ENABLING VIRTUAL PRIVATE NETWORK FOR E-MAIL COMMUNICATION

Mughele, Ese Sophia School of Science and Technology, Computer Science Option. Delta State School of Marine Technology Burutu. Nigeria

Abstract
There is an increasing demand nowadays to connect to internal networks from distant locations. Employees often need to connect to internal private networks over the Internet (which is by nature insecure) from home, hotels, airports or from other external networks. Security becomes a major consideration when staff or business partners have constant access to internal networks from insecure external locations.VPN (Virtual Private Network) technology provides a way of protecting information being transmitted over the Internet, by allowing users to establish a virtual private "tunnel" to securely enter an internal network, accessing resources, data and communications via an insecure network such as the Internet.

Keywords: Virtual private Network, Email, Network, communication.

1. Introduction

Electronic Mail is one of the most used tools when it comes to business and Personal communication in the world today. Notes, Messages and even Pictures can be sent quickly from source to destination using E-Mail. The senders of these messages often assume that the contents are private and are kept sealed from the source to the destination. This is not always the case! With the proper techniques, malicious hackers and spammers can read and send unauthorized E-Mail information that senders and receivers assume is private. This could range from reading/modifying a message being sent between E-Mail servers to sending unauthorized Spam messages to individuals throughout the world. The heavy reliance on E-Mail makes the proper security precautions essential to providing secure and reliable E-Mail solutions in organizations today (Beck, 2008*)*.

Organizations whose facilities are split between two or more locations can connect the locations into a single logical network through the use of routers and wide area networking (WAN) technologies. (Tschabitscher,2007).When a circuit-switched network like telephone network, is used, permanent or switched circuit services are employed to emulate the physical attachment of the two sites for router-to-router packet exchange obviously it is private.

Krasnyansky, (2001) observe that, when a packet network, such as the Internet, is used as WAN for connecting the sites, the private nature of router-to-router communications is threatened, since the network provides no guarantee regarding packet delivery. Routers intending to talk to one another over logical Internet circuits will find that packets can be injected into or ejected out of the circuits indiscriminately. To keep such circuits private, the packets flowing on the circuit must be encrypted so that injected packets will be no use of unintended recipients. These private links between routers are called tunnels. VPNs are so important to organizations supporting telecommuters, branch offices, and off-site partners, that VPNs are becoming a critical part of corporate Information Technology strategy.

1.1 Research Motivation

Electronic Mail is quite arguably the most important application for personal and business communication across the Internet. People depend on it for sending text, image and even sound files quickly to their destinations. E-Mail was designed to be both easy to use and quick for fast end to end message delivery. These factors of E-Mail do not have many built in security measures by default. Barebones E-Mail services do not provide non-repudiation between the sender and receiver. They also fail at providing encryption to protect the clear text nature of E-Mail as it traverses the Internet (Slavic, 2004). E-Mail has become convenient technology that most people rely on for communication today; the adverse implication is enormous, therefore proper measures should be put in place to guarantee security.

Related Literatures

2. What Is Virtual Private Network (Vpn)?

A Virtual Private Network, also known as VPN, is a computer network designed to make networks more

secured. It is most often used by organizations to provide remote access to organization's computers, yet it maintaining a high level of security. (John, 2001).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. Therefore, the communication is virtually but not physically there.(Sweeney, 2000). Private means to keep something a secret from the general public. Although those two devices are communicating with each other in a public environment, there is no third party who can interrupt this communication or receive any data that is exchanged between them. (Sweeney, 2000).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 that can transmit information over long distances effectively and efficiently. (Sweeney, 2000).

Fifteen years ago, virtual private network (VPN) access was a fairly new concept to most businesses. While large corporations already had a good head-start with VPN technologies, the rest were starting to realize the potential and possibilities VPN connections provided them. Vendors such as Cisco, Checkpoint and Microsoft began producing a variety of products that provided VPN services to the business. Today, VPN is considered a standard feature in any serious security- and router-related product and is widely implemented throughout most companies. (Salamone and Salvatore. 1998)

Connolly, (2002) explain that 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 integrated services digital network.

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 tunneling 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. This is 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.

2.1 Types of VPN

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 allows users to connect to their corporate intranets or extranets wherever or whenever is needed. Users have access to all the resources on the organization's network as if they are physically located in organization. The user connects to a local ISP that supports VPN using plain old telephone services (POTS), integrated services digital network (ISDN), digital subscriber line (DSL), etc. The VPN device at the ISP accepts the user's login, then establishes the tunnel to the VPN device at the organization's office and finally begins forwarding packets over the Internet.

