International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 2, No. 2, June-August, 2017 | Pages 30-35

Design and Implementation of a Secure Network

R. Ganeshan[1], Dr. Paul Rodrigues[2]

[1]Assistant Professor, Dept of CSE, St. Joseph College of Engineering Sriperumbudur. India
[2]Professor, Dept of CSE, Indra Gandhi College of Engineering and Technology Chengalpattu. India

Abstract:

Security has been a pivotal issue in the design and deployment of an enterprise network. With the innovation and diffusion of new technology such as Universal computing, Enterprise mobility, E-commerce and Cloud computing, the network security has still remained as an ever increasing challenge. A Campus network is an important part of campus life and network security is essential for a campus. Campus network faces challenges to address core issues of security which are governed by network architecture. Secured network protects an institution from security attacks associated with network. A university network has a number of uses, such as teaching, learning, research, management, e-library, result publishing and connection with the external users. Network security will prevent the university network from different types of threats and attacks. The theoretical contribution of this study is a reference model architecture of the university campus network that can be followed or adapted to build a robust yet flexible network that responds to the next generation requirements. A hierarchical architecture of the campus network is configured with different types of security issues for ensuring the quality of service. In this project, a tested and secure network design is proposed based on the practical requirements and this proposed network infrastructure is realizable with adaptable infrastructure.

Keywords: Campus Network, Security, WAN, Security Threats, Network Attacks, VPN, VLAN, Firewall.

1. INTRODUCTION

As the computers and networked systems thrive in today's world, the need for increase and strong computer and network security becomes increasingly necessary and important. The increase in the computer network system has exposed many networks to various kinds of internet threats and with this exposure. The security may include identification, authentication and authorization, and surveillance camera to protect integrity, availability, accountability, and authenticity of computer hardware or network equipment. There is no laid-down procedure for designing a secure network. Network security has to be designed to fit the needs of an organization Campus network is essential and it plays an important role for any organization. Network architecture and its security are as important as air, water, food, and shelter. Computer

network security threat and network architecture are always serious issues. A campus network is an autonomous network under the control of a university which is within a local geographical place and sometimes it may be a metropolitan area network in the course of maintaining elevated availability, excellent performance, perfect infrastructure, and security. Securing a big network has been always an issue to an IT manager. There are a lot of similarities between securing an outsized network and university network but each one has its own issues and challenges. Present educational institutions pay more attention to IT to improve their students' learning experience. Architects of campus can achieve this if IT managers hold on to the fundamental principles addressed in this reference architecture, namely LAN or WAN connectivity design considerations, security, and centralized management [3]. The network infrastructure design has become a critical part for some IT organizations in recent years. An important network design consideration for today's networks is creating the potential to support future expansion in a reliable, scalable and secure manner. This requires the designer to define the client's unique situation, particularly the current technology, application, and data architecture.

Here, different research papers have been consulted for security in campus network. Lalita Kumari et al introduced various current network information security problems and their solutions. They represented the current security status of the campus network, analyzed security threat to campus network and described the strategies to maintenance of network security [3]. The hierarchical network design is considered in the proposed system and correspondent network will be scalable; performance and security will be increased; and the network will be easy to maintain. A hierarchical architecture of campus network is configured with different types of traffic loads and security issues for ensuring the quality of service.

2. RELATED WORK

There are various types of network such as Personal Area Network (PAN), Local Area Network (LAN), Metropolitan Area Network (MAN), Campus Area Network (CAN), Storage Area Network (SAN) and Wide Area Network (WAN). A Personal Area Network (PAN) is a computer network organized around an individual person. Personal Area Networks typically involve a mobile computer, a cell phone and/or a handheld computing device such as a PDA. A Local Area Network (LAN) is a group of computers and associated devices that share a common communications line or wireless link. Typically, connected devices share the resources of a single processor or server within a small geographic area. A Metropolitan Area Network (MAN) is a network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large Local Area Network (LAN) but smaller than the area covered by a Wide Area Network (WAN). A Campus Area Network (CAN) is a proprietary Local Area Network (LAN) or set of interconnected LANs serving a corporation, government agency, university, or similar organization.

