International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 4 502 - 506

Implementing Policy Based Routing Technique and Providing Security In IPv6 Network

S. Deepa
PG student
Computer Science and Engineering
Easwari Engineering college, Chennai
deepa29392@gmail.com

S. Kayalvizhi
Professor
Computer Science and Engineering
Easwari Engineering college, Chennai.
kayalnag@yahoo.com

Abstract **-** Many organizations are in a process to adopt IPv6 addressing scheme. In order to make the network more efficient Policy Based Routing technique is implemented and security is provided. Normally routing is done based on the destination address present in the routing table. While implementing PBR the packets are delivered to the destination in the path as specified by the network admin. Here, the PBR overwrites the normal routing procedures and these packets choose the path as directed by the network admin. The network can be made more efficient by providing security scheme to secure the packets from the hackers. This process will minimize the network collision and by implementing security schemes in IPv6 network, the IP packets are delivered securely and also take the path as desired by network administrator.

Keywords*: IPv6, IPsec, PBR.*

*****

I. INTRODUCTION:

The overview of network security and an overall introduction about the Internet Protocols and the implementation of Routing Protocols such as Internet Protocol Security (IPsec), Policy Based Routing (PBR) are used to provide enhanced security in the network layer. This paper work is being currently implemented in RGMTTC (Rajiv Gandhi Memorial Telecom Training Center) of BSNL (Bharat Sanchar Nigam Limited) to provide a secured service to its customers by delivering the IP packets, through IPv6 network in an efficient manner by using Routing protocols and security schemes.

a. NETWORK SECURITY

Network security consist of the policies that are adopted to avoid and monitor unauthorized access, exploitation, variation in the computer network and network-accessible resources. Network security comprises the authorization of admission to the data in a network, which is controlled by the network administrator. Network security shelters a wide range of computer networks and communications between businesses organizations, government sectors and individuals. Network security is involved in the organizations, enterprises, and other types of institutions. The most common and simple method of defending a network resource is done by assigning it a unique name and a corresponding password.

b. INTERNET PROTOCOL(IP)

The Internet Protocol involves in the process of distributing the packets from the source to the destination based on IP addresses as mentioned in the packet header. IP defines packet structures that encapsulates the data to be delivered. It also defines addressing methods that are used to tag the datagram with source and destination information. The Internet protocol suite is frequently referred to as TCP/IP, the Transmission Control Program was additionally classified into architecture consisting of the TCP at the transport layer and the IP at the network layer. Each datagram has two components header and payload. The IP header is marked with the source address, the destination address, and other meta-data required. The IP is further classified into two major versions, the first version of IP is Internet Protocol Version 4 (IPv4), is the primary protocol of the Internet and Its replacement is Internet Protocol Version 6 (IPv6).

i. INTERNET PROTOCOL VERSION 4

Internet Protocol version 4 (IPv4) is a fourth version of internet protocol. It is a connectionless protocol used for packet switching in the network. It works on a best effort delivery mode where as IPv4 uses 32-bit addressing. IPv4 can address to approximately 4.3 billion devices. IPv4 is indicated in dotted decimal layout. In IPv4 addressing architecture, IANA gives Regional Internet Registries (RIRs)is provided with /8 address blocks. The extreme address block for a site is provided with a /8, which leaves only 24 bits for sub netting and addressing in the organization. The first header field of an IP packet is provided with four-bit version field. The IETF and the IANA have restricted from general use of various reserved IP address for special purpose. Migration to IPv6 is in progress but completion is likely to take significant time.

ii. INTERNET PROTOCOL VERSION 6

Address depletion of IPv4 which leads to the need for IPv6. IPv6 uses, 128-bit addresses are divided into 8 groups. 8 blocks into 4 digit hexadecimal numbers separated by colons. The resulting illustration is named as colon-hexadecimal. Hexadecimal notation, instead of familiar dotted decimal notation. The packet header in the IPv6 is simpler than the IPv4 header. In this the network layer security is given by various routing protocols, this paper work mainly concentrates on the IPsec protocol and PBR routing technique. While dealing with the IPv6 network, the delivering of IP packets has to be completed in a secure manner. The packets are transmitted in a well-organized manner by providing with some security schemes and routing techniques, this can be processed during implementation. The routing protocols route the packet with their own metrics whereas the network administrator could not implement his own routing methodology in a routing process. When an unauthorized routers are introduced in our network and we have to ensure that the service for them are denied by our routers.

