

# **IKEv2 Remote Access VPN**

**MUM China - October 19, 2019**

**Jesse Liu, Lethbridge**

# About Me

- **Jesse Liu, Lethbridge**
  - Over 13 years experience using RouterOS
  - Specialization in Wireless, Tunnel and Routing
  - MikroTik MTCNA, MTCWE, MTCTCE
  - Cisco CCNP, CCDP (R&S)

# Summary

- IKEv2 is supported in current RouterOS versions, and one way to make it work is by using EAP-MSCHAPv2, which is covered in this presentation.
- How to implement IKEv2 remote access VPN using RouterOS for Windows, macOS, Linux, iOS/iPadOS, Android/ChromeOS and BlackBerry clients.
- Clients do not need to import certificates and special settings just need to create a connection.

# IPsec vs. PPP

## IKEv2



## Other VPN

PPTP

SSTP

L2TP

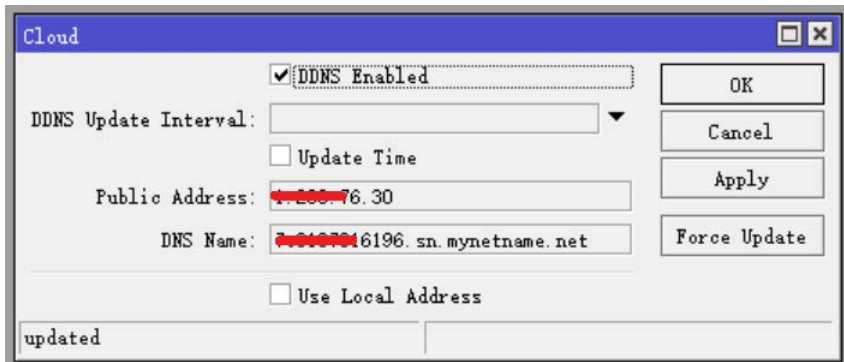


# Public IP

- Static or dynamic public IP.
- This can also be the public IP of a gateway in front of a downstream router if the upstream gateway is port forwarding UDP ports 500 and 4500.

# DNS

- Static public IP only needs to create a DNS A record.
- Dynamically tracks IP changes via IP Cloud DDNS and a DNS CNAME record.



## ← DNS Settings leth.top

✓ DNS Server:dns25.hichina.com, dns26.hichina.com

Add Record

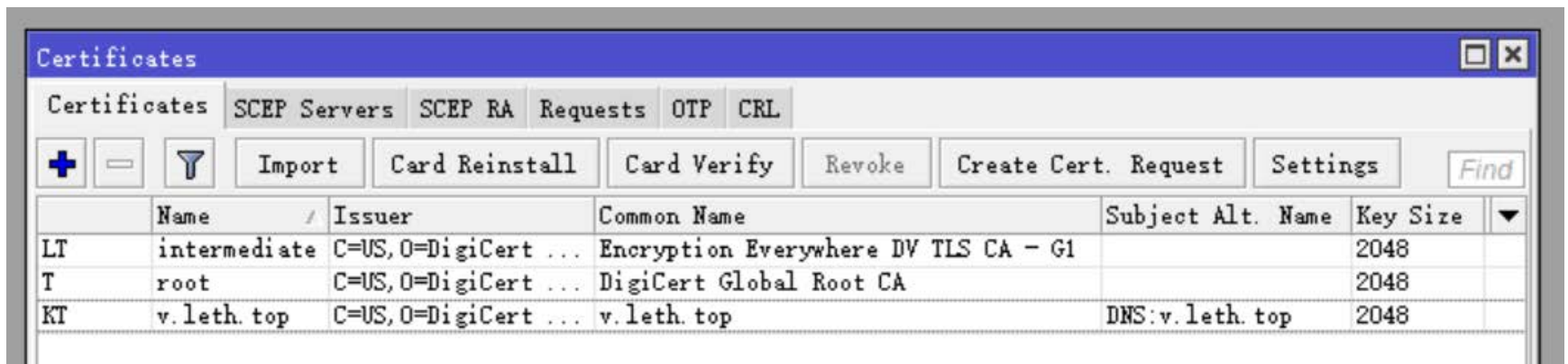
Import & Export

Query Volume

<input type="checkbox"/>	Type ▾	Host ▾	Line(ISP) ▾	Value
<input type="checkbox"/>	<u>CNAME</u>	v	Default	<del>7.200.76.16196</del> .sn.mynetname.net

