International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 5 | ISSN : 2456-3307

Study on Virtual Private Network (VPN), VPN's Protocols And Security

K. Karuna Jyothi*, Dr. B. Indira Reddy
IT Department, Sreenidhi Institute of Science and Technology, Ghatkesar, Telangana, India

ABSTRACT

When an access-desired network is constructed using public network infrastructure such as global Internet to connect remote users or regional offices to company's private network is said to be Virtual Private Network(VPN). A VPN protects the private network, using encryption and other security mechanisms to confirm that only authorized users can access the system and the data can be intercepted. This Literature review paper explains about Virtual Private Network(VPN), It's protocols and Security in VPN.

Keywords: VPN, Network, Protocols, Encryption, WAN, cost, QoS, Encapsulation, Interoperability, Confidentiality.

I. INTRODUCTION

A. *VPN:*

A virtual private network (VPN) extends a private network across a public network, and enables users to send and obtain information across pooled or public networks as if their computing manoeuvres were directly associated to the cloistered system. Applications running across the VPN may therefore benefit from the functionality, security, and management of the private network. [7]

VPN was not the first technology to make remote connections. Several years ago, the most common way to connect computers between multiple offices was by using a leased line. Leased lines, such as ISDN (integrated services digital network, 128 Kbps), are private network connections that a telecommunications company could lease to its customers. Leased lines provided a company with a way to expand its private network beyond its immediate geographic area. These connections form a single wide-area network (WAN) for the business. Though leased lines are reliable and secure, the leases are expensive, with costs rising as the distance between offices increases.

History of VPN:

The technology for implementing VPNs has been in existence for some time. Their origins can be found in the Virtual Circuit. Virtual circuits are easy to implement in highly connected networks as well as being cost effective. We will see that these benefits also apply to VPNs. The virtual circuit was originally produced in the late seventies and early eighties. The basic structure of the virtual circuit is to create a logical path from the source port to the destination port. This path may incorporate many hops between routers for the formation of the circuit. The final, logical path or virtual circuit acts in the same way as a direct connection between the two ports. In this way, two applications could communicate over a shared network. Virtual circuit technology progressed with the addition of encryption equipment to router systems. This new equipment enciphered information between the ports of the virtual circuit. This meant that attackers would not

be able to access information in transit between the communicating entities. Later, other security technologies were added such as token authentication. The communication lines were, unfortunately, still open to attack and this lead to the development of secure communication over a public network, a VPN. [1]

Why we use VPNs?

The major benefit of VPNs, from the consumer's point of view, is that they are considerably cost effective. The alternative to using VPN technology is the high-speed leased line. These lines are expensive, difficult to administrate, and difficult to maintain. Additionally, consider what happens when a leased line fails. The communication between the two parties also fails until the appropriate authorities can repair the line. With Virtual Private technology however, if a node in the path or line between routers goes down, the logical path between the parties is simply changed transparently to the user. Using the Internet as the backbone for communication guarantees reliability of service. The Internet provides further benefit for VPN users. Even extremely remote locations have access to the Internet via dial-up modems. VPNs guarantee secure communication for dial-in users. Mobile users cannot possibly use leased lines for their communication with the corporate site and so VPN technology is the only real solution to this problem. Additionally, with user-based authentication, discussed later, companies can keep a closer watch on the information their employees are accessing and thus limit internal fraud. VPNs use the Internet for communication. The Internet does not provide the highest performance solution, but they allow users to use the Internet as their own private networks. This gives users access to the wealth of information available, while allowing reliable, secure communication channels between parties at low cost. Companies have several strong motivations for building VPNs; they provide § a uniform corporate computing environment that is transparent to users, secure communications, & the cost efficiencies of using a common public infrastructure versus building and operating a private WAN. While many networking technologies have not lived up to their initial hype, this is not the case for VPNs, which are being widely deployed and appear to be earning the nickname "very profitable networks." A VPN not only drastically decreases cost but also increases flexibility because corporations can establish or release global Internet connections on demand. They can also initially pay for low bandwidth and increase bandwidth as demand grows. Internet connectivity is also a VPN's major disadvantage: Guaranteeing quality of service (QoS) over the Internet is difficult because aggregate traffic flows can be unpredictable. Service-level agreements (SLAs) between Internet service providers (ISPs) and corporations are an evolving contractual solution designed to guarantee QoS based on throughput, availability, and/or response time thresholds. [10]

HOW IT WORKS:

To use the Internet as a private wide area network, organizations may have to overcome two main hurdles. First, networks often communicate using a variety of protocols, such as IPX and NetBEUI, but the Internet can only handle IP traffic. So, VPNs may need to provide a way to pass non-IP protocols from one network to another.

Second, data packets traveling the Internet are transported in clear text. Consequently, anyone who can see Internet traffic can also read the data contained in the packets. This is clearly a problem if companies want to use the Internet to pass important, confidential business information. VPNs overcome these obstacles by using a strategy called tunneling. Instead of packets crossing the Internet out in the open, data packets are first encrypted for security, and then encapsulated in an IP package by the VPN

and tunneled through the Internet. To illustrate the concept, let's say we're running NetWare on one network, and a client on that network wants to connect to a remote NetWare server.