The Objectives of the paper is to provide security for the IPv6 packets in the enterprise network from an unauthorized user. Another objective is to implement policy based routing (PBR) that cause packets to take different paths based on source address. By implementing security schemes and PBR in our IPv6 network, the IP packets are delivered safely and also take the path as desired by network administrator.

The scope of this paper work is to enhance the network security and to ensure where the IP packets are delivered safely to its destination. This process is carried out in the path as desired by the network administrator. Here security schemes are used in order to deny the access of unauthorized routers. This helps the packets to process efficiently in the IPv6 network.

The structure of this paper is as follows. In Section II we discuss about the existing techniques and the survey has been carried out based on the related works in IPv6 security. Section III focuses on the proposed methods. Section IV is focused on performance analysis and V we conclude this paper.

II EXISTING TECHNIQUES

a. IPsec PROTOCOL

Internet Protocol Security (IPsec) was developed for IPv6, but found well-known in IPv4, for which it has been re-engineered. IPsec was a required specification of the base IPv6 protocol suite, but has since been made optional for IPv4. IPsec is a protocol suite for secure Internet Protocol (IP) communications by authenticating and encrypting the IP packet of a communication session. IPsec uses cryptography based tools to implement the following security services at the IP layer and for all protocols carried over IP:

- Access control
- Confidentiality
- Integrity

IPsec provides flexibility in the types of security services that are provided through the use of multiple protocols, including the Authentication Header, the Encapsulating Security Payload and cryptographic key management procedures and protocols. The IPsec architecture was developed to allow for the deployment of compliant implementations that provide not only the security services, but also the management interfaces needed to meet the security and operational requirements of the user community. In addition to having multiple protocol options, IPsec can operate in either a transport mode or a tunnel mode.

i. AUTHENTICATION HEADER (AH)

Authentication Header belongs to the member of IPsec protocol suite. AH guarantees integrity and data origin authentication of IP packets. Further, it can be protected against replay attacks by using the sliding window technique and neglecting old packets, Anti-replay protection is also offered. Data authentication states the fact that if a computer receives an IP packet provided with a source address in the IP header, Then, it can be guaranteed that the IP packet are actually originates from that IP address. Data integrity refers to the fact that the content received by the target host should ensure that the contents is not changed along the route from the source to the destination node. Anti-replay protection is to avoid hackers injecting or making alterations in the packets that travel from a source to a destination. Authentication Header fields includes

- Next Header
- Payload Length
- Security Parameters Index (SPI)
- The Sequence Number field

ii. ENCAPSULATION OF SECURITY PAYLOAD (ESP)

The Encapsulating Security Payload header (ESP) provides confidentiality, authentication and data integrity in order to the encapsulated payload. Anti-replay protection, also provided by the ESP header. IP header fields are not protected by the authentication algorithm unless they are

encapsulated in "tunnel mode". Confidentiality refers that while receiving an IP packet it should be assured that nobody else has seen the contents of the IP packet. In the ESP header, both the confidentiality and authentication facilities are optional and at least one of these services must be selected. Encapsulated security payload packet format and also contains a Security Parameters Index (SPI) that is used to detect the Security Association. The Sequence Number field is used to afford anti-replay protection, where the encrypted data is located in the "Payload Data" field. The ESP comprises of the Padding, Pad Length, Next Header and Authentication fields. The padding field contains any padding bytes that may be needed by the encryption algorithm. The Pad Length field holds the number of bytes in the Padding field. The Next Header Field describes the type of data contained in the Payload Data field. The Authentication Data field contains Integrity Check Value which offers the authentication and data integrity.

