IPSEC over L2tp between Debian as server and Mikrotik as client

By

Ehsan Aminian

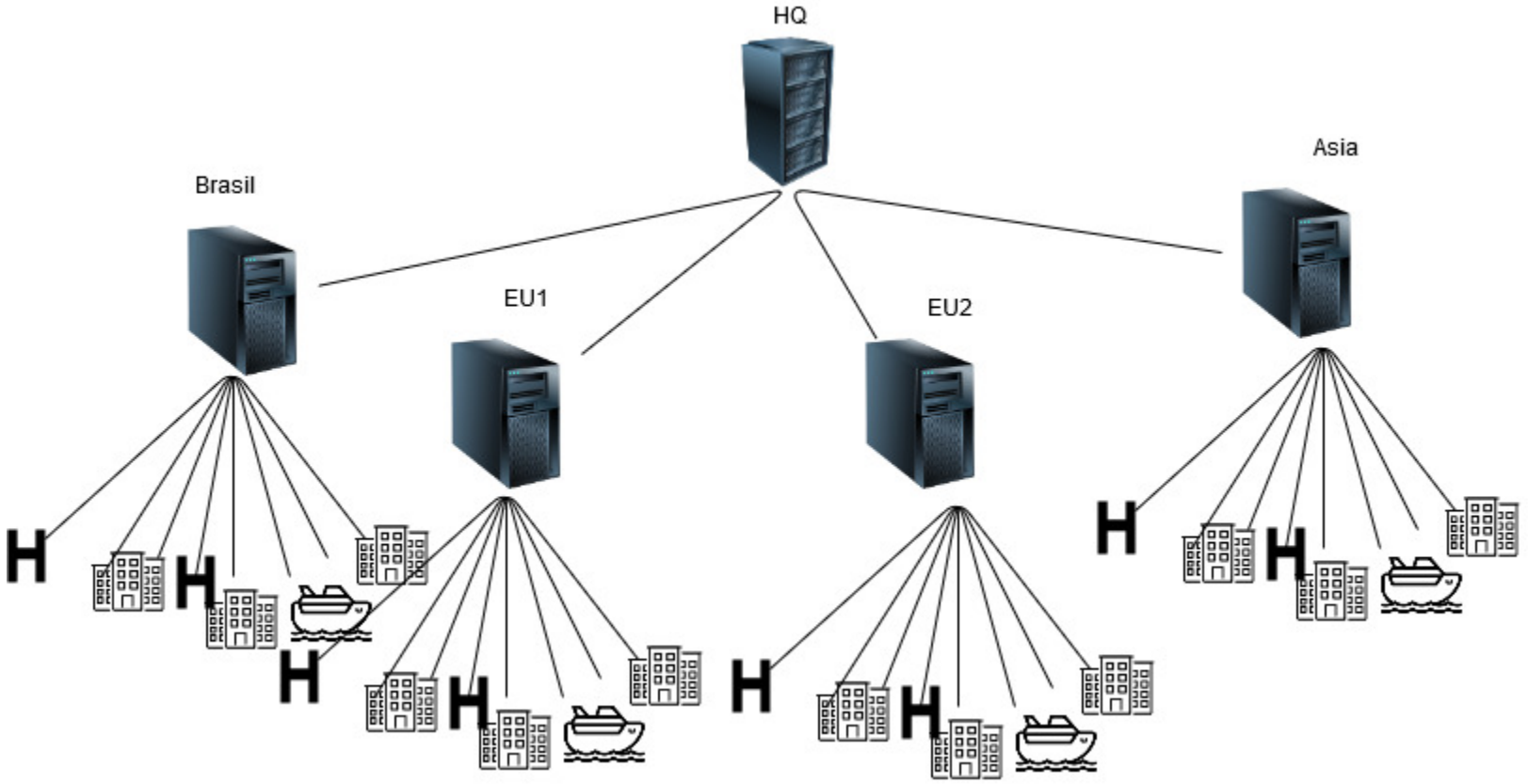
(Certified Trainer - TR0444, MTCNA,MTCRE,MTCUME,MTCINE,MTCTCE)

MikrotikLand (training center)

