www.mecsj.com

Virtual Private Network (VPN) Management and IPSec Tunneling Technology

Lana Ibrahim

Email:lana.ebra.94@gmail.com

Abstract

Virtual private network (VPN) technology takes place for creating an encrypted connection on a lower network security. The advantage of VPN relies on ensuring the suitable security level to the connected systems.

This paper concerns on security issues of virtual private network (VPN), by reviewing the Cisco Easy VPN Server for managing these networks, and reviewing IPsec tunneling technology for enhancing the security level, based on security-related problems that networks may face while connected to the Internet, and VPN's ability in providing a high productivity, security, and flexibility features.

First, VPN categories, benefits, and limitations were reviewed by concerning on its technique. After that, IPsec Tunneling Technology was reviewed by illustrating its technique and characteristics. Also, the role of Cisco Easy VPN Server in VPN management was clarified due to its importance for all sizes of businesses especially the large enterprise networks with Cisco Router and Security Device Manager (SDM).

Keywords: Virtual private network, IPsec ,tunneling technology .

1. Introduction

Virtual Private Network (VPN) is a virtual network that is created under a public network infrastructure, such as the World Wide Web. Companies can use VPN to establish a secure connection to remote offices and remote users by accessing the Internet through a third party at an affordable cost, rather than creating expensive custom WAN links or long distance telephone links (Milanovic & Petrovic, 2001).

VPN provides the highest possible level of security through authentication technologies, IP-based VPNs, encrypted IPsec, or Secure Sockets Layer (SSL). All of these technologies protect data transmitted over VPN networks from unauthorized access.

Businesses can take advantage of the easy-to-save infrastructure of VPNs to quickly add new sites or users. Besides, it can also increase access to VPNs without having to invest heavily in infrastructure expansion (CCNA Security 1.0. Cisco Network Academy, 2010).

There are two types of encrypted VPNs: the IPsec VPN-based from a site location, which represent an alternative choice to WAN based on the migration of leased lines, which allows companies to extend network resources to Branch offices, home offices, and business partner sites. The second type is Remote Access VPN, which can connect any data, audio, or video application to the remote desktop. A VPN can be deployed for remote access using SSL VPN, IPsec, or both, depending on deployment requirements (Heninger, Kari, Rippon & Rubinshtein, 2011).

As the high importance of a security issue between any connections which directly affects the productivity, Cisco Easy VPN Server will be discussed in this paper as a way of troubleshooting complicated network and VPN connectivity issues. As well as, IPsec tunneling technology will be studied here as way of enhancing VPN security and confidentiality.

1.1 Study Objectives

The basic aim of this study is to:

Study methods of managing Virtual Private Network (VPN) and the tole of IPsec Tunneling Technology in enhancing security level

The study sub-aims are to:

1. Highlight the role of VPNs in enhancing communications security for all sizes of businesses, especially the large enterprise networks with Cisco Router and Security Device Manager (SDM).
2. Illustrate the role of IPsec tunneling technology in VPN connection between two LANs (site-to-site VPN) or a remote dial-up user and a LAN.
3. Study the role of Cisco Easy VPN server in facilitating the deployment process of virtual private network (VPN) for remote offices.

2. VPN Categories, Benefits, and Limitations

VPNs provide a high productivity, security, and flexibility, which authorize a remote secure connection by sites and teleworkers to the corporate network from almost any area, by encrypting data on a VPN and denying any unauthorized access to it (Jalava, 2003), as shown in figure [1].

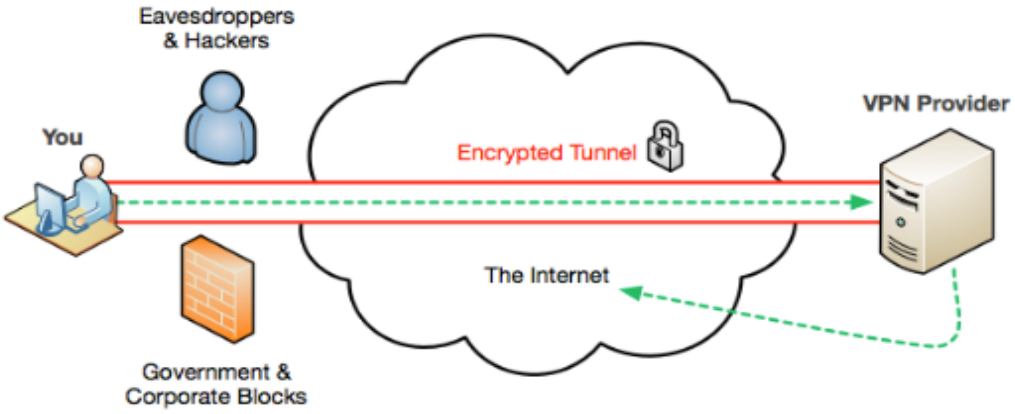

Figure [1]: VPNs technique overview (Lawrence, 2017)

