SECURE NETWORK FOR INSTITUTION

BY

Md. MOZAMMAL HOSEN

ID: 151-15-5269

AND

MD. ARIFUL ISLAM

ID: 151-15-4940

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Computer Science and Engineering

Supervised By

Md. Rakib Hasan
Lecturer
Department of CSE
Daffodil International University

Co-Supervised By

Ms. Nishat Sultana
Lecturer
Department of CSE
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

DECEMBER 2018

APPROVAL

This Project titled **"Secure Network for Institution**", submitted by **Md. Mozammal Hosen, ID No: 151-15-5269** and **Md. Ariful Islam, ID No: 151-15-4940** to the Department of Computer Science and Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on 12 Dec, 2018.

BOARD OF EXAMINERS

_____ **Chairman**

Dr. Sayed Akther Hossain
Professor and Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

_____

Dr. Sheak Rashed Haider Noori
Associate Professor and Associate Head **Internal Examiner**
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

_____

Md Zahid Hasan
Assistant Professor **Internal Examiner**
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

_____

Dr. Mohammad Shorif Uddin **External Examiner**
Professor
Department of Computer Science and Engineering
Jahangirnagar University

DECLARATION

We hereby declare that, this project has been done by us under the supervision of **Md. Rakib Hasan, Lecturer, Department of CSE** Daffodil International University. We also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

Supervised by:

Md. Rakib Hasan
Lecturer
Department of CSE
Daffodil International University

Co- Supervised by:

Ms. Nishat Sultana
Lecturer
Department of CSE
Daffodil International University

Submitted by:

Md. Mozammal Hosen
ID: 151-15-5269
Department of CSE
Daffodil International University

Md. Ariful Islam
ID: 151-15-4940
Department of CSE
Daffodil International University

ACKNOWLEDGEMENT

First we express our heartiest thanks and gratefulness to almighty God for His divine blessing makes us possible to complete the final year project/internship successfully.

We really grateful and wish our profound our indebtedness to **Md. Rakib Hasan**, **Lecturer**, Department of CSE Daffodil International University, Dhaka. Deep Knowledge & keen interest of our supervisor in the field of "E-Commerce Sector" to carry out this project. His endless patience, scholarly guidance, continual encouragement , constant and energetic supervision, constructive criticism , valuable advice, reading many inferior draft and correcting them at all stage have made it possible to complete this project.

We would like to express our heartiest gratitude to Dr. Syed Akhter Hossain, Professor and Head**,** Department of CSE, for his kind help to finish our project and also to other faculty member and the staff of CSE department of Daffodil International University.

We would like to thank our entire course mate in Daffodil International University, who took part in this discuss while completing the course work.

Finally, we must acknowledge with due respect the constant support and patients of our parents.

ABSTRACT

This report is for network Topology development project. We create a secure organization private network where we have created a DMZ and Data center. This report will be helpful for the people who want to create a private network and want to know about Firewall, DMZ and Data center. They can learn how to create a DMZ and Data center in a private network with high security. They can also get the idea of designing topology. Because Topology designing is a very important part to create a LAN network. Security of a network almost vary on topology design because network devices configuration are same for any topology but setup idea depend on you which give the network security theme. The teacher and student can get idea and topics from here to research. In present we all depending on Internet but we can't protect our privacy from hacker. Because our network system is not as strong as we need. Cyber-crime like hacking is increasing day by day for this weak network system so that weak try to give some idea to create a strong private network for an organization.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

Introduction

1.1 Introduction:

In present IOT is taking the huge space of our real life. The companies are using AI robot to do many works and general people also liking AI product which can control by internet. This type of AI robot or other product need huge amount of memory which is providing by different international server company like Google. Organizations are creating their own server and network for business purpose. Now we can control our whole house system using internet by using IOT. So, day by day private network is growing up on the other hand security problem also increasing. To take this theme we developed our project.

This is a network base project where security is given major priority. This topology can be used in Bank, University or any Enterprise network system whom need DMZ server and Data center both together. In our topology we use the latest network devices.

1.2 Motivation:

Now a day there is no alternative of Internet, so people and organization both are mostly dependent on it. That's why the number of privet network for organization increasing day by day, on the other hand they are facing security problem (i.e.). We design our topology with high priority to protect LAN and Data-center from Cyber-attack and give smooth service of network to the LAN user of the organization. Any organization can follow our topology to create a secure private network with highly protected DMZ server and Data center.

1.3 Objective:

In the period of implementing this topology we learn how to develop real life private networking system and use of the networking device like Layer-3 switch, Ethernet switch,

Router, Firewall, cables. We also experienced about ISP, LAN, MAN, WAN, VLAN, routing protocol (STATIC, RIP, EIGRP, OSPF) DMZ server, Data-center.

1.4 Expected Outcome:

Our project theme can help to develop secure private network which is very challenging now a day in the world. Anyone can learn how to configure firewall, DMZ server, Data center. Also any Organization can follow our project to create their organization LAN or DMZ server or Data center. Many international organizations (ISOC, ICANN, IAB, IESG etc.) are trying to create a secure network in the world from many years, we also want to be a part of them. That's why we developed this project because we think this project can be help to create a secure network like other projects in the world.

1.5 Report Layout:

Chapter 1 Introduction: In chapter-1 we introduce our project. Here we discuss about the motivation, objectives and the expected outcome of the developed Topology and report layout.

Chapter 2 Background: This chapter is about the background circumstance of the project. Here we talk about the related work, comparison to other existing application, the scope of the problems and challenges of the developed Topology.

Chapter 3 Requirement Specification: In this chapter we discuss about requirements collection and specification. Here also talk about the use case model of the network Topology, the logical relational database model for it and the design requirements to design this.

Chapter 4 Design Specification: In chapter-4, here discuss about the Topology design with interaction design and UX and the implementation requirements to develop this.

Chapter 5 Implementation and Testing: This chapter discuss about the implementation of Topology, interactions implementation and the test results of the project.

Chapter 6 Conclusion and Future Scope: In this last chapter we give the conclusion and the scope for further develop for this project.

CHAPTER 2

Background

2.1 Introduction:

This project is network base where we developed a private network topology. Here we use GNS3 software to implement this organization secure network topology. In this GNS3 software we use latest Firewall, Router, Layer-3 switch, Ethernet switch. We connect the private network with two different ISP (Internet Service Provider) Company so that if ISP-1 is down then ISP-2 will automatically up. We also use double connection of wire in our whole topology so there is no way down the topology network.

2.2 Related Works:

There is no fixed design of network topology in the world. Generally organizations design there network topology as they need. Security of the network most provably depend on the topology design. So, designing is a very important part to create a private network for the organizations.

There are many network topology developed in the world and those are almost same in design but different in work. Some design topology only to create server or DMZ server or Data center or LAN or DMZ server with LAN or Data center with LAN.

2.3 Comparative Studies:

In related works (2.2) we describe about the topology that are designed for the private network. From there we get some idea about the network topology that are already designed.

Our network topology is not totally different from them but here we use some new idea that make it more secure from others.

In our project we separate DMZ server, LAN and Data center from each other using two firewalls but in almost topology they don't separate those things that's why some security problem can be create in the topology from LAN general user.

We also create two options to connect the topology with two different ISP Company to get the Internet connection all time. Because if one ISP Company link is down then another link will be automatically up. We don't found any topology that connect with to different ISP Company that's why we develop this option in our project.

2.4 Scope of the problem:

- It will be very costly to develop this project in real life. So small organization can't effort to create this topology for their network.
- In our topology we don't develop the tracking option.
- Can create problem in Data center to connect it with branch network of the organization for security purpose.

2.5 Challenges:

❖ Topology designing:

To develop a network topology it is first challenge is designing because the security of network almost depend on it is design of topology. We have to research many topology that already have developed and their limitation. After combining the topologies and their limitations finally we design it.

❖ Latest devices setup:

In our topology we used the latest network devices (cisco ASA-Firewall, cisco3745 Layer-3 switch, cisco7200 router, latest Ethernet switch). Those are different from the old version so that it is very challenging to setup on the topology.

❖ **Latest devices command:**

The new version devices command are not totally same with old version and new device command are not available. So, it is very difficult and challenging to find the correct command for the device to configure the topology.

❖ **Connect with two different ISP Company:**

Generally topology are connected with one ISP Company but in our topology we connect it with two different ISP Company which is very challenging for us. Because we create here a option that two ISP can automatically up or down their link as necessary.

❖ **Separating LAN, DMZ server and Data center:**

When we were researching the topology, we saw almost topologies are designed LAN and DMZ server together or LAN and Data center together but in our topology we create our network combining those two theme.

❖ **Setup Firewall:**

We use two firewall to separate LAN, DMZ server and Data center. It is very challenging for us to setup the Firewall which separate LAN and Data center. Because in this Firewall there are three interface to configure one interface for DMZ server another for LAN and last one for Data center.

❖ **Finding Routing Protocol :**

We know there are several types of routing protocol (OSPF, RIP, EIGRP, BGP) to route. Which routing protocol will be best according to the design of our topology is very challenging to find.

CHAPTER 3

Requirement Specification

3.1 Requirement Collection and Analysis:

- **GNS3 software**: GNS3 software is used to develop and design network topology. We use this software version 2.1.9 to develop our project. There are many other software (Cisco Packet Tracer, NS2, etc.) that can be used to develop our project but we select this software because we can connect here real devices.
  Collect from GNS3 official website.

- **GNS3 VM:** GNS3 VM is a part of GNS3 software by which we can create GNS3 server.
  Collect from GNS3 official website.

- **VMware Workstation 2014:** VMware is used to run GNS3 VM and ASA Firewall Image.
  Collect from VMware official website.

- **VirtualBox-5.2.18:** VirtualBox is used to run Windows Server 2012 and Windows-7 OS.
  Collect from VirtualBox official website.

- **ASAv971 Firewall Image:** ASAv971 Firewall Image is installed in VMware workstation to create Firewall in GNS3 software. This is latest version of ASA Firewall.
  Collect from block site techemergente.blogspot.

- **Cisco3745 Layer-3 Switch Image:** Cisco3745 Image install in GNS3 software to create Layer-3 switch. This is a latest version of Cisco Layer-3 Switch.
  Collect from block site techemergente.blogspot.

- **Cisco7200 Router Image:** Cisco7200 Image install in GNS3 software to create Router. This is a latest version of Cisco Router.
  Collect from block site techemergente.blogspot.

- **Windows Server 2012 OS:** Windows server 2012 OS install in VirtualBox to create server in GNS3 software. This version server OS is most popular in the world.
  Collect from Microsoft official website.

- **Windows-7 OS:** Windows-7 OS install in VirtualBox to create user Windows PC.
  Collect from Microsoft official website.

