Statistical Results of IPSec in IPv6 Networks

Tina Sharma
Research Scholar
Department of CSE
Suresh Gyan Vihar University
Jaipur, Rajasthan, India

Savita Shiwani
Associate Professor
Department of CSE
Suresh Gyan Vihar University
Jaipur, Rajasthan, India

ABSTRACT

IPv6 is an Internet layer protocol used for assigning network addresses to communicate with devices across the Internet. It is an extended version of IPv4 networks. IPv6 is efficient and secure because of it's built in security feature. IPSec is intended to provide security to IP networks. It provides authenticity, integrity and confidentiality of data by using secured tunnel. Organizations which have their branches located across different geographical locations need to protect their data by making secure connection with their respective peers. This secure connection can be implemented using IPSec which avoid security threats related to confidentiality and integrity of data.

Keywords

IPv6, IPv6 security, IPSec, GNS3, Wireshark

1. INTRODUCTION

IPv6 is a next generation Internet layer protocol which is designed by Internet Engineering Task force (IETF) to overcome the limitations of IPv4 networks. IPv4 addresses being 32 bits in size provide approximately 4.3 billion addresses as compared to IPv6 address which is 128 bits in size and provides approximately $3.4*10^{38}$ addresses. Security attacks have been common across the Internet therefore in order to protect IPv6 networks from security attacks, IPSec is made an inbuilt component of IPv6 and it ensures the integrity, authenticity and confidentiality of data transmitted across the networks. IPSec is a networking layer protocol which is used to protect the data between two devices. IPSec encrypts and authenticates the packets before sending them across the Internet. Using IPSec in IPv6 further enhances the security and protects the data sent in IPv6 networks.

2. IPv6

IPv6 or next generation protocol is a new version of Internet protocol designed to replace the older version of IPv4 due to its limitations. IPv6 is an improved version of IPv4 with some advanced features added to enhance its performance. Some of them are auto configuration, multicast, better support for qos etc. Many new networking devices such as PDAs, wireless networks and other integrated electronic appliances require the new and improved version of Internet protocol.

IPv6 has a simplified header structure than IPv4 and has a fixed payload of 40 bytes due to its extension header feature. Ipv6 address consists of 128 bit which is composed of 8 groups of four hexadecimal each. Each set of four hexadecimal digits is separated by colons. It is divided into eight blocks of 16 bits each.

3. IPSEC

IPSec is an Internet layer protocol designed for providing security at the network layer. It is used to provide authenticity, integrity and confidentiality between two peers communicating over the network. It ensures safe transmission of data across networking devices.

The objective of IPSec is to provide:

Authentication – It ensures data has been sent by an identified sender.

Data Confidentiality – It provides protection to data by encrypting the information being transmitted.

Data Integrity – Specifies that there are no changes while transmitting data across the networks and packets are sent to the receiver intact.

Avoid replay attacks – The transmitted packets do not get altered by any of the attacks deployed by any attacker.

IPSec is performed using different algorithms categorized as encryption (aes, 3des), integrity (md5, sha), key exchange (diffie hellman) and authentication methods (pre shared, certificates). These algorithms are needed for implementation in two different phases of IPSec's IKE method. Hash is used in authentication protocol and encapsulation security protocol. IPSec uses Hashed Message Authentication Codes (HMAC) and provides hashing using MD5 (Message Digest 5) and SHA 1 (Secure Hash Algorithm 1). Diffie Hellman key is used in IPSec for two systems who want to establish a secure communication and uses a shared secret key which is known only to them. The shared secret key is generated from public and private keys of both peers. AES is a symmetric key algorithm where the same key is used for encryption and decryption. AES encrypts block size of 128 bits using key size of 128, 192 or 256 bits. AES algorithm consists of steps such as SubBytes, ShiftRows, MixColumns and AddRoundKey. The first stage of the process consists of key expansion where round keys are generated using cipher key. IPSec uses AES-CBC mode (cipher block chaining mode) for providing stronger security to the data. Pre Shared key is used in IPSEC in IPv6 networks to share a secret key between two peers. This shared secret key is calculated during the phase I of IPSec's IKE phase 1 configuration. It is used to provide authentication information between two devices who wish to securely transmit information by creating a secure channel.

