

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*

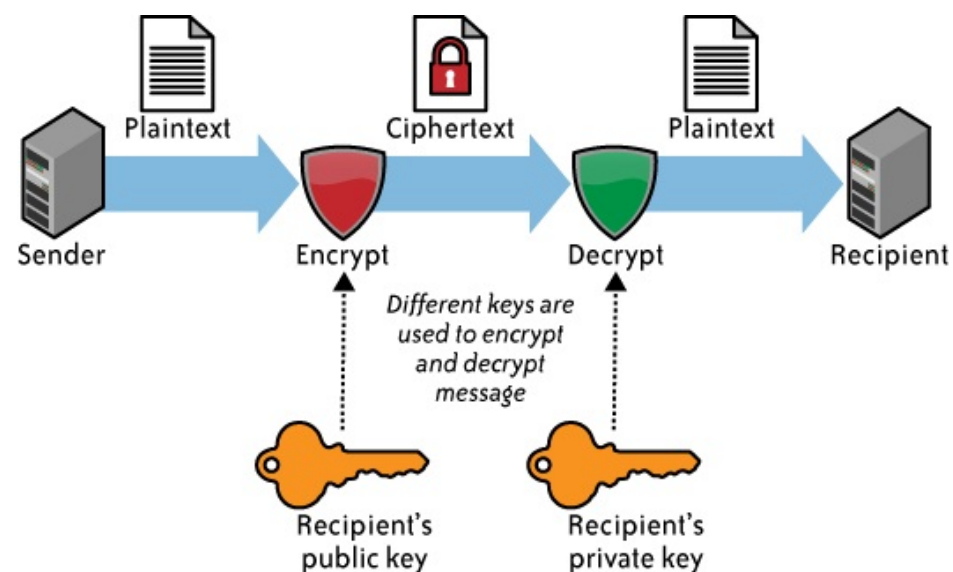
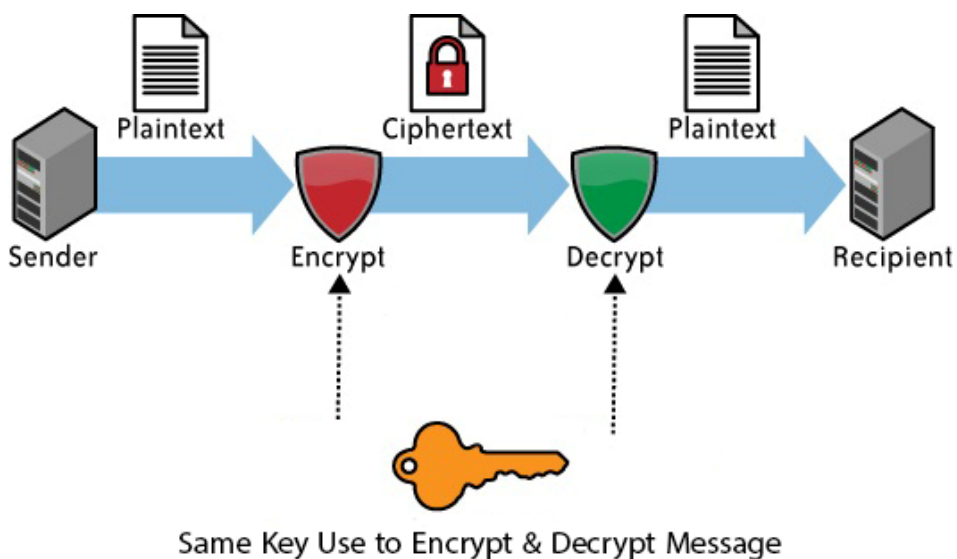
*Powered by: POORIA TAABBODI
October - 2016*

