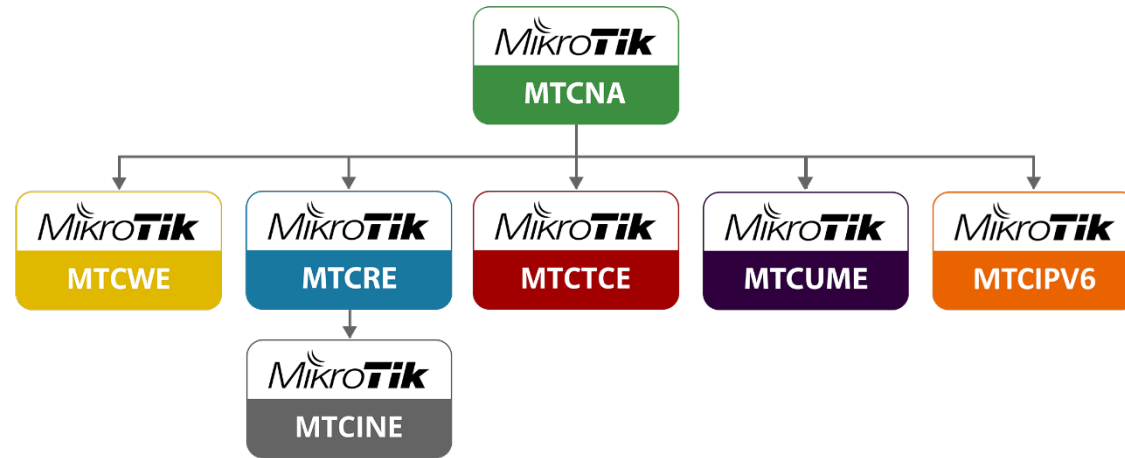


Highly loaded certificate-based VPN solution

By Eugeniu CROITOROV, MUM Moldova 2019

About ME

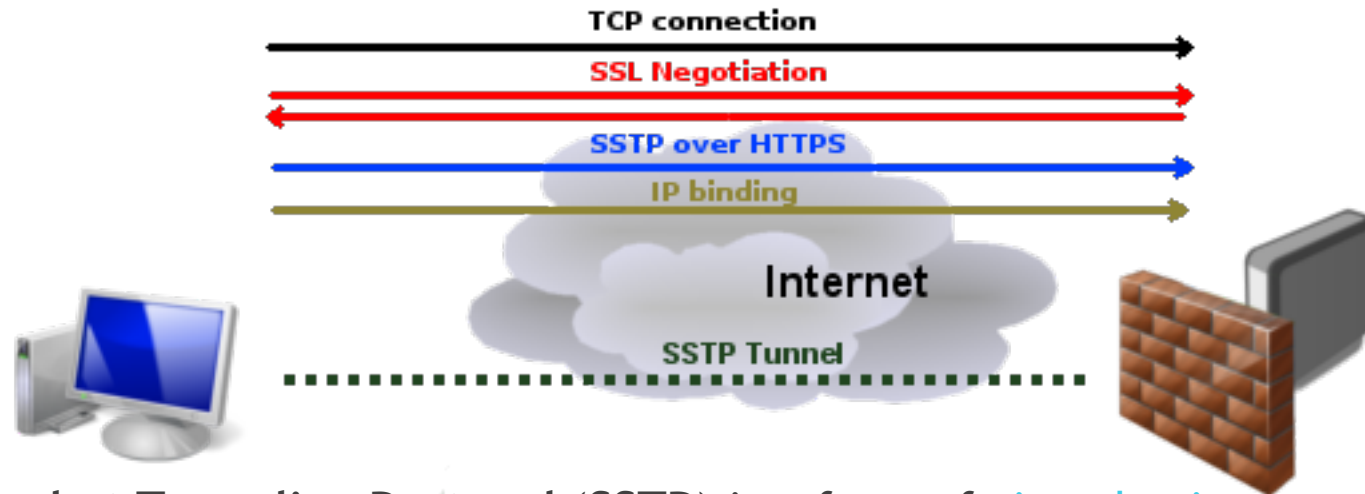
- ▶ Name: Eugeniu CROITOROV
- ▶ Employment: Information Technology and Cyber Security Service (2012-present)
- ▶ MikroTik experience: from 2013
- ▶ Certificates:



Which type of VPN is Right for you?

- ▶ PPTP - obsolete, many security issues
- ▶ L2TP+IPSec - Use IPSec UDP 500,4500,1701 ports
- ▶ SSTP - SSL/TLS encryption, Use TCP 443 port
- ▶ OpenVPN - Opensource, Use TCP 1194 port

What is SSTP?



- ▶ **Secure Socket Tunneling Protocol (SSTP)** is a form of [virtual private network](#) (VPN) tunnel that provides a mechanism to transport [PPP](#) traffic through an [SSL/TLS](#) channel.
- ▶ **TCP 443** - Difficult to block because it use the same port as HTTPS

Advantages and disadvantages

ADNAVTTAGES

- ▶ SSTP encryption offers a decent level of security, almost on par with OpenVPN (SSL 3.0 + 256-bit encryption).
- ▶ SSTP is easy to configure on platforms it is built into.
- ▶ The SSTP VPN protocol is very difficult to block because it uses TCP port 443 (the same one HTTPS uses).
- ▶ SSTP offers good speeds if you have enough bandwidth.