- **Ethernet Switch:** the latest version of Ethernet Switch is include with GNS3 software. This is different from old version. Here console option not work.
  Get from GNS3 software.

3.2 Use Case Modeling:

The flowing figure 3.1 shows the network topology use case that we design for this project.

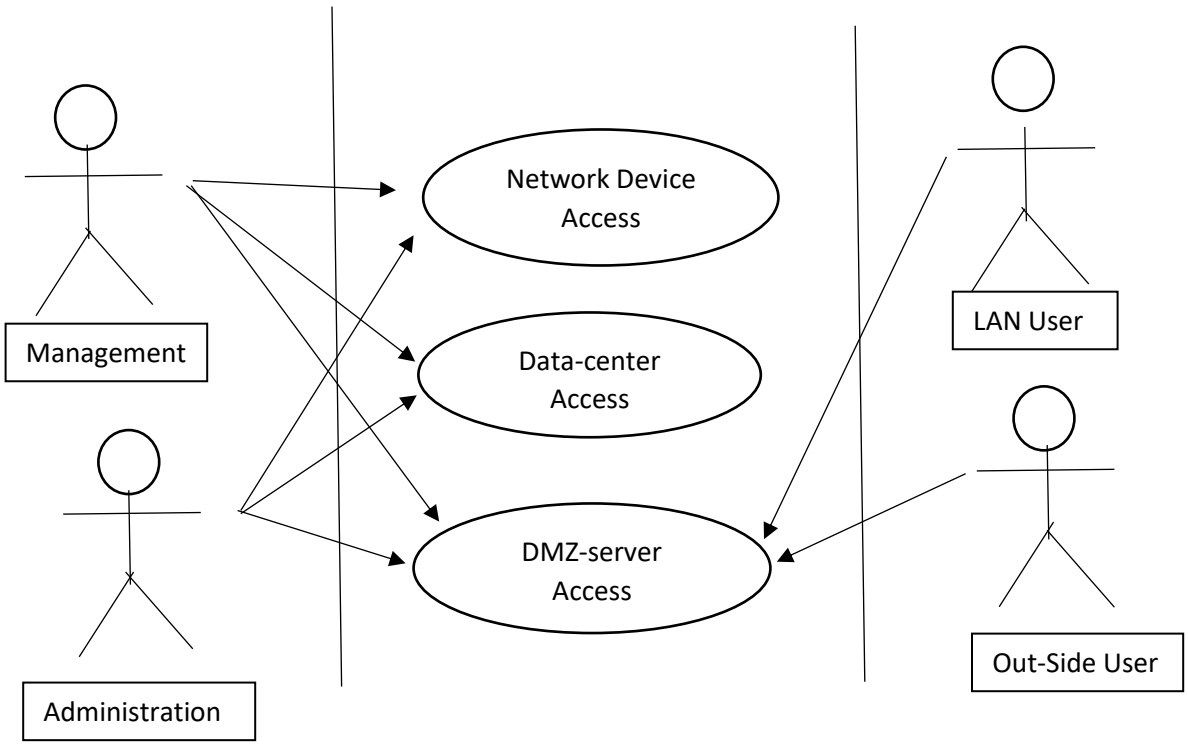


Figure 3.1: Use case for network topology

Simulation of Use case:

- Management User: In this diagram management is an important part of network topology. Management can access in Data-center, DMZ-server and Network devices (Firewall, Router, Layer-3 switch) to change the device configuration. Management will access in Data-center and DMZ-server as Admin.
- Administration User: In our topology there will be a network for Administration from there Administration user can access in Data-center and DMZ-server as Admin.

- LAN User: General LAN user can access only in DMZ-server as general user or Admin.
- Out-Side User: The user can come from outside to take service of DMZ-server as only general user.

3.3 Logical Data Model:

The flowing figure 3.2 shows the network topology logical data model for this project.

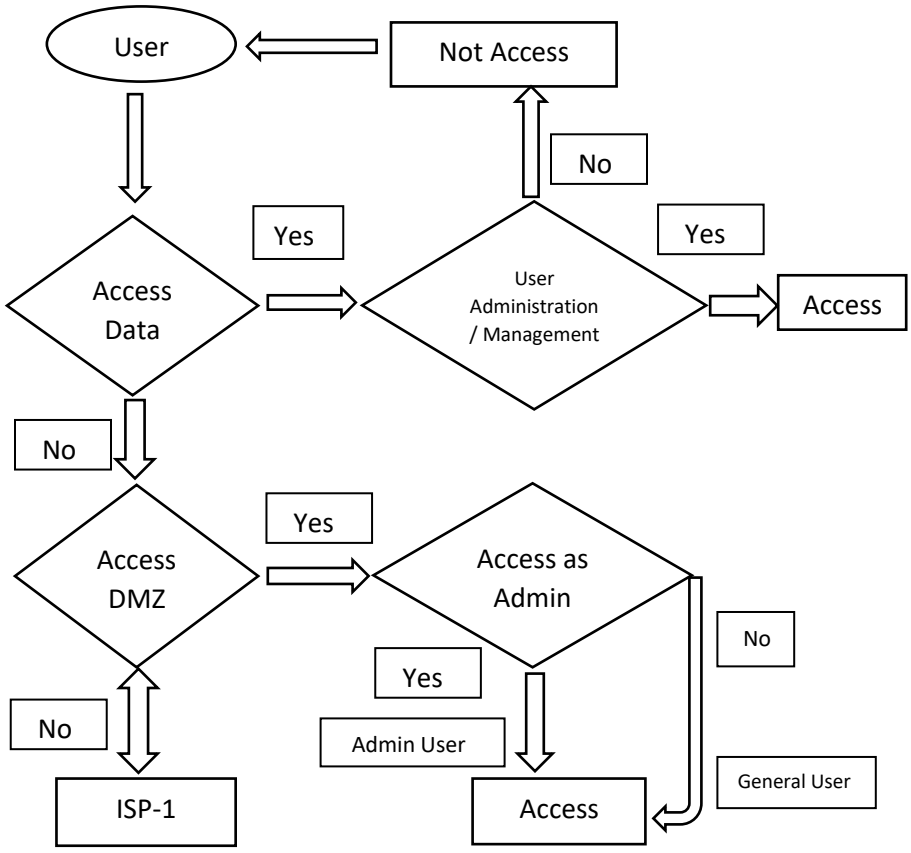


Figure 3.2: Network topology logical data model

Simulation of Logical data model:

- From our topology LAN user can take two types of service. One from DMZ server and another from Data-center. Everyone can access in DMZ server but to access in Data-center user must be come from LAN Administration or Management network. Because this is the most sensitive part of topology, here all important data of organization will be stored.

- When user want service form LAN at first Firewall will check which type of service it wants. If user want to access in Data-center then it will check from which network request has come. If it is came from Administration or Management network then give permission to access in Data-center else it will not give permission to access and give an error and warning message to the user device.

- If the user don't want service from Data-center than the request pass through the router. Then router will check which type of request it is. If the request is to access in DMZ server than it will pass through the request in DMZ Firewall and firewall will check which type of user it is. If it is came from LAN as admin then it will give permission to access as Admin or it will give permission to access as general user.

- After checking the request in router if it is found user don't want service from DMZ-server than it will pass the request to ISP and LAN user can take service from there.

- Here through ISP the outside user of LAN can only take the services of DMZ-server as general user.

3.4 Design Requirement:

In the below there given the requirement that we need to design the Topology:

i. GNS3 software v-2.1.9
ii. GNS3 VM
iii. VMware Workstation 2014
iv. VirtualBox-v5.2.18
v. ASAv971 Firewall
vi. Cisco3745 Layer-3 Switch
vii. Cisco7200 Router
viii. Ethernet Switch
ix. Windows server 2012
x. Windows 7

CHAPTER 4

Design specification

4.1 Network Topology Design:

We design our topology into five part

i. Part 1 - Edge Router and ISPs
ii. Part 2 - DMZ server
iii. Part 3 - Cisco ASA Firewall-1
iv. Part 4 - LAN
v. Part 5 - Data Center

Part 1 – Edge Router and ISPs:

The flowing figure 4.1 shows Organization connection to the internet via router R3 through R1 and R2.

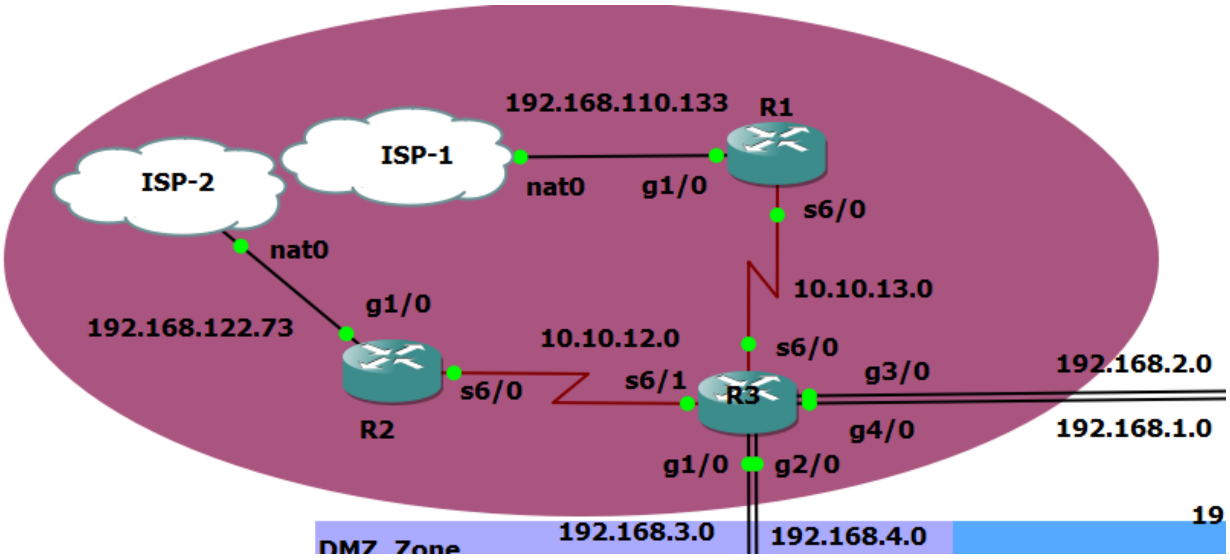


Figure 4.1: Edge Router and ISPs

In this part we configure the router R1, R2 and R3. Here R1 and R2 this two router connected with two different ISP Company and pass internet by R3 router. We connect R1 and R2 with R3 using serial port. Where IP address 10.10.12.1 for R2 which use port serial 6/0, IP address 10.10.12.2 for R3 which use port serial 6/1 and IP address 10.10.13.1 for R1 which use port serial 6/0, IP address 10.10.13.2 for R3 which use port serial 6/0. ISP1 connect with R2's port GigabitEthernet1/0 and ISP2 connect with R1's port GigabitEthernet1/0.

Router R3 also connect with Firewall-1 and Firewall-2 using port GigabitEthernet1/0 with IP address 192.168.3.1 and port GigabitEthernet2/0 with IP address 192.168.4.1 (This two port use to connect with Firewall-2 because there are double connection), using port GigabitEthernet4/0 with IP address 192.168.1.1 and port GigabitEthernet3/0 with IP address 192.168.2.1 (This two port use to connect with Firewall-1 because there are double connection). We use here double connection because if one port is down then another port will auto link up to provide non-stop internet connection.

We configure NAT in Router R1, R2 and R3. After NAT we get IP address 192.168.110.133 at port GigabitEthernet1/0 in router R1 and IP address 192.168.122.73 at port GigabitEthernetg1/0 in router R2.

In Router R1, R2 and R3 we route OSPF because this routing protocol is suitable for this topology. From the flowing figure we can find out the best routing protocol for any topology.

	Distance Vector				Link State	
	RIPv1	RIPv2	IGRP	EIGRP	OSPF	IS-IS
Speed Convergence	Slow	Slow	Slow	Fast	Fast	Fast
Scalability - Size of Network	Small	Small	Small	Large	Large	Large
Use of VLSM	No	Yes	No	Yes	Yes	Yes
Resource Usage	Low	Low	Low	Medium	High	High
Implemenation and Maintenance	Simple	Simple	Simple	Complex	Complex	Complex

Figure 4.2: Finding best routing protocol

From this figure we find out that OSPF routing protocol's speed convergence is fast than another routing protocol, scalability-size of network is large, we can use VLSM, resource uses is high. Though implementation and maintenance is complex but according to our topology this is perfect routing protocol for us.

Every Router takes 512 MB RAM to run their OS on GNS3 software.

Part 2- DMZ server:

The flowing figure 4.3 shows organization DMZ server which is connected with Router R3 and separated by Firewall-1 from LAN.

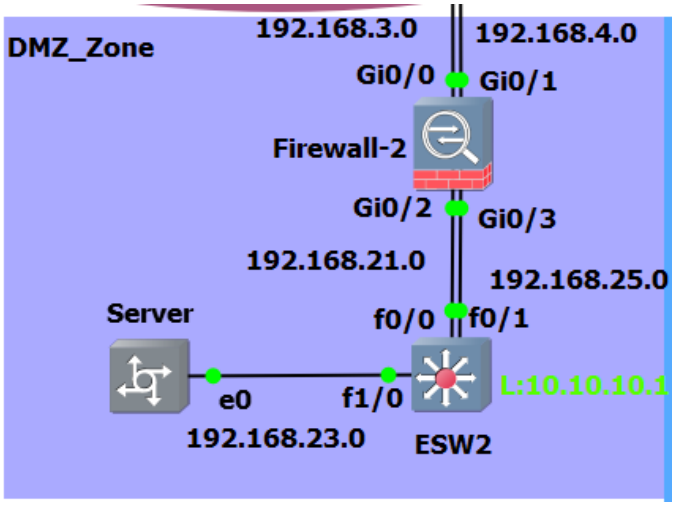


Figure 4.3: DMZ server

In DMZ (Demilitarized Zone) there we setup one Firewall, one Layer-3 switch and one server (Windows server 2012). We know that DMZ is a part of private network which is open for outside user. So we can say DMZ part is less secure in the topology.

To create DMZ at first we connect Firewall-2 with router R3 using the port GigabitEthernet0/0 with IP address 192.168.3.2 and port GigabitEthernet0/1 with IP address 192.168.4.2. Then we connect a Layer-3 switch with Firewall-2 and sever. Here Firewall-2's ports GigabitEthernet0/2 and GigabitEthernet0/3 use to connect with Layer-3

switch ports FastEthernet0/0 and FastEthernet0/1 using network 192.168.21.0 and 192.168.25.0 (Firewall-2: Gi0/2 IP 192.168.21.1, Gi0/3 IP 192.168.25.1; Layer-3 switch: f0/0 IP 192.168.21.2, f0/1 IP 192.168.25.2). Layer-3 switch use port f1/0 to connect with server port e0 (L-3 switch: port f1/0 IP 192.168.23.1; Server: port e0 IP 192.168.23.2). Here also set a Loopback IP 10.10.10.1 at port Loopback Interface 0 in Layer-3 switch.

In Firewall-2 and Layer-3 switch we configure OSPF routing protocol to create connection between router R3 and Firewall-2, Firewall-2 and Layer-3 switch, Layer-3 switch and Server.

We configure Firewall-2 by creating an object for network 192.168.23.0 and NAT. Then we create access list for TCP, UDP and ICMP for any network and give permit to access in DMZ. After all we create access group taking access list and give permission to access DMZ server.

Firewall-1 take 2048 MB RAM to run in GNS3 through VMware software, Layer-3 switch take 380 MB RAM to run and install server in VirtualBox which take 3072 MB RAM to run.

Part 3 - Cisco ASA Firewall-1:

The flowing figure 4.4 shows how to configure MZ (Militarized Zone) using Firewall.

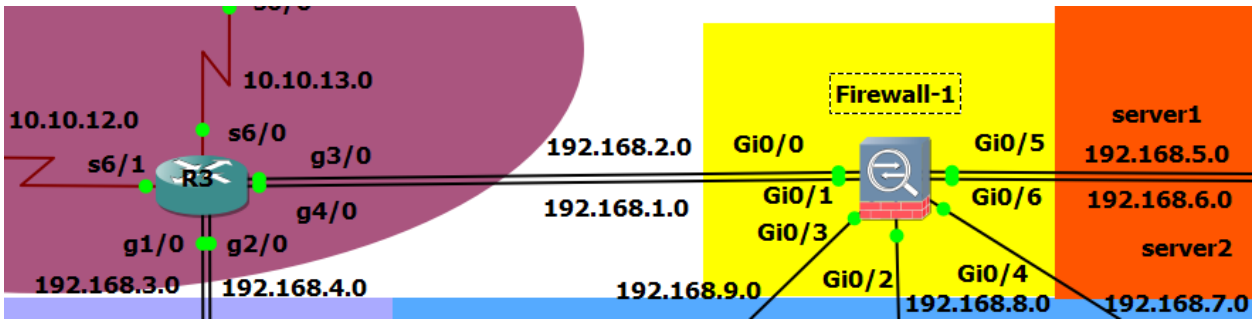


Figure 4.4: Cisco ASA Firewall-1

This Firewall-1 is very sensitive part in our topology because it separate LAN, Data Center and DMZ server. Firewall-1 has seven Interface. Interface GigabitEthernet0/0 and Interface GigabitEthernet0/1 they are declared the outside part; Interface GigabitEthernet0/3 and Interface GigabitEthernet0/4 are declared the Inside part of LAN for general user or employee; Interface GigabitEthernet0/ 2 is also a part of inside LAN for Administration and Management to access in Data center; Interface GigabitEthernet0/5 and Interface GigabitEthernet0/6 are declared as server side of Data-center.

We configure the routing process of Firewall using OSPF routing protocol with network

- 192.168.1.0
- 192.168.2.0
- 192.168.9.0
- 192.168.7.0
- 192.168.8.0
- 192.168.5.0
- 192.168.6.0

OUTSIDE1 Interface GigabitEthernet0/0 use to connect with router R3 (IP 192.168.2.2)

OUTSIDE2 Interface GigabitEthernet0/1 also use to connect with router R3 (IP 192.168.1.2)

INSIDE1 Interface GigabitEthernet0/3 use to connect with LAN (IP 192.168.9.1)

INSIDE2 Interface GigabitEthernet0/4 use to connect with LAN (IP 192.168.7.1)

INSIDE3 Interface GigabitEthernet0/2 use to connect with LAN (IP 192.168.8.1)

SERVER1 Interface GigabitEthernet0/5 use to connect with Data-center (IP 192.168.5.1)

SERVER2 Interface GigabitEthernet0/6 use to connect with LAN (IP 192.168.6.1)

In this firewall we have to create five objects to access in DMZ server.

i. Object for DMZ server network (dmz- 192.168.23.0)
ii. Object for Employee_1 network (emp1- 192.168.40.0)
iii. Object for Employee_2 network (emp2-192.168.45.0)
iv. Object for Administration network (adm-192.168.42.0)
v. Object for Management network (mgm-192.168.50.0)

Also create three objects to access in Data Center.

i. Object for Data Center network (mz-192.168.60.0)
ii. Object for Administration network (adm1-192.168.42.0)
iii. Object for Management network (mgm1-192.168.50.0)

To take service from LAN to DMZ server or Data Center we have to create access list for TCP, UDP and ICMP and give permission. Then have to create access group take the all access list and give them permission to go outside of the LAN. For different INSIDE Interface have to give permission of the access group. INSIDE1 and INSIDE2 give permission access group (dmz_acl_in) to access DMZ server through OUTSIDE1 and OUTSIDE2. INSIDE3 give permission access group (mz_acl) to access Data Center through SERVER1 and SERVER2.

This Firewall take 2048 MB RAM to run in GNS3 software through VMware Workstration.

Part 4 – LAN:

The flowing figure 4.5 shows how to configure LAN (Local Area Network)

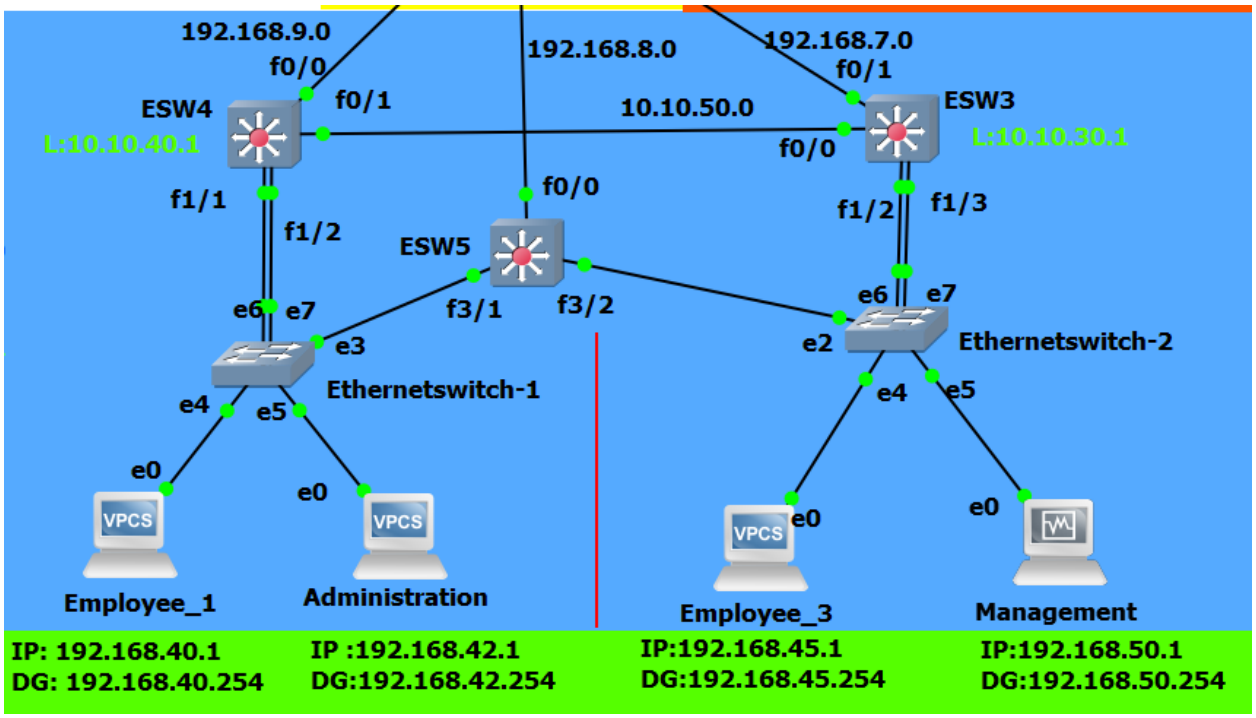


Figure 4.5: Local Area Network

We create Local Area Network using three Layer-3 switch ESW3, ESW4 and ESW5, two Ethernetswitch (E1, E2), two network for Employee (192.168.40.0, 192.168.45.0), one network for administration (192.168.42.0) and one network for Management (192.168.50.0)

Configuration for ESW4:

Here we create VLAN 10 and VLAN20. We connect this switch with Firewall-1 using port FastEthernet0/0 (IP 192.168.9.2), ESW3 using port FastEthernet0/1 (IP 192.168.50.1), Ethernetswitch-1 using port f1/1 and f1/2 (VLAN 10, VLAN20), Loopback IP 10.10.40.1.

Configure here OSPF routing protocol to route ESW4 with Network

- 192.168.9.0
- 192.168.50.0
- 192.168.40.254 (VLAN 10, gateway of Employee_1 network)
- 192.168.42.254 (VLAN 20, gateway of Administration network)
- 10.10.40.0

This L3 switch is used to access the Employee_1 and Administration network to take service.

Configuration for ESW3:

We create here VLAN 30 and VLAN 40. We connect this switch with Firewall-1 using port FastEthernet0/1 (IP 192.168.7.2), ESW4 using port FastEthernet0/0 (IP 192.168.50.2), Ethernetswitch-2 using port f1/2 and f1/3 (VLAN 30, VLAN40), Loopback IP 10.10.30.1.

Configure here OSPF routing protocol to route ESW3 with Network

- 192.168.7.0
- 192.168.50.0
- 192.168.45.254 (VLAN 30, gateway of Employee_3 network)
- 192.168.50.254 (VLAN 40, gateway of Management network)
- 10.10.30.0

This L3 switch is used to access the Employee_3 and Management network to take service.

Configuration for ESW5:

We create here VLAN 20 and VLAN 40. We connect this switch with Firewall-1 using port FastEthernet0/0 (IP 192.168.8.2), Ethernetswitch-1 using port f3/1 (VLAN 20) and Ethernetswitch_2 using port f3/2 (VLAN 40).

Configure here OSPF routing protocol to route ESW5 with Network

- 192.168.8.0
- 192.168.42.254 (VLAN 20, gateway of Administration network)
- 192.168.50.254 (VLAN 40, gateway of Management network)

This L3 switch is used to access Data-center from the Administration and Management network.

Configuration for Ethernetswitch_1:

We create here VLAN 10 and VLAN 20. We connect this switch with ESW4 using port e6 and e7 (VLAN 10, VLAN 20), ESW5 using port e3 (VLAN 20) and with Employee_1 network for which create the VLAN 10 (192.168.40.254), Administration network VLAN 20 (192.168.42.254). This two network use this VLAN as their default gateway.

In this new version of Ethernet switch there we have to create VLAN manually using user interface because console command option not work.

Configuration for Ethernetswitch_1:

We create here VLAN 30 and VLAN 40. We connect this switch with ESW3 using port e6 and e7 (VLAN 30, VLAN 40), ESW5 using port e2 (VLAN 40) and with Employee_3 network for which create the VLAN 30 (192.168.45.254), Management network VLAN 40 (192.168.50.254). This two network use this VLAN as their default gateway.

Employee_1 && Employee_3 Network:

This networks are create for employee of organization. From this networks employee can take service only from DMZ server as general user and Admin. They can't access in Data-center and network devices from this networks.

Administration Network:

This network is create only for administration. They can access both in DMZ server and Data center as Admin. But they can't access in network devices to configure it from this network.

Management Network:

We can call this network super powerful. Because from this network we can access everywhere in our private network. We can access in network devices to configure it and in DMZ server and Data-center as Admin.

Part 5–Data Center:

The flowing figure 4.6 shows how to configure Data Center.

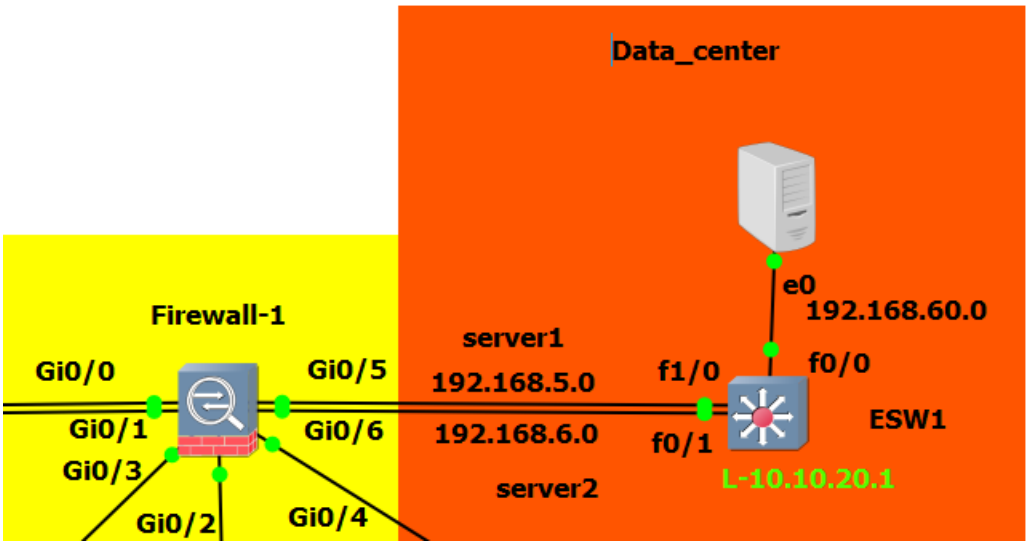


Figure 4.6: Data Center

To configure Data Center we use a Layer-3 switch ESW1 and a Data server desktop. This is height secure and very sensitive part in our topology. Only Administration and Management network can access here.

ESW1:

We connect ESW1 with Firewall-1 using the port FastEthernet1/0 and FastEthernet0/1 (IP 192.168.5.2 and 192.168.6.2) and with Server using the port FastEthernet0/0 (IP 192.168.60.1). We set Loopback IP 10.10.20.1 with Loopback interface.

This Layer-3 switch ESW1 is route using OSPF routing protocol. The route network

- 192.168.60.0
- 192.168.5.0
- 192.168.6.0
- 10.10.20.0

To implement this part of topology need 380 MB RAM for Layer-3 switch and 2048 MB RAM to run Server.

4.2 Interaction Design and UX:

The flowing figure 4.7 shows the interaction of our network topology.

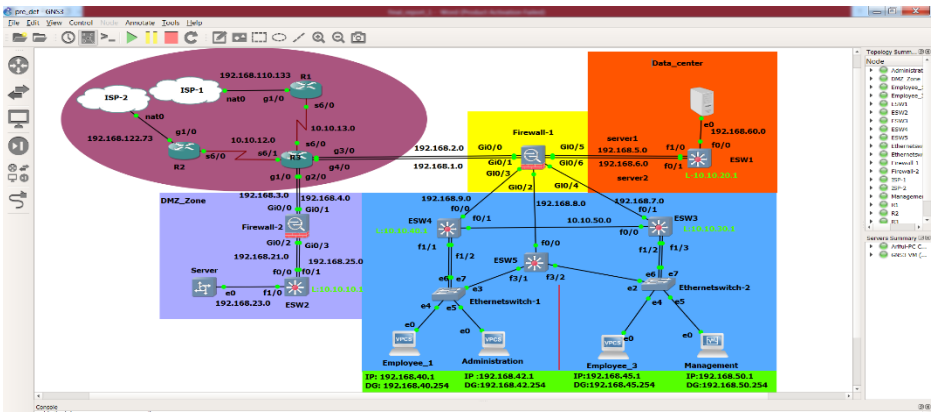


Figure 4.7: Network topology interaction design

In our topology there are four network for user in LAN.

i. Network 192.168.40.0 and 192.168.45.0 for employee user. From this two network user can access on DMZ server.
ii. Network 192.168.42.0 for Administration. This network user can access in DMZ server and Data Center as admin.
iii. Network 192.168.50.0 for Management. From this network the whole topology can control and configure the network devices. They can access both in DMZ and Data Center.

All LAN user can access each other network to communicate. We configure our LAN network to make it user friendly.

4.3 Implementation Requirements:

We configure this project using GNS3 software in a desktop PC which required

- 16 GB RAM, core i5 processor and operating system Windows 7
- Need GNS3 software and GNS3 VM
- Need software VMware to run GNS3 VM for creating GNS3 server
- Need VirtualBox software to run server
- Windows 7 OS, Windows server 2012 OS
- ASAv971 Firewall OS
- Cisco7200 Router Image, Cisco3745 Layer-3 switch Image.

CHAPTER 5

Implementation and Testing

5.1 Implementation of Topology:

The flowing figure 5.1 shows the whole network topology that we are going to implement.

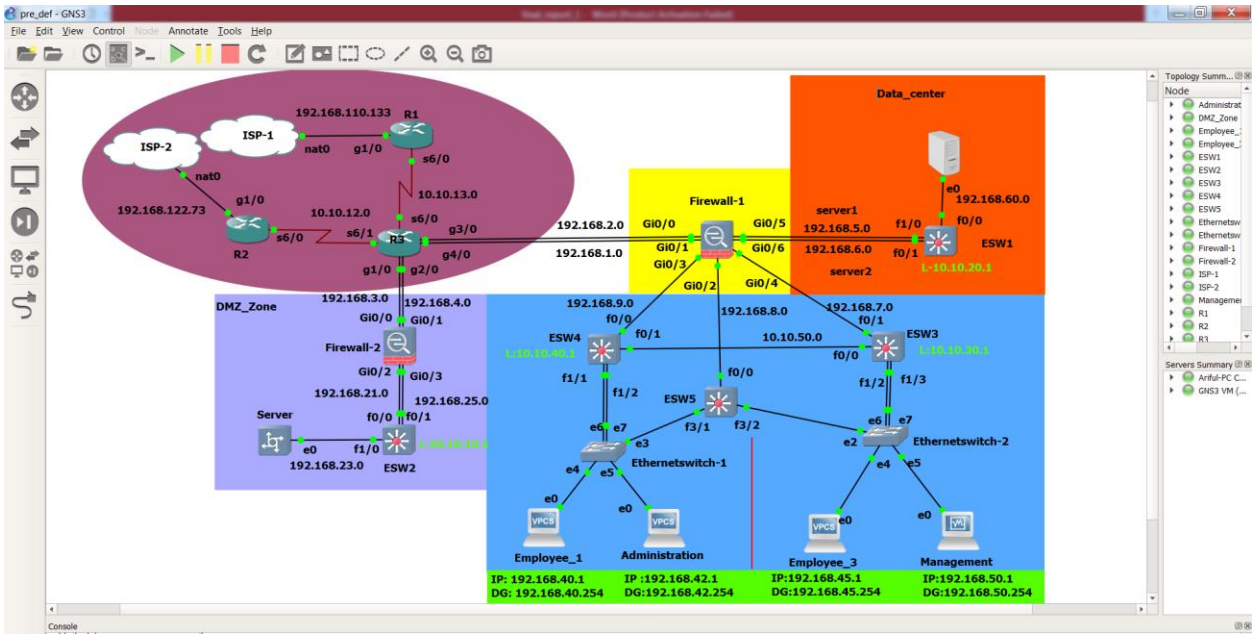


Figure 5.1: Network topology

5.1.1 Router and ISP Implementation:

Router R1 implementation

Router R1 Interface configuration:–

First we have to select the interfaces that are used. Then give the IP addresses and link up.

R1# config t

R1(config)# interface serial6/0

R1(config-if)# ip address 10.10.13.1 255.255.255.0

R1(config-if)# no shutdown

R1(config-if)#exit

R1(config)# interface Gi1/0

R1(config-if)# ip address dhcp

R1(config-if)# no shutdown

R1(config-if)#exit

Router R1 routing configuration:–

We used here OSPF routing protocol to route. There are two networks route in area 0.

R1(config)# router ospf 1

R1(config-router)# network 10.10.13.0 0.0.0.255 area 0

R1(config-router)# network 192.168.110.0 0.0.0.255 area 0

R1(config-router)#exit

Router R1 DNS configuration:–

To access internet severs we configured DNS.

R1(config)# ip domain-lookup

R1(config)# ip name-server 8.8.8.8 8.8.8.4

Router R3 implementation

Router R3 Interface configuration:–

R3 is very sensitive for our protocol because it connect our whole topology with each other. Here six interfaces are configured with IP address and linkup. Interface se6/0 connect with R1, se6/1 connect with R2, Gi1/0 and Gi3/0 connect with DMZ firewall, Gi2/0 and Gi4/0 connect with FireWall-1.

R3# config t

R3(config)# interface serial6/0

R3(config-if)# ip address 10.10.13.2 255.255.255.0

R3(config-if)# no shutdown

```
R3(config-if)#exit
R3(config)# interface serial6/1
R3(config-if)# ip address 10.10.12.2 255.255.255.0
R3(config-if)# no shutdown
R3(config-if)#exit
R3(config)# interface Gi1/0
R3(config-if)# ip address 10.10.3.1 255.255.255.0
R3(config-if)# no shutdown
R3(config-if)#exit
R3(config)# interface Gi2/0
R3(config-if)# ip address 10.10.1.1 255.255.255.0
R3(config-if)# no shutdown
R3(config-if)#exit
```

Router R3 routing configuration:–

Here used OSPF routing protocol to route networks in area 0.

```
R3(config)# router ospf 1
R3(config-router)# network 10.10.13.0  0.0.0.255 area 0
R3(config-router)# network 10.10.12.0  0.0.0.255 area 0
R3(config-router)# network 192.168.1.0  0.0.0.255 area 0
R3(config-router)# network 192.168.2.0  0.0.0.255 area 0
R3(config-router)# network 192.168.3.0  0.0.0.255 area 0
R3(config-router)# network 192.168.4.0  0.0.0.255 area 0
R3(config-router)#exit
```

Router R3 DNS configuration:–

To pass outside internet severs here configure DNS.

```
R3(config)# ip domain-lookup
R3(config)# ip name-server 8.8.8.8 8.8.8.4
```

5.1.2 DMZ implementation:

Firewall-2 implementation

Firewall-2 Interface configuration:–

Interface Gi0/0 and Gi0/1 used to connect with router R3 where name is OUTSIDE, security level in 50. Interface Gi0/2 used to connect with ESW2 where name is INSIDE, security level is 0.

```
Firewall-2 > enable
Password:
Firewall-2# config t
Firewall-2(config)# interface g0/0
Firewall-2(config-if)# description link to R3
Firewall-2(config-if)# nameif  OUTSIDE
Firewall-2(config-if)# security-level 50
Firewall-2(config-if)# ip address 192.168.3.2 255.255.255.0
Firewall-2(config-if)# no shutdown
Firewall-2(config-if)# exit
Firewall-2(config)# interface g0/2
Firewall-2(config-if)# description link to ESW2
Firewall-2(config-if)# nameif  INSIDE
Firewall-2(config-if)# security-level 0
Firewall-2(config-if)# ip address 192.168.21.1 255.255.255.0
Firewall-2(config-if)# no shutdown
Firewall-2(config-if)# exit
```

Firewall-2 routing configuration:–

Here use routing protocol OSPF to route firewall in area 0.

```
Firewall-2(config)# router ospf 1
Firewall-2(config-router)# network 192.168.3.0 255.255.255.0 area 0
Firewall-2(config-router)# network 192.168.4.0 255.255.255.0 area 0
```

Firewall-2(config-router)# network 192.168.21.0 255.255.255.0 area 0

Firewall-2(config-router)# network 192.168.25.0 255.255.255.0 area 0

Firewall-2(config-router)# exit

Firewall-2 object & NAT configuration:–

In Firewall-2 object and NAT in configured to create link between inside and outside network of DMZ. Create object dmz and NAT OUSIDE and INSIDE.

Firewall-2(config)# object network dmz

Firewall-2(config-network-object)# subnet 192.168.23.0 255.255.255.0

Firewall-2(config-network-object)# nat (OUTSIDE,INSIDE) dynamic interface

Firewall-2(config-network-object)#exit

Firewall-2 Access Lists (ACLs) configuration:-

Here we access object dmz to permit tcp, udp, icmp and also access this list group to interface INSIDE.

Firewall-2(config)# access-list dmz_acl permit tcp any object dmz

Firewall-2(config)# access-list dmz_acl permit udp any object dmz

Firewall-2(config)# access-list dmz_acl permit icmp any object dmz

Firewall-2(config)# access-group dmz_acl in interface INSIDE

Firewall-2 Application Inspection configuration:–

Firewall-2(config)# class-map inspection_default

Firewall-2(config-cmap)# match default-inspection-traffic

Firewall-2(config-cmap)#exit

Firewall-2(config)# policy-map global_policy

Firewall-2(config-pmap)# class inspection_default

Firewall-2(config-pmap-c)# inspect icmp

Firewall-2(config-pmap-c)#exit

Firewall-2(config)#service-policy global_policy global

Layer-3 switch (ESW2) implementation

ESW2 Interface configuration:–

Interface fa0/0 and fa0/1 connect with Firewall-2 and link up. Interface fa1/0 connect with server also setup a loopback 0 interface.

```
ESW2#config t
ESW2(config)# int fa0/0
ESW2(config-if)# ip address 192.168.21.2 255.255.255.0
ESW2(config-if)#no shutdown
ESW2(config-if)#exit
ESW2(config)# int fa1/0
ESW2(config-if)# ip address 192.168.23.1 255.255.255.0
ESW2(config-if)#no shutdown
ESW2(config-if)#exit
ESW2(config)# int loopback 0
ESW2(config-if)# ip address 10.10.10.1  255.255.255.0
ESW2(config-if)#no shutdown
ESW2(config-if)#exit
```

ESW2 routing configuration:–

Route the networks with OSPF protocol in area 0.

```
ESW2(config)# ip routing
ESW2(config)# router ospf 1
ESW2(config-router)# network 192.168.21.0  0.0.0.255 area 0
ESW2(config-router)# network 192.168.25.0  0.0.0.255 area 0
ESW2(config-router)# network 192.168.23.0  0.0.0.255 area 0
ESW2(config-router)# network 10.10.10.0  0.0.0.255 area 0
ESW2(config-router)# exit
```

Server implementation:

The flowing figure 5.2 shows how to set IP address in server.

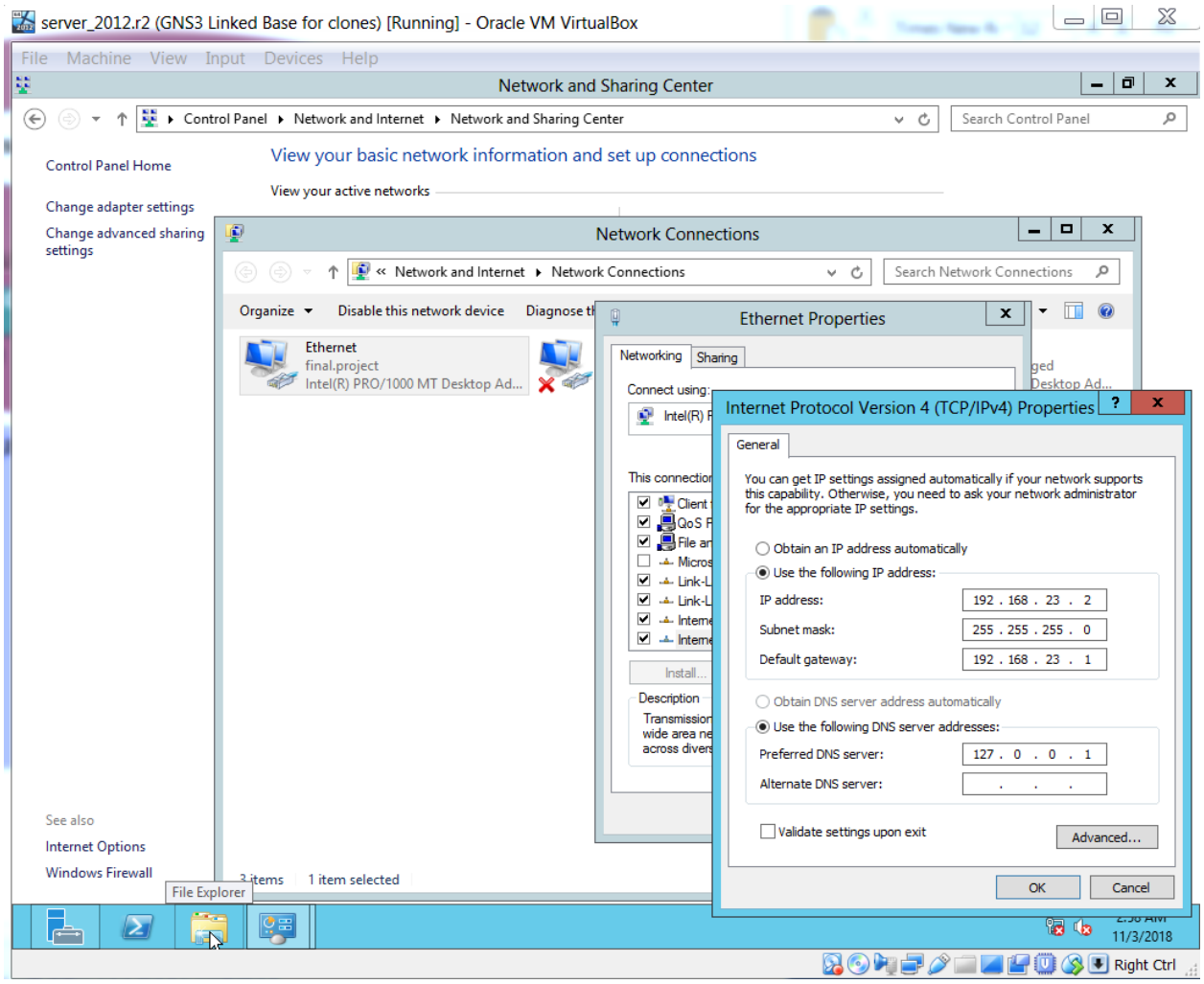


Figure 5.2: DMZ Server IP

The figure 5.2 show the process of server implementation set IP address to connect it with network.

5.1.3 Firewall-1 Implementation:

Firewall-1 Interface configuration:–

We use interface Gi0/0 and Gi0/1 to connect with router R3 which name is OUTSIDE and OUTSIDE2 with security level 0, interface Gi0/3, Gi0/4 and Gi0/2 with ESW4, ESW3 and ESW5 which name is INSIDE1, INSIDE2 and INSIDE3 with security level 100, interface Gi0/5 and Gi0/6 with ESW2 which name is SERVER, SERVER2 with security level 50.

```
Firewall-1 > enable
Password:
Firewall-1# config t
Firewall-1(config)# interface g0/0
Firewall-1(config-if)# description link to R3
Firewall-1(config-if)# nameif  OUTSIDE
Firewall-1(config-if)# security-level 0
Firewall-1(config-if)# ip address 192.168.2.1  255.255.255.0
Firewall-1(config-if)# no shutdown
Firewall-1(config-if)# exit
Firewall-1(config)# interface g0/3
Firewall-1(config-if)# description link to ESW4
Firewall-1(config-if)# nameif  INSIDE1
Firewall-1(config-if)# security-level 100
Firewall-1(config-if)# ip address 192.168.9.1  255.255.255.0
Firewall-1(config-if)# no shutdown
Firewall-1(config-if)# exit
Firewall-1(config)# interface g0/4
Firewall-1(config-if)# description link to ESW3
Firewall-1(config-if)# nameif  INSIDE2
Firewall-1(config-if)# security-level 100
Firewall-1(config-if)# ip address 192.168.7.1  255.255.255.0
Firewall-1(config-if)# no shutdown
Firewall-1(config-if)# exit
```

```
Firewall-1(config)# interface g0/2
Firewall-1(config-if)# description link to ESW5
Firewall-1(config-if)# nameif  INSIDE3
Firewall-1(config-if)# security-level 100
Firewall-1(config-if)# ip address 192.168.8.1  255.255.255.0
Firewall-1(config-if)# no shutdown
Firewall-1(config-if)# exit
Firewall-1(config)# interface g0/5
Firewall-1(config-if)# description link to ESW1
Firewall-1(config-if)# nameif  SERVER
Firewall-1(config-if)# security-level 50
Firewall-1(config-if)# ip address 192.168.5.1  255.255.255.0
Firewall-1(config-if)# no shutdown
Firewall-1(config-if)# exit
```

Firewall-1 routing configuration:–

Use OSPF routing protocol to route the firewall networks in area 0.

```
Firewall-1(config)# router ospf 1
Firewall-1(config-router)# network 192.168.1.0 255.255.255.0 area 0
Firewall-1(config-router)# network 192.168.2.0 255.255.255.0 area 0
Firewall-1(config-router)# network 192.168.5.0 255.255.255.0 area 0
Firewall-1(config-router)# network 192.168.6.0 255.255.255.0 area 0
Firewall-1(config-router)# network 192.168.7.0 255.255.255.0 area 0
Firewall-1(config-router)# network 192.168.8.0 255.255.255.0 area 0
Firewall-1(config-router)# network 192.168.9.0 255.255.255.0 area 0
Firewall-1(config-router)# exit
```

Firewall-1 object & NAT configuration:–

Here we create object dmz for DMZ sever, mz for Data Center, emp1 and emp2 for Employee, adm and adm1 for Administration, mgm and mgm1 for Management. Configure

NAT between interfaces INSIDE1 and OUTSIDE, INSIDE2 and OUTSIDE, INSIDE3 and SERVER.

```
Firewall-1(config)# object network dmz
Firewall-1(config-network-object)# subnet 192.168.23.0 255.255.255.0
Firewall-1(config-network-object)#exit
Firewall-1(config)# object network mz
Firewall-1(config-network-object)# subnet 192.168.60.0 255.255.255.0
Firewall-1(config-network-object)#exit
Firewall-1(config)# object network emp1
Firewall-1(config-network-object)# subnet 192.168.40.0 255.255.255.0
Firewall-1(config-network-object)# nat ( INSIDE1,OUTSIDE) dynamic interface
Firewall-1(config-network-object)#exit
Firewall-1(config)# object network adm
Firewall-1(config-network-object)# subnet 192.168.42.0 255.255.255.0
Firewall-1(config-network-object)# nat ( INSIDE1,OUTSIDE) dynamic interface
Firewall-1(config-network-object)#exit
Firewall-1(config)# object network mgm
Firewall-1(config-network-object)# subnet 192.168.50.0 255.255.255.0
Firewall-1(config-network-object)# nat ( INSIDE2,OUTSIDE) dynamic interface
Firewall-1(config-network-object)#exit
Firewall-1(config)# object network adm1
Firewall-1(config-network-object)# subnet 192.168.42.0 255.255.255.0
Firewall-1(config-network-object)# nat ( INSIDE3,SERVER) dynamic interface
Firewall-1(config-network-object)#exit
Firewall-1(config)# object network mgm1
Firewall-1(config-network-object)# subnet 192.168.50.0 255.255.255.0
Firewall-1(config-network-object)# nat ( INSIDE3,SERVER) dynamic interface
Firewall-1(config-network-object)#exit
```

Firewall-1 Access Lists (ACLs) Configuration:-

We create access list dmz_aclc_in for dmz and mz for object emp1, emp2, adm, adm1, mgm, mgm1 with tcp, udp and icmp mode. Give access permission goup of dmz_aclc_in to INSIDE1 and INSIDE2 and group of mz_acl to INSIDE3.

Firewall-1(config)# access-list dmz_aclc_in permit tcp object emp1 object dmz

Firewall-1(config)# access-list dmz_aclc_in permit udp object emp1 objcet dmz

Firewall-1(config)# access-list dmz_aclc_in permit icmp object emp1 object dmz

Firewall-1(config)# access-list dmz_aclc_in permit tcp object amd object dmz

Firewall-1(config)# access-list dmz_aclc_in permit udp object amd objcet dmz

Firewall-1(config)# access-list dmz_aclc_in permit icmp object amd object dmz

Firewall-1(config)# access-list dmz_aclc_in permit tcp object emp2 object dmz

Firewall-1(config)# access-list dmz_aclc_in permit udp object emp2 objcet dmz

Firewall-1(config)# access-list dmz_aclc_in permit icmp object emp2 object dmz

Firewall-1(config)# access-list dmz_aclc_in permit tcp object mgm object dmz

Firewall-1(config)# access-list dmz_aclc_in permit udp object mgm objcet dmz

Firewall-1(config)# access-list dmz_aclc_in permit icmp object mgm object dmz

Firewall-1(config)# access-list mz_acl permit tcp object amd1 object mz

Firewall-1(config)# access-list mz_acl permit udp object amd1 objcet mz

Firewall-1(config)# access-list mz_acl permit icmp object amd1 object mz

Firewall-1(config)# access-list mz_aclc permit tcp object mgm1 object mz

Firewall-1(config)# access-list mz_acl permit udp object mgm1 objcet mz

Firewall-1(config)# access-list mz_acl permit icmp object mgm1 object mz

Firewall-1(config)# access-group dmz_aclc_in interface INSIDE1

Firewall-1(config)# access-group dmz_aclc_in interface INSIDE2

Firewall-1(config)# access-group mz_acl interface INSIDE3

Firewall-1 Application Inspection configuration:–

Firewall-1(config)# class-map inspection_default

Firewall-1(config-cmap)# match default-inspection-traffic

Firewall-1(config-cmap)#exit

Firewall-1(config)# policy-map global_policy

Firewall-1(config-pmap)# class inspection_default

Firewall-1(config-pmap-c)# inspect icmp

Firewall-1(config-pmap-c)#exit

Firewall-1(config)#service-policy global_policy global

5.1.4 LAN Implementation:

ESW4 Implementation

ESW4 Interface configuration:–

First we select the interfaces which ports are used. Then configure them with IP address and link up to create connection.

ESW4#config t

ESW4(config)# int fa0/0

ESW4(config-if)# ip address 192.168.9.2 255.255.255.0

ESW4(config-if)#no shutdown

ESW4(config-if)#exit

ESW4(config)# int fa0/1

ESW4(config-if)# ip address 10.10.50.1 255.255.255.0

ESW4 (config-if)#no shutdown

ESW4(config-if)#exit

ESW4 VLAN configuration:–

We create vlan 10 and vlan 20 for employee and administration network and access them in interface f1/1 and f1/2.

ESW4# vlan database

ESW4 (vlan)# vlan 10 name employee1

ESW4 (vlan)# vlan 20 name administration

ESW4 (vlan)# exit

```
ESW4#config t
ESW4(config)# int vlan 10
ESW4(config-if)# ip address 192.168.40.254  255.255.255.0
ESW4(config-if)#no shutdown
ESW4(config-if)#exit
ESW4(config)# int vlan 20
ESW4(config-if)# ip address 192.168.42.254  255.255.255.0
ESW4(config-if)#no shutdown
ESW4(config-if)#exit
ESW4(config)# int f1/1
ESW4(config-if)#  switchport mode access
ESW4(config-if)#  switchport  access vlan 10
ESW4(config-if)#no shutdown
ESW4(config-if)#exit
ESW4(config)# int f1/2
ESW4(config-if)#  switchport mode access
ESW4(config-if)#  switchport  access vlan 20
ESW4(config-if)#no shutdown
ESW4(config-if)#exit
```

ESW4 routing configuration:–

We use OSPF routing protocol to route the networks in area 0.

ESW3 and ESW5 implementation

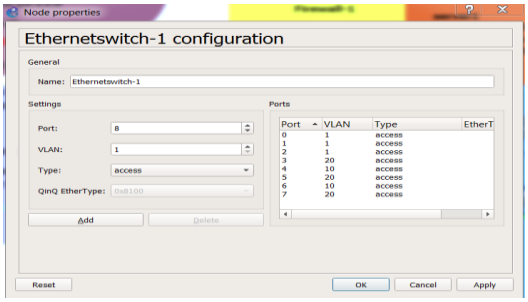
ESW3 and ESW5 implementation is same as ESW4.

In ESW3 we need to create vlan 30 for employee3 (IP 192.168.45.254) and vlan 40 for management (IP 192.168.50.254).

In ESW5 we need to create vlan 20 for administration (IP 192.168.42.254) and vlan 40 for management (IP 192.168.50.254).

Ethernetswitch1 and Ethernetswitch2 implementation

The flowing figure 5.3 and 5.4 shows the implementation of Ethernetswitch 1 &2



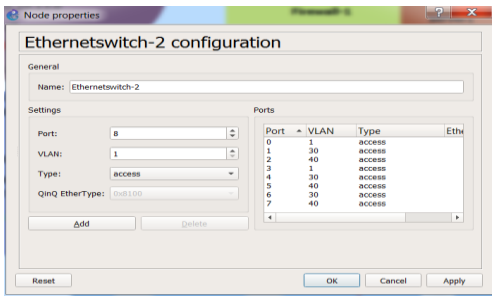


Figure 5.3: Ethernetswitch-1 configuration Figure 5.4: Ethernetswitch-2 configuration

PC IP address implementation

The flowing figure 5.5 shows how to set IP address and default gateway on PC

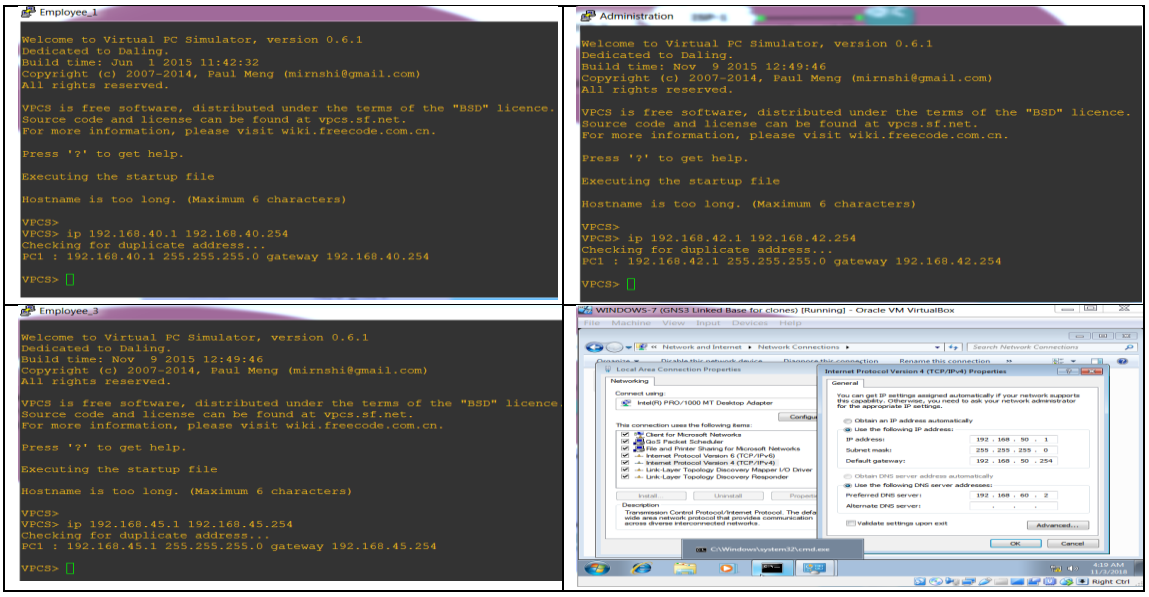


Figure 5.5: PC IP configuration

We set IP address on Management pc manually which process is shown on figure.

5.1.5 Data Center Implementation:

Layer-3 switch (ESW1) implementation

ESW1 Interface configuration:–

Here interface f1/0 configure to connect with Firewall-1 with IP address 192.168.5.2 and interface f0/0 to connect with server with IP address 192.168.60.1. Also configure Loop back 0 interface.

```
ESW1(config)# int loopback 0
ESW1(config-if)# ip address 10.10.20.1  255.255.255.0
ESW1(config-if)#no shutdown
ESW1(config-if)#exit
```

ESW1 routing configuration:–

We use here OSPF routing protocol to route the switch network in area 0.

Server implementation

The flowing figure 5.6 shows how to set IP address in Data Center server.

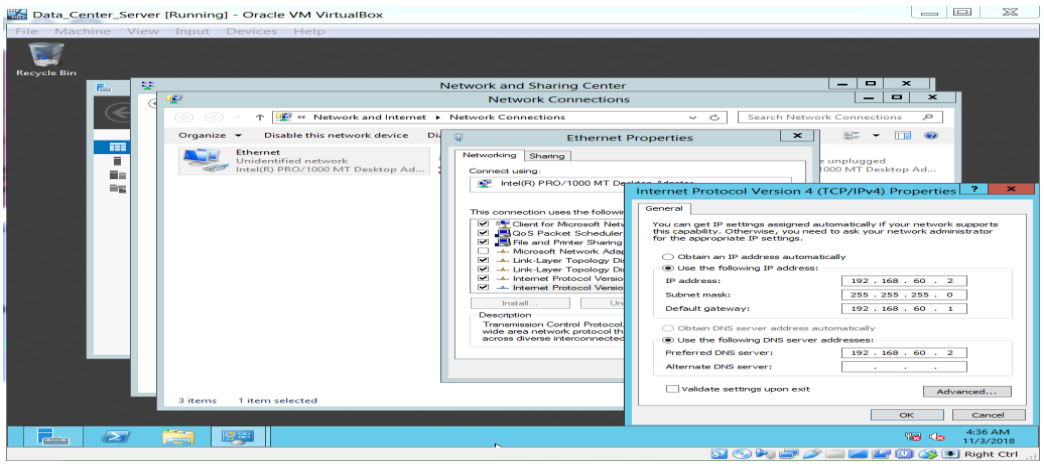


Figure 5.6: Data Center server

We configure the Data center server manually which process is shown in figure.

5.2 Testing Implementation

5.2.1 Router Implementation testing

Router R1:-

The flowing figure 5.7 shows R1 configuration that implement.

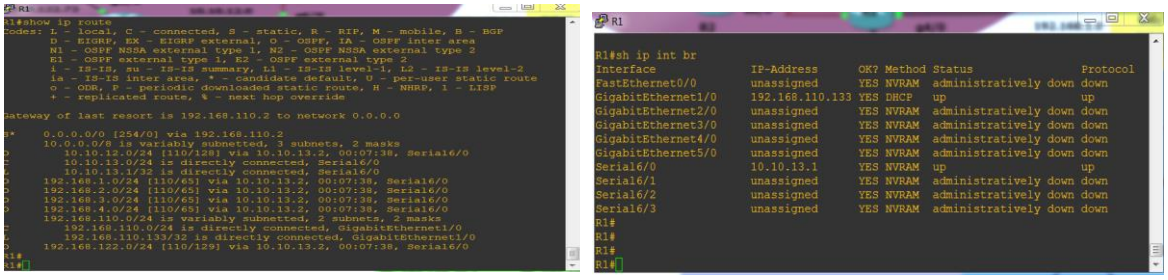


Figure 5.7: Router R1 implementation testing

Form the figure we can see all implementation of router work successfully.

5.2.2 Firewall-1 & Firewall-2 Implementation testing

Firewall-1:-

The flowing figure 5.8 shows Firewall-1 configuration that implement.

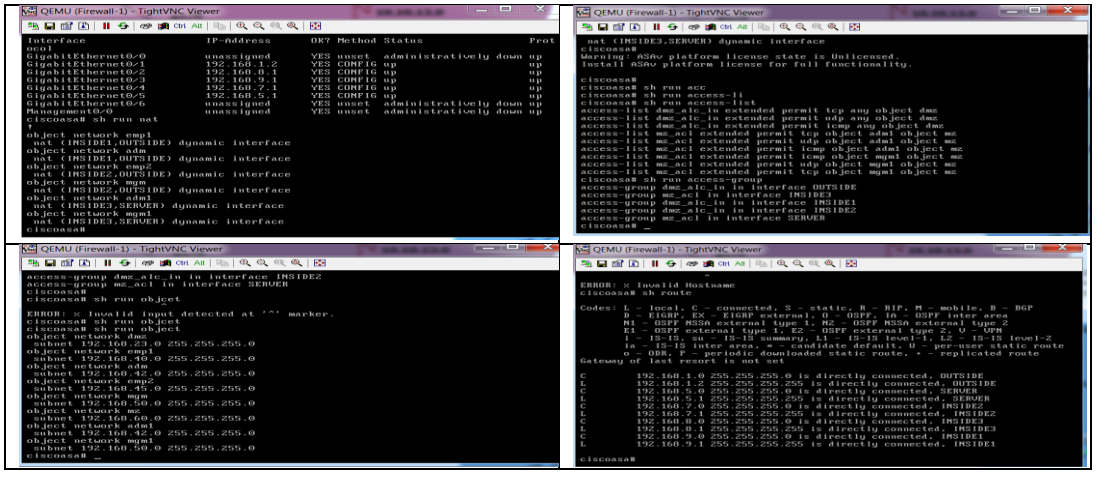


Figure 5.8: Firewall-1 implementation testing

From the figure which has taken from gns3 software screenshot we can see all configuration in successfully implement. All the interfaces are showing their IP addresses and routing network.

Firewall-2:-

The flowing figure 5.9 shows Firewall-2 configuration that implement.

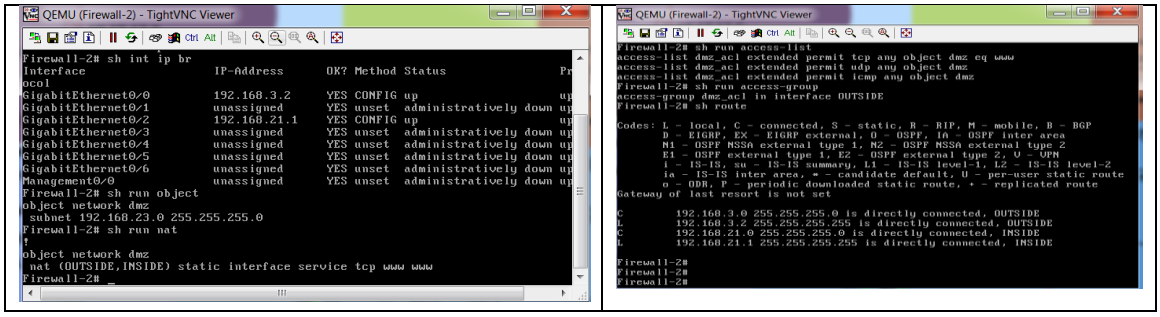


Figure 5.9: Firewall-2 implementation testing

As Firewall-1 we can see all configuration of Firewall-2 also implement successfully.

5.2.3 Layer-3 Switches Implementation Testing

ESW1:-

The flowing figure 5.10 shows ESW1 configuration that implement.

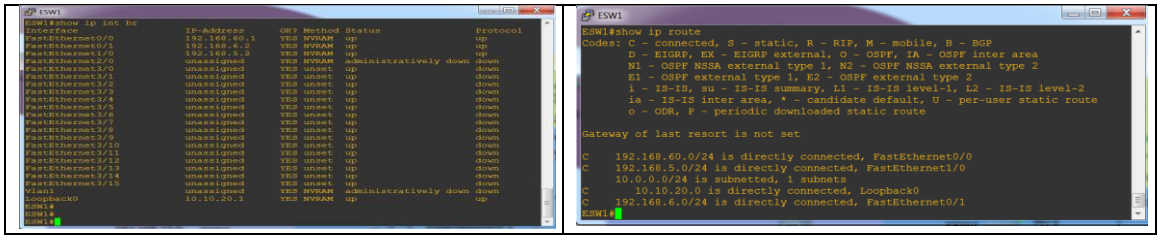


Figure 5.10: ESW1 implementation testing

From the figure we can see IP addresses and routing is successfully implement in L3switch.

5.3 Test Results and Report

5.3.1 Employee Network Test:-

The flowing figure 5.11 shows the employee network test result

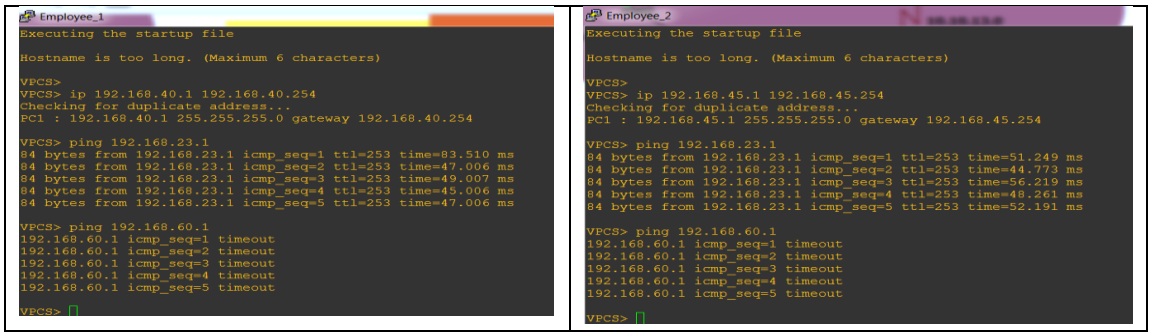


Figure 5.11: Employee network test

From the figure we can see Employee network can access only on DMZ server, can't access on Data center. So, Employee network implementation is successful.

5.3.2 Administration & Management Network Test:-

The flowing figure 5.12 shows the Administration & Management network test result.

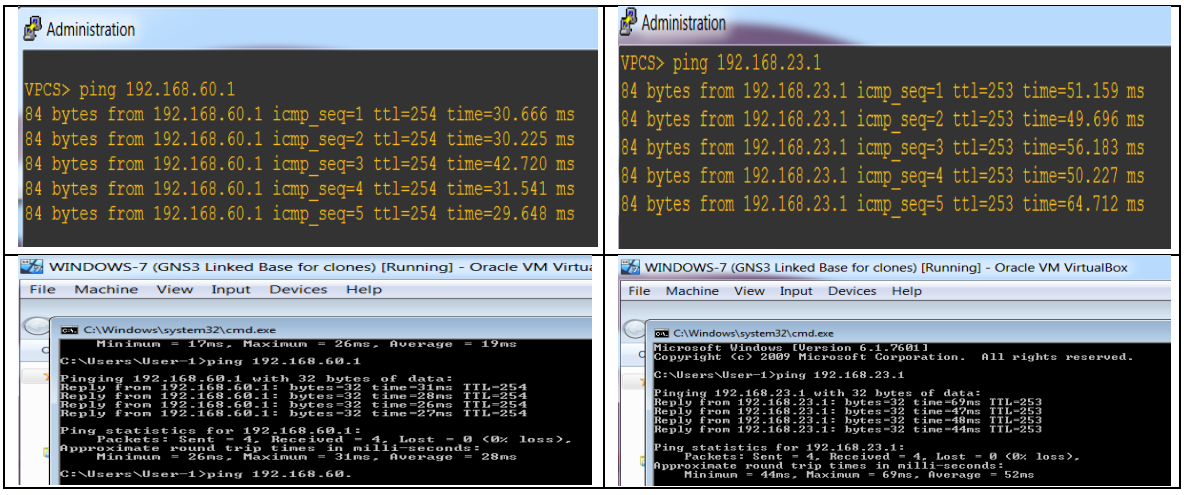


Figure 5.12: Administration & Management network test

We can see that Administration and Management network can access both on DMZ server and Data center. So, their network implementation is successful.

5.3.3 Result report:-

Form the figures we can see that all the devices of our topology implement successfully and working perfect.

Employee network can access DMZ server, Administration and Management network can access both in DMZ server and Data-center. So, the result report is perfect as we expect.

5.4 Impact of DMZ and Firewall:

Firewall is the protector of designed Topology network. We use one firewall to create DMZ server and another to protect our LAN and Data-center. Without firewall we can't create DMZ in the private network it protect our DMZ server from Cyber-attack.

After testing our result we can say that our DMZ and Firewall both are working perfectly.

CHAPTER 6

Conclusion and Future Scope

6.1 Discussion and Conclusion:

This project is very challenging for us to develop. We face many problem to complete this network topology because we use the latest network devices. Latest network devices command are different from old versions. Our topology is not for small organization. It will be very costly to develop this topology in our real life network. To develop this project we have to buy two Cisco ASA Firewall, three Cisco Router, Five Cisco Layer-3 / multilayer switches, two Ethernet-switches, two server (one for DMZ and another for Data center). This is very costly to develop but topology will be highly secure. The network system of this topology can managed very easily. This topology can be used in bank, Govt. agency, Multi-national Company.

After a long research and hard work with bless of Allah we have developed our project. We thanked them who help us to complete this project. We give our best for this project. We develop this project to show that there is no limitation of security in this internet network world. Day by day new way of Cyber-crime will come and on the other hand the way of protecting network will be changed to face this crime.

6.2 Scope for Further Developments:

We design our topology only for Main office of an organization. There are many scope for further developments this topology:

i. Here can connect the branches network topologies of the organization.
ii. Can install more network devices to trace the LAN user.
iii. Here can develop an option to use ipv6 with ipv4.
iv. Can install more server both on DMZ and Data-center.

Reference:

[1] *S D Hubbard and J C Sager, "Firewalling the Net", BT Technol J, Vol 15, No 2, April 1997.*

[2] *Akbar Iskandar, Elisabet Virma and Ansari Saleh Ahmar, "Implementing DMZ in Improving Network Security of Web Testing in STMIK AKBA", International Journal of Engineering & Technology, 7 (2.3) (2018) 99-104.*

[3] *Baha Rababaha, Shikun Zhoub and Mansour Baderc, "Evaluation the Performance of DMZ", I.J. Wireless and Microwave Technologies, 1, 1-13 Published Online January 2018 in MECS.*

[4] *M. KHAN, "Computer security in the human life," Int. J. Comput. Sci. Eng., vol. 6, no. November, 2017.*

[5] *S. Shrimali, "DeMilitarized Zone : Network Architecture for Information Security," Int. J. Comput. Appl., vol. 174, no. 5, pp. 16–19, 2017.*

[6] *S. Dandamudi and T. Eltaeib, "Firewalls Implementation in Computer Networks and Their Role in Network Security," J. Multidiscip. Eng. Sci. Technol., vol. 2, no. 3, pp. 408–411, 2015.*

[7] H. Liu, "Design and Implementation of Computer Network Vulnerability Assessment System," in 5th International Conference on Computer, Automation and Power Electronics, 2017, pp. 145–149.

[8] 'Cisco IOS software solutions', <<http://www.cisco.com/warp/public/732/index.html>>, last accessed on 12-10-18 at 11.00 pm.

[9] 'Cisco PIX Firewall', <<http://www.cisco.com/cpropub/univercd/ciscopro/catalog/cppix.html>>, last accessed on 02-11-18 at 10.43 pm.

[10] 'GNS3 software and GNS3VM', << https://www.gns3.com/>>, last accessed on 03-07-2018 at 9.25 pm.

[11] 'VMware software', << https://www.vmware.com/in.html>>, last accessed on 03-07-2018 at 9.53pm.

[12] 'VirtualBox software', << https://www.virtualbox.org/ >>, last accessed on 03-07-2018 at 10.30pm.

[13] 'Windows OS and Windows server solution', << https://www.microsoft.com/en-us/ >>, last accessed on 05-11-2018 at 9.20pm.