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**



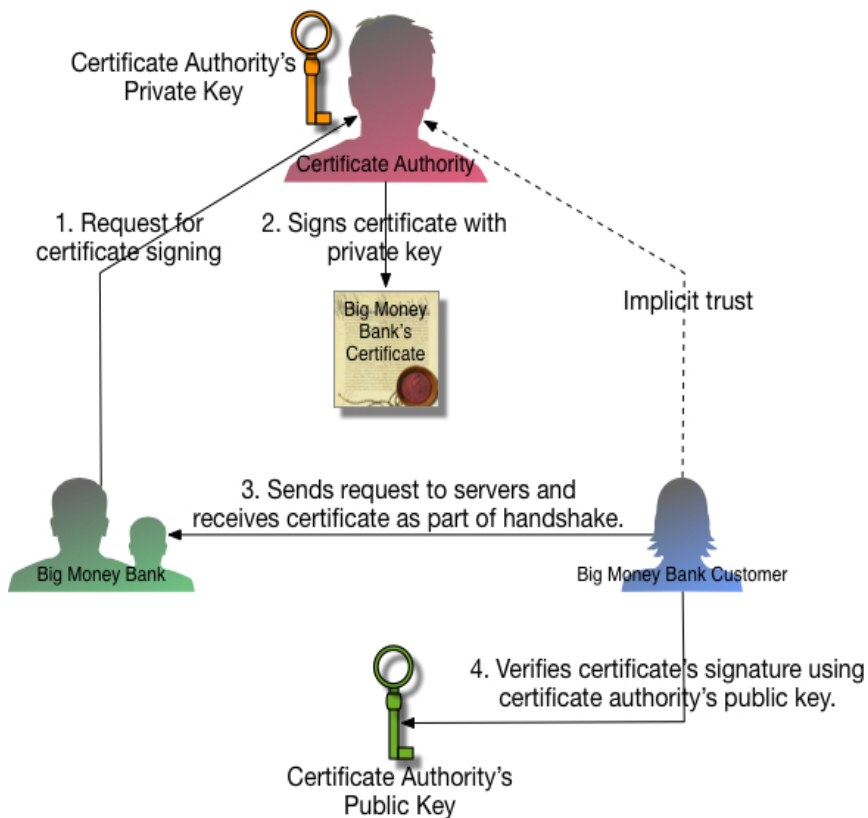
One of the most common Asymmetric Encryption methods is using computer certificates.

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...