DISADNAVTTAGES

- SSTP is closed-source and solely owned by Microsoft.
- The SSTP protocol is available on a limited number of platforms - Windows, Linux, Android, and routers.

The challenge

- ▶ 4000+ VPN clients
- ▶ Data encryption and integrity
- ▶ High availability
- ▶ Scalability



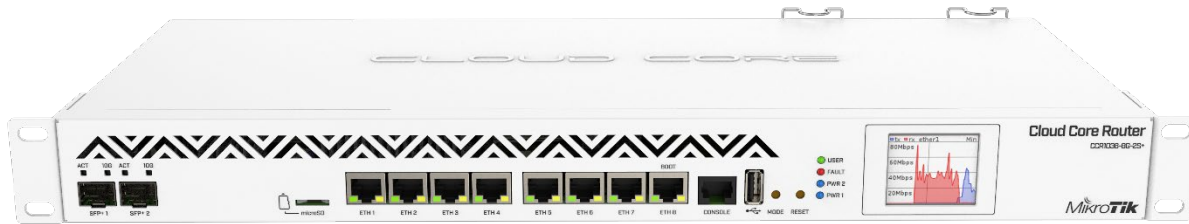
Routeros License level

Level number	0 (Trial mode)	1 (Free Demo)	3 (WISP CPE)	4 (WISP)	5 (WISP)	6 (Controller)
Price	no key 🔗	registration required 🔗	do not sell	\$45	\$95	\$250
Initial Config Support	-	-	-	15 days	30 days	30 days
Wireless AP	24h trial	-	-	yes	yes	yes
Wireless Client and Bridge	24h trial	-	yes	yes	yes	yes
RIP, OSPF, BGP protocols	24h trial	-	yes(*)	yes	yes	yes
EoIP tunnels	24h trial	1	unlimited	unlimited	unlimited	unlimited
PPPoE tunnels	24h trial	1	200	200	500	unlimited
PPTP tunnels	24h trial	1	200	200	500	unlimited
L2TP tunnels	24h trial	1	200	200	500	unlimited
OVPN tunnels	24h trial	1	200	200	unlimited	unlimited
VLAN interfaces	24h trial	1	unlimited	unlimited	unlimited	unlimited
HotSpot active users	24h trial	1	1	200	500	unlimited
RADIUS client	24h trial	-	yes	yes	yes	yes
Queues	24h trial	1	unlimited	unlimited	unlimited	unlimited
Web proxy	24h trial	-	yes	yes	yes	yes
User manager active sessions	24h trial	1	10	20	50	Unlimited
Number of KVM guests	none	1	Unlimited	Unlimited	Unlimited	Unlimited

Routers License level

Level number	0 (Trial mode)	1 (Free Demo)	3 (WISP CPE)	4 (WISP)	5 (WISP)	6 (Controller)
Price	no key 🔗	registration required 🔗	do not sell	\$45	\$95	\$250
Initial Config Support	-	-	-	15 days	30 days	30 days
Wireless AP	24h trial	-	-	yes	yes	yes
Wireless Client and Bridge	24h trial	-	yes	yes	yes	yes
RIP, OSPF, BGP protocols	24h trial	-	yes(*)	yes	yes	yes
EoIP tunnels	24h trial	1	unlimited	unlimited	unlimited	unlimited
PPPoE tunnels	24h trial	1	200	200	500	unlimited
PPTP tunnels	24h trial	1	200	200	500	unlimited
L2TP tunnels	24h trial	1	200	200	500	unlimited
OVPN tunnels	24h trial	1	200	200	unlimited	unlimited
VLAN interfaces	24h trial	1	unlimited	unlimited	unlimited	unlimited
HotSpot active users	24h trial	1	1	200	500	unlimited
RADIUS client	24h trial	-	yes	yes	yes	yes
Queues	24h trial	1	unlimited	unlimited	unlimited	unlimited
Web proxy	24h trial	-	yes	yes	yes	yes
User manager active sessions	24h trial	1	10	20	50	Unlimited
Number of KVM guests	none	1	Unlimited	Unlimited	Unlimited	Unlimited

Which platform to choose?



36 core 1.4Ghz CPU
4GB RAM
IPsec hardware acceleration
License Level6



9 core 1.2Ghz CPU
2GB RAM
IPsec hardware acceleration
License Level6

Which platform to choose?



36 core 1.4Ghz CPU
4GB RAM
IPsec hardware acceleration
License Level6



9 core 1.2Ghz CPU
2GB RAM
IPsec hardware acceleration
License Level6

Cloud hosted router



- ▶ Virtualized platform
- ▶ Can run on multiple hypervisors:
 - ▶ VMware
 - ▶ XEN
 - ▶ HyperV
 - ▶ Virtualbox
 - ▶ Others
- ▶ CHR has full RouterOS features enabled by default but has a different licensing model than other RouterOS versions.