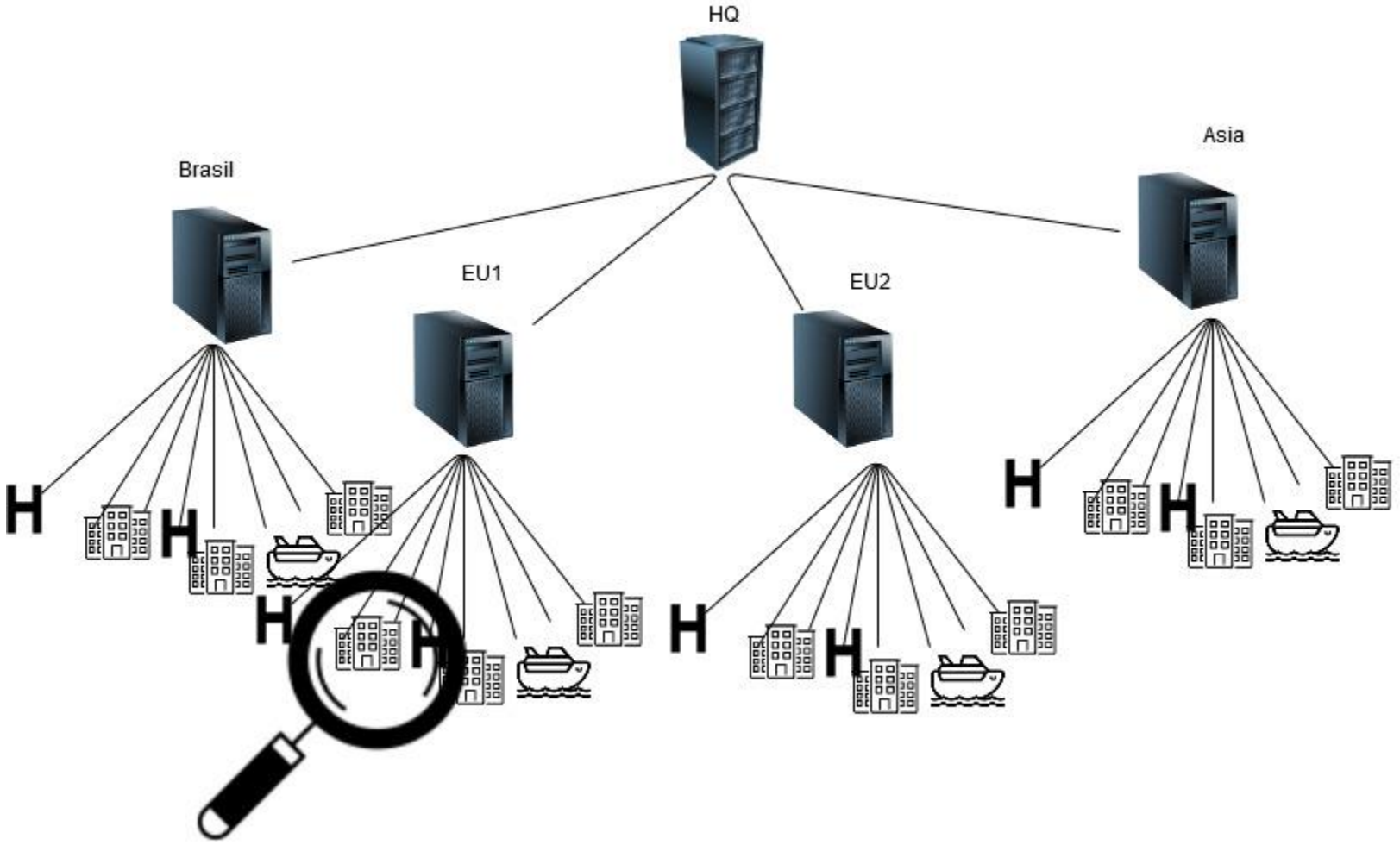
Outline

- Network Topology
- Limitations
- Solution
- Configurations
- Questions

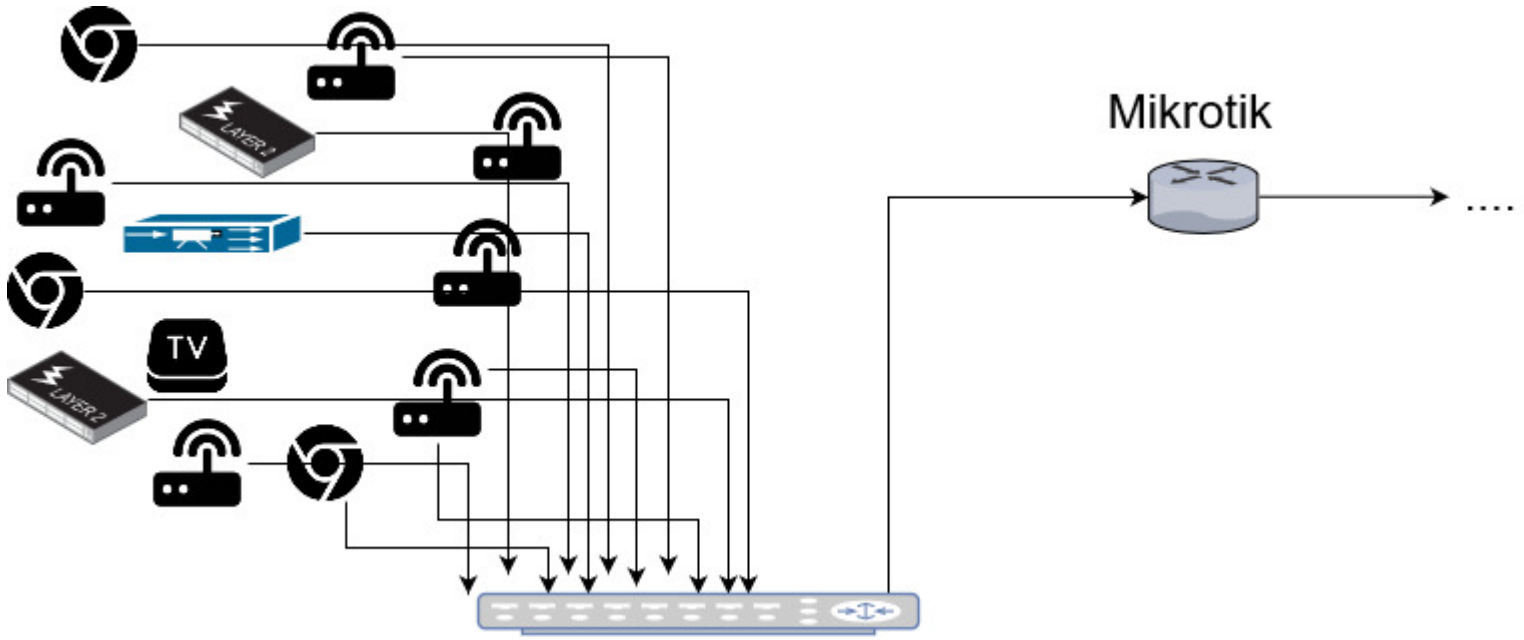
Network Topology



Network Topology

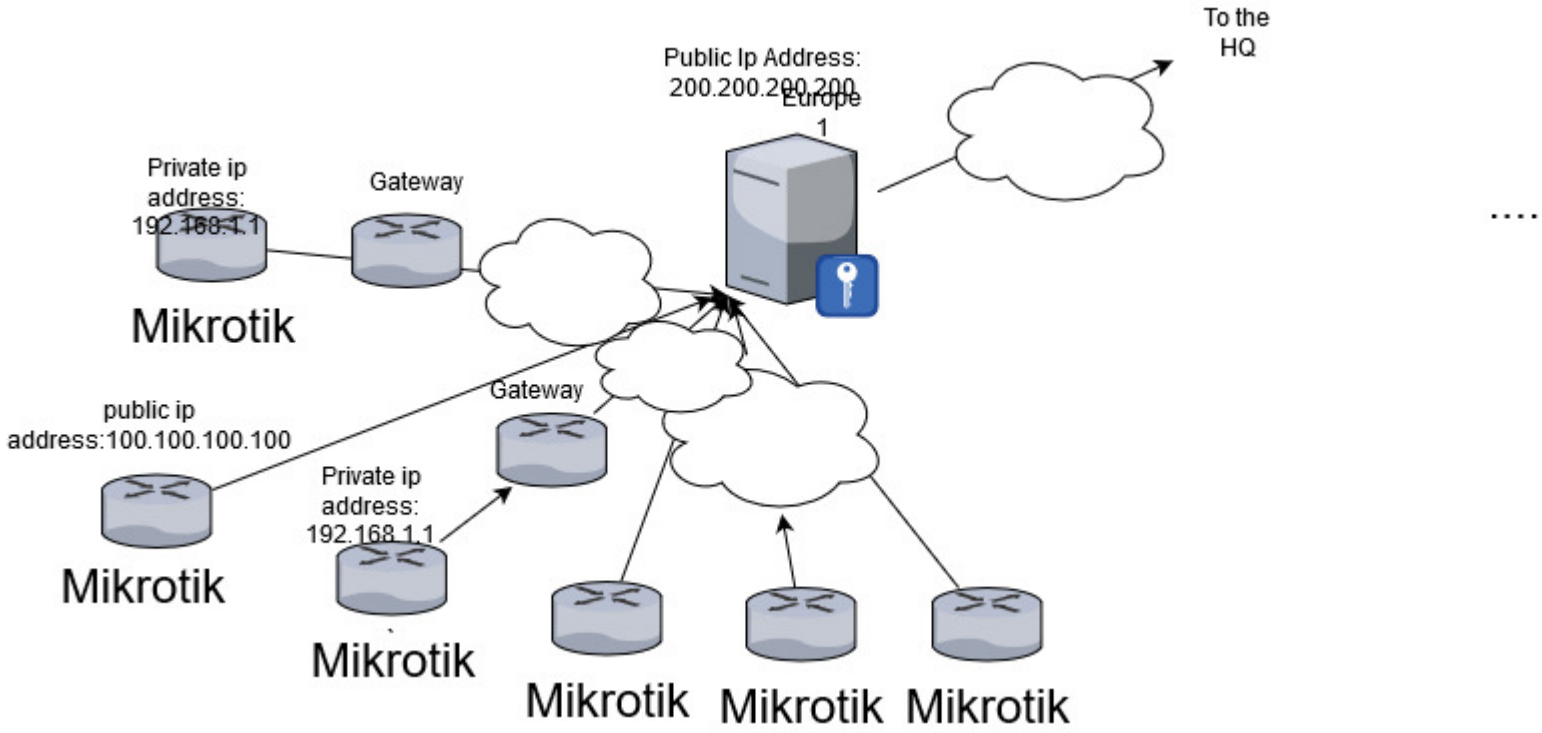


Network Topology



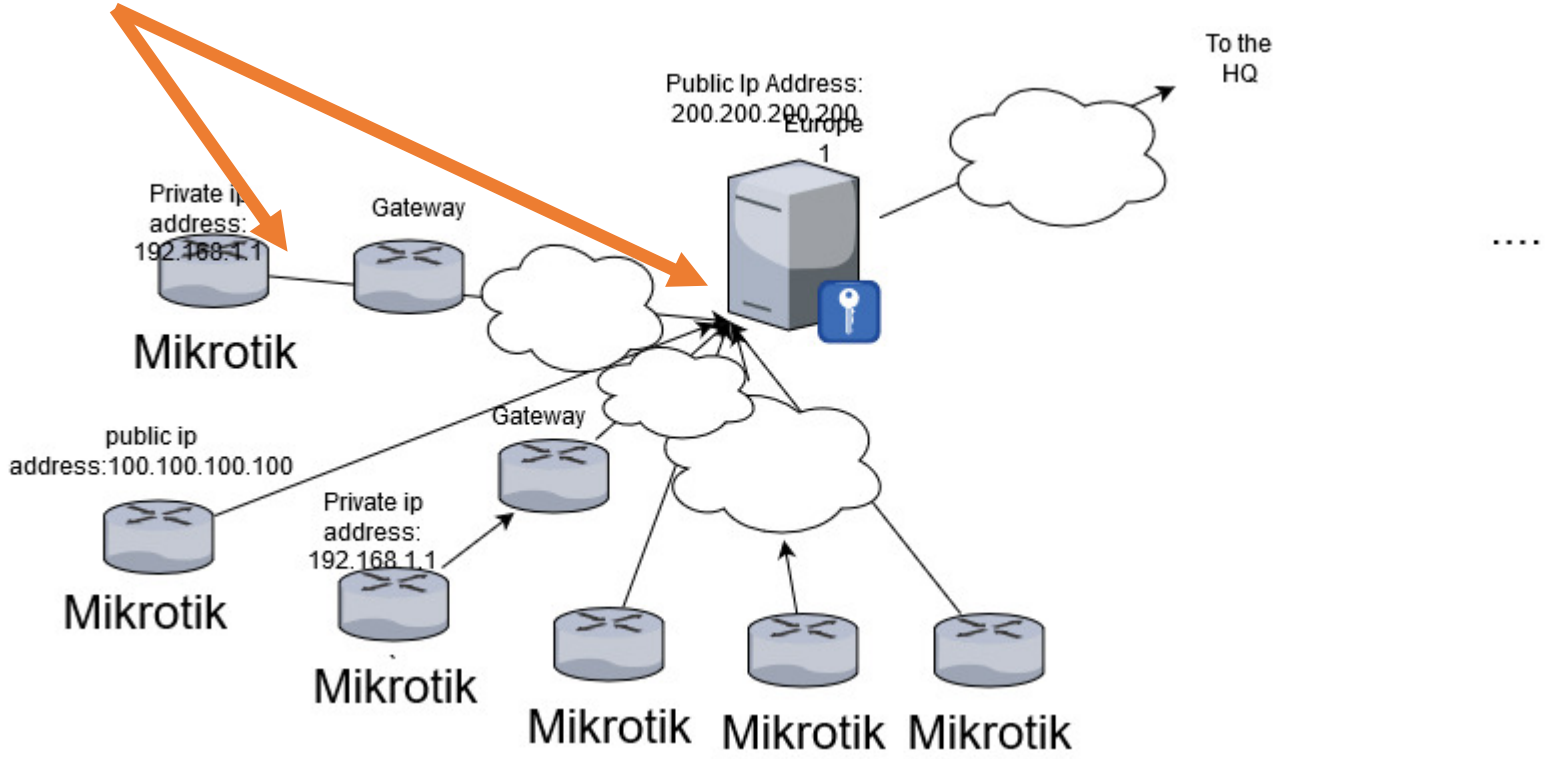
Limitations

- Each customer has its own IP assigning policy.
- Some of Mikrotik may not have even public IP address



Solution

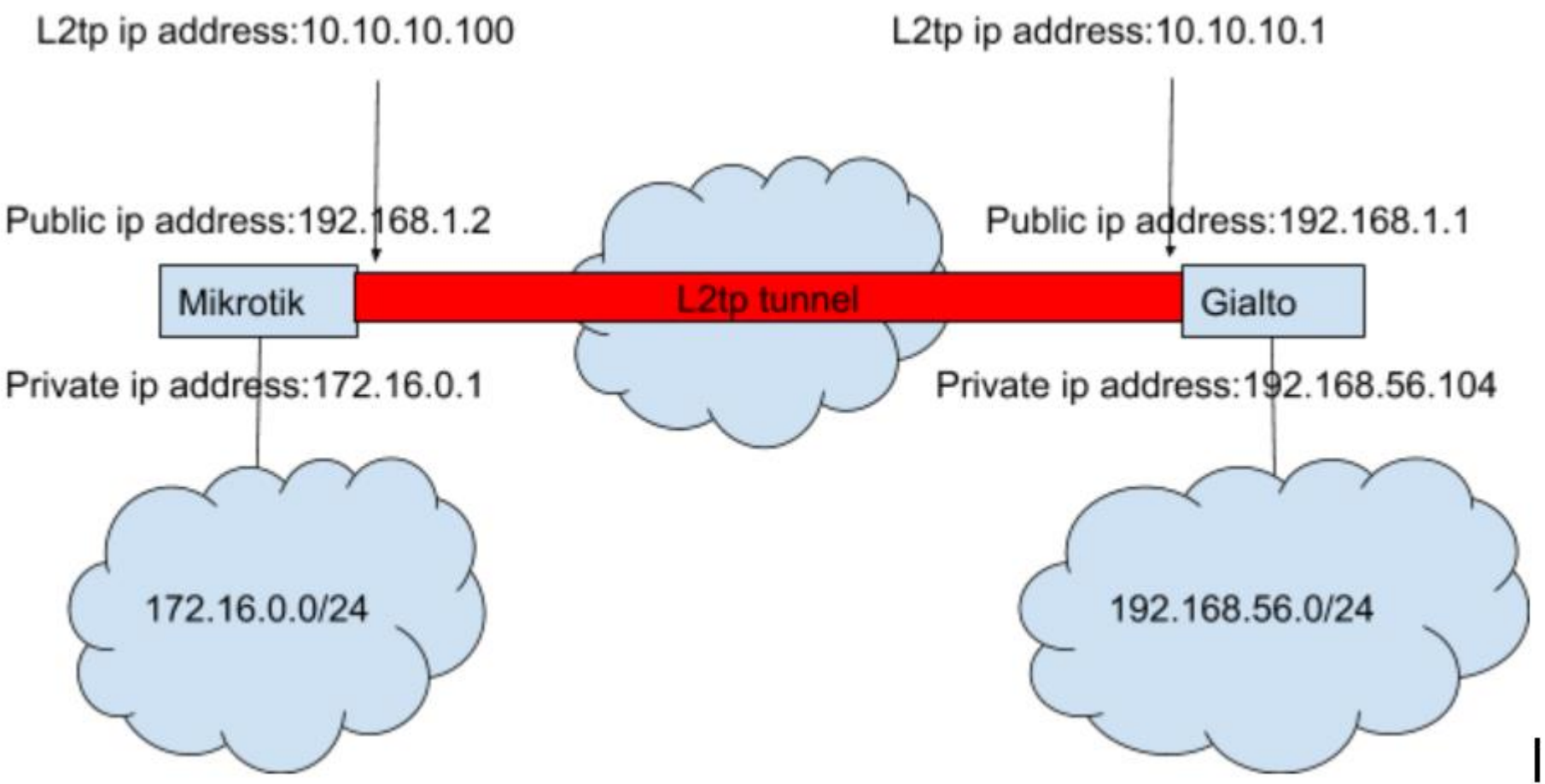
