© 2018 IJSRSET | Volume 4 | Issue 9 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

Design and Implementation of Secure Communication Between Two Branches of a Company Using IPSEC Based VPN (Virtual Private Network) Protocol

V. Sushma, T. Venkateswarlu
ECE Department, S.V.U College of Engineering, Tirupati, Andhra Pradesh, India

ABSTRACT

Now a day's most of the corporate business network infrastructure needs to securely transfer data across the Internet. Data can be a company's top-secret information regarding product designs, product release dates, patent information, HR employee investigations, etc. This project provides insight for a secure solution to this business need using Virtual Private Network (VPN).There are a number of VPN protocols in use that secure the transport of data traffic over a public network infrastructure. IPSec is a protocol suite for securing internet protocol communications via authenticating and encrypting every IP packet of a conversation session. A tunnel is created to secure VPN communication through WAN between two participants. A tunnel can provide Privacy, Content reliability and authentication and Sender authentication and if using certificates no repudiation (via data origin authentication). Juniper SRX Security devices supports the IPSec VPN tunnel formation not only using Policies, it can also be done by routing a traffic to a virtual interface called st0 interface which reduces the burden of policy verification. The aim is to configure a separate secure tunnel logical unit. With route-based VPNs, organizations define the VPN overlay links and then define the static routes that will be used for transport, allowing the route, to determine which traffic goes through the VPN.

Keywords : VPN, IPSec, Routing, OSPF, Authentication, Encryption, Encapsulation

I. INTRODUCTION

IPSEC (Internet Protocol Security) is a network layer security protocol that is designed to support secure TCP/IP environment over the Internet considering flexibility, scalability, and interoperability. Unlike the other security protocols it provides security among the hosts. Recently, IPSEC is emphasized as one of the important security infrastructures in the NGI (Next Generation Internet). It also has suitable features to implement VPN (Virtual Private Network) efficiently and its application areas are expected to grow rapidly. In this paper, the basic concepts and related standard documents of IPSEC.

The IPSEC is an open architecture and an open frame work defined by the IPSEC working group of the IETF. It provides a scalable, long lasting base for providing network layer security. The IPv4 implementations are strongly recommended to support IPSEC and IPv6 implementations are required to do so. IPSec gives the base protection capabilities for the net and furnishes bendy constructing blocks from which comfy and prospering virtual non-public networks (VPNs) may be built.

IPSec Security Features: It was designed to provide high security while transferring packets across the networks and it is the most commercial for connecting network sites.

Authentication: Verifies that the packet at receiver end and at source are same or not. **Integrity:** Ensures that the contents of the packet did not change in transit.

Confidentiality: Conceals the message content through encryption.

IPSec Components: IPSec contains the following elements:

Authentication Header (AH)

Internet Key Exchange (IKE)

Encapsulating Security Payload (ESP)

Authentication Header (AH)

AH provides authentication and integrity, which protect against data interfere, using the same algorithms as ESP. AH also provides optional anti-replay protection, which protects against unauthorized retransmission of packets. The authentication header is inserted into the packet among the ip header and any upcoming packet contents. IPSec introduces the idea of the security affiliation (SA). The payload is not touched.

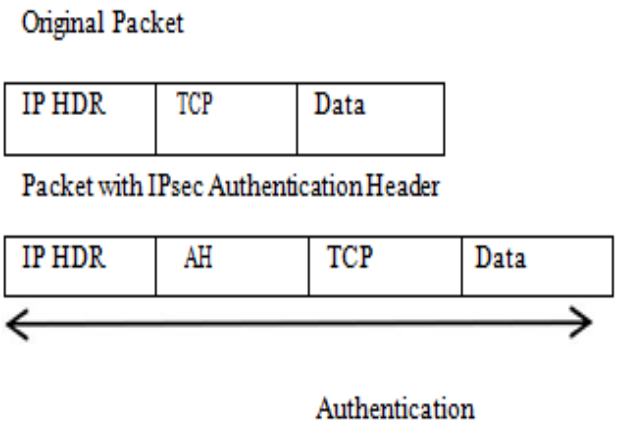

Figure 1.Authentication header

Security Association

IPSec introduces the concept of the Security Association (SA). An SA is a logical connection between two devices used to transfer the data. It provides data protection for unidirectional traffic by using the defined IPSec protocols.