CHR License

License		Speed limit	Price
Free	1Mbit		FREE
P1	1Gbit		\$45
P10	10Gbit		\$95
P-Unlimited	Unlimited		\$250



HOW TO GET SSL CERTIFICATE?

- ▶ Self-signed certificate
 - ▶ RouterOS
 - ▶ OpenSSL
- ▶ Commercial SSL certificate
 - ▶ Comodo
 - ▶ Symantec
 - ▶ Unizeto
- ▶ Free SSL certificate
 - ▶ Let's Encrypt
 - ▶ SSL For FREE

HOW TO GET SSL CERTIFICATE?

[certbot instructions](#)[about certbot](#)[contribute to certbot](#)[hosting providers with https](#)[get help](#)[donate](#)

certbot instructions

My HTTP website is running on

[Help, I'm not sure!](#)

To use Certbot, you'll need...



comfort with the [command line](#) ?



...and an HTTP website ?
that is [already online](#) ?
with an open [port 80](#) ?



...which is hosted on a [server](#) ?
which you can access via [SSH](#) ?
with the ability to [sudo](#) ?
optional if you want a [wildcard cert](#) :
[DNS credentials](#) ?

mum
Mikrotik User Meeting

MikroTik

HOW TO GET SSL CERTIFICATE?

1. Install CertBot using official manuals
<https://certbot.eff.org/#ubuntuxenial-other>
2. Create Certificates manually and put domain TXT record

#certbot certonly --preferred-challenges=dns --manual -d *.\$DOMAIN

```
[Eugenius-MacBook-Pro:~ eugeniucroitorov$ sudo certbot -d *.croitorov.eu -d croitorov.eu --manual --preferred-challenges dns certonly
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator manual, Installer None
Obtaining a new certificate
Performing the following challenges:
dns-01 challenge for croitorov.eu
dns-01 challenge for croitorov.eu

-----
NOTE: The IP of this machine will be publicly logged as having requested this
certificate. If you're running certbot in manual mode on a machine that is not
your server, please ensure you're okay with that.

Are you OK with your IP being logged?
-----
(Y)es/(N)o: █
```

HOW TO GET SSL CERTIFICATE?

3. Now you need to create a DNS TXT record on your domain name

```
Eugenius-MacBook-Pro:~ eugeniucroitorov$ sudo certbot -d *.croitorov.eu -d croitorov.eu --manual --prefer-
red-challenges dns certonly
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator manual, Installer None
Obtaining a new certificate
Performing the following challenges:
dns-01 challenge for croitorov.eu
dns-01 challenge for croitorov.eu

-----
NOTE: The IP of this machine will be publicly logged as having requested this
certificate. If you're running certbot in manual mode on a machine that is not
your server, please ensure you're okay with that.

Are you OK with your IP being logged?
-----
(Y)es/(N)o: Y

-----
Please deploy a DNS TXT record under the name
_acme-challenge.croitorov.eu with the following value:

4JN5bWoCD5RePXPTbPcw0RypFTiw001n1LTHk437XbU

Before continuing, verify the record is deployed.
-----
Press Enter to Continue
```


HOW TO GET SSL CERTIFICATE?

[Add record](#)[Advanced](#)

_acme-challenge.croitorov.eu has a record with content **XqLE6BrwFGpAWUEeCCj5fgCuqPpoErKB_IElIZkSgUM**.

Type

Name *

TTL

TXT

_acme-challenge.croitorov.eu

Auto

Content *

XqLE6BrwFGpAWUEeCCj5fgCuqPpoErKB_IElIZkSgUM

Cancel

Save

Type	Name	Content	TTL	Proxy status
TXT	_acme-challenge	XqLE6BrwFGpAWUEeCCj5fgCuqPpo...	Auto	DNS only

HOW TO GET SSL CERTIFICATE?

```
eugeniucroitorov — -bash — 105x35
NOTE: The IP of this machine will be publicly logged as having requested this
certificate. If you're running certbot in manual mode on a machine that is not
your server, please ensure you're okay with that.

Are you OK with your IP being logged?
-----
(Y)es/(N)o: Y

-----
Please deploy a DNS TXT record under the name
_acme-challenge.croitorov.eu with the following value:

XqLE6BrwFGpAWUEeCCj5fgCuqPpoErKB_IEI1ZkSgUM

Before continuing, verify the record is deployed.
-----
Press Enter to Continue
Waiting for verification...
Cleaning up challenges

IMPORTANT NOTES:
- Congratulations! Your certificate and chain have been saved at:
  /etc/letsencrypt/live/croitorov.eu/fullchain.pem
  Your key file has been saved at:
  /etc/letsencrypt/live/croitorov.eu/privkey.pem
  Your cert will expire on 2019-12-05. To obtain a new or tweaked
  version of this certificate in the future, simply run certbot
  again. To non-interactively renew *all* of your certificates, run
  "certbot renew"
- If you like Certbot, please consider supporting our work by:

  Donating to ISRG / Let's Encrypt:  https://letsencrypt.org/donate
  Donating to EFF:                   https://eff.org/donate-le

Eugenius-MacBook-Pro:~ eugeniucroitorov$
```

