RESEARCH ARTICLE OPEN ACCESS

An Insight into Virtual Private Networks & IP Tunneling

Karthikeyan R[1], Dr.T.Geetha[2] , Sathya G[3] , Aarthi V[4]
[1,2]Asst.Prof, Dept of MCA, Gnanamani college of Technology, Namakkal, INDIA.
[3,4,5]P.G.Scholar, Dept of MCA, Gnanamani college of Technology, Namakkal, INDIA.

Abstract:

Virtual Private Network used to create an end-to-end tunnel over third-party networks such as the Internet or extranets. It cannot guarantee that the information remains secure while traversing the tunnel. There are many different types of VPN technologies available such as Internet Protocol Security, SSL, MPLS, L2F, PPTP, L2TP and GRE. IPSec has become a much more popular VPN security. A Virtual private network possesses all the features of the private network and is built on existing network, but they suffer severe security problems, particularly authentication problem. AVirtual private network possesses all the features of the private network and is built on existing network, but they suffer severe security problems, particularly authentication problem. This paper introduces a authenticated key agreement protocol based on certificateless cryptography to authenticate users to establish a secure session between them.

I. INTRODUCTION

Virtual. Virtual means not real or in a different state of being. In a VPN, private communication between two or more devices is achieved through a public network the Internet.

Private. Private means to keep something a secret from the general public. Although those two devices are communicating with each other in a public environment.

Network. A network consists of two or more devices that can freely and electronically communicate with each other via cables and wire. A VPN is a network. It can transmit information over long distances effectively and efficiently. 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. commonly called Intranets. These networks were installed using costly leased line services, Frame Relay, and ATM to incorporate remote users. used low-speed switched services.

I. VPNs were 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.

1)

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.
3) Hybrid VPN: A mix of a secure and trusted VPN

4) Provider-provisioned VPN: A VPN that is administered by a service provider.

II. VPN Topology

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 Servic Providers and the Internet as a whole.

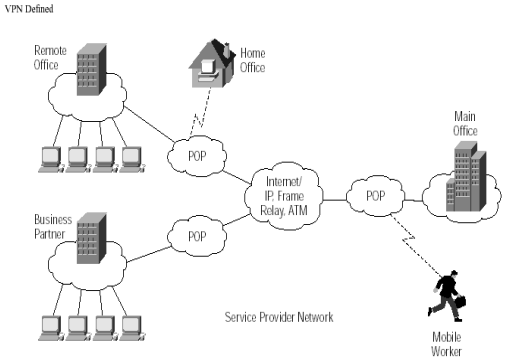


Figure 1. Defined VPN

Note: From A Primer for implementing a Cisco Virtual Private Network

A. Types of VPNs

There are currently three types of VPN in use: remote access VPN, intranet VPN, extranet VPN. Remote access VPNs enables mobile users to establish a connection to an organization server by using the infrastructure provided by an ISP (Internet Services Provider).

Remote access VPN offers advantages such as:

- Reduced capital costs associated with modem and terminal server equipment
- Greater scalability and easy to add new users
- Reduced long-distance telecommunications costs, nationwide toll-free 800 number is no longer needed to connect to the organization's modems

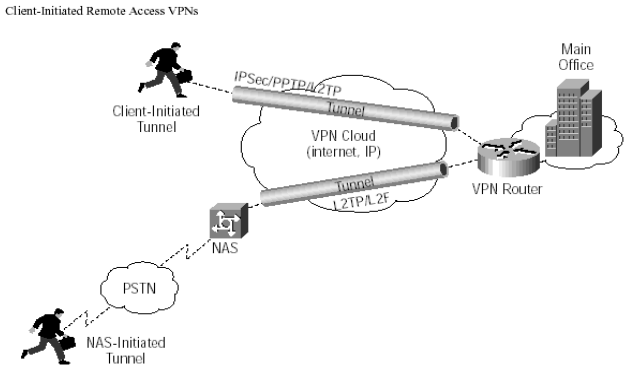


Figure 2. Remote Access VPNs

A Primer for implementing a Cisco Virtual Private Network Intranet VPNs, provides virtual circuits between organization offices over the Internet They are built using the Internet, service provider IP, Frame Relay, or ATM networks. An IP WAN infrastructure uses IPSec or GRE to create secure traffic tunnels across the network. Benefits of an intranet VPN include the following:

- Reduced WAN bandwidth costs, efficient use of WAN bandwidth
- Flexible topologies
- Congestion avoidance with the use of bandwidth management traffic shaping

