Open source system OpenVPN in a function of Virtual Private Network

A Skendzic[1] and B Kovacic[2]

[1]Politehnica “Nikola Tesla” in Gospic, Bana Ivana Karlovica 16, 53000 Gospic, Croatia
[2]University of Rijeka, Department of Informatics, Radmile Matejcic 5, Rijeka, 51000, Croatia

E-mail: wireless82@gmail.com

Abstract. Using of Virtual Private Networks (VPN) can establish high security level in network communication. VPN technology enables high security networking using distributed or public network infrastructure. VPN uses different security and managing rules inside networks. It can be set up using different communication channels like Internet or separate ISP communication infrastructure. VPN private network makes security communication channel over public network between two endpoints (computers). *OpenVPN* is an *open source* software product under GNU General Public License (GPL) that can be used to establish VPN communication between two computers inside business local network over public communication infrastructure. It uses special security protocols and 256-bit Encryption and it is capable of traversing network address translators (NATs) and firewalls. It allows computers to authenticate each other using a pre-shared secret key, certificates or username and password. This work gives review of VPN technology with a special accent on *OpenVPN*. This paper will also give comparison and financial benefits of using open source VPN software in business environment.

1. Introduction

Virtual Private Networks (VPN) can be used to establish a high level of security in network communication. VPN technology enables high-security networking using distributed or public network infrastructure. VPN uses various security mechanisms and rules within a network. It can be set up using different communication channels, such as Internet or separate ISP communication infrastructure. VPN establishes a security communication channel over public network between two endpoints (computers). OpenVPN is an open source software product under GNU General Public License (GPL) that can be used to establish VPN communication between two computers within business local network using public communication infrastructure [1]. This paper provides a basic overview of the way in which VPN technology works, gives information on GNU GPL for OpenVPN tool and its benefits, demonstrates general benefits of OpenVPN tool compared to other similar software solutions, provides an explanation of security level and finally conclusion.

2. Virtual Private Network

Internet, as a communication platform, is a basic communication system today. In addition to many different services relying on Internet infrastructure, Virtual Private Network (hereinafter:VPN) is a very efficient and economical method of communication, especially when connecting remote (virtual) offices. VPN technology transmits potentially “sensitive” information, which can be classified as secret or confidential through insecure networks. VPN system is based on setting up of so-called “communication tunnels”, previously secured using various cryptographic methods (algorithms).

VPN is basically divided into two types [2]:

1. *Site-to-Site* – an example of such connection would be a company branch that needs to be continuously or occasionally connected to the main location (Figure 2)
2. *Remote Access VPN* – used occasionally for connecting individual users to the company server from mobile phones or in cases where an employee works from home (Figure 1).

Internet is not the only option for establishing a VPN connection, we can use many other technologies such as ATM network or private Internet service provider (ISP) network. However, Internet infrastructure offers several advantages over ATM or private ISP networks [2]:

- more affordable,
- greater mobility,
- transparent communication.

In order to establish a VPN connection, the following requirements need to be met [2]:

- confidentiality - protection from unauthorised access to information,
- data integrity - protection of unauthorised modification of data,
- user authentication - verifying the identity of computers or devices at the ends of the tunnel.

The main advantage of using Internet communication for the VPN service is its price. Available VPN services can be completely free [3] (such as HotSpot Shield, CyberGhost, Tunnel Bear, Spot Flux, with several restrictions), while others are subject to charge and require additional training of persons (administrators) to administer such services.

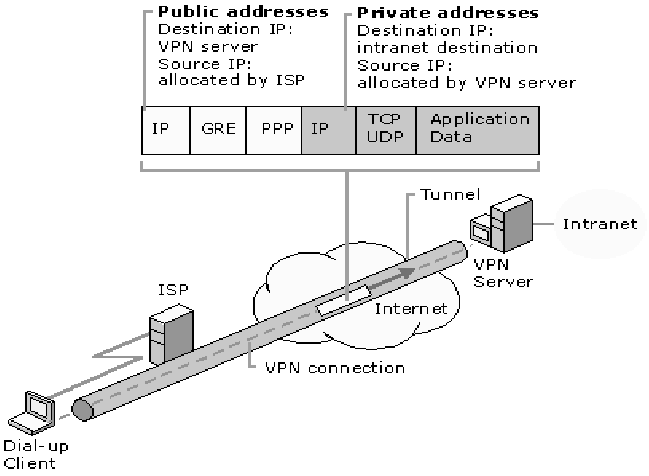


Figure 1. Overview of functioning of a Remote Access VPN network [4]