- Layer 2 **Tunneling** Protocol (**L2TP**) can be used to connect both site of the network



Solution

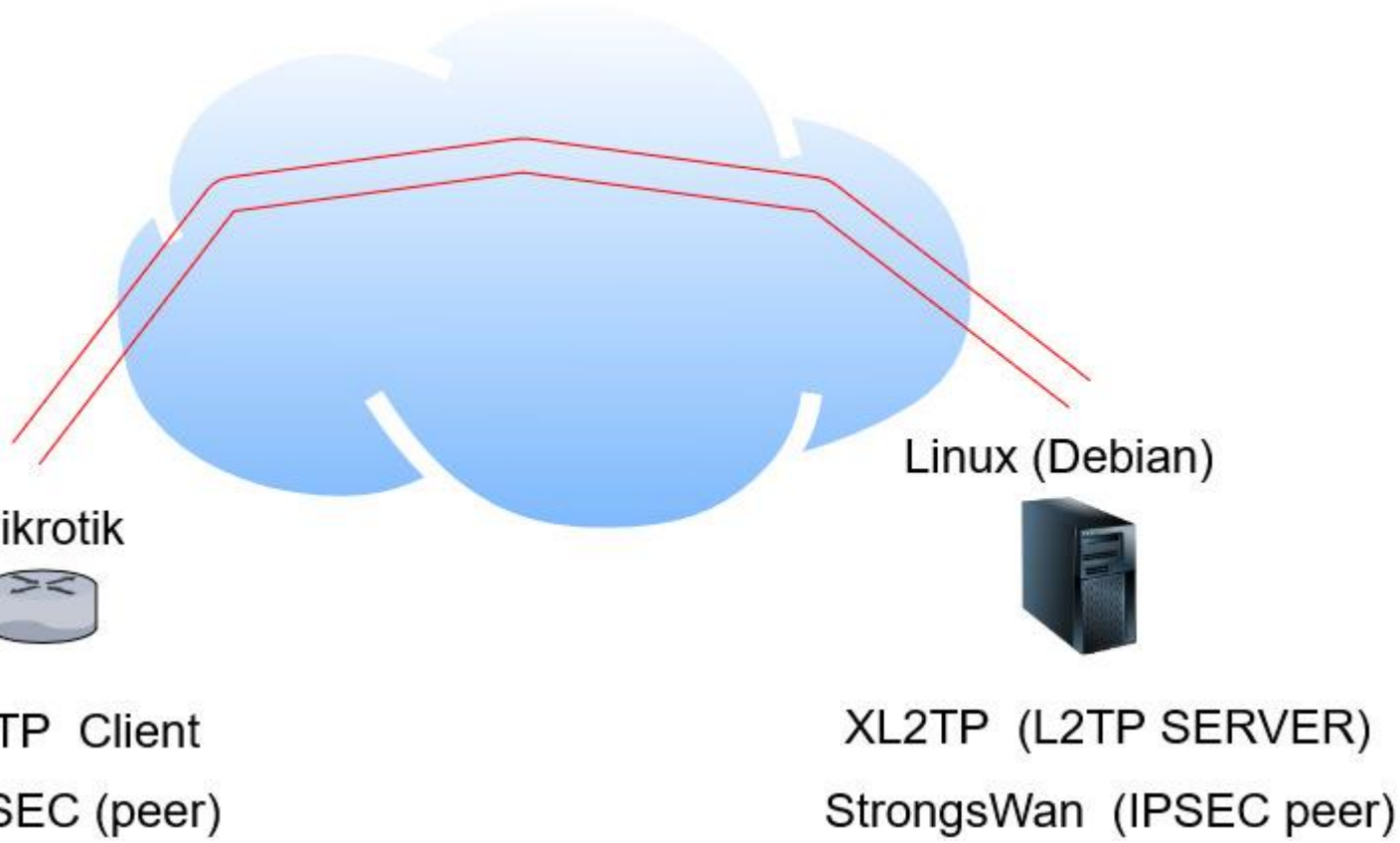
- L2TP Concerns:
  - L2TP is a client server tunnel
    - Regarding to the topology, for establishing L2TP tunnel, we should run L2TP server on the Linux (Debian) and L2TP client on our Mikrotik
  - L2TP does not provide any encryption or confidentiality by itself.
    - IPSEC can solve the problem

