POORIA TAABBODI

MikroTik: MTCNA, MTCWE, MTCRE
MTCTCE, MTCUME, MTCINE

Microsoft: MCSA, MCSE 2003-2012 R2

Cisco: CCNA,CCNP

PaloSanto(VOIP): ECE

Supervisor & Technical Manager of Neda Gostar Saba

Step-by-Step to Implementing SSTP & OVPN on MikroTik RouterBoard

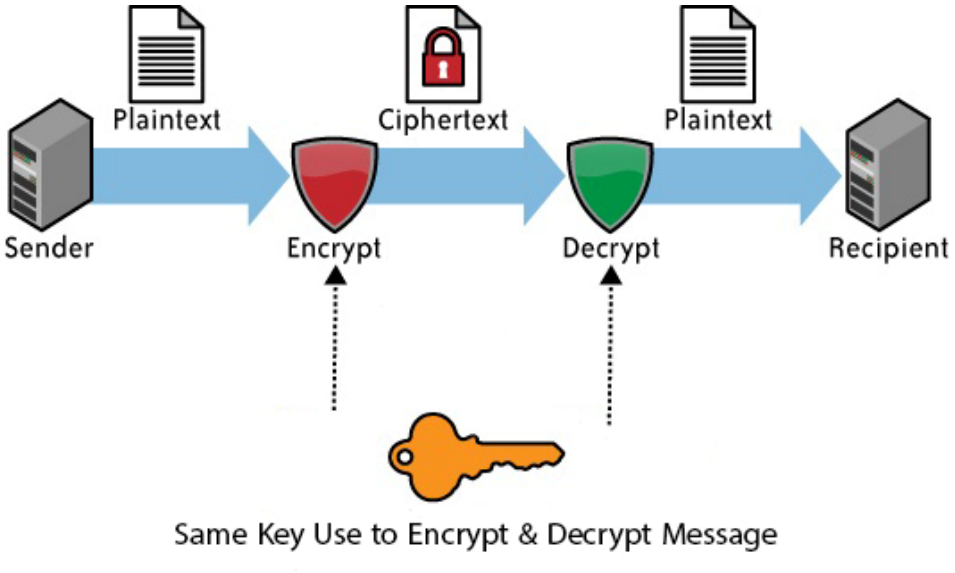
Powered by: POORIA TAABBODI

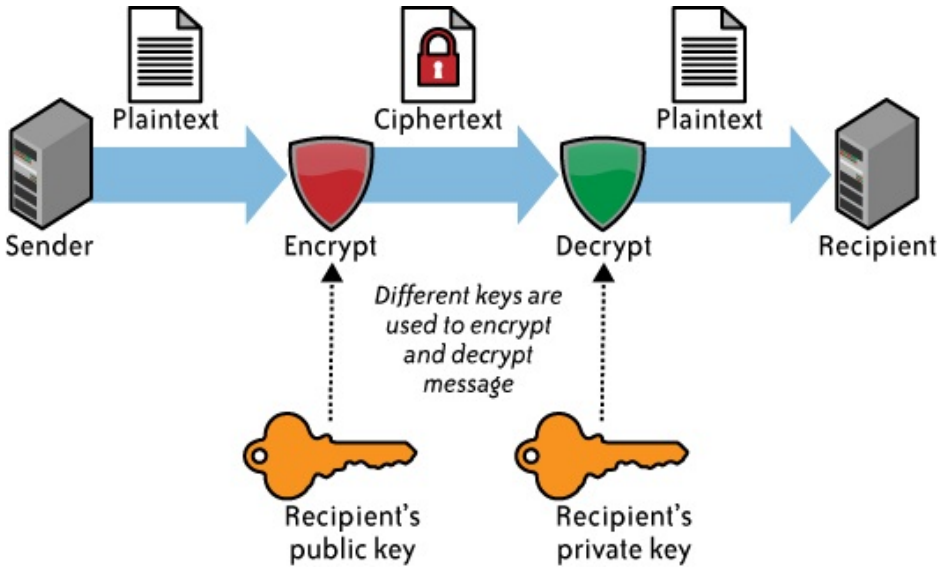
October - 2016

Welcome to this Workshop !

First, some basic concepts about encryption …..

- *As you know, to unlock or even lock anything like a door you need a key.*
- *This applies to computer networks, too.*
- *There are two encryption methods in computer networks.*
  - **Symmetric Encryption**
  - **Asymmetric Encryption**





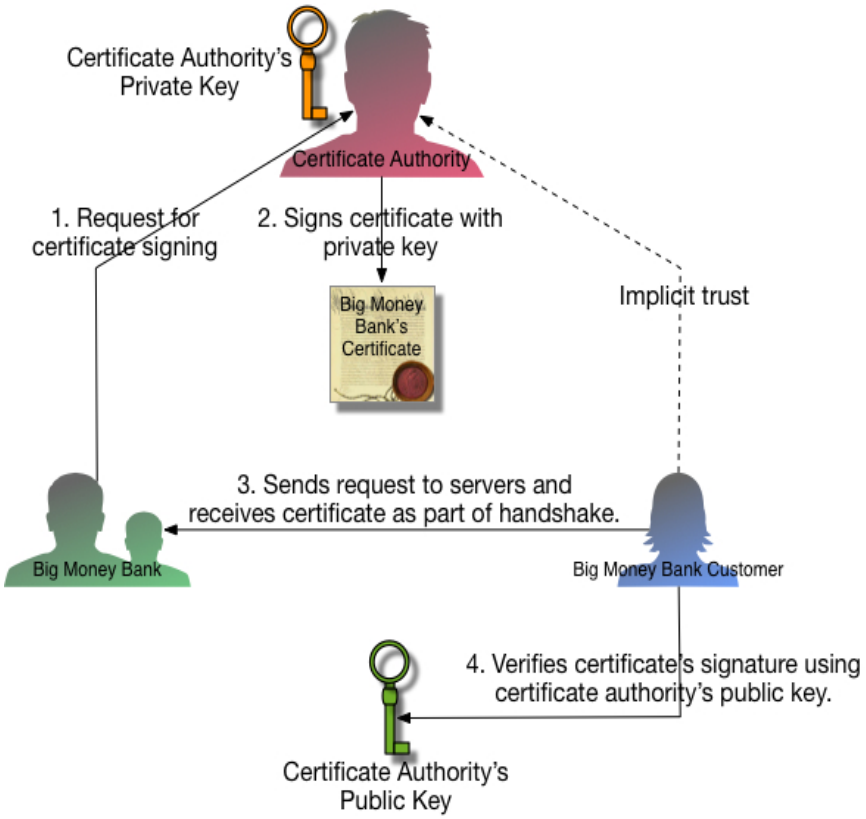
One of the most common Asymmetric Encryption methods is using computer certificates.

In this method, we need to provide a certificate from a well-known Certificate Authority (CA) and import it to our "Local Computer Personal Certificate Store".

After importing, we can use it to encrypt and sign our data.