b. ROUTING PROTOCOLS

A routing Protocol identifies how routers interconnect with each other, broadcasting information that allows them to take routes between any two nodes on a network. Routing algorithms determine the particular choice of route. Each router has a priori knowledge of networks connected to it directly. In this paper, some of the routing protocols like OSPF, and PBR routing techniques are to be used.

i. OSPF

Open Shortest Path First (OSPF) is a protocol used to route the packets in the shortest path to reach its destination. Later It is defined as OSPF Version 2 in RFC 2328 (1998) for IPv4. OSPF was then extensively altered to support IPv6 and it was referred OSPF version 3 which has been updated with RFC 5340. The OSPF technique and algorithms are unaffected but the packet and LSA formats varies in OSPFv3 because of the larger 128-bit IPv6 addresses. Open Shortest Path First version 3 uses link-state routing protocol that supports IPv6 and IPv4 unicast address families (AFs).

ii. PBR

Policy Based Routing (PBR) is a method used to provide routing, based on policies as specified by the network administrator. When a router receives a packet it typically decides where to forward the packets and this is done based on the destination address provided in the packet, which is used to look up an entry in a routing table. However, in some cases, there may be a need to forward the packet based on other conditions. For example, if a network administrator desires to route a packet based on the source address, not by the destination address. Policy-based routing is done based on the size of the packet, the protocol of the payload, or other data present in a packet header or payload. This allows routing of packets initiating from different sources to different networks even though, the destinations are the same and can be useful when communicating with several private networks. In the Cisco IOS, PBR is implemented using route maps.

c. RELATED WORKS

White paper, et al (2011) they have proposed a concept in [1]. The author has summarized the known threats and mitigation techniques for IPv6. Here, IPv6 is more secure due to IP Security (IPsec). IPv6 is shown as being roughly as secure as IPv4 with a short-term temporary issue such as, the lack of IPv6 knowledge by network architects and security officers. Lack of experience while running multiple protocols in parallel within the same network. In some cases, (link-local addresses) IPv6 is somewhat more secure, and in other cases (Hard to Parse the extension headers) IPv6 is slightly less secure. The Issue occurred due lack of IPv6 training about the IPv6 network and security staff is probably the major threat for operation in 2011–2012.

White paper, et al they have proposed a concept in [2]. The author, suggested the idea to carried out the mission for PBR on a router. In PBR, a network engineer has the major ability to command the routing behavior based on a number of different conditions other than destination network. which includes source or destination network, address, port, protocol, packet size, and packet classification among others. PBR disables fast switching of all arriving packets on this interface IP PBR can now be fast-switched. Users' needs PBR to occur at faster speed to implement PBR without slowing down the router. The benefits can be achieved by implementing policy based routing in the networks comprise Source-Based Transit Provider Selection, Quality of Service, Cost Savings and Load Sharing.The log keyword should not be used with this command in policy-based routing because logging is not held at the interrupt level for ACLs.

Isabelle Chrisment, et al (2010) has proposed a concept in [3] where, they have used the essential algorithms and tools to empower the transition to become automatic. Based on the model of an IPv4 network, we describe the algorithms to construct an optimized IPv6 addressing scheme. This may lead to produce automatic, adequate security plan as well as the resultant configurations for the devices in the network. The recent arrangement in core networks of operators, its availability to end users of multiple ISPs together with the readiness of native access to large services which leads to the transmission of IPv6. While its deployment inside the network leading to the edges is successful, the

 ISSN: 2321-8169
502 - 506

transition remains a problem currently for many organizations which may be a tedious and error prone task for network administrators.

V. Grout, J. McGinn, et al (2005) has proposed a concept [4] in order to optimisation problem encountered in the application of traffic policies on network routers. This process results in attempting to reduce the time taken to process an order of rules using Access Control List (ACL). Accurate and heuristic solution methods are introduced and compared to produce computational results given. Considering extensions and modifications, in particular the need to accommodate traffic modelling, queuing and prioritisation, and issues relating to variable traffic flows and timing. The author concludes that, the production routers in environments where minimal latency is a high priority, the simple 2-Opt is the most appropriate solution to adopt. Where, 2-Opt provides effective solutions quickly whereas any more sophisticated method is probable to add to, rather than reduce, packet latency.