# Certificates

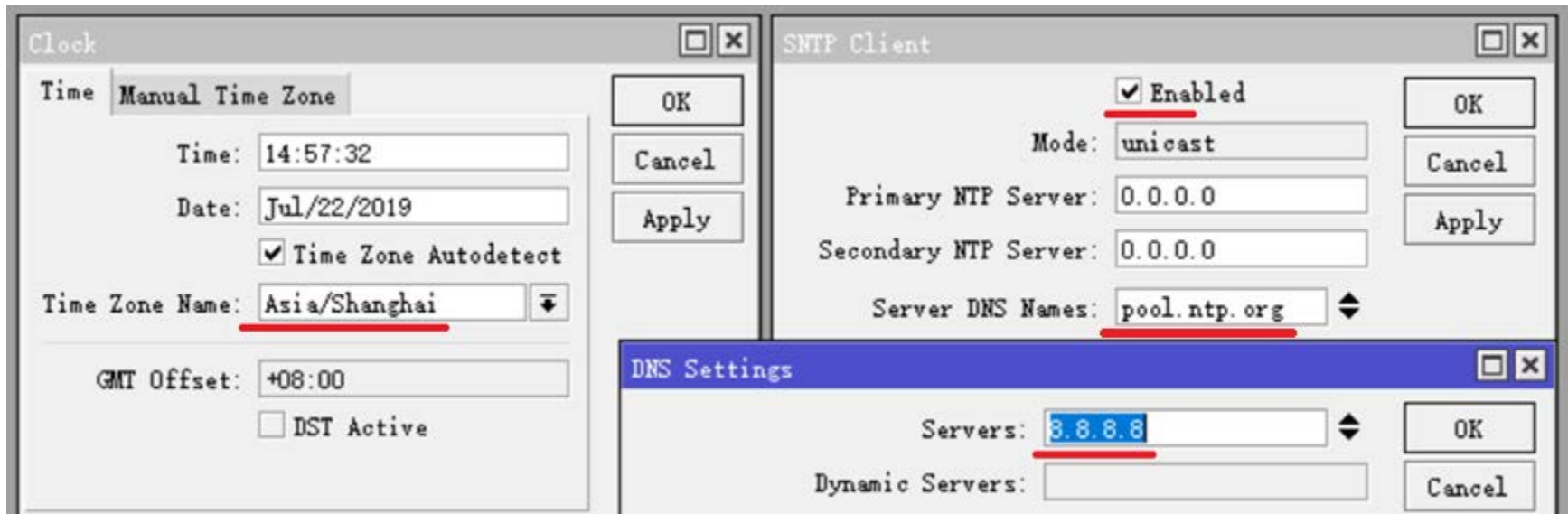
- Root CA (root.pem)
- Intermediate CA (intermediate.pem)
- Server certificate (v.leth.top.pem) and private key (v.leth.top.key)
- Doesn't support wildcard certificates (e.g. \*.leth.top)



The screenshot shows a window titled 'Certificates' with several tabs: 'Certificates', 'SCEP Servers', 'SCEP RA', 'Requests', 'OTP', and 'CRL'. Below the tabs are various action buttons: '+', '-', a funnel icon, 'Import', 'Card Reinstall', 'Card Verify', 'Revoke', 'Create Cert. Request', 'Settings', and 'Find'. The main area contains a table with the following data:

	Name	Issuer	Common Name	Subject Alt. Name	Key Size	
LT	intermediate	C=US, O=DigiCert ...	Encryption Everywhere DV TLS CA - G1		2048	
T	root	C=US, O=DigiCert ...	DigiCert Global Root CA		2048	
KT	v.leth.top	C=US, O=DigiCert ...	v.leth.top	DNS:v.leth.top	2048	