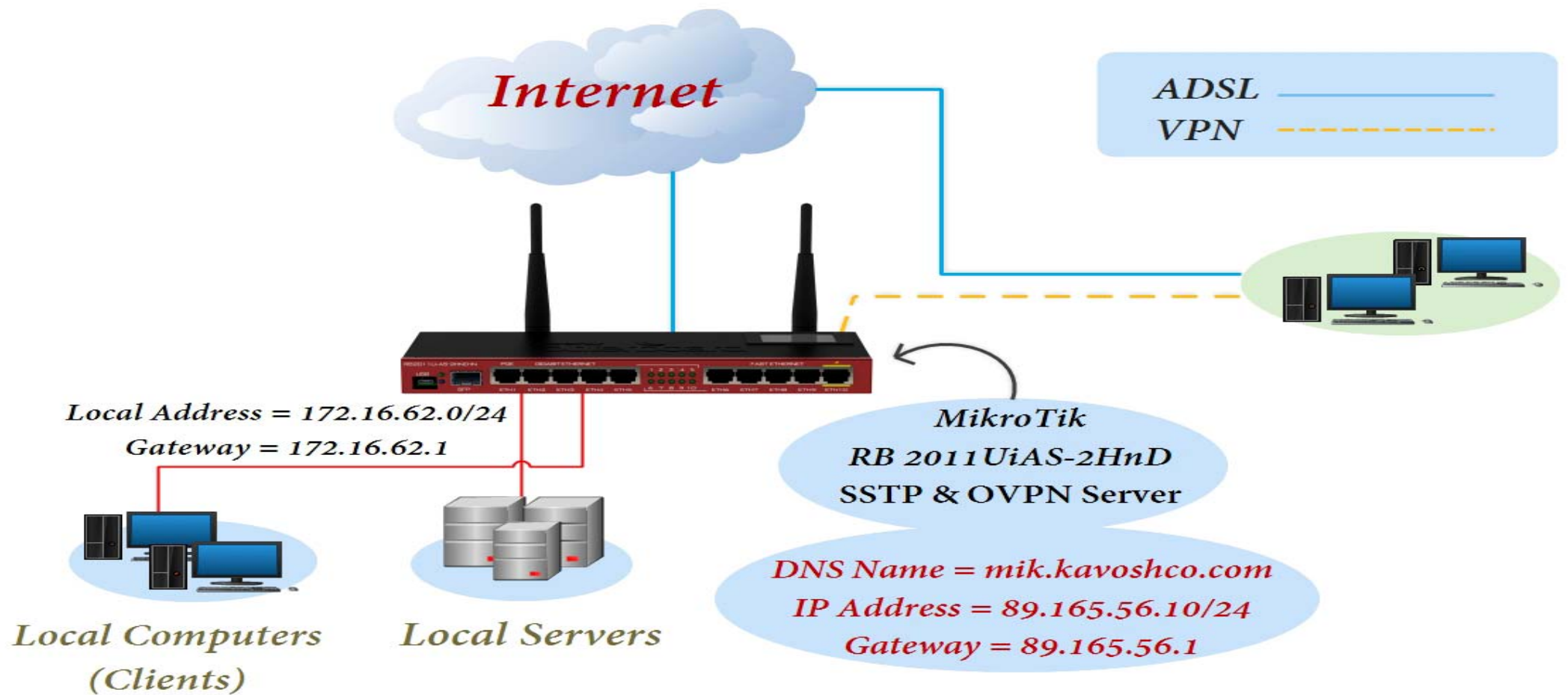


Any Questions?

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

The screenshot displays the MikroTik WinBox interface. The top status bar shows the user 'admin@89.165.56.10 (Kavosh-MikroTik)' on 'RB450G (mipsbe)' with system metrics: CPU: 3%, Memory: 224.4 MB, and Uptime: 24d 23:55:34. The left sidebar contains a menu with 'System' expanded to show 'Clock' (marked with a red '2') and 'SNTP Client' (marked with a red '1').

The 'Clock' configuration window is open, showing the following settings:

- Time: 23:45:41
- Date: Jul/25/2016
- Time Zone Autodetect
- Time Zone Name: Asia/Dubai
- GMT Offset: +04:00
- DST Active

The 'SNTP Client' configuration window is also open, showing the following settings:

- Enabled
- Mode: unicast
- Primary NTP Server: 104.209.134.106
- Secondary NTP Server: 172.16.62.2
- Server DNS Names: (empty)
- Dynamic Servers: (empty)
- Poll Interval: 900 s
- Active Server: 172.16.62.2
- Last Update From: 172.16.62.2
- Last Update: 00:03:50 ago
- Last Adjustment: -13 781 us
- Last Bad Packet From: (empty)
- Last Bad Packet: (empty)
- Last Bad Packet Reason: (empty)

Red arrows point from the 'Clock' and 'SNTP Client' menu items in the sidebar to their respective configuration windows. The numbers '1' and '2' are placed next to the configuration windows to identify them.

- *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

The screenshot displays the Mikrotik WinBox interface for configuring certificates. The main window is titled "Certificates" and contains several tabs: "Certificates", "SCEP Servers", "SCEP RA", "Requests", and "OTP". The "Certificates" tab is active, showing a table with columns for Name, Issuer, Common Name, Subject Alt. Name, Key Size, Days Valid, Trusted, SCEP URL, and CA. A red arrow points to the "+" icon in the top-left corner of the table, which is labeled "1A".

Below the table, there are three "New Certificate" dialog boxes. The first dialog, labeled "1A", is for creating a CA certificate. It has the following fields: Name (CA), Issuer, Country (na), State (na), Locality (na), Organization (na), Unit (na), Common Name (rootca.kavoshco.com), Subject Alt. Name (IP), Key Size (2048), and Days Valid (3650). The "Key Usage" section is also visible, with checkboxes for digital signature, key encipherment, data encipherment, key agreement, crl sign, encipher only, decipher only, server gated crypto, timestamp, ipsec tunnel, email protect, tls client, content commitment, data encipherment, key cert. sign, encipher only, dvcs, ocsp sign, ipsec user, ipsec end system, code sign, and tls server.

