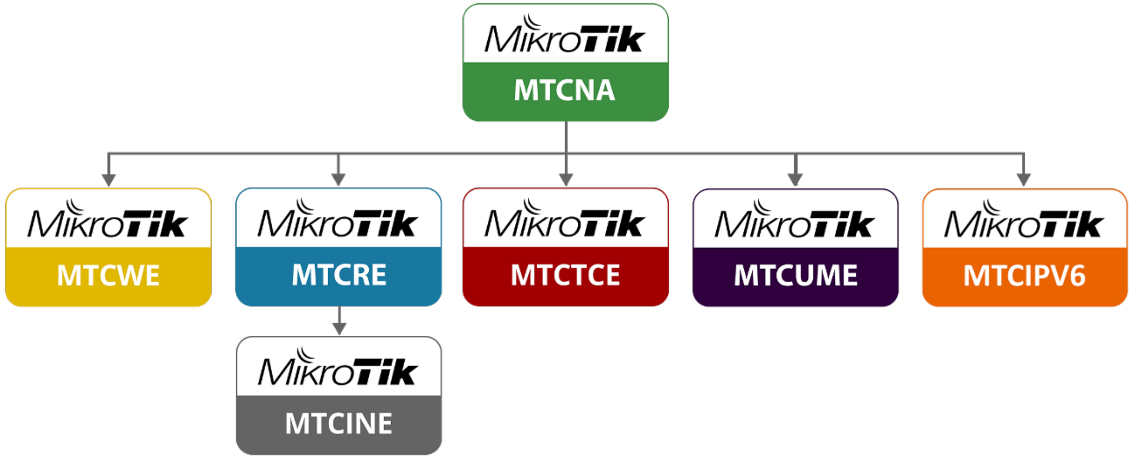
Highly loaded certificate-based VPN solution

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:



MikroTik MTCNA

MikroTik MTCWE

MikroTik MTCRE

MikroTik MTCTCE

MikroTik MTCUME

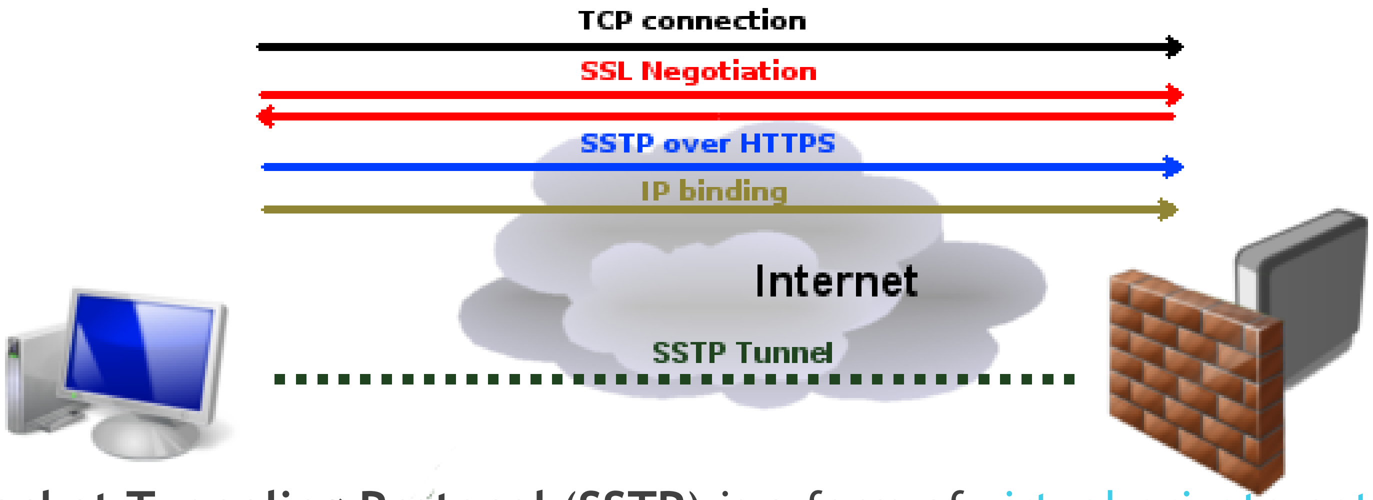
MikroTik MTCIPV6

MikroTik MTCINE

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

ADNAVTAGES

- 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.

