LAB: L2TP/IPsec vpn (strongswan)

Lab Environment:

The workshop wifi:

SSID: workshop

PASS: iij/2497

Hosts - Virtual machines (Ubuntu16.04LTS/LXC):

Hostname: nsXX.local

IPv6: fd00:2497:1::X

IPv4: 10.0.0.X

Note: XX is your group id

For group1, it's ns01.local, fd00:2497:1::1 and 10.0.0.1

For group10, its' ns10.local, fd00:2497:1::10 and 10.0.0.10

username: workshop

password: iij/2497

Install and configure strongswan:

ssh to your host, and install strongswan

$ sudo apt install strongswan xl2tpd

Note: sudo password is iij/2497

Edit '/etc/ipsec.conf' to set ipsec options.

$ sudo vi /etc/ipsec.conf

The contents should be as follows:

```
config setup
    nat_traversal=yes
conn %default
    auto=add
conn L2TP-NAT
    auto=add
    type=transport
    leftauth=psk
    rightauth=psk
```

Put your pre-shared key in /etc/ipsec.secrets file

```
$ sudo vi   /etc/ipsec.secrets
```

The file should be like

```
: PSK "secret"
```

Note: You can configure 'secret' as you like

Edit /etc/xl2tpd/xl2tpd.conf as follows

```
$ sudo vi   /etc/xl2tpd/xl2tpd.conf
```

The contents should be:

```
[lns default]
  ip range = 10.10.0.1-10.10.0.10
  local ip = <IP>
  length bit = yes
  refuse pap = yes
  refuse chap = yes
  require authentication = yes
  name = l2tp
  pppoptfile = /etc/ppp/options.xl2tpd
```

Note: IP is IPv4 address of your nsXX.host

Create /etc/ppp/options.xl2tpd as follows

$ sudo vi /etc/ppp/options.xl2tpd

The contents should be

```
name l2tp
refuse-pap
refuse-chap
refuse-mschap
require-mschap-v2
nodefaultroute
lock
nobsdcomp
mtu 1280
mru 1280
```

Now we create users for the VPN server. Edit /etc/ppp/chap-secrets

$ sudo vi /etc/ppp/chap-secrets

Some thinig like:

```
# client    server    secret        IP addresses
"user01"    *    "password"    *
```

Make your host as a NAT router

$ sudo sysctl -w net.ipv4.ip_forward=1

$ sudo iptables -t nat -A POSTROUTING -j SNAT --to-source <IP> -o eth0

Note: IP is the IPv4 address of your nsXX.host

Restart strongswan and xl2tpd

$ sudo systemctl restart strongswan

$ sudo systemctl restart xl2tpd

Configure clients

Configure new VPN profile. That should be L2TP/IPsec with pre-shared key, using username and password authentication