International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 6 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT195630

Design and Deployment of IPSec VPN Using CISCO Network Infrastructure

Sadia Jabbar Anwar*[1], Ibtehaj Ahmad[2]
*[1]National College of business administration & economics, Bahawalpur, Punjab, Pakistan
[2]Department of Computer Science, Northwestren polytechnical University, Xian, China

ABSTRACT

Online networks have many threats regarding security. The threats are targeting agency networks, private networks or other networks via gaining access to or changing essential information. Less secure networks deliver authorization to the users to access records in a network. Communication managers need powerful police forces to prevent access, misuse or alteration of secure network information. Small businesses or small businesses use firewalls, antibiotics or anti-spam software to protect the network, but do not provide sufficient network protection. Security in the corporate network is an important part of network protection due to the most common hacker goals. A private network is a reliable way of communicating with various business units and communicating with internal networks. Internet Protocol Security (IPsec) Virtual Private Network (VPN) is one of the most powerful security tools in the field of recording and security options. This is the safest and most secure option available in the Private Network store as a combination of two or more networks in remote areas. The goal of this research is to integrate VPN Services and establish IPsec protocols for small business security. The study is based on the networks of National College of business administration & economics (NCBA&E BWP) and its campuses by using the Cisco routers for a secure and private communication interchange between them. The result shows that IPsec VPN is an appropriate way of communication for Small and Medium-Sized Enterprises (SMEs).

Keywords: IPSec, Virtual Private Network, Network Security, Small and Medium-Sized Enterprises, Virtual Private Network, Internet Protocol Security

I. INTRODUCTION

Online networks over a public location are always under the risk of security threats. Hackers are always trying to hack any enterprise's networks because these are the commonplace for the security attacks. Organizations and private networks are included in enterprise networks. Different types of devices are used for defensive organization networks, but they are highly priced and now not are easy to use and more expertise staff is required to handle it. VPN is a secure system for connecting business enterprise branch or private community in far-flung regions and it is not always highly priced. It encrypts information and data with the usage of a tunnel between two hosts. This method makes it possible for the hosts to switch records securely and effectively over a public network. Similarly, Small and medium-sized organizations can pick the VPN carrier due to their reduced costs, and reliable network security, rather than using the WAN services.

In order to secure virtual network, VPN makes use of several protocols. To secure network connectivity IPsec is one of the most powerful VPN protocols. It is an appropriate VPN protocol for connecting agency

department places of work with headquarters because; IPsec uses a tunnel among end-to-end connections. By the use of IPsec VPN the information is more reliable and secure. A standard for SMEs is IPsec and it is most powerful VPN protocols, as this approach does not cost a lot and is simple to configure [1]. SMEs are capable of configure the IPsec VPN because no in-depth knowledge is required. On the opposite, any enterprise, which has many personnel and branches, may be in need of a network engineer for the configuration of an IPsec VPN.

IPsec can be defined as a security scheme for intercommunicating with two networks from one of kind places. The IPsec is built for thriller verbal exchange and it depends on the IP network, through the usage of actual and cryptographic protection offerings. It uses a framework to comfortable statistics, to maintain the facts sent via the IPsec have data integrity and records confidentiality. IPsec VPN assures peer-to- peer facts safety, via the usage of encryption. It is far the maximum famous VPN technology for cheap, aid effective, smooth to install and securing an organization, private, or authority's network [2].

IPsec has mainly two types of modes i.e. Transport mode and Tunnel mode. In the tunnel or exploitation world, there is a common tunnel between the routers or the port. The door will change to file the files to the owner. Using the exploitative environment, IPsec reads the IP and load titles. Tunnelling methods provide complete protection for pocket IP with the help of IPsec protocol and can protect visitors on attractive networks. Tunnel mode works at the gates to the gates, from the serial port to the gates. In the transfer mode, the data is send before, as default in the IPsec modem. Although IPsec protocols cannot send the IP head, they integrate the IP packets.

This research article organized in five sections. Section one describe introduction, in section two previous methods are discussed, section three is about research methodology, results are discussed in section four and final section is conclusion.