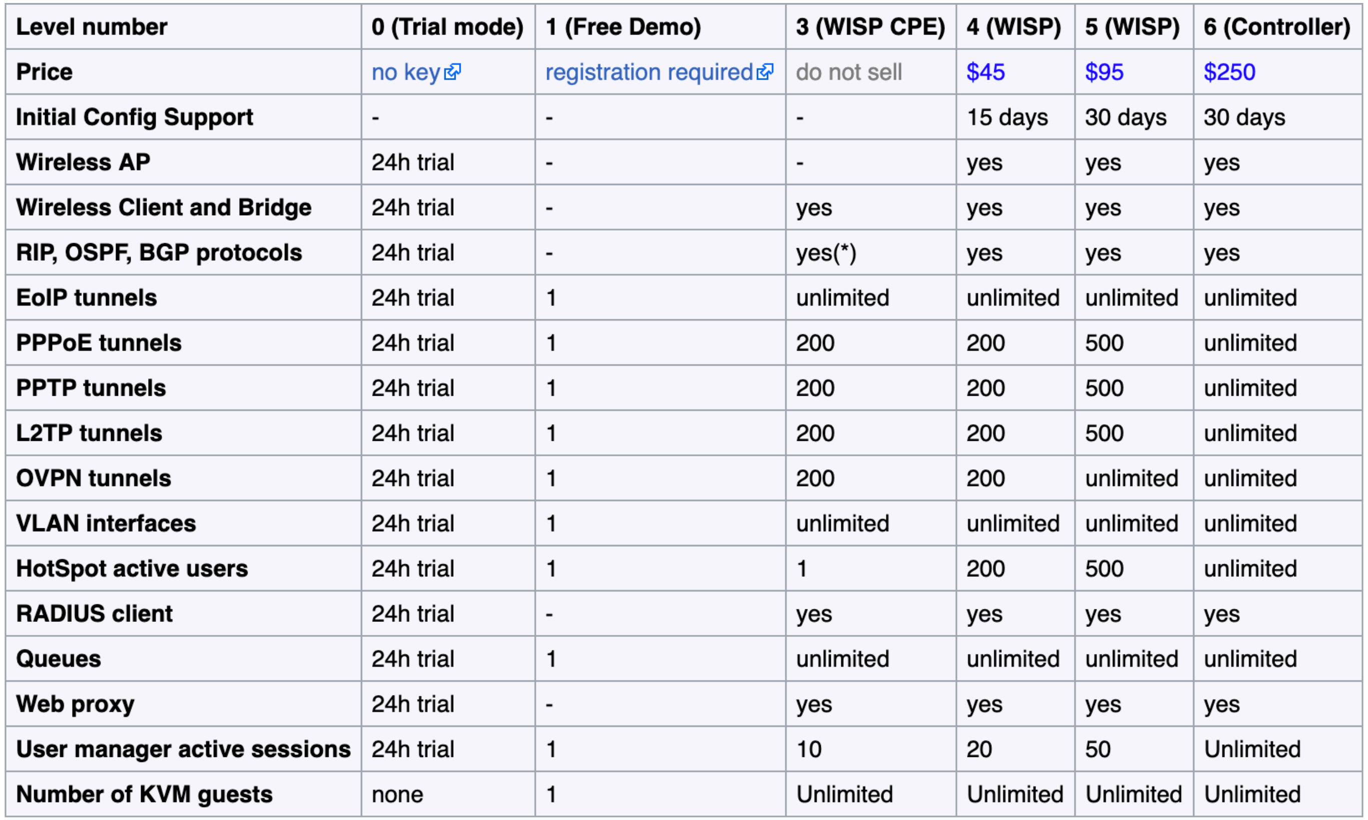
DISADNAVTAGES

- 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

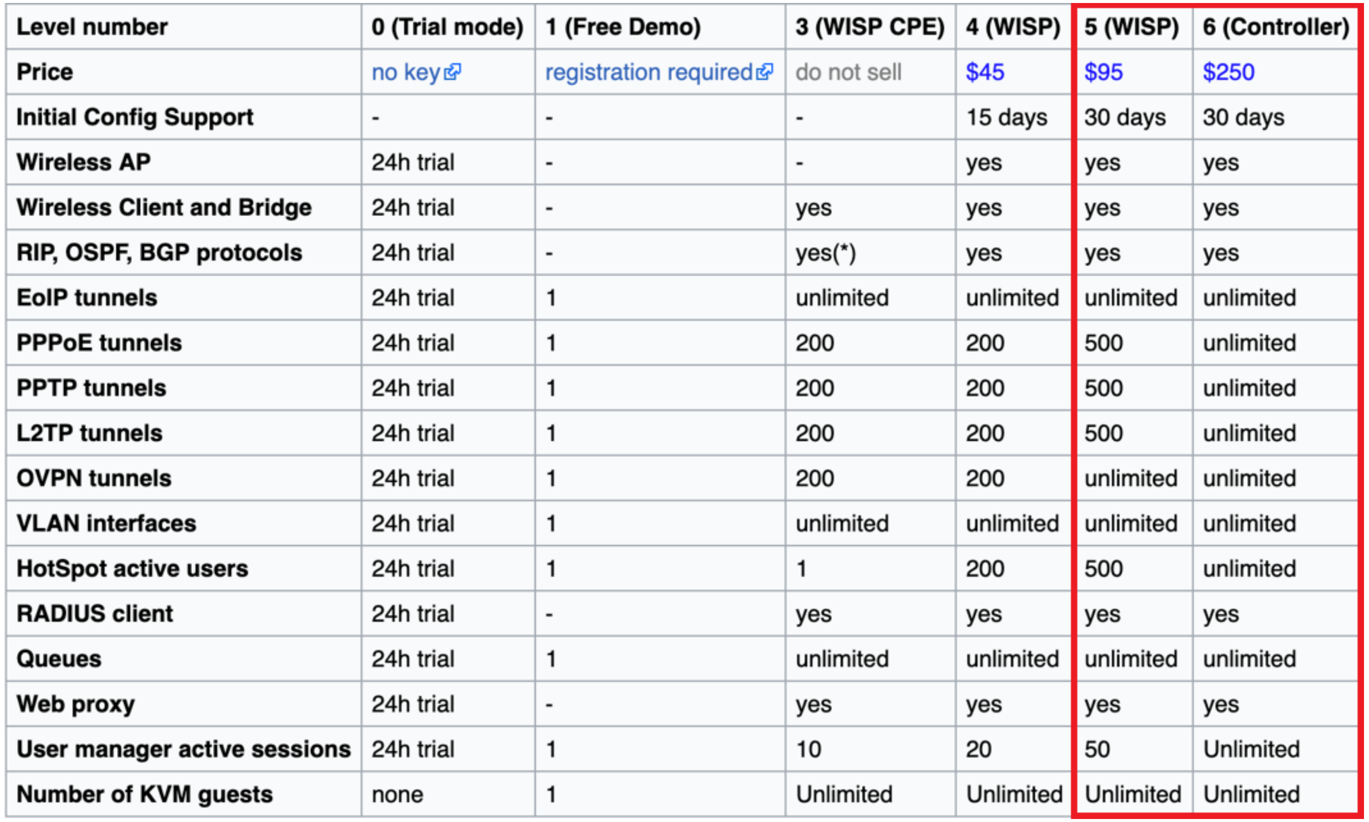
- 4000+ VPN clients
- Data encryption and integrity
- High availability
- Scalability

Routeros License level



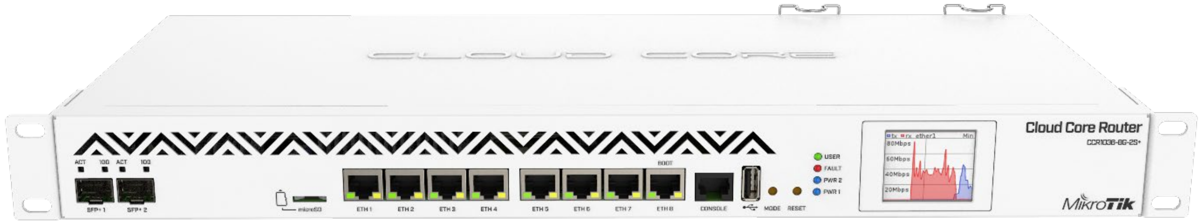
Level number	0 (Trial mode)	1 (Free Demo)	3 (WISP CPE)	4 (WISP)	5 (WISP)	6 (Controller)
Price	no key	registration required	do not sell	$45	$95	$250
Initial Config Support	-	-	-	15 days	30 days	30 days
Wireless AP	24h trial	-	-	yes	yes	yes
Wireless Client and Bridge	24h trial	-	yes	yes	yes	yes
RIP, OSPF, 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

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

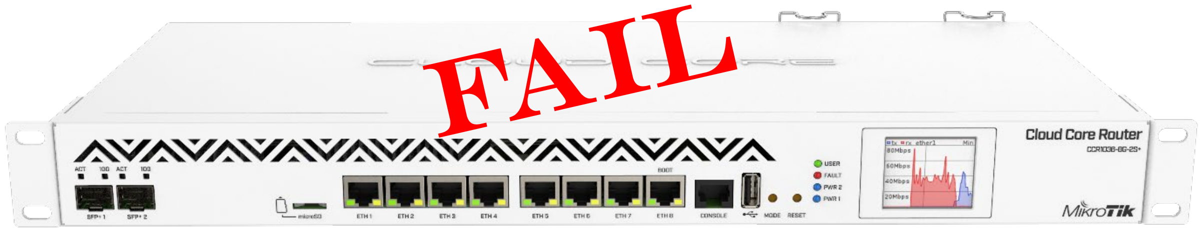
Which platform to choose?



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?



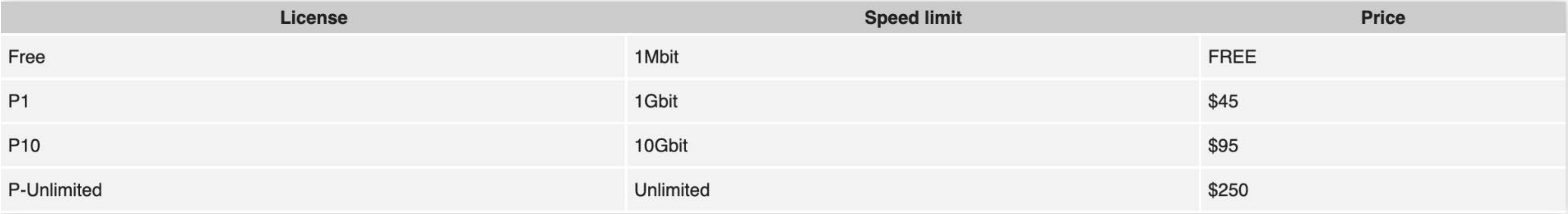
36 core 1.4Ghz CPU
4GB RAM
IPsec hardware acceleration
License Level6