The primary protocol used with traditional NetWare is IPX. So, to use a generic layer-2 VPN model, IPX packets bound for the remote network reach a tunnel initiating device - perhaps a remote access device, a router, or even a desktop PC, in the case of remote-client-to-server connections - which prepares them for transmission over the Internet. The VPN tunnel initiator on the source network communicates with a VPN tunnel terminator on the destination network. The two agree upon an encryption scheme, and the tunnel initiator encrypts the packet for security. Finally, the VPN initiator encapsulates the entire encrypted package in an IP packet. Now, regardless of the type of protocol originally being transmitted, it can travel the IP-only Internet. And, because the packet is encrypted, no one can read the original data. On the destination end, the VPN tunnel terminator receives the packet and removes the IP information. It then decrypts the packet according to the agreed upon encryption scheme and sends the resulting packet to the remote access server or local router, which passes the hidden IPX packet to the network for delivery to the appropriate destination. [12]

UNDERLYING TECHNOLOGY IN VPNS

Before we examine the structure of VPNs, we must understand the structure of the underlying mechanisms that make them possible. These mechanisms are Tunnels and Firewalls and Proxy Servers. The typical VPN system makes use, primarily, of tunnels and sometimes firewalls and proxy servers. What we present here is a brief reminder of firewalls and proxy servers, and an introduction to tunnels.

Tunnels:

Tunneling or encapsulation is a technique of packaging one network packet inside another. The encapsulated packet is called the tunneled packet and the outer, encapsulating, packet is called the transport packet. All the information in the packet is encrypted at the lowest level, which is the link level of the OSI model. Like VPNs, the concept of encapsulation has been available for many years. It has been used to bridge the portions of the Internet that have disjoint capabilities or policies. The tunnel acts as a router on top of the Internet protocol. The method for encapsulation is quite simple. An outer IP header is added to the original header and between the two of these headers is the security information specific to the tunnel. The outer header specifies the source and destination or "endpoints" of the tunnel while the inner header identifies the original sender and the recipient of the packet.

Remote access VPN:

A remote access VPN connection is made by a remote access client. A remote access client is a single computer user who connects to a private network from a remote location. The VPN server provides access to the resources of the network to which the VPN server is connected. The packets sent across the VPN connection originate at the VPN client. The VPN client authenticates itself to the VPN server and, for mutual authentication, the VPN server authenticates itself to the VPN client.

Site-to-site VPN:

A site-to-site VPN connection connects two portions of a private network or two private networks. For example, this allows an organization to have routed connections with separate offices, or with other organizations, over the Internet. A routed VPN connection across the Internet logically operates as a dedicated Wide Area Network (WAN) link. [5]

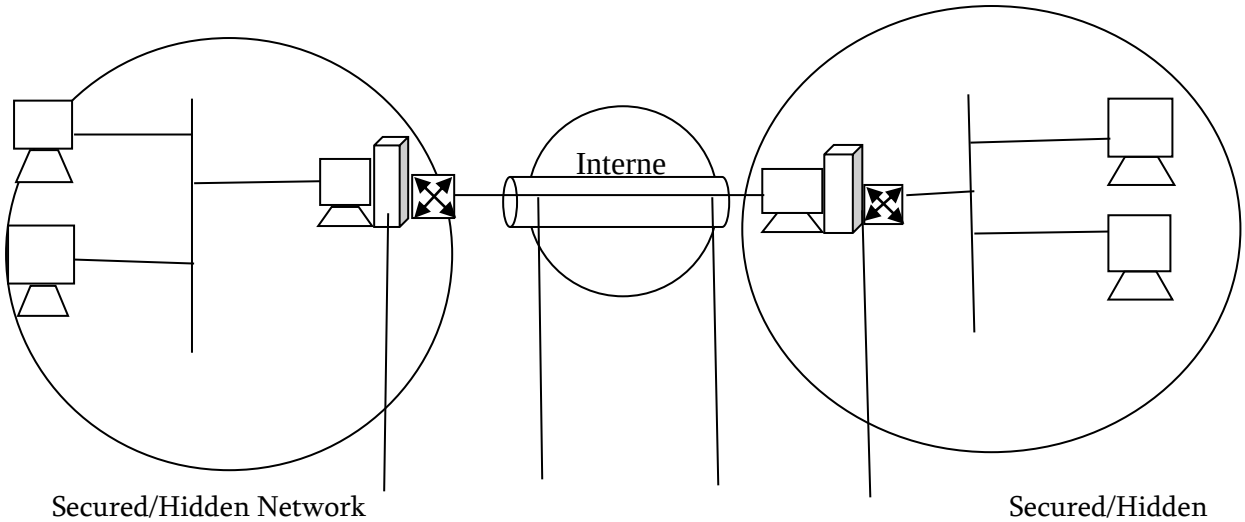


Figure1: VPN ARCHITECTURE [4]

B. ***PROTOCOLS:***

Peer-Peer VPN:

Peer-Peer (P2P) VPN systems that allow only mutually trusted peers to participate. This can be achieved by using a central server such as a connect hub to authenticate clients. Alternatively, users can exchange passwords or cryptographic keys with friends to form a decentralized network. Tunnelling is a network technology that enables the encapsulation of one type of protocol packet within the datagram of a different protocol. For example, Windows VPN connections can use Point-to-Point Tunnelling Protocol (PPTP) packets to encapsulate and send private network traffic, such as TCP/IP traffic over a public network such as the Internet. [18]

The VPN server can be configured to use either Windows or Remote Authentication Dial-In User Service as an authentication provider. If Windows is selected as the authentication provider, the user credentials sent by users attempting VPN connections are authenticated using typical Windows authentication mechanisms, and the connection attempt is authorized using the VPN client's user account properties and local remote access policies.