Advantages of IPSec are packets at the network layer are encrypted and do not provide any overhead in other operations therefore it increases performance. It is scalable and can be implemented in any IP enabled networks. It provides various security mechanisms such as confidentiality, integrity checking and replay protection. Implementations of IPSec do not affect upper layers thus it ensures application transparency. Disadvantage of IPSec are that it is implemented at the end points i.e. security gateways and requires large processing power. Security is compromised if shared keys are exposed. Complexity in maintaining and deploying IPSec can lead to configuration errors due to which organization’s network can lead to security risk.

4. RELATED WORK

Due to increase in demand of IP addresses and shortage of IPv4 addresses, [1] organizations have started using IPv6 addresses to accommodate their needs. [2][3] IPSec is difficult to implement due to modification of IP addresses during the translation process in IPv4/Ipv6 networks. [4]IPSec helps in avoiding spoofing attacks in tunneling process due to specification of valid IP addresses at tunnel endpoints.

There are two types of security issues such as mechanism based security issues and ipv4/ipv6 coexistence based security issues [2]. [4]The attacker can launch denial of service attacks by joining the multicast group and can access information about particular’s node addresses. Attackers can attack a particular host during reconnaissance phase during which it can find any host with security vulnerabilities. It is achieved by sending false messages using multicast address and captures the identity of the host who responds to those messages.

Man in the middle attack on IPv6 networks enables attackers to access the IP address information of a connected node and sending that information to another node on a network. To securely transmit information across the web and in a reliable manner, end to end connectivity and security is needed. [5]Managing costs, complexity of dual networks and interoperability issues in coexistence of ipv4 and ipv6 is a cumbersome task. Network systems can be secured with the help of IPSec security protocol which provides secure connection and is a mandatory component of IPv6. [6][7]IPSec can endanger a network system due to several factors such as improper implementation of policies in tunnel or transport mode and incompatible rules between two end systems which can allow unwanted traffic to be passed through firewalls. [8] Implementing networking configurations including IPSec in a large complex networks can sometimes lead to error and cause network vulnerabilities which ultimately plunges corporate network into risk. [9] Secure Neighbor Discovery Protocol (SEND) provides protection against neighbor discovery attack. It uses cryptographically generated addresses (CGA) to protect IPv6 addresses from stealing and spoofing. [10] In VPN IPSec is implemented by creating a tunnel between two end users. The packet is encrypted based on the need and encrypted traffic is sent across the network with the help of a tunnel. Advantage of IPSec in VPN is that it provides end to end encryption and provides services such as authentication and encryption. It has no affect on higher layers above layer 3 i.e. network layer at which IPSec operates. IPSec can be used to protect information transmitted between two end sites and data which is used to provide authentication services needs to be protected. [11]Stealing usernames and passwords during logging activities are vulnerable to attacks during authentication. [12] There are several security threats at different levels such as traffic analysis, spoofing of MAC addresses, flooding attacks etc.

5. METHODOLOGY

GNS3 is helpful in simulating large networks based on real CISCO IOS images and evaluates the performance of complex network scenarios. It can be used to capture network traffic and detect any flaws in the simulated network with the help of software called wireshark. Wireshark is able to capture packets with help of pcap. Deeper understanding and statistical analysis of packets can be done through various tools available in wireshark program. GNS3 is used for creating the topology to create the network involving two tunnel end points in order to make a secure connection for secure transmission of data. In this topology, ISO image named c3725 for router is used and IPSec is implemented in two routers. The purpose is to create a secure tunnel between two end points i.e. one end point having ipv6 address 1000:: 1:2 and 1000:: 2:2. Three routers R1, R2 and R3 which are at separate geographical locations and tunnel is to be created between two routers i.e. R2 and R3. On all three routers serial interfaces are configured with IPv6 addresses. Switches are connected to the routers through the fast Ethernet interfaces. Further these switches are connected to two hosts each. Loopback interfaces in routers R2 and R3 are assigned with IPv6 address. IPSec is implemented in two phases i.e. phase 1 in which ISAKMP security association is established and phase 2 in which IPSec SA is established. Phase 1 is used to provide authentication and phase 2 is used to specify how the communication will be protected and what parameters are to be used.