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. Extranet VPNs are the same as intranet VPN. The only difference is the users. Extranet VPN are built for users such as customers, suppliers, or different organizations over the Internet (Ferguson & Huston1998).

VPNs were broken into some categories- 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, 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, 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, Provider-provisioned VPN: A VPN that is administered by a service provider.(Remote Access VPN Solutions.(2001, June).

2.2 Properties of VPN

VPN connections have the following properties: Encapsulation, Authentication, Data encryption. Encapsulation-with VPN technology, private data is encapsulated with a header that contains routing information that allows the data to traverse the transit network. Authentication- User-level authentication by using point to point protocol authentication establish the VPN connection, the VPN server authenticates the VPN client that is attempting the connection by using a Point-to-Point Protocol (PPP) user-level authentication method and verifies that the VPN client has the appropriate authorization. If mutual authentication is used, the VPN client also authenticates the VPN server, which provides protection against computers that are masquerading as VPN servers Computer-level authentication by using Internet Key Exchange (IKE). To establish an Internet Protocol security (IPsec) security association, the VPN client and the VPN server use the IKE protocol to exchange either computer certificates or a pre-shared key. In either case, the VPN client and server authenticate each other at the computer level. Computer certificate authentication is highly recommended because it is a much stronger authentication method. Computer-level authentication is only performed for L2TP/IPsec connections.

Data encryption- To ensure confidentiality of the data as it traverses the shared or public transit network, the data is encrypted by the sender and decrypted by the receiver. The encryption and decryption processes depend on both the sender and the receiver using a common encryption key. Intercepted packets sent along the VPN connection in the transit network are unintelligible to anyone who does not have the common encryption key. The length of the encryption key is an important security parameter. You can use computational techniques to determine the encryption key. However, such techniques require more computing power and computational time as the encryption keys get larger. Therefore, it is important to use the largest possible key size to ensure data confidentiality.

3. The concept of Email

Electronic mail, the short form is e-mail or email is text messages that may contain files, images, or other attachments sent through a network to a specified individual or group of individuals. It can also be referred to as messages distributed by electronic means from one computer user to one or more recipients via a network. (webopedia.com, 2010). Mankind has always had a compelling desire to communicate. In ancient times this could be verbally or in some form of writing. If remote communication was required (i.e. if the parties were not physically together) then messages had to be physically carried or sent by a messenger. Examples of early forms of remote transmission of messages not requiring a person to actually move between the sender and the receiver would be in 'jungle drum' or 'smoke signal' transmissions. These were somewhat lacking in security and privacy.

This definition would also include the telex network that was used extensively by business on a world-wide basis from the mid-1920's to the mid-1980. The telex network was independent of the telephone network and telex machines could connect with and communicate with any other telex machine on a global scale. Telex also was relatively secure in that the sending and receiving machines did identifying handshaking. It was relatively expensive to have a 'telex line' installed and subsequent telex messages were charged on a data transmitted basis. During the 1960's and 1970's many companies who were using mainframe and mini computers also used email facilities on those systems. This enabled users of terminals attached to those systems to send messages to each other. As companies began to connect their central systems (hosts) to branch offices and subsidiaries then employees were able to send email to other employees of that company on a world-wide basis. As the Internet became available to more people, both privately and through company connections, the email facilities available to users have evolved from the proprietary email systems available within company networks and via host-based systems through to the current trend of "Intranets" which are effectively private mini-Internets, using the standards-based Internet services, such as mail & web servers in place of proprietary ones.

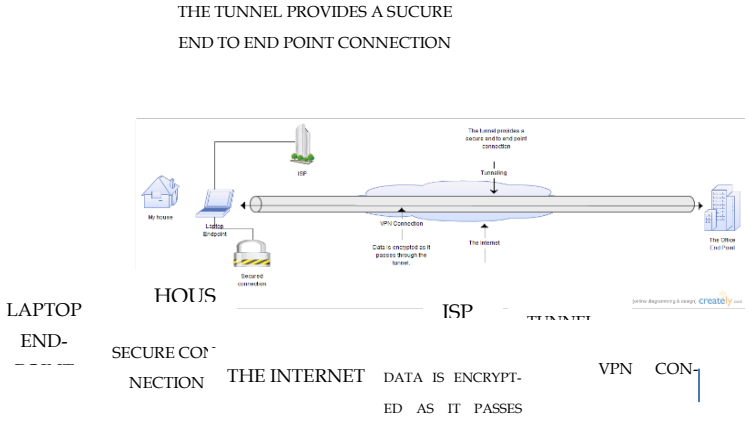
Since 1995 both the Internet and email have been 'hot' topics, but when one cuts away the hype, one realizes that email itself is not new. What is relatively new however is that email is now more readily available, interoperable between systems, available world-wide, inexpensive, much easier to use and fashionable.