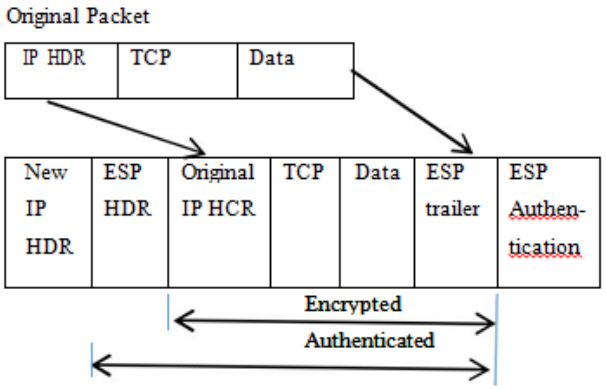

Figure 2.Authentication header in tunnel mode

II. EXISTING METHOD

MPLS based VPN's are based on peer model done in layer 3. It will enables the service provider and the customer to exchange layer 3 routing information .

The service provider relays the data between the customer sites without customer involvement.

The communication between CE and PE can be done by using any routing protocol with company's permit.

MPLS VPN's on the other hand are "private" networks run by service providers where a guaranteed service level can be agreed with the provider. It do not provide confidentiality among the network.

MPLS VPN's are essentially on the carrier provider side, in which this era permits rather scalable VPN architectures with included QoS assist.

III. PROPOSED METHOD

Transport Mode: In this mode IPSec implementation encapsulates only the packet's payload. The IP header is not changed. After the packet is processed with IPSec, the new IP packet contains the old IP header and the processed packet payload. It does not protect the information present in the IP header therefore, an attacker can easily identify the packet's source and destination.

Tunnel Mode: The tunnel mode IPSec implementation encapsulates the entire IP packet. The entire packet becomes the payload of the packet that is processed with IPSec. A new IP header is created by the IPSec which contains two IPSec gateway addresses. The gateways perform the encapsulation on behalf of the hosts. In this mode ESP prevents an hacker from analyzing the data and decrypt it , an attacker cannot identify from where the packet is coming and going.

Key Management:

IPSec uses the Internet Key Exchange (IKE) protocol to ease and automate the SA setup and the exchange of keys between parties transferring data. It ensures that only the sender and receiver of a message can access it. IPSec requires that keys should be dynamic or refreshed frequently so that communication with each other will be secured. IKE manages the process of refreshing keys and user can control the keys strength and the refresh frequency. Refreshing keys provides confidentiality between sender and receiver.

The IPSec software program on host "A" initiates the IPSec process in try and talk with host "B".

The two computer systems then start the key IKE technique.

IKE Phase I.

- ➢ The two parties negotiate the encryption and authentication algorithms to apply in the IKE SAs.
- ➢ The 2 parties authenticate each different using a predetermined mechanism, including pre-shared keys or virtual certificates.
- ➢ A shared master key is generated by way of the Diffie-Hellman public key algorithm within the IKE framework for the 2 events. The grasp key is also used in the 2d section to derive IPSec keys for the SAs.

IKE Phase II.

1. The 2 parties negotiate the encryption and authentication algorithms to apply inside the IPSec SAs.
2. The grasp secret's used to derive the IPSec keys for the SAs. Once the SA keys are created and exchanged, the IPSec SAs are geared up to protect consumer information between the two VPN gateways.

Data transfer. Data is transferred among IPSec peers based totally at the IPSec parameters and keys saved inside the SA database.

IPSec tunnel termination: IPSec SAs terminate through deletion or by timing out.

VPNC IKE Security Parameters

It is important to remember that both gateways must have the identical parameters set for the process to work correctly. The settings in these examples follow the examples given for Scenario 1 of the VPN Consortium.