.

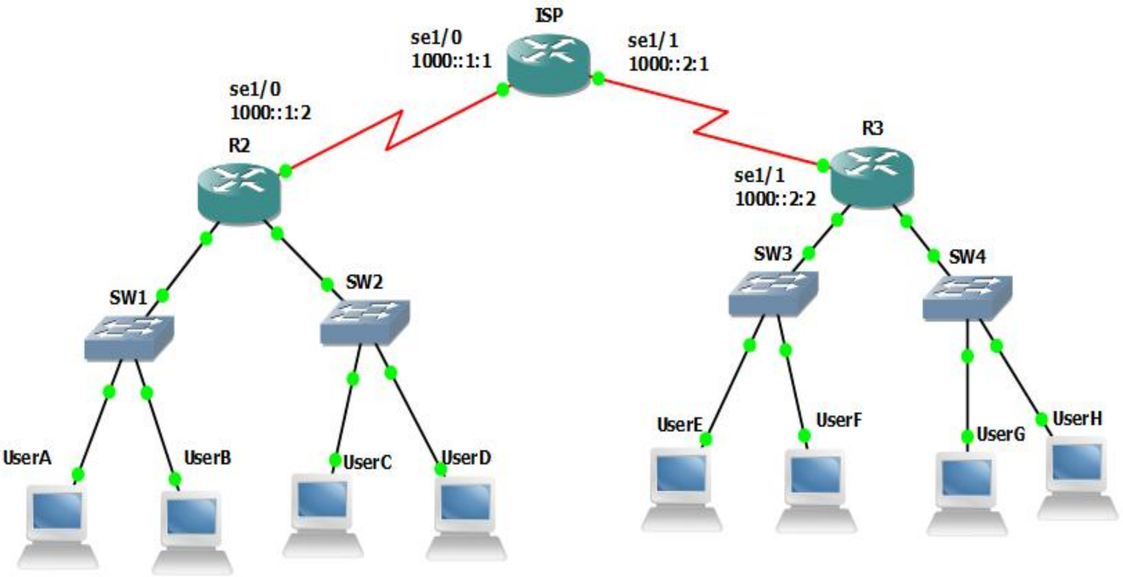

Fig 1: Topology: IPSec Tunnel between Router R2 and Router R3

6. RESULTS

The performance of the network is analyzed using ping. Advantage of using ping is that it ensures the connectivity of the network. Results are obtained by creating repeated traffic by different number of packets and testing the performance of networks in wireshark as well as collecting the results for throughput analysis of different users.