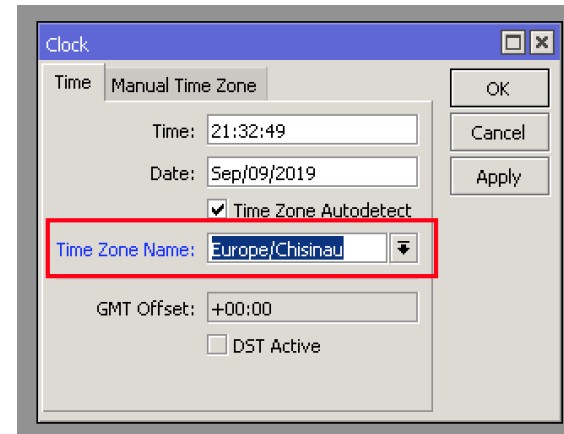
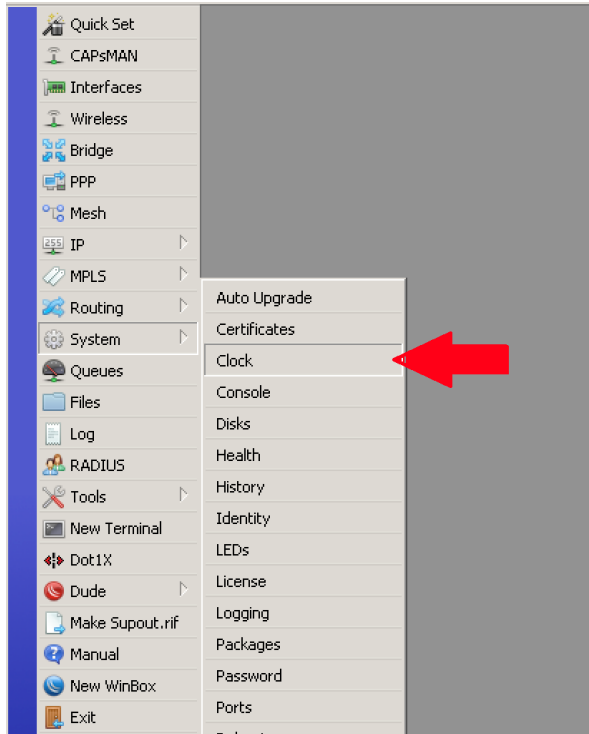
Mikrotik Configuration

mum

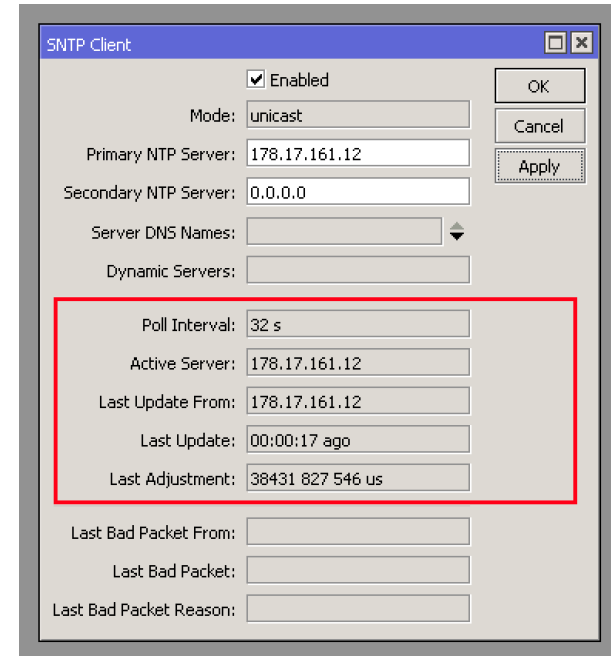
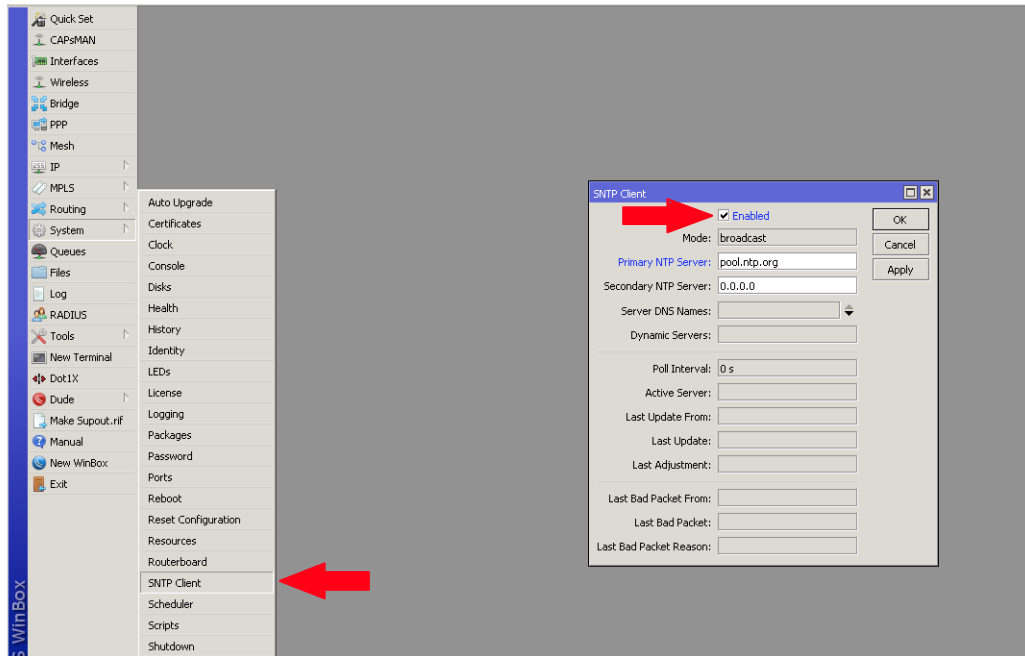
Mikrotik User Meeting

