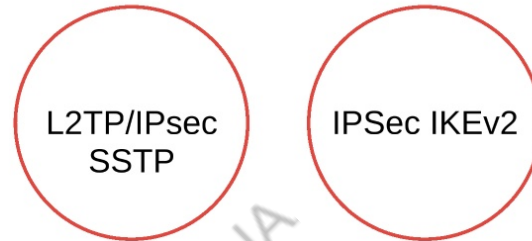


# MikroTik Certified Security Engineer

MTCSE

*Chapter 7:  
SECURE  
TUNNELS for  
Clients (road  
warrior)*



MTI-GROUP LLC / network academy

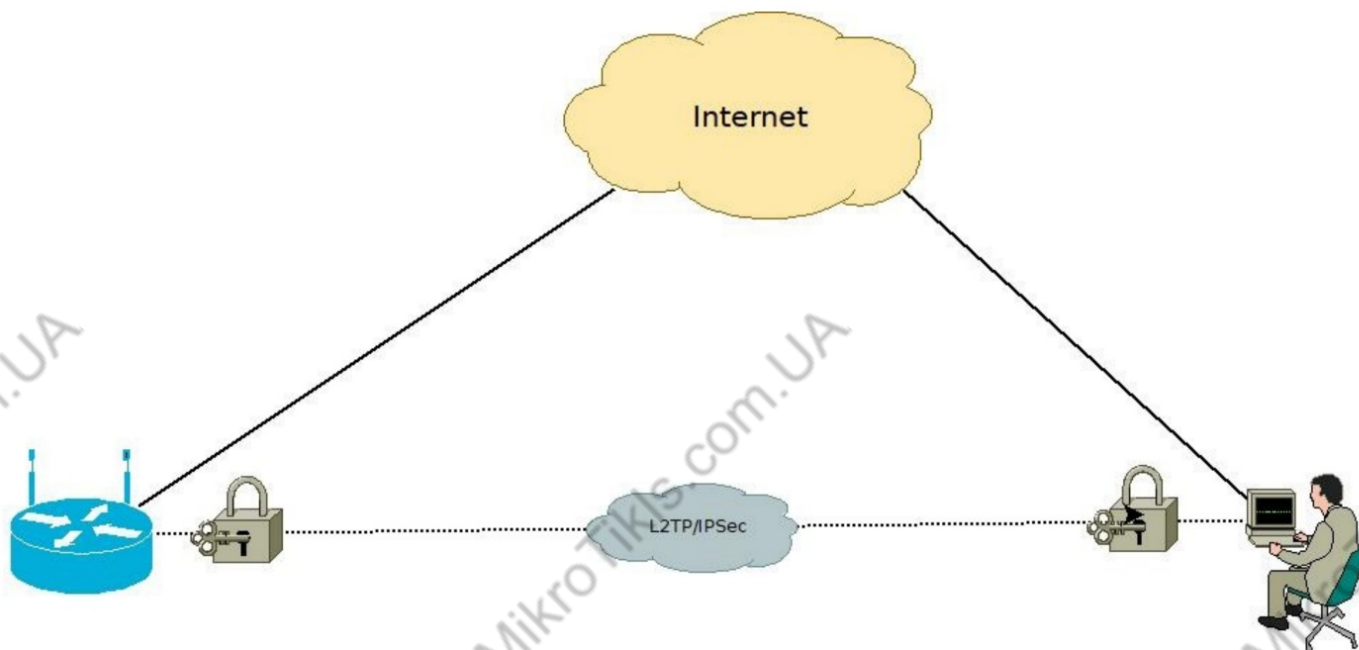
V.19-01

L2TP (англ. Layer 2 Tunneling Protocol – протокол туннелирования второго уровня)

Использует зарегистрированный UDP-порт 1701

- Протокол L2TP был впервые предложен в 1999 году в качестве обновления протоколов L2F (англ. Layer 2 Forwarding Protocol – протокол эстафетной передачи на втором уровне) и PPTP (англ. Point-to-Point Tunneling Protocol – туннельный протокол типа точка-точка).
- Поскольку протокол L2TP сам по себе не обеспечивает надежное шифрование или аутентификацию, то с ним часто используется другой протокол, называемый IPsec.

## Lab Setup



# Lab L2TP/IPSec

PPP

Interface PPPoE Servers Secrets Profiles Active Connections L2TP Secrets

PPP Scanner PPTP Server SSTP Server L2TP Server

Name	Type	Actual MTU	L2 MTU	Tx	Rx
0 items out of 5					

**L2TP Server**

☒ Enabled

Max MTU: 1450

Max MRU: 1450

MRRU:

Keepalive Timeout: 30

Default Profile: default-encryption

Max Sessions:

Authentication: ☒ mschap2 ☒ mschap1  
☐ chap ☐ pap

Use IPsec: yes

IPsec Secret: \*\*\*

Caller ID Type: ip address

☐ One Session Per Host  
☐ Allow Fast Path

OK Cancel Apply

PPP

Interface PPPoE Servers Secrets Profiles Active Connections L2TP Secrets

PPP Scanner PPTP Server SSTP Server L2TP Server

Name	Password	Service
test	test	any
test2	test2	any

2 items (1 selected)

**PPP Secret <test>**

Name: test

Password: test

Service: l2tp

Caller ID:

Profile: default

Local Address: 10.1.1.1

Remote Address: 10.1.1.2

Remote IPv6 Prefix:

Routes:

Limit Bytes In:

Limit Bytes Out:

Last Logged Out: Sep/16/2019 23:23:00

enabled

OK Cancel Apply Disable Comment Copy Remove

# Lab L2TP/IPSec

Добавить VPN-подключение

Поставщик услуг VPN  
Windows (встроенные)

Имя подключения  
L2TP+IPSec-VPN

Имя или адрес сервера  
172.22.22.11

Тип VPN  
L2TP/IPsec с предварительным ключом

Общий ключ  
...