MPLS VPN:

Multi-Protocol Label Switching (MPLS) VPN is a flexible method to transport and route several types of network traffic using an MPLS backbone. MPLS VPNs combine the power of MPLS and the Border Gateway Protocol (BGP) routing protocol. MPLS is used to forward packets over the provider's network backbone, and BGP is used for distributing routes over the backbone. [31]

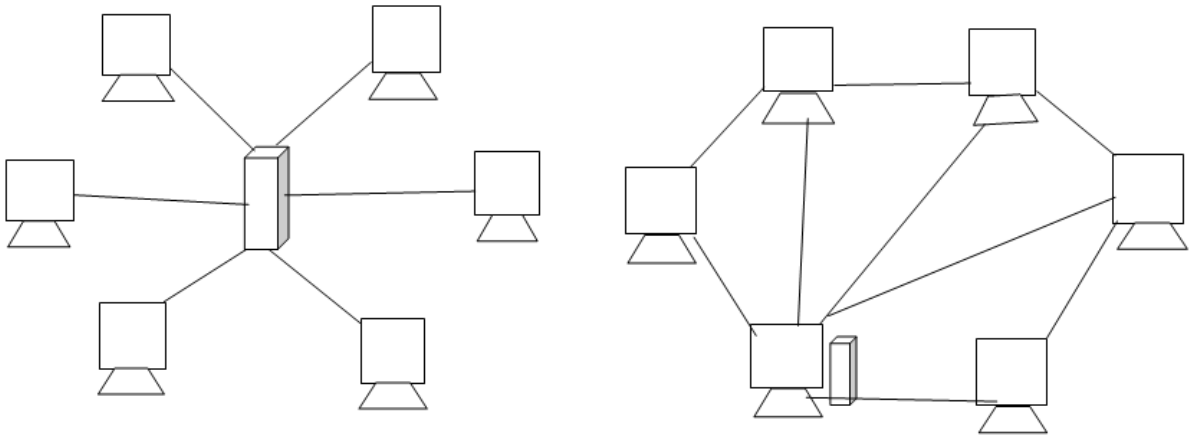
An MPLS virtual private network (VPN) is compromised of the following equipment:

Customer Edge (CE) routers: These are placed on site and are usually owned by the enterprise customer. Some service providers also supply the CE equipment for a small rental fee.

Provider Edge (PE) routers: These are the provider's edge routers to which the CE routers connect to. The PE routers are always owned by the service provider.

Provider (P) routers: These routers are commonly referred to as "transit routers" and are in the service provider's core network.

Routing information is passed from the CE router to the PE router using either static routes or a routing protocol such as BGP. The PE router keeps a per-site forwarding table, also known as a virtual routing and forwarding table (VRF). At the PE router, each VRF serves an interface—or set of interfaces—that belongs to each individual VPN. Each PE router is configured by the service provider with its own VRF that is unique. Routers within the MPLS VPN network do not share VRF information directly. [19]



Centralized Decentralized

Figure 2: Peer-Peer Architecture

The document is arranging as follow. In Section 2 we have **Related Work**, which explains about referred survey and in Section 3, we have **Conclusion**, which is the end part, explains about result in brief.

II. RELATED WORK

VPN meets the four key enterprise necessities are compatibility, security, availability and manageability. A VPN is an extension of an enterprise's private intranet across a public network (the Internet) creating a secure private connection, essentially through a private tunnel. VPNs securely convey information across the Internet connection remote users, branch offices, and business partners into an extended corporate network. The three main types of VPN are i) Network Based VPN ii) CPE Based VPN and iii) Hybrid VPN. [4]

Two approximations that gives optimal solution for MC-VPN (which is more general than MASVPN): ADTH and ASPH. Both algorithms use the same general approach. The algorithms have been tested using simulations and their results have been compared to the results produced by a well-known approximation algorithm for the STP, which does not find a valid solution for MC-VPN but can serve as a benchmark. Although MC-VPN is NP-hard, on the average, both ADTH and ASPH were shown to achieve close to optimal performance. The link's cost over which a VPN tunnels is established and the cost of activating core routers as end points of VPN tunnels. [1]

The main technique underlying VNS is the virtualization of routers in both control and data planes. Virtualization of the control plane enables customizable routing and signalling for VPN. On the other hand, data plane, packet forwarding, and link bandwidth are virtualized. Virtualization of the forwarding mechanism on the data plane enables routing of tracking according to each VPN's topology and policies. Virtualization of the link bandwidth enables each VPN to have guaranteed QoS and

customized resource management policies. VNS is developed using prototype for deployment on the CAIRN network. The VNS prototype implements several resource management mechanisms including packet scheduling, signalling and runtime monitoring. A graphical user interface enables service providers to manage and deploy VPNs remotely. [2]

To guarantee the compatibility and interoperability between various implementations of VPN, the standardization on tunnelling protocol that supporting VPN is necessary. [3]