Solution


L2tp ip address:10.10.10.100
L2tp ip address:10.10.10.1
Public ip address:192.168.1.2
Public ip address:192.168.1.1
Mikrotik
L2tp tunnel
Gialto
Private ip address:172.16.0.1
Private ip address:192.168.56.104
172.16.0.0/24
192.168.56.0/24

Configurations

Services on both sides



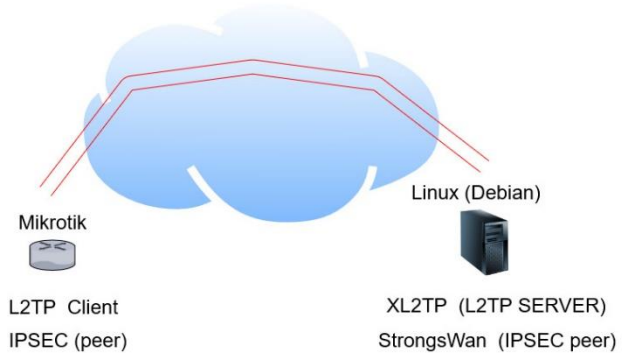
Server Configuration (XL2TP)

Installation: sudo apt-get install xl2tpd

Change the configuration file /etc/xl2tpd/xl2tpd.conf as follows:

```
[global]
ipsec saref = no
debug tunnel = no
debug avp = no
debug network = no
debug state = no
access control = no
rand source = dev
port = 1701
auth file = /etc/ppp/chap-secrets
```

```
[lns default]
ip range = 10.10.10.110-10.10.10.150
local ip = 10.10.10.1
require authentication = yes
name = l2tp
pass peer = yes
ppp debug = no
length bit = yes
refuse pap = yes
refuse chap = yes
pppoptfile = /etc/ppp/options.xl2tpd
```



Server Configuration (XL2TP)

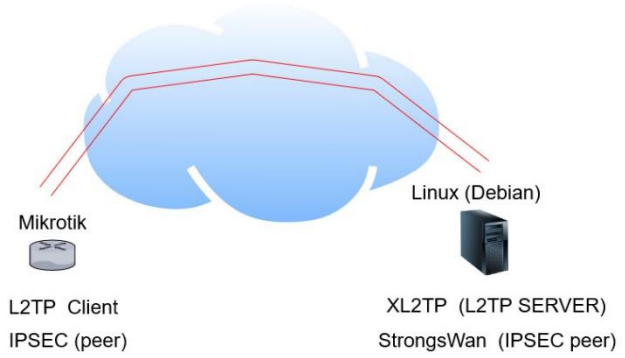
Adding Users and secret for L2TP clients

You have to edit /etc/ppp/chap-secrets file like the following:

```
# Secrets for authentication using CHAP
# client      server   secret          IP addresses
   ali            *      123           10.10.10.100
```

Above file shows this credential:
username: ali
Password: 123
Ip address:10.10.10.100

Run the below command to start XL2TP:
XL2TP or XL2TP –D (to start it in debug mode)

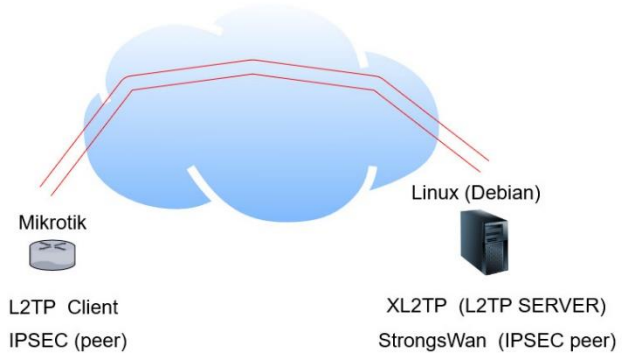


Server Configuration (IPSEC)

Installation: sudo apt-get install strongswan

Edit the file /etc/ipsec.conf:

```
config setup
conn vpnserver
        type=tunnel
        authby=secret
        rekey=no
        keyingtries=3
        left=10.10.10.1
        leftsubnet=192.168.56.0/24
        rightsubnet=172.16.0.0/24
        leftid=10.10.10.1
        right=10.10.10.100
        auto=add
        esp=aes128-sha1-modp1536
        aggressive = no
        ike=aes128-sha1-modp1536
        ikelifetime = 3h
```



Server Configuration (IPSEC)

IPSec Password:

Add the following line to this file **/etc/ipsec.secrets :**

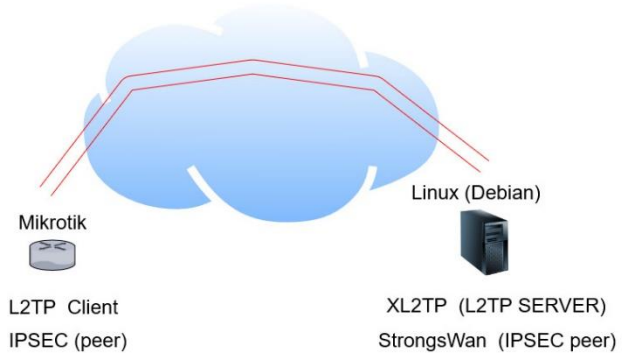
%any %any : PSK "123"

Run this command to start ipsec:

ipsec start

To check if everything is going well, check the status by:

ipsec statusall



Some Extra work

This Linux command shows the policies and states of IPsec tunnel.

```
ip xfrm state

ip xfrm policy
```

Firewall configuration:

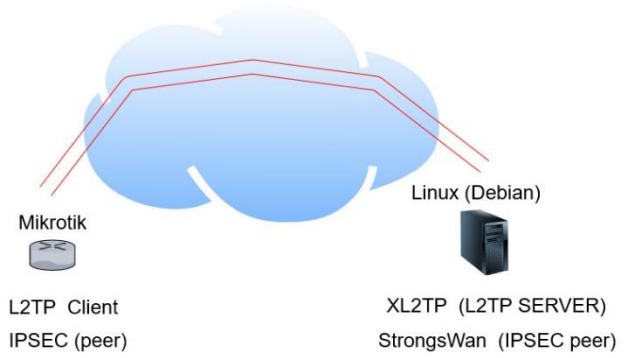
You need to accept packet from your **l2tp** clients. (L2tp is port 1701)

You can see if you receive something in L2tp interface

```
tcpdump -i eth0 'port 1701'
tcpdump -i ppp0
```

How to deny all l2tp without IPSEC encryption from Mikrotik client?