Тип данных для входа  
Имя пользователя и пароль

Имя пользователя (необязательно)  
test

Пароль (необязательно)  
....

☒ Запомнить мои данные для входа

Сохранить Отмена

Параметры

Главная

Найти параметр

Сеть и Интернет

Состояние

Wi-Fi

Ethernet

Набор номера

VPN

Режим «В самолете»

Мобильный хот-спот

Использование данных

## VPN

+ Добавить VPN-подключение

L2TP+IPSec

SSTP

L2TP+IPSec-VPN  
Подключено

## Дополнительные параметры

Разрешить VPN в сетях с лимитным тарифным планом

Вкл.

Разрешить VPN в роуминге

Вкл.

# Lab

- Настройте сервер L2TP+IPSec для своего ноутбука
- Произведите подключение клиента

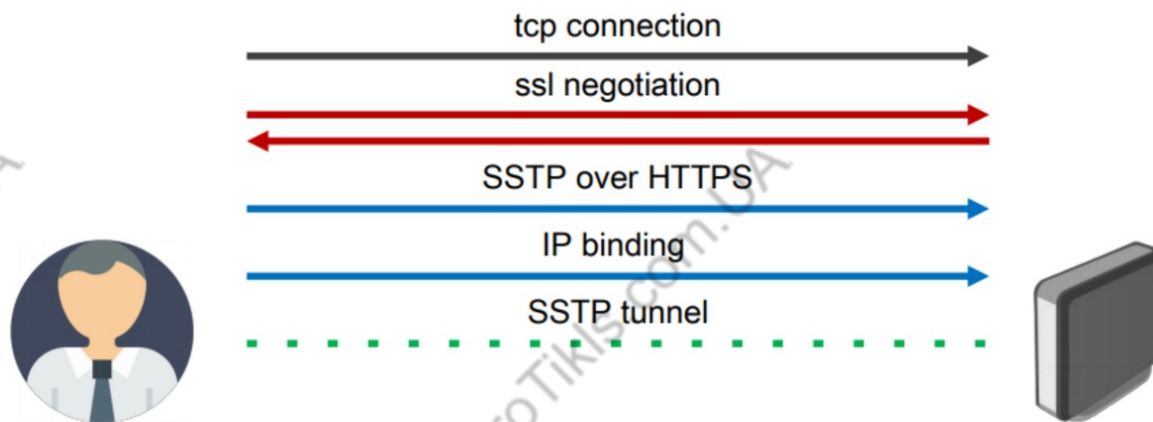
# SSTP

Secure Socket Tunneling Protocol (**SSTP**) – протокол VPN от Microsoft, основанный на SSL и включённый в состав их ОС начиная с Windows 2008 и Windows Vista SP1.

Соединение проходит с помощью HTTPS **по 443 порту**. Для шифрования используется SSL, для аутентификации – SSL и PPP.



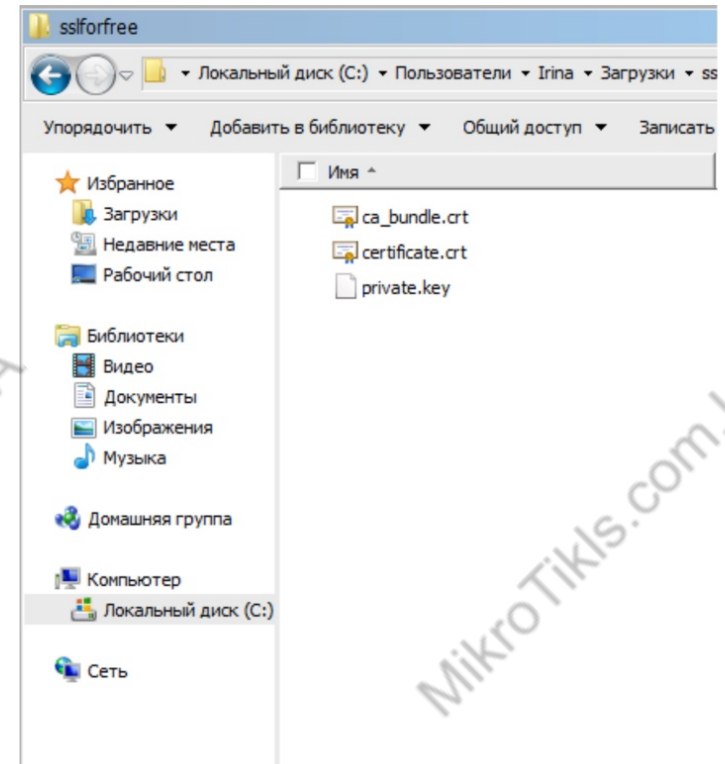
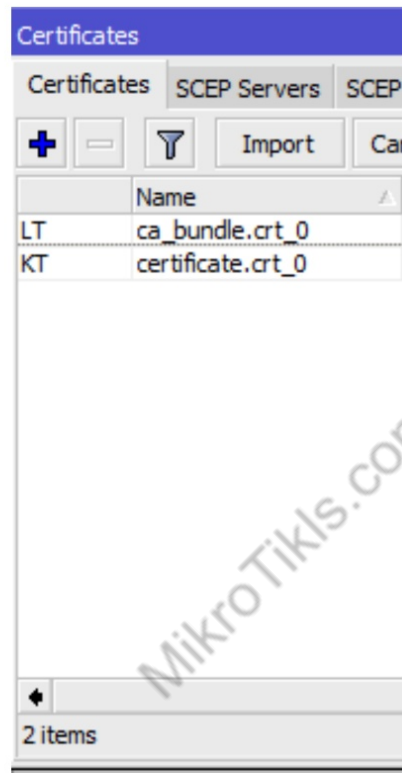
## СТАДИИ SSTP



