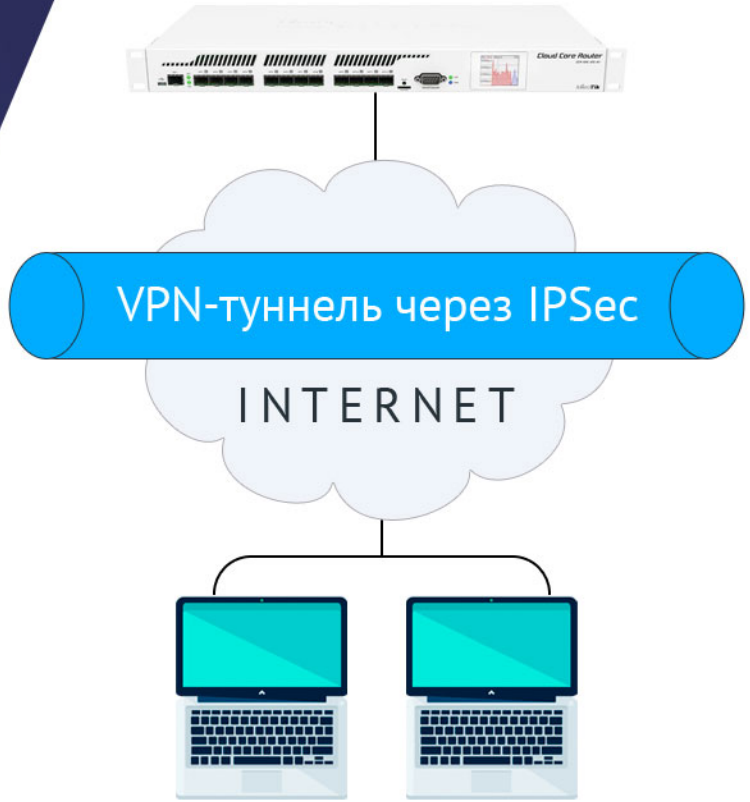


- Добавляем сертификат в конфигурацию
- Указываем identity сервера(FQDN) и клиента(common name)
- **Так же заполняем поля Server certificate Common name – имя сертификата сервера**

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