ijecs open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 2 February , 2014 Page No. 3837-3841

Network Security: Virtual Private Network

Sonika, Monika, Sonal
Computer science and Engineering
(Network Security)
India

Abstract: This paper presents basic about Virtual Private Network (VPN). In this paper, we can basically focus on its Types, Architecture, Functionality and Protocols. A ”VIRTUAL PRIVATE NETWORK” is an authenticated and encrypted communication channel across some form of public network, such as internet. The concept of “VIRTUAL PRIVATE NETWORK” is utilized by almost 60% of firms, companies and organizations to communicate each other.

Keywords-VPN, PPTP, L2TP, IPSec, RAS etc.

I. Introduction

A VPN, Virtual Private Network, is defined as network that uses public network paths but maintains the security and protection of private network. In a VPN network we can effectively and efficiently transmit information over long distances. In the past, VPN has been associated with Public Switched Telephone Network (PSTN) but VPN networks have finally linked with IP-based data networking. Before IP based networking corporations had expended considerable amount of time and resources on costly frame relay, ATM which was very costly to set up complex private network called Intranets. Now VPN overcome the security factor using tunneling protocols and complex encryption procedures, data integrity and privacy is achieved, and the new connection produces which seems to be a dedicated point-to-point connection.

II. Types of VPNs

There are currently three types of VPN are:

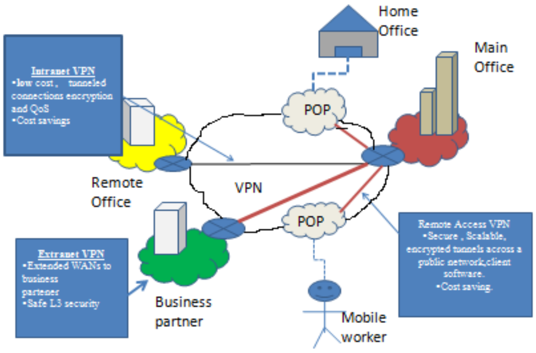
Home Office
Main Office
Intranet VPN
•low cost , tunneled connections encryption and QoS
•Cost savings
POP
Remote Office
VPN
POP
Extranet VPN
•Extended WANs to business partener
•Safe L3 security
Business partner
Mobile worker
Remote Access VPN
•Secure , Scalable, encrypted tunnels across a public network,client software.
•Cost saving.

Fig1. Types of VPN

1. Remote Access (RAS) VPNs

Remote access VPNs establish a connection between mobile users and an organization server by using the infrastructure provided by an ISP (Internet Service Provider).If the users are physically located in organization have access to all the resources on the organisation's network .The user connects to a local ISP that supports VPN using plain old telephone services POTS), integrated services digital networks (ISDN), digital subscriber line (DSL), etc. 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 numbers is no longer needed to connect to the organization's modems.

2. Intranet VPNs

Intranet VPNs using the Internet, service provider IP, Frame Relay or ATM networks provides virtual circuits between organization offices over the Internet. By using IPSec an IP WAN infrastructure create secure traffic tunnels across the network. Intranet VPN offers following benefits:

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

3. Extranet VPNs

Extranet VPNs use the same concept as Intranet VPNs. But the users are different in this network. Extranet VPNs are built for users such as customers, suppliers or different organizations over the internet.

III. Architecture

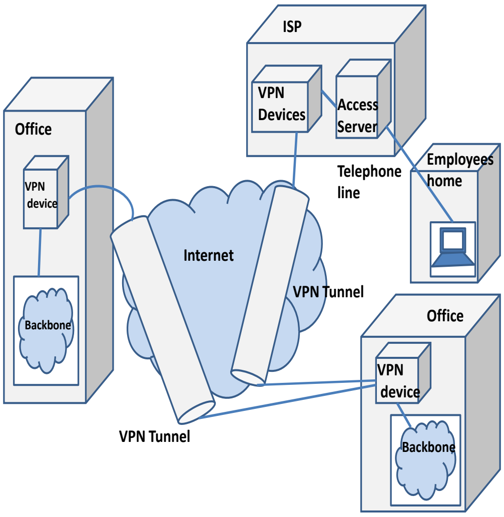

Fig 2: Architecture of VPN

To secure our data from unauthorized parties, VPNs architecture essentially enhance the native internet infrastructure with broadband connection and secured data platforms on the value-added networks.VPN based on public Internet infrastructure so their physical connectivity is less expensive and it provide high speed transmission with security. They essential combine the best characteristics of WANs, leased lines and the Internet into an affordable, robust and secure wide area infrastructure for data transfer between enterprises.

