|  |
| --- |
| **L2TP**[](https://docs.vyos.io/en/latest/configuration/vpn/l2tp.html#l2tp) |

|  |
| --- |
| VyOS utilizes accel-ppp to provide L2TP server functionality. It can be used with local |

|  |
| --- |
| authentication or a connected RADIUS server. |

**L2TP over IPsec**[](https://docs.vyos.io/en/latest/configuration/vpn/l2tp.html#l2tp-over-ipsec)

Example for configuring a simple L2TP over IPsec VPN for remote access (works with native Windows and Mac VPN clients):

|  |
| --- |
| set vpn ipsec interface eth0 |

|  |
| --- |
| set vpn l2tp remote-access outside-address 192.0.2.2  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  set vpn l2tp remote-access ipsec-settings authentication mode pre-shared-secret set vpn l2tp remote-access ipsec-settings authentication pre-shared-secret <secret> set vpn l2tp remote-access authentication mode local  set vpn l2tp remote-access authentication local-users username test password 'test' |

In the above example, an external IP of 192.0.2.2 is assumed.

If a local firewall policy is in place on your external interface you will need to allow the ports below:

 UDP port 500 (IKE)

 IP protocol number 50 (ESP)

 UDP port 1701 for IPsec   
As well as the below to allow NAT-traversal (when NAT is detected by the VPN client, ESP is encapsulated in UDP for NAT-traversal):

 UDP port 4500 (NAT-T)   
Example:

|  |
| --- |
| set firewall name OUTSIDE-LOCAL rule 40 action 'accept'  set firewall name OUTSIDE-LOCAL rule 40 protocol 'esp'  set firewall name OUTSIDE-LOCAL rule 41 action 'accept'  set firewall name OUTSIDE-LOCAL rule 41 destination port '500' set firewall name OUTSIDE-LOCAL rule 41 protocol 'udp'  set firewall name OUTSIDE-LOCAL rule 42 action 'accept'  set firewall name OUTSIDE-LOCAL rule 42 destination port '4500' set firewall name OUTSIDE-LOCAL rule 42 protocol 'udp'  set firewall name OUTSIDE-LOCAL rule 43 action 'accept'  set firewall name OUTSIDE-LOCAL rule 43 destination port '1701' |

|  |
| --- |
| set firewall name OUTSIDE-LOCAL rule 43 ipsec 'match-ipsec' set firewall name OUTSIDE-LOCAL rule 43 protocol 'udp' |

To allow VPN-clients access via your external address, a NAT rule is required:

|  |
| --- |
| 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 |

VPN-clients will request configuration parameters, optionally you can DNS parameter to the client.

|  |
| --- |
| set vpn l2tp remote-access name-server '198.51.100.8' set vpn l2tp remote-access name-server '198.51.100.4' |

Established sessions can be viewed using the **show l2tp-server sessions** operational command

|  |
| --- |
| vyos@vyos:~$ show l2tp-server sessions  ifname | username | ip | ip6 | ip6-dp | calling-sid | rate-limit | state | uptime | rx-bytes | tx-bytes --------+----------+---------------+-----+--------+-------------+------------+--------+----------+----------+---------- l2tp0 | test | 192.168.255.3 | | | 192.168.0.36 | | active | 02:01:47 | 7.7 KiB | 1.2 KiB |

**LNS (L2TP Network Server)**[](https://docs.vyos.io/en/latest/configuration/vpn/l2tp.html#lns-l2tp-network-server)

LNS are often used to connect to a LAC (L2TP Access Concentrator).

Below is an example to configure a LNS:

|  |
| --- |
| set vpn l2tp remote-access outside-address 192.0.2.2  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  set vpn l2tp remote-access lns shared-secret 'secret'  set vpn l2tp remote-access ccp-disable  set vpn l2tp remote-access authentication mode local  set vpn l2tp remote-access authentication local-users username test password 'test' |

The example above uses 192.0.2.2 as external IP address. A LAC normally requires an

|  |  |
| --- | --- |
| authentication password, which is set in the example configuration to lns shared-secret 'secret' .   |  | | --- | |  | |

This setup requires the Compression Control Protocol (CCP) being disabled, the

|  |  |
| --- | --- |
| command set vpn l2tp remote-access ccp-disable accomplishes that.   |  | | --- | |  | |

**Bandwidth Shaping**[](https://docs.vyos.io/en/latest/configuration/vpn/l2tp.html#bandwidth-shaping)

Bandwidth rate limits can be set for local users or via RADIUS based attributes. **Bandwidth Shaping for local users**[](https://docs.vyos.io/en/latest/configuration/vpn/l2tp.html#bandwidth-shaping-for-local-users)

The rate-limit is set in kbit/sec.

