Introduction to OpenVPN

OpenVPN is an open-source software application that implements virtual private network (VPN) techniques. It creates secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities.

The security protocol used is customized to use SSL/TLS for key exchange. It is also capable of traversing network address translators (NATs) and firewalls.

Peers can communicate and authenticate each other using a pre-shared secret key, certificates, or username/password. In a client-server configuration, the server releases an authentication certificate for every client, enable the use of signature and Certificate authority. The OpenSSL encryption library is used extensively, and also the SSLv3/TLSv1 protocol. OpenVPN contains many security and control features as well.

Some advantages of OpenVPN:

1. Supports tunneling between all major operating systems
2. Can be used to Tunnel any IP subnetwork or virtual Ethernet adaptor over a single UDP or TCP port.
3. Easy installation and configuration.
4. Built for portability. It is easier to port because it is written as a user-space daemon rather than a kernel module or a complex modification of the IP layer.
5. Uses the OpenSSL3 library encryption, authentication and certification features of the OpenVPN secure tunnel. Any cipher, key size and HMAC digest supported by this library can be used.
6. Compatible with SSL/TLS, RSA certificates, X.509 PKI, TUN/TAP virtual devices5.

Architecture

a) Encryption

As it uses OpenSSL to do all encryption authentication, it can use all ciphers available in the OpenSSL package. It can also use the HMAC packet authentications feature that adds an additional layer of security to the connection. Hardware acceleration can also be used to get better encryption performance.

b) Authentication

OpenVPN offers pre-shared keys, certificate-based, and username/password-based authentication for the peers. Pre-shared secret key is the easiest, and certificate based being the most robust. Username/password authentications can also be used in later versions but with the use of third-party modules

c) Networking

OpenVPN runs over User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) transports, multiplexing created SSL tunnels on a single TCP/UDP port. The 2.3.x version also support IPv6 as protocol of the virtual network inside a tunnel and the OpenVPN applications can also establish connections via IPv6. It works through most of the proxy servers (including HTTP) and is good at works well through Network address translation (NAT) as well as getting out through firewalls.

References

1. https://en.wikipedia.org/wiki/OpenVPN
2. https://openvpn.net/index.php/open-source/documentation/howto.html