Efficiency is one of the most important benefits in VPNs. without VPN, corporations waste high costs in leasing the dedicated expensive WAN links from ISPs and may without an effective speed in intercompany transportation. It enables the using of cost-effective, third-party Internet transport for connecting remotely, in addition to its role in eliminating the traditional costly dedicated WAN links. It also supports high-bandwidth technologies, like Digital Subscriber Loop (DSL); decrease the organization's connectivity costs, and raising the bandwidth of remote connection (Mason, 2004).

The second important benefit of VPNs is the scalability, which decrease wasting time in creating a new link between headquarter and new branch buildings, by using Internet Service Providers (ISPs) infrastructure. This process eases adding and modifying the number of connected users, so that companies can add important capacity without needing to add infrastructure (Singh, Samaddar, & Misra, 2012).

Telecommuters and mobile workers are allowed to gain a broadband connectivity for accessing to their networks, providing them high efficiency and flexibility, which directly enhancing the productivity.

VPNs supply the highest level of security through using advanced encryption and authentication protocols that provide a protection of data from unauthorized access, such as Password Authentication Protocol (PAP), Challenge-handshake authentication protocol (CHAP), and Extensible Authentication Protocol (EAP).

In the other side, there are different limitations of VPNs. attackers may target client machine, and different bugs or miss-configuration could be exploited using different attacking ways, like VPN hijacking, malwares, or man-in-the-middle attacks (Singh, Samaddar, & Misra, 2012).

In addition, VPN supports limited authentication methods, like PAP, and password is in a clear text. Establishing connection should be done by an authenticated user only, and if this authentication is not robust for denying any unauthorized access, network and its resources can be attacked (Galán-Jiménez & Gazo-Cervero, 2011).

3. IPsec Tunneling Technology

A secure network must begin with robust security policies that dictate the security deployment in the network, and IPsec protocol is one of examples for securing the transfer process of information at the OSI layer.

The job of IPsec suite takes placed at the Network Layer, for protecting and authenticating aim of IP packets between sharable IPsec peers. So, the function of this protocol relies on protecting all application traffic virtually, due to the protection ability to be implemented from Layer 4 through Layer 7 (Yang, 2011).

For providing the framework and the network administrator in IPsec, there is just a need to select the appropriate algorithms for being sure that the similar algorithms are used between two parts, and for investigating the security services. Without obligation of IPsec to particular algorithms, novel and better algorithms will

be allowed to be performed in the IPsec frame. It has the ability to secure the track between site-to-site gateways, the couple of hosts, or to secure a track between gateway and host, which implemented the remote access. Figure [2] shows IPsec framework (Muirhead & Page, 2010).

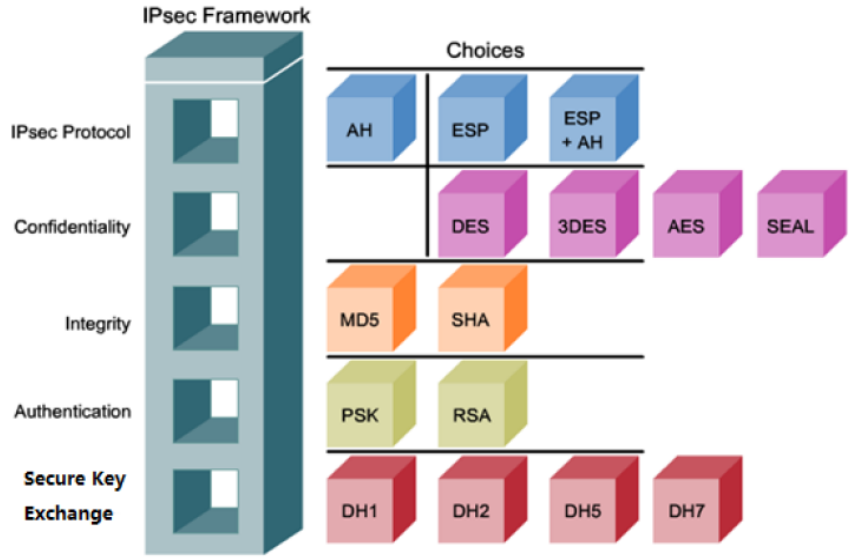

Figure [2]: IPsec Framework (Yang, 2011)

A VPN connection connects two LANs (site-to-site VPN) or a remote dial-up user and a LAN. Flowing traffic between connected points passes out of shared resources. So, IPsec tunnel is used for securing VPN communication at passing time.