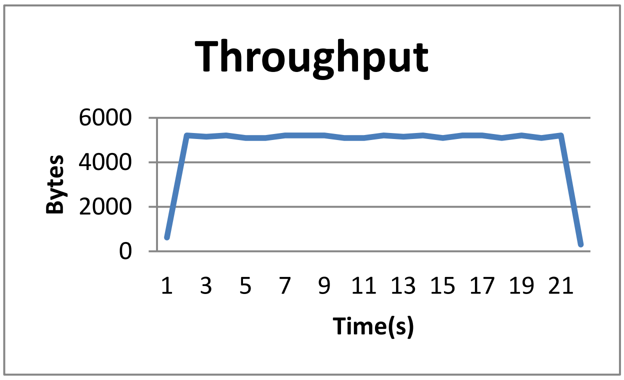

Fig 2: Throughput in bytes/sec for user A

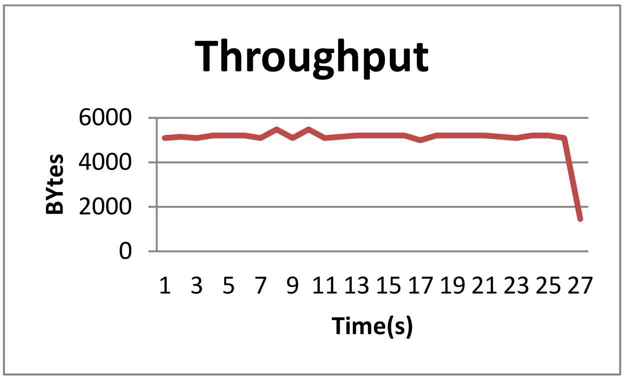

Fig 3: Throughput in bytes/sec for user B

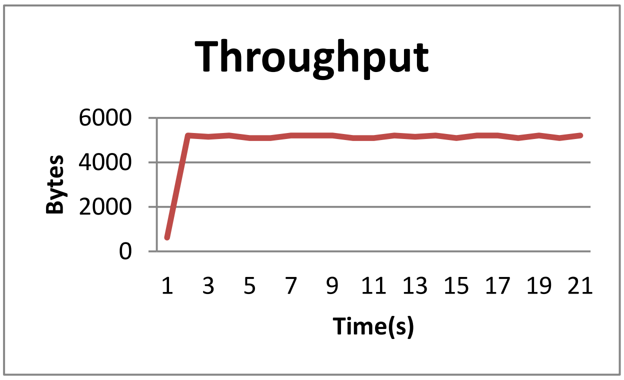

Fig 4: Throughput in bytes/sec for user C

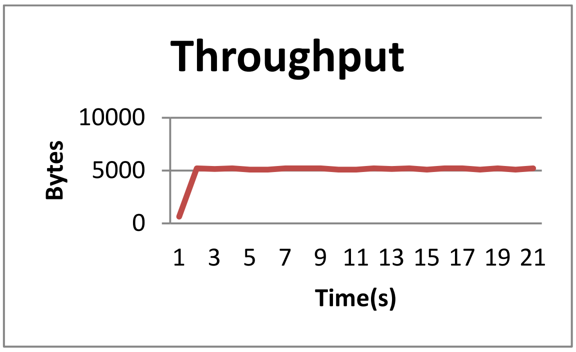

Fig 5: Throughput in bytes/sec for user D

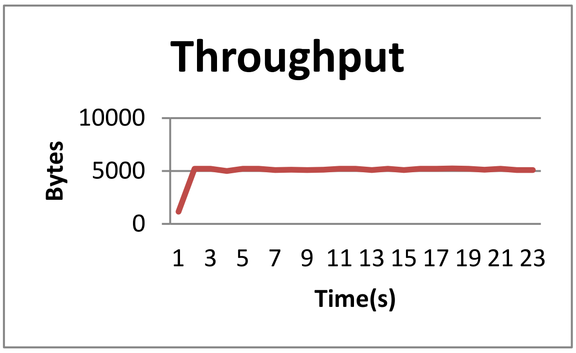

Fig 6: Throughput in bytes/sec for user E

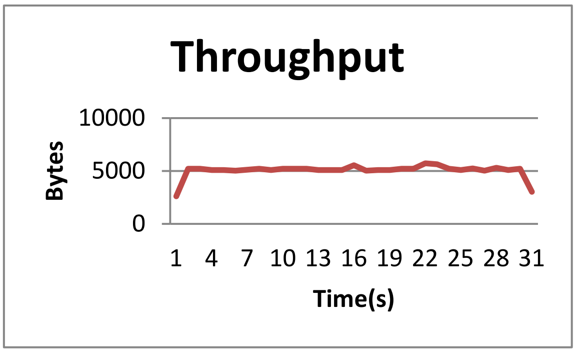

Fig 7: Throughput in bytes/sec for user F

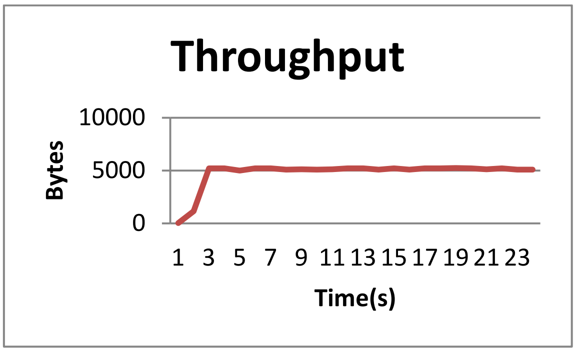

Fig 8: Throughput in bytes/sec for user G

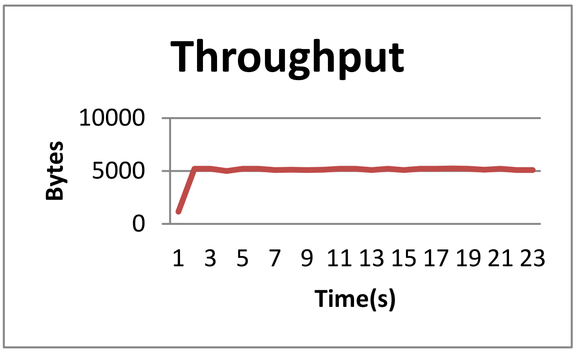

Fig 9: Throughput in bytes/sec for user H

Analysis of these graphs is done through statistical values. Statistics provides tool to analyze data through mean, median, mode etc. Statistical results obtained from these graphs are tabulated below to clearly interpret the results. Mean is the average value obtained by dividing the sum of values by number of values. Mode is the most frequent value occurred. Standard Deviation specifies how far each measurement is from the mean. Median is the midpoint between the highest and lowest value. Sample variance represents how varied the data is and square of the standard deviation. Skewness is used to measure the symmetry of the graph. Kurtosis defines the peakness of the graph related to a specific value. These statistical tools help in analyzing the performance of the throughput graphs in a network.

