iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** II **Month of publication:** February 2023

DOI: https://doi.org/10.22214/ijraset.2023.48722

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue II Feb 2023- Available at www.ijraset.com

Cloud Based VPN Using IP Tunneling for Remote Site Interface

Raj Kumar Patel[1], Dr. Lalan Kumar Singh[2]
[1]*Research Scholar, Magadh University, Bodh-Gaya*
[2]*Associate Prof., Dept. of Mathematics, K.S.M. College, Aurangabad (Bihar)*

Abstract: ***A strong IP technology that builds a secure and encrypted connection tunnel over the less secure internet is required by the majority of enterprise organizations. Joint location and link connectivity issues must be resolved for distant users and branch offices to have secure access to corporate applications and other resources. This ensures security while data passes over encrypted tunnels. Despite the development of IP-based VPN, JLP and LCP for VPN customer edge devices and provider edge nodes have not yet been completely investigated. The purpose of this work is to apply cutting-edge viewpoints to VPN-IP design that may be used in IP multi-protocol label switching (MPLSVPN) infrastructure for cloud computing. The system architecture includes mathematical formulas. End-to-end delay, throughput, and resource consumption behavior for IP tunneling are seen to behave moderately for low scale workloads. While showcasing the benefits of an MPLS-based IP-based VPN architecture, the difficulties of VPN-IP tunneling are explored. This study suggests cloud-based MPLS-VPN as a workable substitute for traditional VPN-IP tunneling in order to get the best performance and service delivery.***
Keywords: Secure Tunneling, Transport-Level-Security, Cloud, Routing Protocols, IPSec, VPN;

I. BACKGROUND

Wireless local area networks (WLAN) are being utilized more and more frequently in a variety of activities, including production, work, learning, life, and other activities. Architecture is relatively simple to maintain, and it costs not much. However, WLAN is exposed to an open environment, and anyone could access it with very basic physical equipment. Information eavesdropping, tampering, counterfeiting, denial of service information, and other issues are the key security issues. Currently, the Wired Equivalent Protocol (WEP) and the elliptical encryption algorithm (ECC) are either too basic or too sophisticated for wireless network security [1]. WLAN security issues are the key issue, and this issue is also limiting WLAN's ability to advance.

The virtual private network (VPN) technology uses a physical network intellectually in order to approximate how two nodes in the network exchange information so that it resembles a private network on the internet. due to its inexpensive cost and enhanced data security protection. Many businesses employ this method because it doesn't require spending a lot of money. In order to increase the effectiveness and safety of a wireless local area network, this paper provides a strategy that uses virtual private network technologies.

II. INTRODUCTION TO TOPIC

In most emerging nations, including Nigeria and countries in South Africa, the need for high bandwidth heavy services has continued to increase due to the requirement for high capacity IP switching backbone. A few years ago, a submarine cable with a capacity of roughly 20 TBPS arrived in Lagos, Nigeria from Europe. Less than 10% of this total capacity has been used in Nigeria up to this point. To fix national optic fibre coverage (NOFC) for service delivery in Nigeria and other SA countries, however, efforts have been made. This has made it possible for telecom operators and Internet service providers like Globacom, Cyberspace, Etisalat, AirTel, MTN, etc. to benefit from MPLS's most recent capabilities **[1]**.

Thus, scalable virtual private networks (VPNs) and end-to-end quality of service are established (QoS). This hasn't been investigated, though, in the context of cloud computing. Both user and company data are protected and encrypted by the VPN using well-established protocols. These protocols include Layer 2 Tunneling Protocol (L2TP), OpenVPN, Secure Sockets Layer (SSL), Transport Layer Security (TLS), Point-to-Point Tunneling Protocol (PPTP), Secure Sockets Layer (SSL), and IP Security (IPsec) **[2].** Site-to-site VPNs and remote access/site VPNs are generally considered to be the two main types of VPNs **[3].**

The former allows for the creation of dedicated, secure connections between locations across the open Internet/public connection, which can be either Intranet-based or extranet-based, while the latter ensures that VPN software clients are securely connected to access centralized network resources that are housed behind VPN servers **[2]**.

The benefit of employing a secure VPN is that it makes it possible to apply a moderate level of security to connected systems when the underlying network architecture cannot. Usually, corporations choose this option due to cost and viability.