IPsec tunneling technology protects entire IP packets, by encrypting the original packets after wrapping it, then it sends new IP header after adding it to the other side of the VPN tunnel (IPsec peer) (Muirhead & Page, 2010).

Figure [3] shows an example of IPsec tunneling mode between a connected Cisco VPN Client and an IPsec Gateway. First, the traffic from the client is encrypted,

and then encapsulated in a novel IP packet, after that it sent to the other end. When the traffic is decrypted by the firewall, the original IP packet of the client is sent to the local network (Snader, 2015).

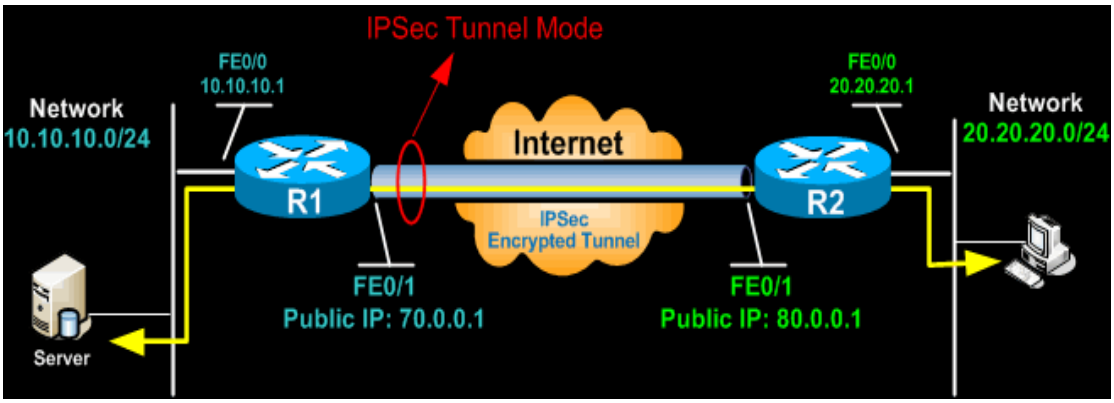

Figure [3]: IPsec-VPN Tunneling Technology (Snader, 2015)

AH or ESP header of IPsec is inserted between both header of the IP and the upper layer protocol. ESP is used more that AH in Tunneling configuration of IPsec-VPN.

4. Cisco Easy VPN Server in VPN Management

Cisco Easy VPN server facilitates the deployment process of virtual private network (VPN) for remote offices. The solution of this server localizes the management of VPN across all Cisco VPN devices. So, it will reduce VPN's deployments management complexity.

Cisco Easy VPN contains both Cisco Easy VPN Remote and Cisco Easy VPN Server components. The remote characteristics permit Cisco IOS routers to extradite security policies over a connection of VPN tunnel from a Server of Cisco Easy VPN.

Also, the remote characteristics have the ability to minimize configuration needs at the remote location (Bibraj, Chug, Nath, & Singh, 2018).

This server permits routers of Cisco IOS to work as VPN head end device in remote-access VPNs and in site-to-site VPNs. This characteristic raises security policies defined on the side of central site to the remote VPN device, which assist in ensuring that these connections have up-to-date policies before establishing the connection.

Cisco Easy VPN supplies automatic configuration and management for parleying tunnel parameters and establishing IPsec tunnels. When the user asked for IPsec connection, the extended authentication (Xauth) will adds another level of authentication that distinguishes the user. Partition tunneling allows the remote router to route the Internet-destined traffic immediately without needing to forward it over the encrypted tunnel. So, this process is easier now for all sizes of businesses especially the large enterprise networks with Cisco Router and Security Device Manager (SDM) (Bibraj et al., 2018).