Potential problems in IPSec policy specification are difficult to analyse due to three reasons. First, Encapsulation in IPSec makes it hard to specify correct selectors. Second, even every policy is correct by its own, policies together might overlap and cause undesired security violation. Third, there is vague relationship between objective and specific policies. To solve the problems, we firstly clear defined security policies in two levels: requirement level security policy and implementation level security policy. Requirement level policies reflect security objective and are implementation independent. Therefore, security requirements become criteria in evaluating policy correctness, i.e. low-level policies are correct if and only if they satisfy all security requirements. We developed algorithms to automatically generate correct low-level policies to meet all requirements. Therefore, people can just specify the desired requirements for protection then correct low level policies will be automatically generated and delivered to appropriate devices to enforce, which will greatly improve policy management. The input of the algorithm is a set of requirements and the output of the algorithm is a set of policies that satisfies all the requirements or return "failure" message if there is no such a set of policies. Three different approaches are the bundle approach in which we generate policies for a set of flows that are subject to a unique set of requirements (we call it a bundle of flows). The approach is correct and complete but not very efficient, next approach, non-overlapping policies for each SCR respectively, and then the resultant policies can satisfy all requirements. This approach is correct and very efficient but not complete, the third approach, combination of the bundle and direct approach to achieve correctness, completeness and efficiency. [6]
VPN technologies are designed to provide the appearance of a dedicated network despite the use of shared resources for physical connectivity. IP-based VPN offer a standard way to exploit the benefits of the public Internet without compromising on the security, reliability and performance that are delivered from dedicated networks. VPN open new opportunities for implementing e-business applications, for extending customer access worldwide, and for connecting remote employees to corporate resources. The deployment of VPN is expected to be a major enabler for business use of the Internet. [8]

In the business world, VPNs let corporate locations share information over the Internet. VPN technology is being extended to the home office, providing telecommuters with the networking security and performance commensurate with that available at the office. Service providers are looking at their geographic footprints and their network routing expertise to create and deliver new revenue-generating VPN services. Looking ahead, these provider-provisioned and managed VPNs are intended to emulate whatever local- or wide-area network connectivity customer's desire. [9]

Hidden Wireless Router Vulnerability for VPN-secured wireless local area networks results that the behaviour of enterprise users might result in a significant number (35% in our test) of legitimately connected wireless terminals being susceptible to becoming HWRs. [11]

Current VPN technologies offer secure and quite stable data connections. One significant drawback which concerns all tested technologies is the dramatic loss of performance and throughput, which goes back to the complex encapsulation and authentication techniques. Thus, it appears that adding VPN technologies to existing protocols comes with additional complexity and high data processing costs. IPSec suffers from a complex tunnel negotiation process, causing interoperability problems between different implementations. L2TP offers data privacy and authenticity if and only if it is combined with IPSec, resulting in excessive data overhead. PPTP is the fastest of the presented technologies, but its security level is, for critical applications, not sufficient. Finally, pheon net fence VPN offers acceptable solutions for the problems which may occur when using e.g. IPSec, but it is only available in combination with the commercial product net fence security gateway series. [13]

A new type of hybrid encryption protocol for VPN data encryption and key management is the VPN server is the trusted authority. The VPN client initiates the request; the VPN server gives the key value. Using the key value VPN client securely encrypt data with the help of AES-Rijndael. Then the key value encrypted using receivers public key with the help of RSA. Then these encrypted values integrated together and send to the receiver. The receiver using its private key and RSA identify the original key value. Using the key to decrypt the encrypted data with the help of AES-Rijndael. [14]

Firewalls provide more security than a border router by making the voice information less susceptible to attacks from an insider to the network and they can easily and reliably handle and protect several types of clients in small office environments, control access restricting traffic coming into the inside network and encrypt IP voice packets using IPSec tunnelling before the voice packets reach the access switch. [15]

For Virtual Private Network to ensure security, data must be encapsulated and encrypted before sending the packets over the Internet. The various protocols used like IPSec, L2TP, PPTP, SOCKS etc. While PPTP, developed by Microsoft and implemented heavily on it legacy operating system, it has its own flaws and require the support of an extra protocol, currently IPSec, to be secure. The different protocols act at different layers of the OSI protocol stack layer model and hence can be combined to enhance security in VPN. [16]

N2N users can create and manage their own secure and geographically distributed overlay network without any need for central administration, typical of VPN systems. [17]

VPN provides a means of retrieving a secure, private, internal network over uncertain public networks such as the Internet. Several VPN technologies have been drawn, among which IPsec and SSL VPN are the most common. Although a secure communication channel can be opened and tunnelled through an insecure network via VPN, client-side security should not be ignored. [20]

Every protocol has its own advantages and disadvantages. If an organisation allows remote access employees, then IPSec based VPN is preferable, but IPSec based VPN doesn't support roaming in such cases SSL based VPN is optimum preferable. [21] Simulation of wireless LAN for IEEE802.11g protocol has been done, and analyses impact of integrating Virtual Private Network technology to secure the flow of traffic between the client and the server farm using OPNET WLAN utility has been carried out. Two Wireless LAN scenarios have been considered and the results compared. These are Normal Extension to a wired network and VPN over Extension to a wired network. The results collected from the two scenarios, indicate the impact of performance, mainly Response Time and Load, of Virtual Private Network over wireless LAN. [22]

Streaming movie over VPN using software base contribute higher CPU utilization compare to VPN hardware device and shows that memory usage achieved approximately the same result for software and hardware over VPN. It is recommended to implement streaming movie over VPN using hardware platform in order that to achieve a good QoS. It is also suggested to have a high CPU and memory performance to support VPN using software and hardware platform. [23]