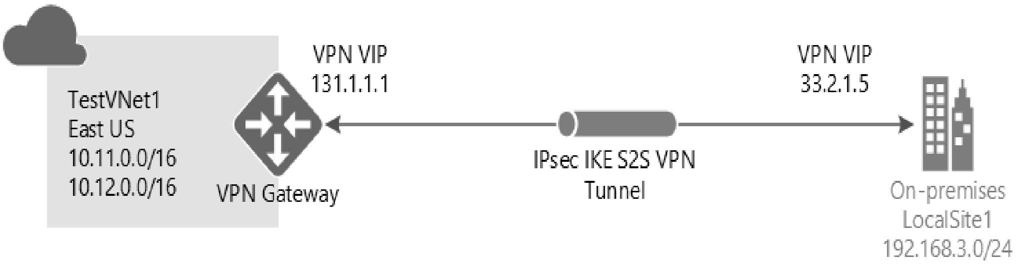


Figure 2. Overview of functioning of Site-To-Site VPN network [5]

3. GNU General Public License

GNU General Public License (hereinafter: GNU GPL) includes sharing and changing of open source software. GNU GPL also introduces certain guarantees that make software free for use [6]. Software under GNU GPL means that it can be copied, shared and distributed. Likewise, there are no limitations regarding the number of copies or the number of computers on which the software can be run. On the other hand, to protect the rights of the ones enabling the use of software under GNU GPL, certain obligations are imposed in case of distribution or modification [5]. When flexibility and limited scopes of software licenses such as EULA are compared to GNU GPL, it is evident that there are clear differences in limiting user rights, assigning user rights and limiting the right to lodge a complaint.

Studies [6] have shown that the following ratios are obtained when EULA[1] license is compared to GNU GPL:

Table 1. EULA – GNU GPL flexibility and limitations

Limitations	EULA	GNU GPL
Limiting user rights	45%	27%
Assigning user rights	15%	51%
iting the right to lodge a complaint	40%	22%

In conclusion, GNU GPL provides users with greater flexibility. User rights are less limited, more rights are assigned, and there are fewer limitations for lodging complaints.

4. OpenVPN

Private network is a new communication model enabling a more flexible and economical communication between employees within a company or within a partnership, that is, a complementary business system [7]. Companies can choose one of the models of setting up a VPN, whether they will take a turnkey service, build a network themselves or, in case of less demanding actions, use free software for setting up a VPN [7].

OpenVPN is also available for other platforms such as MS Windows, even though the benefit of using *OpenVPN* solution comes from the benefit of migrating the business VPN system to Linux platform. Some of the benefits of Linux solution can be [8]:

- robustness,
- flexibility,
- security,
- easy maintenance,
- price.

OpenVPN tool uses SSL/TLS protocol to encrypt data, creating a virtual tunnel between the endpoints. One of the particularities of *OpenVPN* tool is that it does not use a web browser installed on a client computer. Instead, *OpenVPN* package needs to be installed both server-side and client-side.

Advantages of *OpenVPN* tool over other tools can be seen from the following:

- Easy adjustment,
- Possibility of adjustment via script file in order to meet the user’s needs,
- Portability, it is available for almost all popular operating systems,

[1] End User License Agreement (EULA) is an agreement between the software developer and the end user. In essence, it significantly differs from GNU GPL. EULA limits the possibilities and rights of users and releases the software developer from any liability.

- Directing network traffic to UDP[2] port 1194 or other. UDP protocol works on the “fire and forget” principle, which means it does not check whether the message reached the receiver, instead it sends short “datagrams” and checks for errors during sending, which results in faster data transmission,
- By using additional software (TUN or TAP), *OpenVPN* orders other applications to communicate only through the created virtual network interface, in a fully automated manner,
- *OpenVPN* enables secure user authentication using a public (static) key, corresponding certificate or user name and password,
- Use of *OpenVPN* also includes membership in a broad user community providing support and suggesting and adding new functionalities.

Table 2. Software for OpenVPN [2]

Software name	Operating system	Price
OpenVPN GUI	Microsoft Windows	Free of charge
Tunnelblick	Mac OS X	Free of charge
Viscosity	Mac OS X	13.95 €
Shimo	Mac OS X	9 $
OpenVPN	DD-WRT	Free of charge
TomatoVPN	Tomato	Free of charge
TunnelDroid	Android	Free of charge

Table 2 provides the overview of software for *OpenVPN*. It should be noted that some network and communication equipment manufacturers integrate *OpenVPN* into their firmware, which means the installation of *OpenVPN* to computers within the network is not necessary.

