International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 5, Issue 7, July 2015)

Design and Implementation of a Secure Campus Network

Mohammed Nadir Bin Ali[1], Mohamed Emran Hossain[2], Md. Masud Parvez[3]
[1,2,3]*Daffodil International University*

***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.**

I. 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 [1].

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 [2].

Generally, IT manager in a computer network faces plenty of challenges 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.

The physical network infrastructure is required for a contemporary university network. University Management and IT manager may know exactly what kind of network they want to set up, upcoming plans, and expected growths. Contingencies for future area, power, and other resource must be part of the physical plan of a university. Building a contemporary university network atmosphere also contains functional and safety elements that also go beyond the IT department's obligations and skills.

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.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 5, Issue 7, July 2015)

II. BACKGROUND

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. 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 [2].

Network Architecture in Campus Networks

The campus network of our study is designed in a hierarchical manner which is a common practice of campus and enterprise networks [3]. It provides a modular topology of building blocks that allow the network to evolve easily.

A hierarchical design avoids the need for a fully-meshed network in which all network nodes are interconnected [4].

Designing a campus network may not appear as interesting or exciting as designing an IP telephony network, an IP video network, or even designing a wireless network. However, emerging applications like these are built upon the campus foundation. Much like the construction of a house, if the engineering work is skipped at the foundation level, the house will crack and eventually collapse.

If the foundation services and reference design in an enterprise network are not rock-solid, applications that depend on the services offered by the network like IP telephony, IP video and wireless communications will eventually suffer performance and reliability challenges. To continue the analogy, if a reliable foundation is engineered and built, the house will stand for years, growing with the owner through alterations and expansions to provide safe and reliable service throughout its life cycle.

The same is true for an enterprise campus network. The design principles and implementation best practices described in this document are tried-and-true lessons learned over time.

Security Issues in Campus Network

There are a wide range of network attacks and security threats, network attack methodologies, and categorizations of network attacks. The query is: how do we minimize these network attacks? The type of attack, as specified by the categorization of reconnaissance, access, or DoS attack, determines the means of mitigating a network threat [2]

Table 1.
Identify the threats

Threat	Internal \ External	Threat consequences
e-mail with virus	External origination internal use	Could infect system reading email and subsequently spread throughout entire organization.
Network Virus	External	Could enter through unprotected ports, compromise whole network.
Web based virus	Internal browsing to external site	Could cause compromise on system doing browsing and subsequently affect other internal systems.
Web server attack	External to web servers	If web server is compromised hacker could gain access to other systems internal to network
Denial of service attack	Internal	External services such as web Email and ftp could become unusable. If router is attack , whole network could go down.
Network User Attack (Internal employee)	Internal to anywhere	Traditional border firewalls do nothing for this attack. Internal segmentation firewall can help contain damage.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 5, Issue 7, July 2015)

Types of Network Attacks:

Classes of attack might include passive monitoring of communications, active network attacks, close-in attacks, exploitation by insiders, and attacks through the service provider. Information systems and networks offer attractive targets and should be resistant to attack from the full range of threat agents, from hackers to nation-states. A system must be able to limit damage and recover rapidly when attacks occur. Here are some attacks types:

1. Passive Attack
2. Active Attack
3. Distributed Attack
4. Insider Attack
5. Close-in Attack
6. Phishing Attack
7. Hijack attack
8. Spoof attack
9. Buffer overflow
10. Exploit attack
11. Password attack

Real Time Data: Some Network Attacks

A. Denial of Service (DoS):

Denial of service (DoS) is an interruption of service either because the system is destroyed, or because it is temporarily unavailable. Examples include destroying a computer's hard disk, severing the physical infrastructure, and using up all available memory on a resource. Fig1 shows a real time value of DoS attack data in a campus network using Cyberoam security device. After Configure Firewall and VLAN for DoS attack

Attack Type	Source		Destination	
	Applied	Traffic Dropped	Applied	Traffic Dropped
SYN Flood	Yes	44844	No	0
UDP Flood	Yes	48240	No	0
TCP Flood	No	0	No	0
ICMP Flood	Yes	27	Yes	429

UDP Flooders

IP Address	Last Seen
103.21.42.205	Sat 20 June 14:04:48
103.21.42.206	Sat 20 June 14:56:31
172.16.20.141	Sat 20 June 15:19:15
172.16.20.222	Sat 20 June 16:22:57
172.16.21.140	Sat 20 June 16:04:01
172.16.22.22	Thu 18 June 16:59:49
172.16.22.82	Sat 20 June 13:11:56
173.194.49.104	Sat 20 June 14:03:06
173.194.49.112	Sat 20 June 13:48:55
182.48.85.204	Sat 20 June 15:13:37
182.48.85.206	Sat 20 June 15:56:10
185.23.127.61	Fri 19 June 17:06:11
216.58.220.37	Sat 20 June 23:27:40
52.74.248.98	Fri 19 June 17:02:37
74.125.214.208	Sat 20 June 13:58:12

Fig1. Attacker IP List

Attacker attempted DoS Attack but the security device dropped the traffic which we have shown in the diagram.