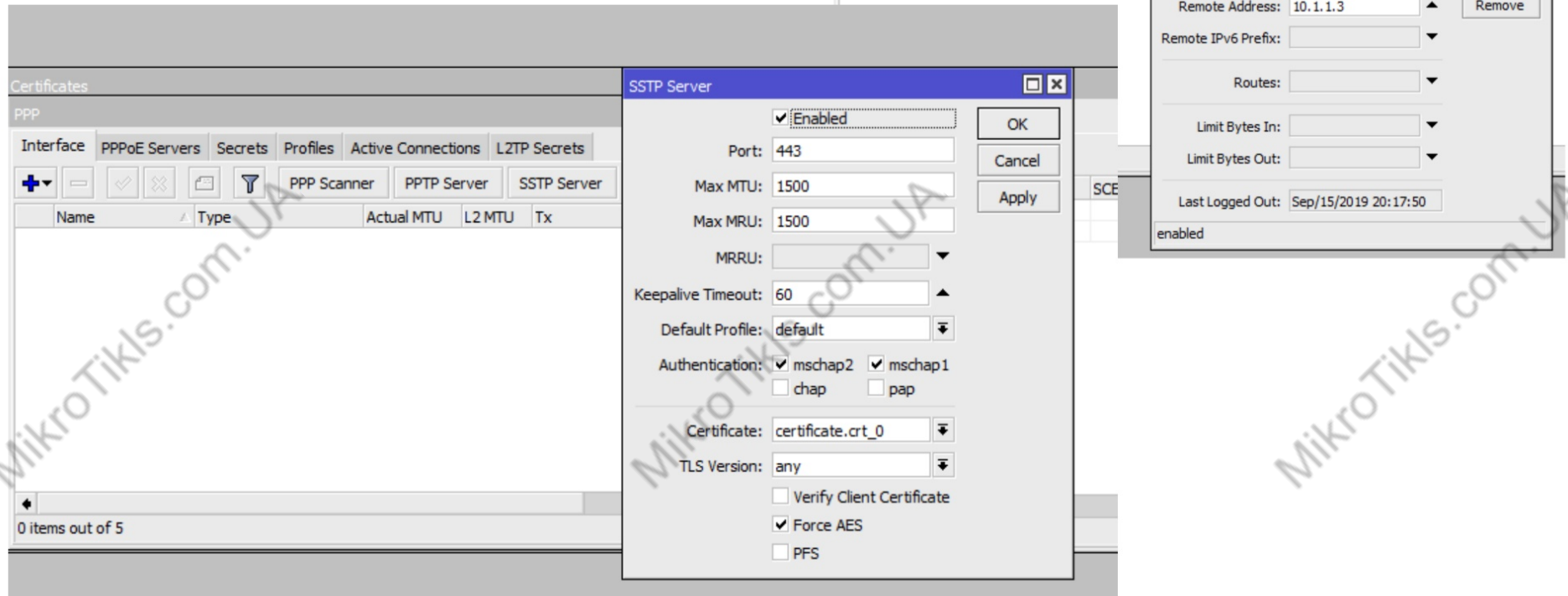
- TCP-соединение установлено от клиента к серверу (по умолчанию для порта 443)
- SSL проверяет сертификат сервера. Если сертификат действителен соединение установлено, иначе соединение разорвано.
- Клиент отправляет контрольные пакеты SSTP в пределах HTTPS.
  - PPP-соединение установлено с IP адресами на интерфейсах
- Note: Two RouterOS devices can establish an SSTP tunnel even without the use of certificates (not in accordance with Microsoft standard)

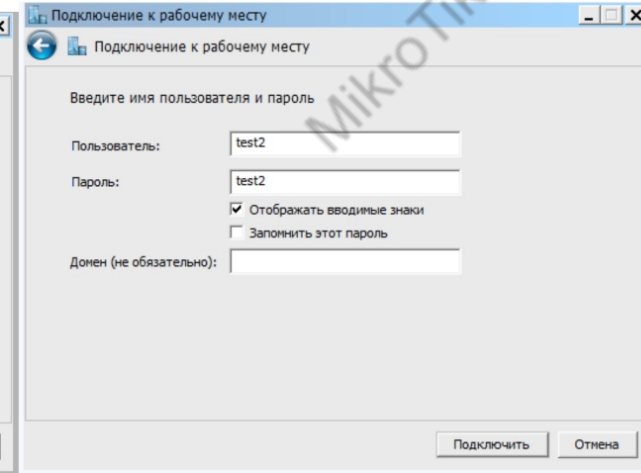
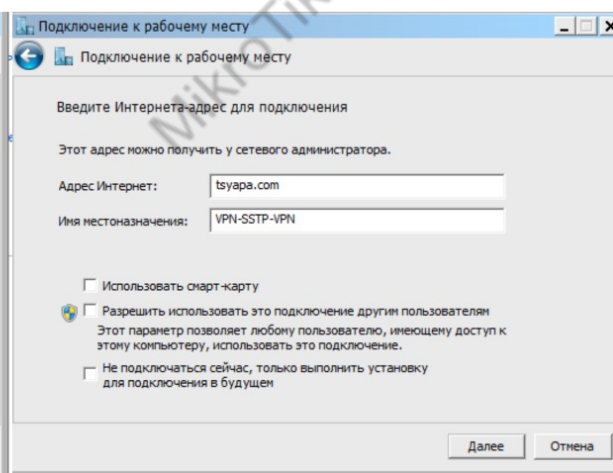
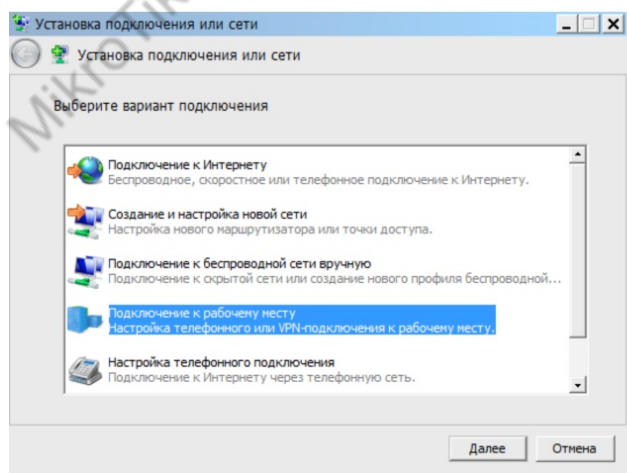
## SSTP-server