The QoS in a videoconference using IP infrastructure is most affected by the packet loss parameter when using IPSec tunnels. The main reason behind this is the traffic load. When IPSec is used to protect the data between two hosts, or between two gateways, or between a host and a gateway then with the data AH and ESP headers are also included so it increases the overhead and that's why the traffic load also increases. And if traffic load increases then there may be the case of congestion in the network that leads to result in packet loss. On the other hand, jitter is not much affected by the IPSec VPN. Even though the average result remained a little over the ideal limit with and without VPN, it did not affect the videoconference quality in a visible or audible way. Other parameters like R-Factor and MOS was also not affected by the IPSec VPN because in all the environments the user is satisfied by the voice quality. From above reasons, it can be deduced that it is feasible to implement IPSec VPNs for the small size network where there is no congestion in the network. And if IPSec VPN is applied in highly saturated networks with higher traffic loads it is necessary to use techniques that can protect and rank the information to make the traffic transmission secure without disturbing the QoS constraints. [25]

EEVPN is more effective because it is faster than other VPNs in sending small data size; where it takes small data transmission time, achieving high level of security. Also, the EEVPN is more extensive because it is not built for a specific environment, which makes the customization of the VPN is very difficult, so it can be installed at any environment which is faster and more secured than many other VPNs like CISCO VPN and IBM VPN in case of transmitting small data size (i.e. less than 1 MB). [26]

VPN technologies which utilize SSL/TLS or IPsec protocols to create secure tunnel for data transmission, e.g. to interconnect two IMS networks. A several tests have been performed to compare these technologies based on constraints such as quantity, response time and so on. We can review that it is difficult to choose the better of these two technologies based on all views. Each user has different needs. For our implementation we decided to choose Open VPN, due to its easiness and fast and straightforward implementation. On the other hand, IPsec is slightly faster and as it has been on the market much longer than SSL VPN solutions and has distant support among hardware and software vendors. [27]

IPSec and SSL VPN technologies are developing out as a popular trend in WLAN as they provide better data confidentiality services. Based on the requirement and need an enterprise can choose any of them. Combination of advantages of both technologies giver more effective and secure communication [28]

IPSec is one of the most efficient ways of securing data communication between remote locations. This makes the IPsec market a very dynamic and challenging one, one of the first conditions when implementing a protocol is to be compliant to the RFC, making the device interoperable with other standard products following the same security policy standard. This may be a good strategy for market capturing but Cisco, for instance, uses another strategy to keep its market share high. Specific closed implementation of the protocol, vendor specific parameters while the IPsec negotiation takes place, private protocols or features are made, available only

on their systems. Trying to create a diverse environment with as many different devices as possible is difficult and confusing. In case of using standard security, policy there is a way of configuring different devices to understand each other and work correctly together, to inter-operate, if a certain feature is supported as declared by its vendor. [29]

To overcome the weakness and combine the advantages of traditional VPN, MPLS VPN has its features and functions to solve a series of problems including address overlapping, data-sending-isolation, transparency, flexibility, high efficiency and easy management. So, it is a cost-effective and secure solution for the company customer to connect different sites around the world together. [30]

The advantages of the formation of the VPN network can avoid the problems that the kernel mode changes in the IP packet format. It is better to go through the network equipment and make network shared resources become more secure and flexible. The disadvantages are that the system handles the packet when it goes through the TCP/IP protocol stack twice. So, the system reduces the processing speed and cannot meet that the network applications develops rapidly fully. However, the way to set up the VPN network is simple and practical, which has a good application prospects in the remote secure transmission. [32]

VPN Encryption methodologies, Advanced Encryption standard, BlowFish, The International Data Encryption Algorithm and RC4 algorithms are preferred for more secure VPN communication. [33]
Security is the most important and critical factor for companies worldwide. Organizations need a secure and reliable infrastructure for their systems to mitigate the risk of malicious activity from both external and internal sources. Organizations worldwide have major security concerns namely, Data access from the remote site, Infection by viruses, Intrusion by hackers and Disruption in the storage network. [34]

The secure data transmission over WiMAX network using VPN technology are evaluated for both MAC layer security and IPSec using test bed experiments. Even though IPSec provides strong data security using IPSec tunnels for both wired and wireless networks, The QoS performance can be improved by using MPLS technology along VPN. However, no articles have reported actual experiments on or real measurements of the overhead of IPSec. Based on the existing research, modified IPSec may be combined with mobile IP (MIP) to support the mobile WiMAX networks. [36]

VPNs represent an extension of a private network made through added features like encapsulating the data packets with a header on both ends, along the lines of the communication as well as throughout setting communication tunnels using composite suite of protocols available. A set of simulated secure data communication tunnels together with a comparison of results of the speed variables measured against the security through different encryption protocols between remote LAN's. These encryption protocols are running onto distributed queries using various database functions. [37]

OPNET Modeler simulator was used as a simulation tools to investigate the impact of VPN and firewall security systems on throughput, delay and traffic received on the system and individual nodes of the network. The applications considered for the mentioned investigation are e-mail application and web browsing application. The followings can be made: I- The integration of VPN with Firewall in cloud computing will reduce the throughput. This is because the number of bits transmitted per second is less than the cloud computing without VPN. This is because the VPN with firewall would not allow every access to the server. Furthermore, the delay in system without VPN is slightly larger than the cloud

computing with VPN. II- No traffic received and sent from server AA for e-mail application in cloud computing with firewall and no VPN. This is because the firewall would prevent any email access to the server AA and the existence of VPN in the system would allow specified stations (PC's) to access server AA. However, there would be no traffic received and sent for server BB in (VPN firewall) and (firewall no VPN) systems. This is now because VPN acts as a tunnel to allow email access to server AA only. III- In web browsing applications, there would be traffic sent and received in the case of cloud computing with VPN and without VPN. This is because the VPN firewall would prevent only access to the server for email application but not web applications. VPN technology is a suitable way to secure cloud computing and decreasing the traffic in the system to achieve the desired level of security. The security was provided in VPN technology should be provided with firewall that allows only specific access to the server. [38]