B. ARP Spoofing Attack

ARP spoofing is a type of attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network. We are showing some real time data that attacker using Netcut software exploit the weakness in the stateless ARP protocol due to the lack of authentication in a campus network.

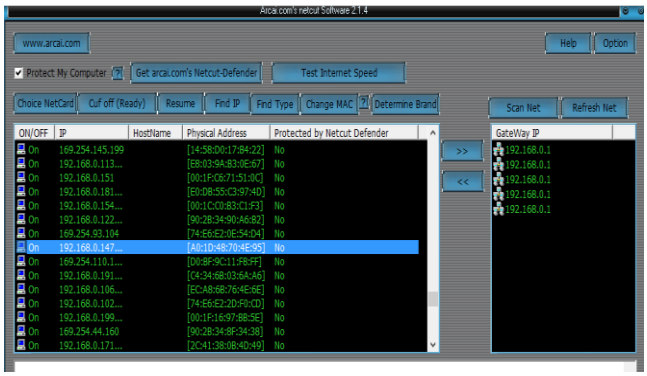

Fig 2. ARP Spoofing Attack in Campus network

Traditional Campus Network Design

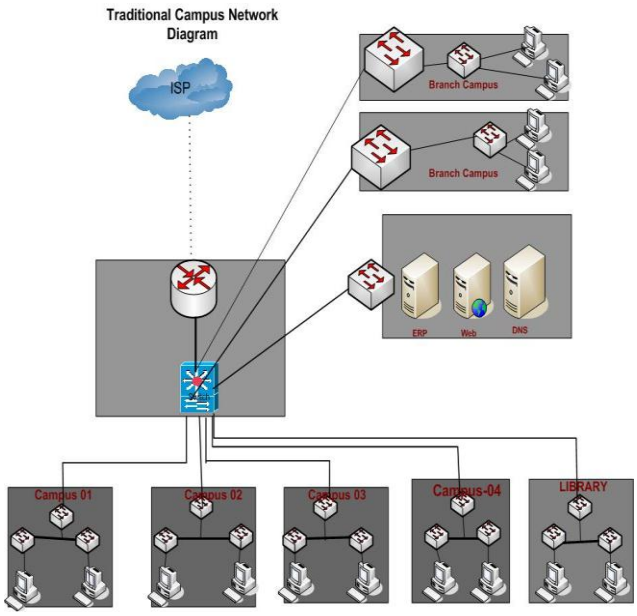

Fig 3. Traditional Campus Network design

III. Mitigating The Known Attacks

Here are some proposed steps for mitigating the known attacks of a campus network:

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 5, Issue 7, July 2015)

a. Proposed cost effective design of a Secure Campus Network.
b. Creation of VLANs (Virtual LAN) for security.
c. Implement firewall for internal and external security
d. Virtual private network use for branch campus