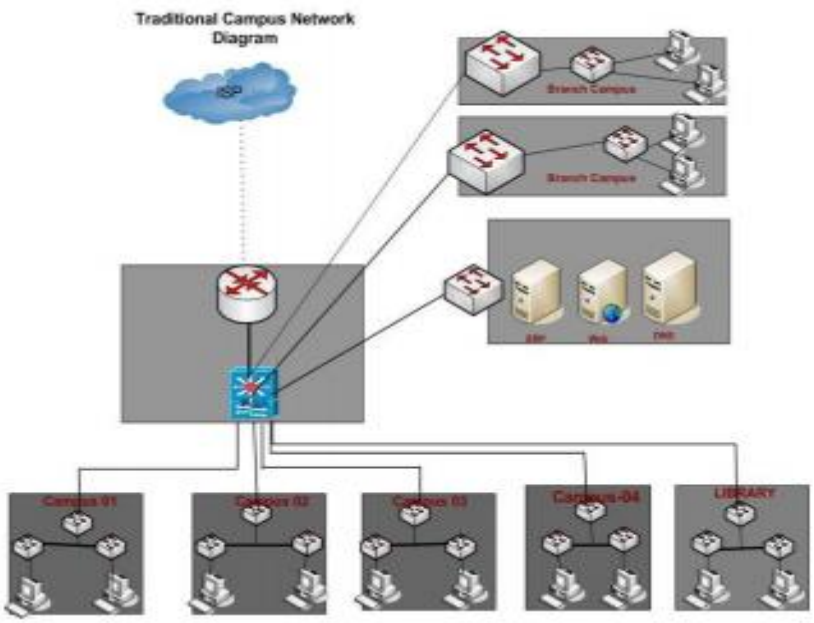

Fig.1.Campus Network

A Storage Area Network (SAN) is a high-speed network of storage devices that also connects those storage devices with servers. It provides block- level storage that can be accessed by the applications running on any networked servers. A Wide Area Network (WAN) is a geographically dispersed telecommunications network. The term distinguishes a broader telecommunication structure from a Local Area Network (LAN). Extensive research or project has been done in the position of network architecture and security issues in campus networks.

3. PROPOSED SYSTEM

A Virtual Private Network (VPN) extends a private network across a public network, such as the Internet. It enables a computer or network-enabled device to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the public network. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption. Major implementations of VPN include Open VPN and IPsec. Campus VPN - provides a full tunnel VPN service that is a secure (encrypted) connection to the network from off campus. Common uses of the Campus VPN include access to file sharing/shared drives and certain applications that require a Campus IP address. The Campus VPN has a 20-hour session limit. When designing complex systems, such as a network, a common engineering approach is to use the concepts of modules and modularity. In this approach, the design of the system evolves by breaking the big task into smaller tasks. Each module is responsible for a specific task and provides services to the other modules to accomplish their tasks. We can interact with a module as a black box that provides certain functionality without knowing the details of how it works.