II. LITERATURE REVIEW

VPN is a private network was created with the help of a public network by using a technology. The employees can securely access their employer's internal community from any region, on a public community. Secure tunnels are used when a VPN is trying to connect to the internal network from remote areas. Virtual networks are used by VPN with the aid of the usage of encryption and a tunnelling protocol. In general, a corporation makes use of WAN for connecting department nodes to the main office. WAN is high priced and the carrier increases when the number of nodes/sites and their relevant sites increase. In contrast, VPN is feasible than WAN for designing community and lowering fees. By using the VPN it can save the cost from around 30 to 80 percentage because VPN ensures reliable conversation by means of using an encrypted channel. There are unique protocols to establish VPN and the IPsec protocol is the most popular for securing tunnels [3]. The researcher investigates various techniques for secure network communication.

Author describes that IPSec competencies will be carried out best if its techniques are efficiently familiar and designed. Manual IPSec policy configuration is not efficient and prone to mistakes. A wrong analysis may be a serious safety breach. A coverage control machine is demanded to regularly manage and affirm numerous IPSec policies. It is a better to make certain the end-to- end protection carrier, so that all the policies are implemented in a good way and there are no security issues. The authors have examined conflicts because of various interactions amongst guidelines. They have defined protection regulations in these two degrees requirement stage security policy and implementation stage protection coverage [4].

Author described that network real-time applications are growing more on these days in networks, especially video and audio streaming, conferencing and telephony programs. The original layout of those applications and their corresponding protocols did not forget safety and confidentiality, which shape a convincing requirement among the Internet users. To apply the IPSec safety protocol is one of the solutions to execute protection on community traffic, which provides verification and encryption to community packets, with the help of which community programs are secured. A crucial query that arises is that how the overhead of IPSec operations have an effect on the performance of community programs in the context of time-sensitive software, such as VoIP and comparable real-time packages [5]. In this research author describes that IPSec digital personal networks are drastically used to establish secure network connections between a pair of hosts, amongst a safety gateway or among a pair of protection gateways. he complexity and type of rules in an IPSec coverage may bring about a mixture of regulations, which may not provide the required protection services, however additionally compromise the security of the network. Efficiency has no longer been a primary scenario for present IPSec stumble upon detection approaches given that they manner the IPSec tips in a disconnected manner. Guidelines are being updated often so these strategies are probably inefficient in dynamic situations. The overall performance of the said coverage is essential in network environments where network administrator desires to frequently upload or delete suggestions to current policy [6-7].

Authors discuss that cell advert hoc networks do not possess base stations or additionally lake of access factors and this makes the advert hoc networks susceptible to jamming assault that is the maximum common assaults. Considering the fact that many advert hoc networks employed IP primarily based routing, they have protection and safety of statistics and communiqué could be relaxed through using it. This research inspects the general overall performance of MANET with the software of IPsec protocol and to see the effectiveness of IPsec protocol in conveying protection at the same time as the MANET is susceptible to jamming assault. On this look at, Riverbed Modellers academic edition simulator is used to simulate an evaluation of mobile nodes with and without IPsec, the use of advert hoc on call for Distance Vector (AODV), Optimized link nation Routing (OLSR) and Thoroughly Ordered Routing algorithm (TORA). The simulation outcomes suggest that AODV routing protocol gives the most important percentage increase of delay and retransmission try in normal operations. However, whilst it has far beneath assault the AODV with acquired the very excellent throughput. Put off and retransmission attempts are the satisfactory with OLSR. by using the MANET simulations the usage of 3 awesome protocols, with imposing the IPsec protocol presents an overhead to the packets at some point of the transmission have impact of lowering the throughput on the network in addition to growing the postpone and retransmission attempts. Despite the fact that there may be a moderate put off. We come to realize that the IPsec protocol have the benefit to provide safety offerings said in the simulation wherein the MANET below attack do better with the employment of IPsec protocol. In ordinary operation, the OLSR routing protocol with IPsec provides good throughput fee although it decrease the throughput by a high percentage [8-12].

