

**NGEKEH PRISCA CHANA**

**CONFIGURING AND USING OPEN VPN ON WINDOWS OS**

**Thesis**

**CENTRIA UNIVERSITY OF APPLIED SCIENCES**

**INFORMATION TECHNOLOGY**

**FEBRUARY 2016**

**ABSTRACT**

<b>Unit</b> KOKKOLA/ PIETARSAARI	<b>Date</b> FEBRUARY 2016	<b>Author/s</b> NGEKEH PRISCA C.
<b>Degree programme</b> INFORMATION TECHNOLOGY		
<b>Name of thesis</b> CONFIGURING AND USING OPEN VPN ON WINDOWS OS		
<b>Instructor</b> RISTO PASSOJA		<b>Pages</b> 46 + 3
<b>Supervisor</b> RISTO PASSOJA		
<p>Hacking is becoming a more critical issue in the world of science and technology today, hence it is necessary to add more security devices to the network to ensure the security of information. Open virtual private network (OpenVPN) is one among the many ways companies use to securely connect in different locations or a remote user connecting to a company's network. This thesis work describes how to configure and use OpenVPN with Windows operating system. The following paragraphs discusses what OpenVPN is all about, the cryptography involved, the configuration process and key generation in both server and client, how to use it and why it is a necessity to all business corporations.</p>		

## LIST OF ABBRIVATIONS

**Asymmetric Encryption:** A method for encrypting and decrypting. Uses two keys which are public and private.

**Authentication:** Method to identify a person. It could be simple user name and password.

**Authentication Header (AH):** A component of IPsec that allows protection of the original source address of packets.

**AES:** Advanced Encryption Standard.

**Certificate:** An electronic data structure that contains identification information and a public key. This public key is usually signed by a certificate authority.

**Certificate authority (CA):** A body that does physical validation of other bodies and then signs their keys in order to prove they are who they claim to be.

**CHAP:** Challenge Handshake Authentication Protocol.

**CRL:** Certificate Revocation List.

**CA:** Certificate Authority.

**Dedicated lease line:** A dedicated line is a communications cable.

**Digital Signature:** code that uniquely identifies the sender of an electronic data.

**DES:** Data Encryption Standard.

**DH:** Diffie-Hellman.

**DSL:** Digital Subscriber Line.

**ESP:** Encapsulating Security Payload.

**GUI:** Graphical User Interface.

**GRE:** Generic Routing Encapsulation.

**IP:** Internet Protocol.

**ISP:** Internet Service Provider.

**IPX:** Internetwork Packet Exchange.

**IKE:** Its keys include Internet Key Exchange.

**ISAKMP:** Internet Security Association and Key Management Protocol.

**Key Agreement:** A process by which two or more parties can calculate and agree on the same key over a public network without eavesdroppers also being able to calculate the key. Both parties can influence the outcomes

**Key Exchange:** System for transferring cryptographic key material between parties, usually over an insecure medium. Keys must be exchanged before used.

**L2TP:** Layer Two Tunneling Protocol.

**MD5:** Message Digest 5 algorithm.

**NCP:** Network Control Protocol.

**Network Address Translation (NAT):** Usually a component of a firewall. NAT allows multiple internal clients to share external addresses.

**OSI model:** Open Systems Interconnection model.

**OpenVPN:** Open Virtual Private Network.

**Public Key Cryptography:** System of using public and private key pairs to protect data and authenticate entities. Includes certificate authorities.

**PAP:** Password Authentication Protocol.

**RSA:** Rivest-Shamir-Adleman.

**RFC:** Request for Comment.

**Secure Socket Layer (SSL):** Protocol used to protect communication over the Internet. SSL is making headway into link encryption environments like VPNs.

**Symmetric Encryption:** System for encrypting/decrypting traffic using the same key on both sides to encrypt and decrypt message. Very fast when compared to asymmetric encryption

**SHA-1:** Secure Hash Algorithm 1.

**TCP:** Transmission Control Protocol.

**TLS:** Transport Layer Security

**TCP:** Transmission Control Protocol

**TAP Virtual Driver:** A driver interface that allows Ethernet bridging. The TAP interface communicates with the actual physical interface eliminating some complexity and rigidity. It has direct access to the system's kernel in Windows operating system.

**Traffic:** Data in Motion.

**URL:** Uniform Resource Locator.

**UDP:** User Datagram Protocol.

**3DES:** Triple Data Encryption Standard.

## **PREFACE**

Though this project is written as a pre-requisite to obtain a bachelor's degree in the field of information technology it is out to help those who want to attend a level of security to their information to be able to install and use OpenVPN on a Windows operating system. Working through this project enables the gain of a good knowledge of how security is very important when dealing with World Wide Web and this can give a deep inside for cyber security carrier.

Sincere gratitude to the Almighty God. It has been so great working together with my supervisor M.Sc Risto Passoja as he has been a source of inspiration, working so hard day and night to realize this project. Also much thank to my English teach Nina Hynynen who gave the basic background on how to present this thesis work. This thesis is going to go a long way to help all those who are interested about knowing what OpenVPN is all about, the protocols involved and how to install and use it.

# TABLE OF CONTENTS

1 INTRODUCTION .....	1
2 VIRTUAL PRIVATE NETWORK (VPN) .....	2
2.1 Advantages of VPN and Open VPN .....	4
2.2 Disadvantages of VPN and Open VPN.....	4
2.3 Secured Communication.....	5
2.3.1 Authentication .....	5
2.3.2 Integrity.....	6
2.3.3 Confidentiality.....	6
2.4 Categories of VPN .....	9
2.4.1 Site to Site VPN .....	9
2.4.2 Remote Access VPN .....	10
2.4.3 Host to Host VPN.....	11
2.5 Types of VPN Technologies .....	12
2.5.1 Point-to-Point Tunneling Protocol (PPTP).....	13
2.5.2 Layer 2 Tunneling Protocol (L2TP) .....	13
2.5.3 IPSec (IP SECURITY) .....	14
2.2.4 Secure Socket Layer (SSL).....	15
2.2.5 Multiprotocol Label Switching (MPLS).....	15
3 OPEN VPN.....	17
3.1 Features .....	17
3.2 Open VPN Installation and Configuration.....	18
3.3 HOW TO USE OPEN VPN .....	39
3.4 OpenVPN Testing Environment .....	41
4 DISCUSSION AND CONCLUSION.....	43
5 REFERENCES .....	45

## 1 INTRODUCTION

VPN is a very common topic in the field of information technology and security. Creating a secure private network connection within the public network has become the top priority of organizations. There are typically many types of VPN depending on the way there are classified. VPN is simply the connection between two or more devices to enable the safe transmission of information. These two devices could be in the same or different network. In VPN the network is private and information only reaches those for whom it is intended. Some people may choose to have more than one ISP so that if one of them is down, they can switch to the other to ensure continues flow of secured data.

In this thesis work there is going to be a discussion on brief history about the evolution of VPN, its importance, how to download, install and use it. Also the properties of VPN that makes it outstanding, the various types of VPNs, VPN technology and the protocols involve. VPN can be implemented at both layer three (Network layer) or layer two (Data Link Layer) of the OSI model. VPN effectively functions by ensuring three basic things which are integrity, confidentiality and authentication. All these features are very important in order to keep information safe.

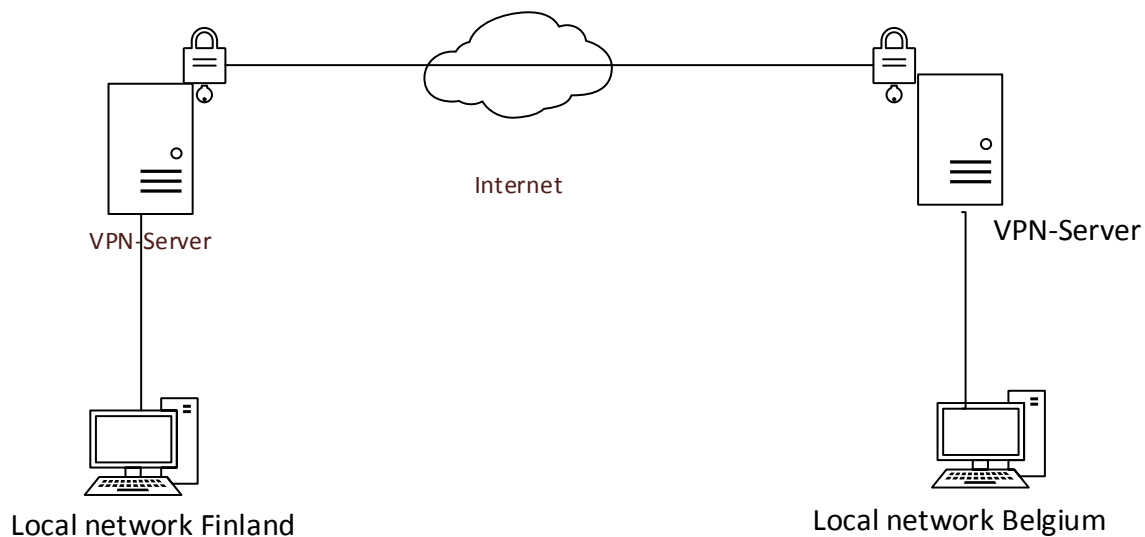


## **2 VIRTUAL PRIVATE NETWORK (VPN)**

VPN is an acronym which stands for virtual private network. It refers to the technology which is involved in the creation of private network through public network like the internet to ensure the safe transmission of traffic. Traffic could be transmitted from a company's headquarter to its branches or between a company and a remote user. Before the 1990s, companies with different branches used paper mails to securely exchange information among themselves. They later on change to the use of telephone and then fax but with all these, there were still challenges in communication which was delay and mails were missing on their way to destinations. Later on came the lease line technology which has to do with the connection of cables from one location to another. This is secure and safe to transmit information from one location to another yet was expensive to run and maintain. Most companies were able to connect using the dedicated lease line. With this each branch needed a separate dedicated lease line in order to communicate with each other. Presently companies are highly involved in virtual private network for the safe transmission of information within their various branches. (Feilner & Graf 2009.)

In 1990 there was a rapid growth in the internet which was very fast and less expensive but not secured. This came about the virtual private network (VPN). VPN technology provided a secure network connection through the internet and enable cooperating agencies to share traffic by remotely connecting to it using a software provided by an authorized organization. Only members connected to that VPN have access to any information in that system. Workers in a branch located in Finland can connect and communicate safely with members of another branch located in Belgium and Germany and no external person will have access to the information being transferred. VPN could also be seen as a connection

secured by software that provided a secure transmission of data through a public network called the internet. Graph 1 is an overview of the idea behind VPN. (Feilner & Graf 2009.)



GRAPH 1. VPN connection (Adapted from Balchunas 2007.)

Looking at Graph 1, there are two branches of same company located in Finland and Belgium each having a server and router. The branches are connected to each other through the unprotected internet. Employees at the branch in Finland will need to work on information found in server at the branch in Belgium likewise employees at branch Belgium will want to work on information found at server in the Finland branch. In order to ensure that this is done successfully they need to establish a VPN tunneling. The lock and key is used to signify security measures used. Information from server located in Belgium will be protected before transmission to server in Finland and when they reach sever in Finland, they will be unprotected and made available for the intended individuals. (Feilner & Graf 2009.)

## **2.1 Advantages of VPN and Open VPN**

VPN is easier and cheaper to implement than the dedicated WAN and other connections. This is because large equipment don't need to be purchase for its implementation. It also ensures a high degree of data security through confidentiality, Integrity and authentication which shall be discussed. OpenVPN ensures scalability as more devices could be added to the network with very little or no cost and within a short time. Compared to other VPNs such as IPsec, OpenVPN is not complex and can be run at layer 2 or layer 3. At layer 2, frames are used to transfer IPX packet and Windows Network Browsing packets which could be a problem to other VPN connections. With open VPN, firewall in the central branch can protect the computer such that only the network port is open to local customers. (Crist & Keijser, 2015.)

An OpenVPN tunnel can be created through every firewall and proxy. It can run as a TCP or UDP service and as a client or server. One port can be used to allow connection and they work well with Network Address Translation (NAT). There is no pressure using static IPsec on each side of the tunnel. They can have DSL with dynamic IPs. OpenVPN is not only easy to install but can be installed on any platform. It has a modular design with a high degree of simplicity which no other VPN can offer. It is also supported by mobile devices which has attracted a large number of people to implement it. The fact that OpenVPN can run on cross platforms gives it the strength over other VPNs. It also supports the use of dynamic IP addresses. (Crist & Keijser 2015.)

## **2.2 Disadvantages of VPN and Open VPN**

When VPN network is installed, it is important to consider a reliable internet service provider (ISP) who will ensure the continued network availability. Otherwise there can be more than one internet service provider. This will

help in case one is down there can be a switch to the next despite the fact that it is cost expensive. VPN uses more megabits hence connection becomes slower than normal. OpenVPN is not compatible to IPsec hence devices that use IPsec cannot connect to applications using OpenVPN. It is difficult to make them compatible because of structural differences. Also many people do not know how to use OpenVPN and it has no enterprise class GUI for administration but there are some promising projects. It can only run on user space and all traffic must go through kernel space to user space and back. (Crist & Keijser 2015.)

## **2.3 Secured Communication**

The primary objective of a VPN is to ensure a safe communication through the public internet. This can be done through; confidentiality which is a function of encryption, Integrity which is a function of hashing, and authentication which is a function of providing identity. Cryptography is the science of creating secret codes and comprises of encryption and hashing. With VPN Company's traffic are highly protected from being hacked. This section discusses the basic components of authentication, integrity, confidentiality and cryptography including the algorithm for hashing, encryption and key management that might all be used by VPN. (Crist & Keijser 2015.)

### **2.3.1 Authentication**

Authentication ensures that no one is able to open data meant for a particular individual. This can be done with the use of password, digital certificates, smart cards and biometric methods. Digital certificates are obtained from a certificate authority (CA) responsible for issuing these certificates. The CA makes sure that a VPN device is real and authentic by

issuing a digital certificate. To be sure that this certificate is authentic, it must be verifiable. The disadvantage of using a public key is that it could be compromised at any level. The common authentication method used is the identity and password for login. (Hosner 2004.)

### **2.3.2 Integrity**

Integrity ensures that the original data remains the same as it travels through the public internet. Integrity is achieved using the hashing algorithm. Hash checks to see if any bit has been altered. While sending traffic, the hash factor is send alongside. This harsh factor is compared at the receiving end by the receiver. In case any bit has been altered, the hash factor will not match indicating that the data has been manipulated. Hashing algorithm could be Massage Digest 5 algorithm (MD5) or Secure Hash Algorithm (SHA-1). MD5 HAS 128 bits and is less secured and slower compared to SHA-1. SHA-1 uses 160 bits, it is the strongest and it is faster compared to MD5. There also exist SHA-2 which is a group of algorithm but SHA-1 is the strongest algorithm so far. There has been some development in the MD family from MD2 to MD4 to MD5 which is a one way hashing algorithm. (Hosner 2004.)