4.1. OpenVPN and security

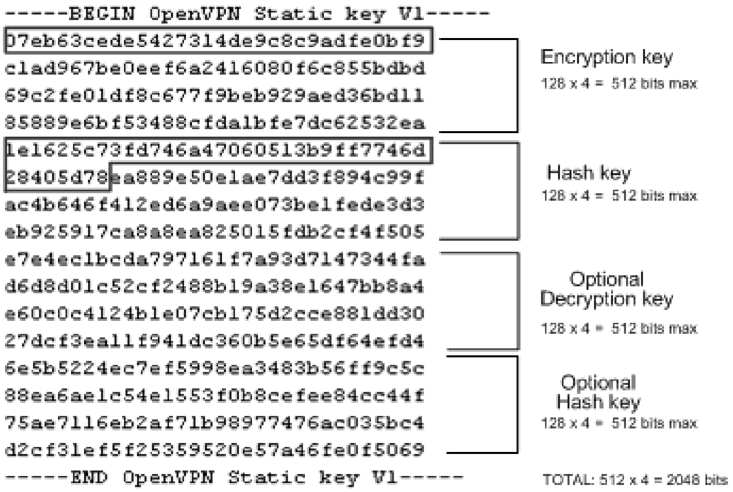
As it was pointed out earlier, the protection of data in *OpenVPN* is based on encryption using symmetric and asymmetric algorithms. Hash function is used to protect message integrity, as well as for digital signatures. Symmetric cryptographic systems use the same secret key for both encryption and decryption of data. The problem of using symmetric cryptographic systems lies in the process of agreement, that is, of key exchange, which in this case goes through an insecure communication channel (e.g. Internet). Asymmetric cryptographic systems are a more reliable method of cryptographic protection because they use both public and private keys. Private key is known only to his owner, while public key is distributed to all users communicating within a VPN network. Public and private keys and their owners are part of so-called PKI (Public Key Infrastructure), which also includes digital signatures and digital certificates.

Table 3 provides the comparison between symmetric and asymmetric keys within OpenSSL Library.

Table 3. *OpenVPN* and use of SSL Library. Comparison between the use of symmetric and asymmetric keys [2]

OpenVPN	Use of static key	Use of OpenSSL Library
Encryption algorithm	Symmetric	Asymmetric
Application	Simple	Complicated
Speed	Higher	Lower
CPU usage	Lower	Higher
User authentication	No	Yes
Key exchange problem	Yes	No

[2] **UDP** (**User Datagram Protocol**) is a protocol in the transport layer of OSI model, and in addition to TCP, it is one of the basic Internet protocols.



```
-----BEGIN OpenVPN Static key V1-----
07eb63cede5427314de9c8c9adfe0bf9
c1ad967be0eef6a2416080f6c855bdbd
69c2fe01df8c677f9beb929aed36bd11
85889e6bf53488cfda1bfe7dc62532ea
1e1625c73fd746a47060513b9ff7746d
28405d78ea889e50e1ae7dd3f894c99f
ac4b646f412ed6a9aee073be1fede3d3
eb925917ca8a8ea825015fdb2cf4f505
e7e4ec1bcda797161f7a93d7147344fa
d6d8d01c52cf2488b19a38e1647bb8a4
e60c0c4124b1e07cb175d2cce881dd30
27dcf3ea11f941dc360b5e65df64efd4
6e5b5224ec7ef5998ea3483b56ff9c5c
88ea6ae1c54e1553f0b8cefee84cc44f
75ae7116eb2af71b98977476ac035bc4
d2cf31ef5f25359520e57a46fe0f5069
-----END OpenVPN Static key V1-----
```

Figure 3. Randomly generated 2048-bit encryption key.
Overview of encryption key structure [9]

4.2. *OpenVPN and security*

OpenVPN also uses *OpenSSL* program package for its work. In general, SSL (Secure Sockets Layer) is a general security standard, and by using SSL the connection between a web server and a browser is encrypted, which is very important in Internet business environment from the aspect of security [10]. *OpenSSL* provides cryptographic support implemented in form of SSL and TLS security protocols. These are SSL v2 and v3, and TLS (Transport Layer Security) v1. Data encrypted using SSL/TSL technology are not visible, nor can they be intercepted or deciphered within a communication channel (Figure 3). *OpenSSL* can be upgraded within *OpenVPN* in case a new version arrives.