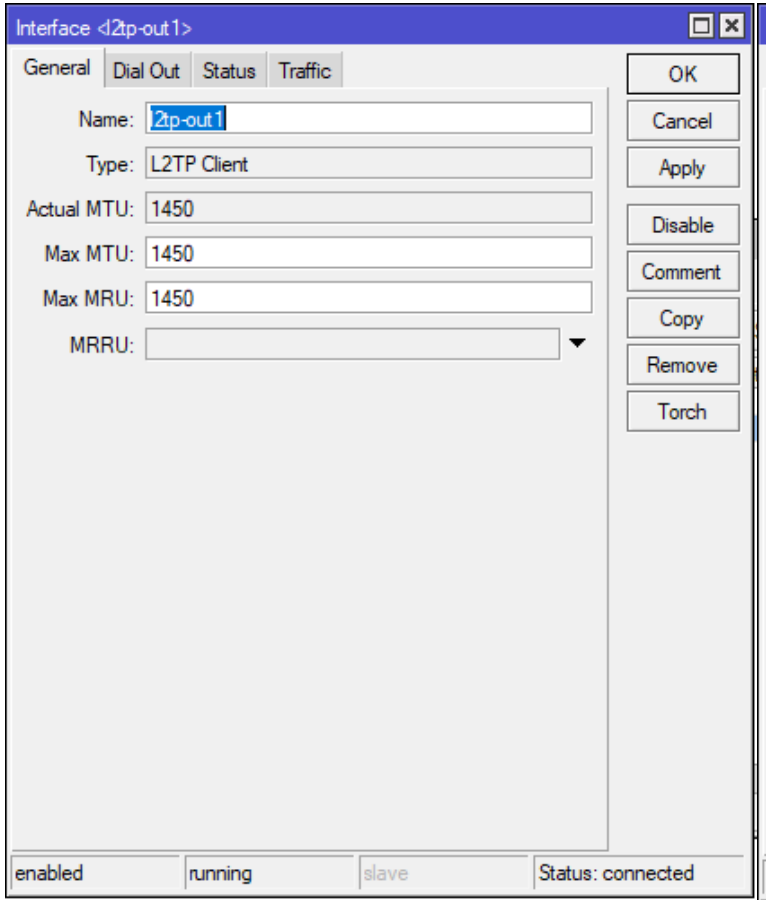
```
iptables -A INPUT -p udp --dport 1701 -m policy --dir in --pol ipsec -j ACCEPT
iptables -A INPUT -p udp --dport 1701 -j DROP
```

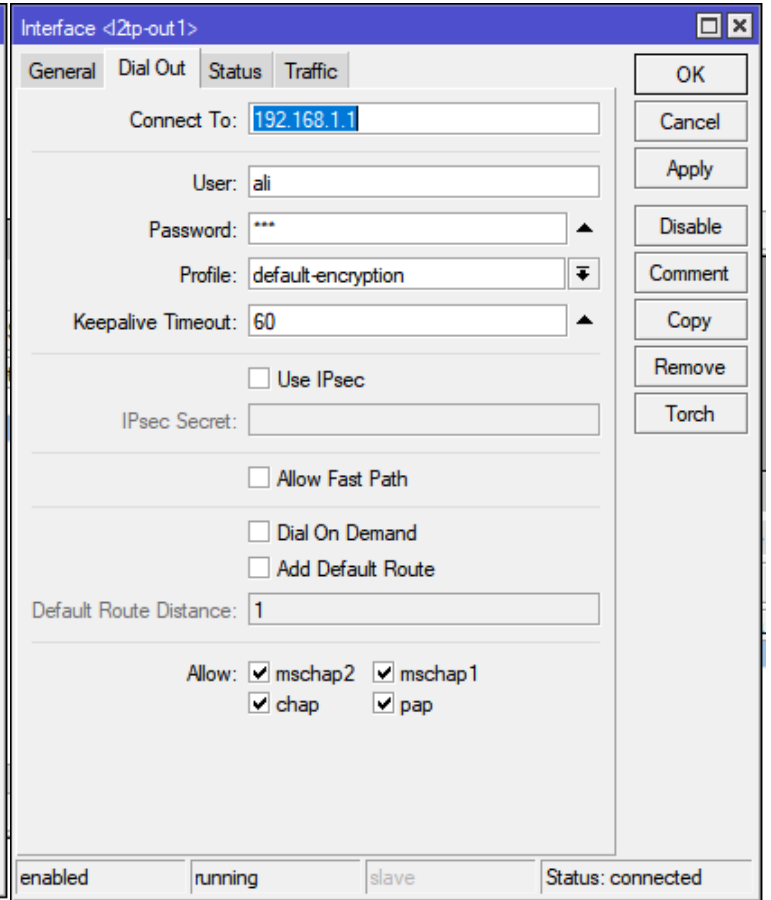


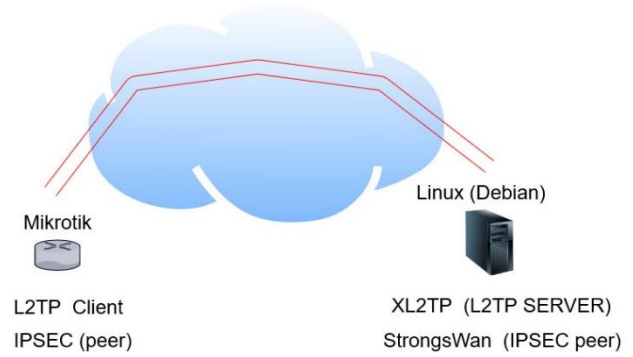
Mikrotik Configuration (L2TP)

Add a l2tpclient in ppp section with the following configuration:

(Don’t forget that user and password should be the same as those in /etc/ppp/chap-secrets)

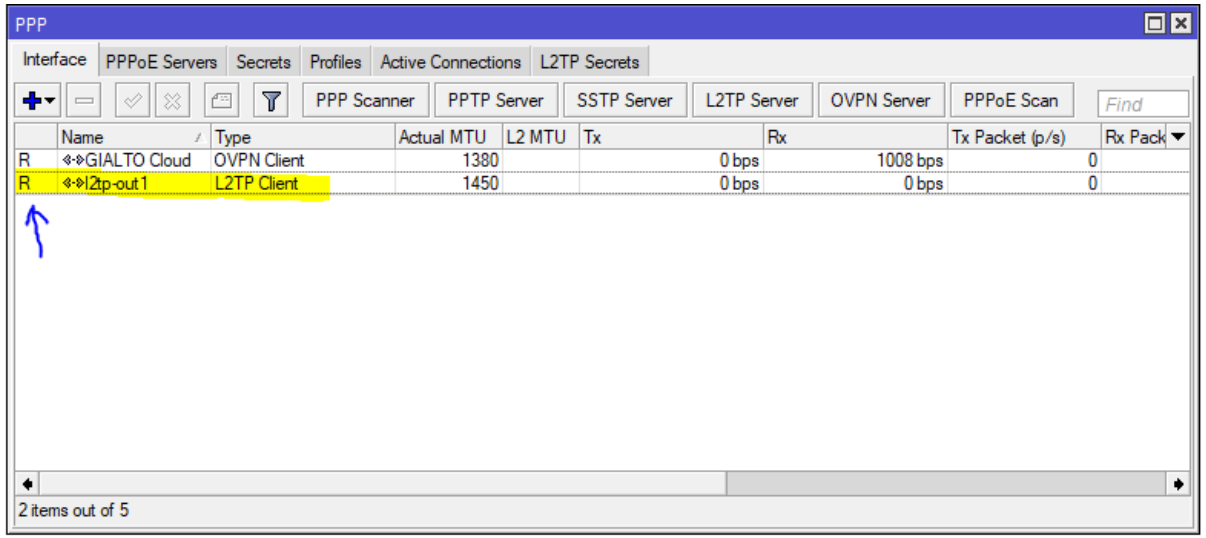


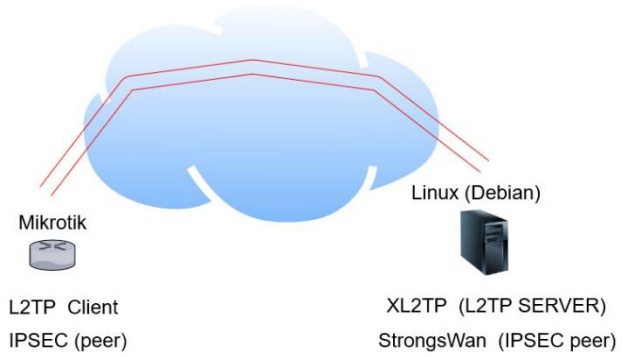




Mikrotik Configuration (L2TP)

