Indonesian Journal of Electrical Engineering and Computer Science
Vol. 7, No. 3, September 2017, pp. 855 ~ 860
DOI: 10.11591/ijeecs.v7.i3.pp855-860

Implementation of IPsec-VPN Tunneling using GNS3

Fatimah Abdulnabi Salman
College of Information Engineering, Al_Nahrain Uninersity, Iraq
*Corresponding author, e-mail: faty.a.salman@gmail.com

Abstract

Virtual private networks (VPN) provide remotely secure connection for clients to exchange information with company networks. This paper deals with Site-to-site IPsec-VPN that connects the company intranets. IPsec-VPN network is implemented with security protocols for key management and exchange, authentication and integrity using GNS3 Network simulator. The testing and verification analyzing of data packets is done using both PING tool and Wireshark to ensure the encryption of data packets during data exchange between different sites belong to the same company.

Keywords*: VPN, IPsec, Tunneling, GNS3*

1. Introduction

A Virtual Private Network (VPN) appears to be the excellent method for distributed services provides on public network structure. VPN offers low cost, efficient use of bandwidth, scalable and flexible functionality, secure and private connections. VPN provides a virtual private line between two network sites that network traffic pass through. VPN network is affected by several points such as operating system, hardware devices being used, interoperability and algorithm being implemented [1].

VPN can be classified according to the tunneling security issue, location of endpoints, connectivity types, security mechanisms robustness, and the types of tunneling protocols [2].

VPN provide connectivity through a tunnel which is a virtual link between two nodes may separate by a number of networks. Figure 1 shows VPN tunneling structure. The tunnel is established within the router and provided with the IP address of the router at the second end. Every packet is encapsulated inside the IP datagram using IP address of the router at the far end of tunnel as a destination address [3]. The two endpoints must use the same tunneling protocol. These logical tunnels that carry the IP packet are independent of the payload, and have different headers due to the protocol implemented [4].

VPN provides secure and encrypted virtual connections over IP network by encrypts and encapsulates each packet before passing it through a tunnel. VPN uses authentication to ensure data integrity and confidentiality [4]. VPN uses dynamic tunnel for efficient bandwidth usage and flexibility matter for creating and removing tunnels at any time [5].

VPNs tunneling add an overhead to IP packets size, that effect bandwidth utilization in network specifically if the packet size is short. This effect lays on the end router to decapsulate the packet, performs decryption for the packet [6].

This paper analyzes the VPN tunneling protocols. The propsed VPN-IPsec tunneling scenario is configured using GNS3 simulator along with virtual network environemwnt for site to site network structure that can be impleneted as a real network desgin for a company, and also it can used as case study for understanding the VPN network structure using flexible, efficient practice.

The paper is arranged as follows: Section 2 presents VPN technologies, their advantages and disadvantages. Section 3 gives VPN simulation model and testing and verfications in section 4. Finally, the conclusions are presented in section 5.

Received June 2, 2017; Revised August 1, 2017; Accepted August 14, 2017

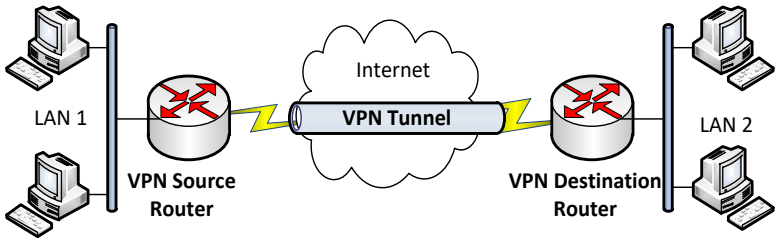

Figure 1. VPN Tunneling structure

2. Virtual Private Network

VPN relies on tunneling techniques for transmitting data. The tunneling protocols work at different OSI layers such as in data link layer, network layer, or the session layer [7]. The most popular protocols that linked with VPN development are point to point tunneling protocol (PPTP), layer 2 tunneling protocol (L2TP), Internet protocol security (IPSec) and Secure socket layer (SSL) [7-9].These protocols secure VPN and provide authentication and encryption mechanisms [4].

1. Point to Point Tunneling Protocol (PPTP)

PPTP specification is described in network working group RFC 2637 [10]. It operates at data link layer. It is an expansion of point-to-point protocol (PPP) using the same authentication mechanisms as PPP [11].