By comparing the RTT (Round Trip Time), Throughput, Jitter and CPU usage in VoIP networks. In their research, they used home edition windows 7 and Fedora 16 to compare VoIP performance with and without IPsec. Authors applied the same conditions in both the window environments one after the other by applying identical protocols and compared the results. It became clear from the effects that the performance of IPv4 became better than IPv6. There have been small variances in UDP throughput for IPv4, IPv6 and

6in4. In maximum of the checks, the performance of IPv4 changed into fine without IPsec. On the complete 6in4 with IPsec had the best RTT, Jitter and CPU utilization and the bottom Throughput. Fedora 16 achieved better than windows 7 for RTT and Jitter while consequences had been as compared. While for Throughput, on Fedora sixteen the consequences had been fairly higher for some formats. While IPsec turned into not enabled on Fedora 16, the consequences were steady for IPv4, IPv6 and 6in4 not like for home windows 7. The outcomes fluctuated more on home windows 7 both with and without IPsec. In end, we can say that the effects for IPv4, IPv6 and 6in4 without IPsec confirmed that the overall performance changed into higher for every kind of addressing. For some codecs the overall performance, become lots higher without the encryption. Their research indicates that even though IPsec can upload safety, it could reduce the VoIP overall performance in terms of higher put off [13-16]. IPSec and SSL (Secure Socket Layer) have different blessings and errors, as other protocols. The authors provide information on IPSec and SSL security. Each protocol has its own rights. Selecting IPSec or SSL relies upon on the safety. If specific issues are needed and is supported by SSL it is much better to pick SSL. If standard services or Gateway-to-Gateway communications are needed then IPSec is given preference compared to others. IPSec makes use of a shorter form of HMAC than SSL for this reason SSL statistics integrity is more comfortable. SSL is more nicely desirable with firewall than IPSec except IPSec and Firewall are blended in the identical device. Not like SSL IPSec clients want unique IPSec software for some distance off access. In a low bandwidth network or dial up networks, using compression is beneficial. SSL does not aid that Pre-shared scheme is much less complex to configure and does not require any PKI infrastructure IPSec allows compression but regrettably, SSL does not help it [17].

Examined to help the conveyance of gathering based remote collective work in the training based learning area of computer networking. Generally, this has introduced challenges in scale, administration, security and mechanical asset to help conveyance, evaluation and learning. With the collaboration of Cisco System team they conducted a research to investigates the innovation potential for an around the work ― simulated ‖ internet and reports on beginning examination. They used blended technique in this research, which is very affective for students. In this study, they traced packets instead of real devices. Packet tracer has functionality to support multiuser support one to one, one too many and many too many. In this research, they used many to month remote or native collaboration eventualities on the available to all. The experiment has already tested the potential for disparate people from assorted areas to associate and interact in a very semi- synchronous, essentially synchronous sensible activity [18]. The present outline and assemble a networking lab, utilizing both physical and visual tools to give trail lab conditions to college students of Software Science Engineering at the University of Salamanca. The tests meet our education modules objects yet additionally address subjects at expert's level. The investigations were planned around the key thought of continually picking the apparatus most appropriate to the student's educational level and of presenting abilities that encourage learning of working framework charges for network administration gear – at first through a GUI and then using CLI. The idea is to exploit the advantages of network emulation tools as low cost solutions that complement work with physical devices. The work carried out with real devices in the prototype of voice and data integration enabled us to validate our proposal and to consider buying new hardware in the future. Moreover, its simulation mode utilizes movement to give a perspective of created activity. Its fundamental restriction is the movement's analyzer and upheld conventions; activity is demonstrated all together, which make difficult study

to traffic at a fastidious link in more unpredictable system outlines. As a graphical network simulation tool that enables one to work with a more noteworthy number of conventions and activity analyzer, for example, Wireshark, we would pick GNS3. It runs pictures specifically of the working framework of real network devices, narrowing the separation between working with simulation and real devices. GNS3 produces setup documents that can be stacked to genuine equipment, permitting coordination of genuine devices, permitting coordination of real and physical labs offering relatively potential outcomes for the outline of complex networks. The main restricting element is the machine running the virtualized arranges components, yet this could likewise be scaled. The planned examinations incorporate ideas running from IP addressing (basic level) to the mix of voice and information activiy (third level). Following on from necessary services such a DNS and DHCP, dynamic and multicast routing, the new of IP (IPv8), VLANs and VoIP, we are as of new taking a shot at the plan of research facility practices for subjects, for example, remote systems and system security [19].