Check if the connection is established or not
(you should see R in front of the connection in ppp - > interface section)

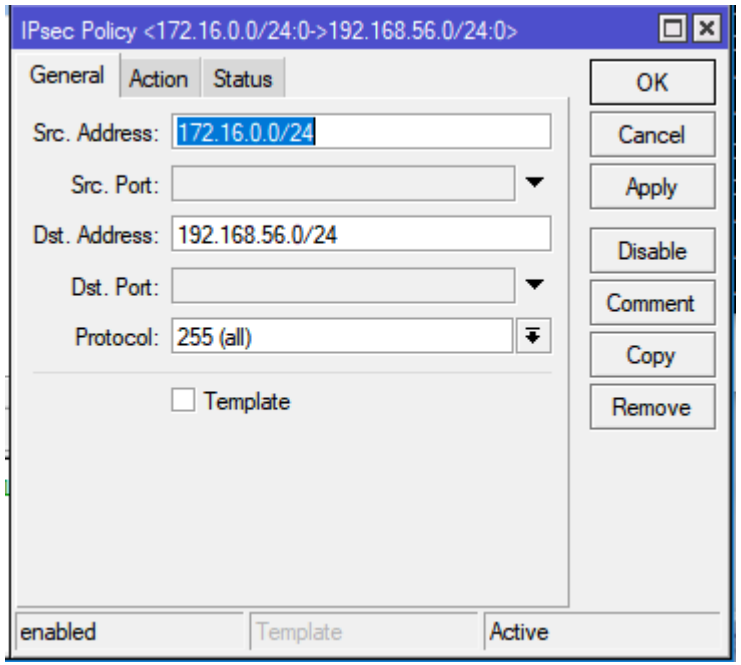


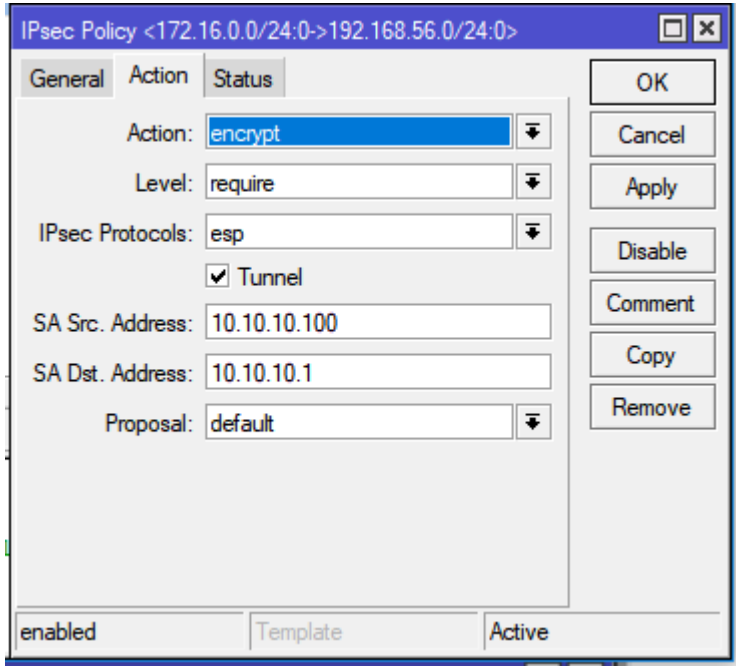


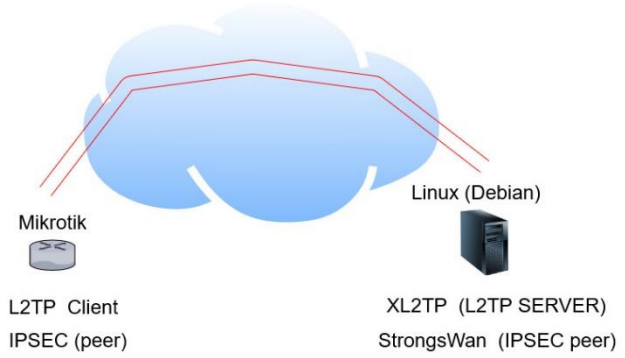
Mikrotik Configuration (IPSEC)

Now, define a new IPSEC manually and set the following configurations:

IPSEC => Policy => Add

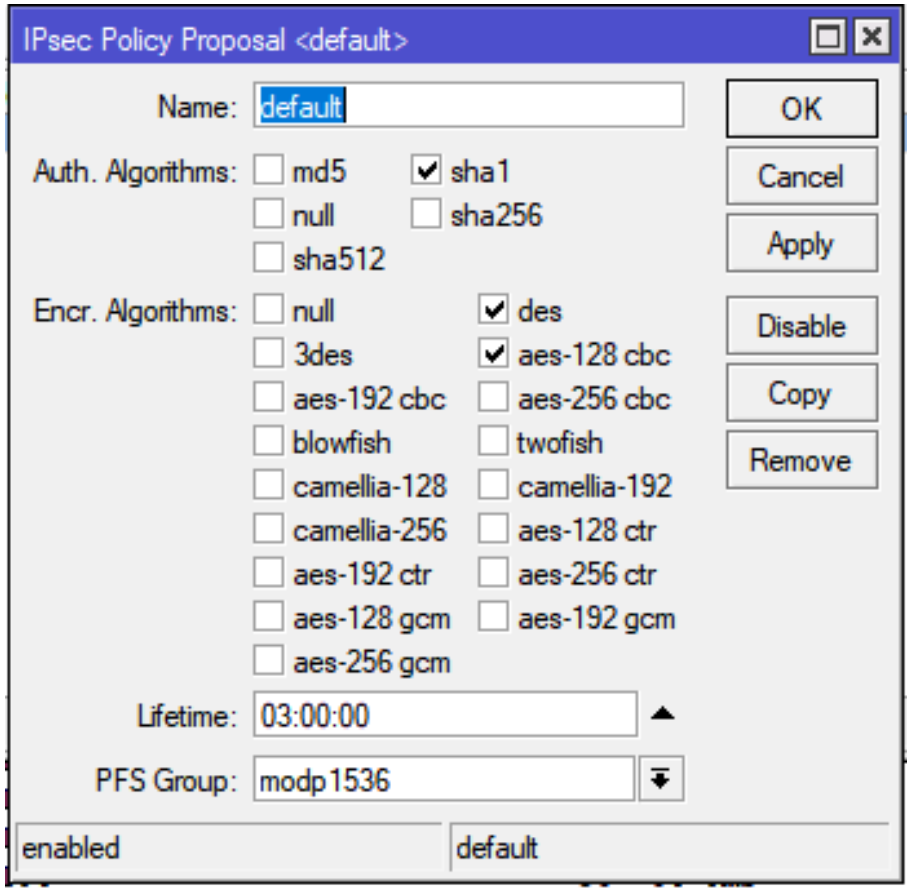




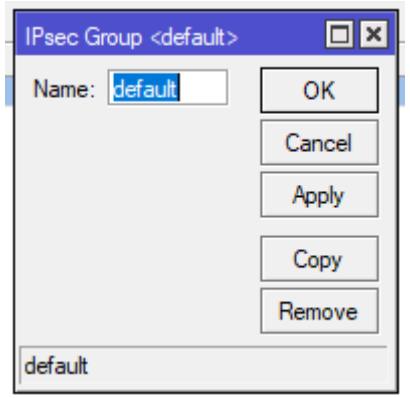


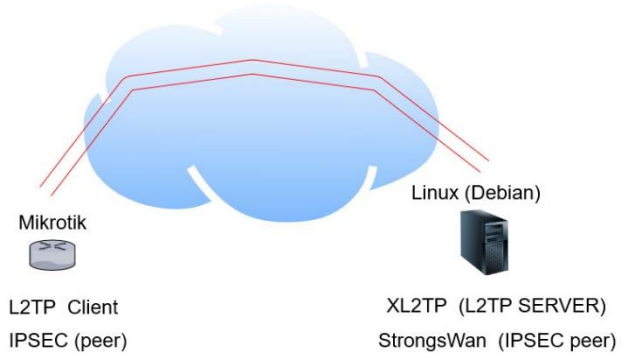
Mikrotik Configuration (IPSEC)