**Note:* you should have your CA, public key certificate in your "Trusted Certificate Authority" list.*

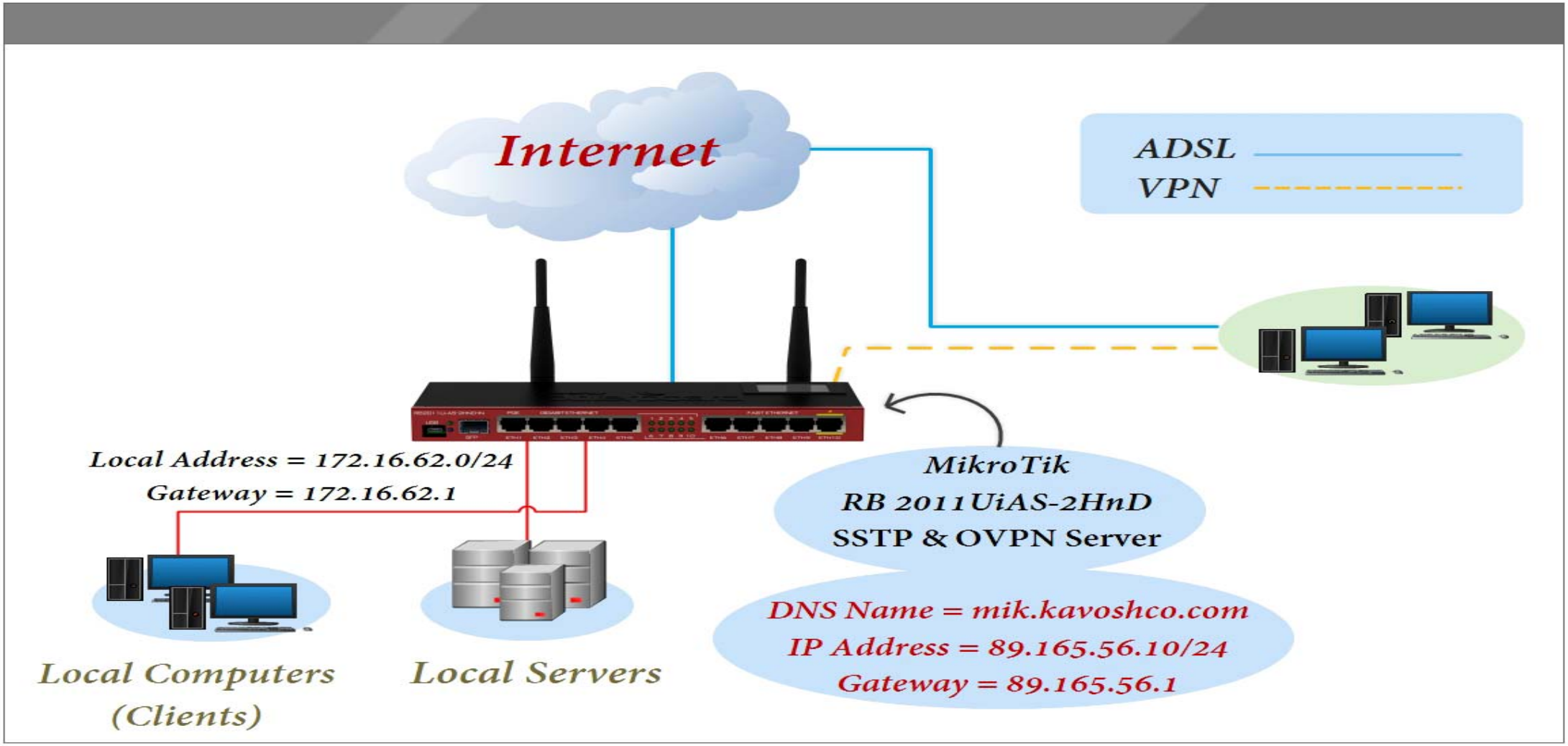
How certificates work and help us to encrypt our data in "HTTPS-(SSL)" communications…




Any Questions?

Let`s go to implementing SSTP & OVPN on our MikroTik RouterBoard as a Server and Microsoft Windows as a Client ……

Imagine that our Network Topology is:

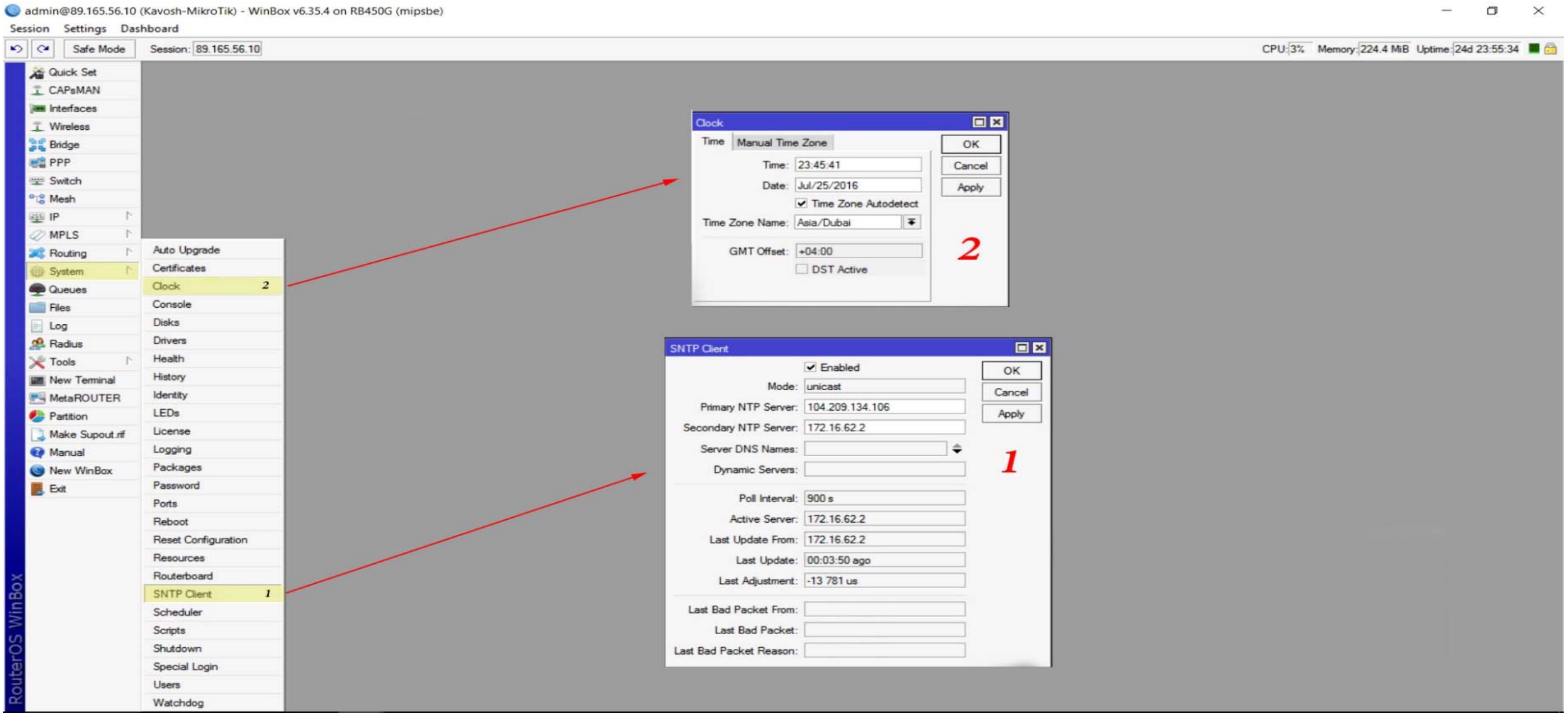


- *First, basic configurations are set, including IP address, MikroTik identity (Name), admin password, ….*

- *Then, as a first step of implementation, we should configure SNTP and MikroTik Clock, because validity time is very important in issuing and using a certificate.*

(See next slide)