The second dialog, labeled "1B", is for creating a Server certificate. It has the following fields: Name (Server), Issuer, Country (na), State (na), Locality (na), Organization (na), Unit (na), Common Name (mik.kavoshco.com), Subject Alt. Name (IP), Key Size (2048), and Days Valid (365). The "Key Usage" section is also visible, with checkboxes for digital signature, key encipherment, data encipherment, key agreement, crl sign, encipher only, decipher only, server gated crypto, timestamp, ipsec tunnel, email protect, tls client, content commitment, data encipherment, key cert. sign, encipher only, dvcs, ocsp sign, ipsec user, ipsec end system, code sign, and tls server.

The third dialog, labeled "2A", is for creating a Certificate (Server). It has the following fields: Name (Server), Issuer, Country (na), State (na), Locality (na), Organization (na), Unit (na), Common Name (mik.kavoshco.com), Subject Alt. Name (IP), Key Size (2048), and Days Valid (365). The "Key Usage" section is also visible, with checkboxes for digital signature, key encipherment, data encipherment, key agreement, crl sign, encipher only, decipher only, server gated crypto, timestamp, ipsec tunnel, email protect, tls client, content commitment, data encipherment, key cert. sign, encipher only, dvcs, ocsp sign, ipsec user, ipsec end system, code sign, and tls server.

The fourth dialog, labeled "2B", is for creating a Certificate (Server). It has the following fields: Name (Server), Issuer, Country (na), State (na), Locality (na), Organization (na), Unit (na), Common Name (mik.kavoshco.com), Subject Alt. Name (IP), Key Size (2048), and Days Valid (365). The "Key Usage" section is also visible, with checkboxes for digital signature, key encipherment, data encipherment, key agreement, crl sign, encipher only, decipher only, server gated crypto, timestamp, ipsec tunnel, email protect, tls client, content commitment, data encipherment, key cert. sign, encipher only, dvcs, ocsp sign, ipsec user, ipsec end system, code sign, and tls server.

On the left side of the interface, there is a sidebar menu with various system and network configuration options. The "Certificates" option is highlighted in yellow. The top status bar shows the session information: "admin@89.165.56.10 (Kavosh-MikroTik) - WinBox v6.35.4 on RB450G (mipsbe)", "Session: 89.165.56.10", "CPU: 1%", "Memory: 224.3 MB", and "Uptime: 24d 23:59:12".

Signing Certificates

admin@89.165.56.10 (Kavosh-MikroTik) - WinBox v6.35.4 on RB450G (mipsbe)

Session Settings Dashboard

Session: 89.165.56.10 CPU: 2% Memory: 224.4 MiB Uptime: 25d 00:06:31

RouterOS WinBox

1

2

The screenshot displays the Mikrotik WinBox interface for configuring certificates. At the top, a table lists existing certificates:

Name	Issuer	Common Name	Subject Alt. N...	Key Size	Days Valid	Trusted	SCEP URL	CA
CA		rootca.kavoshco.com	::	2048	3650			
Server		mik.kavoshco.com	::	2048	365			

Two configuration windows are shown:

- Window 1 (Certificate <CA>):** Shows the configuration for the CA certificate. The Name is 'CA' and the Issuer is empty. A 'Sign' dialog box is open, showing 'Certificate: CA' and 'CA CRL Host: 89.165.56.10'. The 'Sign' button in this dialog is highlighted with a red arrow.
- Window 2 (Certificate <Server>):** Shows the configuration for the Server certificate. The Name is 'Server' and the Issuer is empty. A 'Sign' dialog box is open, showing 'Certificate: Server' and 'CA: CA'. The 'CA' dropdown in this dialog is highlighted with a red circle, and a red arrow points from the 'Sign' button in Window 1 to this 'CA' dropdown.

Both windows have a 'Status' tab selected, and the 'Sign' button in the 'Status' tab is highlighted in yellow.