2. Layer 2 Tunneling Protocol (L2TP)

L2TP may establish a tunnel between the routers or the router and clients. L2TP combined the features of PPTP and layer two forwarding. L2TP eliminates the network traffic by flow control mechanisim to address congestion and keep overhead to minimum. L2TP header contains information about media, L2TP encapsulation that drive for high extent of data packet to surpass between the tunnel endpoints withought increasing high overhead on the network. L2TP is capable of establishing multiple tunnels simultaneously between two tunnel endpoints [12].

3. Internet Protocol Security (IPsec)

IPsec offer data integrity, data confidentiality, and authentication originality of data at the network layer in OSI model [4]. It composed of different protocols such as: IPsec Key Exchange and Management Protocol (ISAKMP) for key management which specifies the negotiation, establishment, alteration, and omission of security association. Internet Key Exchange (IKE) for key exchange which create secure channel to protect the negotiation for setting up the IPsec tunnel for traffic protection. Authentication Header (AH) offers authentication originality, connectionless integrity, and anti-replay service. Encapsulated Security Payload (ESP) offers authentication originality, connectionless integrity, anti-replay service, and data confidentiality.

These protocols used to create connection and transmit traffic securely [4], [13]. IPsec can employ two encryption modes: transport mode which encrypts data only and tunnel mode that encrypts header and data [4, 5], [14].

4. Secure Socket Layer (SSL)

SSL offers encryption and authentication for web traffic over an encrypted tunnel [11]. SSL support specific applications such web and email services since SSL tunnel traffic at session layer [15]. Table 1 summarizes advantages and disadvantages of VPN Protocol tunnel solution.

VPN connection can be classified into two types Site-to-site VPN and Remote access VPN [1]. In Site to site VPN, a VPN connection is established between single sites to the remote location site of an office. All the communication will happen through VPN gateway. It may use different protocols such as IPsec, GRE and MPLS.

In Remote access VPN, a VPN connection is created between users (mobile user) and a server in LAN by using VPN client software for accessing. Only authorized users can logon to VPN tunnel [4]. It may use different protocols such as IPsec, SSL, PPTP and L2TP [1], [4], [8].

Another category of VPN according to network management by customer or by service provider:

a) Trusted VPN in which customer trusted VPN service providers offering data integrity and avoiding network traffic sniffing.
b) Secure VPNs: Networks are established with encryption even though an attacker is able to inspect the traffic, he cannot discover it.
c) Hybrid VPNs: New form of trusted VPN that runs a secure VPN as a part of a trusted VPN [9], [11].

Table 1 advantages and disadvantages of VPN Protocol tunnel solution.

Protocol	Advantages	Disadvantages
PPTP	• Supports Microsoft Windows. • Low cost due to easy installation • No compatibility problem	• Unreliable, do not provide integrity and verification • Low performance for unstable networks.
L2TP	• High data security for censorious application. • High level of encryption for sensitive information. • Low overhead protocol. • Fast, flexible scalable and reliable • Best authentication policy for users.	• Low speed for data transmission • May fail because of security keys mismatch. • Slow down performance, twice packet encapsulation.
IPSec	• High security level implement in network layer • Invisible operation to user. • Monitor all the incoming and outgoing traffic. • Easy mauntience	• compatibility issue due to different standards • Processing overhead due to encryption, decryption, and complex tunneling. • IKE processing overhead due to use an automatic key
SSL	• Low cost • Most browsers and application support SSL. • Safe authentication, accessing • Security imposed restricted access. • No requirement for client software.	• Works on specific operating system: windows • Insecure network and transport header. • Exposed to denial of services attack

3. Simulation Model

The network simulation is done using GNS3 consisting of routers with 7200 series type, two clients and server which implemented with virtual machine and connected to the GNS3 topology as shown in Figure 2. The server provides a web services for the clients in different sites. The routers represent different VPN sites as an IPsec-VPN gateway; they are configured with IPsec tunnel mode. The security strategy implemented in these routers is as follows: the IKE tunnel security with ISAKMP policy 10, AES 256 for encryption and pre-shared key group 5 for authentication.

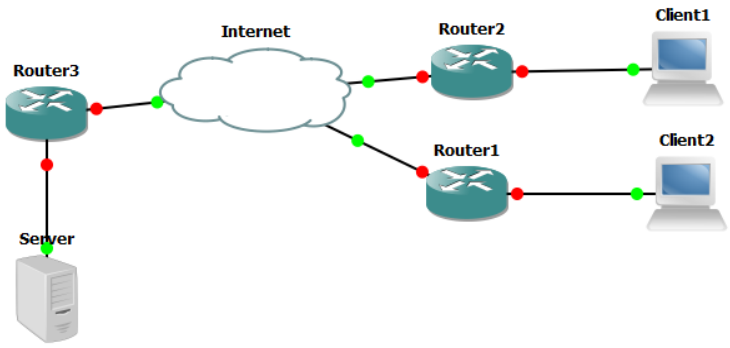

Figure 2. VPN Topology

An IPsec transformation set is configured in the routers to combine the authentication and encryption, a crypto map entry is created to establish the security associations as shown in figure 3. An access list is configured to identify the network traffic.

```
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
crypto isakmp key cisco address 10.0.112.2
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set esp-aes256-sha esp-aes 256 esp-sha-hmac
!
crypto map cmap 10 ipsec-isakmp
 set peer 10.0.112.2
 set transform-set esp-aes256-sha
 match address 121
!
```

