AWS L2TP/IPSec

Dmitriy Eshenko - 2020-09-07 - 0 Comments - in FAQ

All instances on AWS are located behind 1-to-1 NAT and this affectly IPSec negatively.
In this case we can use a simple solution with a dummy interface and DNAT rules on VyOS routers.

Set public IP addresses on the dummy interface:

```
set interfaces dummy dum0 address 'x.x.x.x/32'
```

Create DNAT rules:

```
set nat destination rule 20 inbound-interface 'eth0'
set nat destination rule 20 translation address 'x.x.x.x'
```

Configure L2TP and IPSec:

```
set vpn ipsec nat-traversal enable
set vpn ipsec nat-networks allowed-network 0.0.0.0/0
set vpn ipsec ipsec-interfaces interface 'dum0'
set vpn l2tp remote-access outside-address 'x.x.x.x'
set vpn l2tp remote-access client-ip-pool start 192.168.255.1
set vpn l2tp remote-access client-ip-pool stop 192.168.255.254
set vpn l2tp remote-access dns-servers server-1 '1.1.1.1'
set vpn l2tp remote-access ipsec-settings authentication mode pre-shared-secret
set vpn l2tp remote-access ipsec-settings authentication pre-shared-secret <secret-key>
set vpn l2tp remote-access authentication mode local
set vpn l2tp remote-access authentication local-users username <user> password <password>
```

Optional: Create NAT rules for L2TP customers:

```
set nat source rule 10 outbound-interface 'eth0'
set nat source rule 10 source address '192.168.255.0/24'
set nat source rule 10 translation address 'masquerade'
```