Configuring MikroTik Clock & SNTP Settings

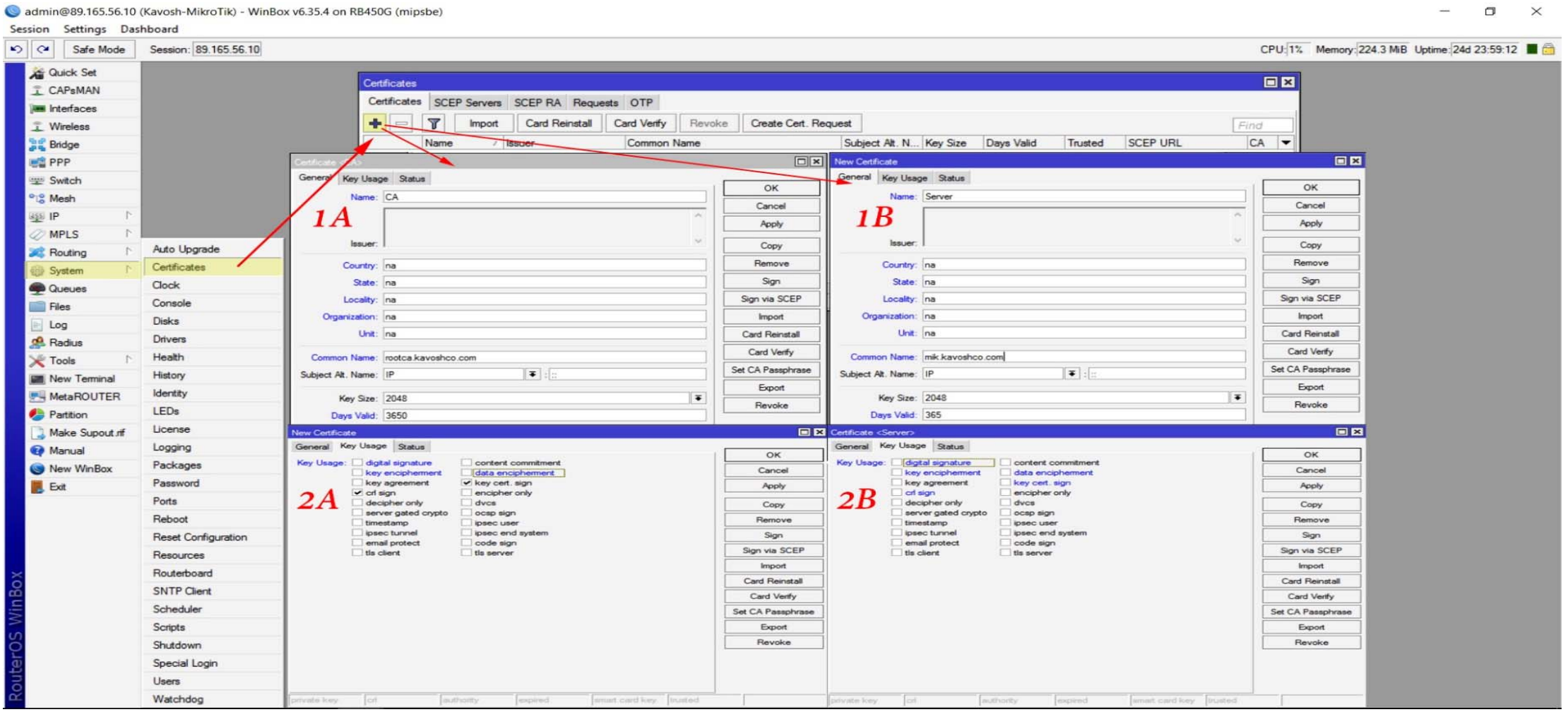


- *Now as a second step, we need to create a CA Certificate and issue a certificate for our SSTP and OVPN Server and finally sign it with our CA Certificate.*

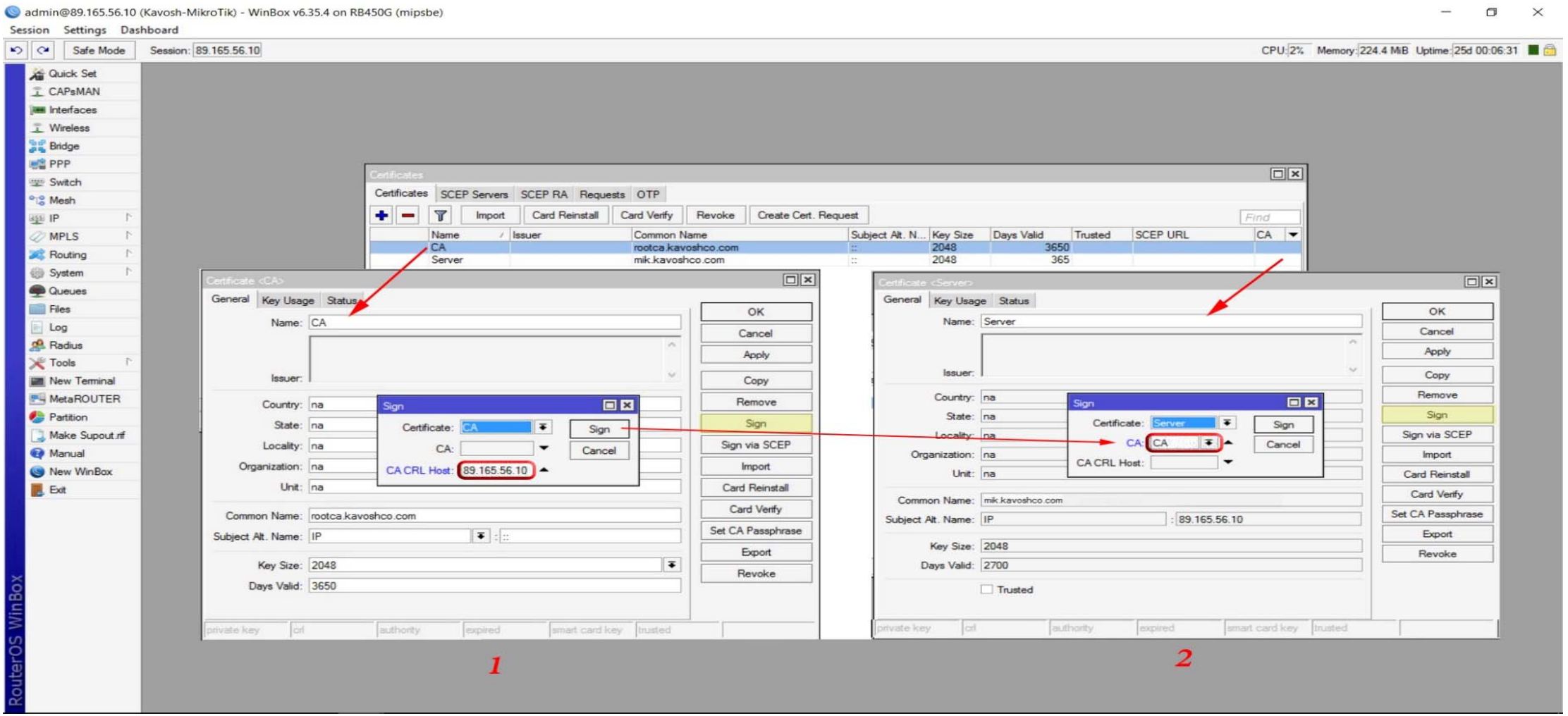
- *After that we should export CA Public Key to import it to our client's "Trusted Root Certification Authorities" List.*

(See next slides)