VPNC IKE Phase I Parameters The

IKE Phase 1 parameters used:

Main mode

TripleDES

SHA-1

MODP group 1

pre-shared secret of "hr5xb84l6aa9r6"

SA lifetime of 28800 seconds (eight hours)

VPNC IKE Phase II Parameters

The IKE Phase 2 parameters used in Scenario

- are:

TripleDES SHA-

1

ESP tunnel mode

MODP group 1

Perfect forward secrecy for rekeying

SA lifetime of 28800 seconds (one hour)

IV. RESULTS

IPSEC is a traditional network layer security which is intended to secure TCP/IP condition over Internet considering adaptability, flexibility and interoperability. IPSEC essentially bolsters security was against clients, not at all the remaining security traditions. IPSec was concerned as the principal safety foundations in NGI. It is like way has sensible highlights to execute VPN gainfully and its application districts are relied on to develop rapidly. In this paper, the essential considerations and related standard records of IPSEC will be shown.

Definition and concepts:

IPSEC is an open outlining and an open framework defined by IPSec working get-together of IETF. It gives a flexible, extreme base for giving security in a network layer. IPv4 usage is truly prescribed to help IPSec whereas IPv6 executions which are required to do all things considered. IPSec gives the base security capacities to the web and outfits adaptable building blocks from which securing and staggering VPNs that can be made.

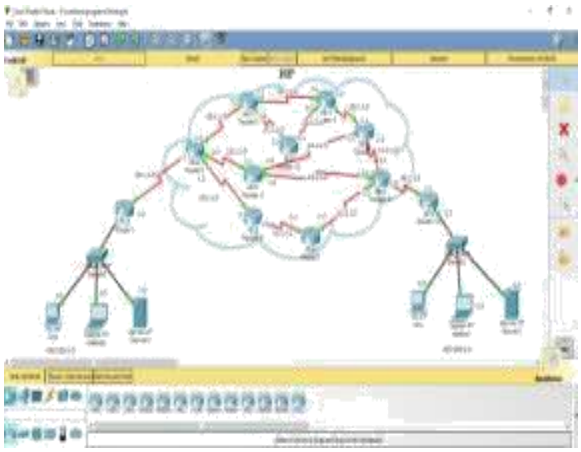

Figure 3.Network

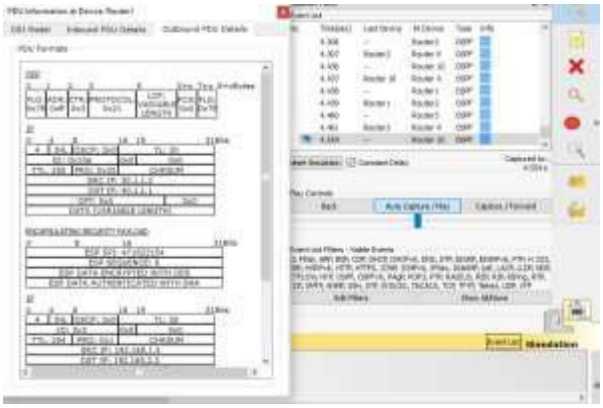

Figure 4. After configuring OSPF routing protocol

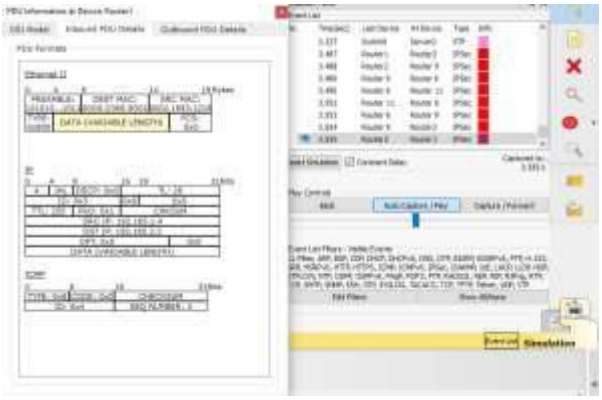

Figure 5.After configuring IPSec based VPN

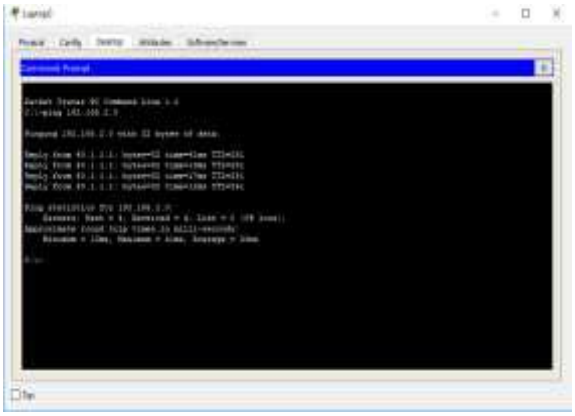

Figure 6.Pinging of two systems

A network with more number of users are constructed in Cisco packet tracer as shown in Figure 3 and the commands are written in particular users as per their IP address. When we considered the OSPF routing without IPSec the source and destination address are visible as shown in Figure 4, whereas we can see the duplicate addresses after the configuration using IPSec as shown in Figure 5.