No doubt the Internet will shape future communications, far beyond the current uses. As to what features and functions that will become available over the next few years, the speed of progress dictates that we can only guess. (First Email System (1954 – 1978).

4. Design of VPN

The system design phase is one in which the actual methods of designing system are considered. In view of this, this chapter stresses out the methods in which data is being collected. The steps in enabling virtual private network (VPN) for email communication, and this will be achieve by providing a solution that will secure the process of communication through the email over the internet by developing some highly efficient method for which information can have a secure means from the sender to the recipient. The source of data to be used for this work will come from the internet, libraries and public journals.

Fig 1. Diagrammatic Representation of VPN over the Internet.



Extracted from a Primer for implementing a Cisco Virtual Private Network© 1999 Cisco systems, Inc All rights Reserved

VPN has gone from obscuring to being a common method of linking private network together across the internet. VPN has become popular because they free users from the expense of connecting networks with dedicated leased lines, and also have help in sending email over the internet securely. This is part of the reason why VPN have become so accepted and tend to be very reliably.

Steps to Connect a Remote System to Virtual Private Network

Below is the step by step procedure in connecting a system to VPN;

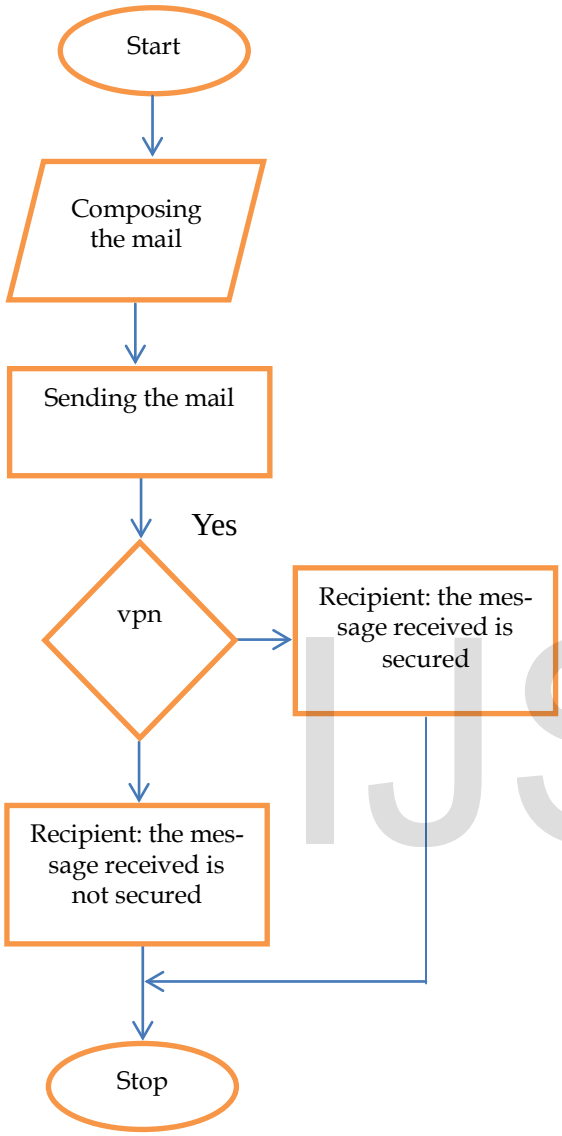
1. Click on the "Start" button and select "Control Panel". Choose "Network and Internet Connections" and then "Network Connections".
2. Find "Create a new connection" under the "Network Tasks" heading. Click it and then click "Next". Click "Next" again on the screen titled "Welcome to the New Connection Wizard".
3. Look at the window titled "Network Connection Type" and click on the radio button next to "Connect to the network at my workplace". Click "Next". Choose "Virtual Private Network connection" on the next page and click "Next".
4. Type a name for your new connection in the text box on the "Connection Name" page and click "Next". If you are using a dial-up Internet connection, you will see the "Public Network" page next. Select the radio button for "Automatically dial this initial connection" and click "Next".
5. Fill in your DNS server name or IP address for the VPN server to which you want to connect in the text box marked "Host name or IP address". Click "Next" and then click "Finish".
6. Enter the user name and passw r of the VPN provided for you. Pu the box to save the information if you want to save it for future use. Click "Connect" to connect to the VPN.