# Correct date/time setting





# Compatible RADIUS server

- FreeRADIUS
- Windows NPS
- TekRADIUS

# FreeRADIUS server



```
pi@raspberrypi:~ $ sudo vi /etc/freeradius/3.0/clients.conf

client LETH {
    ipaddr = 192.168.88.1
    secret = 123
}

pi@raspberrypi:~ $ sudo vi /etc/freeradius/3.0/mods-enabled/eap

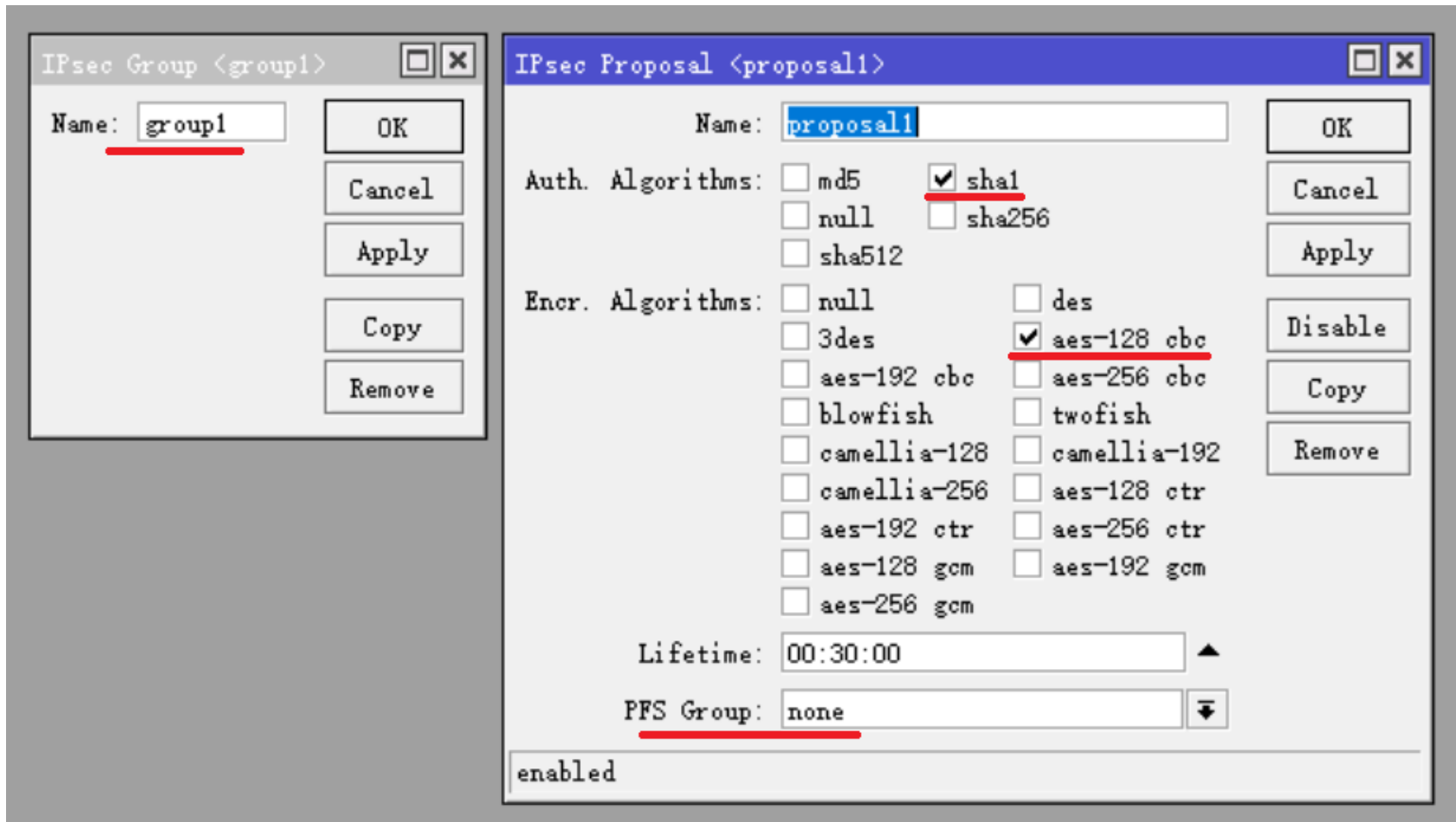
default_eap_type = mschap2

pi@raspberrypi:~ $ sudo vi /etc/freeradius/3.0/users

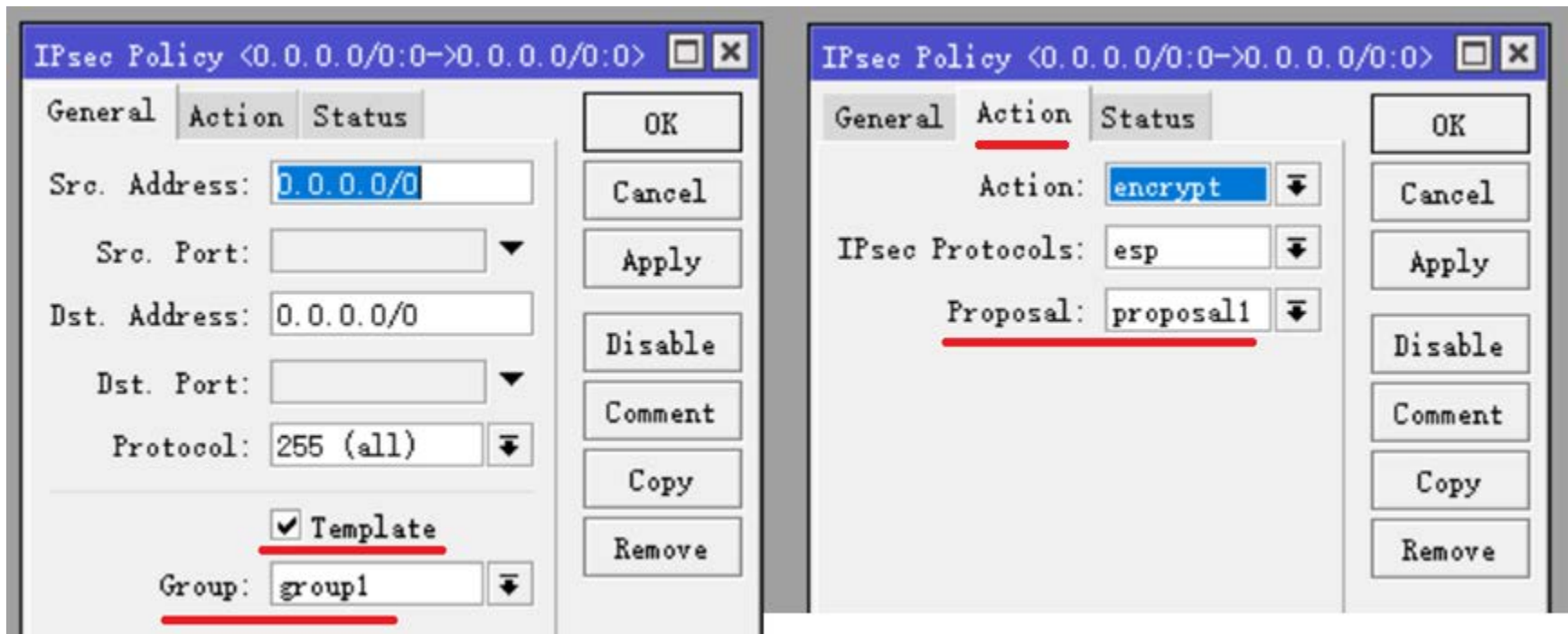
"jesse" Cleartext-Password := "123"
"lulu" Cleartext-Password := "123"
    Framed-IP-Address = 192.168.77.161

pi@raspberrypi:~ $ sudo /etc/init.d/freeradius restart
[ ok ] Restarting freeradius (via systemctl): freeradius.service.
```