Table 1 Statistical Results

	User A	User B	User C	User D	User E	User F	User G	User H
Statistics	4731.636	5041.111	4942.0952	4942.095	4978.087	5036.903	4978.09	4978.086
Mean	5172	5200	5200	5200	5200	5120	5200	5200
Median	5200	5200	5200	5200	5200	5200	5200	5200
Mode	1381.653	723.7722	990.57932	990.579	837.9203	618.845	837.92	837.9202
Standard Deviation	1908966	523846.2	981247.39	981247.4	702110.4	382970.357	702110	702110.355
Sample Variance	8.123284	25.80881	20.884359	20.884	22.734	11.210	22.7349	22.734932
Kurtosis	-3.05896	-5.0238	-4.564555	-4.564	-4.75641	-3.310	-4.7564	-4.756410
Skewness	312	1456	624	624	1144	2600	1144	1144
Minimum	5200	5483	5200	5200	5224	5720	5224	5224
Maximum	4731.636	5041.111	4942.0952	4942.095	4978.087	5036.903	4978.09	4978.086

7. CONCLUSION AND FUTURE WORK

After analyzing the results for all the users, following graph shows the minimum throughput which is achieved in the graph under the influence of IPSec tunnel created in the network. This graph represents the minimum amount of traffic which can be sent from source to destination. After analyzing ping results for all the users it is concluded that minimum throughput is achieved at the rate of 312 bytes/sec for User A. Max throughput is achieved at the rate of 5720 bytes/sec by User F. It states the maximum traffic which can be passed from source to destination.