*Mikro***Tik**

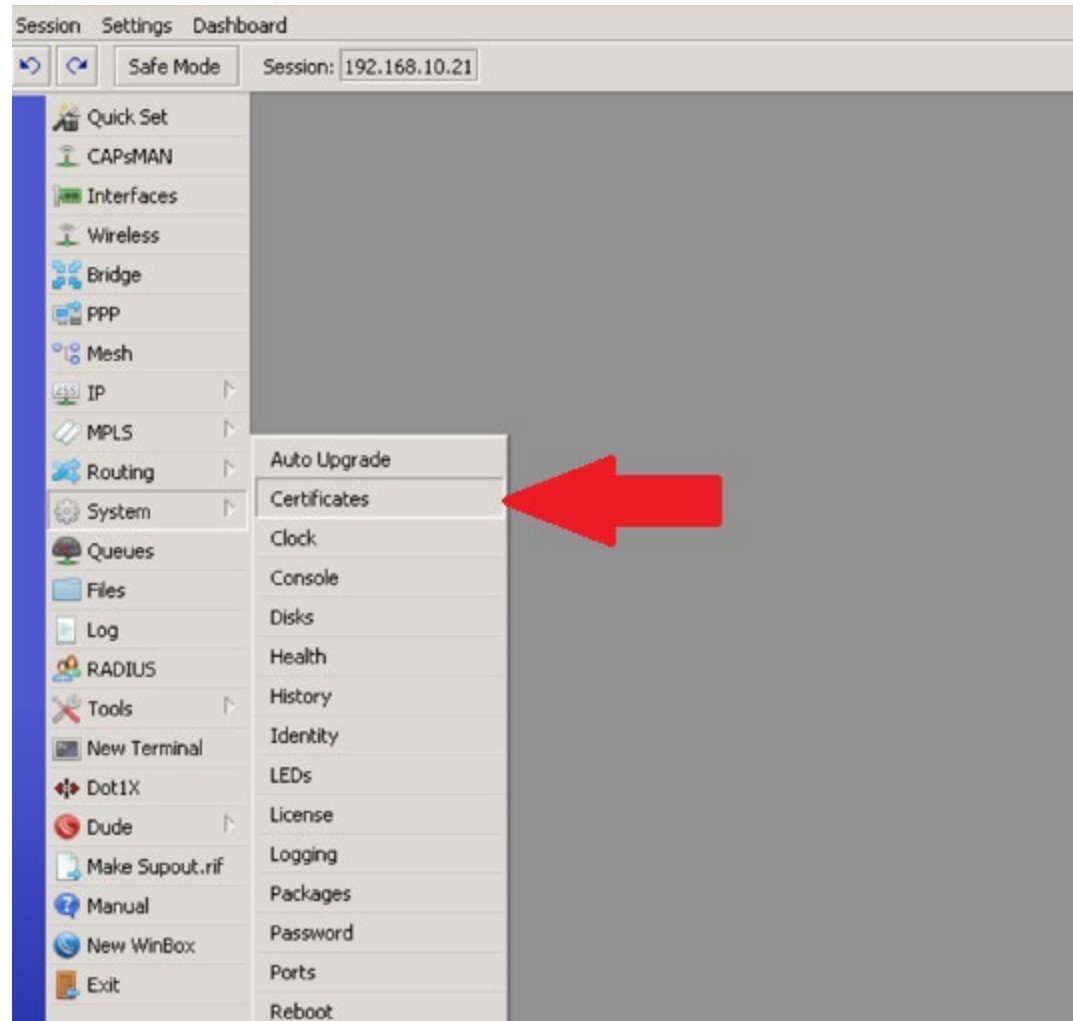
Clock & Time zone setting



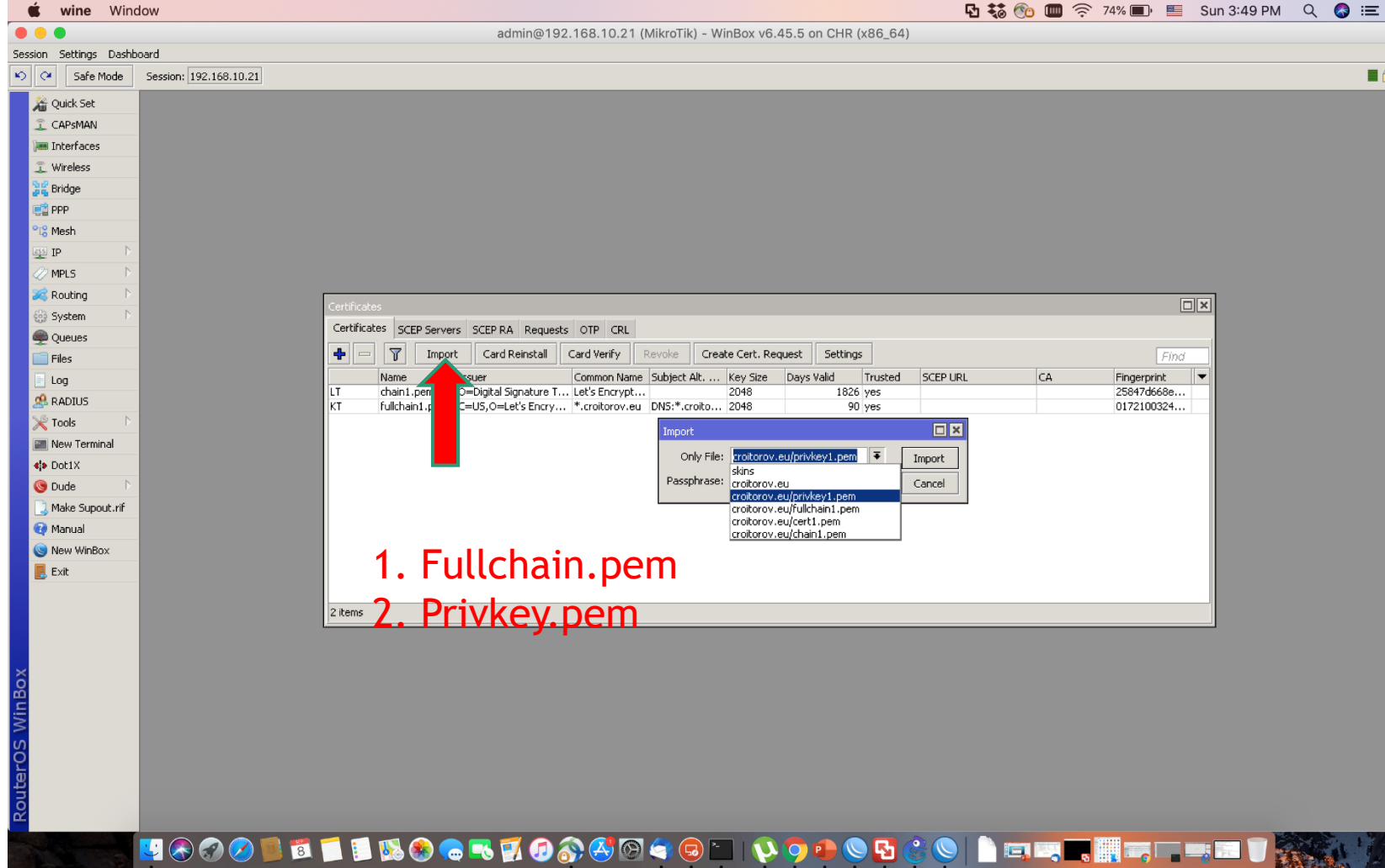
Clock & Time zone setting



IMPORT Certificates



IMPORT Certificates

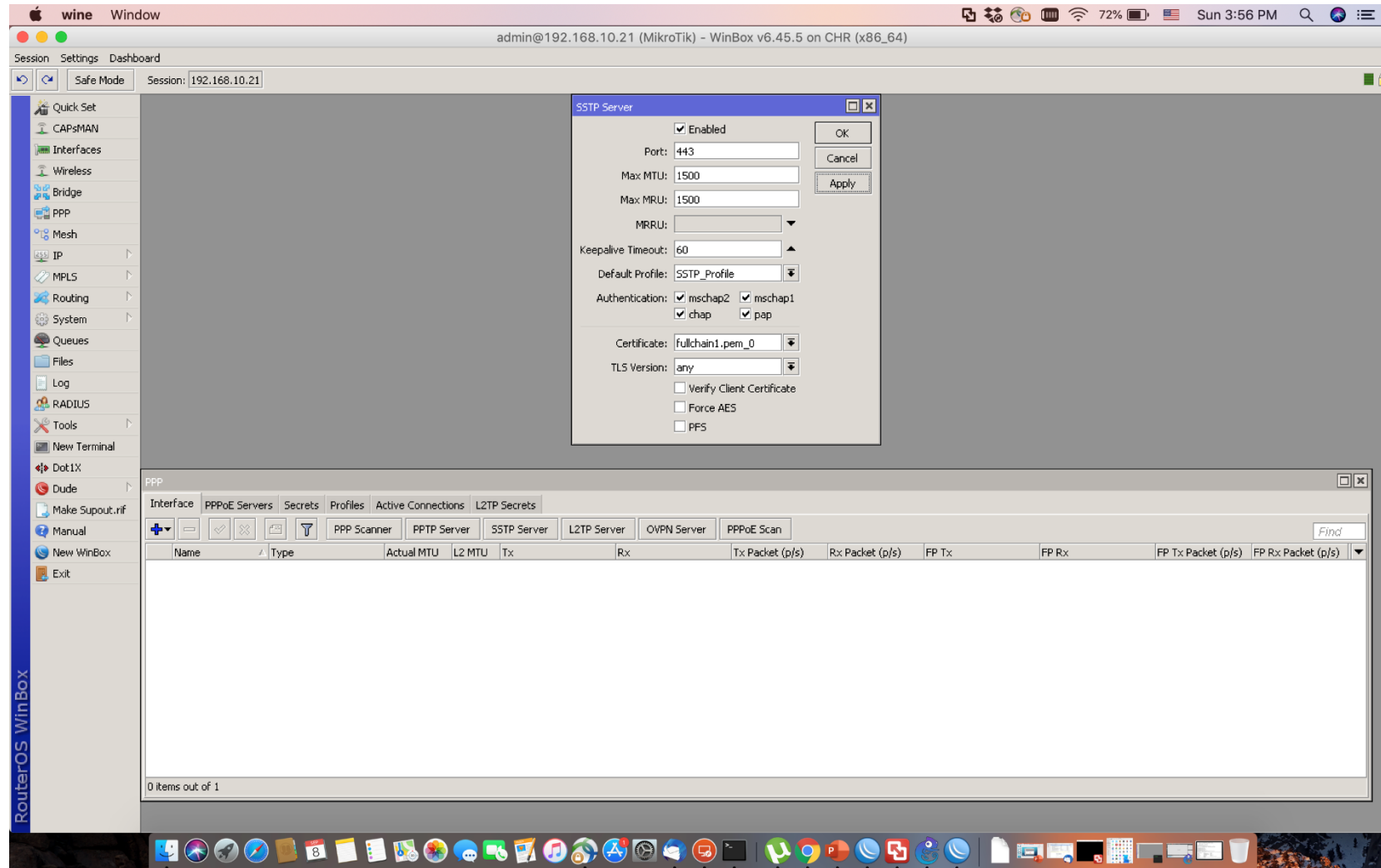