Exporting CA Public Key

admin@89.165.56.10 (Kavosh-MikroTik) - WinBox v6.35.4 on RB450G (mipsbe)

Session Settings Dashboard

Safe Mode Session: 89.165.56.10

CPU: 3% Memory: 223.7 MB Uptime: 25d 01:03:57

- Quick Set
- CAPsMAN
- Interfaces
- Wireless
- Bridge
- PPP
- Switch
- Mesh
- IP
- MPLS
- Routing
- System
- Queues
- Files **3**
- Log
- Radius
- Tools
- New Terminal
- MetaROUTER
- Partition
- Make Supout.rif
- Manual
- New WinBox
- Exit

Certificates

SCEP Servers SCEP RA Requests OTP

Import Card Reinstall Card Verify Revoke Create Cert. Request

Name	Issuer	Common Name	Subject Alt. N...	Key Size	Days Valid	Trusted	SCEP URL
KAT	CA	rootca.kavoshco.com		2048	365	CA	
KA	Server	mik.kavoshco.com		2048	365	CA	

Export

Certificate: CA

Export Passphrase:

Export Cancel

File List

File Name	Type	Size	Creation Time
Last-VOIP-POTI-HA-Queue.backup	backup	515.7 KiB	Jul/23/2016 04:27:22
Last-VOIP-POTI-HA-Queue.rsc	script	64.5 KiB	Jul/23/2016 04:27:41
cert_export_CA.crt	.crt file	1330 B	Jul/26/2016 00:56:45
pub	directory		Apr/08/2015 17:24:43
skins	directory		Jan/02/1970 04:33:13

5 items 20.9 MiB of 512.0 MiB used 95% free

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

The screenshot displays the Windows Certificate Manager application (certlm.msc) window. The window title is "certlm - [Certificates - Local Computer]\Trusted Root Certification Authorities\Certificates". The left pane shows the tree view with "Certificates" selected. A context menu is open over "Certificates", with "Import..." highlighted. The right pane shows a list of certificates with columns: Issued To, Issued By, Expiration Date, Intended Purposes, and Friendly Name. Below the main window, a Run dialog box is open with "certlm.msc" entered in the "Open:" field. A red arrow points from the "Import..." option in the context menu to the "OK" button in the Run dialog box.

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Server Authenticati...	Th
AVG Technologies	AVG Technologies	6/24/2026	<All>	<N
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/13/2025	Server Authenticati...	Dig
Certum CA	Certum CA	6/11/2027	Server Authenticati...	Ce
Certum Trusted Network CA	Certum Trusted Network CA	12/31/2029	Server Authenticati...	Ce
Class 2 Primary CA	Class 2 Primary CA	7/7/2019	Secure Email, Serve...	Ce
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/2/2028	Secure Email, Client...	Ver
COMODO RSA Certification Au...	COMODO RSA Certification Auth...	1/19/2038	Server Authenticati...	CC
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/31/1999	Time Stamping	Mi
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/10/2031	Server Authenticati...	Dig
DigiCert Global Root CA	DigiCert Global Root CA	11/10/2031	Server Authenticati...	Dig
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	11/10/2031	Server Authenticati...	Dig
DST Root CA X3	DST Root CA X3	9/30/2021	Secure Email, Serve...	DS
Entrust Root Certification Auth...	Entrust Root Certification Authority	11/28/2026	Server Authenticati...	Ent
Entrust Root Certification Auth...	Entrust Root Certification Authori...	12/7/2030	Server Authenticati...	Ent
Entrust.net Certification Author...	Entrust.net Certification Authority...	7/24/2029	Server Authenticati...	Ent
Equifax Secure Certificate Auth...	Equifax Secure Certificate Authority	8/22/2018	Secure Email, Serve...	Ge
GeoTrust Global CA	GeoTrust Global CA	5/21/2022	Server Authenticati...	Ge
GeoTrust Primary Certification ...	GeoTrust Primary Certification Au...	7/17/2036	Server Authenticati...	Ge
GeoTrust Primary Certification ...	GeoTrust Primary Certification Au...	12/2/2037	Server Authenticati...	Ge
GlobalSign	GlobalSign	3/18/2029	Server Authenticati...	Glc
GlobalSign	GlobalSign	12/15/2021	Server Authenticati...	Glc
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Server Authenticati...	Glc