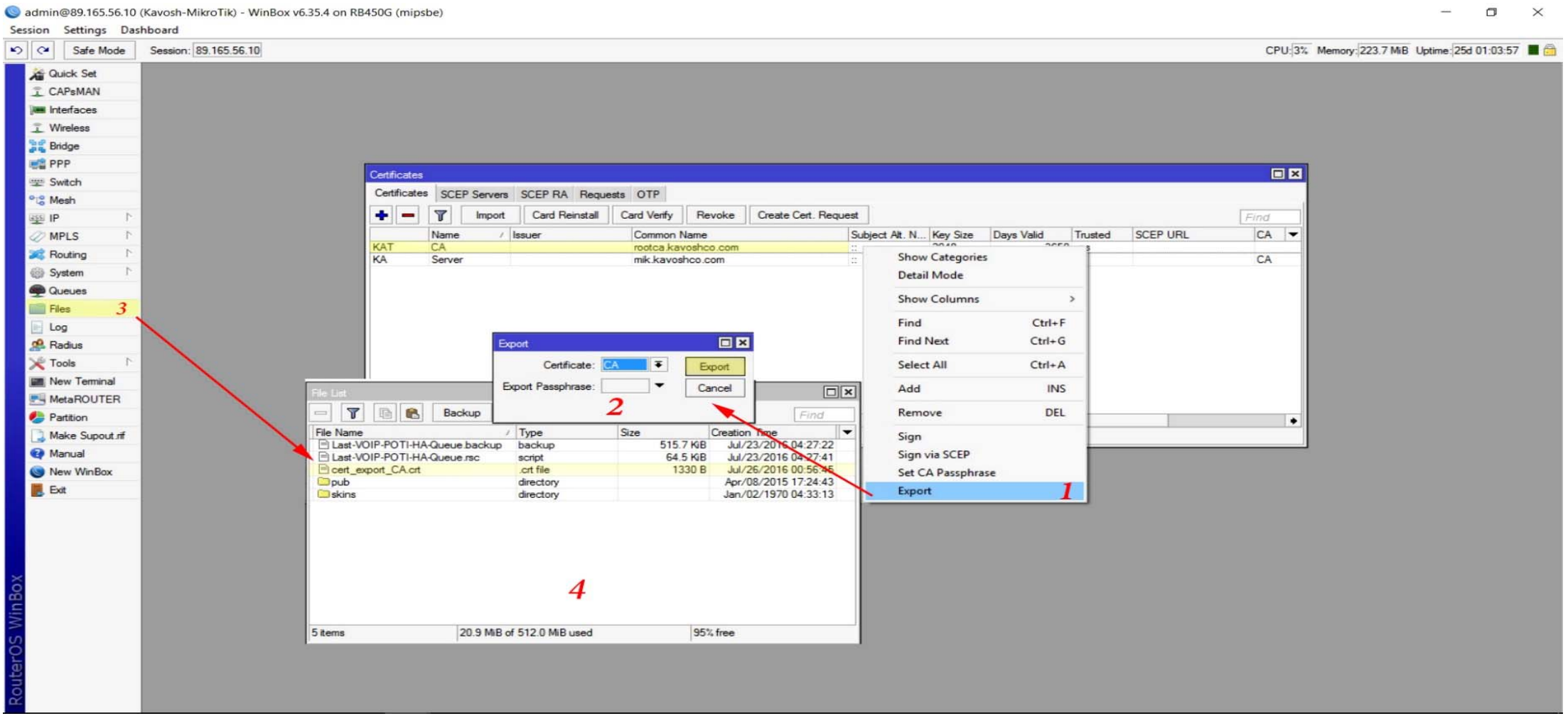
Providing CA & Server Certificates



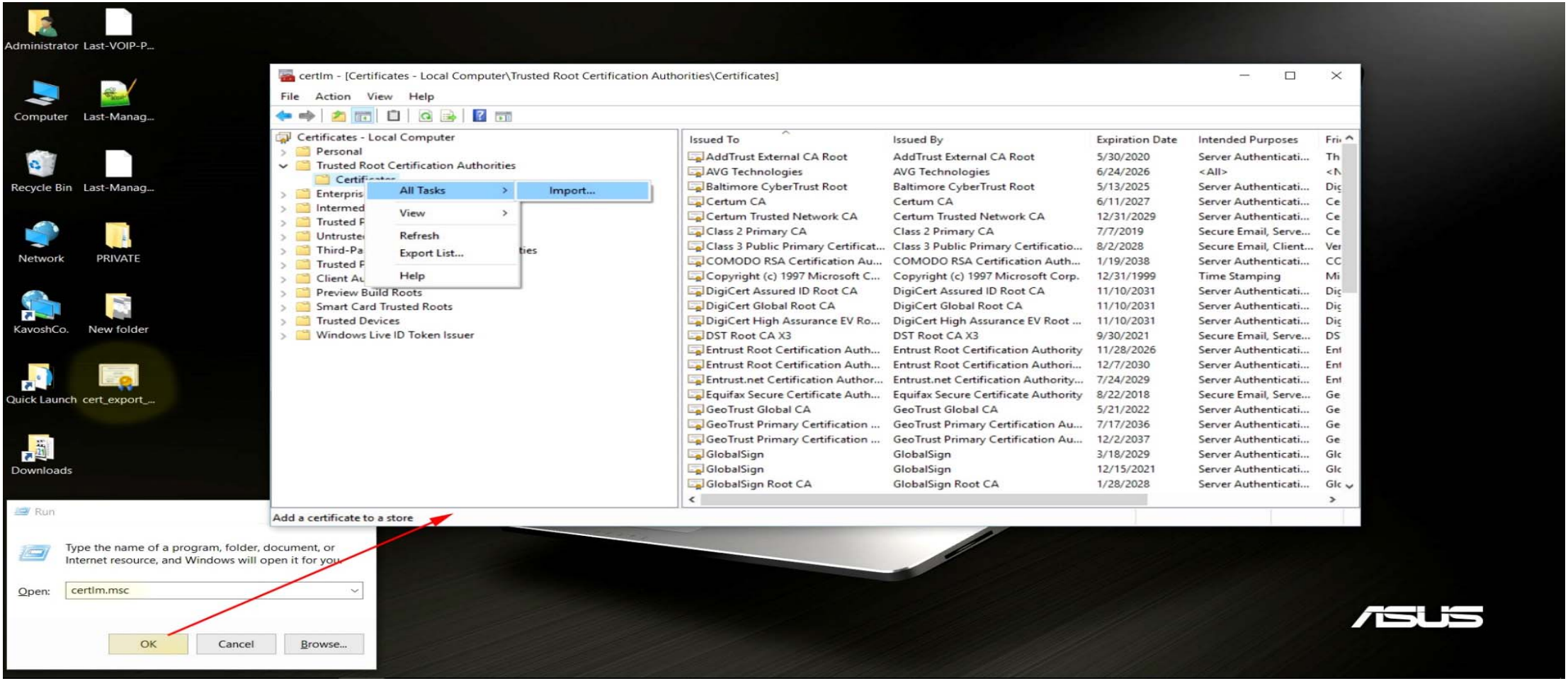
Signing Certificates



Exporting CA Public Key



Importing CA Public Key to Client Local Certificate Store (Trusted Root Certification Authorities List)

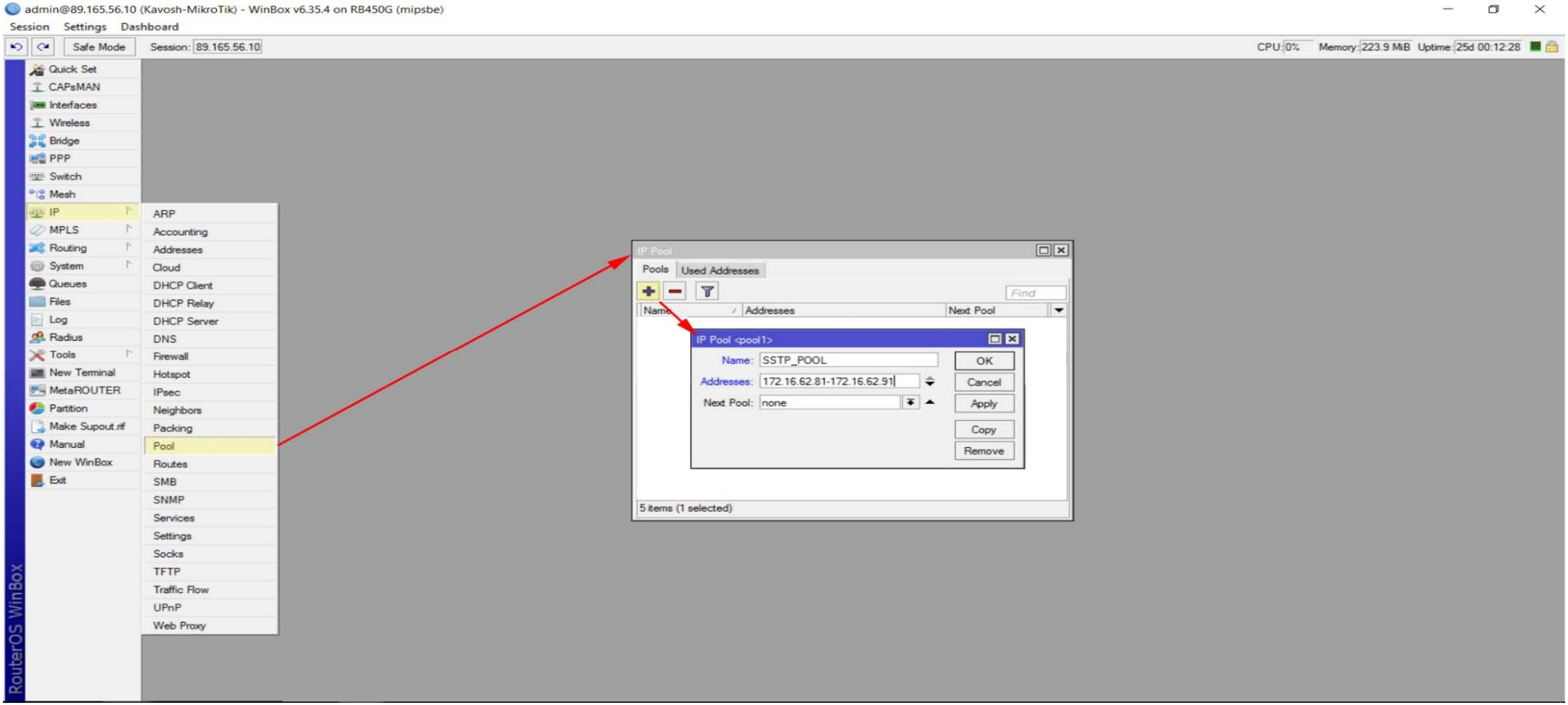


- *Now as a third step, we should create an IP Pool, a PPP Profile and PPP Secret which should be used with Server Certificate in Configurations after enabling SSTP and OVPN.*
- *Finally, in Server Configurations, we should enable "ARP Proxy" on our MikroTik Router "Local Network" Interface.*