Импортируем  
сертификаты на  
сервер



# SSTP-server





Текущие подключения:



**MTI-Group**  
Доступ к Интернету



**VPN-SSTP-VPN**  
Без доступа к Интернету

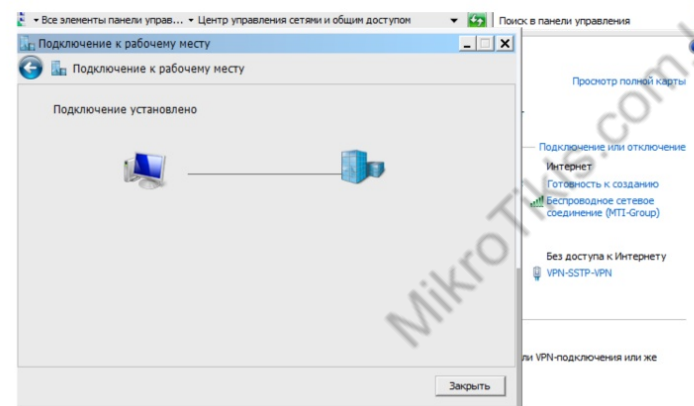
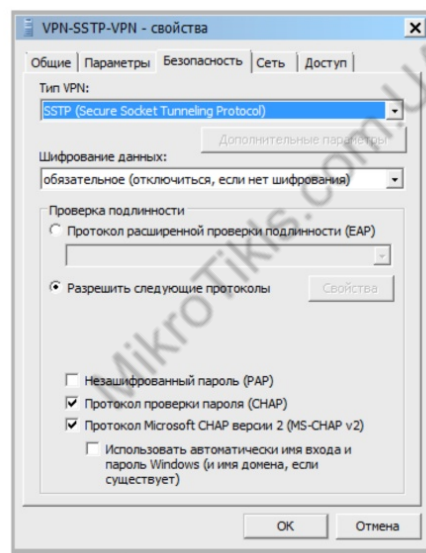
Удаленный доступ и виртуальные частные сети

**VPN-SSTP-VPN**

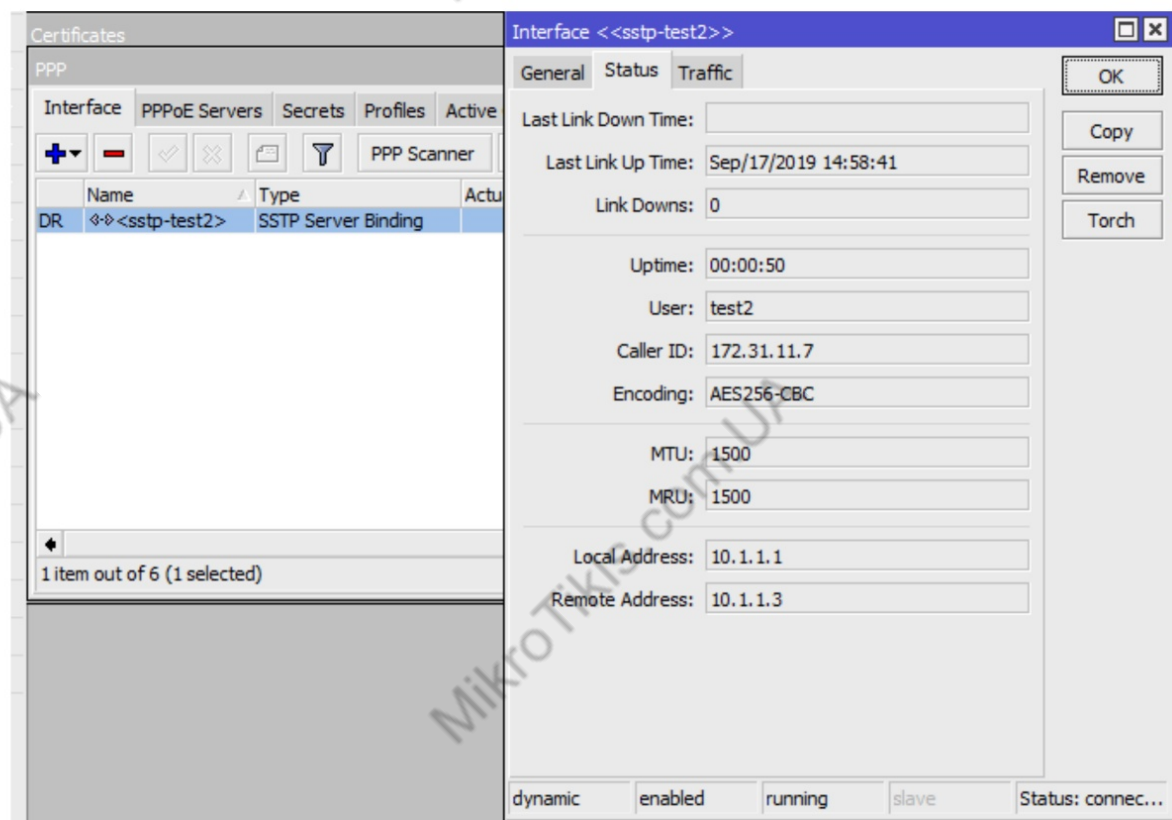
**Подключено**

Отключение  
Состояние  
Свойства

office-mti



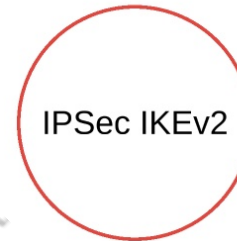
# Успешное подключение



# MikroTik Certified Security Engineer

MTCSE

*Chapter 7:  
SECURE  
TUNNELS for  
Clients (road  
warrior)*



MTI-GROUP LLC / network academy

V.19-01



## IPSec IKEv2 (road warrior)

- Упрощенный обмен между пирами, всего 4 сообщения
- PSK и RSA-Sig аутентификация
- Асимметричная аутентификация
- Сужение селектора трафика разрешено
- Lifetime не нужны
- Rekey – Определен
- NAT-T: Поддерживается по умолчанию
- DPD: Поддерживается по умолчанию
- RoadWarrior: поддерживается EAP и config payload(CP)
- Поддерживает протокол MOBIKE(Mobility, Multi-homing) - более быстрое подключение. Это позволяет IKEv2 поддерживать сеанс VPN, когда пользователь переключает IP-адреса, без необходимости повторно устанавливать соединение.
- Сопротивление DoS улучшено
- Улучшен формат отладки
- Может создавать политики с помощью level=unique
- Несколько клиентов за одним и тем же публичным IP-адресом теперь работают