Then in the proposal tab, choose the following:



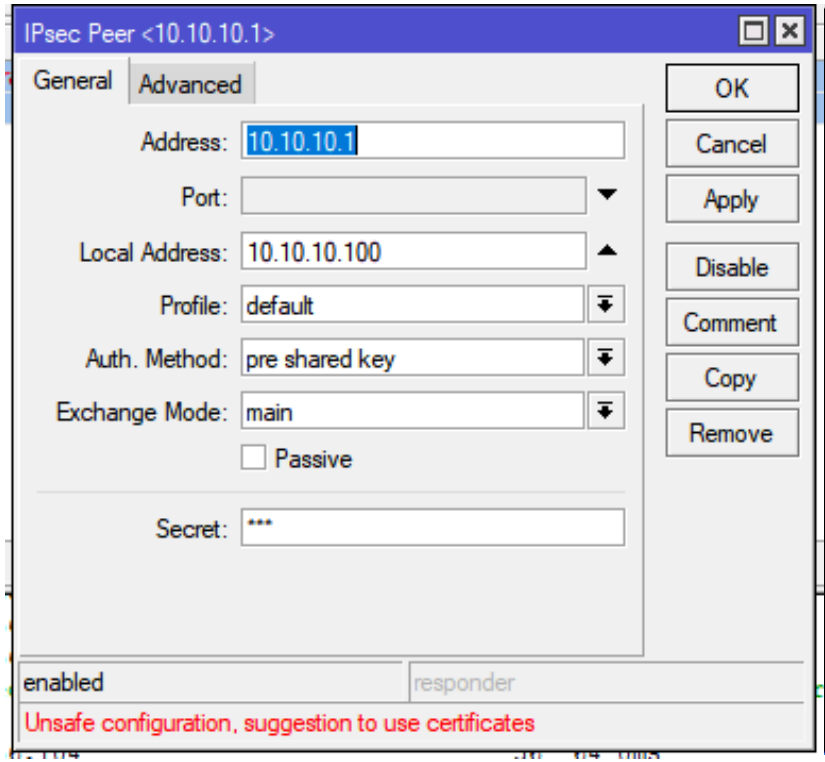
Leave IPSEC group unchanged as:

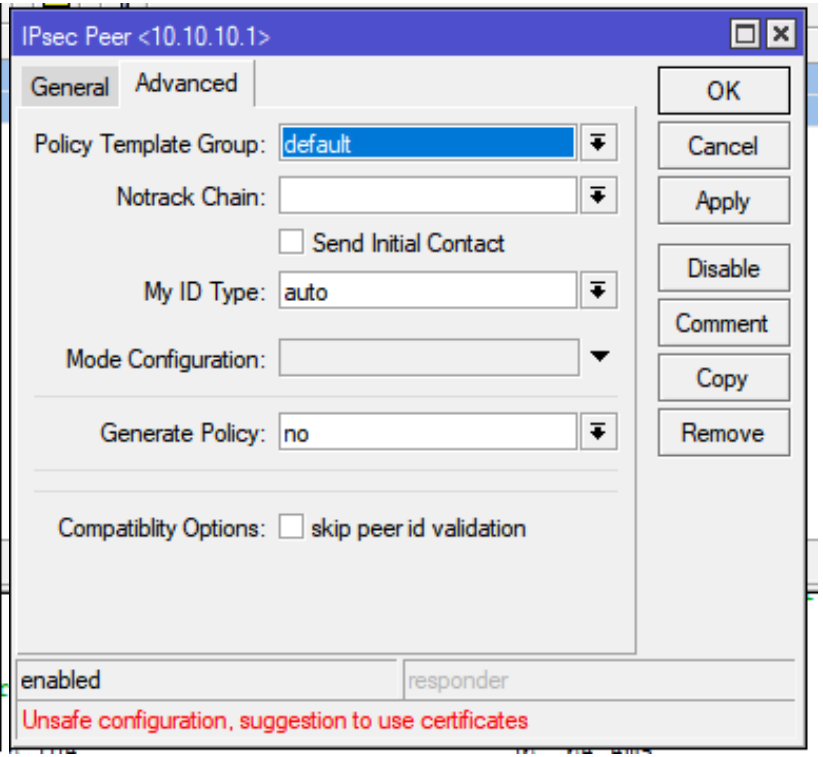


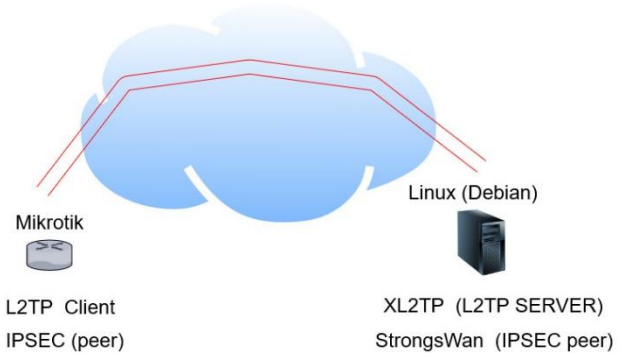


Mikrotik Configuration (IPSEC)

Then add a peer (IPSEC=> peer) like this:

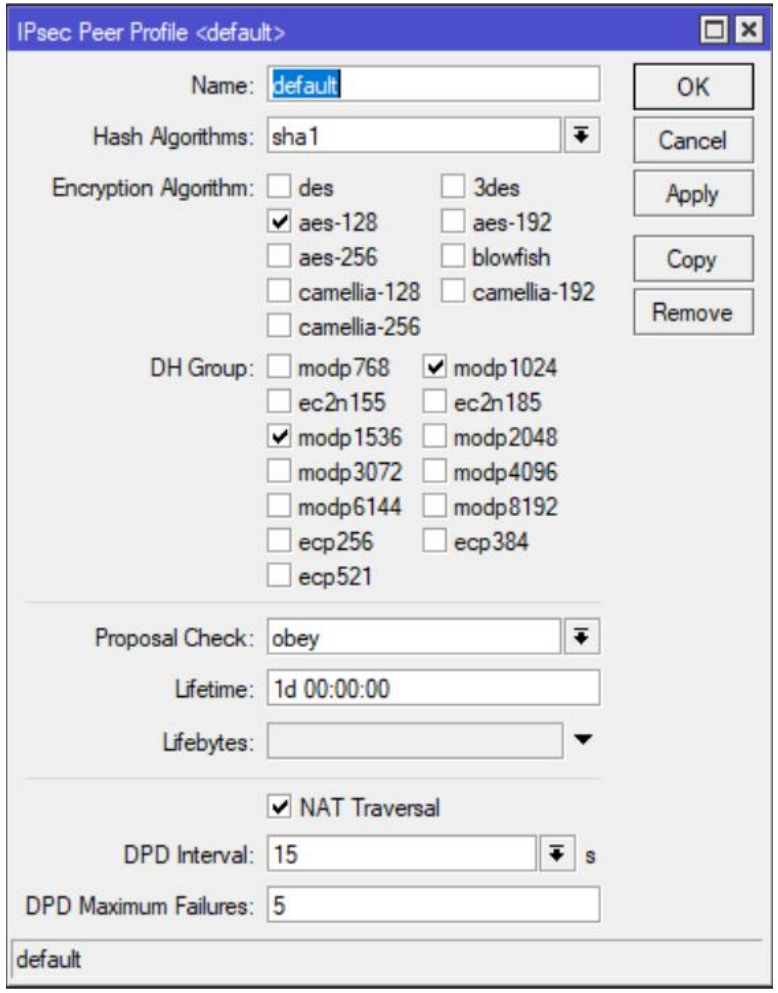


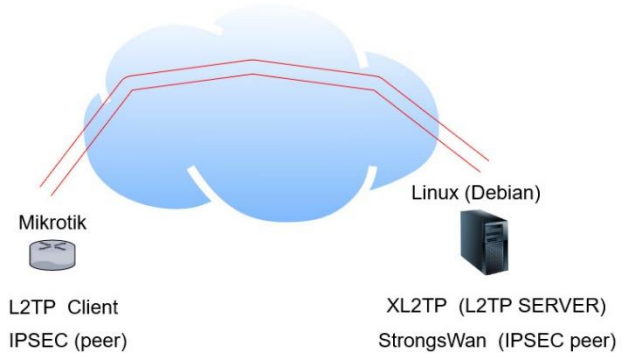




Mikrotik Configuration (IPSEC)