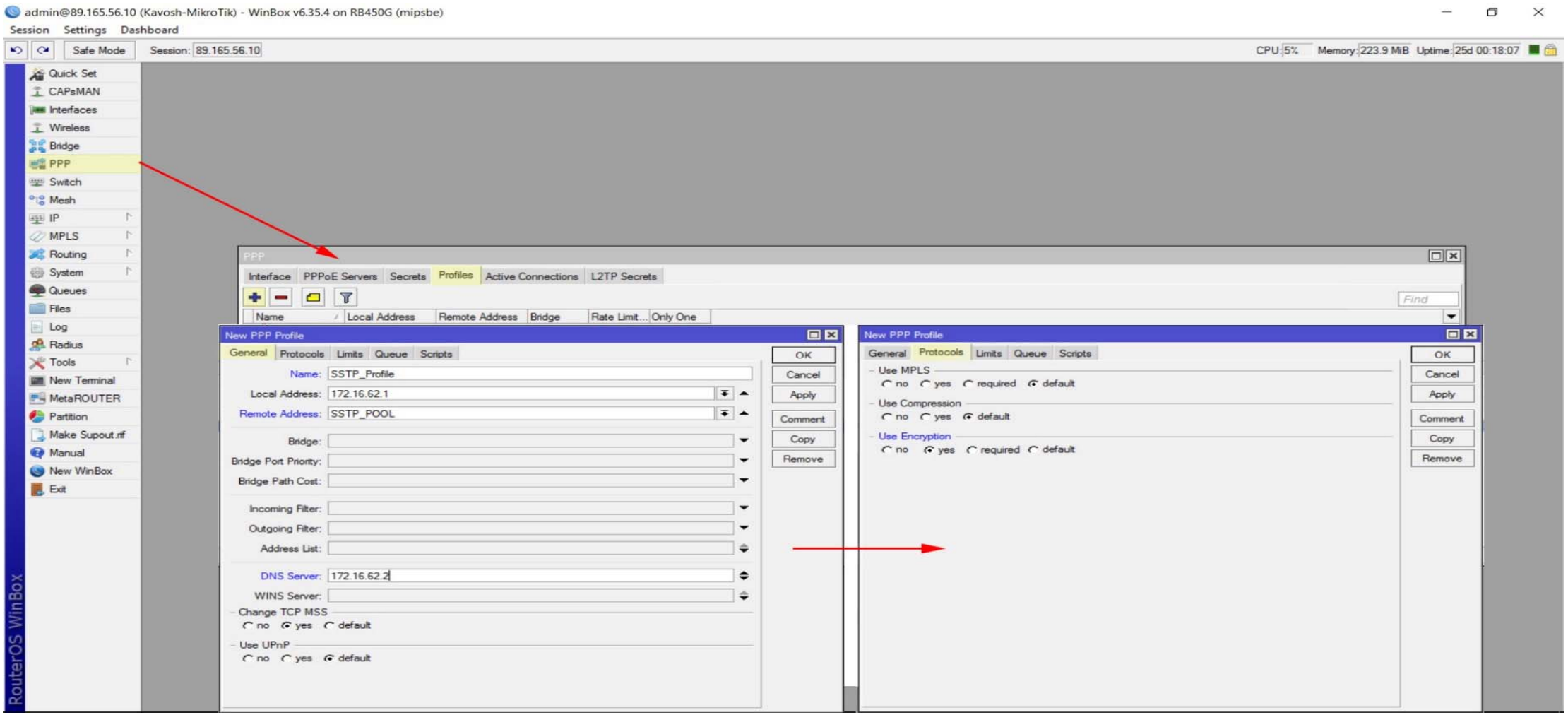
- *It's required to remotely access Local Network.*

(See next slides)

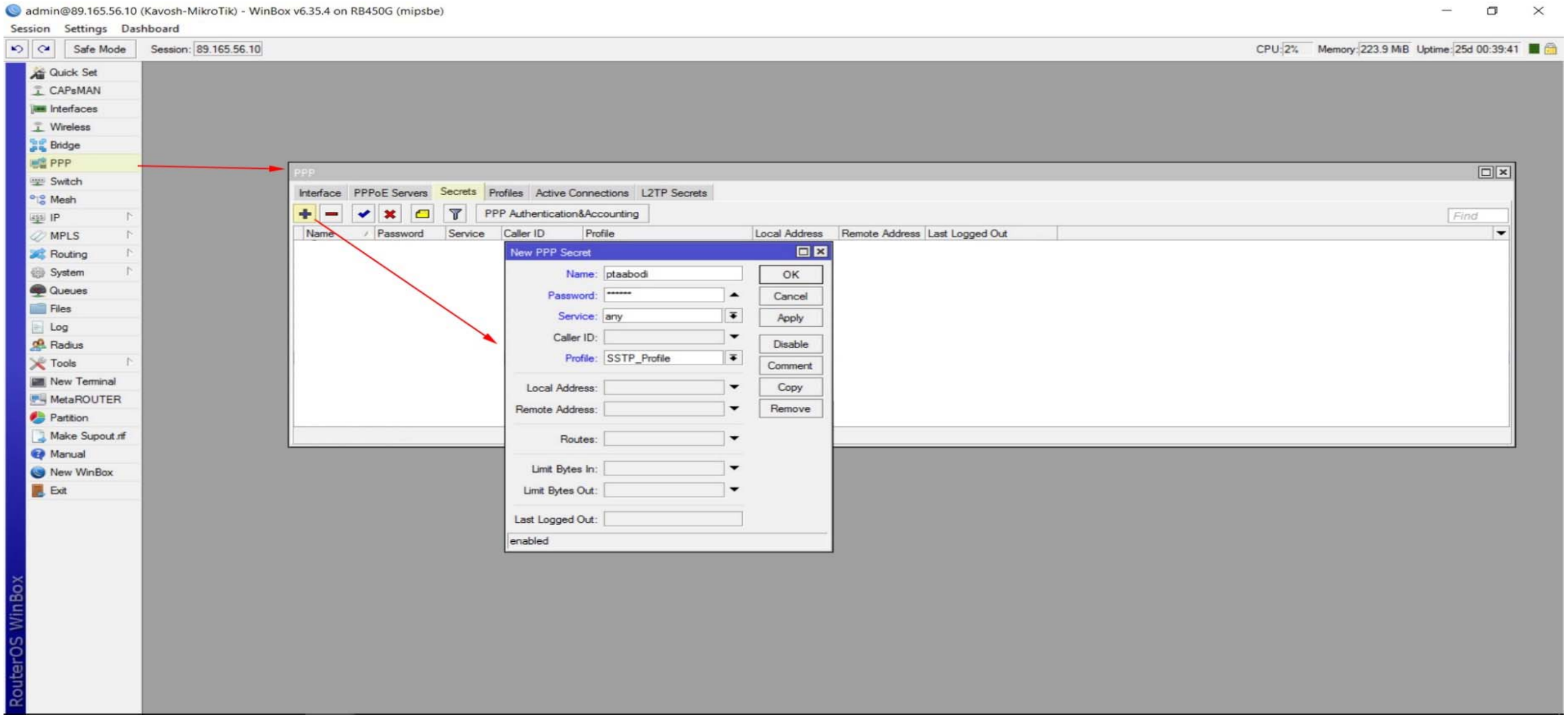
Providing Same "IP Pool" for SSTP & OVPN Clients