### **2.3.3 Confidentiality**

Confidentiality is a way of protecting traffic from being hacked that is being read by unauthorized individuals. This can be done through encapsulation and encryption ensuring that no one is able to capture the traffic. Another word for encapsulation is tunneling. Tunneling is the act of putting an internet protocol into another protocol. Example TCP/IP traffic with a given IP address can be put into a packet with another IP address before sending

through the public internet. When the traffic gets to its destination it is decapsulated for the authorized individual. This is known as Generic Routing Encapsulation (GRE) and can be done at the layer three which is the network layer. At the layer two, encapsulation methods such as Layer two tunneling protocol (L2TP) can be used. The TCP/IP traffic are put in a datagram. (Balchunas 2007.)

Encryption is another way to ensure confidentiality which is a two way business. If there must be an encryption, there must also be a decryption. There exist different mechanisms to encrypt and decrypt which gives rise to different VPN solutions. These solutions are normally built between routers with firewall and VPN software. Software enables connectivity between workers in different locations while the firewall enables certain traffic to pass and encryption provide security of traffic along the transmission process. In order for data to be decrypted, the decryption process must be done with a key. (Feilner & Graf 2009.)

When the sender encrypts data and send it through the public internet, the receiver must decrypt the data before reading or making use of it. This may be done through the use of a key which could be symmetric or asymmetric. Symmetric key is a situation where the sender and the receiver share the same key for encryption and decryption. This key is private and could be as long as 40 to 250 bits. The more the bits the stronger the security. Some examples are Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Advanced Encryption Standard (AES), RC2/4/5/6 (Ron Rivest Rons code) and BLOW FISH. DES has a 64 bit length but only 56 is used for encryption meaning the encryption is not strong. It is a very weak key and should not be used. 3DES has a key size of 168 or 112 which makes it stronger and it could be trusted. AES is widely used encryption method. It has a key length of 128 or 192 or 256 bit and is also trusted and it is highly recommended. (Feilner & Graf 2009.)

Asymmetric algorithms are best known as public algorithms where the private key encrypts the data while the public key decrypts it. The key length is between 512 and 4096 bit. This algorithm is slow because it is based on difficult computation algorithm. In this algorithm, the keys for encryption and decryption are different. Example of the algorithm includes RSA, ElGamal, Elliptic curves and Diffie-Hellman (DH). They are all trusted and the strength of a key is determined by the D-H group used to generate that key. There are several D-H groups which are group 1 with 768 bit, group 2 with 1024 bit and group 5 with 2048 bit. Asymmetric keys require a separate key for encryption (the public key) and decryption (the private key). Public keys are openly exchanged between devices to encrypt data during transfer. Private keys are never exchanged. (Balchunas 2007.)



Graph 2. Data encryption process (Adapted from Balchunas 2007.)

Considering Graph 2, assume the use of a public/private key infrastructure, Router A and router B have their unique private key. Router A and Router B exchange public keys. When router B encrypts data destined for router A, it uses router A's public key and vice versa. Router A decrypts the data using its private key. Only the private keys can decrypt the data. IPSec can use pre-shared keys for authentication. Pre-shared means that the parties agree on a shared secret key that is used for authentication in an IPSec policy on both sides of the VPN tunnel. During security negotiation, information is encrypted before transmission by using a session key. These keys could be public or private (Aaron Balchunas 2007.)

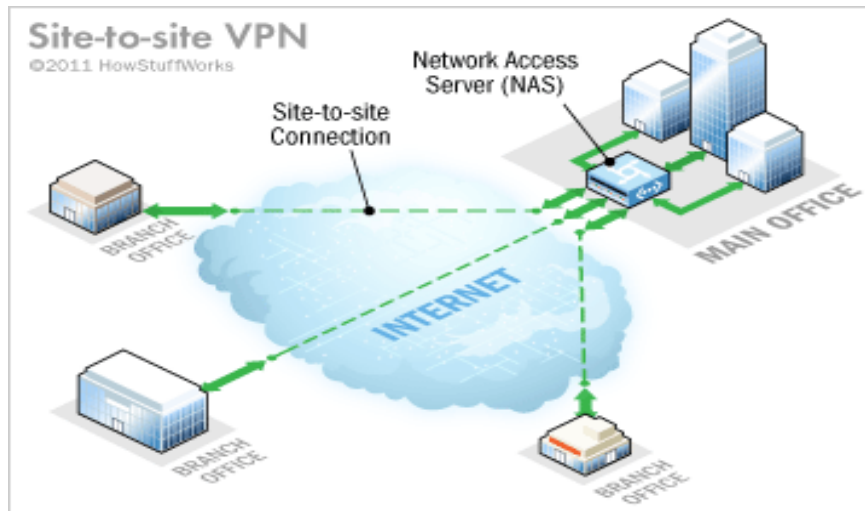
## **2.4 Categories of VPN**

As already discussed before, VPN refers to the technology which involve the creation of a private network through a public network like the internet to ensure the safe transmission of data. Data could be transmitted from company headquarter to company branches or between the company and a remote user. It involves the use of many different protocols and technologies. There are many different types of VPN depending on the way they are classified. Three types of VPN classified according to their connection and application shall be discussed in the subsequent paragraphs. These include site-to-site, remote access and host to host VPN. (Erwin, Scott & Wolfe 1999.)

### **2.4.1 Site to Site VPN**

The site to site VPN is common in companies that are located on two or more sites and they want to connect together securely using the Internet. A secure tunnel is created between two gateways. This enables different branches to share files and other resources in a secured manner. Usually IPSec is used alone or with some other protocols to create this VPN. Site to site VNP can be setup in a way that all the branch offices will be connected to the head office's VPN server as shown on the Graph 3 or each branch office can have its own separate VPN server. (Erwin et al 1999).





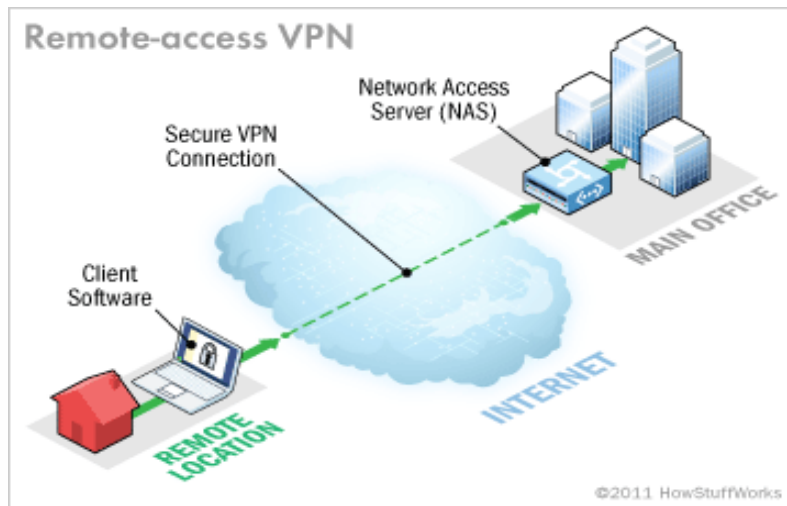
Graph 3. Site to Site VPN (adapted from Tyson & Crawford 2011.)

#### 2.4.2 Remote Access VPN

With remote-access VPN connection, individual user is allowed to connect to a private network from a remote location using a laptop or desktop computer connected to the Internet. A remote access user is someone who accesses a corporate network remotely. A remote access VPN could also be called a mobile VPN. This involves the creation of a secured connection between an individual's computers to a VPN gateway. This enables users to get access to VPN anywhere they go as long as they are connected to the Internet. Remote VPN uses two main technology which are IPSec and SSL. (Internet-Computer-Security 2008.)

Remote users connect to VPN gateway through a software installed in their computers. Installation of the software requires setup which will lead to the VPN gate way. Authentication may be required such as username and password. The software also has firewall protection for both the client and the corporate network from threats. The remote user's laptop could also contain treats such as viruses which could corrupt the corporate network.

Most VPN servers can control their client through network access control. Client computers must meet certain criteria if they are to gain access to the corporate network. (Internet-Computer-Security 2008.)



GRAPH 4. Remote Access VPN (adapted from Tyson 2011.)

### 2.4.3 Host to Host VPN

This type of VPN involves the creation of a safe communication connection directly between two or more specific hosts. This type of VPN cannot take many hosts and have limited scalability. Hosts could be on the same or different networks and a VPN tunnel is established between them. It makes good use of layer three (network layer) using IPSec in transport mode. It need resources to maintain it and configuration is done on each host. It is often used for single purpose need and the technology used here is the IPSec. There is always a need for authentication to allow IPSec connection. It is the only category of VPN that provides protection of data throughout the transmission process and could be a problem because

inspection of data decryption cannot be done by firewalls or other security software. Graph 5 shows an illustration of host-to-host VPN. (Keijser 2011.)



GRAPH 5. Host-to-host configuration (adapted from The Company's Networks 3way site.)

## 2.5 Types of VPN Technologies

Virtual private network (VPN) technology refers to the techniques and protocols involved in implementation and proper functioning of a VPN. There are a number of technologies which had grown over the years due to the rapid growth of the Internet and the need for advance security methods. VPN technologies like the L2TP can operate at only one layer of the OSI model which is the layer 2 of the OSI model while some can operate at both layer two and three of the OSI model such as IPSec. The different types of technologies involved and their various protocols will be discoursed in the subsequent paragraph. Companies select the best technology for their organizations depending on their security needs. (Keijser 2011.)

### **2.5.1 Point-to-Point Tunneling Protocol (PPTP)**

This type of protocol uses Microsoft platform alongside other protocols. With point-to-point tunneling protocol, remote users can securely access their network. Point-to-point tunneling protocol has some drawbacks and it is seen as a weak security protocol. Point to point tunneling protocol is easier to use and configure compared to other tunneling protocols. This protocol can be used directly over the Internet or dial up service. It tunnels packet before sending it to the Internet through Generic Routing Encapsulation. It is part of Windows NT server and can be downloaded freely from the Microsoft web page. (Schneier & Mudge 2005.)

### **2.5.2 Layer 2 Tunneling Protocol (L2TP)**

This layer 2 tunneling protocol is mostly used by internet service providers to provide VPN service to the Internet. This protocol works by combining point-to-point tunneling protocol and layer 2 forwarding protocol with functionalities from IPsec. To negotiate IP address assignment, L2TP uses PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol) and NCP (Network Control Protocol). It has replaced PPTP since it is routable over IP and network unlike PPTP which is routable only over IP. It does not give security on its own but it is used with other protocol to provide the necessary security of the public Internet. (Keijser 2011.)

### 2.5.3 IPSec (IP SECURITY)

IPSec works at the layer three of the OSI model, it is a framework and not a protocol on its own and it comprises of many other protocols put together to ensure its proper functioning. It is very flexible and is the best solution to secure a VPN. It is a collection of protocols, standards, and algorithms to secure traffic over an untrusted network, such as the Internet. It can be used in the Site to Site, Remote Access and host-to-host VPNs. IPSec offers secure measures like confidentiality, anti-replay and integrity like any other technology protocol. (Bauer, Liebscher, & Klaus 2006.)

The important protocols that function in IPsec are Encapsulating Security Payload (ESP) and Authentication Header protocol (AH). Its keys include Internet Key Exchange (IKE) which determines and negotiates protocols, algorithms and keys. It uses protocols such as Internet Security Association and Key Management Protocol (ISAKMP). It is believed that IPsec is so complex to use yet it is used to create a majority of VPN found in companies today such as Cisco PIX, FreeSWAN, and Checkpoint VPN1. It is important to note that FreeSWAN is no longer functional but its code was used to develop OpenSWAN and StrongSWAN. (Hosner 2004.)

IPsec is a standard VPN well known technology. It also contains many Graphical User Interfaces (GUIs) for administrator and the modification of the IP stack is complex modification of the kernel and administrator privileges are necessary. The implementation from different manufacturers can be compatible and requires a step by step process for its implementation. It requires several ports and protocols for firewall and could encounter problems with dynamic addresses on both sides. There could also be security problems with its technology due to its complexity. IPsec most often uses opportunistic encryption mechanism, that is, it makes use of both source and destination address. Each operating system requires an individual implementation of its own IPSec. (Bauer et al. 2006.)

### **2.2.4 Secure Socket Layer (SSL)**

This implements security in the TCP sessions. Works in the transport layer (Layer 4) of the OSI model. This is very common with the uniform resource locator (URL) to ensure web site security. It is symbolized by //https// and the “s” indicated that the web site is encapsulated. SSL was developed by Netscape Communication Corporation and is highly used in modern browsers. This technology is one of its kind and is widely used in banking and e-commerce web sites. It ensures a high level of privacy and security. Every one must have a valid certificate issued by the certificate authority which enables him or her to have a connection to the VPN. If a client is not allowed to connect to the VPN any longer, a Certificate Revocation List (CRL) is used to stop the certificates. VPN connection would be established only if a valid certificate from an authorized certificate authority is presented. SSL grows rapidly because of its high rate of use for Internet browsing. The free and open source of SSL is called OpenSSL and it is used for both encryption and authentication. The encryption is done using standard algorithm like Advanced Encryption Standard (AES), Blowfish, or Triple DES (3DES). ( Keijser 2011.)

### **2.2.5 Multiprotocol Label Switching (MPLS)**

This is a service provided by the ISP where the ISP allows companies with two or more sites to establish a VPN connection using the ISP network to transport data. It gives one the ability to do one-to-many connection. MPLS works alongside IP and frame relay protocol. It uses a label to determine the path a packet will follow to its destination. These paths are known as label switch paths. At each hop the previous label is removed and a new

one place indicating the path it should follow. It works at the layer 2 of the OSI model which is the data linked layer. MPLS can be used to create tunnels without encryption. (Internet-Computer-Security 2008.)

### **3 OPEN VPN**

Open VPN is a type of open source VPN which had similar features like IPsec VPN but it is easy to install. It requires the use of VPN software and with a number of click you can install the already design software. Examples include Transport Layer Security (TLS) protocol, Secure Sockets Layer (SSL) protocol VPN. SSL/TLS VPN presently known as TLS which evolved from SSL version 3. For authentication, OpenVPN provides a pre-shared keys, certificate-based, and username/password-based. Encryption can be symmetrical, in this case both the sender and the receiver uses the same key to encrypt and to decrypt data. This key has to be available to all the computers involved in the VPN connection. This type of key is known as pre-shared key and an attacker can get access to information if they get hold of this key. They can do this by brute-force attack, hence keys should be changed at intervals. (Surhone, Timpledon & Marseken 2010.)

