VPN Simulator

Overview

This README provides instructions for setting up a VPN using OpenVPN on a Windows server and client machines. Follow the steps outlined below to successfully configure the VPN server and client certificates, along with the necessary configurations.

Prerequisites

- Windows Server and Client machines
- Administrator privileges on both machines
- Internet access to download OpenVPN

1. Installing OpenVPN

On the VPN Server and Client Machines

1. Download and install OpenVPN from the official community downloads.
2. Follow the installation prompts to complete the installation.

2. Generating Server Certificates

On the Server

1. Open a Command Prompt with administrative privileges.
2. Navigate to the OpenVPN installation directory.
3. Run the following commands to generate a Certificate Authority (CA) and server certificates:This process generates the server’s certificate and key.

```
./easyrsa init-pki
./easyrsa build-ca
./easyrsa gen-req server nopass
./easyrsa sign-req server server
```

3. Generating Client Certificates

On the Server

1. Generate the client certificates by running:

```
./easyrsa gen-req client1 nopass
./easyrsa sign-req client client1
```

2. Transfer the `client1.crt` and `client1.key` files to the client device for authentication.

4. Configuring ta.key for TLS Authentication

1. Generate the `ta.key` file for TLS authentication:This key secures the control channel.

```
openvpn --genkey --secret ta.key
```

5. OpenVPN Server Configuration

1. Create a configuration file named `server.conf` in the OpenVPN configuration directory (`C:\Program Files\OpenVPN\config`).
2. Include the following configuration in `server.conf`:

```
port 1194
proto udp
dev tun
ca ca.crt
cert server.crt
key server.key
dh dh.pem
tls-auth ta.key 0
cipher AES-256-CBC
```

6. Client Configuration

1. Create a client configuration file named `client.ovpn` in the same configuration directory.
2. Include the following configuration in `client.ovpn`:Replace `SERVER_PUBLIC_IP` with the public IP address of your VPN server.

```
bash
Copy code
client
dev tun
proto udp
remote SERVER_PUBLIC_IP 1194
ca ca.crt
cert client1.crt
key client1.key
tls-auth ta.key 1
cipher AES-256-CBC
```

7. Windows Commands for Client-Side VPN Connection

1. Open the Command Prompt on the client machine with administrative privileges.
2. Run the following command to start the OpenVPN client:

```
openvpn --config "C:\Program Files\OpenVPN\config\clien
t.ovpn"
```

8. Verifying VPN Connection

1. After starting the OpenVPN client, verify the VPN connection by checking the client logs for connection messages.
2. Alternatively, run a ping command to the VPN server:This will confirm the VPN is functioning properly.

```
ping SERVER_IP
```

Conclusion

Following the steps outlined above, you should have a functional OpenVPN setup on your Windows server and client machines. If you encounter any issues, please check the OpenVPN documentation or community forums for additional support.