The quality of service (QoS), the protocol types used by a supporting Internet service provider (ISP), the speed at which users connect to the internet, and the type of VPN encryption utilized all affect performance. The majority of businesses today connect their branches via VPN connections, either in site-to-site or remote-access mode. Additionally, they are utilised for connecting to resources in a PCIaaS (Public Cloud Infrastructure as a Service) domain. In some hybrid-access VNP scenarios, the VPN gateway is located in the cloud and has a secure connection to the cloud ISP's internal network.

Layer 2 may not provide QoS guarantees in high performance networks; instead, layer 3 MPLS-VPN can be utilized as a data-carrying transmission method that transmits data from one network node to another based on a short path label without consulting the routing table.

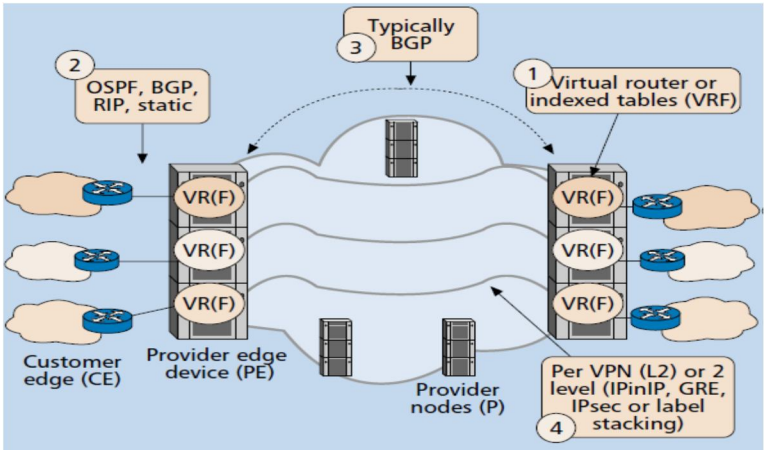


Fig. 1: Elements of L3VPN

Image Source: "https://docs.vmware.com/en/VMware-Smart-Assurance/10.1.0/mpls-manager-discovery-guide-101/GUID-1C3A06FA-C29F-4C8C-A260-AE1912DE55EB.html"