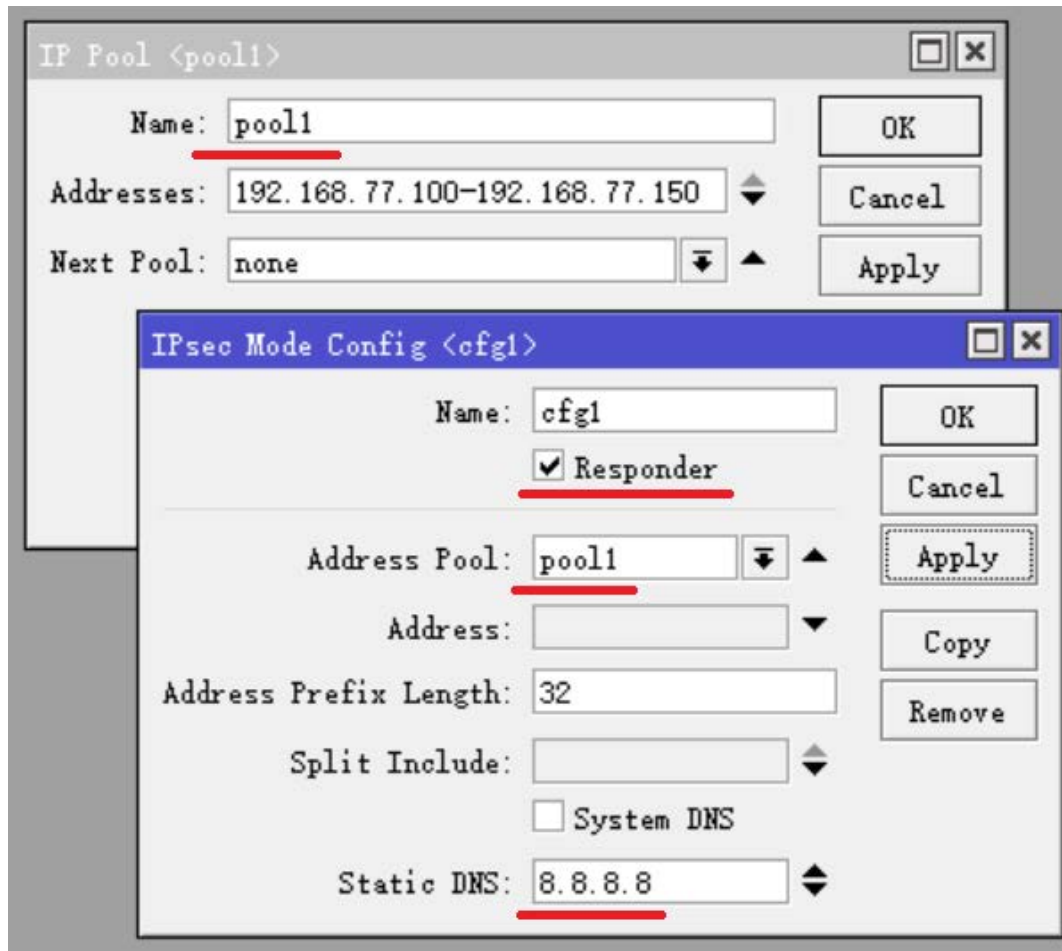
# Group and Proposal



# Policy template



# Pool and Mode config



# Peer and Identity

**IPsec Peer <peer1>**

Name: peer1

Address: ::/0

Port:

Local Address:

Profile: default

Exchange Mode: IKE2

Passive

Send INITIAL\_CONTACT

enabled responder

**IPsec Identity <peer1>**

Peer: peer1

Auth. Method: eap radius

Certificate: v.leth.top

intermediate

Policy Template Group: group1

Notrack Chain:

My ID Type: auto

Remote ID Type: auto

Match By: remote id

Mode Configuration: cfg1

Generate Policy: port strict

# RADIUS client

New RADIUS Server

General Status

Service:  ppp  login  
 hotspot  wireless  
 dhcp  ipsec  
 dot1x

Called ID:

Domain:

Address: 192.168.88.2

Protocol:

Secret: \*\*\*

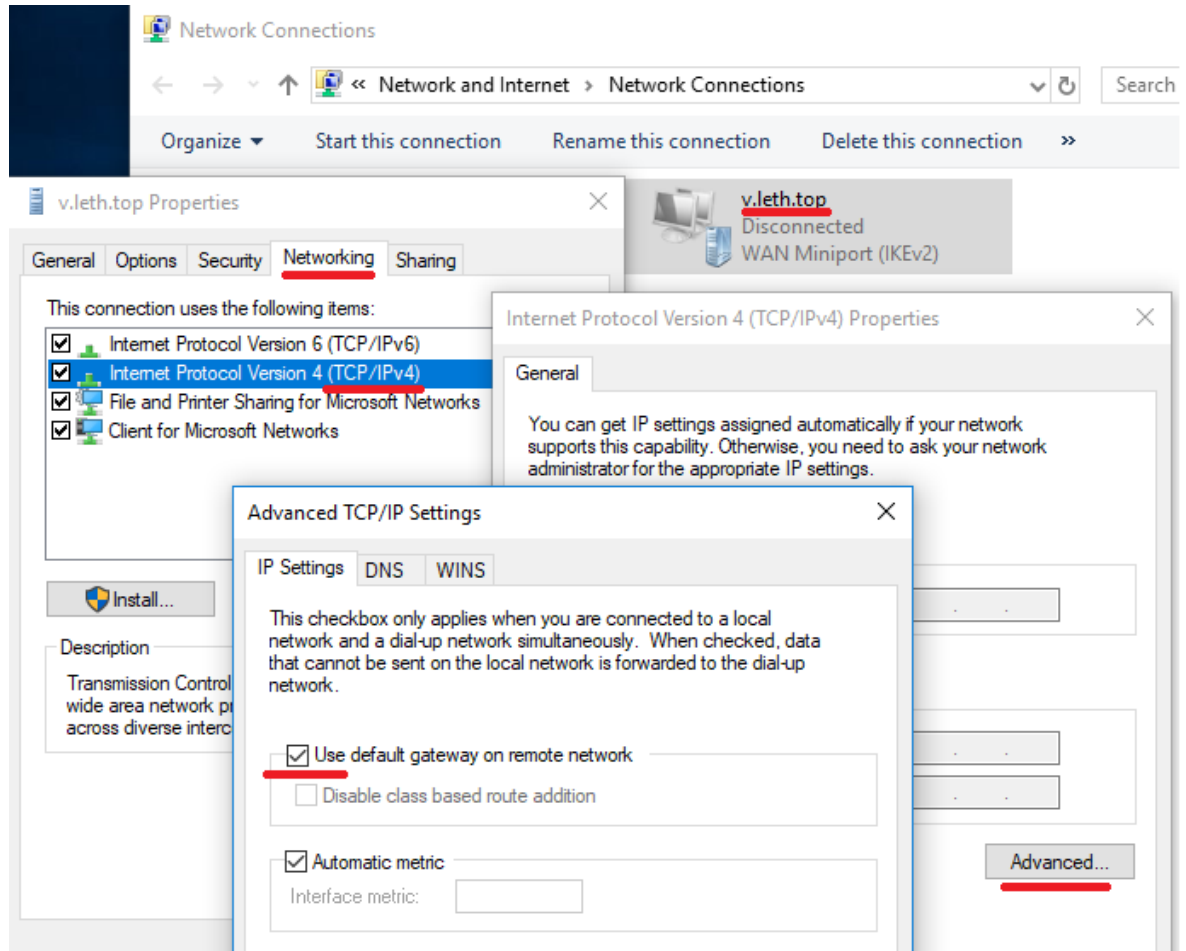
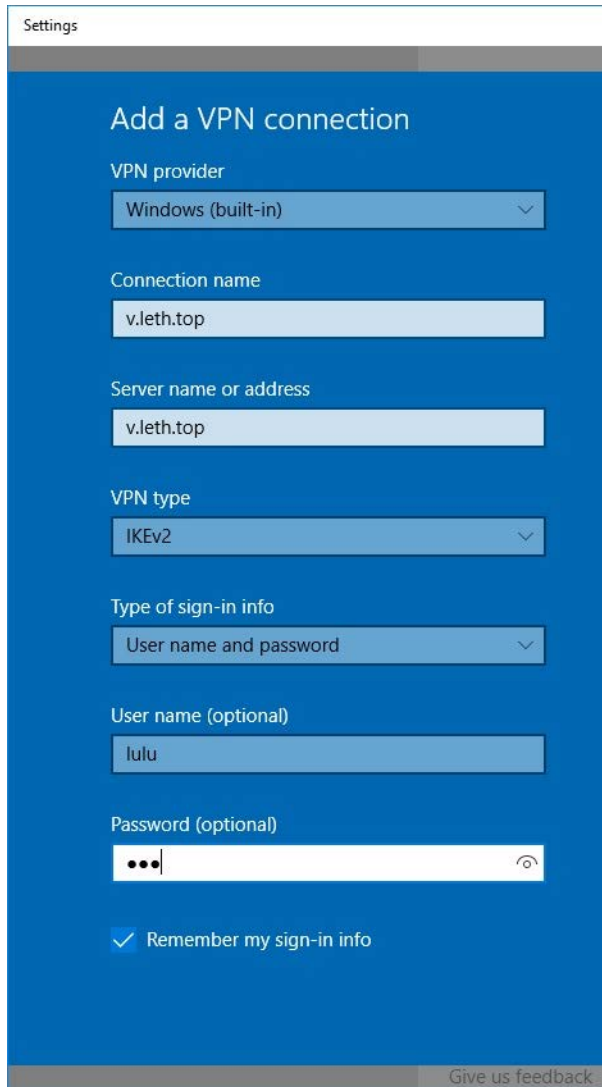
Authentication Port:

Accounting Port:

Timeout:  ms

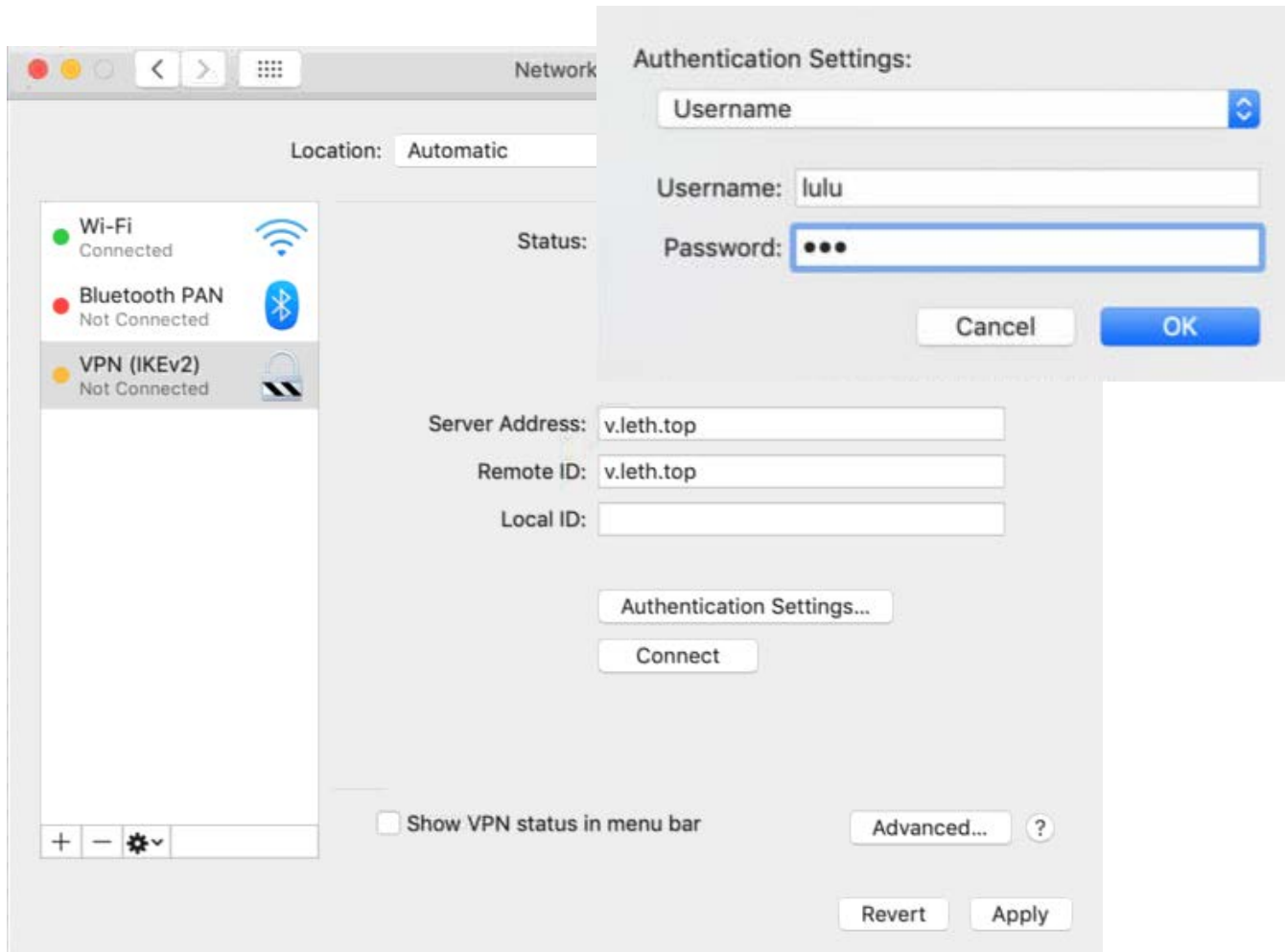
OK  
Cancel  
Apply  
Disable  
Comment  
Copy  
Remove  
Reset Status

