SSN Lab Assignment:

OpenVPN Server

OpenVPN is robust, highly configurable open-source software that enables secure Virtual Private Network (VPN) connections. It is widely used for securely connecting remote clients to a private network over the Internet. OpenVPN uses SSL/TLS for key exchange and can be configured to work with a wide range of encryption algorithms, including AES, RSA, and others.

OpenVPN simplifies the setup of a Public Key Infrastructure (PKI), allowing SSL/TLS certificates for secure authentication and key exchange between the server and clients. It supports routed and bridged VPN modes and can be configured to use UDP or TCP. While the port number can be customized, the default and official port for communication is 1194. OpenVPN clients are available for various platforms, including all Linux distributions, macOS, Windows, and OpenWRT-based WLAN routers.

Task 1 - Introduction

1a. What is PKI, and what is the purpose of PKI with OpenVPN?
b. Distinguish between a master certificate authority (CA) and a separate certificate authority (CA).
NB: Each client has a corresponding private key for the separate certificate, the public key. The primary Certificate Authority signs the server and client certificates.

Task 2 - Set-Up

OpenVPN enables mutual authentication using certificates, requiring both the client and server to verify each other's certificates before

establishing trust. The client verifies the server's certificate, and the server does the same for the client. This is done by first confirming that the presented certificates were signed by the primary Certificate Authority (CA), followed by checking details in the authenticated certificate header, such as the common name or certificate type (client or server).

2a. Install, build, and initialize a Public Key Infrastructure for an installed OpenVPN.

b. What did you notice about the prompt when creating a CA? What is the reason behind creating and using a passphrase?

c. Generate Diffie Hellman parameters and key pair for the server. Show the location(path) of the key pair generated

d. What is the size of the Diffie Hellman parameters and their locations?

e. Create a certificate for the server. What is the commonName value, and how many days are the certificates signed on the server?

f. Create a key for the client and also a client certificate. What is the expiration date of the certificate?

3a. What is the TLS Authentication (TA) Key, and why is it essential in OpenVPN?

b. Generate TLS Authentication (server) and show the server key information

c. Generate a TLS Authentication key (client) and show the client key information

Task 3 - Verification

4a. Simulate a communication between the OpenVPN server and the and client.

b. Using a traffic sniffer like Wireshark, inspect the interface of the VPN traffic. Show the information about this traffic.

References

- OpenVPN in Ubuntu
- Community of OpenVPN
- IBM Setting up VPN