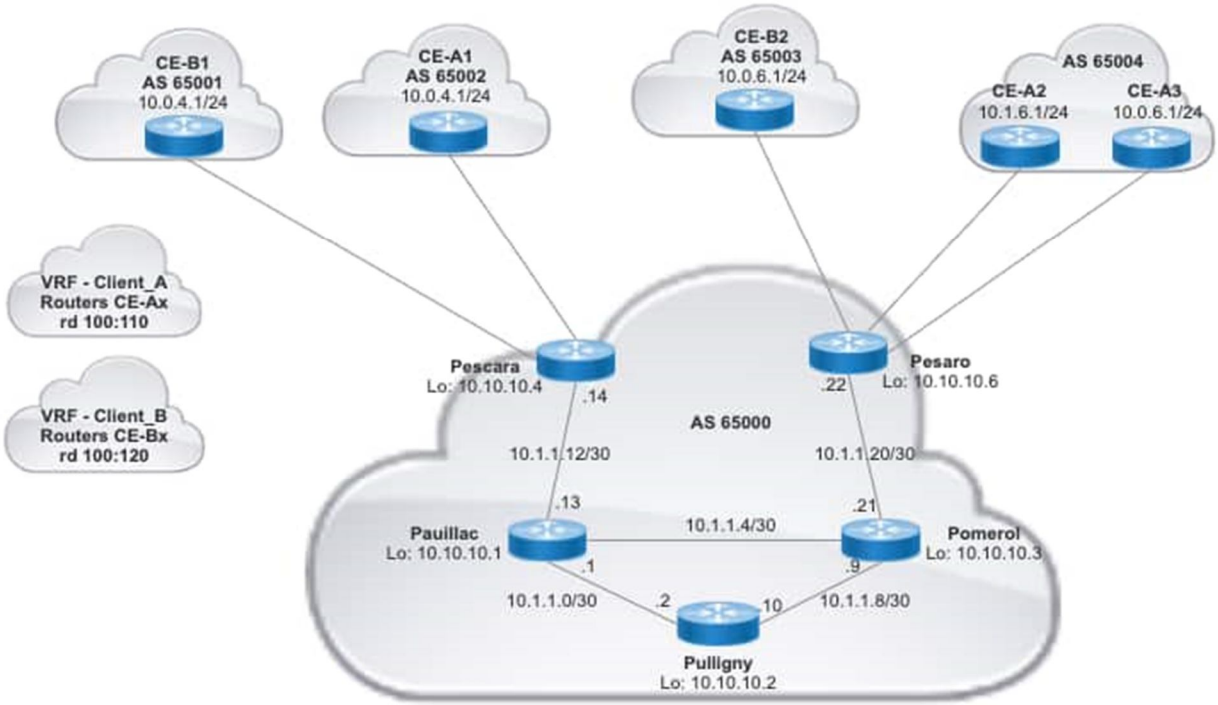


Fig 2: Network Diagram of MPLS-VPN Routing

Image Source: "https://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/13733-mpls-vpn-basic.html"

With MPLS-VPN in Fig. 1a, b, this allows for quick fault correction of link and node failure as well as efficient utilization of provided networks to accommodate future expansion. Delivering highly scalable, unique end-to-end IP services with less complex configuration, management, and provisioning is made possible by MPLS technology. Businesses utilizing MPLS technology can provide dedicated high speed internet services with great uptime by utilizing totally owned submarine optical fiber connection.

Customers with locations all throughout South Africa, Indian sub-continent and other south and East Asian countries may be able to connect and transmit data quickly and securely over a dependable and strong MPLS network **[4], [5].** When fully leveraged, MPLS infrastructure for cloud services may provide businesses with unprecedented connection. The network must be free of connectivity restrictions for multi-site enterprises with branches across the country that need a secure, reliable, and quick way to send, access, and share massive amounts of data, make voice calls, and set up multimedia applications at their various branches on demand.

Unfortunately, Traffic Engineering (TE) and Quality of Service (QoS) in terms of predictable minimum latency, delay fluctuation, and packet loss to users cannot be guaranteed by a standard VPN-IP without multilayer MPLS. Performance would be enhanced with a redesigned layer 2/3 VPN that used traffic engineering (TE) for QoS provisioning.

III. MOTIVATION BEHIND THE RESEARCH TOPIC

Convectional networks face enormous traffic challenges, which have forced telecommunications providers and internet service providers to deploy layered VPN clients inside MPLS networks. However, there are a number of QoS issues with the traditional VPN-IP, especially for real-time applications. For site-to-site routing, layer-3 MPLS VPN over IP adds overhead. Scalability of networks, on-demand routing control, security, convergence, etc. continues to be challenges. JLP and LCP in cloud-based MPLS-VPN are still being investigated. Without developing an ideal infrastructure for QoS maximization, particularly in the overall bandwidth-intensive cloud environment, this will amount to economic wastes for the vast 19.2 TBPS bandwidth accessible in Nigeria. This study's major goal is to define a cloud-based VPN employing IP tunneling. This is applicable to Infrastructure as a Service (IaaS) offerings for cloud computing.

IV. FUNDAMENTAL CONCEPTS

A. Virtual Private Network

A virtual private network, or VPN, connects distant sites or users by use of a public network—typically the Internet. With the aid of a VPN, two offices can communicate with one another in a way that makes it appear as though they are linked directly by a private leased line. A VPN utilizes "virtual" connections routed through the Internet from the company's private network to the remote site or employee in place of using a dedicated line for communication between two parties located on opposite sides of the world. VPN, which secures the network between businesses and users and is also authenticated and encrypted for security, is one of the most significant countermeasures against viruses and hacker threats. Data is tunneled with a unique node identification code during the tunneling phase and sent to authenticated nodes. All of the intermediate nodes tunnel the nodes once more and send in the destination direction. The number of tunneling grows as point-to-point communication expands. The data structure can be decoded up to a certain point using intermediate VPN. Consequently, this method effectively enables the packet to be transferred with guaranteed security.

B. Requirements of VPN Implementation

The following criteria must be met for the V PN to qualify as a "private" network. Support for transport of transparent packets: The packets transported through a V PN might not be connected to those on the public network. Their protocols and addressing mechanisms might differ, and if they do, their address spaces might overlap if they employ the same addressing mechanism. In particular, the non-unique private IP address may be utilized for an Internet-based VPN. Additionally, many VPNs may be supported concurrently on a same public network, and they are all transparent to one another. assistance with security features. Customers that utilize Virtual Private Network (VPN) need security features like user authentication against data spoofing, data encryption against spying, and integrity computation against illegal manipulation because public networks lack these security safeguards. Provide for Quality of Service (QoS) guarantees: VPN should be able to support a range of QoS levels, including bandwidth and delay assurances, according on the needs of the clients.