- *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

The screenshot displays the Mikrotik WinBox interface. The top bar shows the user 'admin@89.165.56.10 (Kavosh-MikroTik)' and the session ID '89.165.56.10'. The left sidebar contains a menu with categories like IP, Routing, System, and Tools. The 'IP' category is expanded, and the 'Pool' option is selected. A red arrow points from the 'Pool' menu item to a dialog box titled 'IP Pool'. This dialog box has two tabs: 'Pools' and 'Used Addresses'. The 'Pools' tab is active, showing a table with columns for Name, Addresses, and Next Pool. A new entry is being added, with the following details:

- Name: SSTP_POOL
- Addresses: 172.16.62.81-172.16.62.91
- Next Pool: none

The dialog box also includes buttons for OK, Cancel, Apply, Copy, and Remove. The status bar at the bottom of the dialog indicates '5 items (1 selected)'. The top right corner of the WinBox window shows system statistics: CPU: 0%, Memory: 223.9 MiB, and Uptime: 25d 00:12:28.

Creating “PPP Profile” for SSTP & OVPN Connections

The screenshot displays the Mikrotik WinBox interface. On the left sidebar, the 'PPP' menu item is highlighted with a red arrow. The main window shows the 'PPP' configuration page with the 'Profiles' tab selected. Below this, two 'New PPP Profile' dialog boxes are open. The left dialog is for a profile named 'SSTP_Profile' with the following settings:

- Name: SSTP_Profile
- Local Address: 172.16.62.1
- Remote Address: SSTP_POOL
- Bridge: (empty)
- Bridge Port Priority: (empty)
- Bridge Path Cost: (empty)
- Incoming Filter: (empty)
- Outgoing Filter: (empty)
- Address List: (empty)
- DNS Server: 172.16.62.2
- WINS Server: (empty)
- Change TCP MSS: no yes default
- Use UPnP: no yes default

The right dialog is for a profile named 'SSTP_Profile' with the following settings:

- Use MPLS: no yes required default
- Use Compression: no yes default
- Use Encryption: no yes required default

A red arrow points from the 'Profiles' tab in the main window to the 'SSTP_Profile' dialog. Another red arrow points from the 'SSTP_Profile' dialog to the 'SSTP_Profile' dialog.

Creating "PPP Secret" for SSTP & OVPN Connections

The screenshot displays the Mikrotik WinBox interface. On the left, a sidebar menu lists various system components, with 'PPP' highlighted. A red arrow points from this menu item to the 'PPP' configuration window. Inside this window, the 'Secrets' tab is active, and another red arrow points to the '+' icon used to add a new secret. A 'New PPP Secret' dialog box is open, showing the following configuration:

- Name: ptaabodi
- Password: [masked]
- Service: any
- Caller ID: [empty]
- Profile: SSTP_Profile
- Local Address: [empty]
- Remote Address: [empty]
- Routes: [empty]
- Limit Bytes In: [empty]
- Limit Bytes Out: [empty]
- Last Logged Out: [empty]
- enabled

Buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', and 'Remove' are visible on the right side of the dialog box. The background shows a table with columns for Name, Password, Service, Caller ID, Profile, Local Address, Remote Address, and Last Logged Out.

Enabling & Configuring SSTP Server

admin@89.165.56.10 (Kavosh-MikroTik) - WinBox v6.35.4 on RB450G (mipsbe)

Session Settings Dashboard

Safe Mode Session: 89.165.56.10 CPU:3% Memory:223.9 MB Uptime:25d 00:41:16

RouterOS WinBox

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

PPP

Interface PPPoE Servers Secrets Profiles Active Connections L2TP Secrets

PPP Scanner PPTP Server **SSTP Server** L2TP Server OVPN Server PPPoE Scan

Name	Type	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx	FP Tx Packet (p/s)	FP Rx Packet (p/s)
------	------	--------	----	----	-----------------	-----------------	-------	-------	--------------------	--------------------