#### **3.1 Features**

OpenVPN supports UDP and TCP transport protocols and its performance depends on the type of protocol. SSL will be able to provide security for a very long time and is easy to implement compared to other protocols. It functions just like IPsec. OpenVPN was introduced as a VPN solution on the 13 May 2001 which could only tunnel IP packets over UDP and encrypted by Blowfish cipher and Secure Hash Algorithm, Hash-based Message Authentication Code (SHA-HMAC) signatures. Version 1.0 was released in March 2002 which provided SSL/TLS- based authentication and key exchanged. Version 2.0 was created in November 2003. Version 2.0 test3 prepared the goal for a multi-client server which is one of the most outstanding features of OpenVPN today. This enables several clients to



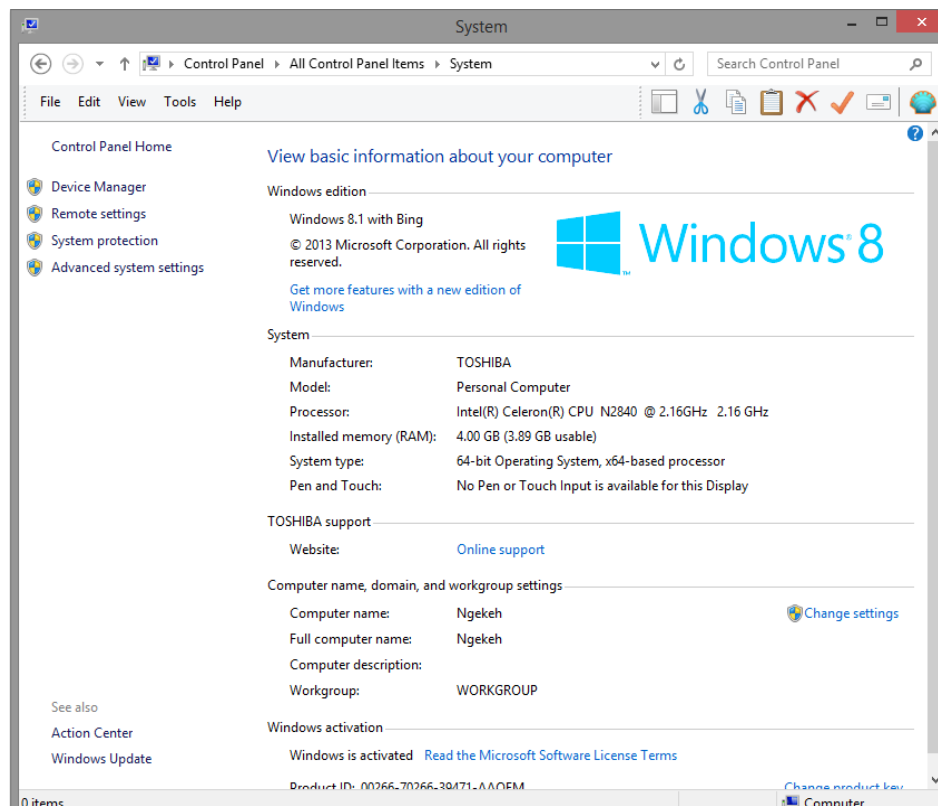
connect on the VPN on the same port. The default port for open VPN is port 1194. OpenVPN network server can tell the client to use a different network setup instantaneously. (Hosner 2004.)

TUN/TAP devices make OpenVPN less complex. TUN works well with IP frame at the layer 3 while TAP works with Ethernet frames at the layer 2. Complexity in VPNs is not compatible with security. OpenVPN works perfectly with a firewall. OpenVPN is already standardized and can run on all operating systems. People are still trying to familiarize themselves with this technology. It is a simple technology to be implemented, learned and used. It has a standardized network, packets and encryption technology. OpenVPN can run on user space. SSL/TLS is an industry-standard cryptographic layer and it can be ran at a speed of 20Mbps on a 1Ghz machine and has no problem with Network Address Translation (NAT). Open VPN and IPsec have different characteristics. Open VPN is ran on user space. Open VPN is not a web application proxy and does not use a web browser as many people might think. Open VPN can be managed using graphical user interfaces on a Mac or Windows operating system. Open VPN is an SSL type of VPN and it is not compatible with IPsec, L2TP and PPTP. (Surhone, Timpledon & Marseken 2010.)

### **3.2 Open VPN Installation and Configuration**

This section discusses the step by step processes involved in the installation and configuration of OpenVPN on a Windows operating system including relevant web pages and screen snapshots. First of all the operating system have to be checked to ensure that it is Vista or a later version. Secondly the size of the operating system has to also be checked whether it is a 64 bit or 32 bit. This is to ensure that, the correct software for the operating system is being downloaded. To know how to check, follow the steps on Graph 6. Go to the start menu and click to open the

control panel, then navigate to system and double click to open it. There one can find information about the system as shown on Graph 6.



GRAPH 6. Features of the operating system.

As can be seen from the screen shot, the system on Graph 6 uses Windows 8.1 operating system and it is 64 bit. Now the specifications of our computer which will be used as a server during the configuration process is known. One can start to download the very first and important file which is the Windows installer. This file can be obtained from this link <https://openvpn.net/index.php/open-source/downloads.html>. There are different installers there for different operating systems like Mac, Linux, UNIX and Windows. So one has to select the package based on the operating system and in our case it is Windows 64 bit Operating System. The web page looks like the one on Graph 7.

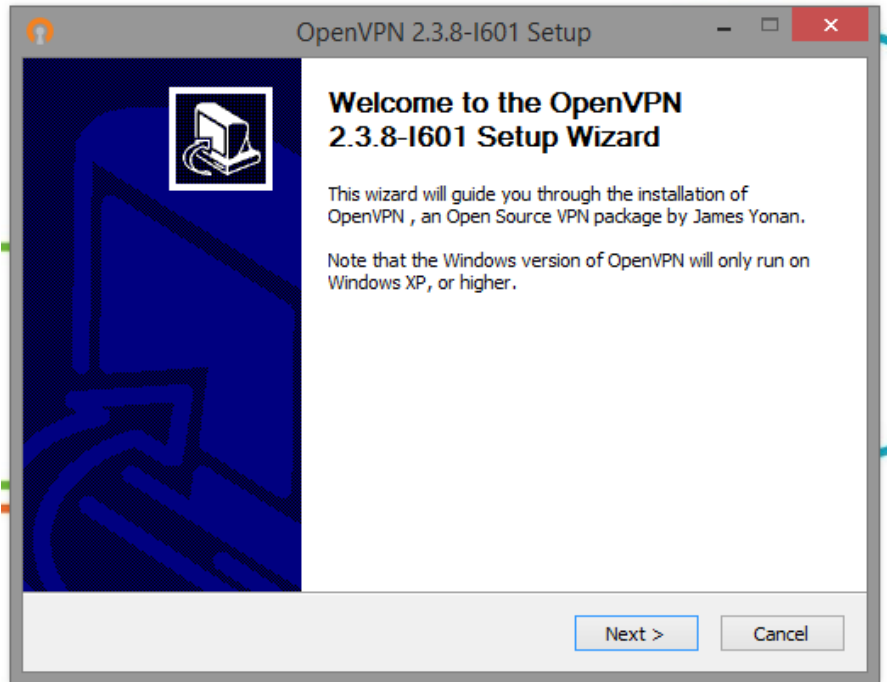
The screenshot shows the OpenVPN website's 'Downloads' page for version 2.3.8. The page includes a navigation bar with 'Home', 'VPN Service', 'VPN Solution', 'Community', and 'Downloads'. A sidebar on the left lists various sections like 'Overview', 'Downloads', 'Source Code', and 'Documentation'. The main content area is titled 'Downloads' and features a sub-header 'OpenVPN 2.3.8 -- released on 2015.08.04 (Change Log)'. Below this, there is a paragraph of text explaining the release and a link to the change log. A table lists various download options, including source tarballs and installers for different operating systems and architectures. Each row in the table includes a description of the file, a direct download link, and a link to the GnuPG signature.

Source Tarball (gzip)	<a href="#">openvpn-2.3.8.tar.gz</a>	<a href="#">GnuPG Signature</a>
Source Tarball (xz)	<a href="#">openvpn-2.3.8.tar.xz</a>	<a href="#">GnuPG Signature</a>
Source Zip	<a href="#">openvpn-2.3.8.zip</a>	<a href="#">GnuPG Signature</a>
Installer (32-bit), Windows XP	<a href="#">openvpn-install-2.3.8-i686.exe</a>	<a href="#">GnuPG Signature</a>
Installer (64-bit), Windows XP	<a href="#">openvpn-install-2.3.8-i686-x86_64.exe</a>	<a href="#">GnuPG Signature</a>
Installer (32-bit), Windows Vista and later	<a href="#">openvpn-install-2.3.8-i686.exe</a>	<a href="#">GnuPG Signature</a>
Installer (64-bit), Windows Vista and later	<a href="#">openvpn-install-2.3.8-i686-x86_64.exe</a>	<a href="#">GnuPG Signature</a>

Instructions for verifying the signatures are available [here](#).

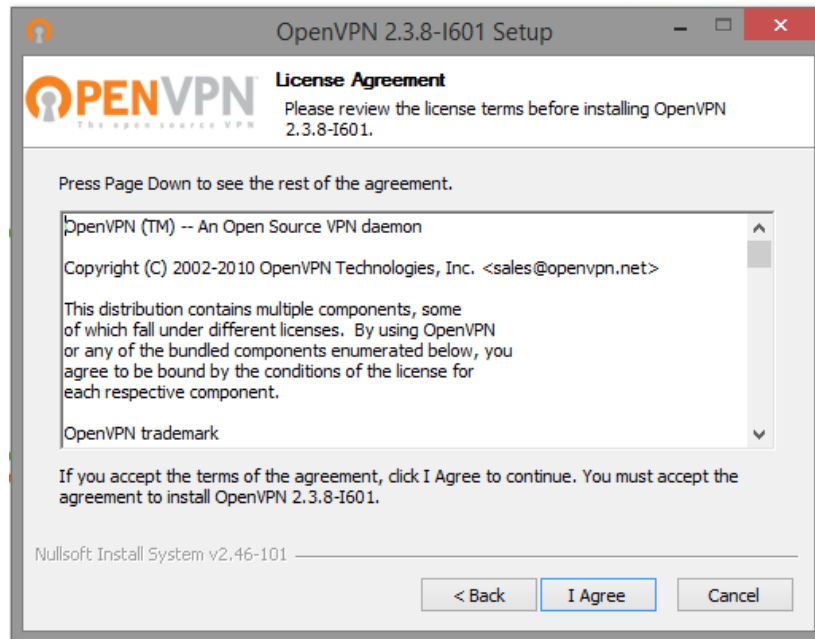
GRAPH 7. Windows installer web page for OpenVPN.

When the correct file is downloaded, the installation has to be done step by step. Navigate to where the file was saved, right click on it and a list of commands will open. Then select Run as administrator. This may request administrator's password depending on the settings on the computer or laptop. In Windows OS, OpenVPN should be ran by the administrator. This is a Window's feature and if ran by a user, the administrator's permission must be needed. This is going to start the installation process by opening a window. Click Next to continue the installation which will open another page as shown on Graph 8.



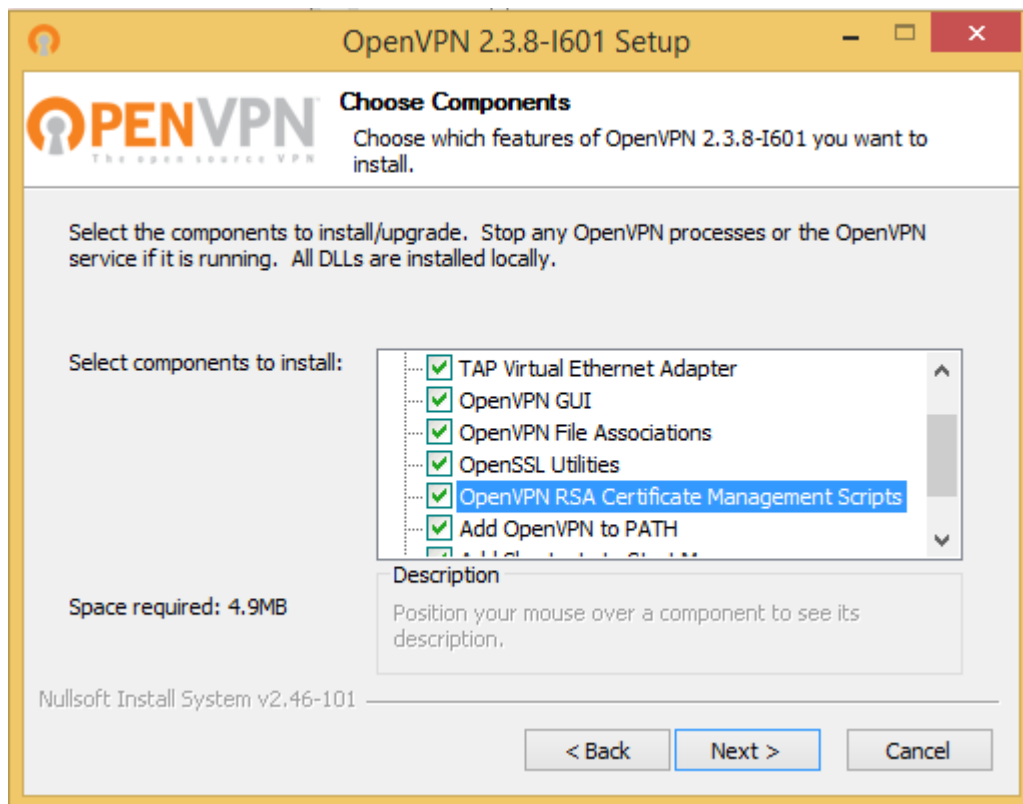
GRAPH 8. OpenVPN installer installation steps.

Click I Agree. This is agreeing to the License Agreement. It is often recommended to read the agreement before proceeding with the installation of any software. (See Graph 9.)



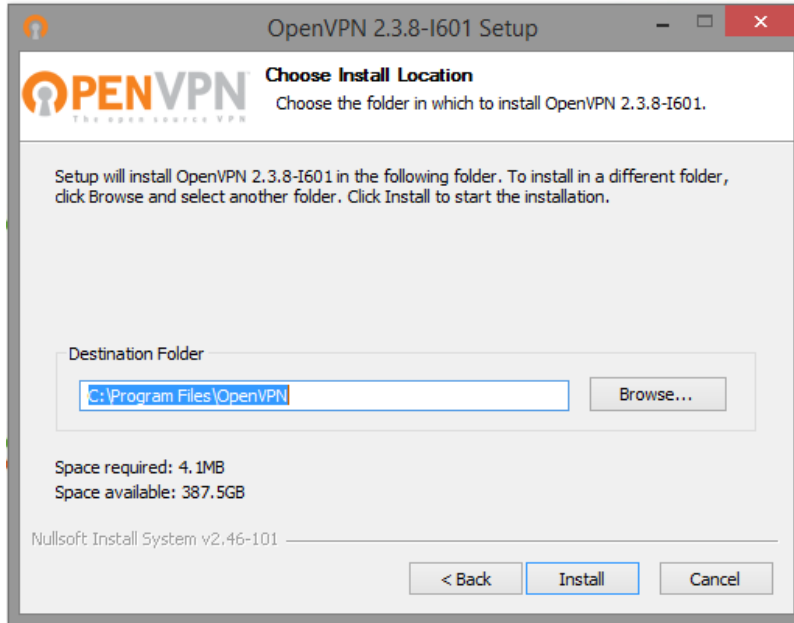
GRAPH 9. OpenVPN installer installation steps.