Create PPP Profile

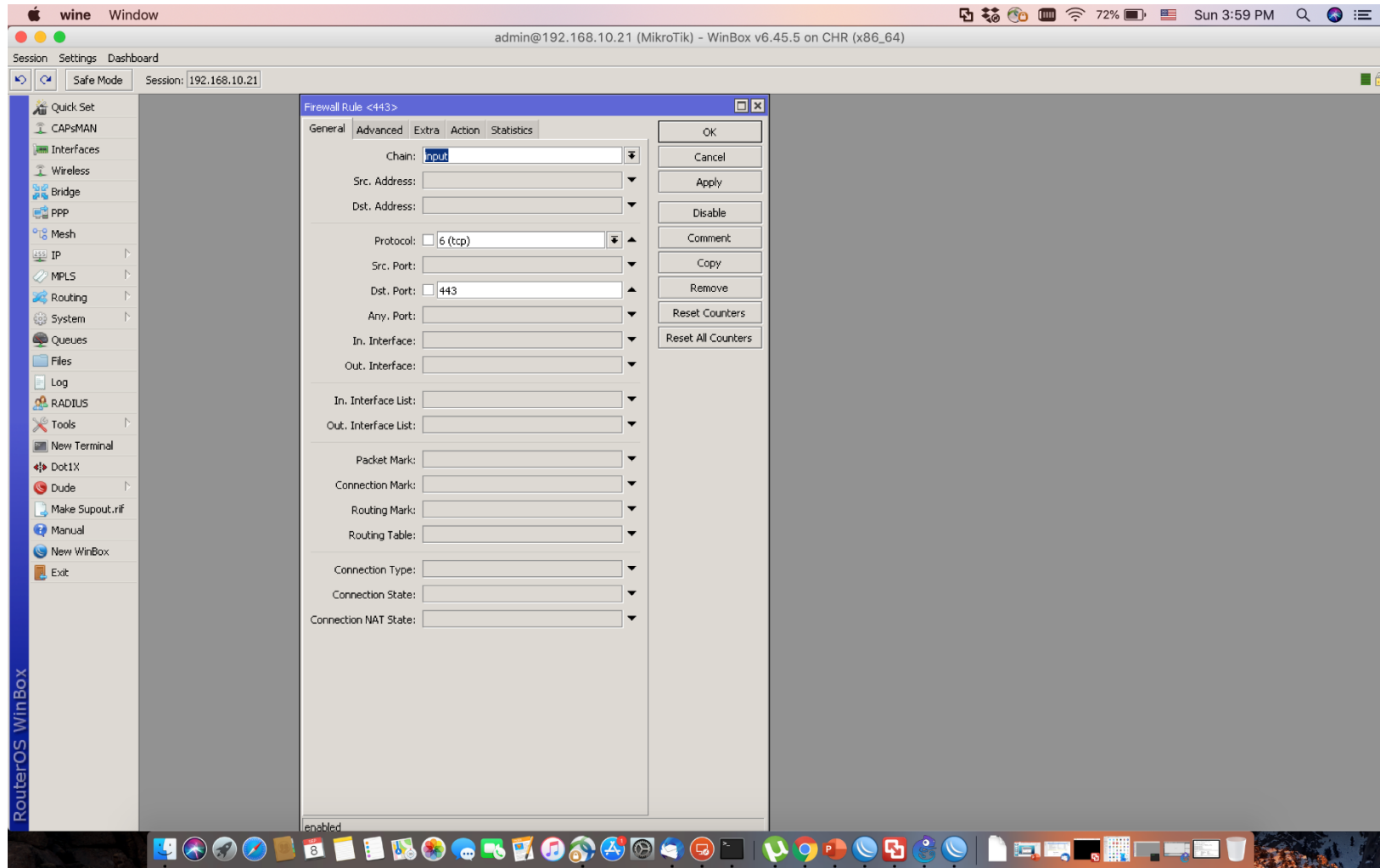
The screenshot displays the Mikrotik WinBox interface for configuring a PPP profile. The 'New PPP Profile' dialog box is open, showing the 'General' tab. The 'Name' field is set to 'SSTP_Profile', the 'Local Address' is '10.10.0.1', and the 'Remote Address' is 'pool1'. The 'IP Pool' window is also open, showing a list of pools with 'pool1' selected. The 'PPP' window is visible at the bottom, showing a table of PPP profiles.