|  |
| --- |
| set vpn l2tp remote-access outside-address 192.0.2.2  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  set vpn l2tp remote-access authentication mode local  set vpn l2tp remote-access authentication local-users username test password test  set vpn l2tp remote-access authentication local-users username test rate-limit download 20480 set vpn l2tp remote-access authentication local-users username test rate-limit upload 10240 |

|  |
| --- |
| vyos@vyos:~$ show l2tp-server sessions  ifname | username | ip | ip6 | ip6-dp | calling-sid | rate-limit | state | uptime | rx-bytes | tx-bytes --------+----------+---------------+-----+--------+-------------+------------+--------+----------+----------+---------- l2tp0 | test | 192.168.255.3 | | | 192.168.0.36 | | active | 02:01:47 | 7.7 KiB | 1.2 KiB |

**RADIUS authentication**[](https://docs.vyos.io/en/latest/configuration/vpn/l2tp.html#radius-authentication)

To enable RADIUS based authentication, the authentication mode needs to be changed within the configuration. Previous settings like the local users, still exists within the configuration, however they are not used if the mode has been changed from local to radius. Once changed back to local, it will use all local accounts again.

|  |
| --- |
| set vpn l2tp remote-access authentication mode <local|radius> |

Since the RADIUS server would be a single point of failure, multiple RADIUS servers can be setup and will be used subsequentially.

|  |
| --- |
| set vpn l2tp remote-access authentication radius server 10.0.0.1 key 'foo' set vpn l2tp remote-access authentication radius server 10.0.0.2 key 'foo' |

|  |
| --- |
| **Note** |

|  |
| --- |
| Some [RADIUS](https://en.wikipedia.org/wiki/RADIUS) severs use an access control list which allows or denies queries, make sure to |

|  |
| --- |
| add your VyOS router to the allowed client list. |

**RADIUS source address**[](https://docs.vyos.io/en/latest/configuration/vpn/l2tp.html#radius-source-address)

If you are using OSPF as IGP, always the closest interface connected to the RADIUS server is used. With VyOS 1.2 you can bind all outgoing RADIUS requests to a single source IP e.g. the loopback interface.

|  |
| --- |
| set vpn l2tp remote-access authentication radius source-address 10.0.0.3 |

Above command will use *10.0.0.3* as source IPv4 address for all RADIUS queries on this NAS.

|  |
| --- |
| **Note** |

|  |  |
| --- | --- |
| The source-address must be configured on one of VyOS interface. Best practice would be a   |  | | --- | |  | |

|  |
| --- |
| loopback or dummy interface. |

**RADIUS bandwidth shaping attribute**[](https://docs.vyos.io/en/latest/configuration/vpn/l2tp.html#radius-bandwidth-shaping-attribute)  
To enable bandwidth shaping via RADIUS, the option rate-limit needs to be enabled.

|  |
| --- |
| set vpn l2tp remote-access authentication radius rate-limit enable |
| The default RADIUS attribute for rate limiting is Filter-Id , but you may also redefine it.   |  | | --- | |  | |

|  |
| --- |
| set vpn l2tp remote-access authentication radius rate-limit attribute Download-Speed |

|  |
| --- |
| **Note** |

|  |
| --- |
| If you set a custom RADIUS attribute you must define it on both dictionaries at RADIUS server |

|  |  |
| --- | --- |
| and client, which is the vyos router in our example.  The RADIUS dictionaries in VyOS are located at /usr/share/accel-ppp/radius/   |  | | --- | |  | |

**RADIUS advanced features**[](https://docs.vyos.io/en/latest/configuration/vpn/l2tp.html#radius-advanced-features)  
Received RADIUS attributes have a higher priority than parameters defined within the CLI

configuration, refer to the explanation below.

**Allocation clients ip addresses by RADIUS**[](https://docs.vyos.io/en/latest/configuration/vpn/l2tp.html#allocation-clients-ip-addresses-by-radius)

|  |  |
| --- | --- |
| If the RADIUS server sends the attribute Framed-IP-Address then this IP address will be   |  | | --- | |  | |

allocated to the client and the option ip-pool within the CLI config is being ignored.

**Renaming clients interfaces by RADIUS**[](https://docs.vyos.io/en/latest/configuration/vpn/l2tp.html#renaming-clients-interfaces-by-radius)

|  |  |
| --- | --- |
| If the RADIUS server uses the attribute NAS-Port-Id , ppp tunnels will be renamed.   |  | | --- | |  | |

|  |
| --- |
| **Note** |
| The value of the attribute NAS-Port-Id must be less than 16 characters, otherwise the interface   |  | | --- | |  | |

|  |
| --- |
| won’t be renamed. |