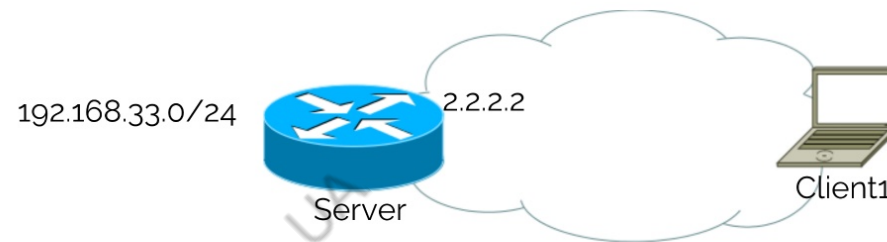
## Variante 1

1 - Генерируем самоподписные сертификаты

- CA (common name=2.2.2.2)
- Server (common name=2.2.2.2)
- Client1

...

common name= лучше dns имя



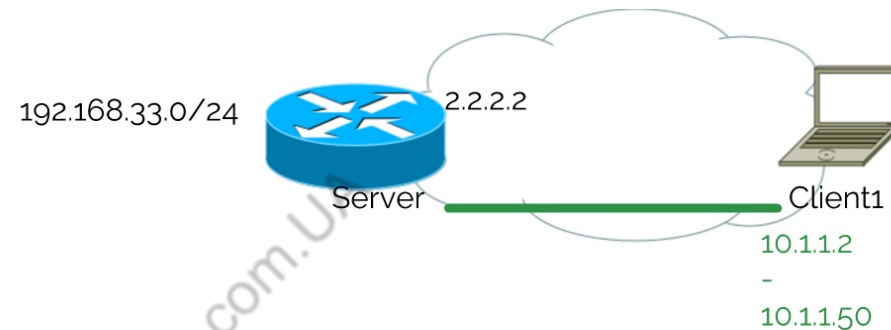
## Variante 1

### 2 - Настройка IPSec - pool for users

Клинтам необходимо выдавать адреса (из пула или каждому индивидуально)

...

создаем pool для наших road warrior  
**/ip pool**



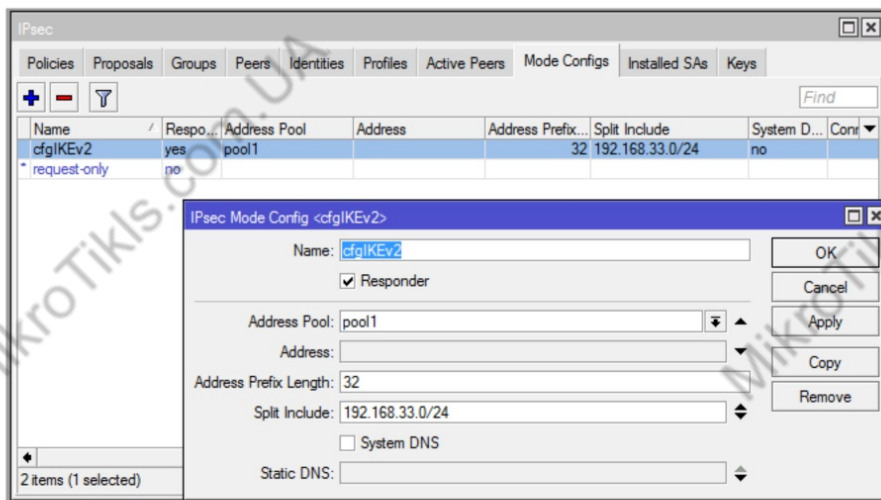
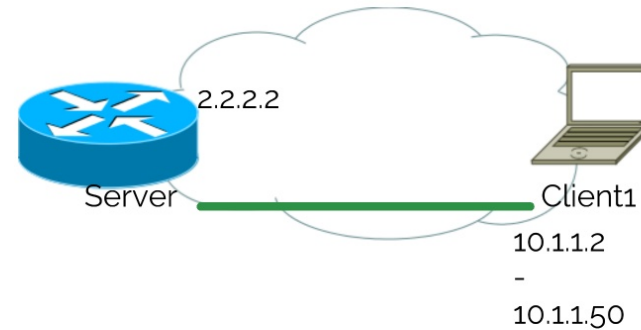
## Variante 1

3 - Настройка IPSec - дополнительные атрибуты (опции) при IKEv2 для клиентов

Клинтам зачастую необходимо выдавать дополнительные опции

...

192.168.33.0/24



**Responder** - указывает, будет ли конфигурация работать как initiator (клиент) или responder (сервер).

**Address Pool / address** - какой адрес выдавать клиентам

**Split Include** - список подсетей в формате CIDR, к которым необходимо клиенту туннелироваться. Подсети будут отправляться Peer-ам с использованием расширения CISCO UNITY, на удаленный Peer-ах (клиентах\*) будут создаваться определенные динамические политики.

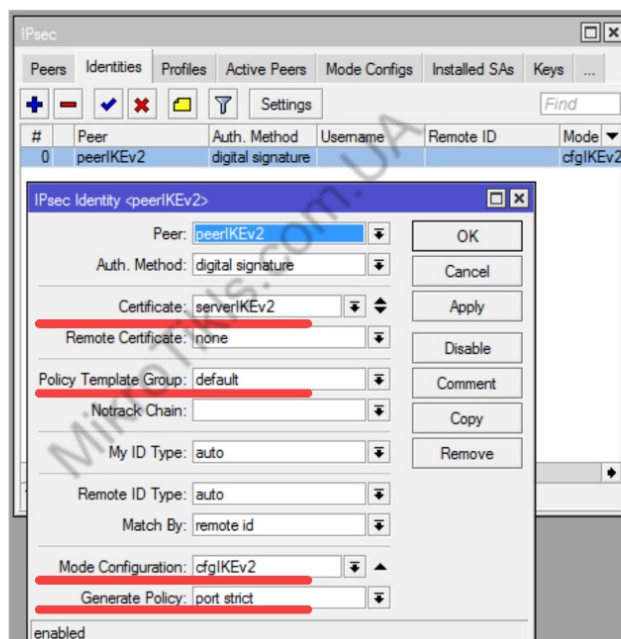
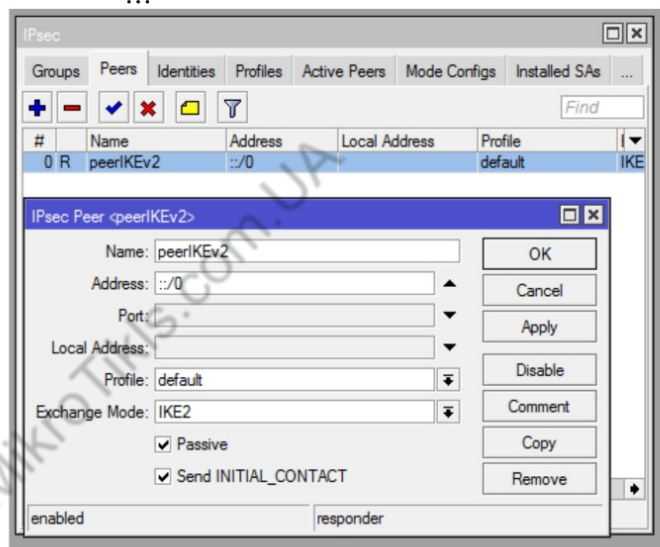
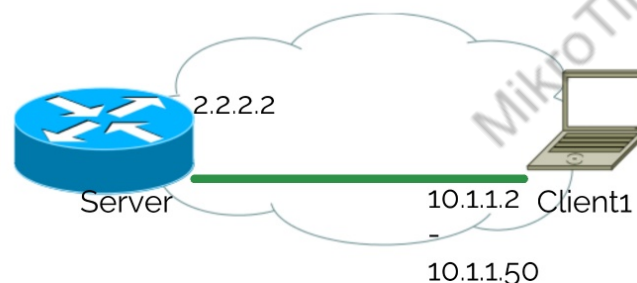
**DNS** - (system or static) - IP адреса DNS серверов которые будут отправляться клиентам

## Variante 1

### 4 - Настройка IPsec - настройка Peer

Необходимо настроить Peer-ов\* с указанием какие дополнительные атрибуты будут им передоваться

192.168.33.0/24

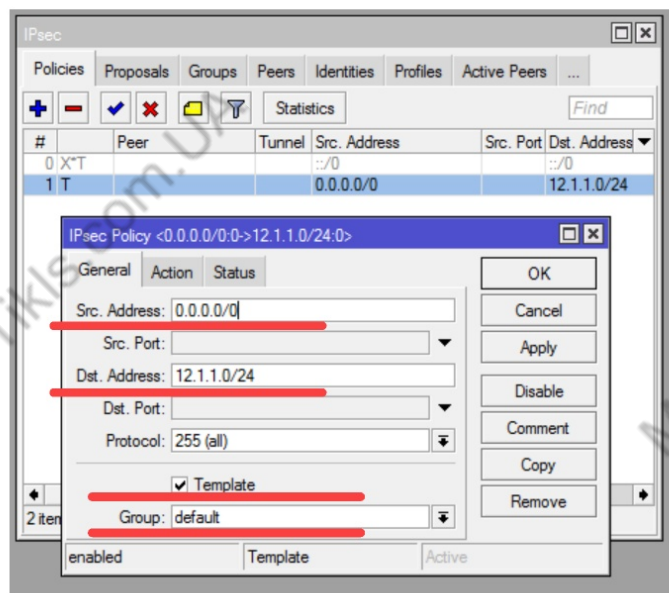
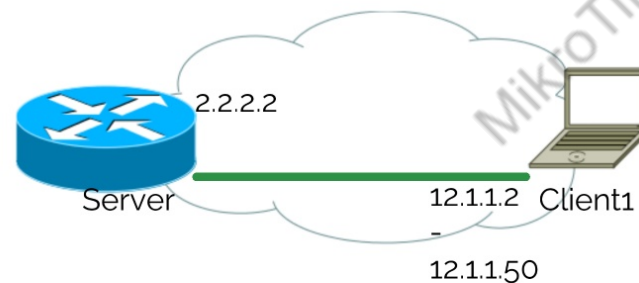


**Generate Policy** - Разрешить с этим Peer-ом устанавливать SA для несуществующих политик (Policy). Такие политики создаются динамически в течение срока службы SA. Автоматические политики необходимы напимере когда IP-адрес удаленного узла неизвестен во время настройки.

## Variante 1

### 5 - Настройка IPSec - Policy

Мы не можем создавать политики вручную т.к. пиры динамические. Следовательно нужно просто создать шаблон для Generate Policy and Policy Template Group (т.к. для какой то группы)



**Template** - Создает шаблон и назначает его указанной группе политик

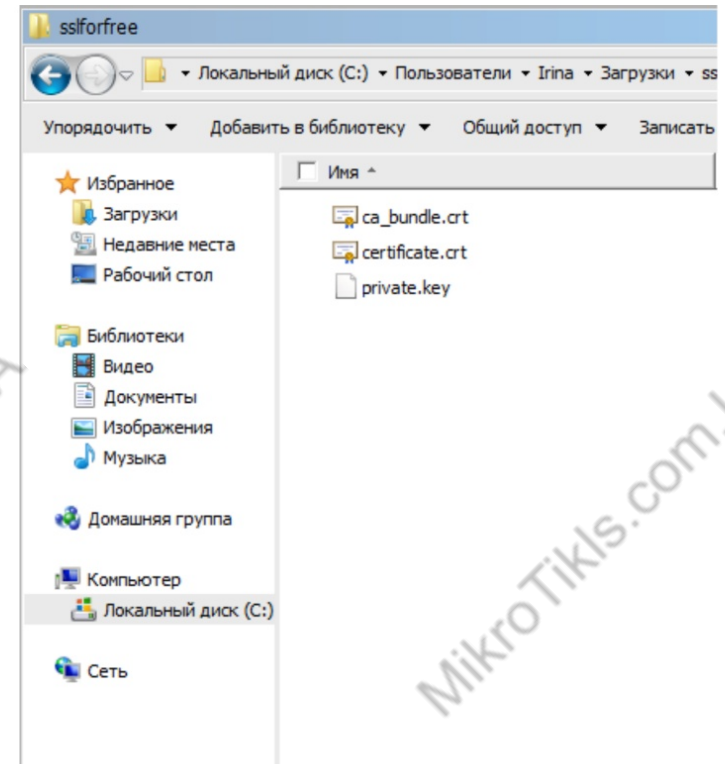
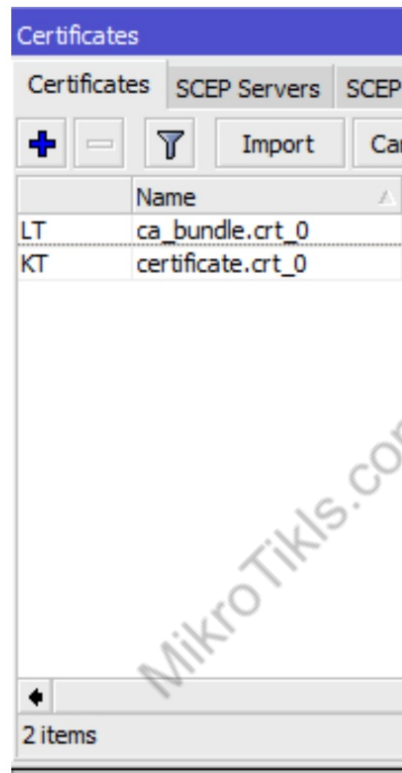
Secure Socket Tunneling Protocol (**SSTP**) – протокол VPN от Microsoft, основанный на SSL и включённый в состав их ОС начиная с Windows 2008 и Windows Vista SP1.

Соединение проходит с помощью HTTPS **по 443 порту**. Для шифрования используется SSL, для аутентификации – SSL и PPP.

- TCP-соединение установлено от клиента к серверу (по умолчанию для порта 443)
- SSL проверяет сертификат сервера. Если сертификат действителен соединение установлено, иначе соединение разорвано.
- Клиент отправляет контрольные пакеты SSTP в пределах HTTPS.
  - PPP-соединение установлено с IP адресами на интерфейсах
- Note: Two RouterOS devices can establish an SSTP tunnel even without the use of certificates (not in accordance with Microsoft standard)