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

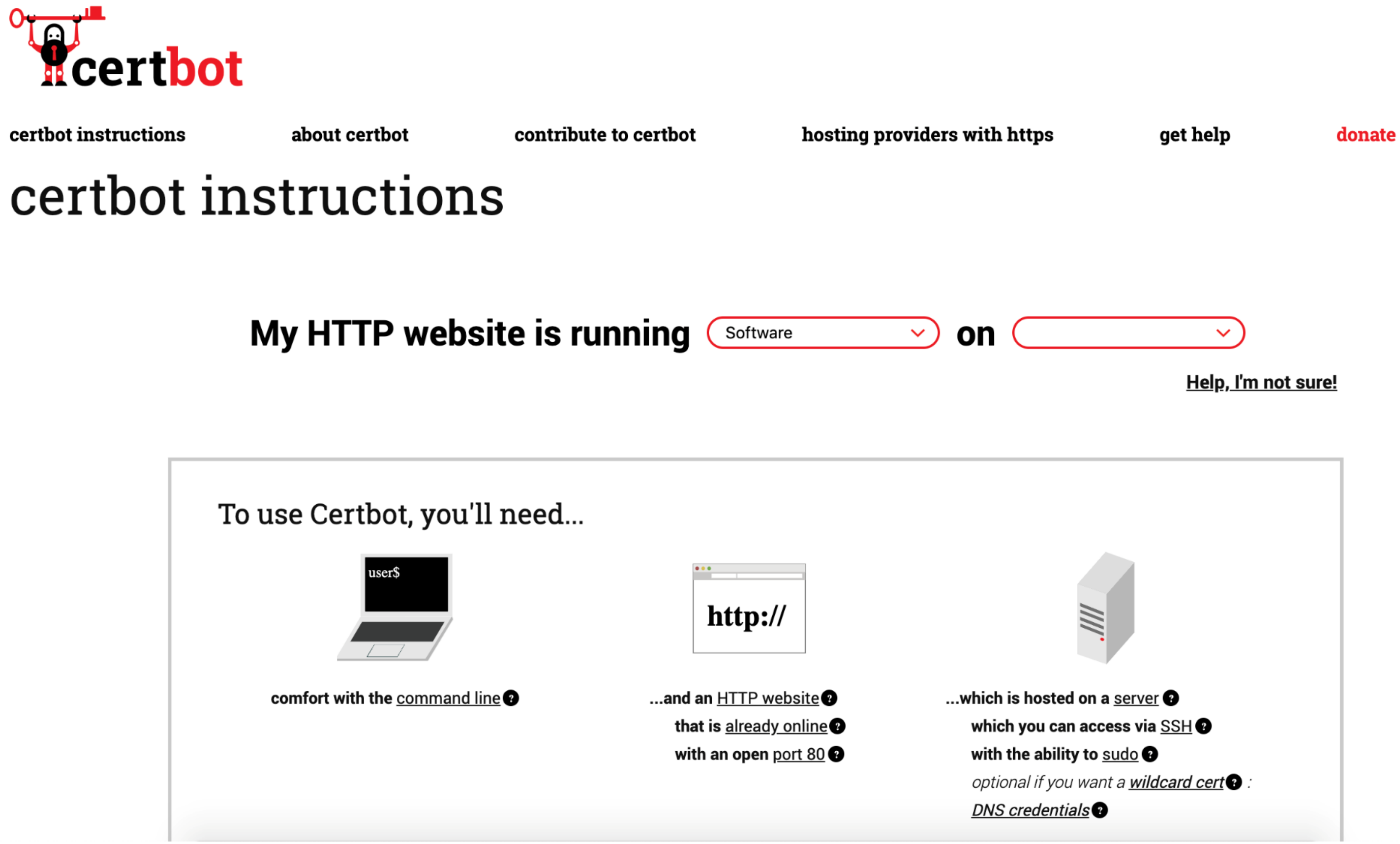


License	Speed limit	Price
Free	1Mbit	FREE
P1	1Gbit	$45
P10	10Gbit	$95
P-Unlimited	Unlimited	$250

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

My HTTP website is running Software **on**

Help, I'm not sure!

To use Certbot, you'll need...

comfort with the command line

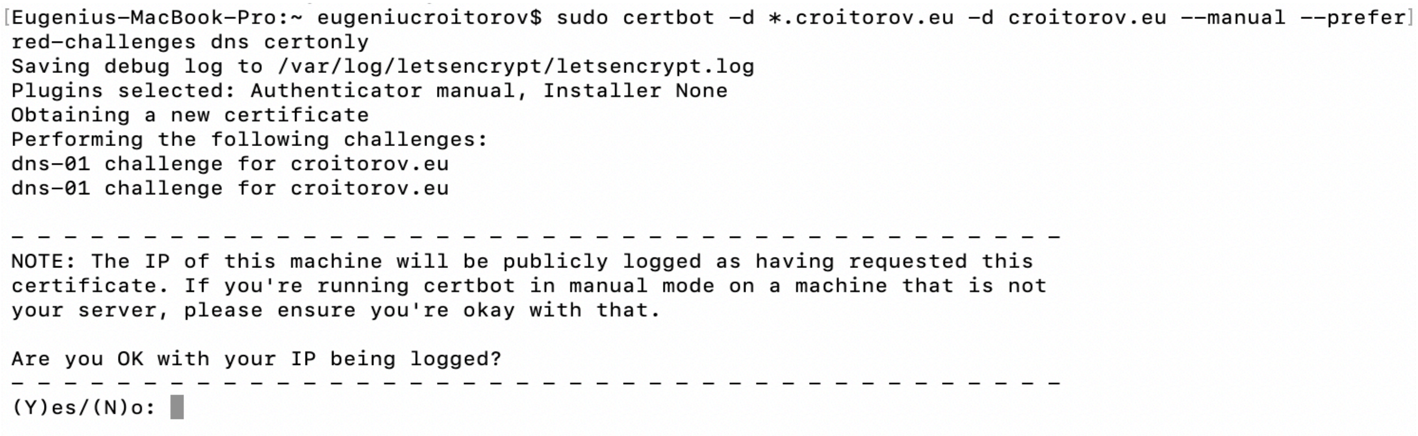
...and an HTTP website
that is already online
with an open port 80

...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

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

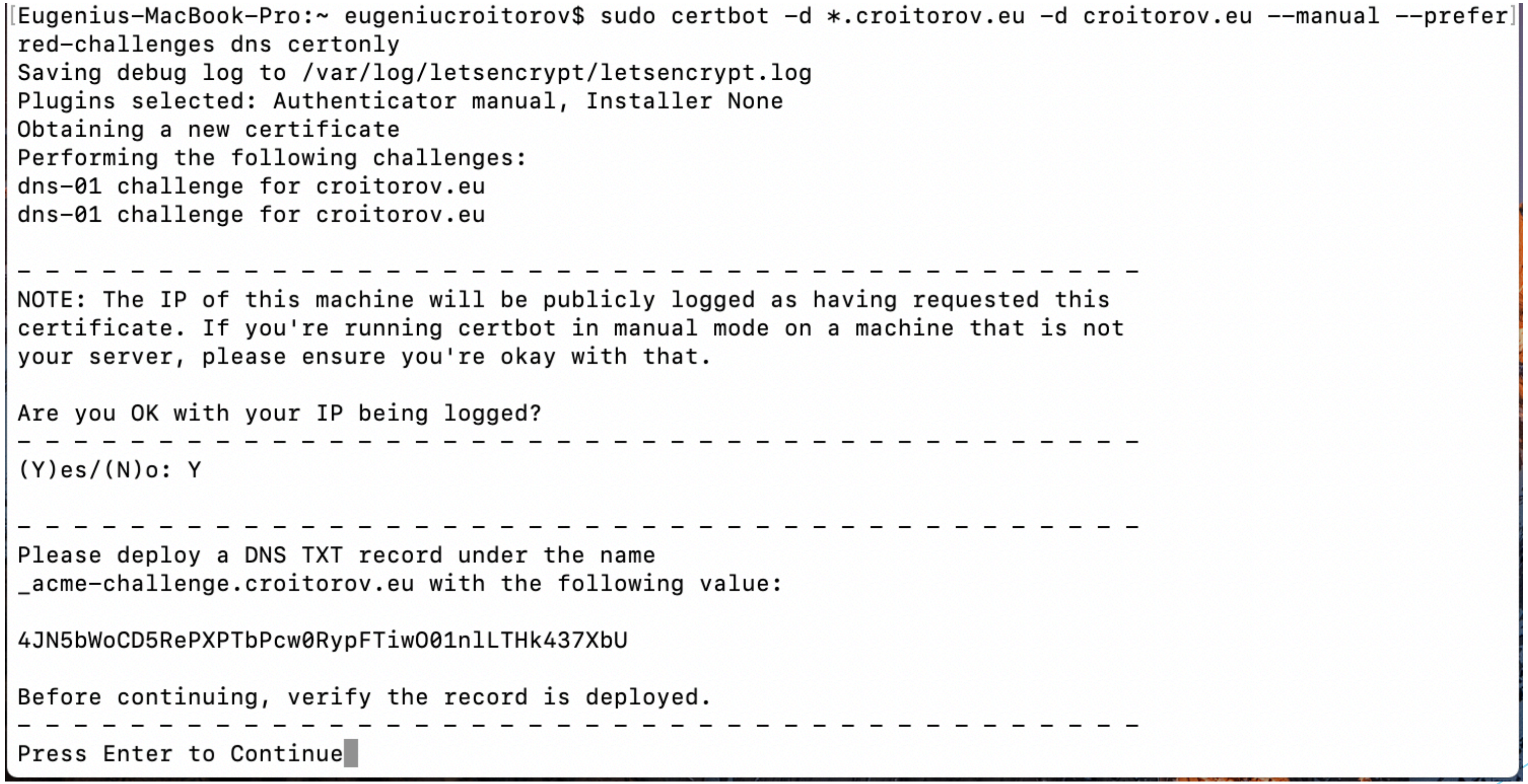
#certbot certonly --preferred-challenges=dns --manual -d *.$DOMAIN



```
[Eugenius-MacBook-Pro:~ eugeniucroitorov$ sudo certbot -d *.croitorov.eu -d croitorov.eu --manual --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:
```