It is possible to install Easy-RSA at the same time with the OpenVPN install as can be seen on the Graph 10. This is pretty an easy way else they have to install it from github.com and it will require the download all the other configuration files to add in the Easy-RSA it is not downloaded alongside the VPN installer.

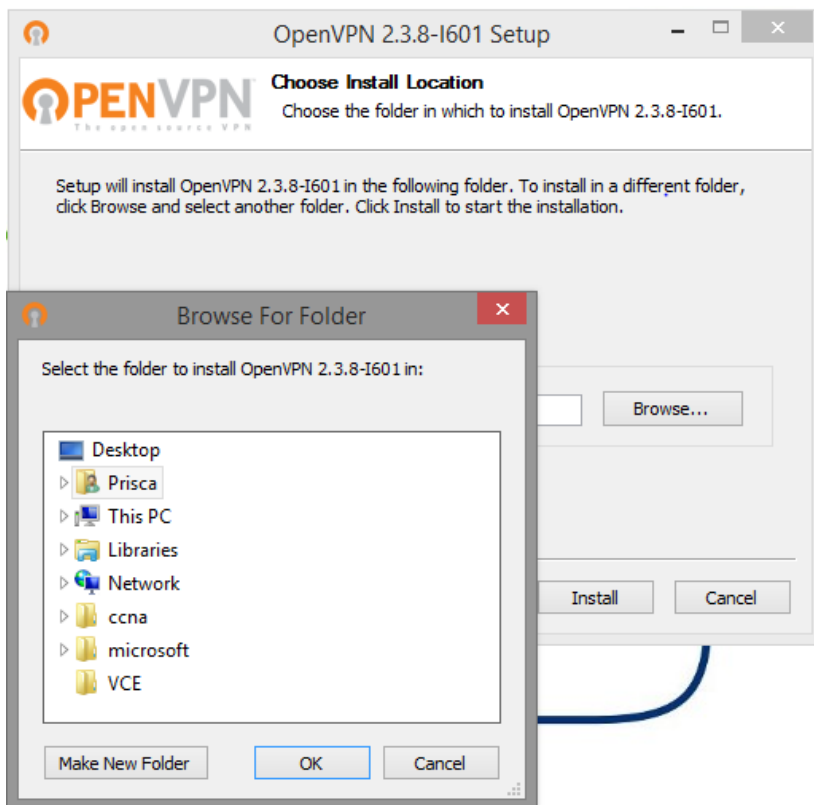


GRAPH 10. Install Easy-RSA alongside openVPN installer.

Now choose the location where the files will be safe permanently unless uninstalled. It is recommended to leave the default path as Program Files in the C drive. After selecting the location click install. (see Graphs 11 and 12.)

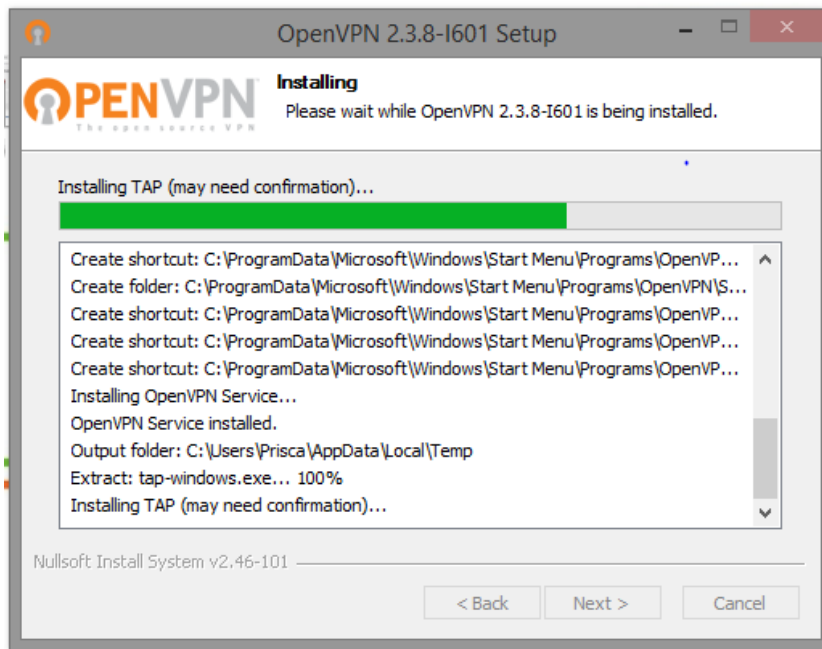


GRAPH 11. Chose the location to store Openvpn.

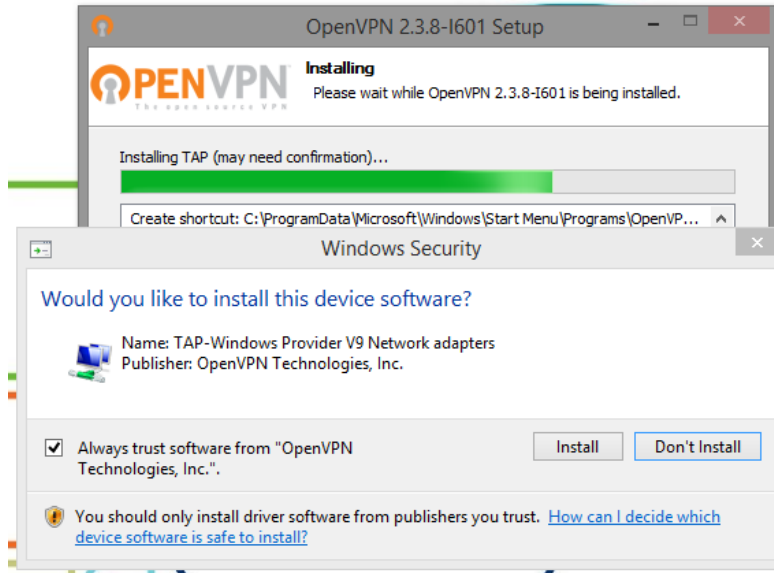


GRAPH 12. Chose the location to store Openvpn.

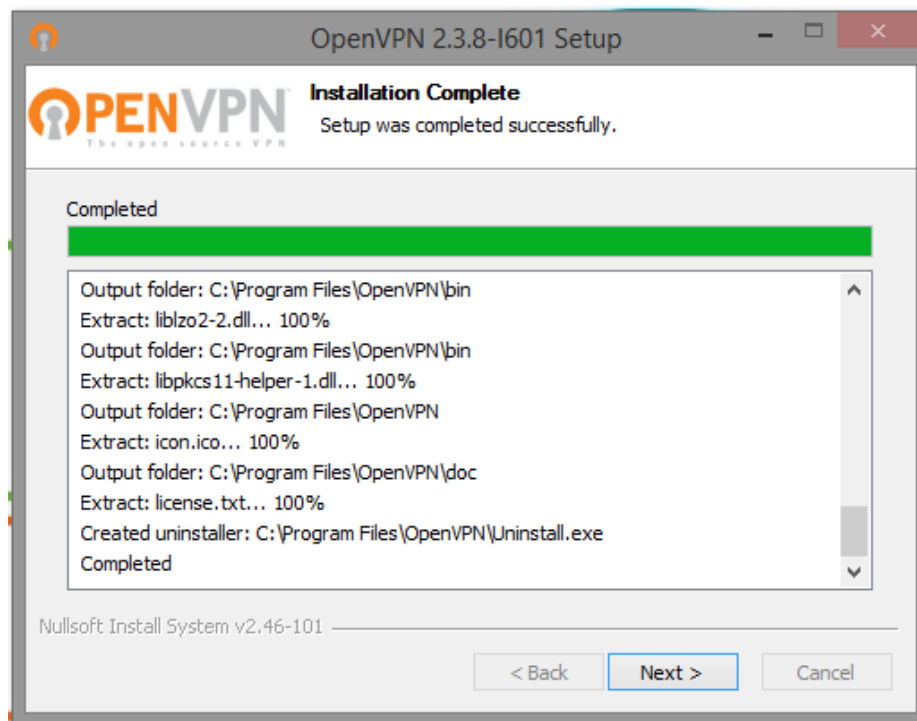
Now wait for a few minutes for the installation process to be completed. It is actually a light weighted program and takes little time to be installed as on Graph 13. If the window on Graph 14 opens, click on install and wait for the installation process to be completed. Click Next to the following dialogue box on Graph 15. Finally click Finnish. One can choose to check the Show Readme dialogue box or not. If the Show Readme dialogue box is checked, the following Readme text will open else nothing will happen (see graph 17). At the end a desktop icon will be created like the one on Graph 18 and the OpenVPN installer file path could be traced to C:\Program Files\OpenVPN with the following files and folders in it as shown on Graph 19.



GRAPH 13. Wait for the installation process to be completed.

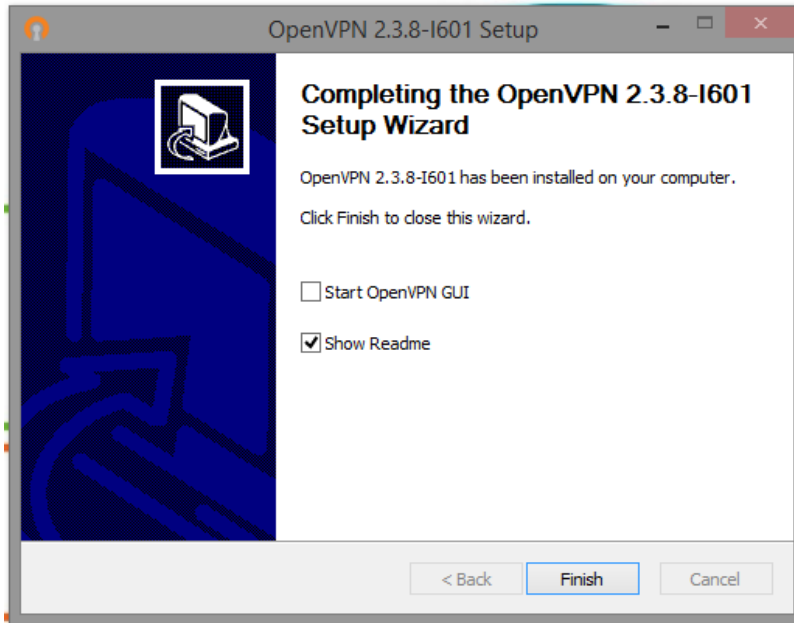


GRAPH 14. Installation process continues.

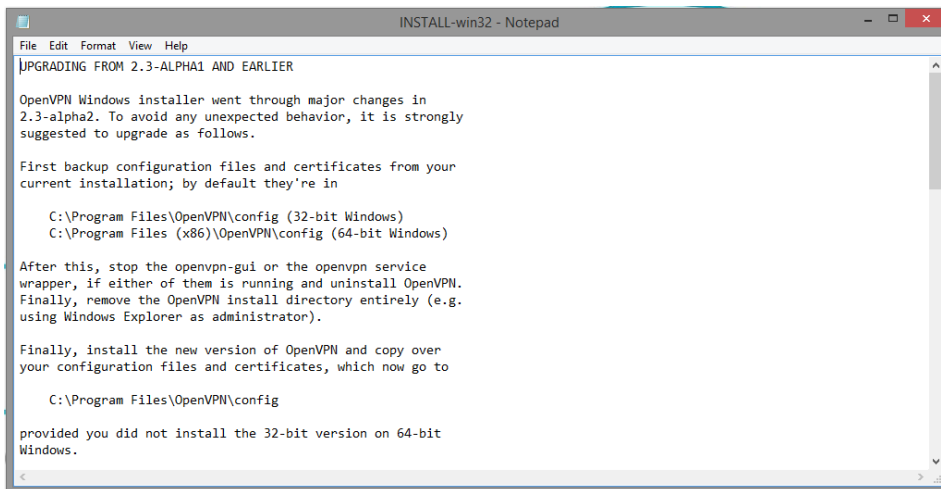


GRAPH 15. Installation process completed.





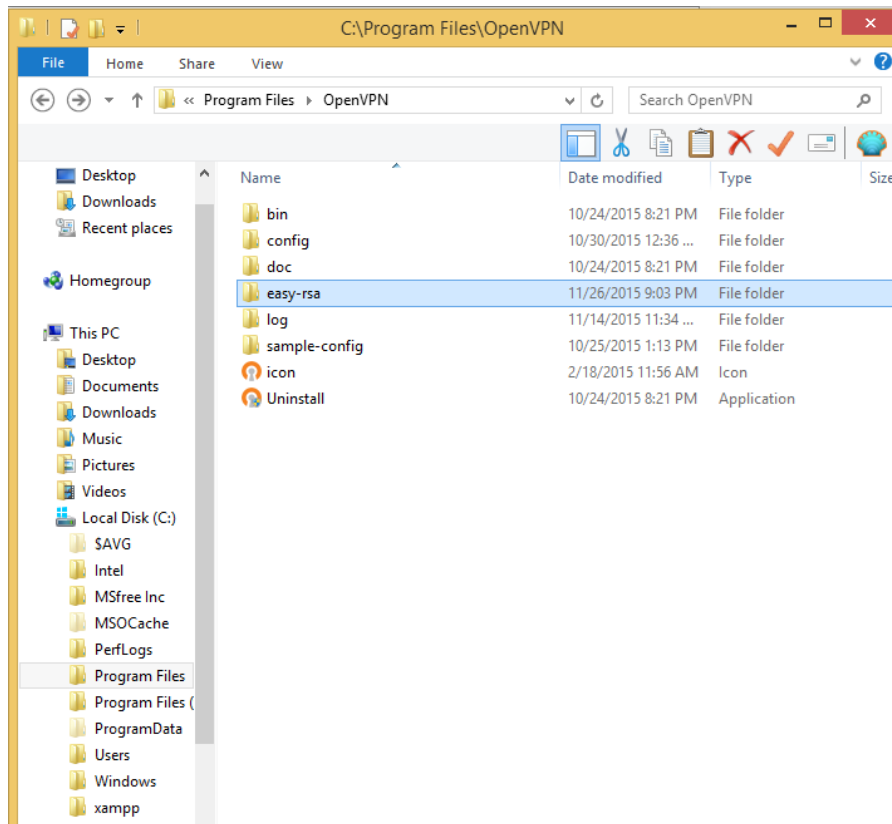
GRAPH 16. End the installation of the installer.



GRAPH 17. Readme file for OpenVPN installer.