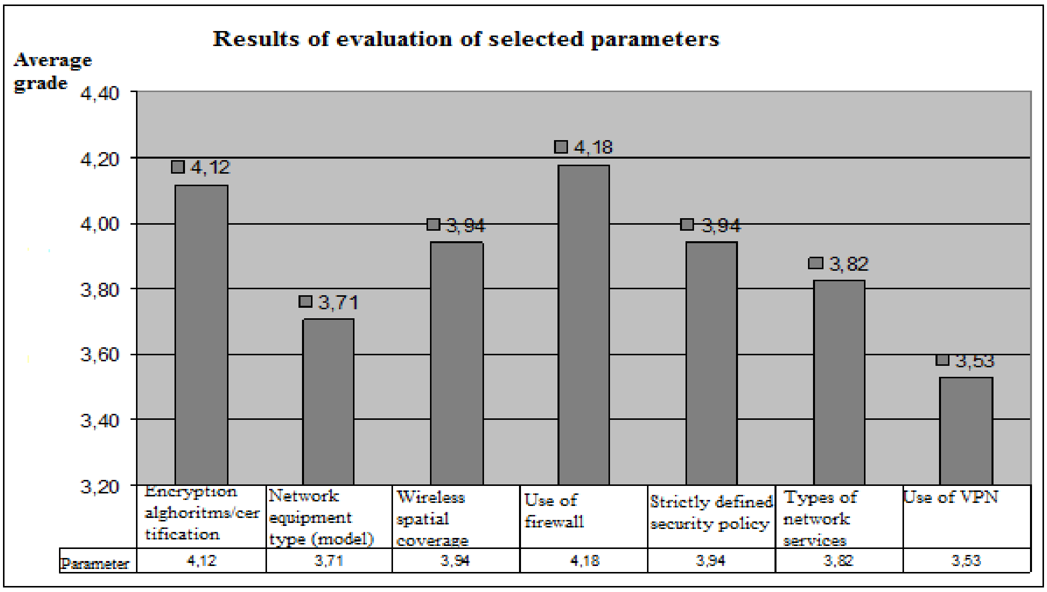


Figure 4. Results of evaluating satisfaction of network administrators with selected parameters in the system model (average values) [11]

Figure 4 shows the results of research[3] on a sample of system engineers (CARNet) who evaluated security parameters that influence the overall security of network communication. Based on the significance expressed for each criterion, weighted values for each criterion (grades 1-5) were established. Since the weighted values obtained were different for each criterion, it was established that different criteria had different influence on the final result of security evaluation. The result achieved by the parameter "Use of VPN" should be singled out, with average result of 3.53. It can be concluded that the sample of subjects on average evaluated the use of virtual private networks in communication as "very good" when it comes to security. This suggests that the use of VPN in combination with a firewall and a clearly defined security policy would achieve an even higher grade regarding security and the use of VPN.

5. Comparison between OpenVPN and SoftEther

Although there are many different software VPN solutions on the market, each solution has its own advantages and disadvantages [12]. It is up to the user to choose the most appropriate solution in line with the user's need, as well as possibilities. SoftEther solution can be given as an example for comparison with VPN software. Differences in their functionalities are given in Table 4.

Table 4. Comparison between OpenVPN and SoftEther tool for setting up a VPN [13]

	OpenVPN	SoftEther
Supported platforms (OS)	Windows, Mac, Solaris, Linux, NetBSD, QNX	Windows, Mac, Solaris, Linux FreeBSD
License	open source	open source
Year	2002	2013
Supported protocols	OpenVPN only	EtherIP, Microsoft SSTP, L2TP/Ipsec
Supported encryption algorithms	AES, Blowfish, 3DES, CAST-128	
Throughput speed	100 Mbs	900 Mbs

There are also various commercial VPN services available on the market. Choice of a high-quality VPN service depends on several factors:

- Supported network protocols,
- Server locations,
- Logs and monitoring,
- Client applications,
- Service price.

Support for modern network protocols is one of the key parameters when choosing a commercial VPN service. The newer and safer the protocol, the faster and safer the communication. The location of VPN server is subject to laws of the country in which servers are located. European countries are more liberal regarding control and privacy than, for example, the USA, where server activities are recorded as so-called logs. Supported client applications enable a simple, fast and secure method of setting up a VPN connection which is fully automated. The service price is proportional to its quality.

In principle, more expensive commercial VPN services offer more.

[3] Research conducted in September 2013 on a sample of 59 CARNet system engineers according to doctoral dissertation: Skendžić A "Model vrednovanja sigurnosti bežičnih lokalnih mreža u obrazovnim ustanovama" (Wireless network security evaluation in educational institutions), Faculty of Humanities and Social Sciences, Zagreb 2014, Croatia. Doctoral Thesis.