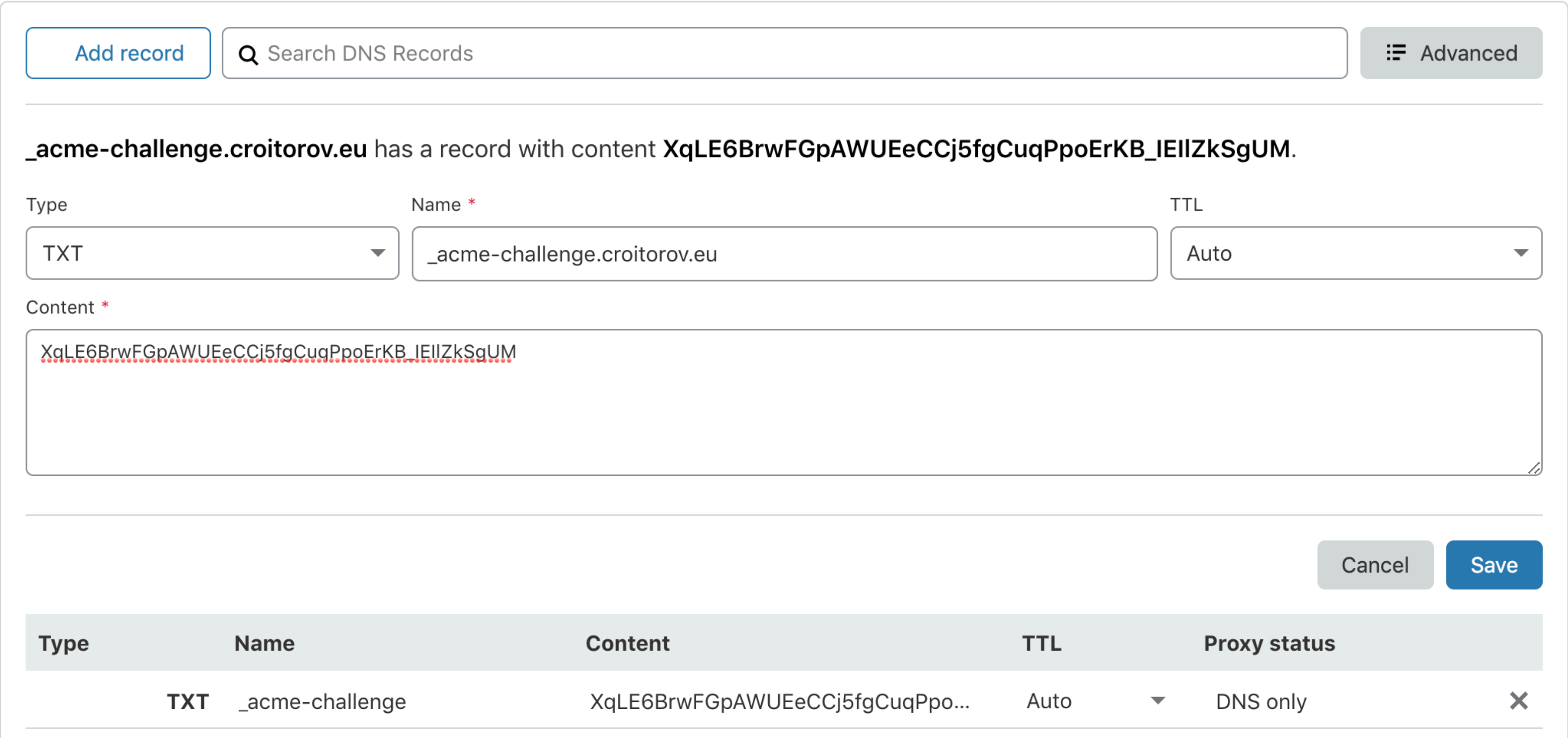
HOW TO GET SSL CERTIFICATE?

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:

4JN5bWoCD5RePXPTbPcw0RypFTiwO01nlLTHk437XbU

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

HOW TO GET SSL CERTIFICATE?



_acme-challenge.croitorov.eu has a record with content **XqLE6BrwFGpAWUEeCCj5fgCuqPpoErKB_IEIlZkSgUM**.

