

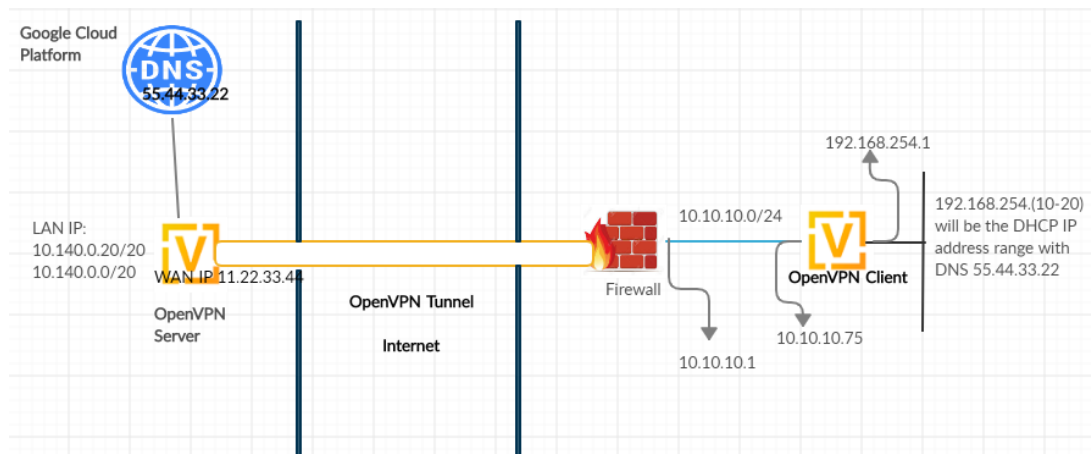


OpenVPN Client-Server Mode Example

Srividya Anantapatnaikuni - 2021-09-21 - 0 Comments - in OpenVPN

Introduction:

A configuration example of Server-Client OpenVPN mode(server is deployed in Google cloud platform and client in VMware premise) where the LAN users behind VyosVPN Client can access DNS in GCP. For deploying the vyos in cloud and virtual environments, refer [this guide](#).



Basic Configuration:

- Refer [this article](#) to create the X.509 certificate and key ,which is needed for the openvpn communication.

-Refer the above image for network specifications.

OpenVPN_server:

In configuration mode, execute the following commands:

```
set interfaces openvpn vtun10 encryption cipher 'aes256'  
set interfaces openvpn vtun10 hash 'sha512'  
set interfaces openvpn vtun10 local-host '11.22.33.44'
```

```
set interfaces openvpn vtun10 local-port '1194'
set interfaces openvpn vtun10 mode 'server'
set interfaces openvpn vtun10 'persistent-tunnel'
set interfaces openvpn vtun10 protocol 'udp'
set interfaces openvpn vtun10 tls ca-cert-file
'/config/auth/ovpn/ca.crt'
set interfaces openvpn vtun10 tls cert-file
'/config/auth/ovpn/OpenVPN_server.crt'
set interfaces openvpn vtun10 tls dh-file
'/config/auth/ovpn/dh2048.pem'
set interfaces openvpn vtun10 tls key-file
'/config/auth/ovpn/OpenVPN_server.key'
set interfaces openvpn vtun10 use-lzo-compression
```

Now we need to specify the server network settings. In all cases we need to specify the subnet for client tunnel endpoints. As we want the clients to access DNS server behind OpenVPN_server, we will use a push-route option for installing that route on clients.

```
set interfaces openvpn vtun10 server client OpenVPN_client ip
'10.140.0.55'
set interfaces openvpn vtun10 server domain-name 'vyos.net'
set interfaces openvpn vtun10 server max-connections '250'
set interfaces openvpn vtun10 server name-server '55.44.33.22'
set interfaces openvpn vtun10 server push-route '55.44.33.22/32'
set interfaces openvpn vtun10 server subnet '10.140.0.0/20'
set interfaces openvpn vtun10 server topology 'subnet'
```

Client name has to be the name mentioned as CN while generating the certs.

OpenVPN_client :

```
set interfaces openvpn vtun10 encryption cipher 'aes256'
set interfaces openvpn vtun10 hash 'sha512'
set interfaces openvpn vtun10 mode 'client'
set interfaces openvpn vtun10 persistent-tunnel
set interfaces openvpn vtun10 protocol 'udp'
set interfaces openvpn vtun10 remote-host '11.22.33.44'
set interfaces openvpn vtun10 remote-port '1194'
set interfaces openvpn vtun10 tls ca-cert-file
'/config/auth/ovpn/ca.crt'
set interfaces openvpn vtun10 tls cert-file
```

```
'/config/auth/ovpn/OpenVPN_client.crt'  
set interfaces openvpn vtun10 tls key-file  
'/config/auth/ovpn/OpenVPN_client.key'  
set interfaces openvpn vtun10 use-lzo-compression
```

DHCP service configured to assign the IP address to the LAN users

```
set service dhcp-server shared-network-name LAN authoritative  
set service dhcp-server shared-network-name LAN subnet  
192.168.254.0/24 default-router '192.168.254.1'  
set service dhcp-server shared-network-name LAN subnet  
192.168.254.0/24 dns-server '55.44.33.22'  
set service dhcp-server shared-network-name LAN subnet  
192.168.254.0/24 lease '86400'  
set service dhcp-server shared-network-name LAN subnet  
192.168.254.0/24 range 0 start '192.168.254.10'  
set service dhcp-server shared-network-name LAN subnet  
192.168.254.0/24 range 0 stop '192.168.254.20'
```

Source nat rule created for the LAN users to reach the DNS server.

```
set nat source rule 10 destination address '55.44.33.22'  
set nat source rule 10 outbound-interface 'vtun10'  
set nat source rule 10 source address '192.168.254.0/24'  
set nat source rule 10 translation address 'masquerade'
```

Output from virtual PC:

```
VPCS> show ip  
NAME          : VPCS[1]  
IP/MASK       : 192.168.254.10/24  
GATEWAY       : 192.168.254.1  
DNS           : 55.44.33.22  
DHCP SERVER   : 192.168.254.1  
DHCP LEASE    : 86351, 86400/43200/75600
```

```
VPCS> ping 55.44.33.22
```

```
84 bytes from 55.44.33.22 icmp_seq=1 ttl=63 time=3.467 ms
84 bytes from 55.44.33.22 icmp_seq=2 ttl=63 time=2.791 ms
84 bytes from 55.44.33.22 icmp_seq=3 ttl=63 time=2.985 ms
84 bytes from 55.44.33.22 icmp_seq=4 ttl=63 time=3.446 ms
```