Figure 3. IPsec_VPN Router Configuration

4. Simulation Test

To test the network operation, two tools is used, PING and Wireshark. The tunneling establishment is ensured using ping tool; Figure 4 show the result of successival connectivity between the client and the server.

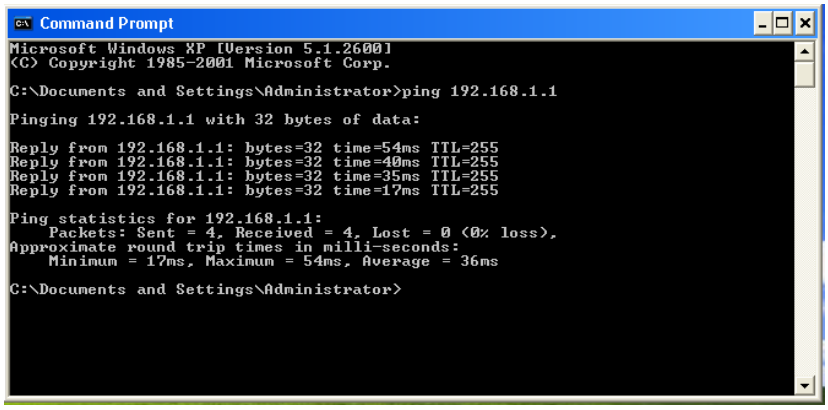

Figure 4. Tunneling test using Ping

The Wireshark is used to capture the traffic between the routers to analyze the network traffic and ensure the work of the security strategy. Figure 5 shows the capturing of data traffic between router 1 and router 3 that presents the ISAKMP process for negiotation, establishment, key management between the two routers. Figure 6 shows that the data traffic between the routers is encrypted with ESP.