Virtual Private Network provides security and privacy to data in a public network. This technology is cost effective and efficient transmission of data among the network. In Window 2003 PPTP shows the highest output while SSL shows the lowest. In Linux SSL shows the better output than IPsec. IPsec values are relatively lower than that on Windows platform. So, it is evident that network performance of VPN tunnel is dependent on the choice of the operating system, VPN protocol, and VPN algorithms. [39]

Internals and their infrastructures being a known issue, VPN services suffer from IPv6 traffic leakage. The work is extended by developing more sophisticated DNS hijacking attacks that allow all traffic to be transparently captured. [41]

The presence of tracking services and malware on VPN app binaries to artefacts implemented by these apps at the network level. Our complete tests allowed us to identify instances of VPN apps embed third-party tracking services and implement abusive practices such as Java Script injection, ad-redirections and even TLS interception. The capability of the BIND_VPN_SERVICE permission to break Android's sandboxing and the naive awareness that most users have about third-party VPN apps suggest that it is urging tore-consider Android's VPN permission model to increase the control over VPN clients. [42]
Based on the multi-campus security interconnection and remote access requirements, the design and deploy of multi campus network VPN security interconnection scheme, has a certain practical significance. Scheme of comprehensive application of IPSec VPN, L2TP over IPSec VPN and firewall technology that improve the safety of campus network interconnection and enhance the accessing experience of users outside the campus to access the resource in remote. The successful implementation of the project can provide effective reference of multi-campus network interconnection for other colleges, universities and enterprise. [43]

First comprehensive analysis of 283 Android apps that use the Android VPN permission, which was extracted from a corpus of more than 1.4 million apps on the Google Play store performs several passive and active measurements designed to investigate a wide range of security and privacy features and to study the behaviour of each VPN-based app. Investigation of possible malware presence, third-party library embedding, and traffic manipulation, as well as gauging user perception of the security and privacy of such apps. Serious privacy and security vulnerabilities, such as use of in secure VPN tunnelling protocols, as well as IPv6 and DNS traffic leakage. We also report on several apps actively performing TLS interception. Of concern are instances of apps that inject Java Script programs for tracking, advertising, and for redirecting e-commerce traffic to external partners. [44]

VPN endpoints are traditionally deployed on specialized network appliances, such as routers or firewalls/security devices. In this paper, we explored the viability of the endpoints virtualization on COTS hardware, with benefits in line with the NFV paradigm. We find that VPN functionality of entry level appliances (up to about 1Gbps) can be easily virtualized even on low end servers. In most cases, both IPSec and OpenVPN will suffice. Although IPSec generally provides better throughput, OpenVPN has an advantage of setting up tunnels over UDP, which can lower latency and in special cases, such as satellite links, improve overall throughput. On mid-range appliances, we expect a throughput of up to about 25Gbps. OpenVPN does not scale on multi-core systems so it is not suitable for such high requirements. Strong Swan's IPSec implementation does scale and it can be used in the lower range of throughput requirements. Depending on a specific use case, and with proper configuration and optimization, it, possibly, might also be used in the upper range. When it comes to high-end security appliances, can't see any benefits of virtualization of their functionality on COTS hardware. [46]

The usefulness of VPN-IP tunnelling is usually disrupted by joint node location and link connection problems for efficient resource utilization the optimization problems have been formulated. Simulation implementation with Riverbed modeler showed the reachability response time for all the VPN sites. Tunnel end-to-end delay, delay variation, throughput and resource utilization metrics were presented. The challenges of VPN_IP backbone were discussed while advancing discussions on MPLS Layer 3 VPNs. The 19.2 Tbps capacity presently in Nigeria can only be harnessed with well-planned traffic engineering with the MPLS Layer 3 VPN domain. However, there are vital features of MPLS VPN to consider when selecting its routing protocol. These have been identified to include: the network topology, addressing and route summarization, route selection, convergence, network scalability and security. In addition, a new routing algorithm for the optimization problems will satisfy following metrics (in determining the best route to a destination network) including: path length, reliability, delay bandwidth, load and communication cost, optimality, simplicity, robustness, rapid convergence, and addressing and summarization. By enabling MPLS Layer 3 VPN traffic engineering (tunnelling signalling) on the router, the resulting QoS will facilitate efficient bandwidth utilization, as well as CPU resource utilization. [47]

It is very efficient to secure user's private information. It protects user's information from the intruders. And VPN technology is a very cost-effective technology. And, this technology is easy to use. Protocols have own different strength. There are some VPN protocols like PPTP, L2TP, IPSec and SSL. Protocols use different ports and provide Encryption. VPN protocols have different speed and security. The IPSec protocol is better than the other protocols. [48]
MPLS platform is currently compatible with the OPNET Modeler tool. Thanks to its data layer, control, and management architecture, this platform can be adapted for any simulator. Platform can generate hundreds of different scenarios in less than a minute, the thing that takes more than an hour with other configuration methods. Platform allows generating scenarios by varying the sites number, the clients by sites, the applications, and the links technology. To facilitate its use, developed a new web tool to guide the user through steps to generate and download his complete project. Evaluating its performance in different cases: increasing the number of scenarios up to 40 scenarios, increasing the number of clients for each scenario up to 29 clients and varying the applications. To adapt it to other network concepts and other simulators. [49]
This document provides an Easy VPN (EzVPN) sample configuration, using Cisco 1800 series, Cisco 2800 series, and Cisco 3800 series routers. [50]

III. CONCLUSION

VPNs allow users or corporations to connect to remote servers, branch offices, or to other companies over a public internetwork, while maintaining secure communications. In all these cases, the secure connection appears to the user as a private network communication-despite the fact that this communication occurs over a public internetwork. VPN technology is designed to address issues surrounding the current business trend towards increased telecommuting and widely distributed global operations, where workers must be able to connect to central resources and communicate with each other.