Type: TXT

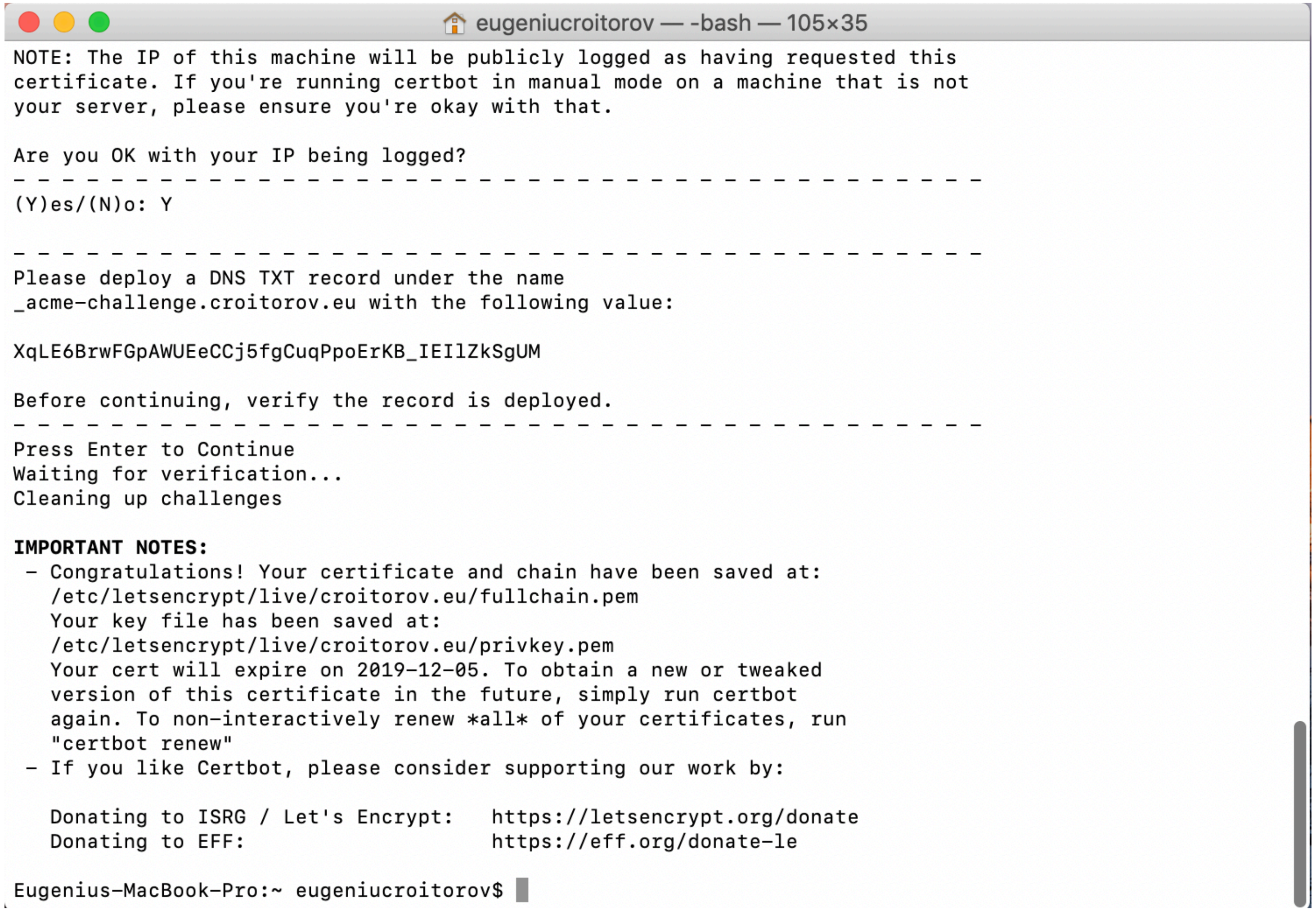
Name *: _acme-challenge.croitorov.eu

TTL: Auto

Content *: XqLE6BrwFGpAWUEeCCj5fgCuqPpoErKB_IEIlZkSgUM

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

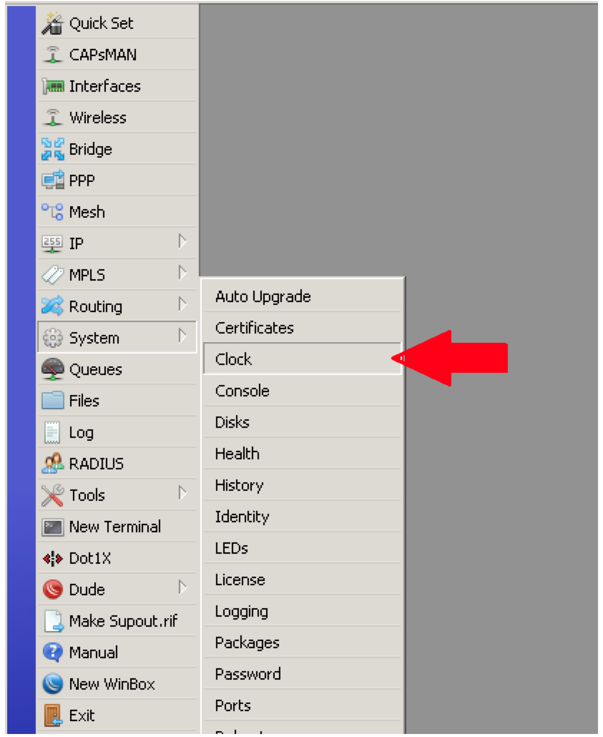
HOW TO GET SSL CERTIFICATE?