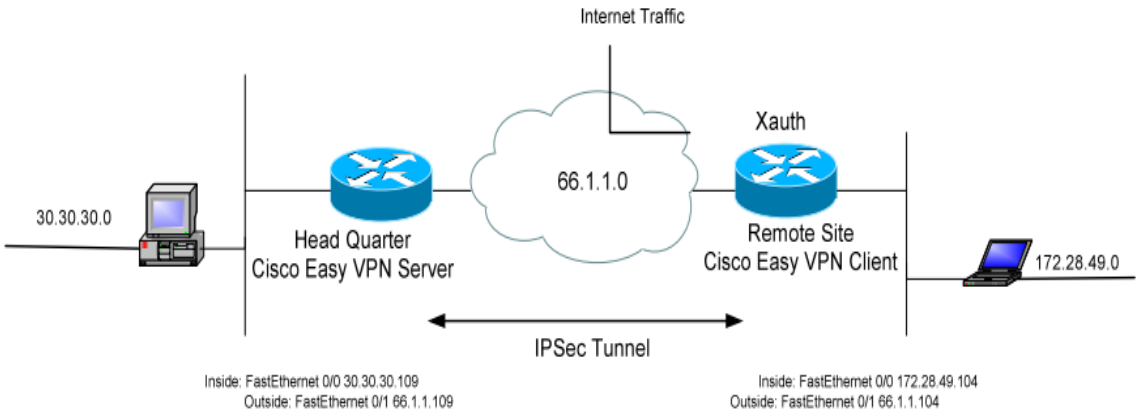

Figure [4]: Example of Cisco Easy VPN Server and Xauth ()

In addition to the authentication process which is done by shared key, Xauth provides an extra level of authentication for recognizing the user who asks a request of IPsec connection, as shown in the example in figure [4]. The remote site waits for a challenge of "username/password" after establishing the Internet Key Exchange (IKE) Security Association (Khalid, Asati, Patil & Akhter, 2011).

Using Cisco Easy VPN Server, configuration of Split Tunneling is done, and is loaded on the Cisco Easy VPN Remote dynamically. This type of tunneling allows a direct Internet intended traffic's routing of the remote router without needing to forward it through the encrypted tunnel.

5. Conclusion

Virtual Private Networks (VPNs) divided into two categories, depending on the security characteristics in place: IPsec or SSL. IPsec-based VPNs allow the security layer to be a portion of the network, which will increase protection for all traffics flowing in and out of the network.

IPsec tunneling has a big important role in enhancing VPNs' security, because it based on the network level, and it is totally hidden in its operation. So, there is no need to learn about it by end users and they never interact with it directly. This is an added security layer for the VPNs running on IPsec.

In addition to IPsec tunneling Cisco Easy VPN was reviewed. Basic configuration and management of Cisco routers are configured with Command Line Interface (CLI). but, Cisco presented Graphical User Interface (GUI) tools for management objectives, like Cisco Easy VPN, it can deals with all network managers, essentially the large enterprise networks with Cisco Router and Security Device

Manager (SDM). This server added another security feature by enhancing authentication method by splitting tunneling.

References

Lawrence, J. (2017). Get a VPN today, Electronic Frontiers Australia. Retrieve from: https://www.efa.org.au/2017/04/13/get-a-vpn-today/

Jalava, M. (2003). U.S. Patent Application No. 10/151,319.

CCNA Security 1.0. Cisco Network Academy. Available in online books. Require user account. Updated 21.7.2010. Referred 15.5.2011. URL: http://www.cisco.com/web/learning/netacad/index.html

Mason, A. (2004). CCSP Self-Study: Cisco Secure Virtual Private Networks (CSVPN). Pearson Higher Education.

Galán-Jiménez, J., & Gazo-Cervero, A. (2011). Overview and challenges of overlay networks: A survey. Int J Comput Sci Eng Surv (IJCSES), 2, 19-37.

Milanovic, S., & Petrovic, Z. (2001). Deploying IP-based Virtual Private Network across the Global Corporation. Communications World, 13-17.

Heninger, I. M., Kari, J. D., Rippon, W. J., & Rubinshtein, G. (2011). U.S. Patent No. 7,975,294. Washington, DC: U.S. Patent and Trademark Office.

Singh, A. K., Samaddar, S. G., & Misra, A. K. (2012, March). Enhancing VPN security through security policy management. In Recent Advances in Information Technology (RAIT), 2012 1st International Conference on (pp. 137-142). IEEE.

Yang, Y. (2011). Virtual Private Network Management, Bachelor of Information Technology Network Optionion.

Muirhead, C. S., & Page, D. J. (2010). U.S. Patent No. 7,684,321. Washington, DC: U.S. Patent and Trademark Office.

Snader, J. C. (2015). VPNs Illustrated: Tunnels, VPNs, and IPsec: Tunnels, VPNs, and IPsec. Addison-Wesley Professional.

Khalid, M., Asati, R., Patil, S. P., & Akhter, A. (2011). Methods and systems for dynamically updating a routing table in a virtual private network U.S. Patent No. 7,987,506. Washington, DC: U.S. Patent and Trademark Office.

Bibraj, R., Chug, S., Nath, S., & Singh, S. L. (2018). Technical study of remote access VPN and its advantages over site to site VPN to analyze the possibility of hybrid setups at radar stations with evolving mobile communication technology. MAUSAM, 69(1), 97-102.