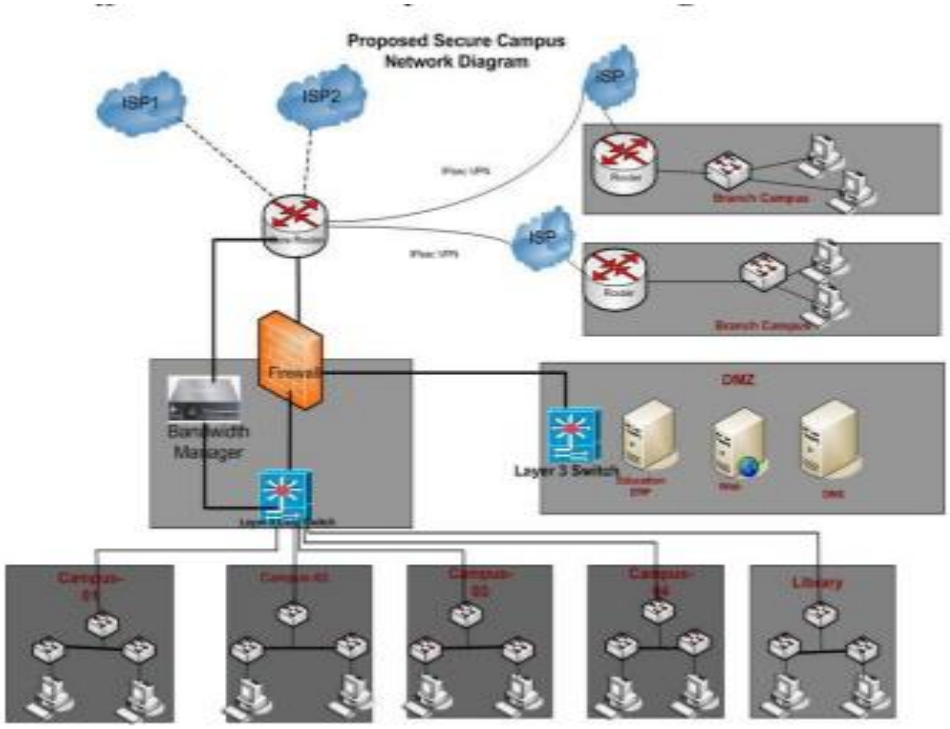

Fig.2.Secure Network Design

We only need to know how to interface with the module. Someone can remove the module and update it with a newer one, and we would still be able to continue our work in the same way. Moreover, modularity is important to simplify tasks (divide and conquer). For instance, in a network, reliability of message delivery and routing of messages can be treated separately by different modules. Changing one would not impact the other. If a better routing procedure is employed, it only affects the module responsible for it. Certainly, we do not desire a change in routing to affect our ability to reliably deliver messages. Modules often interact in a hierarchy. A network is designed as a hierarchical or layered architecture in which every module or layer provides services to the upper layer. Users, sitting at the top layer of the network, communicate as if there is a virtual link between them, and need not be aware of the details of the network.

4. ANALYSIS

Networks are usually classified using three properties: Topology, Protocol, and Architecture. Topology specifies the geometric arrangement of the network. Common topologies are a bus, ring, and star. A bus topology means that each computer on the network is attached to a common central cable, called a bus or backbone. This is a rather simple network to set up. Ethernets use this topology. A ring topology means that each computer is connected to two others, and they arranged in a ring shape.

Fig.3.Secure Connectivity

These are difficult to set up, but offer high bandwidth. A star topology means all computers on the network are connected to a central hub. These are easy to set up, but bottlenecks can occur because all data must pass through the hub. Architecture refers to one of the two major types of network architecture: Peer-to-peer or client/server. In a Peer-to-Peer networking configuration, there is no server, and computers simply connect with each other in a workgroup to share files, printers, and Internet access. This is most commonly found in home configurations, and is only practical for workgroups of a dozen or less computers. In a client/server network, there is usually an NT Domain Controller, which all of the computers log on to. This server can provide various services, including centrally routed Internet Access, mail (including e-mail), file sharing, and printer access, as well as ensuring security across the network. This is most commonly found in corporate configurations, where network security is essential. Audit services allow network managers to monitor user activities, including attempted logons and the file servers or files used. It is achieved by monitoring all user workstations and recording transaction activity. Most network operating systems support audit trails. Securing the network also requires securing the devices. This is particularly important on the devices that interconnect large parts of the enterprise, such as the backbone or campus routers. These devices should be in one spot or in secure rooms placed strategically around the enterprise. They can be engineered to generate an alarm (raise a management event) if the cases are opened, module removed or if anything is changed.

CONCLUSION

Engineering security in network architecture is not an easy task. Risk assessment and anticipated threats to any network should be examined and studied so the proper security policy can be adopted. Some security appliance vendors have acknowledge that the security solutions presently available are not equipped to handle all types of network and application layer attack. Network security is a system engineering discipline. In the end, secure computer network

architecture is not enough, a personal commitment to security awareness and a dedication to a security policy might protect us in an insecure computer network environment.

REFERENCES

1. IPAM – Security Cyberspace: Applications and Foundations of Cryptography and Computer Security, PP. 2.
2. Introudction to System and Network Security, Learning Tree Internation Technology Training Course 468 Material.
3. D . L . Tennen house et a / . , A S u rvey of Active Network Research, IEEE Commun. Mag., vol. 35(1).
4. Christian F. Tschud i n , Active Network Overlay Network (ANON), RFC Draft,.
5. S . Bhatta c h a rjee, K . L.Ca lvert, a n d E W.Zeq u ra , An Architecture for Active Networking, Proc. IEEE INFOCOM.
6. D . Scott et al, A Secure Active Network Environment Architecture, IEEE Network, special issue on Active and Programmable Networks.
7. B. R. Smith, and J. J. Garcia-Luna-Aceves, ―Efficient security mechanisms for the border gateway routing protocol," Computer Communications, vol. 21, no. 3, pp. 203-210.