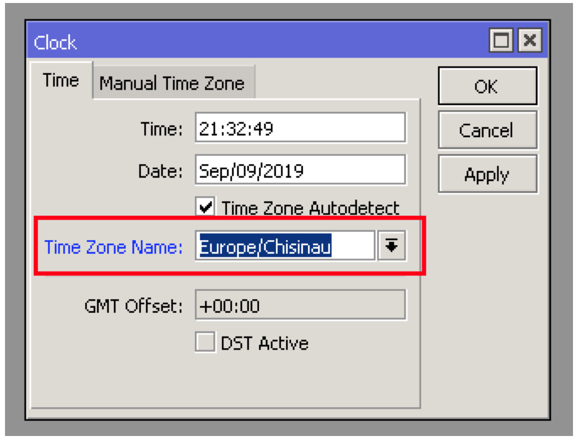


```
NOTE: The IP of this machine will be publicly logged as having requested this
certificate. If you're running certbot in manual mode on a machine that is not
your server, please ensure you're okay with that.

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_IEIlZkSgUM

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

Clock & Time zone setting





Time: 21:32:49

Date: Sep/09/2019

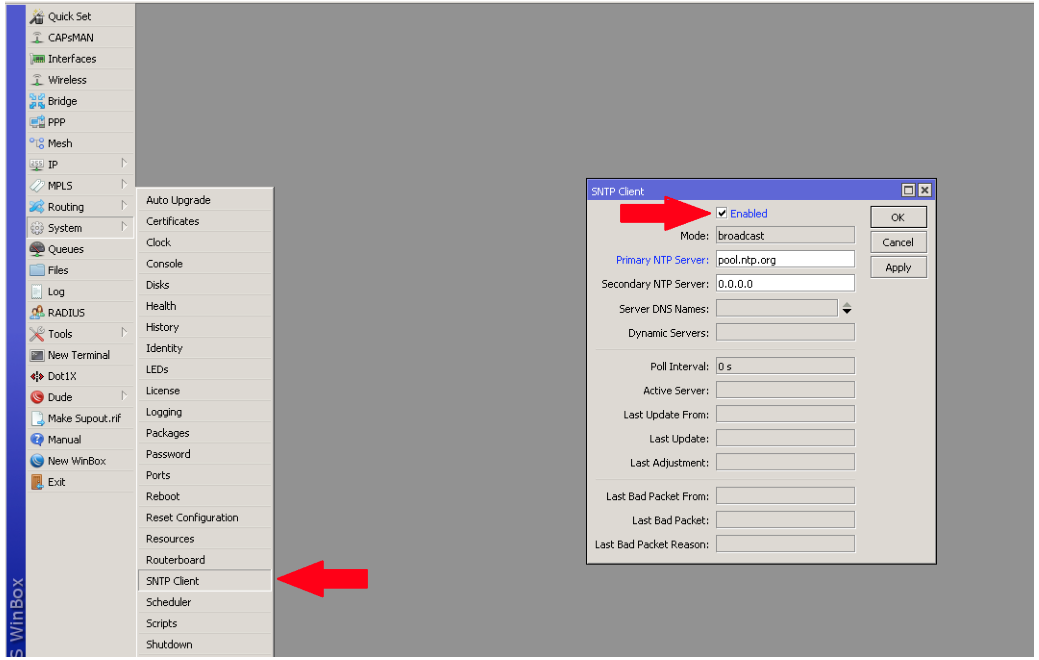
☑ Time Zone Autodetect

Time Zone Name: Europe/Chisinau

GMT Offset: +00:00

□ DST Active

Clock & Time zone setting



SNTP Client

☑ Enabled

Mode: broadcast

Primary NTP Server: pool.ntp.org

Secondary NTP Server: 0.0.0.0

Server DNS Names:

Dynamic Servers:

Poll Interval: 0 s

Active Server:

Last Update From:

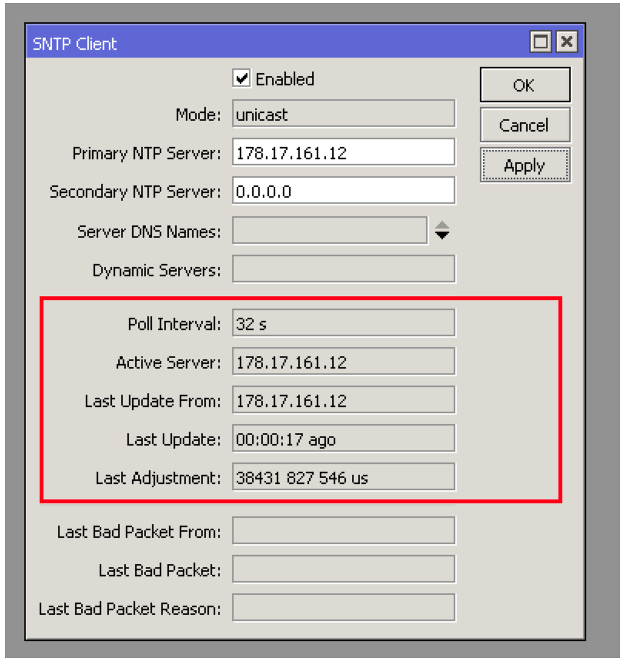
Last Update:

Last Adjustment:

Last Bad Packet From:

Last Bad Packet:

Last Bad Packet Reason:



SNTP Client

☑ Enabled

Mode: unicast

Primary NTP Server: 178.17.161.12

Secondary NTP Server: 0.0.0.0

Server DNS Names:

Dynamic Servers:

Poll Interval: 32 s

Active Server: 178.17.161.12

Last Update From: 178.17.161.12

Last Update: 00:00:17 ago

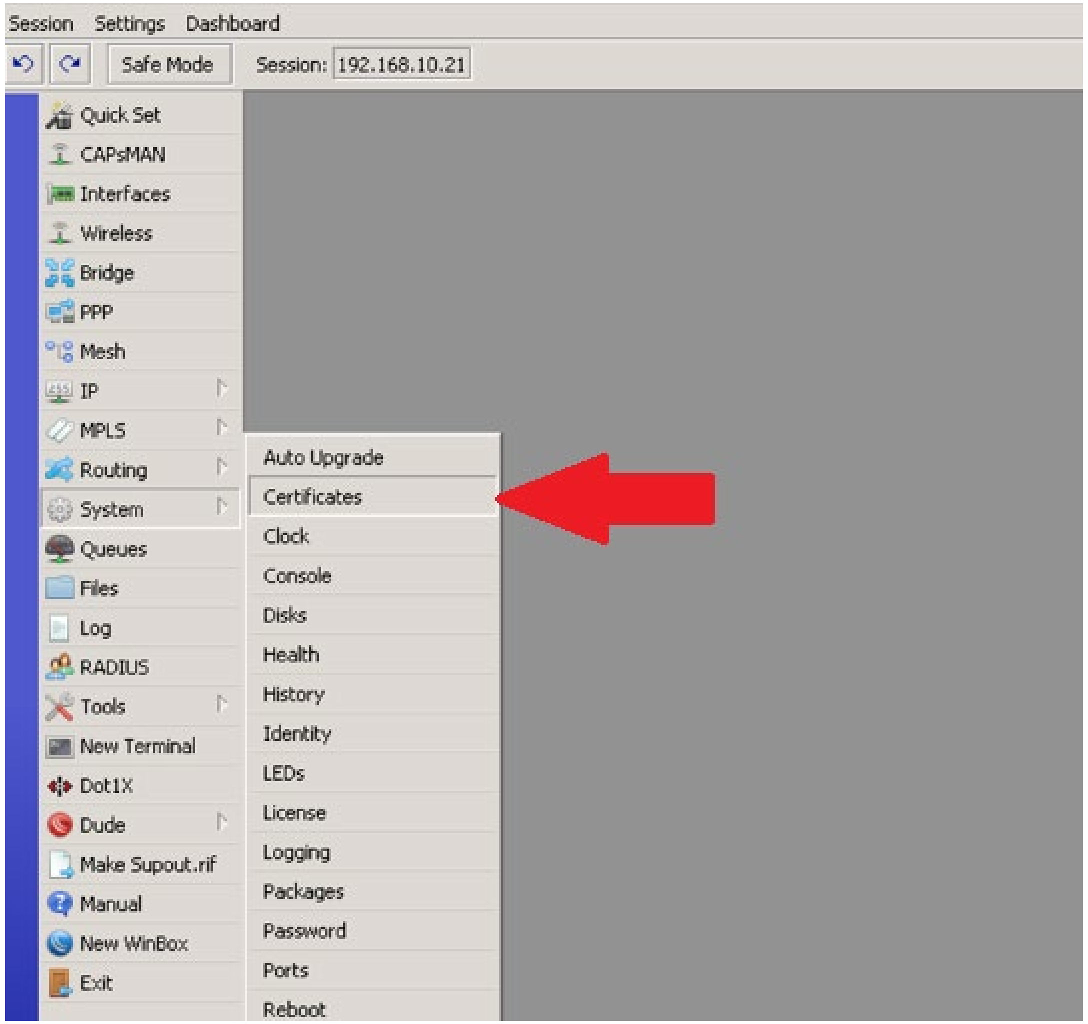
Last Adjustment: 38431 827 546 us

Last Bad Packet From:

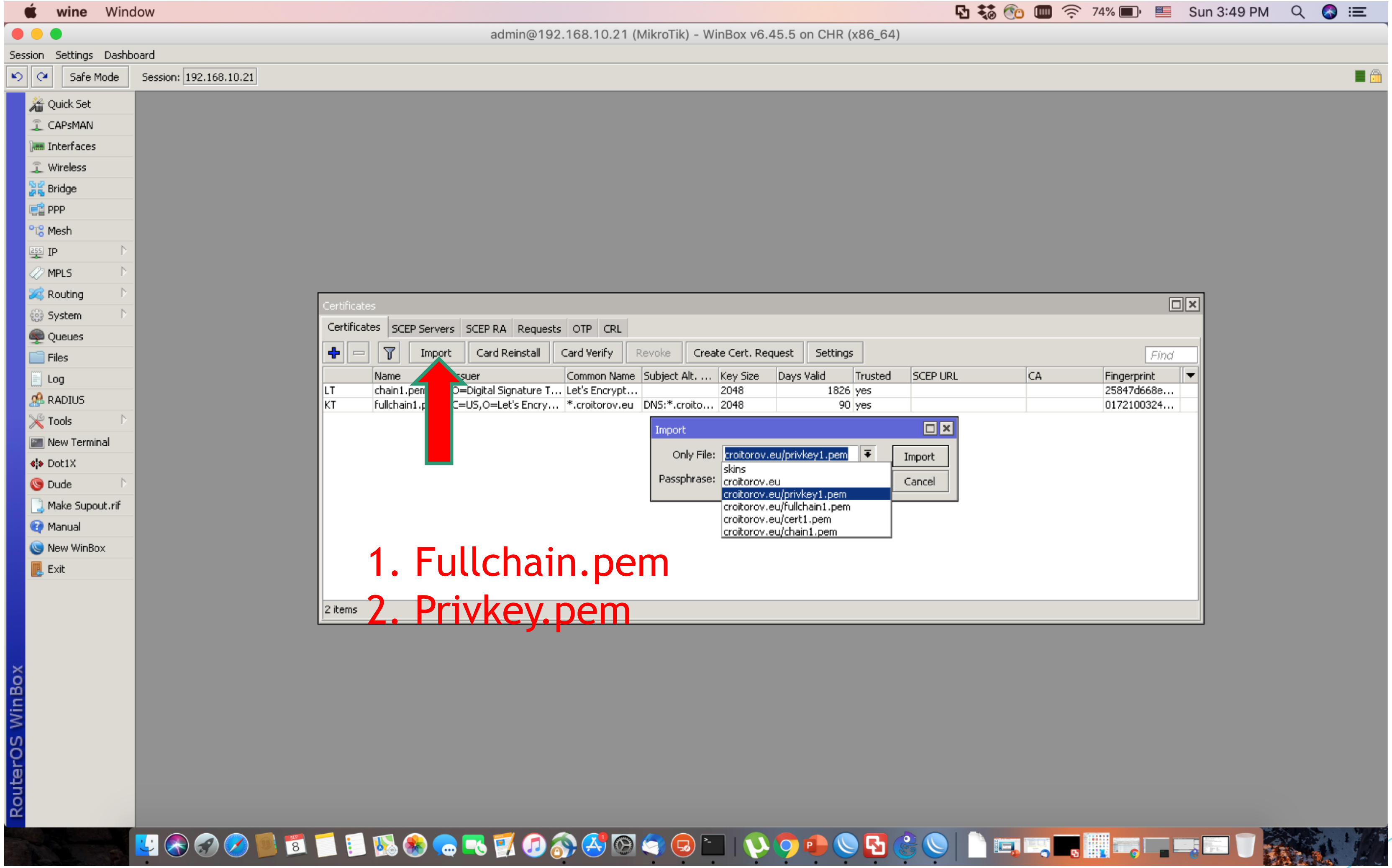
Last Bad Packet:

Last Bad Packet Reason:

IMPORT Certificates



IMPORT Certificates



Session: 192.168.10.21

	Name	ssuer	Common Name	Subject Alt. …	Key Size	Days Valid	Trusted	SCEP URL	CA	Fingerprint
LT	chain1.pem	O=Digital Signature T…	Let's Encrypt…		2048	1826	yes			25847d668e…
KT	fullchain1.p	C=US,O=Let's Encry…	*.croitorov.eu	DNS:*.croito…	2048	90	yes			0172100324…

2 items

Import

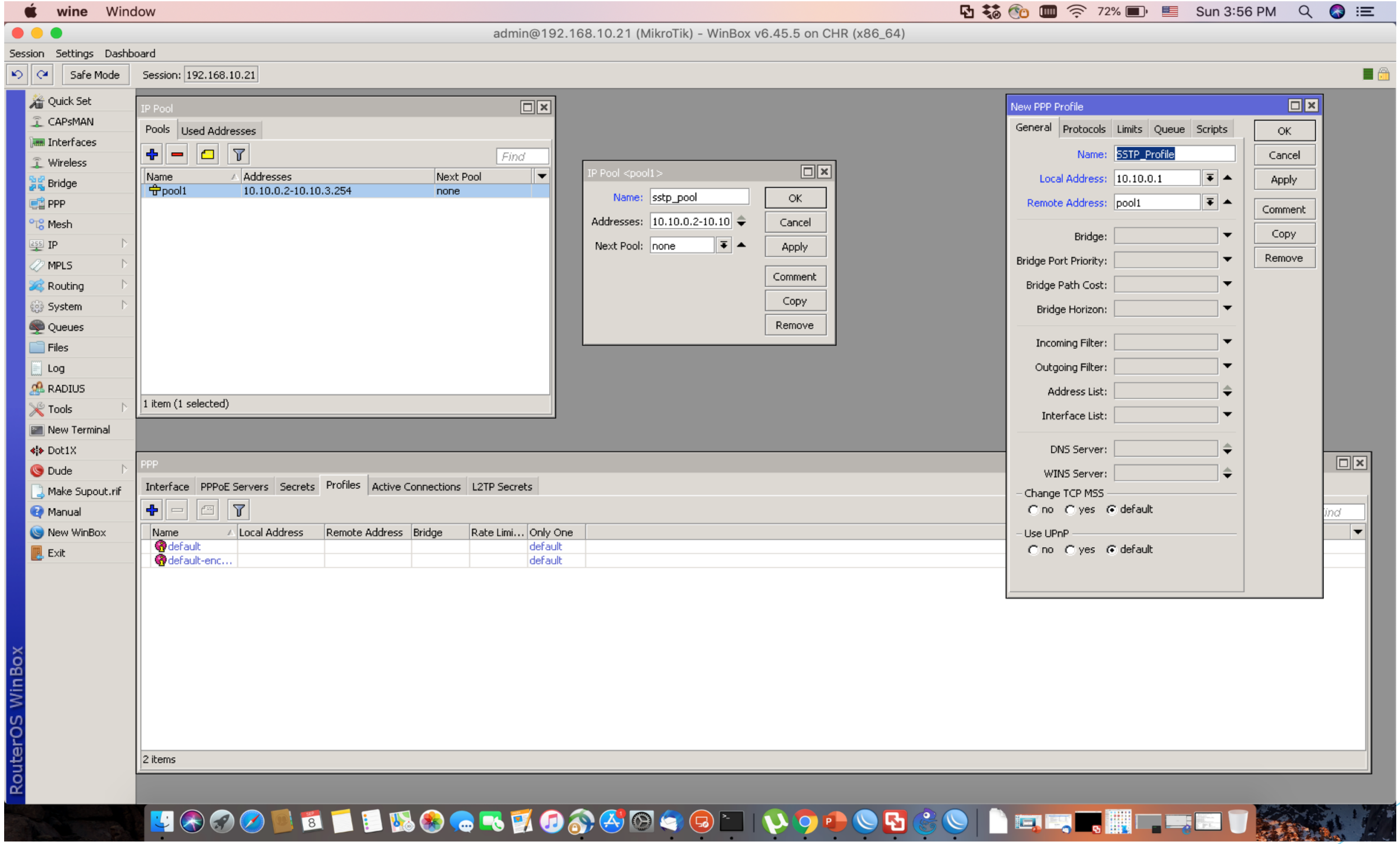
Only File: croitorov.eu/privkey1.pem

Passphrase:

```
skins
croitorov.eu
croitorov.eu/privkey1.pem
croitorov.eu/fullchain1.pem
croitorov.eu/cert1.pem
croitorov.eu/chain1.pem
```

1. Fullchain.pem
2. Privkey.pem

Create PPP Profile



admin@192.168.10.21 (MikroTik) - WinBox v6.45.5 on CHR (x86_64)

Session: 192.168.10.21

IP Pool

Name	Addresses	Next Pool
pool1	10.10.0.2-10.10.3.254	none

1 item (1 selected)

IP Pool <pool1>

Name: sstp_pool
Addresses: 10.10.0.2-10.10
Next Pool: none

New PPP Profile

Name: SSTP_Profile
Local Address: 10.10.0.1
Remote Address: pool1
Bridge:
Bridge Port Priority:
Bridge Path Cost:
Bridge Horizon:
Incoming Filter:
Outgoing Filter:
Address List:
Interface List:
DNS Server:
WINS Server:

Change TCP MSS
○ no ○ yes ● default

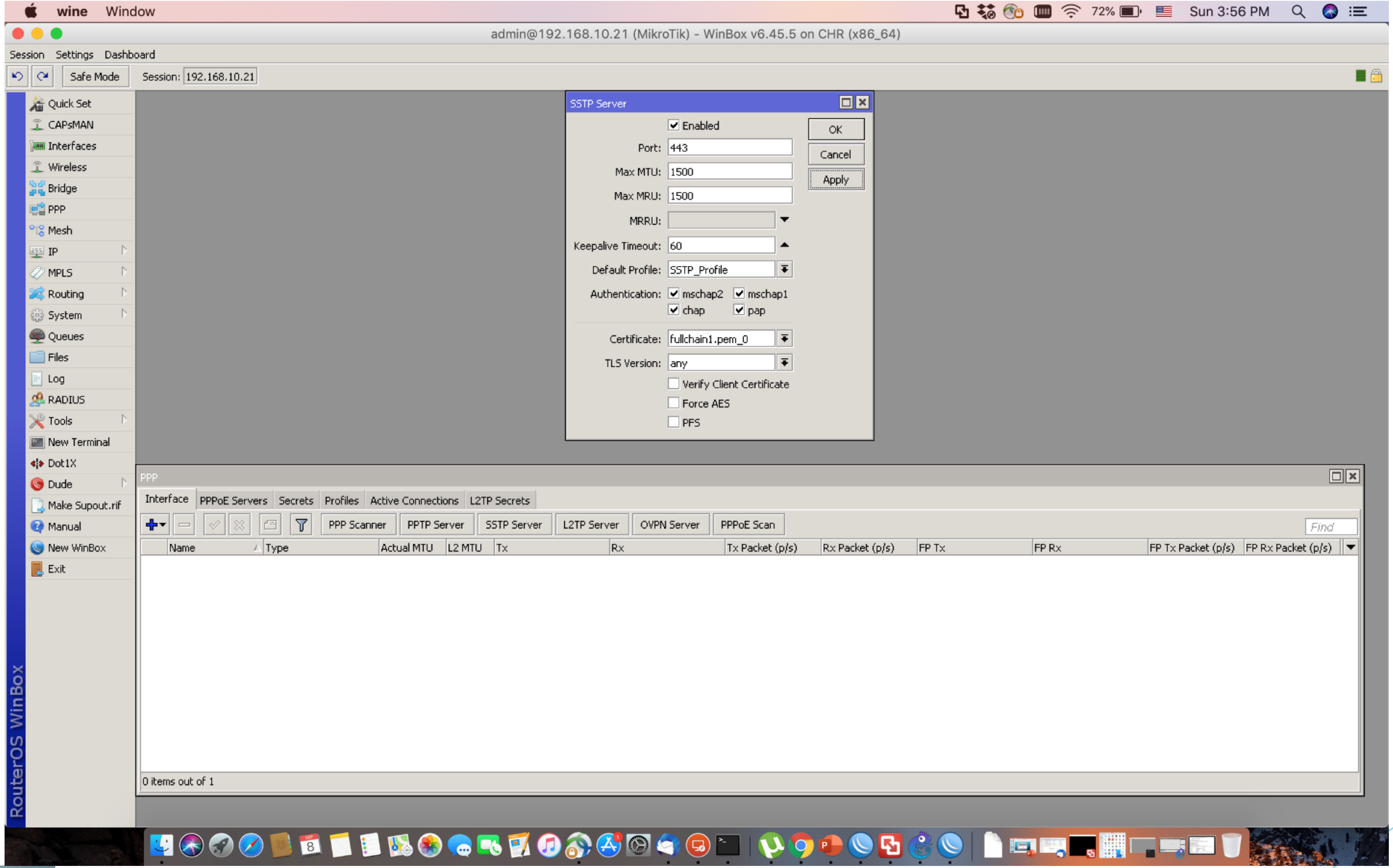
Use UPnP
○ no ○ yes ● default

PPP

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

2 items

Enable SSTP Server



admin@192.168.10.21 (MikroTik) - WinBox v6.45.5 on CHR (x86_64)

Session: 192.168.10.21

SSTP Server

☑ Enabled

Port: 443

Max MTU: 1500

Max MRU: 1500

MRRU:

Keepalive Timeout: 60

Default Profile: SSTP_Profile

Authentication: ☑ mschap2 ☑ mschap1 ☑ chap ☑ pap

Certificate: fullchain1.pem_0

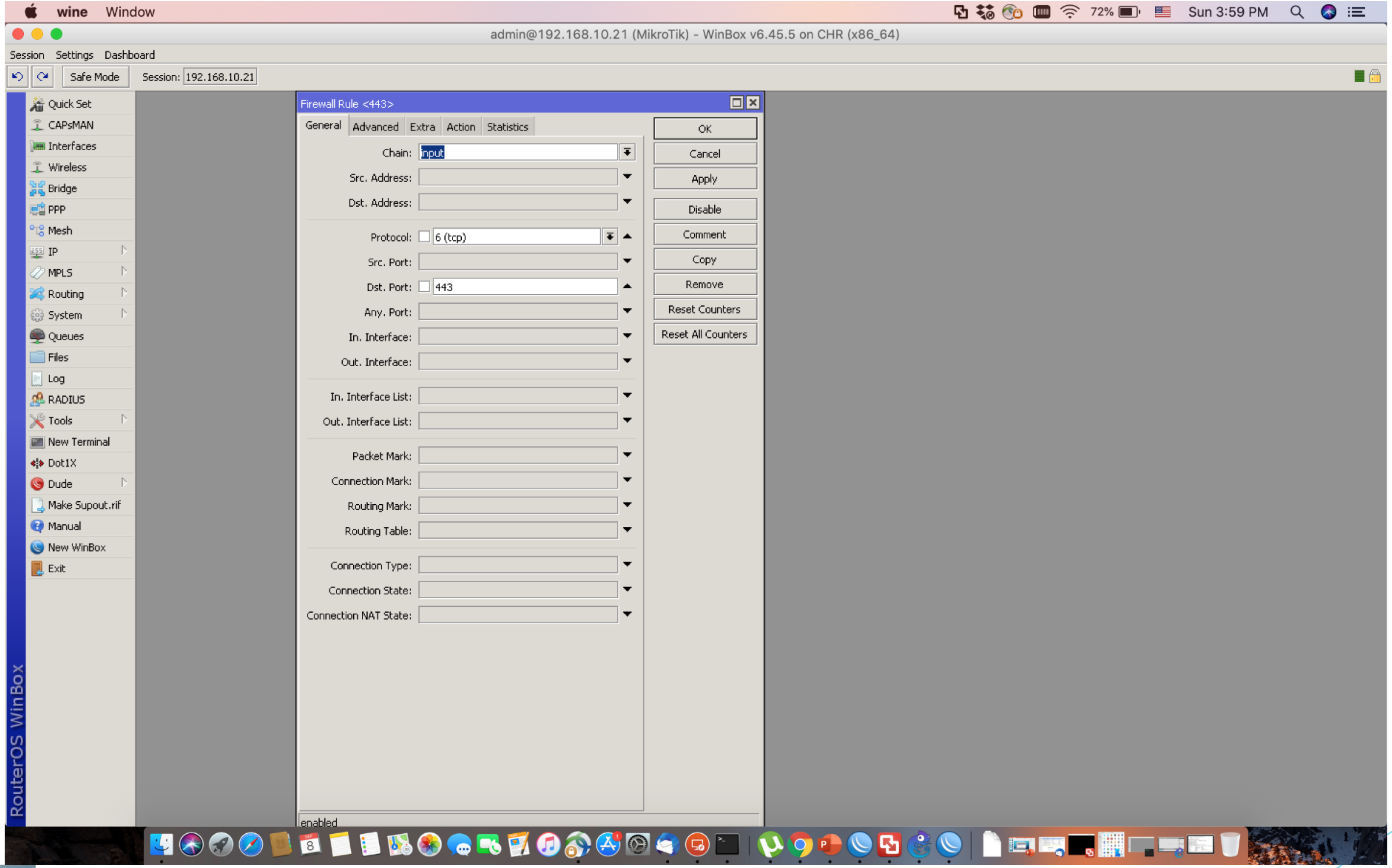
TLS Version: any

□ Verify Client Certificate

□ Force AES

□ PFS

Create Firewall Rule



admin@192.168.10.21 (MikroTik) - WinBox v6.45.5 on CHR (x86_64)

Session: 192.168.10.21

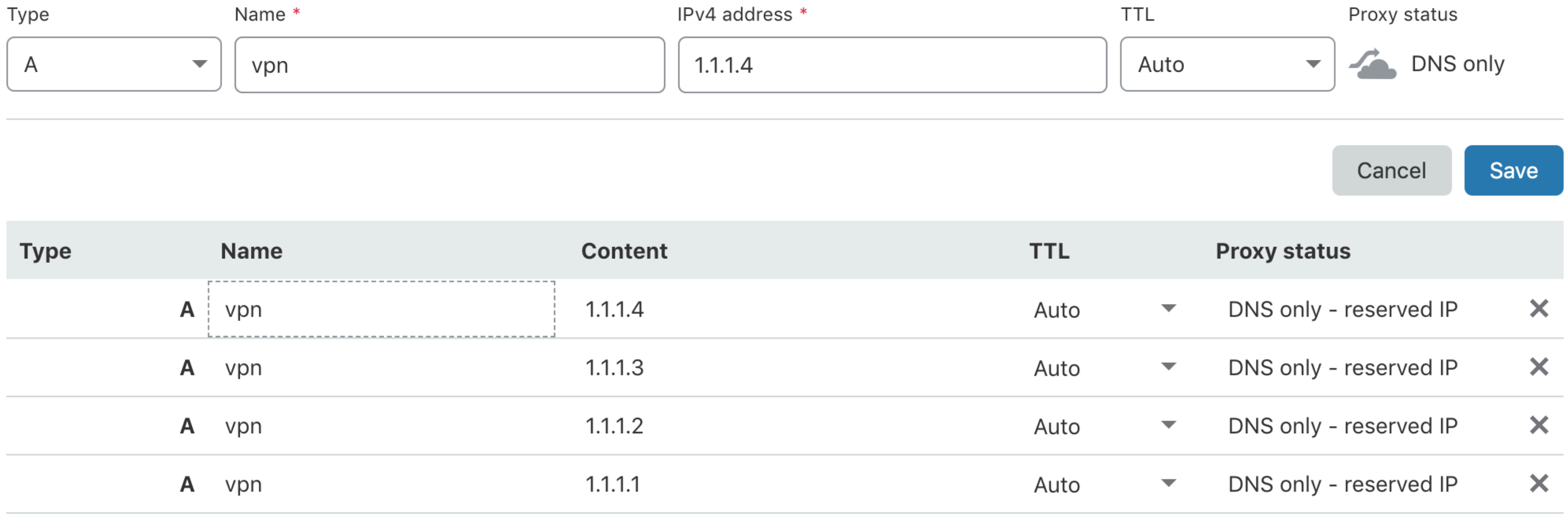
Firewall Rule <443>

General

Chain:	input
Src. Address:	
Dst. Address:	
Protocol:	□ 6 (tcp)
Src. Port:	
Dst. Port:	□ 443
Any. Port:	
In. Interface:	
Out. Interface:	
In. Interface List:	
Out. Interface List:	
Packet Mark:	
Connection Mark:	
Routing Mark:	
Routing Table:	
Connection Type:	
Connection State:	
Connection NAT State:	

enabled

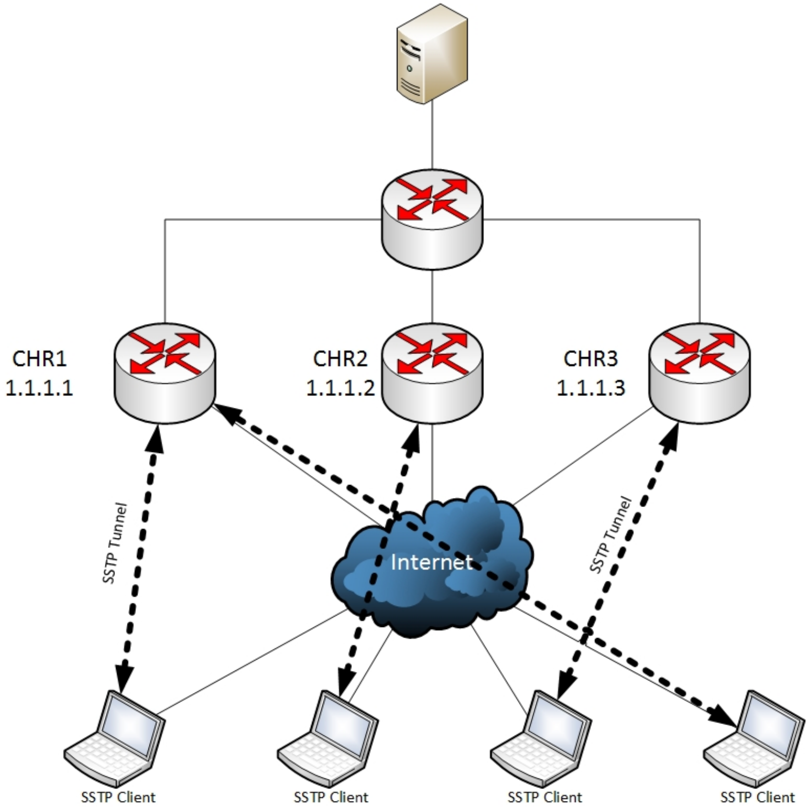
Create domain records



Type	Name *	IPv4 address *	TTL	Proxy status
A	vpn	1.1.1.4	Auto	DNS only

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!