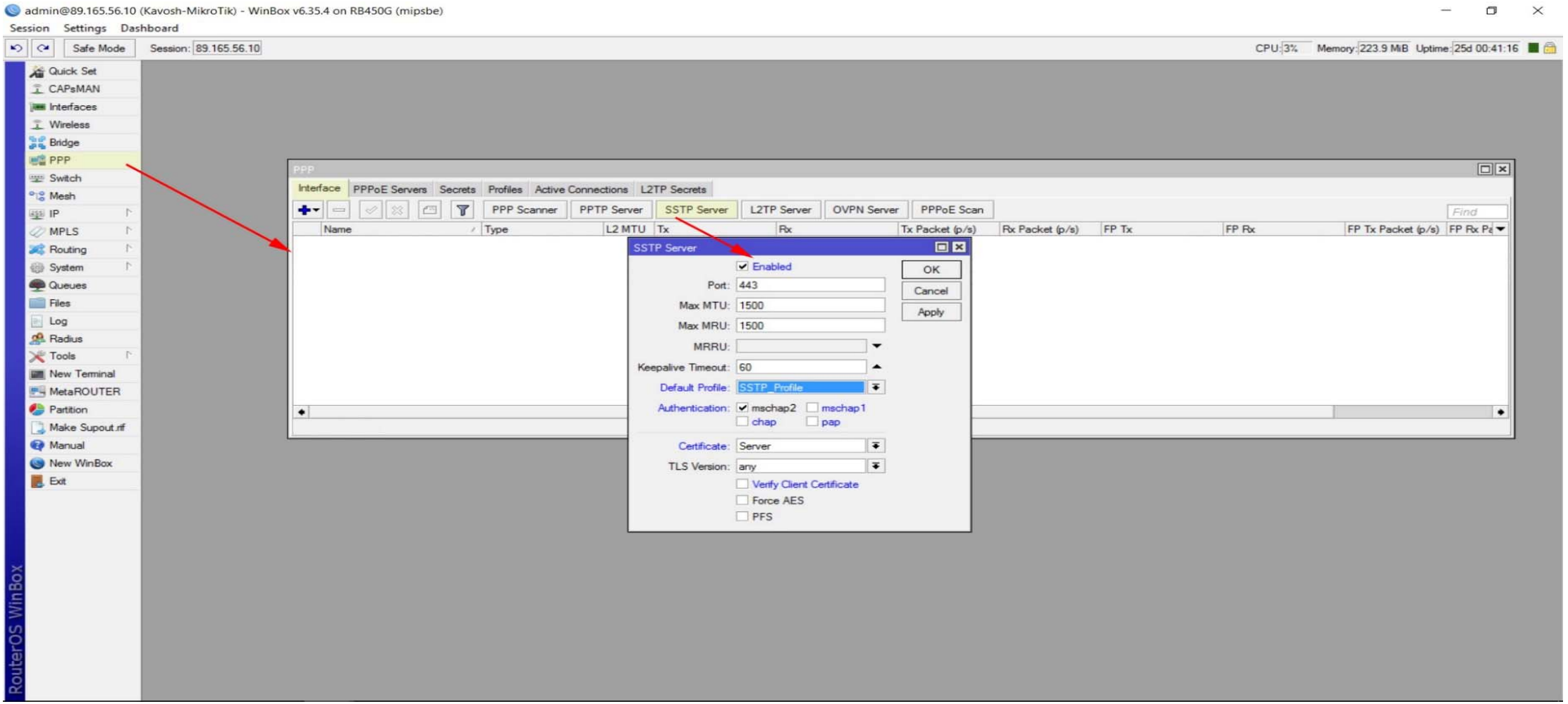
Creating "PPP Profile" for SSTP & OVPN Connections



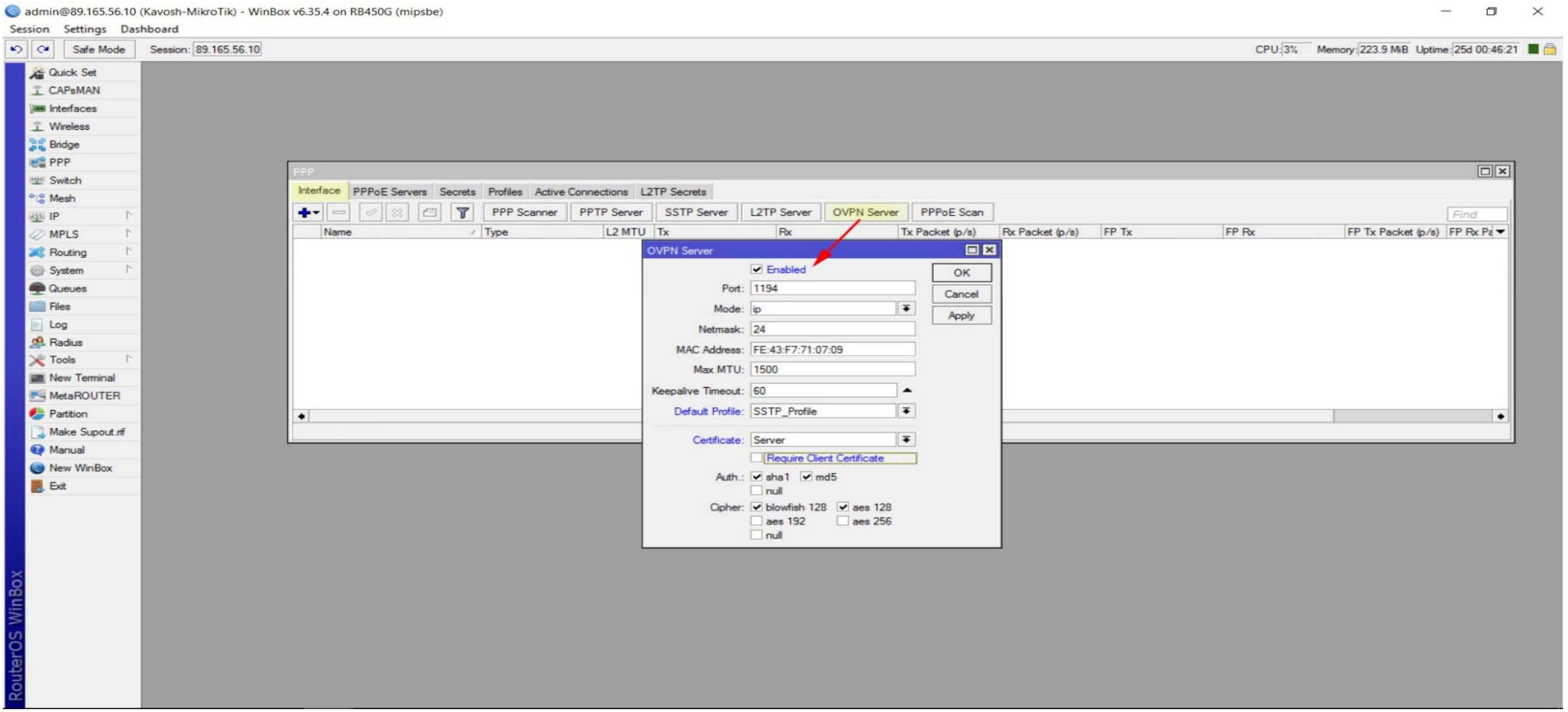
Creating "PPP Secret" for SSTP & OVPN Connections