5. Flow chart design

Below is the flow chart which is a diagrammatic representation of a solution to a problem. This flow chart describe how mail is being compose and send over the internet when virtual private network is active and

when is not active.

Fig.2. A flowchart illustrating solution



6. Discussion

In the process of sending a mail over the internet, there is a need for the sender to compose the mail on his/her computer. After that the person need to send it over the internet to the recipient. But there is no guarantee that the mail sent over the internet is always secure because there are malicious hacker over the internet ready to hack into a mail and send other message to the recipient. So because of these, a secure internet is needed. Implementing a virtual private network will enable email sent on the internet to be secure.

6.1. Summary

More and more people rely on E-Mail for simple and easy communication every day. In order to take advantage of its strengths, E-Mail processes need to be reviewed and updated as newer protocols and technologies are developed. Thus VPN is an outgrowth of the Internet technology, which will transform the daily method of doing business faster than any other technology. A Virtual Private Network, or VPN, typically uses the Internet as the transport backbone to establish secure links with business partners, extend communications to regional and isolated offices, and significantly decrease the cost of communications for an increasingly mobile workforce. VPNs serve as private network overlays on public IP network infrastructures such as the Internet.

6.2 Conclusion

Overall, this study stresses on the importance of enabling virtual private network so as to increase effective security in the process of communicating through the email. Thus, it is believed that this implementation will reduce problem encounter through the process of sending email over the internet.

REFERENCE

A primer for Implementing a Cisco Virtual Private Network. (1999), Cisco Systems. Retrieved October 5, 2014, from http://www.cisco.com/warp/public/cc/so/neso/vpn/vpne/vpn21_rg.htm

A Technology Guide from ADTRAN.(2001, September).Understanding Virtual Private Networking.ADTRAN. Retrieved October 25, 2014, from http://www.adtran.com/all/Doc/0/DTCGA3HEJ3B139RK038BE81ID8/EN286.pdf

Connolly, P.J., (2002, January 21). Taming the VPN.*Computerworld*. Retrieved September 18, 2014, from http://www.computerworld.com/networkingtopics/networking/story/0,10801,67396,00.html

Dix, John. (2001, April 9). Is an integrated VPN in your future? *Network World*. Retrieved October 1, 2014, from http://www.itworld.com/Net/2553/NWW010409edit/

Ferguson & Huston.(1998, April). What is a VPN? Retrieved September 19, 2013, from http://www.employees.org/~ferguson/vpn.pdf

Internetworking Technologies Handbook, Virtual Private Networks. Cisco Systems. Retrieved September 22, 2013, from http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/

Introduction to VPN: VPNs utilize special-purpose network protocols. *Computer Networking.*Retrieved September 14, 2013, from http://www.compnetworking.about.com/library/weekly/aa010701d.htm

Next-Generation Networking: The Future of Greater Performance and Flexibility. (2002, July). IDC Analyze the Future. Retrieved September 28, 2013, from http://www.business.att.com/content/whitepaper/next_generation.pdf

Remote Access VPN Solutions.(2001, June). Check Point Software Technologies Ltd. Retrieved September 20, 2013, from http://www.checkpoint.com/products/downloads/vpn-1_remote_access.pdf

Salamone, Salvatore. (1998), VPNImplementation Calls For A Tunnel Trip.*Internet Week.* Retrieved October 30, 2013, from http://www.internetwk.com/VPN/paper-5.htm

Sandick, H., Nair, R., Rajagopalan, B., Crawley, E., (1998, August).A Framework for QoS-based Routing in the Internet. Retrieved October 1, 2002, from ftp://ftp.isi.edu/in-notes/rfc2386.txt

http://www.webopedia.com/TERM/E/e_mail.html

History of Components Necessary for the Invention of the First Email System (1954 - 1978)

HISTORY OF THE INVENTION OF THE FIRST EMAIL SYSTEM (1978 - 2011)