When we ping from one system to other using the ping command in command prompt as shown in Figure 6, the following data can be obtained

Pinging 192.165.2.0 with 32 bytes of data:
Reply from 40.1.1.1
bytes=32 time=41ms TTL=251
bytes=32 time=13ms TTL=251
bytes=32 time=17ms TTL=251
bytes=32 time=12ms TTL=251
Ping statistics for 192.165.2.0:
Packets: sent=4, received=4, lost=0(0%loss)
Approximate round trip times in milli-seconds:
Minimum=12ms,Maximum=41ms, Average=20ms

V. CONCLUSION

As communicated previously, the paper investigated the IPSec based VPN sorting out a structure and made an exchange on its related traditions. The paper highlights IPSec and its irregularity with the current IP framework and routing. Before arranging IPsec based VPN yield of a structure were a first source and target. Regardless, in the wake of arranging the solicitations of VPN, the outcome was appeared in above figures and the best way to deal with setup the VPN compose is direct and convenient, which has a nice application prospect in the remote secure transmission and shape the ensured correspondence between two branches of an association. So, it is a monetarily adroit and secure response for the association customer to relate various goals around the world together by finishing IPSEC based VPN.

VI. REFERENCES

[1]. Djedjiga Benzid, Michel Kadoch, "Virtual Private Network over Wireless Mesh Networks" International Conference on Future Internet of Things and Cloud 2014. IEEE computer society.

[2]. O. E. Muogilim, K.-K. Loo, and R. Comley, "Wireless mesh network security: A traffic engineering management approach," Journal of Network and Computer Applications, vol. 34, pp. 478-491, 3// 2011

[3]. Ming-SongSun,Wen-HaoWu, "Engineering Analysis and Research of MPLS VPN" Network Information Center, Harbin University of Science and Technology, Harbin, china, IEEE 2013.

[4]. R.Maresca,M.Arienzo,M.Esposito, S.P.Romano and G.Ventre, "An Active Network approach to Virtual Private Networks" Proceedings of the Seventh International Symposium on computers and communications (ISCC'02), 2002.

[5]. Mateusz Korona, Krysztof Skowron, Mateusz Trzepinski, Mariusz Rawski, "FPGA implementation of IPsec protocol suiteformultigigabitnetworks" International Conference on Systems, Signals and Image Processing (IWSSIP), 2017.

[6]. Sebastian Marius Rosu, Marius Marian Popescu, George Drogoi, Ioana Raluca Guica, "The Virtual Enterprise Network based on IPSec VPN Solutions and Management"(IJACSA)International Journal of Advanced Computer Science and Applications.Vol.3, No.11, 2012.

[7]. Sonika, Monika, Sonal, "Network Security: Virtual Private Network" International Journal of Engineering and Computer Science ISSN:2319-7242, Volume3 Issue2 February, 2014.

[8]. Peter B.Busschbach, "Toward QOS-Capable Virtual Private Networks" Bell Labs Technical Journal, October-December 1998.

[9]. Tripti Sharma, Rahul Yadav, "Security in Virtual private network" International Journal of Innovations & Advancement in Computer Science IJIACS, ISSN 2347-8616 Volume4, Special Issue March 2015.

[10]. Antonin Mazalek, Zuzana Vranova, Eva Stankova, "Analysis of the Impact of IPSec on Performance Characteristics of VoIP Networks and Voice Quality" University of Defence, Department of Communication and Information Systems.

[11]. Junaid Latief Shah, Javed Parvez, "Impact of IPSec on Real Time Applications in IPv6 6to4 Tunneled Migration Network" IEEE Sponsored 2nd International Conference on Innovations

inInformationEmbeddedand Communications Systems ICIIECS'15, 2015.