We categorized all the different types of VPNs and noted that their flexibility allows the customer to choose which facilities are desired. VPNs can offer a variety of encryption, authentication, and integrity algorithms. The company can formulate a security profile for their offices and choose the VPN solution best suited to their needs. We examined in detail the various protocols used in VPNs and noted that, due to VPN technology being new, no one standard has yet been adopted by a clear majority. VPNs are still in their infancy and the full potential for VPNs is yet to be exploited. VPNs are promising for the future for secure communication via the Internet. It is expected that the VPN industry will be very big market in the following years. It is important that the chosen standards suit the customer's needs and that their flexibility is maintained.

VPNs are a flexible, low-cost, highly secure communication tool. The development of this new technology over the next few years could well define the standard for secure communication across the Internet.

IV. REFERENCES

[1] Reuven Cohen and Gideon Kaempfer, "On the Cost of Virtual Private Networks", IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 8, NO. 6, DECEMBER 2000.

[2] L. Keng Lim Jun Gao T.S. Eugene Ng Prashant Chandra Peter Steenkiste Hui, "Customizable Virtual Private Network Service with QoS", Zhang Carnegie Mellon University Pittsburgh, PA 15213, August 1, 2000.

[3] ZaoAqun and Yuaan Yuan, "RESEARCH ON TUNNELING TECHNIQUES in VIRTUAL PRIVATE NETWORKS", 2000, IEEE.

[4] O. Satty Joshua, "IP-VPN Architecture and Implementation", 13 December 2001.

[5] Yurcik and W. Doss, "A planning framework for implementing VPNs", Volume: 3 Issue: 3, May-June 2001.

[6] Zhi (Judy) Fu1 and S. Felix Wu2, "Automatic Generation of IPSec/VPN Security Policies in an Intra-Domain Environment",12th International Workshop on Distributed Systems, Oct:15-17,2001.

[7] Dr.Gray, "Virtual Private Network", IS 311, Tuesday 7pm, November 19, 2002.

[8] Sid, "The Advantages of a Virtual Private Network for Computer Security", Sid Sirisukha School of Information Technology Auckland University of Technology, 2003.

[9] Networks and Chris Metz, "The Latest in Virtual Private", Cisco Systems, JANUARY-FEBRUARY 2003.

[10] Shashank Khanvilkar and Ashfaq Khokhar, "Virtual Private Networks: An Overview with Performance Evaluation", University of Illinois at Chicago, IEEE Communications Magazine, October 2004.

[11] Sachin Ganu1, Martin Kappes, A.S. Krishnakumar, P. Krishnan and Lookman Fazal, "Tackling Security Vulnerabilities in VPN-based Wireless Deployments", ,IEEE Communications Society, 2004 IEEE.

[12] Yoshinori Fujimoto, Tokyo (JP); Tomoki Ohsawa and Tokyo, "VIRTUAL PRIVATE NETWORK", U.S, Mar. 18, 2004.

[13] Thomas Berger University of Salzburg, "Analysis of Current VPN Technologies", Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06) 2006 IEEE.

[14] E. Ramaraj and S. Karthikeyan, "A New Type of Network Security Protocol Using Hybrid Encryption in Virtual Private Networking", Journal of Computer Science, Science Publications, 2006.

[15] Sergio Chacon, Driss Benhaddou, and Deniz Gurkan, "Secure Voice over Internet Protocol (VoIP) using Virtual Private Networks (VPN) and Internet Protocol Security (IPSec)", IEEE,2006.

[16] Benjamin Odiyo, Mukunda Dwarkanath, Virtual Private Network, 2007.

[17] Luca Deri1 and Richard Andrews, D. Hausheer and J. Schönwälder, "N2N: A Layer Two Peer-to-Peer VPN", Italy Symstream Technologies, Melbourne, Australiarg, (Eds.): AIMS 2008, International Federation for Information Processing 2008.

[18] Mukherjee et a "METHOD AND APPARATUS FOR ENABLING PEER-TO-PEERVIRTUAL PRIVATE NETWORK (P2P-VPN) SERVICES IN VPN-ENABLED NETWORK", Sep. 2, 2008.

[19] Roy et al, "SYSTEM AND METHOD FOR FORWARDING TRAFFC DATA IN AN MPLS VPN", Apr. 3, 2008.

[20] "VPN SECURITY", February 2008.

[21] A.Venkateswari et al, "COMPARATIVE STUDY OF PROTOCOS USED IN VPN". International Journal of Engineering science and Technology, Vol1 (3), 2009.

[22] H. Bourdoucen, A. Al Naamany and A. Al Kalbani "Impact of Implementing VPN to Secure Wireless LAN", World Academy of Science, Engineering and Technology 27 2009.