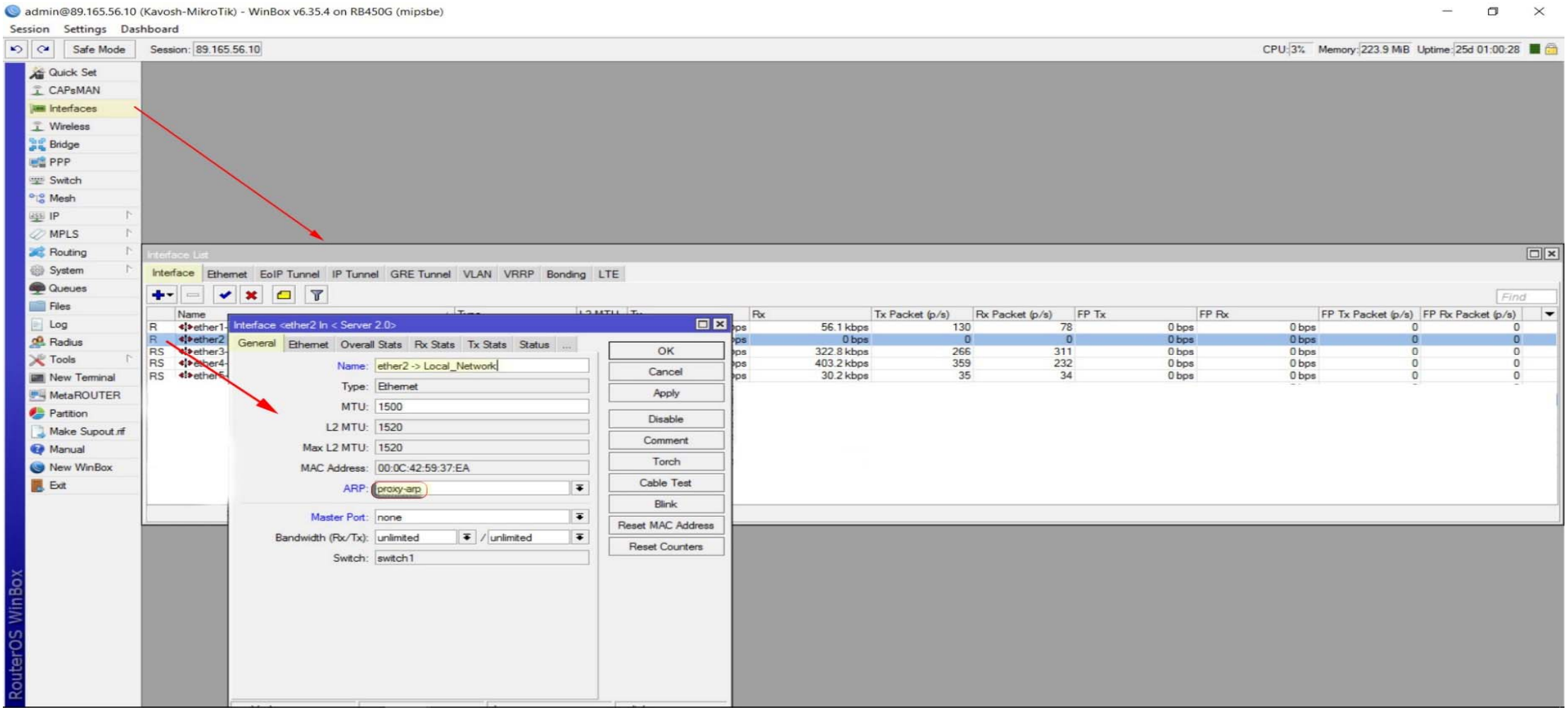
Enabling & Configuring SSTP Server



Enabling & Configuring OVPN Server



Enabling "ARP Proxy" on Local Interface



- *After all server configurations are completed, we should configure the client side.*

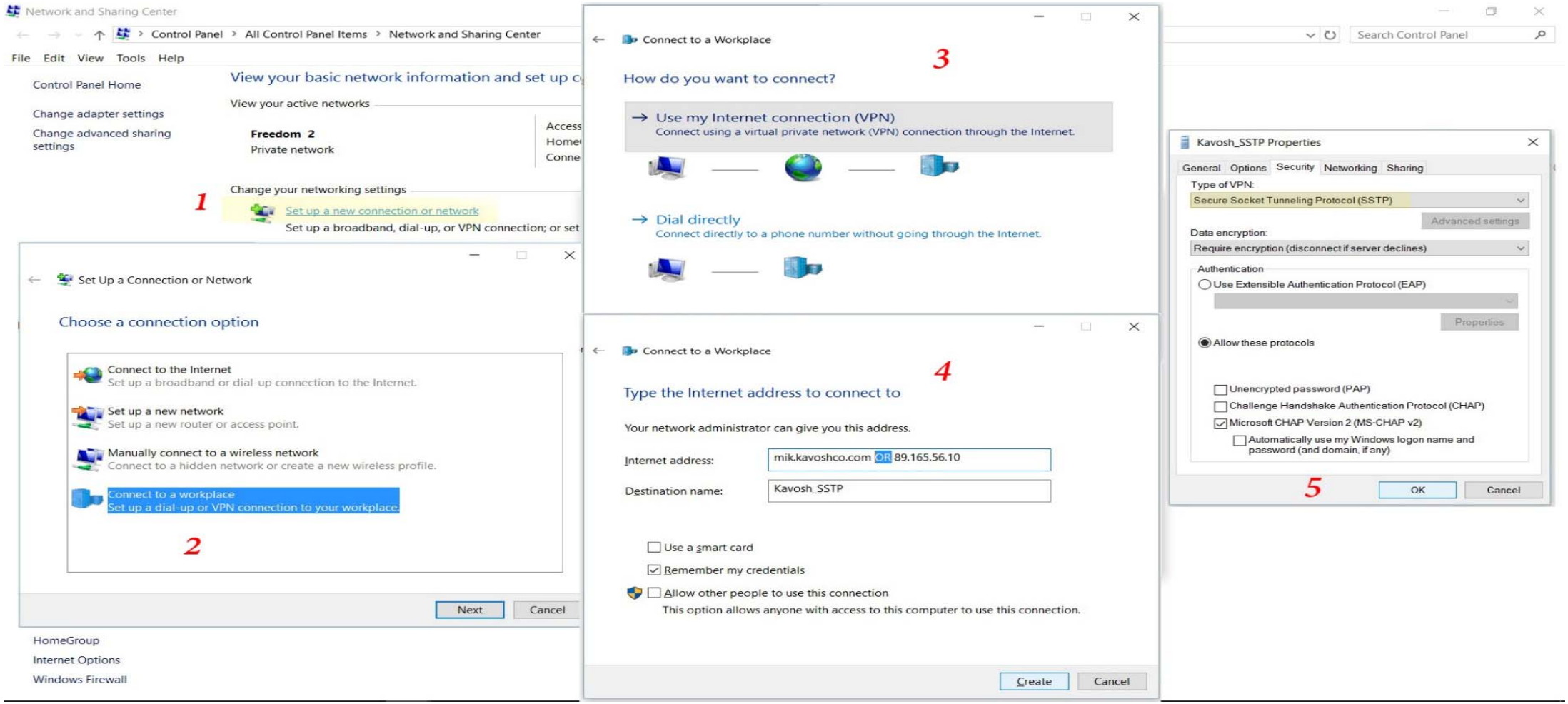
- *To configure a Microsoft Windows operating system as a SSTP Client, a VPN connection should first be created and "VPN type" should be changed to "SSTP".*

- *To configure a Microsoft Windows operating system as an "OVPN Client", some OVPN client applications such as "OPEN VPN GUI" should be installed and then provide a Config File that includes client configurations and finally use it to connect to your OVPN server.*

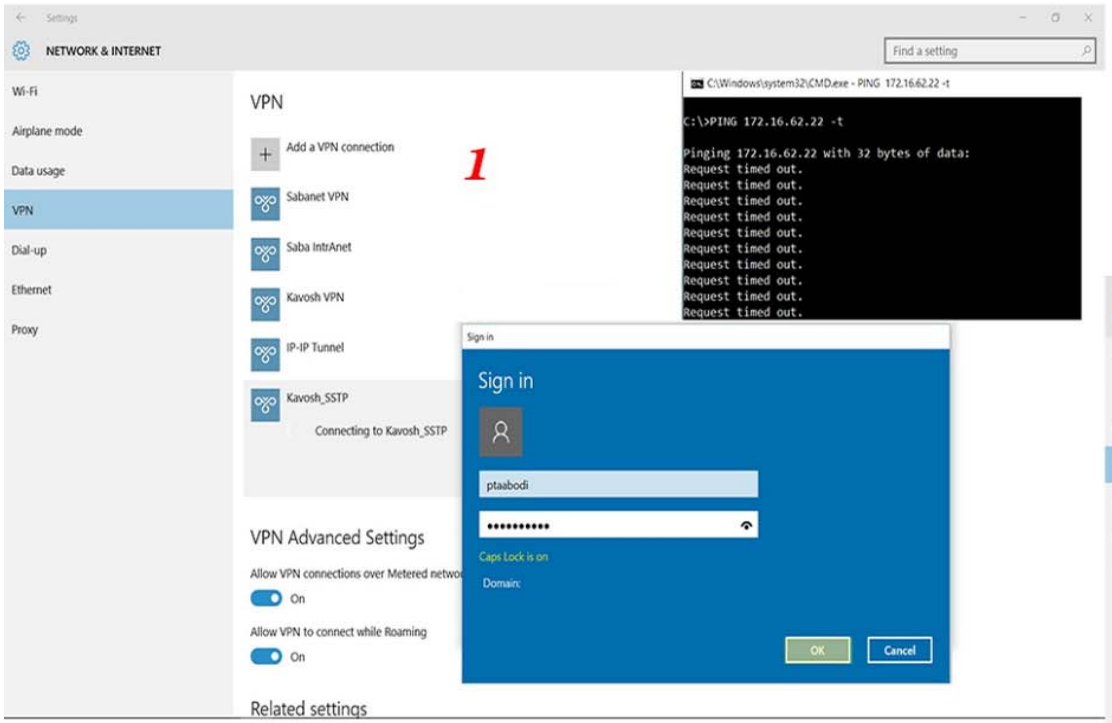
**Tip: (You can use Sample Configuration file that is located in "sample-config" folder and modify it according to your server configurations.*

