International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 09 | Sep 2019 www.irjet.net p-ISSN: 2395-0072

# A SURVEY OF WORKING ON VIRTUAL PRIVATE NETWORKS

**KOMALPREET KAUR[1], ARSHDEEP KAUR[2]**

*[1]Department of Computer Science Engineering, Amritsar College of Engineering and Technology, Amritsar, Punjab, India*
*[2]Department of Computer Science Engineering, Swami Sarvanand group of institution, Dinanagar, Punjab, India*

---

**Abstract -** *Virtual Private Network (VPN) is rapidly growing technology which plays a important role in Wireless LAN (WLAN) by providing secure data transmission. The purpose of VPN is to provide safe and secure communication by creating virtual tunnels between pair of hosts, once tunnel is created data transfer can take place. This paper presents a comprehensive study of VPN.VPN, architecture and protocols used in this paper. 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), its protocols and Security in VPN. In this paper we have discussed about various protocol used in VPN.*

***Key Words*: VPN, Architecture of VPN, Protocol in VPN**

## 1. INTRODUCTION ABOUT VIRTUAL PRIVATE NETWORK

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 man oeuvres 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. [1] 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.

**Features in VPN [6]**

• Provide extended connections across multiple geographic locations without using a leased line.
• Improving security mechanism of data using encryption techniques.
• Provides flexibility for remote offices and employees to use the business intranet over an existing Internet connection as if they're directly connected to the network
• Saves time and expense for employees who commute from virtual workplaces
• VPN is preferred over leased line since leases are expensive, and as the distance between offices increases, the cost of leased line increase
. • IPSec VPN and SSL VPN are two solutions of VPN which are widely used in WLAN. We will discuss both of them together with their advantages and disadvantages.

**Advantages of VPN [7]**

• There are two main advantages of VPN's, namely cost saving and scalability.
• VPN's lower costs by eliminating the need for expensive long-distance leased lines.
• A local leased lines or even broadband connection is all that's needed to connect the internet and utilize the public network to surely tunnel a private connection.
• Data transfers are encrypted
• Cost is low to implement.

**Disadvantages of VPN [7]**

• VPN connection is slow.
• Because the connection travels over public lines, a strong understanding of network security issues and proper precautions before VPN deployment are necessary.
• VPN connection stability is mainly in control of the internet scalability, factors outside an organization control.

- Differing VPN technology may not work together due to immature standards.
- Bad hardware and low speed connection on the user end.

### 1.1 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]

## 2. ARCHITECTURE OF VIRTUAL PRIVATE NETWORK

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.

### 2.1 Tunnel

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 disjointed 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.