[23] MohdNazri Ismail "Study the Best Approach for Virtual Private Network Implementation: CPU and Memory Usage Performance", INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY SCIENCES AND ENGINEERING, VOL. 1, NO. 2, NOVEMBER 2010.

[24] "Mobile Implementations of Virtual Private Networks", 2010.

[25] Ritu Malik, Rupali Syal, "Performance Analysis of IP Security VPN", International Journal of Computer Applications Volume 8– No.4, October 2010.

[26] Tarek S. Sobh, Yasser Aly, "Effective and Extensive Virtual Private Network", Journal of Information Security, Volume 2, 39-49 January 2011.

[27] Kotuliak, P.Rybár and P.Trúchly, "Performance Comparison of IPsec and TLS Based VPN Technologies",ICETA 2011 • 9th IEEE International Conference on Emerging eLearning Technologies and Applications • StaráLesná, The High Tatras, Slovakia, October 27-28, 2011.

[28] Ritika kajal, Deepshikha Saini and Kusum Grewal, "Virtual Private Network", Volume 2, Issue 10, October 2012.

[29] Arun Kumar Singh, Shefalika Ghosh Samaddar and Arun K. Misra, "Enhancing VPN Security through Security Policy Management", Computer Science and Engineering Department, 2012.

[30] Ming-Song Sun, Wen-Hao Wu, "Engineering Analysis and Research of MPLS VPN", Network Information Center, Harbin University of Science and Technology©2012 IEEE.

[31] Luca Cittadini Giuseppe Di Battista Maurizio Patrignani, L. Cittadini, G. Di Battista, M. Patrignani,, "MPLS Virtual Private Networks", Advances in Networking, (2013

[32] LUO Zhiyong, YU Guixin, QI Hongzhuo, "Research of A VPN Secure Networking

Model", International Conference on Measurement, Information and Control, Harbin University of Science and Technology Harbin, China, 2013 2nd.

[33] M.A. Mohamed1, M.E.A. Abou-El-Seoud and A.M. El-Feki2, "A Survey of VPN Security", IJCSI International Journal of Computer Science Issues, Vol. 11, Issue 4, No 1, July 2014.

[34] El bachir El achhab, "On the Impact of Virtual Private Network Technologies on the Operational Costs of Cellular Machine-to-Machine Communications Platforms for Smart Grids", Network Protocols and Algorithms Vol. 6, No. 3, 2014.

[35] JAYANTHI GOKULAKRISHNAN, "A SURVEY REPORT ON VPN SECURITY & ITS TECHNOLOGIES", Vol. 5 No.4 Aug-Sep 2014.

[36] J. Balu and DR.S. THIRUNIRAI SENTHIL, "SECURE DATA TRANSMISSION OVER WIMAX NETWORKS USING VPN TECHNOLOGY IN REALTIME ENVIRONMENTS", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.2, February- 2014.

[37] Muhamed Elezia and Bujar Raufia, "Conception of Virtual Private Networks using IPsec suite of protocols, comparative analysis of distributed database queries using different IPsec modes of encryption", The Authors. Published by Elsevier Ltd. Univeristy,2015.

[38] M. Judith Bellar, "Cloud Computing Security with VPN", International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 8, August 2015.

[39] Sneha Padhiar and Pranav Verma "A Survey on Performance Evaluation of VPN on various Operating System", IJEDR | Volume 3, 2015.

[40] Vasile C. Perta, Marco V. Barbera, Gareth Tyson, Hamed Haddadi1 and Alessandro Mei2, "A Glance through the VPN Looking Glass: IPv6 Leakage and DNS Hijacking in Commercial VPN clients", Proceedings on Privacy Enhancing Technologies 2015.

[41] Krithikaa, M. Priyadharsini and C.Subha, "Virtual Private Network – A Survey", IT Department, Sri Krishna Arts and Science College, Coimbatore, TamilNadu, India, IJTRD | Jan - Feb 2016

[42] Muhammad Ikram, Narseo Vallina-Rodriguez, Suranga Seneviratne1, Mohamed Ali Kaafar1 and Vern Paxson, "An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps", Berkeley, ACM. ISBN,2016.

[43] Shan Jing Shandong and RunyuanSun, "Study on VPN solution based on multi-campus network", IEEE,2016.

[44] Sourabh Kumar Vishali Sharma, "A Security Solution for Wireless Local Area Network (WLAN) Using Firewall and VPN", Innovative Systems Design and Engineering Vol.7, No.7, 2016.

[45] Saugat Bhattarai, "VPN research (Term Paper)", Kathmandu University, Research · January 2016.

[46] D.Lacković and M. Tomić, "Performance Analysis of Virtualized VPN Endpoints", MIPRO 2017, May 22- 26, 2017.

[47] M. N. Ogbu, G.N. Onoh and K.C. Okafor "Cloud Based Virtual Private Networks Using IP Tunnelling for Remote Site Interfaces", , IEEE 3rd International Conference on Electro-Technology for National Development,2017.

[48] Avani, J.Patel and Ankitha Gandhi "A Survey of VPN Performance Evaluation", IJRITCC | May 2017.

[49] Ayoub BAHNASSE and Ben M'SIK Hassan "New Smart Platform for Automating MPLS Virtual Private Network Simulation", university of Casablanca, IEEE,2018.

[50] "Easy VPN Configuration Example" https://pdfs.semanticscholar.org/presentation/a650/730b9067fc8cbe2088bb738dee261f3384b6.pdf.