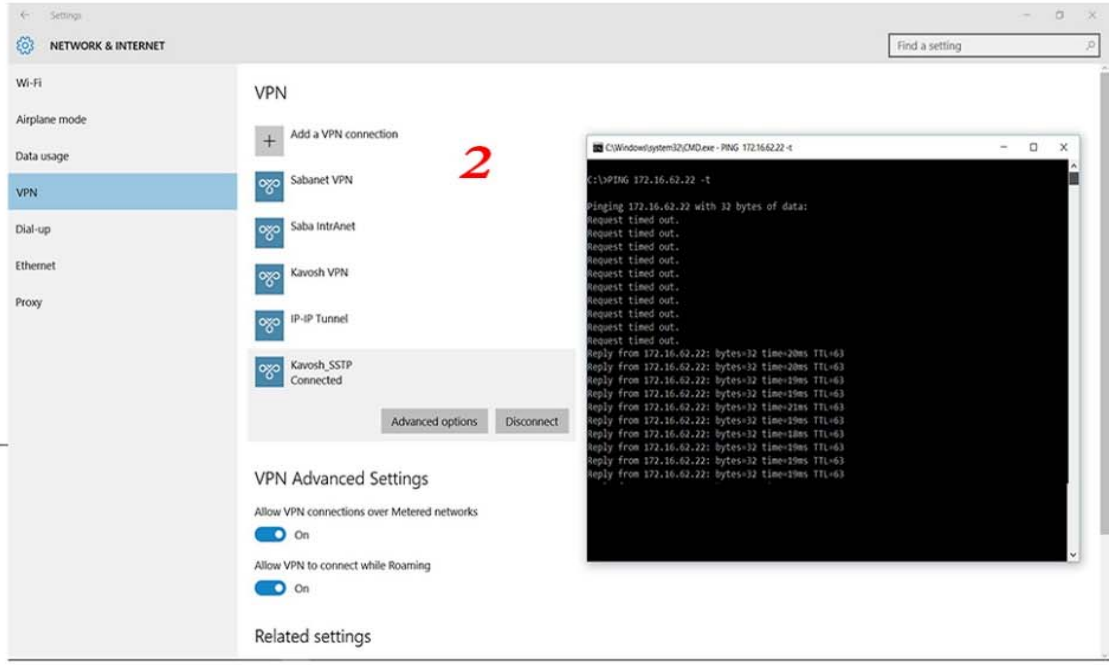
(See next slides)

Configuring SSTP Client on Microsoft Windows



Connecting to the MikroTik SSTP Server

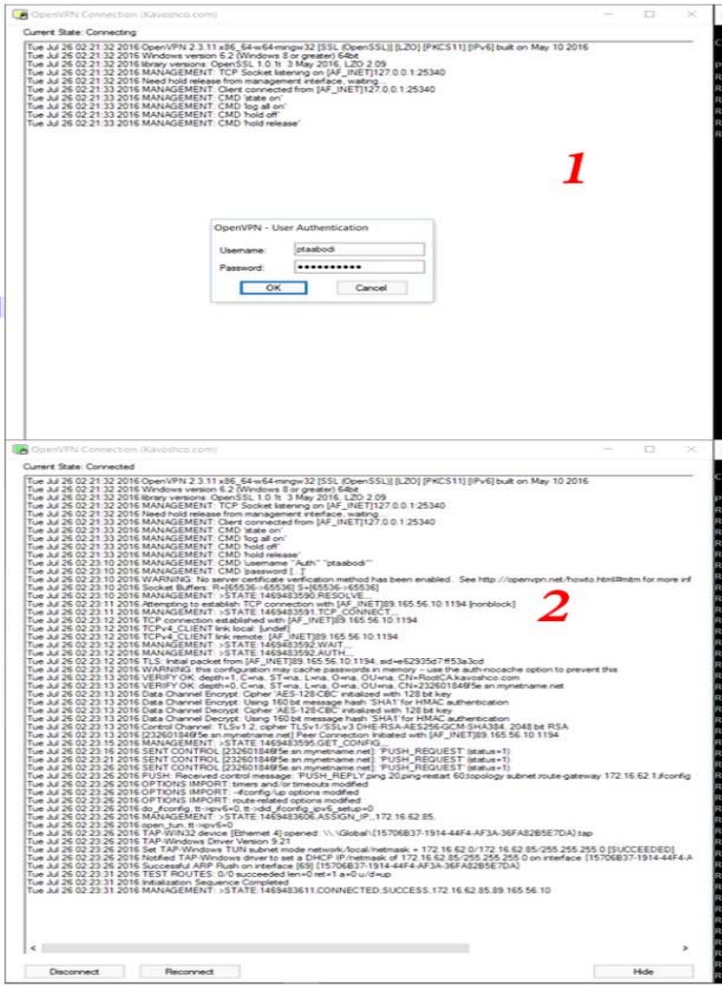


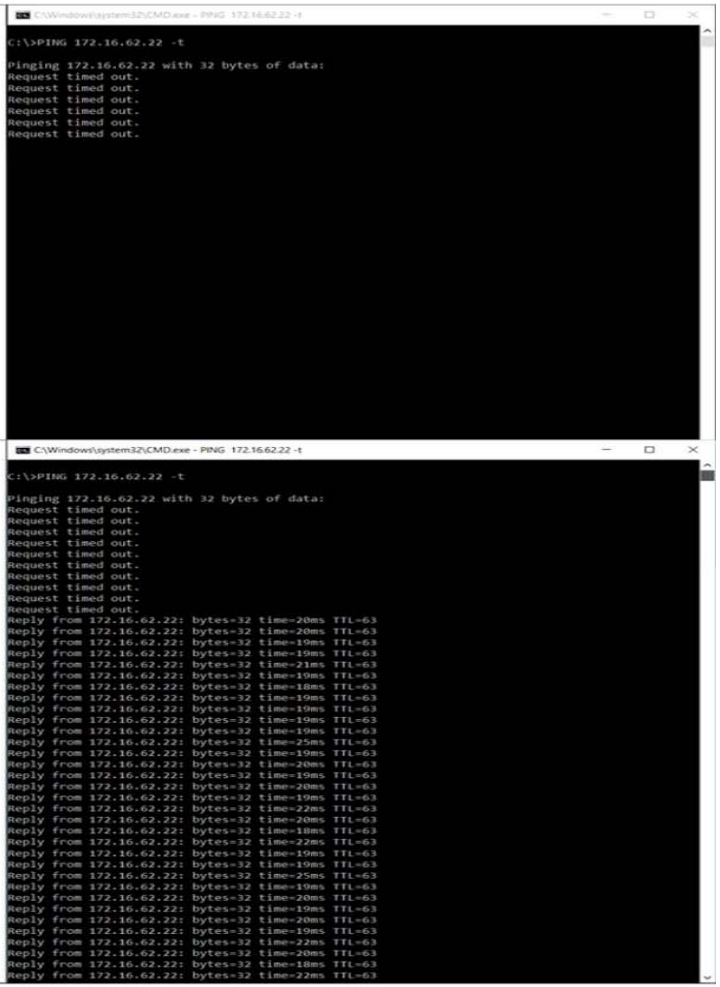


Connecting to the MikroTik OVPN Server

```
# Specify the type of the layer of the VPN connection.
# To connect to the VPN Server as a "Remote-Access VPN Client PC",
#  specify 'dev tun'. (Layer-3 IP Routing Mode)
# To connect to the VPN Server as a bridging equipment of "Site-to-Site VPN",
#  specify 'dev tap'. (Layer-2 Ethernet Bridgine Mode)

dev tun

################################################################################
# Specify either 'proto tcp' or 'proto udp'.

proto tcp

################################################################################
# The destination hostname / IP address, and port number of the target VPN Server

remote mik.kavoshco.com 1194   OR    89.165.56.10 1194

################################################################################
# The encryption and authentication algorithm.

cipher AES-128-CBC
auth SHA1

################################################################################
# Other parameters necessary to connect to the VPN Server.
# It is not recommended to modify it unless you have a particular need.

resolv-retry infinite
nobind
persist-key
persist-tun
client
verb 3
auth-user-pass

################################################################################
# The CA certificate file -(CA Publik Key).
<ca>
-----BEGIN CERTIFICATE-----
BhMCbmExCzAJBgNVBAgMAm5hMQswCQYDVQQHDAJuYTELMAkGA1UECgwCbmExCzAJ
BgNVBAsMAm5hMRwwGgYDVQQDDBNSb290Q0Eua2F2b3NoY28uY29tMB4XDTE2MDcy
NTIxMjIzOVoXDTMxMDcyMjIxMjIzOVowXzELMAkGA1UEBhMCbmExCzAJBgNVBAgM
Am5hMQswCQYDVQQHDA/80JP9SC4h38A==
-----END CERTIFICATE-----
</ca>
```

Sample of "Open VPN" Configuration File






Any Questions?

Thank You!

Powered by: Pooria Taabbodi

ptaabodi@hotmail.com