III. RESEARCH METHODOLOGY

A. Implementing IPSEC VPN for SMES

Most often, IPsec is carried out end-to-end hosts or on host gateways/routers. We will describe the integration of OS (Operating System) with the IPsec, IPsec protocol processing and its implementation of various community devices in Section.

B. Host Implementation

Where IP packets originate called the host device. There exist some advantages in implementing such device:

a) Host offers end-to-end safety.
b) Host offers safety continuity.
c) The host has the ability to that it can apply all IPsec modes.
d) For the purpose of IPsec authentication, it can keep a person context.
e) There are strategies wherein the IPsec host implementation is finished. The one is the implementation with OS and that is known as the OS incorporated. The second one is implementation with community layer and statistics hyperlink layer, this is known as ―Bump inside the Stack‖.

C. OS (Operating System) Integration

The IPsec offers facility to combine it with OS inside the host implementation gadget. IPsec is carried out in this layer, as part of the community layer protocol. To build the IP header, the IPsec layer makes use of the company from the IP layer. We have some blessings of integrating the IPsec with OS. They are following.

i. If the IPsec is firmly protected with the community layer, it can be used for community services consisting of person context, fragmentation and PMTU.

ii. It helps all IPsec modes, when one join in IPsec with OS.

iii. The safety services will be going smoothly, inclusive of a web transaction by this integration. The safety services are applied as the key control. The combination a few of the community layer and IPsec takes vicinity perfectly.

D. Router Implementation

IP packet protection is ensured over part of a community when the IPsec implementation on a router is implemented. The router restricts users from getting into the personal community by means of the use of IPsec authentication and authorization, Router implementation is of sorts: native implementation and Bump within the wire (BITW).

E. Native Implementation

IPsec is running on a router software program. Therefore, it may not be necessary to identify the IPPS device above the router interface. The ―Fig. 1‖, shows the routers that are connected to the local IPsec. The following diagram indicates that the routers A and B are related to the use of local installations that use VPN software to connect jrouters A and B.

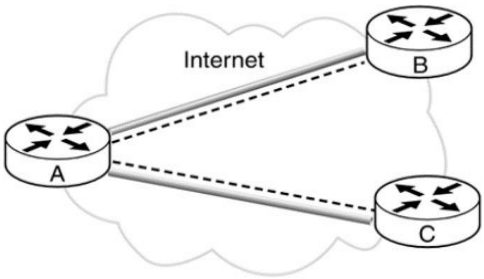

Figure 1. Implementation architecture among the three routers over the public network

F. Bump in the Wire (BITW)

IPsec is performed with the IPsec machine in implementing the BITW. The device is connected to the router's help. The security guard that leaves the network. The next BITW (Bump in the cord) describes how to implement the IPsec device in the Router RB port to the router RB. Then, the device that justifies and gives IP access is from the router RBp. Fig. 2depicts the implementation of BITW among three routers over public network .

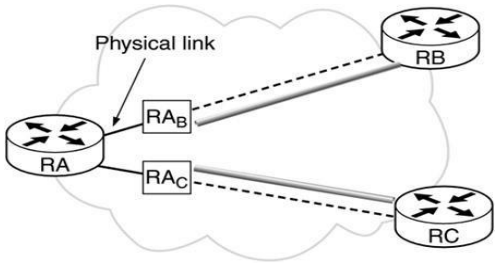

Figure 2. BITW (Bump in the Wire) over public network

G. IPsec Authentication

The IPsec authentication show client's identification protects statistics from out of doors attacks and make certain that data remain confidential. IPsec SAs allows specific varieties of authentication.

H. IPsec Authentication

The IPsec authentication show client's identification protects statistics from out of doors attacks and make certain that data remain confidential. IPsec SAs allows specific varieties of authentication.