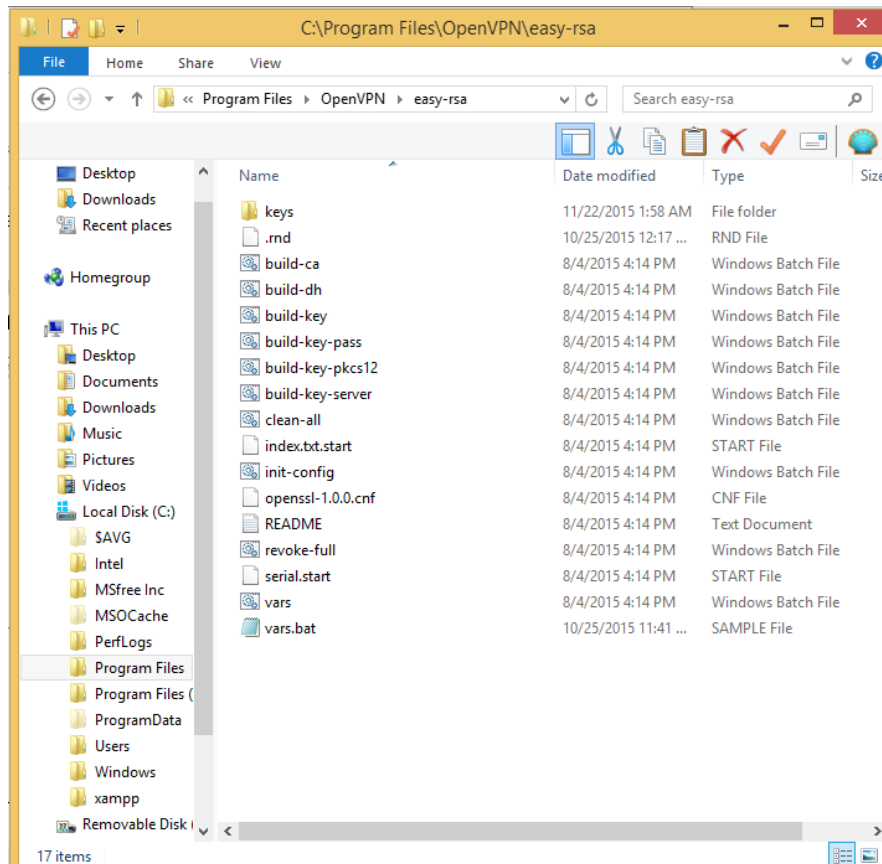


GRAPH 18. OpenVPN icon.



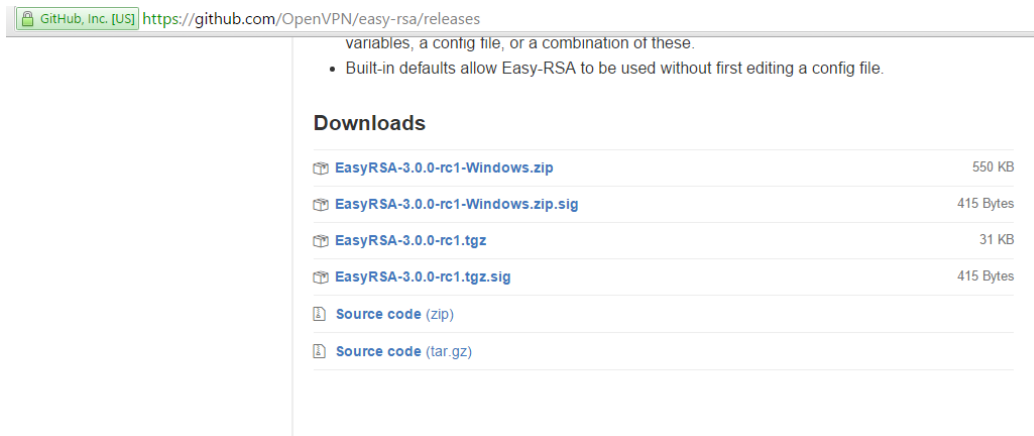
GRAPH 19. OpenVPN path and folders.

The OpenVPN installer which has a graphical user interface (GUI) and the Easy-RSA folder. Easy-RSA is the script used to build the configuration. It contains many files such as `init-config.bat`, `vars.bat.sample`, `clean-all.bat`, `build-ca.bat`, `serial.start` and `index.txt.start`. (See Graph 20). Easy-RSA is a command line tool which is used to build and manage Public Key Infrastructure (PKI) Certificate Authority.



GRAPH 20. Contents of Easy-rsa folder in the openVPN folder.

Another option is to download it separately after the installation process. This will be so if one want to get the latest update of the Easy-RSA folder. This can be download by following the instruction on Graph 21. It can be gotten from the link <https://github.com/OpenVPN/easy-rsa/releases>. Make sure that the correct package for the operating system is downloaded. When downloaded it is a zip file (EasyRSA-3.0.0.RC1.Windows.zip) which is the very first file has to be extracted to the OpenVPN installation folder (See Graph 21). But this method is less recommend because it is complicated as one still have to search on the Internet and download the configuration files like the vars.bat, init-config just to name a few.

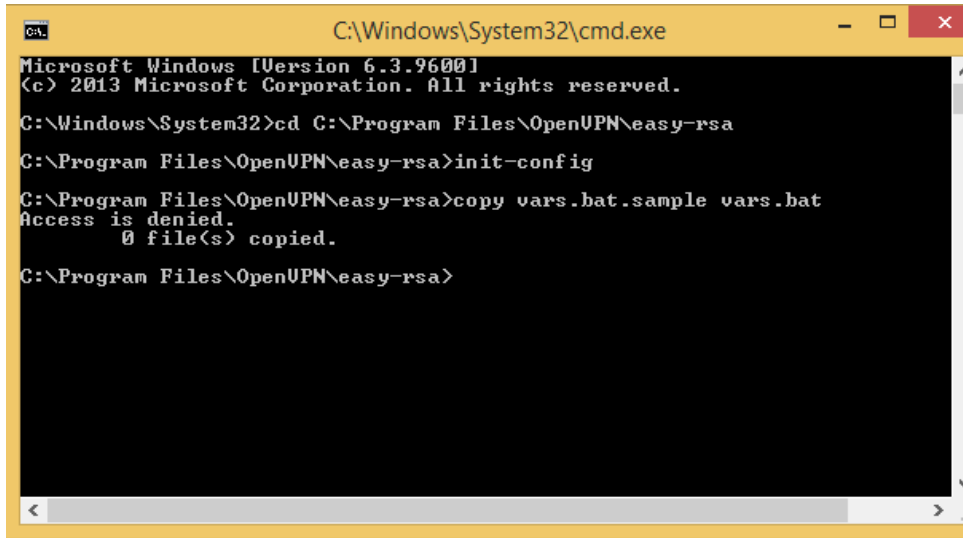


GRAPH 21. Download easy-rsa from GitHub.com.

Now everything is set, so navigate to command line and start to generate the various keys necessary. First of all we move to the command line by typing `cmd.exe` at the start menu. Then move to the Easy-RSA folder by typing the following command at the command line. “`cd C:\Program Files\OpenVPN\easy-rsa`” which will open the Easy-RSA folder as shown on Graph 22. Then initialize the configuration process by typing “`init-config`” but as seen on Graph 23 the file was not copied. This was because the Easy-RSA refused the command line access to its folder.

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Windows\System32>cd C:\Program Files\OpenVPN\easy-rsa
C:\Program Files\OpenVPN\easy-rsa>
```

GRAPH 22. Accessing easy-rsa folder from the command prompt.



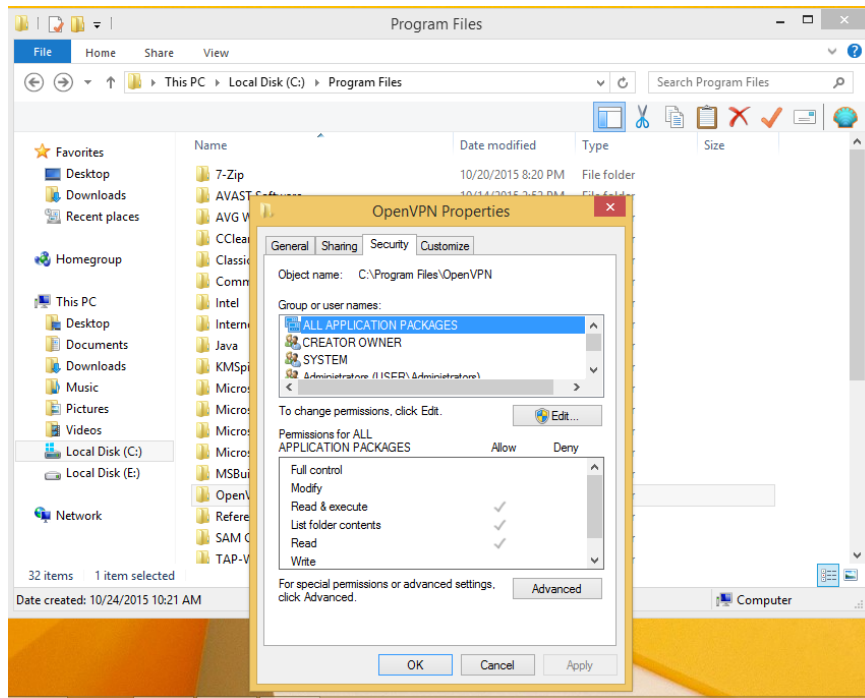
```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\System32>cd C:\Program Files\OpenVPN\easy-rsa
C:\Program Files\OpenVPN\easy-rsa>init-config
C:\Program Files\OpenVPN\easy-rsa>copy vars.bat.sample vars.bat
Access is denied.
      0 file(s) copied.

C:\Program Files\OpenVPN\easy-rsa>
```

GRAPH 23. Configuration process not initialized.

To get access permit to the program file, one have to activate it by right clicking on the Easy-RSA folder and selecting properties, security and select the user to give this access permission to and click on edit, full control, applied and ok as shown below. Note that it is very important to grant access permission to all the folders in the OpenVPN folder. (see Graph 24). When the permission has been granted, run `init-config` which is going to copy the configuration file as can be seen below. Note that this command can only be ran once (See Graph 25). Next open the `vars.bat` file using a text editor on the command line by typing `notepad vars.bat`, edit the information to suit our current location and save it as can be seen on Graph 26.



GRAPH 24 Giving access to open VPN folder.

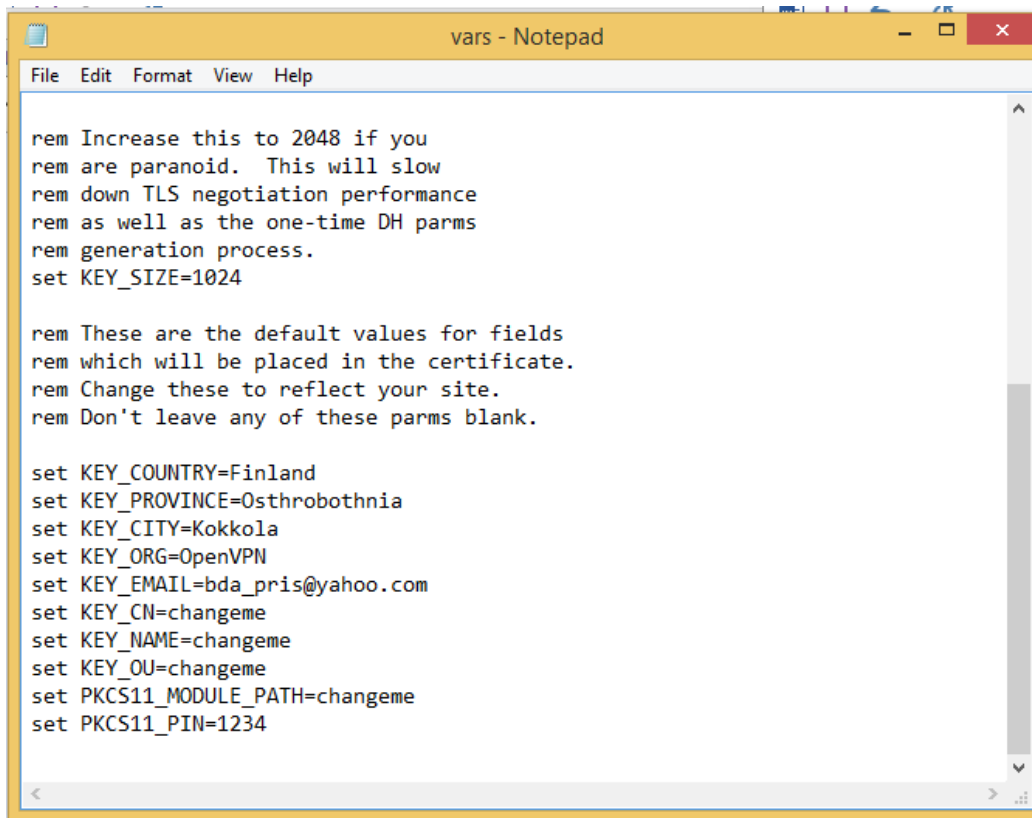
```

C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\System32>cd C:\Program Files\OpenUPN\easy-rsa
C:\Program Files\OpenUPN\easy-rsa> init-config
C:\Program Files\OpenUPN\easy-rsa>copy vars.bat.sample vars.bat
Access is denied.
 0 file(s) copied.
C:\Program Files\OpenUPN\easy-rsa>init-config
C:\Program Files\OpenUPN\easy-rsa>copy vars.bat.sample vars.bat
 1 file(s) copied.
C:\Program Files\OpenUPN\easy-rsa>

```

GRAPH 25. Open VPN configuration process initialized



```
vars - Notepad
File Edit Format View Help

rem Increase this to 2048 if you
rem are paranoid. This will slow
rem down TLS negotiation performance
rem as well as the one-time DH parms
rem generation process.
set KEY_SIZE=1024

rem These are the default values for fields
rem which will be placed in the certificate.
rem Change these to reflect your site.
rem Don't leave any of these parms blank.

set KEY_COUNTRY=Finland
set KEY_PROVINCE=Osthrobothnia
set KEY_CITY=Kokkola
set KEY_ORG=OpenVPN
set KEY_EMAIL=bda_pris@yahoo.com
set KEY_CN=changeme
set KEY_NAME=changeme
set KEY_OU=changeme
set PKCS11_MODULE_PATH=changeme
set PKCS11_PIN=1234
```

GRAPH 26. Edited var.bat file.

Again continue by running the commands “vars” followed by the command “clean-all”. Two files are going to be copied (See Graph 27). The next step is to build the certificate authority and key by entering the command “build-ca”. Many information will be required to enter such as the country name, state or province name, locality, organization and email as shown on graph 28 below. This the public key and will be copied to the configuration file of both server and client computer.

```

C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\System32>cd C:\Program Files\OpenUPN\easy-rsa
C:\Program Files\OpenUPN\easy-rsa> init-config
C:\Program Files\OpenUPN\easy-rsa>copy vars.bat.sample vars.bat
Access is denied.
    0 file(s) copied.

C:\Program Files\OpenUPN\easy-rsa>init-config
C:\Program Files\OpenUPN\easy-rsa>copy vars.bat.sample vars.bat
    1 file(s) copied.

C:\Program Files\OpenUPN\easy-rsa>vars
C:\Program Files\OpenUPN\easy-rsa>clean-all
The system cannot find the file specified.
    1 file(s) copied.
    1 file(s) copied.

C:\Program Files\OpenUPN\easy-rsa>

```

GRAPH 27. Vars and clean-all command ran.