Customers that utilize Virtual Private Network (VPN) need security features like user authentication against data spoofing, data encryption against spying, and integrity computation against illegal manipulation because public networks lack these security safeguards. Provide for Quality of Service (QoS) guarantees: V PN should be able to support a range of QoS levels, including bandwidth and delay assurances, according on the needs of the clients.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue II Feb 2023- Available at www.ijraset.com

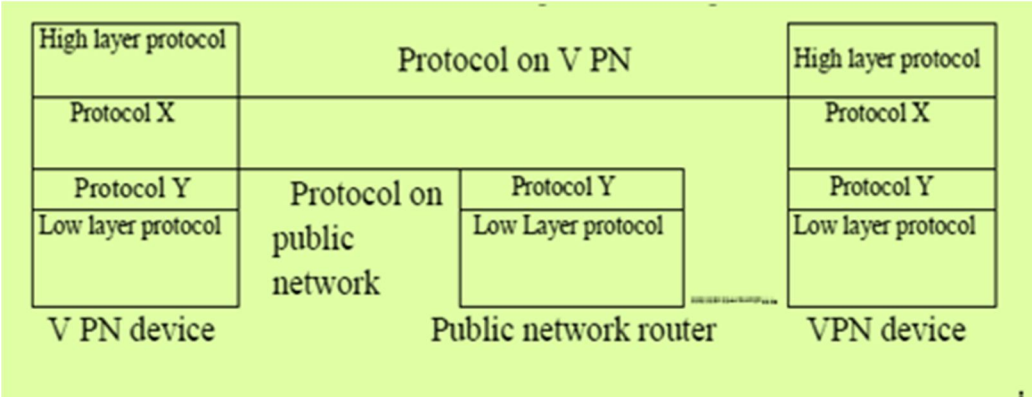


Fig 3: Architecture of VPN Protocol

C. Tunneling Protocol

VPN needs to be implemented using a tunneling mechanism of some kind in order to meet the aforementioned requirements. When a protocol (protocol X) is transported, it is encased within another protocol (protocol Y) in a process known as tunneling. As a result, protocol X is transparent to the public network. Figure 3 depicts the protocol architecture of a VPN that uses a tunneling technique. It is a broad encapsulation protocol that was developed with a specific focus on a number of different encapsulation techniques, including IPX encased within IP and X.25 encapsulated within IP. The encapsulating and encapsulated protocols in this protocol can both be any network protocols. L2TP (Layer 2 Tunnel Protocol) **[6].** It was developed by the IETF's working group on mobile IP and is utilized for mobile IP communications between mobile hosts and their home agents. The tunnel establishing protocol (TEP) **[7]** was another idea put out by this group. IP/IP is encapsulated as (IP(tunnel header(IP))). The aforementioned tunneling protocols were not designed with VPNs in mind, hence they might not meet all of the requirements for VP-V implementation. It was developed by the IETF's working group on mobile IP and is utilized for mobile IP communications between mobile hosts and their home agents. The tunnel establishing protocol (TEP) **[8]** was another idea put out by this group. IP/IP is encapsulated as (IP(tunnel header(IP))). The aforementioned tunnelling protocols were not designed with VPNs in mind, hence they might not meet all of the requirements for VP-V implementation.

D. Protocols Comparison

A variation in the working mode In the aforementioned tunneling technologies, GRE, IPSec, and IP/IP all operate in peer-to-peer mode, with two VPN endpoints performing symmetrical tasks. L2TP, on the other hand, operates in client/server mode. It must be used to implement VPN, and one VPN device must implement the L2TP Access Concentrator (LAC) function while another must implement the L2TP Network Server (LNS) function. The mandatory tunnel style must also be employed. Both VPN devices need to implement LAC and LNS capabilities in order for them to be symmetrical. It goes without saying that this will make setup and management activities more complex and add to the implementation overhead.