III. PROPOSED METHOD:

This paper proposes the idea of PBR and security schemes using GNS3 simulation tool and implement it using IPsec method. Whenever an unauthorized routers are introduced in our network, secured network routers ensure that the services for them are denied. By using policy based routing we can implement policies that selectively cause packets to take different paths based on source address, protocol types or application types. While implementing these concepts in the given network as represented in the Fig 1: system architecture.

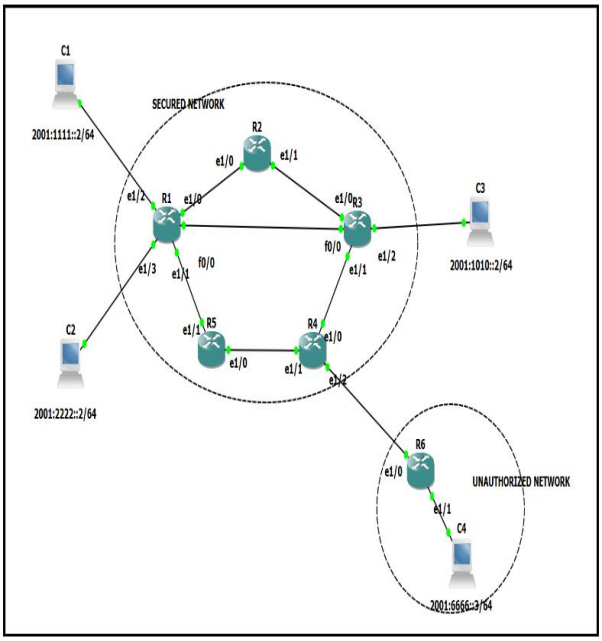

Fig 1: system architecture.

This process may result in better performance of the network and can be achieved by processing these modules one by one. The modules of the proposed system are given as follow

a. CONFIGURATION OF IPv6 NETWORK TOPOLOGY.

The configuration of IPv6 network topology is done with the help of GNS3 simulation tool. In that tool the required topology is designed by using Cisco Router c7200 and Host node. These end nodes and routers are connected with the help of Ethernet cable to the ports. Once, the connection is established it ready for Configuration. The routers that are present in the ipv6 network are configured using some Cisco IP configuration commands. Likewise, all the other routers and host are configured in the ipv6 network topology. Thus the devices present in the network are configured successfully. The Fig.2 below depicts the configuration of IPv6 network topology.

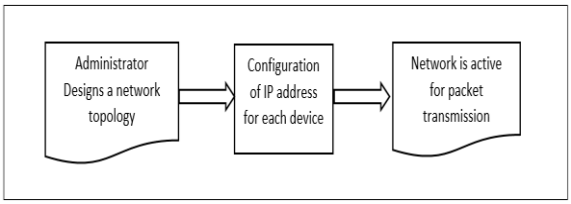

Fig.2: Configuration of IPv6 Network

b. USAGE OF OSPF ROUTING PROTOCOLS IN IPV6 NETWORK

The routing protocols are used to route the IP packet throughout the network in an efficient manner. Here, various routing protocols and security schemes are provided to IP packets, this will deliver the packets safely to its destination. The IPsec protocol are given more security by the Authentication Header (AH) and Encapsulating Security payload (ESP). The Fig.3 shows how the normal packets are routed, encapsulated for security purpose, in order to reach its destination.

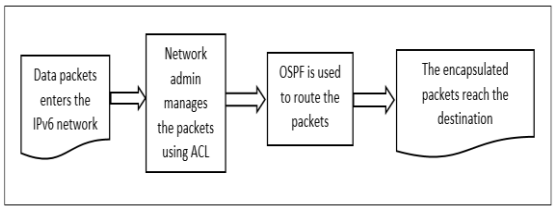

Fig.3 Protocol in IPv6 Network

The IPv6 network is initially provided with OSPF commands for routing the packets with in the network. This routing protocol is used to find the shortest path to reach its destination without any packet failure. In this