I. Pre-Shared secrets

Pre-shared secrets and techniques offer a not unusual password for figuring out their personal customers. One peer has a public IP that keep secret data and it takes any other peer in Pre-shared secrets. Then the information trade between those friends begins, they create vital keys while a settlement element arouse among them. The pre- shared keys configured on each facet, to observe a few other IP cope with and initial mystery keys. The key technology manner starts while number one number one is start up. (Tiller, 2000)

J. J. PAP (Password Authentication Protocol)

PAP is a verification protocol to validate customers. It calls for password and username for authenticating a person whilst coming into in a machine. PAP have all statistics as easy content. However, in playback assaults it is not able to comfortable the device.

K. K. CHAP (Challenge Handshake Authentication Protocol)

The CHAP protocol is used the three-manner handshake rule to pick out a far-flung man or woman while it is miles the usage of the device. It uses a layered authentication gadget of identification this is hard to break. For its customers, ISP (net service company) gives PPP (point-to-point) session. While users dial a cell phone, the ISP permits the person modem to set up PPP with a modem furnished by ISP. Then, the CHAP session starts evolved so it request a miles off character's username and password. By way of changing packet identifier, and a variable undertaking fee, CHAP saves the person from

playback attack. CHAP shop the password in its database so it is miles the trouble by the usage of it.

L. L. IPsec in Action

As a matter of security in networks IPSec in very popular protocol to use. It is also an easy to use and implement strategy. Our IP packet remains safe and can be sent to the other site while using it. By its use and its tunnel mode our records remains intact and any organization's personal data is not

shared with anyone. Only authentic users will have the access.

M. M. End-to-End Security

Every IP packet is secured when they begin and give up any verbal exchange with the aid of the usage of the stop-to-end protection gadget. Client's coverage selectors have a main effect on the safety. SAs afford security between the give up points from each facets of the network. IPsec or tunnel mode is used for quit-to-cease security but in tunnel mode, an extra IP header required to be added. Even as having benefits this quit to end security also have some drawbacks. Precise forms of packages are used that need to check out or regulate and the brief packet will drop while end- to-stop connectivity is installed and make use. Extraordinary applications will no longer recognise about the IP packet, due to the fact they may be unable to make any selections. Within the presence of cease-to-quit community protection, NAT (community deal with Translation) does not run on the device.

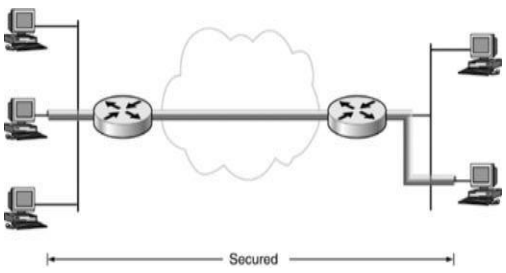

Figure 3. An end-to-end network security

Fig. 3 depicts an end-to-end network protection even as using IPsec VPN tunnel between network hosts.

N. . Network security policies and Implementation

The following diagram describes the community protection policy and implementation techniques. In order to decide network protection rules it is a high-quality model for community admin and management groups. Confidentiality, integrity and availability are created through the network protection regulations. The type of threats and what desired to be done are decided through those guidelines. While the errors find out and some weak holes are determined then it is necessary that the security guidelines will be reviewed and analyzed constantly. However, the present network protection guidelines are carried out with the help of unique methods, for example, with the use of firewall, NAT, proxy, VPN and password encryption.

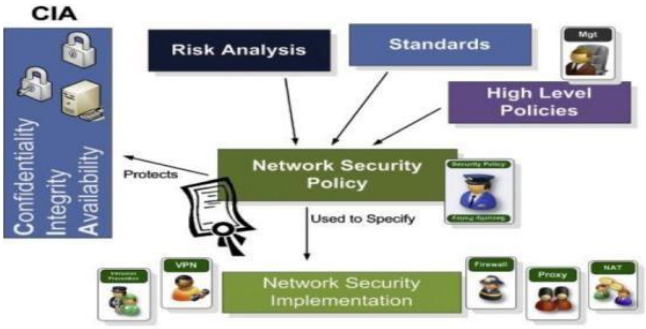

Figure 4. An example of network security policy and implementation system.

O. Configure Site-to-site IPsec VPN using the Cisco Packet Tracer.

Now, it possible to implement IPsec VPN with the help of Packet Tracer by using security devices among the routers available in it. Because all this due to Cisco, it made it possible. With the right setup and by selecting the right devices on Packet Tracer, we can successfully simulate a site-to-site IPsec VPN.