1) *Security:* They may be utilized separately or in combination, depending on the security requirements. The IPSec-based VPN can provide multi-level security services based on the needs of the customer. The other tunneling protocols either offer no security features at all or simply very flimsy ones. For instance, L2TP inherits PPP's authentication and encryption, but it is unable to protect L2TP control and data communications at the packet level. Another illustration is the four-byte Key field, which is an optional feature of GRE and can be used for origin authentication. IP/IP doesn't offer any security safeguards. The "tunneling protocol A + IPSec" approach is typically used to provide stronger security in these protocols. This plan will result in increased protocol overhead and external security.
2) *Multiplexing Support:* According to the VLL paradigm, the VPN device serves as the enterprise Intranet's VPN agent, and each tunnel endpoint can accommodate many users concurrently. In this scenario, a separate tunnel can be created for each set of clients, but this will result in an increase in processing costs and tunnel construction time. Therefore, sharing one tunnel among all clients is the preferable method (multiplexing). A multiplexing field is required in the tunnelling protocol in order to distinguish which packets belong to which customers (the purpose of this is to identify them because various customers may have different transport requirements, such as quality requirements).

3) *Multi-protocol Trans port Support:* Since the IP protocol is not always used in application environments, tunnel protocols should support a variety of protocols, including IP, PX, Apletalk, and others. L2TP derives from PPP in the aforementioned tunnelling protocols, enabling multi-protocol support. General encapsulation, or GRE, was described as having multi-protocol support. Multi-protocol cannot be supported by IP/IP. IPSec was initially intended to carry IP packets, hence multi-protocol cannot be supported. However, we can improve it and adapt it to a multi-protocol environment. Before utilizing IPSec encapsulation, another tunnelling protocol that supports multi-protocols, such as GRE, is used to encapsulate the non-IP protocol (protocol X) in the IP protocol. Since the IP protocol is not always used in application environments, tunnel protocols should support a variety of protocols, including IP, PX, Apletalk, and others. L2TP derives from PPP in the aforementioned tunneling protocols, enabling multi-protocol support. General encapsulation, or GRE, was described as having multi-protocol support. Multi-protocol cannot be supported by IP/IP. Following that, IPSec encapsulation is used. We can see that the encapsulation form will become (IP(IPSec(IP(GRE(protocol X))))) and that the processing and transmission overhead will grow.
4) *QoS Support:* A fundamental prerequisite for a VPN is Quality of Service (QoS). The above-described packet sequence can be viewed as a type of quality of service (QoS), however generally speaking, QoS includes greater contents, such as the bandwidth and delay guarantees, various service levels, and so on. Unfortunately, none of the tunneling protocols mentioned above can offer QoS. An area of active research is how to guarantee QoS in the existing IP network. Resource reservation, admission control, QoS routing, packet scheduling, link sharing, and other topics are covered in the research effort.

E. Scalability

Before talking about this issue, we expand the V LL V PN model from two to (assuming N) multiple firms. The original approach stated that this was necessary to create a complete connecting relationship between them. The number of tunnels on VPN devices is N*(N-l)/2. The (N-l) tunnels between each VPN device and the other VPN devices must be maintained.

The overhead of the tunnel configuration and maintenance activities becomes a significant issue as N rises. The tunnels need to be reconfigured whenever the VPN connection changes. The full-connective network architecture (a tunnel is built between every two VPN devices) and static routing are the elements that contribute to the scalability issue (the tunnel configuration can be seen as a kind of static routing). We must concentrate on the aforementioned two factors in order to address the scalability issue. It is essential to create a dynamic routing protocol that may be used with any topological VPN.

The expression of VPN membership, the conveyance of reachability information, the relationship with the present routing protocols active on the Internet, and other issues should be taken into account when building this routing protocol. Further research must be done on each of them.

V. RELATED RESEARCH WORK

The popularity of layer 3 MPLS VPNs was demonstrated by the use of Multi Protocol Label Switching (MPLS) in the architecture of Virtual Private Networks (VPNs). As security architecture for secure transactions in VPN environments, SMART IDS was suggested in **[3]**. The results of the simulation, which focused on SMART Network Security System (SNSS) branch node throughputs and TCP traffic behavior, utilized VPN configurations that were developed and used successfully. Functional distinction between Layer 2 and Layer 3 VPN in MPLS architecture is defined in **[8]**. The focus of current VPN-IP research has shifted to MPLS traffic engineering, which enables a backbone network using MPLS to mimic and enhance the traffic engineering capabilities of Layer 2 ATM and Frame Relay networks **[9], [10], [11].**

This study notes that VPN-IP networks have not been investigated for traffic engineering involving JLP and LCP. These are crucial for Internet service provider (ISP) backbones and locally based service providers (LSPs). The backbone in this situation can support effective utilization of the available transmission capacity. Given that the network can endure link or node failures, network resilience is important.