 ISSN: 2321-8169
502 - 506

module OSPF commands are used to route the packets within the particular area.

c. IMPLEMENTING POLICY BASED ROUTING TECHNIQUE

Implementing the PBR in the network the packets will take the path as instructed by the network admin. Here in this paper it deals with two type of routing technique such as by choosing the path based on the next hop as specified by the network admin. Another routing technique is done choosing the path based on the OSPF cost value. This process will make the packet to reach the destination in the required path as desired by the network admin. Whereas, by implementing PBR in the network it will overwrites the normal routing procedures and also minimize the network collision so that these packets will reach its destination in an efficient manner. The Fig.4 represent how the policy based routing technique is implemented.

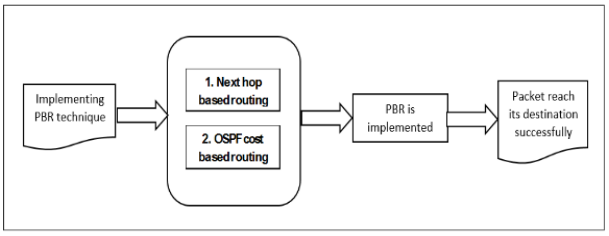

Fig.4: Implementing PBR

d. ENHANCING SECURITY IN IPv6 NETWORK

The security in the network is optimized by assigning unique password in the port throughout the authorized network. This password is an assumption and it should of 32-bit length. The Cisco commands are used to provide password in the network. In this module, each router ports are applied with password for security enhancement. After the successful implementation of passwords for the packets they become more secure. Fig.5 depicts how the authorized packets are processed inside the IPv6 network.

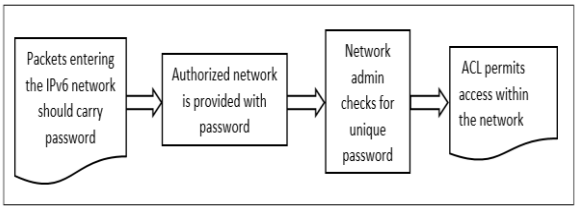

Fig.5: Secured Packet Transmission

e. TESTING THE SECURED NETWORK

After the successful implementation of the above modules, testing is to be performed. Testing is used to check whether the connections are established in the network between the devices for communication purpose. It represents how the ports are secured by holding the unique password in the authorized network. Thus in the secured network is tested successfully in this module to ensure that the packets are secured. The Fig.6 shows how testing is carried out in IPv6 network.

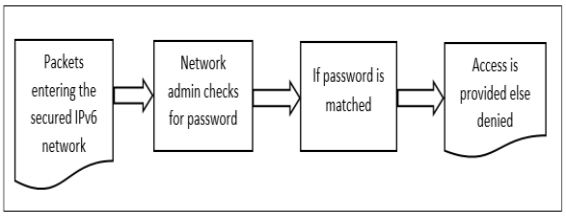

Fig .6: Testing the IPv6 Network

IV. PERFORMANCE ANALYSIS

In this paper the performance analysis has done by comparing the different networks based on its latency and through put. Here the paper concludes that when latency increases, through put will get decreased. In such a way that the latency and through put are inversely proportional.

Performance metrics can be calculated by using the given formula as mentioned below.

$$\text{Latency} = \frac{\text{Average Round Trip Time for Packets}}{2} \text{(ms)}$$

$$\text{Through put} = \frac{\text{Packet Size}}{\text{Latency}} \text{ (Mbits/s)}$$

Thus the fig:7 represents latency analysis. Here the latency is analysed for different network by varying the load in the network.