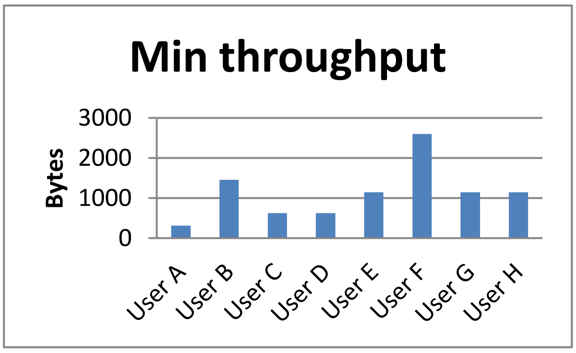

Fig 10: Minimum Throughput

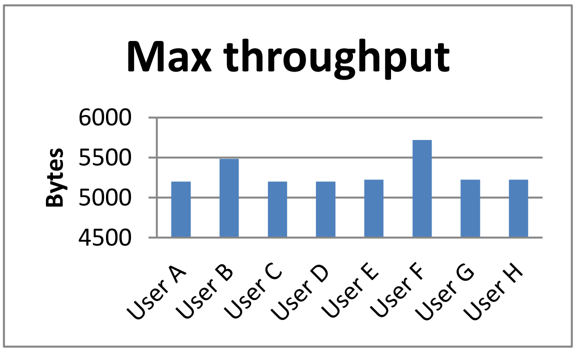

Fig 11: Maximum Throughput

IPv6 networks are next generation networks and will dominate the Internet market soon as there is a need for more and more IP addresses. Therefore several security threats will make these networks vulnerable to attack. There is a need for extensive study and solutions needed related to security of IPv6 networks.

8. ACKNOWLEDGMENTS

I would like to sincerely thank **Mrs. Savita Shiwani, Assosciate Professor** at **Suresh Gyan Vihar University** for guiding and helping me with the research conducted in this paper.

9. REFERENCES

[1] J.Bi, J.Wu, X.Leng, “IPv4/IPv6 Transition technologies and Univer6 Architecture”, International Journal of Computer Science and Network Security, 2007, 7, 232-24.

[2] G.Fairhurst, “IPv6-The Network Protocol of the future”, IEEE Advanced Satellite Mobile Systems, 2008, 7-12.

[3] N.M.Ahmad, A.H.Yaacob, “IPSec over Heterogeneous IPv4 and IPv6 Networks: Issues and Implementation”, International Journal of Computer Networks & Communications, 2012, 4, 7-72.

[4] H.A.Dawood, “IPv6 Security Vulnerabilities”, International Journal of Information Security Science, 2012, 1, 100-105.

[5] J.G.Jayanti, S.A.Rabara, “Next Generation Internet Protocol-Technical realms”, 3rd IEEE Conference on Computer Science and Information Technology ICCSIT 2010, 9, 2010, 394-399.

[6] H.Hamed, E.Al-Shaer, “Taxonomy of Conflicts in Network Security Policies”, IEEE Communication society, 2006, 4, 34, 134-141.

[7] H.Hamed, E.Al-Shaer, W.Marrero, “Modeling and Verification of IPSec and VPN Security Policies”, 13th IEEE International Conference on Network Protocols ICNP 2005, 2005.

[8] E.Al-Shaer W.Marrero, A.El-Atawy, K.Elbadawi, “Network Configuration in a box: towards end to end verification of network reach ability and security”, 17th IEEE International Conference on Network Protocols ICNP 2009, 2009, 123-132.

[9] C.E.Caicedo, J.B.D.Joshi, S.R.Tuladhar, “IPv6 Security Challenges”, IEEE Computer Society, 2009, 42, 36-42.

[10] R.Kajal, D.Saini, K.Grewal, “Virtual Private Network” International Journal of Advanced Research in Computer Science and Software Engineering, 2012, 2, 428-432.

[11] N.Nawarathne, “Overhead of FTPS and FTP over IPSec in IPv6 networks”, 2012 International Journal of Scientific and Engineering Research, 3, 886-891.

[12] J.Granjal, J.Sa Silva, E.Monteiro, R.Sa Silva, F. Boavida, “Why is IPSec a viable option for Wireless Sensor Networks”, 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems MASS 2008, 2008, 802-807.