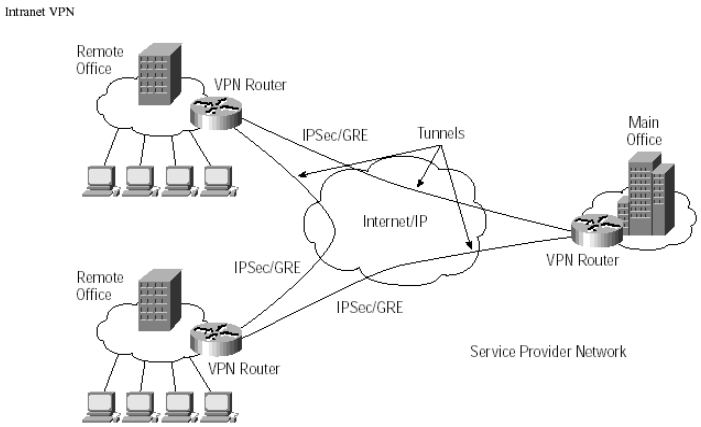


Figure 3. Intranet VPNs

A Primer for implementing a Cisco Virtual Private Network

The concept of setting up extranet VPNs are the same as intranet VPN. The only difference is the users.

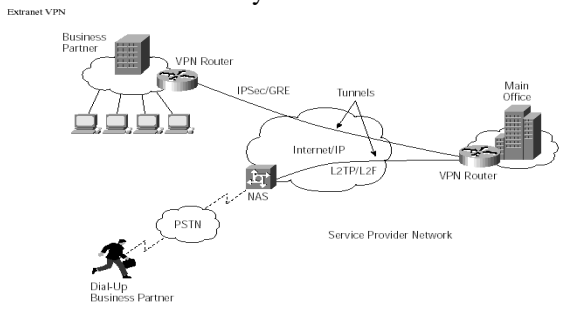


Figure 4. Extranet VPNs

A Primer for implementing a Cisco Virtual Private Network

B. Components of the VPN

1. Security – Companies need to keep their VPNs secure from tampering and unauthorized users. Some examples of technologies that VPN's use are; IP Security (IPSec), Point-to-Point Tunneling Protocol (PPTP),
2. PPTP uses Point-to-Point Protocol (PPP) to provide remote access that can be tunneled through the Internet to a desired site
3. Layer Two Tunneling Protocol (L2TP) exists at the data link layer of the OSI model. L2TP is a combination of the PPTP and Layer two Forwarding (L2F). (Layer two forwarding was also designed for traffic tunneling from mobile users to their corporate server.

IPSec can operate in either transport mode or tunnel mode.

- In tunnel model, intruders can only see where the end points of the tunnel are, but not the destinations of the packet and the sources. IPSec encrypts the whole packet and adds a new IP packet that contains the encrypted packet.
- In Transport mode IPSec leaves the IP packet header unchanged and only encrypts the IP payload to ease the transmission through the Internet.

Multiprotocol Label Switching (MPLS) uses a label swapping forwarding structure. It is a hybrid architecture which attempts to combine the use of network layer routing structures and per-packet switching, and link-layer circuits and per-flow switching.

III. Appliances – intrusion detection firewalls

Firewalls monitors traffic crossing network parameter, and protect enterprises from unauthorized access. The organization should design a network that has a firewall in place on every network connection between the organization and the Internet. Two commonly used types of firewalls are packet-level firewalls and application-level firewalls. Packet-level firewall checks the source and destination address of every packet that is trying to passes through the network.

Application-level firewall acts as a host computer between the organization's network and the Internet. Users who want to access the organization's network must first log in to the application-level firewall and only allow the information they are authorized

IV. Management – managing security policies, access allowances, and traffic management

VPN's need to be flexible to a companies management, some companies chooses to manage all deployment and daily operation of their VPN, while others might choose to outsource it to service providers. In our next section we will discuss how businesses might benefit from a productive VPN and the cost benefits of implementing a VPN.

Productivity and Cost Benefit

In terms of productivity VPN's have come a long way. In the past, concerns over security and manageability overshadowed the benefits of mobility.Larger companies worried, with good cause, about the possibility that providing mobile workers with remote network access would inadvertently provide hackers with a "back door" entry to corporate information resources.

VPN's Benefit a company in the following ways

- 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.

- 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.

