



Mikrotik User Meeting
Colombo, June 5th 2017

L2TP/IPsec Configuration with RouterOS to work with Android

Rafi Naufal
State Vocational High School 1
Indonesia



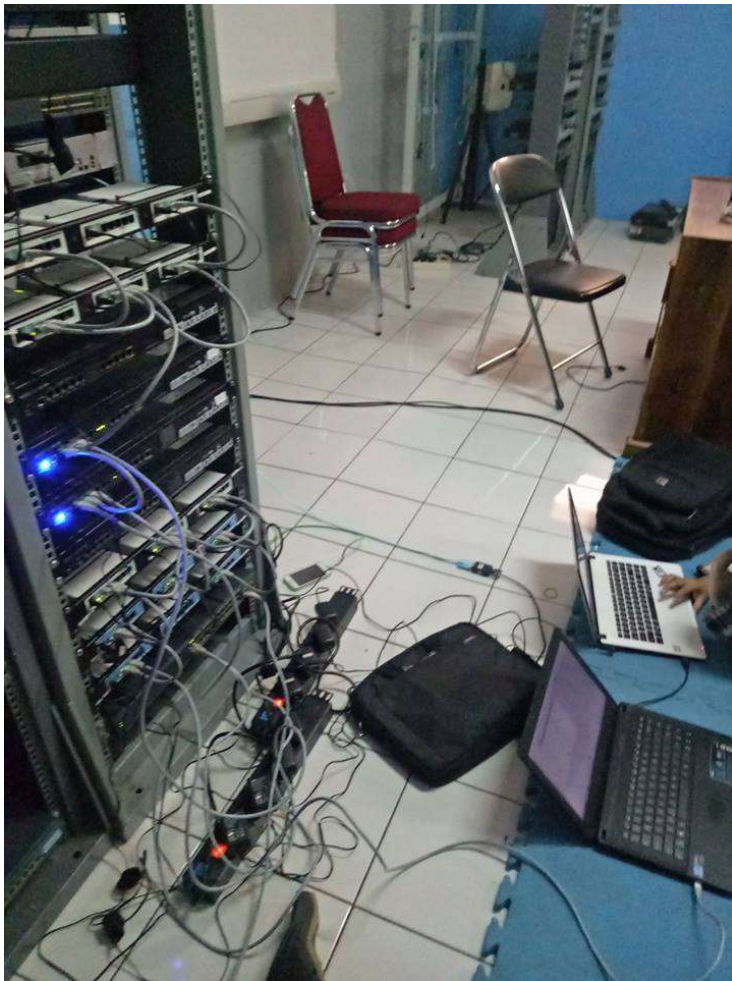
About Me

- Rafi Naufal
- State Vocational High School 1
- Pesantren Networkers
- MTCNA, MTCRE, MTCINE
- Mikrotik Certified Consultant
- Network Trainer at INTRA Training Centre