Cost Effective Secure Campus Network Design

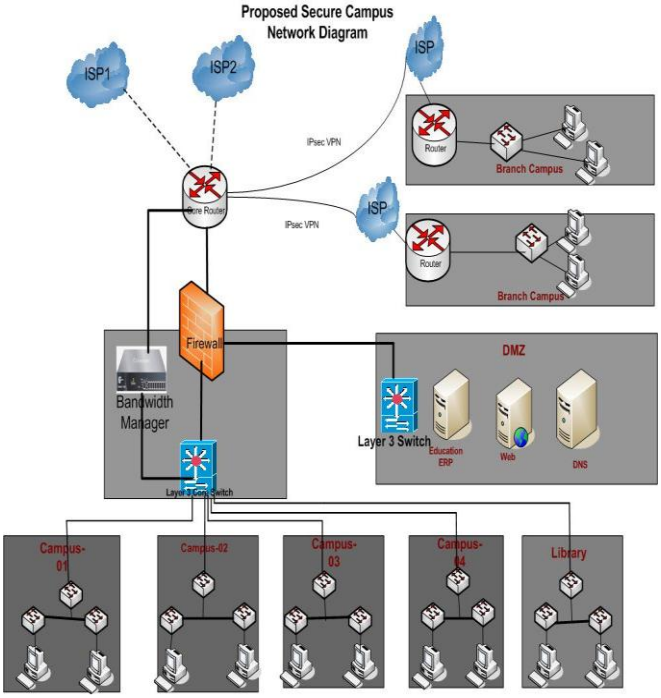

Fig 4. Cost Effective Secure Campus Network Design

Implementation of Cost Effective Secure Campus Network

Several challenges confront the implementation of a secure network on a uuniversity campus, but the challenge central to this topic is security. Henceforth, we have outlined in detail several possible solutions in maintaining a network, the design of our network in order to encompass such solutions.

A. Creation of VLANs (Virtual LAN) for security

It's easy to see why virtual LANs have become extremely popular on networks of all sizes. In practical terms, multiple VLANs are pretty much the same as having multiple separate physical networks within a single organization — without the headache of managing multiple cable plants and switches. Because VLANs segment a network, creating multiple broadcast domains, they effectively allow traffic from the broadcast domains to remain isolated while increasing the network's bandwidth, availability and security.

We have suggested some VLANs for better security of campus network and reducing Broadcast.

Table 2.
Proposed VLAN for Campus Network

Proposed VLAN for Campus Network		
Sl	**VLAN ID**	**VLAN Name**
1	10	Student
2	15	Faculty
3	20	Admin
4	25	Computer Lab
5	30	Exam
6	35	Accounts
7	40	Internal Servers

B. Implementing Firewall for Internal and External Security

A firewall works to monitor and block or allow network traffic, both incoming and outgoing, on a private network. While there is a hardware firewall to help protect the campus network security, this firewall affects certain outbound traffic and prevents unauthorized inbound traffic. NetBIOS, SMTP and other miscellaneous ports determined to pose a security risk are blocked in the outgoing direction. This does not impact the majority of academic work related programs used on the campus.

C. Virtual Private Network (VPN) Use for branch campus

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.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 5, Issue 7, July 2015)

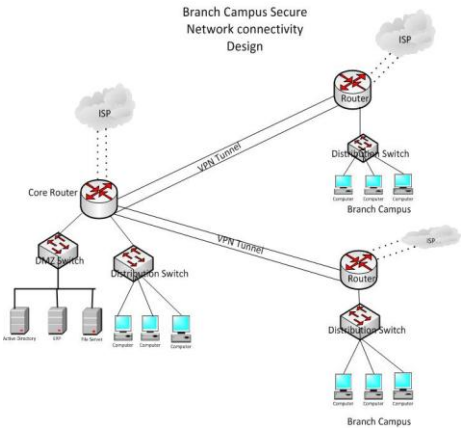

Fig 5. VPN Connectivity Diagram for Branch Campus

IV. Conclusion

Network architecture and its security are important any organization. If we follow the hierarchical network design, network will be scalable, performance and security will be increased, and the network will be easy to maintain. In this work, we proposed a compact cost effective secure campus network design based on the work environment and required scalability, security and other aspects.

This proposed network infrastructure is realizable with adaptable infrastructure. It also provides an overview of the best practices in mitigating the known attacks and recommendation on how to prevent reoccurrence attacks.

REFERENCES

[1] NETWORK SECURITY, SULAIMON ADENIJI ADEBAYO, Bachelor's Thesis (UAS) Degree Program In Information Technology Specialization: Internet Technology.

[2] Network Architecture and Security Issues in Campus Networks, Mohammed Nadir Bin Ali, Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT) 2013.

[3] Security Problems in Campus Network and Its Solutions, 1Lalita Kumari, 2Swapan Debbarma, 3Radhey Shyam, Department of Computer Science1-2, NIT Agartala, India, National Informatics Centre, India.

[4] Network Security: History, Importance, and Future "University of Florida Department of Electrical and Computer Engineering Bhavya Daya ".

[5] Security Analysis of a Computer Network, Jan Vykopal, MASARYK UNIVERSITY FACULTY OF INFORMATICS

[6] Security and Vulnerability Issues in University Networks, Sanad Al Maskari, Dinesh Kumar Saini, Swati Y Raut and Lingraj A Hadimani-- Proceedings of the World Congress on Engineering 2011 Vol I WCE 2011, July 6 - 8, 2011, London, U.K.

[7] Campus Network Design and Implementation Using Top down Approach by Bagus Mulyawan, Proceedings of the 1st International Conference on Information Systems for Business Competitiveness (ICISBC) 2011.