There are a few ways to approach this topic;

1. In House Implementation- companies decide that for their needs an in-house solution is all they need.
2. Outsourced Implementation- companies can choose to outsource if they are large scaled or lack the IT staff to fully implement an in house VPN.
3. Middle Ground Implementation- Some companies would rather have a service provider install the VPN but have their IT staff monitor the specifics such as tunnel traffic After Implementation the company must make sure that it has adequate support for its end users. That's where quality of service comes in.

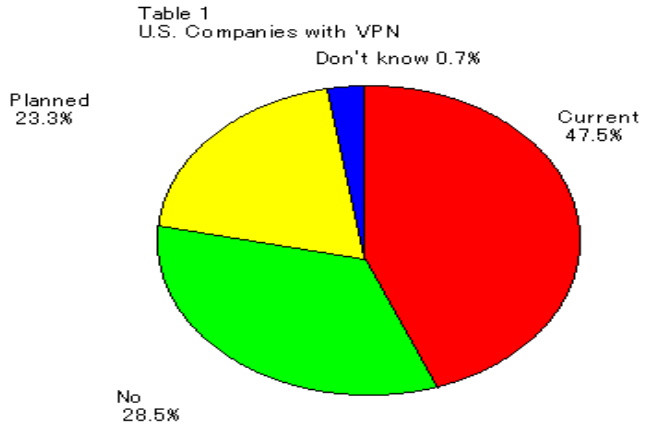
V. Quality of Service (QOS)

QoS (Quality of Service) aims to ensure that your mission critical traffic has acceptable performance. In the real world where bandwidth is limited and diverse applications from videoconferencing to ERP database lookups must all strive for scarce resources.Traffic engineering could even be used to establish LSPs with particular QoS characteristics between particular pairs of sites, if that is desirable. Where an MPLS/BGP VPN spans multiple SPs, the architecture described may be useful. An SP may apply either intserv or diffserv capabilities to a particular VPN, as appropriate.

VI. The 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. 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.

Table 1. Companies with VPN
Source: IDC's 2001 U.S. WAN Manager Survey, IDC #26462, February 2002



The companies for servicing VPN will consider meeting consumer's demands that is voice over IP and other VPN as VOIP VPN. Currently very a few companies have been using this VPN and a few companies will plan to use it in the future. However, contrary to their demands, most produces are standing on difficult situation for improving VOIP VPN because the voice is a kind of special requirement of low latency and jitter.The 21st century invites new ways of viewing the communication networks. Companies that previously managed their own communications requirements are uniting with service providers that can help build up, improve, and manage their networks on a global scale.VPN help service providers build customer loyalties while delivering network services that are valuable to their customers' business operations.

VII. 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 anytime. VPN will also help to make the possibility of a business expanding its services over long distances and globally, more of a reality.

References:

1. Harish Patil, Gowthami Yadav**" Certificateless Key Generation and Agreement Protocol for Virtual Private Networks"** International Journal of Engineering Research & Technology (IJERT).

2. Wassan Saad Hayale"," Elaf Ayyed Jebur" Implementing Virtual Private Network using Ipsec FrameworkInternational Journal of Engineering Research & Technology (IJERT) IJERTIJERT ISSN: 2278-0181 www.ijert.org IJERTV3IS080936 (This work is icensed under a Creative Commons Attribution 4.0 International License.) Vol. 3 Issue 8, August – 2014.

3 R.Karthikeyan," Improved Apriori Algorithm for Mining Rules" in the International Journal of Advanced Research in biology Engineering science and Technology Volume 11, Issue 4, April 2016, Page No:71-77.

4 R.Karthikeyan,Dr.T.Geetha "Honeypots for Network Security", International journal for Research & Development in Technology.Volume 7.Issue 2 ,Jan 2017,Page No.:62-66 ISSN:2349-3585.

5 R.Karthikeyan,"A Survey on Position Based Routing in Mobile Adhoc Networks" in the international journal of P2P Network Trends and Technology, Volume 3 Issue 7 2013, ISSN:2249-2615, Page No.:81-88

6 R.Karthikeyan,"A Survey on Sensor Networks" in the International Journal for Research & Development in Technology Volume 7, Issue 1, Jan 2017, Page No:71-77

7 R.Karthikeyan,Dr.T.Geetha "Web Based Honeypots Network",in the International journal for Research & Development in Technology.Volume 7.Issue 2 ,Jan 2017,Page No.:67-73 ISSN:2349-3585.

8 R.Karthikeyan,Dr.T.Geetha,"A Simple Transmit Diversity Technique for Wireless Communication",in the International journal for Engineering and Techniques. Volume 3. Issue 1, Feb 2017, Page No.:56-61 ISSN:2395-1303.