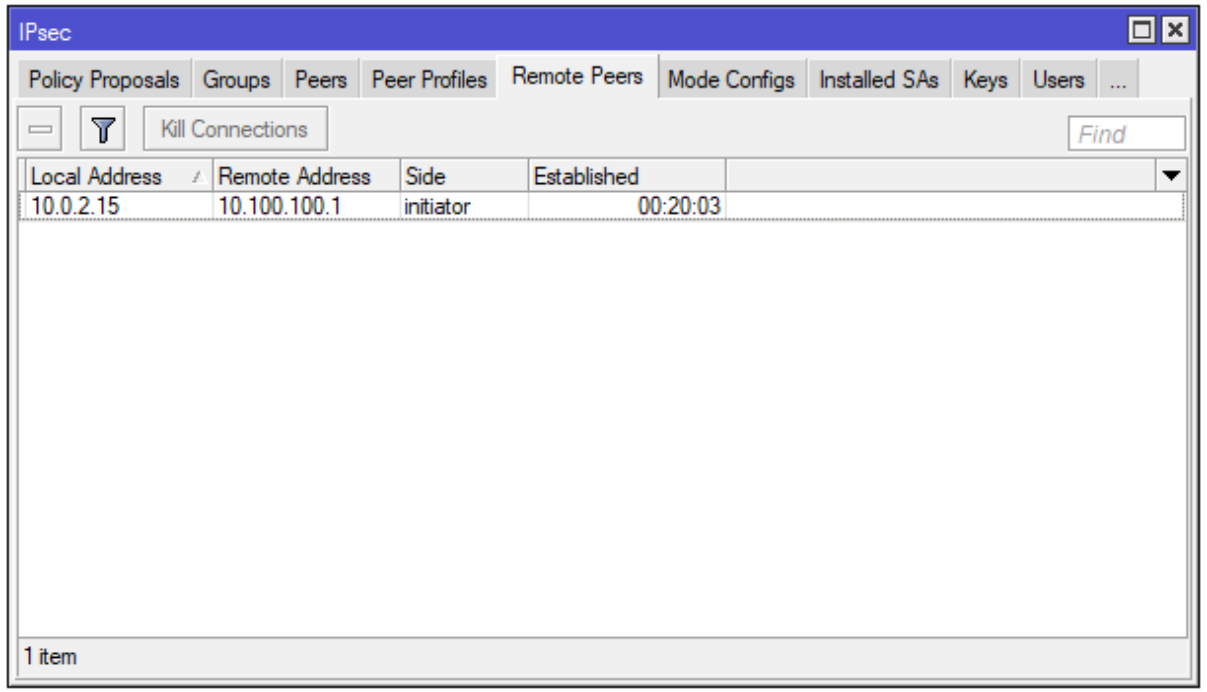
Define peer profile as below:

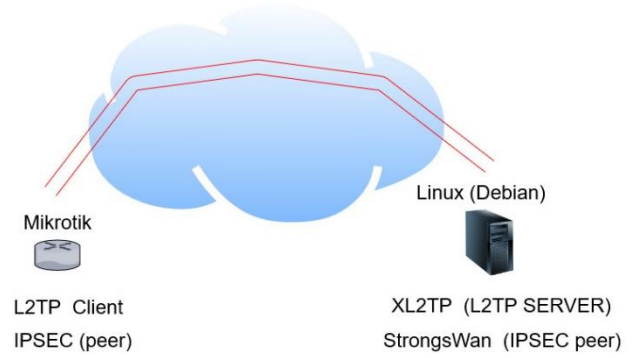




Mikrotik Configuration (IPSEC)

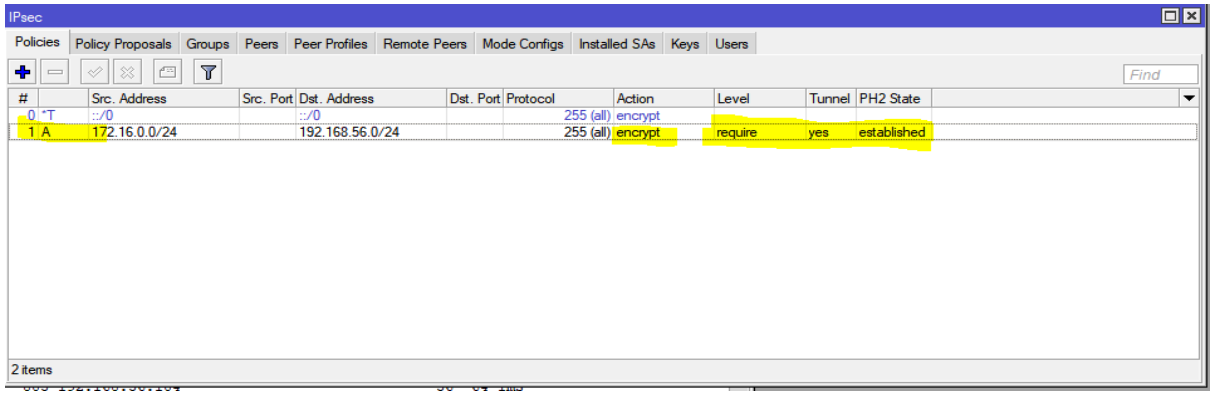
If IPSEC tunnel is established, you should see the following in IP->IPSEC_Remote Peers



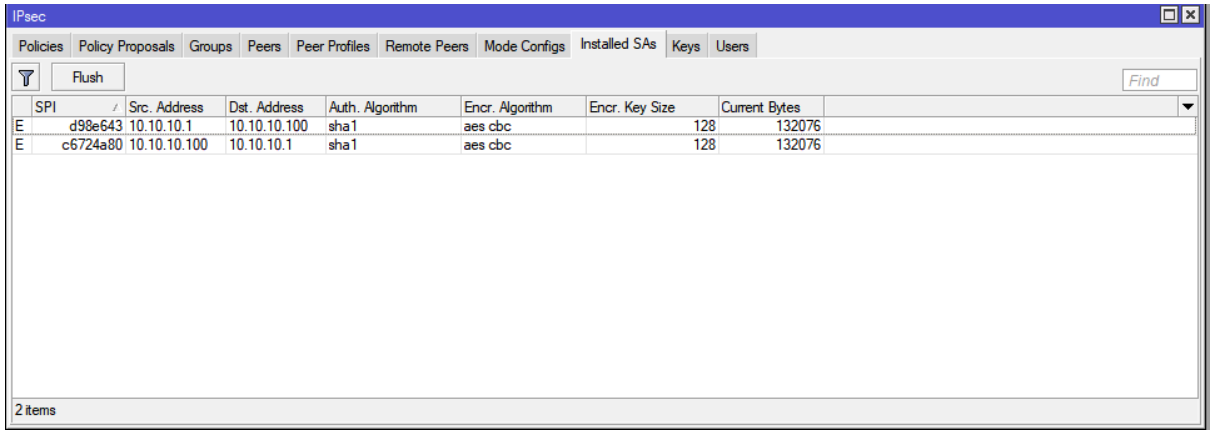


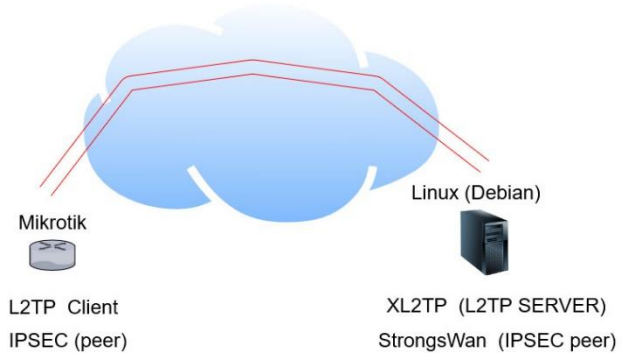
Mikrotik Configuration (IPSEC)

And the following in IPSEC=>Policy:



Also you should see in IPSEC=>INSTALLED SAs:





Questions?

End...