DESIGN AND ANALYSIS OF A SECURE CAMPUS AREA NETWORKS

[1]Amandeep, [2]Vikash Kaushik, [3]Yogesh Kumar

[1]Assistant Professor, [2,3]Students
Computer Science and Engineering
Guru Jambheshwar University of Science and Technology, Hisar, India

Abstract: **In campus area networks design, most of the campuses is not following all security policies, so that attacker can attack easily and access important information. In this paper we designed a secured campus network in GNS3 (Graphical Network Simulator 3), which meat all the security policies and have very hardening of network security. In this system we configured/ implement secured protocol i.e. HTTPS, SSH and CISCO ASA firewall. We compare this design with existing system, and provide an enhanced result.**

Index Terms **- ASA, HTTPS, SSH, Networks attacks, GNS3.**

I. INTRODUCTION

Today, we are in the world of computer networking. As the computer networking increasing, many network threads also increasing. The challenging task is that we must prevent these threads to hacks our users. We have to provide very safe environment to all users so that they can securely surf the internet. Network authentication is not only the one step to secure a network and we can't say that an authenticated network is secured network. We must consider several other approaches and security protocols to design a better secured network. Security mainly focuses on CIA. CIA stands for (Confidentiality, Integrity and Availability) [13]. In previous scenario, network managers focus only for availability of the network. They do not worry about Network Security and other security policies. But in our design, we mainly focus on Confidentiality, Integrity and Availability [13].Network security depends on network hardware and IOS (Internetwork operating system). In campus area network, ARP poisoning [9], DNS poisoning and DHCP snooping [7] are the most common attacks used to break the security policies. We must consider such type of hardware which has ability to prevent these attacks, so our network becomes more secure.

Network Security is 24x7 Revolving process. If we secure our network once, after that forget to audit our network, then every effort of making our network secure is worthless. So we must update ourselves about network threads and should make efforts continuously to secure our network. In network security, logs plays very important role. According to network security spiciest, if we monitor our network traffic and check network logs on the daily basis, then it is very easy to maintain network security to us. Now, finally Network Management is most important thing. Many campuses are not focus on this. If our Control Plane [10] and Data Plane [11] both are secure, then we can go to next level of security. We should hardening of network authentication, so an Admin can change configuration and other person who want to unauthorized access, should block as soon as possible. If we consider only local Admin access to network devices then it is easy to prevent from various attacks like MITM (Man in the Middle) [8] attack. Also, we must consider secure protocol during the access of any network device. Some protocols like TELNET, HTTP are easy to crack so we must avoid them instant of them we should use HTTPS [12] and SSH, they help us to safe our Control Plane. Campuses are the combination of various buildings likes library, teaching departments, facility houses etc. So, during the design of a network, we must consider the security of each and every person. Also, the biggest security thread is user itself. We must train them how to operate a network. Admin should give only limited access to user to surf safe internet and these accesses are should be according to campus policies.

II. EXISTING NETWORK DESIGN

Our Campus (Guru Jambheshwar University Science and Technology) Network is good according to our need. We have one layer 3 switch, on the CWN Cell. Every layer 2 switches (which are deployed in various buildings), are connect to layer 3 switch with the fiber cable. University campus Network [2] [4] is built with the help of many switches of different vendors like Extreme, CISCO, D-Link, HP etc. We have firewall, which are connected to the external network i.e. the ISP (Internet Service Provider). Every user on the Campus must have to authenticate the user-id and password which are provided by the Network Admin. Any unauthorized users, can't use network. All the university departments, Administrative Block, Library, BH1, BH2, and GH1 are connected with fiber optical cable and wireless Access Point. The speed of the network is also fine. Primary BSNL and secondary Airtel, are two ISP's (Internet Service Provider), which provides data services nearly 10GBPS speed in an existing system. A load balancer's is used to divide the total load of the user according to their speed. So, that both links are full utilized and network load managed significantly.

No doubt, it is good network to fulfill users requirement, but it still have some drawback, which is described in next session.

III. LIMITATION OF PRESENT CAMPUS NETWORK

Currently used system has several limitations according to a network security or network engineering. These limitations are described as follow:

Direct communication between different buildings

According to a security specialist the direct communication between two or more building is worthless and not necessary in campus network. Because users in different building can easily hack or try to attack other building system. So, it is always a security hazard that if one person doesn't have system with full patches, it can be easily hacked. Also, during some network activities, it is wastage of bandwidth of the links.

Management access from each VLAN

In existing system management access, access of network devices like switch, router, firewall, Access Point. The access of all these devices is throughout the campus. But, these should be limited and controlled by network admin at one place that is CWN Cell.

Uses of unsecure Protocols

Current design uses unsecure protocol like HTTP and TELNET. The text are flow in clear text format, so that if any attacker capturing the packet, can easily retrieve important information like username and password of any user. So, currently use design are unsecure and the data confidently, integrity, availability are not managed properly.

Network Threats

In campus network IT manager mainly focus only on the connectivity not security. They purchase low cost and less quality devices which are unable to prevent attacks like DHCP snooping [7], ARP poising [9] and DoS Attacks.

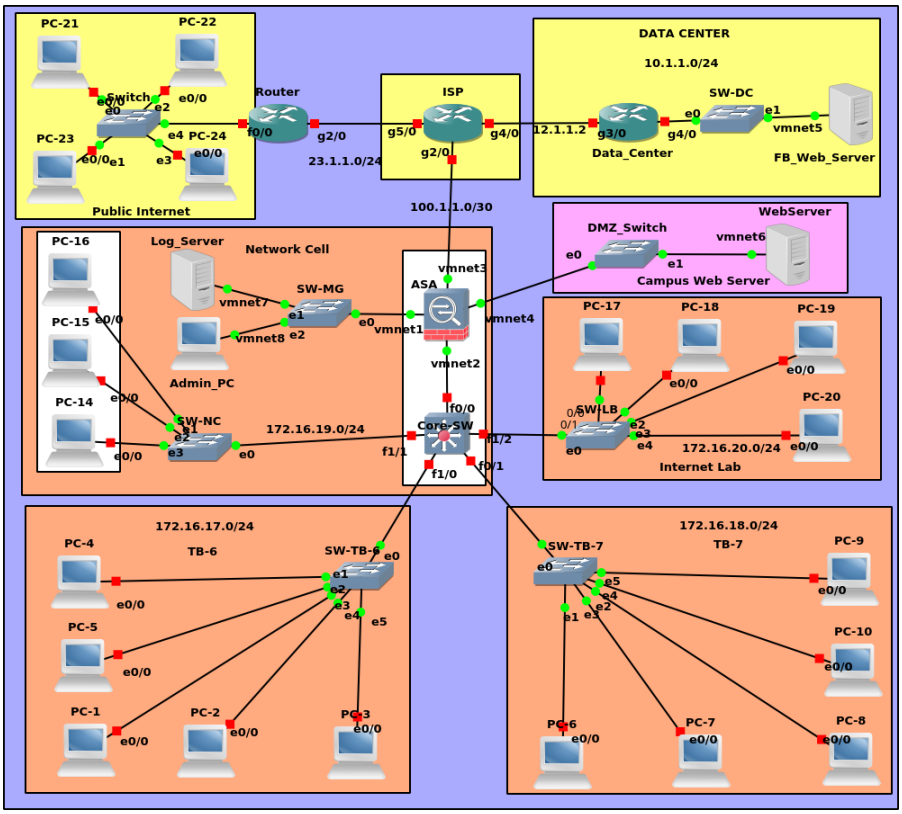

Fig. 1. Campus Area Network Design

IV. PROPOSED CAMPUS NETWORK DESIGN

The idea of this project is comes while the Internship in GJUS&T. During the study of network security, we found that there are some mistakes in the present campus network design, so we got the idea to make a project on Campus Network Design, in which the above disadvantages are removed and the network have fully secured.

In purposed design we mainly consider above limitation. We have use secure protocol instant of unsecure protocols. Hardware used in this system are simple straight forward. A layer three switch & all the layer 2 switch or distributed switches are connected to this switch. Firewall of CISCO vendor i.e. ASA [6] is connected to the outside network, so that it can prevent network attacks.

The communication between different buildings is not allowed at all. Only, authenticated users, login to firewall and then access the main internet.

Here, we used some web server, on which have given access to one port, that means only a particular service is allowed on web servers i.e. web service, reaming all other services are blocked.

Every server located behind NAT (Network Address Translation), so that if any attackers try to attack on web servers, then it is difficult to them to locate original web server. Some services like ICMP are blocked, which is used to trace web server by an attacker.

User can authenticate themselves in a secure manner. An HTTPS protocol is used for the user authentication. It helps to prevent some common attacks like ARP Poisoning [9].

Both Control Plane and Data Plane are secured. All the traffic to the Control Plane is encrypted by some secured protocol, so it is very difficult to decrypt captured data from the control plane. Data Plane, are secured during the time of authentication. Person, can login securely as disused above.

V. SYSTEM DESIGN

In our design, we used GNS3 (Graphical Network Simulator 3) to design and implement this project. CISCO IOS (Internetwork Operating System) are used to configure, design and building many topologies [5] (shown in fig.1). For security purpose, we used hardware firewall CISCO ASA [6]. On ASA, we configure NAT (Network Access Translation) and ACL (Access Control List) which is used for packet filtering. ASA maintain state table, for all outgoing packets. We demonstrate purposed system in Virtual Environment. For virtuality, we used VMWare software in which we used many Operating System including Ubuntu (Web Server), ASA (Firewall), Host Machine (Windows).

In this system, we differentiate our network in different zones like Inside Zone [3], Outside Zone [5], and Demilitarized Zone (DMZ) for users system, public internet and servers respectively. Every zone have its own security policies and security numbers. In inside zone we take physical building Teaching Block 6, Teaching Block -7 and Internet Labs. In Demilitarized Zone we have our web servers. In outside zone, the public internet is there, so have very less trust.

VI. RESULT

In this session, for analyze and verifying the experimental result, we take different parameter CISCO layer 3 switch, layer 2 switch, ASA, Routers, Web server, Log server, PC details are given in table 1. All results are shown by the screenshots which has been taken during simulation. These screenshots show the enhance results which are compared by existing system.

Parameter	*Value*
CISCO Layer 3 Switch	1
CISCO Layer 2 Switch	8
ASA Firewall	1
CISCO Routers	3
Web Server	2
Log Server	1
PC	22
Inside Zone	Internal Internet
Outside Zone	Public Internet
DMZ Zone	Campus Web Server
Queue Hardware/ software hardware	Input Queue, Output Queue
Send Packet	255

Table 1 Simulations Parameters

Fig. 2. IP obtained by DHCP

DHCP Server

In this Scenario, results show that any can get IP from dynamic host configuration protocol (DHCP) but he is not able to configure their own DHCP server for DHCP snooping attack. To Protect DCHP snooping we used DHCP guard [10].

Firewall Authentication

In ASA firewall, CTP (Cut through Proxy) feature is used fig. 3(ii) to authenticate the inside user. Firstly Inside users must authenticate themselves using this features after that they can surf outside or global internet that is shown in fig. 3 (iii). In fig. 3 (i) shows that when a user access their login panel. The web browser show the not secure warning message highlighted with yellow color on the other hand in our system design in fig. 3 (ii) there are no such message because users send their credential information over HTTPS to ASA.

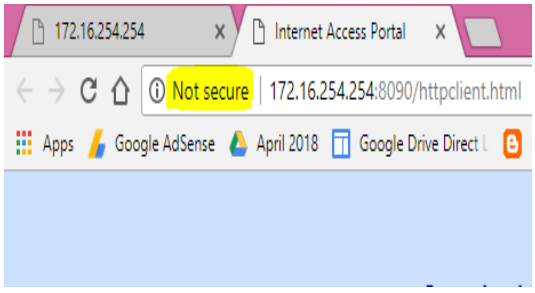

Fig 3 (i) Unsecure Existing system

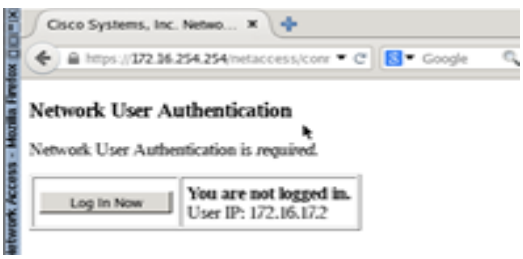

Fig 3 (ii). Secure Authentication on firewall

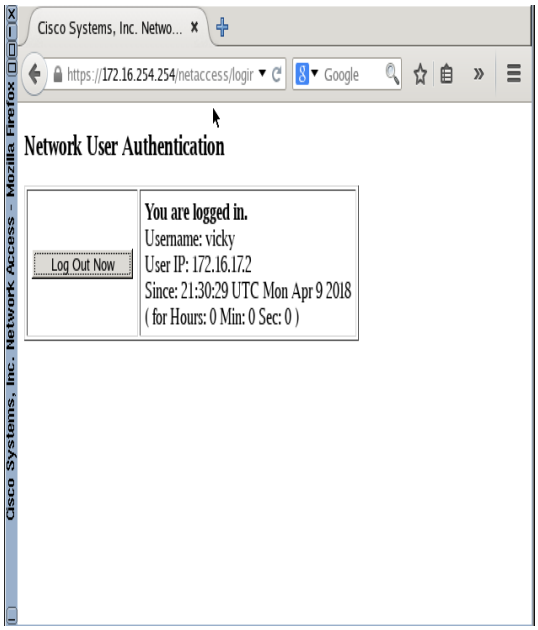

Fig. 3 (iii). Secured Authentication after login on ASA

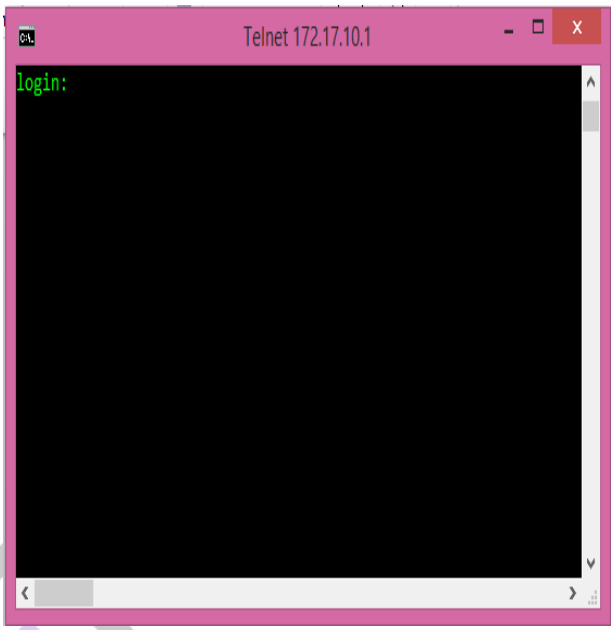

Fig.3 (i) Unsecure Console using Telnet

Secure Management Access

For Secured management Access for admin, two protocols are used HTTPS and SSH. In existing environment Telnet is used for device configuration by admin which is shown in fig 4(i). On the other in our networks design we used SSH which is used port number 22 of TCP layer for secured access of device (shown in fig. 4(ii) for seeking access device & (iii) got secured access) HTTPS is also used for secured graphical configuration, which works on port number 43 of TCP layer.

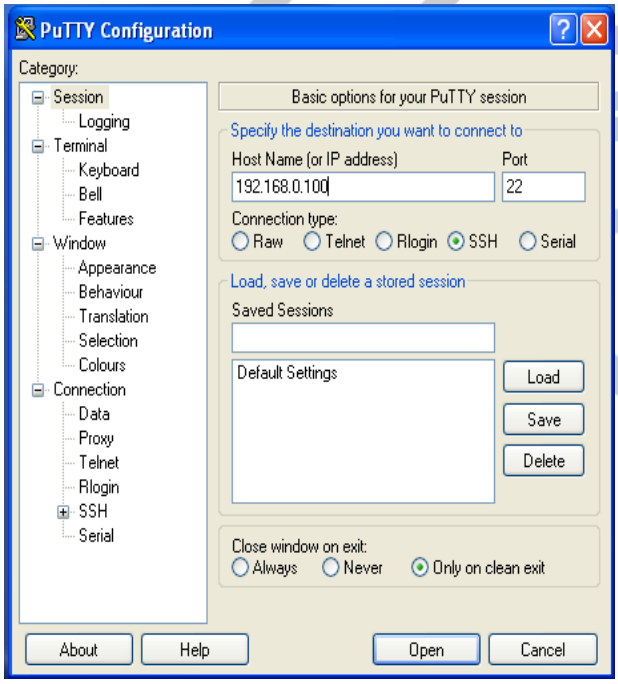

Fig. 4 (ii) SSH Authentication

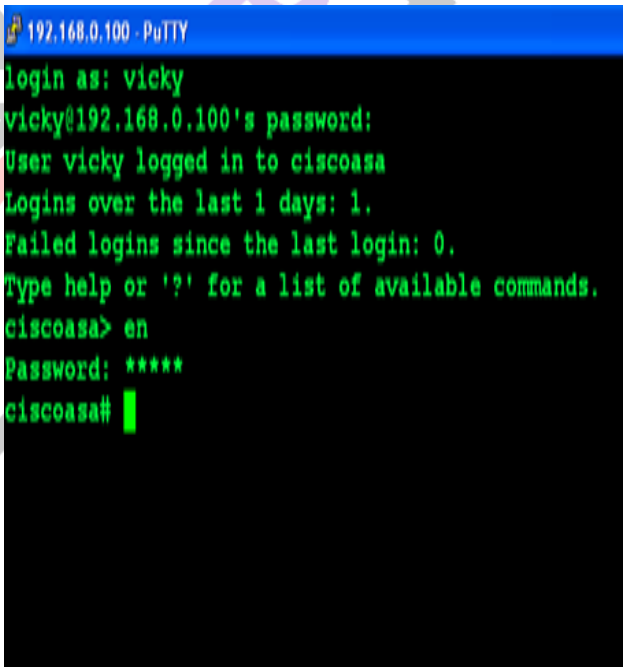

Fig. 4 (iii) SSH Authentication (II)

DMZ Web Server Access

Demilitarized Zone is used for locate the web server. In this zone TCP 80 port is openly allowed and all remaining servers are blocked for every user. TCP 80 port provide web services for inside and outside users (shown in fig 5(i). The all blocked even ICMP (internet control message protocol) services are shown in fig. 5 (ii). .

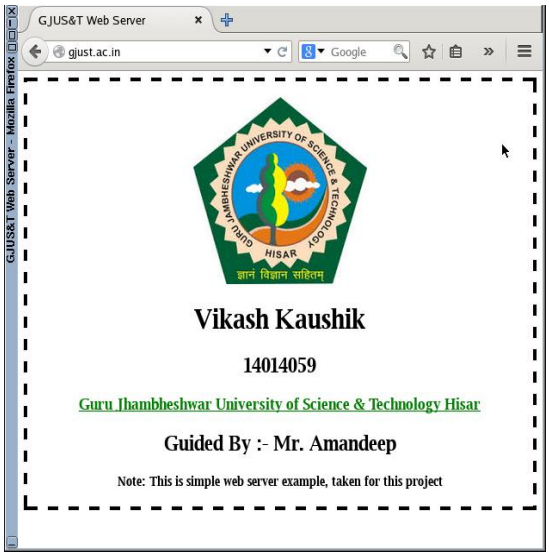

Fig. 5 (i) DMZ web server

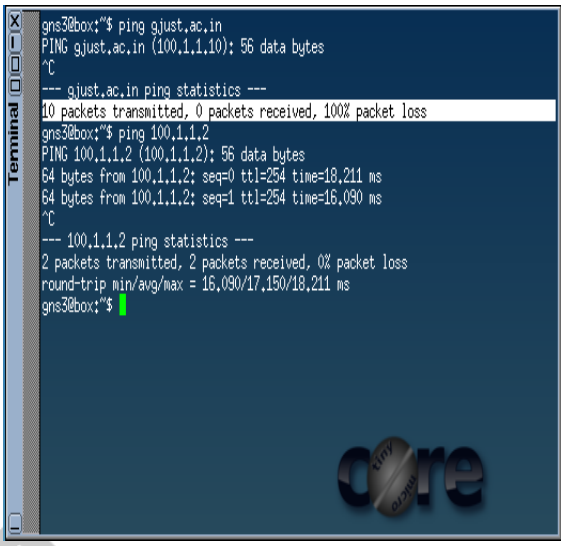

Fig.5 (ii) ICMP Blocked by Firewall

Monitoring /Auditing Networks

ASDM (CISCO) tool used for monitoring and auditing the ASA firewall show different monitoring graph of bit rate, output queue, input queue and input/output packet count for above give simulation parameters.

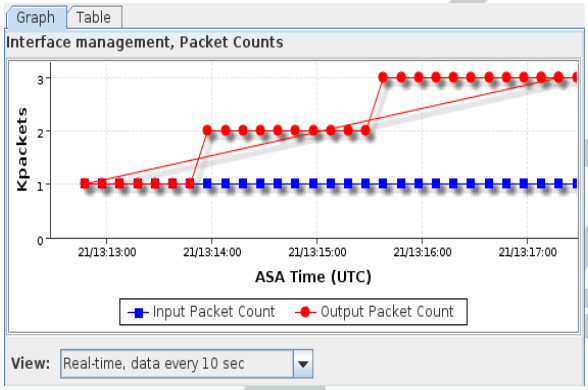

Fig. 6 (i) Input/Output Packet Count

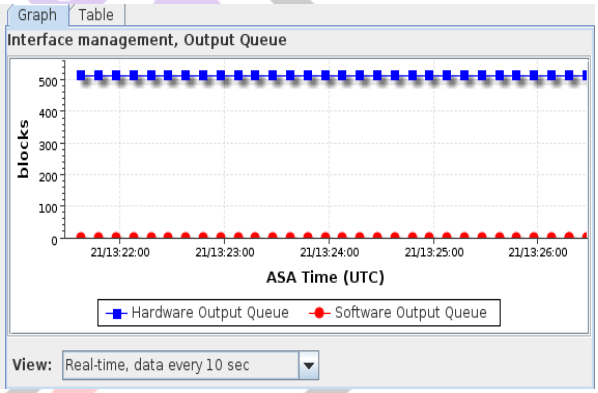

Fig. 6 (ii) Output Queue

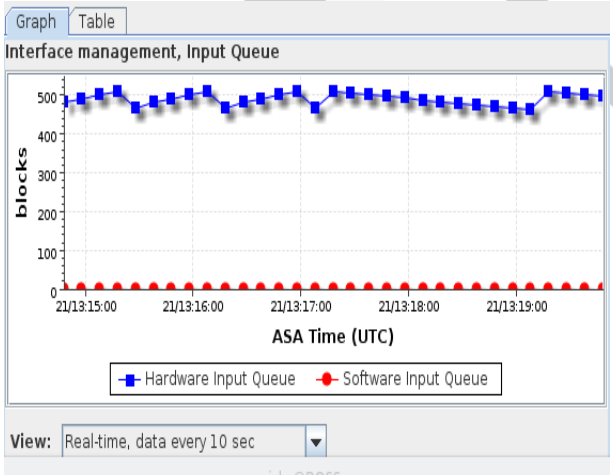

Fig. 6 (iii) Input Queue

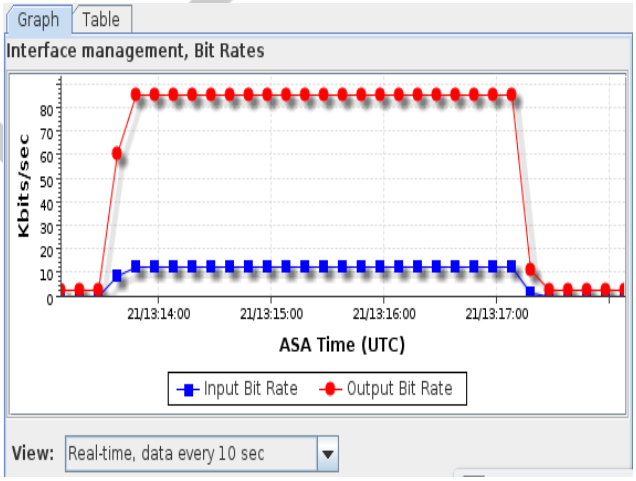

Fig. 6 (iv) Bit Rate

VII. CONCLUSION

In this we design and configured a secured campus area networks in this system firstly we examine the existing system and find the limitation and drawback. After that we implement a secured system on GNS3 simulator and result shown the enhanced security provisioning that is much better than the existing system.

REFERENCES

[1] Brian P. Crow, Indra Widjaja, and Jeong Geun Kim, "Wireless Local Area Networks", *Published in IEEE Communications Magazine September 1999.*
[2] Md. Nadir Bin Ali Daffodil International University, "Design and Implementation of a Secure Campus Network", *Published in Journal of Surface Engineered Materials and Advanced Technology,* Volume 5, Issue 7, pp.370-374, July 2015.
[3] Nathaniel S. Tarkaa, Paul I. Iannah and Isaac T. Iber, "Design and Simulation of Local Area Network Using Cisco Packet Tracer", *Published in The International Journal of Engineering and Science (IJES),* Volume 6, Issue 10, pp. 63- 77,| 2017.
[4] Eze P.U, Diala U.H. and Ndukwe C.I, "Design, Simulation and Pilot Implementation of a Campus Area Network That Supports Teleconferencing", *published in Journal of Multidisciplinary Engineering Science and Technology (JMEST),* volume 2 Issue 4, pp. 550-556, April 2015.
[5] David Kotz and Kobby Essien, "Analysis of a Campus-Wide Wireless Network", *Published in Springer Science Business Media, Inc. Netherlands,* volume 11, pp. 115-113, 2005.
[6] https://supportforums.cisco.com/t5/firewalling/asa-9-3-traffic-zones/td-p/2581844.
[7] https://en.wikipedia.org/wiki/DHCP_snooping.
[8] https://en.wikipedia.org/wiki/Man-in-the-middle_attack.
[9] https://en.wikipedia.org/wiki/ARP_spoofing.
[10] https://en.wikipedia.org/wiki/Control_plane.
[11] https://en.wikipedia.org/wiki/Forwarding_plane.
[12] https://en.wikipedia.org/wiki/HTTPS.
[13] https://en.wikipedia.org/wiki/Information_security.