9 R.Karthikeyan,Dr.T.Geetha "Strategy of Trible – E on Solving Trojan Defense in Cyber Crime Cases", International journal for Research & Development in Technology.Volume 7.Issue 1 ,Jan 2017,Page No.:167-171.

10 .Karthikeyan,Dr.T.Geetha"Advanced Honey Pot Architecture for Network Threats Quantification" in the international journal of Engineering and Techniques, Volume 3 Issue 2, March 2017, ISSN:2395-1303, PP No.:92-96.

11 R.Karthikeyan,Dr.T.Geetha"Estimating Driving Behavior by a smart phone" in the international journal of Engineering and Techniques, Volume 3 Issue 2, March 2017, ISSN:2395-1303,PP No.:84-91.

12 R.Karthikeyan,Dr.T.Geetha" SAMI: Service- Based Arbitrated Multi-Tier Infrastructure for Cloud Computing" in the international journal for Research & Development in Technology, Volume 7 Issue 2, Jan 2017,ISSN(0):2349-3585, Pg.no:98-102

13 R.Karthikeyan,Dr.T.Geetha "FLIP-OFDM for Optical Wireless Communications" in the international journal of Engineering and Techniques, Volume 3 Issue 1, Jan - Feb 2017, ISSN:2395-1303,PP No.:115-120.

14 R.Karthikeyan,Dr.T.Geetha "Application Optimization in Mobile Cloud Computing" in the international journal of Engineering and Techniques, Volume 3 Issue 1, Jan - Feb 2017, ISSN:2395-1303,PP No.:121-125.

15 R.Karthikeyan,Dr.T.Geetha"The Sybil Attack" in the international journal of Engineering and Techniques, Volume 3 Issue 3, May - Jun 2017, ISSN:2395-1303,PP No.:121-125.

16 R.Karthikeyan,Dr.T.Geetha"Securing WMN Using Hybrid Honeypot System" in the international journal of Engineering and Techniques, Volume 3 Issue 3, May - Jun 2017, ISSN:2395-1303,PP No.:121-125.

17 R.Karthikeyan,Dr.T.Geetha "Automated Predictive big data analytics using Ontology based Semantics" in the international journal of Engineering and Techniques, Volume 3 Issue 3, May – Jun 2017, ISSN:2395-1303,PP No.:77-81.

18 R.Karthikeyan,Dr.T.Geetha"A Survey of logical Models for OLAP databases" in the international journal of Engineering and Techniques, Volume 3 Issue 3, May - Jun 2017, ISSN:2395-1303,PP No.:171-181

19 R.Karthikeyan,Dr.T.Geetha"A Client Solution for Mitigating Cross Site Scripting Attacks" in the international journal of Engineering Science & Computing, Volume7,Issue6, June 2017, ISSN(0):2361-3361,PP No.:13063-13067.

20 R.Karthikeyan,Dr.T.Geetha"A Condensation Based Approach to Privacy Preserving Data Mining" in the international journal of Engineering Science & Computing, Volume7,Issue6, June 2017, ISSN(0):2361-3361,PP No.:13185-13189.

21 R.Karthikeyan,Dr.T.Geetha"Biometric for Mobile Security" in the international journal of Engineering Science & Computing, Volume7,Issue6, June 2017, ISSN(0):2361-3361,PP No.:13552-13555.

22 R.Karthikeyan,Dr.T.Geetha"Data Mining on Parallel Database Systems" in the international journal of Engineering Science & Computing, Volume7,Issue7, July 2017, ISSN(0):2361-3361,PP No.:13922-13927.

23 R.Karthikeyan,Dr.T.Geetha"Ant Colony System for Graph Coloring Problem" in the international journal of Engineering Science & Computing, Volume7,Issue7, July 2017, ISSN(0):2361-3361,PP No.:14120-14125.

24 R.Karthikeyan,Dr.T.Geetha"Classification of Peer – To- Peer Architectures and Applications" in the international journal of Engineering Science & Computing, Volume7,Issue8, Aug 2017, ISSN(0):2361-3361,PP No.:14394-14397.

25 R.Karthikeyan,Dr.T.Geetha"Mobile Banking Services" in the international journal of Engineering Science & Computing, Volume7,Issue7, July 2017, ISSN(0):2361-3361,PP No.:14357-14361.

26 R.Karthikeyan,Dr.T.Geetha "Neural Networks for Shortest Path Computation and Routing in Computer Networks" in the international journal of Engineering and Techniques, Volume 3 Issue 4, Aug 2017, ISSN:2395-1303,PP No.:86-91.