SSTP Server

Enabled

Port: 443

Max MTU: 1500

Max MRU: 1500

MRRU: [dropdown]

Keepalive Timeout: 60

Default Profile: SSTP_Profile

Authentication: mschap2 mschap1
 chap pap

Certificate: Server

TLS Version: any

Verify Client Certificate
 Force AES
 PFS

OK
Cancel
Apply

Enabling & Configuring OVPN Server

admin@89.165.56.10 (Kavosh-MikroTik) - WinBox v6.35.4 on RB450G (mipsbe)

Session Settings Dashboard

Safe Mode Session: 89.165.56.10 CPU:3% Memory:223.9 MB Uptime:25d 00:46:21

RouterOS WinBox

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

PPP

Interface PPPoE Servers Secrets Profiles Active Connections L2TP Secrets

PPP Scanner PPTP Server SSTP Server L2TP Server OVPN Server PPPoE Scan

Name	Type	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx	FP Tx Packet (p/s)	FP Rx Pa
------	------	--------	----	----	-----------------	-----------------	-------	-------	--------------------	----------

OVPN Server

Enabled

Port: 1194

Mode: ip

Netmask: 24

MAC Address: FE:43:F7:71:07:09

Max MTU: 1500

Keepalive Timeout: 60

Default Profile: SSTP_Profile

Certificate: Server

Require Client Certificate

Auth.: sha1 md5
 null

Cipher: blowfish 128 aes 128
 aes 192 aes 256
 null

OK
Cancel
Apply

Enabling “ARP Proxy” on Local Interface

admin@89.165.56.10 (Kavosh-MikroTik) - WinBox v6.35.4 on RB450G (mipsbe)

Session Settings Dashboard

Safe Mode Session: 89.165.56.10 CPU: 3% Memory: 223.9 MiB Uptime: 25d 01:00:28

RouterOS WinBox

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

Interface List

Interface	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel	VLAN	VRRP	Bonding	LTE
R ether1								
R ether2								
RS ether3								
RS ether4								
RS ether5								

Interface <ether2 In < Server 2.0 >

General Ethernet Overall Stats Rx Stats Tx Stats Status ...

Name: ether2 -> Local_Network

Type: Ethernet

MTU: 1500

L2 MTU: 1520

Max L2 MTU: 1520

MAC Address: 00:0C:42:59:37:EA

ARP: proxy-arp

Master Port: none

Bandwidth (Rx/Tx): unlimited / unlimited

Switch: switch1

OK
Cancel
Apply
Disable
Comment
Torch
Cable Test
Blink
Reset MAC Address
Reset Counters

	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx	FP Tx Packet (p/s)	FP Rx Packet (p/s)
pps	56.1 kbps	130	78	0 bps	0 bps	0	0
pps	0 bps	0	0	0 bps	0 bps	0	0
pps	322.8 kbps	266	311	0 bps	0 bps	0	0
pps	403.2 kbps	359	232	0 bps	0 bps	0	0
pps	30.2 kbps	35	34	0 bps	0 bps	0	0

- *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

1 Network and Sharing Center

Control Panel > All Control Panel Items > Network and Sharing Center

View your basic network information and set up connections

View your active networks

Freedom 2
Private network

Change your networking settings

[Set up a new connection or network](#)
Set up a broadband, dial-up, or VPN connection; or set up a new network.

2 Set Up a Connection or Network

Choose a connection option

- Connect to the Internet
Set up a broadband or dial-up connection to the Internet.
- Set up a new network
Set up a new router or access point.
- Manually connect to a wireless network
Connect to a hidden network or create a new wireless profile.
- Connect to a workplace**
Set up a dial-up or VPN connection to your workplace.

3 Connect to a Workplace

How do you want to connect?

- Use my Internet connection (VPN)**
Connect using a virtual private network (VPN) connection through the Internet.
- Dial directly
Connect directly to a phone number without going through the Internet.