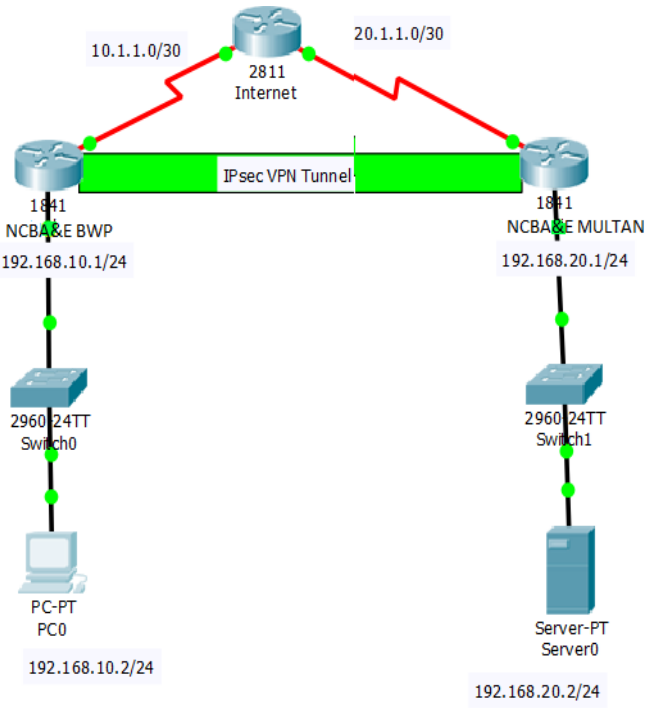

Figure 5. Network diagram for the Configuration of IPSec VPN tunnel

In fig.5 as the Internet router, Cisco 2811 router is used, whereas the 1841 router is implemented in NCBA&E BWP and Multan campuses. These two campuses are the sites on which we have to configure the IPSec VPN policy. We have an https server in Multan that needs to be securely accessed from BWP. To make sure that https request from BWP to the server in Multan go through securely, we want to set up site-to-site IPsec VPN between BWP and Multan campuses.

IV. RESULTS AND DISCUSSION

A. IPsec VPN Verification

i. Verifying the tunnel before interesting.

Issue the ―show crypto ipsec sa‖ command on BWP router. Notice that the number of packets encapsulated, encrypted, encapsulated, and decrypted are all set to 0.

ii. Creating interesting traffic. Ping PC-0 to Server-0.

iii. Verifying the tunnel after interesting traffic.

On BWP router, re-issue the ―show crypto ipsec sa‖ command. If the number of packets are more than 0, then it suggest that the IPsec VPN tunnel is working.

iv. Verifying the tunnel

On BWP, re-issue the ―show crypto ipsec sa‖ command. If the number of packets has not changed, then it suggests that uninteresting traffic is not encrypted.

v. Checking Results

Upon completion, the percentage should be 100%. To see the required components and results. Click check results to see feedback and verification of the routers. Fig. 5 shows the ping results from PC-0 to Server-0.

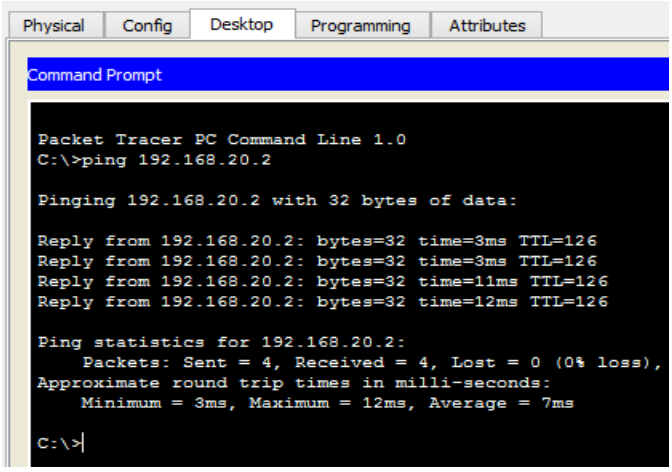

Figure 5. Ping results from PC-0 to Server-0

B. Comparison of IPSec VPN with other Protocols

Many protocols are being used in VPN but we choose to have two main kinds of internet- primarily based VPNs: IPSec VPNs and SSL VPNs. The IPSec operates at Layer three, it has no effect at the higher network layers. IPSec is generally used for inter-website online connections; it is possible that the computers connected to the network at a given website online will not even have IPSec capabilities. In a faraway-get entry to surroundings in which there is no IPSec-enabled router, however, the pc should run a duplicate of the IPSec stack.

One of the drawback of an IPSec remote-get admission to technique is that after a computer is attached to the

IPSec-based network, all of the extra devices connected to that local network may be able to gain get right of entry to throughout the WAN to the corporate network. Therefore, it is possible that a Trojan horse at the "kid's laptop" can be spread.

Eventually, for component-time teleworkers, it is turning into difficult to use the house net connection for company network access if the use of an IPSec-encrypted VPN tunnel. More and more, ISPs bear in mind whatever IPSec- encrypted to be an "enterprise-elegance" transmission. As such, they need to price better charges for IPSec site visitors and will block IPSec traffic if the service kind is not always enterprise magnificence.

Table I shows the compression between VS and SSL.

TABLE I IPSec VS SSL

Function	IPSec	SSL
Configuration	hard	Easy
Client Authentication	Must	Option
Pre-Shared Key	Yes	No
Interoperability	Yes	No
TCP Application Support	All	Some
UDP Support	Yes	No
Throughput Rate	High	High
Compression Support	Yes	Open SSL only
Handshake Time	slow	fast

V. CONCLUSION

The paper is an answer to the research questions that aroused in the mind of any person who is using the network especially students and staff of the NCBA&E campus BWP and MULTAN. Further, it has to make tunnels between its other campuses too. This is a study of the VPN and IPsec protocols. Many methods of the IPsec implementation system are consisted in it. The aim of the study changed into to exemplify the service of VPN and to know that the VPN protocol (IPsec) is used for safeguarding a connection of SME's regions, which are a ways flung from the principle office or campus. Sharing valuable statistics and connecting the friends of work from one region to different public community places are usually a danger of injecting, converting or modifying the authentic information. To overcome the threats for network, the IPSec VPN is a secure protocol to create the non-public connection at low charge. In comparison with the WAN device, the VPN is an inexpensive one. In short we conclude that, the VPN makes use of numerous authentication structures and creates a personal tunnel over a public community. Most effective the authorized customers are prevalent within the network, so unauthorized customers are unware of the network tunnel. IPsec VPN can be applied on hosts and router gateways. The whole IP packet is encrypted and then authenticated in tunnel mode. Then, a new IP packet is created with a brand new IP header connected and encapsulated. Tunnel mode is used to create virtual personal networks for community-to-network communications (like between routers to other sites and hyperlink them), host-to-community communications (like far-flung consumer get right of entry to) and host-to-host communications. As a result, IPsec VPN is an appropriate answer for SMEs.

VI. REFERENCES

[1]. Liu D, Miller S, Lucas M, Singh A, Davis J. Firewall policies and VPN configurations. Elsevier; 2006, Sep 28

[2]. T. Bayley, B. Rohani, A. Johansson, M. Caldera and H. Zepernick, "Call quality monitoring for VoIP," 2011 5th International Conference on Signal Processing and Communication Systems (ICSPCS), Honolulu, HI, 2011, pp. 1-4.

[3]. E. Ramadhan, A. Firdausi and S. Budiyanto, "Design and analysis QoS VoIP using routing Border Gateway Protocol (BGP)," 2017

International Conference on Broadband Communication, Wireless Sensors and Powering (BCWSP), Jakarta, 2017, pp. 1-4

[4]. M. A. Ramirez-Reyna, F. A. Cruz-Pérez, S. L. Castellanos-Lopez, G. Hernandez-Valdez and M. E. Rivero-Angeles, "Differentiated Connection Admission Control Strategy for Wireless VoIP Networks with Adaptive Modulation Coding," 2018 International Conference on Computing, Networking and Communications (ICNC), Maui, HI, 2018, pp. 31-37.