Name	Local Address	Remote Address	Bridge	Rate Limi...	Only One
default					default
default-enc...					default

Enable SSTP Server



Create Firewall Rule



Create domain records

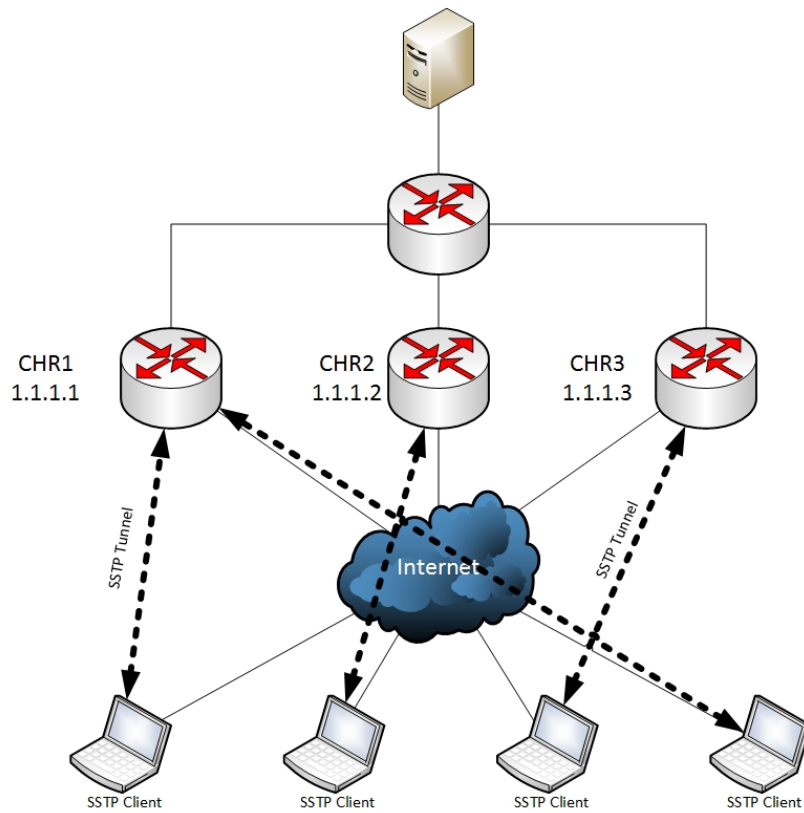
Type Name * IPv4 address * TTL Proxy status

A vpn 1.1.1.4 Auto DNS only

Cancel Save

Type	Name	Content	TTL	Proxy status
A	vpn	1.1.1.4	Auto	DNS only - reserved IP
A	vpn	1.1.1.3	Auto	DNS only - reserved IP
A	vpn	1.1.1.2	Auto	DNS only - reserved IP
A	vpn	1.1.1.1	Auto	DNS only - reserved IP

The topology



DEMO



Thank you!