```

C:\Windows\System32\cmd.exe
C:\Program Files\OpenUPN\easy-rsa>clean-all
The system cannot find the file specified.
    1 file(s) copied.
    1 file(s) copied.

C:\Program Files\OpenUPN\easy-rsa>build-ca
WARNING: can't open config file: /etc/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'keys\ca.key'

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

-----
Country Name (2 letter code) [US]:OpenUPN-P
string is too long, it needs to be less than 2 bytes long
Country Name (2 letter code) [US]:MP
State or Province Name (full name) [CA]:KORKOLA
Locality Name (eg, city) [SanFrancisco]:CENTRIA
Organization Name (eg, company) [OpenUPN]:OpenUPN-MP
Organizational Unit Name (eg, section) [changeme]:TECNOLOGY
Common Name (eg, your name or your server's hostname) [changeme]:PRISCA
Name [changeme]:PRIZEE
Email Address [mail@host.domain]:bda_pris@yahoo.com

C:\Program Files\OpenUPN\easy-rsa>

```

GRAPH 28. Result of the build-ca command

The next instruction is to build the certificate and key for the server by entering the command “build-key-server server”. This is going to build the



server certificate key which is private and should not be shared. Anywhere one is asked to enter common name, put server and when asked to sign the certificate enter “y” for yes and when asked to commit we enter y for yes again (see Graph 29).

```

C:\Windows\system32\cmd.exe

C:\Program Files\OpenUPN\easy-rsa>build-key-server server
WARNING: can't open config file: /etc/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'keys\server.key'

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

-----
Country Name (2 letter code) [Finland]:FI
State or Province Name (full name) [Osthrobothnia]:OS
Locality Name (eg, city) [Rokkolal]:KL
Organization Name (eg, company) [OpenUPN]:M04
Organizational Unit Name (eg, section) [changeme]:OpenServer1
Common Name (eg, your name or your server's hostname) [changeme]:MyServer1
Name [changeme]:Server1
Email Address [bda_pris@yahoo.com]:bda_pris@yahoo.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:prizee
An optional company name []:M04
WARNING: can't open config file: /etc/ssl/openssl.cnf
Using configuration from openssl-1.0.0.cnf
Loading 'screen' into random state - done
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName       :PRINTABLE:'FI'
stateOrProvinceName :PRINTABLE:'OS'
localityName      :PRINTABLE:'KL'
organizationName  :PRINTABLE:'M04'
organizationalUnitName:PRINTABLE:'OpenServer1'
commonName        :PRINTABLE:'MyServer1'
name              :PRINTABLE:'Server1'
emailAddress      :IA5STRING:'bda_pris@yahoo.com'
Certificate is to be certified until Nov 30 16:58:11 2025 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]:y
Write out database with 1 new entries
Data Base Updated

```

GRAPH 29. Result of the build-key-server command.

Now generate the client certificate. To generate client's certificate the command “build-key Eve-laptop” is entered and run. Eve-laptop is the name of the client computer. This certificate is private to the client only and should not be shared with any other computer. When asked to enter a common name, give the name that you chose for example in this case is Eve-laptop. Enter every necessary information as can be seen on the

screen shot below. This step could be repeated for as many client who will be connecting to the server. Note that same certificate name or common name do not have to register twice (See Graph 30). Finally one has to generate the Diffie Hellman Parameters using the command “build-dh” and the result is shown on Graph 31 below.

```

C:\Windows\system32\cmd.exe

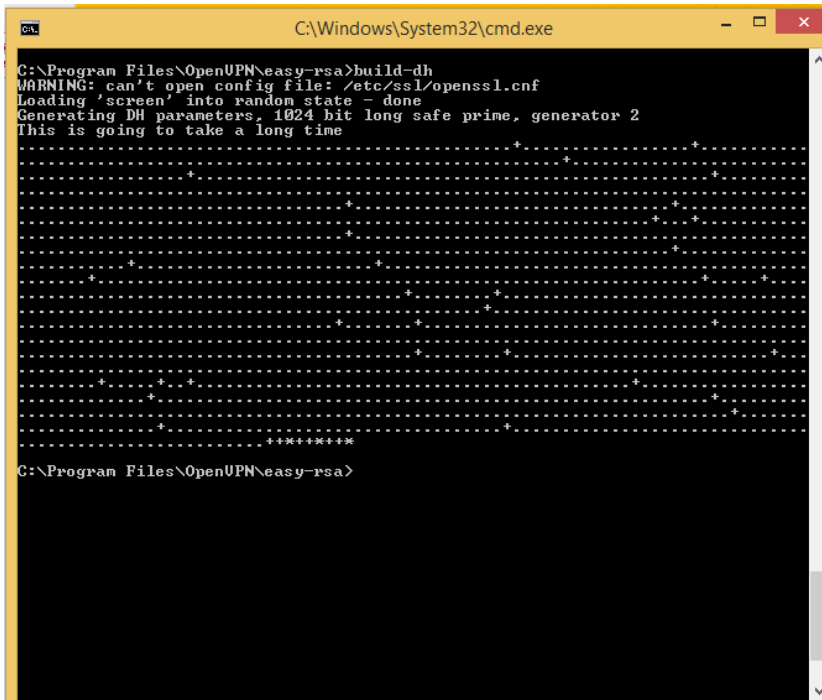
C:\Program Files\OpenVPN\easy-rsa>build-key Eve-laptop
WARNING: can't open config file: /etc/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'keys\Eve-laptop.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [Finland]:FI
State or Province Name (full name) [Osthrobothnia]:OS
Locality Name (eg, city) [Kokkola]:KL
Organization Name (eg, company) [OpenVPN]:M04
Organizational Unit Name (eg, section) [changeme]:OpenClient1
Common Name (eg, your name or your server's hostname) [changeme]:MyClient1
Name [changeme]:Client1
Email Address [bda_pris@yahoo.com]:bda_pris@yahoo.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:prizee
An optional company name []:M02
WARNING: can't open config file: /etc/ssl/openssl.cnf
Using configuration from openssl-1.0.0.cnf
Loading 'screen' into random state - done
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName          :PRINTABLE:'FI'
stateOrProvinceName  :PRINTABLE:'OS'
localityName         :PRINTABLE:'KL'
organizationName     :PRINTABLE:'M04'
organizationalUnitName:PRINTABLE:'OpenClient1'
commonName           :PRINTABLE:'MyClient1'
name                 :PRINTABLE:'Client1'
emailAddress         :IA5STRING:'bda_pris@yahoo.com'
Certificate is to be certified until Nov 30 17:02:32 2025 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]:y
Write out database with 1 new entries
Data Base Updated

```

GRAPH 30. Result of the build-key Eve-laptop command.