VI. COMPLEX SYSTEM FORMULATIONS

There are numerous sites in a non-MPLS aware operation, including subscriber provisioning core, subscriber provisioning edge, and subscriber premises (customer edge) (provider). This study focuses on IP tunnelling at the VPN customer edges. L2VPN supports the utilization of Frame Relay-Data Link Connection Identifier (DLCI), Ethernet, and VLAN interfaces. EIGRP and OSPF are the protocols used for IP tunnel traffic engineering for L3VPN.

VII. INTEGRATED TUNNELING SCHEME

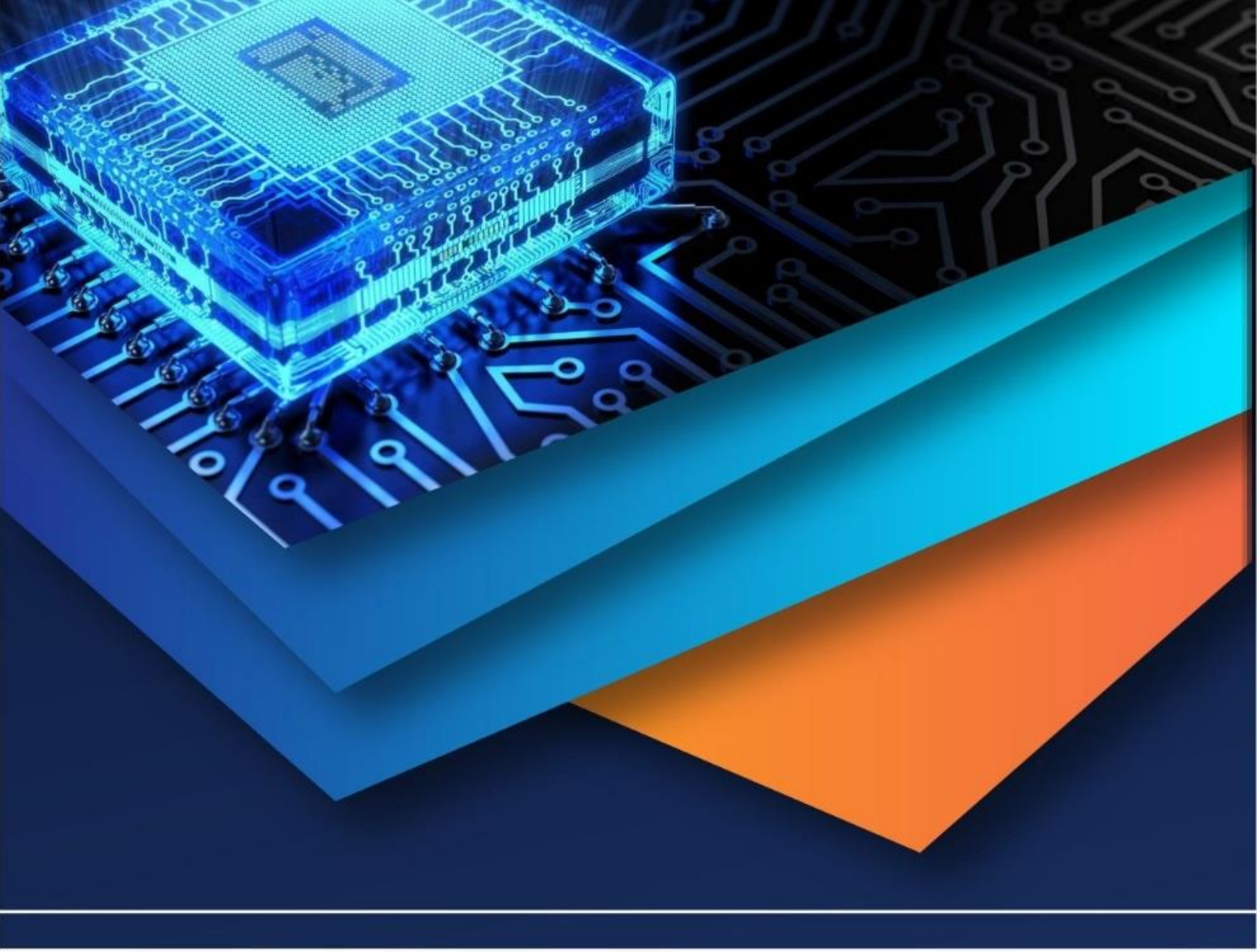
We can observe from the comparison of the aforementioned tunnelling protocols that VPN implementation adds more requirements. None of the tunnelling methods that have been suggested can address every issue with V P N. We suggest an expanded IPSec/IKE tunneling strategy, which has been used in our VPN, under the current circumstances **[12]**. It can meet the VPN criteria after testing. Here is an introduction to it. We use the Internet Key Exchange protocol as the signaling protocol for tunnel configuration, the tunnel mode IPSec as the fundamental encapsulation mechanism, and the soft state mechanism in IP/IP as the means for tunnel administration and maintenance. We suggest a straightforward procedure to enable QoS. There is no need to modify the current IP service paradigm because it can deliver limited user-based different level services. This approach's guiding principle is as follows. Some service levels are predetermined. The requirements and identities of the users are taken into account when configuring the tunnel in the SA. Additionally, in order for the relay routers to take the appropriate measures, the service level recorded in the SA is mapped to the Type of Service (TOS) field in the IP header when creating the tunnel to encapsulate the packets. If support for multiple protocols is required,