About State Vocational High School



Networking Class



RumahNgoprek



About Pesantren Networkers





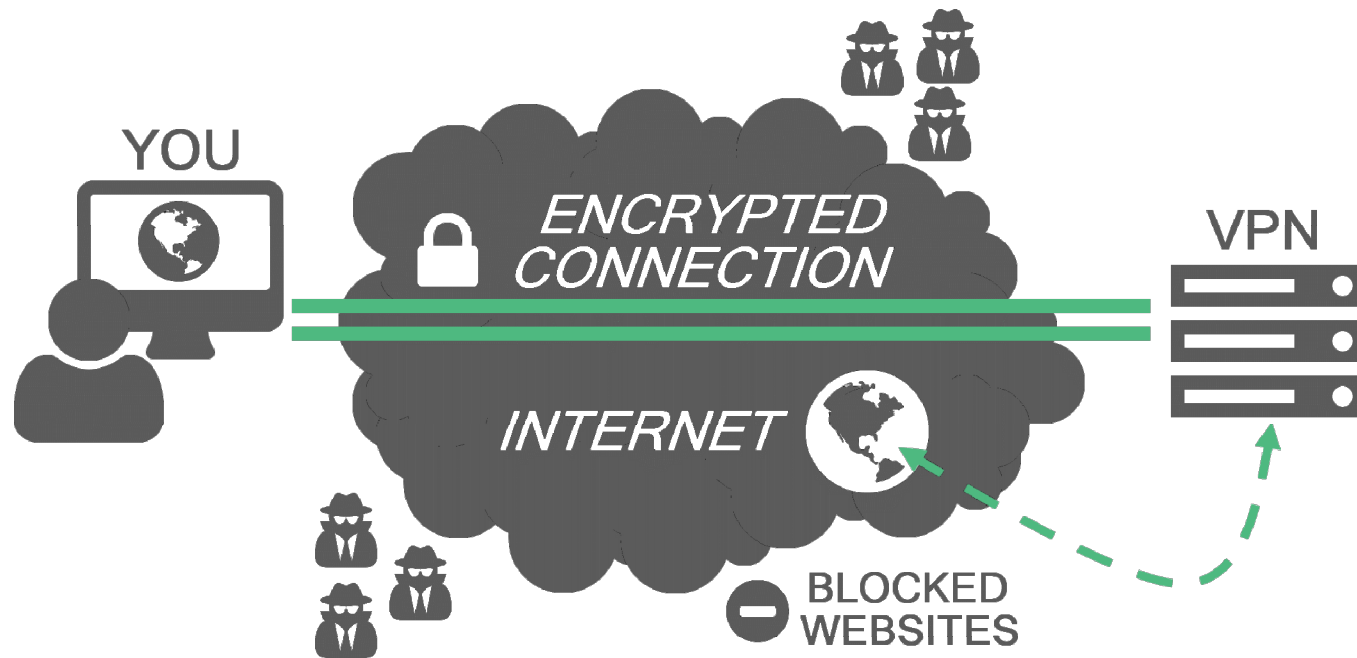
What is Virtual Private Networking

What is VPN



Virtual Private Network is a network technology that allow you to make a secure private network in public network.

How VPN Work?



VPN will make their private network using Tunnel to communicate over Internet.

Advantage if we use VPN

- Your ISP didn't know what you get up to on the internet
- You appear to access the internet from the IP address of the VPN server
- Safe to use Public Wi-Fi Hotspot



Disadvantage if we use VPN

- Your internet will slow down



L2TP

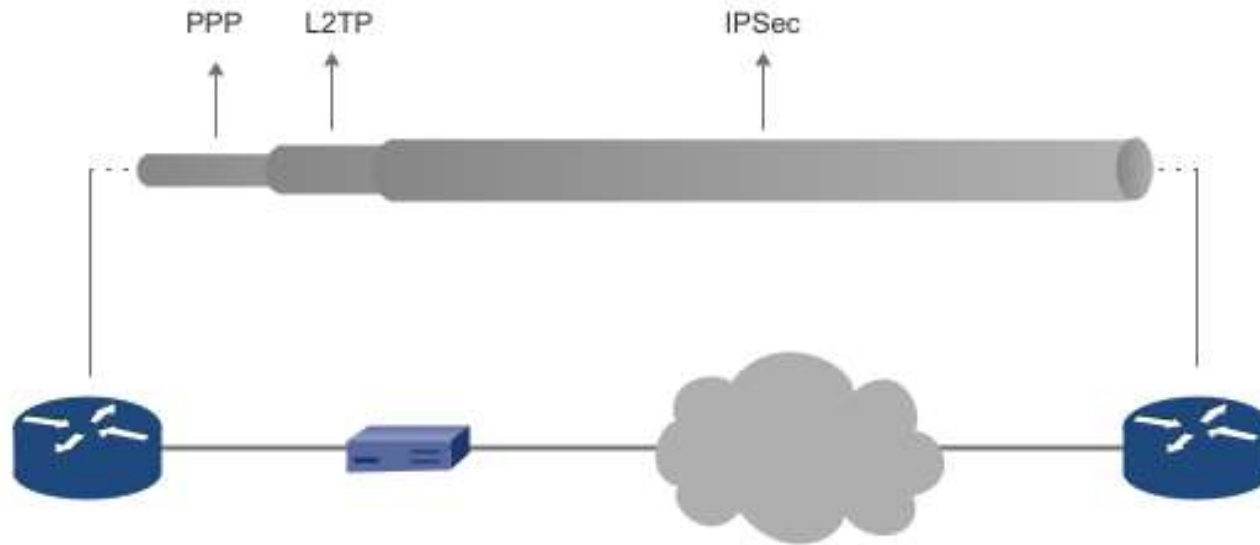
Layer 2 Tunneling Protocol

What is L2TP?



Method that you can use to make a tunnel for your VPN

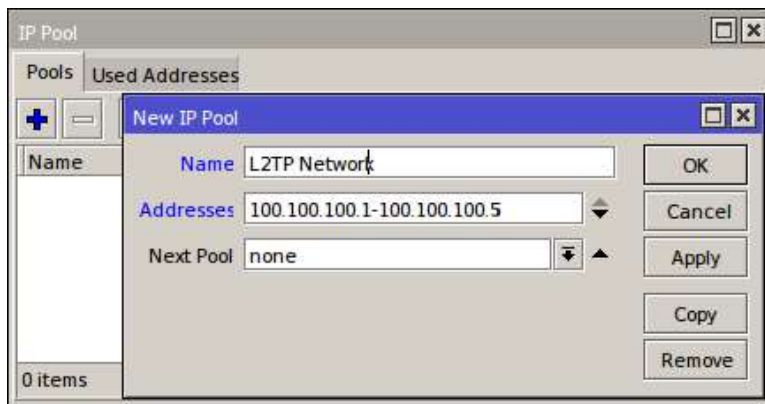
If L2TP Combine with IPSec



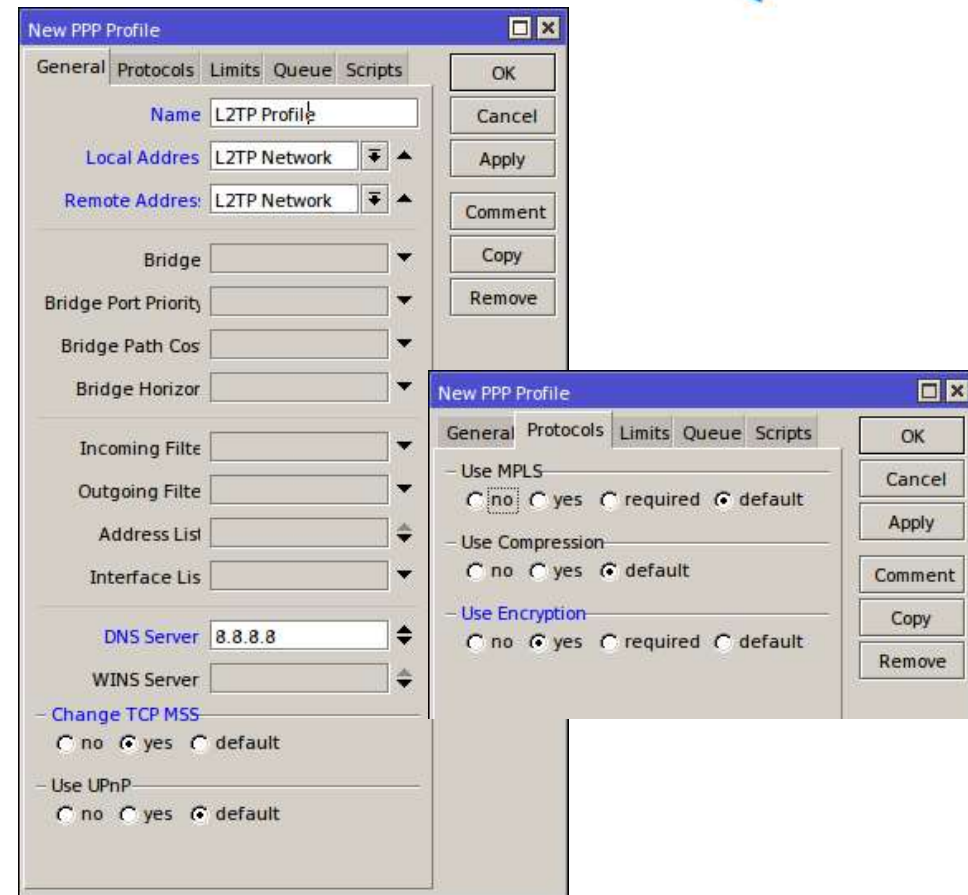
If PPP send from one site to other site, L2TP will encrypt to packet in L2TP Tunnel. And if we combine L2TP with IPsec, IPsec will encrypt L2TP Tunnel.

Configure Mikrotik as L2TP Server for Android Client

L2TP Configuration

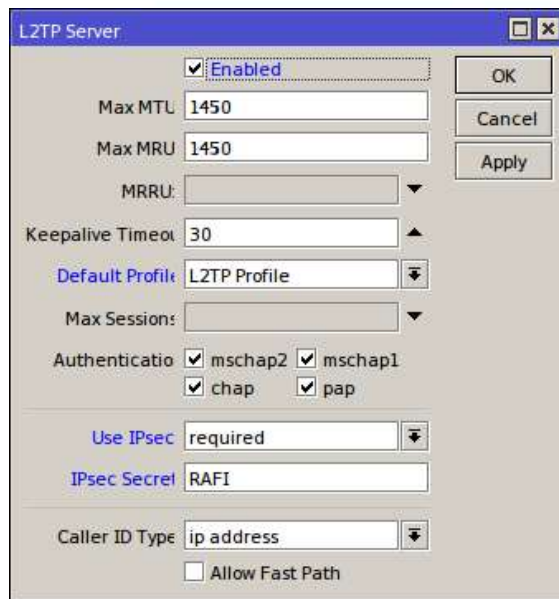


Make IP Pool for L2TP Network



Make a new PPP Profile

L2TP Configuration



The L2TP Server configuration window shows the following settings:

- ☒ Enabled
- Max MTU: 1450
- Max MRU: 1450
- MRRU: (empty)
- Keepalive Timeout: 30
- Default Profile: L2TP Profile
- Max Session: (empty)
- Authentication: ☒ mschap2, ☒ mschap1, ☒ chap, ☒ pap
- Use IPsec: required
- IPsec Secret: RAFI
- Caller ID Type: ip address
- ☐ Allow Fast Path

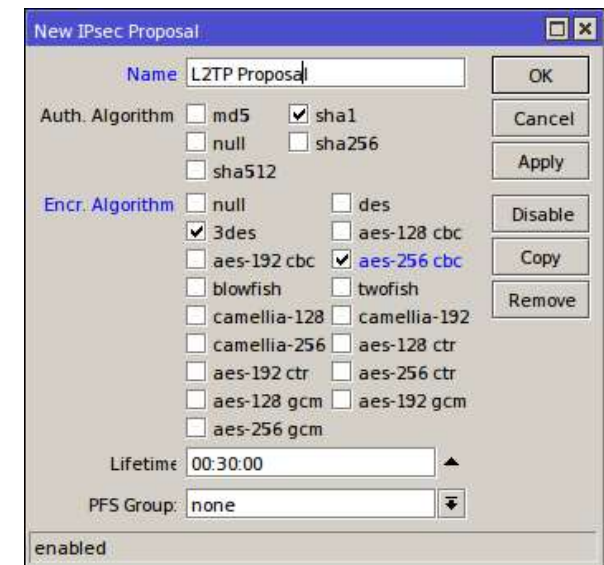
Enable L2TP Server



The New PPP Secret configuration window shows the following settings:

- Name: RumahNgoprek
- Password: Ivocational
- Service: l2tp
- Caller ID: (empty)
- Profile: L2TP Profile

Make a new PPP Secret for L2TP

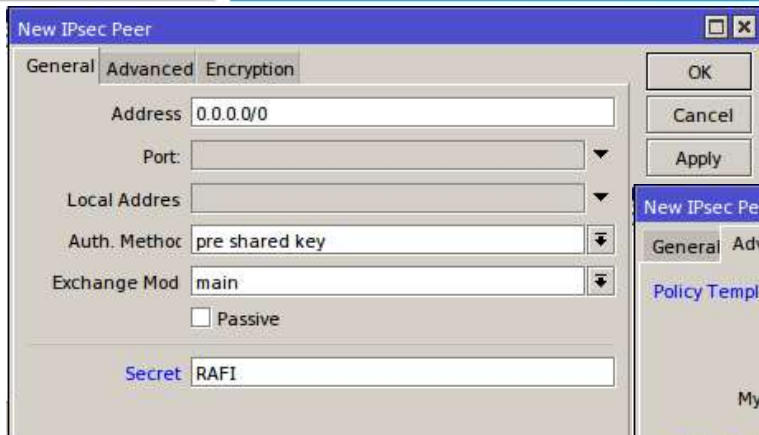


The New IPsec Proposal configuration window shows the following settings:

- Name: L2TP Proposal
- Auth. Algorithm: ☐ md5, ☒ sha1, ☐ null, ☐ sha256, ☐ sha512
- Encr. Algorithm: ☐ null, ☐ des, ☒ 3des, ☐ aes-128 cbc, ☒ aes-256 cbc, ☐ blowfish, ☐ twofish, ☐ camellia-128, ☐ camellia-192, ☐ camellia-256, ☐ aes-128 ctr, ☐ aes-192 ctr, ☐ aes-256 ctr, ☐ aes-128 gcm, ☐ aes-192 gcm, ☐ aes-256 gcm
- Lifetime: 00:30:00
- PFS Group: none
- enabled

Make a new IPsec Proposal for L2TP

Configure IPsec Peer



New IPsec Peer

General | Advanced | Encryption

Address: 0.0.0.0/0

Port: [dropdown]

Local Address: [dropdown]

Auth. Method: pre shared key

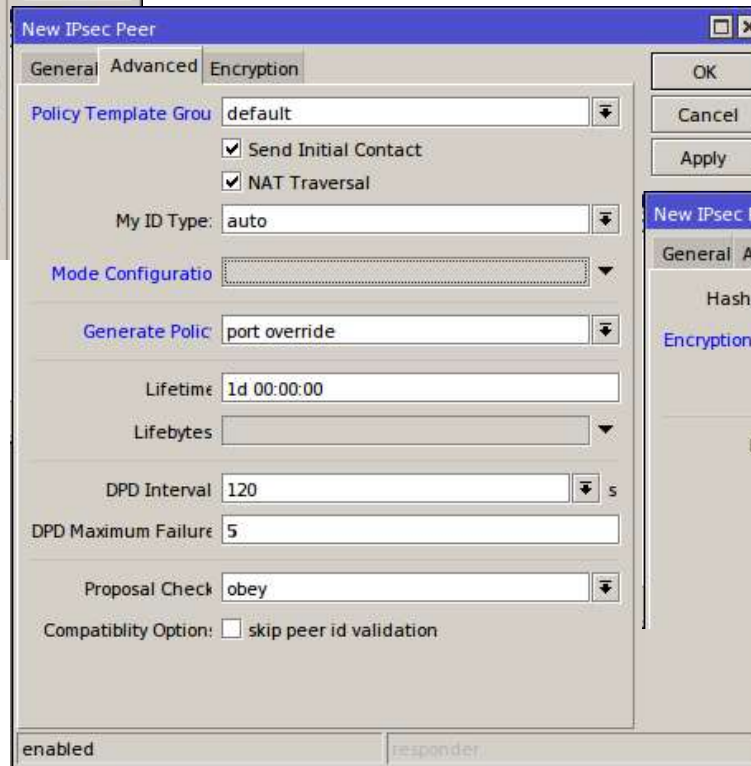
Exchange Mod: main

☐ Passive

Secret: RAFI

OK Cancel Apply

Define that everyone who know ipsec secret, will be connect to ipsec server.



New IPsec Peer

General | Advanced | Encryption

Policy Template Group: default

☒ Send Initial Contact

☒ NAT Traversal

My ID Type: auto

Mode Configuration: [dropdown]

Generate Policy: port override

Lifetime: 1d 00:00:00

Lifeytes: [dropdown]

DPD Interval: 120 s

DPD Maximum Failure: 5

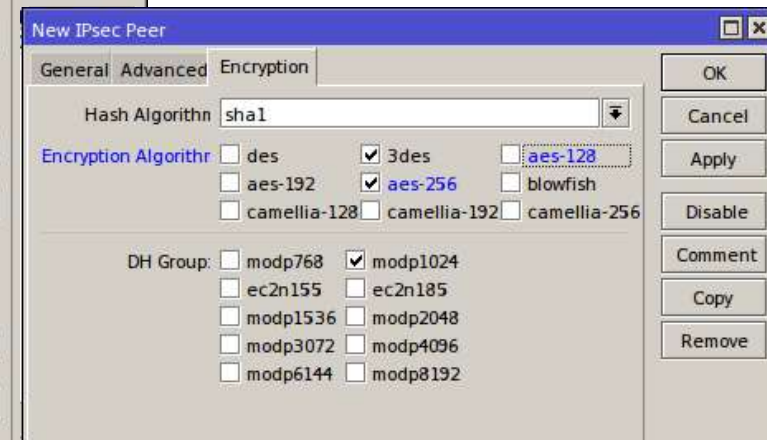
Proposal Check: obey

Compatibility Option: ☐ skip peer id validation

enabled responder

OK Cancel Apply

Configure Policy Template



New IPsec Peer

General | Advanced | Encryption

Hash Algorithm: sha1

Encryption Algorithm:

- ☐ des ☒ 3des ☐ aes-128
- ☐ aes-192 ☒ aes-256 ☐ blowfish
- ☐ camellia-128 ☐ camellia-192 ☐ camellia-256

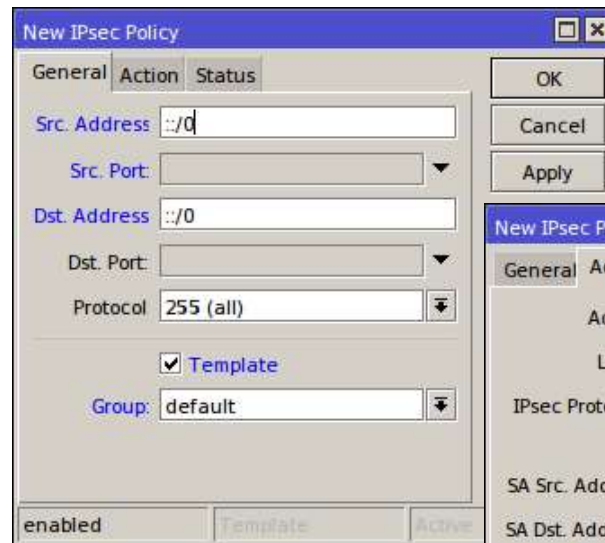
DH Group:

- ☐ modp768 ☒ modp1024
- ☐ ec2n155 ☐ ec2n185
- ☐ modp1536 ☐ modp2048
- ☐ modp3072 ☐ modp4096
- ☐ modp6144 ☐ modp8192

OK Cancel Apply Disable Comment Copy Remove

Configure what encryption algorithm will we use

Configure IPsec Policy



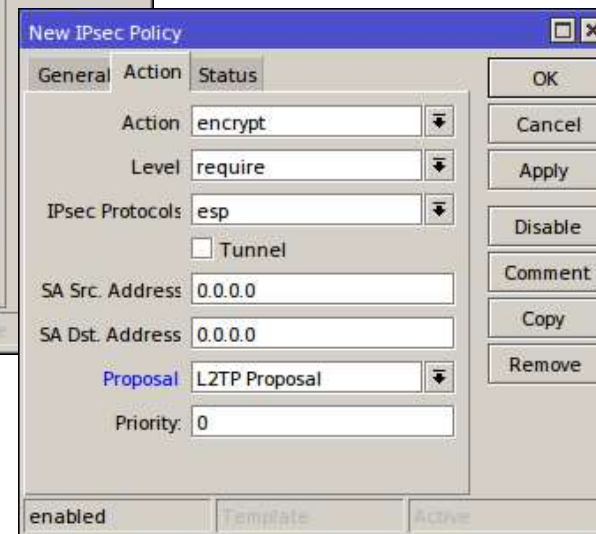
The 'New IPsec Policy' dialog box, General tab, shows the following configuration:

- Src. Address:
- Src. Port:
- Dst. Address:
- Dst. Port:
- Protocol:
- ☒ Template
- Group:

Buttons: OK, Cancel, Apply

Footer: enabled, Template, Active

Configure that all address is include.



The 'New IPsec Policy' dialog box, Action tab, shows the following configuration:

- Action:
- Level:
- IPsec Protocols:
- ☐ Tunnel
- SA Src. Address:
- SA Dst. Address:
- Proposal:
- Priority:

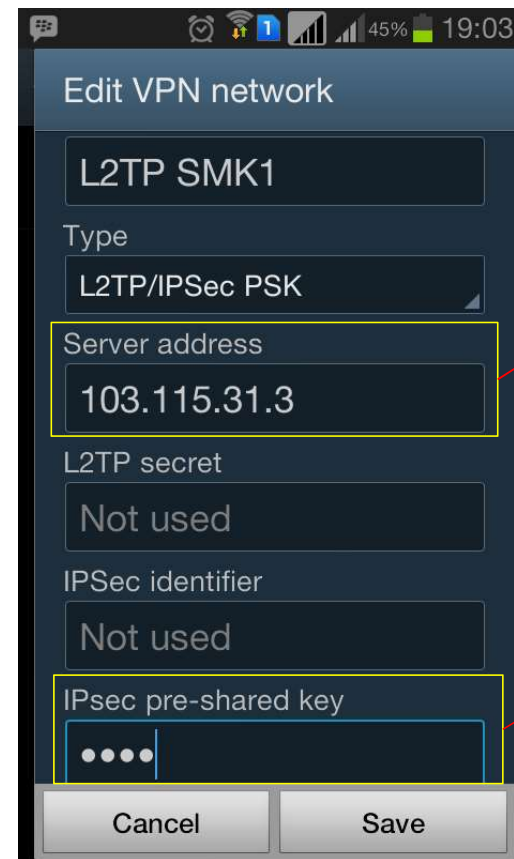
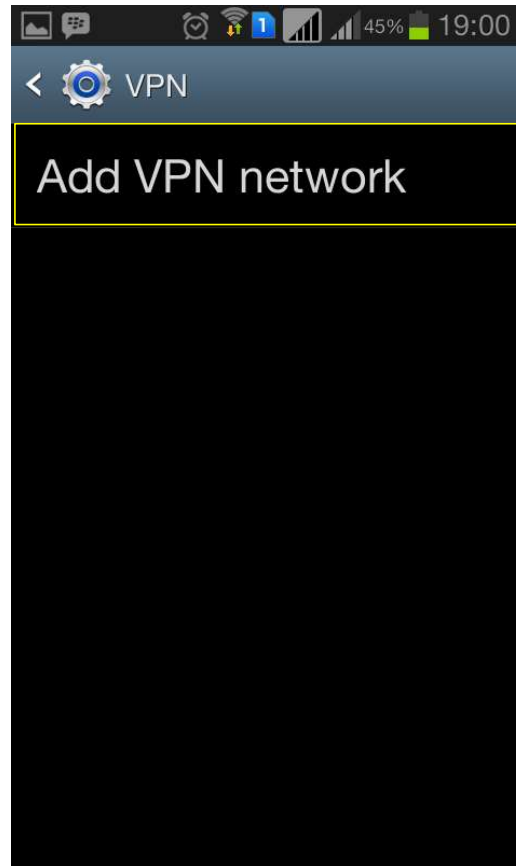
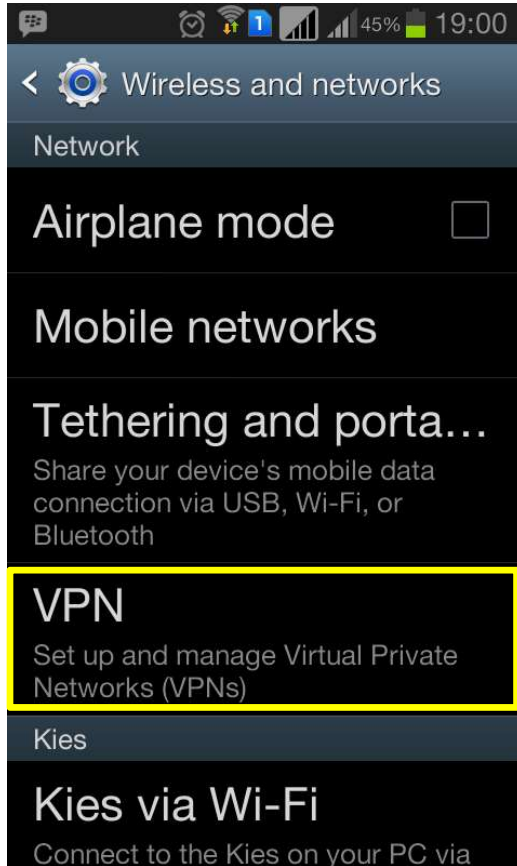
Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove

Footer: enabled, Template, Active

Define what IPsec protocol will we use

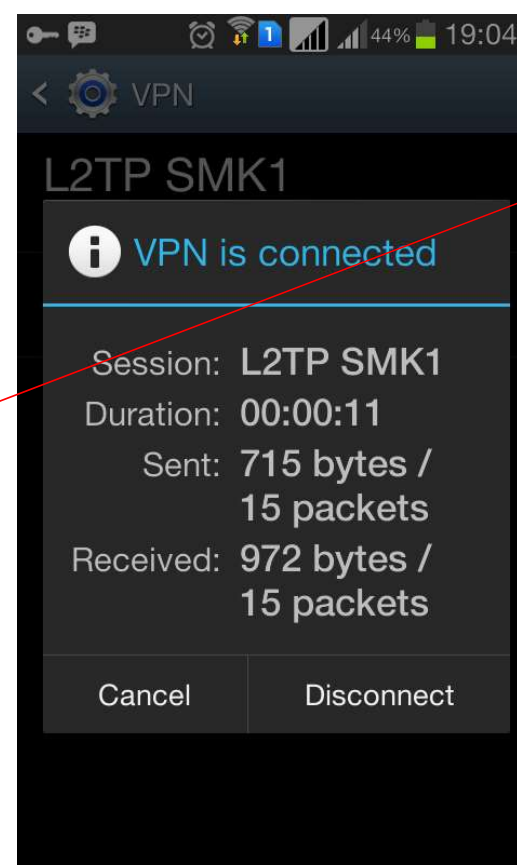
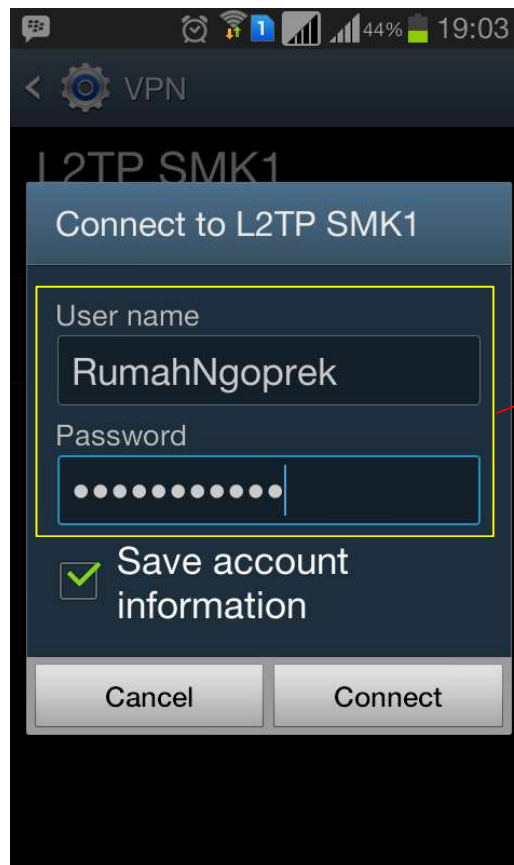
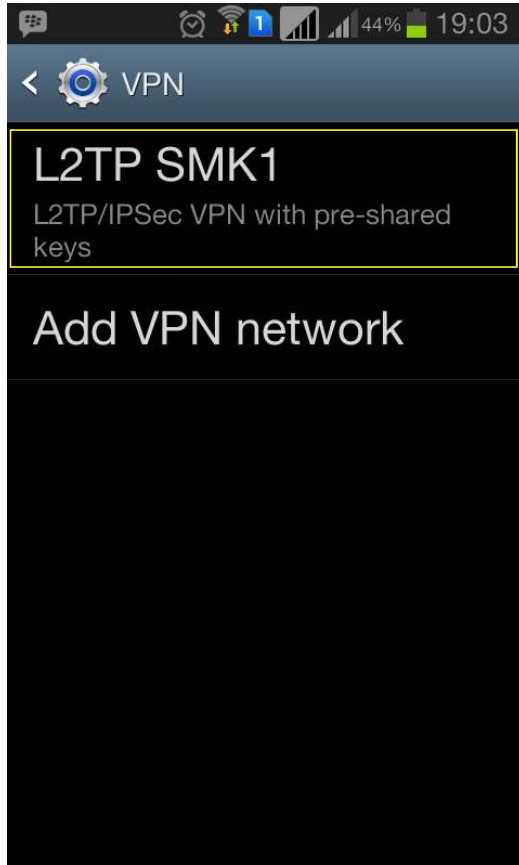
Configure Android Phone

Configuration on Android Phone



Server Address

Secret that we have configure on IPsec Peer



User and password that we have configure in PPP Secret

Verification

PPP

Interface	PPPoE Servers	Secrets	Profiles	Active Connections	L2TP Secrets
<div> <div>—</div> <div>Y</div> </div>					
Name	Service	Caller ID	Encoding	Address	Uptime
L Rumah...	l2tp	103.115.31.2	cbc(aes...	100.100.100.3	00:04:23

There is active connections in PPP

IPsec

Policies	Groups	Peers	Remote Peers	Mode Configs	Proposals	Installed SAs	Keys	Users
<div> <div>—</div> <div>Y</div> <div>Kill Connections</div> <div>Find</div> </div>								
Local Address	Remote Address							
103.115.31.3	103.115.31.2							

IPSec remote peers active

Verification

Address and user

MikroTik

Address
100.100.100.4

Login
admin

Password

☒ Secure mode ☒ Keep password

SAVE CONNECT

Tik-App v0.0.53 Report bug...

RB951Ui-2HnD (mipsbe)
admin@100.100.100.4 (MikroTik)
Safe Mode

Disconnect
CAPsMAN
Interfaces
Wireless
Switch
Bridge
PPP

Discuss about Network?



+62 85211179523



rafi.mcqueen95@gmail.com



www.linkedin.com/in/rafi-naufal-ba3379118/



www.ngonfigterus.id

Terima Kasih
Thank You
ස්තූතියි