```

C:\Windows\System32\cmd.exe
C:\Program Files\OpenVPN\easy-rsa>build-dh
WARNING: can't open config file: /etc/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
+++++
C:\Program Files\OpenVPN\easy-rsa>

```

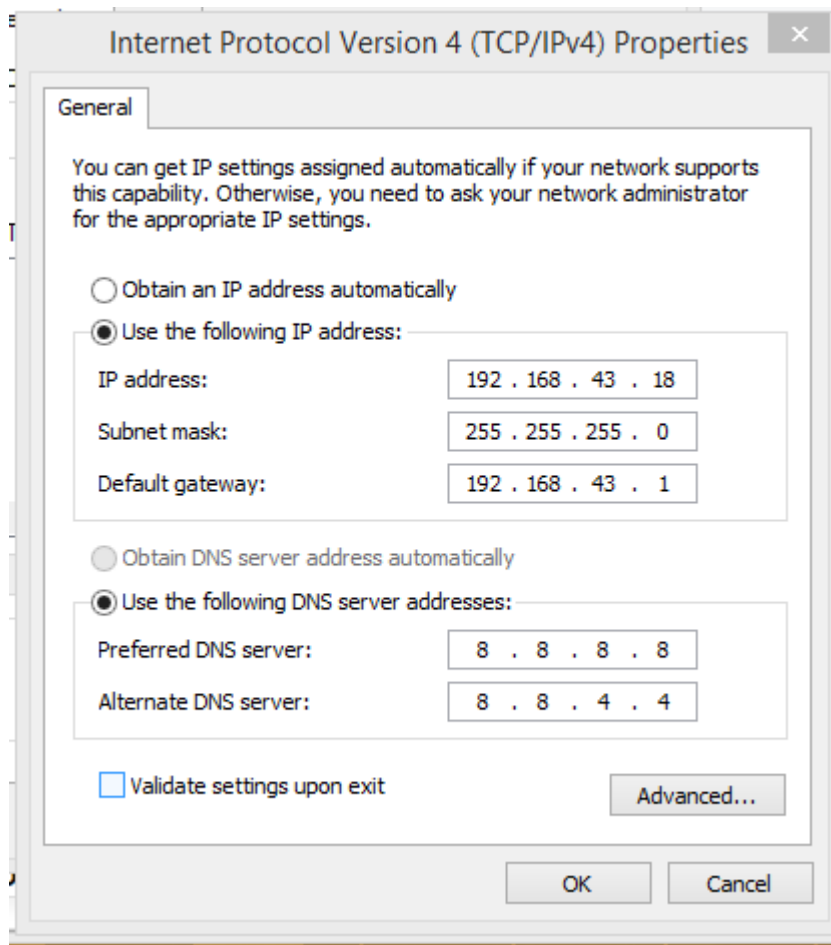
GRAPH 31. Result of the build-dh command.

After having all the configuration files which is generated in the directory “C:\Program Files\OpenVPN\easy-rsa\keys”, the next step is to edit the sample configuration file for server found in the directory “C:\Program Files\OpenVPN\sample-config”. Scroll down the file after opening it in a text editor and change the directories of ca.crt, server.crt, server.key and dh1024.pem to be in the directory “C:\ProgramFiles\OpenVPN\config\ca.crt”, “C:\ProgramFiles\OpenVPN\config\server.crt”, “C:\ProgramFiles\OpenVPN\config\server.key” and “C:\ProgramFiles\OpenVPN\config\dh1024.pem”, respectively. This file should be saved with .ovpn extension for example server.ovpn (see Appendix 2).

For the client, open the client file in a text editor like Notepad, scroll down and edit the lines with the following information ca.crt, client.crt and client.key so that they will be moved to the directory “C:\Program Files\OpenVPN\config\ca.crt”, “C:\ProgramFiles\OpenVPN\config\Eve-laptop.crt”, and “C:\Program Files\OpenVPN\config\ Eve-laptop.key”

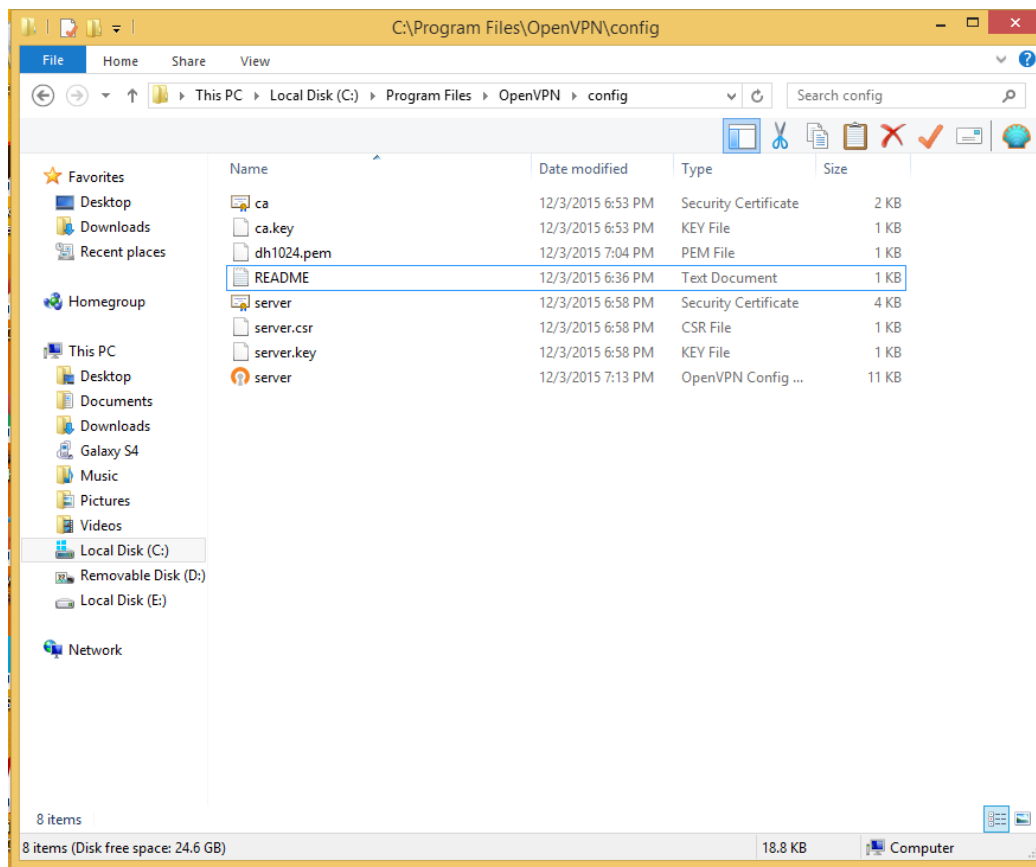
respectively. Also find the line with “remote my-server-1 1194” replace my-server-1 with the server’s static public address and leave the port number to 1194 which is the default port for Open VPN. Save the file as Eve-laptop.ovpn (see Appendix 3).

For help on how to set dynamic IP to static IP, go to Start Menu, Control Panel, Network and Sharing Center, Change adapter settings, right click on the current network that is been used and take properties then scroll down to Internet Protocol Version 4 (TCP/IPv4) and then click on properties then chose Use the following IP address enter your system’s IP address, subnet mask and default gateway. Also fill the Preferred DNS server (see Graph 32).

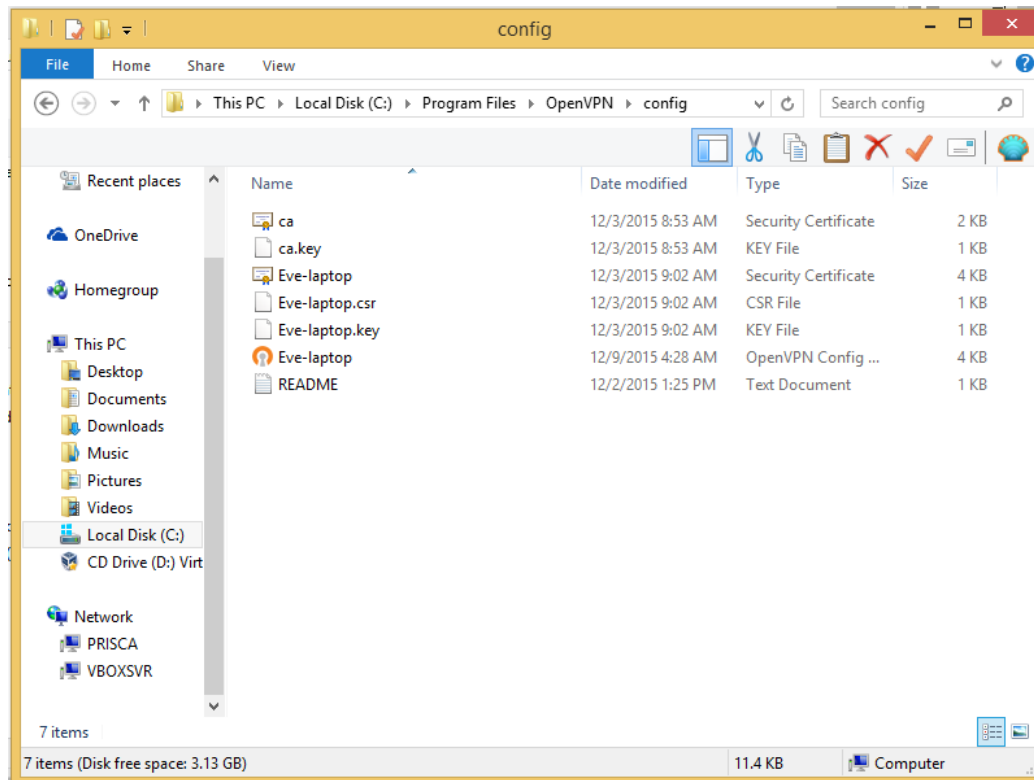


Graph 32. Set IP address.

The final step for the configuration is to move the files to the appropriate machines that will be connected to the server and their appropriate directories. That is the files ca.crt, dh1024.pem, server.crt, server.key, sever.ovpn should be copied from C:\Program Files\OpenVPN\easyrsa\key to C:\Program Files\OpenVPN\config\ on the server computer and for the client computer, ca.crt, Eve-laptop.crt, Eve-laptop.key, and Eve-laptop.ovpn should also be copied from C:\Program Files\OpenVPN\easyrsa\key on the server machine to C:\Program Files\OpenVPN\config\ on the client machine (see Graph 33 and 34 respectively).



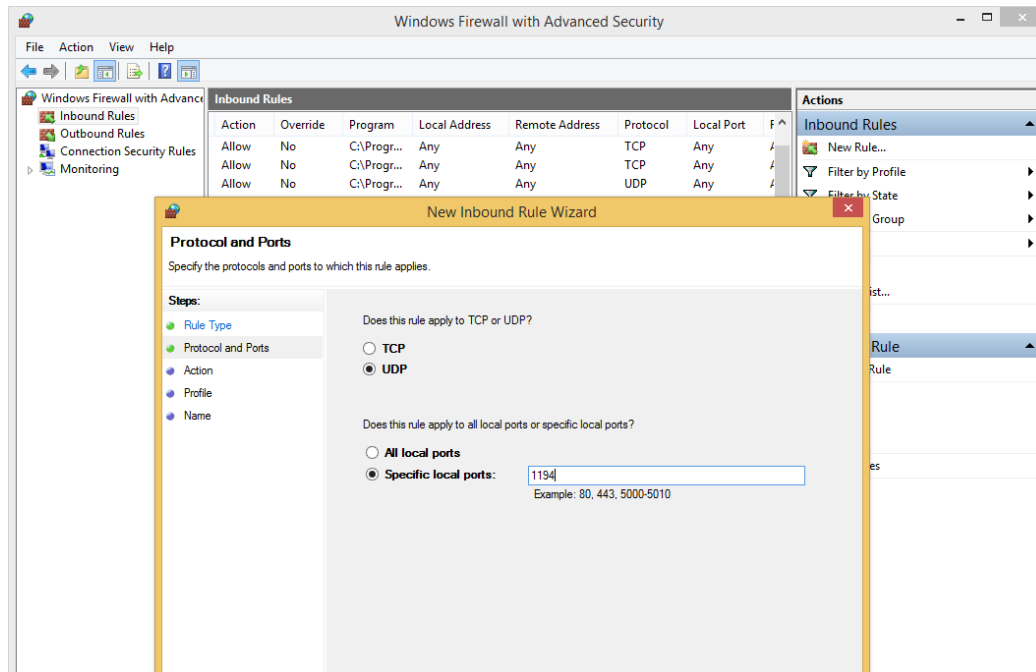
Graph 33. Content of C:\Program Files\OpenVPN\config\ for Server.



Graph 34. Content of C:\Program Files\OpenVPN\config\ for client (Eve-laptop).

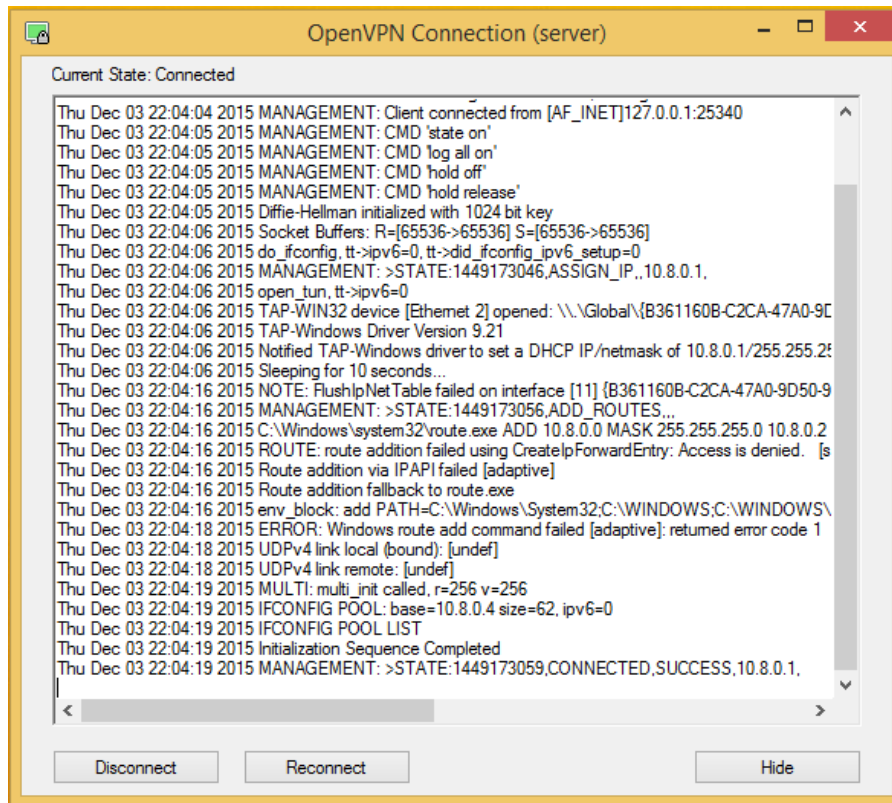
### 3.3 How to use OpenVPN

Now it is time to use the OpenVPN on both the client and server. But before one starts using the OpenVPN, first of all he has to set the firewall rule. This is done by navigating to Control Panel, Windows Firewall, Advanced settings, Inbound Rule, New Rule then enter the required information giving the name, select UDP port and also remember to set the port number to 1194 (See Graph 35).



GRAPH 35. Setting Firewall rule.

Another thing to take note of is the IP address of the client. The server uses the default IP address of 10.8.0.0/24. The client has to use a public IP address and the server must be up and working before the client can be ran. OpenVPN has a graphical user interface which will be launched from there by going to start menu, All Programs, then to OpenVPN and OpenVPN GUI. Right click on the icon and click Run As Administrator. This takes little time to open. OpenVPN will now connect to the server and it will be safe to use. It is going to provide an IP address which all traffic will use in the transmission process. The network's IP will be placed in this IP address and in this case the OpenVPN gave the IP address, 10.8.0.2. When the OpenVPN is started, wait for a few minutes until the lock icon at the top left hand turns green. Meaning the OpenVPN is connected. When finish using it, click disconnect to turn off the connection (see Graph 36).



GRAPH 36. Open VPN connected and running.

### 3.4 OpenVPN Testing Environment

Open VPN is designed to function on different networks and in the test case a laptop as the server and another laptop as the client on a different network and different service provider. The server's static public ip address was used when editing the client config file. Sonera internet service provider was used by the server while the client uses Saunalahti. Many problems were encountered and in many instances everything had to be uninstall and reinstall. Most of the problems were connectivity related. To solve the problem easily open the log file to see what the problem actually was. To open the log file start the OpenVPN and when it is running, right click on the icon on the task bar and click on View log. This helps to easily figure out the problem. Secondly use command line commands like ping "IP address" to test if there is connectivity between the server and client. If the ping result fail, then try to ping the gateway address and ensure that



the correct address is being pinged by typing `ipconfig /all` on the server command line to get the correct address. Also the command `telnet "public IP address" "port"` is to ensure that the computers are connected to each other through the OpenVPN port. This command is written on the client computer and if it fails, check on the client computer and check if there is a port rule created to allow traffic through the fire wall on the default port 1194 of OpenVPN. Another connectivity troubleshooting method used was the use of Wireshark. It captures where each traffic is coming from and where they are going to and also shows the protocol used.

## 4 DISCUSSION AND CONCLUSION

VPNs provide a convenient and cost-effective way for data transmission. VPNs are notorious for being difficult to configure. Data or information security is a very important aspect in the world of technology today and so should be handled with care. Site-to-site VPN are more secured and better to be used in companies rather than remote access. Every company today uses one kind of security method which best protect their data. They are also easy and economical to manage and maintain. There are many other security methods used by companies today with VPN such and anti-virus, anti-spyware and system upgrades and dead peer detection.

VPN must also implement rules for password refresh which could be after one month or in weeks. Rules for password creation which could be a combination of words and figures. The maximum number of login attempts (incorrect password) before the account is locked. The minimum delay between two connection attempts and the maximum number of connections that can be established simultaneously by a single user. OpenVPN is an open source VPN thus allowing anyone to contribute to its development and to ensure its top level of security. Many employees presently will like to connect to the company's server at every location and they may be in a situation where they would have to use the public internet connections such as those of a hotel or airport.

This topic is quite an interesting and a very sensitive topic especially in the area of networking and security. Despite all the efforts put in to see that the reseacher actually come out with something very useful and valuable, there were still limitations and shortcoming encountered in the process. The first problem was getting reliable materials which was quite a challenging part as well. Though there are a lots of materials on the website, getting real an authentic material was not an easy task because other sources needed to be compared with, such as books to be sure that

the information written down is actually correct. For further research could be on the factors that affect OpenVPN, comparison on the different types of VPN, and the latest developments in OpenVPN.

## 5 REFERENCES

Balchunas, A. 2007. Open Shortest Path First. California. O'Reilly Media

Bauer, J. Liebscher, A. Klaus, T.R. 2006. OpenVPN Grundlagen Konfiguration. Paris. Roubaix.

Community Forum. 2002. OpenVPN Technologies. Pleasanton. United States. <https://openvpn.net/index.php/open-source/documentation/howto.html>. September 2015

Eric, F. Crist, B. & Keijser, J. August 2015. Mastering OpenVPN. Packt Publishing Ltd, UK

Erwin, M. Scott, C. & Wolfe, P. 1999. Virtual Private Network. Chicago. Chicago Review Press.

Feilner, M. & Graf, N. 2009. Build and Integrate Virtual Private Using OpenVPN. London. Packet Publishing Ltd.

Hosner, C. 2004. OpenVPN and the SSL VPN Revolution. London. Springer-Verlag

Internet-Computer-Security.com. 2008. Available: <http://www.internet-computer-security.com/>. August 2015.

Keijser, J. 2011. OpenVPN 2 Cookbook. UK. Packt Publishing Ltd.

Lambert M. Surhone, Miriam T. Timplendon & Susan F. Marseken. 2010. Virtual Private Network Pre-Shared Key Certificate Authority Transport Layer Security. Saarbrücken. Betascript Publishing

Olton & Birmingham. 2015. OpenVPN 2 Cookbook. London. Packt Publishing.

Schneier, B. & Mudge. 2011. Cryptanalysis of Microsoft. Minneapolis. Coffee House Press.

Tyson J & Crawford S. 2011. How VPNs work. London. Packt Publishing.

## APPENDICES

### Appendix 1/1

Here is a summary of all the configurations that has been made.

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\System32>cd "C:\Program Files\OpenVPN\easy-rsa"

C:\Program Files\OpenVPN\easy-rsa>init-config

C:\Program Files\OpenVPN\easy-rsa>copy vars.bat.sample vars.bat
    1 file(s) copied.

C:\Program Files\OpenVPN\easy-rsa>notepad vars.bat

C:\Program Files\OpenVPN\easy-rsa>vars

C:\Program Files\OpenVPN\easy-rsa>clean-all
The system cannot find the file specified.
    1 file(s) copied.
    1 file(s) copied.

C:\Program Files\OpenVPN\easy-rsa>build-ca
WARNING: can't open config file: /etc/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
..+++++
.....+++++
writing new private key to 'keys\ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [Finland]:FI
State or Province Name (full name) [Osthrobothnia]:OS
Locality Name (eg, city) [Kokkola]:KL
Organization Name (eg, company) [OpenVPN]:MO4
Organizational Unit Name (eg, section) [changeme]:OpenServer
Common Name (eg, your name or your server's hostname) [changeme]:MyServer
Name [changeme]:Server
Email Address [bda_pris@yahoo.com]:bda_pris@yahoo.com

C:\Program Files\OpenVPN\easy-rsa>build-key-server server
WARNING: can't open config file: /etc/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....+++++
.....+++++ (OpenVPN.net.)
writing new private key to 'keys\server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
```

## Appendix 1/2

What you are about to enter is what is called a Distinguished Name or a DN.  
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.

```
-----
Country Name (2 letter code) [Finland]:FI
State or Province Name (full name) [Osthrobothnia]:OS
Locality Name (eg, city) [Kokkola]:KL
Organization Name (eg, company) [OpenVPN]:MO4
Organizational Unit Name (eg, section) [changeme]:OpenServer1
Common Name (eg, your name or your server's hostname) [changeme]:MyServer1
Name [changeme]:Server1
Email Address [bda_pris@yahoo.com]:bda_pris@yahoo.com
```

Please enter the following 'extra' attributes  
to be sent with your certificate request

```
A challenge password []:prizee
An optional company name []:MO1
WARNING: can't open config file: /etc/ssl/openssl.cnf
Using configuration from openssl-1.0.0.cnf
Loading 'screen' into random state - done
Check that the request matches the signature
Signature ok
```

The Subject's Distinguished Name is as follows

```
countryName      :PRINTABLE:'FI'
stateOrProvinceName :PRINTABLE:'OS'
localityName     :PRINTABLE:'KL'
organizationName  :PRINTABLE:'MO4'
organizationalUnitName:PRINTABLE:'OpenServer1'
commonName       :PRINTABLE:'MyServer1'
name             :PRINTABLE:'Server1'
emailAddress     :IA5STRING:'bda_pris@yahoo.com'
Certificate is to be certified until Nov 30 16:58:11 2025 GMT (3650 days)
Sign the certificate? [y/n]:y
```

