Course: IT-Security
Author: Mohammad Homayoon Fayez Zealand – Academy of Technologies and Business
Associate Professor

Lab:	OpenVPN
Type:	Individual
Author:	Mohammad Homayoon Fayez
Objectives:	Learn VPN server and client installation and configuration
Prerequisites:	Ubuntu running in Virtual Box

Mandatory assignment

Problem definition

A remote user (company employee) needs to access the organization's Private network securely. Security components include Confidentiality, Data integrity, Origin integrity (Authentication), Non-repudiation and Availability

Requirements

It is a startup company; naturally, it wants to spend as less money as possible. Therefore, they prefer open-source software. Their requirements are as follows.

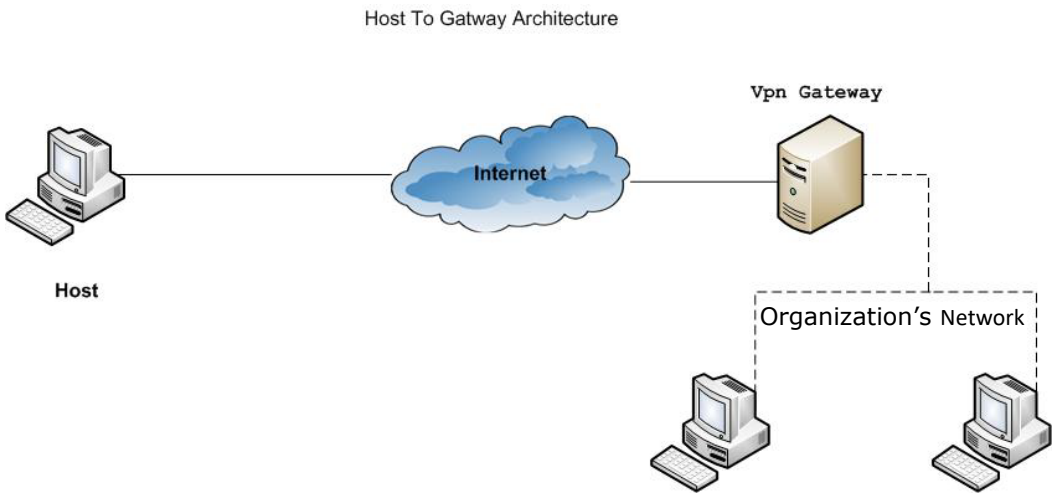
Architecture: Host to Gateway

OS (Gateway): Linux (Ubuntu or any other distros)

VPN server: OpenVPN

VPN client (on host): OpenVPN GUI for windows

Overview of the solution



Host = employee Outside the company's network

Practical Part

You can assist each other and even work in groups of 2-4 students during the practical/configuration part of the assignment, provided that the following requirements are met.

1. Each student must install and configure **OpenVPN server** in a virtual machine on his own laptop
2. Each student must install and configure **OpenVPN client GUI** on own laptop in host operating system i.e. windows
3. Each student must create a secure connection between employee(host) and the OpenVPN server

To prove 1-3 the following steps are required

4. Document the configuration steps of the server and some screen dumps to prove that it is on your laptop
5. Copy of the server log file that shows: a successful handshake, chosen encryption algorithms, client request, client IP assignment etc.
6. Copy of the OpenVPN client's configuration file e.g. client1.ovpn
7. A screen dump of a connected client running in windows on your own laptop
8. A screen dump of client accessing a resource on organizations network e.g. a web-server (optional)

Installation and Configuration

As we do not have a real scenario of an employee and a real organization with a LAN and a registered domain, therefore you should use virtual machines (VMware or VirtualBox) to create the platform for implementing and testing OpenVPN.

- Install OpenVPN server in Ubuntu in Virtual Box
- Install OpenVPN client in your MS Windows
- **Note** : when you update and download packages in ubuntu (OpenVPN server in virtual box), your virtual box's network must be in **NAT mode**

How to test

After you are finished with OpenVPN server configuration and you have installed the OpenVPN client in your Windows and you want to connect to the OpenVPN server, both your Windows and Ubuntu (**OpenVPN server** in virtual box) must be on the same network and subnet (check the IP addresses on both Windows and Ubuntu). Your virtual box's network must be in **bridge mode**. (**note**: in bridge mode your virtual box does not have access to the internet)

Optional: After you successfully connect from your Windows to OpenVPN server running in virtual box then try to connect to another student's server. For this to work, you can use a Router or your Mobile Phone

as access-point and connect 2 laptops to it where one of the laptops runs OpenVPN server in Ubuntu in a VirtualBox [Gateway]. The 2nd laptop will play the role of an employee who is outside the Company's LAN/network. This laptop will be running the OpenVPN Client software. This employee will use the VPN client software to securely connect to the other laptop.

Note: you must first get the client config file from the student running the OpenVPN server.

If things are working against you then may implement your OpenVPN server in cloud e.g. on Digital Ocean droplet then you can connect to it from your laptop. https://www.digitalocean.com/

(It is free for one month. You will be asked for your credit card info. But you will be charged $5/month only if you do not unsubscribe before one month is passed.)

To document your implementation and Configuration take notes and screen dumps of the important steps. Min 5 and Max 7 screen dumps of the important configuration steps.

Theoretical Part

You are not allowed to assist each other in answering the following questions. Server automatically detects plagiarism. Plagiarism is not tolerated.

Hand in

The theoretical part as a pdf file must be uploaded to Wiseflow. You will receive an email from wiseflow about the assignment and the Hand-in date.

Theoretical part's Questions and Topics

Q1. Give a Short description of OpenVpn

Q2. How one can acquire/obtain/get a certificate?

Q3. What a certificate is used for?

Q4. Explain the role of Certificate Authority

Q5. Describe different attributes (Basic Certificate Fields) of x.509 certificate

Q6 Explain the following topics

1. OpenVPN Static Key mode
2. OpenVPN TLS mode
3. Recent Attacks on SSL/TLS
   Find information about recent attacks on SSL/TLS and describe it in your own words.
4. Confidentiality
5. Data Integrity
6. Authentication
7. Non-repudiation
8. Availability

TLS handshake

To establish a secure session, the TLS handshake protocol manages Cipher suite negotiation, authentication of server and optionally the client and session key information exchange.

Q8. Explain each step of the handshake (in the diagram) in detail