OpenVPN, if used on Linux platform, has all the benefits offered by open source licenses. Some of the most commonly used open source licenses are [14]:

- GNU General Public License (GPL),
- Berkeley Software Distribution (BSD) License,
- Artistic License.

Some of the features shared by the licenses above are as follows [14]:

- Software can be installed on an unlimited number of computers,
- Software can be simultaneously used by an unlimited number of people,
- An unlimited number of software copies can be created (free distribution),
- There are no restrictions regarding software modifications,
- There are no restrictions regarding distribution or even sale of software[4].

Since the license allows for free redistribution, once a person receives a copy, they can redistribute it, and even try to sell it. In practice, creation of electronic software copies can actually be done without any costs. Supply and demand will keep the price low. In business environment, the price of product license can be a decisive factor when choosing a product that, according to its specifications, meets the user's requirements. Although commercial VPN services are available through Internet service providers, *OpenVPN* software solution offers an open source license, high level of configurability and, finally, it is free. You only need to ensure a bandwidth that is fast enough depending on the number of VPN network users within a company. The price of VPN service offered by commercial providers can amount to over HRK 20,000[5], depending on the bandwidth (64k – 10G[6]) and the number of users. *OpenVPN* software solution can be a good alternative to the use and adjustment of an own, independently created VPN service.

6. Conclusion

The present-day, modern business environment implies that technology is implemented in the everyday work. Networks and network environments are actual standards in communication, and this will certainly continue in the future since there are over 3 billion Internet users in the world. Mobile office has replaced traditional offices, and employees are now performing their tasks where they are needed in a given moment, always having at their disposal different business materials stored at their own company or office. Fast information flow and mobility are necessary for business success, and in order to achieve this, one must "be connected". In spite of the need for network connection, the issue of security is being raised among users. Communication security within computer networks can be achieved using various technologies. VPN technology certainly belongs to the category of secure remote communication with one's own office, which guarantees data confidentiality, data integrity and secure user authentication. There are many different commercial services offering own VPN solutions, subject to charge. *OpenVPN* does not belong to the category of "chargeable" services, it is part of GNU-GPL community of open source solutions, which is its comparative advantage. Flexibility, upgradeability, support for different platforms, support provided by GNU community are only some of comparative advantages of *OpenVPN*. With respect to disadvantages, it should be noted that *OpenVPN* is not a multi-thread application, which limits its rate of operating network connections (approximately up to 100 connections). In case more connections are needed, additional processes, different ports or IP addresses should be considered. In conclusion, although open source software is not completely free from restrictions, it provides the user with unlimited possibilities, at the same time protecting authors' rights. This is a kind of freedom both authors and users of open source software strive for [14].

[4] The license allows for free redistribution. In practice, creation of electronic software copies can be done without any costs.

[5] According to the current price list of a domestic operator in 2016

[6] According to the current price list of a domestic operator in 2016 Rates 64 kbit/s – 10 Gbit/s)

References

[1] ***https://openvpn.net/index.php/access-server/overview.html (02.11.2016)

[2] ***http://www.cert.hr/sites/default/files/NCERT- PUBDOC-2010-04-298.pdf (02.11.2016)

[3] ***http://onlinetrziste.com/2014/06/predstavljamo-5-besplatnih-vpn-servisa/ (02.11.2016)

[4] ***https://technet.microsoft.com/en-us/library/cc958048.aspx (02.11.2016)

[5] ***https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-create-site-to-site-rm-powershell (02.11.2016)

[6] Dražen O 2005 *Ekscentar* **7** December 2005 (url: http://hrcak.srce.hr/9676)

[7] Dražen D and Crnjac M D 2008 *A role of the VPN network modern business*, "Vallis Aurea", Croatia-Austria

[8] Ivan G 2008 *Iskustvo migracije na Linux desktop i server okruženje velikog korisnika*. HrOUGH, Rovinj, Croatia

[9] ***https://openmaniak.com/openvpn_static.php

[10] Skendžić A 2011 *Virtualne private mreže*, VIDI, VIDI-TO, Zagreb, Croatia

[11] Skendžić A 2014 *Wireless network security evaluation in educational institutions*, Faculty of Humanities and Social Sciences, Zagreb, Croatia, Doctoral Thesis.

[12] ***http://onlinetrziste.com/2014/06/predstavljamo-5-besplatnih-vpn-servisa/ (02.11.2016)

[13] ***https://www.limevpn.com/blog/softether-vpn-vs-openvpn-which-one-is-better-for-you-and-why/ (02.11.2016)

[14] ***https://www.carnet.hr/tematski/opensource/licence.html (02.11.2016)