1 out of 1 certificate requests certified, commit? [y/n]y

Write out database with 1 new entries

Data Base Updated

```
C:\Program Files\OpenVPN\easy-rsa>build-key Eve-laptop
```

```
WARNING: can't open config file: /etc/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
```

```
.....+++++
.....+++++
writing new private key to 'keys\Eve-laptop.key'
```

```
-----
You are about to be asked to enter information that will be incorporated  
into your certificate request.
```

What you are about to enter is what is called a Distinguished Name or a DN.  
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.

```
-----
Country Name (2 letter code) [Finland]:FI
State or Province Name (full name) [Osthrobothnia]:OS
Locality Name (eg, city) [Kokkola]:KL
Organization Name (eg, company) [OpenVPN]:MO4
Organizational Unit Name (eg, section) [changeme]:OpenClient1
Common Name (eg, your name or your server's hostname) [changeme]:MyClient1
Name [changeme]:Client1
Email Address [bda_pris@yahoo.com]:bda_pris@yahoo.com(OpenVPN.net.)
```





## Appendix 2/1

```
#####  
# Sample OpenVPN 2.0 config file for      #  
# multi-client server.                    #  
#                                         #  
# This file is for the server side        #  
# of a many-clients <-> one-server       #  
# OpenVPN configuration.                  #  
#                                         #  
# OpenVPN also supports                   #  
# single-machine <-> single-machine      #  
# configurations (See the Examples page   #  
# on the web site for more info).        #  
#                                         #  
# This config should work on Windows     #  
# or Linux/BSD systems. Remember on      #  
# Windows to quote pathnames and use     #  
# double backslashes, e.g.:              #  
# "C:\\Program Files\\OpenVPN\\config\\foo.key" #  
#                                         #  
# Comments are preceded with '#' or ';'   #  
#####  
  
# Which local IP address should OpenVPN  
# listen on? (optional)  
;local a.b.c.d  
  
# Which TCP/UDP port should OpenVPN listen on?  
# If you want to run multiple OpenVPN instances
```

## Appendix 2 /2

```
# on the same machine, use a different port  
# number for each one. You will need to  
# open up this port on your firewall.  
port 1194  
# TCP or UDP server?  
;proto tcp  
proto udp  
# "dev tun" will create a routed IP tunnel,  
# "dev tap" will create an ethernet tunnel.  
# Use "dev tap0" if you are ethernet bridging  
# and have precreated a tap0 virtual interface  
# and bridged it with your ethernet interface.  
# If you want to control access policies  
# over the VPN, you must create firewall  
# rules for the the TUN/TAP interface.  
# On non-Windows systems, you can give  
# an explicit unit number, such as tun0.  
# On Windows, use "dev-node" for this.  
# On most systems, the VPN will not function  
# unless you partially or fully disable  
# the firewall for the TUN/TAP interface.  
;dev tap  
dev tun  
# Windows needs the TAP-Win32 adapter name  
# from the Network Connections panel if you  
# have more than one. On XP SP2 or higher,  
# you may need to selectively disable the  
# Windows firewall for the TAP adapter.  
# Non-Windows systems usually don't need this.  
;dev-node MyTap  
# SSL/TLS root certificate (ca), certificate(OpenVPN.net.)
```

## Appendix 2/3

```
# (cert), and private key (key). Each client  
# and the server must have their own cert and  
# key file. The server and all clients will  
# use the same ca file.  
#  
# See the "easy-rsa" directory for a series  
# of scripts for generating RSA certificates  
# and private keys. Remember to use  
# a unique Common Name for the server  
# and each of the client certificates.  
#  
# Any X509 key management system can be used.  
# OpenVPN can also use a PKCS #12 formatted key file  
# (see "pkcs12" directive in man page).  
ca "C:\\Program Files\\OpenVPN\\config\\ca.crt"  
cert "C:\\Program Files\\OpenVPN\\config\\server.crt"  
key "C:\\Program Files\\OpenVPN\\config\\server.key" # This file should be kept secret  
# Diffie hellman parameters.  
# Generate your own with:  
# openssl dhparam -out dh2048.pem 2048  
dh "C:\\Program Files\\OpenVPN\\config\\dh1024.pem"  
# Network topology  
# Should be subnet (addressing via IP)  
# unless Windows clients v2.0.9 and lower have to  
# be supported (then net30, i.e. a /30 per client)  
# Defaults to net30 (not recommended)  
;topology subnet  
# Configure server mode and supply a VPN subnet  
# for OpenVPN to draw client addresses from.  
# The server will take 10.8.0.1 for itself,  
# the rest will be made available to clients. (OpenVPN.net.)
```

## Appendix 2/4

```
# Each client will be able to reach the server
# on 10.8.0.1. Comment this line out if you are
# ethernet bridging. See the man page for more info.
server 10.8.0.0 255.255.255.0
# Maintain a record of client <-> virtual IP address
# associations in this file. If OpenVPN goes down or
# is restarted, reconnecting clients can be assigned
# the same virtual IP address from the pool that was
# previously assigned.
ifconfig-pool-persist ipp.txt

# Configure server mode for ethernet bridging.
# You must first use your OS's bridging capability
# to bridge the TAP interface with the ethernet
# NIC interface. Then you must manually set the
# IP/netmask on the bridge interface, here we
# assume 10.8.0.4/255.255.255.0. Finally we
# must set aside an IP range in this subnet
# (start=10.8.0.50 end=10.8.0.100) to allocate
# to connecting clients. Leave this line commented
# out unless you are ethernet bridging.
;server-bridge 10.8.0.4 255.255.255.0 10.8.0.50 10.8.0.100

# Configure server mode for ethernet bridging
# using a DHCP-proxy, where clients talk
# to the OpenVPN server-side DHCP server
# to receive their IP address allocation
# and DNS server addresses. You must first use
# your OS's bridging capability to bridge the TAP
# interface with the ethernet NIC interface.
# Note: this mode only works on clients (such as
# Windows), where the client-side TAP adapter is(OpenVPN.net.)
```

## Appendix 2/5

```
# bound to a DHCP client.
;server-bridge

# Push routes to the client to allow it
# to reach other private subnets behind
# the server. Remember that these
# private subnets will also need
# to know to route the OpenVPN client
# address pool (10.8.0.0/255.255.255.0)
# back to the OpenVPN server.
;push "route 192.168.10.0 255.255.255.0"
;push "route 192.168.20.0 255.255.255.0"
# To assign specific IP addresses to specific
# clients or if a connecting client has a private
# subnet behind it that should also have VPN access,
# use the subdirectory "ccd" for client-specific
# configuration files (see man page for more info).
# EXAMPLE: Suppose the client
# having the certificate common name "Thelonious"
# also has a small subnet behind his connecting
# machine, such as 192.168.40.128/255.255.255.248.
# First, uncomment out these lines:
;client-config-dir ccd
;route 192.168.40.128 255.255.255.248
# Then create a file ccd/Thelonious with this line:
# iroute 192.168.40.128 255.255.255.248
# This will allow Thelonious' private subnet to
# access the VPN. This example will only work
# if you are routing, not bridging, i.e. you are
# using "dev tun" and "server" directives.
# EXAMPLE: Suppose you want to give
# Thelonious a fixed VPN IP address of 10.9.0.1. (OpenVPN.net.)
```

## Appendix 2/6

*# First uncomment out these lines:*

```
;client-config-dir ccd
```

```
;route 10.9.0.0 255.255.255.252
```

*# Then add this line to ccd/TheIonious:*

```
# ifconfig-push 10.9.0.1 10.9.0.2
```

*# Suppose that you want to enable different*

*# firewall access policies for different groups*

*# of clients. There are two methods:*

*# (1) Run multiple OpenVPN daemons, one for each*

*# group, and firewall the TUN/TAP interface*

*# for each group/daemon appropriately.*

*# (2) (Advanced) Create a script to dynamically*

*# modify the firewall in response to access*

*# from different clients. See man*

*# page for more info on learn-address script.*

```
;learn-address ./script
```

*# If enabled, this directive will configure*

*# all clients to redirect their default*

*# network gateway through the VPN, causing*

*# all IP traffic such as web browsing and*

*# and DNS lookups to go through the VPN*

*# (The OpenVPN server machine may need to NAT*

*# or bridge the TUN/TAP interface to the internet*

*# in order for this to work properly).*

```
;push "redirect-gateway def1 bypass-dhcp"
```

*# Certain Windows-specific network settings*

*# can be pushed to clients, such as DNS*

*# or WINS server addresses. CAVEAT:*

*# <http://openvpn.net/faq.html#dhcpcaveats>*

*# The addresses below refer to the public*

*# DNS servers provided by [opendns.com](http://opendns.com). (OpenVPN.net.)*

## Appendix 2/7

```
;push "dhcp-option DNS 208.67.222.222"
;push "dhcp-option DNS 208.67.220.220"
# Uncomment this directive to allow different
# clients to be able to "see" each other.
# By default, clients will only see the server.
# To force clients to only see the server, you
# will also need to appropriately firewall the
# server's TUN/TAP interface.

;client-to-client
# Uncomment this directive if multiple clients
# might connect with the same certificate/key
# files or common names. This is recommended
# only for testing purposes. For production use,
# each client should have its own certificate/key
# pair.
#
# IF YOU HAVE NOT GENERATED INDIVIDUAL
# CERTIFICATE/KEY PAIRS FOR EACH CLIENT,
# EACH HAVING ITS OWN UNIQUE "COMMON NAME",
# UNCOMMENT THIS LINE OUT.

;duplicate-cn
# The keepalive directive causes ping-like
# messages to be sent back and forth over
# the link so that each side knows when
# the other side has gone down.
# Ping every 10 seconds, assume that remote
# peer is down if no ping received during
# a 120 second time period.

keepalive 10 120
# For extra security beyond that provided
# by SSL/TLS, create an "HMAC firewall"(OpenVPN.net.)
```

## Appendix 2/8

```
# to help block DoS attacks and UDP port flooding.  
  
#  
  
# Generate with:  
# openvpn --genkey --secret ta.key  
  
#  
  
# The server and each client must have  
# a copy of this key.  
# The second parameter should be '0'  
# on the server and '1' on the clients.  
;tls-auth ta.key 0 # This file is secret  
# Select a cryptographic cipher.  
# This config item must be copied to  
# the client config file as well.  
;cipher BF-CBC # Blowfish (default)  
;cipher AES-128-CBC # AES  
;cipher DES-EDE3-CBC # Triple-DES  
# Enable compression on the VPN link.  
# If you enable it here, you must also  
# enable it in the client config file.  
comp-lzo  
# The maximum number of concurrently connected  
# clients we want to allow.  
;max-clients 100  
# It's a good idea to reduce the OpenVPN  
# daemon's privileges after initialization.  
#  
# You can uncomment this out on  
# non-Windows systems.  
;user nobody  
;group nobody  
# The persist options will try to avoid(OpenVPN.net.)
```



## Appendix 2/9

```
# accessing certain resources on restart
# that may no longer be accessible because
# of the privilege downgrade.
persist-key
persist-tun

# Output a short status file showing
# current connections, truncated
# and rewritten every minute.
status openvpn-status.log

# By default, log messages will go to the syslog (or
# on Windows, if running as a service, they will go to
# the "\Program Files\OpenVPN\log" directory).
# Use log or log-append to override this default.
# "log" will truncate the log file on OpenVPN startup,
# while "log-append" will append to it. Use one
# or the other (but not both).
;log    openvpn.log
;log-append openvpn.log

# Set the appropriate level of log
# file verbosity.
#
# 0 is silent, except for fatal errors
# 4 is reasonable for general usage
# 5 and 6 can help to debug connection problems
# 9 is extremely verbose
verb 3

# Silence repeating messages. At most 20
# sequential messages of the same message
# category will be output to the log.
;mute 20(OpenVPN.net.)
```

## Appendix 3/1

#####

*# Sample client-side OpenVPN 2.0 config file #*

*# for connecting to multi-client server. #*

*# #*

*# This configuration can be used by multiple #*

*# clients, however each client should have #*

*# its own cert and key files. #*

*# #*

*# On Windows, you might want to rename this #*

*# file so it has a .ovpn extension #*

#####

*# Specify that we are a client and that we*

*# will be pulling certain config file directives*

*# from the server.*

*client*

*# Use the same setting as you are using on*

*# the server.*

*# On most systems, the VPN will not function*

*# unless you partially or fully disable*

*# the firewall for the TUN/TAP interface.*

*;dev tap*

*dev tun*

*# Windows needs the TAP-Win32 adapter name*

*# from the Network Connections panel*

*# if you have more than one. On XP SP2,*

*# you may need to disable the firewall*

*# for the TAP adapter.*

*;dev-node MyTap*

*# Are we connecting to a TCP or(OpenVPN.net.)*

## Appendix 3/2

```
# UDP server? Use the same setting as
# on the server.

;proto tcp
proto udp

# The hostname/IP and port of the server.

# You can have multiple remote entries
# to load balance between the servers.
remote 188.238.113.217 1194
;remote my-server-2 1194

# Choose a random host from the remote
# list for load-balancing. Otherwise
# try hosts in the order specified.
;remote-random

# Keep trying indefinitely to resolve the
# host name of the OpenVPN server. Very useful
# on machines which are not permanently connected
# to the internet such as laptops.
resolv-retry infinite

# Most clients don't need to bind to
# a specific local port number.
nobind

# Downgrade privileges after initialization (non-Windows only)
;user nobody
;group nobody

# Try to preserve some state across restarts.
persist-key
persist-tun

# If you are connecting through an
# HTTP proxy to reach the actual OpenVPN
# server, put the proxy server/IP and
# port number here. See the man page (OpenVPN.net.)
```

## Appendix 3/3

```
# if your proxy server requires
# authentication.

;http-proxy-retry # retry on connection failures
;http-proxy [proxy server] [proxy port #]
# Wireless networks often produce a lot
# of duplicate packets. Set this flag
# to silence duplicate packet warnings.
;mute-replay-warnings

# SSL/TLS parms.

# See the server config file for more
# description. It's best to use
# a separate .crt/.key file pair
# for each client. A single ca
# file can be used for all clients.
ca "C:\Program Files\OpenVPN\config\ca.crt"
cert "C:\Program Files\OpenVPN\config\Eve-laptop.crt"
key "C:\Program Files\OpenVPN\config\Eve-laptop.key"
# Verify server certificate by checking that the
# certificate has the correct key usage set.
# This is an important precaution to protect against
# a potential attack discussed here:
# http://openvpn.net/howto.html#mitm
#
# To use this feature, you will need to generate
# your server certificates with the keyUsage set to
# digitalSignature, keyEncipherment
# and the extendedKeyUsage to
# serverAuth
# EasyRSA can do this for you.
remote-cert-tls server
# If a tls-auth key is used on the server
```

## Appendix 3/4

*# then every client must also have the key.*

*;tls-auth ta.key 1*

*# Select a cryptographic cipher.*

*# If the cipher option is used on the server*

*# then you must also specify it here.*

*;cipher x*

*# Enable compression on the VPN link.*

*# Don't enable this unless it is also*

*# enabled in the server config file.*

*comp-lzo*

*# Set log file verbosity.*

*verb 3*

*# Silence repeating messages*

*;mute 20 (OpenVPN.net.)*