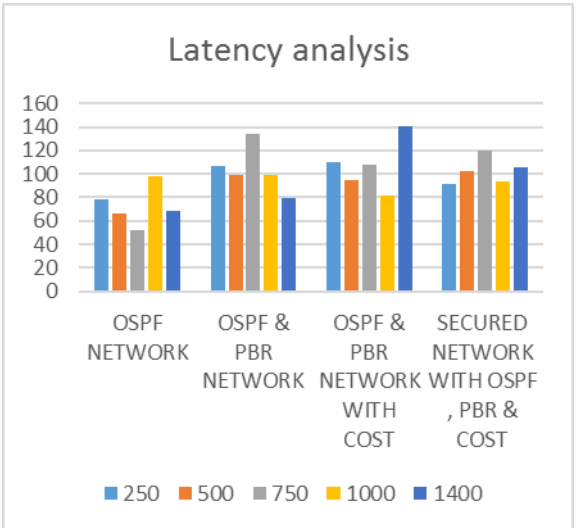

Fig.7: Latency analysis

 ISSN: 2321-8169
502 - 506

Further, through put is analysed for different network by varying the load. Fig:8 represents the through put analysis. Thus the performance analysis is processed for the above given network.

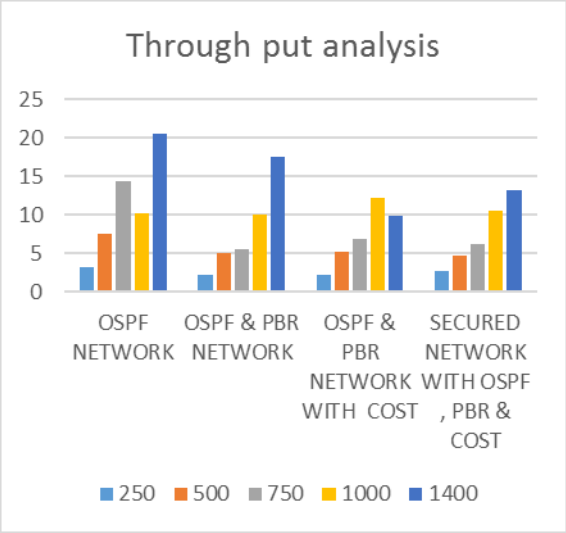

Fig.8: Through put analysis

V. CONCLUSION

This paper concludes how efficiently the packets are delivered to the destination in the specified path as instructed by the network admin in a secure manner. This process is done by using the user friendly software GNS3. The IP packets in IPv6 network faces several security threats and this can be overcome, by providing various security schemes and policy as discussed in this paper. Even though, latency is increased meanwhile the through put gets decreased. This causes the packets to reach its destination faster when compared to the older network. Future work can be focused on the security part for this network by providing some other security schemes to enhance the network. While using PBR routing technique the network collision is avoided.

REFERENCES

[1] Cisco Systems, "IPv6 Security Brief", Last Updated: October 2011.

[2] Cisco Systems, "Configuration Policy-Based Routing", Cisco IOS Quality of Service Solutions Configuration Guide

[3] Frederic Beck, Oliver Festor, Isabelle Chrisment and Ralph Droms, "Automated and Secured IPv6 Configuration in Enterprise Networks", published in "CNSM 2010".

[4] V.Grout, J.McGinn,"Optimization of policy-Based Routing using Access Control List", University of Wales, NEWIPlas Coch Campus,UK.

[5] Harith A. Dawood, "IPv6 Security Vulnerabilities", International Journal of information Security Science.

[6] Samuel Sotillo, "IPv6 Security Issues" East Carolina University

[7] Amer Nizar Abu Ali, "Comparison study between IPv4 & IPv6", IJCSI International Journal of Computer science Issues, in may 2012

[8] Cynthia E.Martin and Jeffrey H.Dunn, "internet Protocol version 6 protocol security assessment",IEEE,2007.

[9] Tomasz Bilski, "from IPv4 to IPv6-Data security in the Transition Phase",ICNS,2011

[10] S. Deering and R.Hinden,"Internet Version 6 (IPv6) specification", RFC 2460 (Draft Standard), IETF, Dec. 1998, updated by RFC 6096

[11] S. Thomson, T. Narten, and T. Jinmei, "IPv6 Stateless Address auto configuration", RFC 4862 (Draft Standard), IETF, Sept. 2007

[12] T. Narten, E. Nordmark, W. Simpson, and H. Soliman, "Neighbour, discovery for IP version 6", RFC 4861, IETF, Sept. 2007.