[5]. J. H. Klink and T. Uhl, "Quality-aware network dimensioning for the VoIP service," 2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, 2017, pp. 1-6.

[6]. N. Kamat, Ju Wang and J. C. L. Liu, "A delay-efficient rerouting scheme for VoIP traffic," 2003 International Conference on Multimedia and Expo. ICME '03. Proceedings (Cat. No.03TH8698), Baltimore, MD, USA, 2003, pp. III-245.

[7]. E. Luchian, R. Terebes and M. Cremene, "Design and implementation of a mobile VoIP system on Android," 2014 11th International Symposium on Electronics and Telecommunications (ISETC), Timisoara, 2014, pp. 1-4.

[8]. M. Behdadfar, E. Faghihi and M. E. Sadeghi, "QoS parameters analysis in VoIP network using adaptive quality improvement," 2015 Signal Processing and Intelligent Systems Conference (SPIS), Tehran, 2015, pp. 73-77

[9]. N. Brahmbhatt, P. Mann and A. Rawat, "Design and implementation of compatible VoIP," 2017 6th International Conference on Computer Applications In Electrical Engineering-Recent Advances (CERA), Roorkee, 2017, pp. 103-107.

[10]. C. Cioponea, M. Bucicoiu and D. Rosner, "Analysis of VoIP encryption performance using dedicated hardware," 2013 11th RoEduNet International Conference, Sinaia, 2013, pp. 1-4.

[11]. Feng, Z. Wang, C. Zhang and Y. Fang, "Design and Analysis of a Prioritized Adaptive Multiple Access Scheme for VoIP over WLANs," 2015 IEEE Global Communications Conference (GLOBECOM), San Diego, CA, 2015, pp. 1-6.

[12]. R. Dantas, C. Exton and A. Le Gear, "Comparing Network Performance of Mobile VoIP Solutions," 2018 6th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), Bamberg, 2018, pp. 43-50.

[13]. Murhammer, M.W., Atakan, O., Badri, Z., Cho, B., Lee, H.J. and Schmid, " A Comprehensive Guide to Virtual Private Networks", Volume III, Cross-Platform Key and Policy Management, 1999.

[14]. J. Gupchup, Y. Hosseinkashi, M. Ellis, S. Johnson and R. Cutler, "Analysis of problem tokens to rank factors impacting quality in VoIP applications," 2017 Ninth International Conference on Quality of Multimedia Experience (QoMEX), Erfurt, 2017, pp. 1-6.

[15]. C. N. Lin, T. L. Lin, T. S. Chen, J. Chen and W. J. Chen, "VoIP communication quality and flow volume preference — A SIP and Red5 example," 2016 3rd International Conference on Systems and Informatics (ICSAI), Shanghai, 2016, pp. 782-786.

[16]. A. Lebl, M. Mileusnic, M. Stanic, D. Mitic, V. Matic and Ž. Markov, "Packet interleaving and its influence on the VoIP connection quality," 2017 13th International Conference on Advanced Technologies, Systems and Services in Telecommunications (TELSIKS), Nis, 2017, pp. 132-135.

[17]. C. Lili, "VoIP System Simulation Design and Implementation," 2012 Second International Conference on Instrumentation, Measurement, Computer, Communication and Control, Harbin, 2012, pp. 296-298.

[18]. S.R.Javid, Role of Packet Tracer in learning Computer Networks,‖ International Journal of

Advanced Research in Computer and Communication Engineering Vol. 3, 5 May ,2014 no. 5, pp. 6508–6511.

[19]. S. Zeadally and F. Siddiqui, "Design and implementation of a SIP-based VoIP architecture," 18th International Conference on Advanced Information Networking and Applications, 2004. AINA 2004., Fukuoka, Japan, Vol.2, 2004, pp. 187-190 .

Cite this article as :

Sadia Jabbar Anwar, Ibtehaj Ahmad, "Design and Deployment of IPSec VPN Using CISCO Network Infrastructure", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 6, pp. 237-247, November-December 2019. Available at doi : https://doi.org/10.32628/CSEIT195630
Journal URL : http://ijsrcseit.com/CSEIT195630