ALI BOUANANE
TABBECH ZINEEDDINE

OPEN VPN

Ensuring Privacy and Security
in Internet Communication

Start Now →

WHAT IS A OPEN-VPN

- OPEN-SOURCE VIRTUAL PRIVATE NETWORK (VPN) SOFTWARE.
- PROVIDES SECURE CONNECTIONS OVER PUBLIC AND PRIVATE NETWORKS.
- HIGHLY CUSTOMIZABLE AND WIDELY USED FOR PRIVACY AND REMOTE ACCESS.

KEY FEATURES OF OPENVPN

Encryption

Protects data using AES-256.

Protocols

Operates over UDP/TCP for flexibility

Authentication

Supports certificates and passwords

Compatibility

Works on most platforms (Windows, Linux, macOS, Android ..ect)

Open-Source

Free to use and highly transparent

COMMON USE CASES

Remote Access : Securely access office networks

Bypassing Restrictions : Unlock censored websites

Wi-Fi Protection : Stay safe on public networks

IoT Device Security : secures communications between IoT devices, like smart cameras protecting them from cyberattacks

CERTIFICATES

CA

- Issuer: Self-signed (the CA itself).(CN=OpenVPN-CA)
- Subject: The CA's own name or identity.(CN=OpenVPN-CA)
- Public Key: The CA's public key.
- Validity: Time period the CA certificate is valid.
- Signature: Self-signed (hash of certificate data encrypted with the CA's private key)

CERTIFICATES

server

- Issuer: Self-signed (CN=OpenVPN-CA)
- Subject: The CA's own name or identity(CN=VPN-Server)
- Public Key: The CA's public key.
- Validity: Time period the CA certificate is valid.
- Signature: The CA signs the server certificate using the CA's private key.

CERTIFICATES

client

- Issuer: The CA (CN=OpenVPN-CA).
- Subject: The client’s identity (Client1).
- Public Key: The client’s public key.
- Validity: Time period the client certificate is valid
- Signature: The CA signs client certificate using the CA's private key.

THE BIG PICTURE

STEPS TO CONNECT OPENVPN SERVER AND CLIENT

See You Next →

SERVER SETUP

- Generate Certificates & Keys:

  Create a CA (Certificate Authority) : The server acts as its own CA, generating a root certificate used to sign the server and client certificates.(CA is the one who signs each side and tells if its legetimate meaning CA is liek a third trusted party)

  Generate Server & client Certificate : The server creates its own certificate and signs it using the CA certificate and the same for the client

  Generate Diffie-Hellman Parameters : These parameters are needed for secure key exchange between the server and client.

- Configure OpenVPN Server :Define the VPN network, routing rules, security settings, and link required certificates and keys server.conf

- share to client : Ca.crt, client.crt, client.key

- Start OpenVPN Server : Launch the OpenVPN server to listen for incoming client connections

CLIENT SETUP

- the client install the openvpn : the software of openvpn that contains functions for the process

- Configure OpenVPN Client : Set up the client configuration file, specifying the server’s IP address, port, and certificates path client.ovpn

- Start OpenVPN Client : Launch the OpenVPN client to connect to the server

ESTABLISHING THE VPN CONNECTION

- Handshaking Process:
    - The client sends a connection request to the server.
    - The server sends its certificate (self-signed in this case), and the client verifies the server's certificate using the CA certificate and same thing for the client he sends his ceritificate
- Key Exchange :The server and client exchange keys securely using Diffie-Hellman and perform the encryption handshake.
- Tunnel Established : Once the keys are exchanged and verified, the encrypted tunnel is established, and the client can securely communicate with the server over the VPN

VERIFYING THE CONNECTION

- **Check Connection :** Once the VPN is established, check that the client is connected using another network interface named tun (depends on the configuration file)

- **Ping the server:** Attempt to ping the server using the IP address specified in the server.conf file.

PURPOSE AND BENEFITS OF SETTING UP OPENVPN IN A LOCAL NETWORK:

Secure Communication:

- Even within the same local network, sensitive data is encrypted, preventing interception by unauthorized devices or malicious actors

Authentication:

- The server-client setup ensures only authorized users (clients with valid certificates) can access the network, enhancing security

Simulated Real-World Environment:

- Practicing VPN setup locally prepares us for deploying secure connections over the internet, where similar principles apply.

PURPOSE AND BENEFITS OF SETTING UP OPENVPN IN A LOCAL NETWORK:

Data Integrity:

- VPN protects against data tampering, ensuring the integrity of communications even on a shared network.

Layered Security:

- Demonstrates how additional security layers (TLS, encryption, certificates) can enhance the protection of a local network beyond simple local connectivity

Learning Objective:

- Teaches practical skills in VPN deployment, certificate management, and understanding secure communication protocols

OPEN VPN

CONCLUSION

OpenVPN is a trusted solution for secure, flexible, and private communication. Its open-source nature, adaptability to various needs, and widespread community support make it an ideal choice for individuals and businesses alike

THANK YOU FOR ATTENTION

See You Next →