# Windows client

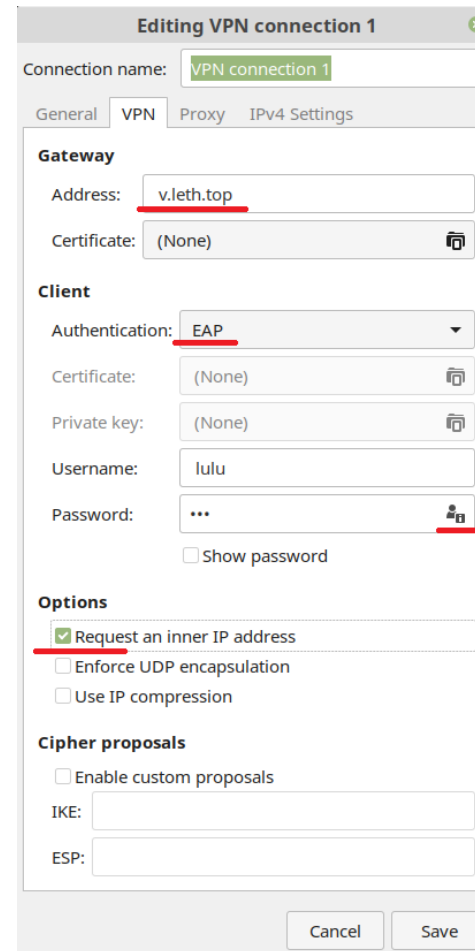
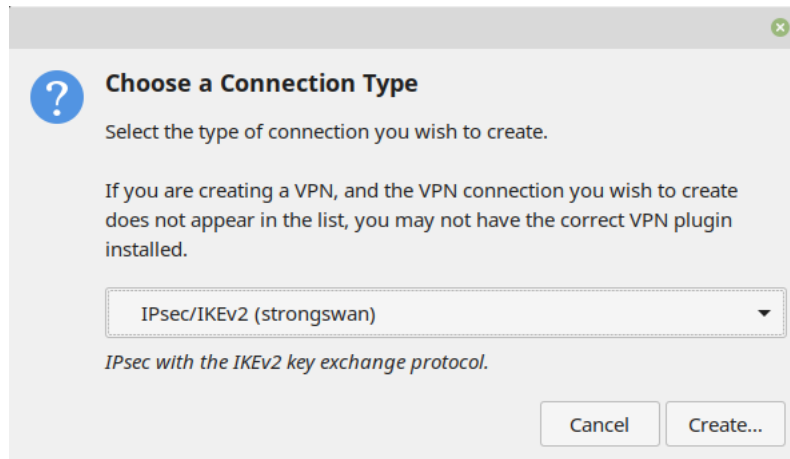