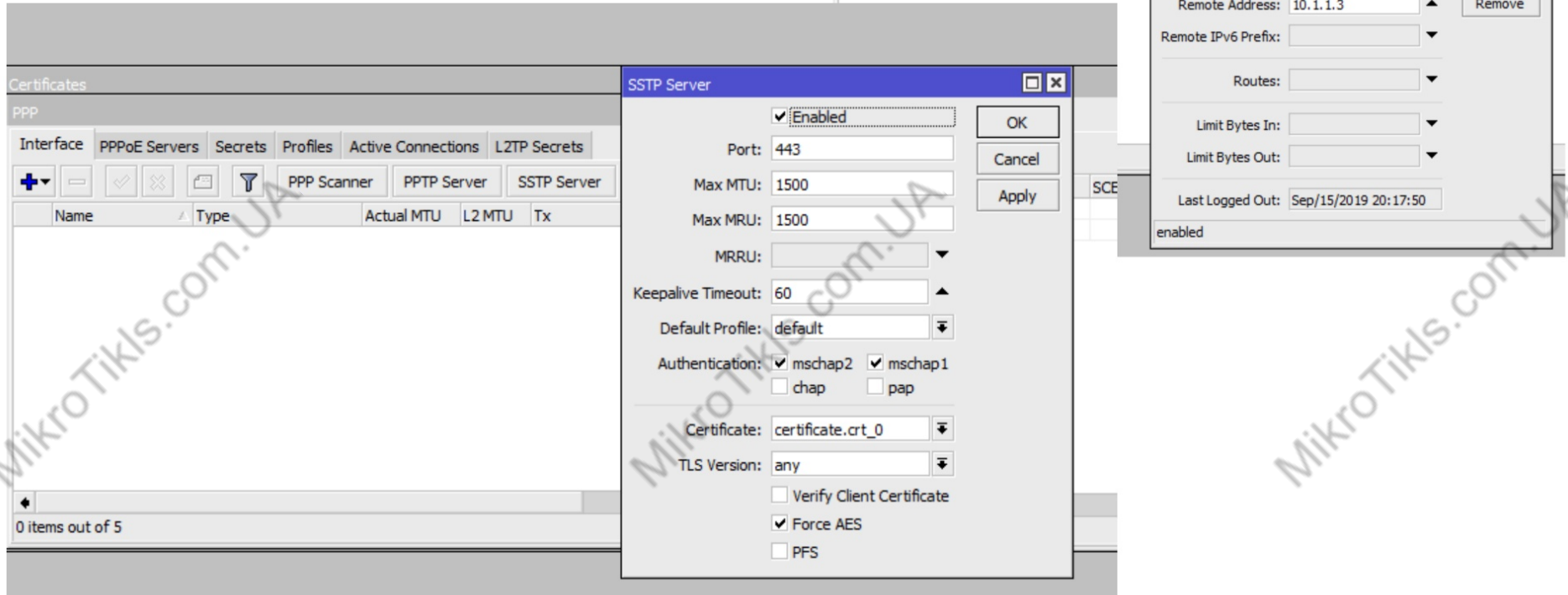
## SSTP-server

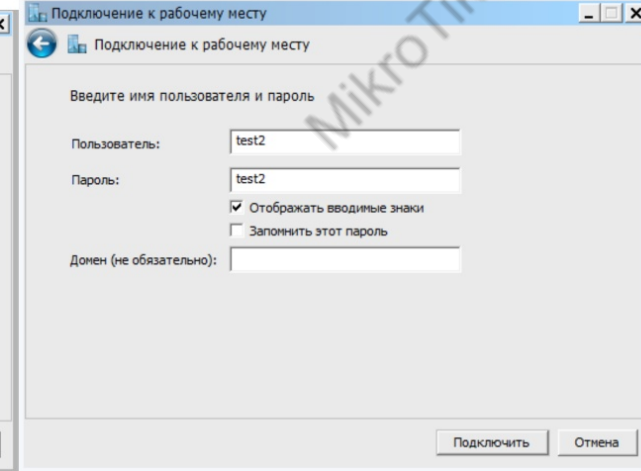
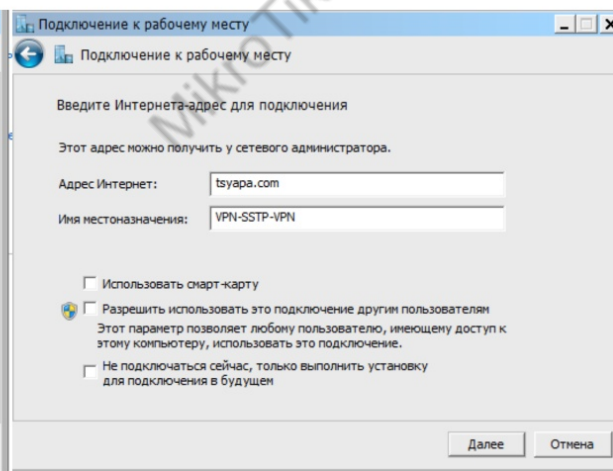
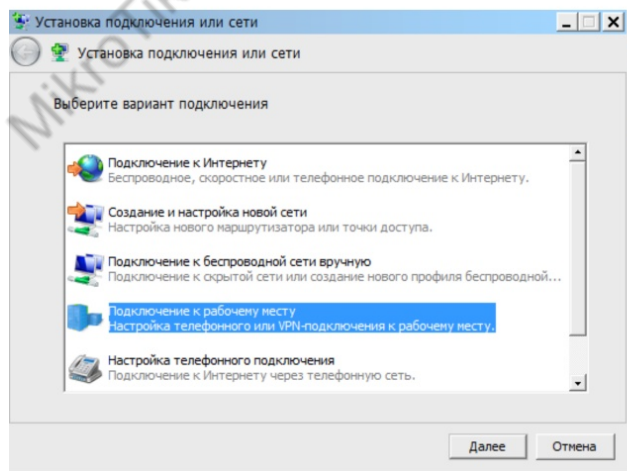
Импортируем  
сертификаты на  
сервер





# SSTP-server





Текущие подключения:



**MTI-Group**  
Доступ к Интернету



**VPN-SSTP-VPN**  
Без доступа к Интернету

Удаленный доступ и виртуальные частные сети

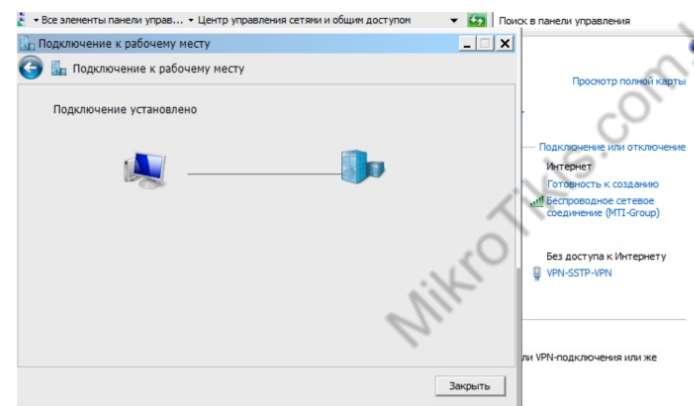
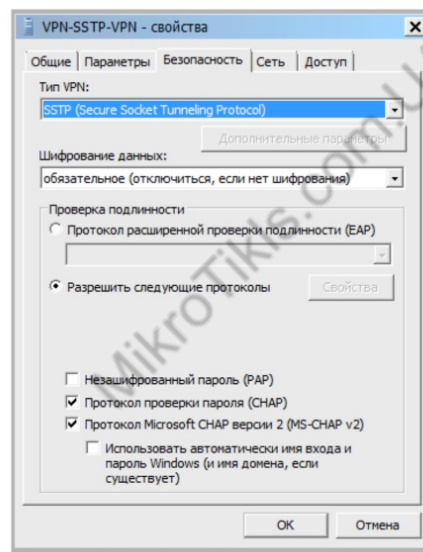
**VPN-SSTP-VPN**

Подключено

Отключение  
Состояние  
Свойства

VPN-SSTP

office-mti



# MikroTik Certified Security Engineer

MTCSE

*Chapter 7:  
SECURE  
TUNNELS for  
Clients (road  
warrior)*

L2TP/IPsec  
SSTP

IPSec IKEv2



**qualitytraining**  
Succeed with Quality

MTI-GROUP LLC / network academy

V.19-01