Basic OpenVPN Client-Server Configuration

Yuriy Andamasov - 2020-08-21 - 0 Comments - in OpenVPN

Introduction

In addition to site-to-site configuration, OpenVPN also supports a client-server model for VPNs. This mode is more popular than using it in site-to-site mode, and allows for multiple remote client connections to a single centralized server.

In this mode, you might have multiple configured sites connecting to a single centralized router. For instance, you may have several branch offices, as well as a central headquarter office with your central router. The central router can serve as the OpenVPN server, with the branch office routers acting as OpenVPN clients.

The use of server-client VPNs in OpenVPN requires X.509 certificates to be setup. If you do not have an existing PKI (Public Key Infrastructure), you may set up a simple one using this guide.

Configuration Example

Network Specifications

In our example configuration, we will be using the following layout and goals for our network:

Routers:

- Three VyOS routers; one OpenVPN server, and two OpenVPN clients.
- Server router: `central-rtr`, located at the central office.
- First client router: `branch1-rtr`, located at the first branch.
- Second client router: `branch2-rtr`, located at the second branch.

Networks and Addresses:

- `central-rtr` has a public IP address of `203.0.113.2`.
- `central-rtr` has a private physical LAN that needs to be accessible through the client VPNs. The LAN's subnet is `192.168.0.0/24`.
- Both branch routers have dynamic public IP addresses.
- The address range for the tunnel endpoints for clients will be in `10.23.1.0/24`.
- Each client will have a `/24`-size subnet assigned to it in the `10.23.0.0/16` range.
- `branch1-rtr` will have the tunnel endpoint address of `10.23.1.10` and the subnet of `10.23.10.0/24` assigned to it.

- `branch2-rtr` will have the endpoint address of `10.23.1.20` and the subnet of `10.23.20.0/24`.

X.509 Certificate Information:

- Root CN (Common Name): `my-root-ca`.
- Server CN: `central`.
- Server key name: `server.key`.
- Branch 1 CN: `branch1`.
- Branch 1 client key name: `branch1.key`.
- Branch 2 CN: `branch2`.
- Branch 2 client key name: `branch2.key`.

All above certs are signed against our root cert. The file locations for the relevant files will be in each of the routers at the path `/config/auth/ovpn/`

Configuring the Server
Firstly, we need to configure our `central-rtr` to act as our OpenVPN server.

In configuration mode, issue the following commands:

```
set interface openvpn vtun0 mode 'server'
set interface openvpn vtun0 server subnet 10.23.1.0/24
set interface openvpn vtun0 persistent-tunnel
set interface openvpn vtun0 protocol udp
set interface openvpn vtun0 tls ca-cert-file
'/config/auth/ovpn/ca.crt'
set interface openvpn vtun0 tls cert-file
'/config/auth/ovpn/server.crt'
set interface openvpn vtun0 tls dh-file
'/config/auth/ovpn/dh1024.pem'
set interface openvpn vtun0 tls key-file
'/config/auth/ovpn/server.key'
```

We also need to install a push-route to push the route of the server's LAN of `192.168.0.0/24` to the clients:

```
set interfaces openvpn vtun0 server push-route 192.168.0.0/24
```

Now we need to set each of the client's configuration options. Client names are identified by the CN field in their certs:

```
set interface openvpn vtun0 server client branch1 ip 10.23.1.10
set interface openvpn vtun0 server client branch1 subnet
```

```
10.23.10.0/24
set interface openvpn vtun0 server client branch2 ip 10.23.1.20
set interface openvpn vtun0 server client branch2 subnet
10.23.20.0/24
```

Configure the Clients

Now we need to configure the client routers. We'll again assume the proper certificate and key files have been moved to the `/config/auth/ovpn/` directory on each client.

Branch 1's Router:

```
set interfaces openvpn vtun0 mode client
set interfaces openvpn vtun0 remote-host 203.0.113.2
set interfaces openvpn vtun0 tls ca-cert-file
/config/auth/ovpn/ca.crt
set interfaces openvpn vtun0 tls cert-file
/config/auth/ovpn/branch1.crt
set interfaces openvpn vtun0 tls key-file
/config/auth/ovpn/branch1.key
```

We also need to set up a static route to our `10.23.0.0/16` subnet on each router, as OpenVPN does not install this route automatically:

```
set protocols static interface-route 10.23.0.0/16 next-hop-interface
vtun0
```

Branch 2's Router:

```
set interfaces openvpn vtun0 mode client
set interfaces openvpn vtun0 remote-host 203.0.113.2
set interfaces openvpn vtun0 tls ca-cert-file
/config/auth/ovpn/ca.crt
set interfaces openvpn vtun0 tls cert-file
/config/auth/ovpn/branch2.crt
set interfaces openvpn vtun0 tls key-file
/config/auth/ovpn/branch2.key
set protocols static interface-route 10.23.0.0/16 next-hop-interface
vtun0
```