Introduction
Layer 2 Tunnel Protocol (L2TP) over IPsec is a very common way of configuring remote access via VPN. This article shows an example of the configuration process in VyOS.

Configuration
IPsec
Assuming an external interface of eth0:

```
set vpn ipsec ipsec-interfaces eth0
set vpn ipsec nat-traversal enable
set vpn ipsec nat-networks allowed-network 0.0.0.0/0
```
L2TP
Assuming a public IP of 203.0.113.2 and an address pool for VPN clients of 192.168.255.2 - 192.168.255.254:

```
set vpn l2tp remote-access outside-address 203.0.113.2
set vpn l2tp remote-access client-ip-pool start 192.168.255.2
set vpn l2tp remote-access client-ip-pool stop 192.168.255.254
```

Authentication may be configured either using a pre-shared-secret (a text password given to all clients) or by using X.509 certificates.

Client authentication for L2TP may be configured either using a username/password combination, or by using a RADIUS server. For simplicity, we will use a pre-shared-secret and basic username/password authentication; not-so-secret for the secret, alice for the user, and notsecure for the user's password:

```
set vpn l2tp remote-access ipsec-settings authentication mode pre-shared-secret
set vpn l2tp remote-access ipsec-settings authentication pre-shared-secret "not-so-secret"
set vpn l2tp remote-access authentication mode local
set vpn l2tp remote-access authentication local-users username alice password notsecure
```

Firewall
Additional configuration may be needed if you have a firewall policy on the external interface.

The following ports will need to be open:

- UDP port 500 for IKE
- IP protocol number 50 (ESP)
- UDP port 1701 for IPsec
- UDP port 4500 for ESP NAT traversal

When NAT is detected by the client's VPN software, ESP is encapsulated in UDP for NAT traversal, hence UDP port 4500.

Allow clients to reach external hosts
If you want the VPN to be used for external access (that is, allow clients connected to reach external hosts from the VPN server), SNAT will need to be properly configured:

```
set nat source rule 110 outbound-interface eth0
set nat source rule 110 source address 192.168.255.0/24
set nat source rule 110 translation address masquerade
```
Additionally, clients will need their DNS servers configured (this example uses Google's public DNS servers; replace with your organization's if desired):

set vpn l2tp remote-access dns-servers server-1 8.8.8.8
set vpn l2tp remote-access dns-servers server-2 8.8.4.4

Additional Configuration Options
A full list of configuration options for L2TP can be seen by hitting the tab key after typing set vpn l2tp remote-access:

vyos@vyos# set vpn l2tp remote-access
Possible completions:
  > authentication  
          Authentication for remote access L2TP VPN
  > client-ip-pool 
          Pool of IP address to be assigned to remote clients
          description Description for L2TP remote-access settings
          dhcp-interface  
          DHCP interface to listen on
  > dns-servers  Domain Name Service (DNS) server
  > ipsec-settings  
          Internet Protocol Security (IPsec) for remote access

L2TP VPN
  mtu  Maximum Transmission Unit (MTU)
  outside-address  
          Outside IP address to which VPN clients will connect
  outside-nexthop  
          Nexthop IP address for reaching the VPN clients
  > wins-servers Windows Internet Name Service (WINS) server settings

And for set vpn ipsec:

vyos@vyos# set vpn ipsec
Possible completions:
  auto-update  Set auto-update interval for IPsec daemon.
  disable-uniqreqids  
          Option to disable requirement for unique IDs in the Security Database
  +> esp-group  Name of Encapsulating Security Payload (ESP) group
  +> ike-group  Name of Internet Key Exchange (IKE) group
  > ipsec-interfaces  
          Interface to use for VPN [REQUIRED]
Tweak these options and their sub-options as needed/desired.

**Viewing VPN Status**
Currently connected clients may be viewed through the following operational mode command:

```bash
vyos@vyos:~$ show vpn remote-access
Active remote access VPN sessions:

<table>
<thead>
<tr>
<th>User</th>
<th>Proto</th>
<th>Iface</th>
<th>Tunnel IP</th>
<th>TX byte</th>
<th>RX byte</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>alice</td>
<td>L2TP</td>
<td>l2tp0</td>
<td>192.168.255.2</td>
<td>3.2K</td>
<td>8.0K</td>
<td>00h06m13s</td>
</tr>
</tbody>
</table>
```