IV. Tunneling

The process of using an internetwork infrastructure to transfer data for one network over another network is called Tunneling. Instead of sending frame as it is produced by an originating node, the tunneling protocol encapsulates the frame in an additional header. To traverse the intermediate internetwork this additional header is required for providing the routing information to the encapsulated payload. Over the internetwork the encapsulated packets are routed between endpoints. The encapsulated packets travel through the internetwork using logical path is called a “tunnel”. The encapsulated packets are decapsulated when they reach the destination to get the original data. Tunneling includes this entire process encapsulation, transmission and decapsulation of packets. The most widely known real world example is the public internetworks “the Internet”.

V. Function of VPN

1. Authantication:

The VPN server can be configured to use either Windows or Remote Authentication Dial-In User Service (RADIUS) 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 attempted is authorized using the VPN client’s user account properties and local remote access policies.

2. Encryption:

To ensure confidentiality of the data it traverses the shared or public transit network, it is encrypted by the sender and decrypted by the receiver. The stronger the encryption algorithm, the greater the delay the encryption and decryption process introduce. The type of key is also affects performance. Secret key encryption, such as 3DES, is popular with VPNs because it is fast.

3. Data Intigrity:

To protects our data from interception and modification we can use Data Intigrity. When our data is transmit then integrity ensures that our data has not been altered or changed. We use a hash mechanism to accomplish the integrity of data .Common hashing algorithms are: SHA family of algorithms, the MD family of algorithms, of Haval and Tiger.

4. Confidentiality:

Data Confidentiality is whether the information stored on a system is protected against unauthorized access. It is an integral component of security. In this it measure the ability of the system to protect its data because systems are sometimes used to manage sensitive information. Confidentiality means only authorized people can view the data.

5. Access Control:

In access control there is access control list (ACL) which contain a list of permissions attached to an object with respect to a computer file system. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects. A subject and an operation of each entry can be specifies by typical ACL

VI. VPN Protocols

The Three most popular VPN protocols are:

1. PPTP (Point-To-Point Tunneling Protocol):

To provide remote access PPTP uses Point-to-Point Protocol (PPP) that can be tunneled through the Internet to adesired site. Tunneling allows senders to encapsulate their data in IP packets that hide the routing and switching infrastructure of the Internet from both senders and receivers to ensure data security against unauthorized users. Internet packet exchange (IPX) and network basic input/output system extended user interface(NetBEUI) can also handle by PPTP. It is designed to run on the Network layer of the Open systems interconnection (OSI).

2. L2TP (Layer 2 Tunneling Protocol):

Layer Two Tunneling Protocol (L2TP) is a combination of PPTP and Layer 2 Forwarding(L2F), a technology developed by Cisco Systems, Inc. Over the Internet or over private intranets L2TP can be used as a tunneling protocol. It encapsulates ppp frames to be sent over IP, X.25, Frame relay, or ATM networks. For both tunnel maintenance and tunneled data over IP networks L2DP uses UDP messages. It exists at the data link layer of the OSI model.

3. IPSEC (Internet Protocol Security):

For encrypting data IPSec uses data encryption standard (DES) and other algorithms, public-key cryptography to guarantee the identities of the two parties to avoid man-in-the-middle attack, and digital certificates for validating public keys. IPSec is focused on Web applications, but it can be used with a variety of application-layer procotols. It can operate in either transport mode or tunnel mode.

VII. Conclusion

In today’s time a large amount of data is travelling across different networks because a no. of peoples, companies, institutions and many other firms tends to communicate with each other and exchange data and other information. The information travelling on the network might be confidential and the people want it not to be reached to unauthorized persons. Such information should be sent on a public network with a higher degree of security and this security can be provided by the use of ”VIRTUAL PRIVATE NETWORK”.VPN will also help to make the possibility of a business expanding its services over long distances and globally, more of a reality.

Refrences

[1] Chris Brenton and Camerron Hunt ,”Mastering Network security”, Second Edition, BPB Publications

[2] A primer for Implementing, a Cisco Virtual Private Network.(1999).Cisco System. Retrieved October 5,2002, form

http://www.cisco.com/warp/public/cc/so/neso/vpn/vpne/vpn21rg.htm

[3]Using Point-to-Point Tunneling Procotol, (2001 july), Microsoft Retrieved September 20,2002,from http://www.microsoft.com/ntserver/techresources/commnet/PPTP/pptpwp.asp

[4] Perlmutter, B. and Zarkover, J.,"Virtual Private Networking: A View from the Trenches" ,Prentice Hall PTR,2000.