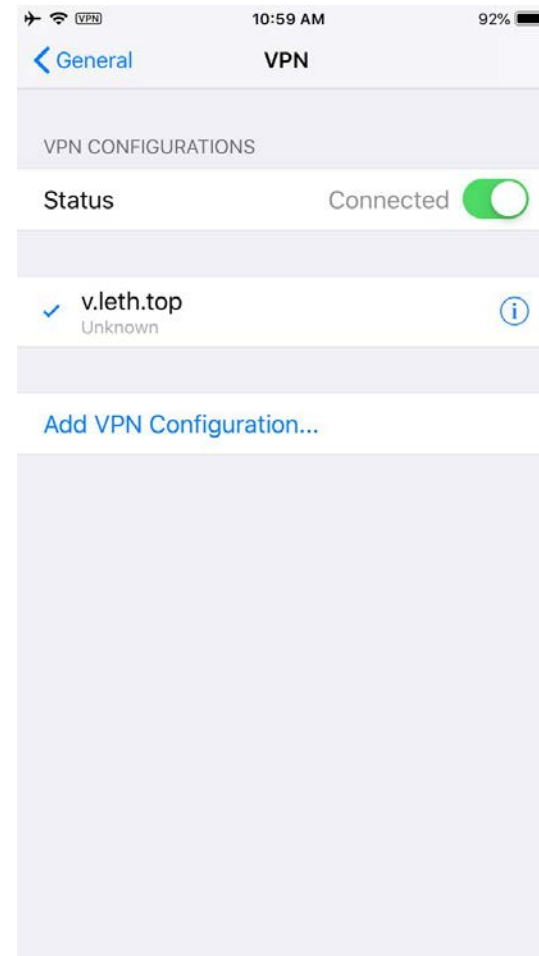
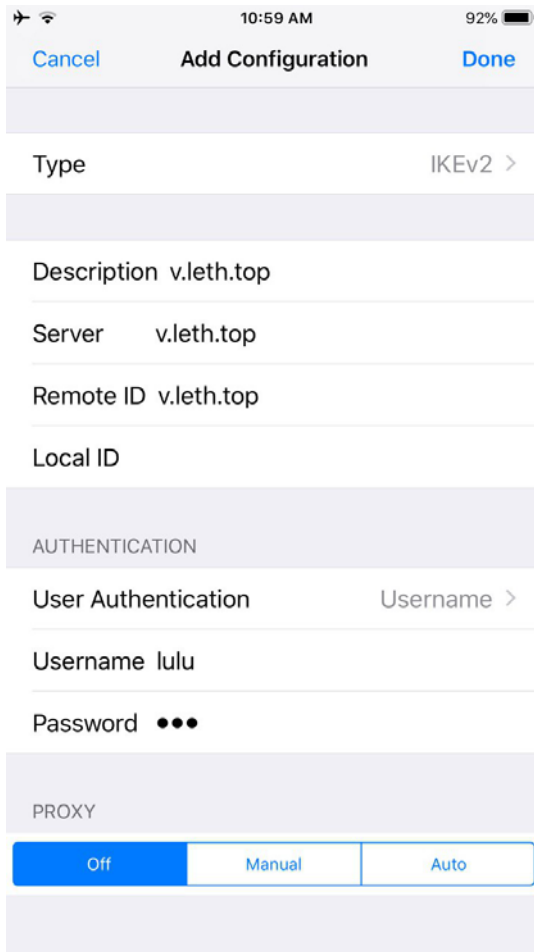
# macOS client



# Linux Mint client

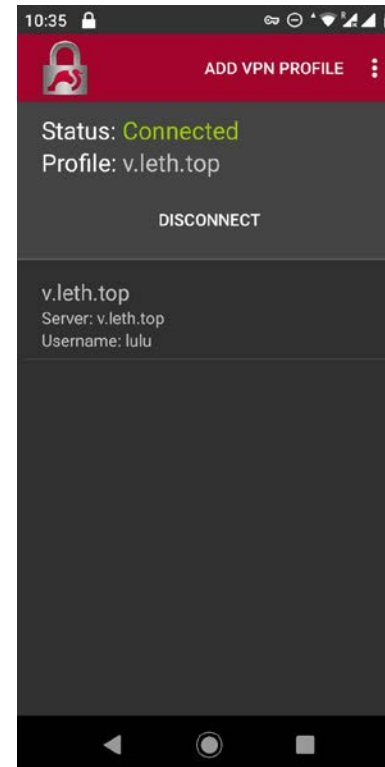
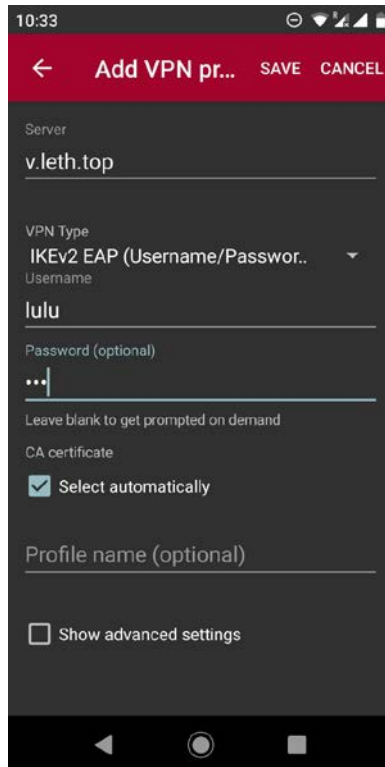


# iOS/iPadOS client



# Android and ChromeOS client

- <https://play.google.com/store/apps/details?id=org.strongswan.android>
- <https://download.strongswan.org/Android/>



# RouterOS client

The screenshot displays the Mikrotik WinBox interface for configuring IPsec. The main window is titled 'Certificates' and contains a table of certificates. Overlaid on this are four configuration dialog boxes:

- New Firewall Address List:** Name: list1, Address: 192.168.88.8
- IPsec Mode Config <request-only>:** Name: request-only, Src. Address List: list1
- IPsec Peer <peer1>:** Name: peer1, Address: v.leth.top, Exchange Mode: IKE2, Send INITIAL\_CONTACT checked
- IPsec Identity <peer1>:** Peer: peer1, Auth. Method: eap, EAP Methods: MS-CHAPv2, Username: lulu, Password: \*\*\*

The 'Certificates' table at the top shows the following data:

Name	Issuer	Common Name	Subject A...	Key Size	Days Valid	Trusted
T root	C=US,O=DigiCert ...	DigiCert Global Root CA		2048	9131	yes

More information at:

<https://wiki.mikrotik.com/wiki/Manual:IP/IPsec>

Thank you for participating