### 2.2 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.

### 2.3 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]

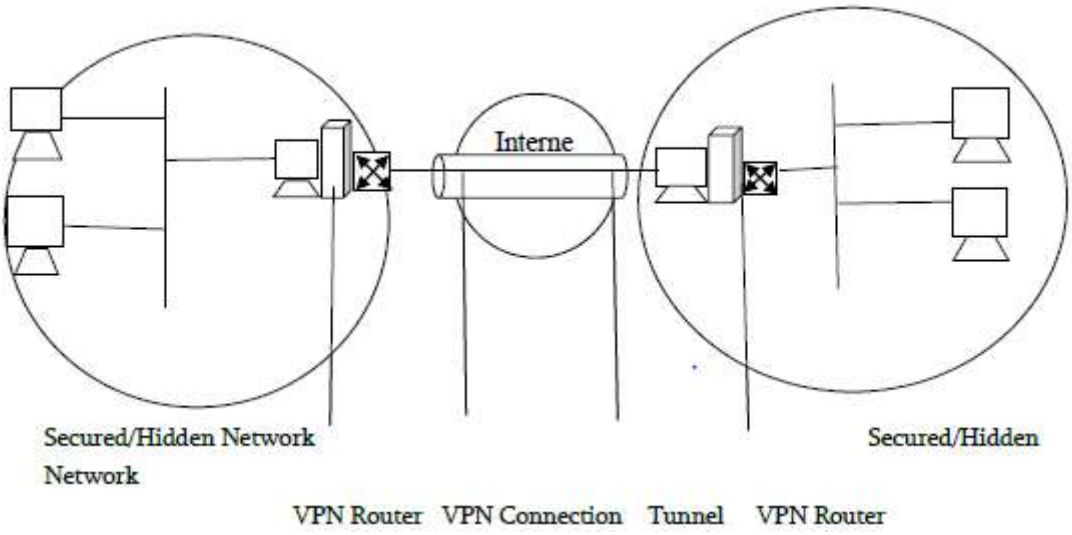



**Figure1:** VPN ARCHITECTURE

## 3. 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. [2]

## 4. PROTOCOL IN VPN

### 4.1 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. Tunneling 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 Tunneling Protocol (PPTP) packets to encapsulate and send private network traffic, such as TCP/IP traffic over a public network such as the Internet. [3] 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.

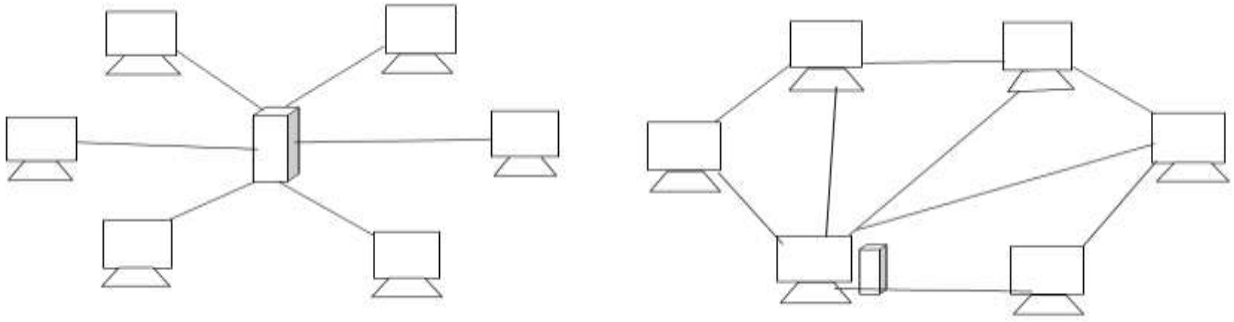
### 4.2 MPLS VPN

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. [4] 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).



Centralized Decentralized

**Figure 2**: Peer-Peer Architecture

## 5. CONCLUSION

VPNs allow users or corporations to connect to remote servers, branch offices, or to other companies over a public inter-network, while maintaining secure communications. 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. In this paper, we have a survey on Virtual Private networks. Firstly, we discussed about Virtual private networks and its architecture, advantages, disadvantages. We have also defined how to works VPN. Thus in the end we have reviewed various protocol in VPN.

## REFERENCES

[1]. K. Karuna Jyothi*, Dr. B. Indira Reddy, "Study on Virtual Private Network (VPN), VPN's Protocols And Security", International Journal of Scientific Research in Computer Science, Engineering and Information Technology © 2018 IJSRCSEIT | Volume 3 | Issue 5 | ISSN : 2456-3307
[2]. Yoshinori Fujimoto, Tokyo (JP); Tomoki Ohsawa and Tokyo, —VIRTUAL PRIVATE NETWORK, U.S, Mar. 18, 2004.
[3]. Mukherjee et a —METHOD AND APPARATUS FOR ENABLING PEER-TO-PEERVIRTUAL PRIVATE NETWORK (P2P-VPN) SERVICES IN VPN-ENABLED NETWORK||, Sep. 2, 2008.
[4]. Luca Cittadini Giuseppe Di Battista Maurizio Patrignani, L. Cittadini, G. Di Battista, M. Patrignani,, —MPLS Virtual Private Networks||, Advances in Networking, (2013).
[5]. Yurcik and W. Doss, —A planning framework for implementing VPNs||, Volume: 3 Issue: 3, May-June 2001.
[6]. Ritika kajal, Deepshikha Saini, Kusum Grewal- International Journal of Advanced Research in Computer Science and Software Engineering (2012) Volume 2, Issue 10, October 2012.
[7]. M.Krithikaa, 2M.Priyadharsini and 3C.Subha- Virtual Private Network – A Survey, International Journal of Trend in Research and Development, Volume 3(1), ISSN: 2394-9333.