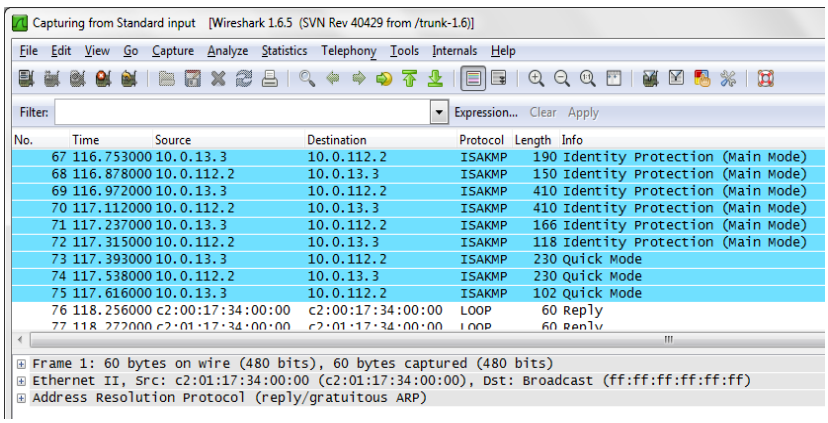

Figure 5. Capturing Data of ISAKMP

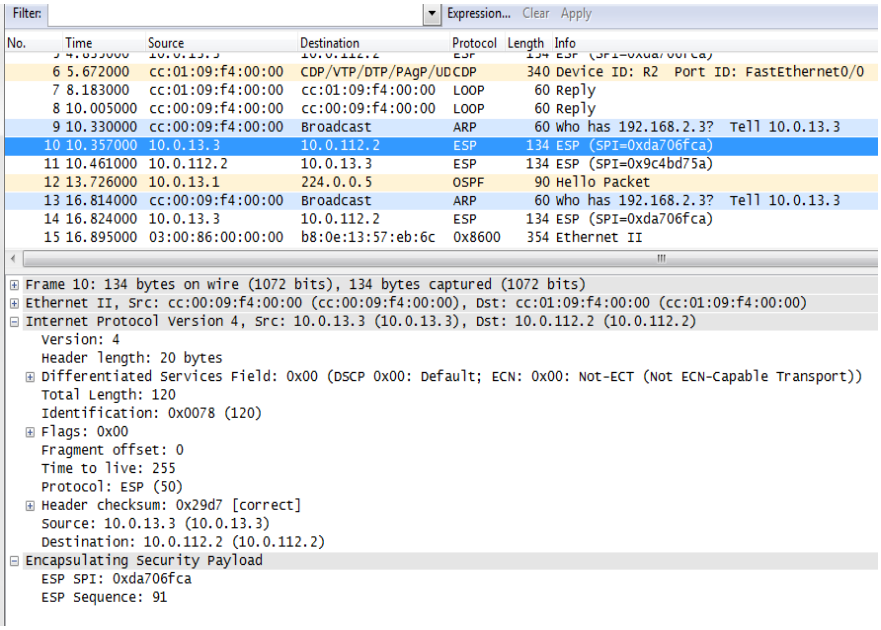

Figure 6. Capturing Data of ESP

5. Conclusion

VPN offers the enterprise company privacy issues and cost effectiveness services without distributing the communication. The main goal of this paper is to implement VPN network using IPsec tunneling mechanisim using GNS3 withh virtual clients and servers. The testing shows the successful verification of the security stratgey of IPsec and data packet processing under using security protocols.

References

[1] Gamundani A, Nambili J, Bere M,. A VPN Security Solution for Connectivity over Insecure Network Channels: A novel study. *SSRG International Journal of Computer Science and Engineering (SSRG-IJCSE)*. 2014,1(7):1-8 .

[2] Shrivastava A, Rizvi M, .Analysis and Comparison of major mechanisms implementing Virtual Private Networks. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*. 2014 3(7):2374-2381.

[3] Wang C, Chen J, .*Implementation of GRE Over IPsec VPN Enterprise Network Based on Cisco Packet Trace.* 2nd International Conference on Soft Computing in Information Communication Technology (SCICT). Taipei, Taiwan, 2014:142-146.

[4] Ahamed S, Rajamohan P, .Comprehensive Performance Analysis and Special Issues of Virtual Private Network Strategies in the Computer Communication: A Novel Study. *International Journal of Engineering Science and Technology (IJEST)*. 2011, 3(7):6040-6048.

[5] Elezi M, Raufi B. *Conception of Virtual Private Networks using Ipsec Suite of Protocols, Comparative Analysis of distributed Database Queries using different Ipsec Modes of Encryption*. World Conference on Technology, Innovation and Entrepreneurship. Istanbul, Turkey, 2015,195:1938-1948.

[6] Hussein S, Abdul Hadi A. The Impact of Using Security Protocols in Dedicated Private Network and Virtual Private Network", *International Journal Of Scientific & Technology Research,* 2013 2(11):170-175.

[7] Diab WB, Tohme S, Bassil C, .*VPN Analysis and New Perspective for Securing Voice over VPN Networks*. IEEE Fourth International Conference on Networking and Services. 2008, 73-78.

[8] Malik A, Verma H,. Performance Analysis of Virtual Private Network for Securing Voice and Video Traffic. *International Journal of Computer Applications*. 2012, 46(16):25-30.

[9] Scripcariu L, Bogdan I,. Virtual Private Networks: An Overview", *TELECOMUNICAŢII,* Anul LII, nr. 2009, 32-37.

[10] Hamzeh AK, Pall G, Verthein W, Taarud J, Little W, Zorn G, RFC 2637: Point-to-Point Tunneling Protocol (PPTP), Network Working Group, July 1999.

[11] Padhiar S, Verma P,. A Survey on Performance Evaluation of VPN on Various Operating System. *International Journal of Engineering Development and Research (IJEDR)*. 2015 3(4): 516-519.

[12] Haider A, Houseini M,. The Difference Impact on QoS Parameters between the IPsec and L2TP. *International hournal of Innovative n Advanced Engineering (IJIRAE)*. 2016, 11(3):31-42
[13] Shue CA, Gupota M, Myers SA,. *IPSec: Performance Analysis and Enhancements.* IEEE International Conference on Communications (ICC), Glasgow, Scotland **.** 2007.
[14] Bensalah F, El Kamoun N, Bahnasse A,,. Analytical Performance and Evaluation of the Scalability of Layer 3 Tunneling Protocols: Case of Voice Traffic Over IP. *International Journal of Computer Science and Network Secuirty (IJCSNS)*. 2017, 17(4):361-369.
[15] Bourdoucen H, Al Naamany A, Al Kalbani A,. Impact of Implementing VPN to Secure Wireless LAN", *International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering.* 2009,3(3): 502-507.