IJFEAT

INTERNATIONAL JOURNAL FOR ENGINEERING APPLICATIONS AND TECHNOLOGY

VIRTUAL PRIVATE NETWORK

Suneet S. Khare[1]

[1]*Student, MBA, Ashoka Business School, Maharashtra, India,* ***suneetk853@gmail.com***

Abstract

Virtual. Virtual means not real or something which do not exist materially. Through a public network called as Internet, private communication between two users is carried out in VPN. Thus here the communication is virtual rather than the physical.

Private. Private means to keep something to yourself. In VPN word private means, two users communicate in public environment but a third party or user cannot interrupt their communication or receive any data.

Network. A network can be defined as a place where two or more devices can freely and electronically communicate with each other via cables and wire. A VPN is a network in which information can be transmitted over long distances effectively and efficiently.

---------- *** ----------

1. INTRODUCTION

The term VPN has been associated in the past with such remote connectivity services as the (PSTN), Public Switched Telephone Network. But VPN networks have finally started to be linked with IP-based data networking. Before IP based networking corporations had expended considerable amounts of time and resources, to set up complex private networks, now commonly called Intranets. These networks were installed using costly leased line services, Frame Relay, and ATM to incorporate remote users. For the smaller sites and mobile workers on the remote end, companies supplemented their networks with remote access servers or ISDN.

Small to medium-sized companies, who could not afford dedicated leased lines, used low-speed switched services. As the Internet became more and more accessible and bandwidth capacities grew, companies began to put their Intranets onto the web and create what are now known as Extranets to link internal and external users. However, as cost-effective and quick-to-deploy as the Internet is, there is one fundamental problem – security. Today's VPN solutions overcome the security factor using special tunnelling protocols and complex encryption procedures, data integrity and privacy is achieved, and the new connection produces what seems to be a dedicated point-to point connection. And, because these operations occur over a public network, VPNs can cost significantly less to implement than privately owned or leased services. Although early VPNs required extensive expertise to implement, technology has matured to a level where deployment can be a simple and affordable solution for businesses of all sizes.

1.1 TYPES OF VPN

VPNs are broken into 4 categories-

1) Trusted VPN: A customer "trusted" the leased circuits of a service provider and used it to communicate without interruption. Although it is "trusted" it is not secured.
2) Secure VPN: With security becoming more of an issue for users, encryption and decryption was used on both ends to safeguard the information passed to and fro. This ensured the security needed to satisfy corporations, customers, and providers.
3) Hybrid VPN: A mix of a secure and trusted VPN. A customer controls the secure parts of the VPN while the provider, such as an ISP, guarantees the trusted aspect.
4) Provider-provisioned VPN: A VPN that is administered by a service provider.

2. VPN TOPOLOGY

To begin using a VPN, an Internet connection is needed; the Internet connection can be leased from an ISP and range from a dial up connection for home users to faster connections for businesses. A specially designed router or switch is then connected to each Internet access circuit to provide access from the origin networks to the VPN. The VPN devices create PVCs (**Permanent Virtual Circuit**- a virtual circuit that resembles a leased line because it can be dedicated to a single user) through tunnels allowing senders to encapsulate their data in IP packets that hide the underlying routing and switching

infrastructure of the Internet from both the senders and receivers.

The VPN device at the sending facility takes the outgoing packet or frame and encapsulates it to move through the VPN tunnel across the Internet to the receiving end. The process of moving the packet using VPN is transparent to both the users, Internet Service Providers and the Internet as a whole. When the packet arrives on the receiving end, another device will strip off the VPN frame and deliver the original packet to the destination network.

VPNs operate at either layer 2 or layer 3 of the OSI model (Open Systems Interconnection). Layer-2 VPN uses the layer 2 frame such as the Ethernet while layer-3 uses layer 3 packets such as IP. Layer-3 VPN starts at layer 3, where it discards the incoming layer-2 frame and generates a new layer-2 frame at the destination. Two of the most widely used protocols for creating layer-2 VPNs over the Internet are: layer-2 tunneling protocol (L2TP) and point-to-point tunneling protocol (PPTP).

2.1. BENEFITS OF VPN

VPN's Benefit a company in the following ways

1) Extends Geographic Connectivity- a VPN connects remote workers to central resources, making it easier to set up global operations.

2) Boosts Employee Productivity- A VPN solution enables telecommuters to boost their productivity by 22% - 45% (Gallup Organization and Opinion Research) by eliminating time-consuming commutes and by creating uninterrupted time for focused work.

3) Improves Internet Security – An always-on broadband connection to the Internet makes a network vulnerable to hacker attacks. Many VPN solutions include additional security measures, such as firewalls and anti-virus checks to counteract the different types of network security threats.

4) Scales Easily – A VPN allows companies to utilize the remote access infrastructure within ISPs. Therefore, companies are able to add a virtually unlimited amount of capacity without adding significant infrastructure.

3. CONCLUSION

VPN is an emerging technology that has come a long way. From an insecure break off of Public Telephone networks to a powerful business aid that uses the Internet as its gateway. VPN's technology is still developing, and this is a great advantage to businesses, which need to have technology that is able to scale and grow along with them. With VPN businesses now have alternative benefits to offer to their employees, employees can work from home, take care of children while still doing productive, and have access work related information at any time. VPN will also help to make the possibility of a business expanding its services over long distances and globally, more of a reality.

4. FUTURE OF VPN

As more and more businesses demand a higher level of network access, the business is migrating from a private network environment to a new model in which information is distributed throughout the enterprise network. Thus, expanding their network in the near future and actually seeing the benefits of using the Internet as the backbone to create Virtual Private Networks (VPN). VPN is designed to meet the demands for information access in a secure, cost-effective environment.

Multi-vendor interoperability for VPN is crucial in today's networking environment due to the nature of business successes, the need to extend corporate networks to contractors and partners, and the diverse equipment within company networks. The Microsoft Windows operating system has integrated VPN technology that helps provide secure, low-cost remote access and branch office connectivity over the internet.

REFERENCES

[1]. http://www.checkpoint.com/products/downloads/vpn-1_remote_access.pdf

[2]. ftp://ftp.isi.edu/in-notes/rfc2386.txt

[3]. http://www.iec.org/online/tutorials/vpn/index.html

[4]. http://www.iec.org/online/tutorials/vpn/topic02.html