A Mini Project Report on

Defense Network

Submitted in partial fulfillment of the requirements
of the Semester VII Subject of

Network Design Lab

in

Information Technology

by

Sanjana Nalawade (17104056)

Sahil Naik (17104054)

Himanshu Raut (17104035)

Subject Incharge

Prof.Vishal Badgujar

Department of Information Technology
A.P. Shah Institute of Technology
G.B.Road,Kasarvadavli, Thane(W), Mumbai-400615
UNIVERSITY OF MUMBAI
2019-2020

CERTIFICATE

This is to certify that Network Design Lab (NDL) Mini Project entitled ***"Defense Network"*** Submitted by ***"Sanjana Nalawade (17104056), Sahil Naik (17104054), Himanshu Raut (17104035)"*** for the partial fulfillment of the requirement for Semester VII Subject of ***Network Design Lab*** in ***BE Information Technology***to the University of Mumbai, is a bonafide work carried out during Semester VII in Academic Year 2019-2020

Prof. Vishal Badgujar
Subject Incharge

Prof. Kiran Deshpande
Head Department of Information Technology

External Examiner(s)

1.

Place:A.P.Shah Institute of Technology, Thane
Date:

Declaration

I declare that this written submission represents my ideas in my own words and where others' ideas or words have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

_____

(Signature)

_____

Sanjana Nalawade (17104056)

Date: 10/12/2020

Declaration

I declare that this written submission represents my ideas in my own words and where others' ideas or words have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

_____

(Signature)

_____

Himanshu Raut (17104035)

Date: 10/12/2020

Declaration

I declare that this written submission represents my ideas in my own words and where others' ideas or words have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

_____

(Signature)

_____

Sahil Naik (17104054)

Date: 10/12/2020

Introduction

Networking is referred as connecting computers electronically for the purpose of sharing information. For the very purpose of sharing information we need to build a secured network with which transfer of information becomes reliable.Defence network is for the securing of military and government computer systems. Like everyone else in the world, national agencies also have to secure their systems against malicious cyber attacks. Hence we have decided to build a design for Defense Network which consist of two functional areas naming Central Command (Headquarters) and Base Camp network. In this project we are establishing a secured communication between both these functional areas.

Objectives

Build a compatible wireless and wired solutions for use in the required environment. Securing headquarters offices and the base camp offices with the required firewalls, access control lists, and special privileges.

Network Requirements

- Firewall(Security) : A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
- Routers(Connectivity): A router receives and sends data on computer networks. Routers are sometimes confused with network hubs, modems, or network switches. However, routers can combine the functions of these components, and connect with these devices, to improve Internet access or help create business networks.
- End Devices: The network devices that people are most familiar with are called end devices, or hosts. These devices form the interface between users and the underlying communication network.
- Main Server: A server is a computer that provides data to other computers. It may serve data to systems on a local area network (LAN) or a wide area network (WAN) over the Internet. Many types of servers exist, including web servers, mail servers, and file servers.
- ACL's: An Access Control List (ACL) is a set of rules that is usually used to filter network traffic. ACLs can be configured on network devices with packet filtering capabilities, such as routers and firewalls.
- Wireless Access Points: Wireless access point (WAP), or more generally just access point (AP), is a networking hardware device that allows other Wi-Fi devices to connect to a wired network.

- Virtual LAN A VLAN (virtual LAN) is a subnetwork which can group together collections of devices on separate physical local area networks (LANs). A LAN is a group of computers and devices that share a communications line or wireless link to a server within the same geographical area.
- Secured Communication etc

Major Design Areas and Functional Areas

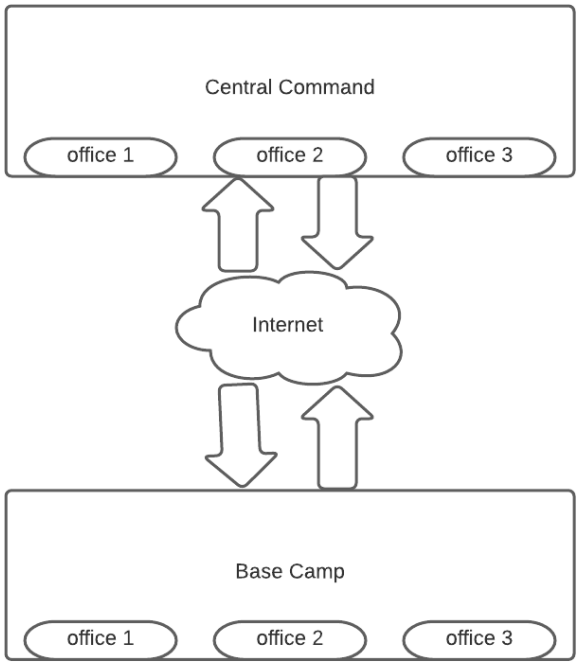
DESIGN AREA:

1. Central Command Designing (HEADQUARTERS)
2. Base Camp Designing
3. Internal LAN Designing
4. Network Distribution

FUNCTIONAL AREA:

1. Central Command
2. Internal and External secured communication using ACL's defined using firewalls
3. Base Camp offices
4. Internal working and communication in the camp
5. External access and communication with the central command.

Existing Infrastructure



Network Devices

1. Router
2. Server
3. Switches
4. Access Point
5. Smart Devices
6. Tablets

Request for Proposal (RFP)

Following is a bill of materials of all networking devices used for developing the required network design

Sr.No	Device	Quantity	Cost/Unit
1	Wired Cisco 2811 Router	4	5000
2	Cisco UCS C220 M3 Server (Basic Server)	2	99999
3	Cisco 2950 Series 24 Port Switch	4	8500
4	Cisco WAP121	4	5999
Total Cost			253998

Remote Site Connectivity

1. Specially designed secured private server
2. Server Connectivity
3. Private credentials for the authorised users

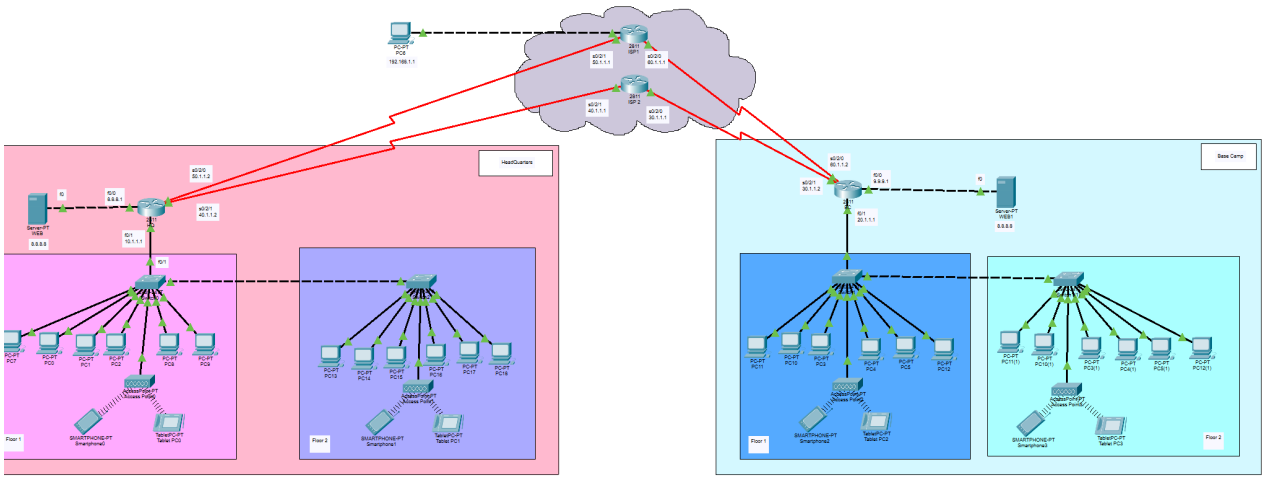
IP addressing Plan

Class A network as it has 126 networks and have almost 1.6 millions of hosts available. We will be using private networks for LAN and Nating for internet transfer messaging. We will be using DHCP for automatic IP assignments.

Routing Protocol Plan

We will be using OSPF(Open Shortest Path First) routing protocol. It is Dynamic routing protocol. Thus it works on the basis of auto-path decision. It is a standard routing protocol. It is a link state routing protocol which means it also checks it s neighbouring routers are still alive or not. If the routers are not alive it automatically drops the router from its table. It has unlimited hop counts.It supports wild card masking. Thus it suits the needs of our network the best way.

Network Design (Topology Created)



Summary

In this project we have achieved the main objective of this network which is to provide secure communication to the Central Command Offices and Base Camp Offices and vice a versa. It is designed to be functionally and physically isolated from access by people not employed by the military organization so as to minimize the risk of unauthorized use. We have used many networking concepts to make it an impactful and wise network in the working state.

References

[1] https://www.google.com/search?q=why+ospfoq=why+ospfaqs=chrome.0.0i457j0l7.2393j0j9sourceid=8

[2] https://www.imperva.com/learn/application-security/defense-in-depth/

[3] https://www.nap.edu/read/11516/chapter/5

[4] https://www.researchgate.net/publication/235163800$_{B}ase_{C}amp_{D}esign_{S}ite_{S}election_{a}nd_{F}acility_{L}ayout$