4 Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address:

Destination name:

Use a smart card

Remember my credentials

Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

5 Kavosh_SSTP Properties

General Options Security Networking Sharing

Type of VPN:
Secure Socket Tunneling Protocol (SSTP)

Data encryption:
Require encryption (disconnect if server declines)

Authentication

Use Extensible Authentication Protocol (EAP)

Allow these protocols

- Unencrypted password (PAP)
- Challenge Handshake Authentication Protocol (CHAP)
- Microsoft CHAP Version 2 (MS-CHAP v2)
 - Automatically use my Windows logon name and password (and domain, if any)

OK Cancel

Connecting to the MikroTik SSTP Server

1

Settings - NETWORK & INTERNET

VPN

- + Add a VPN connection
- Sabanet VPN
- Saba IntraNet
- Kavosh VPN
- IP-IP Tunnel
- Kavosh_SSTP

Connecting to Kavosh_SSTP

VPN Advanced Settings

- Allow VPN connections over Metered networks: On
- Allow VPN to connect while Roaming: On

Related settings

```
C:\Windows\system32\CMD.exe - PING 172.16.62.22 -t
C:\>PING 172.16.62.22 -t
Pinging 172.16.62.22 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

2

Settings - NETWORK & INTERNET

VPN

- + Add a VPN connection
- Sabanet VPN
- Saba IntraNet
- Kavosh VPN
- IP-IP Tunnel
- Kavosh_SSTP Connected

Advanced options Disconnect

VPN Advanced Settings

- Allow VPN connections over Metered networks: On
- Allow VPN to connect while Roaming: On

Related settings

```
C:\Windows\system32\CMD.exe - PING 172.16.62.22 -t
C:\>PING 172.16.62.22 -t
Pinging 172.16.62.22 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 172.16.62.22: bytes=32 time=20ms TTL=63
Reply from 172.16.62.22: bytes=32 time=20ms TTL=63
Reply from 172.16.62.22: bytes=32 time=19ms TTL=63
Reply from 172.16.62.22: bytes=32 time=19ms TTL=63
Reply from 172.16.62.22: bytes=32 time=21ms TTL=63
Reply from 172.16.62.22: bytes=32 time=19ms TTL=63
Reply from 172.16.62.22: bytes=32 time=18ms TTL=63
Reply from 172.16.62.22: bytes=32 time=19ms TTL=63
Reply from 172.16.62.22: bytes=32 time=19ms TTL=63
Reply from 172.16.62.22: bytes=32 time=19ms TTL=63
```

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 Bridging 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-----
BhMChmExCzAJBgNVBAGMAm5hMQswCQYDVQQLHDAuYUJTElMAkGALUECGwChmExCzAJ
BgNVBAsMAm5hMRwwGgYDVQQDDBNsb290Q0Eua2F2b3NoY28uY29tY29tY29tY29tY29t
NTIxMjIzOVoXDTMxMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYy
Am5hMQswCQYDVQQLHDAuYUJTElMAkGALUECGwChmExCzAJBgNVBAGMAm5hMQswCQYDVQQLHDAuYUJTElMAkGALUECGwChmExCzAJ
-----END CERTIFICATE-----
</ca>
```

Sample of "Open VPN" Configuration File

The screenshot shows the OpenVPN Client Manager interface. The top window displays the current state as 'Connecting' and shows a log of events including TCP socket listening, client connection, and management commands. A red '1' is overlaid on this window. Below it, a 'User Authentication' dialog box is shown with 'staabod' entered in the Username field and a masked password in the Password field. The bottom window shows the current state as 'Connected' and displays a detailed log of the connection process, including the establishment of a TCP connection, the start of the OpenVPN client, and the successful completion of the connection. A red '2' is overlaid on this window.

The screenshot shows a Windows command prompt window with the command 'ping 172.16.62.22 -t' entered. The output shows a series of 'Request timed out.' messages, indicating that the connection to the specified IP address is failing. The window title is 'C:\Windows\system32\cmd.exe - PING 172.16.62.22 -t'.

Any Questions?

Thank You!



Powered by: Pooria Taabbodi

ptaabodi@hotmail.com