[12]. LUOZhiyong,YUGuixin,QI Hongzhuo, LIU Yahui, "Research of A VPN Secure Networking Model" 2nd Internal Conference on Measurement, Information and Control, 2013.

[13]. LI Gang, XUE Yibo, WANG Dongsheng, Design and Implementation of a Gigabit Rate Network Intrusion Prevention SystemJ], Journal of Chinese Computer Systems, pp: 2025-2029,2006.

[14]. Shaneel Narayan, Cameron J.Williams, Daniel K.Hart, Max W.Qualtrough, "Network Performance Comparision of VPN protocols on Wired and Wireless Networks" International Conference on Computer Communication and Information (ICCCI) Jan 08-10, 2015.

[15]. Richard S.Kagan, "Virtual Private Networks-New Strategies for Secure Enterprise Networking" VPNet Technologies, San Jose, USA, IEEE 1998.

[16]. Victor Neumann, Clodomiro Unsihuay, Christian Lyra Gomes,Keiko V.Fonseca, PedroRodriguesTorres, "Parameterization of IPsec Framework for Security in the Smart Grid Interoperability", "Latency and Throughput IPsec Overhead" IEEE PES innovative Smart Grid Technologies Latin America(ISGTLATAM), 2015.

[17]. IETF-RFC 6071. IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap. Internet Engineering Task Force (IETF). Request for Comments, p. 1-63, February 2011. ISSN: 2070-1721.

[18]. Cryptography and network security, William Stallings "Voice Security in Virtual Private Network "Deep Shikha Computer Science and Engineering ITM University Sec 23-A Gurgaon, India. Volume 3, Issue 7, July 2013

[19]. Mohd Nazri Ismail and MohdTaha Ismail. "Analysing of Virtual Private Network over Open Source Application and Hardware Device Performance". European Journal of Scientific Research (EJSR), Vol. 28 No.2, pp. 215-226, Euro Journals Publishing, Inc. 2009.

[20]. Rosen E, Rekhter Y, RFC 4364 BGP/MPLS IP Virtual Private Networks (VPNs)S], IETF, 2006

[21]. Pylarinos,S.Louvros,K.IoannouA.Gramps and S.Kotsopoulos, "Traffic analysis in GSM/GPRS networks using voice pre-emption priority, "World Scientific and Engineering Academy and Society, pp.120-123, 2005

[22]. Luo Zhiyong, Duo Zhihua, Qiao Peili, Formal Description of IPSec Security Policy in VPN NetworksJ], Journal of Hua Zhong University of Science and Technology (Natural Science Edition), pp: 14-16,2011.

[23]. Ma Chunguang, Firewall Intrusion Detection VPNM], Beijing University of Posts and Telecommunications Press, pp: 158-166,2008.

[24]. GuangLu Sun, Yibo Xue, Yingfei Dong, Dongsheng Wang, Chenglong Li. A Novel Hybrid Method for Effectively Classifying Encrypted TrafficC], Proceedings of IEEE Globecom, pp: 7-9, Miami, USA, 2010.

[25]. Wang Wende, AES-Rijndael Algorithm IPSec VPNJ], Liaocheng University (Natural Science), pp: 107-110,2008.

[26]. Cohen R. On the Establishment of an Access VPN in Broadband Access NetworksJ], IEEE Communications Magazine, pp: 156-163,2003.

[27]. LI Gang, XUE Yibo, WANG Dongsheng, Design and Implementation of a Gigabit Rate Network Intrusion Prevention SystemJ], Journal of Chinese Computer Systems, pp: 2025-2029,2006.

[28]. L1U Kelong, QING Sihan, Meng Yang, An Improved Way on Kerberos Protocol Based on Public-Key AlgorithmsJ]. Journal of Software, pp: 872-877,2001.

[29]. Neuman, B. Ts' 0, T. Kerberos, An Authentication Service for Computer Networks. IEEE Communications, pp: 12 4-130, 1994.

[30]. SUN Guang-Iu, LANG Fei, YANG Ming-Ming, Traffic Measurement System Based on Hybrid MethodsJ]. Electric Machines and Control, pp: 91-96,2011.