VIII. CONCLUSION

We suggest a more direct approach in addition to the "twice encapsulation" scheme. In this approach, IPSec is used to directly encapsulate the non-IP protocol. But the SA that is chosen while configuring the tunnel needs the encapsulated protocol type item added to it. Multi-protocol is now supported by IPSec**.** IP/IP GRE L2TP IPSec operating mode Peer-to-peer Client/Server Peer to peer peer to peer security protocols Authentication Validation and encryption all built-in security features None Tunnel construction and configuration network administration, explicit I'm licit, same as GRE IKE exchange similar to the upkeep and management of the GRE Tunnel. Scalability problem is yet to be solved.

REFERENCES

[1] L. Cittadini, G. Di Battista, M. Patrignani, “MPLS Virtual Private Networks”, in H. Haddadi, O. Bonaventure (Eds.), Recent Advances in Networking, (2013), pp. 275-304.
[2] Paul Knight, and Chris Lewis, “Layer 2 and 3 Virtual Private Networks: Taxonomy, Technology, and Standardization Efforts”,IEEE Communications Magazine • June 2004, Pp.124-131
[3] K.C. Okafor, C.C. Okezie, C.C. Udeze, N. Okwuelu (2013). SMART IDS: An Enhanced Network Security Model in IP-MPLS Based Virtual Private Network. Afr J. of Comp & ICTs. Vol 6, No. 3. Pp135- 146
[4] Rosen, E., and Rekhter, Y. BGP/MPLS IP Virtual Private Networks (VPNs). RFC 4364, 2006.
[5] Rosen, E., Viswanathan, A., and Callon, R. Multiprotocol Label Switching Architecture. RFC 3031, 2001.
[6] D. Harkins & D. Carrel, "The Internet Key Exchange (IKE)'t , RFC2409, November 1998.
[7] Lan jun and Lin bi ying, 2011 International Conference on Mechatronic Science, Electric Engineering and Computer, “Research for Service Deployment Based on MPLS L3 VPN Technology”, August 19-22, 2011, Jilin, China page 1484- 1488
[8] PushpaYadav and RohitSinghal, “ Effect ive tunneling of Tra fficand Data in Network with L2TP Based on L2F, February 2014”
[9] Lan jun and Lin bi ying, 2011 International Conference on Mechatronic Science, Electric Engineering and Computer, “Research for Service Deployment Based on MPLS L3 VPN Technology”, August 19-22, 2011, Jilin, China page 1484- 1488.
[10] Rahul Aggarwal, Juniper Networks, OAM Mechanisms in MPLS Layer 2 Transport Networks, IEEE communication magazine October 2004 , page 124-130.
[11] Yoo-Hwa Kang, and Jong-Hyup Lee, “The Implementation of the Premium Services for MPLS IP VPNs ”Advanced Communication Technology, 2005, ICACT 2005. The 7th International Conference on Volume: 2 Digital Object Identifier: 10.1109/ICACT.2005.246152 ,Publication Year: 2005 , Page(s): 1107 – 1110.
[12] Dr. Narendra Kumar, Shankar Kumar, Dr. Nandeshwar Pd. Singh,."Mechanism, Tools and Techniques to Mitigate Distributed Denial of Service Attacks", Volume 11, Issue I, International Journal for Research in Applied Science and Engineering Technology (IJRASET) Page No: 855-861, ISSN : 2321-9653, www.ijraset.com



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY